PREDICTING THE SURVIVABILITY OF LINKS IN AN AD HOC NETWORK

LIM VIVI

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

JUNE 2006

PREDICTING THE SURVIVABILITY OF LINKS IN AN AD HOC NETWORK

LIM VIVI

DISSERTATION SUBMITTED IN PARTIAL FULFILMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF COMPUTER SCIENCE

FACULTY OF COMPUTER SCIENCE AND INFORMATION
TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

JUNE 2006

Abstract

Ad hoc networks are composed of a collection of self-configuring mobile routers that do not rely on any pre-existing network infrastructure. Nodes within an ad hoc network are expected to be able to route data-packets for other nodes in the network in a peer-level multi-hopping networks, constructing a interconnecting structure for the mobile nodes. Routing schemes that are adaptations of static network routing protocols do not perform well for the dynamic, infrastructure-less and self-operated environment of ad hoc networks. Therefore, ad hoc networks require a novel routing scheme that provides efficient and high throughput communication among mobile nodes. The ideal ad hoc network routing scheme must be scalable and able to cope with constantly changing topology that results from node mobility, conserve precious transmission power by reducing transmission overhead and avoid packet collisions. Routing protocols for ad hoc networks developed in existing researches are either table-driven (proactive) and demand-driven (reactive). We look into improving the performances of reactive protocols through caching and link survivability predictive strategies. Based on the On-Demand Multicast Routing Protocol (ODMRP), we enhanced the protocol to include route selection metrics that utilise delay time and hop count and implement and evaluate our modified protocol by comparing simulation results, using GloMoSim, with performance of the basic ODMRP (without enhancement). We proved that the modified protocol performs significantly better in Multicast traffic for most simulated scenarios and the performance is more consistent across the varied scenarios than the basic protocol. The modified protocol performs significantly better in Multicast traffic for most node speeds and Multicast group sizes. However, for Unicast traffic, the performance difference between the modified ODMRP and the basic ODMRP is insignificant for most node speeds.

Acknowledgement

I would like to extend my gratitude to my supervisor for this dissertation, Dr Mazliza Othman, for her invaluable advise, guidance and patience.

Thanks is extended as well to the many fellow researchers contributing to the MANET mailing list which often provide useful information.

Table of Contents

Abstract ii

Acknowledgement iii

Table of Contents iv

Table of Figures vi

List of Tables vii

Chapter 1 Introduction 1

1.1 What is an ad hoc network? 1

1.2 Motivation of this Project 3

1.3 Objectives of the Project 4

1.4 Significance of Project 5

1.5 Hypothesis Statement of Project 5

1.6 Dissertation Overview 6

Chapter 2 Literature Review 7

2.1 Introduction 7

2.2 Applications of Ad Hoc Networking 8

2.2.1 Original Motivations from Military Needs 8

2.2.2 Commercial Application 9

2.3 Mobility Models in Ad Hoc Network 11

2.3.1 Independent Mobility 12

2.3.2 Group Mobility 12

2.4 Survivability in Ad Hoc Wireless Network 14

2.5 Novel Routing Protocol 16

2.6 An Overview on ODMRP 17

2.7 Problems identified and how it can be addressed 20

Chapter 3 Design and Methodology 22

3.1 GloMoSim 22

3.2 Protocol Modification Approach 23
3.3 System and hardware Requirements 25
3.4 Methodology 28
3.4.1 Codes Modification 28
3.4.2 Simulation Environment 35
Chapter 4 Results and Discussion 37
4.1 Simulation Scenarios and Hypothesises 37
4.2 Unicast Traffic with Varying Mobility Speeds 39
4.3 Multicast Traffic with Varying Mobility Speeds 43
4.4 Multicast Traffic with Varying Multicast Group Sizes 46
4.5 Summary 49
Chapter 5 Conclusion and Suggestions 51
5.1 Summary of Project Findings 51
5.2 Significance of Findings 53
5.3 Concerns and Suggestions for future studies 55
5.3 Conclusion 57
Reference 58

Table of Figures

Figure 1.1 Node S communicates with node D over multi-hop paths 2
Figure 3.1 Process flow chart of basic ODRMP 26
Figure 3.2 Process flow chart of modified ODRMP 27
Figure 3.3 Modification of ODRMP_MC in odmrp.h 28
Figure 3.4 Modification to Insert Message Cache function 29
Figure 3.5 Modification to the Insert Message Cache function declaration 29
Figure 3.6 Additional Lookup Message Cache function in odmrp.pc 30
Figure 3.7 Additional Lookup Message Cache function declaration in odmrp.h 30
Figure 3.8 Modification of Handle Join Query Function 32
Figure 3.9 Modification of Check Route Exist Function 33
Figure 3.10 Modification of Check Route Exist declaration 33
Figure 3.11 Modification of Insert Route Table In Order Function 34
Figure 3.12 Abstract on fixed configuration file for all simulations 36
Figure 4.1 Packet Delivery Ratio over varying movement speeds 40
Figure 4.2 Packet Delivery Ratio over varying movement speeds for Multicast Group of 10 44
Figure 4.3 Packet Delivery Ratio over varying movement speeds 47

List of Tables

Table 4.1 Packet Delivery Ratios for Unicast Traffic with varying movement speeds ……………………………………………………………..……..40

Table 4.2 Z test results for Unicast Traffic for each varying node movement speeds ………………………………………………………………………….41

Table 4.3 Packet Delivery Ratios for Multicast Traffic of Basic ODMRP and modified ODMRP with varying movement speeds. 43

Table 4.4 Z test results for Multicast Traffic for each varying node movement speeds. 45

Table 4.5 Packet Delivery Ratios for Multicast Traffic with varying multicast group sizes.. 47

Table 4.6 Z test results for Multicast Traffic for each varying node movement speeds. 48

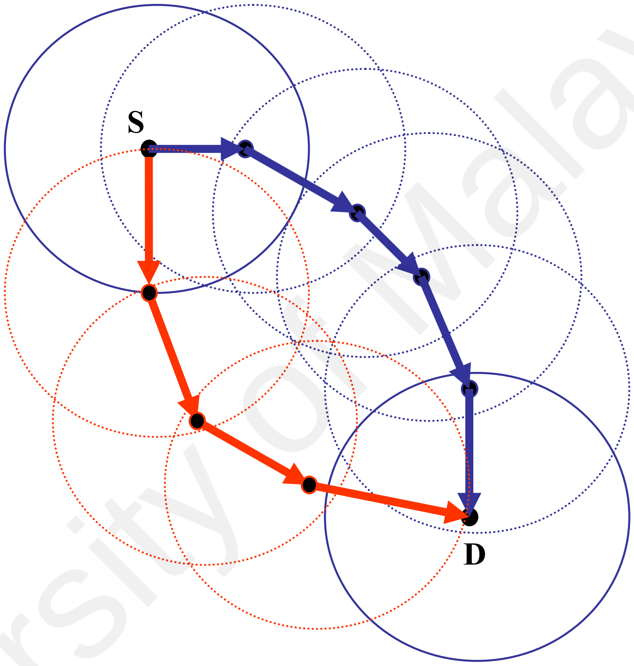
Chapter 1 Introduction

The world of communication has revolutionised in the past decade. Today, we take for granted our satellite television, our wired telephone or cellular telephone and the Internet. Millions of people world-wide use communication technology everyday to access, post and exchange information or interact with each other for social, academic or business activities. In the office or at home, users utilise the wired networks to get connected while the wireless cellular networks let users get connected while on the move. As recently as 10 years ago, the nearly instantaneous communication and connectivity that we experience today would not have been possible.

The computing technology evolved from the mainframes in the 1970s to the palmtops presently and in the future and we can expect even smaller and more powerful computers in our everyday devices. Inevitably, people expect the contemporary lifestyle of ubiquitous connectivity to prevail, whether they are at home, at work or on the move anywhere. Unfortunately, there are and will be situations or locations where communication infrastructures are not be available. In situations where the wired or cellular wireless network infrastructures are not available or are destroyed, mobile ad hoc networks are promising alternatives for some applications. Examples of such application are indoor and outdoor meetings/conferences, personal area networks (PANs), military and law enforcement activities, disaster relief and emergency rescue operations.

1.1 What is an ad hoc network?

Ad hoc is a Latin word that means “this purpose”. Mobile ad hoc networks (also known as MANET) are composed of a collection of self-configuring mobile routers, each equipped with a wireless transceiver that are free to move about arbitrarily without relying on any pre-existing network infrastructure. Nodes within an ad hoc network are expected to be able to route data-packets for other nodes in the network that want to reach other nodes beyond their own transmission range in what is known as peer-level multi-hopping. Peer level multi-hopping is the base for ad hoc networks in the construction of the interconnecting structure for the mobile nodes (Figure 1.1). An ad hoc network can be used to extend the coverage area of another existing network such as wired or wireless cellular networks, or it can be used independently in a standalone fashion.



Note: The large circle denotes the transmission range of each node.

Figure 1.1 Node **S** communicates with node **D** over multi-hop paths

An ad hoc network is attractive because it includes several advantages over traditional wireless networks, including: ease of deployment, speed of deployment, and independence on a fixed infrastructure. With the rapid advent of mobile telecommunications, personal digital assistants and embedded computing application in devices, ad hoc networking may also have potential for applications such as home networks, sensor networks and personal area networks (Rajaraman, 2002)

1.2 Motivation of this Project

Ad hoc network usually consist of nodes that are relatively mobile compared to a wired network. Therefore, the network topology is much more dynamic and the changes may be unpredictable. Since ad hoc wireless networks are formed spontaneously without any underlying infrastructure, a central administration does not exist. These facts, coupled with limitation of the different resources like bandwidth and battery power or energy constraints, make many challenging issues in researches for ad hoc network routing protocols. Ensuring fast and reliable communication in ad hoc wireless networks is a challenging task.

Ad hoc networks require a novel routing scheme that provides efficient and high throughput communication among mobile nodes. Routing schemes that are adaptations of static network routing protocols do not perform well for the dynamic, infrastructure-less and self-operated environment of ad hoc networks. The ideal ad hoc network routing scheme must be scalable and able to cope with constantly changing topology that results from node mobility. Moreover, since mobile nodes have limited power supply, the routing scheme has to conserve precious transmission power by reducing transmission overhead traffic. Network congestion and packet collisions must be avoided.

Routing protocols for ad hoc networks developed in existing researches are either table-driven (proactive) and demand-driven (reactive). In proactive protocols, routing information within the network is always known beforehand through continuous route updates. On the other hand, reactive protocols invoke route discovery on demand only. Proactive protocols consume large network capacity as continuous updates of large route tables are required while reactive protocols causes delivery delays as route discovery precedes actual data transmission. The performances of reactive protocols can be improved through caching strategies. However, both types of protocols suffer performance degradation with high node mobility.

The performance of these routing protocols can be improved through the prediction of link survivability as this will enable nodes to tell in advance which link will have a better chance of delivering the messages to the intended destinations through the possible multi hop paths that exist.

An experiment was successfully conducted by Lee, Su and Gerla (2001) where improvements to route selection criteria and reliability of transmission in ODMRP were proven through simulation. They predicted the link expiration time using the distance, movement directions and the movement speed information of two nodes obtained from Global Positioning System (GPS).

Utilising GPS, in our opinion, does not cater for a truly ad hoc wireless network as GPS may not be available in certain situations. Instead, we propose utilising information of total delays and hop numbers of a packet from source and destination. We expect that a path is a less attractive choice if it delivers a packet slower and has more intermediary nodes as the chances of link breakage is higher when more intermediary nodes are involved. We refrained from using signal strength information in our prediction method as we doubt that it is practical as standard signal strength measuring components may be needed which are not already available in mobile devices participating in an ad hoc network.

1.3 Objectives of the Project

In this project, we attempt to predict the survivability of links in wireless ad hoc networks using an adaptation of the On-Demand Multicast Routing Protocol (ODMRP) that maintains viable routes through caching and maintaining of route tables on each node. ODMRP is the routing protocol of choice for ad hoc wireless networks due to its simplicity and scalability (Lee, Su and Gerla, 2001). Moreover, ODMRP can support both multicast and unicast traffic without any underlying unicast protocol (Lee, Su and Gerla, 2001).

Our objective is to create a method of links survivability prediction that is easily adopted to help ensure faster and more reliable communication in ad hoc wireless networks without relying on other existing infrastructure or requiring additional hardware components to current mobile devices.

1.4 Significance of Project

This project offers an alternative way to predict link survivability that is based on total delay and as well as hop count. Using the routing protocol for ODMRP as a base, we modified this protocol to select a better link between nodes by allowing the protocol to select possible uplink routes that are based on delay and hop count instead of just minimum delay or link survivability through mobility prediction via GPS. This alternative method of link survivability prediction is easier to adopt as it does not rely on other existing infrastructure such as the GPS, or requiring additional hardware components to current mobile devices when utilising transmission power of nodes to predict the link survivability.

1.5 Hypothesis Statement of Project

The proposed modified ODMRP algorithm is expected to perform significantly better than the basic ODMRP protocol in terms of ratio of successful delivery of packets for:

- *Unicast Traffic as a function of node speed*
- *Multicast Traffic as a function of node speed*
- *Varying Multicast Single Group Sizes with constant node speed*

1.6 Dissertation Overview

The remainder of this dissertation is organised as follows. Chapter 2 provides an introduction to ad hoc network and its original military motivation and potential in commercial applications. A survey of the literature on the research interests in mobile ad hoc is also provided that covers the survivability, mobility of nodes and routing protocol. A brief overview of the routing protocol of interest i.e. On-Demand Multicast Routing Protocol (ODMRP) and an enhanced ODMRP version done by previous researchers is also presented. The chapter concludes with the problem that we identify and how it is addressed in this dissertation by introducing a modification of the ODMRP that uses hop count and delay information for route selection.

Chapter 3 depicts the design and methodology of this dissertation to address the identified problem. A concise description of the system specifications, software requirement and codes modifications followed by the simulation environment bring the chapter to a conclusion.

In Chapter 4, the simulation results are presented and discussed. Lastly, Chapter 5 concludes this whole dissertation by providing a summary of our research findings and set forth the future research direction in the area identified.

Chapter 2 Literature Review

2.1 Introduction

Mobile communication and wireless networking are gaining popularity, often in integration with traditional network infrastructures, such as intranets and the Internet. This type of wireless networking is dependent on base stations that monitor and administer mobile nodes. Although two mobile nodes are in transmission range of each other, they must still communicate via the base station to reach each other. This may be undesirable because precious transmission resources are not used optimally and dependency on static infrastructure hampers mobility of nodes instead of supporting it.

On the contrary, an ad hoc wireless network is not restrictive of mobility because it does not rely on any pre-existing communication infrastructure. Ad hoc wireless networks are composed of a collection of mobile routers, each equipped with a wireless transceiver and they are free to move about arbitrarily. Nodes rely on each other to keep the network connected. Applications of ad hoc networks include military tactical communication, emergency relief operations, commercial and educational use in remote areas, outdoor/open area activities, meetings, conferences such as in youth camps, police and traffic operations. Ad hoc wireless network has generated increasing interest among researchers.

Ad hoc wireless networks are convenient infrastructure-free communication that seem to be very promising alternatives for some applications. However, the absence of a centralised administration makes it a challenging task to ensure fast and reliable communication in ad hoc wireless networks. Moreover, as the nodes in ad hoc networks are mobile, network topology changes may occur frequently, further complicating the challenge. Therefore, ensuring fast and reliable communication in ad hoc wireless networks rightfully becomes an area where much research is ongoing.

The objective of this project, the interest is to study and predict the survivability of links in ad hoc wireless networks. A link between two wireless nodes is the wireless channel that they use to communicate with each other while paths are a collection of links that connects a source to a destination that may otherwise be beyond each others' transmission range. Link survivability in ad hoc networks is an important issue as a proper predictive strategy will assist in providing a network specification that will help to support effective communication in a dynamic network such as ad hoc wireless networks (Paul et. al.., 2000).

2.2 Applications of Ad Hoc Networking

In this section, we present the original motivations of ad hoc networks and its potential commercial applications.

2.2.1 Original Motivations from Military Needs

Ad-hoc networks evolved largely from the DARPA packet-radio network (PRNET) and related systems and were developed to support the tactical requirements of advanced weapons and command and control systems. The major attractions of the PR network architecture were rapid deployability and improved survivability, since there is no infrastructure that could be destroyed. Perkins (2000) stated several motivations of ad hoc networking that were derived from military needs. The military needed an ad hoc network with high survivability whereby mobile communication systems required for coordinating military group actions can operate in a distributed manner and avoid any single point of failure.

An additional motivation is the need of a rapidly deployed, self-organising mobile infrastructure that do not rely on any fixed infrastructure. This need arises when military actions are in regions with no terrestrial communication infrastructure, such as in the dessert and jungles or when all local communication infrastructure has been destroyed.

The third motivation is derived from situations where terrain, foliage and man-made structures obstruct electromagnetic propagation beyond the line of sight (LOS). A multi-hop protocol is required to allow communications between nodes that are not in the LOS of each other.

However, since the 1980s few advances were made largely due to the cost and limitations of available hardware, and a lack of sufficient unlicensed radio spectrum. Advances in transmission systems, microprocessor technology and power efficient portable communications devices have lead to a re-emergence of interest in PR **networks**. In particular, the Department of Defense (DoD) continues to pursue a research agenda which is aggressively investigating the possibility of evolving **ad-hoc** network technology to support the military's mobile communications needs.

2.2.2 Commercial Application

Herzog (2005) provided an overview of several application areas for ad-hoc networks:

Personal Area Networks (PANs) are formed between various mobile (and immobile) devices mainly in an ad-hoc manner, e.g. for creating a home network. They can remain an autonomous network, interconnecting various devices at home, for example, but PANs will become more meaningful when connected to a larger network. In this case, PANs can be seen as an extension of the telecom network or Internet. Closely related to this is the concept of **ubiquitous / pervasive computing** where people, noticeable or transparently will be in close and dynamic interaction with devices in their surrounding.

Sensor networks can be used for environmental monitoring. They can be used to collect various types of data, e.g. temperature, humidity, and vibration. Applications are the measurement of ground humidity for agriculture, forecast of earthquakes, or monitoring the progress of bushfires.

Ad-hoc networks formed by users near a hotspot could **extend that hotspot's coverage**. Hotspot coverage is often limited in densely built areas. Their extension would enable other users to get access even if they are not in direct reach. Going a step further, other systems, for instance UMTS cells, could be extended beyond their range. This idea is not that absurd if one remembers the numerous white spots (small areas with no reception) on the GSM coverage maps still existing today. A crucial prerequisite for this, however, is the availability of suitable authentication, accounting, and charging mechanisms to ensure revenues for operators.

Automotive networks are widely discussed currently. Cars should be enabled to talk to the road, to traffic lights, and to each other, forming ad-hoc networks of various sizes. The network will provide the drivers with information about road conditions, congestions, and accident-ahead warnings, helping to optimise traffic flow.

Herzog (2005) went on to conclude in his article that ad-hoc networks have the potential to become a serious part of tomorrow's 4G communications networks and they can open up new business opportunities for network operators and service providers.

2.3 Mobility Models in Ad Hoc Network

Simulation is an important method for evaluating characteristics of ad hoc networking protocols. As there are no fixed infrastructures, ad hoc networks are not associated with any fixed topologies. On the other hand, topology changes may be rampant, implicated by mobility of nodes. In order to study the robustness of routing protocols and topology control protocols, simulation studies need to analyse situations in ad hoc wireless applications through different mobility models.

Topology changes of wireless ad hoc networks occur largely with node mobility and they are key factors that impact the performance of the network protocol under simulation. Since mobility models are commonly used to analyse newly designed systems and protocols in wireless networks (Hong, Gerla, Pei and Chiang, 1999; Jardosh et. al. 2003), a realistic model is essential. Simulation results obtained with unrealistic movement models may not correctly reflect the true performance of the protocol being evaluated, leading to invalid conclusions (Hong, Gerla, Pei and Chiang, 1999; Nettstetter, 2001; Jardosh, et. al. 2003) and subsequently, failure of the new wireless ad hoc network strategies in implementation.

Bettstetter (2001) surveyed existing mobility models for wireless networks and categorised the degree of randomness of the different approaches into three:

models that allow users to move anywhere in the system pane following pseudo-random process for speed and direction;
models that bound the movement of users to streets, buildings, etc. but uses a pseudo-random process for speed and direction choices at crossings;
models that bound the movement of users to a predefined path.

Basically, there are two approaches to modelling mobility in ad hoc networks, i.e. random mobility models where each node moves independently and group mobility models where groups of nodes move in a similar pattern in relation to each other (Hong, Gerla, Pei and Chiang, 1999; Nettstetter, 2001).

2.3.1 Independent Mobility

The movement of each node is modelled independently of any other nodes in the simulation of independent models. Most researchers use random mobility models where the speed and direction of motion in a new time interval has no relation to their past values. This includes Random Walk and Random Waypoint. These models can generate unrealistic mobile behaviours such as sharp turning or sudden stopping/drastic change of speed (Hong, Gerla, Pei and Chiang, 1999). The Smooth Random Mobility Model (Nettstetter, 2001) includes autocorrelation feature for both speed and direction changes so that speed changes are incremental from current states and any direction changes are smooth. Other researchers take into account previous motion behaviour in the current movement in speed and/or direction, such as Markov Mobility Model and Random Gauss-Markov Mobility Model.

2.3.2 Group Mobility

In group mobility models, there exists some relationship among mobile nodes and their movement. Group mobility models are less well studied compared to the independent models. The simplest of this example is the Fluid Flow mobility model where the motion of the mobile nodes is modelled as a set of constant velocity fluid flow equation. Other models that are more intuitive than mathematical are Column, Pursue and Nomadic Group. These mobility models are more realistic because in real-life application scenarios, mobile users are often involved in team activities and exhibit collaborative mobility behaviour (Wang and Li, 2003).

Hong et. al. (1999) introduced the Reference Point Group Mobility (RPGM) model where a network is partitioned into several teams/groups as each team member shares a common mobility behaviour (location, speed, direction and acceleration) in association with a logical center. This model allows independent random motion for each node in addition to the group motion. The group motion is defined for a group explicitly by assigning a motion path to each group. The motion path will follow a defined sequence of check points along the path corresponding to given time intervals. Each time a group center reaches a new check point in its path, a new motion vector is computed from the current point to the next check point. By proper selection of check points, many realistic situations can be modelled, providing a flexible framework to describe many mobility patterns. Hong, et. al. (1999) also illustrated several representative cases with RPGM model, i.e. In-Place Mobility Model, Overlap Mobility Model and Convention Mobility Model.

Wang and Li (2003) extended the RPGM model by adding a group velocity representation for each mobility group and named the model Reference Velocity Group Mobility (RVGM) Model. In this model, members of a group have velocities close to the group velocity, i.e. the group velocity is also the mean group velocity. By integrating the group velocity with the local velocity deviation of a mobile node, the reference point representation from the velocity representation is derived. The advantages include a direct generation of mobility parameters of each group and the variance in the node in each group; provides a clearer characterisation of the mobility groups and enable prediction of eventual network partitioning by determining the node velocity and velocity distribution in the groups. Wang and Li (2003) further argued that the prediction of network partitioning and when it will happen will allow the ad hoc network to act in advance to minimise service disruption and improve efficiency and performance of mission critical services in the ad hoc network.

These models are difficult to work with. Moreover, mobility models are application dependent (Hong, Gerla, Pei and Chiang, 1999). Clearly, mobility patterns would differ from application to application. Apart from that, it is also difficult to determine the accuracy of a certain simulation reflecting a real live ad hoc wireless network situation as there is no standard way of assessment of survivability of an ad hoc network. We have been unable to find any prior work that measures movements of users in a real world scenario or any work related in stimulating a live scenario to measure mobile nodes motion. Most mobility models are difficult and complicated to work with and the accuracy of these models in simulation depicting a live situation is also unknown.

2.4 Survivability in Ad Hoc Wireless Network

More attention is required to study the survivability issues in order to provide a network specification to support effective communication in such a dynamic environment (Paul et. al., 2000). Network survivability is important for reliable communication services. Essentially, the major goals of a survivable network is to establish and maintain a connected network (Sterbenz et. al., 2002) and assuring that the connection is uninterrupted until a finite volume of data transfer has been accomplished (Paul et. al., 2000).

Survivability in network system is defined as the capacity of a system to fulfil its mission, in a timely manner, in the presence of failures and attacks (Paul et. al.., 2000; Sterbenz et. al., 2002). Survivability in an ad hoc wireless network is far more challenging than other infrastructure-based (wired or wireless) networks because of the following reasons (Sterbenz et. al., 2002; Zhou and Haas, 2003):

High susceptibility to link attacks, ranging from passive to active attacks. These attacks may introduce adversary access to secret information, violating the confidentiality or may allow adversary message deletion, injection or modification of fictitious messages and impersonation of a node, thus violating availability, integrity, authentication and non-repudiation.

Higher probability of compromised nodes. Understandably, being mobile with relatively poor physical protection, the chances of a node being compromised is nonnegligible. As such, a distributed, decentralised architecture is important to reduce this vulnerability.

Harsher communication environment. Issues that affect this communication medium include rapid attenuation with distance, multipath fading, weather effects and terrain obstructions.

Frequent changes in network topology and its memberships. Nodes are allowed to move and join or leave the network at will. These changes have to be adapted on-the-fly with the appropriate security mechanism and network protocol.

Scalability. Ad hoc wireless networks should be able to handle from a few nodes up to hundreds or thousands on nodes using the same protocol.

All the issues above play significant roles in the survivability of ad hoc wireless networks. However, we only concentrate on the last three related issues that result in system dynamisms of ad hoc wireless networks due to the constant changing of topology of wireless ad hoc networks. We are interested in improving the physical wireless connectivity amongst mobile nodes to ensure faster and more reliable communication in ad hoc networks. Vulnerability to security attacks (first two issues above), although is of significant importance, falls beyond the scope of this current project. To secure an ad hoc wireless network from adverse attacks, attributes such as availability, confidentiality, integrity and authentication has to be maintained. Techniques like authentication protocols, data encryption and digital signature are commonly employed to secure networks. As it is apparent, security issues in wireless ad hoc networks are quite complicated and require separate in-depth studies and are not addressed here.

To ensure better survivability of ad hoc wireless networks and the fulfilment of a specified quality of service level, it will useful to be able to predict the survivability of links, as this will enable nodes to tell in advance which paths/links will have better chances of delivering the messages to the intended destinations.

2.5 Novel Routing Protocol

Ad hoc wireless networks require a novel routing scheme that provides efficient and high throughput communication among their mobile nodes. Intermediary nodes in ad hoc wireless networks act as routers in forwarding packets from sender to receiver nodes which may otherwise be beyond the wireless transmission range of each other. Routing schemes that are adaptations of static network routing protocols do not perform well for ad hoc wireless networks. Furthermore, factors such as node mobility, wireless transmission range limitation and interference as well as changes in the wireless propagation environment further implicate the routing problem within such networks (Hu and Johnsons, 2002). The ideal ad hoc wireless network routing scheme must be scalable and be able to cope with constantly changing topology (triggered by node mobility). It will also need to conserve precious transmission power by reducing overhead traffic. Network congestion and packet collisions must be avoided.

Much of the recent studies concentrate on developing a routing framework for IP-based protocols in ad hoc networks which can generally be categorised to 2 classes: table-driven (proactive) and demand-driven (reactive) (Lou and Fang, 2002). Proactive routing algorithms maintain routes and when a packet is to be transmitted, the route to a certain destination is simply picked from the cache. Although packets can be transmitted instantly, nodes have to work hard in the background to maintain route tables, which would likely be large, wasting precious resources. On the other hand, reactive routing algorithms try to evolve the route to a destination only when there is a need to transmit a data packet to that destination. These algorithms use precious resources more efficiently, but the route discovery phase usually precedes an actual send phase, the transmission of the first packet may take a relatively longer time.

However, both types of protocols suffer performance degradation with high node mobility. Route updates and route discovery overheads may become too high if topology changes are great. Route computational delays may be too long whilst in the meantime intermediate nodes may have moved out of transmission range. Even reactive algorithms that utilises route caching to minimise delays are inefficient if mobility of nodes are high. Therefore, the ideal routing protocol must be scalable to support any ad hoc wireless networking environment, from small networks with low mobility to large networks with high mobility (Rajan, 2000). Furthermore, as mobile nodes often carry out tasks in groups in most ad hoc wireless environment (Lee, Su and Gerla, 2001), the protocol should support multicasting in addition to unicasting.

One protocol that is simple, scalable and supports both unicast and multicast traffic without any underlying additional protocol is On-Demand Multicast Routing Protocol (ODMRP) (Lee, Su and Gerla, 2001).

2.6 An Overview on ODMRP

ODMRP establishes and maintains group membership and multicast routes by the source on demand. When a source has a multicast packet to send, it periodically broadcast its JOIN TABLE packet to all its neighbours. When a node receives a non-duplicate JOIN REQUEST, the upstream node address is stored in its route table and the packet is rebroadcast. When the JOIN REQUEST packet reaches a multicast receiver, the source entry is created or updated into its Member Table. The receiver periodically broadcast JOIN TABLE packets as long as there are valid entries in the Member Table. When a node receives a JOIN TABLE packet, it checks if the next node address of one of the entries matches its own. If so, it sets the FG_FLAG and broadcast its own JOIN TABLE. This repeats until the JOIN TABLE packet reaches the source. In this way, routes from sources to receivers are constructed as a mesh of nodes called the forwarding group (Lee, Su and Gerla, 2001). The advantage of maintaining forwarding groups is that it improves connectivity by providing flooding redundancy and it requires less frequent reconfigurations.

ODMRP requires periodic flooding of JOIN REQUESTS to build and refresh route. Route selections are based on minimum delays (i.e. the route taken by the first received

JOIN REQUEST). However, excessive flooding will degrade network performance causing wastage, congestion and collision. Lee, Su and Gerla (2001) suggested a scheme that adapts route refresh intervals to mobility patterns and speeds. They utilised information on node location and mobility obtained through Global Positioning System (GPS) to predict the duration of time two nodes will remain connected, $D_{t.}$

Assume two nodes *i* and *j* are within the transmission range *r* of each other. Let (x_i, y_i) and (x_j, y_j) be the coordinates of nodes *i* and *j* respectively. Also let v_i and v_j be the speeds, and θ_i and θj $\left(0 \le \theta_i, \theta_j < 2\pi\right)$ be the moving directions of the nodes *i* and *j* respectively. D_t is predicted using the calculation below:

$$D_t = \frac{-\left(ab + cd\right) + \sqrt{\left(a^2 + c^2\right)r^2 - \left(ad - bc\right)^2}}{a^2 + c^2}$$

where

$a = v_i \cos\theta_i - v_j \cos\theta_j$,

$b = x_i - x_j$,

$c = v_i \sin\theta_i - v_j \sin\theta_j$ and

$d = y_i - y_j$

When a source sends JOIN REQUESTS, it appends its location, speed and direction and set the Minimum Link Expiration Time (MIN_LET) value to MAX_MIN_LET as there is no previous hop node. The next hop neighbour, which receives the JOIN REQUEST, predicts the link expiration time between itself and the previous node. This value is compared to the previous MIN_LET and the minimum of them will be used as the MIN_LET value of the JOIN REQUEST because a path is as stable as its weakest link as a break in any single link will invalidate the entire path. The location and mobility information of the JOIN REQUEST is also overwritten with the current node information before it is re-broadcasted.

When a multicast receiver receives the JOIN REQUEST, it predicts LET of the last link. The minimum between the predicted LET and the MIN_LET value in the JOIN REQUEST it receives is set as the Route Expiration Time (RET) value. The receiver waits for an appropriate period from the first JOIN REQUEST it receives so that it will know several/all possible routes. It then selects the most stable path with the largest RET value which is attached to the JOIN TABLE before it is broadcast.

When a forwarding group node receives multiple JOIN TABLES with different RET values belonging to different paths from the same source to multiple receivers, the minimum RET is selected and attached to its own JOIN TABLE before it is broadcast. The source, upon receiving the JOIN TABLES, selects the minimum RET value and JOIN REQUEST is re-broadcast to build new routes before the minimum RET approaches.

However, routes refresh intervals need to be adjusted to avoid too many or too few JOIN REQUESTS sent by the source. If JOIN REQUESTS are propagated too excessively because of high node mobility rate and topology changes, network collision and congestion may degrade network performance. On the other hand, if JOIN REQUESTS are rarely re-broadcast because of very little change in topology, any sudden changes in speed and direction of intermediary nodes will not be reflected in the RET value, or when a new node wants to join the multicast group, it cannot do so until the next JOIN REQUEST. Hence, to avoid these conditions, Lee, Su and Gerla (2001) suggested to include a MIN_REFRESH_INTERVAL and a MAX_REFRESH_INTERVAL parameters that are adaptive to different network situations to ensure better network survivability. An alternative method using transmission power measurements was also suggested by Lee, Su and Gerla (2001) for mobility prediction usage in the absence of GPS.

2.7 Problems identified and how it can be addressed

Utilising GPS, in our opinion, does not cater for a truly ad hoc wireless network. GPS may be unavailable for reasons such as damage, physical barriers or simply, beyond the coverage area of existing satellite systems.

Despite what is suggested by Lee, Su and Gerla (2001), we deliberately refrain from using signal strength information in our prediction method as we are doubtful that current mobile devices are equipped with signal strength measurement capacity. Even if they do, it will also be unlikely that the measurements made will be comparable across different devices of different manufacturers. Therefore, we feel that the practicality of such a method is quite low.

In summary, our objective is to create a method of links survivability prediction that is easily adopted to help ensure faster and more reliable communication in ad hoc wireless networks without relying on other existing infrastructure or requiring additional hardware components to current mobile devices. We intend to create a standard and universal technique of choosing the best links to form a reliable route by predicting links survivability in ad hoc wireless networks without relying on any underlying system.

Instead of predicting link expiration time by calculating the distance, movement directions and the movement speeds of two nodes which depends on information obtained from GPS, our approach is based on delays and hop numbers when a packet is sent from node to node. The node predicts reliability of each upstream link by comparing the hop count the packet has travelled and the time it took to reach it. The rationale is that if a certain path delivers a packet slower compared to another, it is clearly a less attractive choice of path. At the same time, if a path consists of more intermediary nodes (or hops) than another, it will also be a less attractive choice as the chances of link break is higher as any intermediary nodes may move out of range or fail to assist in forwarding packets for one reason or another.

In Chapter 3, we explain how we modify the routing protocol for the existing ODMRP and simulate both original and modified protocol using a network simulator program.

Chapter 3 Design and Methodology

In order to enable each node to predict the reliability of each upstream link by comparing the hop count the packet travels and the time it takes to reach its destination, several adaptations have to be performed on the original ODMRP that is specified in Lee, Su and Gerla (2000). This version of ODMRP is chosen as the base to modify and to compare against as it is the version distributed with the open source simulation program (Glomosim, distribution 2.03) that we utilise to test our protocol.

3.1 GloMoSim

GloMoSim is a scalable simulation environment for wireless and wired network systems designed using the parallel discrete-event simulation capability provided by Parsec. GloMoSim was designed using a layered approach that is similar to the OSI seven layer network architecture. The protocol stack in Glomosim includes models for the channel, radio, MAC, network, transport, and higher layers. Standard APIs are used between the different simulations layers, allowing rapid integration of models developed at different layers by different people.

A simple approach to designing a network simulation would be to initialize each network node in the simulation as a Parsec entity. However, each entity initialization requires its own stack space in the runtime. This greatly affects the scalability of the network simulation as instantiating an entity for each node in runtime will increase the memory requirements dramatically and degrade the performance of the system.

GloMoSim is highly scalable because the network girding approach is used instead of initializing each node as an entity. Network girding simulates several network nodes as one entity in the system. This means that we can increase the number of nodes in the system while maintaining the same number of entities in the simulation.

Each entity also encompasses all the layers of a simulation and each layer is now implemented as functions. Initialisation of the functions that will be called for each layer of each node is performed at the beginning of the simulation. The functions for each layer are used to send messages between the layers.

3.2 Protocol Modification Approach

In our approach, each node predicts the reliability of each upstream link by comparing the hop count the packet has travelled and the time it takes to reach it. The upstream link with the lower value of hop count number of the packet received is chosen over previous upstream link with a higher value of hop count number even if the delay time is higher. However, if the hop count number is the same then the previous upstream link with the less delay time is retained. In order to implement our approach in the GloMoSim simulation environment, several modification to the existing ODMRP distributed in GloMoSim distribution 2.03 (known as basic ODMRP henceforth) is necessary.

Using the basic ODMRP defined in the internet draft On-Demand Multicast Routing Protocol by Lee, Su, and Gerla (2000) as a base, we modified the protocol operations to incorporate our enhancement. The modification only affects the part of the protocol where nodes process the “Join Query” received. The pseudo codes followed by the process flow charts (Figure 3.1 & 3.2) for when a node receives a Join Query packet for the basic ODMRP (as defined in IETF Internet-draft by Lee, Su, and Gerla (2000)) and the ODMRP with the modification are respectively provided below.

When a node receives a Join Query packet (basic ODMRP):

- Check if it is a duplicate by comparing the (Source IP Address, Sequence Number) combination with the entries in the message cache. If a duplicate, then discard the packet. DONE.

- If it is not a duplicate, insert an entry into the message cache with the information of the received packet (i.e., sequence number and source IP address) and insert/update the entry for routing table (i.e., backward learning).
- If the node is a member of the multicast group, it originates a Join Reply packet and transmit via selected route.
- Increase the Hop Count field by 1 and decrease the TTL field by 1.
- If the TTL field value is less than or equal to 0, then discard the packet. DONE.
- If the TTL field value is greater than 0, then set the node's IP Address into Last Hop IP Address field and broadcast. DONE.

When a node receives a Join Query packet (Modified ODMRP):

- Checks if it is a duplicate by comparing the (source IP address, sequence number and last hop IP address) combination with the message cache.
- If it is not a duplicate, checks route table.
- If the source IP address matches an existing route entry but last hop IP address is not the same, check if the current hop count is less than the hop count of existing entry in the particular route entry. If so, replace last hop IP address and current timestamp into the particular route entry (i.e., backward learning). Otherwise do not insert route information.
- Check if it is a duplicate by comparing the (Source IP Address, Sequence Number) combination with the entries in the message cache. If a duplicate, then discard the packet. DONE.
- If it is not a duplicate, insert an entry into the message cache with the information of the received packet (i.e., sequence number, source IP address and last hop IP address)
- If the node is a member of the multicast group, it originates a Join Reply packet and transmit via selected route.
- Increase the Hop Count field by 1 and decrease the TTL field by 1.
- If the TTL field value is less than or equal to 0, then discard the packet. DONE.
- If the TTL field value is greater than 0, then set the node's IP address into last hop IP address field and broadcast. DONE.

3.3 System and hardware Requirements

Our coding modifications are conducted with a personal computer with the below specifications:

Intel Pentium 4 Processor, 1.5GHz
128 MB SD RAM
2 x 20GB IDE HDD
Microsoft Windows XP, service pack 2
Microsoft Visual C++ 6.0/Text Editor

Our simulation is also run on the same personal computer with the additional essential requirements of:

Parsec Compiler
GloMoSim
Microsoft Visual C++ version 6.0.

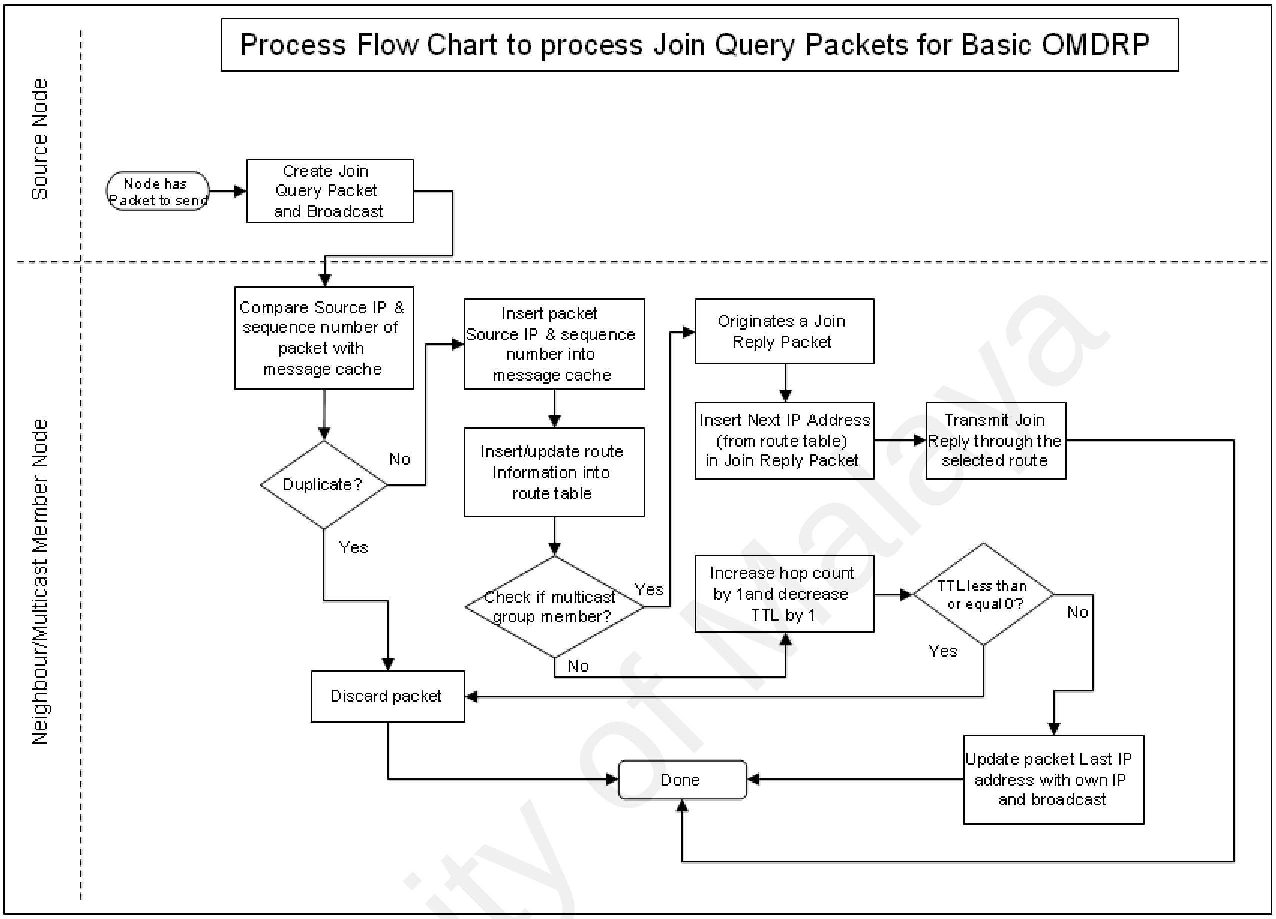

Process Flow Chart to process Join Query Packets for Basic OMDRP
Source Node
Neighbour/Multicast Member Node
Node has Packet to send
Create Join Query Packet and Broadcast
Compare Source IP & sequence number of packet with message cache
Duplicate?
No
Yes
Insert packet Source IP & sequence number into message cache
Insert/update route Information into route table
Check if multicast group member?
Yes
No
Originates a Join Reply Packet
Insert Next IP Address (from route table) in Join Reply Packet
Transmit Join Reply through the selected route
Increase hop count by 1and decrease TTL by 1
TTL less than or equal 0?
Yes
No
Discard packet
Done
Update packet Last IP address with own IP and broadcast

Figure 3.1 Process flow chart of basic ODRMP

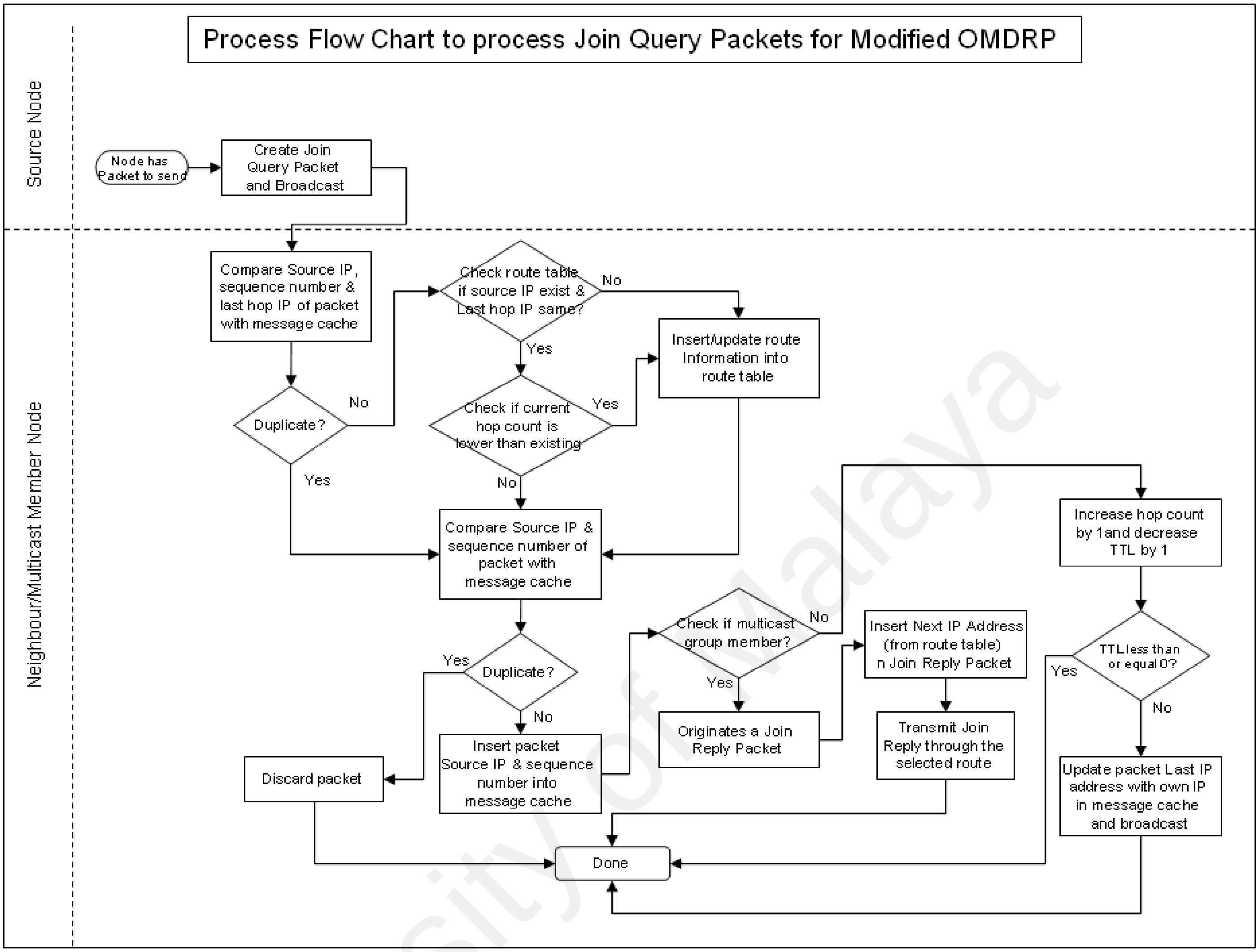

Process Flow Chart to process Join Query Packets for Modified OMDRP
Source Node
Neighbour/Multicast Member Node
Node has Packet to send
Create Join Query Packet and Broadcast
Compare Source IP, sequence number & last hop IP of packet with message cache
Duplicate?
No
Yes
Check route table if source IP exist & Last hop IP same?
No
Yes
Insert/update route Information into route table
Check if current hop count is lower than existing
Yes
No
Compare Source IP & sequence number of packet with message cache
Duplicate?
Yes
No
Discard packet
Insert packet Source IP & sequence number into message cache
Check if multicast group member?
No
Yes
Originates a Join Reply Packet
Insert Next IP Address (from route table) n Join Reply Packet
Transmit Join Reply through the selected route
Increase hop count by 1and decrease TTL by 1
TTL less than or equal 0?
Yes
No
Update packet Last IP address with own IP in message cache and broadcast
Done

Figure 3.2 Process flow chart of modified ODRMP

3.4 Methodology

In order to implement the enhancement explained in section 3.2 earlier, two files that require modification are odmrp.h and odmrp.pc which are in the network folder of the GloMoSim program distribution. This section details the important modifications to the two files followed by the simulation environment designed for the testing of the modified codes.

3.4.1 Codes Modification

Each node maintains a Message Cache to detect duplicate and to provide next hop information of routes. In our modified protocol, the message cache lookup function was modified to enable the node to consider more than one instance of a packet with the same sequence number received. To do this, a new field is added into the message cache data structure, ODMRP_MC, of the protocol which is defined in odmrp.h. The new field, **lastAddr**, is inserted into the structure of odmrpMCE which is part of the ODMRP_MC_Node structure. It is used to compare the Join Query packets received against an earlier (if any) Join Query packet with the same sequence number based on minimum delay. Figure 3.3 shows the addition necessary.

```
typedef struct odmrpMCE
{
            NODE_ADDR srcAddr;
            int seqNumber;
            NODE_ADDR lastAddr;  /* Addition */
            BOOL sent;
            struct odmrpMCE *next;
} ODMRP_MC_Node;

typedef struct /* Message Cache */
{
   ODMRP_MC_Node *front;
   ODMRP_MC_Node *rear;
   int size;
} ODMRP_MC;
```

Figure 3.3 Modification of ODRMP_MC in odmrp.h

In order for the new field, lastAddr, to be inserted into the message cache, the Insert Message Cache function in odmrp.pc file needs to be modified as shown in Figure 3.4 and this is reflected as well in the declaration in odmrp.h, shown in Figure 3.5.

```
/*
 * FUNCTION     RoutingOdmrpInsertMessageCache
 * PURPOSE      Insert new entry into message cache.
 *
 * Parameters:
 *    node:           Node that is inserting the new entry into message cache.
 *    sourceAddr:     Packet originator.
 *    seqNumber:      Packet sequence number.
 *    lastAddr        Packet last address
 *    messageCache: Message cache.
 */
void RoutingOdmrpInsertMessageCache(GlomoNode *node,
                        NODE_ADDR srcAddr,
                        int seqNumber,
                        NODE_ADDR lastAddr, /* Addition */
                        ODMRP_MC *messageCache)
{
   if (messageCache->size == 0)
   {
      messageCache->rear = (ODMRP_MC_Node *)pc_malloc(sizeof(ODMRP_MC_Node));
      assert(messageCache->rear != NULL);
      messageCache->front = messageCache->rear;
   }
   else
   {
      messageCache->rear->next = (ODMRP_MC_Node *)
                           pc_malloc(sizeof(ODMRP_MC_Node));
      assert(messageCache->rear->next != NULL);

      messageCache->rear = messageCache->rear->next;
   }

   messageCache->rear->srcAddr = srcAddr;
   messageCache->rear->seqNumber = seqNumber;
   messageCache->rear->lastAddr = lastAddr;  /* Addition */
   messageCache->rear->sent = FALSE;
   messageCache->rear->next = NULL;

   ++(messageCache->size);

   RoutingOdmrpSetTimer(
         node, MSG_NETWORK_FlushTables, ANY_DEST, ODMRP_FLUSH_INTERVAL);

} /* RoutingOdmrpInsertMessageCache */
```

Figure 3.4 Modification to Insert Message Cache function

```
void RoutingOdmrpInsertMessageCache(GlomoNode *node,
                        NODE_ADDR srcAddr,
                        int seqNumber,
                        NODE_ADDR lastAddr,  /* Addition */
                ODMRP_MC *messageCache);
```

Figure 3.5 Modification to the Insert Message Cache function declaration

The lastAddr field is required by a new function we include in the protocol. This function is duplicated from the existing Lookup Message Cache function in the original GloMomSim distribution in the omdrp.pc file but with modifications shown in Figure 3.6. The additional function must be declared in odmrp.h file, shown in Figure 3.7.

```
/* (Additional Function)
 * FUNCTION     RoutingOdmrpLookupMessageCache1
 * PURPOSE      Check if the join query/data packet w/ same lastAddr is seen before.
 *
 * Parameters:
 *    sourceAddr: Originating node of the packet.
 *     seqNumber: Sequece number of the packet.
 *      lastAddr: Last Address of the packet.
 *  messageCache: Message cache table.
 *
 * Return: TRUE if seen before; FALSE otherwise.
 */

BOOL RoutingOdmrpLookupMessageCache1(
          NODE_ADDR srcAddr, int seqNumber, NODE_ADDR lastAddr, ODMRP_MC messageCache)
{
   ODMRP_MC_Node *current;

   if (messageCache->size == 0)
    {
      return (FALSE);
    }

   for (current = messageCache->front;
       current != NULL;
       current = current->next)
   {
            if (current->srcAddr == srcAddr && current->seqNumber == seqNumber && current->lastAddr == lastAddr)
     {
       return (TRUE);  /* if current package has same source address and sequence number and last address, return TRUE */
     }
   }
   return (FALSE);
} /* OdmrpLookupMessageCache1 */
```

Figure 3.6	Additional Lookup Message Cache function in odmrp.pc

```
BOOL RoutingOdmrpLookupMessageCache1(
           NODE_ADDR srcAddr, int seqNumber, NODE_ADDR lastAddr, ODMRP_MC
*messageCache);
```

Figure 3.7	Additional Lookup Message Cache function declaration in odmrp.h

This new function which we named Lookup Message Cache 1 is different from the original Lookup Message Cache function because we include a comparison of the current Join Query packet's last address in addition to source address and sequence number with the information that may be contained in the existing message cache. If all three are the same with the information in the existing message cache, the function returns TRUE, i.e. the packet has been seen before. Otherwise, the function returns False, i.e. packet is not seen before.

Lookup Message Cache1 function is called by Handle Join Query function of odmrp.pc. The modifications necessary to enable the additional function to be called is shown in Figure 3.8 below.

Join Query packets received by the node will be compared against any earlier ones maintained in its' message cache, using the additional function Lookup Message Cache1 which we explained earlier. If the result returned from the function is FALSE, the protocol proceeds to call the Insert Route Table function (which will be explained later). Otherwise, the protocol proceed to call the original Lookup Message Cache which determines if the received packet has been seen before by comparing its' source address and packet sequence number against the message cache maintained. This original lookup Message Cache is required because we do not want the protocol to proceed to broadcast to its' neighbours even if our additional Lookup Message Cache returns False. This is because, although we require the route information from the packet to be update into the node's route table since the packet is from a different up link node, we do not want the protocol to broadcast the data again since it may have already done so previously with a packet received earlier with the same sequence number as that will be a wasted effort. Therefore, the protocol proceeds to call the original Lookup Message Cache function to determine if that packet needs to be broadcasted or not.

```
/*
 * FUNCTION     RoutingOdmrpHandleJoinQuery
 * PURPOSE      Processing procedure when Data Join is received.
 *
 * Paremeters:
 *     node:  Node handling the data join packet.
 *     msg:   The data join packet.
 */
void RoutingOdmrpHandleJoinQuery(GlomoNode *node, Message *msg)
{
   GlomoNetworkIp* ipLayer = (GlomoNetworkIp *) node->networkData.networkVar;
   GlomoRoutingOdmrp* odmrp = (GlomoRoutingOdmrp *) ipLayer->routingProtocol;
   IpHeaderType *ipHdr = (IpHeaderType *)GLOMO_MsgReturnPacket(msg);
   NODE_ADDR sourceAddress;
   NODE_ADDR destinationAddress;
   unsigned char IpProtocol;
   unsigned int ttl;
   NetworkQueueingPriorityType priority;
   clocktype delay, jrDelay;
   ODMRP_MT_Node *mcastEntry;
   ODMRP_RPT_Node *mEntry;
   NODE_ADDR srcAddr = ipHdr->ip_src;
   NODE_ADDR mcastAddr = ipHdr->ip_dst;
   OdmrpIpOptionType option = GetOdmrpIpOptionField(msg);
   Message *newMsg = NULL;

/* Process packet only if not duplicate. */
   if (!RoutingOdmrpLookupMessageCache1(
                  srcAddr, option.seqNumber, option.lastAddr, &odmrp->messageCache))
             {
      RoutingOdmrpInsertRouteTable(
         srcAddr, option.lastAddr, option.hopCount, &odmrp->routeTable);
             }
   if (!RoutingOdmrpLookupMessageCache(
                  srcAddr, option.seqNumber, &odmrp->messageCache))
             {RoutingOdmrpInsertMessageCache(
         node, srcAddr, option.seqNumber, option.lastAddr, &odmrp->messageCache);
#ifdef DEBUG
   printf("Node %ld received Join Query from %d\n", node->nodeAddr, option.lastAddr);
#endif
       /*If the node is a member of the group */
      if (RoutingOdmrpLookupMembership(mcastAddr, &odmrp->memberFlag))
      {
#ifdef DEBUG
           printf("       Member got it!\n");
#endif

….
```

Figure 3.8   Modification of Handle Join Query Function

If the Lookup Message Cache1 function returns FALSE, the Insert Route Table function will be called which in turn calls the functions Check Route Exist and Insert RT In Order. The latter 2 functions and their declarations need to be modified. Check Route Exist function is modified to include a comparison of the current packet’s next address information with existing route table besides checking if the packet’s destination address exists in the route table. If yes, the function returns TRUE, i.e. the route exist. Otherwise, the function returns FALSE. The modifications in this function and its' declaration is shown in Figure 3.9 and 3.10 respectively.

```
BOOL RoutingOdmrpCheckRouteExist(NODE_ADDR destAddr, NODE_ADDR nextAddr, ODMRP_RT *routeTable)
{
   ODMRP_RT_Node *current;

   if (routeTable->size == 0)
   {
      return (FALSE);
   }

   for (current = routeTable->head;
        current != NULL && current->destAddr <= destAddr;
        current = current->next)
   {
      if (current->destAddr == destAddr && current->nextAddr == nextAddr) /*Modification*/
      {
         return (TRUE);
      }
     else if (current->destAddr == destAddr && current->nextAddr != nextAddr) /* Modification*/
             {
                         return (FALSE);
             }

   }

   return (FALSE);
```

Figure 3.9 Modification of Check Route Exist Function

```
BOOL RoutingOdmrpCheckRouteExist(NODE_ADDR destAddr, NODE_ADDR nextAddr,
ODMRP_RT *routeTable);
```

Figure 3.10 Modification of Check Route Exist declaration

If the Check Route Exist function returns a FALSE, the Insert Route Table function calls Insert RT In Order function. This function checks if the destination address is the same but the next address is not, it proceeds to check if the hop count in the route table is larger than the hop count of the current packet being processed (shown in Figure 3.11). If so, the function continues to replace the new route information into the existing route for the same destination address in the route table.

```
ODMRP_RT_Node *RoutingOdmrpInsertRTInOrder(
   NODE_ADDR destAddr, NODE_ADDR nextAddr, int hopCount, ODMRP_RT_Node *old)
{
   ODMRP_RT_Node *newOne;

   if (old == NULL)
   {
      newOne = (ODMRP_RT_Node *)pc_malloc(sizeof(ODMRP_RT_Node));
      assert(newOne != NULL);

      newOne->destAddr = destAddr;
      newOne->nextAddr = nextAddr;
      newOne->hopCount = hopCount;
      newOne->timestamp = simclock();
      newOne->next = NULL;
   }
   else if (old->destAddr > destAddr)
   {
      newOne = (ODMRP_RT_Node *)pc_malloc(sizeof(ODMRP_RT_Node));
      assert(newOne != NULL);

      newOne->destAddr = destAddr;
      newOne->nextAddr = nextAddr;
      newOne->hopCount = hopCount;
      newOne->timestamp = simclock();
      newOne->next = old;
   }
/* Addition*/
  else if (old->destAddr == destAddr && old->nextAddr != nextAddr && old->hopCount  > hopCount)
   {
      newOne = (ODMRP_RT_Node *)pc_malloc(sizeof(ODMRP_RT_Node));
      assert(newOne != NULL);

      newOne->destAddr = destAddr;
      newOne->nextAddr = nextAddr;
      newOne->hopCount = hopCount;
      newOne->timestamp = simclock();
      newOne->next = NULL;
   }
   else
   {
      newOne = old;
      newOne->next = RoutingOdmrpInsertRTInOrder(
                  destAddr, nextAddr, hopCount, old->next);
   }

   return (newOne);
}
```

Figure 3.11 Modification of Insert Route Table In Order Function

With the modifications done onto the codes, our modified protocol effectively chooses the route with a lower hop count number. In this way, our modified protocol implements a link survivability predictive mechanism by selecting the path with the least hop count with the rationale that less intermediary nodes increases the chance of a more stable link.

3.4.2 Simulation Environment

Modelled based on Lee et. al. (2001), all our simulations consist of a network of 50 nodes placed randomly within a square terrain area of 1000 meter x 1000 meters. Where mobility of nodes is simulated, Random-Waypoint mobility model is selected. With Random-Waypoint model, all nodes move at predefined speeds in the directions to their randomly selected destinations. Once the destination is reached, the nodes immediately choose another random destination and moves in the new directions. However, the simulation time is revised to 200 seconds instead of 600 seconds as test runs carried out showed that simulation set at 200 seconds is more manageable. Other requirements not specified otherwise are left to the defaulted values in the configuration file from the original GloMoSim distribution and is shown in Figure 3.12 below.

We conduct each scenario using random seed number and the collected data is averaged over the runs. Seed numbers are drawn out randomly from lots with numbers ranging from 1 to 50. Further more, similar to Lee et. al. (2001), all scenarios are subjected to a constant bit rate generation from a single node with a payload size of 512MB. The CBR generation is continuous from the start of the simulation until the end with a pause time of 500 milliseconds between each packet generated. In total, in each simulation run, the source will generate a total of 200000/500 = 400 packets with size of 512MB.

```
# ***** GloMoSim Configuration File Abstract*****

SIMULATION-TIME     200S

SEED              1

TERRAIN-DIMENSIONS  (1000, 1000)

NUMBER-OF-NODES     50

NODE-PLACEMENT      RANDOM

MOBILITY-POSITION-GRANULARITY 0.5

PROPAGATION-LIMIT      -111.0

NOISE-FIGURE    10.0

TEMPARATURE     290.0

RADIO-TYPE             RADIO-ACCNOISE

RADIO-FREQUENCY     2.4e9

RADIO-BANDWIDTH     2000000

RADIO-RX-TYPE           SNR-BOUNDED
RADIO-RX-SNR-THRESHOLD  10.0

RADIO-TX-POWER       15.0

RADIO-ANTENNA-GAIN  0.0

RADIO-RX-SENSITIVITY -91.0

RADIO-RX-THRESHOLD -81.0

MAC-PROTOCOL       802.11

NETWORK-PROTOCOL    IP
NETWORK-OUTPUT-QUEUE-SIZE-PER-PRIORITY 100

ROUTING-PROTOCOL    ODMRP
MCAST-CONFIG-FILE    member.conf

APP-CONFIG-FILE   ./app.conf


APPLICATION-STATISTICS         YES
ROUTING-STATISTICS             YES
```

Figure 3.12 Abstract on fixed configuration file for all simulations

Chapter 4 Results and Discussion

To investigate the impact of our enhancement, we compare the following two protocols in simulation:

- Basic ODMRP protocol as specified in Lee, Su, and Gerla (2000), with minimum delay as the route selection metric
- Modified ODMRP protocol with minimum delay and hop count as the route selection metrics

4.1 Simulation Scenarios and Hypothesises

To evaluate if the performance of our modified protocol is better than the basic protocol, we designed the below scenarios in three different environments:

Experiment 1

Unicast Traffic as a function of node speed, based on Lee et. al. (2001): All node speeds are set constant at 0, 10, 50, 150 and 200 m/s. Two members are randomly selected by drawing lots with number 0 to 49 and the selected numbers are configured into the member.conf file in the bin folder as a single multicast group (effectively unicast). The member with the lower node number of the two is configured as the sole source node generating the continuous CBR traffic of 512MB payload size with pause time of 500 milliseconds between each packet send. This is configured in the app.conf file in the bin folder. Meanwhile the other member node will be the sole recipient. For each protocol and each node speed, three different pairs of node numbers are drawn randomly from lots containing the numbers 0 to 49 and for each pair, simulations are run three times with different random seed numbers. Random seed numbers are drawn from lots containing the numbers 1 to 50.

- *Purpose:* To evaluate and compare the performances of the modified ODMRP and the basic ODMRP for Unicast traffic at varying speeds.
- *Hypothesis:* We expect the modified ODMRP to perform significantly better than the basic ODMRP for Unicast traffic at each varying speeds.

Experiment 2

Multicast Traffic as a function of node speed, based on Lee et. al. (2001): 10 members are randomly selected by drawing from lots containing the numbers 0 to 49. The members are configured in a single multicast group out of which the node with the smallest node number is configured as the traffic generating node, similar to the Unicast environment, while the others are recipients. For each protocol and each node speed, different sets of random 10 member nodes are selected. The set of simulation to test the multicast traffic scenario with varying node speeds at 0, 10, 50, 150 and 200 m/s, similar to the Unicast environment. For each group of multicast members in each simulation in this scenario, three runs are conducted using different random seed numbers.

- *Purpose:* To evaluate and compare the performances of the modified ODMRP and the basic ODMRP for Multicast traffic at varying speeds.
- *Hypothesis:* We expect the modified ODMRP to perform significantly better than the basic ODMRP for Multicast traffic at each varying speeds.

Experiment 3

Varying Multicast Single Group Sizes with node speed of 5 m/s, based on Lee et. al. (2001): To evaluate the effectiveness of the protocols with different multicast (single) group sizes, we utilise the constant node speed of 5 meters per second and simulate with varying multicast group sizes, i.e. 2 (unicast), 5, 10, 15 and 20. For each multicast group size, we run 3 simulations using different randomly drawn seed number (from numbers 1 to 50).

- *Purpose:* To evaluate and compare the performances of the modified ODMRP and the basic ODMRP for Multicast traffic at varying group sizes at the constant node speed of 5 m/s.

- *Hypothesis:* We expect the modified ODMRP to perform significantly better than the basic ODMRP for Multicast traffic at each varying group sizes at the constant speed of 5 m/s.

The metric of interest of all our simulation is packet delivery ratio, i.e. number of packets delivered to recipient over number of packets should be delivered.

To know if the results we obtained for the 3 different environments are significantly different between the two protocols, we utilise the Z-Test for two samples. The z-test is used to find significant differences between the two sample means. It indicates how likely it is that both samples with a certain mean and standard deviation came from the population.

For a 95% confidence interval, if the z is greater than 1.96 or less than -1.96, it means that *p*<.05, and the difference is statistically significant. That is, it is so unlikely that the sample came from this population (5% chance or less) that we reject the null hypothesis and say that the sample is different from the population. For a 99% confidence interval, if the z is greater than 2.58 or less than -2.58, it means that *p*<.01, and the difference is even more significant—the null hypothesis can be rejected with greater confidence.

4.2 Unicast Traffic with Varying Mobility Speeds

The summary result of the Unicast environment simulation is given in the Table 4.1 and Figure 4.1 below. Table 4.2 shows the detailed z test results for each set of tests in this scenario.

	Average Packet Delivery Ratio				
Speed of nodes (m/s)	0	5	10	15	20
basic ODMRP	0.43	0.60	0.48	0.59	0.48
modified ODMRP	0.43	0.40	0.49	0.56	0.50
z test	0.00	*20.79*	-0.70	*2.53*	*-2.34*

Table 4.1 Packet Delivery Ratios for Unicast Traffic with varying movement speeds.

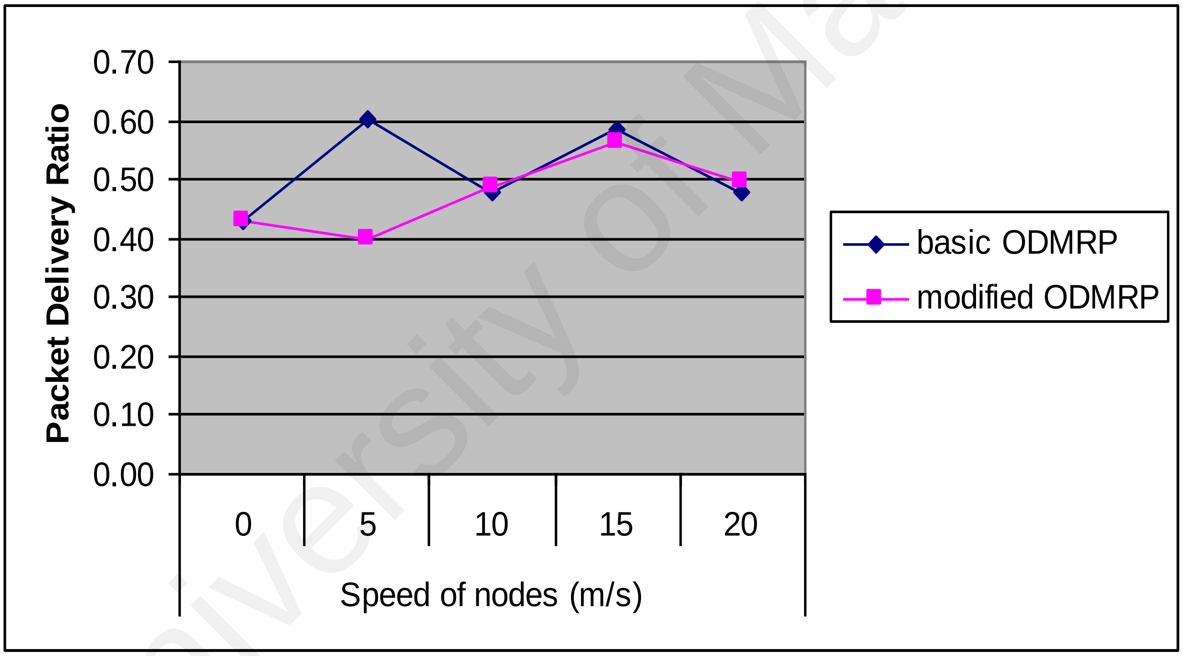


Figure 4.1 Packet Delivery Ratio over varying movement speeds

a) z-Test: Two Sample for Means for
Node Speed 0 m/s

	Basic	*Modified*
Mean	172	172
Known Variance	171	171
Observations	9	9
Hypothesized Mean Difference	0	
z	0	
P(Z<=z) one-tail	0.5	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	1	
z Critical two-tail	1.959964	

b) z-Test: Two Sample for Means for
Node Speed 5 m/s

	Basic	*Modified*
Mean	240.3333	159.7778
Known Variance	70.85901	64.30937
Observations	9	9
Hypothesized Mean Difference	0	
z	20.7864	
P(Z<=z) one-tail	0	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0	
z Critical two-tail	1.959964	

c) z-Test: Two Sample for Means for
Node Speed 10 m/s

	Basic	*Modified*
Mean	192.1111	194.8889
Known Variance	52.85462	87.64765
Observations	9	9
Hypothesized Mean Difference	0	
z	-0.70304	
P(Z<=z) one-tail	0.241017	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0.482034	
z Critical two-tail	1.959964	

d) z-Test: Two Sample for Means for
Node Speed 15 m/s

	Basic	*Modified*
Mean	234.6667	225.5556
Known Variance	52.76125	64.30937
Observations	9	9
Hypothesized Mean Difference	0	
z	2.526205	
P(Z<=z) one-tail	0.005765	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0.01153	
z Critical two-tail	1.959964	

e) z-Test: Two Sample for Means for
Node Speed 20 m/s

	Basic	*Modified*
Mean	191.4444	198.7778
Known Variance	51.79312	36.61549
Observations	9	9
Hypothesized Mean Difference	0	
z	-2.33978	
P(Z<=z) one-tail	0.009647	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0.019295	
z Critical two-tail	1.959964	

Table 4.2 Z test results for Unicast Traffic for each varying node movement speeds.

In this experiment, a single source sends packets to a single destination (of 512 MB size) continuously with pause time of 500 milliseconds between each packet sent. The simulation result shows that the two protocols performed significantly different from each other for speeds of 5, 15 and 20 m/s while their performances differences are insignificant at 0 and 10 m/s. Although at speeds 15 and 20 m/s the performance of both protocols are significantly different from each other, the differences are very small, i.e. less than 3% each. However, at speeds of 5 m/s, the basic protocol out performed our modified protocol significantly (at 99% confidence level) by 20%.

Our hypothesis for this set of experiment that the performance of the modified ODMRP is significantly better than the basic ODMRP is true for node speed at 20 m/s only and not for rest of the node speeds.

The result shows that the basic ODRMP works particularly well at slow node speed (5 m/s) with 60% average packet delivery ratio, a 20% advantage over the modified ODMRP at the same slow node speed. As explained in Section 2.7, the rationale for the enhancements in our modified ODMRP is that we believe that if there are more intermediary nodes along a route/path, the chances of one of more of the intermediary nodes moving away from transmission range is higher hence causing the route to fail.

When node movements are slow (at 5m/s), successful paths are established, using minimum delay as the route selection metric in basic ODMRP. The continuous random movement did not affect the packet deliveries adversely because although the nodes are moving, they did not move quickly enough and continue to remain in transmission range to allow packets to be delivered rapidly with the existing initial routes. In the modified ODMRP, the continuous movement of nodes have allowed for new routes to be established and chosen (due to our enhanced route selection metric using hop count on top of minimum delay) over the initially established route. The continuous new routes establishment and the frequent change of routes failed to take advantage of the initially established routes which are still valid. By choosing the new routes over the initial route, our modified ODMRP failed to produce better performance compared to the basic

ODMRP as time taken to establish the new routes results in packets being dropped in interim.

4.3 Multicast Traffic with Varying Mobility Speeds

The result of the Multicast Group of 10 simulations is given in the Table 4.3 and Figure 4.2 below. Results of the z test conducted are shown in Table 4.4. Similarly, the metric of interest for all simulation is the Packet Delivery Ratio (Packet received/Packet supposed to be received) by destination nodes.

Speed of nodes (m/s)	Average Packet Delivery Ratio				
	0	5	10	15	20
basic ODMRP	0.43	0.70	0.50	0.52	0.51
modified ODMRP	0.49	0.52	0.53	0.53	0.54
z test	7.19	28.71	-6.07	-2.45	-5.32

Table 4.3 Packet Delivery Ratios for Multicast Traffic of Basic ODMRP and modified ODMRP with varying movement speeds.

For multicast traffic with a group size of 10, a single source sends packets (of 512 MB in size) to all other member nodes continuously with pause time of 500 milliseconds between each packet sent. Overall, the simulation result shows that the two protocols performed significantly different from each other for all speeds with at least 95% confidence level. Except for at low node speed (5 m/s), our hypothesis for this set of experiment that the modified ODMRP performs significantly better than the basic ODMRP has been proven correct. However, disregarding speed 0, the performance improvement of the modified ODMRP over the basic ODMRP is small (up to 3%).

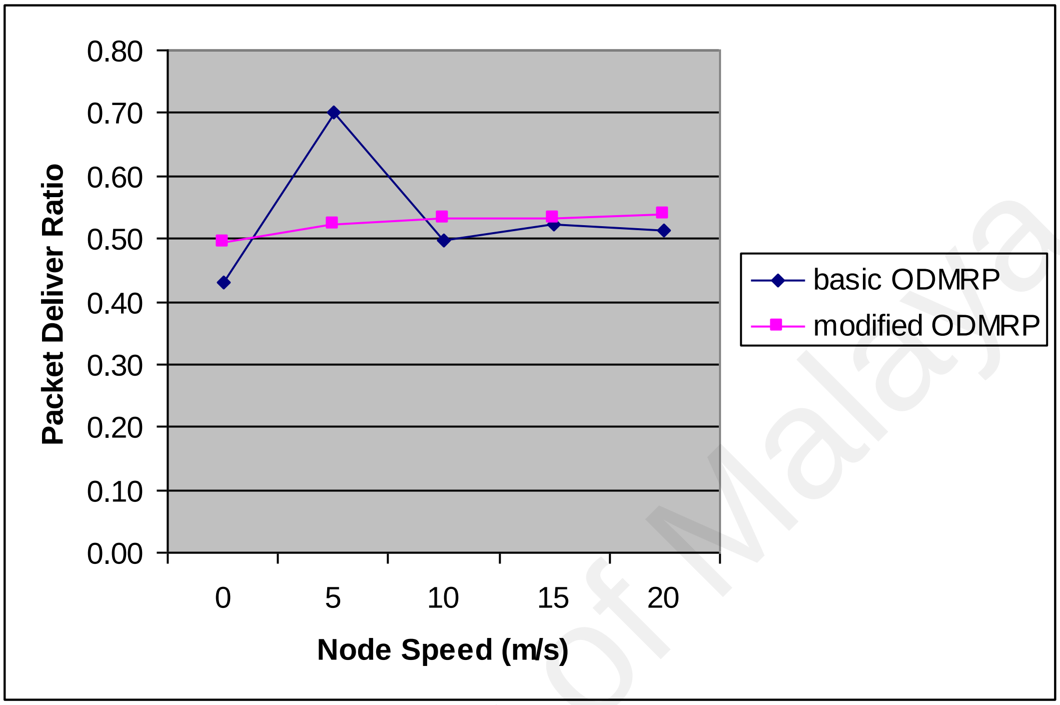


Figure 4.2 Packet Delivery Ratio over varying movement speeds for Multicast Group of 10

Similar to the Unicast experiment results discussed earlier in Section 4.2, when the movement of nodes are at low speed (5 m/s), the basic ODMRP shows an 18% performance improvement in terms of average packet delivery ratio over the modified ODMRP. As explained in Section 4.2, the continuous random and slow movement allowed for valid routes to be established and the routes continue to be valid as nodes are not moving quickly enough and remain in transmission ranges to allow packets to be delivered rapidly.

a) z-Test: Two Sample for Means for Node Speed 0 m/s

	Basic	*Modified*
Mean	197.3333	172
Known Variance	171.2434	164.2915
Observations	27	27
Hypothesized Mean Difference	0	
z	7.1863	
P(Z<=z) one-tail	3.33E-13	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	6.66E-13	
z Critical two-tail	1.959964	

b) z-Test: Two Sample for Means for Node Speed 5 m/s

	Basic	*Modified*
Mean	280.963	208.7778
Known Variance	80.34516	90.34691
Observations	27	27
Hypothesized Mean Difference	0	
z	28.70935	
P(Z<=z) one-tail	0	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0	
z Critical two-tail	1.959964	

c) z-Test: Two Sample for Means for Node Speed 10 m/s

	Basic	*Modified*
Mean	199.0741	212.8519
Known Variance	60.63188	78.28435
Observations	27	27
Hypothesized Mean Difference	0	
z	-6.07414	
P(Z<=z) one-tail	6.23E-10	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	1.25E-09	
z Critical two-tail	1.959964	

d) z-Test: Two Sample for Means for Node Speed 15 m/s

	Basic	*Modified*
Mean	208.5556	213.4815
Known Variance	47.92328	61.10984
Observations	27	27
Hypothesized Mean Difference	0	
z	-2.45127	
P(Z<=z) one-tail	0.007118	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0.014235	
z Critical two-tail	1.959964	

e) z-Test: Two Sample for Means for Node Speed 20 m/s

	Basic	*Modified*
Mean	205.3333	215.4815
Known Variance	51.40488	46.74347
Observations	27	27
Hypothesized Mean Difference	0	
z	-5.32264	
P(Z<=z) one-tail	5.11E-08	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	1.02E-07	
z Critical two-tail	1.959964	

Table 4.4 Z test results for Multicast Traffic for each varying node movement speeds.

On the contrary, in the modified ODMRP, the continuous movement of nodes have allowed for new routes to be established and chosen continually over the initially established route. The continuous new routes establishment and the frequent change of routes failed to take advantage of the initially established routes which are still valid. By choosing the new routes over the initial route, our modified ODMRP failed to perform better than the basic ODMRP as time taken to establish the new routes results in some packets being dropped in the interim.

From medium to fast node speeds (10 m/s to 20 m/s), the modified ODMRP produces small performance improvement (up to 3%) over the basic ODMRP. As movement speed is increased, the chances of nodes moving in and out of transmission ranges become higher. The modified ODMRP continuous new route establishments enable invalid routes to be replaced by new ones more quickly. The new routes are established using our link survivability predictive approach, i.e. a route with less hop counts will have a higher chance of lasting longer. Therefore, by selecting route with less hop counts on top of minimum delay, we have chosen the routes based on their predicted survivability. In the basic ODMRP, the initial routes expire and new routes are re-established again on minimum delay with no link survivability prediction. Our experiment result has proven that performance is enhanced for Multicast traffic at medium to fast node speeds (10 m/s to 20 m/s).

4.4 Multicast Traffic with Varying Multicast Group Sizes

The result of the Multicast Traffic with Varying Multicast Group Sizes and constants speed simulation is detailed in Table 4.5 and Figure 4.3. Results of the z test conducted are shown in Table 4.6. Similarly, the metric of interest for all simulation is the Average Packet Delivery Ratio (Packet received/Packet supposed to be received) by destination nodes.

Multicast Group Size	Average Packet Delivery Ratio				
	2	5	10	15	20
basic ODMRP	0.51	0.41	0.69	0.54	0.46
modified ODMRP	0.56	0.56	0.60	0.55	0.61
z test	3.88	15.83	-14.22	15.69	32.96

Table 4.5 Packet Delivery Ratios for Multicast Traffic with varying multicast group sizes

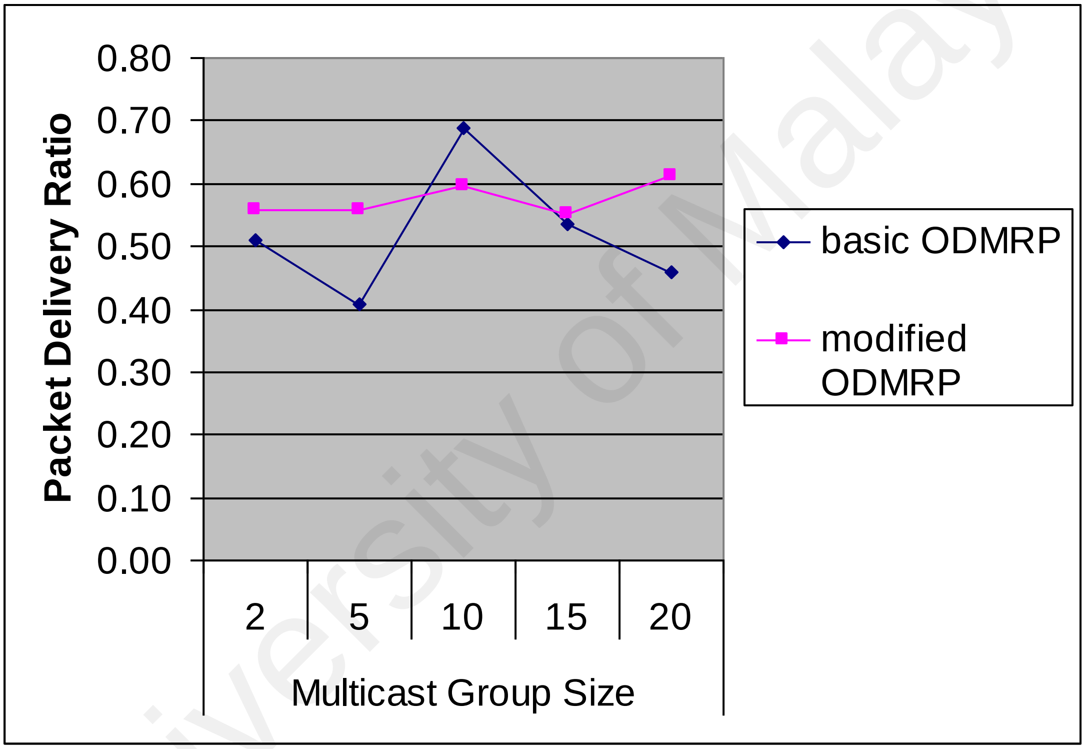


Figure 4.3 Packet Delivery Ratio over varying movement speeds

a) z-Test: Two Sample for Means for Multicast Group size of 2 (Unicast)

	Basic	*Modified*
Mean	204	223
Known Variance	25.11971	46.67976
Observations	3	3
Hypothesized Mean Difference	0	
z	-3.88377	
P(Z<=z) one-tail	5.14E-05	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0.000103	
z Critical two-tail	1.959964	

b) z-Test: Two Sample for Means for Multicast Group size of 5

	Basic	*Modified*
Mean	163	223.0833
Known Variance	65.58548	107.3596
Observations	12	12
Hypothesized Mean Difference	0	
z	-15.8267	
P(Z<=z) one-tail	0	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0	
z Critical two-tail	1.959964	

c) z-Test: Two Sample for Means for Multicast Group size of 10

	Basic	*Modified*
Mean	275.2593	238.963
Known Variance	76.84329	98.98277
Observations	27	27
Hypothesized Mean Difference	0	
z	14.22337	
P(Z<=z) one-tail	0	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0	
z Critical two-tail	1.959964	

d) z-Test: Two Sample for Means for Multicast Group size of 15

	Basic	*Modified*
Mean	214.4762	220.5476
Known Variance	94.12401	76.2135
Observations	42	42
Hypothesized Mean Difference	0	
z	-3.01481	
P(Z<=z) one-tail	0.001286	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0.002571	
z Critical two-tail	1.959964	

e) z-Test: Two Sample for Means for Multicast Group size of 20

	Basic	*Modified*
Mean	183.2456	244.7719
Known Variance	101.5233	97.05135
Observations	57	57
Hypothesized Mean Difference	0	
z	-32.9637	
P(Z<=z) one-tail	0	
z Critical one-tail	1.644854	
P(Z<=z) two-tail	0	
z Critical two-tail	1.959964	

Table 4.6 Z test results for Multicast Traffic for each varying node movement speeds.

For this experiment, a single source sends packets (of 512 MB in size) to varying multicast group sizes continuously with pause time of 500 milliseconds between each packet sent, and all nodes moved continuously and randomly at a constant speed of 50 m/s. The result shows that except for Multicast group size of 10, the modified ODMRP performed significantly (with confidence level of 99%) better than the basic ODMRP, with improvement of up to 15% for large Multicast group size (20 members). Our hypothesis for this set of experiment that the modified ODMRP performs significantly better than the basic ODMRP has been proven correct for all Multicast group sizes (2, 5 and 20) except group size of 10.

At Multicast group size of 10, the basic ODMRP performs 10% better than the modified protocol at packet delivery ratio of 69% at 99% confidence level. This result is consistent with that obtained in Section 4.3 where for nodes speed of 5 m/s and constant multicast group size of 10, the packet delivery ratio achieved 70%. This result again proved that for node movements at low speed (5 m/s), the basic protocol out performs the modified protocol.

For the other Multicast group sizes tested, the modified ODMRP performed significantly better compared to the basic ODMRP. The improved performances at those multicast group sizes is due to the adaptability of the modified ODMRP that allowed more routes to be evaluated and selected continuously as opposed to the basic ODMRP. The nodes moving randomly continuously at the speed of 5 m/s complements the modified ODMRP and increases the successful delivery of the packets. As the Multicast group size increases, the chance of nodes moving in and out of transmission is amplified as the member nodes are increased.

4.5 Summary

In Experiment 1 for Unicast traffic, the performance of the modified ODMRP is similar to the basic ODMRP except for when the node speeds are at 5 m/s where the basic protocol performed significantly better (20%). However, in Experiment 2 for Multicast traffic, the modified ODMRP performed significantly better than the basic ODMRP at all node speeds except for 5 m/s where basic outperformed modified protocol by 18%. In Experiment 3, the performance of the modified ODMRP is significantly better compared to the basic ODMRP at all multicast group sizes except for when the multicast group size was 10.

In summary, the proposed modified ODMRP shows mixed results. The modified ODMRP shows some but not total improvement over the basic ODMRP in the different scenarios sets.

Chapter 5 Conclusion and Suggestions

This chapter summarises and concludes our findings on all the simulation experiments that have been tested, before we raise our concerns of our methodology of our experiment. We also provide suggestions on how future studies can be designed to resolve them.

5.1 Summary of Project Findings

With dynamic topology changes and an absence of any underlying infrastructure, ad hoc networks require a novel routing scheme that provides efficient and high throughput communication among mobile nodes. Among protocols designed for ad hoc networks is On Demand Multicast Routing Protocol (ODMRP) which is a reactive protocol that uses caching strategies. ODMRP can be improved through the prediction of link survivability. In this study, our objective is to create a method of link survivability prediction in ODMRP that is easily adopted to help ensure faster and more reliable communication in ad hoc wireless networks without relying on other existing infrastructure or requiring additional hardware components to current mobile devices. We utilise total delays and hop numbers of packets to predict link survivability as we expect that a path is a less attractive choice if it delivers a packet slower and has more intermediary nodes as the chances of link breakage is higher when more intermediary nodes are involved.

To evaluate our link survivability prediction enhancement to ODMRP, we modified and recompiled the source code of the ODMRP protocol in GloMoSim and designed 3 experiments to test and compare the performance of the modified ODMRP with the basic ODMRP, i.e.:

- Experiment 1 - *Unicast Traffic as a function of node speed*
- Experiment 2 – *Multicast Traffic as a function of node speed*

- Experiment 3 – *Varying Multicast Single Group Sizes with constant node speed*

The simulation results of Experiment 1 for Unicast traffic do not show that the modified ODMRP performed significantly better over the basic ODMRP. The performance of the modified protocol is similar to the basic protocol except for when the node speeds are at 5 m/s where the basic protocol performed significantly better (20%).

However, the simulations results in Experiment 2 for Multicast traffic indicate the modified ODMRP shows significant better performance over the basic protocol at all node speeds except for 5 m/s where basic outperformed modified protocol by 18%.

Experiment 3 tests the performance of the modified ODMRP compared to the basic ODMRP in varying multicast group sizes but at a constant speed of 5 m/s. The result shows that the performance of our modified protocol is significantly better at all multicast group sizes except for when the multicast group size was 10.

In conclusion, the proposed modified ODMRP shows mixed results. The modified ODMRP shows some but not total improvement over the basic ODMRP in the different scenarios sets. At the speed of 5 m/s, the basic ODMRP protocol outperformed the modified protocol for both Unicast and Multicast traffic environments. At a constant speed of 5 m/s, the varying multicast group size simulation results showed that for a group size of 10, the basic protocol prevailed to outperform our modified protocol. We have also proven that our modified protocol produced the desired improvement in performances over the basic protocol for multicast traffic at other node speeds except 5 m/s and for all multicast group sizes except for 10. In general, the graphical representations of the results in all the three experiments show inconsistent performance of the basic protocol with more sharp peaks and valleys across the various sets of scenarios. On the other hand, the modified protocol shows more consistent performance in the different sets of scenarios with lesser fluctuations.

5.2 Significance of Findings

In both Experiment 1 (Unicast traffic) and Experiment 2 (Multicast traffic), we found that the basic ODMRP and the modified ODMRP do not deliver packets to destinations well when nodes are static. Firstly, as destination and source were randomly picked and placed in the 1000 x 1000 terrain, there is a high possibility that the source and destination nodes were not within the transmission range of each other and could not be connected through any successful formation of forward groups in the protocol due to the pre-fixed hop count of 10. Since nodes are static, there are no topology changes, therefore, no new routes can be established throughout the simulation. Secondly, since the traffic is very heavy, i.e. continuous packet were generated every 500 milliseconds by the source, there is high congestions where many packets were dropped as a result.

An interesting phenomenon was noticed in both Experiments 1 and 2. The performance of the basic protocol was at its peak at node speed of 5 m/s for both Unicast and Multicast traffic. The slow topology changes as a result of node movement at low speed and the original route selection metric using delay time is already producing a good packet delivery ratio. In our modified protocol, our additional route selection metric of hop count in addition to delay time caused a delay in route establishment process and did not produce better delivery ratios at 5 m/s node speeds. The additional route information that we have included to provide predictive link survivability in our modified protocol do not provide any advantage at that speed because node movements are relatively low. The nodes forming the forward group are still within the transmission range, allowing high success rate of packet delivery.

However, as the speed of nodes increase this phenomenon is removed as the nodes are moving in and out of transmission ranges more frequently. The more rampant node movement increased the chances of forwarding members of the established forward groups moving in and out of transmission ranges before the route table entries expires. Our modified protocol enabled the node route tables to be continuously updated with more recent route information using hop count as an additional route selection metric. In Unicast traffic, the improvements shown by the modified protocol is slight and insignificant but as numerous destinations are involved, the cumulative results amplified the improvement into significance. We have proven that the modified protocol produced advantageous predictive measures in Multicast traffic resulting in the selection of routes that with higher survivability despite the rampant movements.

In Experiment 3, as the multicast group size was set at 10, the adaptability of the modified protocol to obtain better routes in a comparatively low topology changing environment was overshadowed by the original protocol which was able to provide good delivery of packets to destinations. Moving at 5 m/s, nodes were likely not to move out of transmission ranges within the period of our simulation runs. When the multicast group sizes were increased further, more destination nodes were involved and the basic protocol cannot sustain the high average packet delivery ratios. As more destinations were involved and movement are random at the constant speed of 5 m/s, the chances of the destination nodes moving in and out of transmission ranges is higher compared to a smaller multicast group. Our modified protocol with the route selection enhancement increased the chances of retention of good route information with link survivability predictive measures. Again, we have proven that the modified protocol produced advantageous predictive measures resulting in the selection of routes that have higher link survivability when multicast group sizes increases, even when node movements were not rampant.

Analysing the trends of both protocols across the three experiments, we discover that the basic protocol gave inconsistent results with more sharp peaks and valleys across the different sets of scenarios as compared to the modified protocol. This shows that the basic protocol do not give consistent performance in varied situations which translates to the lack of adaptability and stability of the protocol in regards to varied situations. The performance of the modified protocol is more consistent across the different scenarios indicating the adaptability of the modified protocol.

In summary, we proved that the modified protocol performs significantly better in Multicast traffic for most simulated scenarios and the performance is more consistent across the varied scenarios than the basic protocol.

5.3 Concerns and Suggestions for future studies

In this study, the mobility model was a highly random model, i.e. Random-Waypoint. We recognise that this model does not allow our findings to reflect a true situation where the wireless ad hoc network can be potentially useful. In other words, the simulation tested were actually the worst case scenarios where mobile ad hoc nodes move in total randomness. The danger of this is that we may be inclined to create a protocol that does too much to cater for a random mobility situation when in real life there is actually no good use of it. However, it is with regret that this dissertation has been limited in scope of study, due to many reasons, but mainly due to the constraints of time and resources. More areas of studies can be looked into that could reduce this consequence while testing out a new or modified protocol to improve survivability of links in a mobile ad hoc network. Firstly, we could take a closer look on each potential usage of ad hoc networks and come up with a more realistic mobility models that we could in turn use to test the modified or new protocols we created. This could be done, for example, by observing a real life situation of movements of rescue workers in a search of a lost trekker in a wild terrain or observing and recording the movements of participants of outdoor camps or indoor seminars. The movements recorded could be studied and simulated in GloMoSim using the self-defined node placement and node mobility that could be fed into the configuration files already provided for this use in GloMoSim. This will definitely provide us the basis of a more accurate and closer to real life simulation environment.

In addition, due to the randomness of the simulation scenarios, a higher sample rate will yield more accurate results. In our tests, we conducted three runs using different seed numbers and different node numbers selected in random from the numbers 1 to 50 and 0 to 49 respectively. We arrived at running three runs mainly because three is a manageable number at the point of this study. The accuracy of the results could be further improved by conducting more runs with different seed numbers and higher sampling. However, as in every experiment design, arriving at the optimum sampling sizes can be of economical and practical reasons. Using a sample size too big, we could be over doing it and result produced would have no significant statistical impact and make very little the economical sense. Using a sample size that is too small, we risk having arriving at conclusions that are incorrect. There are resources and tools that can be utilise to calculate the correct sample sizes and this area calls for come research.

With reference to the abovementioned concerns of the randomness of mobility model, another ambiguity surfaced while the dissertation was in progress. More thoughts need to be brought into this area as many of the other configurations could be explored apart from mobility model, node speed and routing protocol. Where we could see no apparent effect, the configurations were left to default as per the original distributed configuration file in GloMoSim 2.03 distribution. A proper exploration on these other configuration could allow for a different set of configurations that may reflect a simulation environment that is closer to a potential use for mobile wireless ad hoc networks.

Lastly, another area that more research and study could benefit from is the metric suggested to improve or help predict the survivability of the links. In this dissertation, we suggested a simple incorporation of hop count as an additional metric apart from delay to help to predict the link survivability. The metric has not been looked into in a more mathematical and probabilistic perspectives. Guiding by the suggested idea that less hop counts to a path is better, a mathematical approach could be applied to come up with formula that best determines the attractiveness of a link compared to another in terms of better predicted survivability.

5.3 Conclusion

In conclusion, the proposed modified ODMRP by using an additional metric of hop count numbers in addition to delay as our route selection, was incorporated into basic ODMRP and tested in simulation using GloMoSim.

Our hypothesis for this study that the performance of the modified ODMRP is significantly better than the basic ODMRP is proven correct in some scenarios. We proved that the modified protocol performs significantly better in Multicast traffic in for most node speeds (except 5 m/s) and Multicast group sizes (except group size of 10) and the performance is more consistent across the varied scenarios than the basic protocol. However, for Unicast traffic, the performance of the modified ODMRP is insignificantly different than the basic ODMRP for all node speed, except for when the node speeds are at 5 m/s where the basic protocol performed significantly better (20%).

Many other areas of studies as mentioned in the above section has been suggested for a more detailed and comprehensive study to better determine if the idea suggested in this dissertation could indeed be a practical way of improving the performance of ODMRP by predicting survivability of links.

Reference

Anyu Gao, 2003 GloMoSim 2.03 Installation in Windows XP http://www.home.mylkcn.net/gaoanyu/glomosim.html

Hong, Xiaoyan; Gerla, Mario, Pei, Guangyu and Chiang, Ching-Chuan, 1999 A Group Mobility Model for Ad Hoc Wireless Networks in MSWiM 99 ACM Pg. 53-60

Lee, Sung-Ju; Su, William and Gerla, Mario (2001) Wireless Ad Hoc Multicast Routing with Mobility Prediction in Mobile Networks and Applications 6 Kluwer Academic Publishers The Netherlands Pg. 351-360

Lee, Sung-Ju; Su, William and Gerla, Mario (2000) On-demand multicast routing protocol (ODMRP) for ad hoc networks in IETF Internet Draft draft-ietf-manet-odmrp.02.txt

Lou, Wenjing and Fang, Yuguang, 2002 Predictive Caching Strategy for On-Demand Routing Protocols in Wireless Ad Hoc Networks in Wireless Networks 8 Kluwer Academic Publishers The Netherlands Pg.671-679

Nettstetter, Christian; 2001 Smooth is Better than Sharp: A Random Mobility Model for Simulation of Wireless Networks in MSWiM 2001 ACM Pg. 19-27

Paul, Krishna; RoyChoudhuri, Romit and Bandyopadhyay, Somprakash, 2000 Survivability Analysis of Ad Hoc Wireless Network Architecture in C.G. Omidyar (Ed.), MWCN 2000, LNCS 1818 Springer-Verlag Berlin Heidelberg Pg.31-46

Rajaraman, Rajmohan, 2002 Topology Control and Routing in Ad Hoc Networks: A Survey ACM Pg. 60-73

Sterbenz, James P.G. et. al., 2002 Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions in WiSe '02, September 28, 2002 ACM Pg 31-40

Uwe Herzog, 2005 "Ad-hoc networks - New life for an old concept" Online article on Eurescom mess@ge 1/2005 http://www.eurescom.de/message/messageMar2005/default.asp

Wang, Karen H. and Li, Baochun, 2003 Group Mobility and Partition Prediction in Wireless Ad Hoc Networks http://www.eecg.toronto.edu/~bli/papers/icc02.pdf

Yu-Liang Chang and Ching- Chi Hsu, 2000 Routing in wireless/mobile ad hoc networks via dynamic group construction in Mobile Networks and Applications 5 (2000) Baltzer Science Publishers BV Pg. 27-37

Zhou, Lidong and Haas, Z. J., 2003 Securing Ad Hoc Networks http://research.micorsoft.com/users/lidongz/adhoc.pdf