A NOVEL SCALABLE MULTICAST MESH ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS

KHALID ABDUL FATTAH FARHAN

Ph. D. **2008**

University of Sunderland

A NOVEL SCALABLE MULTICAST MESH ROUTING PROTOCOL FOR MOBILE AD HOC NETWORKS

Khalid Abdul Fattah Farhan

A thesis submitted in partial fulfillment of the requirements of the University of Sunderland for the degree of Doctor of Philosophy

School of Computing and Technology
University of Sunderland
Sunderland
United Kingdom

October 2008

Table of Contents

List of Tables

List of Figures

بسم الله الرحمن الرحيم

اللهم لك الحمد كما ينبغي لجلال وجهك وعظيم سلطانك, والصلاة والسلام على رسول الله الكريم وعلى اله وصحبه ومن سار على دربه الى يوم الدين،

إهداء

الى اعز ما في الكون على قلبي بعد الله و رسوله, ابي و امي ... اطال الله في عمريهما،
الى اختاي و اخواني،
الى زوجتي و ابنائي،
اليكم جميعا اهدي هذا الجهد المتواضع.

خالد عبدالفتاح فرحان

Dedication

This work is dedicated to the most beloved people to me, after god and his messenger, my father and my mother, may god give them long life,
to my sisters and my brothers,
to my wife and my children.

Khalid Farhan.

Acknowledgments

This thesis has only been possible through the help of Allah almighty, my lord and cherisher. All that is right and worthy within this thesis is from Allah, the great the magnificent. If there are any flaws and shortcomings within this then it is only from me for Allah is above from any blemish.

I express my deepest gratitude to my family, especially my father and my mother for their continuous prayers and support. I would also like to thank my sisters, my brothers, my wife and my children for their encouragement.

I would like to sincerely thank Prof. Peter Smith, my director of studies, for his kind support, advice and supervision throughout my PhD study. I would also like to thank Dr. Banie Amin for his help and constructive criticism.

Thanks also go to Al-Zaytoonah university of Jordan for sponsoring my research.

Abstract

In recent years the use of portable and wireless equipment is becoming more widespread, and as in many situations communication infrastructure might not be available, wireless networks such as Mobile Ad Hoc Networks (MANETs) are becoming increasingly important. A mobile ad hoc network is a collection of nodes that exchanges data over wireless paths. The nodes in this network are free to move at any time, therefore the network topology changes in an unpredictable way. Since there is no fixed infrastructure support in mobile ad hoc networks, each node functions as a host and a router. Due to mobility, continuous change in topology, limited bandwidth, and reliance on batteries; designing a reliable and scalable routing protocol for mobile ad hoc networks is a challenging task.

Multicast routing protocols have been developed for routing packets in mobile ad hoc networks. Existing protocols suffer from overheads and scalability. As the number of senders, groups, and mobility speed increases, the routing overhead and the packet collision increases, and therefore the packet delivery ratio decreases. Thus none of the existing proposed multicast routing protocols perform well in every situation.

In this study a novel multicast routing protocol for ad hoc networks is proposed. It is an efficient and scalable routing protocol, and named Network Sender Multicast Routing Protocol (NSMRP). NSMRP is a reactive mesh based multicast routing protocol. A central node called mesh sender (MS) is selected periodically from among the group(s) sender(s) to create one mesh in order to be used in forwarding control and data packets to all multicast group(s) member(s). One invitation message will be periodically flooded to all group(s) member(s) by MS to join the group(s).

The proposed routing protocol is evaluated by simulation and compared with a well known routing protocol. The results are analyzed and conclusions are drawn.

Chapter 1

Introduction

1.1 Motivation for the Research

In many situations a communication infrastructure might not be available, therefore wireless networks such as Mobile Ad Hoc Networks (MANETs) are becoming increasingly important. A Mobile Ad Hoc Network is a group of two or more wireless hosts that has no fixed infrastructure support, and each wireless node can function as a router. In this network hosts can move randomly, therefore the network topology changes in unpredictable way (e.g. emergency disaster, class rooms, conferences and battlefield etc.). In order to allow hosts to communicate with each other, a routing protocol is needed to establish routes between nodes. The routing protocol determines how a data packet is transmitted over multiple hops from a source node to a destination node.

Mobility and lack of infrastructure support in a MANET, makes the design of an effective and scalable multicast routing protocol a challenging task for researchers [Dhillon and Ngo, 2005]. Many efficient multicast routing protocols exist for wired Networks, but these protocols do not take into consideration node movement, frequent topology changes and reliance on batteries. For that reason, adopting existing wired multicast routing protocols to a MANET will not bring efficient multicast routing protocols. Furthermore, multicast routing protocols for MANET have been proposed [Schumacher et al., 2004; Cordeiro et al., 2003].

Out of all available protocols for multicast routing in mobile ad hoc networks, the On Demand Multicast Routing Protocol (ODMRP) outperforms other routing protocols [Dhillon and Ngo, 2005; Puthana and Illendula, 2005; Viswanath et al., 2004; Sobeih et al., 2004; Gui and Mohapatra, 2004; Mohan et al., 2002; Sharma et al., 2002; Lee et al., 2000]. ODMRP routing protocol shows good performance even in dynamic scenarios. Due to the mesh topology this protocol is robust to link failure [Sharma et al., 2002], and transmits almost as much data as flooding because it uses multiple routes for delivering the data packets [Lee et al., 2000].

Unfortunately ODMRP builds per-source meshes, and if the number of senders increases, the number of JOIN REQUEST packets also increases and thus control overhead increases rapidly, and the JOIN REPLY packets sent by the receivers collide more frequently. Scalability and overhead are the major drawbacks of ODMRP, as the network size, the number of groups and the number of multicast source nodes increase. By increasing the load, buffer overflow grows and the delay at each link also increases, and thus packet delivery ratio decreases [Dhillon and Ngo, 2005; Puthana and Illendula, 2005; Gui and Mohapatra, 2004; Viswanath et al., 2004; Cordeiro et al., 2003; Sharma et al., 2002; Mohan et al., 2002; Lee et al., 2000; SINGH, 2000]. Finally with increasing mobility the average miss ratio also increases [Sobeih et al., 2004].

None of the existing multicasting routing protocols is good in all different conditions (e.g. mobility, different number of senders and different number of nodes in each group) [Singh, 2000]. And there are still many issues that deserve more research, and are considered as an open problems [Cordeiro et al., 2003; Peltotalo et al., 2004]. Therefore the design of a new routing protocol is needed in order to satisfy the requirements of mobile ad hoc networks [Staub, 2004].

1.2 Aim and Objectives

This research addresses the routing problem in mobile ad hoc networks (MANETs). The main aim of this research is to design a novel routing protocol for mobile ad hoc networks based on multicast technique. Based on this aim the research objectives of this study are as follows:

1. Investigating existing methods for routing protocols in mobile ad hoc networks.
2. Addressing and determining the major problems and drawbacks of the existing multicast routing protocols in mobile ad hoc networks.
3. Developing a novel multicast routing protocol for mobile ad hoc networks.
4. Implementing the developed multicast routing protocol.
5. Comparing the developed multicast routing protocol with one of the competitive multicast routing protocols in mobile ad hoc networks.

1.3 The Research Hypothesis

In this research a new multicast routing protocol for ad hoc networks is designed, and the main hypothesis of this study is that this proposed routing protocol can show better performance than On Demand Multicast Routing Protocol by reducing the packet overhead and collisions and increasing the packet delivery ratio.

Based on the main hypothesis, the following sub hypotheses will be studied:

- Each source in the existing routing protocols broadcasts its own Join request message and Join reply message, therefore existing routing protocols suffer from overhead and scalability. This research claims that using only one Join request message, one Join reply message, and constructing one multicast mesh for all senders and groups, the packet collision and overhead will be reduced and the packet delivery ratio will be increased.

- Furthermore, this research claims that by electing one of the senders to become the network sender, and by choosing this sender to be the one that is located in the most crowded area, the network load will be balanced and the performance of the proposed routing protocol will be improved and thus the proposed routing protocol will outperform the existing routing protocol.

1.4 The Originality of the Work

The following points describe the original contribution to knowledge that is provided by this study:

1. The main originality of this research is the design of a new multicast routing protocol for ad hoc networks called "Network Sender Multicast Routing Protocol (NSMRP)". This new protocol outperforms the existing

protocol by decreasing the overhead and collision and increasing the packet delivery ratio.

2. The originality also comes from the development of simulation tools for mobile ad hoc networks, which were used for comparing the new protocol with the existing one.
3. Finally the originality also comes from the statistical evidence of the robustness of the proposed protocol.

1.5 The Structure of the Thesis

Under this section, the structure of this thesis is presented as follows:

Chapter 2 Gives an introduction to wireless networks including their major types. Then the types of ad hoc networks and routing protocol design issues are highlighted. And then a survey of classifications of ad hoc network routing protocols is given and discussed in detail.

Chapter 3 Multicast routing in mobile ad hoc networks and the multicast routing design issues are studied, and a categorization of the existing multicast routing protocols is given, then a detailed description of the most important multicast routing protocols is discussed with examples.

Chapter 4 The Network Sender Multicast Routing Protocol (NSMRP) is introduced and described in detail with examples, and the main characteristics of the new protocol are also highlighted.

Chapter 5 The evaluation method and metrics are highlighted, and the proposed multicast routing protocol is evaluated and compared to the on-demand multicast routing protocol, and experimental results are presented and discussed in detail.

Chapter 6 In this chapter a summary of findings is discussed including the main objectives of the study. And a summary of research contributions is given. The experimental results and conclusions are discussed and evaluated and suggestions for further research are presented.

Chapter 2

Wireless Ad Hoc Networks and Routing Protocols

2.1 Introduction

In this chapter, a brief introduction to wireless networks and some general background information is given including the major types of wireless networks according to the network's topologies and the node mobility. Then the three types of ad hoc networks are presented and routing in mobile ad hoc networks is defined. The challenges that face the design of an efficient routing protocol for MANET are discussed. A survey of classifications of ad hoc network routing protocols is presented and discussed in detail by exploring their mechanisms, advantages and disadvantages.

2.2 Wireless Networks

A computer network is a collection of autonomous computers which have the ability to communicate with each other and exchange data in different ways. Similar to fixed wired networks, wireless networks are created by nodes and routers. In a computer network, the routers are in charge of delivering data in the network. The main difference between wired and wireless networks is the way that the network nodes communicate. A fixed wired network relies on cables (e.g. cooper cable and optic fibre) to transfer data. On the other hand the communication between the wireless network nodes can be either wired and wireless or just wireless (e.g. wireless radio waves). In 1970 at University of Hawaii the first computer communication network was developed by connecting seven computers over four islands, and the development of the first wireless network that combines the fields of computing and communication was in the late 1970's and the early 1980's [Murthy and Manoj, 2004]. Wireless networks enable users to use their portable devices on the move. If buildings are separated by rivers or railway tracks, installing a wireless network would be easier, faster and more economical than a wired network [Geier, 2002]. These are some of the advantages of a wireless network.

Wireless networks can be categorized according to the topology size or according to the node mobility.

2.2.1 Wireless networks types according to the topology size

Wireless networks are able to cover areas varying in size from small areas such as class rooms to larger sizes such as countries and continents. Wireless networks can be classified into four different topologies [Nuaymi, 2007; Coleman and Westcott, 2006; Murthy and Manoj, 2004].

2.2.1.1 Wireless Wide Area Network (WWAN)

WWAN usually uses cellular telephone technologies such as General Packet Radio Service (GPRS) which can enable mobile phones to connect a laptop to the Internet and thus allow users to access internet while on the move. WWAN provides low data rate from 56 up to 114 Kbps [Coleman and Westcott, 2006; Murthy and Manoj, 2004].

2.2.1.2 Wireless Metropolitan Area Network (WMAN)

WMAN covers an area such as a city, and for controlling the use of the wireless medium this network uses IEEE 802.16 as the medium access control (MAC) protocol. One of the technologies based on this protocol is Worldwide Interoperability for Microwave Access (WiMAX) which is the competing technology to DSL [Coleman and Westcott, 2006; Murthy and Manoj, 2004].

2.2.1.3 Wireless Personal Area Network (WPAN)

A WPAN covers a small area within 10 metres range and allows computers and other devices such as personal digital assistants (PDA) and telephones to communicate with each other. The MAC protocol used for WPAN is IEEE 802.15 which is the standard for technologies such as Bluetooth and Infrared [Coleman and Westcott, 2006; Murthy and Manoj, 2004].

2.2.1.4 Wireless Local Area Network (WLAN)

WLAN provides network communications to areas varying in size from a small number of computers to a campus. IEEE 802.11 is the MAC protocol for WLAN; Wireless Local Area Network can extend a wired LAN by using access points [Coleman and Westcott, 2006; Murthy and Manoj, 2004].

2.2.2 Wireless network types according to node mobility

Wireless networks can be categorized into three types according to the nodes mobility:

2.2.2.1 Fixed Wireless Networks

Wireless nodes which are placed in fixed locations and instead of relying on batteries to receive electrical power they rely on utility mains. Fixed wireless nodes use wireless channels to communicate with one another. Figure 2.1 illustrates fixed wireless network formed by buildings using transmission towers [Murthy and Manoj, 2004].

2.2.2.2 Wireless Networks with Fixed Access Points

This type of wireless network is formed by wireless nodes and one or more access points (APs) which are attached to a wired network. An access point is a hub comprising a radio card and antenna and it is a half duplex node since one radio card is allowed to transmit packets at any given time [Coleman and Westcott, 2006]. Access points are connected to the wired network by cables and use their antenna for transmitting and receiving the data over the network. Figure 2.2 illustrates a wireless networks with fixed access points formed by wireless devices and wired network.

2.2.2.3 Ad Hoc Networks

Ad hoc networks (MANETs) can be defined as a group of two or more wireless hosts that has no fixed infrastructure support, and each wireless node should be able to function as a router. Ad hoc networks can be categorized into three types:

1) Wireless Sensor Networks

A Wireless Sensor Network (WSN) is formed by more than one sensor placed across a large geographical area which can communicate with each other. Sensors are specialized nodes which are responsible for collecting and making computation on specific types of data, usually about environmental and Health Monitoring, physical conditions or Industrial Control [Lewis, 2004]

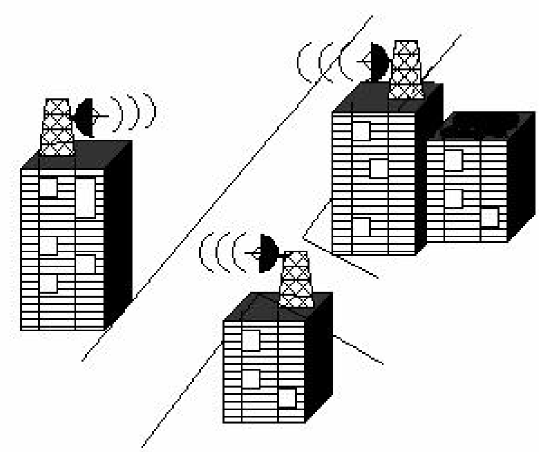


Figure 2.1: Fixed wireless network.

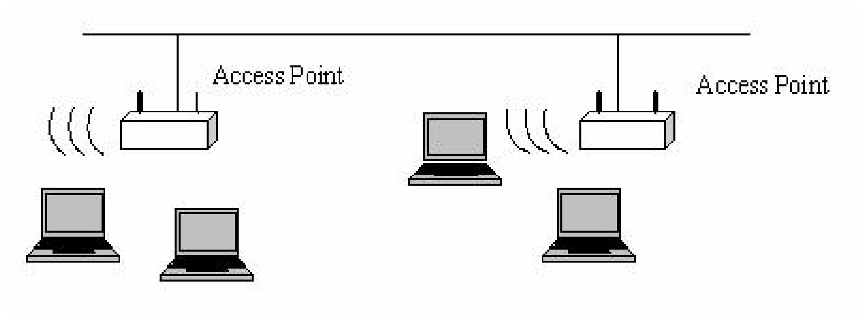


Figure 2.2: Wireless networks with fixed access points.

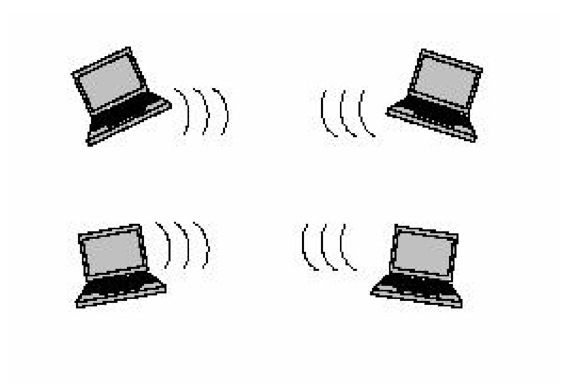


Figure 2.3: Mobile ad hoc network.

2) Mobile Ad Hoc Networks

A Mobile ad hoc network (MANET) is a collection of nodes that exchange data over wireless paths and each node is provided with wireless networking capability. The nodes in this network are free to move at any time, therefore network topology changes in unpredictable ways (e.g. emergency disaster (earth quake, fire, flood), class rooms, conferences and battlefield etc.). Due to the lack of a fixed infrastructure support in MANETs (no routers or system administrator), each node functions as a host and a router. Ad hoc networks are believed to be the next generation of wireless networks [Lai et al., 2002]. An example of mobile ad hoc network is shown in Figure 2.3. The standardizing body for mobile ad hoc networks is the Internet Engineering Task Force (IETF) MANET working group.

3) Hybrid Wireless Networks

A Hybrid wireless network combines the advantages of both mobile ad hoc networks and traditional cellular networks. In this type data can be transmitted from a source node to a destination node using the ad hoc multi-hop technique or the cellular network’s infrastructure [Liu et al., 2003]. Multi-hop cellular network (MCN) is one of the applications of a hybrid wireless network [Murthy and Manoj, 2004].

2.3 Routing in Ad Hoc Networks

In order to allow hosts to communicate with each other, a routing protocol is needed to establish routes between nodes; a routing protocol determines how a data packet is transmitted over multiple hops from a source node to a destination node.

Due to the characteristics of mobile ad hoc networks, the design of an efficient routing protocol for MANET faces many challenges. Some of these challenges are the following [Murthy and Manoj, 2004; Sesay et al., 2004; Schumacher et al., 2004]:

2.3.1 Mobility and Dynamic topology

Mobility is one of the major characteristics of mobile ad hoc networks. By increasing node mobility the topology changes and thus positions of the nodes will change and the number of control packets needed to determine the new positions will increase. Since the nodes in this type of network are free to move at any time, therefore network topology changes in an unpredictable way. This causes path breaks and increases packet collisions [Schumacher et al., 2004; Murthy and Manoj, 2004].

2.3.2 Limited bandwidth

The limited bandwidth of wireless networks is another problem that can limit the capability of routing protocols. By increasing the number of nodes and the traffic they handle in the same transmission range region, the available bandwidth that each node can use will become smaller. Therefore routing protocols should have good mechanisms to use the limited bandwidth optimally by decreasing the number of data and control packets to become as low as possible [Murthy and Manoj, 2004].

2.3.3 Congestion

Frequent link breaks and increasing the control packet overhead in mobile ad hoc networks are the main reasons that make reaching the capacity limit become very fast. To avoid / reduce congestion routing protocols should be able to decrease control packet overhead and have an efficient mechanism to deal with frequent link breaks [Schumacher et al., 2004; Murthy and Manoj, 2004].

2.3.4 Energy constraints

Ad hoc network nodes rely on batteries, routing protocols must minimize their operations by reducing data and control packet overhead and eliminating unnecessary or repeated transmissions and avoiding collisions.

And thus power consumption in ad hoc networks should be managed efficiently [Sesay et al., 2004; Schumacher et al., 2004; Murthy and Manoj, 2004].

2.3.5 Limited transmission range and no fixed infrastructure support

Because of the limited transmission range and the lack of infrastructure support in ad hoc networks routes are typically multi-hop. Therefore nodes in ad hoc networks have to act as senders, receivers, intermediate nodes and routers. Routing protocols should be designed to allow nodes to perform these operations efficiently [Murthy and Manoj, 2004].

2.4 Classification of Ad Hoc Networks Routing Protocols

Mobile ad hoc routing protocols can be categorized into a number of types based on more than one criterion. The most important classes have been chosen to be presented.

2.4.1 Route information and topology based strategies

Mobile ad hoc routing protocols can be classified into three types according to the way the information about the route and topology is gathered. Information can be obtained in advance (proactive) or whenever it is needed (reactive) or hybrid method which makes use of both types.

2.4.1.1 Proactive routing protocols (table driven)

Proactive routing protocols collect information about all nodes within a network and store it in tables. So whenever a route is needed the information is ready to be used. This strategy can be achieved in two different ways:

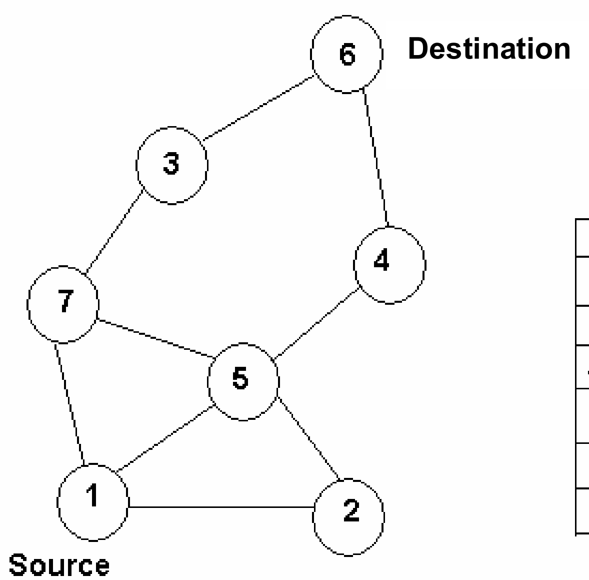
a) Event driven protocols (Distance Vector)

In event driven protocols nodes will exchange information about the topology only if they discover new changes in it. This new information will be sent by each node to all other nodes in the network, when nodes receive the new information they update their own tables. Routing protocols have different strategies for how routing update packets are delivered. DSDV [Perkins and Bhagwat, 1994] and WRP [Murthy and Garcia-Luna-Aceves, 1996] routing protocols are examples of this type.

1) Destination Sequenced Distance Vector Routing protocol (DSDV)

Destination Sequenced Distance Vector Routing protocol (DSDV) is a proactive routing protocol and it is based on Distributed Bellman Ford Distance Vector Routing protocol which suffers from routing loops. DSDV was one of the first algorithms designed to deal with routing in mobile ad hoc networks. In this routing protocol each node creates a table and maintains in it a special record for each node in the network. Each record comprises four fields, the first field has the node number, the second field has the next node on the shortest route to this node, the third field has the distance (number of hops) to this node and the fourth field has the sequence number that is determined by the node. Whenever a node sends a new table it increases the sequence number therefore the higher sequence number is an indication of new information. Upon detecting any changes in the topology or after a predetermined period of time, this table will be exchanged between the near neighbours. Figure 2.4 illustrates route creation in DSDV. In Figure 2.4 (a) node 1 is the source and node 6 is the destination, Figure 2.4 (b) shows the shortest path to node 6 is through node 7 and the distance equals 3 hops. When a node receives a new table it updates the path to destination if either the new sequence number is larger than the old one or if both of them were the same but the number of hobs in the new route was smaller. And thus the sequence number has been proposed to prevent loops. According to this sequence number the table might be transmitted to the neighbours or rejected. [Jain, 1999; Lang, 2003; Mohapatra and Krishnamurthy, 2004; Murthy and Manoj, 2004]

Destination Sequenced Distance Vector routing protocol's advantages are the avoidance of routing loops and the availability of any needed route. But by increasing the number of nodes or increasing the mobility speed in DSDV the control overhead increases and thus ad hoc network's performance degrades due to the limited bandwidth and mobility. Therefore DSDV has a scalability problem.



Des	NxtNod	Dis	SeqN
2	2	1	24
3	7	2	51
4	5	2	77
5	5	1	79
6	7	3	120
7	7	1	158

(a) Network topology (b) Routing table for node 1

Figure 2.4: Route creation in DSDV.

b) Regular updated protocols (Link State)

In regular updated protocols topology information is updated and exchanged regularly and all the time whether there are changes or not in the topology. STAR [Garcia-Luna-Aceves et al., 1999] and OLSR [Clausen and Jacquet, 2003] routing protocols are examples of this type.

1) Optimized Link State Routing (OLSR)

It is a proactive link state routing protocol and the route information in this protocol is updated by exchanging periodic messages between neighbours. The multipoint relay (MPR) concept is used in OLSR; the multipoint relay for a node is a subset of its neighbours. Each node in the network which can be called a selector chooses a group of nodes that consists of a subset of its near neighbours to be its MPR set.

MPR is designed so that the nodes are able to reach all their neighbours and their neighbours' neighbours (two hops away) with a minimum number of forwarding messages. Figure 2.5 illustrates an MPR set for a node where the black circle represents the selector node, the grey circles represent the MPR set and the white circles represent the two hop neighbours. The MPR set members are the only nodes that are allowed to forward the selector's link state messages while the rest of the nodes can only receive these messages.

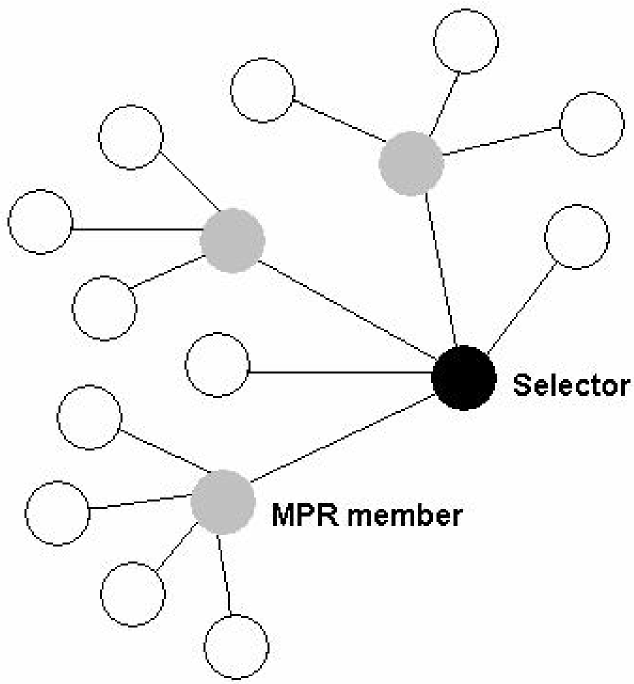


Figure 2.5 MPR set for a selector node.

In order for the route information to be shared between all nodes in the network, every node periodically broadcasts a topology control message (TC). This message comprises the originator address and its MPR set name. And thus any node can be reached by contacting any member of its MPR set. [Staub, 2004; Mohapatra and Krishnamurthy, 2004; Murthy and Manoj, 2004; Haas et al., 2002].

Compared to other proactive routing protocols, OLSR reduces the number of control packets by forwarding the messages only to a subset of the node's neighbours, and thus the overhead will be reduced. A performance comparison in [Christensen and Hansen, 2001] showed that OLSR and AODV routing protocols perform the same in many cases but OLSR outperforms AODV in high density networks and in static topology and in the other hand AODV outperforms OLSR in high mobility situations, and in most cases the overhead for AODV was higher than that of OLSR.

In proactive routing protocols the information about the routes to any destination is already known, since route information is searched for continuously, and at all times therefore the routes to all destinations are ready to use. And thus proactive routing protocols have no route discovery delay and this is one of its advantages. But the price will be increasing overhead which affects bandwidth and throughput especially when the size of the network increases, and also there will be more packet collisions. Battery power and bandwidth will be wasted by collecting information that it might never be used.

2.4.1.2 Reactive routing protocols (on demand)

In reactive routing protocols route information will not be collected and maintained in advance and nodes do not exchange route information periodically. Instead the state information is acquired only when there is a need for it (on demand). When a sender node has data to send it usually starts a route discovery procedure which completes by finding a route from source to destination. This procedure usually starts by broadcasting a message to the sender's near neighbours, and as the sender node receives the reply messages from the receivers the route from the source node to the destination can be established. Once a route is obtained and constructed, it will be maintained by a special process until the route is no longer needed or the route becomes not valid any more due to node movements.

But since the route information must be obtained before sending the data, a path discovery delay occurs whenever a new path is needed. The advantage of this type is the reducing of the control overhead by not collecting information about unused routes, and also lower bandwidth is used and the battery power will also be saved. DSR [Broch et al., 2003] and AODV [Perkins and Royer, 1999] routing protocols are examples of reactive routing protocols.

a) Source Routing Method

In the Source Routing Method, the source determines the route for each packet. All intermediate addresses that the packet needs will be encapsulated into the packet header. An example of the source routing method is the DSR routing protocol [Broch et al., 2003].

1) Dynamic Source Routing Protocol (DSR)

In the DSR routing protocol [Broch et al., 2003], the complete route from source node to destination node must be stored in each packet. This protocol is mainly based on two phases; route discovery phase and route maintenance phase.

When a route to a destination is not available, the source node broadcasts a Route Request Packet to its neighbours and the neighbours also broadcast it to their neighbours until the message reaches the destination as shown in Figure 2.6 (a). The destination node replies to the source node with a Route Reply Packet which comprises the addresses from source to the destination as shown in Figure 2.6 (b). The source stores this route information in its cache to be able to use it before it is expired due to node movement.

If an intermediate node has in its cache the route address to the destination it will not forward the route request, instead it replies to the source with the full address and update its cache.

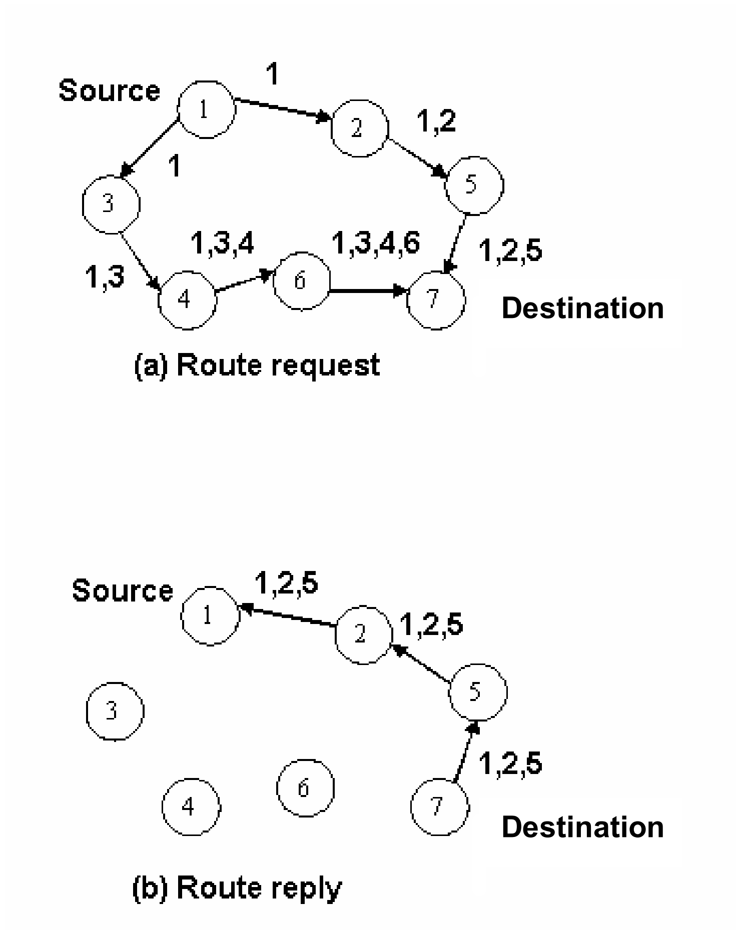


Figure 2.6 Route discovery phase in DSR Routing protocol.

In the route maintenance phase, if a node detects any changes in the topology for example by realizing that the neighbour node is not forwarding its packets, in this case the node reports a broken link to the source node by sending Route Error Packet. Upon receiving the link failure information, the source node deletes any route that contains this broken link [Johnson et al., 2007; Mohapatra and Krishnamurthy, 2004; Murthy and Manoj, 2004; Zhou, 2003; Jain, 1999].

DSR is a reactive routing protocol therefore route information is collected only when needed, and thus the overhead of proactive routing protocols caused by updating the route information periodically is eliminated in DSR. The disadvantage of DSR is that the broken links are not repaired locally and the use of stale routes that are stored in the cache wastes the limited bandwidth in ad hoc networks, and has a bad effect on route reconstruction. There is no effective mechanism in DSR to solve the stale routes problem. Since route information is not already known there will be a delay before collecting the route information to establish the route. By increasing mobility the performance of DSR degrades and by increasing the network size the control packets also increase and thus overhead increases. Hence DSR has a major scalability problem because of the nature of source routing.

DSR was compared in [Lee et al., 1999] to ABR and DBF, Both protocols DSR and ABR have better performance than DBF. In [Lee et al., 2003] DSR was compared to LAR, WRP, FSR and DREAM routing protocols and the results show that DSR has less overhead than other protocols since no beacon messages are exchanged. However the disadvantage is that the broken link is discovered only after the packets are unable to use the broken route and this increases the delay.

b) Non Source Routing Method

Unlike the source routing method the addresses from source to destination are not encapsulated into the packet header, instead any intermediate node which is part of the route, stores in its cache the previous node address and the next node address. An example of non source routing method is AODV routing protocol [Perkins and Royer, 1999].

1) Ad Hoc On Demand Distance Vector Routing Protocol (AODV)

Ad hoc on demand distance vector routing protocol [Perkins and Royer, 1999], is a reactive routing protocol, therefore routes are built on demand. Whenever a source node has a data packet to send, and the destination address is not available, a Route Request Packet will be broadcast across the network. Any intermediate node which receives the Route Request Packet, stores the Reverse Route to the sender, and forwards the packet. The stored address will be used in forwarding the reply later. The Route Request Packet comprises the destination sequence number, the time to live, the destination identifier, the source sequence number, the broadcast identifier and the source identifier. The destination sequence number determines the freshness of the information about the Reverse Route to the sender and it is also used to prevent stale route information and routing loops. The Route Request Packet will be initially sent using a small time to live value, and if the destination has not been found the packet will be resent with a higher value. This reduces the overhead caused by broadcasting the packet across the network.

Upon receiving the Route Request Packet, the receiver sends a Route Reply Packet to the sender using the Reverse Route addresses which are stored in the intermediate node's caches. As the source receives the Route Reply Packet the route becomes available and the data can be sent. If the Route Request Packet was received by an intermediate node which has a valid route to the destination, a Route Reply Packet will be sent to the sender. If an intermediate node detects a broken link, the source node and the destination node will be informed. After receiving the broken link notification, the source node reconstructs the route to the destination.

Compared to other routing protocols, the control packet overhead is reduced in AODV, by constructing the routes on demand and using the time to live value. The routing loops are prevented by using the destination sequence number which also determines the newest route to the destination.

As mentioned above AODV was compared to OLSR in [Christensen and Hansen, 2001], where the performance of both protocols was the same in many cases but OLSR outperforms AODV in high density networks and in a static topology. On the other hand AODV outperforms OLSR in high mobility situations, and in most cases the overhead for AODV was higher than that of OLSR.

In [Boppana and Konduru, 2001], ADV, AODV, DSDV and DSR routing protocols have been compared with one another. The results show that ADV outperforms AODV and DSR in high mobility situations, AODV suffers from the packet overhead because of the route request packets and in DSR the route reply packets and the route error packets wastes the network's limited bandwidth.

2.4.1.3 Hybrid routing protocols

In proactive protocols the route information is ready to use and the route can be constructed any time, but this wastes the network resources and increases the overhead, since route information is updated all the time. Reactive routing protocols may decrease the overhead and the used bandwidth, but this type suffers from the delay caused by broadcasting the route request across the network. Both of these routing types may not perform well in high mobility situations and frequent topology changes as it is in mobile ad hoc networks. Hybrid routing protocols are another type of routing protocol that combines the advantages of both types: proactive and reactive. An example of this type is the Zone Routing Protocol (ZRP) [Haas et al., 2002].

a) Zone Routing Protocol (ZRP)

The Zone routing protocol (ZRP) [Haas et al., 2002], is a hybrid routing protocol. This protocol benefits from both reactive and proactive routing. The proactive method is used in the local area, whereas the reactive method is used in the global area. In the zone routing protocol every node has a local zone which is determined to be the nodes within a limited distance in hops, and all nodes that are located beyond this local zone will be considered as within a global zone. Every node periodically maintains and exchanges route information only with its local zone nodes. Figure 2.7 shows a routing zone for a source node, the radius for the local zone equals 2, and the circle in the figure separates the local zone from the global zone. Nodes within the zone and closest to the zone radius are called peripheral nodes (border nodes). In the figure nodes 1,2 and 3 are peripheral nodes.

When a source node has a data packet to send to a destination as shown in figure 2.7, the node searches for the destination within its local zone. If the destination is a member of its local zone, then the data will be sent directly to it. Otherwise a reactive method will be used by broadcasting a route request message to the peripheral nodes. As the route request message is received, each of the peripheral nodes checks whether the destination node is within its own local zone.

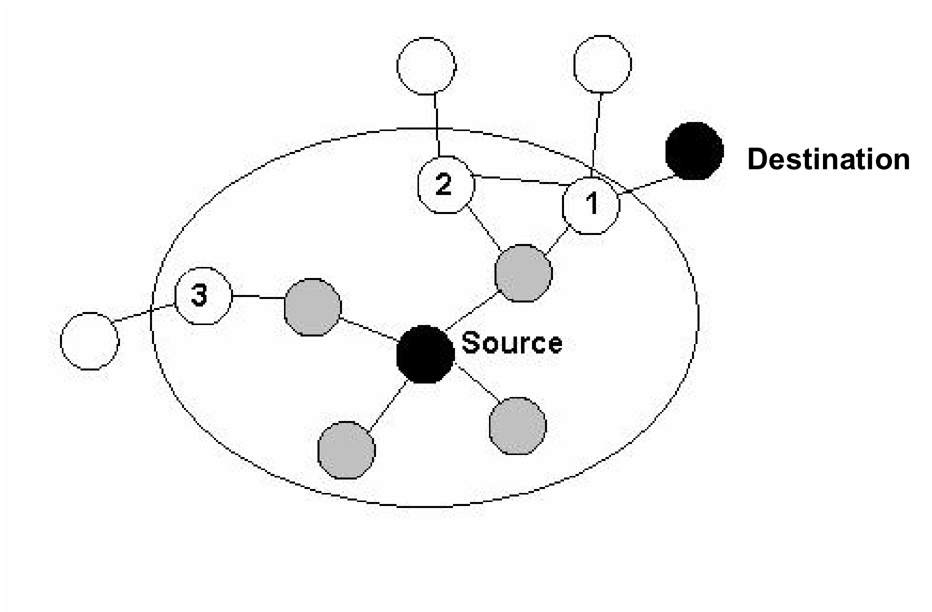


Figure 2.7 Routing zone for a source node in ZRP Routing protocol.

If the destination node is found, a route reply message will be sent back to the sender, otherwise the peripheral nodes will send route request messages to their own peripheral nodes, and this process will be repeated until the destination is found.

In figure 2.7 the source node checks whether the destination is within its own local zone, and since it is not a member of its zone, the source sends a route request message to the peripheral nodes (1, 2 and 3), node number 1 found the destination within its own local zone, therefore the destination sends a route reply message the sender indicating the path.

Any node that forwards the route request message appends its own address to it; these addresses will be used while sending the route reply message back to the sender. If the source node receives more than one route reply message each one with a different path, the route with the shortest path will be chosen. If an intermediate node in the path between the source node and the destination node discovers a broken link, a local repair will be performed by finding an alternate link, and then informs the source node by sending a link update message to it.

Unlike proactive routing protocols, the zone routing protocol reduces the control overhead by not broadcasting route information across the network, instead the broadcasting will be only to the local zone. And the bandwidth will be saved in ZRP comparing to reactive routing protocols since the route request message will be sent only to the border nodes.

A link local repair in ZRP may result in a sub optimal route between the source and the destination, and since each node has its own local zone, the network will have a large number of zones, and thus the control overhead will be increased because of the large overlapping of local zones [Hong et al., 2002; Murthy and Manoj, 2004].

2.4.2 Hierarchical routing strategies

In this type of routing protocols, nodes will be assigned to different levels and nodes at each level are partitioned into groups which are controlled by centre nodes. The goal of hierarchical type of routing protocols is to reduce the control overhead by exchanging the route information with minimum number of nodes and reducing the size of the routing table. An example of this type is Hierarchical State Routing Protocol (HSR) [Iwata et al., 1999].

2.4.2.1 Hierarchical State Routing Protocol (HSR)

Hierarchical State Routing Protocol [Iwata et al., 1999], is a multilevel hierarchical protocol that uses clustering at more than one level. At the first level (the physical level) nodes are divided into clusters, and each cluster has a cluster head. The cluster head chooses its nearest neighbours to be its cluster members and each node can be a member of more than one cluster. At the next higher level all clusters' heads are grouped into clusters and each cluster selects one of its members to become a cluster head, and the same processes will be performed by the higher levels. A virtual link is used to keep cluster heads at the higher levels connected. The virtual links formed by intermediate nodes are called gateway nodes.

In the HSR routing protocol, route information will be exchanged periodically between the cluster head and the members of its cluster, and this information will be provided to the cluster heads at the higher levels. When a node has data to send to a destination the local cluster will be searched, and if the destination is not a member of the local cluster the cluster head forwards the route request to the next higher level and the same process will be repeated until the destination is reached. The sender passes a data packet up to the cluster head of the higher level which in turn sends the packet to the destination cluster head using the virtual links, then the packet will be sent to the destination on the lowest level.

The HSR routing protocol was compared in [Iwata et al., 1999] with FSR (hierarchical routing protocol), DSDV (table driven routing protocol) and on demand routing protocol, when HSR compared with FSR, the results show that the size of route information packet was reduced in HSR by using a hierarchical method, but it was difficult to find the destination. On the other hand FSR reduces the control overhead by reducing the route updating frequencies and because of the size of the route information packet, FSR suffers from scalabilities. Both protocols, HSR and FSR, show better scalability than the table driven routing protocol DSDV. But when compared with the on demand protocol, HSR and FSR have high packet loss since as the link breaks due to mobility, the packets must be dropped. In the on demand protocol the packets will be buffered until the route is reconstructed. Exchanging route information about multilevel and the cluster heads election process increases the control packet overhead in HSR [Murthy and Manoj, 2004].

2.4.3 Position (Location) based routing

In the previous types of routing protocols the nodes broadcast messages across the network to obtain an idea about the network topology. In this type of routing protocols the Global Positioning System (GPS) is assumed to be available and each node is aware of its location. The exchanging of messages is used between neighbours only to collect information about their positions. An example of this type is Location Aided Routing protocol (LAR) [Ko and Vaidya, 2000].

2.4.3.1 Location-Aided Routing (LAR) Protocol

Location-aided routing (LAR) Protocol [Ko and Vaidya, 2000], is an on demand routing protocol that uses the source routing technique. This protocol depends on GPS to obtain location information in order to minimize the flooded area of route information packets. The protocol uses two schemes to find a path to a destination, in the first scheme the source is assumed to be aware of some information about the destination, such as its location and speed. And according to this information the source determines a circular area around the destination, and the smallest rectangle that contains the source node and the circle area will be defined. The rectangular area is called a Request Zone, and only the nodes which are located in this area are allowed to forward the source's route request message.

In the second scheme, the source node calculates the distance to the receiver according to the location information. Both the distance and the destination's position will be stored in the route request message, which will be sent by the source to its nearest neighbours. Upon receiving the route request message the node calculates its distance to the receiver, and the route request message will be forwarded only if the calculated distance is less than or equal to the distance stored in the message. If the node decides to forward the route request message, the distance value in the message will be replaced by its own distance value.

In both schemes, upon receiving the route request message, the destination replies back to the sender with a route Reply Message that contains its position. On the other hand, if the route to a destination is not available after a predetermined period of time, the protocol uses pure flooding by broadcasting a route request message across the network.

As a proactive routing protocol, LAR saves the limited bandwidth in ad hoc networks by not forwarding route request messages when no route is needed. LAR was compared with GeoCast, DREAM and GPSR routing protocols in [Hong et al., 2002], and in [Lee et al., 2003] it was compared against WRP, FSR, DSR and DREAM. The results show that since the location information is used in LAR, and the propagating of the route request messages are limited to a small area, therefore the overhead was reduced. But in LAR and DREAM the location information is obtained by flooding messages throughout the network and thus by increasing the network size the control overhead will increase.

As mentioned above, in this type of routing protocols all nodes are assumed to know their positions because of the availability of GPS or some other sources of localization technique. And thus this type of protocols cannot be used where these types of devices are not available [Murthy and Manoj, 2004; Lee et al., 2003].

2.4.4 Routing by Flooding

Flooding is the simplest method which can be used to deliver packets from a source node to a destination node in the network. In flooding if the source has data to send, it simply broadcasts the packet to its neighbours and the neighbours in turn rebroadcast the data packet to their neighbours, finally the data reaches the destination. In flooding the intermediate nodes forward the packet only if it is received for the first time, otherwise the packet will be discarded. In this technique the same data packet can be received from more than one neighbour, and every node in the network must receive the data packet at least once. An intermediate node is allowed to forward the data packet only one time, therefore the forwarding of the same packet can be terminated and the loops will be avoided [Mohapatra and Krishnamurthy, 2004].

The flooding method does not require any information about the network topology, therefore no need for broadcasting route request packets or route reply packets and thus route setup overhead and route maintenance overhead is very low in flooding. Pure flooding was compared in [Viswanath et al., 2004] to ODMRP and MAODV and the results show that the data forwarding overhead in flooding was the highest in all different scenarios, and this is because by increasing the number of nodes the number of forwarded packets increases therefore the overhead and collisions increases. Hence flooding has a scalability problem. The bandwidth is wasted in flooding since whenever a data packet is sent by the source node, every node in the network must receive and forward this packet.

Because of the many drawbacks of flooding two different efficient flooding methods were proposed in [Viswanath and Obraczka, 2002] Scoped Flooding and Hyper Flooding.

2.4.4.1 Scoped Flooding

The Scoped Flooding method [Viswanath and Obraczka, 2002], was developed for low mobility scenarios such as conferences, and with the aim of reducing the number of rebroadcast messages in order to avoid collisions and reduce overhead. In this method every node periodically sends a hello message to its neighbours, and this message includes the originator node's neighbours. Nodes use these messages to update the neighbour lists which are stored in their cache list by adding the received list to their own list. If a node receives a data packet, a comparison will be made between the neighbour list of the sender and its own neighbour list. If its own list is a subset of the sender's set the packet will not be retransmitted.

2.4.4.2 Hyper Flooding

The Hyper Flooding technique [Viswanath and Obraczka, 2002], is designed for high mobility situations in order to increase reliability. In this method neighbours also exchange hello messages. As a node receives a hello message, the identity of the originator will be added to its own neighbour list. In Hyper Flooding a node rebroadcasts the data packet in three different cases. In the first case the data packet will be rebroadcast as soon as it is received, and in the second case if the data packet was received from a node that is not a member of the neighbours list and in the third case if a hello message is received from a new neighbour. In the last two cases the node rebroadcasts all packets in its cache, and this is because the nodes may have missed the first broadcasting due to mobility.

A simulation study was carried out in [Viswanath et al., 2004] to test the performance of the two techniques. The results show that scoped flooding can reduce the forwarding overhead by 20% compared to pure flooding. But its disadvantage is that the overhead increases as the network size increases, and thus scoped flooding is not a scalable method. In the hyper flooding technique the results show that the data packets were guaranteed to be delivered under high mobility scenarios, but this is accomplished at very high overhead even when compared to pure flooding.

2.5 Conclusion

In this chapter the challenges that face routing protocols in mobile ad hoc networks including node mobility, dynamic topology changes, congestion, energy constraints, the lack of a fixed infrastructure support and the limited bandwidth are discussed. A survey of classifications of ad hoc networks routing protocols, including event driven proactive protocols, regular update proactive protocols, source routing reactive protocols, non source routing reactive protocols, hybrid routing protocols, hierarchical protocols, position based protocols, and routing by flooding (scoped flooding and hyper flooding) are given and discussed in detail by exploring their mechanisms, advantages and disadvantages.

In proactive protocols, the route information is collected all the time and thus as the number of nodes or mobility increases the control overhead increases and therefore the networks performance degrades. In source routing reactive protocols the broken link is discovered only after the packets are unable to use the broken route and this increases delay. And in non source routing, reactive protocols suffer from overhead due to the route request packets. In hybrid routing protocols, since each node has its own local zone, the network will have a large number of zones, and thus the control overhead will be increased because of the large overlapping of local zones. In hierarchical routing protocols the packet loss is high since as the link breaks due to mobility the packets must be dropped and also exchanging route information about multilevel and the cluster heads election process increases the control packet overhead. In position based protocols nodes are assumed to know their positions because of the availability of GPS or some other source of localization technique. And therefore this type of protocol cannot be used where these types of devices are not available.

In general, the source node in unicast routing protocols sends a separate copy of the message for each destination node and as the number of nodes increases the control packet overhead increases accordingly, therefore unicast methods are not suitable for ad hoc networks.

Chapter 3

Multicast Routing in MANET Networks

3.1 Introduction

Compared to wired networks, multicast routing in mobile ad hoc networks faces many challenges. These challenges make the design of a reliable routing protocol a difficult task. Delivering the packets by using multicast rather than multiple unicast saves the limited bandwidth in mobile ad hoc networks. In this chapter, multicast routing in mobile ad hoc networks is studied, and the major issues that are needed to be considered while designing routing protocols for mobile ad hoc networks are highlighted, and a categorization of the existing multicast routing protocols is presented. Then a detailed description of the most important multicast routing protocols is given with examples.

3.2 Multicasting

Data communication can be achieved by unicast, broadcast, anycast or multicast. Unicast is one-to-one communication, and a separate copy of the same message will be delivered from a source node to each destination. Broadcast is one-to-all nodes in the network and Anycast is one-to-selected members of a group. Multicasting is the transmission of data from one node to n receivers, and only one copy of the message will be delivered to all receivers, hence communication cost will be reduced and the limited bandwidth in ad hoc networks will be saved. Because of the characteristics of MANET, multicast is the most suitable communication mechanism for ad hoc network applications [Dhillon and Ngo, 2005; Sesay et al., 2004; Cordeiro et al., 2003; Sharma et al., 2002].

There are several issues that should be considered while designing routing protocols for mobile ad hoc networks

3.2.1 Robustness

In mobile ad hoc networks links break because of node movement, therefore data and control packets may be dropped and this can cause packet delivery ratio to decrease. Therefore the routing protocol should be robust to mobility [Murthy and Manoj, 2004].

3.2.2 Efficiency

The bandwidth is limited in mobile ad hoc networks, therefore the efficiency is an important issue for ad hoc routing protocols. Efficiency in multicast is defined as the number of control packets and data packets transmitted per data packet delivered [Murthy and Manoj, 2004].

3.2.3 Control overhead

In order to create a mesh or tree to allow group members to communicate with one another the control packets are needed. And by increasing the number of control packets the control overhead increases and the limited bandwidth will be wasted. Therefore the routing protocol should keep the number of control packets to a minimum [Murthy and Manoj, 2004].

3.2.4 Depending on unicast protocol

Some of the routing protocols require the support of a specific routing protocol. In this case it is difficult for the protocol to work in heterogeneous situations. And thus it is very important that the protocol is independent of a unicast protocol [Murthy and Manoj, 2004].

3.2.5 Resource management

Some of the characteristics of mobile ad hoc networks are the limited bandwidth, relying on batteries and limited memory. And thus the power consumption should be reduced by reducing the number of transmissions and minimum routing information should be used to save the node's memory [Murthy and Manoj, 2004].

3.3 Classification of multicast Routing Methods

Multicast routing protocols can be classified according to the route construction, and also can be further classified according to the way the information about the route and topology is collected.

3.3.1 Classification according to the route construction

Multicast routing protocols can be classified into four categories according to the route construction: tree based, mesh based, hybrid, and stateless routing protocols. ODMRP and CAMP are examples of mesh and MAODV and AMRIS are examples of tree. AMRoute is an example of hybrid and DDM is an example of a stateless routing protocol [Mohapatra and Krishnamurthy, 2004; Murthy and Manoj, 2004; Cordeiro et al., 2004; Viswanath et al., 2004; Peltotalo et al., 2004; PalChaudhuri, 2004; Staub, 2004; Zhou, 2003; Mohan et al., 2002].

3.3.1.1 Tree based strategies

Tree based multicasting is used in wired multicast protocols. In this type of multicast routing protocol the sender and the receiver are connected with only one path. The major disadvantage of tree based multicast routing protocols is that their performance is not robust in highly mobile situations. Tree based multicast routing protocols can be categorized into two classes, source tree based routing protocols and shared tree based routing protocols.

a) Source tree based multicast routing protocols

In source tree based multicast routing protocols each source constructs its own tree to be able to communicate with its multicast group members. An example of this type is Bandwidth Efficient Multicast Routing Protocol [Murthy and Manoj, 2004].

1) Bandwidth Efficient Multicast Routing Protocol (BEMRP)

In bandwidth efficient multicast routing protocol the multicast tree is established by the receivers. If a receiver decides to join a multicast group, a Join Control Packet will be broadcast across the network. Upon receiving the Join Control Packet, the existing receivers send reply packets. The new node will receive many reply packets, therefore one of them will be chosen and a Reserve Packet will be sent to it.

When a link break occurs, bandwidth efficient multicast routing protocol uses one of two schemes to reconfigure the tree. The first scheme is called Broadcast Multicast Scheme, and in this scheme the node that is closer to the sender is responsible for fixing the broken link by finding a new route which is usually achieved by flooding and connecting the downstream node. The second scheme is called Local Rejoin Scheme, and in this scheme the downstream node repairs the broken link by flooding a limited number of Join Packets which are controlled by a Time To Live value (TTL). The value of TTL depends on the network topology.

With regard to route optimization in BEMRP, when some of the tree nodes come close to each other due to mobility, an intermediate node might become unwanted; in this case the node can be pruned by sending Quit Message to it.

A bandwidth efficient multicast routing protocol saves bandwidth and reduces the number of control packets by constructing the tree using the nearest forwarding node instead of the shortest path. On the other hand using longer paths increases delay and reduces packet delivery ratio.

Source tree based multicast routing protocols construct a tree for each source, and by increasing the number of sources the number of trees increases and this causes packet collision and increases packet loss. And thus this type of protocol has a scalability problem.

b) Shared tree based multicast routing protocols

In shared tree based multicast routing protocols one tree is constructed to be used by all sources that belong to the same multicast group. The shared tree will be used to establish group communication between the sources and their multicast group's members. Forwarding the packets will be only performed by the tree members, therefore the bandwidth will be saved. An example of this type is Multicast Ad Hoc On Demand Distance Vector routing protocol (MAODV) [Perkins and Royer, 2000; Royer and Perkins, 1999].

1) Multicast Ad Hoc On Demand Distance Vector routing protocol (MAODV)

Multicast Ad Hoc On Demand Distance Vector routing protocol is an extension of AODV routing protocol. MAODV uses a multicast tree to deliver packets to multicast group receivers. Constructing a multicast tree starts when a node decides to join a group. If the route to the Group Leader is known, a route request packet (RREQ) will be unicast to it, otherwise a route request packet will be sent across the network as shown in Figure 3.1. This message will be resent a number of times and if no answer was received within a predetermined period of time, the sender node assumes that no more multicast group members exist, and in this case it will become the Group Leader. The Group Leader usually is the first node that joins the group and each group has its own sequence number which is assigned to one by the new Group Leader; then it will be incremented with every new hello packet that is broadcast. The group sequence number determines the freshness of the route.

Each member of the multicast tree keeps in its cache a multicast route table, which includes the multicast group address, the multicast Group Leader address, the group sequence number, the hop count to the next member and the hop count to the Group Leader. If a node has data packets to send and the route information is not available, also a route request packet will be sent across the network. Upon receiving the route request packet, an intermediate node stores the address of the upstream node and forwards the packet. When a member of the multicast group receives the route request packet, and the sequence number that is stored in its cache is high enough, a route reply packet (RREP) will be sent back to the sender. The route reply packet includes the number of hops between the sender and the replying node, the sequence number of the multicast group and the multicast Group Leader address.

If the Group Leader receives more than one route reply packet, one of them will be accepted and the all other will be ignored. This is to guarantee a loop free property. The accepted packet will be the one with the highest sequence number and that has the shortest hop count to the multicast group members. If an intermediate node leaves its group, it will continue to route the group's packets. But if a leaf node decides to leave its group, then a Leave Message will be sent to its immediate multicast group member. Upon receiving the message, the neighbour updates its tables.

If a link breaks because of node mobility, the downstream node will take the responsibility of repairing the link. The repairing will be performed by broadcasting a route request packet to a small area determined by a small TTL value, and if no reply was received after a predetermined period of time, a route request packet will be broadcast across the network.

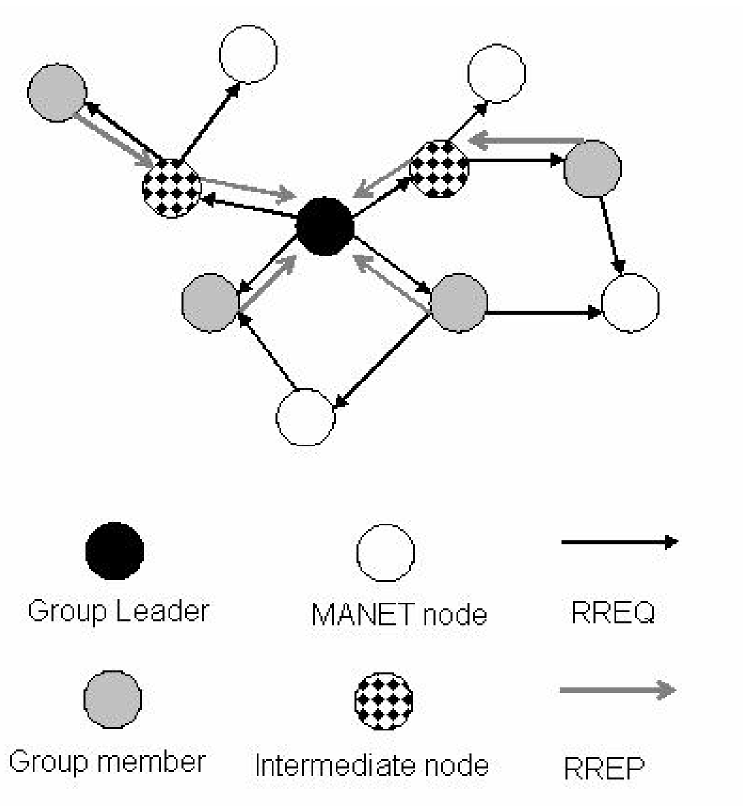


Figure 3.1: Tree construction in the MAODV routing protocol.

Compared to source tree based multicast routing protocols, MAODV reduces the overhead and saves the limited bandwidth in ad hoc networks, by using one tree for all the group's senders, and MAODV is also a loop free protocol. On the other hand by increasing the number of senders the load on the shared links becomes heavier, and thus packet congestion increases and packet loss also increases. Any break in the shared link will effect all multicast sessions. And also having one leader for the shared tree is a single point of failure.

Multicast Ad Hoc On Demand Distance Vector routing protocol was compared in [Mohan et al., 2002] to ODMRP, and the results show that the performance of both protocols degrades when the number of senders increases above 20. This is due to the increasing of the load on the shared tree in MAODV when the number of senders increases. By increasing mobility, the links of the shared tree break more frequently, therefore the performance of MAODV is affected. On the other hand, when the group size was increased MAODV outperforms ODMRP.

3.3.1.2 Mesh based strategies

In mesh based multicast routing protocols, a multicast mesh will be created to allow multicast group members to communicate with each other. Mobility is one of the major characteristics of ad hoc networks, and network's links break because of node mobility. Mesh based protocols provide multiple routes between a source node and destination node, and thus when a link breaks packets can use a different route [Dhillon and Ngo, 2005]. On Demand Multicast Routing Protocol (ODMRP) [Lee et al., 2002], is an example of a mesh based multicast routing protocol.

a) On Demand Multicast Routing Protocol (ODMRP)

On Demand Multicast Routing Protocol is a mesh based multicast routing protocol. A mesh is created in order to deliver control and data packets from a source node to a destination node. Just like on demand unicast protocols, this protocol has two phases, the route request phase and the route reply phase.

Creating the mesh is performed by the source. If a source has data to send and no route information is available, it broadcasts a group invitation message periodically across the network. This message is called a JOIN REQUEST packet as shown in Figure 3.2. Upon receiving a non duplicate JOIN REQUEST packet, the intermediate node stores the upstream node address, which is considered as backward learning, and forwards the packet. If the JOIN REQUEST packet is received by a multicast group receiver, the member table that is stored in its cache will be updated with the source information and a message called a JOIN REPLY packet will be sent to the neighbours. If a node receives the JOIN REPLY packet, the packet's entries will be checked, and if the "next node ID" entry matches its own ID, the node realizes that it is one of the forwarding group and it is on the path to the source.

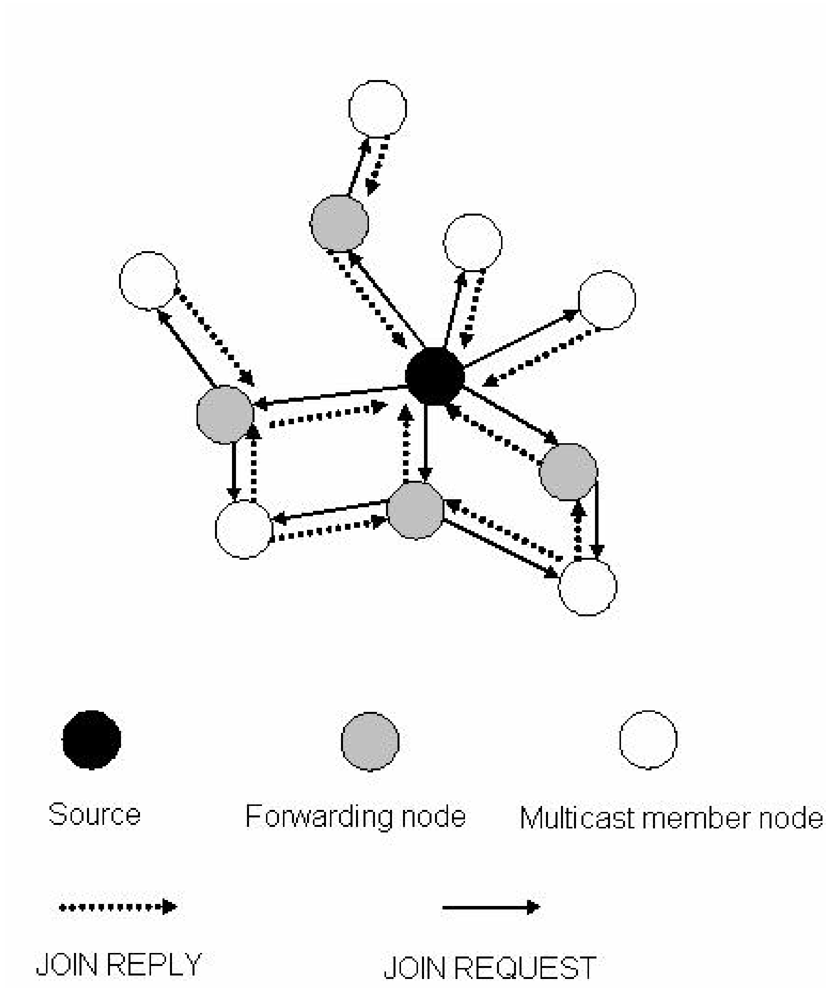


Figure 3.2: Mesh creation in the ODMRP routing protocol.

Therefore the FG_Flag will be set and the JOIN REPLY packet will be broadcast. Each forwarding node repeats the same procedure until the JOIN REPLY packet reaches the source node. When the source receives the JOIN REPLY packet, the mesh will be created.

On Demand Multicast Routing Protocol uses sequence numbers to prevent packet duplication and looping. Each packet that is broadcast by the sender is assigned a new sequence number, and if a node receives a packet with an old sequence number value, the packet will be ignored. When a node receives a JOIN REPLY packet and non of the entries matches its own ID, the packet also will be ignored.

In On Demand Multicast Routing Protocol the multicast group membership is renewed after every predetermined period of time by broadcasting the JOIN REQUEST and JOIN REPLY packets. If a node decides to leave a group no additional messages are needed. If the node is the source node, it stops sending JOIN REQUEST and JOIN REPLY packets, and if it was a receiver, the node only ignores the JOIN REQUEST and JOIN REPLY packets. This is called the soft state method of joining and leaving the group, and this approach saves the limited bandwidth and reduces the overhead in mobile ad hoc networks.

One of the advantages of On Demand Multicast Routing Protocol is its unicast capability in routing. ODMRP can work as multicast and unicast routing protocol. Other multicast protocols must operate on top of a unicast protocols.

ODMRP was compared in [Viswanath et al., 2004] to Multicast Ad Hoc On Demand Distance Vector routing protocol, and the results show that mesh based protocols such as ODMRP outperforms tree based protocols such as

MAODV. And the performance of MAODV was not as good as the other protocols in terms of reliability and packet delivery ratio. But on the other hand the routing overhead for MAODV was the lowest. In [Mohan et al., 2002], the packet delivery ratio decreases for ODMRP when the group size increases. In [Kunz and Cheng, 2002] ODMRP was compared to AODV and the results show that ODMRO is robust to mobility because of the redundant routes that the mesh provides, and ODMRP outperforms AODV in terms of packet delivery ratio. On the other hand AODV scales better than ODMRP.

In [Lee et al., 2002], ODMRP was compared to AMROUTE, CAMP, AMRIS and FLOODING, and the results show that due to the mesh topology ODMRP has a good performance in dynamic situations, as the mobility speed increases ODMRP performance improves. ODMRP outperforms all other protocols in terms of packet delivery ratio under different scenarios such as increasing the number of senders, increasing the group size and increasing the speed.

b) Mesh Based method versus Tree based method

Existing studies show that the mesh protocols performed significantly better than the other categories in mobile ad hoc networks [Dhillon and Ngo, 2005; Puthana and Arun Illendula, 2005; Peltotalo et al., 2004; Cordeiro et al., 2003; Hongbo Zhou, 2003; Lee et al., 2002; Mohan et al.,2002; Sharma et al., 2002; Lee et al., 2000; Garcia-Luna-Aceves and Madruga, 1999; Lee et al., 1999]. In trees, when links are not available due to node movements, the packets must be buffered or dropped until the tree is reconstructed, and this causes the packet delivery ratio to decrease. On the other hand, redundant routes in the mesh provide alternate routes for data delivery in case of link breaks due to mobility and even if the major routes were not available the packet can still be delivered to the destination . Data packets can take different routes to the destination while the primary route is being repaired. Mesh based protocol may consume more bandwidth than tree based protocols, however mesh is more flexible to network dynamics. It is trade off between efficiency and reliability.

3.3.1.3 Hybrid based strategies

In the hybrid approach, protocols combine tree and mesh approaches to enhance the performance of ad hoc routing protocols. This approach has performance degradation with a high degree of mobility, and encounters problems like congestion and buffer overflow [Sesay et al., 2004; Cordeiro et al., 2003; Lee et al., 2000]. Ad Hoc Multicast Routing Protocol (AMRoute) [Bommaiah et al., 1999] is an example of hybrid based multicast routing protocols.

a) Ad Hoc Multicast Routing Protocol (AMRoute)

In Ad Hoc Multicast Routing Protocol, a multicast tree is constructed over the underling multicast mesh. This protocol has two major phases, the first phase is the mesh creation phase and the second is the virtual user multicast tree construction phase. In AMRoute one of the group members is elected to become a logical core node which is responsible for finding new multicast members and creating the mesh and the tree.

1) Mesh creation phase

When a node decides to become a member of a group, it declares itself as the logical core for the group. Every core periodically broadcasts a Join Request message to discover other group members. The message comprises the source ID, the group ID, the message ID and the Time To Live (TTL). When a core receives this message from another core, a Join Reply message will be sent, and the two cores form a new mesh. Each one of the cores marks the other as a mesh neighbour and a bidirectional tunnel will be established between them. The Join Reply messages comprise the source ID, the group ID, the message ID and the Time To Live (TTL). Due to multicast mesh emerges, a mesh might have more than one core, and in this case one of them will be chosen to become the core for the multicast mesh.

If a node decides to leave its own group, a message called JOIN_ACK will be sent to its near neighbour nodes.

2) Tree creation phase

When a mesh is created, the logical core periodically broadcasts TREE_CREATE packets across the mesh. Upon receiving this packet, a multicast group member forwards it to other mesh members and selects this

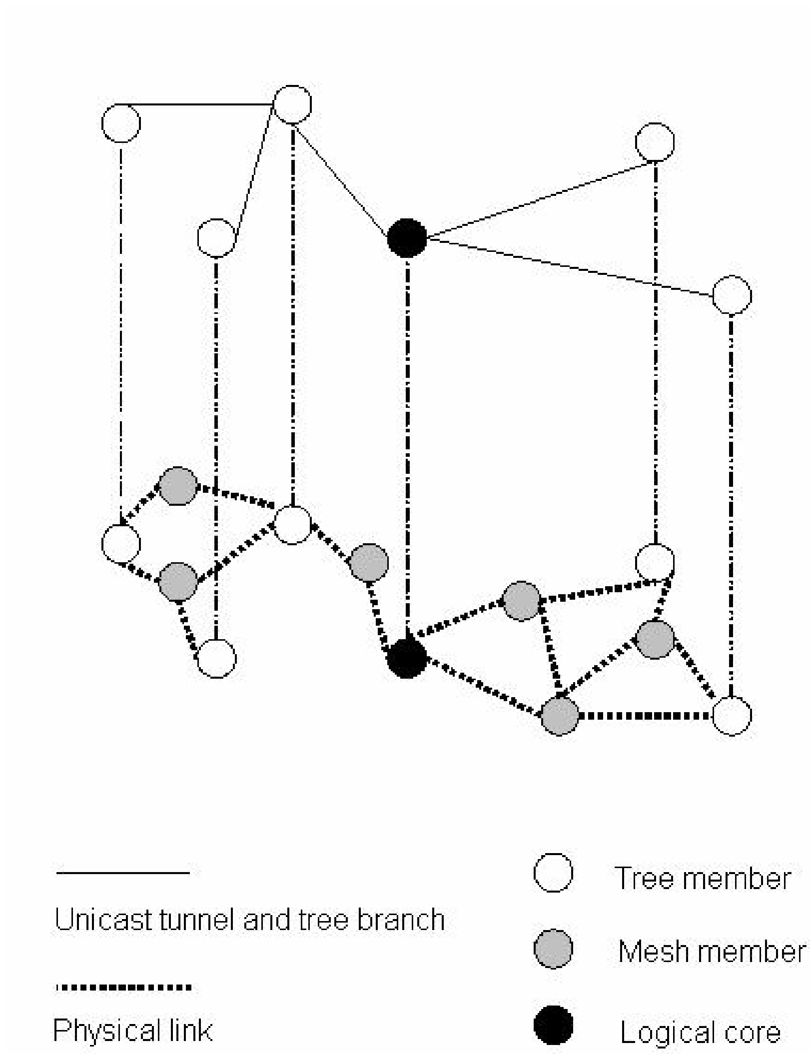


Figure 3.3: Hybrid topology in AMRoute.

link to be the tree link. If duplicate packets are received, the node replies with a TREE_CREATE_NAK message. When a node receives a TREE_CREATE_NAK message, the link will be marked as a mesh link. Figure 3.3 shows the hybrid topology in AMRoute.

In Ad Hoc Multicast Routing Protocol the tree links are virtual links and they are created using the multicast mesh. In this protocol, nodes which are not members of the multicast tree are not supposed to forward data packets. Data packets are forwarded using the unicast tunnel, and AMRoute routing protocol can work with any unicast protocol.

If the mesh splits due to mobility and node movement, some segments might end up without a virtual core. In this case nodes wait for a predetermined period of time and if no TREE_CREATE packet is received, one of the nodes becomes a virtual core. And if the segments rejoin, one of the cores will be elected to become the virtual core for the multicast group.

The disadvantage of the AMRoute routing protocol is that temporary loops, and with mobility, the protocol constructs non optimal trees [Cordeiro et al., 2003; Lee et al., 2000], By increasing speed, the number of hops of the unicast tunnel becomes larger, therefore the throughput decreases. The core in this protocol is a single point of failure; if a core fails the packet loss and delay will increase [Murthy and Manoj, 2004].

AMRoute was compared in [Lee et al., 2002] to ODMRP, CAMP, Flooding and AMRIS. The results show that AMRoute has a good packet delivery ratio in static situations, and on the other hand by increasing the mobility speed the protocol's performance degrades. This is because of the formation of loops and the creation of sub optimal trees. The performance of AMRoute was good when the network load was low, and by increasing the load the performance drops very quickly. This is caused because of the buffer overflow at the tree and mesh members.

3.3.1.4 Stateless based strategies

In the stateless approach, protocols do not create a mesh or tree to establish group communication, instead all intermediate nodes addresses from source node to destination node are contained in the packet header, and no routing information is stored at any intermediate node except for the sender node. The Stateless approach focuses on small groups and it has performance degradation with a high degree of mobility; it also relies on an underlying unicast protocol [Mohapatra and Krishnamurthy, 2004; Cordeiro et al., 2003]. Differential Destination Multicast Routing Protocol (DDM) [Ji and Corson, 2001] is an example of a stateless routing protocol.

a) Differential Destination Multicast Routing Protocol (DDM)

Differential Destination Multicast Routing Protocol introduces a different way of multicast routing in mobile ad hoc networks. If a node decides to join a multicast group, a Join Request packet will be unicast to the source node. When receiving a Join Request packet, the source node checks the validity of the packet and stores the destination address in a table called Member List (ML) in its memory, and sends an Acknowledgment control packet to the destination. All multicast group members periodically send Join Request packets to the source node; the source uses these packets to update the Member List. If a destination does not send a Join Request packet within a predetermined period of time, the source node removes its entry from the Member List. If a member node decides to leave the group, an explicit LEAVE packet must be sent to the source.

DDM can deliver data packets to a destination using two different modes, stateless mode and soft state mode. In stateless mode if a source has data to send, the destination address will be inserted into the data packet's header field which is called DDM block and unicast to the next hop. This transmission is performed by using the underlying unicast protocol. When the packet is received by the next node, its next node address will be taken from the DDM block field. Then the packet will be forwarded until the destination node is reached. In soft state mode, every node along the forwarding route stores the address of the destination node and the address of the next hop in its forwarding set (FS). And thus in future transmissions there is no need to store the entire destination addresses in the data packet's header since they are available in the intermediate nodes' memories. If any changes happen to the route, the upstream node informs the downstream node about the new addresses needed to reach the destination.

In Differential Destination Multicast Routing Protocol the multicast route information is not maintained, therefore node's memory will be saved. On the other hand the major disadvantage of DDM is that when the number of nodes increases the number of the addresses needed to be stored in the packet's header also increases, and thus the limited bandwidth will be wasted. In DDM all receivers must periodically send JOIN REQUEST messages to the source node and by increasing the number of group members the number of control messages increases therefore the overhead increases. Hence DDM has a scalability problem [Murthy and Manoj, 2004; Mohapatra and Krishnamurthy, 2004; Cordeiro et al., 2003].

3.3.2 Topology and route information classes

Multicast routing protocols can be classified into two categories according to the way the information about the route and topology is collected, Multicast proactive (table driven) protocols and Multicast reactive (on-demand) protocols, an example of Multicast proactive is CAMP [Garcia-Luna-Aceves and Madruga, 1999],and an example of Multicast reactive is AMRIS [Wu and Tay, 1999].

3.3.2.1 Multicast table driven strategies

Proactive protocols maintain tables that store routing information. The advantage is that at all times the routes to all destinations are ready to use, but the price will be increasing overhead, affecting bandwidth and throughput especially when the size of network increases, and also there will be more packet collisions. An example of multicast Table driven routing protocols is The Core-Assisted Mesh Protocol (CAMP).

a) The Core Assisted Mesh Protocol (CAMP)

In the Core Assisted Mesh Protocol, a shared mesh is constructed and maintained in order to allow group members to communicate with each other. CAMP keeps the shortest routes from the receiver's nodes to the source's nodes in the multicast mesh. Each node keeps a multicast routing table (MRT) stored in its memory and nodes store in this table the membership and routing information. And in order to reduce the control overhead, this protocol uses cores to limit the number of control packets needed for the nodes to join their multicast group.

Nodes in CAMP are categorized into three types, simplex, duplex and nonmember. A Simplex node is allowed to send packets from a specific node to the group members, but it does not forward packets from the group members. On the other hand the duplex node can forward packets from group members, whereas the nonmember node is not allowed to be a member of the multicast mesh. If a receiver node decides to join a group and one of its neighbours is a group member, a JOIN REQUEST message will be sent to it. Otherwise the receiver node broadcasts a JOIN REQUEST message to one of the group cores or tries to reach any member by an expanding ring search. If the JOIN REQUEST message is received by a duplex node, a JOIN ACK message will be sent back to the originator of the JOIN REQUEST.

Each receiver periodically checks its cache to verify whether it is receiving data packets from its neighbours that are on the shortest route to the core. If no packets are received, the node sends a HEARTBEAT message to the source along the shortest route and if none of the neighbours is a mesh member, a PUSH JOIN message will be sent. This process forces the successor to join the mesh and to ensure that the shortest route is part of the mesh.

Core Assisted Mesh Protocol avoids flooding the control packets, therefore the packet delivery ratio increases while the control overhead is kept very low. CAMP relies on a unicast routing protocol and thus by increasing the mobility the control overhead increases, and the core node in CAMP is a single point of failure and this is another disadvantage.

CAMP was compared in [Lee et al., 2002] to ODMRP, AMRoute, Flooding and AMRIS. The results show that since CAMP uses a mesh topology its performance was better than a tree based protocol, and on the other hand the mesh based protocol ODMRP outperforms CAMP, because the paths to a receiver node have fewer redundant routes than those near the mesh centre and therefore in CAMP many packets forwarded to the destinations were not delivered. By increasing mobility the performance of CAMP degrades, because CAMP relies on the WRP unicast routing protocol, and WRP requires a period of time to construct a new route when a link breaks. Thus by increasing mobility the overhead of CAMP also increases. When the number of sources was increased CAMP achieves a better performance and this is because by increasing the number of senders the redundant routes in the mesh also increases and therefore the packet delivery ratio improves.

3.3.2.2 Multicast on demand strategies

In reactive protocols the state information is acquired only when there is a need for it. This will reduce control overhead by not collecting information about unused routes, and also lower bandwidth is used. But this strategy causes a path discovery delay when a path to a destination is needed. An example of multicast on demand routing protocols is the Ad hoc Multicast Routing Protocol Utilizing Increasing Id numbers (AMRIS).

a) Ad hoc Multicast Routing Protocol Utilizing Increasing Id numbers (AMRIS)

Ad hoc Multicast Routing Protocol Utilizing Increasing Id-numbers is on demand routing protocol, in which a shared tree is created to support multicast group sources and multicast group receivers. Each group member in the multicast session is assigned an id called the multicast session number identifier (MSM ID).

To construct a multicast tree one of the multicast group sources broadcasts a control packet across the network, this packet is called the New Session message. The source that is elected to create the session is called Sid and its MSM ID is the smallest, and the multicast group nodes' MSM ID's are incremented with their distance from the multicast group source. The MSM ID message includes the source ID, the multicast session ID and membership status. When a node receives the New Session message, the information derived from the message will be stored in a table called the neighbour status table, and then the node calculates its own MSM ID which is larger than the one stored in the message, and it replaces the MSM ID that is stored in the message with its own MSM ID and rebroadcasts it.

To join a session, a node checks its own New Session message and determines an upstream node with the smallest MSM ID, and then a Join Request message will be unicast to it. If the upstream node is a group member, it will reply with a Join Ack message. Otherwise the upstream node forwards the Join Request message to its own upstream nodes in order to join the multicast group and create the tree.

In Ad hoc Multicast Routing Protocol Utilizing Increasing Id-numbers, every node must broadcast beacons to its near neighbours. The beacon message includes the node ID, the MSM ID, the membership status, the upstream nod ID, the upstream nod MSM ID, the downstream node ID, and the downstream node MSM ID. The beacon message is used to maintain link availability. If a link breaks, the downstream node is responsible for reconstructing the broken link.

The major advantage in AMRIS is that the loop formation is eliminated by using the MSM ID, and also link breaks are reconstructed locally therefore the overhead is reduced. The major disadvantages of AMRIS are the wastage of the limited bandwidth which is caused by using the beacons, and also packet loss increases due to beacons colliding.

Only tree members are allowed to forward the data packets, and link breaks are detected by beacon messages, and therefore when a link breaks the data packets must be dropped or buffered until the multicast tree is reconstructed, and thus end to end delay increases and packet loss also increases. The upstream node is selected based on MSM ID and this increases the average hop length between the multicast receiver and the sender and thus increases the delay and packet loss.

AMRIS was compared in [Lee et al., 2002] to ODMRP, AMRoute, Flooding and CAMP. Compared to other protocols AMRIS has lower packet delivery ratio due to the use of tree configuration. The tree provides only one path between source and receiver and if a link breaks due to node mobility, packet congestion and collision. In AMRIS neighbours exchange beacons every second and if no beacons are received within three seconds, the node realizes that the neighbour has moved away. So if a link breaks it takes at least three seconds before the link is reconstructed and during this time a number of packets can be lost. The results show that even in a static situation the protocol's packet delivery ratio was 60%, although the other protocols' packet delivery ratio was nearer to one, and this is also due to the beacon messages.

On the other hand the performance of AMRIS was not affected when the number of senders and number of group members were increased and this is because the protocol uses shared tree and by increasing the number of sources more nodes can use the same tree and more nodes can be used to deliver the packets to the group members.

3.3.3 Session initialization categories

Starting a group session can be initiated either by the source node or by the group receivers. When the session is initiated by the source of the group it is called a source initiated approach and if it is initiated by the multicast receivers then it belongs to the receiver initiated type. ODMRP, DCMP and ABAM multicast routing protocols are examples of the source initiated approach, and DDM, WBM, and BEMRP multicast routing protocols are examples of the receiver initiated approach.

3.3.4 Topology maintenance categories

Maintaining the multicast group topology can be achieved by two different ways, either by the soft state mechanism or by the hard state mechanism. In the soft state mechanism no specific action has to be taken whenever a link breaks, instead the protocol periodically broadcasts control messages in order to keep all group members connected. This flooding of the control packets increases the control overhead but the packet delivery ratio improves. On the other hand in the hard state mechanism the protocol executes a specific procedure whenever a link breaks. This type of protocol reduces the number of control packets and thus the control overhead decreases, but the packet delivery ratio degrades. MZRP, DCMP and NSMP multicast routing protocols are examples of the soft state mechanism, and

ABAM, WBM and PLBM multicast routing protocols are examples of the hard state mechanism.

3.3.5 Location based category

When a global positioning system (GPS) is available, multicast routing protocols can use position and mobility information in order to improve their performance. An example of this type is Location Guided Tree Construction Algorithms for Small Group Multicast (LGT) [Chen and Nahrstedt, 2002].

3.3.5.1 Location Guided Tree Construction Algorithms for Small Group Multicast (LGT)

Location Guided Tree Construction Algorithms for Small Group Multicast is an overlay multicast routing protocol and it is designed for small groups, and in this protocol the multicast data packets are encapsulated into a unicast packet and delivered to the destination among the multicast group members. This protocol uses the position information of the multicast group members to create the multicast tree without any information about the network topology. Two types of trees are created in this protocol, Location Guided K Array (LGK) and Location Guided Steiner (LGS). In the Location Guided K Array, the sender chooses the nearest K destinations to become

Multicast routing Protocols	Flooding of Control Packets	Initialization method	Multicast group Topology	Maintenance method	Free of Looping	Independent of unicast Routing Protocol	Periodic Message
BEMRP	Yes	Receiver initiated	Source tree	Hard state	Yes	Yes	No
MZRP	Yes	Source initiated	Source tree	Hard state	Yes	Yes	Yes
PLBM	No	Receiver initiated	Source tree	Hard state	Yes	Yes	Yes
AMRIS	Yes	Source initiated	Shared tree	Hard state	Yes	Yes	Yes
ODMRP	Yes	Source initiated	Mesh	Soft state	Yes	Yes	Yes
FGMP	Yes	Receiver initiated	Mesh	Soft state	Yes	Yes	Yes
NSMP	Yes	Source initiated	Mesh	Soft state	Yes	Yes	Yes
DDM	Yes	Receiver initiated	Source tree	Soft state	Yes	No	Yes
ABAM	Yes	Source initiated	Source tree	Hard state	Yes	Yes	No
MCEDAR	Yes	(Source or Receiver) initiated	Hybrid	Hard state	Yes	No	No
MAODV	Yes	Receiver initiated	Shared tree	Hard state	Yes	Yes	Yes
WBM	Yes	Receiver initiated	Source tree	Hard state	Yes	Yes	No
AMRoute	Yes	(Source or Receiver) initiated	Hybrid	Hard state	No	No	Yes
DCMP	Yes	Source initiated	Mesh	Soft state	Yes	Yes	Yes
CAMP	No	(Source or Receiver) initiated	Mesh	Hard state	Yes	No	No

Table 3.1 Comparison of multicast routing protocols.

children nodes, and the rest of the group members will be grouped to the K destinations. The sender sends the encapsulated packet to its K children with the sub tree as destination. This process will be repeated until the nodes receive a packet that has an empty destination. On the other hand in Location Guided Steiner, the multicast tree is created according to the geometric destines as an indication of closeness.

3.4 Conclusion

Multicast routing in mobile ad hoc networks is discussed in this chapter, and the multicast routing protocol design issues are explored, including the robustness, the efficiency, the control overhead, the dependency on unicast protocol, and resource management. A categorization of the existing methods of multicast routing in mobile ad hoc networks is given, including the tree based strategies (source tree based strategies and shared tree based strategies), the mesh based strategies, the hybrid strategies, the stateless based strategies, the table driven strategies, the on demand strategies, the session initialization strategies, the topology maintenance strategies, and the location based strategies. Then a detailed description of the most important multicast routing protocols is given with examples.

In the stateless routing method all intermediate node's addresses are stored into the packet's header and by increasing the number of groups or the network size the performance of the network degrades. This type of routing protocol is designed for small networks. In hybrid methods, routing protocols combine tree and mesh strategies. In this type of routing protocol as mobility increases a non optimal tree will be created and loops will be formed and therefore the network's performance degrades.

Existing studies show that the mesh based routing protocols outperform the tree based routing in mobile situations, in tree based protocols, if a link breaks the packets must be dropped or buffered until the link is recreated and on the other hand in mesh based routing protocols if a link breaks the packet can take a different route to the destination as the broken route being recreated and this is because of the redundant routes that the mesh provides.

In Proactive strategies, the state information is collected all the time therefore routing protocols create tables in order to store the route information. The disadvantage is that as the network size increases the size of tables also increases and this increases the overhead and affects the bandwidth. In reactive strategies, routing protocols collect the route information only when it is needed. In this strategy no state information is collected about unused routes therefore the control overhead will be reduced, and also lower bandwidth is used. Thus the reactive strategies are more suitable to ad hoc networks than proactive strategies.

Table 3.1 summarizes key characteristics and properties of multicast routing protocols. ODMRP requires periodic messaging join-request only when sources have data to send, and on the other hand, in routing protocols such as AMRIS, each node maintains a neighbour status table by periodically transmitting control packets, and thus the limited bandwidth will be wasted. In ODMRP a mesh will be constructed rather than a tree, and the mesh topology provides redundant routes and when a link breaks due to mobility, the packets can take different route to destination while the primary route is being repaired. In tree based routing protocols such as BEMRP, MAODV, ABAM, DDM, and MZRP when a link breaks the packets must be buffered or dropped until the tree is reconstructed and therefore the packet lose and the delay will be increased. In order to reduce the control overhead, ODMRP uses soft-state as a maintenance method, the join request packets and the join reply packets are used in constructing and maintaining the mesh therefore the control overhead will be reduced. On the other hand the hard-state method is used in routing protocols such as BEMRP, MZRP, PLBM, AMRIS, ABAM, MAODV, AMROUTE, and CAMP, and in this method a special procedure must be invoked whenever the mesh or tree is needed to be maintained and thus the control overhead will be increased. Finally ODMRP is a loop-free routing protocol; therefore packets are prevented from sending the same packet more than one time. On the other hand the loops in AMROUTE waste the limited bandwidth and increase the control overhead.

ODMRP routing protocol is a well known multicast routing protocol and it is a reactive and mesh based routing protocol. Existing studies show that ODMRP outperforms all other routing protocols. And on the other hand ODMRP builds per source meshes and by increasing the number of groups or sources the overhead and packet collisions increase, and therefore the packet delivery ratio will be decreased and the limited bandwidth will be wasted. This protocol suffers from overhead, collision and scalability, therefore new multicast routing protocol is needed.

Chapter 4

The Network Sender Multicast Routing Protocol

4.1 Introduction

Existing multicast routing protocols have many drawbacks and none of them is good in all different situations. Existing routing protocols suffer from overhead, packet collisions, and scalability therefore a new protocol is needed. As mentioned in chapter 2, delivering the packets by using multicast rather than multiple unicast saves the limited bandwidth in mobile ad hoc networks therefore the new proposal is based on the multicast method of delivering the packets. As presented in chapter 3, existing studies show that the mesh based routing protocols outperform the tree based routing in mobile situations and the reactive strategies are more suitable to ad hoc networks than proactive strategies, therefore the new routing protocol is a reactive and mesh based routing protocol. The new routing protocol will overcome the existing drawbacks such as the packet overhead, the packet collisions, and the scalability by creating one multicast mesh for all group (s) members rather than building per source meshes. And also each source in the previous studies uses its own join request message and join reply message, and on the other hand, in the new routing protocol one join request message and one join reply message will be broadcast for all groups. Finely one sender is chosen to become the only sender of the mesh in the new routing protocol.

In this chapter the Network Sender Multicast Routing Protocol (NSMRP) is introduced, a full description of the protocol is given including multicast route construction and maintenance. The formats of the Join Request Packet, the Join Reply Packet and the New Source Packet are described in detail. Examples of how the Join reply is handled and the creation of the multicast group mesh and the multicast route maintenance are given. Some of the main characteristics of the new protocol are also highlighted.

4.2 Overview of the Network Sender Multicast Routing Protocol

Nodes in mobile ad hoc networks (MANET) collaborate with one another through group communication. This type of network may have one or more groups, and each group may have one or more senders. The Network Sender Multicast Routing Protocol is designed for mobile ad hoc networks and using the multicast method in order to forward control and data packets. The new protocol is based on a mesh scheme rather than a typical multicast tree based routing protocol. In the new protocol all group (s) sender (s) will send their multicast data packets to one chosen sender which is called: Mesh Sender (MS), and in turn this MS will take the responsibility of delivering the messages to all group members in the network.

4.3 Multicast Route Construction

The new routing protocol is a mesh based protocol. Redundant routes in the mesh provide alternate routes for data delivery in the case of link breaks due to mobility. Data packets can get to their destination using a different route, while the old route is being repaired. A mesh based protocol is more flexible to network dynamics.

When a source has a multicast data packet to send, it verifies the existence of MS, by checking an MS-flag in its own memory. If the flag is set to false this means that MS dose not exist and this source has to become an MS.

4.3.1 Case 1: If there is no Mesh Sender

The first thing a new MS has to do is to send a message to the nearest neighbours set in order to find the value of K where (K = number_of_neighbours + number_of_neighbour's_ neighbours). When K is known, MS starts constructing the mesh by periodically broadcasting a join request message (JOIN RQ) to the entire network to invite nodes to become members of the group (s). A JOIN RQ message comprises the following fields (Type, K, Hop Count, MS Address, Sequence Number, First Upstream Node Address, Second Upstream Node Address, Group1 Address, Group2 Address, … , Group n Address) as shown in Figure 4.1. When a node receives a fresh JOIN RQ it sets its MS-flag to true, initializes the message's timer to 0, and stores the message in its own memory. The node then makes a new copy of the message by reassigning the following values (second upstream node address = first upstream node address; first upstream node address = its own address), and rebroadcasts it to its neighbours.

During a period of time if the node overhears a message with its own address assigned to the second upstream node address (which means new nodes in the network need to be invited to become members of the group (s)), it waits until a reply message (JOIN RP) is received, otherwise a JOIN RP message will be sent to its upstream node since no more near neighbours are rebroadcasting a JOIN RQ message. A JOIN RP message comprises the following fields (Type, MS Address, Sequence Number, Downstream Address, Group1 Address, Group2 Address, … , Group n Address) as shown in Figure 4.2. If any node receives a non duplicate JOIN RP message, it will update its memory with the new copy of this message and reply to its upstream node. Eventually, the JOIN RP message will reach the MS and the mesh will be built.

Multicast receivers update a JOIN RP message by adding their own group (s) address (s) before the message is resent, and this is done if their group (s) address (s) has/have not been added by other receivers, this is also done by the intermediate nodes when they overhear a JOIN RP message from neighbours that comprise new group address.

In receiving the JOIN RP message (from the downstream node or by overhearing the neighbours), the upstream node stores in its memory the group (s) addresses in the JOIN RP message, in order to forward multicast data packets destined to multicast group (s) in the future. JOIN RP message will be dropped and the link will be eliminated if the group address field was empty.

32 bits

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Type	K	CPU Speed	Hop Count
MS Address			
Sequence Number			
First Upstream Node Address			
Second Upstream Node Address			
Group1 Address			
Group2 Address			
:			
:			
:			
Group n Address			

Figure 4.1: Join Request Packet (JOIN RQ) Format.

32 bits

<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="8">Type</td><td colspan="24">Reserved</td></tr>
<tr><td colspan="32">MS Address</td></tr>
<tr><td colspan="32">Sequence Number</td></tr>
<tr><td colspan="32">Downstream Address</td></tr>
<tr><td colspan="32">Group1 Address</td></tr>
<tr><td colspan="32">Group2 Address</td></tr>
<tr><td colspan="32">:</td></tr>
<tr><td colspan="32">:</td></tr>
<tr><td colspan="32">:</td></tr>
<tr><td colspan="32">Group n Address</td></tr>
</table>

Figure 4.2: Join Reply Packet (JOIN RP) Format.

The following are the descriptions of Join Query packet fields and Join Reply packet fields:

- **Type:** This field identifies the packet as a Join Query packet or a Join Reply packet.
- **K:** A number that is calculated by each source (K = number_of_neighbours + number_of_neighbour's_ neighbours).

- **Hop Count:** The number of links that this packet has traveled so far.
- **MS Address:** The IP address of the MS node.
- **The Sequence Number:** It is a unique number for each packet that is assigned by the MS.
- **First Upstream Node Address:** The IP address of the upstream node which is the first node on the path to the MS.
- **Second Upstream Node Address:** The IP address of the upstream node of my upstream node which is the second node on the path to the MS.
- **Downstream Address:** The IP address of the downstream node which is the first node on the path to the destination.
- **Group (1 - N) Addresses:** The IP address of the multicast groups (1 - N).

An example of a join reply is illustrated in Figure 4.3, the black circle is the MS node and the white circles are the intermediate nodes and the grey nodes are the group members. When G1-R1 (i.e. receiver 1 belongs to group one) sends a JOIN RP message to node A the message will have node A in the next field and group 1 in the group name field as shown in Table 4.1, and when G2-R1 (i.e. receiver 1 belongs to group two) sends a JOIN RP message to node A the message will have node A in the next field and group 2 in the group name field as shown in Table 4.2. The JOIN RP message from G3-R1 will be received by node A and MS, and the reply message will have node MS in the next field and group 3 in the group name field as shown in Table 4.3. When node A forwards the JOIN RP message, the group name field will have group 1 and group two only, group three will not be included since the JOIN RP message from G3-R1 has MS in the next field as shown in Table 4.4

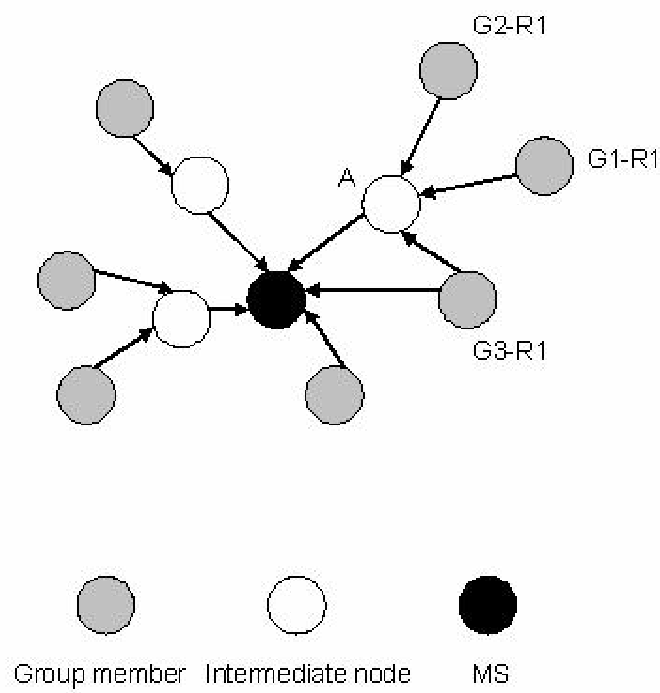


Figure 4.3: Join reply example.

Table 4.1 Join packet of node G1-R1

Next node	Group ID
A	Group 1

Table 4.2 Join packet of node G2-R1

Next node	Group ID
A	Group 2

Table 4.3 Join packet of node G3-R1

Next node	Group ID
MS	Group 3

Table 4.4 Join packet of node A

Next node	Group ID
MS	Group 1
MS	Group 2

Node A receives three JOIN RP messages but it will forward only one JOIN RP message since all information is included in the same JOIN RP message. And by using this method the new protocol will not be affected when the number of groups or receivers increases, since only one control message will be used by all groups and receivers. And thus the control overhead will be decreased and the new protocol will be scalable.

4.3.2 Case 2: If there is a Mesh Sender

In this case, the source finds the value of K and sends a "new source" message (N-SOURCE) to MS through the upstream path. A N-SOURCE message comprises the following fields (Type, K, MS Address, New Source Address, Group Address) as shown in Figure 4.4. If the new source belongs to a group that already exists, it starts sending the messages to MS, otherwise the new source must wait until a JOIN RQ message that comprises its group address is received, and then it will start sending the messages to MS. Upon receiving multicast data packets, MS will start forwarding the data immediately to group receivers through multicast mesh.

32 bits

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Type	K	CPU Speed	Reserved
MS Address			
New Source Address			
Group Address			

Figure 4.4: New Source Packet (N-SOURCE) Format.

4.4 Multicast Route Maintenance

Mobility is one of the major characteristics in ad hoc networks, and due to mobility network links break. In the new protocol no additional control packets are needed to be sent in order to reconstruct the broken links in the network, and this is called “soft state”. To repair the broken links the new protocol depends on two methods. The first one uses the redundant routes that the mesh topology provides, therefore if a link breaks the packets can use a different path to destination as shown in Figure 4.5.

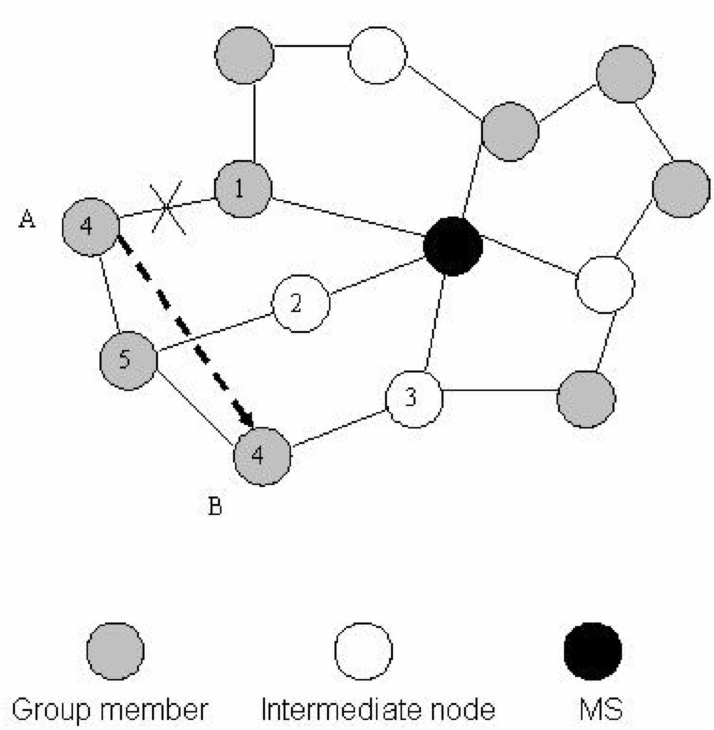


Figure 4.5: Multicast route maintenance in NSMRP routing protocol.

Because of node movement node 4 moves from A to B and therefore the link MS - 1 - 4 breaks. But the data packets can still be received by node 4 through MS - 2 - 5 - 4 and this increases the packet delivery ratio for the new protocol.

The second method the new protocol uses to reconstruct the broken links is by the periodic JOIN RQ messages that the MS sends to create and maintain the mesh. And as shown in Figure 4.5 after receiving the new JOIN RQ message node 4 will has two different routes, the first is MS - 2 - 5 - 4 and the second one is MS - 3 - 4 and in this case node 4 will chose MS - 3 - 4 since it is the shortest path.

Choosing the shortest path makes the distances that the packet needs to travel to reach the destination become shorter, and therefore packet latency will be reduced and the limited bandwidth in mobile ad hoc networks will not be wasted and also the battery power will be saved. Thus the protocols efficiency will be enhanced.

4.5 Data Forwarding

When a mesh is constructed and ready to be used, the MS starts sending data packets as they are received from group (s) sender (s). MS first sends data packets to its near neighbours, and whenever a neighbour node receives a non duplicate data packet, it checks the message's group address, and if this node belongs to this group, a copy of the message will be stored in its memory. The node then checks the JOIN RP messages in its memory to find out which of its neighbours this message should be sent to. The message will be sent to group members and intermediate nodes that will forward the message to group receivers.

This action will be repeated until the message reaches all group members in the network.

4.6 Mesh Sender re-election

MS transmits multicast data packets to group (s) member (s) through the multicast mesh, by using intermediate nodes and receivers. If the position of MS was not in the centre of the network, multicast data packets and control packets must travel long distances in order to reach group (s) member (s).

The new protocol has a new mechanism that allows replacing MS with another sender that is closer to the network centre. Many election algorithms can be used to choose the centre node of a network, but most of them consume the limited bandwidth of ad hoc networks. Wasting bandwidth has a bad effect on packet delivery ratio by increasing latency.

The new protocol uses a simple mechanism with almost no cost. The new mechanism is based on the number of K that MS and all senders calculate. Whenever MS receives N-SOURCE messages, it chooses the sender with the highest value of K. If MS chooses to hand over control to another sender, a message will be sent to the chosen sender with the names of all existing groups. The new MS will take control and start constructing the mesh.

Moving MS to be near to the centre balances the network load, and thus the distance between MS and receivers will become shorter. Packet collision and latency will be decreased and packet delivery ratio will be increased and the limited bandwidth in ad hoc networks will be saved and nodes will consume less battery power.

4.7 The existence of more than one Mesh Sender

If several sources simultaneously become MSs when no available MS exists, JOIN RQ messages from MSs will collide with each other. In this case intermediate nodes choose to send JOIN RQ messages from the MS with the highest value of K. After an MS is chosen, all messages from other MSs are ignored. The same calculation is also done by the other MSs, and thus they will decide not to become an MS since the new MS is elected. Each one of the sources sends a N-SOURCE message to the new MS to inform it about their existence, and then the sources start sending their data packets to the new MS. When receiving the data packets the new MS forwards it to group (s) receiver (s).

4.8 Mesh Sender failure

In case of its failure MS chooses one of its near neighbours to become a backup node. Backup information will be periodically sent to the backup node, and if this information is not received within a predetermined period of time, the backup node chooses one of the senders to become the new MS. The backup node broadcasts a message across the network to inform all nodes about the new MS, and upon receiving this message the new MS chooses its backup node and start broadcasting JOIN RQ messages. And the other senders start sending their data packets to the new MS in order to be delivered to the destinations.

4.9 Leaving and joining a group

One of the main characteristic of mobile ad hoc networks is that any node can join a group or leave it on demand. In the new protocol a soft state is used and therefore no additional control packets need to be sent by any node in order to join or leave a group. If a source decides to leave a group the only thing it will do is stop sending data packets, and if node desires to leave a group it stops sending the JOIN RP messages unless it is an intermediate node in a group. By using this method the new protocol reduces the number of control packets and thus the control overhead will be reduced.

4.10 Mesh Creation Example

An example of Mesh creation is shown in Figure 4.6. MS broadcasts JOIN RQ message to its neighbours (A, B, R1-G1 (i.e. receiver 1 belongs to group one), S-G1 (i.e. sender belong to group one)).

None of R1-G1's neighbours belong to any group, therefore only group 2 address will be added to the JOIN RP message, and then it will be sent to MS. Node A, node B and S-G1 broadcast JOIN RQ messages to their neighbours and wait to hear the neighbours' replies. R1-G2 adds group 2 address to the JOIN RP message and replies to S-G1, then S-G1 forwards the JOIN RP message to MS without adding the group 1 address (its own group), because it is not a receiver; it is only a sender.

Node B broadcasts a JOIN RQ message to node R3-G1 and node

S-G2, and as S-G2 is only a sender and none of its neighbours belong to any group, it replies to node B without adding any group address. Node B must wait for a JOIN RP message from node R3-G1; and node R2-G1 and node R4-G1 receive JOIN RQ messages from R3-G1; both of them add group 1's address and reply to R3-G1. The JOIN RP message that has the address of group 1 will be sent from R3-G1 to node B and then from node B to MS.

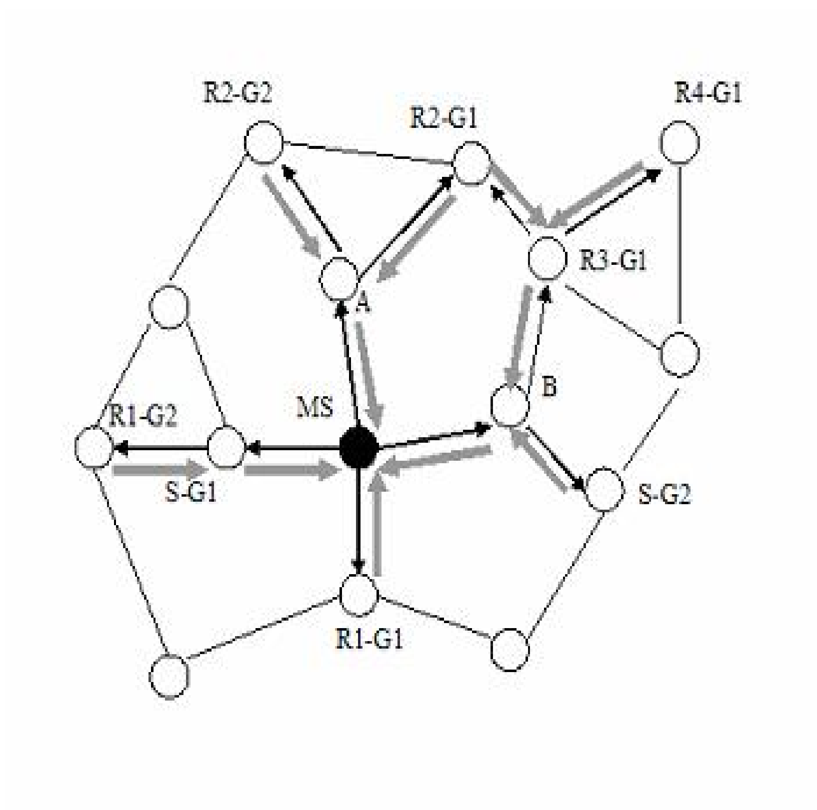


Figure 4.6: Mesh creation example.

Node A sends a JOIN RQ message to R2-G2 and R2-G1. A JOIN RP message that has the address of group 2 will be sent from R2-G2 to node A, and another JOIN RP message will be sent from R2-G1 to node A after adding the address of group 1. Node A replies to MS with a message that has the addresses of group 1 and group 2 added to it.

We can notice that node B stores the R3-G1 address to be able to forward data packets destined to group 1 and node A stores the addresses of R2-G2 and R2-G1 to be able to forward data packets destined to group 1 and group 2. As shown in Figure 4.6, the multicast mesh provides alternative routes. Even if a link between node A and R2-G1 is broken, the packet will be transferred to R2-G1 via R2-G2 or via node B, R3-G1 respectively.

4.11 Loop prevention

Loops can occur in mobile ad hoc networks since any node can receive a packet more than one time, and when the nodes keep forwarding these packets loops will occur. Loops increase the number of control packets and therefore the control overhead increases, and also transmitting unneeded packets wastes the limited bandwidth in mobile ad hoc networks.

The new protocol prevents looping by using the sequence number.

When a node receives a packet, the sequence number of the packet will be stored in the node's cache, and if the same packet is received again its sequence number will be compared with the sequence number that is stored in the node's cache, and if the number was greater than the one stored in the cache then the packet will be forwarded since it is a new packet, and otherwise the packet will be discarded because it is an old message.

4.12 Operating as a unicast routing protocol

One of the major drawbacks of many of the existing protocols is that they are dependent on the unicast protocols such as AMRoute and CAMP, and some of them run on top of particular unicast routing protocol such as CAMP, LAM, and RBM. The new protocol can run with any unicast routing protocol, and also can run as a unicast routing protocol.

4.13 The Parameter K

The value of K is calculated by each sender, and this value gives an indication of the node density around each sender. And based on this value the next MS will be chosen. The new protocol chooses the sender with the higher number of K to be the next MS, and therefore the MS will be the one which is located in the most crowded area. The value of K is used in the new protocol for several reasons; the following points are the major advantages of this value:

- **Balancing the network load:**

  When the network load is unbalanced network congestion will increase and packets need to wait a longer time before they are delivered. The new protocol uses the value of K in order to balance the network load. Based on this value the MS position will be near to the centre and it will be the one with highest number of neighbours, and since the MS depends on its neighbours in delivering the control and data packets, and by having more neighbours, the network load on each link will be lighter, and thus the network load will be balanced.

- **Reducing the distance to the destinations:**

  When the MS is positioned near to the centre of the network, the number of hops needed to reach the destinations will be reduced. And therefore the packet latency will be decreased and the packet delivery ratio improves.

- **Decreasing the packet congestion**

Congestion is one of the major drawbacks of many of the existing routing protocols. In the new protocol by increasing the number of neighbours, the packets will have redundant routes available to use to reach the destinations. The number of packets that each neighbour needs to deliver will be decreased and therefore the waiting time for each packet at the node will be decreased; hence the congestion will be decreased.

- **Saving the network resources**

Some of the main characteristics of mobile ad hoc networks are the limited bandwidth and relying on batteries. In the new protocol by using the value of K, the number of hops that each packet needs in order to reach the destination will be decreased, and thus the bandwidth will be saved and the battery power will not be wasted. By decreasing the packet congestion the size of memory that is used to store the delayed packets will be minimized. Hence the network resources will be saved and its efficiency will be improved.

4.14 One mesh for all groups

The new protocol is a mesh based protocol rather than a typical tree based protocol, redundant routes in the mesh provide multiple paths to a destination in case of link breaks. One of the major drawbacks of the existing mesh based routing protocols is that by increasing the number of groups the number of meshes needed to be constructed also increases. And in the presence of multiple meshes, each mesh has its own control and data packets, the packet collision and congestion increases. Thus packets must be buffered or dropped, and in this case packet latency increases and the packet loss also increases. Therefore the packet overhead increases, and the packet delivery ratio decreases. Thus the existing routing protocols have scalability problem.

The new protocol overcomes this problem by constructing only one mesh for all groups, and by increasing the number of groups the number of meshes will not increase. Since there is only one mesh the redundant routes in this mesh serves all groups members, the packet collision will be eliminated since all nodes use the same routes that the mesh provides. Therefore the new protocol will not be affected when the number of groups increases. Hence the new protocol will be a scalable multicast routing protocol.

4.15 One join request and one join reply for all groups

In the existing routing protocols each source broadcasts its own join request message and join reply message, and by increasing the number of sources or groups the number of control messages will be multiplied by the number of sources, and therefore the control overhead increases sharply when the number of sources or groups increase. The new protocol uses only one join request message and one join reply message for all groups. These join request and one join reply packets will carry route information for all group (s) members, and therefore when the number of senders or groups increases the number of control packets will not increase and this improves the scalability of the new protocol.

4.16 Using passive acknowledgments

When a node receives a packet from a neighbour node usually a control packet called an acknowledgment packet is sent to the originator in order to inform it about the reception of the packet. Therefore each join request message and join reply message has its own acknowledgment packet in order to make sure that it has been delivered. The new protocol eliminates the acknowledgment packet by using the “First Upstream Node Address” field and the “Second Upstream Node Address” filed in a join request packet. When a node receives a join request packet from an upstream node, it assigns the following values (second upstream node address = first upstream node address; first upstream node address = its own address), and rebroadcasts it to its neighbours. When the node overhears a message with its own address assigned to the second upstream node address (which means that its message has been received and rebroadcasted by the neighbour node. It then waits until a join reply message is received. This is called a passive acknowledgment and by using this method the new protocol reduces the number of control packets and thus the overhead will be reduced and the limited bandwidth will be saved. Thus the efficiency and scalability of the protocol will be improved.

4.17 Using the shortest path

Due to the availability of multiple paths in the mesh topology, the packets can use longer routes in the presence of a shorter one and this has a bad effect on the packet latency and the efficiency of the protocol. Therefore the new protocol uses the “hop count” field in order to deliver the packets through the shortest path. The hop count is an indication of the number of links that this packet has traveled so far which means the distance. And by using this method the new protocols decrease the packet latency and improve its efficiency.

4.18 Conclusion

A novel routing protocol for ad hoc networks has been proposed. The new protocol uses the multicast method in order to forward packets to their destination. It is a reactive and mesh based routing protocol and one central node propagates one message to all different groups to invite them to join any group in the network. All senders that belong to all groups send their data packets to this central node, to be forwarded to all groups members.

In this chapter, a detailed description of the proposed routing protocol is presented including multicast route construction and maintenance with suitable examples. And some of the main characteristics of the proposed routing protocol are also highlighted including, loop prevention, operating as a unicast routing protocol, the advantages of using the parameter K, using the passive acknowledgment, using the shortest path, creating one mesh for all groups, and sending one join request message and one join reply message for all group (s) members. Special cases such as the existence of more than one mesh sender and the mesh sender failure are discussed.

Chapter 5

Experiments and Performance Evaluation

5.1 Introduction

In this chapter, the performance of the Network Sender Multicast Routing Protocol (NSMRP) is evaluated and compared to the ODMRP routing protocol. The evaluation method and metrics are introduced, and the results of all the performed experiments are presented and discussed in detail. Experiments are carried out in order to determine the effects of the following on the performance of the routing protocols:

- **Experiment 1**: the effect of changing the number of groups.
- **Experiment 2**: the effect of changing the number of senders.
- **Experiment 3**: the effect of mobility.
- **Experiment 4**: a final experiment is performed to determine the reliability of NSMRP.

5.2 Methodology

In order to evaluate the performance of the new multicast routing protocol, this study compares the NSMRP routing protocol with the ODMRP routing protocol. Previous studies have shown that ODMRP outperforms all other currently available protocols for multicast routing in MANET [Dhillon and Ngo, 2005; Puthana and Illendula, 2005; Viswanath et al., 2004; Sobeih et al., 2004; Gui and Mohapatra, 2004; Mohan et al., 2002; Sharma et al., 2002; Lee et al., 2000]. ODMRP shows good performance even in highly dynamic situations. Due to the use of a mesh topology in ODMRP, it is robust to link failure [Lee et al., 2000].

The experiments used the GloMoSim simulator [Bajaj et al., 1999; Nilsson, 2002]. GloMoSim is a scalable simulation environment, and it has been designed for wireless and wired network systems, and uses the parallel discrete event simulation capability that is provided by Parsec. GloMoSim is supported by many platforms and several previous studies have used it. To guarantee a fair comparison, seven runs with different seed numbers were conducted for each scenario and collected data was averaged over those runs. Therefore each data point in the graphs represents the average across the number of runs. And each number in the results tables is rounded to three decimal places.

5.3 GloMoSim simulator

The GloMoSim (GLObal MObile information system SIMulator) is a software that supports scalable simulations of many types of wireless protocols. It is designed using the parallel discrete-event simulation capability provided by PARSEC (PARallel Simulation Environment for Complex Systems). It is a C based simulation language developed by the Parallel Computing Laboratory at UCLA, for sequential and parallel execution of discrete event simulation model. GloMoSim uses a layered structure, similar to the Open Systems Interconnection (OSI) seven layer network stack, with standard Application programming interfaces (APIs) for composition of protocols across different layers. This makes it easy to implement and integrate new protocols and models at different layers, a wide range of models and protocols are supported at different layers and it has built-in statistics collection at each layer. GloMoSim is a scalable simulator and has capabilities to simulate thousands of mobile nodes and can be used for real-time simulation of networks and provides a graphical user interface (GUI).

The following are the available models in GloMoSim at each of the major layers:

• **Application**: Replicated file system, NetMeeting, WebPhone, synthetic traffic generators, ftp, telnet, cbr, web caching.

• **Transport** : UDP, DBS satellite models, TCP(FreeBSD), NS TCP (Tahoe).

• **Multicasting**: ODMRP, DVMRP, CAMP, AMRIS, AMRoute, AST, CAMP, AMRIS, AMRoute, AST.

• **Routing**: Distributed Bellman-Ford, LAR, NS-DSDV, DREAM, MMWN, Flooding, Fisheye, DSR, DSDV, WRP.

• **MAC**: IEEE 802.11, MACA-W, CSMA.

• **Radio**: DS SS with and without capture.

• **Propagation**: 2-ray ground reflection model, analytical (free space, Rayleigh, Ricean), path loss trace files.

• **Mobility**: Trace files, random waypoint.

GloMoSim has a layered structure and the whole simulator has been built such that each layer handles one aspect of the simulation. And the simulator allows users to set various parameters relating to the simulation environment.

These layers interact with one another in order to produce the simulation results. And the output is presented in a statistics file after the simulation has completed. The following is an example of the statistics file:

```
Node:   5, Layer:  RadioAccnoise, Signals transmitted: 42
Node:   5, Layer:  RadioAccnoise, Signals arrived with power above RX sensitivity: 552
Node:   5, Layer:  RadioAccnoise, Signals arrived with power above RX threshold: 290
Node:   5, Layer:  RadioAccnoise, Signals received and forwarded to MAC: 266
Node:   5, Layer:  RadioAccnoise, Collisions: 6
Node:   5, Layer:  RadioAccnoise, Energy consumption (in mWhr): 25.001
Node:   5, Layer:         802.11, pkts from network: 0
Node:   5, Layer:         802.11, UCAST (non-frag) pkts sent to chanl: 0
Node:   5, Layer:         802.11, BCAST pkts sent to chanl: 42
Node:   5, Layer:         802.11, UCAST pkts rcvd clearly: 0
Node:   5, Layer:         802.11, BCAST pkts rcvd clearly: 266
Node:   5, Layer:         802.11, retx pkts due to CTS timeout: 0
Node:   5, Layer:         802.11, retx pkts due to ACK timeout: 0
Node:   5, Layer:         802.11, pkt drops due to retx limit: 0
Node:   5, Layer:         802.11, RTS Packets ignored due to Busy Channel 0
Node:   5, Layer:         802.11, RTS Packets ignored due to NAV 0
Node:   5, Layer:   RoutingNsmrp, Number of Join Queries Txed = 20
Node:   5, Layer:   RoutingNsmrp, Number of Join Replies Txed = 22
Node:   5, Layer:   RoutingNsmrp, Number of Acks Txed = 0
Node:   5, Layer:   RoutingNsmrp, Number of CTRL Packets Txed = 42
Node:   5, Layer:   RoutingNsmrp, Number of Data Txed = 20
Node:   5, Layer:   RoutingNsmrp, Number of Data Packets Originated = 0
Node:   5, Layer:   RoutingNsmrp, Number of Data Packets Supposed to be Received = 0
Node:   5, Layer:   RoutingNsmrp, Number of Data Packets Received = 96
```

```
Node:     5, Layer:      NetworkIp, Number of Packet Attepted to be Sent to MAC: 42
Node:     5, Layer:      NetworkIp, Number of Packets Routed For Another Node: 266
Node:     5, Layer:      NetworkIp, Number of Packets Delivered To this Node: 0
Node:     5, Layer:      NetworkIp, Total of the TTL's of Delivered Packets: 0
Node:     5, Layer:      NetworkIp, Number Fragments dropped because Node was
Unreachable: 0
Node:     5, Layer:      NetworkIp, Number Fragments dropped because TTL expired: 93
Node:     5, Layer:    TransportUdp, Number of pkts from application 0.
Node:     5, Layer:    TransportUdp, Number of pkts to application 96.
Node:     5, Layer:    AppCbrServer, (0) Client address: 1
Node:     5, Layer:    AppCbrServer, (0) First packet received at [s]: 0.002580342
Node:     5, Layer:    AppCbrServer, (0) Last packet received at [s]: 99.502580407
Node:     5, Layer:    AppCbrServer, (0) Average end-to-end delay [s]: 0.003192974
Node:     5, Layer:    AppCbrServer, (0) Session status: Not closed
Node:     5, Layer:    AppCbrServer, (0) Total number of bytes received: 49152
Node:     5, Layer:    AppCbrServer, (0) Total number of packets received: 96
Node:     5, Layer:    AppCbrServer, (0) Throughput (bits per second): 3932
```

5.4 The structure of the new simulation code

The structure of the new simulation code is briefly described using the following flowchart which includes eighteen figures. The rest of the flowchart is in Appendix B. The creation and initialization of each node is shown in Figure 5.1 (a), and in Figure 5.1 (b) the message is given to the destination’s event handler function. In Figure 5.1 (c) the output results from the simulation run are obtained.

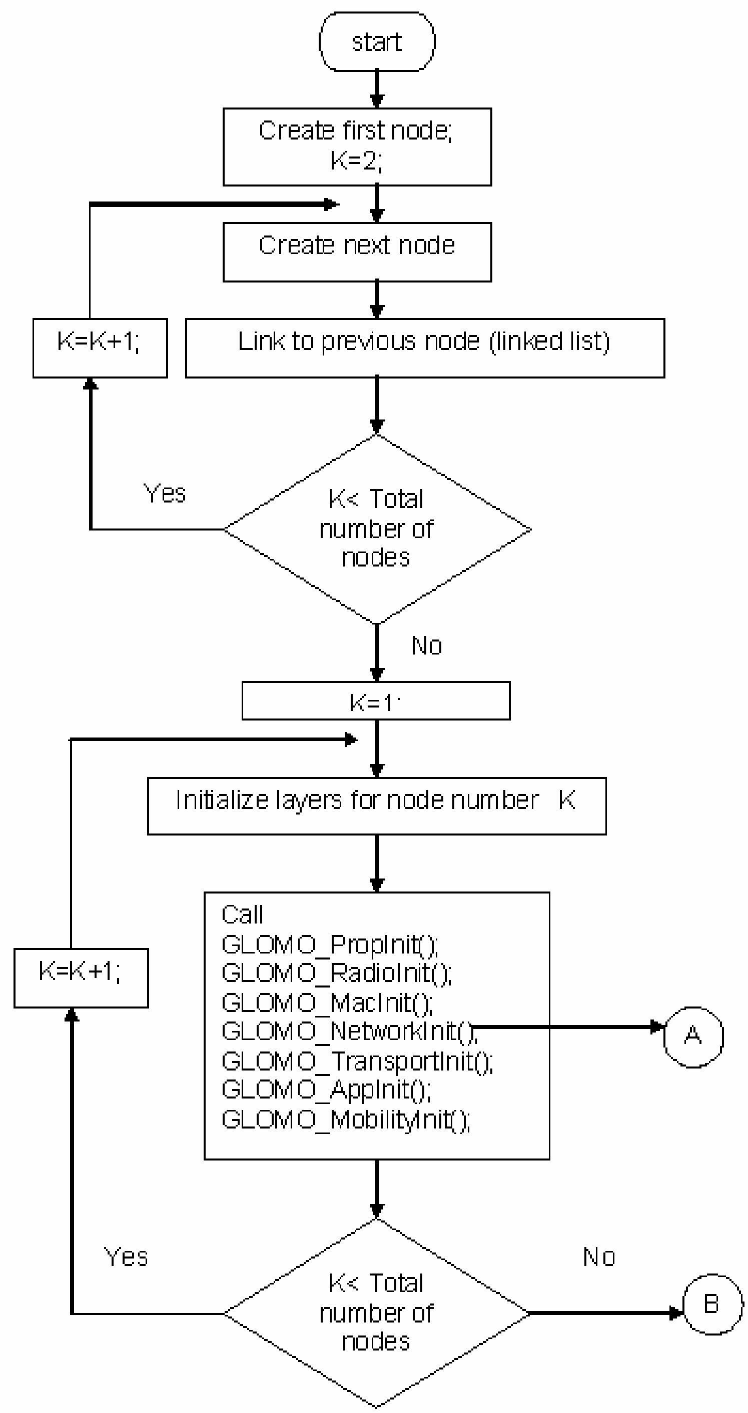


Figure 5.1 (a) The initialization phase of the simulation code.

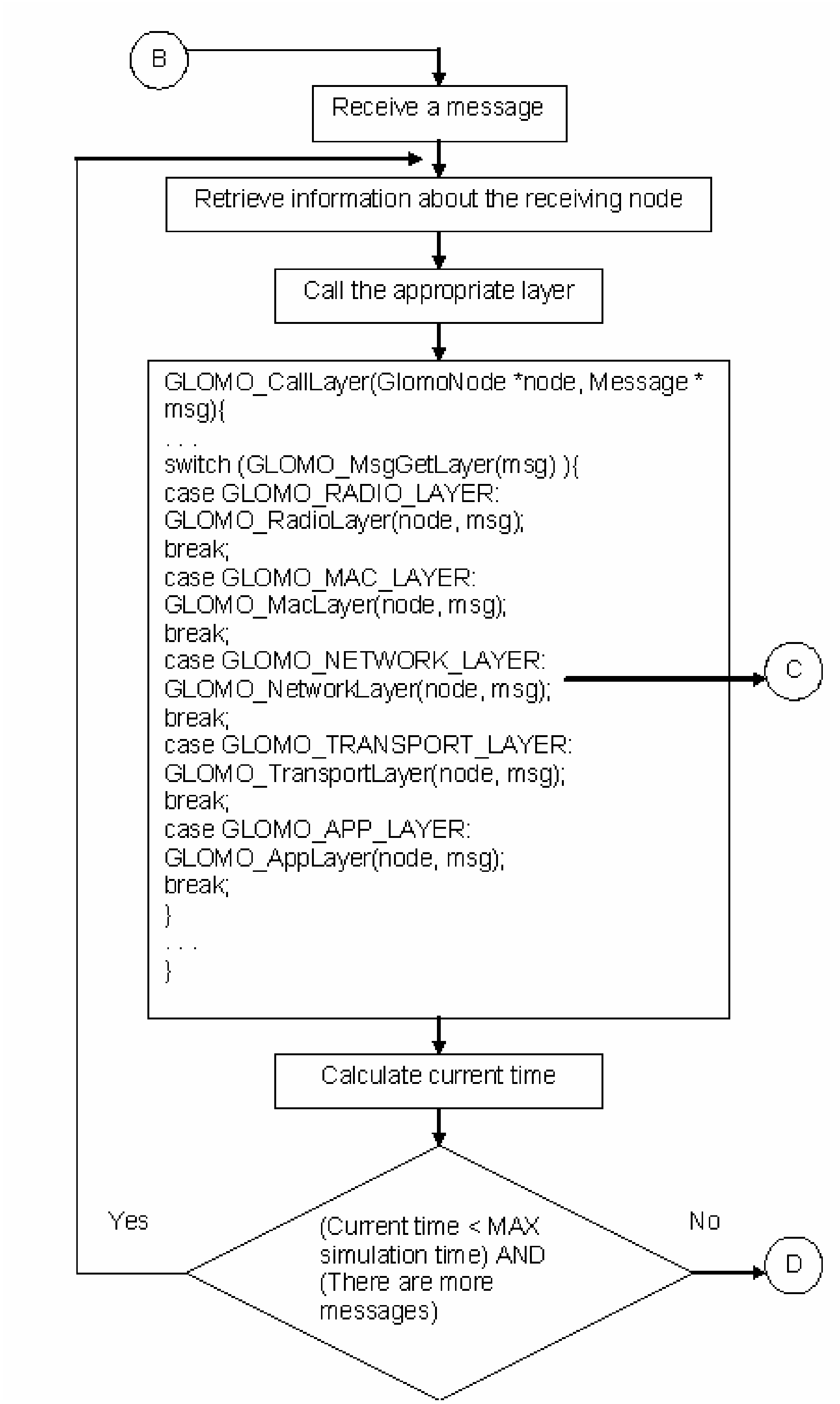


Figure 5.1 (b) The event handling phase of the simulation code.

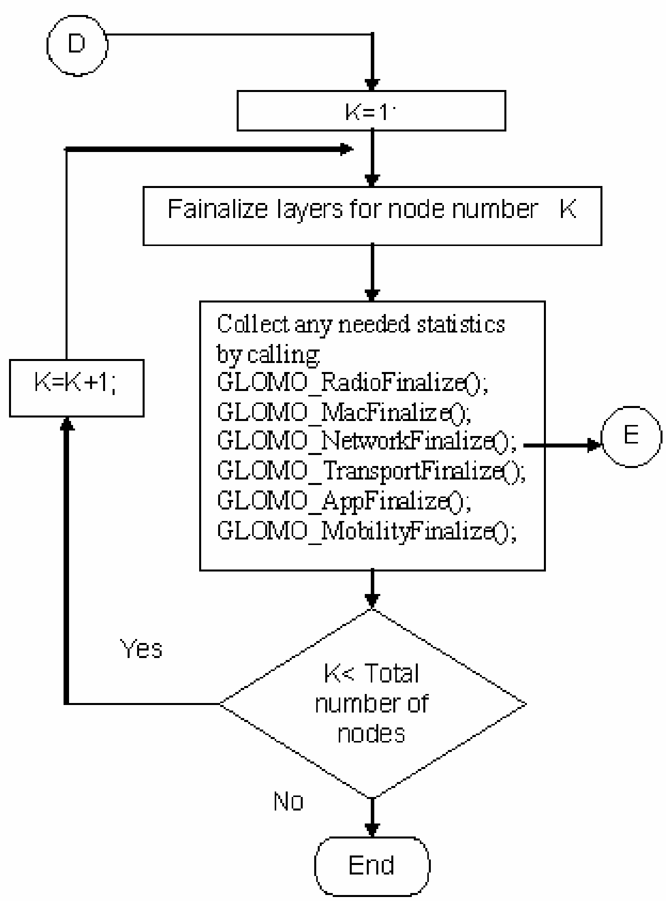


Figure 5.1 (c) The finalization phase of the simulation code.

According to the design of both routing protocols, ODMRP and NSMRP, they must give the same results under specific scenarios such as a group with one sender. And since ODMRP simulation code comes with Glomosim simulator and its results are widely accepted in the previous literature and studies, therefore the ODMRP simulation results under these scenarios were used to validate the new protocol's code under the same scenarios. The new code has been debugged until the right results were obtained.

5.5 Performance evaluation metrics

To evaluate the performance of the new protocol, this study will use similar metrics to those used in previous studies, and given by the IETF MANET working group for routing/multicast protocol evaluation:

1. Packet delivery ratio (ratio of packets actually delivered vs. the amount of packets supposed to be delivered); this value indicates the effectiveness of the protocol.
2. Data packet overhead (number of data packets transmitted per data packet delivered). Data packets transmitted is the count of every transmission of data by each node over the network. This count includes transmissions of packets that are dropped and retransmitted by intermediate nodes.

3. Routing overhead or Control packet overhead (Number of control packets transmitted per data packet delivered) gives a measure of efficient utilization of control packets in delivering data.
4. Number of control packets and data packets transmitted per data packet delivered; this measure shows the efficiency in terms of the network channel access.
5. Total number of packet collisions.

The evaluation of the above metrics will be against:

1. Mobility speed (metre/sec).
2. Number of senders.
3. Number of multicast groups.

5.6 Experiment 1: the effect of increasing the number of groups

This experiment studies the effects of increasing the number of groups on the NSMRP routing protocol and the ODMRP routing protocol, in terms of the above mentioned metrics. The number of multicast groups is varied in order to investigate the reliability and scalability of both routing protocols.

5.6.1 Simulation model

The network simulation consisted of 200 nodes placed in (1000 metre * 1000 metre) area. The node placement was uniform, and the simulation time was 800 seconds. The bandwidth used in this simulation was 2Mbps and the radio propagation range was 125 metres. Node speed varied between 0 and 10 m/sec. The type of mobility was Random-Waypoint. The MAC protocol was IEEE 802.11. The simulator used a number of groups from 1 to 11. The traffic type was constant bit rate (CBR) protocol. Every node Joins its group at the start of the simulation and stays as a member until the end of the simulation. The experimental parameters are shown in Table 5.1.

The following are the definitions of some of the parameters:

1. **Random-Waypoint Mobility type**

In this method a node randomly chooses a destination point from a physical area. Then it moves in the direction of the destination point in a speed chosen between the minimum and maximum speed (metre/sec). When the destination is reached, the node stays there for the pause time period.

2. The traffic type CBR

It is a constant bit rate generator. In this method every source continuously sends one 512 bytes packet per second to its group members from the start to the end of the simulation.

Parameter	**Value**
Number of nodes	200 nodes
Terrain range	1000 metre * 1000 metre area
Power range	125 metre
Bandwidth	2 Mbps
Simulation time	800 seconds
Node placement	uniform
The type of Mobility	Random-Waypoint
Nodes speed	varied between 0 and 10 m/sec
Traffic type	CBR
Pause time	0 sec to 30 sec
number of groups	1 to 11
The MAC protocol	IEEE 802.11

Table 5.1. Parameter settings for Experiment 1.

5.6.2 Simulation results

In order to compare the performance of the two routing protocols NSMRP and ODMRP, in the first experiment the number of senders and groups was varied (each sender belongs to a different group) to investigate the protocol's scalability.

The total number of nodes was 200, and each group had the same number of members.

Figures 5.2 to 5.6 show the effects of changing the number of groups on the protocols scalability. NSMRP performs better than ODMRP. In Figure 5.2 the value of the packet delivery ratio is the same when the number of groups is one, and this is because both protocols construct one mesh and send one join request and one join reply packet , and when number of groups increases this ratio decreases for the ODMRP protocol and increases for the NSMRP protocol. As the number of groups and number of senders increases in ODMRP the number of JOIN-RQ messages increases and the number of JOIN-RP messages also increases accordingly. This causes the number of dropped packets to increase due to collisions and thus packet delivery ratio decreases. By increasing the number of groups in ODMRP, there are more forwarding meshes competing for radio channel and this increases the traffic and causes collision. In NSMRP, since the same JOIN-RQ message is propagated to all groups members and one mesh is created for all groups, all groups members cooperate together to deliver data packets to their destination. By increasing the number of groups, more nodes will help to deliver the data packets, and thus packet delivery ratio will increase. The packet delivery ratio difference between the two protocols is 5% when the number of groups is two and the difference increased to 19.2% when the number of groups and senders became eleven.

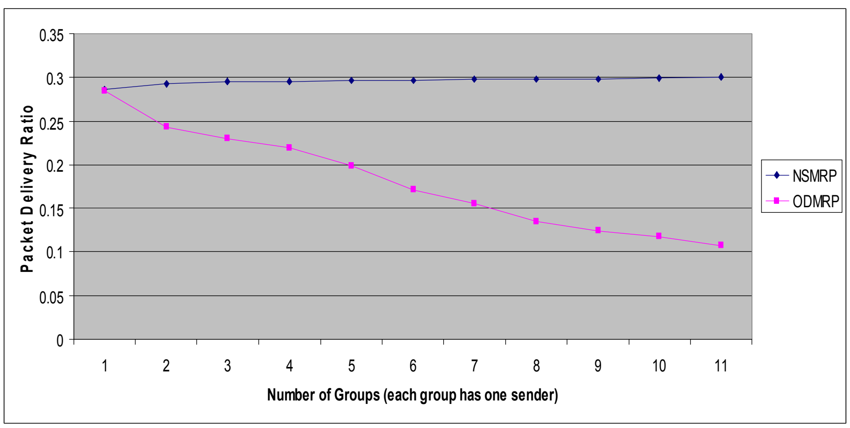


Figure 5.2. Packet Delivery Ratio for various number of groups.

	1	2	3	4	5	6	7	8	9	10	11
NSMRP	0.286	0.292	0.295	0.295	0.297	0.297	0.298	0.298	0.298	0.3	0.3
ODMRP	0.285	0.243	0.23	0.22	0.199	0.171	0.155	0.134	0.124	0.117	0.108

Table 5.2. Packet Delivery Ratio for various number of groups.

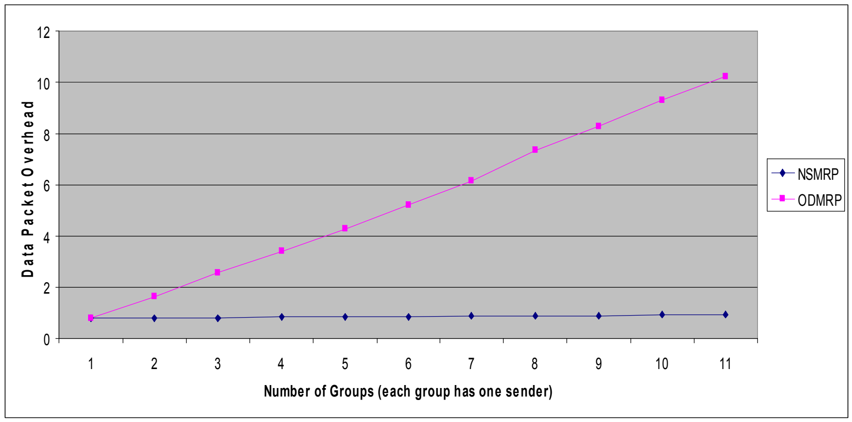


Figure 5.3. Data Packet Overhead for various number of groups.

	1	2	3	4	5	6	7	8	9	10	11
NSMRP	0.787	0.783	0.800	0.816	0.833	0.856	0.869	0.886	0.902	0.924	0.942
ODMRP	0.782	1.635	2.559	3.413	4.279	5.219	6.142	7.347	8.276	9.281	10.227

Table 5.3. Data Packet Overhead for various number of groups.

Figures 5.3 to 5.6 show the stability and robustness of the NSMRP protocol; it is not affected by increasing the number of groups. The gap increases as the number of groups increases. In Figure 5.3 the number of data packets transmitted for each data packet delivered increases for ODMRP, and this is an indication of the dropping of data packets due to congestion. NSMRP kept the same low number of dropped data packets. The data packet overhead difference between the two protocols increased from 1.8 when the number of groups was 3, to 9.28 when the number of groups increased to 11, and this is because by increasing the number of groups in ODMRP the collision and congestion will increase and therefore packet lose will increase and this forces the sender to re-transmit the undelivered data packets.

Figures 5.4 and 5.5 show the number of control packets transmitted for each data packet delivered and the number of control packets and data packets transmitted for each data packet delivered, respectively. For ODMRP the number of control packets increases as the number of groups increases, and this is because ODMRP builds per source meshes and since each mesh has its own control packets, this number will increase by increasing the number of meshes. NSMRP builds one mesh for all groups and when the number of groups increases the same control packets will be used by more nodes, and thus NSMRP saves the limited bandwidth and limited battery power in ad hoc networks.

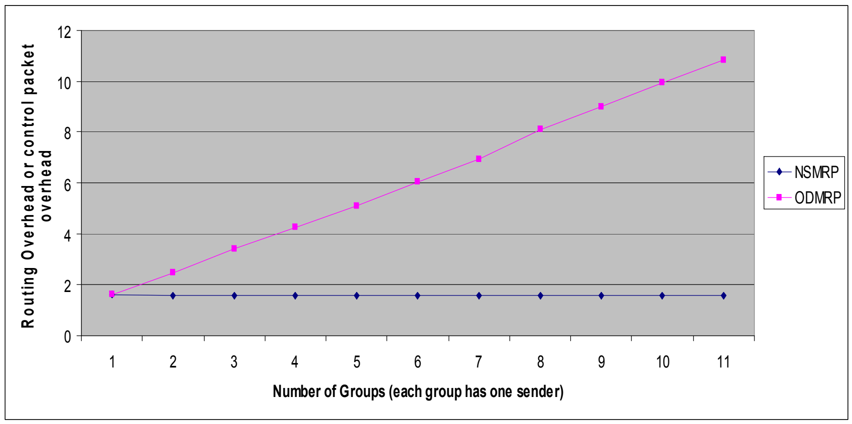


Figure 5.4. Routing Overhead for various number of groups.

	1	2	3	4	5	6	7	8	9	10	11
NSMRP	1.604	1.563	1.558	1.554	1.554	1.562	1.556	1.553	1.552	1.557	1.558
ODMRP	1.607	2.485	3.419	4.262	5.113	6.028	6.924	8.103	8.983	9.949	10.832

Table 5.4. Routing Overhead for various number of groups.

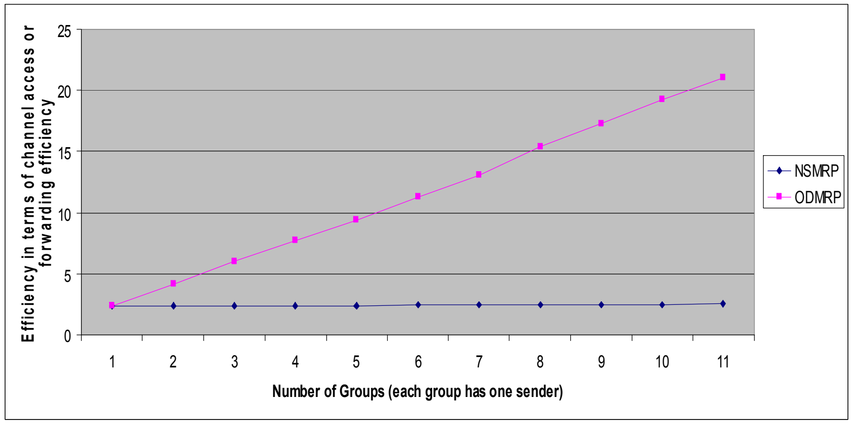


Figure 5.5. Forwarding efficiency for various number of groups.

	1	2	3	4	5	6	7	8	9	10	11
NSMRP	2.39	2.346	2.358	2.37	2.387	2.418	2.424	2.44	2.455	2.481	2.499
ODMRP	2.389	4.12	5.978	7.675	9.392	11.247	13.066	15.449	17.259	19.23	21.059

Table 5.5. Forwarding efficiency for various number of groups.

Figure 5.6 shows that the number of collisions increases by increasing the number of groups in ODMRP. This is because of the increase of the control packets and congestion that is caused by the increasing of number of meshes. Because of the low number of control packets in NSMRP, the number of collision stays at the same level.

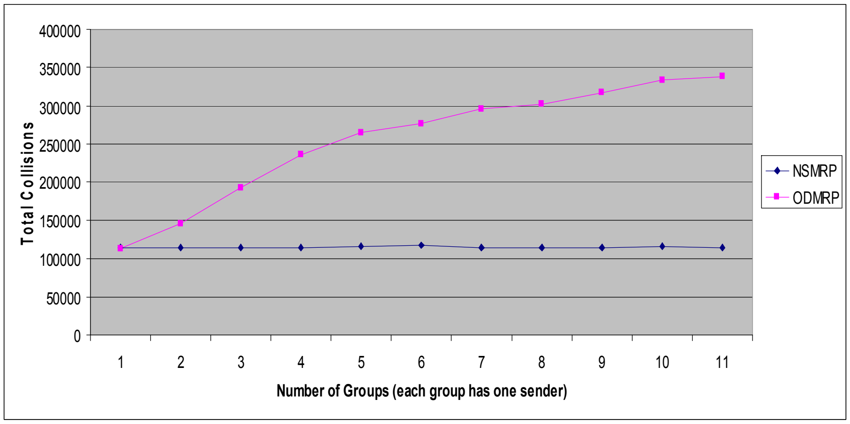


Figure 5.6. Total Collisions for various number of groups.

	1	2	3	4	5	6	7	8	9	10	11
NSMRP	114581	113935	114505	113610	115078	116832	114558	114661	114686	115196	115033
ODMRP	112104	146308	192946	235596	264388	277346	295949	302802	317456	334161	337845

Table 5.6. Total Collisions for various number of groups.

5.6.3 Conclusion

In this experiment the number of groups was varied from 1 to 11 to investigate the reliability and scalability of both routing protocols. By increasing the number of groups the packet delivery ratio increases for NSMRP and decreased sharply for ODMRP. The data packet overhead, control packet overhead, the efficiency in terms of the network channel access, and total the number of packet collisions increased sharply for ODMRP and remained the same for NSMRP.

5.7 Experiment 2: the effect of mobility

This experiment studies the effects of increasing the mobility speed on the NSMRP routing protocol and the ODMRP routing protocol, in terms of the Packet delivery ratio, Data packet overhead, Control packet overhead, the efficiency in terms of the network channel access, and total the number of packet collisions. The mobility speed is varied in order to investigate the effectiveness and robustness of both routing protocols.

5.7.1 Simulation model

The network simulation consisted of 60 nodes placed in (500 metre, 500 metre) area. The node placement was uniform, and the simulation time was 800 seconds. The bandwidth used in this simulation was 2Mbps and the radio propagation range was 125 metres. Node speed varied between 0 and 30 m/sec. The type of mobility was Random-Waypoint. The MAC protocol was

IEEE 802.11. The number of groups used in the simulator was four and the number of senders was also four senders. The traffic type was constant bit rate (CBR) protocol. Every node Joins its group at the start of the simulation and stays as a member until the end of the simulation. The experiment's parameters are shown in Table 5.7.

Parameter	**Value**
Number of nodes	60 nodes
Terrain range	500 metre * 500 metre area
Power range	125 metre
Bandwidth	2 Mbps
Simulation time	800 seconds
Node placement	uniform
The type of Mobility	Random-Waypoint
Nodes minimum speed	0 m/sec
Nodes maximum speed	varied between 0 and 30 m/sec
Traffic type	CBR
Pause time	0 sec
number of groups	4 groups
number of senders	4 senders
The MAC protocol	IEEE 802.11

Table 5.7. Parameter settings for Experiment 2.

5.7.2 Simulation results

In this experiment the total number of nodes is 60, and they are divided into four groups and each group has a sender. The minimum speed is 0 m/sec. Figures 5.7 to 5.11 show the effects of changing mobility speed on the protocol's performance. By increasing the mobility speed NSMRP and ODMRP kept their results at the same level, except the number of collisions increases by increasing mobility speed for ODMRP. By increasing the mobility speed, the network topology changes more frequently, and in order to repair the broken links ODMRP re-constructs a mesh for each source and therefore more control packets will be broadcasted as shown in Figure 5.9, and thus the number of collisions increases as shown in Figure 5.11. NSMRP outperforms ODMRP in all cases. In Packet Delivery Ratio terms as shown in Figure 5.7, NSMRP outperforms ODMRP by 36%, and this is because choosing the MS to be located at the centre of the network reduces the distance that the packet has to travel to reach its destination and balances the network load, therefore NSMRP saves the network's resources such as bandwidth and battery power.

NSMRP creates one mesh and propagates one JOIN-RQ message and thus the number of control packets will be low, and the protocol performance will not be affected by increasing mobility speed. Hence NSMRP is more robust than ODMRP to mobility.

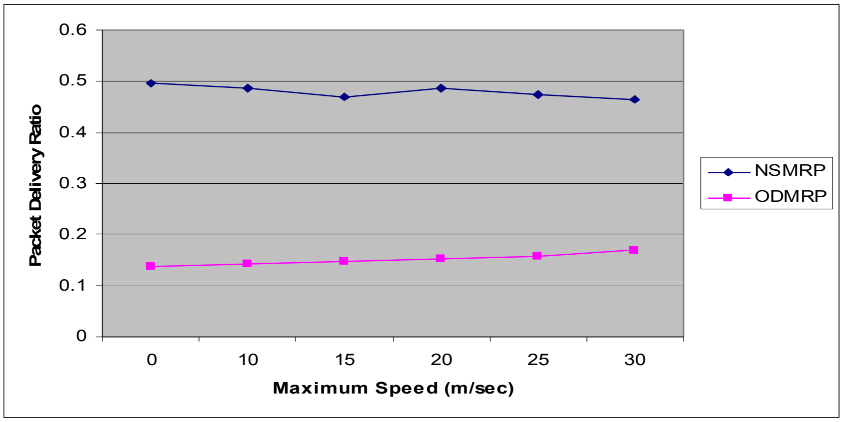


Figure 5.7. Packet Delivery Ratio at various speeds.

	0	10	15	20	25	30
NSMRP	0.495	0.485	0.469	0.486	0.475	0.464
ODMRP	0.138	0.143	0.1478	0.153	0.158	0.1689

Table 5.8. Packet Delivery Ratio at various speeds.

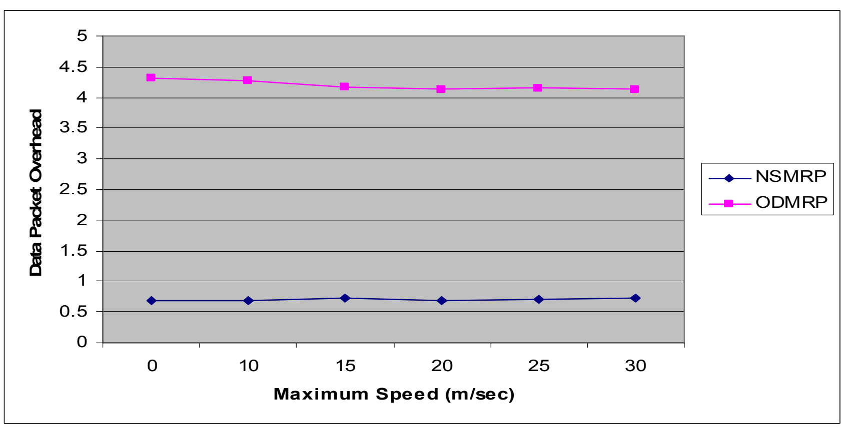


Figure 5.8. Data Packet Overhead at various speeds.

	0	10	15	20	25	30
NSMRP	0.681	0.694	0.718	0.692	0.709	0.725
ODMRP	4.317	4.273	4.178	4.127	4.148	4.124

Table 5.9. Data Packet Overhead at various speeds.

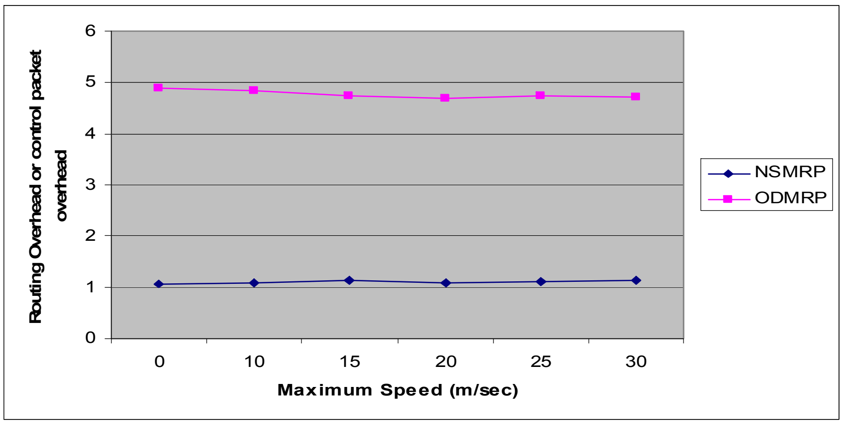


Figure 5.9. Control packet overhead at various speeds.

	0	10	15	20	25	30
NSMRP	1.077	1.097	1.135	1.094	1.12	1.146
ODMRP	4.88	4.844	4.74	4.691	4.732	4.727

Table 5.10. Control packet overhead at various speeds.

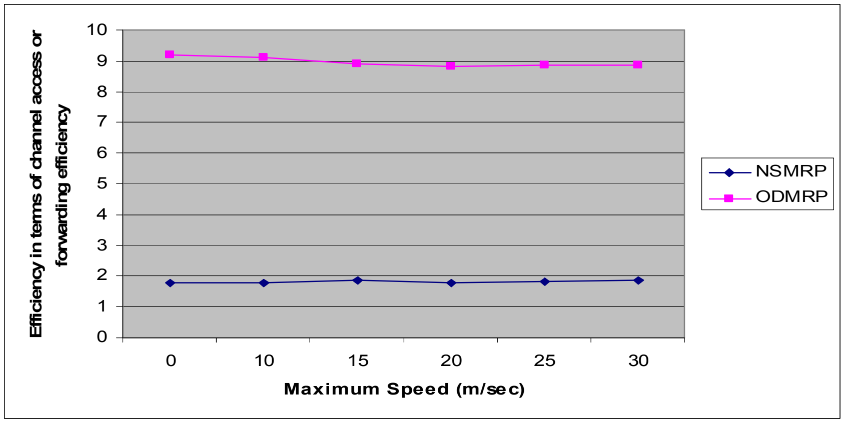


Figure 5.10. Efficiency in terms of channel access at various speeds.

	0	10	15	20	25	30
NSMRP	1.758	1.792	1.853	1.786	1.829	1.871
ODMRP	9.197	9.117	8.918	8.819	8.88	8.851

Table 5.11. Efficiency in terms of channel access at various speeds.

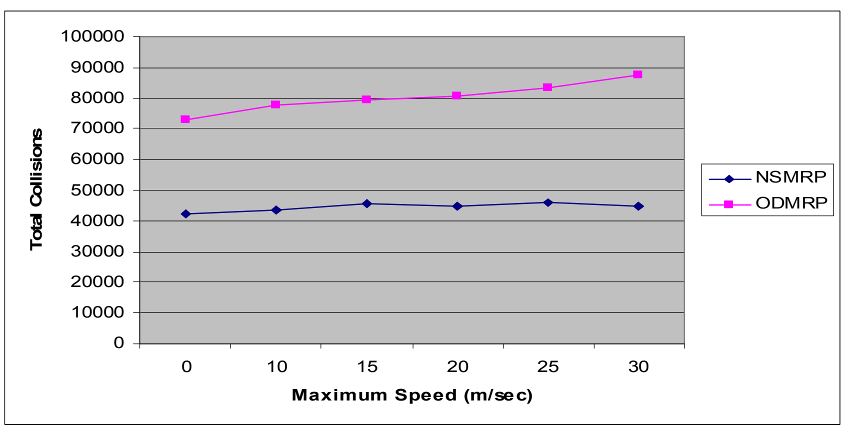


Figure 5.11. Total Collisions at various speeds.

	0	10	15	20	25	30
NSMRP	42525	43474	45489	44852	46009	44911
ODMRP	72792	77896	79272	80638	83505	87524

Table 5.12. Total Collisions at various speeds.

5.7.3 Conclusion

In this experiment the mobility speed was varied from 0 m/s to 30 m/s to investigate the effectiveness and robustness of both routing protocols. The results show that the proposed routing protocol outperforms ODMRP in all cases. By increasing the mobility speed, the packet collision increases for ODMRP and remains the same for NSMRP. In packet delivery ratio terms NSMRP outperforms ODMRP by 36%.

5.8 Experiment 3: the effect of increasing the number of senders

This experiment studies the effects of increasing the number of senders on the NSMRP routing protocol and the ODMRP routing protocol, in terms of the Packet delivery ratio, Data packet overhead, Control packet overhead, the efficiency in terms of the network channel access, and the total number of packet collisions. The number of senders is varied in order to investigate the scalability of both routing protocols.

5.8.1 Simulation model

The network simulation consisted of 400 nodes. The node placement was uniform. The bandwidth used in this simulation was 2Mbps and the radio propagation range was 250 metres. Node speed was 50 m/sec. The type of mobility was Random-Waypoint. The MAC protocol was IEEE 802.11. The simulator used a number of senders from 1 to 80. The traffic type was constant bit rate (CBR) protocol. Every node Joins its group at the start of the simulation and stays as a member until the end of the simulation. The experiments parameters are shown in Table 5.13.

Parameter	Value
Number of nodes	400 nodes
number of senders	1, 10, 20, 30, 40, 50, 60, 70, and 80
Power range	250 metre
Nodes speed	50 m/sec
Pause time	0 sec
Bandwidth	2 Mbps
Node placement	uniform
The type of Mobility	Random-Waypoint
Traffic type	CBR
Terrain range	700 metre * 700 metre area
The MAC protocol	IEEE 802.11

Table 5.13. Parameter settings for Experiment 3.

5.8.2 Simulation results

In order to investigate the scalability of the NSMRP routing protocol and the ODMRP routing protocol the number of senders is varied from 1 to 80 senders. By increasing the number of senders the packet delivery ratio increases for the NSMRP routing protocol and decreases for the ODMRP routing protocol as shown in Figure 5.12 and Table 5.14. When the number of senders is one both routing protocols have the same performance; this is because each routing protocol constructs only one multicast mesh for the multicast group. The packet delivery ratio difference between the two protocols is 38% when the number of senders is ten and the difference increased to 59% when the number of senders became eighty, this is because ODMRP builds per source meshes and by increasing the

number of senders the number of meshes increases accordingly and since each multicast mesh has its own join request packets and join reply packets the meshes will compete for the radio channel and this causes traffic jam and packets loss due to collision, and thus the packet delivery ratio will decrease for ODMRP as the number of senders increases.

On the other hand NSMRP builds one multicast mesh for all senders and uses one join request packet and one join reply packet for all senders, and by increasing the number of senders the number of meshes will not increase and the number of join request packets and join reply packets will stay the same. The packet delivery ratio will increase for the NSMRP when the number of senders increases and this is because the mesh and the join request packets and join reply packets will be utilized by more senders in order to deliver more data packets.

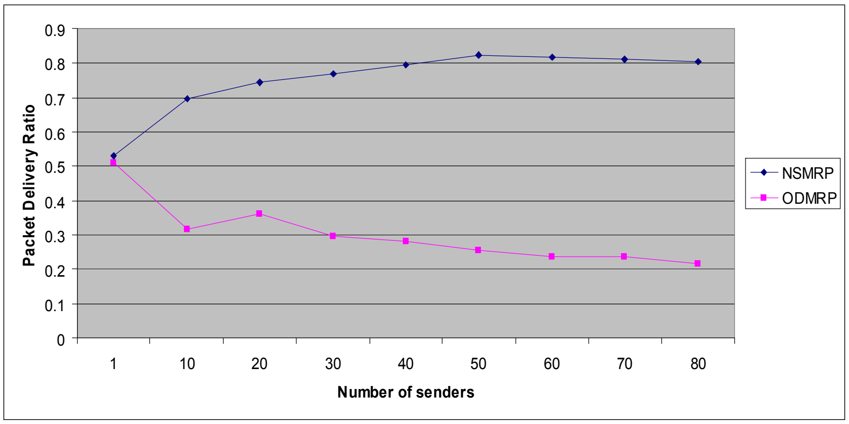


Figure 5.12. Packet Delivery Ratio for various number of senders.

	1	10	20	30	40	50	60	70	80
NSMRP	0.531	0.695	0.745	0.768	0.796	0.823	0.818	0.812	0.805
ODMRP	0.511	0.316	0.36	0.296	0.28	0.257	0.236	0.235	0.217

Table 5.14. Packet Delivery Ratio for various number of senders.

Figure 5.13 and Table 5.15 show the effects of increasing the number of senders on the NSMRP routing protocol and the ODMRP routing protocol, in terms of the data packet overhead (number of data packets transmitted per data packet delivered). This count includes transmissions of packets that are dropped and retransmitted by intermediate nodes. The data packet overhead difference between the two protocols is 7 when the number of senders is ten and the difference increased to 67 when the number of senders became eighty. As the number of senders increases the data packet overhead increases for the ODMRP routing protocol and remains the same for the NSMRP routing protocol. And this is because by increasing the number of senders for ODMRP the number of meshes will increase and the network load will increase accordingly and therefore the packets loss increases. The dropped or lost data packets will have to be retransmitted and thus the data packet overhead will increase for the ODMRP routing protocol.

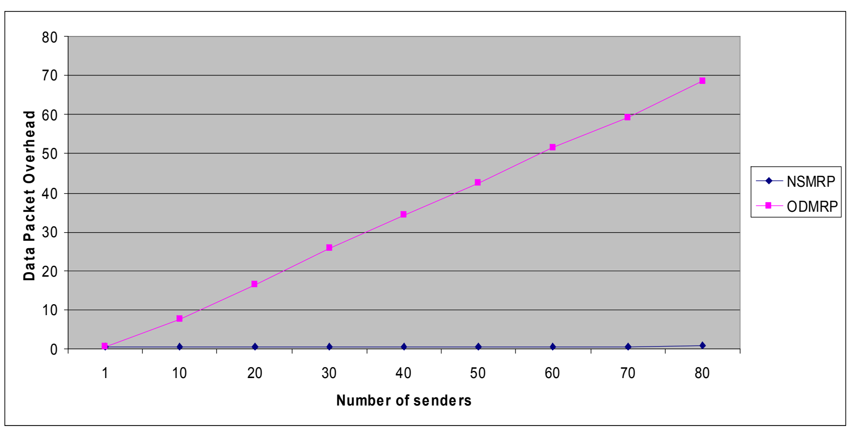


Figure 5.13. Data Packet Overhead for various number of senders.

	1	10	20	30	40	50	60	70	80
NSMRP	0.476	0.517	0.501	0.526	0.552	0.581	0.636	0.697	0.762
ODMRP	0.494	7.561	16.441	25.714	34.236	42.557	51.59	59.309	68.628

Table 5.15. Data Packet Overhead for various number of senders.

Figure 5.14 and Table 5.16 show the effects of increasing the number of senders on the NSMRP routing protocol and the ODMRP routing protocol, in terms of the control packet overhead (Number of control packets transmitted per data packet delivered). As the number of senders increases the Control

packet overhead increases sharply for the ODMRP routing protocol and remains the same for the NSMRP routing protocol. The control packet overhead difference between the two protocols is 7.5 when the number of senders is ten and the difference increased to 67.9 when the number of senders became eighty. And this is because, as the number of senders increases in ODMRP the number of meshes increases and since each sender forwards its own join request packets and join reply packets the number of control packets increases, and thus the control packet overhead increases sharply. NSMRP builds one mesh and forwards one join request packet and join reply packet for all senders therefore as the number of senders increases the control packet overhead will not increase for the NSMRP routing protocol.

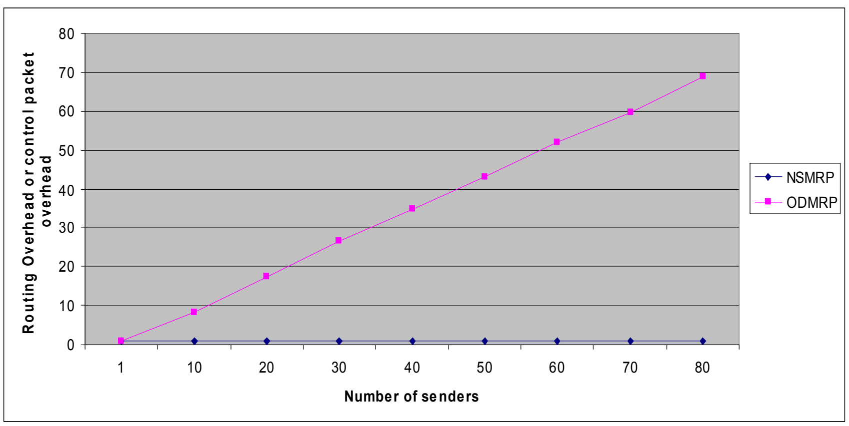


Figure 5.14. Routing Overhead for various number of senders.

	1	10	20	30	40	50	60	70	80
NSMRP	0.943	0.846	0.782	0.769	0.759	0.753	0.777	0.806	0.837
ODMRP	1.019	8.362	17.33	26.518	34.953	43.165	52.066	59.667	68.811

Table 5.16. Routing Overhead for various number of senders.

Figure 5.15 and Table 5.17 show the effects of increasing the number of senders on the NSMRP routing protocol and the ODMRP routing protocol in terms of the network channel access (efficiency) and it is equal to the number of control packets and data packets transmitted per data packet delivered. The network channel access difference between the two protocols is 14.5 when the number of senders is ten and the difference increased to 135.8 when the number of senders became eighty. As the number of senders increases this value increases sharply for the ODMRP routing protocol and stays the same for the NSMRP routing protocol. The ODMRP routing protocol constructs per source meshes and each mesh uses its own control packets, therefore by increasing the number of sources the number of control packets increases and also due to packet loss the number of retransmitted packets also increases and thus the number of control packets and data packets transmitted per data packet delivered increases for ODMRP. On the other hand since the NSMRP routing protocol constructs one mesh and uses the same control packets for all senders, as the number of senders increases more data packets will be delivered using the same control packets. Thus the NSMRP routing protocol saves the limited bandwidth in ad hoc networks.

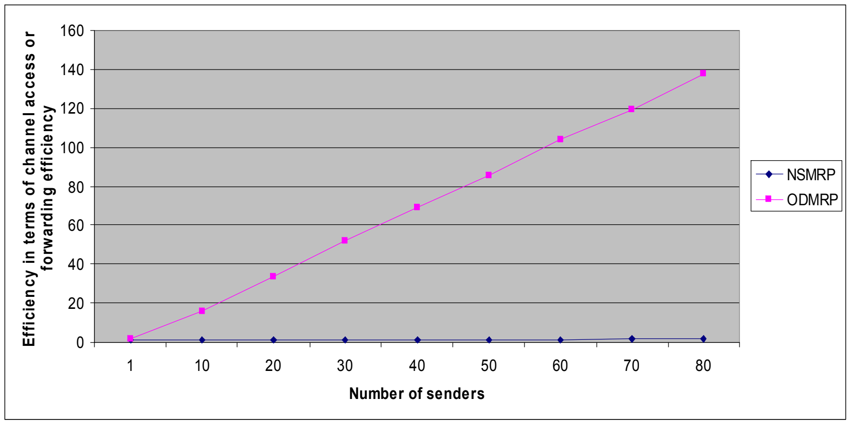


Figure 5.15. Forwarding efficiency for various number of senders.

	1	10	20	30	40	50	60	70	80
NSMRP	1.418	1.363	1.283	1.295	1.312	1.334	1.413	1.503	1.599
ODMRP	1.513	15.923	33.771	52.232	69.188	85.722	103.656	118.975	137.439

Table 5.17. Forwarding efficiency for various number of senders.

Figure 5.16 and Table 5.18 show the effects of increasing the number of senders on the NSMRP routing protocol and the ODMRP routing protocol in terms of the total collisions. As the number of senders increases the total collisions increases for the ODMRP routing protocol and remains stable for the NSMRP routing protocol. In ODMRP, by increasing the number of senders the number of meshes and the number of control packets increase, and these meshes will compete for the radio channel and this causes traffic jam and increases packet collisions. With this high number in packet collisions, ODMRP is not considered to be working properly.

On the other hand the NSMRP protocol creates one mesh and uses the same control packets for all senders, and by electing the sender that is located at the centre of the network to become the MS, the packets will use less number of hops in order to reach the destination and the network load will be balanced. Thus collisions will be reduced.

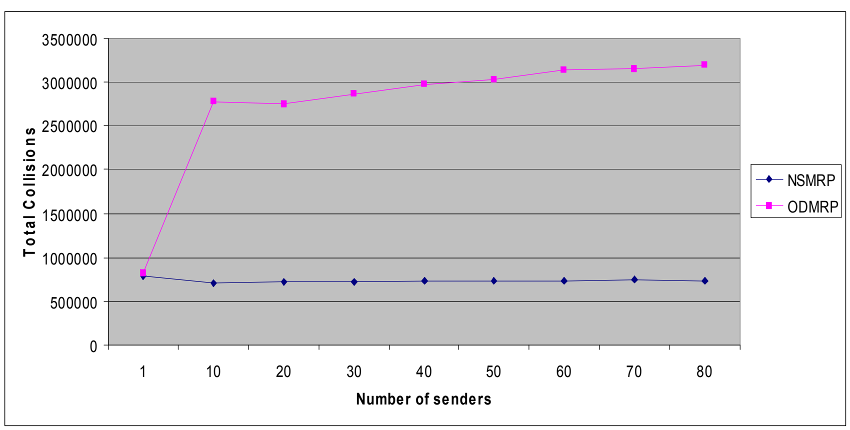


Figure 5.16. Total Collisions for various number of senders.

	1	10	20	30	40	50	60	70	80
NSMRP	783770	699908	721654	723797	731239	732348	737729	740281	737632
ODMRP	815842	2775141	2757411	2857980	2971046	3027861	3146974	3159982	3192838

Table 5.18. Total Collisions for various number of senders.

5.8.3 Conclusion

In this experiment the number of senders was varied from 1 to 80, to investigate the scalability of both routing protocols. By increasing the number of senders the packet delivery ratio increases for NSMRP and decreases for ODMRP. The data packet overhead, control packet overhead, the efficiency in terms of the network channel access, and total the number of packet collisions increased sharply for ODMRP and remained the same for NSMRP. In packet delivery ratio terms NSMRP outperforms ODMRP by 59% as the number of senders increases to 80.

5.9 Experiment 4: the Reliability of Network Sender Multicast Routing Protocol

This experiment studies the effects of increasing the number of groups under different pause times and different propagation ranges on the NSMRP routing protocol, in terms of the Packet delivery ratio, Data packet overhead, Control packet overhead, the efficiency in terms of the network channel access, and the total number of packet collisions. The number of groups, the pause time and propagation ranges are varied in order to investigate the reliability and the scalability of the NSMRP routing protocol.

5.9.1 Simulation model

The simulated network consists of 200 mobile nodes placed using uniform placement in an area of 1000m * 1000m. The simulation was executed for 800 seconds and the bandwidth used was 2Mbps. The minimum mobility speed for each node was 0 m/sec and the maximum was 10 m/sec. The pause time was varied between 0 and 50 seconds and the type of mobility used in the simulation was Random-Waypoint. Three values of the radio propagation range were used in the simulation: 250m, 280m and 310m. Five different numbers of multicast groups were used (5, 10, 15, 20, and 25 multicast groups). And every node Joins its group at the start of the simulation and stays as a member until the end of the simulation. The experiment's parameters are shown in Table 5.18.

Parameter	**Value**
Number-of-nodes	200 nodes
Terrain range	1000 m * 1000 m
number of groups	5, 10, 15, 20, 25 groups
Power-range	250 m, 280 m, 310 m
Bandwidth	2 Mbps
Simulation time	800 seconds
Node-placement	uniform
The type of Mobility	Random-Waypoint
Nodes speed	varied between 0 and 10 m/sec
Traffic type	CBR
Pause time	0 sec to 50 sec
The MAC protocol	IEEE 802.11

Table 5.19 Parameter settings for Experiment 4.

5.9.2 Simulation results

In order to investigate the reliability performance and scalability of the NSMRP routing protocol, the number of pause times for different number of groups was varied. The first experiment's results are shown in Figure 5.17. The transmission range of the wireless nodes used is 250m. In this experiment the impact of increasing the pause time on the packet delivery ratio for various numbers of groups is studied. As shown in Figures 5.17, 5.18 and 5.19 the packet delivery ratio increases as the number of groups increases. This is because NSMRP broadcasts one invitation message to all groups members, and by increasing the number of groups the message will be utilized by more nodes and thus control packets will be decreased as shown in Figure 5.20. The number of data packets delivered will increase, hence the packet delivery ratio increases, and this result gives an indication of scalability for the protocol. Figures 5.17, 5.18 and 5.19 also show that by increasing the number of groups the gap between the lines become smaller and this is because the protocol is getting closer to reaching the maximum performance while using one control packet for all groups.

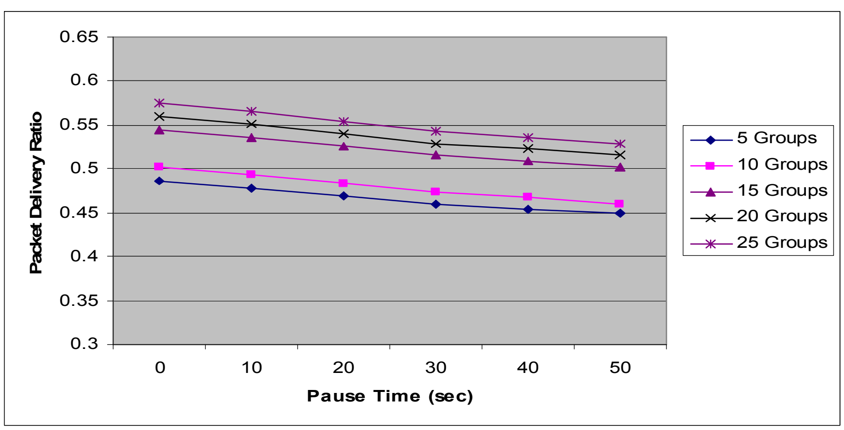


Figure 5.17. Packet Delivery Ratio for various number of pause time (sec), and the transition range is 250m.

	0	10	20	30	40	50
5 Groups	0.486	0.478	0.47	0.46	0.454	0.45
10 Groups	0.501	0.494	0.483	0.473	0.468	0.459
15 Groups	0.545	0.536	0.526	0.515	0.508	0.501
20 Groups	0.56	0.551	0.541	0.529	0.522	0.516
25 Groups	0.575	0.565	0.553	0.542	0.536	0.528

Table 5.20. Packet Delivery Ratio for various number of pause time (sec), and the transition range is 250m.

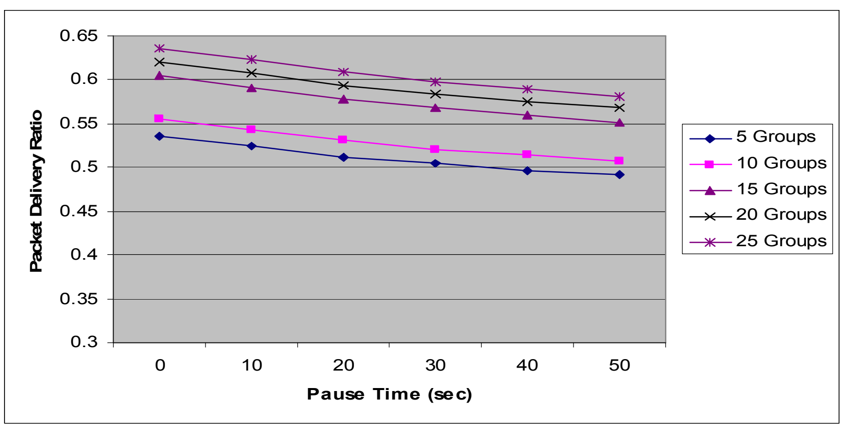


Figure 5.18. Packet Delivery Ratio for various number of pause time (sec), and the transition range is 280m.

	0	10	20	30	40	50
5 Groups	0.536	0.524	0.512	0.505	0.497	0.491
10 Groups	0.556	0.543	0.531	0.521	0.514	0.508
15 Groups	0.605	0.591	0.578	0.568	0.559	0.551
20 Groups	0.621	0.608	0.594	0.583	0.575	0.568
25 Groups	0.637	0.622	0.609	0.598	0.589	0.581

Table 5.21. Packet Delivery Ratio for various number of pause time (sec), and the transition range is 280m.

By increasing the transmission range to 280m and 310m as shown in figures 5.18 and 5.19, respectively, the packet delivery ratio for all groups increases. As the transmission range increases the number of neighbours that can be reached will increase, therefore packets will be delivered to their destination via less number of hops.

The packet delivery ratio for NSMRP increases when the number of groups increases as shown in Figures 5.17 – 5.19. Since NSMRP constructs only one mesh for all groups' members, and by increasing the number of groups, the number of multicast mesh members increases, and therefore more redundant links are created, and that prevents performance degradation when the number of groups is increased. Hence this is another indication of scalability for the protocol.

When mobility speed increases with less pause time, NSMRP shows good performance as illustrated in Figures 5.17 – 5.19 and also a lower overhead as shown in figure 5.20. Creating one mesh for all groups in NSMRP and choosing the MS node to be close to the centre reduces the distance and the time that the packet needs to reach its destination. Also the number of control packets will be reduced by broadcasting one invitation message to all groups. Thus the NSMRP routing protocol is robust to mobility.

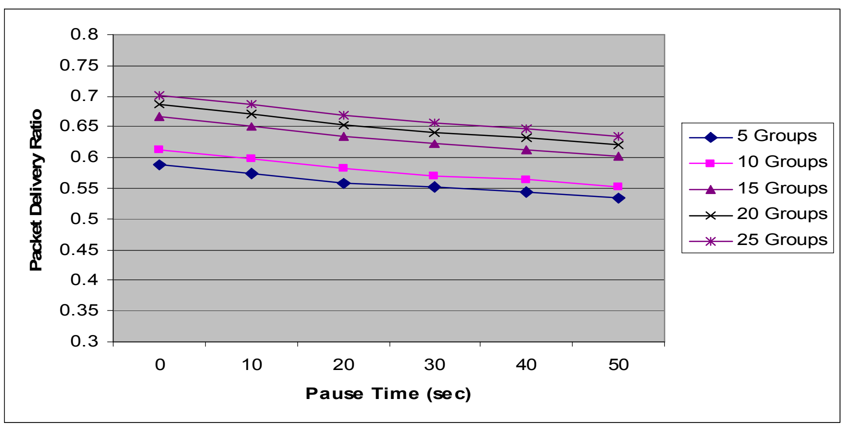


Figure 5.19. Packet Delivery Ratio for various number of pause time (sec), and the transition range is 310m.

	0	10	20	30	40	50
5 Groups	0.588	0.574	0.559	0.551	0.543	0.534
10 Groups	0.612	0.599	0.583	0.571	0.563	0.553
15 Groups	0.667	0.651	0.634	0.623	0.613	0.602
20 Groups	0.686	0.671	0.653	0.641	0.632	0.621
25 Groups	0.702	0.687	0.669	0.657	0.647	0.636

Table 5.22. Packet Delivery Ratio for various number of pause time (sec), and the transition range is 310m.

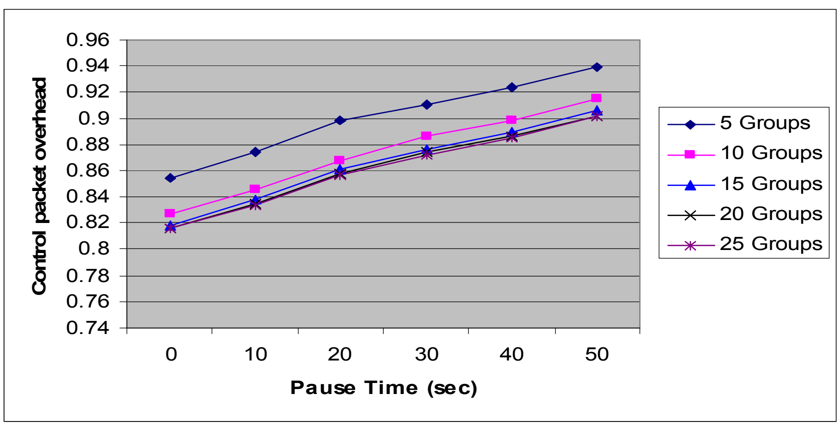


Figure 5.20. Control packet overhead for various number of pause time (sec), and the transition range is 310m.

	0	10	20	30	40	50
5 Groups	0.855	0.875	0.899	0.911	0.924	0.939
10 Groups	0.827	0.845	0.868	0.886	0.898	0.915
15 Groups	0.818	0.838	0.861	0.876	0.89	0.906
20 Groups	0.816	0.834	0.858	0.874	0.886	0.902
25 Groups	0.816	0.834	0.857	0.872	0.885	0.901

Table 5.23. Control packet overhead for various number of pause time (sec), and the transition range is 310m.

The control packet overhead decreases when the number of groups increases as shown in Figure 5.20 and Table 5.22. The NSMRP routing protocol constructs one mesh and uses the same control packets for all groups, and by increasing the number of groups the mesh and the control packets will be utilized by more groups, hence the number of control packets transmitted per data packet delivered will be decreased.

5.9.3 Conclusion

In this experiment the number of groups was varied from 5 to 25 and the pause time was varied from 0 sec to 50 sec to investigate the reliability and the scalability of the NSMRP routing protocol. The experiment was implemented using three different propagation ranges (250, 280, and 310 m). The results show that by increasing the number of groups the packet delivery ratio increases and the overhead decreases. As mobility speed increases with less pause time, the performance of NSMRP improves. NSMRP shows good performance under all scenarios, thus NSMRP is a reliable routing protocol.

5.10 Overall conclusion

This chapter studied the effect of mobility and the increase of the number of groups and senders on the reliability, scalability, and robustness of the Network Sender Multicast Routing Protocol in terms of the data packet delivery ratio, the control packet overhead, the efficiency in terms of the network channel access, and the total number of packet collisions. NSMRP was implemented and simulated by the GloMoSim simulator and compared to ODMRP. The simulation results show that NSMRP outperforms ODMRP by increasing the packet delivery ratio and reducing the control packet overhead as the number of senders, groups and the value of maximum speed increases.

The simulation results show that when the number of groups increases the data packet delivery ratio improved while the control packet overhead continues to decrease. The Network Sender Multicast Routing Protocol shows robustness to the number of groups and senders, and its performance even improves when the number of groups and senders is increased. Hence NSMRP is scalable and reliable.

Chapter 6

Conclusions and Future Work

6.1 Summary of findings

The main aim of this research has been to develop a new multicast routing protocol for mobile ad hoc networks using mesh topology to forward control and data packets between senders and receivers, to reduce overhead and collisions and to improve packet delivery ratio and scalability. In order to review the findings of this research, the main objectives of this study are reviewed in this section:

1. **Investigating the existing methods for routing protocols in mobile ad hoc networks.**

In chapter 2, the wireless networks and their major types are highlighted. The types of ad hoc networks are given with the challenges that face the design of an efficient routing protocol for MANET. The unicast routing methods are described, including the route construction based strategies (proactive routing strategies, reactive routing strategies, and Hybrid routing strategies), hierarchical routing strategies, position based methods, and routing by flooding. The types of proactive routing protocols are described, including event driven protocols and regular updated protocols. The types of reactive routing protocols are discussed, including the source routing method and the non source routing methods.

In chapter 3, multicast routing in mobile ad hoc networks is studied, and the most important issues that are needed to be considered while designing a routing protocol for mobile ad hoc networks are given. The classes of multicast routing methods are reviewed, including the location based category, the topology maintenance categories, and the session initialization categories. The topology and route information classes are discussed including the multicast table driven strategies and the multicast on demand strategies. The route construction based types are presented including the mesh based strategies, hybrid based strategies, stateless based strategies, and the tree based strategies (the source tree based multicast routing protocols and the shared tree based multicast routing protocols).

Each of these methods mentioned in chapter 2 and chapter 3 is discussed in detail by exploring their mechanisms, advantages and disadvantages with suitable examples.

In multicasting one copy of the message will be sent to all receivers, and thus control overhead and the limited bandwidth will be saved. Because of the characteristics of mobile ad hoc networks, multicast routing protocols outperform unicast routing protocols.

In reactive routing protocols the state information is collected only when it is needed, therefore reactive routing protocols show a better performance than proactive routing protocols in mobile ad hoc networks.

Due to redundant routes that the mesh provides, packets can have more than one route to a destination in case of link breaks because of mobility. Mesh routing protocols are more suitable for ad hoc networks than tree based routing protocols.

2. Addressing and determining the major problems and drawbacks of the existing multicast routing protocols in mobile ad hoc networks.

In chapter 3, multicast routing in mobile ad hoc networks is studied. The routing protocol design, characteristics, advantages, and disadvantages are investigated. A comparison between the best multicast routing protocols is given. As mentioned above, mesh, reactive, and multicast based routing protocols show a better performance than tree, proactive, and unicast based routing protocols. the ODMRP routing protocol is a mesh, reactive, and multicast based routing protocol, and studies show that ODMRP outperforms all other currently available protocols for multicast routing in mobile ad hoc networks. the ODMRP routing protocol suffers from overhead and scalability. As the number of groups or senders increases the networks performance degrades and the overhead increases and the packet delivery ratio decreases. Since none of the existing routing protocols is good in all situations, a new routing protocol for mobile ad hoc networks is needed.

3. Developing a novel multicast routing protocol for mobile ad hoc networks.

In chapter 4, a novel routing protocol for mobile ad hoc networks is presented. It is a mesh, reactive, and multicast-based routing protocol, and it is called the Network Sender Multicast Routing Protocol (NSMRP). In this protocol the groups' senders periodically re-elect one of them to be the next mesh sender (MS), by choosing the sender that is located in the most crowded area and closer to the centre of the network. The MS receives control and data packets from all senders that belong to all groups, and forwards it to the entire network.

In order to create the multicast mesh, the MS node periodically broadcasts a join request message to its near neighbours. The message comprises the identity of all the existing groups. Upon receiving a non duplicate join request packet, the intermediate node stores the packet and the upstream node address, which is considered as backward learning, and updates the packet by reassigning the following values (second upstream node address = first upstream node address ; first upstream node address = it's own address) , and forwards the packet. During a predetermined period of time if the node overhears a message with its own address assigned to the second upstream node address, it waits until a join reply packet is received; otherwise a join reply packet will be sent to its upstream node.

If any node receives a non duplicate join reply packet, it stores the packet and replies to its upstream node. Eventually, the join reply packet will reach the MS and the mesh will be created. Multicast receivers update a join reply packet by adding their own group(s) address(s) before the message is resent. In receiving the join reply packet, the upstream node stores in its memory the group(s) addresses in the join reply packet in order to forward the packets destined to the multicast group(s) in the future.

4. Implementing the developed multicast routing protocol.

In chapter 5, the Network Sender Multicast Routing Protocol is implemented and evaluated using GloMoSim simulator. The experiments were performed to determine the effects of changing the number of senders, number of groups, and the effects of changing the mobility speed on the performance of the routing protocol. The new protocol shows good performance under all situations.

5. **Comparing the developed multicast routing protocol with one of the competitive multicast routing protocols in mobile ad hoc networks.**

The ODMRP multicast routing protocol outperforms all other currently available protocols for multicast routing in mobile ad hoc networks. Therefore the Network Sender Multicast Routing Protocol is compared with ODMRP in chapter 5. The comparison was performed to determine the effects of increasing the mobility speed, the number of groups, and the number of senders on the NSMRP routing protocol and the ODMRP routing protocol, in terms of the Packet delivery ratio, Data packet overhead, Control packet overhead, the efficiency in terms of the network channel access, and total the number of packet collisions.

The results show that the proposed routing protocol outperforms the ODMRP routing protocol under all scenarios, by reducing the overhead and collisions and increasing the packet delivery ratio.

6.2 Summary of Research Contributions

Nodes in mobile ad hoc networks are free to move any where and at any time therefore the network topology changes continuously. Also in this type of network the bandwidth is limited and nodes rely on batteries. Due to the characteristics of mobile ad hoc networks, designing a scalable and efficient routing protocol is a difficult task for researchers. In summary this study has the following main contributions:

- Developing a novel multicast routing protocol for ad hoc networks it is named the Network Sender Multicast Routing Protocol. It is a mesh based routing protocol and uses the reactive technique in order to collect the route information.

- Building a simulation tool for mobile ad hoc networks by using C++ programming language and GloMoSim simulator, and by using this simulation tool the proposed protocol is evaluated and compared with the ODMRP routing protocol.

- Statistical evidence of the robustness of the proposed protocol is also provided.

6.3 Summary and Discussion of the Results

In order to investigate the proposed protocol performance, different scenarios are presented in chapter 5. In the following sections the experimental evidence and the results are summarized:

6.3.1 The effects of increasing the number of groups

In this experiment the number of groups is varied in order to investigate the protocol's performance with a different number of groups. The results show that by increasing the number of groups the packet delivery ratio increases for the proposed protocol and decreases for the ODMRP routing protocol. The data packet overhead, the routing overhead, the forwarding efficiency, and the number of packet collisions increases for ODMRP routing protocol and remains almost the same for the proposed routing protocol. Hence the new routing protocol outperforms the ODMRP routing protocol and it shows robustness to the number of groups.

6.3.2 The effects of mobility

In this experiment the effects of increasing the mobility speed is studied. The mobility speed is varied in order to investigate the protocols performance under different mobility speeds. The results show that in packet delivery ratio terms the proposed routing protocol outperforms ODMRP by 36%. By increasing the mobility speed the packet collision increases for the ODMRP routing protocol and remains the same for the proposed routing protocol. The proposed protocol outperforms ODMRP in the data packet overhead, the routing overhead, and the forwarding efficiency. Thus the proposed routing protocol is robust to mobility.

6.3.3 The effects of increasing the number of senders

In this experiment the number of senders is varied from 1 to 80 senders in order to investigate the protocol's scalability. The results show that by increasing the number of senders the packet delivery ratio increases for the proposed protocol and decreases for the ODMRP routing protocol. The data packet overhead, the routing overhead, the forwarding efficiency, and the number of packet collisions increases for the ODMRP routing protocol and remains almost the same for the proposed routing protocol. Thus the new routing protocol is scalable and it outperforms the ODMRP routing protocol.

6.3.4 The Reliability of Network Sender Multicast Routing Protocol

In this experiment the number of groups is varied under different pause times and different propagation ranges in order to investigate the protocol's reliability. The results show that by increasing the number of groups or the propagation range the packet delivery ratio increases. When mobility speed increases with less pause time, the proposed routing protocol shows a good performance, and the control overhead decreases when the number of groups increases. The proposed routing protocol's performance is enhanced when increasing the number of groups and the propagation range and when decreasing the pause time. Therefore the proposed routing protocol is a reliable routing protocol.

6.4 Applications of ad hoc networks

An Ad Hoc Network is a wireless mobile network which consists of a group of two or more wireless hosts that communicate as a team. This type of network has no fixed infrastructure support therefore each wireless node can function as a router. In this network hosts can move randomly, thus the network topology changes all of the time. Some of the many possible uses of ad hoc networks are the following:

- **Emergency disaster:** In situations such as earth quake, fire, and flood, the communication infrastructure will be destroyed and therefore it is very important to re-establish communication as quickly as possible. Using ad hoc networks in these situations can help save lives and money.

- **Class rooms and conferences:** Mobile ad hoc networks can allow students and researchers to exchange notes and information.

- **Battlefield:** In a battlefield environment nodes are free to move into and out of propagation range with each other and normally the nodes cannot depend on a fixed infrastructure. Therefore mobile ad hoc networks would be the most suitable network for this environment.

6.5 Future Work

In this section, the following points have been suggested as future work for enhancing the performance of the proposed routing protocol.

- The proposed routing protocol is evaluated by simulation. The evaluation with a real network will be more useful.

- The proposed routing protocol can be enhanced by enabling the use of the Global Positioning System (GPS) information when it is available.

References

Bajaj, L., Takai, M., Ahuja, R., Tang, K., Bagrodia, R. and Gerla, M. (1999). GloMoSim: A scalable network simulation environment, Technical Report 990027, Computer Science Department, University of California, Los Angeles, May.

Bommaiah, E., McAuley, A. and Talpade, R. (1999). AMRoute: ad hoc multicast routing protocol, Internet Draft, February. http://www.isi.edu/div7/yoid/otherProj/draft-talpade-manet-amroute-00.txt.

Boppana, R. V. and Konduru, S. (2001). An adaptive distance vector routing algorithm for mobile ad hoc networks. In Proceedings of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies, volume 3, pages 1753–1762.

Broch, J., Johnson, D. and Maltz, D. (2003). The dynamic source routing protocol for mobile ad hoc networks. Internet-Draft Version 08, IETF, February.

Bur, K. and Ersoy, C. (2004). Multicast Routing for Ad Hoc Networks with a Multiclass Scheme or Quality of Service, LNCS, ISCIS 2004, Antalya, October.

Chen, K. and Nahrstedt, K. (2002). Effective location-guided tree construction algorithms for small group multicast in MAET, IEEE INFOCOM, pp.1180–1189.

Christensen, L. and Hansen, G. (2001). The optimized link state routing protocol. Master's thesis, Department of Computer Science, Aalborg University, Fredrik Bajers Vej 7, 9220 Aalborg Ost.

Clausen, T. and Jacquet, P. (2003). Optimized Link State Routing Protocol, http://hipercom.inria.fr/olsr/rfc3626.txt, Internet Draft, IETF MANET Working Group, October.

Coleman, D. D. and Westcott, D. A. (2006). CWNA Certified Wireless Network Administrator Wiley Publishing, Inc. Indiana, USA.

Cordeiro, C. D. M., Gossain, H. and Agrawal, D. P. (2003). Multicast over Wireless Mobile Ad Hoc Networks: Present and Future Directions, IEEE Network, Vol.17, No.1, January.

Das, S. R., Perkins, C. E. and Royer, E. (2000). Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks, Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Tel Aviv, March, p. 3-12.

Dhillon, H. and Ngo, H. Q. (2005). CQMP: A Mesh-based Multicast Routing Protocol with consolidated Query Packets, in Proceedings of the IEEE Wireless Communications & Networking Conference (WCNC 2005), Mar 13-17, New Orleans, Louisiana, U.S.A.

Garcia-Luna-Aceves, J. and Madruga, E. (1999). The Core-Assisted Mesh Protocol, accepted for publication in IEEE Journal on Selected Areas in Communications, Special issue on Ad-Hoc Networks.

Garcia-Luna-Aceves, J., Spohn, M. and Beyer, D. (1999). Source tree adaptive routing (star) protocol. Internet Draft, draft-ietf-manet-star-00.txt, Oct.

Geier, J. (2002). Wireless Lans Implementing High Performance IEEE 802.11 Networks second edition, Sams Publishing, USA.

Gui, C. and Mohapatra, P. (2004). Scalable Multicasting in Mobile Ad Hoc Networks, INFOCOM 2004.

Haas, Z., Deng, J., Liang, B., Papadimitratos, P. and Sajama, S. (2002). Wireless ad hoc networks, in Encyclopedia of Telecommunications, John G. Proakis, Ed. Wiley.

Haas, Z., Pearlman, M. and Samar, P. (2002). The Zone Routing Protocol (ZRP) for Ad Hoc Networks, IETF Internet Draft: draft-ietf-manet-zone-zrp-04.txt, July.

Hong, X., Xu, K. and Gerla, M. (2002). Scalable Routing Protocols for Mobile Ad Hoc Networks, IEEE Network, special issue on Scalability in Communication Networks, July-Aug, pp. 11-21.

Iwata, A., Chiang, C., Pei, G., Gerla, M. and Chen, T. (1999). Scalable Routing Strategies for Ad Hoc Wireless Networks, IEEE J. Selected Areas in Comm., special issue on ad hoc networks, vol. 17, no. 8, pp. 1369-1379.

Jain, A. (1999). Routing Protocols For Mobile Ad-Hoc Networks, Report department of computer science and engineering, indian institute of technology, kanpur, http://citeseer.ist.psu.edu/348952.html.

Ji, L. and Corson, M. S. (2001). Differential destination multicast-a manet multicast routing protocol for small groups. In INFOCOM 2001, volume 2, pages 1192–1201, Anchorage, AK USA, Apr.

Johnson, D., Maltz, D. and Hu, Y. (2007). The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks, Internet Draft, at http://www.ietf.org/rfc/rfc4728.txt, February.

Ko, Y. and Vaidya, N. H. (2000). Location-Aided Routing (LAR) in Mobile Ad-Hoc Networks, IEEE/ACM Wireless Networks, Volume 6 , Issue 4, Pages: 307 321, July.

Kunz, T. and Cheng, E. (2002). On-demand multicasting in ad-hoc networks: comparing AODV and ODMRP. In Proc. of IEEE ICDCS, July.

Lang, D. (2003). A Comprehensive Overview about Selected Ad-Hoc Networking Routing Protocols. Technical Report. Department of Computer Science. Technische Universit¨at M¨unchen. March 14.

Lee, S., Gerla, M. and Chiang, C. C. (1999). On-Demand Multicast Routing Protocol, Proceedings of IEEE WCNC 1999, pp. 1298-1302, September.

Lee, S., Gerla, M. and Toh, C. (1999). A simulation study of tabledriven and on-demand routing protocols for mobile ad hoc networks. IEEE Network, 13:48–54.

Lee, S., Hsu, J., Hayashida, R., Gerla, M. and Bagrodia, R. (2003). Selecting a routing strategy for your ad hoc network. Computer Communications, 26(7):723--733.

Lee, S., Hsu, J., Hayashida, R., Gerla, M. and Bagrodia, R. (2003). Selecting a Routing Strategy for Your Ad-hoc Network, Computer Communications, Vol. 26, pp.723-733, Oct.

Lee, S., Su, W. and Gerla, M. (2002). On-demand multicast routing protocol in multihop wireless mobile networks, Mobile Networks and Applications, vol. 7, no. 6, pp,441 453, December.

Lee, S., Su, W., Hsu, J., Gerla, M. and Bagrodia, R. (2000). A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols, Proc. of IEEE INFOCOM'00, March.

Lewis, F. L. (2004). Wireless Sensor Networks, chapter 4 In Smart Environments: Technologies, Protocols, and Applications. John Wiley, New York.

Liu, B., Liu, Z. and Towsley, D. (2003). On the capacity of hybrid wireless networks, in Proceedings of the IEEE INFOCOM.

Mohan, P. M., Johnson, J. J., Murugan, K. and Ramachandran, V. (2002). A Comparative and Performance Study of On Demand Multicast Routing Protocols for Ad Hoc Networks, 9th International Conference on High Performance Computing (HiPC 2002) December 18-21, Bangalore, India.

Mohapatra, P. and Krishnamurthy, S. (2004). ad hoc networks technologies and protocols, Springer Science and Business Media, Inc. , USA.

Murthy, C. S. R. and Manoj, B. S. (2004). ad hoc wireless networks architecture and protocols, Pearson Education, Inc. new jersey, USA.

Murthy, S. and Garcia-Luna-Aceves, J. (1996). An Efficient Routing Protocol for Wireless Networks, ACM/Baltzer Mobile Networks and Applications, vol. 1, no. 2, Oct., pp. 183-197.

Nilsson, T. (2002). A Tutorial on GloMosim, Department of Computing Science. University of Umea, Jun.

Novatnack, J., Greenwald, L. and Arora, H. (2005). Evaluating ad hoc routing protocols with respect to quality of service, IEEE Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2005) . Montreal, Canada, August 22 - 24.

Nuaymi, L. (2007). WIMAX Technology for broadband wireless access John Wiley and Sons, Ltd France.

Perkins, C. and Bhagwat, P. (94). Highly dynamic Destination-Sequenced Distance Vector routing (DSDV) for mobile computers, In Proceedings of the SIGCOM'94 Conference on Communication Architectures, Protocols and Applications, Pages 234-244, August.

Perkins, C. E. and Royer, E. M. (1999). Ad-hoc On-Demand Distance Vector Routing, Proc. IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, Feb.

Perkins, C. E. and Royer, E. M. (2000). Multicast ad hoc on-demand distance vector (MAODV) Routing,. IETF Draft, July. http://www.ietf.org/proceedings/00dec/I-D/draft-ietf-manet-maodv-00.txt

Puthana, S. and Illendula, A. (2005). Multicasting Protocols for Ad-Hoc Wireless Networks: Study and Performance Comparison based on Simulation of Protocols in QualNet. www.eece.unm.edu/~wu/course/505f03/ adhocmulticast.ppt

Royer, E. and Perkins, C. E. (1999). 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, Aug. pages 207-218.

Schumacher, A., Painilainen, S. and Luh, T. (2004). Research Study of MANET Routing Protocols, Department of Computer Science University of Helsinki, Finland, Researh Seminar on Hot Topics in Internet Protocols - Spring 2004.

Sesay, S., Yang, Z. and He, J. (2004). A Survey on Mobile Ad Hoc Wireless Network, Information Technology Journal 3 (2): 168-175.

Shan, L. M., Lamarque, O. F. and Kwang, Y. Y. (2008). Evaluating MANET Routing Protocols with respect to Scalability using QualNet, Department of Computer Science, School of Computing, National University of Singapore, http://www.comp.nus.edu.sg/~cs4274/termpapers/0405-I/paper-4.pdf

Sharma, J., Shademan, B. and Train, J. (2002). Multicasting in AdHoc Networks, February 15, http://nile.usc.edu/ee499/josh-EE499Presentation.ppt.

Singh, H. (2000). SURVEY OF Ad-Hoc MULTICAST PROTOCOLS, DEC'7TH, web.cecs.pdx.edu/~harkirat/projects/AdhocMcast.pdf

Sobeih, A., Baraka, H. and Fahmy, A. (2004). On the Reliability of ODMRP in Mobile Ad Hoc Networks, Proceedings of the IEEE International Performance, Computing, and Communications Conference (IEEE IPCCC 2004), Phoenix, AZ, April.

Staub, T. (2004). Ad-hoc and Hybrid Networks, Computer Science Project, Computer Networks and Distributed Systems (RVS), Institute of Computer Science and Applied Mathematics (IAM), University of Berne, Switzerland Februar. www.iam.unibe.ch/~rvs/research/publications/projekt_thomas _staub.pdf

Viswanath, K. and Obraczka, K. (2002). An Adaptive Approach to Group Communications in Multi-Hop Ad Hoc Networks, in Proc. of International Conference on Networking.

Viswanath, K., Obraczka, K. and Tsudik, G. (2004). Exploring Mesh- and Tree Based Multicast Routing Protocols for MANETs, Transaction of Mobile Computing (TMC 2004).

Wu, C. W. and Tay, Y. C. (1999). AMRIS: A multicast protocol for ad hoc wireless networks, IEEE MILCOM, vol.1, pp.25–29.

Zhou, H. (2003). A Survey on Routing Protocols in MANETs, Technical Report: MSU-CSE-03-08.

Appendix A: List of Published Papers

The following are the published papers; these papers are part of the work of this study:

1. Khalid A. Farhan, "Network Sender Multicast Routing Protocol," *icn*, pp. 60-65, The Seventh International Conference on Networking (IEEE ICN 2008), Cancun, Mexico, 2008.

   http://www.IEEExplore.IEEE.org/xpl/freeabs_all.jsp?isnumber=4498126&arnumber=4498142&count=131&index=15

2. Khalid A. Farhan, "On the Scalability and Reliability of Network Sender Multicast Routing Protocol," The Fourth Advanced International Conference on Telecommunications, (IEEE AICT 2008), Athens, Greece, 2008.

   http://www.IEEExplore.IEEE.org/xpl/freeabs_all.jsp?isnumber=4545486&arnumber=4545525&count=86&index=38

Appendix B: The structure of the new simulation code

The following are the extensions to the flowcharts for the structure of the new simulation code which is introduced in chapter five (Figures 5.1 (a), 5.1 (b), and 5.1 (c)):

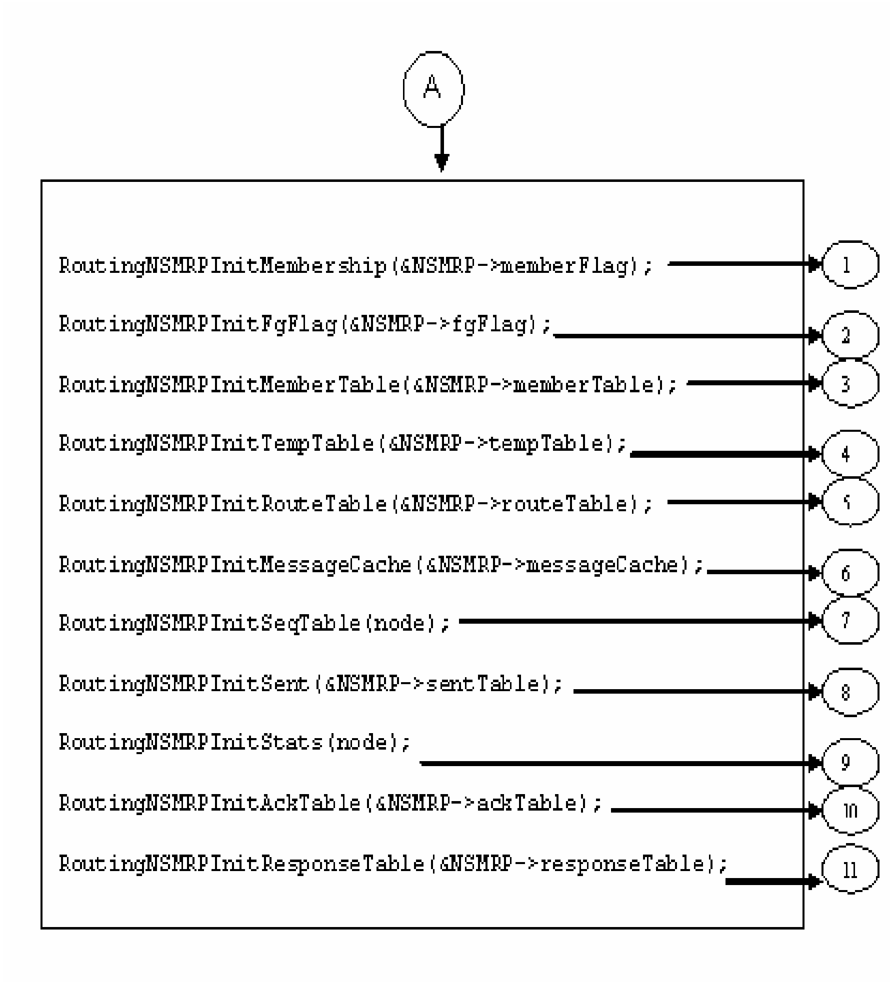


Figure B.1 Calling the network layer for initializing the nodes.

Figure B.2 illustrates the linked-list structure where each node can hold its own groups' addresses.

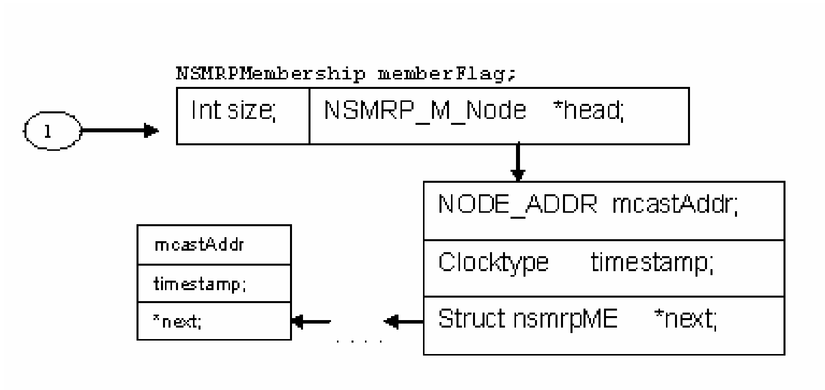


Figure B.2 The member flag linked-list structure.

Forwarding group members use the linked-list structure shown in Figure B.3 in order to maintain their groups' addresses.

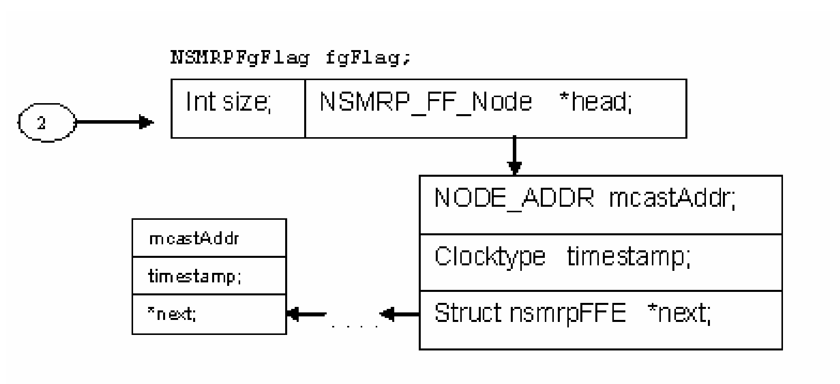


Figure B.3 The forwarding group linked-list structure.

Figure B.4 illustrates the linked-list structure where the sources' addresses of each multicast group are maintained.

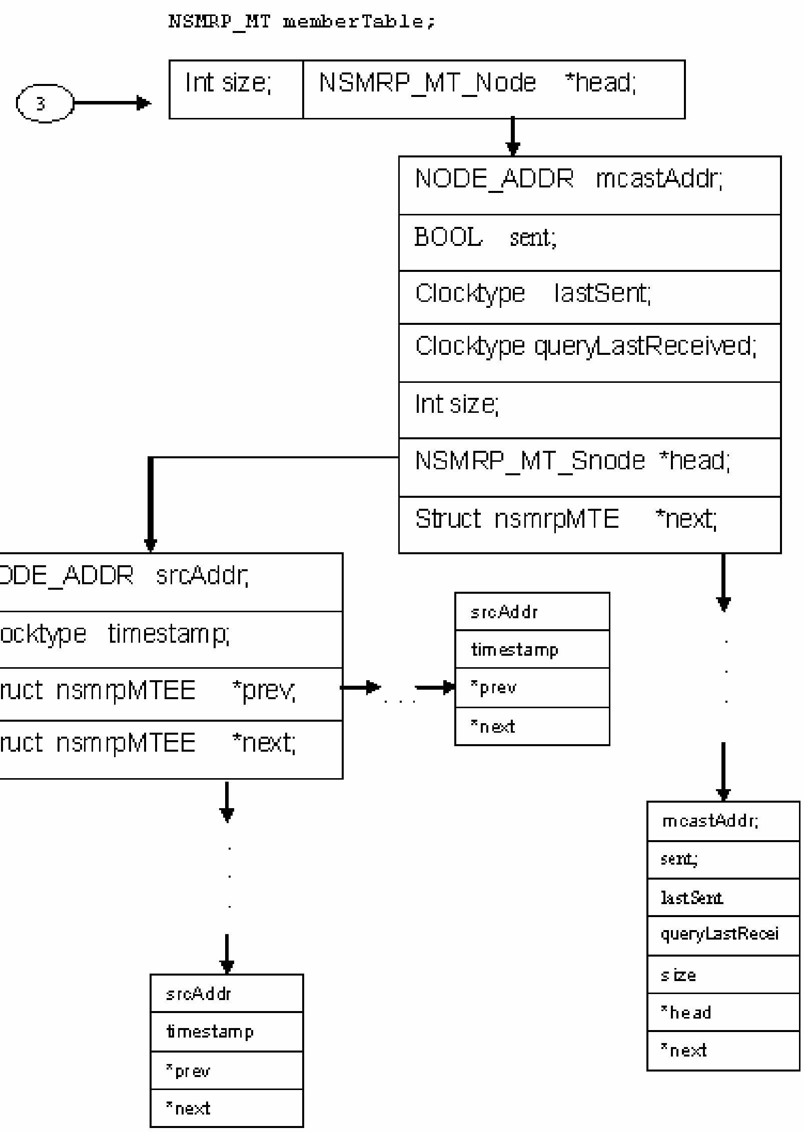


Figure B.4 The member table linked-list structure.

The linked-list structure shown in Figure B.5 is a temporary table that is used to build and hold the Join reply packets.

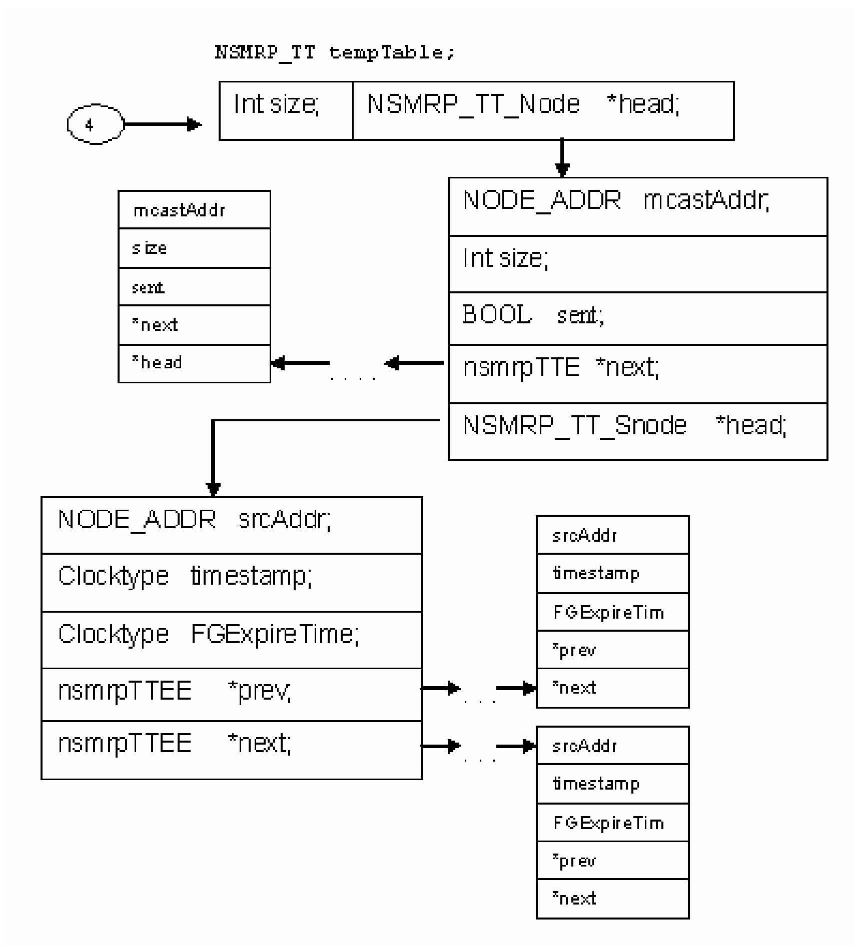


Figure B.5 The temporary table linked-list structure.

The linked-list structure shown in Figure B.6 is used to store the source address, the downstream node address, and the hop count in order to be used for routing the packets.

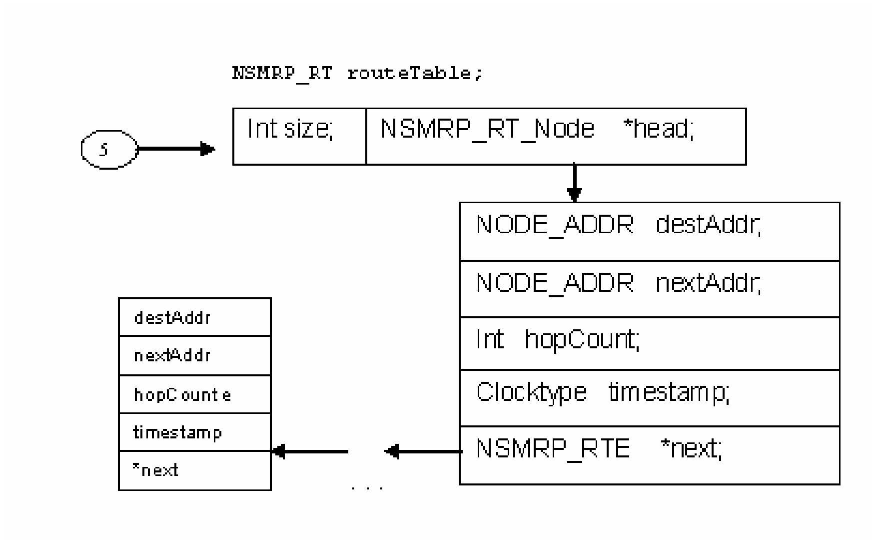


Figure B.6 The routing table linked-list structure.

In order to prevent unnecessary retransmission, each node maintains the linked-list structure shown in Figure B.7.

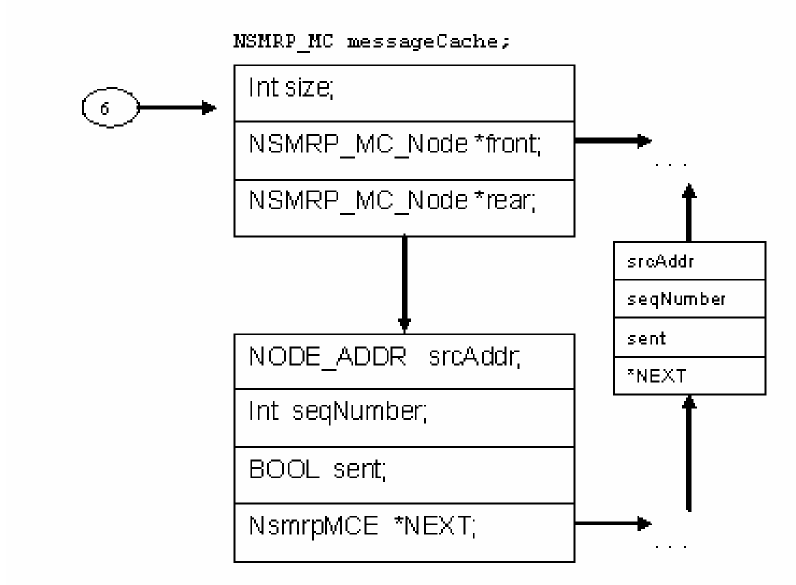


Figure B.7 The message cache linked-list structure.

The structure shown in Figure B.8 is used to hold the sequence number for each packet; this number enables the node to continue sending the data.

Figure B.8 The sequence table linked-list structure.

The linked-list structure shown in Figure B.9 is maintained by each source to build and forward the Join Query packets.

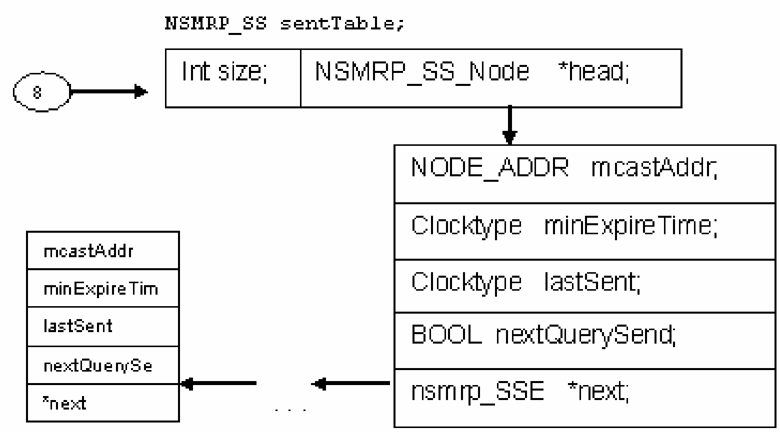


Figure B.9 The sent table linked-list structure.

The stats table linked-list structure shown in Figure B.10 is used to store the total number of join query txed, the total number of join reply packets sent, the total number of Acknowledgments sent, the total number of data packets sent by the source, the total number of data packets received by the destination, the total number of data packets should be received by the destination, and the total number of data packets transmitted by each node.

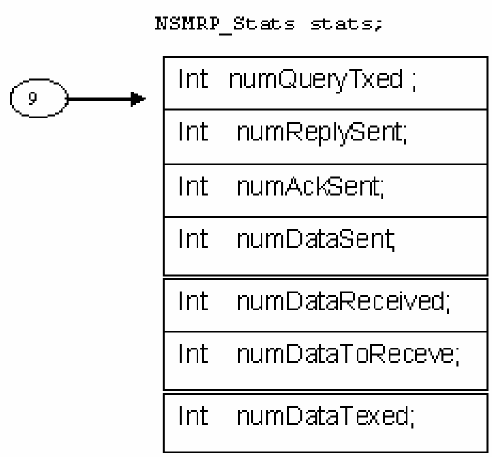


Figure B.10 The stats table linked-list structure.

The linked-list structure shown in Figure B.11 is used by the node to store the acknowledgments of its upstream node toward the source.

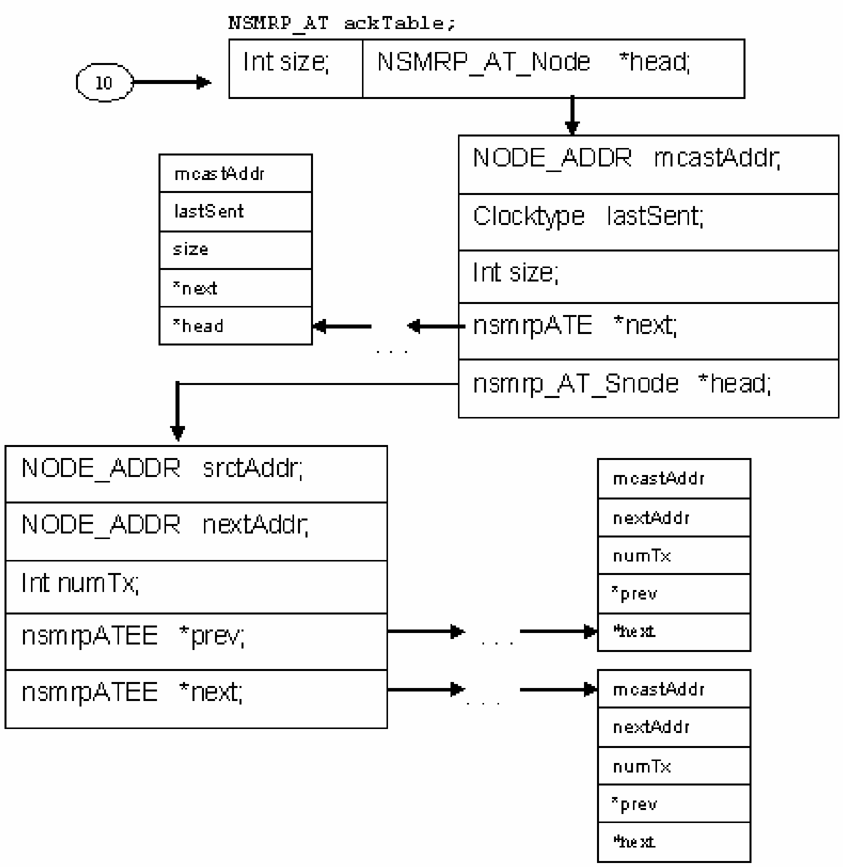


Figure B.11 The acknowledgment table linked-list structure.

The linked-list structure shown in Figure B.12 is used by the node to keep track of which source to reply.

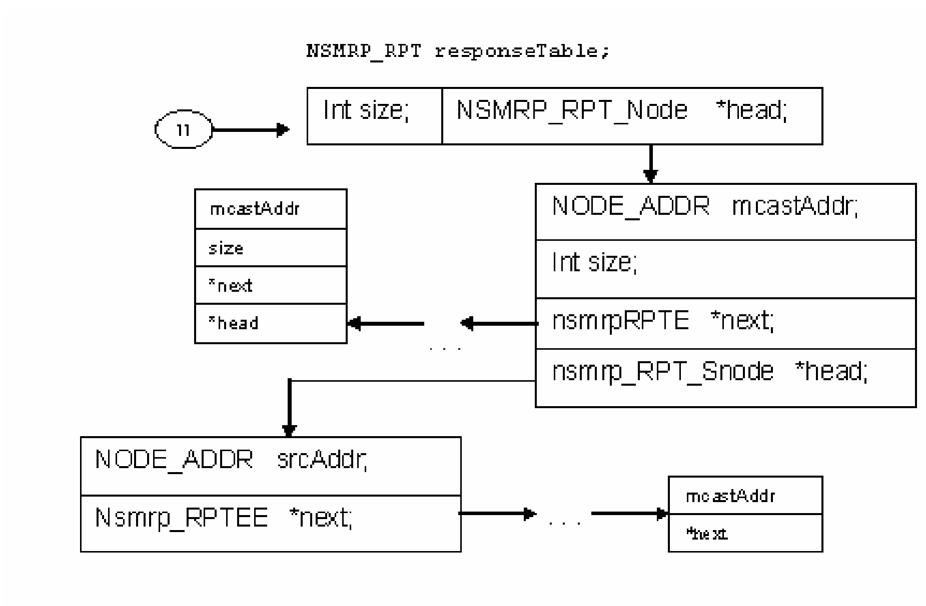


Figure B.12 The response table linked-list structure.

Figure B.13 and B.14 show the event that will be handled according to the received message.

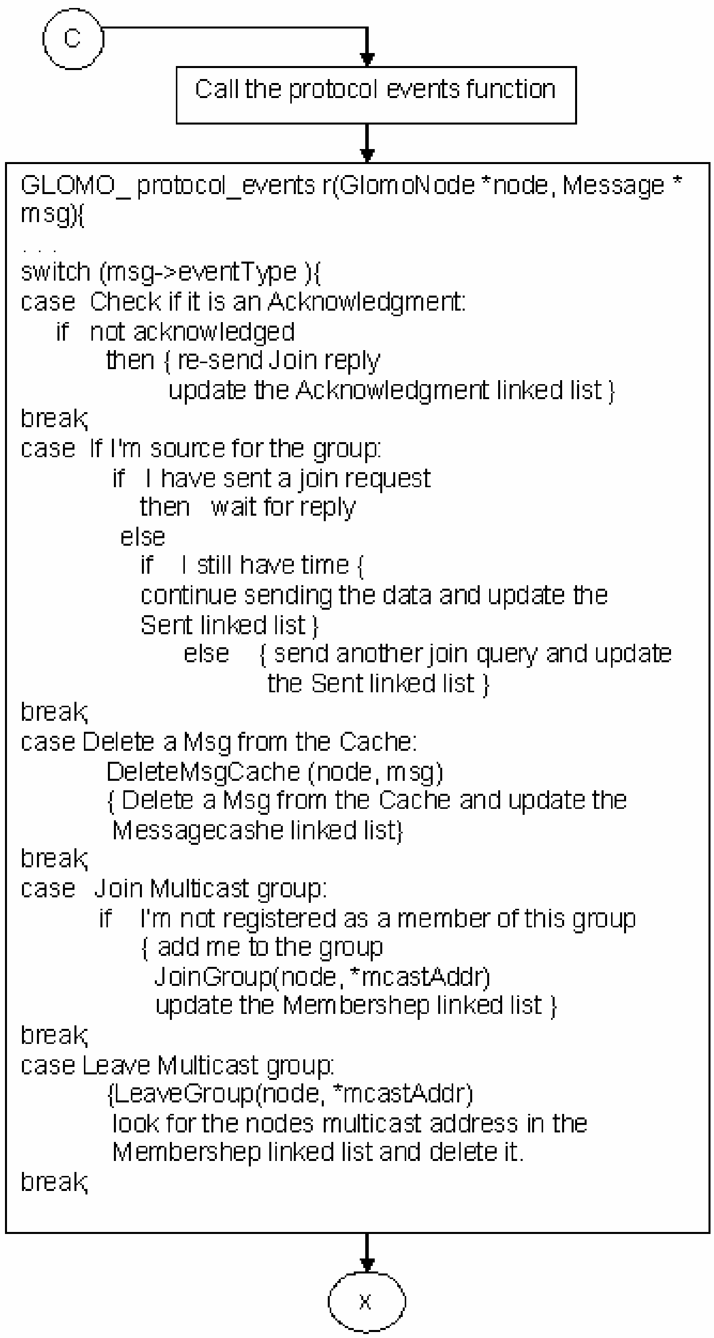


Figure B.13 Calling the network layer for the event handling.

X

```
case Send a Reply:
              { SendReply(node, *mcastAddr, &odmrp-
               >memberTable, &odmrp->tempTable)
               reply to my neighbours
               update the Acknowledgment linked list }
break;
case Check if Forwarding Group flag has been expired:
          if    I'm a Forwarding Group member
               if Forwarding Group expired
                then  {reset the flag
                         update the Forwarding Group linked list}
break;


}
. . .
}
```

Figure B.14 Calling the network layer for the event handling.

The finalizing function will be called to collect the final simulation results as shown in Figure B.15.

E

```
Call_Fainalize(GlomoNode *node, Message * msg){
. . .

Collect the results of the simulation from the stats linked
list:

Total number of join query Txed;
Total number of join reply packets sent;
Total number of Acknowledgments sent;
Total number of data packets sent by the source;
Total number of data packets received by the destination;
Total number of data packets should be received by the
destination;
Total number of data packets transmitted by each node;


. . .
}
```

Figure B.15 Calling the network layer for the finalizing.