CHAPTER 1

INTRODUCTION

The popularity of wireless portable and computing capable devices has made possible the dream of “Anytime and anywhere communication”. Users can remain connected to the world while being on the move. This is mobile computing or ubiquitous computing or nomadic computing.

One such class of wireless networks is the Mobile Ad-hoc Networks that have been a recognized field of research from the last over a decade.

Mobile Ad-hoc Networks, popularly called as MANETs, are infrastructure-less, multihop networks without any physical connections. MANETs consists of a number of mobile hosts that are connected by means of wireless links. These MANET nodes acts as routers and are themselves responsible for forwarding packets within a MANET without the need of a centralized authority. The key feature of Mobile Ad-hoc Networks is its easiness of deployment. So it makes it suitable for battlefield, search and rescue and disaster management. In MANETs, nodes rely on multihop communication (nodes within each other’s transmission range can directly communicate through wireless channels whereas, those outside the range have to communicate indirectly through intermediate nodes) to exchange data between source and destination nodes. MANET nodes can move freely in the network. When the nodes move, the network topology will be changed frequently, i.e., the more the node mobility, the higher is the frequency of topology change.

MANETs are highly spontaneous, self organized, self-maintained and decentralized in nature. Hence, in Mobile Ad-hoc Networks, there is no fixed topology due to node mobility, interference, multipath propagation and path loss. Also, each mobile node has limited resources such as battery, memory and processing power. As a result, establishing a correct and efficient routing protocol for MANETs is quite a challenging task to accomplish since traditional routing

protocols may not be suitable for MANETs. Routing protocol design for MANETs is therefore, an active field of research.

1.1 Problem Description

Mobile Ad-hoc Networks require an efficient routing strategy, which is capable of handling limited resources as well as simultaneously being able to adapt to dynamic network conditions like network size, topology and traffic density.

Shortest path or path with least hop count has been the most widely known way for finding the best path from source node to destination node. However, such a path may not always be the best path in terms of Quality of Service (QOS) metrics defined for the sending and receiving application. Also, the basic design of MANETs is not fully capable to provide support to multimedia services and also due to uncertainties associated with MANETs (unreliable wireless channel, node mobility, decentralized architecture etc.), providing QOS guarantees to MANET applications is quite an arduous task.

The objective of this Master Dissertation was to deal with a critical QOS aspect of MANET i.e. Delay and hence, propose a delay aware routing protocol that discovers routes for a source destination pair with the delay constraints provided by the applications. This has been presented through simulation.

The delay constraint provided by the application that wishes to transmit its traffic are used to find suitable routes that can send the application traffic from source to destination node within the specified delay bound.

1.2 Motivations and Contribution

The chief motivations behind the research in this thesis are the previous research works attempted in the field of MANET routing protocol design.

The major challenge in the way of realizing the practical benefits of MANETs is the Quality of Service guarantees since these networks are aimed at providing multimedia services in portable

hand-held devices. Hence it becomes quite critical to provide some level of QOS for data transfer which becomes difficult due to associated design challenges since the basic design of Mobile Adhoc Networks is not completely capable to do so.

Several attempts have been made in this direction by either providing QOS guarantees in existing routing protocols or by designing new QOS aware routing protocols. Numbers of metrics like delay, packet loss ratio, jitter, throughput etc. are used for providing QOS guarantees. Delay is one of these metrics on which a lot of research work has been done. Delay aware routing protocols discover routes between source-destination pair based on various delay constraints provided by the application which can be in the form of propagation delay. Jitter, end to end delay, routing delay etc. Each delay aware solution tries to deal with this problem in its own way.

In this respect, this thesis will contribute towards ongoing research in this area by proposing a delay aware routing protocol for discovering routes on the basis of application provided delay constraints. This method uses a reactive routing approach to find delay aware routes during the route discovery phase along with performing clock synchronization of nodes.

1.3 Dissertation Structure

In figure 1.1, we have presented the structure of this thesis. Chapter 2 and 3 elaborates the background study undertaken before performing the research in this thesis. Chapter 2 consists of a detailed literature survey of Mobile Ad hoc Networks and chapter 3 introduces the concept of Quality of Service in MANETs as well as summary of previous research work done in this field. Chapter 4 and 5 presents the main contributions of this thesis by reporting the details of research methodology followed in chapter 4 and analysis of simulation results in chapter 5. Chapter 6 concludes this thesis by proposing future extensions.

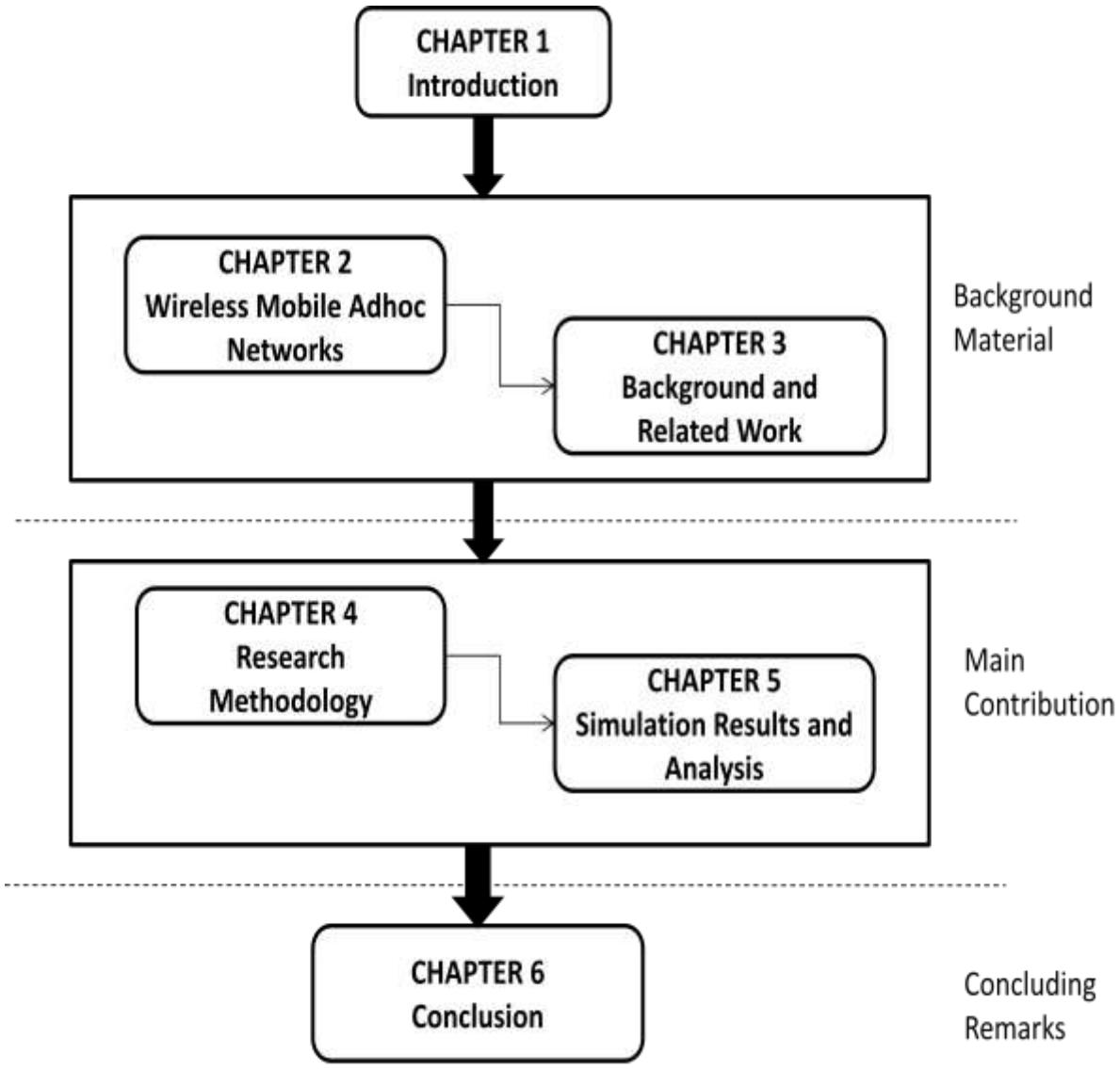

Figure 1 Dissertation Structure

CHAPTER 2

LITERATURE SURVEY: WIRELESS MOBILE AD-HOC NETWORKS

Introduction

Wireless Mobile Ad hoc networks are typically decentralized in nature. “Ad-hoc” is basically a Latin term meaning “for this purpose”. They are ad-hoc since they are independent of any pre existing centralized infrastructure. Instead, for routing and forwarding functions, each node acts as a router itself.

MANETs have now become quite an active research area since last couple of decades. This is mainly due to the advent of laptops and growth of 802.11/Wi-Fi wireless networking. MANETs usually have a networking environment that is routable on top of link layer network.

Several efforts have been made towards designing efficient routing protocol for multihop ad-hoc networks based on diverse set of assumptions. Application set of MANETs is quite diversified, from small, power constrained static network to large, highly mobile and dynamic networks. Majority of these protocols are usually designed for medium sized networks of 10 to 100 nodes. These protocols are evaluated on the basis of various performance metrics like end to end delays, network throughput, packet drop rate, routing protocol overheads etc.

2.1 Mobile Ad-Hoc Network

A Mobile Ad-hoc Network is a network consisting of a number of mobile hosts, also called MANET nodes, which communicate with each other over wireless channels without the need of base stations or any other centralized authority.

The interest in this field of research has been growing hugely over the last 20 years. MANETs provide wireless communication that is highly mobile, spontaneous and robust [1] in scenarios

where it's not possible or quite difficult to provide centralized infrastructure, for example, Vehicle to vehicle networks (VANETs), battlefield communications, disaster recovery operations etc. MANET nodes are characterized by limited resources like limited battery, processing ability, memory, constrained bandwidth etc.[2]. Hence, designing a reliable routing strategy that efficiently uses these confined resources is quite a difficult task. MANET hosts can move freely in the network, thereby causing frequent network topological changes. MANET nodes have the ability to configure them and can be deployed easily and urgently without any fixed configured network. They need not have any centralized authority or base station to assist in routing mechanism or data transmission. Hence, MANETs score an edge over other traditional wireless networks.

In these networks, all nodes themselves act as routers and are responsible for forwarding and routing operations.

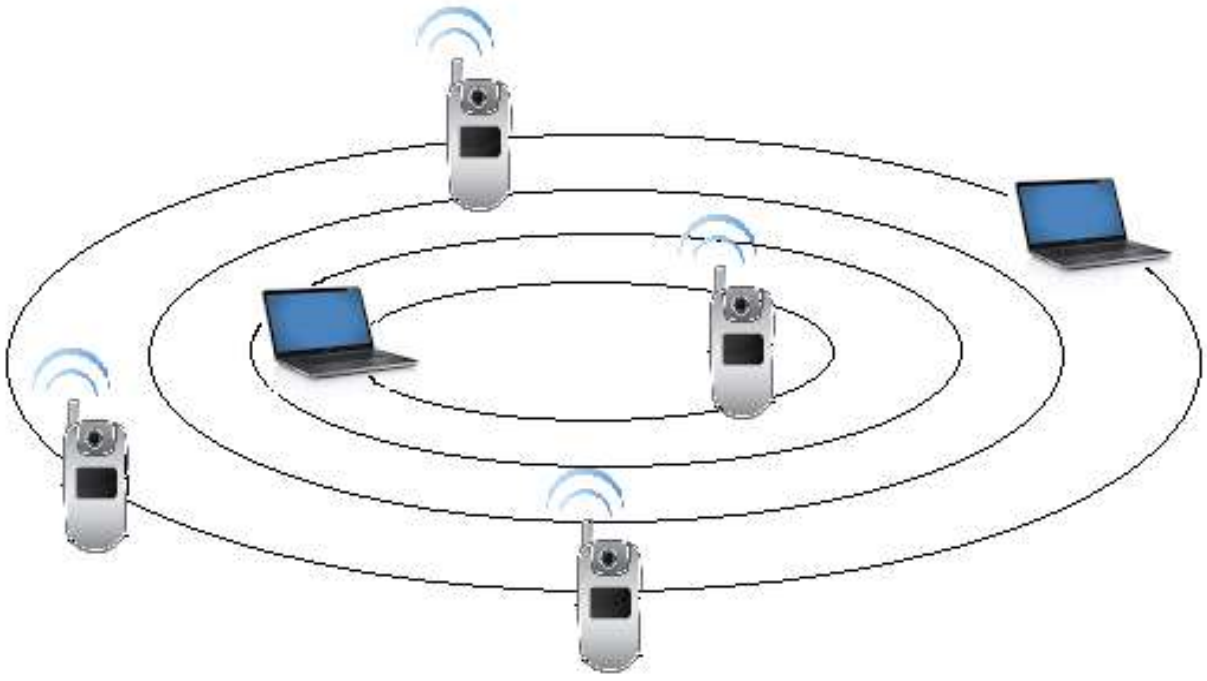

Figure 2 A typical MANET system

2.1.1 Characteristics

Mobile Ad-hoc Networks are mainly characterized by:

i) Scant Resources

The wireless channels between MANET nodes have lower capacities compared to those in wired networks. Also, due to signal fading, noise and interference, the link capacity available is often lower than the total capacity of channel. Therefore, network congestions are more common phenomenon in these networks compared to fixed networks [3].

Also, MANET routing strategies needs to be competent enough to deal with the issue of limited battery life so as to optimize resource usage.

Consequently, signaling protocols in Mobile Ad-hoc Networks are quite challenging to draft due to such resource constraints.

ii) Decentralized Architecture

Due to dynamic nature of MANETs, hosts are organized in a decentralized manner. Any central node or base stations that are usually responsible for controlling routing, forwarding and discovery functions are completely absent. Such architecture presents its usefulness by increasing ability to recover in case of breakdown and at the same time posing harder challenges in designing capable and effective protocols.

iii) Continuous changing Topologies

MANET hosts can freely move and due to their arbitrary movement, their topology will be changed frequently and repeatedly.

Also, the nodes might run out of battery power and gets switched off or restarted, thereby causing random changes in network topology. Hence, MANET protocols need to be robust enough to deal with these recurrent changes in topology.

Other general features of Mobile Ad-hoc Networks can be summarized as follows [4]:

- Wireless mode of communication
- Dual functional nodes, i.e. as hosts and as routers
- Bandwidth constrained
- Power constrained
- Higher frequency of routing updates

2.1.2 Applications

Mobile Ad-hoc Networks can be used in scenarios where either no already available infrastructure is present or is quite difficult to deploy due to factors like convenience or cost [5]. Examples of similar scenarios can be in disaster recovery or military applications where usual infrastructure has either been destroyed or is unavailable.

Another application can be in file sharing at conferences or any informal gathering or group of students interacting during a lesson or a presentation.

In brief, some major applications areas of Mobile Ad-hoc Networks can be summarized as follows:

- Defense exercises (in battlefields)
- Disaster relief operations
- Mining sites
- Business or informal gatherings
- Vehicular networks (VANETs)

2.1.3 Advantages of MANETs

For Mobile Ad-hoc Networks, following advantages can be identified:

- High mobility and portability irrespective of geographic position
- MANETs are easily deployable at any place and time

2.1.4 Disadvantages of MANETs

- Resource constrained
- Lesser physical security
- Decentralized infrastructure (lack of authorization)
- Compatibility issues [4]

2.2 Issues and Challenges for Routing in Mobile Ad-hoc Networks

Section 2.1 briefly outlined the influence of routing protocols on MANETs. This section presents a survey of literature on routing protocols in MANETs.

Routing has always been a popular and active topic for research. In the last two decades, there have been continuous efforts in designing correct and effective routing protocols for MANETs that can also deal with various constraints associated with these networks .[6]

Before describing the types of routing protocols, it is worth mentioning the development goals for a MANET routing protocol so that certain limitations specific to Mobile Ad-hoc Networks can be dealt with accordingly.

As has already been stated in previous sections of this thesis, some characteristics that define ad hoc networks includes resource constrained devices, limited battery power and bandwidth, security concerns and dynamic topologies. Therefore, exemplary design goals can be summarized for routing protocols for ad hoc networks:

i) **Minimal overheads**

Control messages exchanged during route discovery and other operations introduces unnecessary overheads by consuming battery power and bandwidth. Since these resources are critical and limited, routing operations should involve exchanging the minimum number of control messages between the nodes. This can help in conserving battery power [6].

Similarly, processing overheads are also introduced in the ad hoc networks due to algorithms that are computationally complex. This results in using up more resources and hence more battery power is consumed.

Therefore, research studies shows that it is advisable to implement protocols that are lightweight and involve minimal processing cycles so that battery power can be reserved for other useful tasks.

ii) **Multihop routing**

Because of limited transmission range of devices, it is required to use multiple hops to exchange data between source and destination hosts in a Mobile Ad-hoc Network since there is high possibility of them not being within each others' direct transmission range [6].

Therefore, for communication to be possible in the network, routing protocol must effectively be able to detect multihop routes.

iii) **Dealing with dynamic topologies**

In Mobile Ad-hoc Networks, route breakages are quite common due to unrestricted movement of nodes causing network topology to change continuously. Also, links can break due to devices getting switched off or restarted. So a path must be sustained during the movement of intermediate as well as end nodes.

Since a single channel is shared among multiple nodes, breakages must be treated rapidly with minimum delay and overhead.

iv) **Prevention of loops**

Generating loops that are free from loops is one of the substantial properties of a routing protocol. Protocols must also provide guarantees to produce fresh routes that consume fewer resources [7].

When a data packet encounters a loop while transmission, it may have to traverse the same path again and again [6]. This leads to wastage of already scarce resources like bandwidth and battery power and also results in packet loss in the network, hence making the forwarding process quite expensive. Therefore, loops must be avoided in MANETs since they are highly wasteful of resources.

v) **QOS guarantee**

In recent times, majority of focus has been shifted to providing QOS guarantees in MANET routing since MANETs are capable of supporting multimedia applications as well as real time traffic [5]. For such application, certain QOS parameters like delay, energy, bandwidth etc. needs to be taken into account. None of the traditional routing protocols deal with these characteristics in their implementation, but a lot of research is now being centered on extending these protocols with more functionality and are still under expansion. The primary goal of these QOS enabled routing protocols is to find the best QOS aware route from source to destination, not just the "shortest" one.

2.3 MANET Routing Taxonomy

With these goals in mind, several strategies for routing have been designed for Mobile Ad-hoc Networks. The proposed routing protocols fall into two broad categories:

i) Reactive (On demand) approach

ii) Proactive (table driven) approach

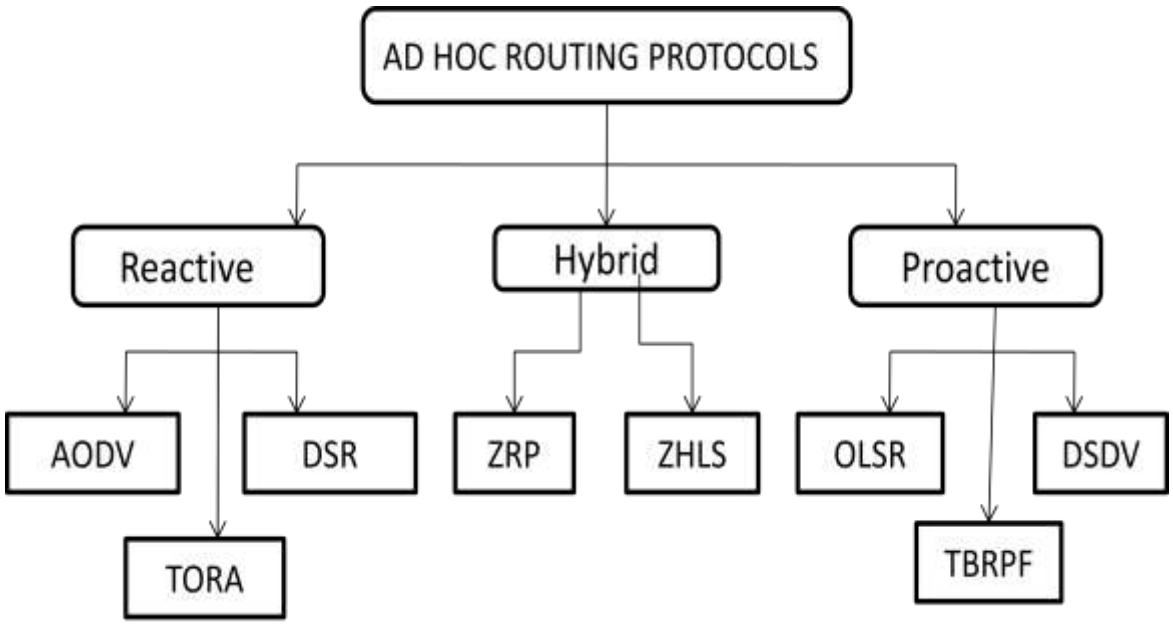

Figure 3 Classification of routing protocols in MANETs

i) <u>Reactive protocols</u>

Reactive protocols determine routes only when a source node has data to send to a destination node. If the route from the source to required destination is not already available, the source node initiates a route discovery operation to find the needed routes. In route discovery operation, a request message is flooded throughout the network resulting in reply messages from a subset of nodes. The most optimum route out of the search results is used for connection establishment and transmission till the chosen path is being used or till it becomes invalid or gets unavailable or broken [7].

DSR and AODV are the most widely used routing protocols based on On-Demand strategy. The most peculiar advantage of reactive routing approaches is their ability to immediately present a route when needed, thus eliminating any extra overheads in maintaining static routing tables.

Protocols belonging to this category discover the routes when required or demanded, hence also called as On-demand protocols.

Reactive protocols do not consume any bandwidth when any node is not sending data packet, which means, bandwidth is only consumed when the node has some data to transmit to a destination. They considerably reduce network bandwidth overhead and battery power since no routing advertisement or update messages are exchanged in the network.

ii) Proactive protocols

The proactive routing approaches for Mobile Ad-hoc Networks have originated from the distance vector and link state protocols for wired networks [6].

In proactive protocols, a route is always available between every two nodes in the network. Periodic route update messages are propagated in the network for the purpose of route creation and maintenance. Periodic updates are exchanged between nodes at specific intervals irrespective of traffic state and mobility of nodes. On the other hand, event triggered updates occurs only when some specific event like link breakage or addition takes place. Since an increase in node mobility has a direct impact on link changes, hence frequency of event triggered updates also increases.

In this category of protocols, routing information is maintained in number of routing tables. These tables are updated in the manner as discussed as above, therefore also called as Table-driven routing protocols.

The primary advantage of proactive protocols is the availability of consistent and up-to-date routes in routing tables between all nodes at all times in the network. However, a major disadvantage is in terms of large overheads incurred in creation, updation and maintenance of these routing table since table updation can become quite frequent in case of high mobility.The most widely used proactive routing protocols in Mobile Ad-hoc Networks are:

a) Destination-Sequenced Distance Vector (DSDV)

b) Optimized Link State Routing (OLSR)

iii) Hybrid routing protocols

A routing scheme that is purely proactive is not suitable for MANET environment due to large overheads associated with routing tables. In the same way, a pure reactive protocol cannot be completely successful in MANETs due to its associated disadvantages. Hence, certain characteristics of both these approaches can be integrated to form an enhanced class of ad-hoc networking routing protocols, called as Hybrid protocols [6]. These protocols demonstrate reactive behavior in some instances and proactive one in other set of circumstances; hence they allow flexibility and scalability in the MANET environment by assuming the entire network as being partitioned into zones [8].

Examples of Hybrid routing protocols are:

a) Zone Routing Protocol (ZRP)

b) Zone-Based Hierarchical Link State Routing Protocol (ZHLS)

This thesis will mainly concentrate on one of the most popular and widely used reactive routing protocol, AODV and the way in which it can be enhanced to provide some degree of support to some Quality Of Service (QOS) metric. Therefore, this literature will focus mainly on AODV and the operations associated with this protocol for route discovery and establishment.

2.4 Ad-hoc On-demand Distance Vector (AODV) routing protocol

The Ad-hoc On-demand Distance Vector protocol is an ad-hoc network routing protocol that is purely reactive in nature because no routing tables are needed by the nodes to maintain any routing information. AODV is based upon DSDV and DSR routing protocols [2]. Being an on-demand protocol, AODV maintains information only “active” routes.

In AODV, a node can either be a source or a destination or an intermediate node. If a source node has some data to send to a destination, it checks its routing table to decide whether it has an already available “working” route [6]. In case no such route exists, it performs a route

discovery operation to find the needed path. The route discovery process is dynamic and is accomplished in MANETs through various control messages. If there isn't any transmission ever between a pair of nodes, they need not to maintain a path between each other, hence saving on resources that otherwise would have been wasted in maintaining a path between them.

AODV inherits and enhances some of the typical features of DSDV protocol like periodic beaconing, multihop routing between participating nodes and sequence numbers. AODV ensures freshness of routes through sequence numbers. Periodic beaconing is the time to time exchange of Hello messages in the network used for identifying the neighboring nodes.

AODV accomplishes the complete process of routing through the following two mechanisms:

a) Route Discovery

b) Route Maintenance

Route Discovery

AODV uses a combination of two messages for accomplishing route discovery in Mobile Ad-hoc Networks:

a) Route Request (RREQ)

b) Route Reply (RREP)

When a source node wants to establish a connection with a destination for data transmission, it sends the RREQ message to all its immediate neighbors. RREQ contains the IP address of the source and the destination, a pair of fields related to sequence numbers and a hop count field initialized to zero. Each RREQ message is uniquely identified by a RREQ ID which goes on increasing with each newly generated RREQ in the network [6]. If a node receives an already processed RREQ via some other neighbor node, it is discarded. The source broadcasts this RREQ to its immediate neighbors. The neighbor nodes on receiving the RREQ, generates a

backward route to the initiating source. Also, the hop count (distance from source node) in RREQ message format is increased by one.

The node receiving the RREQ checks its route table for the availability of fresh route(s) to the required destination. If it does not have any such route, it simply rebroadcast the RREQ further to its immediate neighbors with the previous hop count value being incremented. Hence, to search a valid route to a destination, RREQ packet is flooded in the network.

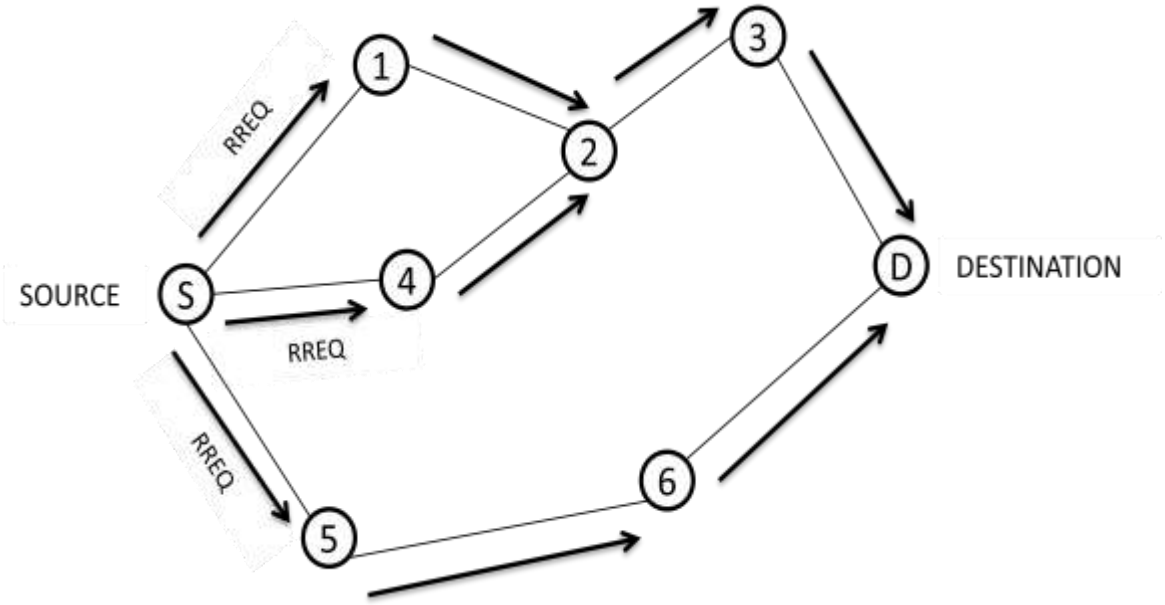

Figure 4 Flooding of Route Request (RREQ) packet

On the other hand, if the node receiving the RREQ is itself the destination or it does have an unexpired route to the required destination with the sequence number of the path to that destination (indicated in node's routing table) greater than or equal to the sequence number mentioned in the RREQ message, the node creates a *Route Reply* (RREP) message and transmit that on the backward route it created towards the node that sent RREQ. Hence, the backward node that was created during RREQ broadcast from source is now utilized for sending RREP back to the source node.

RREP packet contains the source and destination IP addresses, the sequence number of the path to the destination as indicated in the node's route table and the hop count field set equal to the distance between the node and the destination. The hop count is zero if the destination is creating and sending the RREP itself.

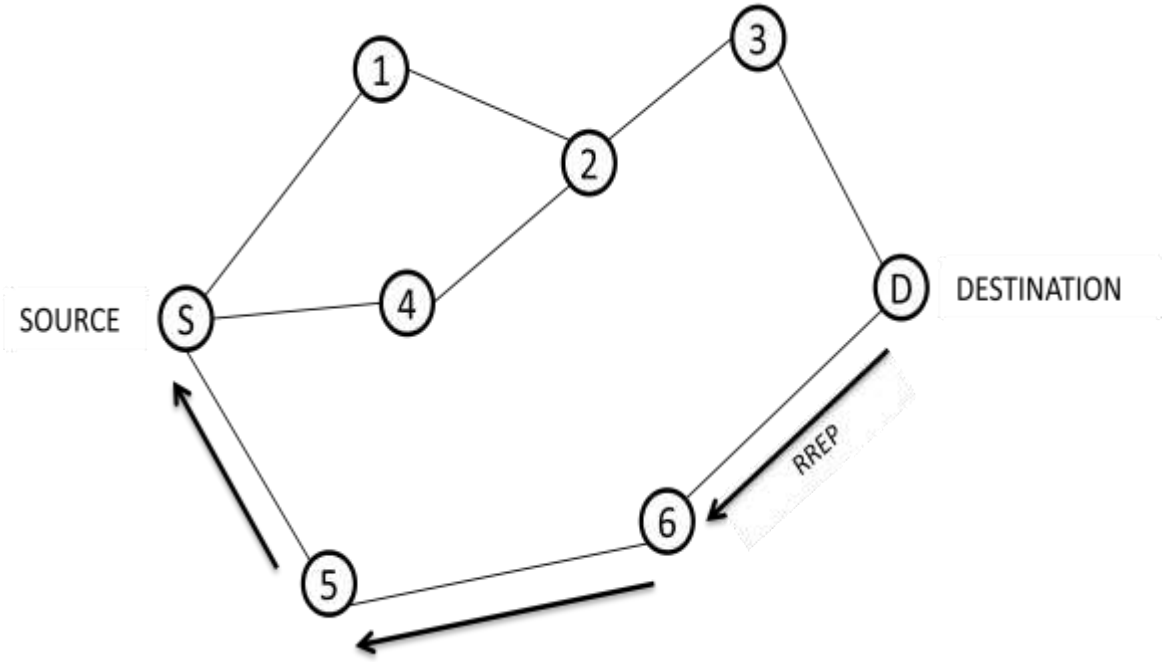

Figure 5 Propagation of Route Reply (RREP) packet

As soon as the source node receives an RREP from the destination, the source start utilizing the discovered path for transmission of data packets, till it expires or the topology changes.

Route Maintenance

After establishment, a route is maintained as long as it is "actively" in use. A path is said to be "active" if it is being used for the transmission of data packets. After the ongoing transmission along the path from source to destination stops, the link will eventually expire and will be removed from the routing tables of neighbor nodes. Another possibility may occur when the link

breakage occurs while it is still active. This may happen as a result of sudden topological changes due to mobility of nodes. Link breakages along an active path must be repaired as soon as possible to avoid packet drops and decrease in overall throughput of the network. In such cases, the node upstream of the point of link break creates a *Route Error* (RRER) message and propagates it towards the source node via its upstream neighbors that were using that link. The RRER message is used for invalidating the broken paths. The source node, after receiving the RRER, can either repair the route or can initiate a new route discovery operation. If the source initiates the route repair, it is termed as a Global repair strategy.

In AODV, a route repair process can also be carried out locally. A local route repair is where the intermediate nodes themselves try to repair the route locally instead of sending an RRER message to the source. The major advantage of the local route repair is the fact that since the route is repaired sooner compared to the global approach, hence lesser number of data packets will be dropped. If local repair is unsuccessful, the repair can be executed globally as described.

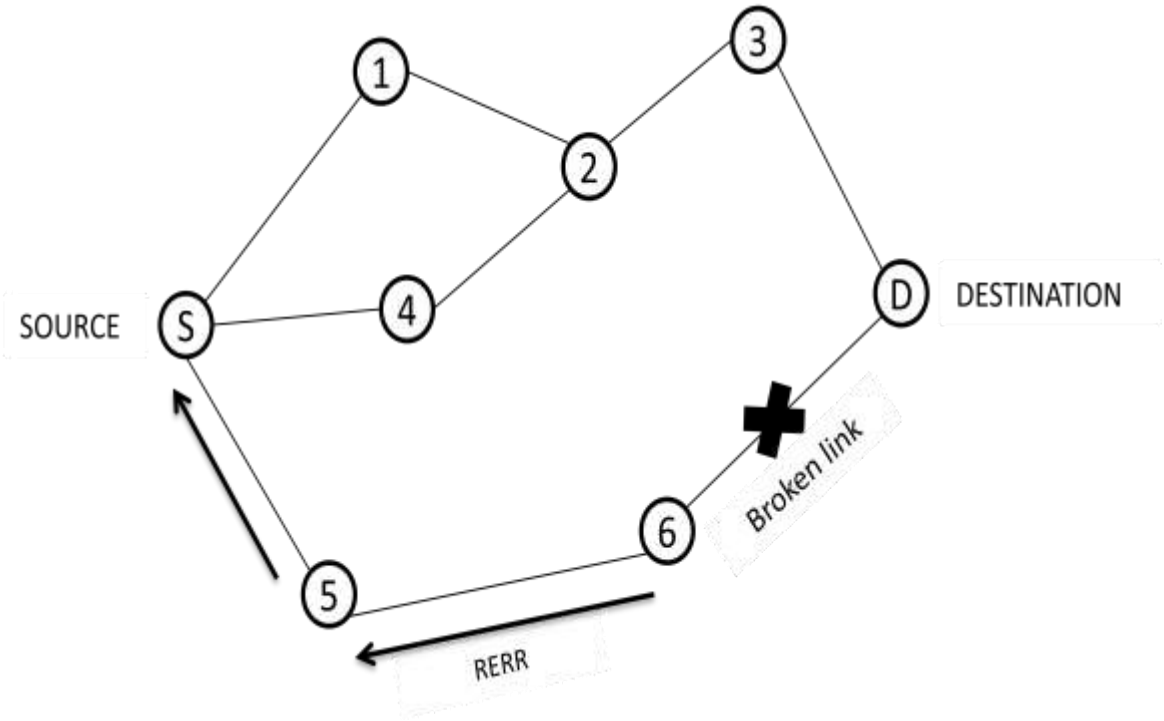

Figure 6 Propagation of Route Error (RERR) packet for Route maintenance

2.4.1 AODV Messages

a) Route Request (RREQ)

The broadcast of RREQ message is initiated by the source node that wish to communicate with another node in the network. A time to live (TTL) value is associated with every RREQ message that indicates the number of hops till RREQ can be transmitted. If the source node has no route in its routing table for the required destination for data transmission, it initiates route search by broadcasting RREQ to its adjoining neighbors. Two separate counters are maintained at every node, node sequence number and broadcast ID of source node.

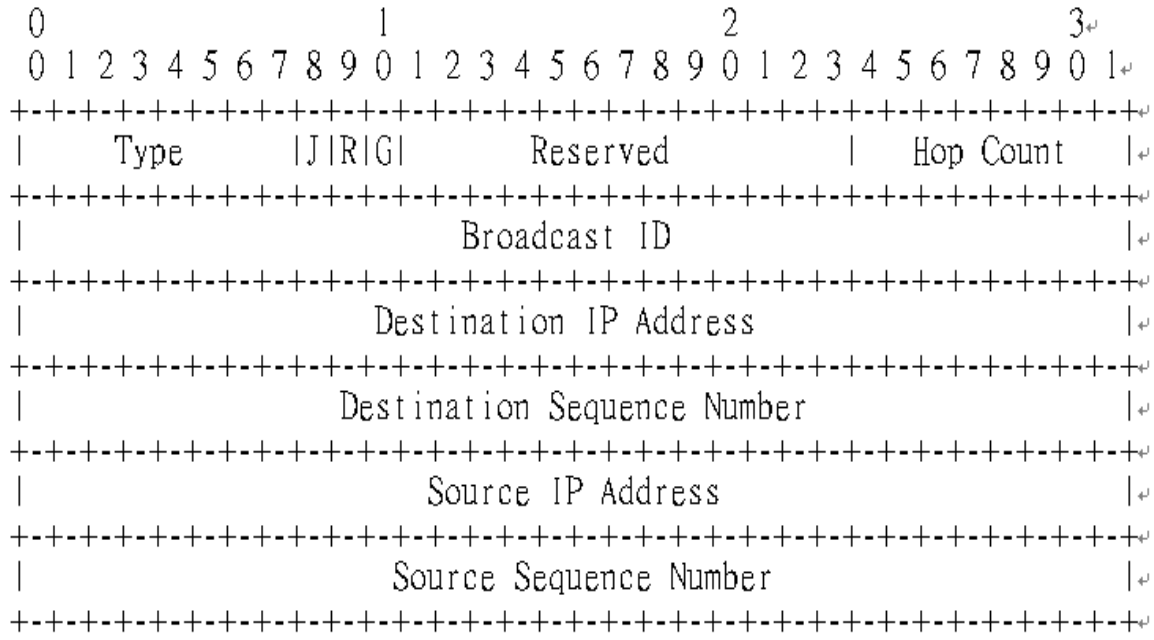

Figure 7 Packet format: RREQ [9]

The RREQ message format, as shown above, comprises of the following fields:

TABLE 1 FIELDS IN RREQ MESSAGE FORMAT

Fields/flags	**Meaning**
J	Join, reserved for multicast
R	Repair, reserved for multicast
G	Gratuitous, denotes whether a gratuitous RREP should be unicast to the IP address of the destination
D	Destination only, specifies that only the destination can respond to this RREQ
U	Unknown sequence number, shows that the sequence number of the destination is unknown
Type	1
Reserved	Contains zero while sending which is ignored on reaching destination
Hop Count	Distance (in hops) from the source to the node handling the RREQ message
RREQ ID	A sequence number that uniquely identifies the RREQ message in combination with the

	source node's IP address
Destination IP address	IP address of the destination for which the path is required
Destination sequence number	The last sequence number received by the source for any path towards the needed destination
Source IP address	IP address of the node that initiated the route request
Source sequence number	Current sequence number to be used in the route entry indicating towards the RREQ initiating source

b) **Route Reply (RREP)**

The destination node or any intermediate node that has a path to the requested destination sends an RREP message back to the source after receiving RREQ.

The RREP messages are transmitted on the backward routes set up by the intermediate nodes while broadcast of RREQ during route discovery.

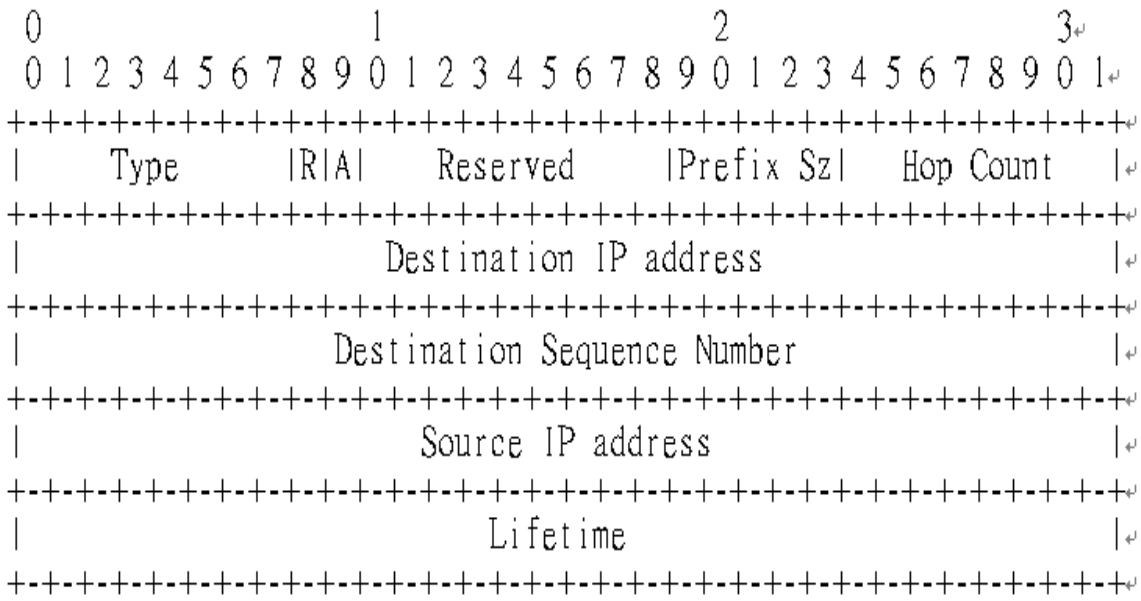

Figure 8 Packet format: RREP [9]

TABLE 2 FIELDS IN RREP MESSAGE FORMAT

Fields/flags	**Meaning**
Type	2
R	Repair, reserved for multicast
A	Acknowledgement required
Reserved	Contains zero while sending which is ignored on reaching destination
Prefix size	Is a non zero value. This 5-bit field means that next hop can be used for any node with

	the same routing prefix as the required destination
Hop Count	Distance (in hops) between the source IP address and the destination IP address
Destination IP address	IP address of the destination for which the route is being provided
Destination Sequence number	The sequence number associated with the route towards the destination
Source IP address	IP address of the node that initiated the RREQ propagation
Lifetime	Time (in milliseconds) for which the route will be considered valid by the nodes receiving the RREP

c) **Route Error (RERR)**

Apart from the primary messages for route establishment, RREQ and RREP, an additional message is exclusively meant for route maintenance, i.e. RERR.

RERR message is sent to initiate route repair in case of link breakage.

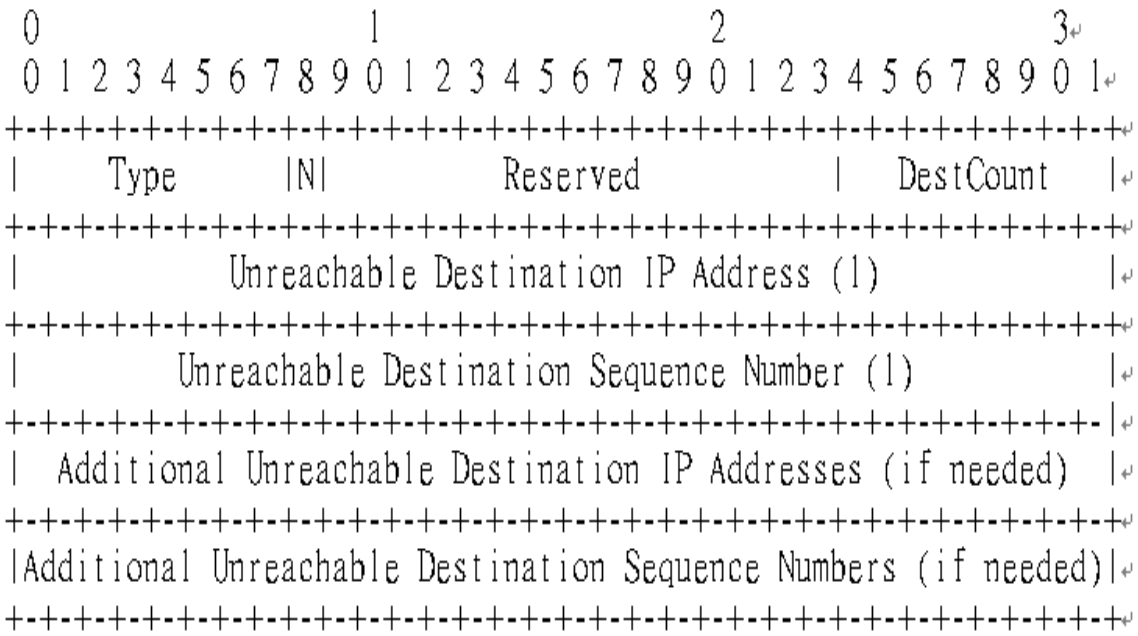

Figure 9 Packet format: RERR [9]

As shown above, the message format of the RERR packet contains the following fields.

TABLE 3 FIELDS IN RERR MESSAGE FORMAT

Fields/flags	Meaning
Type	3
N	No delete; this flag is set when the link has been repaired and used to indicate to upstream nodes that the link is functional and should not be deleted from their route tables

Reserved	Contains zero while sending which is ignored on reaching destination
DestCount	The total number of unreachable destinations; must be atleast 1
Unreachable destination IP address	The IP address of the destination that has become unreachable due to link breakage
Unreachable destination sequence number	The sequence number in the routing table entry of the unreachable destination whose IP address was mentioned in the "Unreachable Destination IP address" field of RERR message

The RERR message is transmitted in the network when one or more destinations become unreachable as a result of link breakage.

2.4.2 Characteristics of AODV

- Multiple mode of communication: Unicast, Broadcast and Multicast
- Route establishment is On-Demand
- Effective link repair strategies in case of breakages: Global or Local repair
- Generation of loop-free and fresh routes with the help of sequence numbers
- Keeps track of only next hop instead of the entire route, hence reducing the overheads considerably
- Exchange of periodic beacon messages to trace and identify neighbor nodes
- Reduced number of routing messages in the network

2.4.3 Limitations of AODV

- The delay involved while establishing the route is quite large as compared to other reactive routing protocols
- More overheads, with respect to bandwidth and energy, required to maintain the routing table in case of high node mobility
- In case of Global repair, the throughput of the network reduces since more and more packets are dropped till the time RERR reaches the source which then initiates the repair
- Periodic exchange of beacon messages and generation of multiple RREP messages in response to a single RREQ message can cause unnecessary wastage of bandwidth and generate control overheads
- If the source sequence number is not updated from a long time and the intermediate nodes do not have the latest sequence number of the destination, this can lead to inconsistent routes since they will have stale entries in their route tables.

CHAPTER 3

BACKGROUND AND RELATED WORK

In this chapter, we provide a survey of the background information on Quality Of Service in ad-hoc networks. Initially, an explanation of the basic concepts on QOS in Mobile Ad-hoc Networks is provided in section 3.1 followed by a brief description of various QOS design considerations associated with MANETs, in section 3.2. The chapter will be concluded by summarizing various related research work undertaken in the field of providing QOS enhancements to routing protocols for Mobile Ad-hoc Networks.

3.1 Quality Of Service in MANETs

With the proliferation of inexpensive and infrastructure-less mobile ad hoc networks (MANETs), research focus has shifted to issues related to security and quality of service (QoS) in these networks. MANETs are collections of mobile hosts (also called nodes), which are self-configurable, self-organizing, and self-maintainable. The nodes communicate with each other through wireless channels with no centralized control. With the evolution of wireless prevalence in the last decade, we are witnessing more and more applications moving and adapting to wireless methods to communicate. MANET nodes rely on multihop communication; that is, nodes within each other's transmission range can communicate directly through radio channels, whereas those outside the radio range must rely on intermediate nodes to forward messages toward their destinations. Mobile hosts can move, leave, and join the network whenever they want, and routes need to be updated frequently because of the dynamic network topology [10].

In MANETs, one of the important issues is routing, that is, finding a suitable path from a source to a destination. Because of the rapid growth in the use of applications, such as online gaming, audio/video streaming, voice-over IP (VoIP), and other multimedia streaming applications in MANETs. It is mandatory to provide the required level of QoS for reliable delivery of data. Providing the required QoS guarantees in wireless multihop networks is much more challenging

than in wireline networks mainly because of its dynamic topology, distributed on-the-fly nature, interference, multihop communication, and contention for channel access. In particular, it is important for routing protocols to provide QoS guarantees in terms of metrics, such as achievable throughput, delay, packet loss ratio, and jitter.

Despite the large number of routing solutions available in MANETs, their practical implementation and use in the real world is still limited. Multimedia and other delay- or error-sensitive applications that attract a mass number of users toward the use of MANETs have led to the realization that best-effort routing protocols are not adequate for them. Because of the dynamic topology and physical characteristics of MANETs, providing guaranteed QoS in terms of achievable throughput, delay, jitter, and packet loss ratio is not practical. So QoS adaptation and soft QoS have been proposed instead [11]. Soft QoS means failure to meet QoS is allowed for certain cases, such as when a route breaks or the network becomes partitioned [11]. If node mobility is too high and topology changes very frequently, providing even soft QoS guarantees is not possible.

QoS in MANETs is defined as a set of service requirements that should be satisfied by the network when a stream of packets is routed from a source to a destination [12]. A data session can be characterized by a set of measurable requirements, such as maximum delay, minimum bandwidth, minimum packet delivery ratio, and maximum jitter. All the QoS metrics are checked at the time of connection establishment, and once a connection is accepted, the network has to ensure that the QoS requirements of the data session are met throughout the connection duration [13].

QOS guarantees the network to provide a set of definite service and performance features with respect to jitter, bandwidth, end to end delay and packet loss probability.

Several enhancements to existing routing protocols for MANETs have been proposed aiming on choosing routes based on the above QOS metrics, delay being one of them [14]. Delay aware protocols reckon delay as the chief QOS metric for discovering routes for a source-destination pair, i.e., the paths are selected based on delay constraints provided by the application. Delay can be in the form of routing delay, end to end delay, propagation delay, delay jitter etc. [14]. A

major issue with the routing strategies in current scenario is that they are not designed to support QOS metrics, hence delay aware protocols comes into picture to deal with this problem.

3.2 QOS provisioning in MANETs: Issues

The performance of QOS based solutions is hugely influenced by several design issues. In earlier routing protocols, no provision for QOS support existed. For an application to be QOS enabled, a route with ample resources to fulfill rigid QOS demands should be used.

Challenges in QOS provisioning over MANETs

A brief description of major issues encountered in MANETs while providing QOS enhancements to routing protocols are given below:

i) Uncertain physical features

Wireless channels are quite prone to errors that occur due to interference because of simultaneous transmission by neighbor nodes, fading, noise etc.

ii) Decentralized network architecture

Inherent nature of MANETs i.e. being easy to deploy, quite inexpensive and infrastructure-less seems extremely promising for being used in variety of domains. Being decentralized, MANET hosts are required to send their QOS state information to all other hosts, thereby making QOS aware protocols quite complex and prone to overheads.

iii) Contention for channels

In MANETs, nodes talk to each other through shared channels. This communication is necessary so that most updated information about network states, routes and nodes must be exchanged among nodes. This frequent communication will eventually result in high collision due to interference among node signals causing increase in battery consumption and delay along with decrease in packet delivery ratio and link bandwidth utilization.

iv) Multihop mode of communication

Apart from being the host devices, MANET nodes also function as routers and perform the basic operations of forwarding packets between source and destination. Prior to forwarding, an optimal route is discovered with the help of intermediate nodes. The data is then transmitted on the discovered path hop by hop through intermediate nodes; hence if failure occurs in even a single node, the entire MANET transmission can fail.

v) Resource constraints

The mobile devices that constitute the entire MANET system have limited available battery power, processing ability, speed of operation and limited on-board memory space. Also, compared to wireline networks, the channel capacity is lower in wireless networks. Due to above mentioned constraints; resources need to be managed efficiently for their best utilization in traditional as well as QOS aware scenario.

3.3 Related Work

This section gives a summarized overview of various research work undertaken previously in the field of providing QOS aware capabilities to existing routing protocols in Mobile Ad-hoc Networks. In past decade, many delay aware extensions have been proposed to earlier routing protocols like AODV, DSR and OLSR to make them QOS capable. This section includes a summarization of some recent studies on QOS enhancements to existing routing protocols. We will here concentrate on delay metric as the primary metric for QOS aware protocols.

In [15], Shen Ting Zhi et al. applied certain modification to AODV to mitigate the delay issues present in AODV, simultaneously ensuring optimal utilization of battery power. Their approach was based on the received Log Likelihood Ratios(LLR) on the basis of which the intermediate hosts decide whether to take part in the transmission or not, hence the nodes that decide not to communicate saves quite a considerable amount of energy. Also, the nodes function at high transmission range if the traffic is real time in nature; as a result end to end delay is greatly reduced due to decrease in number of intermediate nodes.

In literature [16], the authors have developed a QOS aware routing approach for Mobile Ad-hoc Networks based on Dynamic Source Routing (DSR) that focused on two metrics: energy and delay. They named their approach as DSR_ED. They introduced some new fields in packet formats of RREQ, RREP and RERR messages. These new fields are specific to the two metrics used. This method claims enhanced timeliness and efficient utilization of energy by avoiding nodes that are busy and low on battery power. This concept makes routing decisions based on residual energy levels of the nodes. Hence, this proposed method (DSR_ED) uses the network resources optimally, decreases latency and prolongs network lifetime.

Sudheendra Murthy et al. introduced a new routing protocol in [17] which they named as LDAR (Link Delay Aware Routing). LDAR is based on a new metric that takes into consideration the various kinds of delay experienced by the link, namely, processing delay, queuing delay and transmission delay. The proposed metric for link delay avoids any additional network overhead and supports varying link rates.

In literature [18], authors proposed a novel routing approach which they named as CODAR (Congestion and Delay Aware Routing). CODAR conducts routing by taking care of delay and congestion in the network. Each node gathers information individually as in a distributed system. CODAR avoids congested nodes during route establishment process itself and precisely adjusts nodes' data rate during congestion mitigation. Hence, by considering congestion parameters during routing operations, CODAR provides reliable and well-timed detection of crucial incidents in the network.

In literature [19], authors have designed an energy aware and delay aware routing protocol by adopting a time delay function in flooding RREQ packets. This function varies inversely with the remainder battery power of the intermediate nodes. They named their proposal as Time Delay On-demand Multipath routing protocol (TIDOM). TIDOM is an extension to AODV. The time delay function promotes nodes having good battery backup and avoids those nodes having poor residual battery power. Authors have proved through Qualnet simulations that TIDOM is capable of conserving battery capacity of the constituent nodes, increasing packet delivery ratio,

decreasing overheads, increasing lifetime of links and hence, increasing lifetime of the network as a whole.

Another delay aware routing aware routing approach has been proposed in [20] named by the authors as Delay aware Multipath Source Routing (DMSR) protocol. This approach is QOS capable for real time multimedia applications in adhoc networks. This protocol introduces node delay as a QOS metric to assess the node's state. For admission control, the metric considered is accumulation delay and for selecting the path, the metric used is node delay. The authors have proved DMSR to be better performing than DSR in terms of packet delivery ratio, average end to end delay and throughput.

Authors in reference [21] have proposed another QOS aware routing method extended from the AODV protocol, which they named as Delay Aware Ad-hoc Multipath (DAAM). DAAM considers end to end delay as the chief metric for selecting route between source and destination, instead of hop counts. Nodes stores more than one path for a pair of source and destination hosts in the routing table along with their respective end to end delays. If a node fails, alternative route is searched for in the routing table before starting a new route discovery operation. Authors have proved that DAAM lowers end to end packet delays and jitter of multimedia traffic and considerably reduces routing overheads compared to traditional routing protocols like AODV, OLSR and DSR.

CHAPTER 4

RESEARCH METHODOLOGY

This chapter will present the detailed explanation of the research work carried out in this thesis in the field of QOS provisioning in Mobile Adhoc Networks. In section 4.1, we have introduced various methodologies being used for carrying out research works across the globe and why simulation is the preferred method for research activities in ad hoc networks. Section 4.2 introduces the approach of delay aware routing in MANETs using on demand approach. Section 4.3 will present the detailed version of our proposed protocol DS-AODV followed by its extended working.

4.1 Research Paradigm

In networking and related areas, several methodological approaches for evaluation and analysis of routing protocols are used. These can be either of the following methods:

- Direct/real experiment
- Analytical modeling
- Computer simulation

Real experiment is capable of providing quite accurate results since the research is performed in real world scenario. In such scenarios, the influence of the surroundings on the setup can be experienced in practice. But this method has its limitations in terms of high costs and complexity associated with practical setup of real world Mobile Adhoc networks. Since MANETs require huge resources and efforts to perform the performance evaluation and experiments.

Analytical modeling involves mathematical computations and their analysis. This research method is quite inefficient in handling the dynamic nature of MANETs. Hence, the performance of this experimental methodology is limited.

A simulation process constructs model of a system [7] consisting of an issue and thereafter carrying out experiments with the help of that model using a computer program, also called as a simulator. The simulator helps to solve the given problem. The simulator or the simulation tool helps to predict the behavior of a real world problem as well as model it in a system.

Simulation is the most efficient and widely used software based method for comparing the performance of existing protocols as well as for performance evaluation of new protocols in the field of networking. In order to produce accurate results, detailed knowledge about a simulation tool is needed. Simulation encompasses an array of processes like validation of parameters, graphics showing operations, comparison, validation of historical data that needs to be compared with data generated during simulations and their analysis.

The research in this thesis is carried out using simulation method. This method has a prominent advantage over other research methodologies (discussed earlier in this section) as it uses lesser assumptions, is more flexible and easy to use and can efficiently handle complex routing algorithms.

To address one of the most vital QOS metric in MANET routing protocol i.e. Delay, we have proposed a delay aware routing protocol based on AODV, Delay Sensitive AODV (DS-AODV), whose performance has been examined on the MANET scenarios constructed using a powerful simulation tool "Exata Cyber" using the simulation methodology.

4.2 AODV based Delay Aware Reactive Routing Protocol

In this section, we will give a brief overview of our proposed delay aware protocol based on AODV which we named as DS-AODV (Delay Sensitive Ad hoc On-demand Distance Vector) algorithm.

In Mobile Ad-hoc Networks, source and destination communicate with each other in hops (if source is not in direct contact with the destination) after a valid route is discovered by the source using the route discovery mechanism. This is done by means of request and reply messages namely RREQ and RREP, initiated by source and destination respectively and forwarded by intermediate nodes.

In AODV routing protocol, route discovery is accomplished in a “reactive” manner, i.e. valid route is discovered between source and destination as and when needed by the source for packet transmission, and thereafter, the route is deleted after use. Another approach for discovering routes in MANETs is the proactive one that maintains static routes between each source-destination pair, hence also called as static table driven approach. Proactive protocol discovers all possible routes between all possible source-destination pairs at the network startup only. The discovered routes are maintained in static routing tables and updated periodically due to network topological changes by various control messages. Since this research is centered at AODV, we will focus on reactive/on demand mechanisms only.

Apart from route discovery, AODV is also capable of finding out broken links as well as repair them by its route maintenance mechanism. A node comes to know about a broken link when it forwards the data to the intended destination on a link and despite repeated retransmissions, fails to get an acknowledgement. The broken route is notified to the source by an RERR message. The source on its reception, initiates a fresh route discovery process for the same destination.

As discussed previously in **Chapter 3,** QOS provisioning is quite a mandatory requirement for delay sensitive multimedia applications like video, voice etc. and other real time applications where the time aspects of data arrival and sending are considered vital. For most of the traditional routing protocols for MANETs, shortest path/least number of hops is considered as the chief metric for best route to be searched. But this metric becomes insignificant in case of the above mentioned QOS aware applications.

Hence, attention needs to be shifted on QOS metrics like bandwidth, delay, energy etc since the existing routing protocols do not take into account these aspects. So, for modern day adhoc networks, it is desirable for the routing protocols to incorporate QOS awareness in discovering a route for supporting end to end QOS provisioning. This can be done either by proposing new QOS aware routing protocols or by incorporating certain enhancements to traditional routing protocols to make them QOS oriented. Out of these two, the later seems a better approach in terms of feasibility, time consumption and effort.

To address the issues associated with delay constraints in real time MANET applications, this thesis will also follow the later approach by modifying the most widely used routing protocol, AODV, to make it delay aware since delay is the most critical QOS metric while considering real time applications. Delay aware protocols selects path between source and destination on the basis of delay constraints of requesting application.

Here, we propose a reactive AODV based Delay Sensitive routing protocol (DS-AODV) that discovers path between a Source-Destination pair on which application traffic can be sent within the specified delay bound. The proposed protocol will make required enhancements to AODV and extend its capabilities to make it discover valid routes within the delay threshold of the requesting application.

4.3 Delay Sensitive AODV (DS-AODV) Routing Protocol

Our proposed routing protocol DS-AODV is based on AODV routing protocol. DS-AODV will try to search delay aware path during the route discovery stage. With this approach, we will be able to provide some degree of QOS, in terms of end to end delay, to the application by searching suitable routes on which traffic can be transmitted from source to destination within bounded delay. If such a route is not available in the network, our proposed solution will reject the source's request for the session admission in the network, thus avoiding the overloading of network. In this way, DS-AODV ensures that the flow transmissions are not degraded due to incorrect admission of new sessions in the network.

For selecting the base routing protocol for our research, the motivation for choosing AODV mainly comes from its popularity and widespread use in adhoc networks. Apart from that, distance vector routing, being simpler, doesn't need much computations and memory.

The subsection below will provide explanation of our proposed routing algorithm DS-AODV.

4.3.1 DS-AODV Message Formats

DS-AODV uses mainly two control message during the route discovery phase of its connection establishment. The initial message used by the requesting source application for requesting a route towards the destination is called the RREQ message. The response message for RREQ is named as Route Reply (RREP). Apart from these two, DS-AODV also uses the Route Error (RERR) message which is particularly used for route maintenance operations, i.e., for reporting broken links to the source node so that it can carry out route repair and initiate new route discovery process for finding an alternate valid route.

RERR packet used in DS-AODV is exactly same as the one being used in traditional AODV, whereas to impart delay aware capabilities, we have added some extra fields in the message formats of RREQ and RREP messages so that delay oriented routes are discovered in the route discovery process. In the text that follows, these extra fields are depicted in bold.

a) **RREQ** (msg_type, source, source_seq, dest, dest_seq, broadcast_id, hop_count, **max_delay, offset_time**)

   The usual fields that are part of the RREQ message have already been discussed in section 2.4.1 in detail. To these fields we have added a couple of fields to search delay bounded routes.

   Max_delay: this field is used to carry the delay specified by the requesting application i.e. the maximum delay that can be tolerated by a delay sensitive application running at the source node S. Hence, this is through this field that the source node specifies the delay bound for the source application that wants to establish a route with destination D.

   Offset_time: when the RREQ message is forwarded hop by hop by the initiating node S to its intermediate nodes that in turn forwards it to their neighbor nodes until it reaches D. During this process, at any node N, offset_time field of RREQ carries the time that is spent by the RREQ message from the source S till the current node N. The value of this field is updated by each node in the process of RREQ forwarding till it finally reaches D. In brief, this field contains the cumulative delay upto the node that is currently processing the packet.

The above two fields are added in our proposed solution to ensure its delay aware property.

b) **RREP** (msg_type, source, source_seq, dest, dest_seq, **max_delay, offset_time**)

Like RREQ, the usual fields that are part of the RREP message have already been discussed in section 2.4.1. The two extra delay aware fields that we have added to RREQ packet format, are part of RREP message also that originate from the destination after arrival of RREQ.

The function of these new fields **max_delay** and **offset_time** is same as that discussed under RREQ in the above text, except the fact that now the "requesting application at source" is replaced by the application running at destination D. The rest of the procedure is same as discussed above in RREQ message format.

c) **RERR** (msg_type, unreachable_dest_list)

A Route Error message is meant to notify the source S of a broken path to the destination D. This is done so that the waiting time at source is reduced and it can initiate a new route discovery operation to find an alternate valid route to D to accomplish the data transmission. In DS-AODV, this packet is the same as the one that is used in traditional AODV routing protocol.

d) **DATA** (Type, **Source**, Destination, NextHop, Payload): The data packets contains their source and destination addresses and the next hop for the destination from the routing table of the node that forwards this data packet.

4.3.2 Data Structures

In a mobile adhoc network, each node maintains various tables that contain values used for data forwarding as well as keeps the routes and information used during route discovery.

The seen_table is used by the node on receiving a RREQ message to identify whether this RREQ is a unique message or a duplicate RREQ from some other node. The routing table is also maintained at each node and contains routes for the destination of the active data transmission in the network.

- **Seen_table:-** This table is used by each node whenever it receives a RREQ message from any of its neighbor nodes to identify whether it has received the same RREQ previously from some other neighbor node. This is necessary since in a typical MANET topology, it is highly probable that a node may receive the same RREQ from its multiple neighbours and hence, the already scarce MANET resources are wasted. Hence this table is used to avoid that.

This table contains the combination of source address and broadcast_id from the received RREQ. This combination uniquely identifies a particular RREQ in the network.

- **Route_table:-** The route_table contains an up-to-date list of all possible routes to the required destinations. This table is independently maintained at each node in the network. Each entry in this table is represented by some entries to which we have added a new field route_delay (represented in bold), in our proposed protocol DS-AODV.

<dest_ip, seq_num, hopcount, next_hop, activated, lifetime, precursor_list, **route_delay**>

- **Dest_ip**:- destination node's IP address whose route is present in this routing table.
- **Seq_num**: contains the sequence number of the destination node that shows the freshness of the stored route for this destination in the routing table, when a new route is found for the same destination.
- **Hopcount**: this field carries the distance (in hops) between the current node and destination node whose entry is present in the routing table.
- **Next_hop**: contains the address of the next hop towards the destination node.
- **Activated**: used to denopte whether the route in the routing table for a destination is currently active and available for use or not.
- **Lifetime**: this field signifies the time duration since last packet transmission after which the route will expire i.e. the maximum allowable time for which a route can be active since the last data transmission.

- **Precursor_list**: contains the list of those neighbor nodes to which a route reply was forwarded [9].
- **Route_delay**: contains the link delays, i.e., l_delay values of links that connect it to its immediate downstream neighbors. These values are used to calculate offset_time values, at any node N, to accomplish route discovery process in DS-AODV. These values are precomputed and stored in route_table at network startup.

4.4 Route Discovery

In this section, we will elaborate the working of our proposed protocol DS-AODV, focusing mainly on the route discovery, since route maintenance operation in DS-AODV will be same as that in the traditional AODV routing protocol. The DS-AODV protocol searches all available routes between a source and destination that lies within the specified delay constraints. The applications running at source and destination specifies their maximum allowable delay thresholds in the RREQ and RREP messages respectively during the route discovery operation. This is specified in the extra added field “max_delay” in both these message formats.

We have shown in figure 10 the process of initiating a route discovery operation in DS-AODV.

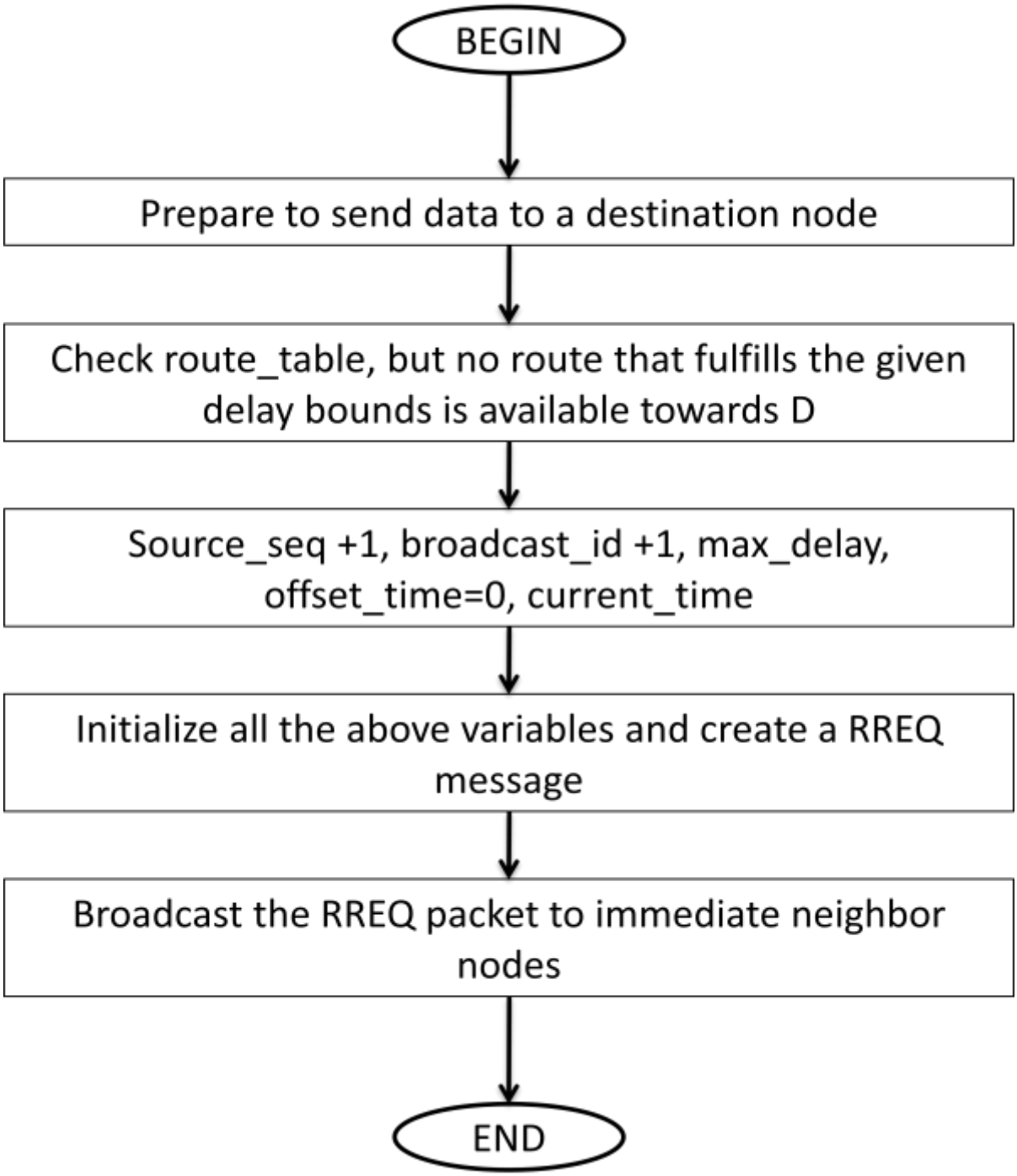

Figure 10: flowchart for the initiation of Route Discovery process in DS-AODV

The main purpose of DS-AODV is to discover delay bounded paths and hence provide QOS to the requesting application in terms of delay metric which is quite vital for multimedia applications. To achieve this goal, before searching any route towards the destination, the source node has to specify its maximum allowable delay bound in the RREQ message before sending it. The field offset_time is initialized to zero. Also, the session admission control process assigns a timer to the source application so that when it expires, route discovery can be attempted again.

In DS-AODV, the routing table contains an additional field route_delay, as discussed earlier. Each intermediate node will update this entry on receiving the RREQ message.

After initializing all the required fields, the RREQ message is created and broadcasted by the source node to its immediate neighbors. When a RREQ arrives at its destination, the destination creates a RREP packet by initializing all the fields including max_delay and offset_time and unicast it back towards the source Sthat originated the RREQ message.

Algorithm 1 shows the detailed proposed protocol DS-AODV and how RREQ and RREP messages are handled at each node in the network.

Algorithm 1

DS AODV ALGORITHM

Variables used in the Algorithm:

S is the source node;

D is the destination node;

l_delay is the link delay;

q_delay is queuing delay;

t_delay is transmission delay;

Max_delay carry the maximum delay specified by the requesting application;

Offset_time specifies the time that is spent by the RREQ(RouteREQuest packet) till the current node;

R_count is the average number of retransmissions over a fcartion of time ;

Difs, sifs, p_len, c_bwd are predefined MAC values;

Algorithm:

// Set the fraction of time to t seconds over which a node monitors the loss probability (Pl) by using the number of HELLO messages it receives

// The Pl is used to calculate the link loss probability using the equation:

Link_Pl = 1 – Pl

// Based on the retransmission policy of 802.11 MAC the approx. retransmission count can be calculated using the following equation:

R_count = 1/(1-Link_Pl)

Back_off_time= ((2 pow (5 + r_count) – 1)/2) * slot_time

//Back_off_time is set to initial contention window size specified in MAC 802.11 specification. Back_off_time increases with increase in number of retransmission of a data packet

t_delay= (difs + (p_len/c_bwd) + sifs + back_off_time) * (r_count + 1)

l_delay= p_delay + q_delay + t_delay

//offset_time is initialized with zero

For (each node N in route discovery phase)

l_delay= p_delay + q_delay + t_delay

$Offset\_time_N = l\_delay + offset\_time_{N-1}$

If (l_delay is less than max_delay)

Then RREQ message is initiated

Else

Re-broadcast towards the destination

//D receives RREQ

//D initiates unicast RREP message that contain l_delay (link delay) in one direction

S receives RREP message

S calculates link delay (l_delay_S)

If (l_delay_S is less than max_delay)

Session is admitted by source S

Else

Source S rejects the session request

Repeat steps 1 to 6

We will explain the working of this protocol with the help of an example discussed in the following text. Figure 11 is the MANET scenario that has been considered for this example.

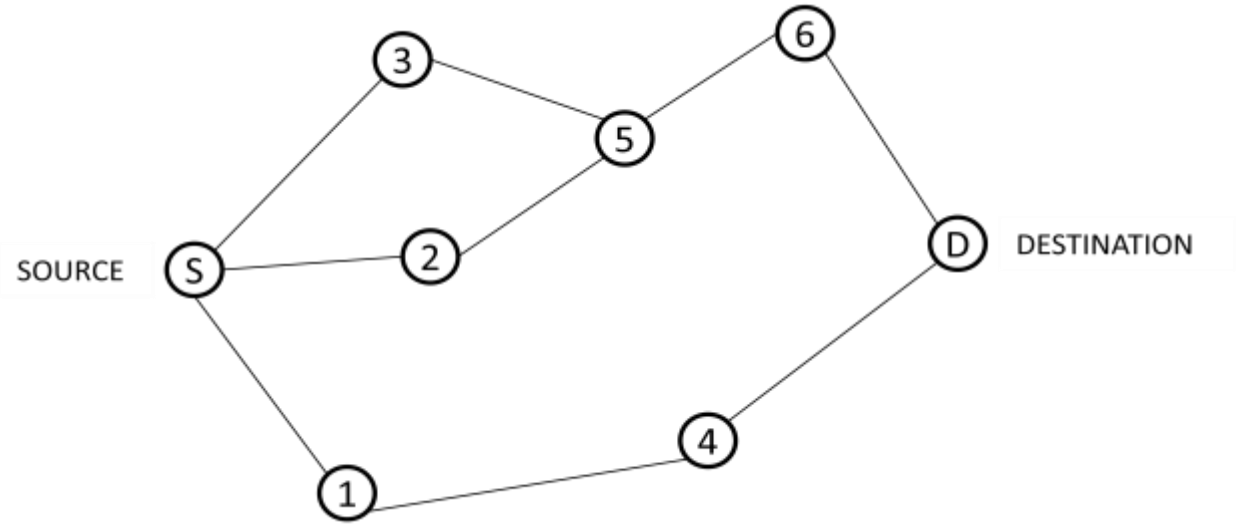

Figure 11: Sample MANET scenariofor DS-AODV example

Suppose S is the source node and D is the destination node in an infrastructure less MANET scenario. When S receives a data packet from an application running on it, it searches its route_table for a valid route towards D. If S already has an entry in its route_table for destination D, S will send the data to D using the next hop given in the routing table. Whereas if S does not have an existing valid route to D, it initiates a route discovery process. In this case, the route discovery is initiated using DS AODV that will discover routes that satisfies delay constraints specified by source application.

The source initiates the delay aware QOS routing by broadcasting the RREQ into the network to all its next hop nodes. RREQ is checked for duplicity as well as for whether the receiving node is itself the destination or not. When the source application first sends RREQ, it specifies its maximum supported delay constraint in max_delay field. Also, offset_time is initially set to zero which is updated by each node on arrival of RREQ.

Let node 1 received RREQ from S. Node 1 will now calculate its offset_time and update this field in the received RREQ. For this, it will refer its route_table for the route_delay value stored in it for the receiving node S. The route_delay stored against node S in route_table of node 1 is added to the offset_time in RREQ to get offset_time of node 1. This is updated in

RREQ and hence, forwarded by node 1 to all its immediate neighbors. The route_delay entry is also checked by node 1 for whether it is greater than max_delay in RREQ.\

Now, let node 4 receives RREQ from node 1. Node 1 checks for RREQ duplicity as well as checks whether it is the required destination or not. It now checks its route_table for route_delay stored against node 1, this route_delay is added to offset_time field of RREQ to get offset_time of node 4. This is updated in the offset_time field of RREQ which is broadcasted to its next hop nodes. Now, let it is received by destination D. D will again perform the checks for RREQ duplicity with the help of seen_table as well as whether it is the destination node or not by looking the destination IP field of RREQ. Since it is the required destination, it will not forward RREQ anymore. It will again calculate offset_time by adding route_delay from node D in the offset_time stored in RREQ to get offset_time of D which is actually the cumulative link delay in one direction and will be stored in offset_time field of RREP created by D. The destination will receive multiple RREQ messages but it will send RREP packet on that link only having the least link delay/ cumulative offset_time out of all its immediate neighbors. After receiving RREP, the source S checks whether the link delay it received in offset_time field is less than max_delay. If offset_time sent by D is within the max_delay, session request is accepted by source, else discarded. Hence, in this way, DS-AODV is able to find valid routes that can send the application traffic from S to D within the specified delay constraints.

CHAPTER 5

SIMULATION RESULTS AND ANALYSIS

This chapter will elaborate the performance evaluation of our proposed routing protocol DS-AODV based on the analysis of simulation results to validate its correctness and effectiveness.

In our analytical part, we have used Exata Cyber Developer Version 2.0 to design MANET scenarios as well as for generating simulation results.

5.1 Simulation Setup

This section provides a extended explanation of the implementation details of this simulation study. This section has been divided into 4 subsections. In section 5.1.1, we will provide a brief introduction of the simulator that has been used to carry out simulations in this research. In section 5.1.2, an overview of the mobility model has been provided, that has been used in the simulations. Section 5.1.3 mentions the network scenario being considered for simulations along with several simulation parameters with their values that have been used while conducting simulations. Section 5.1.4 will describe the various metrics based on which we will evaluate our proposed protocol.

5.1.1 Simulation Tool: Exata Cyber

This section will briefly introduce the simulation tool that has been used to carry out the research in this thesis. We have used the trial version of the industry used commercial scalable network simulator Exata cyber to create various MANET scenarios.

Exata Cyber belongs to the breed of new software tool [22] developed specifically for incorporating in communication networks, cyber security capabilities [22]. Hence, Exata Cyber is most suited to simulate wireless mobile ad-hoc network due to their unprotected and mobile nature that makes them quite vulnerable.

Exata Cyber has simulation as well as emulation capabilities [23]. Using Exata Cyber, we can create different types of network scenarios, including mobile ad-hoc networks with different scenario parameters set to different values. It allows us to create Software Virtual Networks (SVNs) [24] by which it is possible to replicate physical networks in virtual space.

5.1.2 Mobility Model

A mobility model denotes the pattern of movement of mobile nodes as well as variation in mobility speed and location over time. The role of mobility models is quite vital in performance evaluation of routing protocols since they simulate the movement of network's real world application in a reasonable manner else the results could be misleading.

The mobility model that has been considered for this simulation is the most common and widely used "Random Waypoint Model". This model is quite easier to simulate and simple to use. In this model, the mobile node waits for a definite pause time in the beginning of the simulation, after which it randomly chooses any target node in the simulation area. It also picks a random speed with a uniform distribution between 0m/s to 20 m/s.

All the source-destination pairs are selected randomly in from the network. To model the source nodes as a data generating nodes we configure each source node in the network using the constant bit rate (CBR) application. The CBR generates data based on parameters like packet size, packet flow (packets per second) etc.

All the simulations performed in this thesis run for a time period equal to 500 simulated seconds. Each data point shown in the graphs and tables are averaged on three runs with similar traffic models, but different randomly generated mobility scenarios by using different seed values.

5.1.3 Network Scenario and Simulation Parameters

The network scenario that we have used in our simulation is depicted n figure 5.1. We have used a terrain with dimensions of 1000x1000 and deployed 60 nodes in it. Random Waypoint

Mobility model has been used during simulation that decides the movement of these nodes in any random direction.

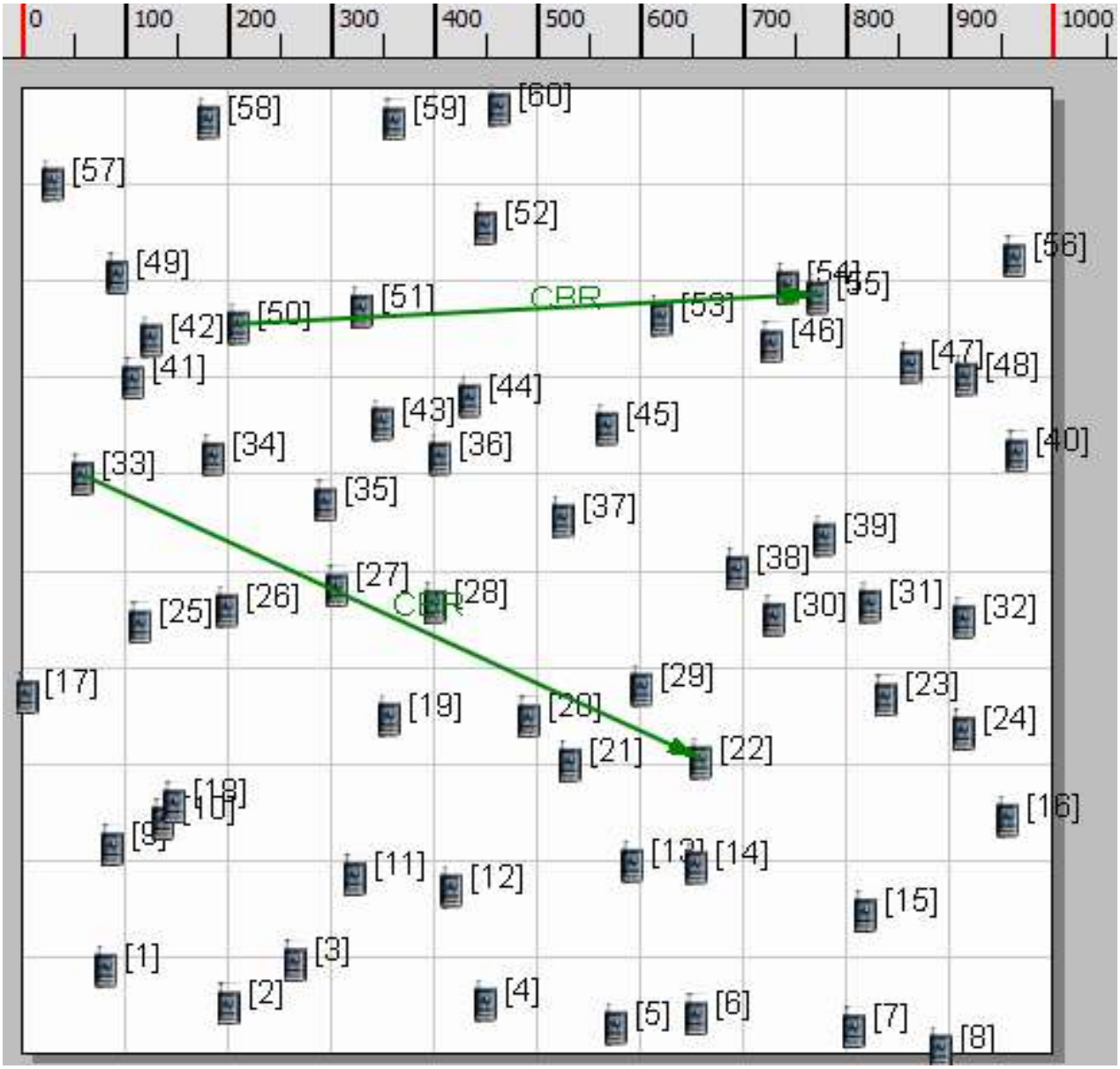

Figure 12 Network scenario for simulation study

We have defined several parameters to evaluate the performance of our proposed protocol DS-AODV by comparing it with AODV. In table 5.1, we have mentioned various parameters for designing a typical MANET scenario that we have considered to carry out our simulation study.

TABLE 4 Simulation Parameters

Simulation Tool	Exata Cyber Developer Version 2.0
Topology area	1000x1000m
Simulation Time	300 sec
Application Traffic type	CBR (Constant Bit Rate)
Number of nodes	80
Node Placement model	Uniform
Routing protocols under study	DS-AODV, AODV
MAC Layer protocol	IEEE 802.11
Physical Layer protocol	802.11b
Data Rate	12 mbps
Node Mobility model	Random Waypoint model
Packet size	512
Flow specification	50 packets/second
Node pause time	20 m/s (for constant network load)

During the simulation, nodes start their movement from a source to a destination node, resulting in continuous changes in the network topology throughout the simulation [25].

5.1.4 Performance Metrics

This section will provide an overview of the metrics [26] that have been considered for evaluation of results produced by our study.

a) **Average End to End delay**

This metric refers to the time interval difference between the times at which the destination receives a data packet from the time when it is sent by the source. This is calculated by the destination node on receiving the packet completely by the help of its send and receives timestamp. On completion of the simulation, total time of the packets received at the destination is divided by total number of received data packets, i.e. ,

End to End Delay = delay of each successfully received packet/ total number of packets received

In other words, it is the time taken by the data packet to traverse from a source to a destination node.

b) Packet Delivery Ratio (PDR)

It is defined as the ratio of total number of error free data packets received by the destination to the total number of packets sent by the source, i.e. ,

PDR = total number of packets received / total number of packets sent by CBR application

This metric can efficiently define the loss rate of the data sent by the application, hence an important metric to estimate the reliability of the routing protocol in use.

c) Normalized routing Overhead (NRO)

Normalized routing overhead is defined as the total number of control packets transmitted per data packet delivered successfully at the destination. It is calculated as the ratio of total number of routing control packets sent to the total number of data packets received by the destination.

This metric is used to measure how efficient and scalable the protocol is along with the amount of extra overhead it generates during routing operations. This gives a measure of the bandwidth consumed by the routing control messages of a routing protocol.

5.2 Simulation results

In this section, we will evaluate the performance of our proposed routing protocol, DS-AODV, by comparing it with the traditional reactive routing protocol AODV over the three performance metrics discussed in previous section. The chief objective of this study is to demonstrate that DS-AODV will score above the reference protocol chosen here, i.e., AODV, in terms of varying scenario parameters like:

- Number of data sessions
- Mobility of nodes

The simulation results are calculated by averaging the values of 3 different runs. During simulation, initially we vary the number of source-destination pairs, i.e., number of CBR sessions keeping the node pause time constant and equal to 20 m/s. This is done to study the effect of varying network load in the network. We take values for number of data sessions equal to 2, 4, 6, 8, 10 and 12.

Next, we vary the node mobility speed from 5 to 45 m/s keeping the number of CBR sessions constant at 4. We collect results for this simulation at pause times of 5, 15, 25, 35 and 45.

5.2.1 Varying number of data sources

In this section, we will present the simulation results for the network scenario in which we have chosen constant pause time of 20 m/s, whereas we vary the network load by increasing the number of sources. Number of sources is taken to be 2, 4, 6, 8, 10 and 12. Other parameters, as mentioned in table 5.1 are fixed.

5.2.1.1 Normalized Routing Overhead

The Normalized Routing Overhead of DS-AODV and AODV is depicted in figure 5.2. The graph shows that the Normalized Routing Overhead varies proportional to the network load. This is because increase in number of data sources increases the network congestion and therefore, the probability of packet collision also increases, thereby increasing the Normalized Routing Overhead. The graph in figure 1 supports the fact that DS-AODV has a lower Normalized Routing Overhead than AODV for moderate to high number of data sources. This is because DS-AODV avoids wrong admission of a new data flow into the network, hence preventing the network from being overloaded.

Table 5 Effect of increased network load on routing overhead

Number of data sessions	DS-AODV	AODV
2	0.14	0.13
4	0.46	0.44
6	0.59	0.58
8	0.61	0.67
10	0.64	0.69
12	0.73	0.84

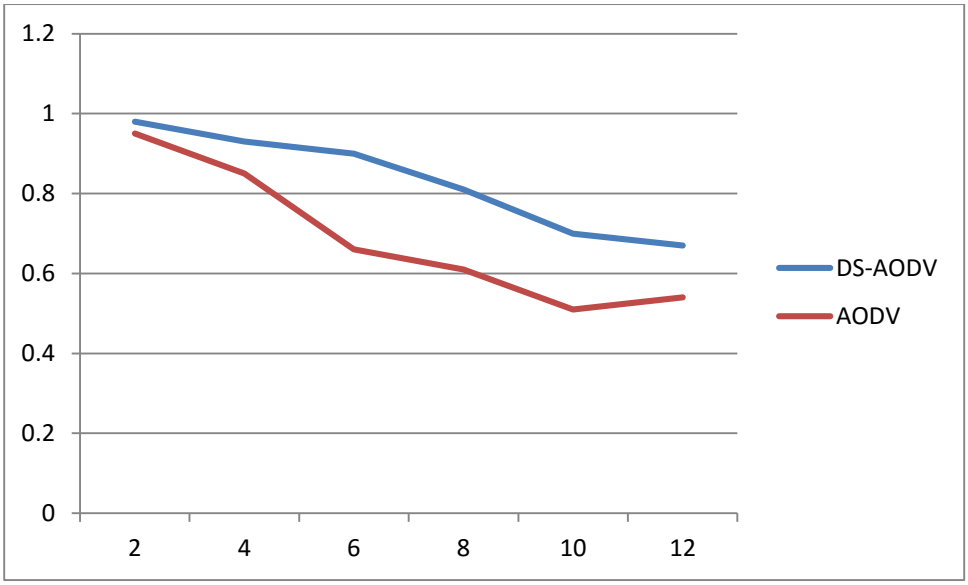

Figure 13 Overhead with increased number of data sessions

5.2.1.2 Average End to End Delay

The comparison of average end to end delay of DS-AODV and AODV is shown in figure 5.3. It is quite evident that end to end delay of DS-AODV is quite lower than that of AODV and varies as a function of number of sources under all values of number of data sessions. This is due to the fact that DS-AODV is specifically meant for delay aware transmission of application data and due to additional delay oriented fields in request and reply messages, the discovered routes

is bounded by a specific required delay. Hence the end to end delay of DS-AODV is drastically lower than that of AODV.

Table 6 Effect of increased network load on end to end delay

Number of data sessions	DS-AODV	AODV
2	0	0
4	0.01	0.05
6	0.02	0.11
8	0.02	0.12
10	0.03	0.37
12	0.04	0.65

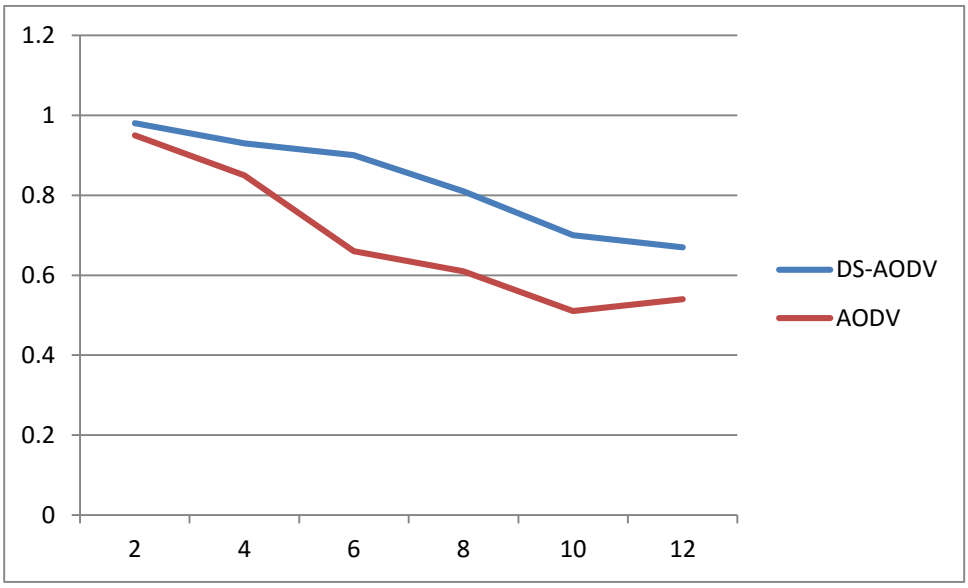

Figure 14 Effect of increased number of data sessions on delay

5.2.1.3 Packet Delivery Ratio

The graph in figure 5.4 demonstrates the effect of varying number of sources on packet delivery ratio in DS-AODV protocol compared to AODV. The figure shows clearly that the on packet delivery ratio for AODV is quite lower than DS-AODV, with increasing network load. The

AODV protocol drops a larger amount of packets with increase in number of sources. The on packet delivery ratio of DS-AODV decreases faster with larger number of sources but is found to be greater than almost 70% always. The reason behind this tradeoff is that a larger number of sources in the network increase the probability of congestion leading to packets being dropped.

Table 7 Effect of increased network load on packet delivery ratio

Number of data sessions	DS-AODV	AODV
2	0.98	0.95
4	0.93	0.85
6	0.90	0.66
8	0.81	0.61
10	0.70	0.51
12	0.67	0.54

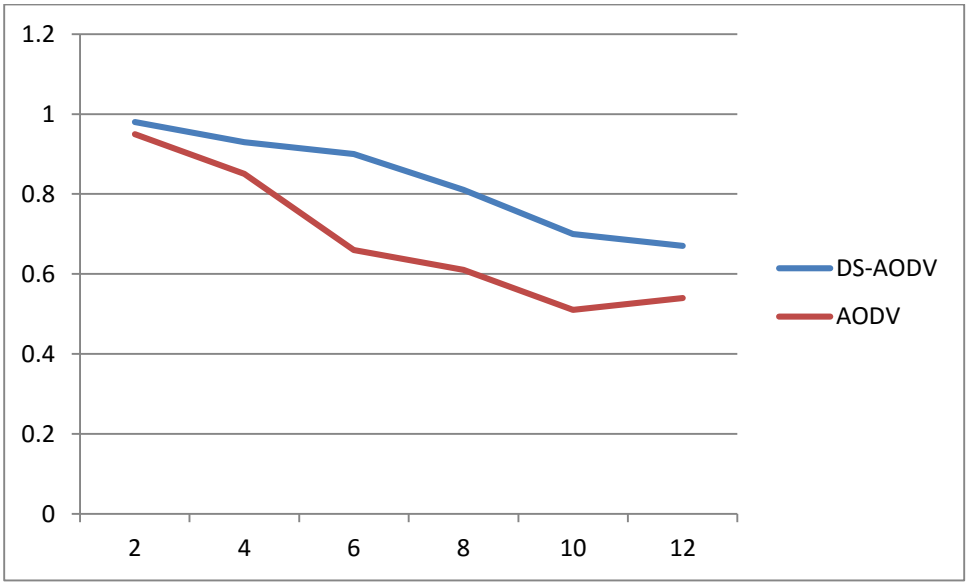

Figure 15 Effect of increased number of data sessions on PDR

5.2.2 Varying Node Mobility

In this section, we will demonstrate the influence of varying node speed (pause time) maintaining a constant number of sessions. The results are obtained by keeping number of data sessions equal to 4 and varying pause times at 5, 15, 25, 35 and 45 m/s.

5.2.2.1 Normalized Routing Overhead

The graph in figure 5.5 shows the variation of normalized routing overhead with changing node mobility for both protocols: DS-AODV and AODV. The normalized routing overhead is calculated as the ratio of total number of routing control packets sent to the total number of data packets received by the destination. This is quite a critical metric to estimate the efficiency of a routing protocol as well as scalability of the network by defining how much bandwidth is consumed by the control packets for a particular routing protocol. So this metric can be efficiently used to compare the performance of routing protocols.

The graph in figure 2 shows that DS-AODV has a higher routing overhead than AODV for almost all values of node pause time. This is because of the fact that in DS-AODV, due to increased node mobility, larger number of link breakages will occur resulting in higher number of route discovery processes to initiate, causing larger overheads. This limitation of DS-AODV can be rectified in its future extensions.

Table 8 Effect of varying node mobility on normalized routing overhead

Node Speed (m/s)	DS-AODV	AODV
5	0.35	0.34
15	0.33	0.32
25	0.30	0.31
35	0.29	0.27
45	0.25	0.23

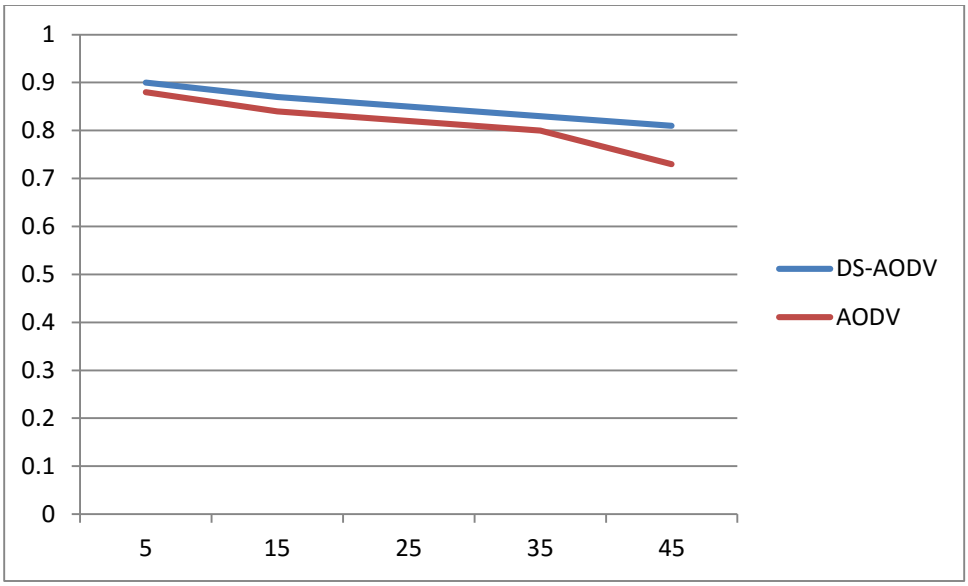

Figure 16 Overhead with increased network mobility

5.2.2.2 Average End to End Delay

The moment the packet is generated and sent by the source till the time it is received by the destination is considered as end to end delay. There are certain factors that affect this metric. They are:

a) Route discovery time
b) Queuing delay (waiting time in buffer/queue before transmission)
c) Route length (distance in hops between source and destination)

Figure 5.6 shows the variation of end to end delay with respect to change in node mobility. It can be clearly observed that average end to end delay is quite lower in DS-AODV, as compared to AODV. This is due to the fact that DS-AODV discovers routes within the delay requirements of the source application, hence, end to end delay cannot exceed beyond an acceptable limit, else the session would not have been admitted.

Table 9 Effect of varying node mobility on delay

Node Speed (m/s)	DS-AODV	AODV
5	0.05	0.08
15	0.08	0.12
25	0.10	0.15
35	0.12	0.17
45	0.14	0.23

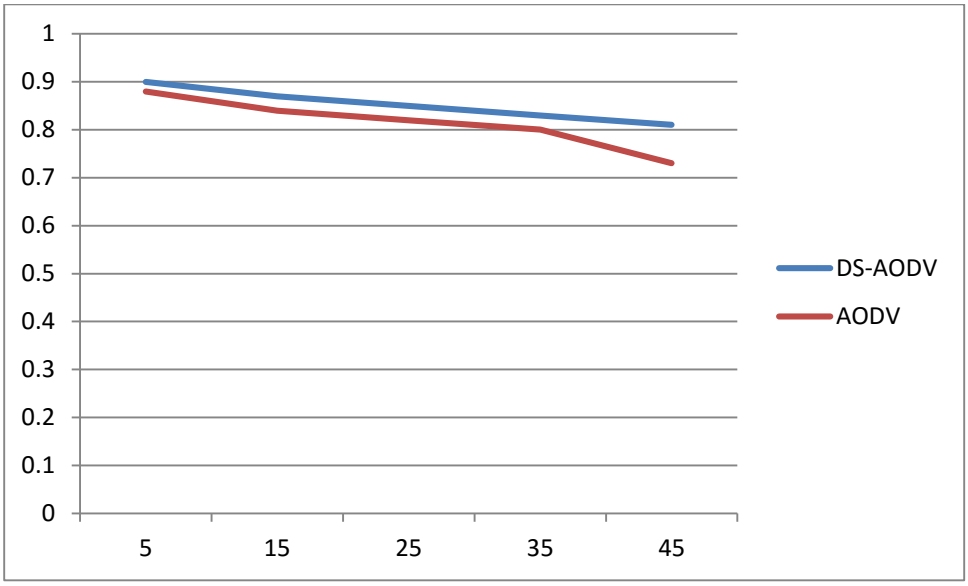

Figure 17 Effect of increased network mobility on delay

5.2.2.3 Packet Delivery Ratio

It is the ratio of data packets delivered at the destination to those generated and sent by the CBR source. This is quite an important metric since it defines the loss rate of the application data which ultimately defines the overall throughput of the network.

The packet delivery ratio of the two protocols is depicted in figure 5.7. The graph shows the variation of packet delivery ratio with the changing node mobility values. The increase in nodes' movement results in high probability of route breakages causing an increase in number of

packets being dropped. DS-AODV has a better packet delivery ratio than AODV for all values of node pause time. The simulation study shows that more than 80% data packets are delivered by DS-AODV to the specified destination for all node mobility values. Hence, DS-AODV is found to be more robust than AODV.

Table 10 Effect of varying node mobility on packet delivery ratio

Node Speed (m/s)	DS-AODV	AODV
5	0.90	0.88
15	0.87	0.84
25	0.85	0.82
35	0.83	0.80
45	0.81	0.73

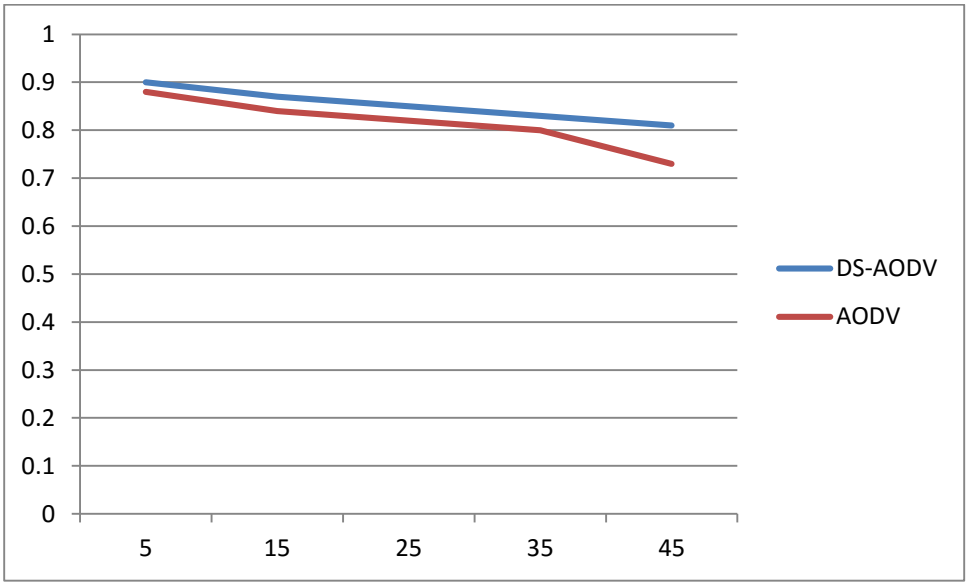

Figure 18 Effect of increased network mobility on PDR

5.3 Summary

In this chapter, we have analyzed the performance of our novel proposed routing protocol DS-AODV, based on various performance metrics. This reactive routing protocol has been specifically designed for mobile adhoc networks and is based on the traditional protocol Ad hoc On-demand Distance Vector. The simulation study performed in this chapter demonstrates that DS-AODV is able to perform fairly well over a range of node mobility and network load values. The simulations have been performed on Exata Cyber simulator. The results produced by the simulations have been represented graphically for a better analytical understanding. These results have been used for comparing the performance of DS-AODV with AODV over various performance metrics. The analysis supports that the performance of DS-AODV is quite better as compared to AODV protocol.

CHAPTER 6

CONCLUSION

Delay sensitive applications like multimedia and real time applications require data transmission in a timely manner; otherwise the data becomes obsolete if it is received after the specified time. Therefore, the concept of delay aware routing becomes a vital research domain in the field of Adhoc networking.

In this thesis, we have proposed and implemented a delay constrained reactive routing protocol based on AODV routing protocol. We have named it as DS-AODV (Delay Sensitive Adhoc On-demand Distance Vector). The chief objective of this protocol is to discover valid routes that are constrained by a maximum delay value during route discovery phase. The application running at source that needs to initiate a date transmission with the destination will specify its maximum allowable delay prior to route discovery. This value will be used as the reference for discovering routes that lie within these delay bounds. Simulation results are developed using a powerful simulation tool caslled as “Exata Cyber”. The analysis of these results shows that our proposed protocol DS-AODV is able to perform better than AODV by delivering lower end to end delay values.

Looking at the future extensions in this research, we can try to implement this with node mobility models other than the random waypoint mobility model that we have followed in this thesis. Also, in DS-AODV, route_delay values stored in routing tables of nodes may not always be up-to-date due to dynamic nature of mobile adhoc networks. A common synchronized update mechanism can be implemented to solve this problem.

Also, the robustness of DS-AODV can be verified in case of congestion of network. Lastly, we recommend a performance comparison of DS-AODV, based on various parameters, with other QOS aware protocols that have been proposed in recent past to verify its performance further in terms of various parameters, other than delay.

CHAPTER 7

REFERENCES

[1] Lajos Hanzo II, Rahim Tafazolli, "Admission Control Schemes for 802.11 Based MultiHop Mobile Ad hoc Networks: A Survey," IEEE Communications Surveys &Tutorial., vol. 11, pp. 78–108, Fourth quarter 2009.

[2] M. Tarique, K.E. Tepe, S. Adibi, S. Erfani, "Survey of Multipath Routing Protocols for Mobile Ad hoc Networks," Journal of Network and Computer Applications 32, pp. 1125–1143, Nov. 2009.

[3] Y. Huang "Improving Signaling Performance of Proactive MANET Routing Protocols," Doctorate thesis, University of London, U.K., 2007.

[4] Vivek Kumar "Simulation and Comparison of AODV and DSR Routing Protocols in MANETs,"M.E. Thesis, Thapar University,India., July 2009.

[5] T. Larsson, N. Hedmen "Routing Protocols in Wireless Ad hoc Networks: A Simulation Study," Master's thesis, Lulea University of Technology, Sweden, 1998.

[6] Stefano, M. Conti, S. Giordano, Ivan S., Mobile Adhoc Networking, A JOHN WILEY & SONS, INC., PUBLICATION 2004.

[7] W. Gibson "An Investigation of the Impact of Routing Protocols on MANETs using Simulation Modeling,"M.E. thesis, Auckland University of Technology, 2008

[8] Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz, " A review of routing protocols for mobile ad hoc networks", Science Direct: Ad hoc Networks(Elsevier), vol. 2, pp. 1-22, 2004

[9] C. Perkins (2003) Network Working Group, AODV RFC, [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[10] Chhagan Lal, Dr. V. Laxmi, Dr. M.S. Gaur, Book Chapter in Building Next Generation Converged Networks: Theory and Practice, "Taxonomy of QOS Aware Routing Protocols for MANETs", CRC Press, pp. 533–560, Publication 2013.

[11] Chen, S., and K. Nahrstedt. "Distributed quality-of-service routing in ad hoc networks." Selected Areas in Communications, IEEE Journal, Aug. 17, 1999, 1488–1505.

[12] Crawley, E., R. Nair, B. Rajagopalan, and H. Sandick. A Framework for QoS-based Routing in the Internet. RFC2386, IETF, 1998.

[13] Reddy, T. B., I. Karthigeyan, B. S. Manoj, and C. S. R. Murthy. "Quality of service provisioning in ad hoc wireless networks: A survey of issues and solutions." Ad Hoc Networks, Jan. 4, 2006, 83–124.

[14] S. M. Zaki, M. Ngadi, S. Razak, "A Review of Delay Aware Routing Protocols in MANETs" ISSR Journals, vol. 1, June2009.

[15] M. Malik,Shen Ting Zhi, U. Farooq, "Latency Aware Routing Mechanism to Maximize the Lifetime of MANETs" IEEE Communications Surveys &Tutorial., pp. 158–162, December 2011.

[16] X. Zhen, X. Juan, "Energy Aware and Delay Aware QOS Routing in Mobile Ad hoc Networks", in ICCP 2012, pp. 511, October 2012.

[17] S. Murthy, P. Hedge, A. Sen, "Design of a Delay-Based Routing Protocol for Multi-Rate Multi-Hop Mobile Ad Hoc Networks", in ICC 2009, pp. 1, June 2009.

[18] M. Bhuiyan, I. Gondal, J. Kamruzzaman "CODAR: Congestion and Delay Aware Routing to detect time critical events in WSNs", in ICOIN 2011, pp.357, January 2011.

[19] W. Cho, D. Kim, T. Kim, S.H. Kim, "Time Delay On-Demand Multipath routing protocol in mobile ad-hoc networks", in ICUFN 2011, pp. 55, June 2011.

[20] S. Liu, J. Liu, “Delay-aware multipath source routing protocol to providing QoS support for wireless ad hoc networks”, in ICCT 2012, pp. 1340, November 2010.

[21] J.N. Boshoff, A.S.J. Helberg, “Improving QoS for real-time multimedia traffic in Ad-hoc Networks with delay aware multi-path routing”, in WTS 2008, pp. 1, April 2008.

[22] Launch of Exata Cyber press release [online] http://www.prnewswire.com/news-releases/new-exatacyber-provides-advanced-emulation-for-cyber-security-capability-development-89422207.html

[23] Scalable Network Technologies [online] http://web.scalable-networks.com/ content/ exatacyber

[24] Exata Cyber [online] http://www.superinst.com/docs/snt/SNT_exata_cyber.pdf

[25] D. Vir,Dr. S.K. Agarwal,Dr. S.A. Imam, “A simulation study on node energy constraints of routing protocols of Mobile d hoc networks by use of Qualnet simulator,” IJAREEIE., vol. 1, issue 5, pp. 401–410, Nov. 2012.

[26] IEEE Computer Society LAN MAN Standards Committee, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE standard 802.11, 1997. The Institute of Electrical and Electronics Engineers, New York, NY, 1997.