A Major Project-II Report
On

REDUCING BUFFER OVERHEAD IN A RELIABLE MULTICASTING PROTOCOL FOR MANETS

Submitted in Partial Fulfilment of the Requirement for the Degree
of

MASTER OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

ADITYA TOMAR
2K15/CSE/02

Under the Esteemed guidance of
Mr. VINOD KUMAR
(Associate Professor)

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahabad Daulatpur, Main Bawana Road,
Delhi-110042.

June 2017

CERTIFICATE

This is to certify that Major Project-II Report entitled **“REDUCING BUFFER OVERHEAD IN A RELIABLE MULTICASTING PROTOCOL FOR MANETS”** submitted By **ADITYA TOMAR, Roll No. 2K15/CSE/02** for partial fulfilment of the requirement for the award of degree of Master of Technology (Computer Science and Engineering) is a record of the candidate work carried out by him under my supervision.

(Project Guide)
Mr Vinod Kumar
Associate Professor
Department Of Computer Science & Engineering
Delhi Technological University

DECLARATION

I hereby declare that the major Project-II work entitled "**REDUCING BUFFER OVERHEAD IN A RELIABLE MULTICASTING PROTOCOL FOR MANETS**" which is being submitted to Delhi Technological University, in partial fulfilment of requirements for the award of degree of Master of Technology (Computer Science and Engineering) is a bonafide report of Major Project-1I carried out by me. The material contained in the report has not been submitted to any university or institution for the award of any degree.

Aditya Tomar
M.Tech (CSE)
2K15/CSE/02

ACKNOWLEDGEMENT

First of all, I would like to express my deep sense of respect and gratitude to my project supervisor Mr Vinod Kumar for providing the opportunity of carrying out this project and being the guiding force behind this work. I am deeply indebted to him for the support, advice and encouragement he provided without which the project could not have been a success.

Secondly, I am grateful to Dr. Rajini Jindal, HOD, Computer Science & Engineering Department, DTU for his immense support. I would also like to acknowledge Delhi Technological University library and staff for providing the right academic resources and environment for this work to be carried out. Last but not the least I would like to express sincere gratitude to my parents and friends for constantly encouraging me during the completion of work.

Aditya Tomar
University Roll no: 2K15/CSE/02
M.Tech (Computer Science & Engineering)
Department of Computer Engineering
Delhi Technological University
Delhi – 110042

ABSTRACT

As the technology of Mobile ad hoc networks (MANETs) develops, many kinds of new applications emerge demanding new and better services with each research being done. The major area of challenge for these ad hoc networks is the multicast service as it is difficult to adapt this in an environment where failures are frequent. The level of reliability differs with the framework of different applications. At its minimum, reliability is assurance of the final delivery of all the multicast data packets to the entire destinations. It also guarantees delivered data packets to be error free along with minimal use of bandwidth and power. The second level of the reliability is to retain the order (partial or total) between data packets. Maintaining the order is crucial for the real- time applications, which requires that all packets be received to every receiver in precisely that order. Various issues of the reliable multicasting include detection of loss of packet, starting the recovery process from such loss and managing the buffer overhead of nodes. However, depending upon the protocol, any of the sender or the receivers may be responsible for these processes.

To perform a reliable multicast delivery of data packets, it is necessary to get a feedback from each multicast receiver which in turn indicates whether or not a retransmission is required. A reliable multicast delivery refers to receipt of multicast packet by each of the mentioned receivers. Thus, one or all members need to buffer data packet for possible error recovery. A number of multicast protocols support group communication in MANETs and the main purpose of these protocols is to deliver multicast packets in an efficient and reliable manner.

In this project we have proposed an algorithm to improve the performance of Reliable Multicasting AODV Protocol by reducing the buffer overflow and managing the buffers of different nodes. Uniqueness of this algorithm is the selection of one hop set of neighbours of the sender as forwarding nodes (FNs). These forwarding nodes forward the data packets to all the receivers and keep the packets in their respective buffers so as to retransmit the packets whenever it gets a retransmission request. So this distributes the buffer usage from sender to FNs and hence reducing the buffer overhead of the sender. Finally, simulation results show that the modified protocol has low packet dropping as compared to original Reliable MAODV protocol.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

MANET	Mobile Ad hoc Network
MAC	Medium Access Control
AP	Access Point
MN	Mobile Node
QoS	Quality of Service
AODV	Ad hoc On demand Distance Vector
MAODV	Multicast Ad hoc On demand Distance Vector
FNs	Forwarding Nodes
NACK	Negative Acknowledgement
RREQ	Route Request
RREP	Route Reply
DES	Discrete Event Simulation
PDR	Packet Delivery Ratio
DARPA	Defence Advanced Research Project Agency
IWN	Integrated Wireless Network

CHAPTER 1

INTRODUCTION

1.1 Background

With the rising need of mobile devices, continuous network connectivity demand has spurred interest in the use of MANET, regardless of physical location. A versatile specially appointed system (MANET) is a system of a few cell phones or nodes which are associated through remote radios without utilizing any current settled system topology. MANET have so many characteristics like Tactical networks, Data Networks, Device Networks, Wireless Sensor Network, etc. Nodes or devices in MANET work like both as a router and a host. To establish connectivity in a MANET, all nodes which are participating will perform routing of the network traffic. The network immensely depends upon the cooperation of its nodes for successful communication between them. Hence, MANET have the property of quick foundation less sending and no concentrated controller which makes it advantageous to peoples and vehicles would thus be able to be web worked in zones without a previous accord framework or when the utilization of such framework requires remote expansion. By developing scope of portable nodes specially appointed systems underpins multi-jump steering by which they can broaden the chance of remote systems. This range relies on the centralization of remote clients.

Ad hoc networks are preferred when there is a requirement for setting fixed access points and backbone infrastructure may not be viable for the scenario. That is why an infrastructure based solution may not be practical for such short range radio and in disaster prone areas. So, it can be connected anyplace where there is practically no correspondence foundation or the current framework is costly or badly designed to utilize. Ad- hoc networking, due to its flexibility of operations, allows any device in network to maintain connectivity as well as helps in easily appending and removing devices in and out of the network. Besides its use in military battlefields, sensor networks and disaster area network, MANET conquered personal area networks too.

Group oriented services are of much importance in MANETs now as broadcasting nature of network is in high demand. Therefore, multicasting in these networks has been a high area of research in past few years.

1.2 Wireless Networks

Remote systems have encountered remarkable advancement in the previous decade. Remote systems have encountered exceptional advancement in the previous decade. Truth be told, it is anticipated that remote information get to will surpass wired access in coming years .The past several years have shown a wealth of new protocols for Remote systems, including both routing and Medium Access Control protocols. However, the convergence of wireless technologies including mobile devices, personal digital assistants, commonly known as PDAs, pagers and laptops, presents many new challenges in order to make the anytime, anywhere computing paradigm real and effective. Ad hoc networks take this concept one step further by envisioning networks without any fixed infrastructure or central control.

System Components in a remote system speak with each other utilizing remote channels. The use of remote systems has been increasingly prevalent. In light of the sort of system foundation utilized for correspondence, wireless communication network are of two types:

- Infrastructure based network
- Infrastructure less network

1.2.1 Infrastructure based network

A framework based system comprises of remote versatile nodes and at least one scaffolds. As Figure 1.1 delineates, these extensions associate the remote system to the wired system. These scaffold like units are otherwise called base stations. A portable node inside the system scans for the closest base station, interfaces with it and speaks with it. Settings up a foundation modes arrange requires no less than one remote get to point (AP). All neighbourhood remote customers and get to indicate must be arranged utilize a same system name. The Access Point is connected to the wired system to permit remote customers access to, for instance, Internet associations or printers. Extra APs can be joined to this system to expand reach of the foundation and bolster more remote customers. Home systems with remote switches bolster foundation mode naturally as these switches incorporate a worked in AP.

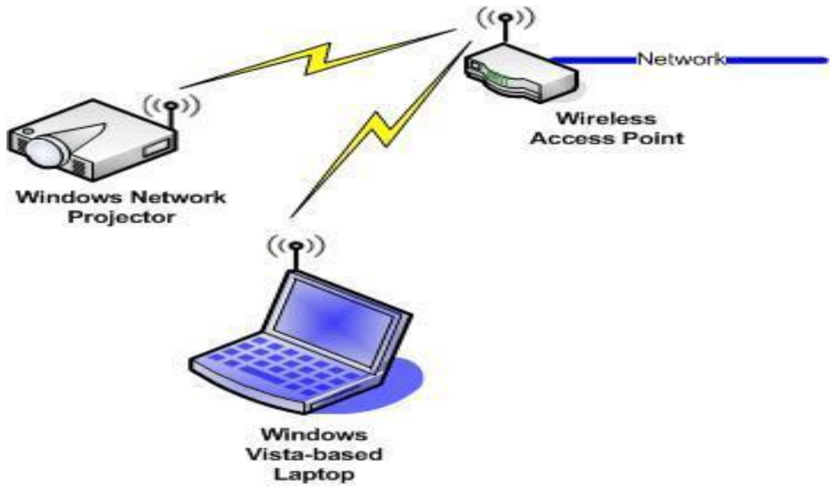

Figure 1.1 A sample layout of infrastructure based network

1.2.2 Infrastructure less network

Opposite to layout of a typical Infrastructure network, every device in the system hence producted shows both as a router and a host. The network topology is created such that it is dynamic, because the range and connectivity among the devices involved may vary with time due to node movements or improvements in location or otherwise. There is no base station or AP. Nodes can communicate with each other by forming a multi hope route as shown in Figure 1.2. Hence there is a need for efficient routing protocol to allow the nodes to communicate over multi-hop paths without access point. Since these frameworks pose various perplexing issues, there are various issues for research and responsibilities. Flexible Ad Hoc Networks is a sort of structure few frameworks in which centres are helpful contraptions, for instance, phones and convenient workstations.

The pervasive use of cellular and handheld devices is most probably going to increase the popularity of wireless ad-hoc networks. Conventional wireless networks (e.g., cellular networks or satellite networks) rely on a fixed infrastructure, e.g., fixed base-stations and wired communications, which connects the users always by routing data through these fixed base-stations. Thus, traditional wireless networks are usually called Infrastructure based wireless networks. Installing such an infrastructure is often either too expensive or technically impossible for some remote localities. In contrast to conventional networks of wireless connectivity, the outstanding feature of ad hoc wireless networks is the absence of any fixed or pre-existing network infrastructure. Due to this property where the requirement of any such infrastructure has been eliminated, they are also known as Infrastructure less wireless networks.

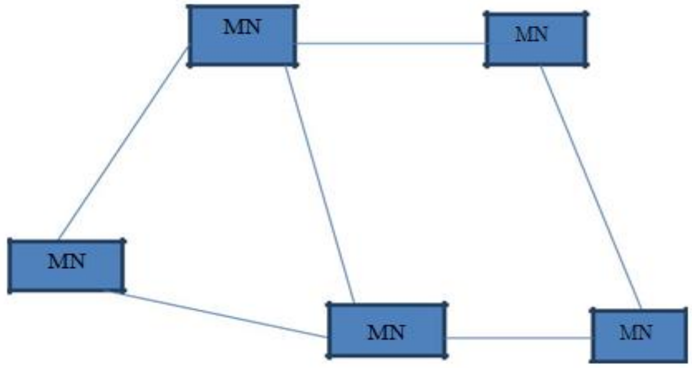

Figure1.2 An infrastructure less network

1.3 Mobile Ad hoc Networks

The concept of MANETs dates back to the DARPA packet radio network program in the 1970's [2]. Among other aspects, MANETs are distinguished from other IWNs classes by the feature of dynamic topology, which is mainly attributed to free node movements. Because the network topology changes arbitrarily as the devices move, routing information is subject to becoming obsolete, and different nodes often have different views of the network, both in time (information may be outdated at some nodes but current at others) and in space (a node may only know the network topology in its neighbourhood). The momentary node associations in MANETs limit the link lifetime, thus affecting the route lifetime. As such, the most challenging issue in MANETs is routing, which is further exacerbated when routes need to satisfy certain quality of service (QoS) guarantees in terms of bandwidth or end-to-end delays. Figure 1.3 shows an example of multi hop connectivity in MANETs where circle represent the mobile nodes and line represent the link between them. Here, mobile nodes use the wireless channel to make peer-to-peer communication through single or multi-hop paths. Since collecting fresh knowledge pertaining to the network in entirety is often both costly and impractical, many routing protocols in MANETs are on demand protocols, i.e., they collect routing information only when necessary, and to destinations they need routes to. By doing this, routing overhead is significantly reduced when observed in contrast with the traditional proactive protocols, which require each and every node in the network to maintain routes (optimal routes), to all destinations throughout.

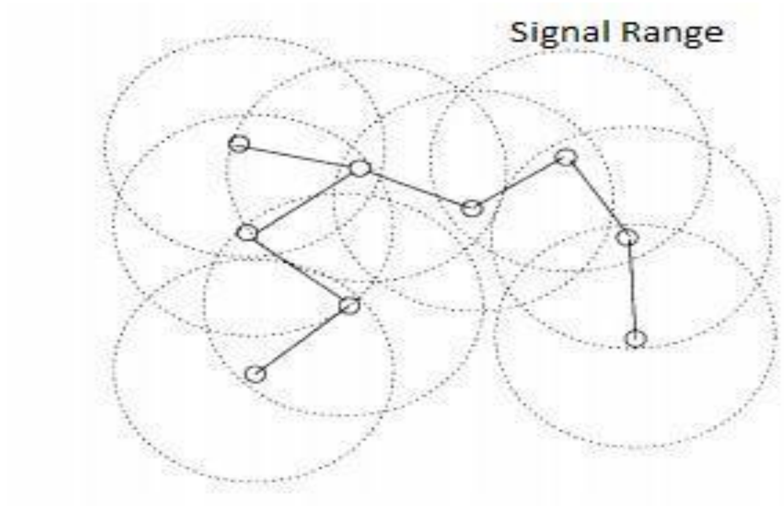

Figure 1.3 Multi-hop connectivity in MANETs

In addition to routing, many research challenges in MANETs require efforts from researchers in order for these networks to become common place. In particular, the following research topics are very important in the design of future MANETs:

- **Topology Control:**

Topology management and control is an active area of research in MANETs.The substitute for physical framework is the development of a virtual spine or foundation. A virtual spine assumes an extremely helpful part in directing, where the quantity of nodes in charge of steering can be lessened to the quantity of nodes in the spine. The virtual spine additionally assumes a critical part for information broadcasting and availability administration in remote specially appointed systems. Proficient topology control calculations are required for MANETs.

- **Quality-of-service (QoS) routing:**

Directing is the most effectively explored region in MANETs. Directing winds up plainly difficult when the course needs to fulfil certain QoS ensures, e.g., bundle misfortune proportion, transfer speed and end-to-end delay. A majority of already proposed steering conventions in MANETs address the issue of directing from a solitary layer viewpoint, that is, at the system layer. As of late, it has been reasoned that between layer conditions assume a basic part in giving an effective and extensive answer for the QoS directing issue, and this view is a key outline rule that we exploit in the QoS steering conventions proposed in this thesis. The utilization of cross-layer outline improvement has been effectively shown with regards to remote Internet conveyance and convention structures for dynamic remote systems. The effect of layers communication outline (interoperability) and the impact of this on the organize execution have not been archived yet quantitatively. Without a doubt, layer associations are more articulated in MANETs.

1.4 Characteristics of MANETs

MANET is a a term used for a set of portable and autonomous elements such as laptops, PDAs, smart phones, tablet, etc. These networks do not have a backbone topology because of its mobile nodes. Network topology is effective because of the node improvements due to connectivity between different nodes. Each node in a MANET is required to act as a router as well as host i.e. no particular node acts as a sender. In absence of a central router or master node, all nodes communicate through multi hop routes. Every node can communicate only within its wireless range i.e. demonstrated in Figure 1.4. In mobile ad hoc network, nodes are portable devices like laptops, mobile phones, etc. So, the ever increasing usage of mobile devices is leading to the possibility for spontaneous, real-time or ad-hoc wireless communication like MANETs.

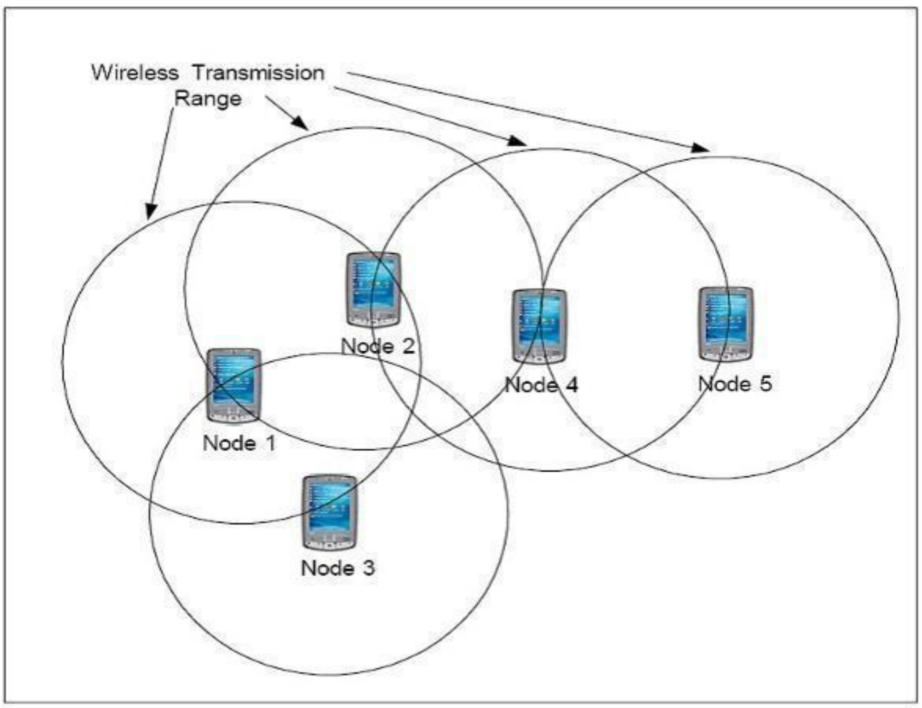

Figure 1.4 Mobile Ad hoc Network

Main characteristics of MANET are as follows:

Wireless Links:

Remote associations make MANET dishonest and defenceless to various sorts of attacks. Because of obliged control supply of remote centres and flexibility of centre points, the remote associations between those centre points in the convenient uniquely named framework are not enduring for correspondence individuals.

Node Movement:

Portable centre points are self-decision units in arrange which tirelessly change their position and topology unreservedly. As a result of incessant development of centre points the topology changes once in a while which mean finding of particular center twist up recognizably troublesome. The canters can without quite a bit of an extend left or into the radio extent of various centers. The coordinating information of centre points changes industriously as their improvement winds up perceptibly subjective.

Power limitation:

The mobile hosts are small and light weight. They are given by obliged control resources, for instance, little batteries. This limitation makes vulnerability be particular when aggressors may concentrate on some centre point batteries to isolate them that may incite framework section. A couple of attacks may endeavour to attract the compact centers un-basically, with the objective that they keep using their battery for early drainage.

Bandwidth-constrained and variable capacity links:

Wireless links have significantly lower Capacity then their hardwired counterparts. In view of the effects of various get to, obscuring, confusion, and impedance conditions, the point of confinement of a remote association can be degraded after some time and the feasible throughput may be not as much as the radio's most extraordinary transmission restrict.

1.5 Routing in MANETs

Due to obvious reasons, the task of route detection in Mobile ad-hoc networks is an engaging problem and have received inimitable amount of attention from scientist and researchers around the world. There are a few directing conventions intended for MANET. Directing conventions are either delegated responsive or proactive. There are some directing conventions which are a mix of both responsive and proactive steering conventions called as cross breed conventions. Figure 1.5 depicts the three types of Routing Protocol:

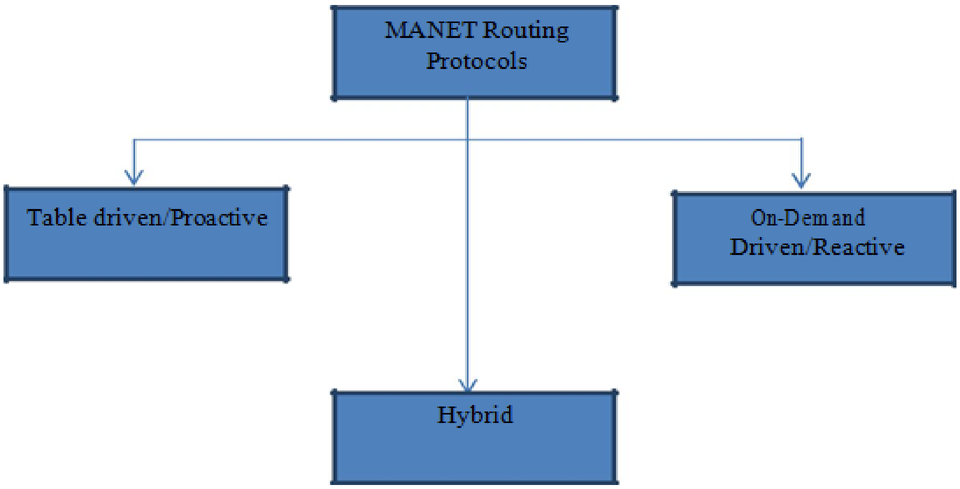

Figure 1.5 MANET Routing Protocols

Proactive Routing Protocols

These traditions are also known as table driven controlling traditions since they keep up the coordinating information as a table before it is required. Each node point in the framework keeps up guiding information to each other node point in the framework. Generally, routes information is kept in the routing tables and is periodically updated as the network topology changes. An extensive part of these coordinating traditions begun from the association state directing. There exist a couple of complexities between the traditions that gone under this class dependent upon the coordinating information being invigorated in each controlling table. In addition, these coordinating traditions keep up different number of tables. As proactive protocols that we have explained above, need to maintain node entries, for each and every node in the routing table of every node, these are not suitable for large networks. This causes more overhead in the coordinating table provoking use of more information transmission. Example: DSDV, CGSR, and so on.

Reactive Routing Protocols

They are also known as on demand routing protocols due to their on demand route finding nature. They don't keep up guiding information or coordinating activity at the network nodes if there is no correspondence. Exactly when a node needs to send a package to another node then this protocol search for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet [8]. The course disclosure as a rule occurs by flooding the course request packages all through the framework. Responsive traditions have a tendency to decrease the control action messages overhead at the cost of extended lethargy in discover another courses. In open traditions there is no need of scattering of information. It consumes transmission limit when trade data source to objective Reactive Protocols are AODV (ad-hoc on demand distance vector), DSR (distance vector routing) and ABR (Associatively Based Routing) protocols.

Hybrid Routing Protocols

Hybrid routing protocols are a combination of both proactive and reactive routing protocols. It was proposed to reduce the control overhead of proactive routing protocols and also decrease the latency caused by route discovery in reactive routing protocols. ZRP (Zone routing protocol) is a hybrid routing protocol.

1.6 Reliable multicasting in MANET

Multicasting is the transmission of packets from a sender to a group of receivers identified by a single destination address. Multicasting is proposed for assemble arranged figuring. Ordinarily, the participation of a host aggregate is dynamic, i.e. hosts may join and leave the gatherings whenever. No limitation is there on the area or number of individuals in a host gathering. Host might be an individual from more than one gathering at any given moment. A host require not need to be an individual from a gathering to send packets to it. Presently, one especially difficult condition for multicasting is versatile impromptu system (MANET). As there is no supposition of basic settled framework in MANET, multicast conventions for wired systems can't be utilized here. Hardly any multicasting conventions have been proposed for portable specially appointed systems: On request multicast steering convention (ODMRP), Forwarding bunch multicast convention (FGMP), Multicast impromptu on request remove vector directing convention (MAODV), and so forth.

Therefore, we have to characterize what precisely we mean by "solid multicast". Various conceivable definitions are there. A number of possible definitions are there. Reliable multicast has to fulfil the following:

- All information packets are conveyed,
- Causal arrange between the information packets are kept up, or
- Achieving an aggregate request of information packet conveyance.

Achieving reliable packet delivery in a MANET is not trivial. As in [9], A couple of production contemplates have investigated the execution of MANET multicast steering conventions, for example, the multicast augmentations for AODV and ODMRP. The outcome demonstrates that exclusive a subset of the MANET nodes joined a solitary multicast gathering, where as a portion of the hubs send settled size information packets to every single other hub at a consistent rate (i.e., CBR movement). Building and keeping up a multicast transport structure (commonly a tree or work) in a MANET with its exceedingly one of a kind topology shows its own particular complexities and overheads (information structures at middle hubs, control messages, and so on.) In view of the above investigations, this exertion does not really bring about great execution; it thusly ends up noticeably flawed whether it is surely justified regardless of the exertion. Considering this line of thought, a few analysts have investigated whether broadcasting/flooding a MANET with bundles could be a reasonable other option to guarantee high packet conveyance proportions.

1.7 Buffer Management

The buffer management has an important role on the performance of the protocol. The nodes ought to have sufficient number of information bundles inside their in order to contribute to recovery of missing packets of the other nodes. Buffer management is a basic assignment for the unwavering quality and the effectiveness of the convention. . It needs to keep up the two buffers of the convention and performs information conveyance in FIFO arrange as clarified beneath.

Buffer Maintenance:

Each node has its own data buffer where packets are buffered so as to retransmit the lost packets. The information support of the buffer is kept up by utilization of various systems which is worked intermittently at a predefined rate. This mechanism works contrastingly in various conventions in order to settle on a choice about the status of each packet. Packets enter and leave the data buffer of nodes either intermittently or relying upon some threshold value. A missing packet which couldn't be recovered amid any methods is declared as lost and the convention does not recover it anymore.

FIFO Order Delivery:

The packets in the data buffer are lined in FIFO order. Upon receipt of a data packet, the buffer management unit performs a delivery operation on the data buffer. The packets are conveyed to upper layer on the off chance that they are in FIFO arrange and there is not a hole between them. Otherwise, they are hold in the buffer until the missing packets causing the gap are received or declared as lost.

1.8 Problem Statement

Multicasting is an essential service for ad-hoc wireless networks. As it is one of the relevant issues of communication in infrastructure or centralized administration networks, it is very important to make this multicasting scheme as reliable as possible. Accordingly, many reliable multicast schemes were studied in order to overcome packet losses in the network. The reliable delivery of multicast data packets needs feedback from all multicast receivers to indicate whether a retransmission is needed. A reliable multicast delivery in the wireless Ad-hoc network requires a multicast packet to be received by all multicast receiver nodes. So, one or all members need to buffer data packet for possible error recovery. Furthermore, different buffer strategies are essentially used in existing reliable multicast protocols towards support error recovery and reducing buffer overflow**.**

Reliable multicasting AODV protocol (RMAODV) is a reliable multicasting protocol which provides the delivery of an ordered contiguous sequence of data packets from one sender to many receivers in an ad-hoc network. As a sender sends the packets to all its multicast receivers, it has to buffer the packets for retransmission in case there is any news of lost packet from any of the receivers through acknowledgement. All the receivers send their acknowledgement and retransmission request to the sender which in turn retransmits the requested packets to the respective receivers. Sender discards the packet as soon as it gets the acknowledgement of the packet from all the receivers. Or if, when sender's buffer is full, it starts discarding the old packet so as to allow the new packets in its buffer. This causes problem if the packet has not been received by all the receivers as sender may discard a packet before it receive acknowledgement from all the receivers due to buffer capacity. As sender buffers all the packets for retransmission and receives acknowledgement from all the receivers, it however increases the buffer overhead of the sender. So it is essential for the protocol to support error recovery and buffer management to manage the buffer overhead of existing nodes.

1.9 Aim of the thesis

"The goal of this thesis is to manage the buffer overhead by distributing the overhead to dynamically selected set of one-hop neighbors from the sender which in turn will retransmit and receive acknowledgement from different receivers."

1.10 Objective of thesis

1. To reduce the buffer overhead of nodes and avoid the ack-implosion problem.
2. To generate an algorithm which selects a set of forwarding nodes for each sender so as to distribute the overhead of sender node at the time.
3. To analyse the impact of proposed algorithm by comparing the end results of modified and previous protocol.
4. To observe the number of packets dropped, average retransmissions, packet delivery ratio and number of RREQs sent in modified and original protocol.

1.11 Thesis Layout

Chapter 1 introduces the mobile ad hoc networks and the multicasting in them in detail. First of all, background and characteristics of MANETs are discussed where each characteristic is summarized. Three types of routing protocols in MANETs and their comparison is done. Multicast routing is described and how it is done in ad hoc networks. Problem statement and aim of the thesis is mentioned.

Chapter 2 consists of the brief literature review which was done in order to understand the existing protocols for the multicasting, reliability and buffer management while routing in mobile ad hoc networks. Different approaches used in different protocols are studied here.

Chapter 3 introduces the existing protocol "Reliable Multicasting AODV" in which the proposed algorithm has been added to work better. Feature of Reliable MAODV are detailed in the form of path discovery process, packet loss and retransmissions.

Chapter 4 has the main thesis work which includes the proposed algorithm in the existing protocol. Changes made in the existing protocol are mentioned so that it works better in terms of reliability and buffer management.

Chapter 5 discuss the tool we have used for our simulation i.e. OPNET. The experimental setup is described briefly introducing how the tool works while creating the **13** network and running the simulation. Simulation setup is also mentioned which clearly tells about the area, number of nodes and parameters used.

Chapter 6 shows the result and analysis of the simulation of our thesis. This discusses how much positive result the new protocol shows as compared to the existing one in terms of different performance metrics.

Chapter 7 concludes the thesis with conclusion and future work that what are the drawbacks of the protocol which we can overcome in our future work.

CHAPTER 2

LITERATURE REVIEW

Many approaches have been used in recent years covering the reliable communication to the nodes in MANETs as well as their buffer management which is obvious so as to manage the error recovery mechanism. With every approach different protocols are proposed and hence many sources have been used to find the background of this project.

2.1 Based on Negative Acknowledgements

Hoda Baraka and Ahmed Sobeih proposed in [12] a Reliable Multicast Protocol for Ad-hoc (Remhoc). It follows receiver-initiated Negative Acknowledgement (NAK). This protocol relies on receivers to detect the lost packets and to initiate loss recovery process for such losses. Source has a very small role in it as compared to the receivers. While sending the packets, source makes sure to send the packets with increasing sequence number so that it'd be easy for the receivers to detect packet loss, if any. Receivers detect the gaps between the sequence numbers as they receive the packets on their part. After the detection, receivers request for retransmission by sending NAK to the source. Multiple receivers may send the retransmission appeal at the same time, so to avoid the request collapse problem every receiver has a request timer which is random for each receiver. As this timer expires, receiver can send its NAK. To keep an eye on the last packet being received, receiver also has a heartbeat timer which when expires, a heartbeat packet containing highest sequence number been received till now is sent to the source. These timers depend on distance between the nodes, hence increases overhead and more delays.

Ken Tang et.al in [13] proposed blockage controlled adaptive lightweight multicast transport protocol (CALM) where blockage in the network is indicated through NAK. Negative acknowledgement from any receiver urges the source to add that receiver into the 'receiver list' and then the source enter the curb control phase. In blockage control phase, sender selects a acceptor from the acceptor list and send the data packet which has a kind of indicator attached to the header. This will indicate the receiver that it has to reply with an acknowledgement. On the receipt of this acknowledgement, receiver is deleted from the receiver list. When the acceptor list becomes nil on following the same scheme, source assumes that there is no congestion and hence it exits the congestion control phase.

2.2 Based on Hop Distance

Mohamed A. Kalil et.al introduced Hop-aware buffer management scheme [14] multi-hop networks to improve the reliability. N number of nodes are considered which are consistently distributed among the network and having a common sending range, all nodes are distributed into four classes: Class 1, Class 2, Class 3 and Class 4. Classification is done based on number of hops which can be taken from the information table:

Let max = Maximum number of hops

k = 0,1,2,3,4,……, max

where k represents the number of hops that packet traverse from source to current node.

$1 \leq k < N/3$ Class 1

$N/3 \leq k < (2N/3)-1$ Class 2

$(2N/3)-1 \leq k < (2N/3)+2$ Class 3

$(2N/3)+2 \leq k < max$ Class 4.

According to this classification, packets are said to be real time or non-real packets. Scheduling of packets is based on number of hops information. Higher priority is being given to the low-hop packets. As buffer is divided into four division according to the classification, loss of packet from the partition is possible while the partition is full. But considering hop count information alone is not preferable because there are factors like energy consumed in each hop which can't be ignored while improving the reliability via this technique.

2.3 Sender Initiated Algorithms

Thiagaraja Gopalsamy et.al developed in [15] an algorithm named Reliable multicasting algorithm (RMA) which supports sender initiation to provide lossless delivery of data packets among reachable nodes. This algorithm doesn't depend on any underlying mechanism (tree or mesh) and works with all. Connectivity between reachable nodes is maintained by periodically exchanging HELLO messages between neighbors. Unlike wired networks where criteria to select the best path for any packets is minimum number of hops, RMA considers path with longer lifetime as the best path. Also, path must have more of the group members rather than negligible group members. Acknowledgement from the receiver to source follows the same path back. A multicast session takes place in which sender sends data packets to different hosts and these hosts can leave or join this session at random. Source creates sequence table for each multicast session where it stores the sequence number of message which is sent. Sequence entry gets deleted each time all the group members receives the packet and in case packet is not received by all the receivers, it is resend and a special field is marked in the table. Here, as all receivers send the acknowledgement to the source, it may suffer from feedback implosion problem.

J. C. Lin and S. Paul introduced Reliable multicasting transfer protocol (RMTP) in [16] which guarantees higher reliability as well as lossless delivery of data packets even in bulk transfer. This protocol avoids acknowledgement implosion and end-to-end delay problem. Here acceptor is grouped into local sector where every sector has a representative called designated receiver (DR). DRs are chosen according to the approximate distance of all acceptor. These are themselves acceptor of the data packet from the source but as the DRs represent their local region, only they are permitted to send status of the packets to the sender about its whole local region. Other acceptor send the status whether the packet has received or not to their designated receiver which further forwards it to the source. So, the whole process is being distributed among the source and the designated acceptor only. DRs basically handle the retransmissions, process the received acknowledgements and buffer the received data. But for long sessions where they may have shortage of space, the caching part can be impractically large.

2.4 Buffer Usage Reduction

K. P. Birman et.al came up with an extension of gossip protocol named Bimodal Multicast Protocol (BMP) in [17]. Gossip protocol basically works by exchanging information just like gossips which in turn is propagated in a similar way as viral infection. So, if X receive a news and then have to set communication with Y, X will send a copy of the news to Y. BMP is based on probabilistic broadcast and has mainly two phases: 1st phase recognize message loss and 2nd phase correct such losses but second phase runs only when needed. Nodes send their message summary history to some randomly selected nodes and through this gossip they themselves detect the missing packets hence sending the retransmission request. Messages are prioritized first and then recovered accordingly. In case if a message is there for recovery from too long, the protocol give up on it and mark the packet as lost. The process continues to buzz about a message for a fixed number of bulbous and it is necessary to send the retransmission request within the same round where the message has lost otherwise the request would be dropped. In BMP, each node buffers the packet for a fixed amount of time and this assigns to a heavy drawback of this protocol.

Z. Xiao et.al improved the bimodal multicast protocol as a lightweight protocol to optimize its buffer management, namely Lightweight Randomized reliable multicast protocol (RRMP)[18] . Acceptor are grouped into number of division based on their distance from the sender. RRMP has two kinds of buffers: Short term buffers and long term buffers. Short term buffers can keep the message for a fixed interval of time, say T. After time T, the buffer discards the information or keeps it in the long term buffer. Wherein a long term buffer stores the message for quite a long time and discards the message only when there is no retransmission request for it in a long time. Lost packets are recovered in this protocol either using local or remote recovery. In remote recovery, a node sends the request to its parent region's node while in a local recovery node randomly chose another node from its local region and sends it the retransmission request. To avoid multicast requests for error recovery, RRMP uses back-off algorithm. However, this process takes a long time for the acceptor to search and find the correct repair nodes as the number of participants increase.

2.5 Packet Stability

A packet is stable when it is conveyed to all group members. Buffer management approaches that unequivocally consider exist. In [23] The specialists proposed a security identification calculation for disposing of safe packets from the buffers. The members are divided into groups, and in error recovery, each node is added. This procedure keeps running by letting the receiver periodically exchange history information about the received sets of packets. Inevitably, one beneficiary in the group ends up noticeably mindful that all the receiver in the group effectively got the packet and declares this to all the group members. In addition, all individuals can securely dispose of the packet from the buffer. `Disadvantage of this algorithm is that it causes high message traffic because of the frequent exchange of messages.

A.M. Costello proposed the search party protocol where clock contribution disposes of packets from the buffer. Every one of the individual's discard packets after a settled measure of time to achieve stability. In any case, the convention stays unclear on the issue of choosing the best possible time interim for disposing of packets. A heuristic buffer management strategy in view of

ACKs and NAKs is proposed in [24] to give scalability and reliability. In each group acceptor, one or more members possess higher error rates than the other members. These nodes are those with the slightest solid and slowest links. The possibility of this strategy is that when a message is accurately gotten by the nodes, it has been most likely gotten by the majority of alternate nodes. Hence, repair nodes that buffer the message can dispose of it.

J. Pereira et.al developed a network friendly epidemic multicast which combines a standard epidemic protocol with a novel buffering technique that combines different selection techniques for discarding messages in case of a buffer overflow. The utilized choice procedures are irregular cleansing, age-based cleansing, and semantic cleansing. Arbitrary cleansing alludes to the irregular disposing of a thing from the cushion. Age-based cleansing is essentially disposing of the most established message, while semantic cleansing means disposing of a message perceived Obsolescence relation is determined by the application.

As observed, the existing algorithms and protocols are not sufficient to guarantee an efficient buffer management and reliable multicasting. Drawbacks of aforementioned protocols are summarized in Table 2.1.

Table 2.1 Comparison of studied protocols/algorithms

S.No.	Protocols/Algorithms	Drawback
1.	Reliable Multicast Protocol for Ad-hoc (Remhoc)	Increased overhead and delay as timers depend on distance between the nodes.
2.	Congestion controlled adaptive lightweight multicast transport protocol (CALM)	Congestion control alone doesn't give perfect reliability
3.	Hop-aware buffer management Scheme	Considering hop count information alone is not preferable as there are more important factors.
4.	Reliable multicasting algorithm (RMA)	It may suffer from feedback implosion problem
5.	Reliable multicasting transfer protocol (RMTP)	For long sessions, the caching part can be impractically large

In this dissertation, work has been done on overcoming certain drawbacks like feedback implosion problem and increased overhead on sender.

CHAPTER 3

RELIABLE MULTICASTING AODV PROTOCOL

3.1 Introduction

The Multicast Ad-hoc On-Demand Distance Vector routing protocol [25] finds multicast routes on demand using a broadcast route-discovery mechanism. Route Request (RREQ) message is started by a portable node when it has data to send to a multicast group however it doesn't have a route to that group or when it wishes to join a multicast group. On accepting a join RREQ, just an individual from the coveted multicast group may react. On the off chance that a join RREQ for a multicast group is gotten by an intermediate node of which it is not a member, or assume on the off chance that it gets a RREQ and it doesn't have a route to that group, the RREQ is rebroadcasted to its neighbors. In react to RREQ, receiving node sends back the route answer as RREP. Receipt of RREP gives the information of route to the sender and through this route sender may send the data packet to the goal.

3.2 Path Discovery Process

As the nodes are portable, each time they want to communicate to each other, a path discovery process is necessary. This procedure chooses the way depending on the freshest route and little hop count. Route request and route reply are persistently traded in order to characterize most likely the best way between the nodes. To start with, sender sends RREQ either to join a multicast group or to send information packet to multicast collectors. Route reply comes in the event that nodes have a place with the multicast group or not. As the RREQ is communicated over the system, pointers are set up by nodes to build up the invert route in their route tables. At whatever point a node gets a RREQ to begin with, it refreshes its route table to record the succession number and the following jump data for the source node. This is done in light of the fact that the invert course passage may later be utilized to transfer a reaction back to the source. An extra passage is added to the multicast route table for join RREQs. The passage done here is not initiated unless the course is chosen to be a piece of the multicast tree. In the event that a node gets a join RREQ for a multicast group, it might answer on the off chance that it is a part for the multicast group's tree and its recorded succession number for the multicast group is in any event as extraordinary as that contained in the RREQ. The node which has reacted refreshes its route and multicast route tables by putting the asking for node's next jump data in the tables, and after that unicasts a Request Response (RREP) back to the source node. As nodes along the way to the source node get the RREP, both multicast route table and route table passage are included by them for the node from which they got the RREP, in this way making the forward way as appeared in Figure 3.1. Inthis figure, the multicast source is represented by S, the multicast receiver is represented by Rand the intermediate nodes are represented by N. Arrowed line depicts the RREQ being send and dotted arrow line depicts the RREPs.

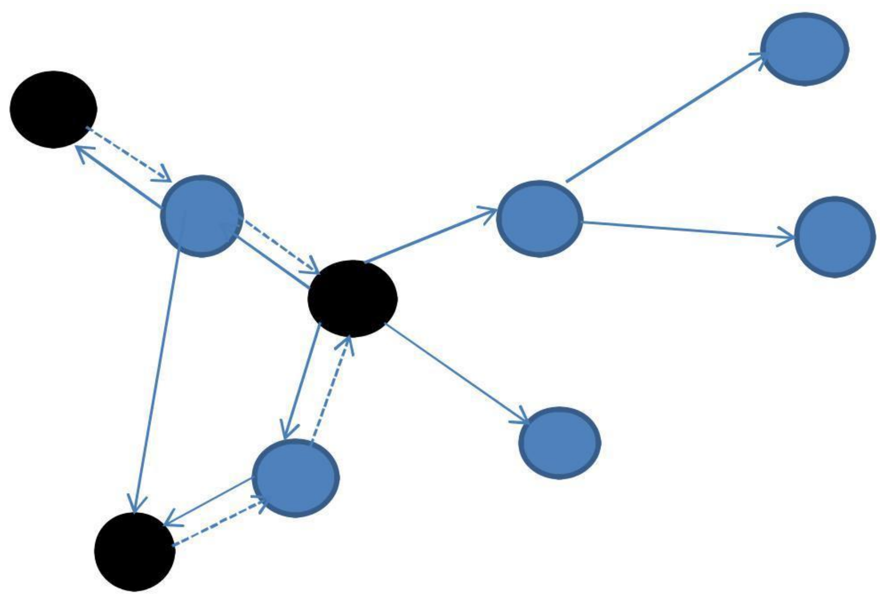

Figure 3.1 Path discovery process in Reliable Multicasting AODV

When a source node broadcasts a RREQ for a multicast group, it mostly receives more than one reply. The source node keeps the got course with the best arrangement number and most limited jump check to the closest individual from the multicast tree for a predetermined timeframe, and every single other course are ignored At the last of this period, source node point interfaces with the picked next influence in its multicast route table, and unicasts a start message (MACT) to this picked next hop. When get the MACT message, associates with the district for the source node point in its multicast course table. It doesn't fast the message any further, if this node point is a man from the multicast tree. In case there is an inside point which is not a man from the multicast tree, it may get no shy of what one RREPs from its neighbour's. It keeps the running with hop which is best for its route to the multicast group, unicasts the MACT message to that next skip, and allows the relating segment in the multicast route table. This procedure keeps running until the route point that started the RREP member of tree) is come to. The incitation message however ensures that the multicast tree does not have particular approaches to manage any tree node. node concentrations basically forward data disperses induced courses in their multicast course tables. Since AODV keeps hard state in its arranging table, the custom needs to adequately track and react to changes in this tree. In case a section rejects its choice with the get-together, the multicast tree needs pruning.

3.3 Packet lost detection and Retransmissions

The fundamental thought behind Reliable Multicasting AODV [26] is to give dependable transmissions of information from sender to every one of the receiver. Sender breaks the to-be-transmitted information into packets of some settled size aside from the last one. It assign the arrangement number to every packet beginning from 0 in increasing order, with the goal that receiver can recognize the copy packets. This sequence number likewise helps in recognizing the lost packet. As the recipient gets the packet from the source, it monitors the sequence number relegated to packets. For each receive packet, it sends a positive acknowledgment (ACK packet) to the sender. A lost packet is recognized by the gap in grouping number. Sender gets the acknowledgement from various recipients. As the nodes are portable, there are chances that nearby nodes may move far from each other and that is the reason, sender does not wait for all the children to respond due to their frequent mobility. Sender reacts to retransmission demands at general time interims i.e. packets are retransmitted to the asking for receivers occasionally from the retransmission line.

In the wake of sending the bundle, every sender sits tight for a specific time (Tack). On the off chance that affirmation of the sent packet is not gotten till time Tack, sender accept the bundle as lost and does the passage in its retransmission line, retxQ. Every passage in retxQ comprises of a succession number of a bundle and rundown of collector nodess where packet is to be despise.

The retransmission line is inspected each Tretx by the sender nodes. In the event that the line is not unfilled, every bundle is multicast to the asking for nodess if the quantity of nodess surpasses a limit;

generally the packet is unicast just to the asking for nodes. A case of a retransmission line is appeared in Table 3.1.

Sequence no.	Receivers
19	R_7, R_{12}, R_{14}
23	R_5

Table 3.1 Example of a Retransmission queue (retxQ)

Although the protocol provides high reliability to the multicasting scheme from the sender to receivers, the overhead increases as there is only one node (sender node) which has to buffer all packets until the retransmission is done for lost packets. It is only the sender node which receives all the acknowledgements from different receivers. So, due to these reasons there are chances of buffer overflow. Buffer overflow creates problem when buffer starts dropping the new packets even before it is buffered, or else it may drop those packets for which all acknowledgements has not been received.

CHAPTER 4

THE PROPOSED APPROACH & METHODOLOGY USED

4.1 Overview

In the proposed approach, an algorithm has been developed which selects a set of one-hop acquaintance from the sender, named as Forwarding Nodes (FNs). These FNs receive the packets from the sender so as to forward it to the further receivers. When FNs receive the packet from sender, it buffers the packet for retransmission purpose, in case if there is any retransmission request. Receivers in turn send the ACK packet to the FNs and not to the sender. Primary reasong behind selecting the subset of one hop acquaintance is to retransmit the requested data lessening buffer overhead and receiving the acknowledgements from different receivers avoiding ACK-implosion problem.

While sender has to send a packet to the multicast group, it sends a message to all its FNs indicating them to find a way to the destination. After the way-finding, FNs update their table and reply back to the sender with their table entry. Sender selects a FN on the basis of freshest sequence number and number of hop routes. Now it is the responsibility of the FN to send, receive acknowledgement and retransmit for the packet.

4.2 Proposed algorithm for selection of Forwarding Nodes (FNs)

1. H_One = One-hop neighbours
2. H_Two = Two-hop neighbours
3. FN is initialized to be an empty buffer
4. FN = Nodes in H_One with different neighbours in H_Two
5. H_One = H_One – FN
6. H_Two = H_Two – N(FN)
7. while(H_One ≠ null or H_Two ≠ null)
8.   for each node in H_One
9. B_f for each node
10.   ghest B_f node
11.   FN = FN + n
12.   H_Two = H_Two – N(n)
13.   H_One = H_One – n
14. end while
15. return FN

Using this algorithm, forwarding nodes (FNs) are selected for each sender whenever it needs to send packets to multicast receivers. As observed, the set is nothing but just few one-hop neighbors of the sender so as to send packets to all multicast receivers. As the one-hop neighbors connecting with unique two-hop neighbors, it makes sure that this set together has link with all the nodes where packets are to be sent.

this algorithm, we use N_k (u) to represent the neighbor set of u, where nodes in the set are not further than k−hops from u. N_k (u) includes u itself, i.e. N_1 (u), one-hop neighbor set, can be simply represented as $N(u)$. Neighboring nodes exchange their one-hop neighbor set information and therefore, each node u has its two-hop neighbor set information N_2 (u). The proposed algorithm is executed at the sender to determine its own forwarding nodes set: A sender S selects its forwarding nodes set from its one-hop neighbor set N(S) to cover all the nodes in its two-hop neighbor set N_2 (S). Consequently, each node u in N(S) can be one of these mentioned two cases:

1. u is a forwarding node, it will not discard the packet from its buffer until all their children have received the multicast packet and retransmit lost packets by multicasting them only to the requesting receivers in local group of the forwarding nodes.

2. u is not a forwarding node and if it is a receiver node, it will reply an acknowledgement to the forwarding nodes, else the node will discard the packet.

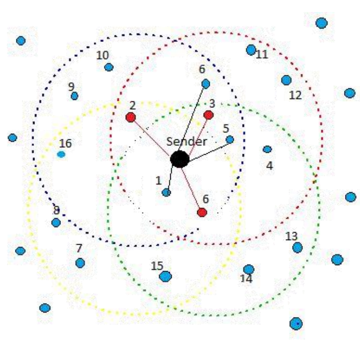

Figure 4.1 Sample network using the proposed algorithm

From Figure 4.1, let us assume N(I) = {1, 2, 3, 4, 4.5, 5, 6,} and N2 (I) = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}. By utilizing the proposed algorithm in this sort of system, sender chooses nodes 2,3 and 6 as the sending nodes. In the calculation, the sender utilizing this calculation to create a pool of one bounce (H_One) and two jump (H_Two) neighbouring node. All nodess that are neighbour's of the past multicasting are expelled from both pools. nodes in H1 with novel neighbour's in H_Two are expelled from H_One and added to the arrangement of FSs. Hence every one of the one jump neighbours of the FN are expelled from H_Two. The rest of the nodes in H_One with no interesting neighbour's are allocated a buffer figure (Bf) in Equ.1. An allotment at that point happens, which includes the nodes in H_One with the most astounding cushion variable to the arrangement of FNs and expels its neighbors from H_Two. The cradle calculate for the rest of the nodes is then changed. This proceeds until the point when H_One or H_Two is a void set. The arrangement of picked FNs is then connected to the multicast message at the sender. Nodess not in the connected FN set are restrained from multicasting.

The proposed approach also supports mobility in a different way by dynamically selecting the forwarding nodes. The sender chooses a subset of 1-bounce neighbour's in the topology as FNs to forward multicast information packet and gets the ACK packet from beneficiaries the choice in light of a cushion calculate approach, Bf (Equation (1)). The Buffer factor (Bf) for a node i is equivalent to the staying buffer space in the node i isolated by the aggregate buffer estimate. The chose FNs must cover every one of the nodes inside 2 jumps of the sender. The sender sits tight for a predefined length to get ACKs from its FNs. On the off chance that the sender does not get all ACKs from its FNs in sending time of ACK, it accept that a transmission disappointment has occurred for this multicast and that the packet should be detest. In the event that the sender neglects to get ACKs from all its chose FNs after it sends the packet an edge number of times, the sender expect the FN that don't answer are out of its transmission range and stops further attempts.

$$B_f = \frac{\text{Remaining buffer space}}{\text{Total Buffer space}} \quad \text{Equation (1)}$$

We apply the accompanying augmentation to enhance the execution of the algorithm. When a sender S neglects to get an ACK from its FN u after greatest number of retries, S re-chooses elective FN to cover the set which should be secured by u. This algorithm likewise stays away from the ACK implosion issue as it requires just the chose FNs to send ACKs to the sender, rather than all recipients sending the ACKs to the sender.

CHAPTER 5

EXPERIMENTAL SETUP

5.1 Introduction

The simulation was done using D3(Data Driven Documents) library of JavaScript. It runs on JavaScript V8 engine and allows user to create cross-platform applications upon JavaScript language. The compiler has minimal system footprint that allows users to run the simulation on minimal amount of hardware capability. It was created by Mike Bostock in 2011.
Its items and arrangements address the accompanying parts of interchanges systems:

- Application performance management
- Planning
- Engineering
- Operations
- Research and development

Its utilization can be separated into four noteworthy strides. The initial step is displaying (making system models), second is to pick measurements, at that point run reproductions lastly see and break down outcomes. This device set is capable and can make and test substantial system conditions by means of programming. To address each of these viewpoints, our program in Javascript, gives comparing item modules all through its product offering. It assumes a key part in today's rising specialized world in, developing and enhancing the remote innovation protocols‟, for example, Wi-Fi, Universal Mobile Telecommunication System (UMTS), and so on, „design of MANET directing protocols", working on new power administration frameworks over sensor networks‟ and „enhancement of system technologies", for example, IPv6, MPLS.

Features of D3 Library

1. Provides programmable, yet convenient API for creating the GUI.
2. Helpful in assessment of plans for new system models and structures rapidly and repeatedly
3. Good execution investigation of existing frameworks in light of client conditions.
4. Easy for understanding and implementing the system conduct in different situations.
5. Very adaptable and simple graphical interface to see the outcomes

5.3 Model Design

The basic working flow of our research can be seen in the flowchart below Figure 5.1. First, model is designed i.e. according to the scenario, a network is created. Necessary DES statistics are chosen so as to analyze the scenario better. After applying the statistics, simulation runs by selecting the simulation time. If results are no satisfactory or if result is to be checked for some other scenario, re-modelling is done.

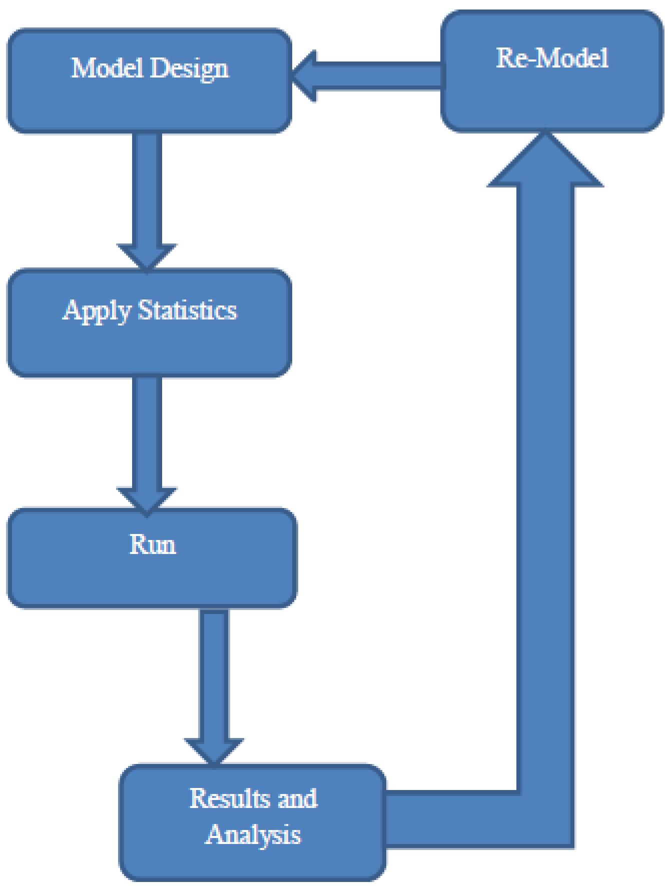

Figure 5.1 Model Design

Initial step while making a system is to make a clear situation. This is furnished by defining the key parameters for our network simulation using JavaScript. The D3 library and its various functions provide us with various simulation options that can be programmed in order to obtain the required simulation environment. The outline is done either consequently or physically. It is done either consequently via naturally creating topologies utilizing quick setup or physically by dragging articles from the protest palette to the venture proof-reader workspace. Pre-characterized situations can likewise be transported in the event that they suit client necessities. Be that as it may, remote systems can be composed by bringing in situations. After the system is composed, nodes must be arranged. Arrangement is likewise performed either physically or by utilizing pre-characterized parameters in the work process.

Figure 5.2 depicts the object palette showing the models under MANET. Different models defined under MANET are shown in the object palette tree, for example, Node Models. Node models consists of Application Config, manet_gtwy_wlan_ethernet_slip4, manet_station (fixed and mobile), Mobility Config, Profile Config, Rxgroup Config, Task Config, wlan2_router (fixed and mobile), wlan_ethernet_router (fixed and mobile), wlan_server (fixed and mobile) and wlan_wkstn (fixed and mobile).

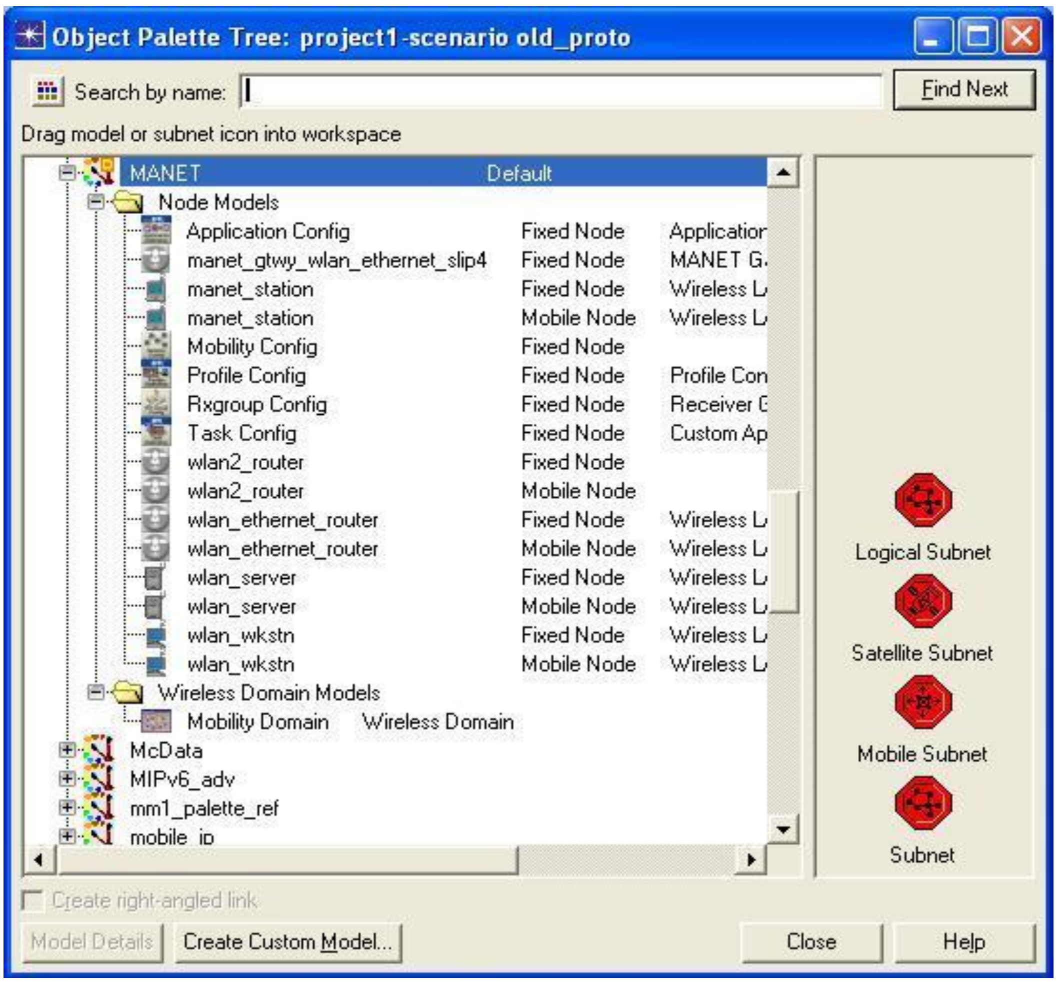

Figure 5.2 MANET Object Palette

Simulation set up of a network is shown in figure 5.3 comprising around 50 mobile nodes moving with different defined trajectories at a speed of 10m/s.

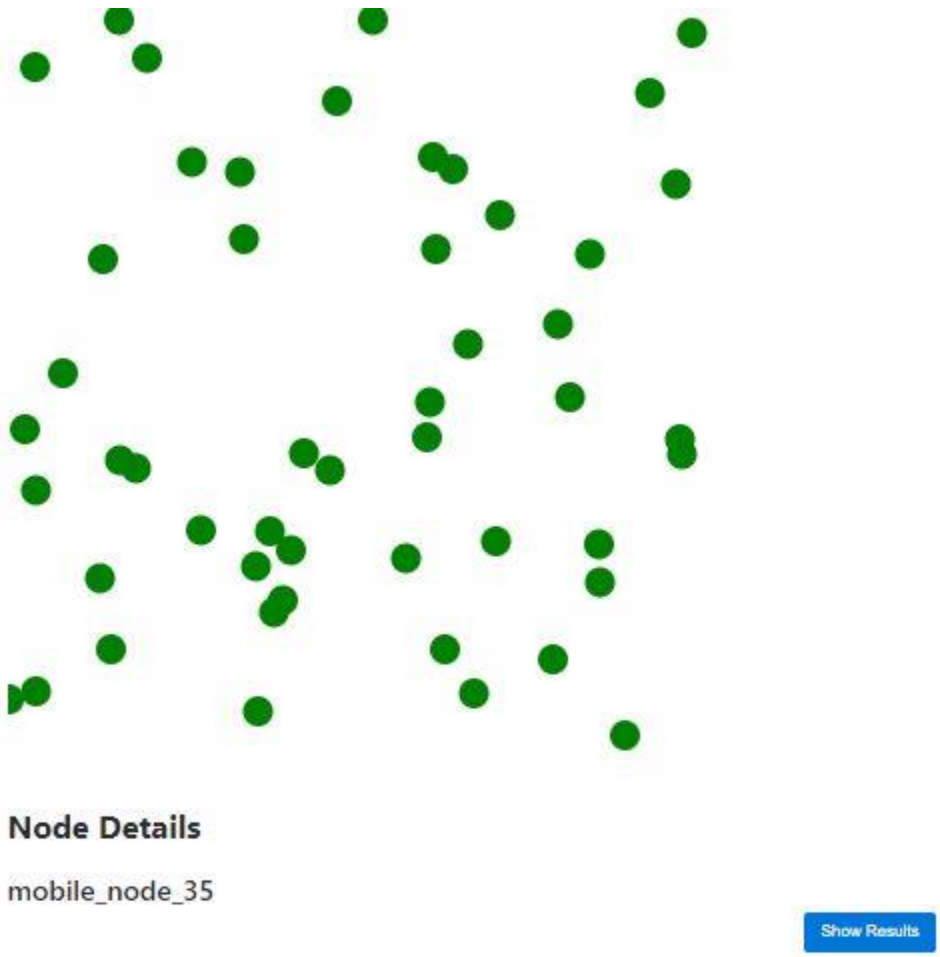

Figure 5.3 An example of network model design

5.3.1 Mobile Nodes

Nodes are workstations which work as a raw packet generator transmitting packets over IP and WLAN. We can assign start time and end time of the simulation in our network. It has 3 attributes:

1. **MANET Traffic Generation Parameters**:

   Attribute to indicate the rate at which bundles are produced.

2. **IP Forwarding Rate**:

   It indicates the rate (in bundles/second) at which the nodes can play out a directing choice for an arriving packet and exchange it to the suitable yield interface.

3. **IP Gateway Function**:

   It determines whether the nearby IP nodes is going about as a portal. Workstations ought not go about as portals, as they just have one system interface.

Movement via trajectories

There are two types of trajectories:

- **Segment based trajectory**
- **Vector based trajectory**

Segment based trajectory:

Section based directions characterize development way with a progression of fragments isolated by pre-characterized focuses. A section based direction is made out of a progression of way fragments. Every way portion can have singular elements. There are two section based direction sorts: settled interim and variable-interim. For settled interim direction, a portable nodes sets aside a similar measure of opportunity to navigate each way fragment. For variable-interim direction, each point along the direction has its own particular determined elevation, hold up time, section traversal time, and introduction. The holdup time makes a portable nodes delay at each section point before crossing the following fragment.

Vector based trajectory:

Vector based trajectories define movement via bearing, ground speed, and ascent rate of attributes of a mobile node. In contrast to segment-based trajectory, there is no explicit end point for vector-based trajectory. Vector-based trajectory follows the circular path around the Earth. Unlike segment based trajectory, which uses multiple segments to form a trajectory path, vector-based trajectory relies on the circle around the Earth, so the trajectory path is determined once the bearing, ground speed, and ascent rate are determined.

Applying Statistics

To determine the measurements that must be gathered amid a discrete occasion recreation we need to browse the "Pick singular DES insights" can be found in workspace fly up menu. Insights should be connected for a composed model is fundamentally two sorts: worldwide or situation wide measurements and protest insights. Worldwide measurements will be gathered from the entire system display planned and the question insights will be gathered over nodes These insights can be connected to a system demonstrate in light of the client prerequisite for his outline. In our outline for our examination we have picked worldwide measurements of MANET that incorporate packets dropped, normal retransmissions and number of RREQs in order to break down the execution of convention.

5.5 Setup

In this research we are using simulation program created upon the well known D3 (Data Driven Documents) library version 4. D3 and Javascript provide us with a programmable interface capable of cross-platform programming. It has high reliability and fault tolerance for failed or incomplete operations. It serves as a highly customizable option for the programming and simulation of networks. D3 is data oriented library, hence it serves as the best platform for manipulation and management of huge amount of data generated by our research. The nodes are scattered in normal distribution across the area of our office in the example described below. Each node is allowed to generate and forward packets as defined in its parameter “MANET Traffic Generation Parameter” as shown in table 5.1 and table 5.2

5.5.1 Simulation Environment:

Simulation environment of 75 nodes are taken so as to analyse the results more properly. Each scenario is made run for approximately 30 minutes, i.e. 1800 sec. Table 5.1 depicts the simulation environment in detail. While creating the simulation network, office network was selected with the network area of 1500*1500 meters square. Each mobile node has the transmission range of 250 meters.

Table 5.1 Simulation Environment

Number of nodes	75
Network Scale	Office Network
Network Area	$1500*1500\ m^2$
Simulation Time	1800 seconds
Trajectory	User-defined trajectory (Vector based)
Transmission Range	250m

Path is defined by the user using vector based trajectory in this simulation. Four different trajectories are created using different attributes. All nodes use any one of these trajectories in the network. Trajectories are shown in Figure 5.4 in brief.

Figure 5.4(a)

depicts the first trajectory used in the simulating network. Trajectory is named „tra_1" and has ground speed of approximately 15m/s.

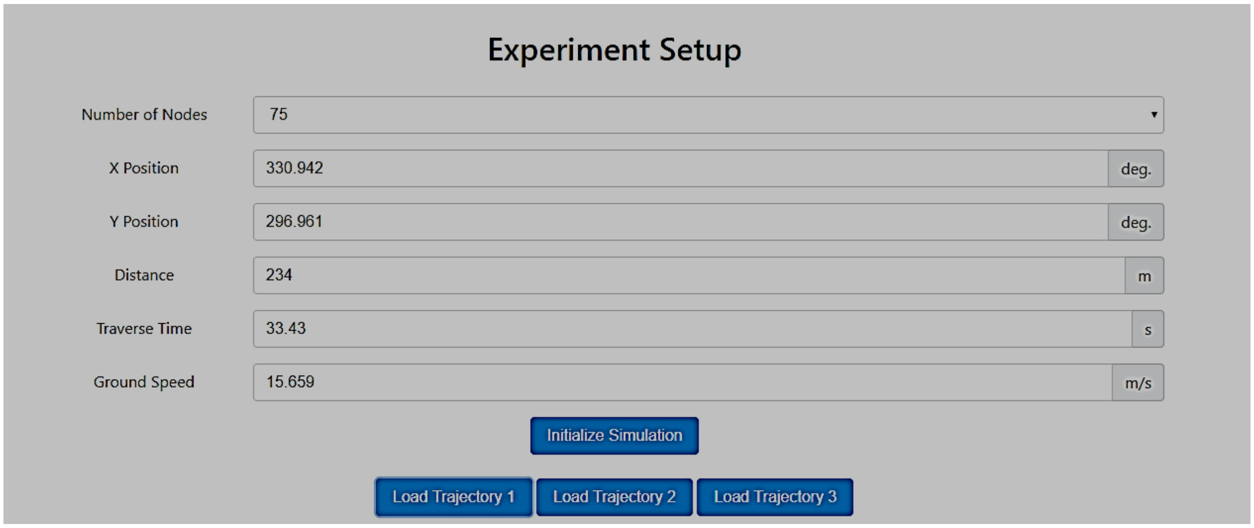

Figure 5.4(a)

Figure 5.4(b)

depicts the second trajectory used in the simulating network. Trajectory is named „trajectory_1“ and has ground speed of approximately 6m/s.

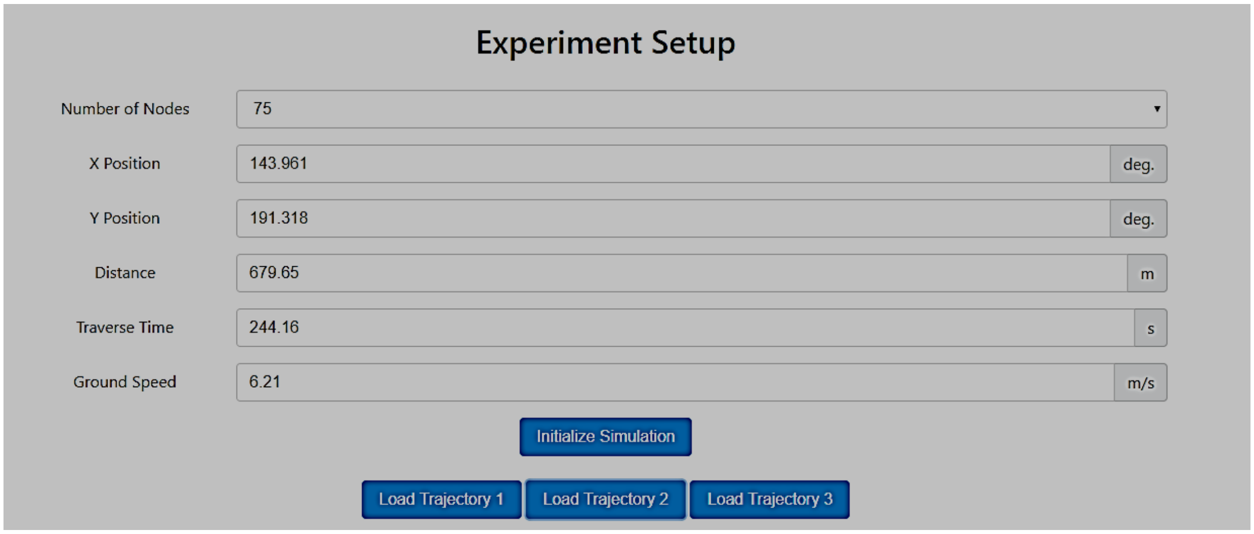

Figure 5.4(b)

Figure 5.4(c)

depicts the third trajectory used in the simulating network. Trajectory is named "trajectory_2" and has ground speed of approximately 6m/s.

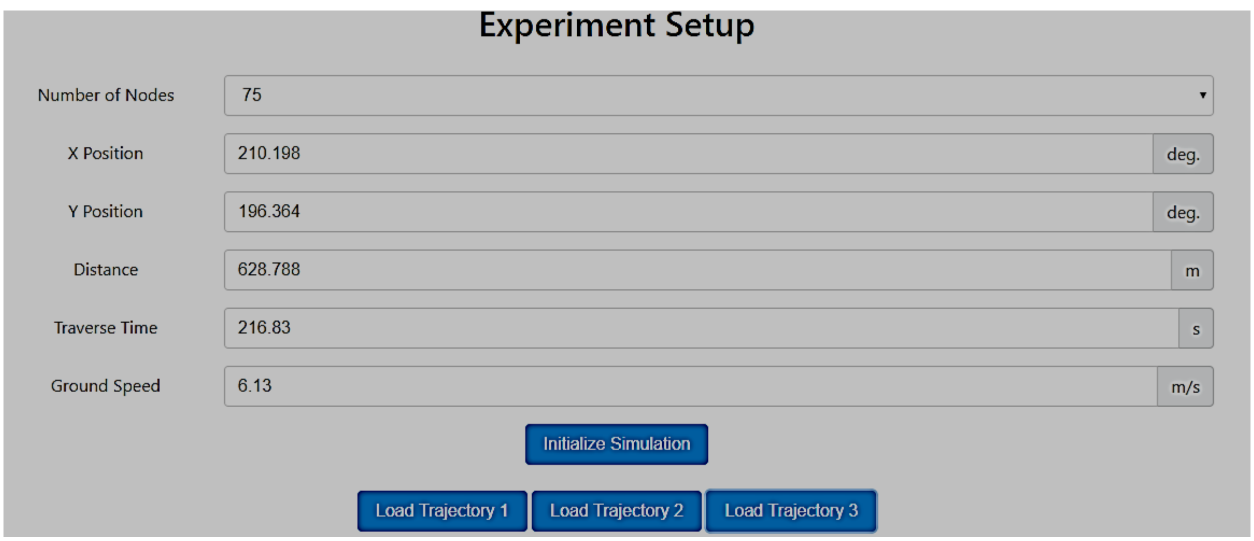

Figure 5.4(c)

Figure 5.4 (a), (b)& (c) : Different vector-based trajectories

5.5.2 MANET Traffic Generation Parameters

In a MANET network, nodes itself are the source of generating packets. So nodes are defined with certain attributes so as to generate packets at different packet inter-arrival time for certain time. In each scenario, out of all the nodes, around half of the nodes have been made the source of generating packets in various intervals. Two kinds of traffic generation parameters are defined: Traffic_Generation_Parameter_1 and Traffic_Generation_Parameter_2. Each node in the simulation network follows any one of these two traffic generation parameters.

Table 5.1 Traffic_Generation_Parameter_1

Attribute	Value
Start time (seconds)	100
Packet Inter-arrival time (seconds)	Constant (28)
Packet size (bits)	Constant (1024)
Destination IP address	Random
Stop time (seconds)	1800

Traffic_Generation_Parameter_1 starts generating the traffic from 100 seconds until 1800 seconds. Packet sizes of 1024 bits are generated continuously with the packet inter-arrival time of 28 seconds. Destination IP address is taken randomly each time packet is sent.

Table 5.2 Traffic_Generation_Parameter_2

Attribute	Value
Start time (seconds)	200
Packet Inter-arrival time (seconds)	Constant (25)
Packet size (bits)	Constant (1024)
Destination IP address	Random
Stop time (seconds)	1800

Traffic_Generation_Parameter_2 generate the packets of size 1024 bits with the packet inter-arrival time of 25 seconds. It starts generating the traffic from 100 seconds until 1800 seconds. Each time a packet is sent, destination IP address is taken randomly.

CHAPTER 6

RESULTS AND ANALYSIS

In this summary simulation environment is modelled in D3(Data Driven Documents) library of JavaScript with reliable AODV and improved AODV protocol. Improvement of the protocol has been measured in terms of number of packets dropped, average retransmissions, packet delivery ratio and number of RREQs sent. These metrics help us in examining the improved AODV protocol in the office area of 1500 meters X 1500 meters. To observe the effect of scalability over the protocol, we have developed two simulation scenarios each scenario constitute 75 nodes as this scenarios contain low and high number of nodes. Changes have been made in a Reliable AODV protocol. Protocol with new algorithm has been named as Improved AODV.

6.1 Performance Metrics

The following accomplishment metrics are taken into account so as to calculate the requirement of the proposed algorithm in the existing protocol by comparing both the protocols. Result of these performance metrics will determine how much improvement has been done by using the algorithm.

Total Packets dropped:

It refers to the total packets dropped by the buffer when there is no more space in it to keep new packets. As new packet comes along, buffer may discard the old packet so as to make some space for the new ones. This metric plays an important role as it determines how much buffer overhead has been affected.

Packet Delivery Ratio (PDR):

PDR determines the reliability of a protocol by calculating the number of packets sent and number of packets actually delivered. PDR is taken as the ratio of total packets received to the total packets sent.

Average Retransmitted Packets:

It computes the normal number of packet retransmissions in the recreation arrange. It is taken as the proportion of number of retransmission packets transmitted to the aggregate number of unique information bundles transmitted.

Number of Route Requests:

Entire number of route requests has been measured by measuring the total number of RREQ messages sent over the network.

6.1.1 Total Packets Dropped

Graphs in Figure 6.1 show detailed comparison of total packets dropped in the original and improved protocol for 75 nodes respectively. It clearly shows that the packet dropping has been decreased in the improved protocol as compared to the original protocol, which gives a positive sign for the new protocol. As the overhead has been distributed, each buffer has lesser number of packets to deal with and hence less packet dropping. Hence, total packets dropped have decreased.

In the initial minute, improved AODV has its packets dropped increasing slowly as compared to original protocol which takes a steep rise at early stage. Both the protocol however gave nearly a constant increase with each passing time. Figure 6.1 shows that for 75 nodes, at the end of simulation, packet dropped has decreased from 142 to 125. Graph has shown that improved protocol drops lesser number of 75 nodes.

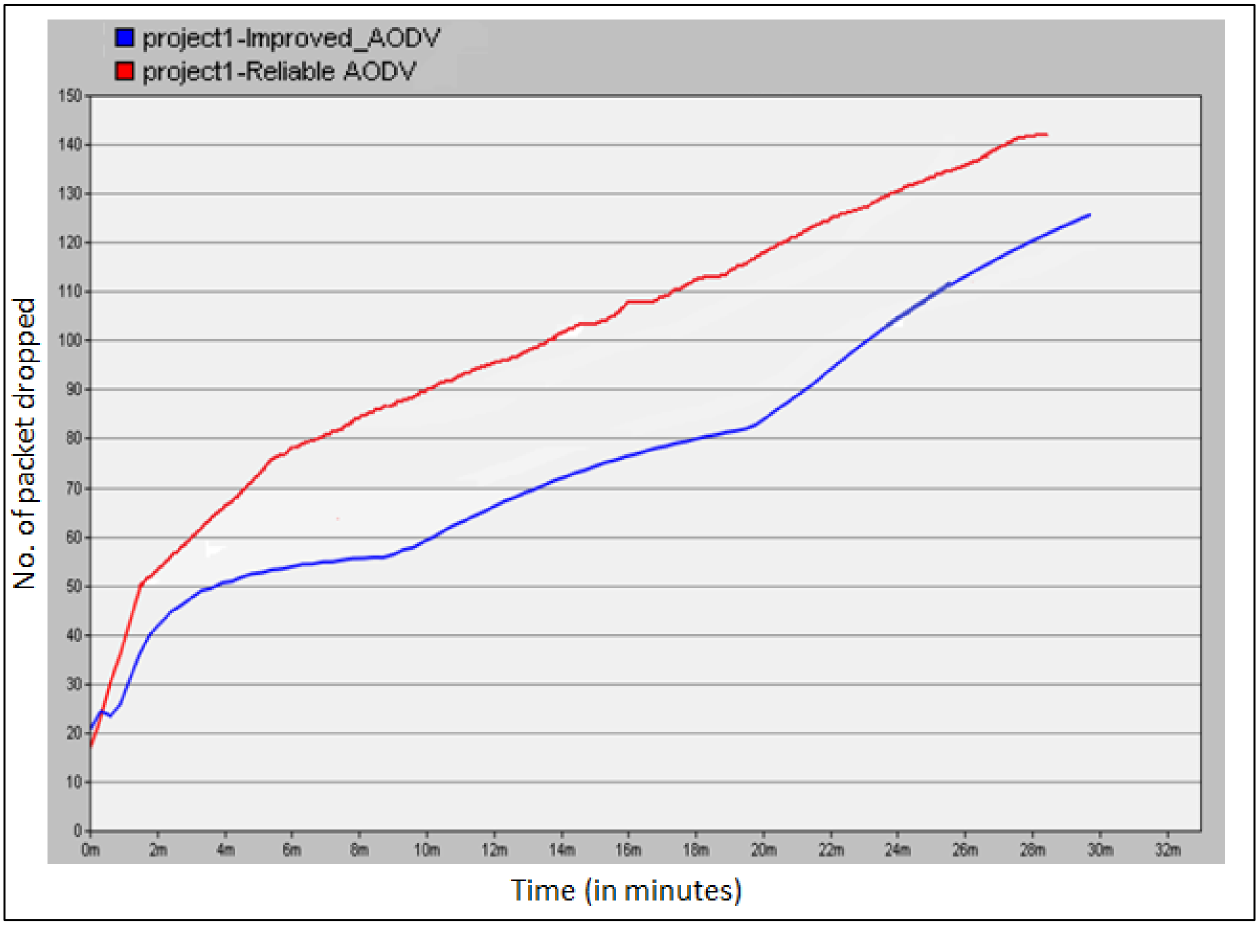

Figure 6.1 Comparison of Total Packets dropped for 75 nodes with Improved AODV protocol and Reliable multicasting Protocol

6.1.2 Packet Delivery Ratio

As PDR determines the rate of packet delivery at the receiver side, it adds in the comparison of protocols testing for reliability. PDR determines the reliability of a protocol by calculating the number of packets sent and number of packets actually delivered. PDR is taken as the ratio of total packets received to the total packets sent. As graph depicts, packet delivery has increased, hence increasing the reliability of the protocol. Figure 6.3 graphical comparison of Packet Delivery Ratio for 75 nodes in Reliable MAODV and Improved AODV. As can be seen from the results, it can be analysed that Improved AODV has better packet delivery ratio than Reliable AODV in case of both the scenarios, i.e. scenario with 75 nodes.

With the addition of algorithm in Reliable MAODV, packet delivery ratio of improved AODV has increased from 90% to 94% in the scenario with 75 nodes.

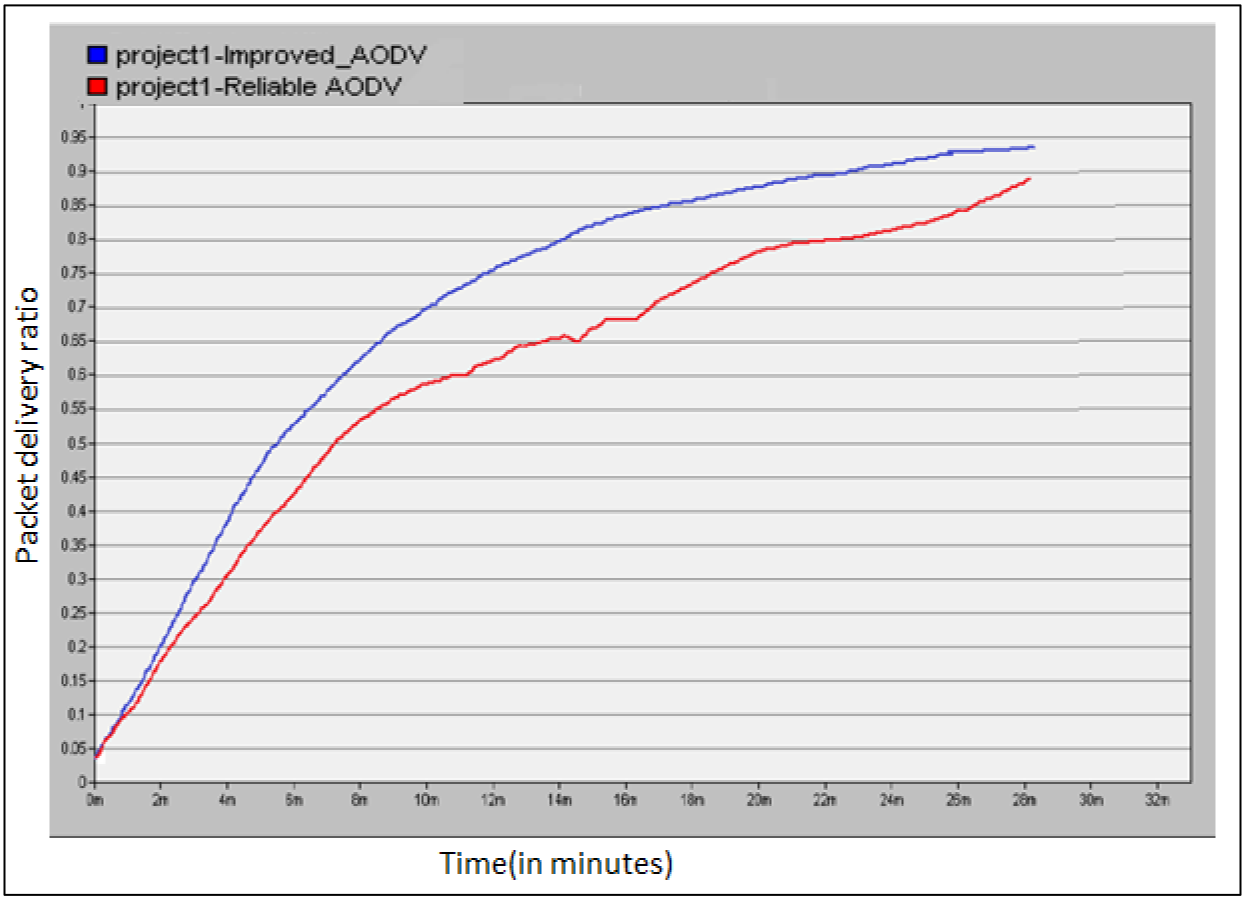

Figure 6.3 Comparison of Packet Delivery Ratio for 75 nodes in improved AODV protocol and Reliable Multicasting AODV Protocol

6.1.3 Average Retransmitted Packets

As shown in Figure 6.5, average number of retransmitted packets has decreased in Improved AODV as compared to Reliable AODV. It is taken as the ratio of number of retransmission packets transmitted to the total number of original data packets transmitted. The average ratio keeps on increasing with the simulation time in case of both the protocols.

With addition of the algorithm for selection of forwarding nodes to decrease the overhead of the sender node, FNs only are responsible for all the retransmissions. As compared to the sender, each FN has less overhead of retransmissions. So this decreases the average retransmission ratio in Improved AODV as compared to the Reliable AODV.

As Figure 6.5 depicts, the ratio keeps on increasing in Reliable AODV from 3 to 12. In case of Improved AODV, the ratio decreases at first minute but after that, it kept on increasing from 3.5 to 8.5. Comparing both the protocols, the ratio of average retransmitted packets has decreased from 12 to 8.5 in case of scenario with 75 nodes.

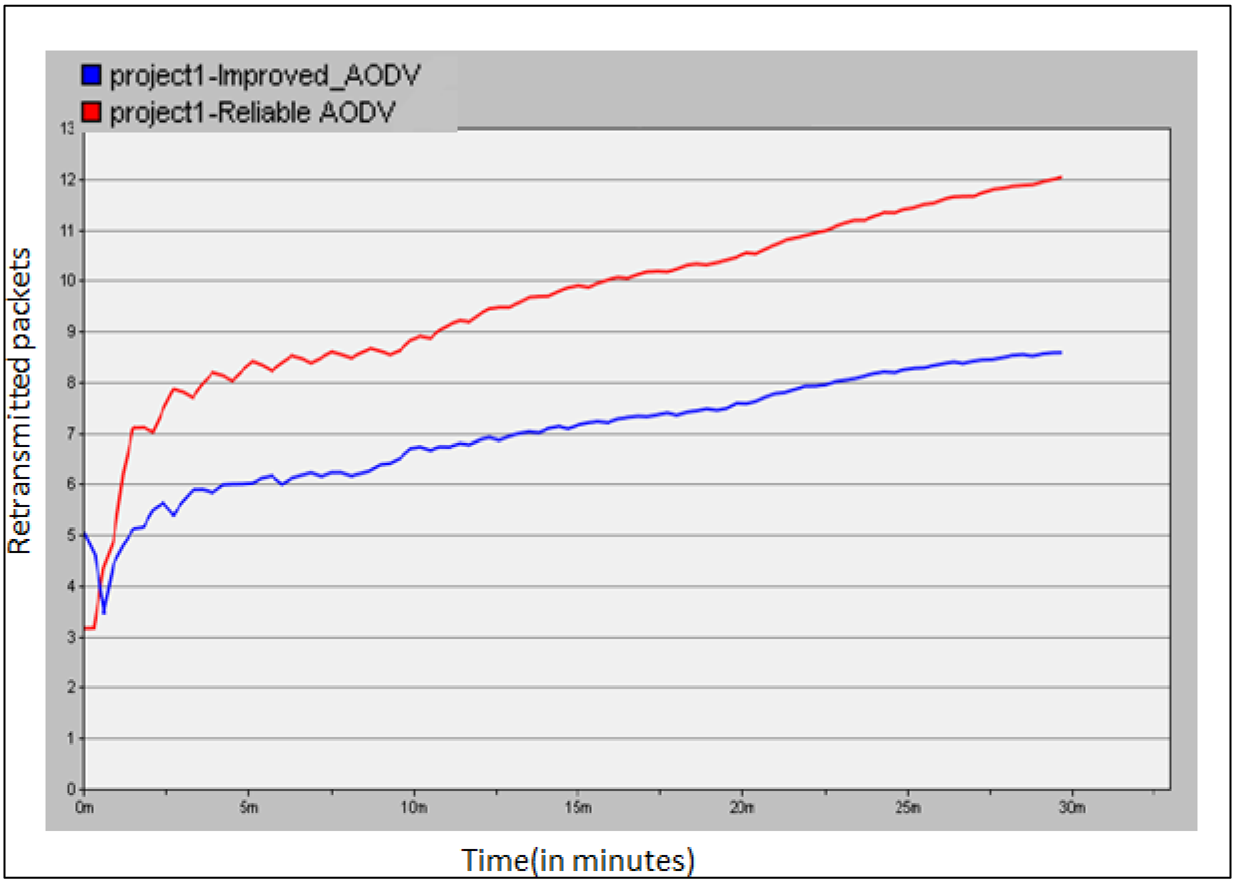

Figure 6.5 Comparison of Average Retransmitted Packets for 75 nodes in Improved AODV protocol & Reliable multicasting Protocol

6.1.4 Total RREQs sent

Total number of RREQ messages determines the total number of route requests. A route request is sent by the sender node to discover the best path in terms of freshest route and small hop count. So, before a data packet is sent, RREQ message is sent so as to update the path.

As can be seen from Figure 6.7, total RREQs has decreased in Improved AODV as compared to the total RREQs in Reliable AODV for both the scenarios with 75 nodes. This decrease may be due to the reason that the average retransmissions have decreased. For each retransmission, RREQ is needed for the freshest path again. So, in this case total RREQs increases or decreases with average retransmission. So with decreased retransmissions, there is a decrease in total route requests sent.

Figure 6.7 shows that at the end of simulation time, for 75 nodes, improved protocol have around 2800 RREQs while original protocol has around 3300 RREQs.

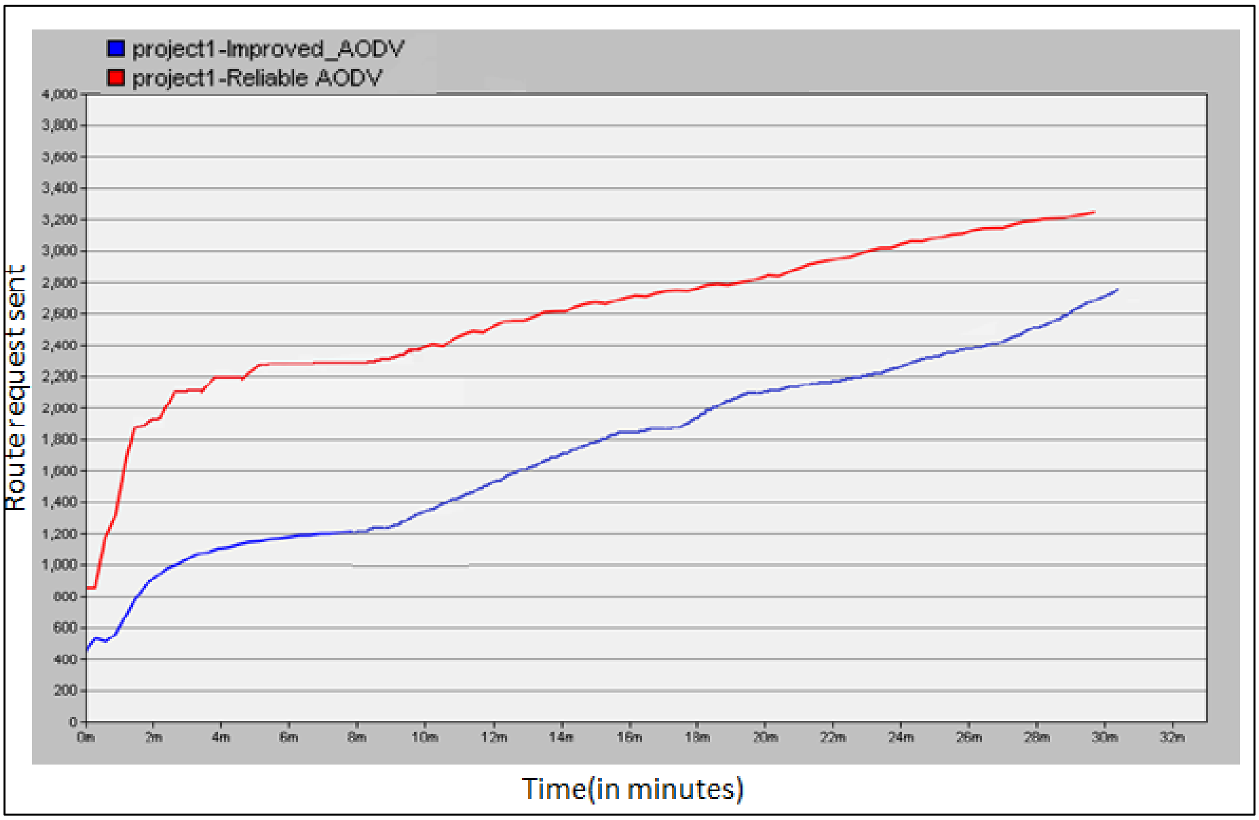

Figure 6.7 Comparison of Total RREQs in 75 nodes in Improved AODV protocol & Reliable multicasting AODV protocol

CHAPTER 7

CONCLUSION AND FUTURE WORK

As we add the proposed algorithm in the existing protocol, both the protocols are compared for number of packets dropped, average retransmissions, packet delivery ratio and number of RREQs sent. The main aim of this thesis is to reduce the buffer overhead at each sender node while sending packets. The comparison result shows that buffer overhead has reduced as the number of packets dropped has decreased. Packet delivery ratio has increased showing better reliability. There are changes in average retransmissions and number of RREQs sent indicating positive result in terms of retransmissions. So the protocol with proposed algorithm: "Improved AODV" has shown positive results as compared to the original existing protocol.

While analyzing more deeply, it is realized that while running the algorithm at each sender before sending the data packets, end to end delay has increased. Original protocol runs simply by sending and receiving RREQs/RREPs, but the improved protocol has to run the algorithm in addition to the existing process. This affects the throughput too. So, throughput and end to end delay shows a little negative result for the new improved protocol.

Future work of the thesis can be overcoming the increased end to end delay as delay plays an important role in the network simulation of MANETs. Overall throughput can also be considered so that there are more packets sent per unit time.

REFERENCES:

[1] X. Bangnan, S. Hischke, B. Walke, ―The role of ad hoc networking in future wireless communications‖, *International Conference on Communication Technology (ICCT 2003)*, Vol. 2, Pages: 1353-1358, 2003.

[2] J. Jubin and J.D. Tornow, ―The DARPA packet radio network protocols‖, *In Proceedings of IEEE*, Vol. 75, Pages: 21-32, 1987.

[3] D. J. Baker and A. Ephremides, ―The architectural organization of a mobile radio network via a distributed algorithm,‖ *IEEE Trans. Commun.*, Vol. COMM-29, Pages: 1320–1332, 1981.

[4] D. Ayyagari, A. Michail, A. Ephremides, ―A unified approach to scheduling, access control and routing for ad-h.oc wireless networks‖, *VTC 2000*, Vol. 1, Pages: 380-384, 2000.

[5] H. Xiaoyan, X. Kaixin and M. Gerla, ―Scalable routing protocols for mobile ad hoc networks‖, *IEEE Network*, Volume: 16, Pages: 11-21, 2002.

[6] M. Abbott and L. Peterson, ―Increasing network throughput by integrating protocol layers‖, *IEEE/ACM Transactions on Networking*, Vol. 1, Pages: 600-610, 2003.

[7] T. C. Chiang, C. Y. Hsu, and J. L. Chang, "Immediate Group ACK tree (IGA) for reliable multicast in mobile Ad Hoc networks," in *IEEE 3rd International Conference on Communication Software and Networks (ICCSN)*, 2011.

[8] Tseng Y.C., Shen C.C, and Chen W.T., ―Mobile ip and ad hoc networks: An integration and implementation experience‖, *In Proceedings of the IEEE Wireless Communications and Networking Conference*, 2003.

[9] S.-J.Lee, Mario Gerla, and C.-C. Chiang‖, On-Demand Multicast Routing Protocol‖, *In Proceedings of the IEEE Wireless Communications and Networking Conference*, WCNC

’99, Pages: 1298–1304, 1999.

[10] B. S. Manoj, Subir Kumar Das, C. Siva Ram Murthy, ―A Dynamic Core Based Multicast Routing Protocol for Ad Hoc Wireless Networks", *Proceedings of 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Pages: 24-35, 2002.

[11] R. Bagrodia, M. Gerla, J. Hsu, W. Su, and S.-J. Lee. ―A performance comparison study of ad hoc wireless multicast protocols‖, *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies*, Pages: 565 –574, 2000.

[12] Mohamed A. Kalil, Hassan Al-Mahdi and Andreas Mitschele, ―Performance Evaluation of Hop-Aware Buffer Management Scheme in Multihop Ad Hoc Networks‖, *IEEE,* 2008.

[13] Thiagaraja Gopalsamy, Mukesh Singhal, D. Panda, and P. Sadayappan, ―A reliable multicast algorithm for mobile ad hoc networks‖, *22nd IEEE International Conference on Distributed Computing Systems*, 1998.

[14] J. C. Lin and S. Paul, ―RMTP: A reliable multicast transport protocol‖, *Proceedings of IEEE INFOCOM'96*, 1996.

[15] Ken Tang, Katia Obraczka, Sung-Ju Lee, and Mario Gerla, ‖Congestion controlled adaptive lightweight multicast in wireless mobile ad hoc networks‖, *In Proceedings of IEEE ISCC*, 2002.

[16] K. P. Birman, M. Hayden, O. Ozkasap, Z. Xiao, M. Budiu, and Y. Minsky, "Bimodal multicast", *ACM Transactions on Computer Systems (TOCS)*, 2008.

[17] Ozkasap, Oznur, van Renesse, Robbert, Birman, Kenneth and Xiao, Zhen, ―Efficient Buffering in Reliable Multicast Protocols‖, *Proceedings of the First Workshop on Networked Group Communication. (NGC01)*, 2001.

[18] H. B. A. Sobeih and A. Fahmy. ―Remhoc: A reliable multicast protocol for wireless mobile multi hop ad hoc networks‖, *In IEEE Consumer Communications and Networking Conference (IEEE CCNC)*, 2004.

[19] Z. Xiao, K. P. Birman, and R. Van Renesse, "Optimizing buffer management for reliable multicast", *In Proceedings of the IEEE Wireless Communications and Networking Conference*, 2002.

[20] E. Royer, and C. E. Perkins, ―Multicast operation of the ad hoc on demand distance vector routing protocol‖, *In the proceedings of MobiCom*, Pages: 207-218, 1999.

[21] K. Guo and I. Rhee, "Message stability detection for reliable multicast", *In Proceedings of the 19th IEEE Conference on Computer Communications (INFOCOM 2000)*, Vol. 2, Pages: 814-823, 2007.

[22] E. Ahi, M. Caglar, and O. Ozkasap, "Stepwise probabilistic buffering for epidemic information dissemination", in *International Conference on Bio-Inspired Models of Network, Information, and Computing Systems*, Pages: 1-8, 2010.

[23] E. Royer, and C. E. Perkins ―Multicast operation of the ad-hoc on-demand distance vector routing protocol*", Proc. of the 5th ACM/IEEE Annual Conf. on Mobile Computing and Networking*, Pages: 207-218, 1999.

[24] A. M. Costello and S. McCanne, "Search party: Using randomcast for reliable multicast with local recovery", *in Proceedings of the 18th IEEE Conference on Computer Communications (INFOCOM '99*), Pages: 1256-1264, 1999.

[25] Li Xiao, Abhishek Patil, Yunhao Liu, Lionel M. Ni, Abdol-Hossein Esfahanian, "Prioritized Overlay Multicast in Mobile Ad Hoc Environments", *IEEE Computer Society*, Vol. 37, Pages: 67-74, 2004.

[26] S. Sethi and S.K. Udgata, ―A Reliable Multicasting AODV for Mobile Ad Hoc Network‖, in *International Conference and Workshop on Emerging Trends in Technology (ICWET)*, 2012.

[27] Rajashekhar C. Biradar, Sunilkumar S. Manvi, ―Channel Condition and Mobility Based Choice of Neighbor Node for Routing in MANET‖, *Proceedings of International Conference on Advances in Computer Engineering, (ACE)*, Pages: 74-78, 2010.

[28] D. Ayyagari, A. Michail, and A. Ephremides, ―A Unified Approach to Scheduling, Access Control and Routing for Ad-Hoc Wireless Networks‖, *In Proceedings of the Vehicular Technology Conference (VTC 2007-Spring),* Vol. 1, Pages: 380 –384, 2007.

[29] Morteza Maleki and Massoud Pedram, "Lifetime-aware multicast routing in wireless ad hoc networks", *In the Proceedings of IEEE Wireless Communications and Networking Conference (WCNC 2004),* 2004.

[30] J. Pereira, U. do Minho, L. Rodrigues, U. De Lisboa, M. Monteiro, R. Oliveira, and A. M. Kermarrec, "Neem: Network-friendly epidemic multicast", *in Proceedings on 22nd International Symposium on Reliable Distributed Systems (SRDS'03)*, Pages: 15-24, 2003.

[31] M.Maleki and M. Pedram, ―Lifetime-Aware Multicast Routing in Wireless Ad Hoc Networks‖, in *IEEE Wireless Communications and Networking Conference (WCNC)*, Volume 3, Pages: 1317 – 1323, 2004.

[32] R. Agarwal and M. Motwani, ―Survey of clustering algorithms for MANET‖, *International Journal on Computer Science and Engineering (IJCSE),* Vol. 1, Pages: 98– 104, 2009.

[33] Das R. and Purab S., ―Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks‖, *IEEE Infocom*, 2000.

[34] Song Yean Cho, Adjih,C. , ―Optimized Multicast based on multi point relay‖, *IEEE*, WICON, 2005.

[35] Lee, S.J., M. Gerla and C.C. Chiang, ―On-demand multicast routing protocol‖, *In Proceedings of the IEEE Wireless Communications and Networking Conference, WCNC '99*, Pages: 1298-1304, 1999.

[36] Alahdal, T., S. Shamala, M. Othman and Z. Zukarnain, ―A simulation engine model analysis for reliable multicast protocol in ad hoc network‖, *International Journal of Computer Science and Network Sec.*, 2008.

[37] Alsaqour, R., M. Abdelhaq and T. Abdullah, ―Modeling the position information inaccuracy in MANET Position-based routing protocols‖, *Res. J. Appl. Sci. Eng. Techn.,* 2008.

[38] Floyd, S., V. Jacobson, C.S. Liu., S. McCanne and L. Zhang., ―A reliable multicast framework for Light-weight sessions and application level framing‖, *IEEE/ACM T. Network*, Pages: 784-803, 197.

[39] Ken, T., K. Obraczka., S.J. Lee and M. Gerla., ―Congestion controlled adaptive lightweight multicast in wireless mobile ad hoc networks‖, *Proceedings of 7th International Symposium on Computers and Communications, ISCC 2002,* Pages: 967-972, 2002.