PERFORMANCE ANALYSIS OF A RELIABLE AODV ROUTING PROTOCOL IN MANETs

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
In
Computer Science and Engineering

Submitted By
Mona Gupta
(Roll No. 801132016)

Under the supervision of
Dr. Neeraj Kumar
Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

June 2013

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Performance Analysis of a Reliable AODV Routing Protocol in MANETs"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Computer Science and Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of **Dr. Neeraj Kumar** and refers other researcher's work which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for award of any other degree of this or any other University.

Mona Gupta
(Mona Gupta)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Neeraj Kumar)
Assistant Professor
Department of Computer
Science and Engineering

Countersigned by:

06/06/13.

(Dr. Maninder Singh)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. K. Mohapatra)
Dean (Academic Affairs)
Thapar University
Patiala

Acknowledgement

First of all I would like to thank the Almighty, who has always guided me to work on the right path of the life.

This work would not have been possible without the encouragement and able guidance of my supervisor **Dr. Neeraj Kumar.** I thank my supervisor for their time, patience, discussions and valuable comments. Their enthusiasm and optimism made this experience both rewarding and enjoyable.

I am equally grateful to **Dr. Maninder Singh**, Associate Professor and Head, Computer Science & Engineering Department, for motivation and inspiration that triggered me for the thesis work.

I will be failing in my duty if I don't express my gratitude to **Dr. S. K. Mohapatra,** Senior Professor and Dean of Academic Affairs the University, for making provisions of infrastructure such as library facilities, computer labs equipped with net facilities, immensely useful for the learners to equip themselves with the latest in the field.

I am also thankful to the entire faculty and staff members of Computer Science and Engineering Department for their direct-indirect help, cooperation, love and affection, which made my stay at Thapar University memorable.

Last but not least, I would like to thank my parents for their wonderful love and encouragement, without their blessings none of this would have been possible. I would also like to thank my brother, since they insisted that I should do so. I would also like to thank my close friends for their constant support.

Abstract

Ad hoc network is a subset of wireless networks that allows the mobile stations to dynamically form a temporary network and carry out the communication without a fixed centralized infrastructure. There are a number of routing protocols proposed till date in order to make routing more efficient and effective. The most prominent routing protocols include the Ad Hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR) and Destination Sequenced Distance Vector routing (DSDV).

In this work, an attempt has been made to introduce a new routing protocol in the mobile ad hoc networks called the Reliable ad Hoc On-Demand Distance Vector (RAODV) routing protocol, which is reactive and tries to make routing time efficient and resource saving. The work mainly focuses on reliability factor which is individually associated with each mobile workstation. Further, the proposed model is compared with an existing shortest path determination model which shares the similar platform of being on-demand driven. The performance is evaluated using different scenarios. The results presented in the thesis focus on analyzing the performance of RAODV and illustrate the importance in deploying RAODV routing protocol in the ad hoc networks.

Table of Contents

List of Figures

List of Tables

Abbreviations

ABR	Associativity Based Routing
AODV	Ad Hoc On-demand Distance Vector Routing
BQ	Broadcast Query
CGSR	Clusterhead Gateway Switch Routing
DRP	Distance Routing Protocol
DSDV	Destination Sequenced Distance Vector Routing
DSR	Dynamic Source Routing
GSR	Global State Routing
HSR	Hierarchical State Routing
IARP	IntrAzone Routing Protocol
IERP	IntErzone Routing Protocol
LAN	Local Area Network
MAC	Medium Access Control
MANET	Mobile Ad Hoc NETworks
MN	Mobile Node
MRL	Message Retransmission List
MPR	MultiPoint Relays
OLSR	Optimized Link State Protocol
P2P	Peer-to-Peer
QoS	Quality-of-Service
RAODV	Reliable AODV
RDMAR	Relative Distance Micro-discovery Ad Hoc Routing
RIP	Routing Information Protocol
RPGM	Reference Point Group Mobility
SRP	State Routing Protocol
SSR	Signal Stability based adaptive Routing
SST	Signal Stability Table

TORA Temporally Ordered Routing Algorithm

WRP Wireless Routing Protocol

ZRP Zone Routing Protocol

Chapter 1
Introduction

1.1 Background

Wireless communication is becoming prominent than ever before. The Ad Hoc Network (a special case of wireless networks) is an infrastructure less network where the nodes (having equal status or designation) communicate directly to one another and those having different status communicate via some intermediate nodes [1], thus each of the node in the network forwards its packet for the peer nodes and the end to end flow traverses many of the hops of the wireless links from the source to the destination. Also, the network is decentralized where the discovery of topology and delivering of messages is executed by nodes themselves and they automatically forms and conforms to change. Thus, the ad hoc networks are flexible and rapidly deployed; at the same time possess some epochal technical challenges [2]. With the restricted transmission range of wireless network interfaces, a number of network hops may be necessary for one node to exchange data with another across the network. There are number of characteristics in wireless ad-hoc networks, such as the network topology, bandwidth and energy limitations in the network. Mobile ad hoc network is useful for many different purpose e.g. military operations for providing communication between squads, emergency case in out-of-the-way places, medical control and many more areas [3]. A path between two mobile nodes in ad hoc networks can be made by either one or multiple hops. Therefore, there could be many changes in the network topology caused due to the mobility of the mobile nodes. Thus it becomes important to choose the routes wisely. In order to perform this task efficiently, there are many on-demand routing protocols that have been developed. All existing on-demand routing protocols uses one or the other technique to effectively establish a path between a pair of source and destination and send the packets accordingly.

Routing protocols play very vital role in the implementation of mobile ad hoc networks. Because of the characteristics of mobile ad hoc networks it is a non-trivial problem to determine a route from the source to the destination and carry out the communication between the nodes for a long period of time. Routing protocols are used whenever delivered data packets need to be handed over various intermediate nodes to arrive at the destinations. Routing protocols have to determine paths for packet delivery and make sure the packets are delivered to the correct exact destinations. The routing protocols such as distance vector routing and link-state routing were originally designed for static, wired networks and dynamic topology are not considered now. The Routing Protocols for ad hoc networks can be classified into

various types according to different criteria's which may include the static or dynamic protocols, centralized or distributed protocols, and pro-active, re-active or hybrid protocols [4].

1.2 Problem Description

The objective of this thesis is to evaluate the performance of a Reliable Ad hoc On-demand Distance Vector (RAODV) routing protocol which simulates the concept of Ad hoc On-demand Distance Vector (AODV) routing protocol. RAODV routing protocol associates each node with a unique value called its reliability factor and on the basis of this reliability factor, an appropriate reliable path or route is determined from a given source to the destination. Further the performance of the routing protocol is compared with an existing protocol that uses the shortest path determination between a pair of source and destination. The evaluation of the RAODV routing protocol is done theoretically and through simulation. The thesis also included the goals and objectives to produce a simulation environment that could be used as a platform for further studies within the area of ad-hoc networks.

The various goals of the thesis include:

- Awareness and understanding of the basic concepts of mobile ad hoc networks.
- Producing a scenario of routing that can be used to carry out future work.
- Deploy the existing routing protocol in wireless ad hoc networks and compare its performance with the proposed one.
- Carry out the performance analysis of the protocols theoretically as well as through simulation.
- Suggest different routing protocols for different network scenarios.

1.3 Related Work

There are various routing protocols that have been proposed till date in order to successfully route the packets from the source to the destination. All of them are suitable to one or more network scenarios. Also few comparisons between the different protocols have been made in order to determine the following features:

- **Robustness**: It must be able to recover and reconfigure quickly.
- **Efficiency**: It should make a minimum number of transmissions to deliver a packet.
- **Control overhead**: It demands minimal control overhead.
- **Quality of service**: QoS support is essential.

- **Efficient group management** needs to be performed with minimal exchange of control messages.
- **Scalability**: It should be able to scale for a large network

The various ad hoc routing protocols have been implemented in different simulation scenarios, of which work done by the protocols to find optimum path in [5] has compared some of the different proposed routing protocols and evaluated them based on the same quantitative metrics.

1.4 Disposition

This thesis is organized into the following divisions:

Chapter 2- Gives a review of ad hoc networks and its routing protocols in general.

Chapter 3- Specify the problem statement and what is new in the proposed work.

Chapter 4- Explains the Proposed model and its implementation.

Chapter 5- Analyze the experiments performed and evaluates the results achieved.

Chapter 6– Concludes the report and provides some suggestion for future work.

Chapter 2
Background Information and Literature Review

2.1 Wireless ad-hoc networks

2.1.1 General Concepts

A Mobile Ad hoc NETwork (MANET) [6] is a collection of mobile nodes which act as both a host and a router, and thus exchange data dynamically without relying on any fixed base station. The transmissions of packets take place via the intermediate nodes within a specified range that does certain functions on its received data. The application areas of MANET include emergency search, battlefield, acquiring data and rescue sites in distant areas, sharing data dynamically in conventions and classrooms by mobile computing devices [7]. An ad-hoc network is a Local Area Network (LAN) that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of messages to each node in the network, the individual network nodes forward packets to and from each other. In Latin, ad hoc literally means "for this," meaning "for this special purpose" The idea of an ad hoc network is sometimes also called an infrastructure-less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. Ad hoc network begins with at least two nodes broadcasting their presence (beaconing) with their respective address information. They may also include their location information if GPS is equipped, beaconing messages are control messages. If node A is able to establish a direct communication with node B verified by appropriate control messages between them, they both update their routing tables. Some examples of the possible use of ad hoc networks include students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information for situational awareness on the battlefield, and emergency disaster relief personnel coordinating efforts after a hurricane or earthquake. Therefore an ad hoc network is said to be a self-organizing and adaptive methodology that allows spontaneous formation and deformation of mobile networks [8]. Here, each mobile host acts as a router and supports peer-to-peer communications and peer-to-remote communications. There is reduced administrative cost and ease of deployment.

The following figure represents an ad hoc network which does not consist of a fixed infrastructure and each node in the network acts as a router itself.

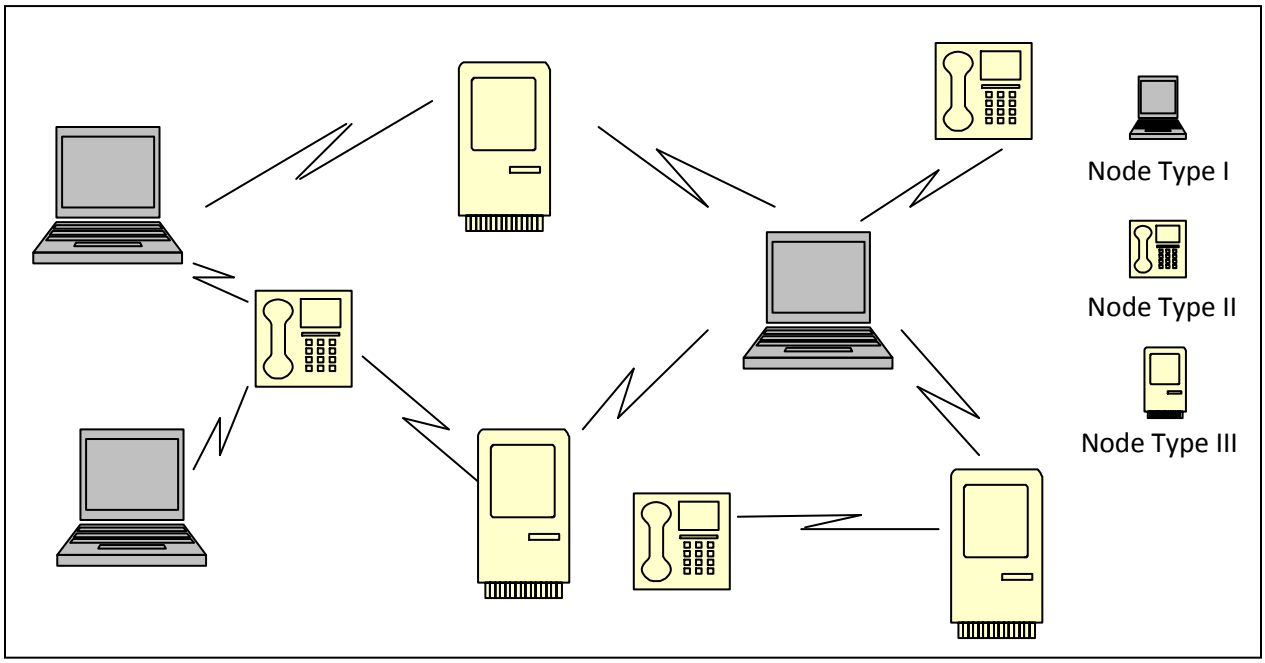


Figure 2.1: Infrastructure-less Communication in Ad hoc Networks.

2.2.2 Characteristics

There are multiple features of ad hoc networks; several of them are discussed below:

- **Infrastructure-less:** Fixed infrastructure is a pre-defined topology that features static connectivity and is not altered for the entire lifetime of a connection. Therefore, a fixed infrastructure is directly proportional to the factors like the mobility of nodes, change of power, change of node etc…Internet, cellular networks and wireless LANs possess such infrastructures. Ad hoc networks have no fixed infrastructure which makes their deployment easy and fast. The connectivity in the ad hoc networks could be featured by a graph via a connectivity topology (which is time varying) at any time instant.
- **Multi-hop wireless links:** A multi-hop ad hoc wireless network is a collection of nodes that have wireless transceivers and that provide store-and-forward functionalities on top of the physical and medium access protocols in use, as needed to enable multihop wireless communications. Such nodes can thus be classified as routers in the resulting wireless network. The important characteristics of these multi hop wireless links include the asymmetry, time-variation, non-transitivity. When defining what a link is in a multi-hop wireless network, first identify which link model may be suitable [9].

- **Shared radio channel:** The ad hoc networks are also featured by a common shared radio channel which is more suitable for best-effort data traffic. Therefore, the nodes could communicate with one another even if they possess just one common shared channel. This property allows the multiple pair of nodes to communicate or transmit at the same time. The shared channel in the ad hoc networks remarkably reduces the waiting time to access the channel and therefore enhancing the utilization of the common shared channel and the connectivity in the network.
- **Distributed Routing:** The ad hoc network is characterized by distributed routing, where the route between a pair of nodes is determined by a distributed computation during which the control messages are exchanged in between the nodes. The state information which is kept at each node is collectively utilized to find a route. A distributed routing process is used to prevent any centralized path computation that could be very expensive for the quality of service routing in the large networks. In the distributed routing, it is not mandatory for any node to maintain the topology information. The frequent topology is used during the hop-by-hop route selection process [10].
- **Packet Switched:** The Packet switching in ad hoc networks allows the nodes to disseminate the information in the network by means of context-aware packet switching which allows the statistical multiplexing of bandwidth, processing and storage of the resources utilizing integrated signaling covering channel access, routing and other functions, that share and store the context within which information is disseminated. Data packet headers consist of simple pointers to their context, and elections and opportunistic reservations integrated with routing are used to attain high throughput and low channel-access delay. The packet switching in ad hoc networks is further evolving toward emulation of circuit switching [11].
- **Quick and cost-effective deployment:** The ad hoc networks are also featured by their quick and cost-effective implementation. As each node in the network is independent so the transmission or communication is done quickly. No centralized authority makes it easy for each node to quickly deploy itself. Further, the overall cost only includes the expenses of nodes participating in the network. The nodes not participating do not contribute to the overall cost.
- **Dynamic frequency reuse based on carrier sense mechanism:** The wireless local area network specifications are intended to give a shared medium access and radio signaling support for ad hoc

networks. Carrier sensing could reduce the number of packet collisions in the ad hoc network. The carrier sensing range is an important factor that could essentially affect the MAC performance in multihop ad hoc networks. It balances between the amount of spatial frequency reuse and the probability of packet collisions. Hence, it must be carefully chosen, based on network parameters such as network topology, traffic pattern, and transceiver power [12].

- **Bandwidth reservation requires complex medium access control protocols:** As the wireless network is a tightly controlled medium, it has restricted channel bandwidth which is actually much less than the bandwidth of wired networks, also the wireless medium is inherently error prone. Although the radio may have sufficient channel bandwidth, parameters such as multiple accesses, signal fading, and noise and interference can cause the effective throughput in wireless networks to be essentially low. Since the nodes are mobile, the network topology changes more frequently without any predictable pattern. Ad hoc network nodes conserve energy as they mostly rely on batteries as their power source [13].
- **Self-organization and maintenance properties are built into the network:** Self-organization is a spontaneous procedure where some form of global order or coordination emerges out of the local interactions between the nodes of an initially disordered system. In the aspect of ad hoc networks, the nodes in a given network are self-organized with no pre-defined centralized authority for management. As the nodes are independent so the properties of maintenance and self-organization are in-built within the nodes to carry out a long smooth communication process.
- **Mobile hosts require more intelligence:** The communication in ad hoc networks is carried out without a central authority to manage all nodes at one place. Therefore, it becomes mandatory for the host in the network to have more intelligence to carry out a fault free communication. It should possess the capabilities of a transceiver as well as routing/switching. The host in the network is more intelligent and responsible for transmitting, reception and routing processes for an effective communication.
- **Minimum routing overhead and quick reconfiguration of broken paths:** The main aim of routing in the ad hoc networks is to find paths with minimum overhead and also quick reconfiguration of broken paths. The several algorithms and data structures are deployed in order to find the optimum path between a pair of nodes intended for communication. Also, to

reconfigure from the broken path, several schemes are implemented within the algorithms for finding the optimum route from a given source to the destination.

2.1.3 Applications

The application domain of the ad hoc networks includes tremendous fields, some of which are discussed below [14]:

- **Military Applications:** The ad hoc network is used for establishing communication among a group of soldiers for tactical operations. To provide with the coordination of military object moving at high speeds such as fleets of airplanes or ships, it requires reliability, efficiency, secure communication, and multicasting routing. Ad hoc networks have the capability to provide all such features for the military applications. In most of the cases, military operations are often spontaneous i.e. with little or no fixed network infrastructure. In comparison with geographical positioning systems, mobile ad-hoc networks can support the built-in geographical location by using an extremely accurate form of triangulation. This feature enables soldiers in a military operation to triangulate its position based on the mobile enabled vehicles or other devices. In mobile ad hoc networks, readings are faster than the geographical positioning systems because the soldiers don't have to wait for multiple satellites to acquire a centralized security. The devices must be able to address both communications security and a way to secure the network from unauthorized use. Mobile ad hoc networks also allow devices to transmit at a lower output power to the neighbors which benefits the over-all network by lowering the probability of detection and by increasing the battery. Therefore if the device is captured, the soldiers can list that device to maintain the integrity of the network.
- **Collaborative and Distributed Computing:** A group of people in a conference can share data in ad hoc networks. The ad hoc networks provide the streaming of multimedia objects among the participating nodes. Distributed file sharing is also one of the major applications where people or organizations from different areas share the common information. Ad hoc networks are applicable where the need for collaborative computing is more important outside the office environment than inside, such as in a business meeting outside the office to brief clients on a given assignment.

- **Emergency Operations:** The ad hoc networks support real-time and fault-tolerant communication paths which are dependent on search, rescue, crowd control, and commando operations. Further, for the disaster recovery process, replacement of fixed infrastructure in case of environmental disasters, policing and fire-fighting and supporting doctors and nurses in hospitals all are common applications of ad hoc networks in case of emergencies.
- **Commercial and civilian environments**: Ad hoc networks are used in e-commerce for electronic payments anytime and anywhere, in business for dynamic database access, mobile offices, in vehicular services for road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks, and in sports stadiums, trade fairs, shopping malls, network of visitors at airports.
- **Entertainment**: The ad hoc network provide with the multi-user games (multi-person decision making where each decision maker tries to maximize his utility), wireless P2P networking, outdoor Internet access, robotic pets, theme parks.
- **Sensor networks**: Ad hoc networks are used in home applications: smart sensors and actuators embedded in consumer electronics, body area networks, and data tracking of environmental conditions, animal movements, and chemical/biological detection.

2.1.4 Challenges of Ad Hoc Mobile Networks [14]

- **Changing the network topology over time**: Due to lack of a fixed infrastructure, network topology may change from time to time depending on the characteristics of nodes. The changing topology may alter various static features of the network.
- **Potentially frequent network partitions:** As the network is not centralized, therefore the communication between different-different pair of nodes in the network lead to various partitions of the network.
- **Every node can be mobile:** In an ad hoc network, every node can be mobile acting as a transmitter; receptor and routing at the same time which is further a challenge to deal with. Management of such nodes is also challenging.

- **Limited power capacity:** Power is a critical parameter for the design and evolution of ad hoc networks. Further, with the restricted power capacity it becomes challenging to carry out the communication process.
- **Limited wireless bandwidth:** The nodes with the limited bandwidth and battery resources might be reluctant to forward data packets for other nodes, unless there is an additional mechanism in place to give an incentive to provide this service.
- **Presence of varying channel quality:** In ad-hoc networks, the channel quality is time-varying and it is affected by fading, path loss and interference. Thus, it becomes challenging to manage the varying channel quality.
- **No centralized entity–distributed:** The network is decentralized where the discovery of topology and delivering of messages is executed by nodes themselves and they automatically forms and conforms to change. Thus, the ad hoc networks are flexible and rapidly deployed; at the same time possess some epochal technical challenges
- **Routing:** It becomes a challenging issue to route the packets from a given source to the destination in an environment where there is not pre-defined infrastructure. Various protocols are deployed day by day to handle the routing scenarios and determine an optimum path.
- **Mobility:** The mobility of nodes makes it challenging to design various models (random way point model, manhattans model, reference point group model) that can handle the issues.
- **Power Conservancy:** Due to the limited power available, it becomes a necessity to conserve the power in order to make it available for the future scenarios. Power conserving yields a long term utilization of the available resources which is again a challenging task.
- **Moving routers:** As the nodes itself act as routers, and mobility of nodes mean the mobility of router, it thus becomes a challenging work to route a packet to its destination.
- **Link changes are happening quite often:** In the ad hoc networks, due to a given transmission range of a node, link changes keep on happening occasionally.
- **Packet losses due to transmission errors:** The mobility of nodes may lead to certain errors in transmission called the transmission faults. Handling the packets losses due to these errors are challenging issues as the reliability of the network is then questioned.

- **Event updates are sent often**: Due to lack of a centralized infrastructure, event updates are sent very often leading to a lot of control traffic and to manage such traffic is a cumbersome task to deal with.
- **Routing table management**: Due to the existence of routing loop in between the path from source to destination, the routing table may not be able to converge. Further, in order to manage such tables which possess mobility itself is a challenging issue.
- **Distributed channel access:** With no fixed base station concept it becomes a difficult task to access the distributed channel which may lead to fading, path loss or interference.
- **Battery technology is not progressing as fast as memory or CPU technologies:** The power constraints are not permitting the battery technology to progress because unless there is a proper power conservancy, battery is unable to compete with the fast memories or cpu.
- **Wireless transmission, reception, retransmission, beaconing, consumes power:** As the nodes in the ad hoc network are acting as transmitters, receptors, routers and hosts at the same time instant consuming more power than the ordinary node that performs one job at a time, it becomes a challenging issue to manage such nodes in a network on very large scale.
- **Scalability:** Test beds and operational ad hoc networks made so far contain only a limited number of nodes and may not be good examples of ad hoc performance. The performance of ad-hoc network degrades drastically with the increase of the number of nodes and one may expect commercial realization of, at least, thousands of nodes.
- **Quest for power-efficient protocols:** There has always been a need for effective better protocols and better power management schemes. Many such protocols are designed and deployed in order to accomplish an efficient power management technique.
- **Deployment:** The deployment of ad-hoc network has the benefits like low cost (no cables, no configuration, no maintenance);incremental (functioning starts immediately after minimum configuration is done); short time (no cables, no configuration, no maintenance); re-configurability (no cables, no configuration, no maintenance).
- **Quality of service provisioning**: Effect of service performance determining the degree of satisfaction of a user of the service in the ad hoc network. It uses values of traffic engineering variables that constitute the so-called Grade of Service.
- **Security:** The ad hoc networks are more vulnerable to attacks due to lack of central

coordination and shared wireless medium. To have a reliable and secure communication among the nodes in the network is again a challenge.

2.2 Routing and Conventional Routing Protocols

Routing is defined as traversing the data or information from a given source to the destination in a network consisting of a number of nodes. The routing protocols in ad hoc networks adjust quickly as topology changes. The essential characteristic of routing is finding an optimum path between a pair of nodes called source and destination. In order to determine this optimum route, important parameters undertaken include the minimum latency, proper utilization of available bandwidth, available power etc. and minimum number of hops. The source node is used to determine the entire path and intermediate nodes are used to forward the packets. In ad hoc networks, only the nodes within the transmission range in a given time can communicate with each other. The frequent mobility of the nodes can change the routes. The routing protocols in ad hoc network possess some qualitative and quantitative features [15].

Table 2.1: Properties of routing protocols.

Qualitative Features	Quantitative Features
Demand based routing (means when a node finds any disturbance in the predefined path then it calls route discovery function to find a new route and hence limiting the routing overhead).	Route Discovery Time (Time taken by a packet to discover the route to its destination)
Distributed Routing(any node in the network can join or leave the network Whenever it wants)	Memory Byte Requirement (To store the routing tables and other management tables)
Loop Free (Loop free routing for CPU utilization to increase the overall network performance)	Network Recovery Time (Time taken to settle down after some network collisions due to heavy load or communication may be broken due to heavy mobility of nodes)

Secure and Reliable (Various measure to protect a network from impersonation attacks. Authentication and encryption to ensure security)	Delay (Average time taken by a packet to reach its destination)
	End to End Throughput (number of successful packets received at the final destination per unit time)

Routing protocols for ad hoc networks can be classified into various categories [4] as per one of the following scheme.

- **Pro-active, re-active or hybrid**: A. Shrivastava [16] proposed that, in a proactive routing scheme (or table- driven routing), each node keeps the complete routing information of the network. This is obtained by flooding the network occasionally with update information and evaluating the known routes to determine the changes in topology. Hence, the delay of new path discovery is avoided because the path is already known to forward a packet. Maintaining such up-to-date information requires dense bandwidth and unlimited battery power in mobile ad hoc networks. Some of the examples [17] of pro-active protocols include Global State Routing (GSR), Hierarchical State Routing (HSR), and Destination Sequenced Distance Vector Routing (DSDV).

  The re-active protocols (on-demand protocols) initiate to discover a path on demand, means when a source wants to send information to its destination, the process does not need continuous updates being sent through the network because no routes are initially available. A route search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the route. Hence, delays are found here. Protocols such as DSR [18] and AODV [19] belong to the re-active protocol class.

  Hybrid protocols are globally reactive and locally proactive in nature. It is based on the fact that most communication in mobile ad hoc networks takes place between nodes that are close to each other, and the changes in topology are only essential when they happen in the vicinity of a node. Link failures affect only the local neighborhoods and not the global. Hybrid routing algorithm is ideal for Zone based Routing Protocol (ZRP) [20].

- **Centralized or distributed**: When a routing protocol is centralized, all the decisions are made by a central node, however in a distributed routing protocol, all the nodes cooperate in a symmetric way to reach a particular routing decision.
- **Static or Dynamic**: This strategy is based on the nature of the information used for the routing. A dynamic protocol changes its behavior according to the network status, which may have congestion. The protocol should discover these changes, automatically adjust its routing tables, and inform other routers of the changes. Static protocols do not change when the network status changes, the changes should be added manually.

The basic conventional routing protocols are:

2.2.1 Distance Vector Routing Protocol

K. Gorantala et al [19] proposed that in such protocols each node maintains a routing table containing the distance from itself to all the possible nodes. Hence, every entry contains the next hop to the destination and the distance to the destination. Every node determines the shortest paths to the destinations using the broadcasted information. Every router over the internetwork sends the neighboring routers, the information about destination that it knows how to reach. The protocol allows the nodes to forward the packets to the neighboring node (or destination) with the available shortest path in the routing table and assumes that the receiving node would know how to forward the packet beyond that point. The protocol is easier to implement as compared to other protocols and require less storage space. However, it can cause the formation of both short-lived and long-lived routing loops. The best example for such protocols is the Routing Information Protocol (RIP).

2.2.2 Link State

In link-state routing, every node keeps a check on the complete topology with a cost for each link. The costs are maintained by each node via broadcasting the link cost of its outgoing links to all other nodes. As each node gets this data, it updates its view of the network and applies a shortest path algorithm to select the next-hop for the destination. In such protocols, a router gives the information about the topology of the network which contains network segments and links. Such information is spread throughout the network and every node in the network then builds its own scenario of the current state of all the links in the network [19].

2.2.3 Source Routing

M. Steenstrup et al [18] proposed that in the Source Routing all data packets carry their routing information as their header. The nodes are provided with this routing information by a source routing protocol. Source routing means that every packet should carry the complete route it takes to reach destination. The routing decision is made at the source node. The protocol makes it possible to avoid routing loops but requires overhead for each packet.

2.2.4 Flooding

Flooding is a type of broadcasting where, in order to spread the control information broadcasts are used. Flooding means that a node sends out its information to all other neighbor nodes and they forward all received information to their neighbors and so on [18].

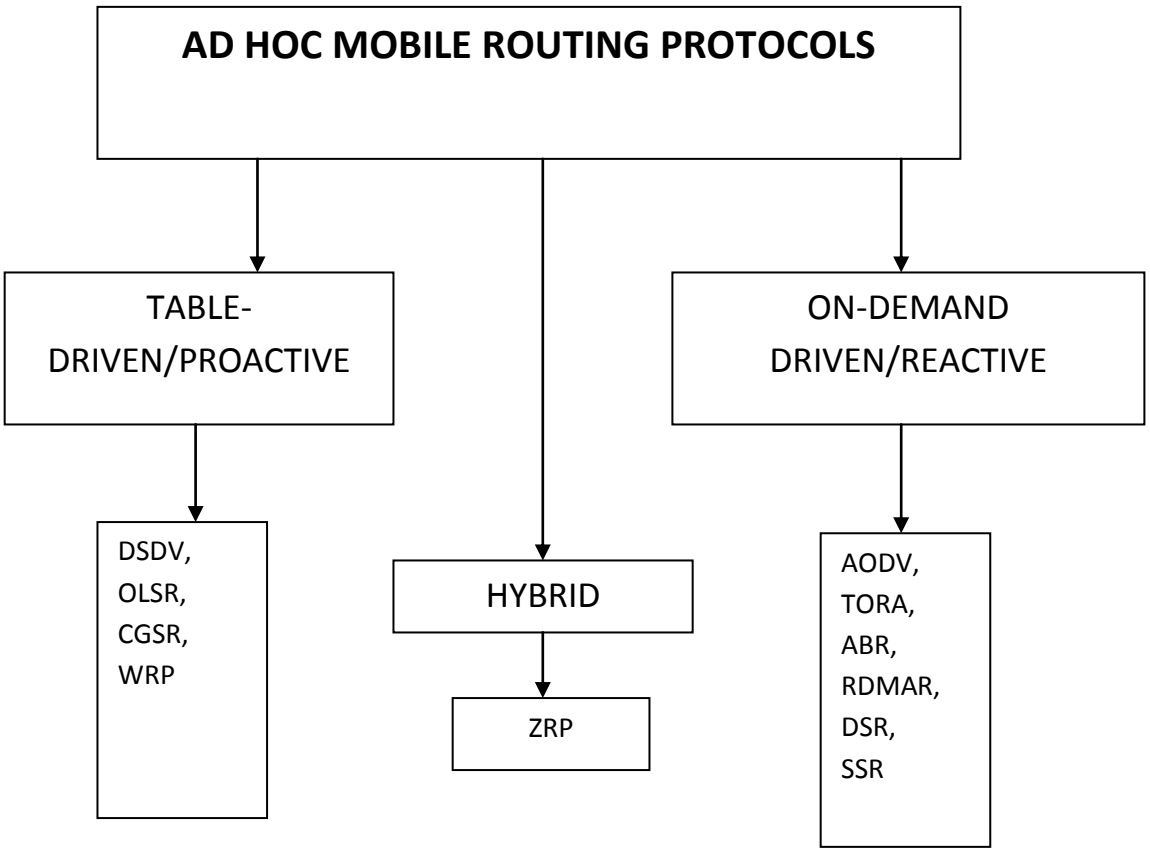


Figure 2.2: Routing Protocols.

2.3 Table Driven Protocols

2.3.1 Destination Sequenced Distance Vector Routing (DSDV)

G. He et al [21] proposed that DSDV routing is based on the idea of the classical Bellman-Ford Routing algorithm with certain improvements. DSDV is similar to Routing Information Protocol (RIP) of ad hoc networks routing where a new parameter called the sequence number is added to route table. In DSDV, each routing table of a mobile node of an ad hoc network contains lists all available destinations, the metric and next hop to each destination and a sequence number generated by the destination node. Therefore, these routing tables are used to transmit the packets between any pair of nodes. The nodes keep on updating their routing tables frequently with the essential data needed to maintain the consistency of the network and meet the changing topology of the ad hoc network.

Thus, each node periodically forwards routing table to neighbors and increments and appends its sequence number when sending its local routing table. Each route is tagged with a sequence number; routes with greater sequence numbers are preferred, each node advertises a monotonically increasing even sequence number for itself. When a node decides that a route is broken, it increments the sequence number of the route and advertises it with infinite metric. Destination advertises new sequence number. As the routing information is broadcast on the network, tables are exchanged between nodes at regular intervals (or significant change in local topology) and updates initiated by destination with a new sequence number. Node receives and updates this information automatically and waits for some time to ensure it has a route with lowest number of hops. Each node on receiving the update with weight quickly disseminates it to its neighbours. Therefore a single broken link propagates throughout the network.

The limitations of this protocol includes using too much bandwidth just to send messages, using control overhead proportional to the square of the number of nodes in the network, no very scalable in ad-hoc networks and the results are in stale routing information at nodes .

2.3.2 Optimized Link State Routing (OLSR)

P. Jacquet et al [22] proposed that OLSR falls under the class of proactive routing protocol and hence the routes are always available immediately when needed. OLSR is based on the link state protocol and is an optimized version for wireless networks taking into consideration the various issues in wireless data transmission. The topological changes in the mobile nodes cause the flooding of the topological

information to all available hosts in the network. To reduce the possible overhead in the network OLSR uses MultiPoint Relays (MPR) which reduces the flooding of broadcasts by reducing the same broadcast in some regions in the network. The reduction in the time interval for the control messages transmission can bring more reactivity to the topological changes which are a desired feature as it reduces the control message bandwidth utilization. Hello and Topology control are two types of control messages used in OLSR. Hello messages are used for finding the link status information and the immediate neighbors to the host. In an ad hoc network the link can be either bidirectional or unidirectional which is required by the host to know about its neighbors. The Hello messages are broadcasted periodically to check the presence of the neighbor. Hello messages are only broadcasted one hop away so that they are not forwarded further. When a node receives the Hello message from another node, it sets the host status to asymmetric in the routing table. When the first node sends a Hello message and includes that, it has the link to the second node as asymmetric, the second node set first node status to symmetric in its own routing table. Finally, when second node sends Hello message again, where the status of the link for the first node is indicated as symmetric, then first node changes the status from asymmetric to symmetric. In the end both nodes knows that their neighbor is available and the corresponding link is bidirectional [23].

2.3.3 Wireless Routing Protocol (WRP)

M. Steenstrup et al [18] proposed that WRP is a table-based distance-vector routing protocol. Each node in the network maintains a Distance table, a Routing table, a Link-Cost table and a Message Retransmission list.

The Distance table of a node x contains the distance of each destination node y via each neighbor z of x. It also contains the downstream neighbor of z through which this path is realized. The Routing table of node x contains the distance of each destination node y from node x, the predecessor and the successor of node x on this path. It also contains a tag to identify if the entry is a simple path, a loop or invalid. Storing predecessor and successor in the table is beneficial in detecting loops and avoiding counting-to-infinity problems. The Link-Cost table contains cost of link to each neighbor of the node and the number of timeouts since an error-free message was received from that neighbor. The Message Retransmission List (MRL) contains information to let a node know which of its neighbor has not acknowledged its update message and to retransmit update message to that neighbor.

Nodes exchange routing tables with their neighbors using update messages periodically as well as on link changes. The nodes present on the response list of update message (formed using MRL) are required to acknowledge the receipt of update message. If there is no change in routing table since last update, the node is required to send an idle Hello message to ensure connectivity. On receiving an update message, the node modifies its distance table and looks for better paths using new information. Any new path so found is relayed back to the original nodes so that they can update their tables. The node also updates its routing table if the new path is better than the existing path. On receiving an ACK, the mode updates its MRL. A unique feature of this algorithm is that it checks the consistency of all its neighbors every time it detects a change in link of any of its neighbors. Consistency check in this manner helps eliminate looping situations in a better way and also has fast convergence.

2.3.4 Clusterhead Gateway Switch Routing (CGSR)

V. U. Chezhian et al [24] proposed that CGSR uses as basis the DSDV Routing algorithm. The mobile nodes are aggregated into clusters and a cluster-head is elected. All nodes that are in the communication range of the cluster-head belong to its cluster. A gateway node is a node that is in the communication range of two or more cluster-heads. In a dynamic network cluster head scheme can cause performance degradation due to frequent cluster-head elections. Cluster-head change occurs only if a change in network causes two cluster-heads to come into one cluster or one of the nodes moves out of the range of all the cluster-heads. The general algorithm works in the following manner. The source of the packet transmits the packet to its cluster-head. From this cluster-head, the packet is sent to the gateway node that connects this cluster-head and the next cluster-head along the route to the destination. The gateway sends it to that cluster-head and so on till the destination cluster-head is reached in this way. The destination cluster-head then transmits the packet to the destination.

Each node maintains a cluster member table that has mapping from each node to its respective cluster-head. Each node broadcasts its cluster member table periodically and updates its table after receiving other node and broadcasts using the DSDV algorithm. In addition, each node also maintains a routing table that determines the next hop to reach the destination cluster. On receiving a packet, a node finds the nearest cluster-head along the route to the destination according to the cluster member table and the routing table. Then it consults its routing table to find the next hop in order to reach the cluster-head selected in step one and transmits the packet to that node.

2.4 On-demand Routing Protocols

2.4.1 Ad hoc On-demand Distance Vector (AODV)

C. E. Perkins et al [25] proposed that AODV routing protocol is a reactive, stateless, single path on-demand routing protocol for a MANET. The authors of AODV call it a pure on-demand routing protocol because the mobile nodes that are not on a selected path neither keep any routing information nor share any routing table information. The protocol works in two phases by discovering a route and maintaining a route. When a node (source) wants to send data to another node (destination), the route discovery phase is started to find the other node. The Route REQuest packet (RREQ) is broadcasted with a unique Route IDentification (RID) to all its neighbors. The broad cast is done till a sink is found or a node with new path to sink is known. All the neighbors make an entry in their routing table for the given RID. The Route REPly (RREP) packet is created when the destination node or an intermediate node with an acceptable route to destination has got the RREQ. The RREP will be a unicast in the reverse direction. When RREP is routed in reverse direction, nodes in this direction set up a forward direction entry in their routing tables that point to a node from which RREP came. There is another packet called the Route ERRor (RERR) packet. When a mobile node moves away, a link failure may happen in between the two nodes, the RERR packet is broadcasted in that case. The source may have to re-initiate discovering route to the desired destination. A HELLO message is exchanged in between the neighboring mobile nodes in order to give the information related to link status.

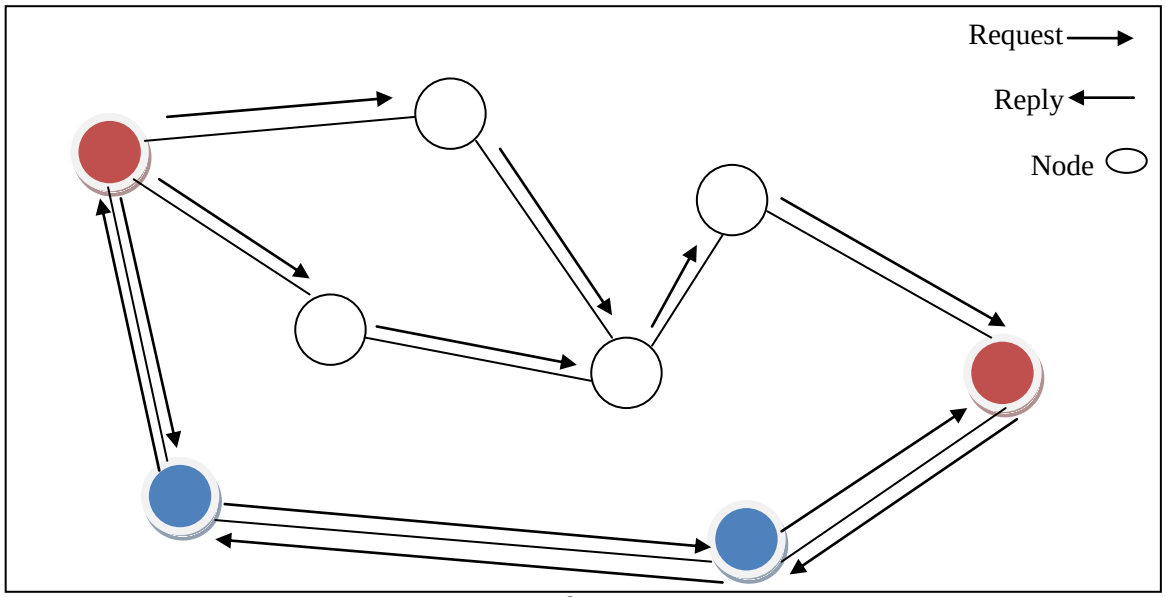


Figure 2.3: Path discovery from source to destination.

In order to find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has recent route information about the destination or till it reaches the destination.

A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only. When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source, the nodes along the path enter the forward route into their tables. If the source moves then it can reinitiate route discovery to the destination. If one of the intermediate nodes move then the moved nodes neighbor realizes the link failure and sends a link failure notification to its upstream neighbors and so on till it reaches the source upon which the source can reinitiate route discovery if needed.

The concepts of AODV that make it desirable for MANETs with limited bandwidth include the following:

- Minimal space complexity: The algorithm makes sure that the nodes that are not in the active path do not maintain information about this route. After a node receives the RREQ and sets a reverse path in its routing table and propagates the RREQ to its neighbors, if it does not receive any RREP from its neighbors for this request, it deletes the routing info that it has recorded.
- Maximum utilization of the bandwidth: This can be considered the major achievement of the algorithm. As the protocol does not require periodic global advertisements, the demand on the available bandwidth is less. And a monotonically increased sequence number counter is maintained by each node in order to supersede any stale cached routes. All the intermediate nodes in an active path updating their routing tables also make sure of maximum utilization of the bandwidth. Since, these routing tables will be used repeatedly if that intermediate node receives any RREQ from another source for same destination. Also, any RREPs that are received by the nodes are compared with the RREP that was propagated last using the destination sequence numbers and are discarded if they are not better than the already propagated RREPs.

- Simple: It is simple with each node behaving as a router, maintaining a simple routing table, and the source node initiating path discovery request, making the network self-starting.
- Most effective routing info: After propagating an RREP, if a node finds receives an RREP with smaller hop-count, it updates its routing info with this better path and propagates it.
- Most current routing info: The route info is obtained on demand. Also, after propagating an RREP, if a node finds receives an RREP with greater destination sequence number, it updates its routing info with this latest path and propagates it.
- Loop-free routes: The algorithm maintains loop free routes by using the simple logic of nodes discarding non better packets for same broadcast-id.
- Coping up with dynamic topology and broken links: When the nodes in the network move from their places and the topology is changed or the links in the active path are broken, the intermediate node that discovers this link breakage propagates an RERR packet. And the source node re-initializes the path discovery if it still desires the route. This ensures quick response to broken links.
- Highly Scalable: The algorithm is highly scalable because of the minimum space complexity and broadcasts.

2.4.2 Dynamic Source Routing (DSR)

P. Misra et al [18] [26] proposed that DSR Protocol is a source-routed on-demand routing protocol. A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as and when it learns about new routes.

The two major phases of the protocol are: route discovery and route maintenance. When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet. The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. To limit the number of route requests propagated, a node processes the route request packet only if it has not already seen the packet and it's address is not

present in the route record of the packet. A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet. A route request packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node. As the route request packet propagates through the network. If the route reply is generated by the destination then it places the route record from route request packet into the route reply packet. On the other hand, if the node generating the route reply is an intermediate node then it appends its cached route to destination to the route record of route request packet and puts that into the route reply packet. Following figure shows the route reply packet being sent by the destination itself. To send the route reply packet, the responding node must have a route to the source. If it has a route to the source in its route cache, it can use that route. The reverse of route record can be used if symmetric links are supported. In case symmetric links are not supported, the node can initiate route discovery to source and piggyback the route reply on this new route request.

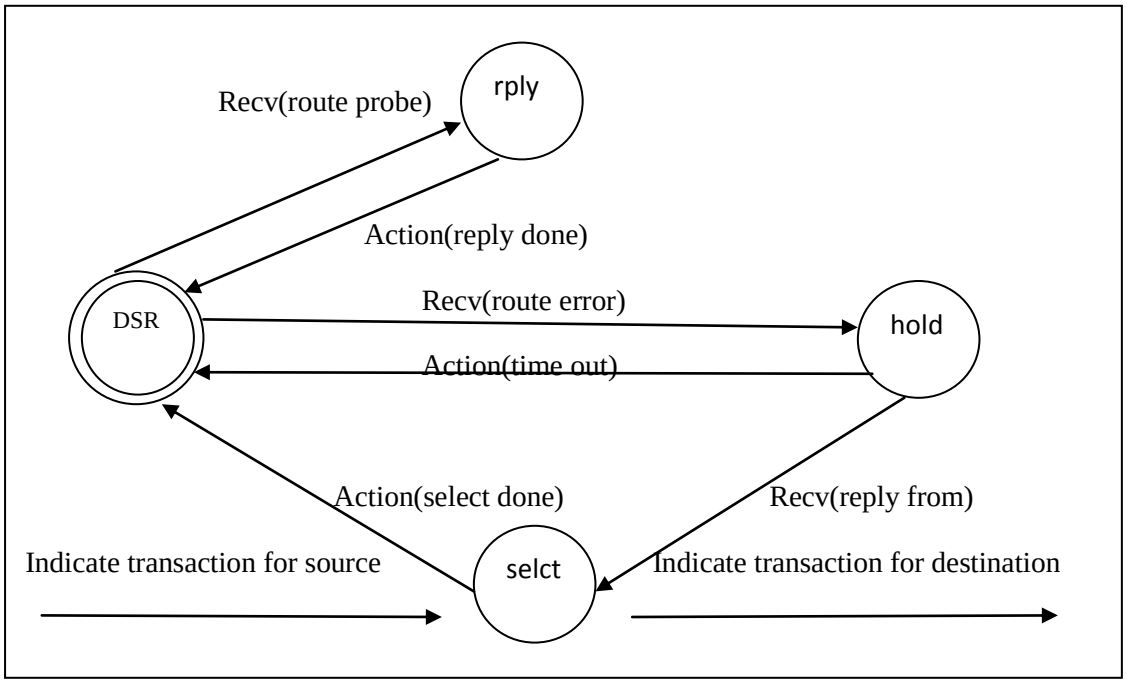


Figure 2.4: Transition diagram of DSR.

DSRP uses two types of packets for route maintenance: Route Error packet and Acknowledgements. When a node encounters a fatal transmission problem at its data link layer, it generates a Route Error packet. When a node receives a route error packet, it removes the hop in error from its route cache. All

routes that contain the hop in error are truncated at that point. Acknowledgment packets are used to verify the correct operation of the route links. This also includes passive acknowledgments in which a node hears the next hop forwarding the packet along the route.

2.4.3 Temporally-Ordered Routing Algorithm (TORA)

M. T. Toussaint et al [4][18][26] proposed that TORA is a distributed routing protocol based on a link reversal algorithm. It is designed to discover routes on demand, provide multiple routes to a destination, establish routes quickly, and minimize communication overhead by localizing the reaction to topological changes when possible. Route optimality (shortest-path routing) is considered of secondary importance, and longer routes are often used to avoid the overhead of discovering newer routes. It is also not necessary (nor desirable) to maintain routes between every source/destination pair at all times.

The actions taken by TORA can be described in terms of water flowing downhill towards a destination node through a network of tubes that model the routing state of the network. The tubes represent links between nodes in the network, the junctions of the tubes represent the nodes, and the water in the tubes represents the packets flowing towards the destination. Each node has a height with respect to the destination that is computed by the routing protocol. If a tube between two nodes becomes blocked such that water can no longer flow through it, the height of the nodes are set to a height greater than that of any neighboring nodes, such that water will now flow back out of the blocked tube and find an alternate path to the destination.

At each node in the network, a logically separate copy of TORA is run for each destination. When a node needs a route to a particular destination, it broadcasts a route query packet containing the address of the destination. This packet propagates through the network until it reaches either the destination, or an intermediate node having a route to the destination. The recipient of the query packet then broadcasts an update packet listing its height with respect to the destination (if the recipient is the destination, this height is 0). As this packet propagates back through the network, each node that receives the update sets its height to a value greater than the height of the neighbor from which the update was received. This has the effect of creating a series of directed links from the original sender of the query to the node that initially generated the update. When a node discovers that a route to a destination is no longer valid, it adjusts its height so that it is a local maximum with respect to its neighbors and transmits an update

packet. When a node detects a network partition, where a part of the network is physically separated from the destination, the node generates a clear packet that resets the routing state and removes invalid routes from the network. TORA is one of the largest and most complicated protocols. In terms of memory requirements, each node must maintain a structure describing the node's height as well as the status of all connected links per connection supported by the network. In terms of CPU and bandwidth requirements, each node must be in constant coordination with neighboring nodes in order to detect topology changes and converge.

2.4.4 Associativity Based Routing (ABR)

M. Steenstrup et al [18][26] proposed that ABR protocol is a new approach that defines a new metric for routing known as the degree of association stability. It is free from loops, deadlock, and packet duplicates. In ABR, a route is selected based on associativity states of nodes. The routes thus selected are liked to be long-lived. All nodes generate periodic beacons to signify its existence. When a neighbor node receives a beacon, it updates its associativity tables. For every beacon received, node increments its associativity tick with respect to the node from which it received the beacon. Association stability means connection stability of one node with respect to another node over time and space. A high value of associativity tick with respect to a node indicates a low state of node mobility, while a low value of associativity tick may indicate a high state of node mobility. Associativity ticks are reset when the neighbors of a node or the node itself move out of proximity. The fundamental objective of ABR is to find longer-lived routes for ad hoc mobile networks. The three phases of ABR are Route discovery, Route ReConstruction (RRC) and Route deletion.

The route discovery phase is a broadcast query and await-reply cycle. The source node broadcasts a Broadcast Query (BQ) message in search of nodes that have a route to the destination. A node does not forward a BQ request more than once. On receiving a BQ message, an intermediate node appends its address and its associativity ticks to the query packet. The next succeeding node erases its upstream node neighbors' associativity tick entries and retains only the entry concerned with itself and its upstream node. Each packet arriving at the destination will contain the associativity ticks of the nodes along the route from source to the destination. The destination can now select the best route by examining the associativity ticks along each of the paths. If multiple paths have the same overall degree

of association stability, the route with the minimum number of hops is selected. Once a path has been chosen, the destination sends a reply packet back to the source along this path. The nodes on the path that the reply packet follows mark their routes as valid. All other routes remain inactive, thus avoiding the chance of duplicate packets arriving at the destination.

2.4.5 Signal Stability-Based Adaptive Routing protocol (SSR)

R. K. Bansal et al [3][26] proposed that SSR is an on-demand routing protocol that selects routes based on the signal strength between nodes and a node's location stability. This route selection criterion has the effect of choosing routes that have stronger connectivity. SSR comprises of two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP). The protocol is characterized by the features like on-demand beacon-based protocol; routes are selected based on temporal stability of wireless links based on temporal stability, each links is classified as stable or unstable. It's used to determine temporal stability; each node measures the signal strength of beacons.

The whole protocols consist of the following two parts where the first one maintains the routing table interacting with other hosts and other part is responsible for forwarding of packets to destination. The DRP maintains the Signal Stability Table (SST) and Routing Table (RT). The SST stores the signal strength of neighboring nodes obtained by periodic beacons from the link layer of each neighboring node. Signal strength is either recorded as a strong or weak channel. All transmissions are received by DRP and processed. After updating the appropriate table entries, the DRP passes the packet to the SRP.

The SRP passes the packet up the stack if it is the intended receiver. If not, it looks up the destination in the RT and forwards the packet. If there is no entry for the destination in the RT, it initiates a route-search process to find a route. Route-request packets are forwarded to the next hop only if they are received over strong channels and have not been previously processed (to avoid looping). The destination chooses the first arriving route-search packet to send back as it is highly likely that the packet arrived over the shortest and/or least congested path. The DRP reverses the selected route and sends a route-reply message back to the initiator of route-request. The DRP of the nodes along the path update their RTs accordingly.

2.4.6 Relative Distance Micro-Discovery ad hoc routing (RDMAR)

D. Kumar et al [27][3] proposed that in the RDMAR protocol, calls are routed between the stations of

the network by using routing tables which are stored at each station of the network; each node is treated as a host as well as a store-and-forward node. Each routing table lists all available destinations, and the number of hops to each. Therefore, the routing table of each node is a column vector of maximum (N - 1) row entries, where N is the set of participating nodes in the network. Apart from the available destination addresses, additional information is maintained for each destination address D. This includes: the Default Router field that indicates the next hop node through which the current node can reach D, the RD field which shows an estimate of the Relative Distance (RD) (in hops) between the node and D, the Time Last Update (TLU) field that indicates the time elapsed since the node last received routing information for D, a RT Timeout field which records the remaining amount of time before the route is considered invalid, and a Route Flag field which declares whether the route to D is active. Thus the protocol reduce the routing overhead in the network, minimize the flooding effect by limiting route request to certain number of hops, used in Route Construction and Maintenance, do not require GPS and at the first time it works like normal flooding operation which means the route discovery will have global effect.

2.5 Hybrid Protocols

2.5.1 Zone Routing Protocol (ZRP)

J. Schaumann et al [20] proposed that the ZRP combines the advantage of both table driven and on-demand routing protocols by using the on-demand protocol globally and table-driven protocol locally. ZRP uses a pro-active protocol in the neighborhood of a node called the IntrAzone Routing Protocol (IARP) and a re-active protocol for routing between neighborhoods called the IntErzone Routing Protocol (IERP). The local neighborhoods are called zones and are different for every node. Each node could be present in multiple overlapping zones, which may all have different sizes. ZRP is not so much a distinct protocol as it provides a framework for other protocols. The separation of a nodes local neighborhood from the global topology of the entire network allows for applying different approaches and therefore taking advantage of each technique's features for a given situation. Therefore, the ZRP is not so much a distinct protocol as it provides a framework for other protocols. The separation of a nodes local neighborhood from the global topology of the entire network allows for applying different approaches – and thus taking advantage of each technique's features for a given situation. These local

neighborhoods are called zones (hence the name); each node may be within multiple overlapping zones, and each zone may be of a different size. The routing in ZRP is divided into two parts Intrazone routing (first, the packet is sent within the routing zone of the source node to reach the peripheral nodes) and the Interzone routing (then the packet is sent from the peripheral nodes towards the destination node).

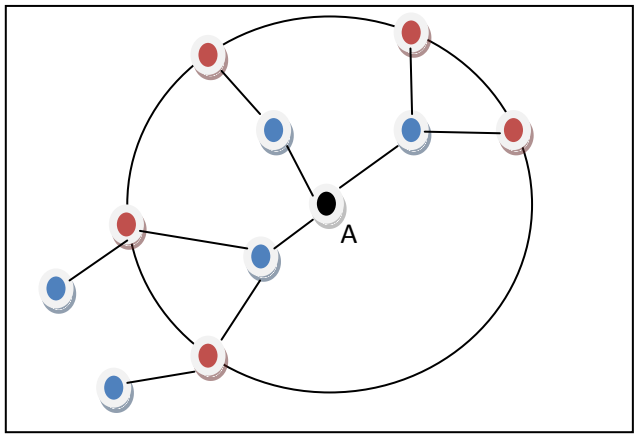


Figure 2.5: Routing Zone of node A.

Chapter 3

Problem Statement

There are different routing protocols in the wireless ad hoc networks that have their own advantages and disadvantages. Some of the routing protocols determine the optimum path between the source and the destination using the algorithms of the graph theory [5] that uses various metrics like shortest path for route optimization while other protocols [28] uses the statistical approaches in order to determine best suitable path.

Discussions in the literature review indicate that most of the existing routing protocols for ad-hoc network use one of the strategies which may be flat vs. hierarchical architecture or pro- active vs. re-active routing protocol or hybrid protocols [16]. The various performance metrics like packet delivery ratio, routing overhead, average end-to-end delay, average hop count, bandwidth, synchronization, transmission time, quality of service (QoS), network size, network scalability and mobility are considered in order to optimize the task of finding the path between the source and the destination.

This thesis presents a new approach for detecting the reliable path between a pair of source and destination. For this, it introduces a routing protocol that helps to generate the most reliable path between two nodes simulating the concepts of AODV routing protocol. Further, each node in the wireless ad hoc network has been associated with a reliability factor, based on which the protocol advances. By associating each node with a reliable value, the path chosen for the communication between two nodes becomes almost reliable and the chances of occurring of faults reduces. This algorithm is then compared with an existing algorithm that uses the dijkstra algorithm [29] for finding the shortest path between a pair of nodes where although the path chosen is shortest but the proposed algorithm over performs in the case of reliability.

Chapter 4
Proposed Solution

4.1 Proposed Solution

4.1.1 Simulation Model

In order to carry out the simulation process for ad hoc networks in different environments, there are various mobility models which can be used. The most commonly used are:

1. Random Waypoint mobility model

Random waypoint model is a frequently used synthetic model for mobility in the wireless ad hoc networks. This is a fundamental model that illustrates the movement pattern of independent nodes by using simple terms. The random way point mobility model includes pauses between changes in direction as well as speed. A mobile node begins by staying in one location for a certain period of time called a pause. Once the time expires, the mobile node choses a random destination in the simulation area and a speed that is uniformly distributed between the minimum and maximum. The mobile then travels toward the newly chosen destination at the selected speed. Upon arrival, the mobile node pauses for a specified period of time starting the process again [30].

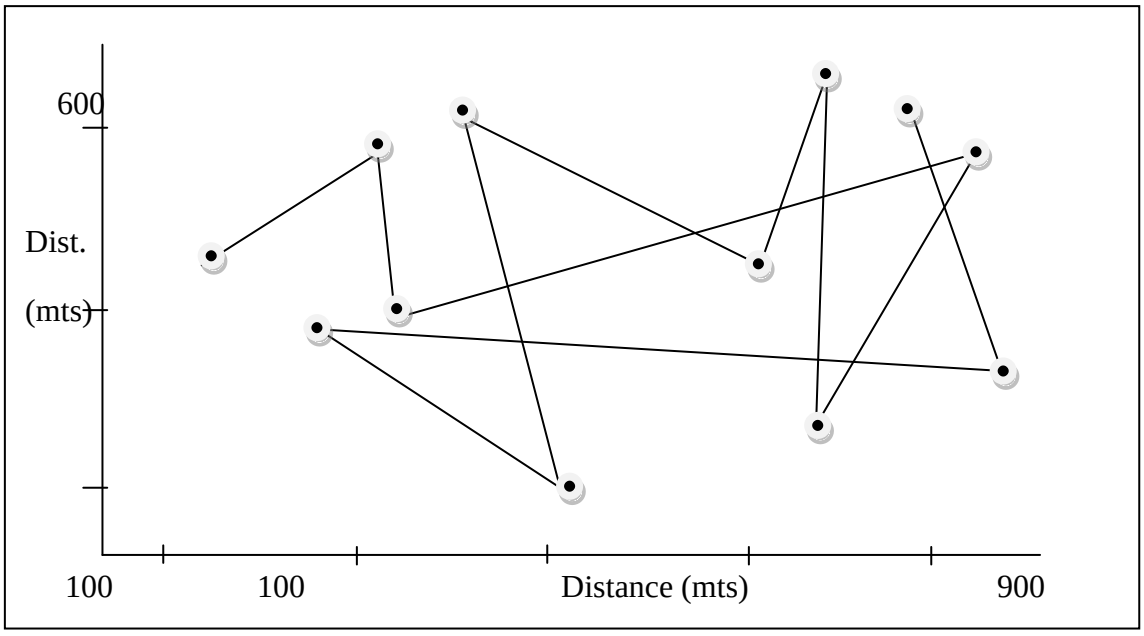


Figure 4.1: A Random waypoint mobility model.

In this model:

- Every node moves along a zigzag line from one waypoint to the other waypoint.
- These waypoints are being uniformly distributed over a given convex area.
- A random velocity is drawn from the velocity distribution at the starting.
- The nodes possess the thinking time (optionally) when they reach every waypoint before continuing on the next leg, the durations being independent and identically distributed random variables.

The simplicity of Random Waypoint model is the reason for its widespread use in the simulations. However, ad hoc networks are being used in various applications where complex mobility patterns are there. Therefore, the new research has been started that focus on some of the alternative mobility models that have different mobility characteristics. In such models, the movement of a node is somehow restricted by its history, or by the other nodes in the vicinity or the environment.

2. MANHATTEN mobility model

The Manhattan mobility model is commonly used to compute the movement pattern of nodes on streets that are defined by the maps. The model could be used in the modeling movement in the areas where wide spread emulating services between the portable devices is provided [31].

This model works by using its own map. This map is comprised of a number of horizontal and vertical lines called streets. Every line consists of two lanes one for each direction (north and south direction for vertical line and east and west for horizontal lines). Here, a mobile node is restricted to move across the grid of horizontal and vertical lines on the map. The mobile nodes could turn right, left, or go straight at meeting point of a horizontal and a vertical line. The choice contains probability: the probability of moving on the same line is half and the probability of turning left and turning right is quarter. The velocity of a mobile node at a given time instant is directly proportional to its velocity at the previous time slot. In addition to it, the velocity of a node is constraint by the velocity of the node preceding it on the same lane of the line. Therefore, the Manhattan mobility model is likely to have large spatial dependence and large temporal dependence. Geographical restrictions are also being provided on the mobility of a node. Also however, the mobile nodes are allowed to change its direction. The Manhattan mobility model is based on a grid road topology that was designed for the roaming in urban area, where the streets are in an organized manner. The essential features of the Manhattan Mobility model include:

- The mobile nodes are permitted to move across the grid of horizontal and vertical lines called streets on the map.
- At the meeting point of a horizontal and a vertical street, the mobile node can turn left, right or go straight via certain conditions.
- The model gives flexibility for the nodes to change the direction but it also provides the geographic restrictions on mobility of a node.

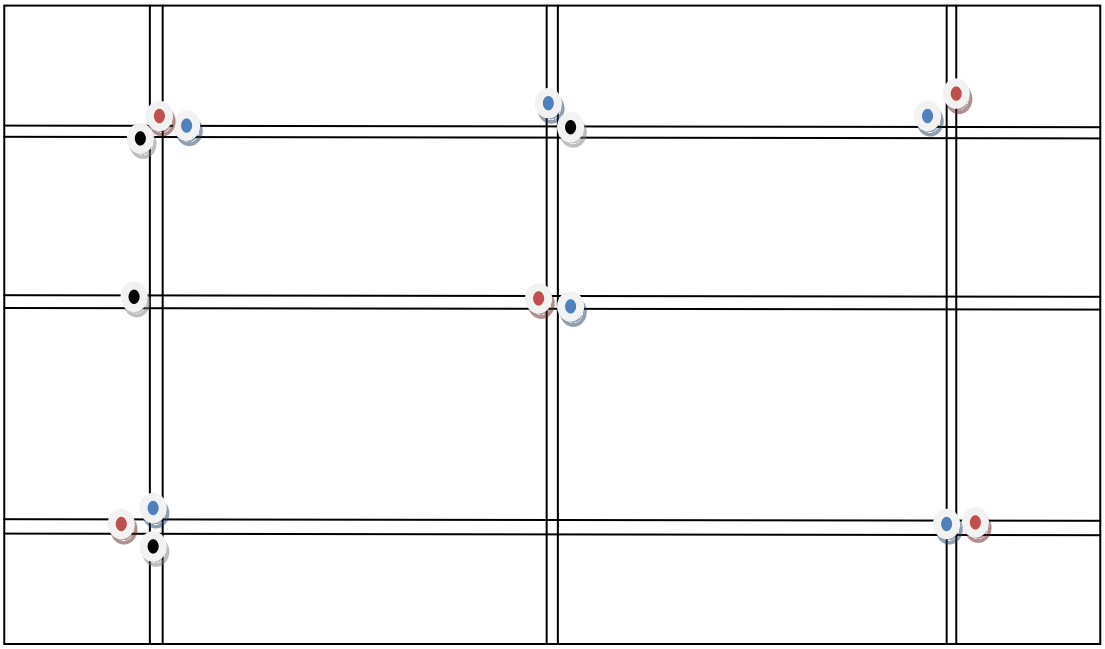


Figure 4.2: Nodes' movement in Manhattan Mobility Model

3. Reference point group mobility model (RPGM)

The Reference point group mobility model shows a logical relationship between the Mobile Nodes (MNs) moving together. A reference center (logical center) is defined by every group whose movement is followed by all the mobile nodes in the group [32]. The node destination is chosen randomly within a certain radius of its Reference Point (RP). The RP scheme allows for random motion along with group motion the behavior of motion of a group (that includes direction, acceleration, velocity and location) is defined by the center's motion. Therefore, by providing a route for the center, a group trajectory can be found out. Here also, the nodes are uniformly distributed within the geographic scope of a group. The

following figure shows the movements of three MNs using the RPGM model where RM represent the motion vector.

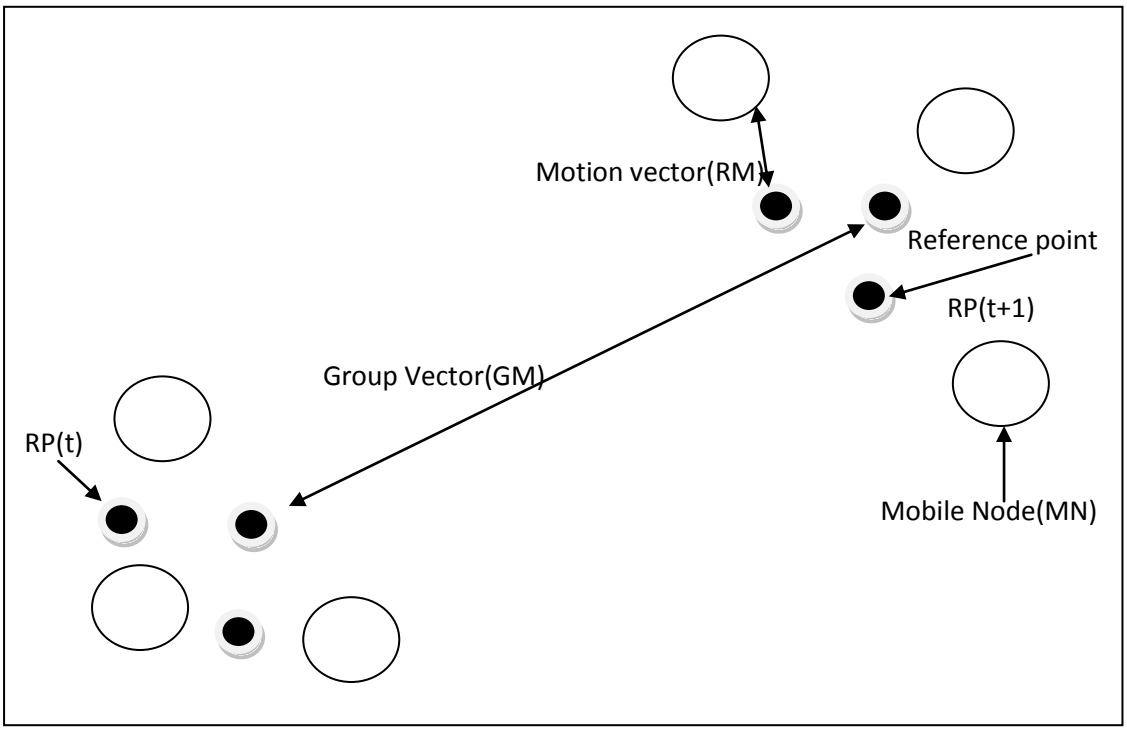


Figure 4.3: Movements of 3 MNs using the RPGM model.

In this thesis we have used the random waypoint mobility model in order to carry out the simulation process as it illustrates the movement pattern of independent nodes by using simple terms. Further MATLAB is used to implement the proposed algorithm and generate graphs illustrating the performance of the proposed model.

4.1.2 Motivation and Objectives of RAODV

Routing in ad hoc networks has interesting security problems. Use of wireless links renders an ad hoc network susceptible to link attacks. Nodes roaming in a hostile environment, with relatively poor physical protection, have non negligible probability of being compromised. And there is very little published prior work on the security issues in ad hoc routing protocols. Therefore there is a need to make the communication reliable and secure amongst the nodes in the network. The main objectives of

this thesis are:

- To incorporate reliable transmission of information into ad hoc networks routing protocols.
- Discuss whether the algorithms would be applicable to the other ad hoc routing protocols or not.
- Present how the key management scheme could be used in conjunction with the proposed algorithms.
- RAODV is used as an example of ad hoc routing.
- To design a routing protocol for MANET that is efficient, scalable, distributed and simple to implement.
- Ensuring the survivability of network services despite denial-of-service attacks which is the availability.
- Ensuring that certain information is never disclosed to an unauthorized entity which is called the confidentiality.
- Guaranteeing that a message being transferred is never corrupted that is called the integrity.
- Enabling a node to ensure the identity of the peer node with which it is communicating which is called the authentication process.
- Ensuring that the origin of the message cannot deny having sent the message called the non-repudiation.

In the thesis the security problem that happens due to the instability of physical layer or link layer are not concerned, and the assumptions that are made include that each node in the network has the ability to recover all of its neighbors; the nodes in the network can broadcast various important messages to its neighbors with high rate of reliability; each node in the network is associated with a unique ID that can be distinguished from others.

The key features of RAODV include that RAODV is an on-demand routing protocol, there are unicast / multicast / broadcast provided in the protocol, the protocol is loop free, there is quick aging, the link breakages are efficiently repaired, there is distributed routing, hop-by-hop routing, deterministic and reliable Routing. Every node maintains a routing table with all known nodes, reliable value, next hop and costs. The routing table entries include destination IP, destination Sequence Number, hop Count to the destination (cost per hope = 1), next Hop, lifetime, last Hop Count, routing Flags, interface (i.e. eth0, eth1), list of Precursors, set of reliable values.

4.1.3 Routing Operations in RAODV:

In the following discussions, we present the reliable approbation mechanism used in RAODV. This is then followed by defining some norms for a node in RAODV. In order to make the routing decisions as per the reliable values, the nodes have to obey these rules.

Reliable Approbation:

When applying the reliable model into the network applications, it becomes obligatory to design a reliable data exchange mechanism. Existing models connected with the security issues are seldom concerned with the exchange of reliable information amongst the nodes. In RAODV we try to provide with an efficient and effective reliable approbation mechanism. Similar to conventional AODV protocol's REQuest packet (REQ) and REPly packet (REP), RAODV also uses two such packets in the approbation procedure called Reliable ReQuest (RRQ) packet and Reliable RePly (RRP). The reliable value associated with each node is based on the changing characteristics of that node and is kept static during any route discovery or path determination process. This reliable value is kept in the routing table of each node and is updated time to time whenever necessary. When a node X wants to know the reliability of another node Y, it will simply broadcast the RRQ packet to all the nodes within the transmission range of node X. Now if Y is under the transmission range of X, then node Y will send a RRP packet to X informing about its reliability value, otherwise X will receive the reliability information of Y via some intermediate nodes in the network. Also note that, in this approbation protocol, a node could request as well as reply different reliability values of different nodes at the same time instant in the form of a RRQ or RRP message. Therefore, one can efficiently update itself with the reliability information of the nodes in the network without the overhead of many messages. The routing table entries are updated every time the reliability value of a node changes.

Reliable Updation:

The reliability amongst the nodes keep on changing dynamically due to the increase in communication events which may sometimes be successful and sometimes unsuccessful. There are certain rules which govern when and how to update the reliable values amongst the nodes:

i. Whenever a node X has done a successful communication with another node Y (which includes

generating route request or route reply normally and forwarding route request or route reply normally etc…) then this successful event of node Y is being incremented in the routing table of node X.

ii. Whenever a node X has done an unsuccessful communication with another node Y (which includes generating route request or route reply abnormally and forwarding route request or route reply abnormally etc…) then this unsuccessful event of node Y is being incremented in the routing table of node X.

iii. Due to these successful and unsuccessful events, every time when their field changes, the corresponding value of reliability is affected and updated in the routing table of each node.

iv. If the route entry of a node X is deleted from another node Y's routing table (means X is not reachable from Y), then its corresponding reliability value is set to 0.

4.1.4 RAODV route discovery process

The RAODV routing protocol could be used for the determination of optimum path from the given source to a specific destination in a network based on a set of some reliability values associated with each node. The route discovery procedure advances forward by selecting the most reliable node within a given transmission range and then verifying if this selected node really takes us to the destination. The procedure is repeated again and again in the form of hop-by-hop routing till the destination is reached and we finally get a set of nodes determining the reliable optimized path between a pair of nodes. A neighbor of node is considered active for a routing table entry if the neighbor sent a packet within active route timeout interval and was forwarded using that entry and if a source node moves, a new route discovery process is initiated.

Suppose source s wants to send the information to destination d (Figure 4.4), then to establish a path, s will broadcast a RRQ within its transmission range (i.e. p1, p2, p3), but only the node (p2) with the maximum reliability value will send a RRP packet to s (verification is done before (by sending a HELLO packet) in order to check if destination d is reachable from node p2 or not. If no, then the second maximum reliable node is chosen and so on…). Following the similar strategy we reach the destination d and obtain a set of nodes giving an optimum reliable path. The overall reliability of the path is obtained by adding the reliability value of nodes in the path.

The procedure may be more efficient than other protocols when rate of information transmission is low enough that the overhead of explicit route discovery and maintenance incurred by other protocols is

relatively higher. There is potentially higher reliability of data delivery because packets may be delivered to the destination based on the reliability values.

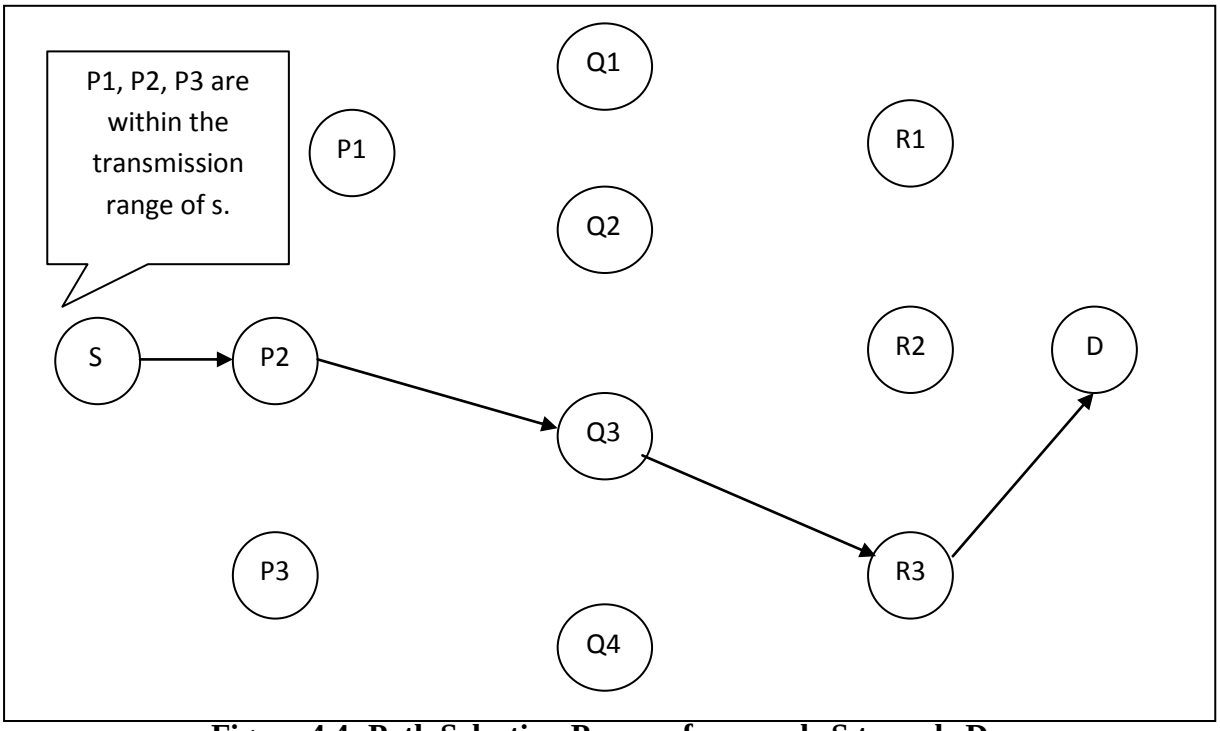


Figure 4.4: Path Selection Process from node S to node D

4.1.5 RAODV route maintenance process

Battery drainage, congestion and fading effects may lead to broken routes which may interrupt the routing [33]. A route-error packet is transmitted in the event of failure of link or an intermediate node moving out of range. When a route-error packet is received from a node, the route becomes invalid via that link and switches to some other alternative path. Therefore, the node which does not contain the next node of one that sent a route error packet, the source node now chooses that alternative path. RERR is initiated by the node upstream (closer to the source) of the break and it's propagated to all the affected destinations. RERR lists all the nodes affected by the link failure (Nodes that were using the link to route messages (precursor nodes)). When a node receives an RERR, it marks its route to the destination as invalid, setting distance to the destination as infinity in the route table. When a source node receives an RRER, it can reinitiate the route discovery.

4.2 Heuristic Algorithm

Algorithm

Input: n(nodes),source s, destination d, Reliability array R(containing reliability value for each node).
Output: Optimized path RS and Reliability_factor .

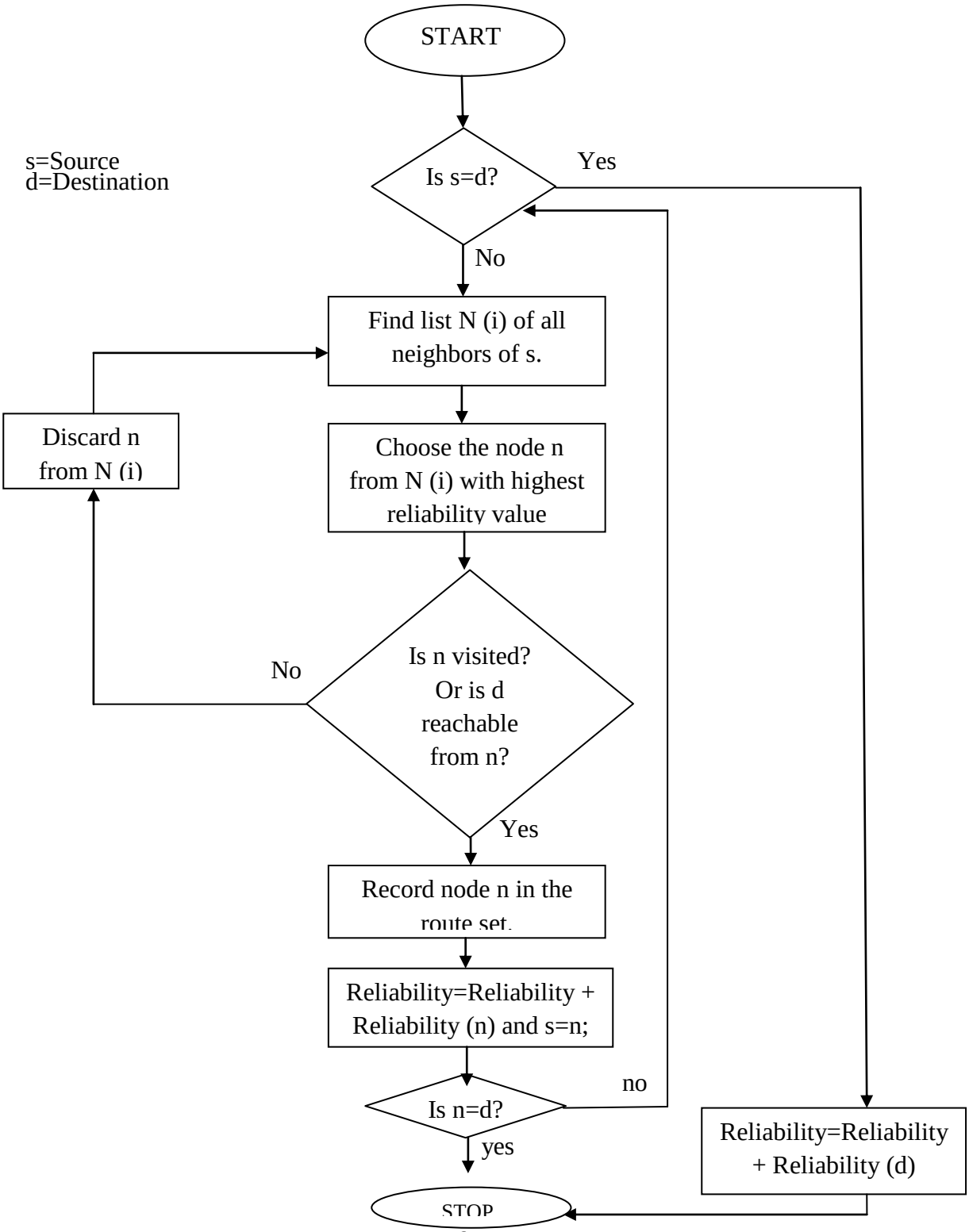
```
Procedure opt_pth:
{
    Let route set RS={}, m=|RS|=0 and reliability_factor=0.
    repeat
        {
          i.  Find the set N of all the neighbors of s (in wireless networks, neighbor
              means within the transmission range).
              N = {}
              For i = 1 to n:
                    {
                        If ( Range(node(i)) <= Range (s))
                            N = N + node (i) // append the neighbor set n with the ith node.
                     }

         ii.  From N determine the node u with the maximum reliability value.
              I.e. R [u] = maximum ( R [N(1)], R [N(2)], R [N(3)],…)

        iii.  Determine if d is reachable from u or if u is already visited?
              If ( ! d reachable from u OR u already visited )
                 {
                    Discard node u;
                    Go to step (i).
                 }
              Else
                 {
                    Append node u in the route set RS;
                    m=m+1;
                    R = R + R[u];
                  }

         } until (s == d) // Destination reached.
```

4.3 Flow Chart



4.5: Flow Chart of the Proposed Solution

Chapter 5
Analysis and Performance Evolution

5.1 Results and Discussions

As the thesis work considers the random way point mobility model, therefore a random destination according to the proposed algorithm is chosen at each step. After reaching that destination point, the mobile node again pause the time before selecting a new way point. Hence a hop-by-hop routing is performed in the proposed model. The mobile nodes or the source-destination pairs are randomly distributed over the network and by changing the number of mobile nodes, we get different scenarios.

To test the algorithm, the proposed model is implemented in MATLAB. The parameters used to simulate the proposed model includes 10 mobile nodes randomly spread within the network with each node having the transmission range of 5 units and the network possessing a total 55 source-destination pairs. Further, the reliability value associated with each node lies within the range of 0 and 1, where 1 indicates 100% reliability of a mobile node. A random topology is defined for the corresponding network. As we are focusing on the wireless networks, therefore a mobile node A is neighbor of another node B if B lies within the transmission range of node A.

Running the code for the proposed model in MATLAB, presents the results in two output windows:

- Output window 1: It is the command window representing the overall reliability of the chosen path, number of hops, reliable path, distance travelled and the time taken by the algorithm.
- Output window 2: It is a graphical user interface depicting network with the nodes in a 2-dimenstional area, the random topology and the reliable optimum path between the source (node1) and the destination (node10).

The following screen shots represent the two output windows:

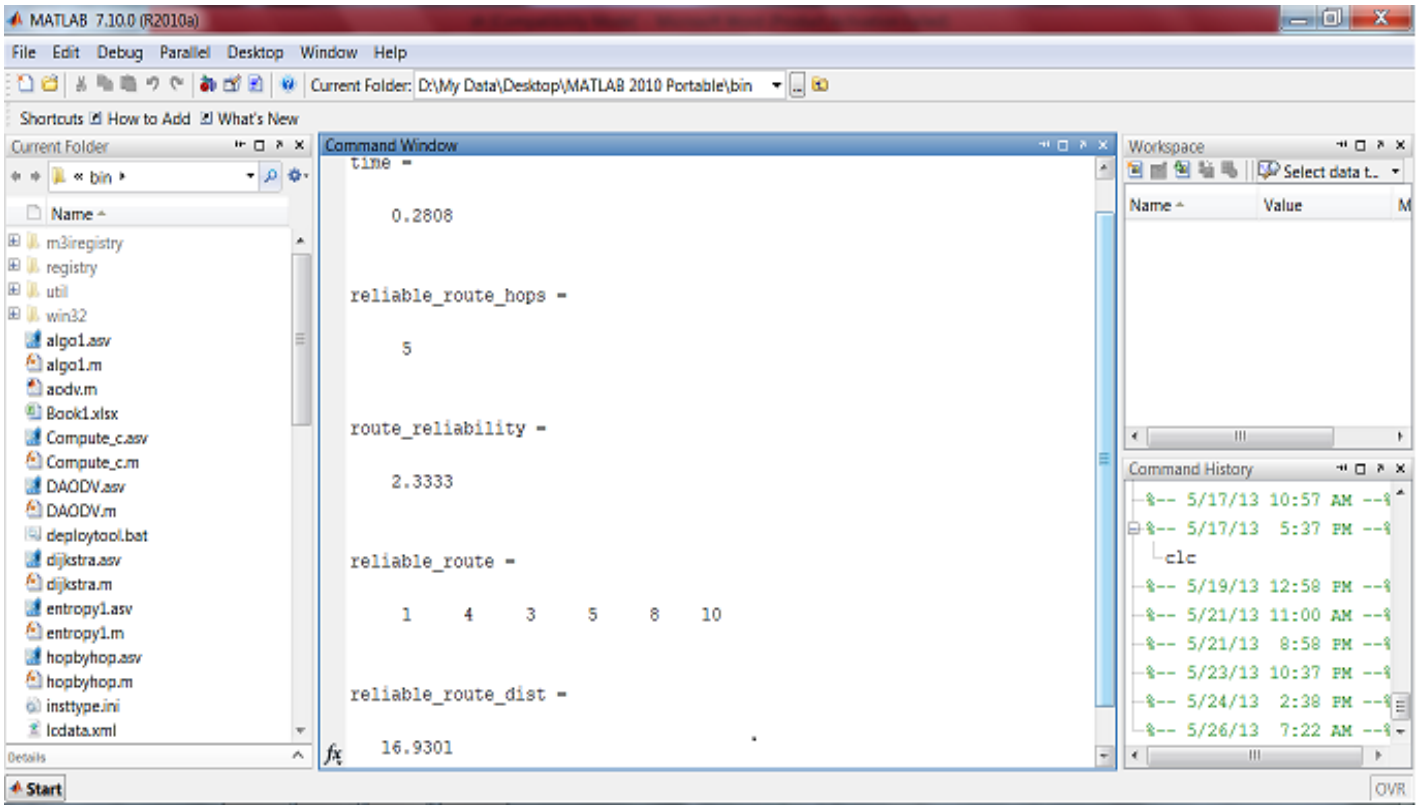


Figure 5.1: Output window 1.

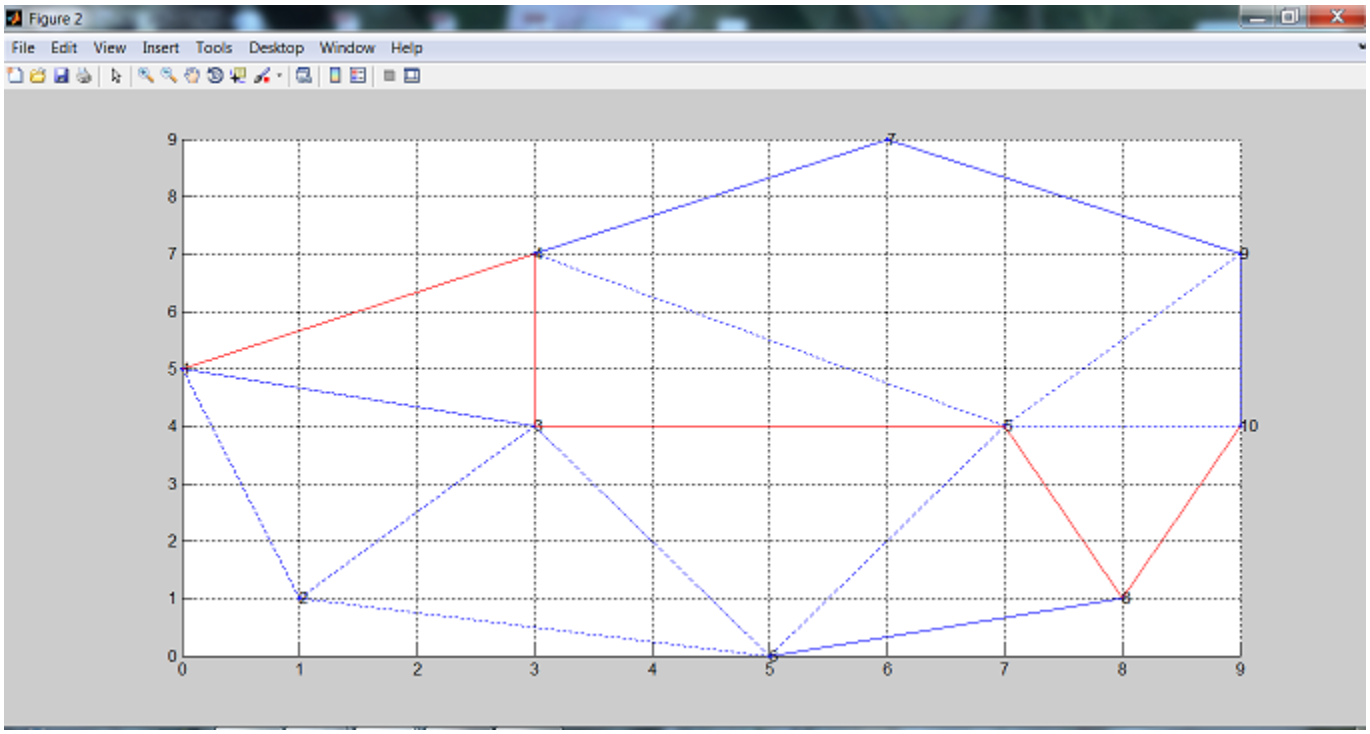


Figure 5.2: Output Window2.

5.2 Performance Metrics

In order to evaluate the efficiency of the proposed routing protocol, following three performance metrics are considered:

- **Reliability:** Reliability of a network is its quality that indicates the degree of consistency maintained within a network. A more reliable path is preferred to have a secure transmission of information from a specific source to the destination. Although, as the number of mobile nodes increases, it keeps on decreasing.

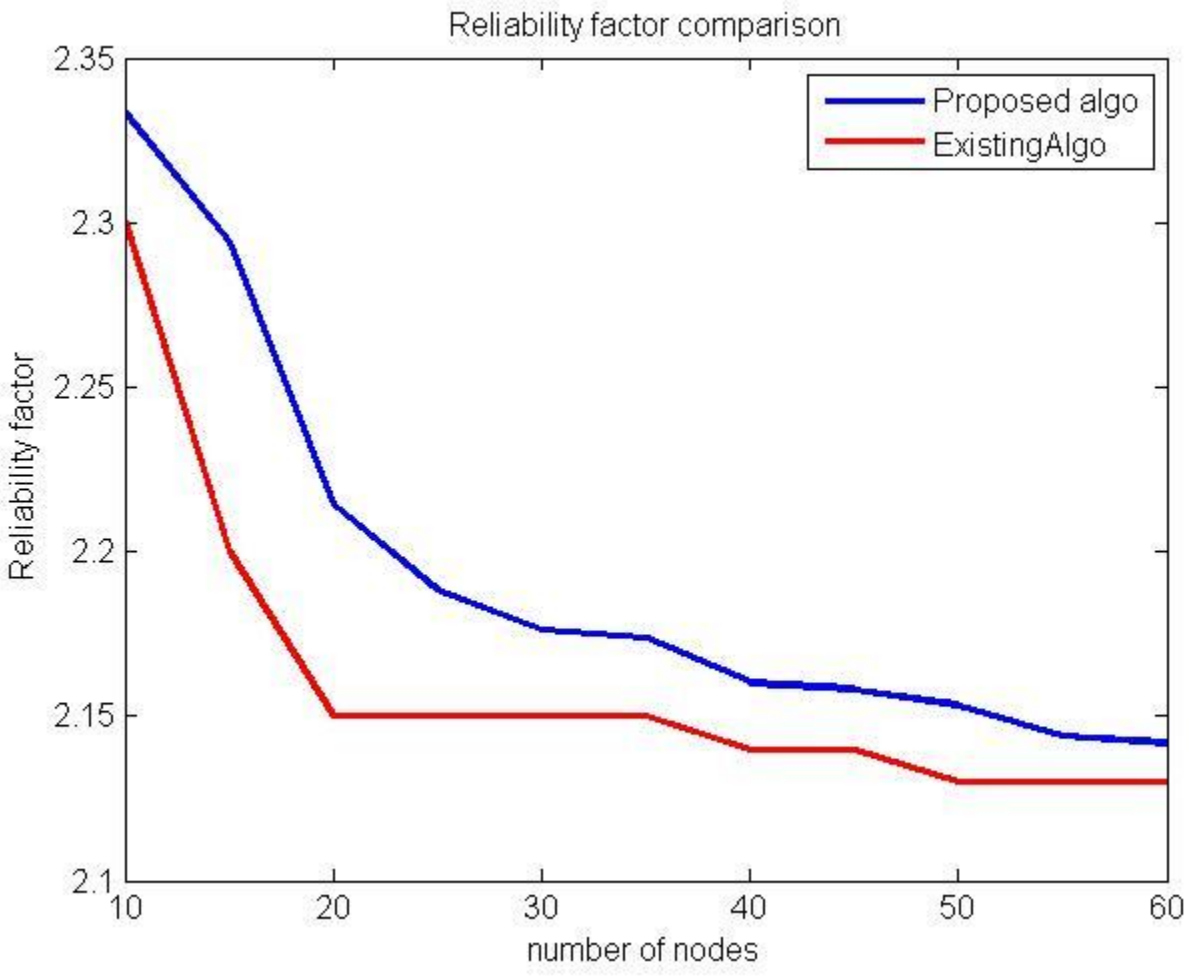


Figure 5.3: 10-node model with different number of traffic sources I.

- **Hop Count:** Hop count is the number of intermediate nodes visited by the packet before reaching its destination. The results shows that though the number of hops or the distance travelled by the packets is more in the proposed algorithm but still the reliability factor is more. Moreover, the existing model does a blind search and thereby consuming a lot of time wastage of necessary resources whereas the proposed model is much simpler as it advances forward in a more reliable direction towards the destination and consuming less resources.

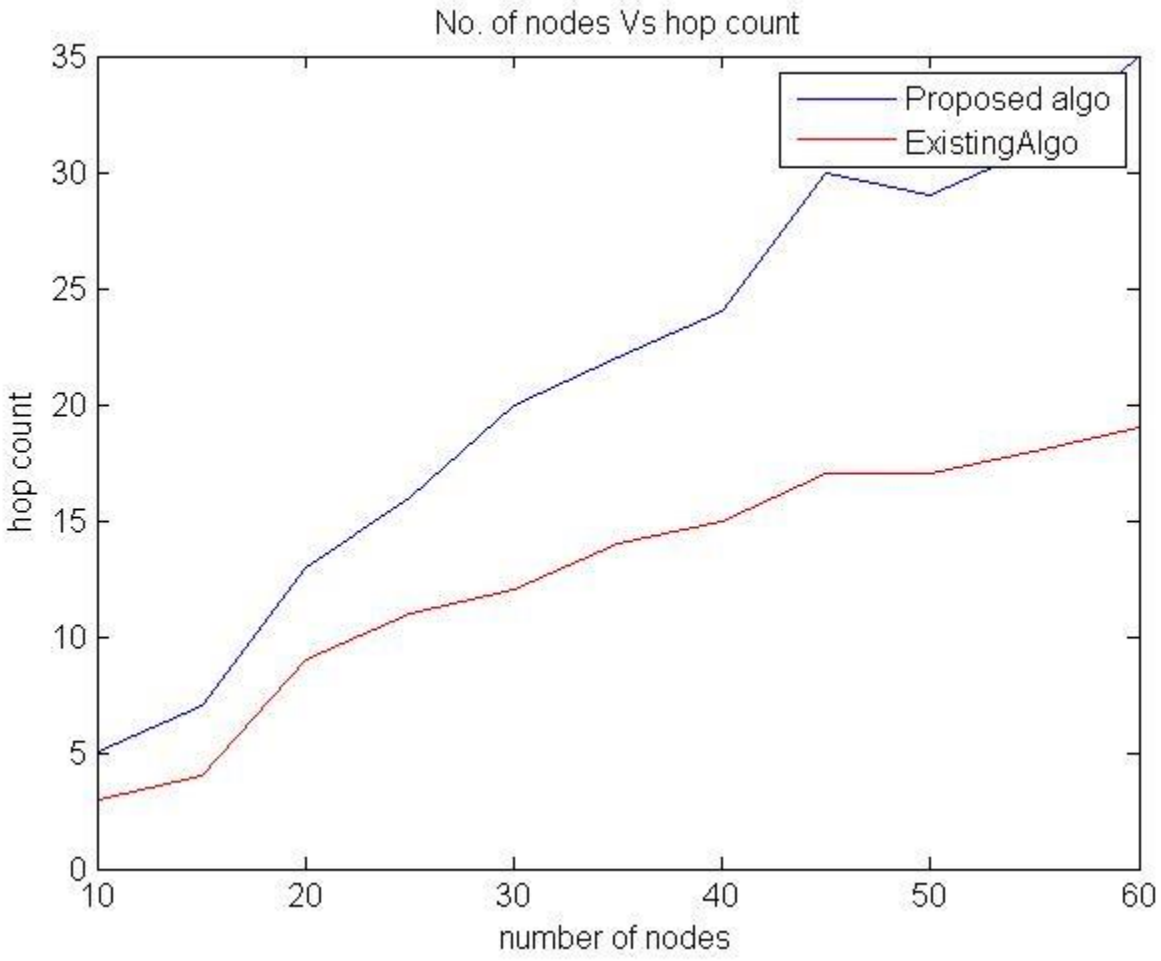


Figure 5.4: 10-node model with different number of traffic sources II.

- **Average time taken:** This average time is the time taken by the proposed algorithm to generate

the reliable path from the source to the destination and thus implement the proposed algorithm. For large networks the proposed model over performs as delays generated are less.

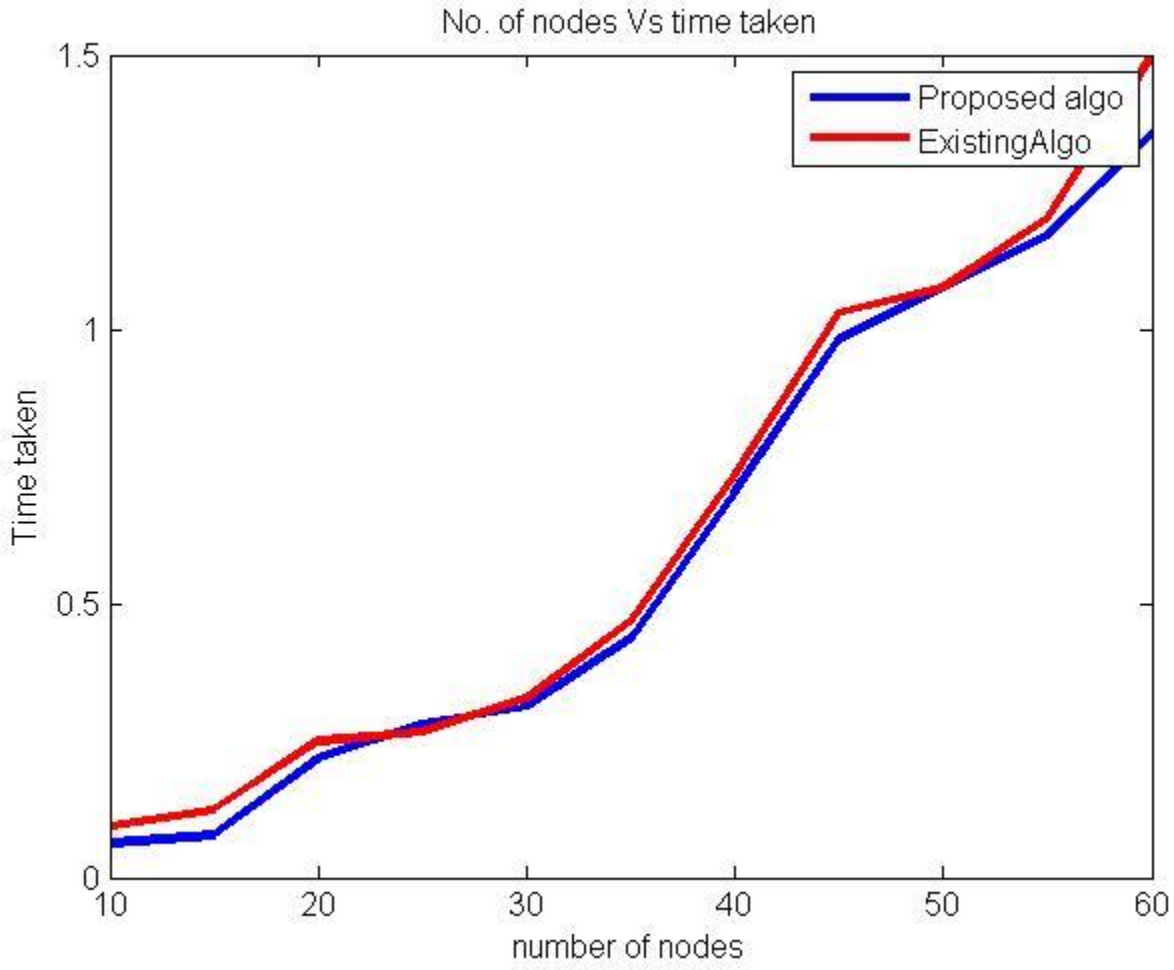


Figure 5.5: 10-node model with different number of traffic sources III.

Note that these parameters are not completely independent. The variation in the number of mobile nodes and other supporting factors may cause alteration in the results. For example, less number of mobile nodes leads to a more reliable path discovery and less end-to-end delay. Also, the scenarios tested here is a random situation as the real world ad hoc networks possess the different traffic and mobility models. The problem here is that different applications possess different scenarios and it is not predictable in advance that which scenario is suitable for a specific application.

Chapter 6
Conclusion and Future Work

6.1 Conclusion

Ad hoc wireless networks possess the mobile stations communicating solely through the wireless channels. Therefore, such networks are bent upon playing essential roles in various fields like emergency, defense settings and communication support in other different areas. Further, lack of a fixed centralized infrastructure makes it essential tool in areas where a fixed infrastructure may be economically non-profitable.

In the current thesis work, we focused on the routing in ad hoc networks which is supposed to be reliable, resource saving and time efficient. One such way discussed is by associating each mobile station with a reliability value in an on-demand distance vector routing environment. We presented the simulation study in order to find the best reliable path between a pair of nodes which came out to be more reliable and time efficient as compared to one of the model that uses shortest path algorithm to discover the route. Therefore, from the present thesis it could be concluded that:

- RAODV and existing shortest path routing protocol, both uses on-demand route discovery process, but RAODV performs better in case of reliability.
- The time taken by the proposed model is less than the existing protocol which does a blind search in order to determine the shortest path.
- As the number of mobile workstations increases, reliability decreases due to the additional overheads.
- The proposed model results in more number of hops and distance travelled, but then there is always a trade-off between resources, time and reliability.

Due to variations in the capabilities, responsibilities, mobility models, traffic characteristics etc.., the performance criteria (like energy consumption and throughput) keeps on altering from time to time leading to increased research work in this field.

6.2 Future Work

- The thesis presents only one way of implementing reliability factor within ad hoc networks, several other algorithms could be used.
- In present simulation studies, only one propagation model (Random way point mobility model) is used, there are several other models which could be deployed.
- The proposed model uses only the on-demand driven approach; it could be applied on table-driven routing protocols as well.
- The current work is tested in MATLAB; it could be extended to other languages or simulation tools.
- A comparison with an existing routing protocol is being made, its proposed to compare the algorithm with all other routing protocols considering identical simulation parameters.

References

[1] J. Z. Sun "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", Info-Tech and Info-net, 2001.

[2] A. J. Goldsmith and S. Wicker, "Design Challenges for Energy-Constrained Ad Hoc Wireless Networks", IEEE wireless communication, volume 9, no. 4, 2002.

[3] R. K. Bansal, "Performance Analysis of Cluster Based Routing Protocol in MANETs", M.E. Thesis, Thapar University, India, 2006

[4] M. T. Toussaint, "Multipath Routing in Mobile Ad Hoc Networks", DTC.5966 Freeband/CACTUS Project, 2003. http://www.cactus.tudelft.nl.

[5] N. Meghanathan, "Graph Theory Algorithms for Mobile Ad Hoc Network", Informatica; volume 36, no. 2, pp. 185-200, 2012.

[6] IETF Mobile Ad-Hoc Networks (MANET) Working Group, http://www.ietf.org/

[7] S. Baolin, G. Chao, Z. Qifei, Y. Bing, L. Wei, "A Multipath on-demand Routing with Path Selection Entropy for Ad Hoc Networks", International Conference of Young Computer Scientists (ICYCS), 2008.

[8] B. Awerbuch and A. Mishra, "Introduction to Ad Hoc Networks CS-647:Advanced Topics in Wireless Networks", Johns Hopkins University, 2008.

[9] E. Baccelli, "IP Links in Multihop Ad Hoc Wireless Networks?" , Telecommunications and Computer Networks, SoftCom, 2009.

[10] S. Chen and K. Nahrstedt, "Distributed Quality-of-Service Routing in Ad Hoc Networks", IEEE journal on selected areas in communications, volume 17 no.8, 1999.

[11] J. J. Garcia-Juna-Aceves, M. Mosko, I. Solis, R. Braynard, R. Ghosh, "Context-Aware Packet Switching in Ad Hoc Networks", Personal Indoor and Mobile Radio Communications (PIMRC), 2008.

[12] J. Deng, B. Liang, P. K. Varshney, "Tuning the Carrier Sensing Range of IEEE 802.11 MAC", IEEE Comminications Society, Globecom, 2004.

[13] S. Kumar, V. S. Raghvan, J.nDeng,"Medium Access Control Protocols for Ad Hoc Wireless Networks: a survey", ELSEVIER, 2004.

[14] D. A. Maltchanov, "Challenges and Specifics of Ad Hoc Networks", TUT, 2009, http://www.cs.tut.fi/kurssit/TLT-2756/

[15] I. B. N. Islam, "Performance Analysis of Wireless Ad Hoc Networks in Different Network Situations from Routing Point of View", M.E. Thesis, Blekinge Institute of Technology, Sweden, 2008.

[16] A. Shrivastava, A. R. Shanmogavel, A. Mistry, N. Chander, P. Patlolla, V. Yadlapalli, "Overview of Routing protocols in MANETs and Enhancements in Reactive Protocols", Department of Computer Science, Lamar University, 2005.

[17] P. Misra, "Routing protocols for Ad Hoc Mobile Wireless Networks", http://www.cse.ohio-state.edu/~jain/cis788-99/ftp/adhoc_routing/ #TDRP, 1999.

[18] M Steenstrup, "Routing in Communication Networks", New Jersey, Prentice Hall. ISBN 0-13-010752-2.

[19] K. Gorantala, "Routing Protocols in Mobile Ad Hoc Networks", M.E. Thesis, Umea University, UMEA, Sweden, 2006.

[20] J. Schaumann, "Analysis of the Zone Routing Protocol", course CS765, Stevens Institute of Technology Hoboken, New Jersey, 2002.

[21] G. He, "Destination-Sequenced Distance Vector (DSDV) Protocol", Technical Report, Helsinki University of Technology, Finland, 2003.

[22] P.Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot,"Optimized Link State Routing Protocol for Ad Hoc Networks", Hipercom Project, France, 2005.

[23] P. Suganthi, Dr, A. Tamilarasi, "Performance of OLSR Routing Protocol Under Different Route Refresh Intervals in Ad Hoc Networks", International Journal on Computer Science and Engineering (IJCSE), volume 3, no.1, 2011.

[24] V. U. Chezhian, K. Karthikeyan, T. Subash, "Comparison Of Two Proactive Protocols: OLSR and TBRPF using the RNS (Relay Node Set) Framework", International Journal of Computer Science and Emerging Technologies (IJCSET), volume 2, no. 2, 2011.

[25] C. E. Perkins, E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing (AODV)", International Engineering Task Force (IETF) , 2003.

[26] P. Misra, "Routing Protocols for Ad Hoc Mobile Wireless Networks", http://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc-routing/

[27] D. Kumar, P. K. Jakhar, “Reletive Distance Mobile Ad Hoc Networks (RDMAR)”, International Journal of Computer Technology and Applications (IJCTA), volume 2, no. 4, pp. 733-735, 2011.

[28] E.Y. Hua and Z. J. Haas, “Path Selection Algorithms in Homogenous Mobile Ad Hoc Networks”, International Conference on Wireless communications and Mobile Computing (IWCMC), pp. 275-280, New York, NY, 2006.

[29] S. J. Castillo, “Distributed Detection in Ad Hoc Sensor Networks”, Cornell University, 2003.

[30] J. Broch, D. A. Maltz, D. B. Johnson, Y. -C. Hu, and J. Jetcheva, “A Performance Comparison of Multi-hop Wireless Ad Hoc Network Routing Protocols”, Proceedings of the fourth annual ACM/IEEE International Conference on Mobile Computing and Networking (mobicom), ACM, 1998.

[31] Masoud Moshref Javadi, “Mobility Simulator”, http://www.masoudmoshref.com/old/myworks/documentpages/mobisim/manhattan.htm.

[32] M. Sivajothi and E. R. Naganathan, “Analysis of Reference Point Group Mobility Model in Mobile Ad Hoc Networks with an Ant based Colony Protocol”, International Multiconference of Engineers and Computer Scientists (IMECS), volume 1, 2009.

[33] V. Shabnam, M. Maryam, A. Darehshoorzadeh, “Design a Multipath Routing Algorithm in Ad Hoc Networks in order to improve Fault Tolerance”, Personal Indoor and mobile radio communications (PIMRC), 2007.

Appendix

The code for the proposed model in MATLAB:

```
function RAODV
clc;
N=10;  % no. of nodes
figure(2);
clf;
hold on;
s =1;%source node
d=10;%destination node
time=cputime  ;
Tr =5; %transmission range
X = [0 1 3 3 7 5 6 8 9 9];
Y = [5 1 4 7 4 0 9 1 7 4];
R =[0.8 0.1 0.7 0.8 0.6 0 0.1 1 0.9 1];% reliable value of nodes.
for i = 1:N
 plot(X(i), Y(i), '.');
 text(X(i), Y(i), num2str(i));
   for j = 1:N
      dist = sqrt((X(i) - X(j))^2 + (Y(i) - Y(j))^2);
      if dist <= Tr
         topmat(i, j) =1;
         relymat(i,j)=(R(i)+ R(j))/2;
         line([X(i) X(j)], [Y(i) Y(j)], 'LineStyle', ':');
         distmat(i,j)=dist;
      else
         topmat(i,j) = inf;
         relymat(i,j)= inf;
         distmat(i,j)=inf;
```

```
        end

    end
end
grid

[route,rel]=Path_func(s,d,relymat);
 reliable_route=route;
route_reliability=3-rel;
reliable_route_hops=length(route)-1;
reliable_route_dist=0;

for k=2:length(route)
    reliable_route_dist= reliable_route_dist + distmat(route(k-1),route(k));
end
reliable_route_dist;

for p =1:(length(route)-1)
    line([X(s) X(route(1))],[Y(s) Y(route(1))],'Color','r','LineWidth', 1, 'LineStyle', '-')
    line([X(route(p)) X(route(p+1))], [Y(route(p)) Y(route(p+1))], 'Color','r','LineWidth', 1, 'LineStyle','-
')

end
time = cputime-time;
display (time);
display (reliable_route_hops)
display (route_reliability)
display (reliable_route)
display (reliable_route_dist)
return
```

```
function [route,rel]=Path_func(source,des,relymatrix)
Nodes = size(relymatrix, 1);
path=[];
path(1)=source;
route_src=source;
[route_chk]=checkroute(route_src,des,relymatrix);
if (route_src~=des && route_chk ==1)
   m=1;
   n=2;
   while(route_src~=des)
      Neigh_rely=[];
      i=1;
      for j= 1:Nodes
         if relymatrix(route_src, j)~=inf
            Neigh_rely(i,1)=j;
            Neigh_rely(i,2)=relymatrix(route_src,j);
            i=i+1;
         end
      end
 Neigh_rely =sortrows(Neigh_rely,-2);
 nextnode = Neigh_rely(m,1);
 check = find_visited(path,nextnode);
 if check==1
[route_chk]=checkroute(nextnode,des,relymatrix);
     if(route_chk==0)
       m=m+1;
     else
        path(n)=nextnode;
        route_src=nextnode;
```

```
        m =1;
        n=n+1;
      end
    else
     m = m+1;
  end
   end
else
   disp('source =dest or cannot reach destination')
end
route =path;
rel=0;
for l=2:length(route)
      rel= rel+relymatrix(route(l-1),route(l));
end
rel=rel/length(route);

function check =find_visited(path,nextnode)
count =0;
for z=1:length(path)
   if nextnode==path(z)
      count=count+1;
   end
end
if count>0
   check = 0;
else
   check = 1;
end
```

```
function [route_chk]=checkroute(route_src,des,relymatrix)
if relymatrix(route_src,des)~=0 || relymatrix(route_src,des)~=inf
   route_chk=1;
else
   route_chk=0;
end
return
```

Publications

M Gupta and N. Kumar, "Node-Disjoint On-demand Multipath Routing with Route Utilization in Ad-Hoc Networks" International Journal of Computer Applications (IJCA), volume 70, no. 9, 2013. (Communicated).