Efficient Route Discovery for Reactive Routing Protocols in Wireless Mobile Network

A thesis submitted for the degree of Doctor of Philosophy

By

Sofian Hamad

Department Electronic and Computer Engineering
School of Engineering and Design
Brunel University

February 2013

Abstract

Information on the location of mobile nodes in Mobile Ad-hoc Networks (MANETs) has the potential to significantly improve network performance. This thesis uses node location information to develop new techniques for route discovery in on-demand routing protocols such as the Ad-hoc On-Demand Distance Vector (AODV), thus making an important contribution to enhancing the experience of using mobile networks.

A Candidate Neighbours to Rebroadcast the Route Request (CNRR) approach has been proposed to reduce the deleterious impact, known as the broadcast storm, of RREQ packets flooding in traditional on-demand routing protocols. The main concept behind CNRR is specifying a set of neighbours which will rebroadcast the received RREQ. This is a departure from the traditional approach of all receiving nodes rebroadcasting RREQs and has the effect of reducing the problem of redundancy from which mobile networks suffer. The proposed protocol has been developed in two phases: Closest-CNRR and Furthest-CNRR. The simulation results show that the proposed algorithms have a significant effect as they reduce the routing overhead of the AODV protocol by up to 28% compared to the C-CNRR, and by up to 17.5% compared to the F-CNRR. Notably, the proposed algorithms simultaneously achieve better throughput and less data dropping.

The Link Stability and Energy Aware protocol (LSEA) has been developed to reduce the overhead while increasing network lifetimes. The LSEA helps to control the global dissemination of RREQs in the network by eliminating those nodes that have a residual energy level below a specific threshold value from participation in end-to-end routes. The proposed LSEA protocol significantly increases network lifetimes by up to 19% compared with other on-demand routing protocols while still managing to obtain the same packet delivery ratio and network throughput levels.

Furthermore, merging the LSEA and CNRR concepts has the great advantage of reducing the dissemination of RREQs in the network without loss of reachability among the nodes. This increases network lifetimes, reduces the overhead and increases the amount of data sent and received. Accordingly, a Position-based Selective Neighbour (PSN) approach has been proposed which combines the advantages of zoning and link stability. The results show that the proposed technique has notable advantages over both the AODV and MA-AODV as it improves delivery ratios by 24.6% and 18.8%, respectively.

Acknowledgments

I am grateful to the creator who taught the names to Adam and gave human beings authority to pass beyond the zones of heavens and earth; without his blessing and mercy, this thesis would not have been possible.

I owe my deepest gratitude to **my great parents**, my brother and sister, and especially to my wife and son, without whom I would not have made it through my PhD degree. Their tremendous help and prayers showed me the way and always guided me to the end of right way.

It is my pleasure to thank all those who made this thesis possible. I am heartily thankful to my supervisor, Professor Hamed Al-Raweshidy, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of this work. I appreciate all his help and support.

I am indebted to many of my colleagues at the WNCC and friends at Brunel University. I would like to show my gratitude to the National Council for Training - Sudan and the Sudan Academy of Sciences for funding my PhD in the UK; I would like to thank them for their encouraging and supportive attitude.

I would like to express gratitude to those who helped me to finalize my thesis; without them, I could not have written this thesis.

Lastly, I offer my regards to all of those who supported me in any respect during the completion of the project.

Table of Contents

List of Figures

List of Tables

List of abbreviations

AODV	Ad hoc On-demand Distance Vector
AP	Access Point
A-LSEA	Average Link Stability and Energy Aware
BSS	Basic Service Set
CNRR	Candidate neighbours to rebroadcast the RREQ
C-CNRR	Closest-CNRR
CN	Candidate Node
CL	Candidate List
CBR	Constant Bit Rate
CAP	Controlled Access Period
CBF	Contention-Based Forwarding
CFP	Contention Free Period
CS	Carrier Sensing
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CW	Contention Window
DSDV	Destination-Sequenced Distance Vector
DREAM	Distance Routing Effect Algorithm for Mobility
DCF	Distributed Coordination Function
DIFS	DCF IFS
DLA	Distributed Location Aided
DS	Distribution System
DSR	Dynamic Source Routing
EIFS	Extended IFS
ERP	Extended Rate PHY
F-CNRR	Furthest-CNRR
F-LSEA	Fixed Link Stability and Energy Aware
IBSS	Independent Basic Service Set
IFS	Inter Frame Spaces

LSEA	Link Stability and Energy Aware
LLT	Link Life Time
LAR	Location-Aided Routing
MAC	Medium Access Control
MANET	Mobile Ad-hoc Network
MA-AODV	Mobility Aware AODV
MPDU	MAC Protocol Data Unit
MPR	Multipoint relays
MSDU	MAC Service Data Unit
NS2	Network Simulator-2
NAV	Network Allocation Vector
OLSR	Optimized Link State Routing
OSI	Open Systems Interconnections
PSN	Position-based Selective Neighbour
PCL	Potential Candidate List
PCN	Potential Candidate Neighbour
PDR	Packet Delivery Ratio
PCF	Point Coordinated Function
PIFS	PCF IFS
PMD	PHY Media Dependent
PPDU	PLCP protocol data unit
PSDU	PLCP Service Data Unit
QoS	Quality of Service
RE	Remaining Energy
RREP	Route Reply
RREQ	Route Request
Rerr	Route Error
RTS	Request To Send
SAG	Stability Aware Greedy
SIFS	Short IFS
SSA	Sender Suppression Algorithm

STA	(IEEE 802.11 conformant) Station
TCL	Tool Command Language
TTL	Time to Live
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WMN	Wireless Mesh Network
WSN	Wireless Sensor Network
WiMax	Worldwide interoperability for Microwave Access

Author’s Declaration

The work described in this thesis has not been previously submitted for a degree in this or any other university and unless otherwise referenced it is the author’s own work.

Statement of Copyright

CHAPTER 1

Introduction

1.1 Introduction

This chapter presents a brief background to the problems to be investigated, the motivation behind the work, and the aim and objectives of undertaking this research. Further, the major contributions of the work and its research methodology are been described. Finally, this chapter briefly outlines the later chapters of this thesis.

1.2 Motivation

Wireless communication has become one of the most important communication paradigms worldwide due to its rapid technological growth and a sharp decline in deployment costs. Wireless access networks provide many alternative methods of on-the-go connectivity and have evolved into different types based on user requirements and their application scenarios, such as Wireless Mesh Networks (WMNs) [1], Mobile Ad-hoc Networks (MANETs) [2], Wireless Sensor Networks (WSNs) [3] and Worldwide interoperability for Microwave Access (WiMAX) [4]. All these wireless technologies have different application domains and vary based on end-users' bandwidth requirements, capacities and scalability.

MANETs have attracted enormous research attention and interest due to their promise to extend connectivity beyond traditional fixed infrastructure networks.

The motivation for this research thesis can be summarized as follows:

1- In MANETs, the routing task is distributed among wireless nodes which act as both data generating end-points and routers in wireless multi-hop network environments. Further, MANET nodes are spread across multiple collision domains. To discover a route to a specific destination node, existing on-demand routing protocols employ a broadcast scheme referred to as simple flooding, whereby a Route Request packet (RREQ) originating from a source node is blindly disseminated to all network nodes. This can lead to excessive redundant retransmissions, causing high channel contention and packet collisions in the network, a phenomenon called the broadcast storm problem [5].

To reduce the deleterious impact of flooding RREQ packets in the network, constant and even thorough research is required to improve the existing route discovery phase in on-demand routing protocols.

2- Nodes in a MANET rely on a limited battery source. Therefore, all node operations, such as reception, transmission and retransmission operations, consume battery power. For this reason, there is a high level of motivation to improve node energy performance in MANETs by taking care over each node's activity, allowing only selective necessary operations and discarding all others. There are several ways to improve performance or save node power in MANETs; for instance, the power management feature in 802.11 interfaces allows two modes of operation: power saving and active modes [6]. In the power saving mode, a node goes temporarily into sleep mode, with no activity, and awakens only at scheduled time intervals for short durations. While in the active mode, the wireless card is always ready to transmit or receive frames in accordance with the specifications of the 802.11 Medium Access Control (MAC) protocols.

The computational power of a mobile node cannot be neglected includes memory usage, processor processing times and I/O devices. Usually, these devices have low memory capacity and limited processing power. Therefore, algorithms for communication protocols need to be lightweight in terms of computational and storage requirements [7].

3- Mobility is the main feature of MANETs and all mobile nodes can move anywhere at any time without constraint. This feature makes routing between the nodes a very challenging task and more efforts are required to predict nodes' locations. Under normal conditions, any two nodes falling inside each other's transmission range can receive and transmit data between them. However, the connection between them is lost if either of them move out of that transmission range. Considering the high mobility in these types of networks, there is a high probability of link breakages over time between any two connected nodes in the network. For instance, consider an end-to-end path, consisting of multiple individual links, between any two nodes, N_1 and $N_{2,}$ in a multi-hop environment. Since some of the nodes in the end-to-end path have the potential to be cut off from communication due to their power limitations or mobility, the validity of the existing path cannot be guaranteed over time (short or long). The re-establishment of the broken link(s) depends upon the discovery of the end-to-end path between these two nodes through re-initiating the RREQ packets. These link breakages, which normally occur in MANETs, lead to more overhead and delays in the overall network. Therefore, estimating the Link Life Time (LLT) between any two nodes in the network and predicting when these two nodes will remain connected will assist and improve the performance of the network.

1.3 Statement and Aims of the Research

The on-demand route discovery process applies the simplest flooding method, where a mobile node blindly rebroadcasts the received RREQ packets irrespective of any knowledge of the required destination intended in the RREQ packet. This approach can potentially lead to the broadcast storm problem, which research [5] reports as affecting the network performance negatively.

A number of performance evaluation studies have demonstrated that the broadcast storm problem associated with route discovery operations can be reduced (*e.g.*, the neighbour knowledge [8] and probability [9] routing protocols). However, neighbour knowledge methods are expensive in terms of the overhead and most of the proposed route discovery solutions in this method have been evaluated under the assumption that a node has full knowledge of at least its one-hop neighbours. This mechanism requires a node to exchange information regularly with their neighbours, leading to more overhead in the network. Furthermore, probability-based routing protocols are not accurate and assigning a value based on probability does not give an accurate prediction of a highly mobile environment.

The aim and objectives of the research presented in this thesis can be summarized as follows:

- Firstly, to design an efficient routing protocol that can help to improve the route discovery phase. This routing protocol should:
  - Reduce overhead in the network while maintaining at least the same level of reachability as other routing protocols.
  - Allow only a specific set of nodes to rebroadcast the RREQ in cases where there is no available information in the routing table, to eliminate redundant RREQ packets.
  - Increase the network throughput as a normal reflection of reducing the overhead.

- Secondly, the research aims to design a MANET routing protocol where the route selection process takes into account the Link Life Time (LLT) between the nodes in the network to acquire stability in the end-to-end path. Considering the mobility of nodes in the MANETs, and selecting a path that contains long link lifetime among the nodes, involved in the end-to-end path, will reduce the costs of re-initiating RREQ packets to the minimum and will improve network performance overall.

- Thirdly, designing and developing a routing protocol that is aware of MANET characteristics, *i.e.,* especially constraints such as the energy/power limitation in the mobile node. The intelligent routing protocol should include only those nodes in the end-to-end path which have a good level of residual energy, rather than establishing a route containing nodes which have low residual energy and will soon be unavailable due to their batteries running out.

1.4 The Main Contributions

The key contributions of this research work are summarised as follows:

1. A new position-based routing protocol called Candidate Neighbours to Rebroadcast the RREQ (CNRR) has been specifically designed to reduce the overhead caused by blind flooding. CNRR makes use of the nodes' location information to select four neighbour nodes to rebroadcast the RREQ packets in cases where there is no fresh route in the routing table for the intended destination in the RREQ packet. It applies the source routing strategy according to the neighbours' distance from the source nodes perspective; the source/forwarder selects the four neighbour nodes. This source routing strategy has rarely been used in geographical routing protocols to improve the route discovery phase. The original flooding mechanism of the reactive routing protocols has been optimized into two phases:

   - Further Candidate Neighbours to Rebroadcast the RREQ (F-CNRR).
   - Closest Candidate Neighbours to Rebroadcast the RREQ (C-CNRR).

In both the above proposed routing algorithms, the hello message scale has been updated to carry the (x, y) coordinates of the nodes and allow neighbours to be aware of the position of the node. Furthermore, the RREQ packet has been modified by adding a CNRR field to carry the four candidate nodes' addresses. In F-CNRR the selection of the four candidate nodes is based on the distance between the sender and the neighbours, where the furthest nodes from the source/forwarder node which still lie within 80% of its transmission range are selected. The 80% threshold is set to ensure that the signal does not become very weak as a weak signal is likely to affect transmission and the data might be dropped. On the other-side, the C-CNRR selects the node that is closest to the sender/forwarder while being outside the first 20% of its transmission range, thus seeking to provide a wider coverage area if re-broadcasting by the receiving RREQ node occurs.

2. A new routing protocol that considers the Link Life Time (LLT) between the source/forwarder and the receiving nodes of the RREQ packet has been designed and developed. In addition, the protocol considers the Residual Energy (RE) of the node at the same time. By considering these two parameters in the establishing of the end-to-end route, the best available route in the network is guaranteed with respect to the LLT and the RE. A Link Stability and Energy Aware routing protocol (LSEA) has been developed to increase the stability of the selected routes and reduce the occurrence of broken links. The LSEA has been developed to contain two parts:

- Fixed Link Stability and Energy Aware (F-LSEA)
- Average Link Stability and Energy Aware (A-LSEA)

The key concepts behind the LSEA protocol are:

- On receiving the RREQs packet, the node must check the LLT (with the sender of the RREQ) and RE parameters.
- If the F-LSEA is applied as a routing protocol in the network and if both parameters are above the fixed thresholds, then the receiver node will forward the received RREQ packet. Otherwise, the receiver node will discard the received RREQ packet. The fixed threshold parameters (LLT, RE) are pre-defined in the F-LSEA routing protocol

and cannot be changed during working/simulation times unless F-LSEA is re-designed to a new fixed threshold.

- If the A-LSEA is applied as a routing protocol in the network, the node will gather all the neighbours REs through the hello messages, which have been modified to allow this. Furthermore, the receiver node will gather the LLTs of all its neighbours through the hello messages, which have also been changed to share LLT information between neighbours. Based on the computed LLT_{avg} and RE_{avg} , the receiver node compares its RE and LLT (LLT between the sender and itself) with the RE_{avg} and LLT_{avg} ,respectively.
- In both the proposed routing protocols, the receiver node will compare its LLT and RE with the fixed threshold for F-LSEA or compare it to the average threshold for the A-LSEA routing protocol. If the node have parameters above the threshold, the receiving node rebroadcasts the received RREQ; otherwise, it is discarded.

3. An intelligent routing protocol that can reduce the overhead to the minimum without losing reachability among the nodes has been designed and developed. The proposed routing algorithm tries to discover an end-to-end route, thus greatly reducing RREQ propagation in the network. The advantages of LSEA and CNRR have been further combined and improved to achieve better routing paths that can apply the zoning concept and select four candidate nodes from each zone based on their residual energy and LLT with respect to the sender/forwarder node. Furthermore, the candidate node applies an advanced algorithm to discover the number of nodes in its neighbourhood that have already received the same copy of the RREQ. This way, the candidate node will forward the existing RREQ if only 75% or fewer of its neighbouring nodes have received the same copy of the RREQ. The RREQ packet is discarded if more than 75% of the neighbouring nodes have already received the same RREQ. This helps further reduce RREQ flooding from dissemination inside the global network.

1.5 Research Methodology

The research methodology used for conducting the research presented in this thesis is summarized as follows:

1. The initial phase of this research focused on a literature review: books, relevant research articles, research papers that included conference proceedings and journal papers, IEEE standards, progress and proposals of IEEE task groups and different white papers on MANETs and their applications. Then the focus turned to on-demand routing protocols in MANETs, such as the Ad hoc On-Demand Distance Vector Routing Protocol (AODV) and Dynamic Source Routing (DSR), and highlighting the various issues that needed tackling.
2. A more comprehensive analysis of various published articles on routing protocols for MANETs was carried out, mainly involving on-demand routing protocols and how they perform their route discovery process.
3. A review of various MANET routing protocols, specifically those where the research focus was related to the flooding problem.
4. New routing protocols were suggested to overcome the problems that have been observed in the literature review and assumptions have been defined, such as the node being able to get its position using specific technologies such as Global Position System (GPS) [10].
5. Furthermore, the proposed routing protocols were designed, implemented and tested in NS-2 [11], which is an open source network simulator, and new models can be implemented using both C++ and the Tool Command Language (TCL).
6. Validation of the developed protocols and tests of the individual functions of the protocols in a simulation environment.
7. Performance tests and comparison of the proposed solutions with existing techniques.
8. A deep analysis and explanation was given of the obtained results.

1.6 Thesis Structure

This thesis consists of six chapters. Each chapter is structured independently. Conceptually, the chapters are inter-dependent and the reader should follow the right order in order to better understand the contributions presented in the thesis.

Following the introductory Chapter-1, Chapter-2 gives a brief overview of IEEE 802.11 WLAN technology and the principles and characteristics of MANETs. The fundamentals of the MAC and PHY layers and the main terminology used in the standard are given in Chapter-2, along with a summary of the DCF and PCF coordination functions. Alongside this, the advantages of MANETs and the various classes of routing protocols are also elaborated on, with a strong focus on on-demand and position-based routing protocols. Furthermore, Chapter-2 introduces the flooding problem in on-demand routing protocols. Chapter-3 gives detailed insight into route discovery techniques, analyses various aspects of such protocols and focuses on their implications for communication performance. This chapter presents two route discovery schemes and provides a detailed description of the different components of the CNRR protocol. It also describes CNRR simulation models and explains the output of the comparative analysis of different versions of CNRR (F-CNRR and C-CNRR) and the existing MANET protocols under various scenarios.

Chapter-4 presents studies of different energy and link lifetime routing schemes and analyses existing techniques and their implications for protocol performance. The chapter also describes the simulation model and the output results of the comparison between the proposed technique and the existing on-demand routing protocol flooding mechanisms. It also highlights the effectiveness of the inclusion of LSEA techniques in the route discovery phase.

Furthermore, Chapter-5 discusses the improvement in the route discovery phase as a normal result of reducing the propagation of RREQ in the network while maintaining the same delivery ratio level and reachability among network nodes. It also discusses the work presented in [12] and the simulation model and explains the output results. Furthermore, the proposed routing algorithm in this chapter is compared to CNRR and LSEA (proposed in the Chapters-3 and 4) and the original flooding techniques used in the on-demand routing protocols. In addition, the proposed protocols introduced in this chapter are compared with the (MA-AODV) [12], and an in depth analysis of the proposed work is presented.

Finally, Chapter-6 concludes the research findings of the thesis and presents future work to be carried out in connection with the presented research.

1.7 References

[1] Akyildiz, I.F., Wang, X. and Wang, W. "Wireless mesh networks: a survey", Computer networks, vol. 47, no. 4, pp. 445-487, 2005.

[2] Giordano, S. "Mobile ad hoc networks", Handbook of wireless networks and mobile computing, , pp. 325-346, 2002.

[3] Akyildiz, I.F., Su, W, Y. and Cayirci, E. "A survey on sensor networks", Communications magazine, IEEE, vol. 40, no. 8, pp. 102-114, 2002.

[4] Abichar, Z., Peng, Y. and Chang, J.M. "WiMAX: The emergence of wireless broadband", IT professional, vol. 8, no. 4, pp. 44-48, 2006.

[5] Tseng, Y.C., Ni, S.Y., Chen, Y.S. and Sheu, J.P. "The broadcast storm problem in a mobile ad hoc network", Wireless networks, vol. 8, no. 2, pp. 153-167, 2002.

[6] K. MAHMUD, M. INOUE, H. MURAKAMI, M. HASEGAWA, and H.MORIKAWA, "Energy Consumption Measurement of Wireless Interfaces in Multi-Service User Terminals for Heterogeneous Wireless Networks," IEICE Transactions Communications, vol. E88-B, pp. 1097-1110, March, 2005.

[7] T. Fuhrmann, "Scalable Routing in Sensor Actuator Networks with Churn," Proceedings of 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006. SECON '06, vol. 1, pp. 33-39, September 2006.

[8] Lee, S.H. and Ko, Y.B. "An Efficient Neighbor Knowledge Based Broadcasting for Mobile Ad Hoc Networks", Computational Science–ICCS 2006, pp. 1097-1100, 2006.

[9] Abdulai, J. "Probabilistic route discovery for Wireless Mobile Ad Hoc Networks (MANETs)", available at Glasgow University Library (http://www.gla.ac.uk), 2009. Retrieved in *June 2012*.

[10] Kaplan, E.D. and Hegarty, C.J. Understanding GPS: principles and applications, Artech House Publishers, ISBN 1-58053-894-0, 2006.

[11] Simulator, NS2. ns-2, http://www.isi.edu/nsnam/ns, 1989. Retrieved in *July 2012.*

[12] Khamayseh, Y., Darwish, O.M. and Wedian, S.A. "Ma-AODV: Mobility aware routing protocols for mobile ad hoc networks", Systems and Networks Communications, ICSNC'09. Fourth International Conference on IEEE, pp. 25, 2009.

CHAPTER 2

Mobile Ad-hoc Network: Concepts, Characteristics, Application and Routing

2.1 Introduction to Wireless Communications

Wireless communication has evolved very fast and become one of the most important means of allowing devices to communicate and share data. In fact, the development of the internet and its services has increased demand. Devices such as laptops, PDAs and mobile telephones can be easily obtained and these devices are used to connect wirelessly to the internet. Furthermore, wireless communication networks have more advantages than the traditional wired networks as they allow anytime, anywhere connectivity. They can be deployed in places without a pre-existing infrastructure or where it is difficult and expensive to run cables around the area. Furthermore, the installation of wired infrastructure networks is more expensive than that of wireless networks, making it an attractive option. There are many kinds of wireless communication and differences how they communicate and the frequencies they use. For instance, WiMax, WMN, MAN, Zigbee [1], WSN and MANET are all types of wireless communication.

To gain a better understanding of Mobile Ad-Hoc Networks (MANETs) it is important to describe the characteristics of WLAN Medium Access Control (MAC) and Physical (PHY) layers, as most of the MANET research work was based on those characteristics. Therefore, an introduction to MAC and PHY [2] layers will be given in the following sections.

2.2 Wireless Networking Overview

In wireless networking, data are sent between connected devices using radio frequency signals. Various types of wireless networks exist and can be grouped in different ways depending on the criteria chosen for the classification. Such criteria include the network architecture (infrastructure or infrastructure-less), network coverage (personal area networks, local area networks or wide area networks) and network applications (home, sensor, vehicular networks etc...).

2.3 Introduction to 802.11 Wireless Local Area Networks (WLANs)

2.3.1 Architecture

The 802.11 [3] network architecture, illustrated in Figure 2-1, consists of different elements that interact to provide a WLAN. These elements are the Basic Service Set (BSS), the Distributed System (DS) and the Independent Basic Service Set (IBSS).

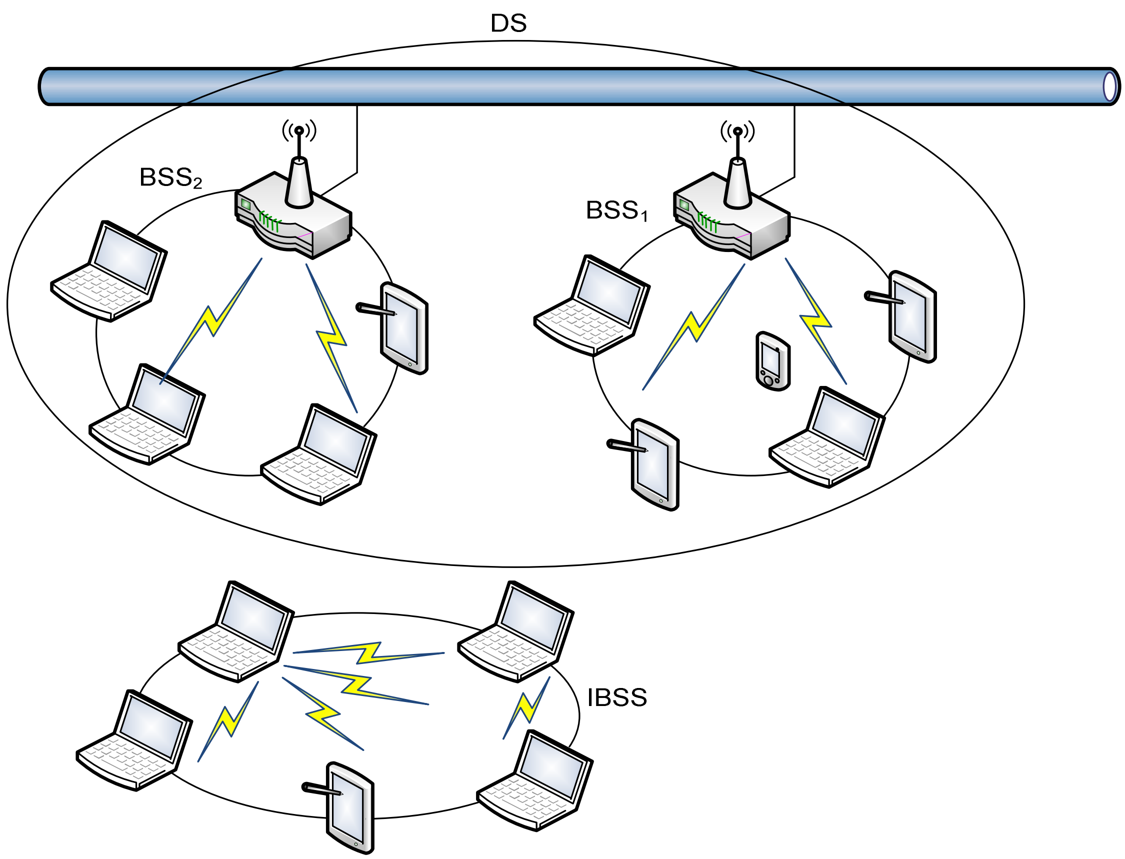

Figure 2-1: The architecture of 802.11 wireless networks

2.3.2 Basic Service Set (BSS)

The BSS constitutes the basic element of the 802.11 WLAN. It represents a group of wireless stations (STAs) controlled by a Coordination Function (CF). The coordination function is a logical set of rules that manage the stations' access to the wireless medium. The Distributed Coordination Function (DCF) is used by the STA as the basic coordination function, while the Point Coordination Function (PCF) is optional and can be used to support QoS traffic.

2.3.3 Independent Basic Service Set (IBSS)

A BSS that operates without a Distributed System (DS) is called an Independent Basic Service Set (IBSS). The WLAN is formed amongst the STAs without a pre-planning phase; for this reason it is called an *Ad-hoc Network*. The mode of operation in the IBSS involves direct communication between the STAs.

2.3.3.1 Distributed System (DS)

The DS is the architectural element defined by the 802.11 standard as interconnecting multiple BSSs. The DS provides the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs.

2.3.4 Medium Access Control (MAC)

2.3.4.1 Coordination Function (CF)

The 802.11 standard specifies the coordination function used by the MAC to manage access to the wireless medium. The basic coordination function is the Distributed Coordination Function (DCF); this follows the Carrier Sense Multiple Access (CSMA) technique, based on the concept of listen-before-talk. Another optional coordination function supported by the 802.11 MAC is the Point Coordination Function (PCF), used for traffic with QoS requirements. According to PCF, the stations are assigned priorities in accessing the medium coordinated by the Point Coordinator (PC), which usually resides in the Access Point (AP).

2.3.4.2 Carrier Sensing (CS)

DCF uses the Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) scheme to share the wireless medium amongst wireless stations. There are two possible ways of achieving this:

- *Physical-CS:* CSMA/CA implements a listen-before-talk scheme, according to which any node willing to transmit data must sense the wireless channel in order to determine whether another station is transmitting. If the channel is found to be idle, the station initiates the transmission; otherwise, the transmission is deferred for a random period. In addition, CSMA/CA employs an acknowledgment mechanism, in accordance with which the receiving station transmits an acknowledgment (ACK) packet back to the sender, after a short interval of time, to indicate successful reception. If the ACK packet is not received, the data packet is considered lost and a retransmission is scheduled.
- *Virtual*-CS: this optional "virtual carrier sensing" mechanism, specified in the IEEE 802.11 standard, is employed by the Request-To-Send/Clear-To-Send (RTS/CTS) handshake. Its purpose is to prevent wireless stations from accessing the wireless channel simultaneously. Therefore, it eliminates the interference caused by hidden stations and decreases packet collisions, which improves the network throughput. RTS/CTS packets are exchanged prior to data transmission, if the data frame size is larger than the specified RTS threshold, to reserve the wireless channel for the sending station. The process is initiated by the sending station, which senses the channel and sends RTS packets if it finds the channel idle. The sending station waits for a CTS packet from the receiver before it starts the effective data transmission.

2.3.4.3 Inter-Frame Spaces (IFS)

The time interval between adjacent MAC frames is called the "Inter-Frame Space" (IFS) which illustrated in the Figure 2-2. Various IFSs are employed to provide different priorities for the MAC frames. Four IFSs have been specified in the standard and are listed below from the shortest to the longest:

1. ***Short IFS (SIFS)***

   The SIFS is used before the transmission of the following frames:

   - An acknowledgment (ACK) frame of a data frame
   - A Clear-To-Send (CTS) frame of a Request-To-Send (RTS) frame

- A subsequent MPDU of a fragment of MSDU during fragment burst mode.

The SIFS is also used before responding to any polling in PCF mode and before any frames from the Access point during the Contention Free Period (CFP).

For instance, the SIFS for the 802.11a [4] MAC is 16 µs and 10 µs for the 802.11b/g [5, 6] MAC.

2. *Point Coordination Function IFS (PIFS)*

The PIFS is used to provide stations operating under PCF mode (APs) with the highest priority for gaining medium access.

3. *Distributed Coordination Function IFS (DIFS)*

The DIFS is used by stations operating under DCF mode to transmit data and management frames when the medium is determined to be idle.

4. *Extended IFS (EIFS)*

The EIFS is used by the DCF station whenever the physical (PHY) layer indicates that the frame reception contained an error or the MAC Frame Check Sequence (FCS) value was not correct. Therefore, the receiving stations should wait for a longer period before attempting to access the medium. The EIFS provides the other stations with enough time to complete their ongoing transmission before the STA that received the erroneous frame commences transmission.

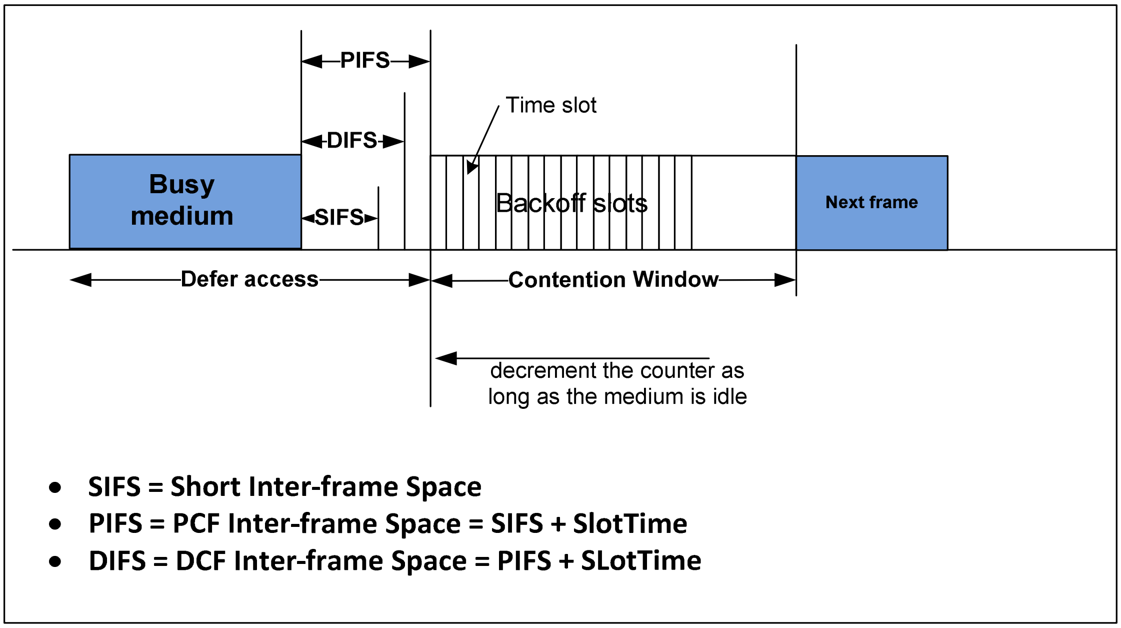

Figure 2-2: The different inter-frame spaces defined by the IEEE 802.11 MAC

The relationships between the different IFSs specified in the standard are defined by the following equations:

$$SIFS = aRxRFDelay + aRxPLCPDelay + aMACProcessingDelay + aRxTxTurnaroundTime \quad (2.1)$$

$$aSlotTime = aCCATime + aRxTxTurnaroundTime + aAirPropagationTime + aMACProcessingDelay \quad (2.2)$$

$$PIFS = SIFS + aSlotTime \quad (2.3)$$

$$DIFS = SIFS + 2 \times aSlotTime \quad (2.4)$$

$$EIFS = SIFS + DIFS + ACKTxTime \quad (2.5)$$

Some of the parameters in the above equations are PHY layer-dependent. The various characteristics of the different PHY layer specifications require the inter-frame spaces to be dependent on the transmission scheme in use.

- *aSlotTime*: a time unit in microseconds used by the MAC to define the PIFS and DIFS periods. The value of aSlotTime is dependent on the PHY characteristics, e.g. the aSlotTime is 9μs for 802.11a.

- *aRxRFDelay*: the nominal time in microseconds between the end of a symbol in the air interface and the moment the PMD indicates the arrival of data at the PLCP.
- *aRxPLCPDelay:* the nominal time in microseconds used by the PLCP to deliver the last bit of a received frame from the PMD to the MAC.
- *aMACProcessingDelay:* the maximum time in microseconds available to the MAC to change the PHY mode for either transmission or CCA.
- *aRxTxTurnaroundTime:* the maximum time in microseconds that the PHY requires to change its reception state to transmission state.
- *aCCATime:* the minimum time in microseconds available for the CCA to sense the medium and determine whether it is busy or idle.
- *aAirPropagationTime:* twice the time required by a signal to cross the distance between the most distant allowable STAs.
- *ACKTxTime:* the time in microseconds required to transmit an ACK frame at the lowest PHY mandatory rate.

2.3.4.4 Random backoff time

The CS mechanism is invoked prior to any frame transmission to determine whether the medium is busy or idle. If the medium is found to be busy, the STA defers its transmission for a time equal to DIFS if the last frame was correctly received or for a time equal to EIFS in the opposite case. When the CS reports the medium state to be idle after DIFS or EIFS, the STA must generate a random backoff period before attempting to access the medium. The random backoff period is used in order to minimise the chances of collision and is calculated as follows [6]:

$$BackoffTime = Random() \times aSlotTime \qquad (2.6)$$

Where Random() is a function used to generate a pseudo-random integer from a uniform distribution over the interval [0,CW]. The value of the Contention Window (CW) parameter varies between CW_{min} and CW_{max}. The initial value of CW is CW_{min} and is incremented to the next higher value after an unsuccessful transmission of an MPDU. When the CW reaches the value of CW_{max}, it remains at that value until the CW is reset.

2.3.4.5 DCF access procedure

The foundation of the DCF procedure is the CSMA/CA access method, which is implemented in all STAs for use in IBSS and infrastructure network configurations. When a STA has a frame to transmit, the CS mechanism is invoked to determine that the medium is idle for a period greater than DIFS or EIFS before proceeding with the transmission. The STA will then generate a backoff counter for an additional deferral time unless the counter has a zero value, in which case the STA is allowed to access the medium immediately. If the medium state changes to *busy* while performing the backoff, the STA freezes the backoff procedure and waits for the medium to become *idle* again.

The basic operation of the DCF procedure is illustrated in Figure 2-3.

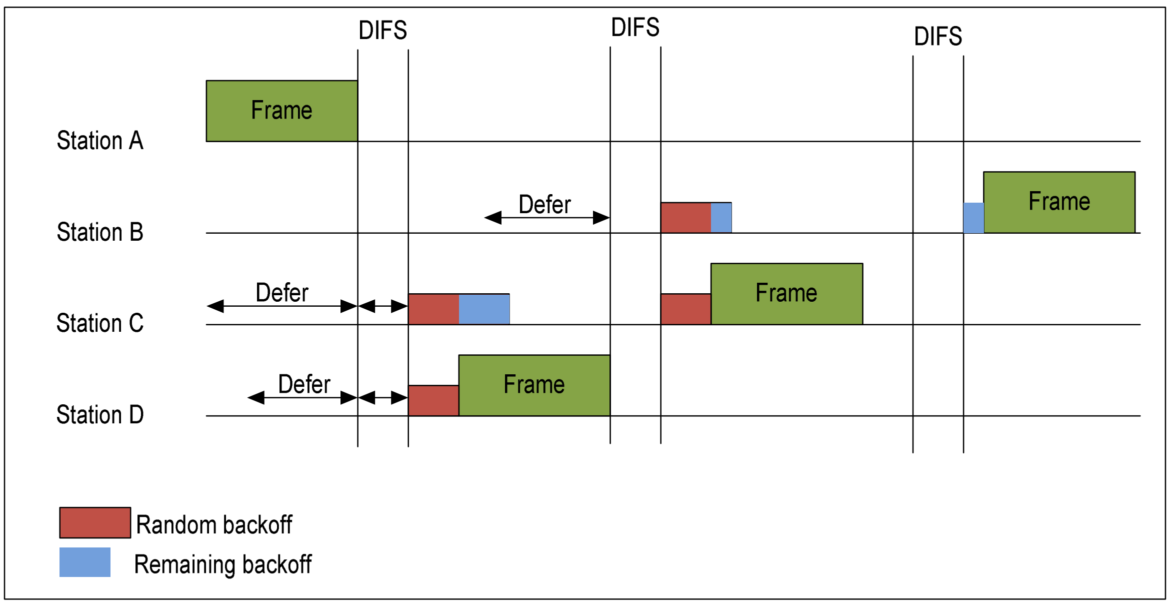

Figure 2-3: An example of the DCF operation

2.3.4.6 PCF access procedure

The optional PCF access method is used in infrastructure network configurations. PCF requires the use of Point Coordination (PC), which typically operates at the AP of the BSS in order to control the STAs' priority access to the wireless medium. According to PCF, the time is divided into repeated periods called superframes. The start of the superframeis indicated by the beacon, which is a management frame generated by the PC in order to synchronise the station timers and deliver a set of parameters. Furthermore, a superframe includes a

Contention Free Period (CFP).This uses the PCF access method followed by a Contention Period (CP), which involves the DCF access method. The Network Allocation Vector (NAV) is employed in order to protect PCF access from DCF access. In addition, PC maintains a polling list that includes the selected STAs that are eligible to receive CF-polls during CFP. An STA indicates whether or not to be placed on the polling list during the association process. After transmitting a beacon frame and indicating the start of the superframe, the PC waits for SIFS and sends a data frame, a *data+CF-poll* frame, a management frame or a CF-end frame. Finally, the duration of the CFP is represented by the *CFPMaxDuration parameter*. Given that no traffic exists and the polling list does not include any entries, the CFP can be terminated by the PC before *CFPMaxDuration*.

Figure 2-4 depicts the operation of the PCF access method.

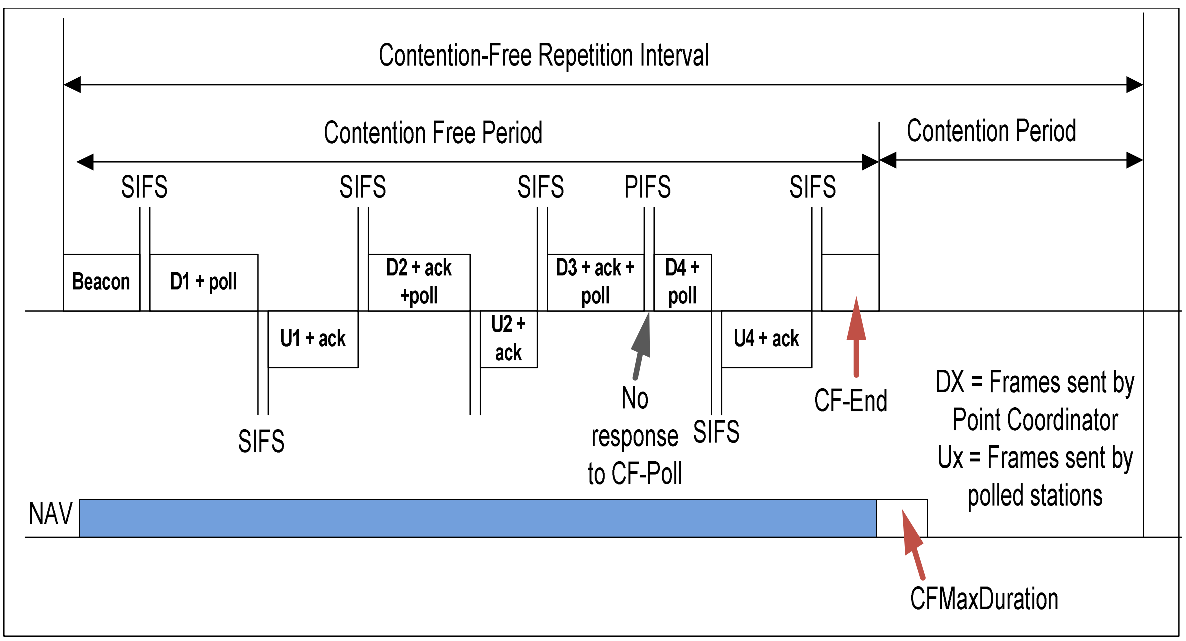

Figure 2-4: An example of DCF operation

2.3.5 PHY Layer

Different PHYs are defined in the IEEE 802.11 standard. Each PHY consists of two protocol functions:

1. A PHYMedia Dependent (PMD) system that defines the characteristics and method of transmitting and receiving data through the wireless medium amongst STAs
2. A PHY layer convergence protocol (PLCP) which defines a method of mapping the IEEE 802.11 MPDUs into a framing format suitable for sending and receiving user data and management information between the STAs using the associated PMD system.

A reference model of the 802.11 architecture showing the interaction between the PHY, MAC and higher layers is illustrated in Figure 2-5.

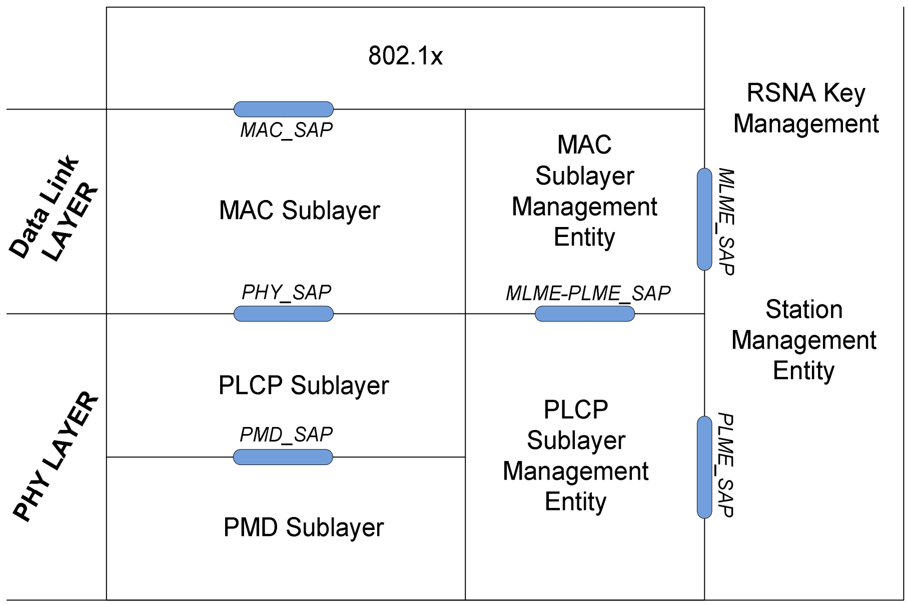

Figure 2-5: The protocol reference model for the IEEE 802.11 architecture showing the interaction of the PHY sub-layers with the MAC and higher layers

In order to transmit frames, PLCP forms what has been transferred from the MAC layer into PLCP protocol data units (PPDUs). The PPDU format consists of three parts: a PLCP preamble, a PLCP header and a PSDU. The PLCP preamble field allows synchronisation and defines the frame start. The PLCP header is used to specify the length of the whitened PSDU field and provide PLCP management information. The PLCP preamble and PLCP header are transmitted at 1 Mbps, while the PSDU can be transmitted at any supported transmission rate. The PLCP frame fields are depicted in Figure 2-6.

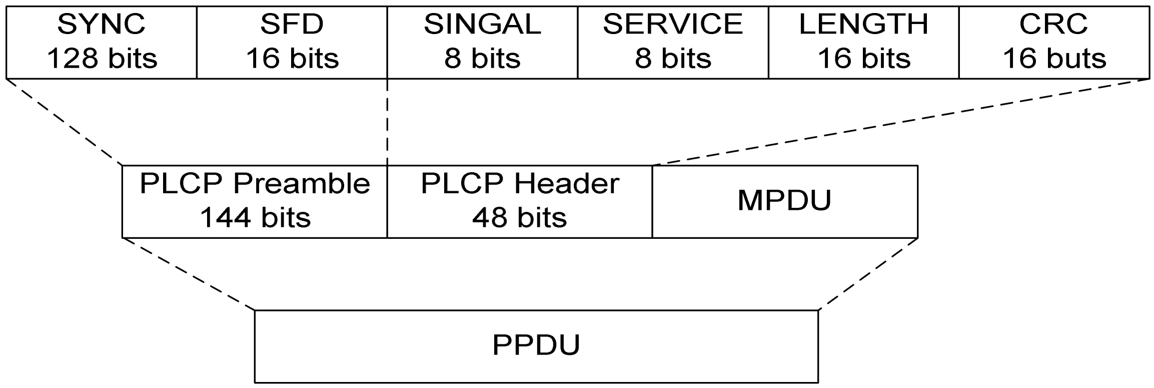

Figure 2-6: The PPDU packet format

Three different types of PYHs are defined in the original 802.11 standard, including the Frequency Hopping Spread Spectrum (FHSS), the Direct Sequence Spread Spectrum (DSSS) and Infrared (IR).

The static characteristics of FHSS-PHY, DSSS-PHY and IR-PHY are given in Table 2-1.

Table 2-1: The timing characteristics of FHSS, DSSS and IR PHYs

Characteristic	FHSS-PHY	DSSS-PHY	IR-PHY
aSlotTime	50 µs	20 µs	8 µs
aSIFSTime	28 µs	10 µs	10 µs
aCCATime	27 µs	≤ 15 µs	5 µs
aRxTxTurnaroundTime	20 µs	≤ 5 µs	0 µs
aRxPLCPDelay	2 µs	Any[1]	Any[1]
aRxRFDelay	4 µs	Any[2]	1 µs
aAirPropagationTime	1 µs	1 µs	1 µs
aMACProcessingDelay	2 µs	≤ 2 µs	2 µs

In addition, various extensions of the previously mentioned PHYs have been identified in order to increase the supported data transmission rate. The high rate DSSS (HR/DSSS) is an extension of the DSSS system which is designed to support higher payload transmission data rates at 5.5 and 11 Mbps. The Extended Rate PHY (ERP), which makes use of the Orthogonal

[1] Any value may be chosen as long as the requirements of *aSIFSTime* and *aCCATime* are met.
[2] Any valuemay be chosen as long as the requirements of *aRxTxTurnaroundTime* are met.

Frequency Division Multiplexing (OFDM) PHY, was developed to provide a data transmission rate of up to 54 Mbps. Table 2-2 illustrates the various PHYs and their supported data rates, taking into consideration the 2.4 GHz ISM band.

Table 2-2: The supported data rates of the various 802.11 PHYs

PHY	Supported Data rate (Mbps)
FHSS	1,2
DSSS	1,2
IR	1,2
HR/DSSS	1,2,5.5,11
ERP	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 and 54

Various 802.11 sub-standards have been defined based on the different PHY specifications and the frequency band used. The 802.11a operates in the 5 GHz frequency band and uses the OFDM PHY to support a data rate of up to 54 Mbps. The 802.11b and 802.11g operate in the same 2.4GHz frequency band; however, the 802.11g PHY is based on OFDM to provide high data rate of up to 54 Mbps. Table 2-3 depicts the values for the MAC parameters of the various IEEE 802.11 standards.

Table 2-3: Some MAC parameters in microseconds for different PHYs

802.11x	*SIFS*	*DIFS*	*Slot Time*	*CWmin*
802.11a	16	34	9	15
802.11b	10	50	20	31
802.11g	10	50	20	15

Figure 2-7 depicts the wireless channels of the 2.4 GHz frequency band allocated to the 802.11 standard, showing the three non-overlapping channels.

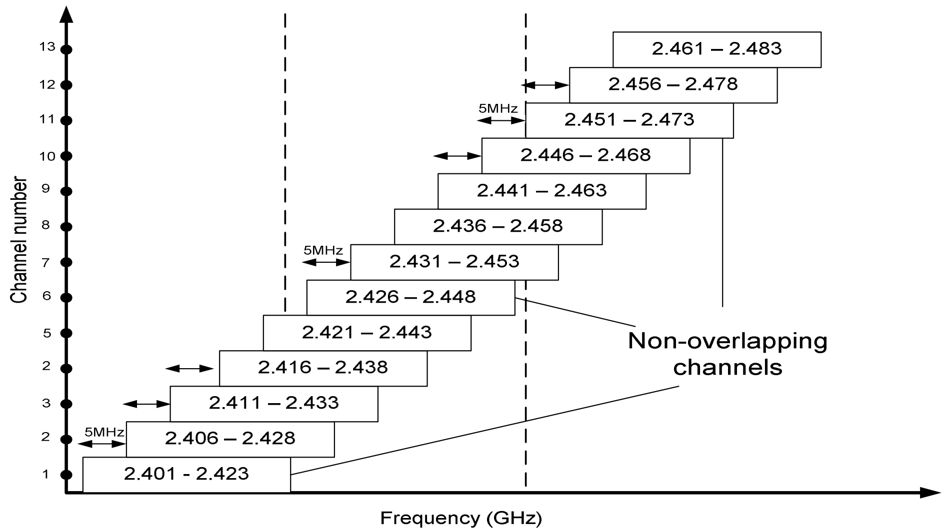

Figure 2-7: The wireless channels of the 2.4 GHz frequency band

2.4 MANET: An Introduction

MANETs are characterized as networks where the nodes are interconnected via wireless links in the absence of any fixed infrastructure. The topology of the network is very de-centralized due to the absence of a central authority in the network [7]. The network topology in a MANET can change hastily and arbitrarily because of the random motion of the nodes anywhere and at anytime. Unlike in many other wireless access networks, MANET nodes act as data-generating points/clients as well as relaying data for other nodes in a multi-hop environment. Figure 2-8 shows an example of a MANETs where the nodes on the left hand side of the topology create an ad-hoc wireless set-up to relay each other's data in a multi-hop fashion. As can be seen from the figure, MANETs can optionally be connected to external networks/the internet through WLAN access points.

MANET applications can be found in situations where rapid deployment of a network is necessary without a pre-planned existing infrastructure.

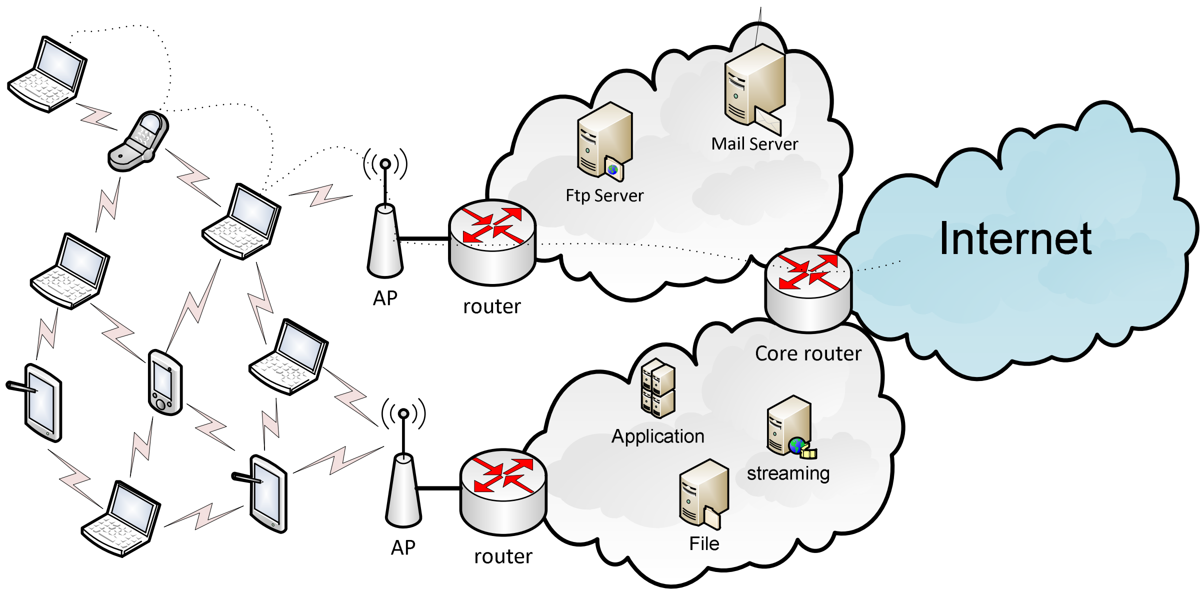

Figure 2-8: An instance of a MANET connected to external networks

2.4.1 MANET Characteristics

MANETs inherently belong to the category of wireless access networks as they share some common characteristics with all of them. However, there are some characteristics which distinguish them from the rest. Below are some of the characteristics of the MANETs.

- *Wireless medium*: since MANET nodes share a common wireless medium to communicate with each other, the problems of interference from other transmissions and link interferences cannot be entirely avoided. MANETs suffer from the same transmission and interference phenomena as all other access technologies [8,9].
- *Multi-hop communications*: MANET nodes are deployed in a multi-hop fashion. This means that the disjoint sets of nodes belong to different collision domains. This helps the nodes to achieve non-line-of-sight communication through multi-hop forwarding.
- *Autonomous and infrastructure-less:* MANETs do not have a permanent infrastructure and therefore the nodes join and leave the network freely. Similarly, MANETs are formed very fast and the initiating operation time is very low due to there being no centralized authority.

- *Mobility and dynamic topology:* one distinguishing feature of MANETs is that the nodes of the network may be extremely mobile. This gives an edge to MANETs over all other access technologies because extremely mobile nodes can be accommodated in the network at any scale. Further, this characteristic of MANETs enables them to accommodate application scenarios where node mobility is required. However, the mobility of the nodes gives rise to the fundamental problem of link breakages as the nodes act as the generating as well as forwarding entities inside the network.
- *Limited energy:* since the MANET nodes are mobile, one of the constraints of the non-stationary node is limited energy. The nodes rely on non-permanent power supplies such as batteries. For this reason, much research has focused on energy-efficient protocol design for MANETs.

2.4.2 Application

MANET networks can be deployed in different application scenarios, ranging from those as simple as conferences and shopping malls to complicated high-risk emergency services and battlefield operations [10-12]. In the following sub-section we outline some of the most important MANET applications. Readers interested in finding out more about MANET applications in the real world can refer to the study of [11] for more details.

2.4.2.1 Civil and Commercial Applications

Two promising application scenarios, which are likely to become part of daily life, are vehicular communication and wireless personal communication. Vehicularcommunicationhas most potential in urban areas, where it is predicted that most cars will have a wireless device to monitor the vehicle’s mechanical components, enabling faults to be reported instantly. Furthermore, another wireless network scenario is to provide vehicles with the ability to communicate with other vehicles on the road. Possible applications include coordinated navigation and other peer-to-peer interactions, avoiding congestion and providing road safety messages. Also, Personal Area Networks (PANs) are currently formed between various mobile (and immobile) devices, mainly in an ad-hoc manner. For example, on a university campus students can form small workgroups to exchange files and share presentations, results etc. At conferences, participants can connect their laptops or PDAs to share files and other network services. However, PANs will become more useful when connected to a larger network. Used in this way, PANs become extensions of the telecom network or the internet. Similarly, PANs could be used in smart grids, where the communication of the real time data would be achievable via multi-hop communication for the efficient utilization of electricity. Closely related to this is the concept of ubiquitous/pervasive computing, where people, whether transparently or not, will be in close and dynamic interaction with devices in their environment.

2.4.2.2 Emergency Services

One important MANET application scenario is in disasters or rescue and emergency situations. In such scenarios, conventional access technologies cannot be applied because a permanent infrastructure is necessary for network deployment. In some situations, *i.e.* earthquakes and tsunamis, all other networks are destroyed due to the level of the disaster. Due to the infrastructure-less characteristics and self-configuring nature of MANETs, however, networks can be easily deployed and configured in such situations.

2.4.2.3 Battlefield Operations

In battlefield operations each jeep, or even soldier’s gun, has the ability to include a wireless card. These nodes can together form a MANET network and communicate with each other on the battlefield. In future battlefield operations, autonomous agents such as unmanned ground vehicles and unmanned airborne vehicles will be sent to the front line for intelligence, surveillance, enemy anti-aircraft suppression, damage assessment and other tactical operations. It is envisaged that these agents, acting as mobile nodes, will organise themselves into groups of small unmanned ground, sea and airborne vehicles in order to provide fast wireless communication, perhaps participating in complex missions involving several such groups. Examples of such activities might include coordinated aerial sweeps of large urban/suburban areas, reconnaissance of enemy positions in the battlefield etc [12].

2.5 Routing in MANET

Routing protocols in MANET can be classified into different types using various criteria. Such criteria include how the routes to the destination nodes are established (reactive or proactive), the topological structure (flat or hierarchical), the routing method (hop-by-hop or source routing) and the type of information that the protocol relies on to perform the routing process (link or position). Based on the latter, routing in MANETs is classified into topology-based and position-based.

2.5.1 Topology-based Routing

Topology-based routing protocols perform routing based on link information. These types of protocols maintain a routing table where they store topological information that will be used in the routing process. Topology-based routing can be classified into three types based on how a node will discover other nodes in the network: reactive or on-demand, proactive or table driven and hybrid routing protocols. On-demand routing protocols discover routes when needed and the routing table is small compared to that of proactive routing protocols. Meanwhile, proactive routing protocols periodically make changes in the topology to maintain updated routes to all the destinations in the network. The way that proactive routing protocols maintain an up-to-date routing

table increases the overhead as the nodes send update messages in response to any change in the topology; on the other hand the proactive routing protocols reduce the delay in the on-demand routing protocols as the routes is always available when needed. Hybrid routing protocols combine the advantages of both of the previously mentioned schemes. Accordingly, the network area is divided into zones. Communication within the zone (intra-zone) is performed in a proactive manner, while routing between the zones (inter-zone) is performed reactively.

2.5.1.1 Ad-Hoc On-Demand Distance Vector (AODV)

One of the most famous routing protocols is AODV [13], which is a reactive routing protocol using the hop-by-hop routing protocol concept that discovers routes to the destination when needed. When a node running an AODV algorithm has data to send, it initiates the route discovery process if there is no information available in the routing table for the requested destination. The AODV protocol uses the broadcasting technique, which is the process of sending or flooding a Route Request (RREQ) message to the neighbouring nodes. Any neighbours falling within the transmission range of the node sending the RREQ will receive this RREQ. Any intermediate nodes receiving the RREQ message will continue to rebroadcast the received RREQ if they do not have a valid route in their routing table. This broadcasting will continue across the entire network until the RREQ reaches either the destination node or an intermediate node with a valid route to the destination. Upon receiving a RREQ message, an intermediate node creates or updates a route to the previous sender of the RREQ. The received RREQ is discarded if the node has received a RREQ with the same originator and RREQ ID within, at least, the last PATH_DISCOVERY_TIME. The node then checks whether a valid entry for the destination exists in its table. If this is the case, a Route Reply (RREP) message is unicasted back to the originator of the RREQ using the already created reverse path. The same procedure is followed if the RREQ reaches the destination node. If no valid entry is found in the table, the RREQ message is rebroadcasted after incrementing the hop count value by one. Moreover, the AODV uses a sequence number field in its control messages to determine the freshness of the information acquired from the originating node. When the source node receives multiple RREPs, the route with the lowest hop count value is selected.

The propagation of the RREQ is controlled by an expanding ring search technique. The originator of the RREQ sets the Time-To-Live (TTL) of the IP header to TTL_START and waits for a RING_TRAVERSAL_TIME before attempting to broadcast the RREQ with an incremented TTL.

This continues until the TTL of the RREQ reaches the TTL_THRESHOLD, after which a TTL = NET_DIAMETER is used for each subsequent attempt. In addition, the nodes of an active route monitor the link status of the next hops. If a link breakage is detected, a Route Error (Rerr) message is flagged to notify the other nodes and to indicate the destinations that are no longer reachable through the broken link. Finally, as a part of an active route, the mobile node periodically broadcasts hello messages. The broadcasting of hello messages is restricted to the one-hop neighbourhood.

2.5.1.2 Distance Source Routing (DSR)

In the DSR routing protocol the entire route to the destination is discovered and consequently made known to the source node prior to data transmission [14]. Similarly to the AODV, the discovery process is initiated when a source node attempts to transmit data to a destination node with an unknown route. The source node broadcasts a RREQ message throughout the network until the requested destination node or an intermediate node with a valid route to the destination is reached. The DSRRREQ packet is different from AODV's as the former contains the entire discovered route. Upon receiving a RREQ, the node checks its cache for a valid route to the requested destination. If no route is found in the cache, the node adds its address to the RREQ and rebroadcasts it further. If, however, the node has a valid route to the RREQ destination, the complete route (the route included in the RREQ + the cached route) is copied to a RREP message and is sent back to the source node. Finally, when the destination node is reached, it simply sends a RREP to the originator of the RREQ by reversing the route recorded in the RREQ.

DSR introduces the concept of *route salvaging,* according to which an intermediate node uses an alternative route from its cache to the packet's destination when the next hop link along the packet's route is detected as broken. Therefore, the node *salvages* the packet rather than discarding it by replacing the original source route of the packet with the route of its cache.

In addition, DSR uses a *route shortening* mechanism, which is applied when one or more intermediate nodes become unnecessary to the route.

2.5.1.3 Optimised Link State Routing (OLSR)

The OLSR is proactive routing protocol where the shortest routes to all possible destinations in the network are discovered in advance by regularly exchanging topological information among the mobile nodes [15]. OLSR significantly minimizes the routing overhead by handing the control traffic dissemination process over to Multi-Point Relays (MPRs),which continuously maintain the routes to destinations. Each node in the network selects MPRs in its symmetric 1-hop neighbourhood to forward its messages. The selection is performed in such a way that the selected MPRs cover all symmetric 2-hop nodes. Therefore, any two-hop neighbour of a node ‘N’ must have a link to one of the MPRs of N. Each MPR maintains information about the set of neighbours that has been selected, called the MPR-selector set, through its received hello messages.

Changes in the network topology are advertised across the entire network by the selected MPRs. Each node selected as MPR must at least disseminate the links between itself and the nodes in its MPR-selector set in order to build a link information base. Each node maintains a routing table that contains routing entries to each destination in the network based on the link information base. Therefore, any changes occurring in the topology result in re-calculations of the routing table.

A routing entry consists of four fields: <R_*dest_addr, R_next_addr, R_dist*and *R_iface_addr*>, meaning that the destination node *R_dest_addr* is *R_dist hops* away from the current node and the next hop node in the route is *R_next_addr*, reachable through the interface *R_iface_addr*.

2.5.2 Position-based Routing

2.5.2.1 Existing Position-based Routing Protocols

Several researchers have proposed improving routing performance in MANETs by making location information available at the nodes to enhance the routing performance. A survey of position-based routing algorithms is extensively discussed in [16] and [17]. Below, we highlight several location-based routing protocols which consider the locations of nodes when designing protocols.

A. Greedy forwarding schemes:

Algorithms that use a greedy forwarding strategy which selects a neighbour that satisfies specific criterion as the next hop relaying node are proposed in [18], [19], [20] [21], [22], [23] [24], [25] and [26]. A random progress method is proposed in [18], according to which packets destined for a destination node D are routed with equal probability towards any one neighbouring node that makes progress in the direction of D. The source node will select among the (n) neighbours in one terminal located in the direction of the destination D as all neighbours have the same probability (1/n). Progress is defined as the distance separating the transmitter and the receiver projected onto the line joining the transmitter and the final destination. In [19] a variant of random progress method called Cartesian Routing is proposed. Progress in Cartesian Routing is defined as the distance between the transmitter (X_t, Y_t) and the final destination (X_d, Y_d). According to this, packets are forwarded to any direct neighbour (X_i,Y_i) for which the distance [(X_i, Y_i) to (X_d, Y_d)] is less than the distance [(X_t, Y_t) to (X_d, Y_d)]. If no direct neighbour closer to the destination is found, on the condition the network is an n-Cartesian regular one a search of no farther than (n-1) hops will lead to a node that makes progress. According to [19], a network is called n-Cartesian regular if for any transmitter node T and any destination node D some other node Ni exists within n-hops of T and closer to D. Takagi and Kleinrock [20] proposed the Most Forward within Radius (MFR) routing algorithm. MFR forwards the packet to the next neighbour that maximizes progress. Progress is defined as the distance between the transmitted node and the neighbouring node projected onto the line joining the transmitter node and the final destination. In the MFR strategy, a case might arise where the selected neighbour providing maximum progress is further from the destination. The Nearest with Forward Progress (NFP) routing algorithm is introduced in [21], where the nearest neighbour with forward progress is selected as the next hop node. Furthermore, greedy forwarding schemes are characterized by routing data packets while relying on the positions of one-hop neighbours only. However, there are topologies in which some of these schemes fail to deliver the packet to the destination even though a route exists, e.g. a topology where the node itself is closer to the destination than any of its neighbours. This case is referred to as local maxima. The Greedy Perimeter Stateless Routing (GPSR) algorithm proposed in [22] maintains information about its direct neighbours' positions to make a routing decision. It consists of two methods of packet forwarding: greedy forwarding and perimeter forwarding. The GPSR header includes a field indicating whether the packet is in greedy mode or perimeter mode. Upon receiving a packet for forwarding, a node applies the greedy scheme and searches for the neighbour geographically closest to the destination. When no neighbour is closer to the destination than the node itself, the packet is marked as perimeter and forwarded using simple planar graph traversal.

In [23] Stojmenovic and Lin proposed two-hop flooding GEDIR, two-hop flooding MFR and two-hop flooding DIR, comprising modifications of GEDIR [24], MFR and compass routing schemes to avoid packet dropping. The proposed algorithms are referred to as 2-f- GEDIR, 2-f- MFR and 2-f- DIR respectively. The main idea behind these variants is that the transmitter nodes choose the closest terminal to the destination from among all the first and second hop neighbours apart from a concave node that floods the packet to all its neighbours. A node is called concave if it is the only neighbour of the node selected for forwarding closer to the destination. Greedy Routing with Anti-Void Traversal (GAR) is introduced [25] to solve the void problem of greedy forwarding schemes by exploiting the boundary finding technique for the unit disk graph (UDG). A rolling-ball UDG boundary traversal (RUT) technique is further proposed in [25] to solve the boundary-finding problem.

Liu and Feng have developed the Largest Forwarding Region (LFR) [26] routing protocol, which selects the neighbour that possesses the largest Extended Forwarding Region (EFR). EFR is associated with every neighbour containing both the distance and the direction information related to the destination. Note that the forwarding region is defined as the area including the closest nodes to the destination. Furthermore, Backward Constraint (BC) and Dead End Recovery (DER) mechanisms are defined to resolve backward loops and dead-end problems in the network. Although LFR resolves the problem of voids in the network by transmitting the packet back to the concave node, it would be more efficient not to consider nodes that lead to voids at all, as will be shown in this paper.

B. Directional routing schemes:

Directional routing methods that rely on the destination direction to select the next forwarding node are discussed in [27], [28], [29], [30] and [31]. In the Compass Routing presented in [27], the transmitter node T (source or intermediate node) forwards the packet to the closest neighbour N to the destination D that minimizes the angle (TND). The same procedure is applied at every intermediate node until the packet reaches the destination. In [28] Ko and Vaidya demonstrate, with their Location Aided Routing (LAR) protocol, how the utilization of location information can improve the flood mechanism of route discovery messages and hence reduce the routing overhead. In LAR, the source node defines the zone where the destination is expected to be based on the location information of the destination and the speed that the destination can reach. The source node only broadcasts the discovery request within the request zone, which is the smallest rectangle formed by the expected zone and the source node's position. Two LAR algorithms are also presented in [28]: LAR scheme-1 and LAR scheme-2.These differ in the manner in which the request zone is specified in the request message. In scheme-1, the zone is specified explicitly by the source node, while in scheme-2 it is implicitly specified as the source includes additional information about the destination coordinates and the distance to the destination in the request message. Although LAR reduces the routing overhead as it reactively discovers a route to the destination, it still requires the maintenance of an explicit path between every source and destination prior to data transmission. In [29], a Location Aided-Routing algorithm challenge is discussed and an improved version of the protocol is presented. Although the destination node receives a request from different routes during the route discovery phase it only responds to the earliest request received. Therefore, any later route breakages will lead to a new route discovery process. The author proposes selecting a back-up route as a secondary route in cases failures in the primary route. Location Aided Knowledge Extraction Routing (LAKER) [30] utilizes a combination of a caching strategy in Dynamic Source Routing [14] and limited flooding in Location-Aided Routing [28]. The idea of LAKER is to learn the topological characteristics of the network and use this information to guide the route discovery more precisely in the request zone. Simulation results show that LAKER saves up to 30% more of the broadcast messages than LAR. A variant of the LAR protocol is Multipath Location Aided Routing in 2D and 3D, referred to as MLAR [31], which is designed to work efficiently in three dimensions by using an alternate path caching strategy. MLAR caches several paths, although one path is used at a time and the others are alternate routes to be used when the primary path fails.

The Distance Routing Effect Algorithm for Mobility (DREAM) has been proposed by Basagni et al. [32]. DREAM represents an all-to-all location service that disseminates and updates nodes' locations throughout the entire network. The frequency of updates is determined based on the distance between the nodes and the mobility rate. Data packets are transmitted to all one-hop neighbours that lie in the direction of the destination represented by the angular range that includes the node's position, the destination's position and the zone that the destination is expected to be in. The same procedure is applied at every node until the destination has been reached. Although transmitting data packets through multiple paths may increase the probability of reaching the destination, the protocol lacks scalability due to the communication overhead and data message redundancy.

C. Hierarchical routing schemes:

The hierarchical approach is discussed in [33] and [34]. The GRID protocol discussed in [33] exploits location information in route discovery, packer forwarding and route maintenance. It considers MANETs as 2D logical grids controlled by grid gateways. Packet routing is performed in a grid-by-grid manner and the gateway hosts are responsible for discovering and maintaining the routes and forwarding data packets to the neighbouring grids. In [34] Blazevic et al. proposed Terminode routing, which combines location-based routing and link state routing. Location routing, referred to as Terminode Remote Routing (TRR), is used when the destination node is far away, while link state routing, referred to as Terminode Local Routing (TRL), is used when the destination is up to two hops away. Moreover, the concept of anchors, which represent imaginary geographical locations installed in the packet header to assist in the routing process, is introduced. In Position and Neighbourhood-based Routing (PNR) [35], the network is represented by a set of quadrants. The quadrants are organised in a hierarchical manner where each higher level quadrant is divided into four lower level quadrants. PNR requires each node to initiate an initial flooding as a start-up phase. Any node moving more than a pre-defined distance must send an update packet. The dissemination of the update packets is optimised using the concept of quadrants. Accordingly, when receiving an update packet the node maintains the exact location of the packet originator if they are in the same quadrant, or it stores the quadrant that the originator belongs if they are not in the same quadrant. Routing is based on the shortest path, using the concept of greedy forwarding.

D. Other schemes

The GPS/Ant-Like Routing Algorithm (GPSAL) routing protocol is described in [36]. The key point of GPSAL is that the mobile software agents are modelled on ants so as to disseminate and collect nodes' location information more rapidly. An ant holds a routing table and is transmitted to a specific destination. Upon receiving an ant packet, older entries are updated by the current host and the ant is passed to another node, carrying the most up-to-date routing table. The same procedure is followed until the ant has reached its destination, at which point it is sent back to the node that created it. In [37] Zeng et al. Introduced the Geographic On Demand Disjoint Multipath routing protocol, to be used instead of blind flooding route discovery in the network. Every node knows the position of its one-hop neighbours. Before transmitting a route request (RREQ) message, the source node selects the k nearest neighbours to the destination and includes their addresses in the packet. Upon receiving the RREQ, only intermediate nodes which have their addresses stated in the packet forward the request, after selecting a new list of nearest neighbours to the destination. This is repeated until the destination has been reached, which in turn transmits a route reply (RREP) message back to the source. In addition, the authors described two schemes: Geographic Node-disjoint–paths routing and Geographic Edge-disjoint-paths routing. The difference between these schemes lies in the processing of the duplicate RREQ messages. While the first scheme drops all duplicate RREQs, edge-disjoint routing may forward duplicate RREQs which have been received from different neighbours.

[38], [39] and [40] present recent work on developing different geographic routing algorithms. Predictive Mobility and Location Aware Routing (PMLAR) [38] predicts the movement behaviour of the mobile nodes to assist the routing operation. PMLAR is designed in such a way that the source node predicts the current and the future locations of the destination to increase routing efficiency. The prediction is based on a previous update on the destination's location, acquired through a location service. To transmit data packets the source node determines the predicted zone, which is expected to include the potential future position of the destination. The route discovery process is then initiated to establish a valid route to the destination. During the discovery phase, the intermediate nodes apply the Velocity-Aided Routing (VAR) mechanism to ensure that the RREQ is forwarded by nodes that are moving toward the destination along their connecting lines. In [39], Location-Aware Routing for Delay tolerant networks (LAROD) is proposed, which is a beacon-less routing protocol designed for intermittently connected MANETs that combines the store-carry-forward technique with geographical positioning. LAROD consists of an enhanced location service and a location dissemination service to update the nodes' location information. Finally, a Prediction-Based Routing (PBR) protocol for vehicular ad hoc networks is proposed in [40]. PBR takes advantage of the predictable mobility patterns of vehicles on highways to predict route lifetimes and pre-emptively create new routes before existing ones fail.

2.5.2.2 Distance Routing Effect Algorithm for Mobility (DREAM)

DREAM [32] is a hop-by-hop position-based routing protocol, specifically designed for mobility, which proactively disseminates location information across the network. Each mobile node maintains a Location Table (LT), which contains the location information of all the other nodes. Therefore, when a source node wants to transmit data to a specific destination, it refers to the LT to select all its one-hop neighbours in the direction of the destination that will be the next hop forwarding nodes. The same process is applied at every intermediate node until the destination is reached. The direction of the destination, as shown in Figure 2-9, is defined as the sector formed by the source node and the zone in which the destination node is expected to be located.

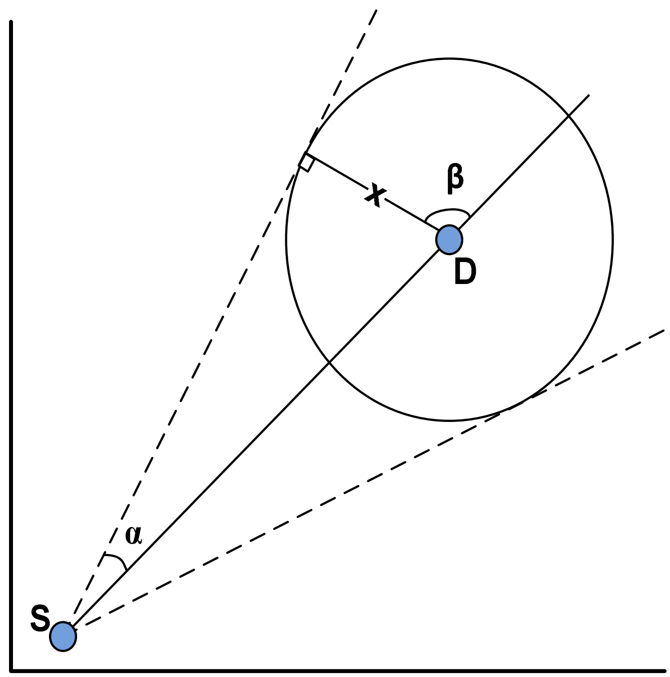

Figure 2-9: The direction of a destination node D, where x is the maximum distance that D can travel during t1-t0. t0is the time at which the information on D was received and the t1 is the time taken to send data to D

Each node periodically broadcasts a control packet containing its own coordinates. To control the routing overhead injected into the network, DREAM uses the distance effect, according to which the further apart the two nodes are, the slower they appear to be moving with respect to each other and, subsequently, the less their LTs need updating. Therefore, an age parameter is associated with every control message to limit the distance that the message travels from the sender. Alongside this, DREAM introduces a mobility rate factor to determine the frequency at which the control packets are transmitted. Accordingly, the faster the node moves, the more often it must communicate its location.

Furthermore, DREAM supports two types of control messages: short-lived and long-lived. Every node periodically broadcasts a short-lived control message that should be delivered to all nodes whose Euclidean distance from the originator is less than a predefined distance (K grid units). Following the transmission of a specific number (ρ) of short-lived messages, one long-lived control message is disseminated throughout the network. To control the frequency with which control messages are transmitted further, DREAM uses a mobility rate, which allows the node to self-optimise its dissemination frequency. Accordingly, the faster a node moves, the more often it updates its location information.

2.5.2.3 Location-Aided Routing (LAR)

The LAR [28] protocol is a position-based routing protocol that discovers routes to destinations reactively. It uses location information to reduce the routing overhead caused by the route discovery process. Its main concept is confining the propagation area of route request (RREQ) messages to the geographical zone that leads to the destination node. For this reason, LAR defines two zones: the expected zone and the request zone. The expected zone, illustrated in Figure 2-10, is the circle where the destination node is expected to be located.

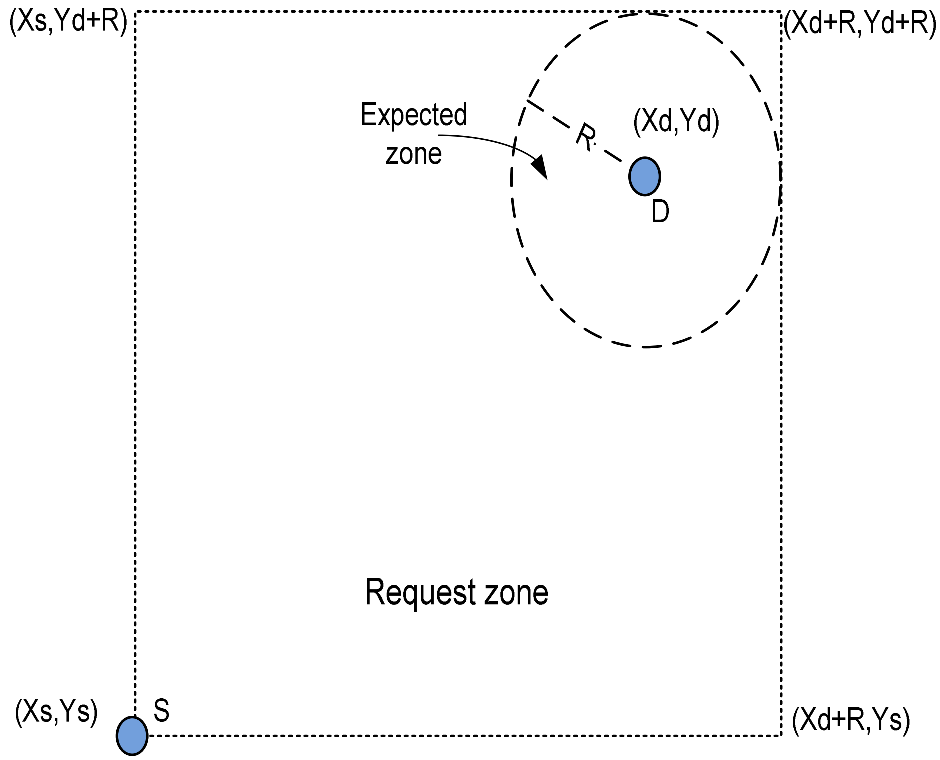

Figure 2-10: LAR request and expected zones

The source node only broadcasts the discovery request within the request zone, which is the smallest rectangle formed by the expected zone and the source node's position. Furthermore, LAR defines two schemes: scheme-1 and scheme-2. The difference resides in the way the request zone is specified within the request message. In scheme-1, the source node explicitly specifies the request zone by including the coordinates of the zone's four corners in the RREQ. Those receivers located outside the specified rectangle discard the RREQ. On the other hand, in scheme-2 the source node includes the destination's coordinates in the RREQ as well as the distance, Dists, to the destination. The receiving nodes will then calculate their distance from the destination node, and only those nodes whose distance is greater than $Dist_s$ will forward the RREQ.

2.6 Conclusion

This chapter gave an overview of IEEE 802.11 Mobile Ad-Hoc Networks. The main objectives were to outline the fundamentals of WLAN technology by highlighting the basic operations of its MAC and PHY layers, and to explain the principles and characteristics of MANETs. A detailed study of routing approaches in MANETs was then presented, especially position-based types, and this forms the basis of the related discussion in chapters 3, 4 and 5.

2.7 References:

[1] Ergen, S.C. "ZigBee/IEEE 802.15.4 Summary, avilable online at http://www.prism.uvsq.fr ", 2004, Retrieved in *June 2012.*

[2] H. Noureddine "Position-based routing and MAC protocols for wireless ad-hoc networks"Thesis was submitted for the degree of Doctor of Philosophy - Brunel University 2011.

[3] "IEEE Std 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications," IEEE Std 802.11-1997 , vol., no., pp.i-445, 18 Nov 1997.

[4] "Supplement to IEEE standard for information technology telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: high-speed physical layer in the 5 GHz band," IEEE Std 802.11a-1999 , 1999.

[5] "Supplement To IEEE Standard For Information Technology- Telecommunications And Information Exchange Between Systems- Local And Metropolitan Area Networks-Specific Requirements- Part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension In The 2.4 GHz Band," IEEE Std 802.11b, 2000.

[6] "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999) , 2007.

[7] C. K. Toh, Ad-hoc Mobile Wireless Networks: Protocols and Systems, 1st ed: Prentice Hall, Inc., ISBN 0-13-007817-4, December 3, 2001.

[8] S. Y. Tan, M. Y. Tan, and S. H. Tan, "Multipath delay measurements andmodeling for interfloor wireless communications," IEEE Transactions on VehicularTechnology, vol. 49, pp. 1334-1341, July, 2000.

[9] R. Gummadi, D. Wetherall, B. Greenstein., and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," Proceedings of the conference on Applications, technologies, architectures, and protocolsfor computer communications, pp. 385-396, 2007.

[10] C. S. R. Murphy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols. New Jersey: Prentice Hall PTR, May 24, 2004.

[11] P. Mohapatra and S. Krishnamurthy, Ad hoc networks: technologies and protocols, 1 ed: Springer, September, 2004.

[12] K. D. Wong, T. J. Kwon, and V. Varma, "Towards commercialization of ad hoc networks," Proceedings of IEEE International Conference on Networking, Sensing and Control, 2004, vol. 2, pp. 1207-1211, 2004.

[13] C. E. Perkins, E. Belding-Royer, S.R. Das. Ad hoc on-demand distance vector (AODV) routing, http://www.ietf.org/rfc/rfc3561.txt, July 2003. RFC 3561. Retrieved in *May 2012*.

[14] D.B. Johnson, and D. A. Maltz, “Dynamic source routing in ad hoc wireless networks. In Mobile Computing”, T. tiefinski and H. F. Korth, Eds. Kluwer Academic PubUshers, Dordrecht, The Netherlands, pp. 153-181, 1996.

[15] T. Clausen and P. Jaqcquet, Optimized Link State Routing (OLSR) RFC 3626, IETF Networking Group, October 2003, http://www.ietf.org/rfc/rfc3626.txt, Retrieved in *May 2012.*

[16] M. Mauve, A. Widmer, and H. Hartenstein, “A survey on position-based routing in mobile ad hoc networks”. IEEE Network, vol. 15, no. 6, pp. 30-39, 2001.

[17] I. Stojmenovic, “Position-based routing in ad hoc networks,” IEEE Communications Magazine, vol 40, no. 7, pp. 128-134, July 2002.

[18] R. Nelson and L. Kleinrock, “The spatial capacity of a slotted ALOHA multihop packet radio network with capture,” IEEE Transsactions on Communications, vol. 32, no. 6, pp. 684–694, Jun. 1984.

[19] G.G. Finn, “Routing and Addressing Problems in Large Metropolitan-Scale Internetworks”, Research Report ISU/RR-87-180, Inst. For Scientific information, Mar. 1987.

[20] H. Takagi and L. Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals," IEEE Transactions on Communications, vol. 32, no. 3, pp. 246–257, March 1984.

[21] Ting-Chao Hou Victor Li , "Transmission Range Control in Multihop Packet Radio Networks," IEEE Transactions on Communications, vol. 34, no. 1, pp. 38- 44, Jan 1986.

[22] B. Karp and H. T. Kung, "GPRS: Greedy perimeter stateless routing for wireless networks," in ACM/IEEE International Conference on Mobile Computing and Networking, pp. 243-254, 2000.

[23] I. Stojmenovic and X. Lin, "Loop- hybrid single-path/flooding routing algorithms with guaranteed delivery for wireless networks," IEEE Transactions on Parallel and Distributed Systems, vol. 12, no. 10, pp. 1023 – 1032, October 2001.

[24] I. Stojmenovic and X. Lin, "GEDIR: Loop-free location based routing in wireless networks", IASTED Int. Conf. on Parallel and Distributed Computing and Systems, pp, 1025-1028, 1999.

[25] W.J Liu, K.T Feng, "Greedy Anti-Void Routing Protocol for Wireless Sensor Networks", IEEE Communications Letters, vlo. 11, no. 7, pp. 562-564, July 2007.

[26] Wen-Jiunn Liu; Kai-Ten Feng, Largest Forwarding Region Routing Protocol for Mobile Ad Hoc Networks, Proc. IEEE GLOBECOM, pp. 1 – 5, 2006.

[27] E. Kranakis, H. Singh, and J. Urrutia, "Compass routing on geometric networks", Canadian Conference on Computation Geometry (CCCG), pp. 51-54, 1999.

[28] Young-Bae Ko , Nitin H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks", Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, pp.66-75, 1998.

[29] S.Kalhor, M. Anisi, A.T.Haghighat, "A New Position-Based Routing Protocol for Reducing the Number of Exchanged Route Request Messages in Mobile Ad-hoc Networks", Proc. ICSNC, pp. 13 – 13, 2007.

[30] Jian Li; Mohapatra, P.v, “LAKER: location aided knowledge extraction routing for mobile ad hoc networks”, IEEE Wireless Communications and Networking Conference (WCNC), pp. 1180 – 1184, 2003.

[31] S. Nanda, R.S Gray, “Multipath location aided routing in 2d and 3d”, IEEE Wireless Communications and Networking Conference (WCNC), pp. 311-317, 2006.

[32] S. Basagni et al., “A Distance Routing Effect Algorithm for Mobility (DREAM)”, Proc. of ACM MOBICOM’98, pp.76-84, 1998.

[33] W.H. Liao, Y.C. Tseng, J.P. Sheu, “GRID: a fully location-aware routing protocols for mobile ad hoc networks”, Telecommunication Systems 18 (1−3),pp. 37−60, 2001.

[34] L. Blazevic et al., ”Self-organization in Mobile Ad Hoc Networks: The Approach of Terminodes,” IEEE Commun.Mag., vol 39, no. 6, pp. 166–175, 2001.

[35] Hossein Ashtiani, Shahpour Alirezaee, S. mohsen mir hosseini and Hamid Khosravi, “PNR: New Position based Routing Algorithm for Mobile Ad Hoc Networks“, Proceedings of the World Congress on Engineering, vol 1, 2009.

[36] Daniel Câmara and Antonio A.F. Loureiro, "A Novel Routing Algorithm for Ad Hoc Networks," Hawaii International Conference on System Sciences, vol. 8, pp.8022, 2000.

[37] Kai Zeng Kui Ren, Wenjing Lou, “Geographic On-Demand Disjoint Multipath Routing in Wireless Ad Hoc Networks”, Proc IEEE Military Communications Conference MILCOM, pp. 1-7, 2005.

[38] E. Kuiper and S. N. Tehrani, “Geographic Routing With Location Service in Intermittely Connected MANETS”, IEEE Transaction on Vehicular Technology, vol. 60, no. 2, pp. 592-604, 2011.

[39] K.T. Feng, C.H. Hsu and T.E. Lu, “Velocity-Assisted Predictive Mobility and Location-Aware Routing Protocols for Mobile Ad Hoc Networks, IEEE Transactions on Vehicular Technology, vol. 57, no. 1, pp. 448-464, 2008.

[40] V. Namboodiri and L. Gao, “Prediction-Based Routing for Vehicular Ad Hoc Networks”, IEEE Transactions on Vehicular Technology, vol. 56, no. 4, pp. 2332-2345, 2007.

CHAPTER 3

Candidate Neighbours to Rebroadcast the RREQ in Mobile Ad-Hoc Networks

3.1 Introduction

Mobile Ad-hoc Networks (MANETs) have been investigated deeply during recent years due to their success in both civilian and military applications [1]. MANETs are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using an existing fixed network infrastructure or any centralized administration [2]. The nodes organize themselves randomly and are free to move anytime, anywhere; thus, the network's wireless topology may change hastily and arbitrarily. Nodes in MANETs act as data-generating entities as well as relay routers to forward data packets to other nodes in a wireless multi-hop environment. Designing a dynamic routing protocol that can efficiently find an end-to-end path is one of the fundamental challenges in MANETs, especially in a multi-hop scenario [2].

Recently, many routing protocols have been proposed for MANETs to help with performing the routing process among nodes in multi-hop scenarios [3-8]. In general, the topological routing protocols for MANETs can be classified into three categories: proactive, on-demand/reactive and hybrid routing protocols [10]. Proactive routing protocols, such as the Destination Sequenced Distance Vector (DSDV) [3], Optimized Link State Routing (OLSR) [4] and Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) [5], attempt to maintain consistent and up-to-date routing information tables on each node to every possible destination in the network by periodically exchanging routing table information. In those protocols, any change in the network causes nodes to propagate "update messages" and leads to greater bandwidth usage and more overhead. On the other hand, in on-demand routing protocols, such as the Ad-hoc On-demand Distance Vector AODV [6] and Dynamic Source Routing DSR [7], routes are only discovered when and where needed. This reduces the routing overhead in reactive routing protocols by maintaining information for active routes only. Furthermore, hybrid routing protocols such as the Zone Routing Protocol (ZRP) [8] have been introduced by combining the features of on-demand and proactive routing protocols.

In conventional on-demand routing protocols [6-7] a node discovers routes to a particular destination by broadcasting a Route Request (RREQ)packet. Upon receiving the RREQ, the node checks whether the packet has been previously received or not. If the packet has already been received, the node will drop it; otherwise, it will send a Route Reply (RREP) back to the source node if the route is available. If no available information in the routing table, the node will rebroadcast the RREQ to its immediate neighbours until the destination is found. This can potentially lead to excessive redundant retransmissions and, therefore, high channel contention and excessive numbers of packet collisions in dense networks. Such a phenomenon is referred to as a broadcast storm problem [9]. It significantly increases network communication overhead and end-to-end delay, and causes more loss of the available bandwidth [9, 10].

Many approaches to improving flooding performances based on reducing the number of redundant messages have been proposed. However, reducing the number of redundant messages leads to a low degree of coverage and connectivity. This interdependency between the two phenomena poses a challenge to balancing message overhead (i.e., the level of redundancy) and coverage [2].

This chapter proposes two algorithms to deal with the flooding problem in Mobile Ad-Hoc Networks, which widely use reactive routing protocols to disseminate RREQ packets and find a route from the source to the destination. Basic flooding has been proven to cause high retransmissions, packet collisions and media congestion that can significantly degrade the network performance. Knowing the geographical positions of mobile nodes can assist the protocol to reduce the number of retransmissions and therefore enhance its performance. Two methods were used in the algorithms to select four Candidate Neighbours to Rebroadcast the RREQ (CNRR); the first method is the Closest CNRR (C-CNRR), while the second is the Furthest CNRR (F-CNRR). The proposed algorithms were applied to the route discovery process of the Ad-hoc On Demand Distance Vector (AODV) as an instance of on-demand routing protocols. The simulation results showed that the proposed algorithms reduced the routing overhead of the AODV protocol by up to 28% compared to C-CNRR and up to 17.5% compared to F-CNRR.

3.2 Related Work

Broadcasting is the basic operation of reactive routing, whereby a source node sends the same RREQ message to all its neighbours and then the intermediate nodes forward the same message to all their neighbours. This process will continue until the RREQ message reaches the destination or one of the intermediate nodes has a valid route to the destination attached to the RREQ message. Therefore, broadcasting seems to reduce network performance by increasing the number of unnecessary RREQs in the network, utilizing the bandwidth and causing collisions among the nodes. Hence, it is important to choose the intermediate nodes used to rebroadcast the RREQ message cautiously so as to avoid redundancy in the dissemination process. Several researchers have proposed methods of tackling the broadcast problem in MANETs. Some have used the concept of probability. In this, a high probability number is assigned to nodes that have a small number of neighbours that will allow the node to rebroadcast the RREQ. In contrast, a low probability number is given to nodes that have more neighbours that will stop this node from forwarding the RREQ, assuming that their neighbours have already received the same RREQ message and there is no need to rebroadcast it [11]. Further techniques [12, 13] proposed include location-based approaches to reducing the amount of RREQ packet forwarding by exploiting geographical information about the network using location information devices such as GPS receivers [14]. Furthermore, two approaches can be implemented at the physical layer (transmission model) to tackle the broadcast problem: the one-to-all model and the one-to-one model. In the one-to-all model, each node's transmission can reach all nodes that are within its transmission radius, while in the one-to-one model each transmission is directed towards only one neighbour (using narrow beam directional antennas or separate frequencies for each node) [15]. However, studies of broadcasting in the literature mainly refer to the one-to-all model [16]. This is primarily because most current mobile devices have omni-directional antenna implementation, where the communication signal is propagated to and received from all directions.

In [17] the authors proposed an Estimated Distance (EstD)-based routing protocol (EDRP) to decrease the routing overhead by controlling the propagation range of RREQ packets. The EstD is a combination of Estimated Geometrical Distance (EGD) and Estimated Topological Distance (ETD). They used the EstD to divide the network area into 3 zones and adopted a different strategy for forwarding the RREQ packet in each zone. In [18] the authors proposed a dynamic probabilistic approach to rebroadcasting RREQ messages. They set the rebroadcast probability of a host according to the number of neighbour nodes. The rebroadcast probability would be low when the number of neighbour nodes was high and vice versa. This proposed approach dynamically sets and adjusts the value of the rebroadcast probability for every host node according to the information it has on its neighbouring nodes. Coverage Based Route Maintenance (CBRM) has been proposed in [19]. The CBRM is combination of proactive and reactive methods on finding the path to the destination. The area of the node's transmission range has been divided into outer-set and inner-set and the node that wants to send a RREQ will specify all the neighbour nodes according to these two sets, then based on the neighbours location the end-to-end path will be created.

The work presented in this chapter is an extension of our previously published work [20], in which rebroadcasting of RREQ messages was controlled through source/forwarding nodes.

3.3 Candidate Neighbours to Rebroadcast the RREQ

The aim of this work is to design an efficient flooding mechanism for the reactive routing protocols in MANETs. The objective of the proposed algorithms is to improve network performance by eliminating redundant retransmissions of Route Request (RREQ) messages during the end-to-end routing path finding phase. On one hand, the elimination of redundant RREQs reduces the chances of channel contention and collisions among neighbouring nodes by reducing routing traffic. On the other hand, a smaller routing overhead leads to improved system throughput overall. During the normal operation of most reactive routing protocols for end-to-end path establishment, a source node broadcasts an RREQ packet to all its neighbours. This RREQ is re-broadcasted by all the neighbouring nodes and this process continues until the intended destination is reached. This takes a maximum of (N-2) broadcasts, for a network of N nodes, to find the route between any source, S, to any destination, D. The proposed methods of controlling the RREQ involve removing the redundant re-broadcasting of RREQ packets by all nodes involved in the packet forwarding process. To achieve this goal, the proposed methods first select a few nodes among the neighbours of the source/forwarding node and broadcast/rebroadcast the RREQ to them only. The area around the node (the transmission range of the node) which wants to broadcast or rebroadcast the RREQ packet is partitioned into different zones. The proposed methods further select candidate neighbour nodes within each zone based on their distance from the current node. Once selected, the RREQ packet is unicasted to these candidate nodes only. This process is repeated for all nodes involved in forwarding the RREQ until the destination, D, is reached.

Selecting the best nodes to use as candidate neighbours for re-broadcasting RREQs is a crucial task for the following reasons. Firstly, if this selection is made randomly, without any intelligent steps, the system cannot provide the required results. Secondly, selecting candidate nodes based on furthest distance from the source could lead to frequent route breakages due to mobility (nodes move out of each other's transmission ranges) and weak signals as packet reception probability depends on the transmission range being directly related to the distance between any two nodes. Thirdly, selecting candidate neighbours based on minimum distance from the source may give better results due to there being high signal quality. However, this again leads to high redundancy because the first broadcast will cover most of the nodes before the closest neighbour rebroadcasts the received RREQ. There is a clear trade-off between the distance away of source-candidate neighbours and the overhead. The greater this distance, the greater the coverage area that can be obtained by the selected nodes. Similarly, smaller distances result in strong paths in terms of good reception but at the expense of obtaining a smaller coverage area.

For optimal operation, the key concept of the proposed algorithms is to eliminate various nodes from rebroadcasting the RREQ and restrict it to only four neighbouring nodes. When the sender node, S, wants to find a path for a specific destination, D, which is not in the routing table, node S first needs to begin the process of initiating the RREQ packet. Before sending the RREQ, the radio transmission range of node S is partitioned into different zones. In the next step, one node per zone is selected to forward the RREQ.

This chapter proposes two algorithms to select four candidate nodes for re-broadcasting RREQ packets. The Hello message has been modified to carry the (x, y) coordinates of the node. Each node updated its position and inserted the (x, y) coordinates inside the hello message before sending it to its neighbours. Thus, each node, when it received a hello message from any neighbour, was able to get the position of that neighbour.

3.3.1 Furthest Candidate Neighours to Rebroadcast the RREQ

In the Furthest Candidate Neighbours to Rebroadcast the RREQ (F-CNRR) approach, the selection of candidate neighbours is performed by the source node, S, or any node which needs to re-broadcast the received RREQ to initiate/continue the route discovery process. From this point, the source node, S, or any node which wants to broadcast/re-broadcast the RREQ will be referred to as the forwarding node, X, for simplicity. The proposed routing discovery protocol works as follows. Any forwarding node first divides the area within its transmission range into a set of zones, Z, based on the (x, y) coordinates of all the neighbouring nodes within its own transmission range, as shown in Figure 3-1. To achieve this, every node frequently shares its position information with all of its direct neighbours through an in-built hello message mechanism such as those found in the AODV and DSR routing protocols. Every node obtains its own position in the form of (x,y) coordinates using a global positioning system (GPS) [14].

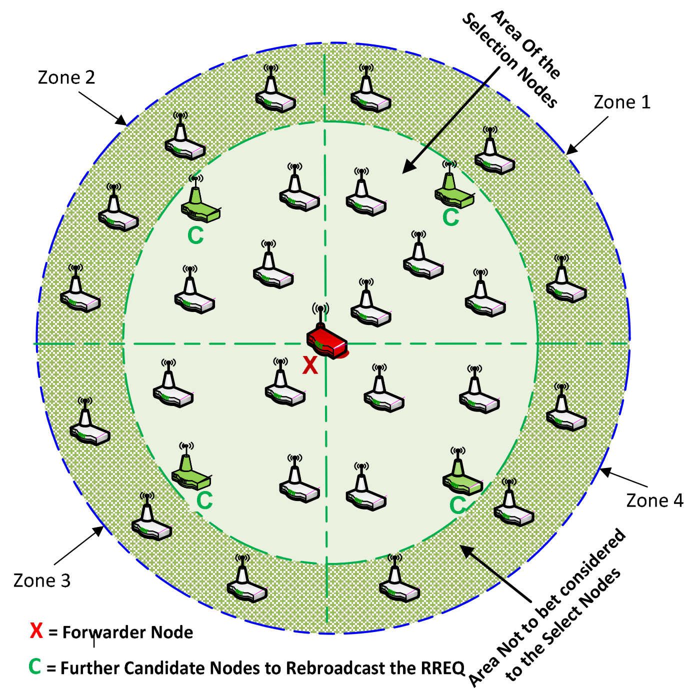

Figure 3-11: Further Candidate Neighbours to Rebroadcast the RREQ

The area around the forwarding node is divided into a set of four zones, Z= {Z_1,Z_2,Z_3 and Z_4}, according to Algorithm 1, as shown in Table 3-1. Let R_{tx} be the transmission range of a forwarding node, X, and let set N represent all its neighbour nodes N= {N_1, N_2, N_3, ….,$N_{|n|}$} ∈ R_{tx}. The output of Algorithm 1 divides the area into four separate zones and places each neighbour in one of these zones, Z_n. To determine the zone of a neighbour node, the forwarding node compares the (x, y) coordinates of that node with its own and places it in the appropriate zone. The forwarding node continues this process until the entire zone is determined for all neighbouring nodes, as shown in Algorithm 1 in Table 3-1.

After locating each neighbour in the right zone, the forwarding node further selects those nodes belonging to its Candidate List (CL). The CL is a set of those neighbouring nodes in each Zone, Z_n, which are within β, where β = 80% of the forwarding node's transmission area. The distance between the forwarding node and all of its neighbours within each zone is calculated by Equation (3-1).

$$Distance\ (X, N) = \sqrt{(X_x - N_x)^2 + (X_y - N_y)^2} \qquad (3\text{-}1)$$

Table 3-1: Partition the Transmission Range of the Forwarder Node

Algorithm 1

Input: Set of nodes N= {$n_1, n_2, n_3, \ldots, n_{|N|}$} $\in$ $the\ transmission\ range\ of\ the\ Sender$ S.

Output: Partition Sender S' neighbours into set of four separate zones **Z**= {Z_1, Z_2, Z_3, Z_4}.

for i= 1 to |N|
  If $n[i]_x \geq S_x$ & $n[i]_y \geq S_y$
    $n[i] \in Z_1$
  else if $n[i]_x < S_x$ & $n[i]_y \geq S_y$
    $n[i] \in Z_2$
  else if $n[i]_x \leq S_x$ & $n[i]_y > S_y$
    $n[i] \in Z_3$
  else if $n[i]_x \leq S_x$ & $n[i]_y < S_y$
    $n[i] \in Z_4$
  end if
next I

As shown in Figure 3-1, the nodes selected by the forwarding node as its CL set in each zone are represented by an inner circle, in accordance with Algorithm 2 in Table 3-2.

Table 3-2: Selection of Candidate List sets within each zone

Algorithm 2

Input: *Distance (S, N)* = $\sqrt{(S_x - N_x)^2 + (S_y - N_y)^2}$,

$\beta = 80\ \%\ distance\ of\ the\ Source\ node\ (S' transmission\ range)$

Output: Selection of the set Candidate Lists (CL) in each zone, **Z**= {Z_1, Z_2, Z_3, Z_4}.

for I = 1 to 4
  While ($n \in Z_i$)
    if $D(S, n) \leq \beta$
      CL=CL **U** {n}
    end if
  Do
next i

After selecting the sets of CLs in each zone, the forwarding node further selects the Candidate Nodes within each CL. As shown in Figure 3-1, the Candidate Node in each CL is the node furthest away from the forwarding node. To select the Candidate Node, the forwarding node, X, calculates the distances away from itself of all the nodes within the CL set and selects the node with the greatest distance in accordance with Algorithm 3, as shown in Table 3-4.

The final step is to insert the IP addresses of the four candidate neighbours into the Candidate Neighbour to Rebroadcast RREQ (CNRR) field inside the modified RREQ packet. The RREQ packet is modified with an array of four fields, each having 32 bits of length for the inclusion of a CNRR field, as shown in Table 3-3. In the final phase, the forwarding node, X, sends the RREQ packet, which now contains the addresses of the four Candidate Neighbours (A, B, C and D) as determined in the previous stage of Algorithm 3.

Table 3-3: Modified RREQ Packet

Type	J	R	G	D	U	Reserved	Hop Count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							
CNRR IP Addresses							

Upon reception of a RREQ, each node neighbouring the forwarding node, X, checks the CNRR field inside the RREQ packet and the decision to rebroadcast is taken based on the inclusion of the receiving node's network address in the list. If the receiving node finds its own address inside this field, this means the node is the furthest away from the perspective of the forwarding node, X, and it should further rebroadcast the RREQ in accordance with the F-CNRR. Otherwise, the receiving node discards the RREQ.

Table 3-4: Selection of the Candidate Node within each CL of each zone

Algorithm 3

Input: Z= {Z_1, Z_2 , Z_3, Z_4 }, CL= {*n1, n2, ….., $n_{|CL|}$*} in each zone

Output: Candidate Nodes in each zone

```
for i= 1 to 4
    for j= 1 to |CL| ∈ Zi
        //calculate the distances of each node in candidate
          list from the source node calculate D(S, nj)
    next j
        //select the candidate node in the Candidate List in the
          current Zone based on the maximum distance from the source
    for k= 1 to |CL|
        if D(S ,nk) > D (S, nk +1)
            candidate node= nk
        else
            candidate node= nk+1
        end if
    next k
next i
```

For instance, when the nodes A, B, C and D in Figure 3-1 receive the RREQ packet, they check the CNRR field and, since they find their addresses inside the RREQ, they do the same as the forwarding node, X, and re-broadcast the RREQ to their neighbours in accordance with the F-CNRR.

3.3.2 Closest Candidate Neighbors to Rebroadcast the RREQ

In MANETs, since all nodes move randomly with high mobility there is a high probability that the furthest neighbours will frequently move out of communication range [21]. In addition, due to collisions, interferences and decreases in channel capacity in cases of long distances between the sender and the receiver, the furthest neighbours in the CL set may fail to receive the broadcast RREQ successfully. To deal with this problem, this section proposes a mechanism called Closest Candidate Neighbours to Rebroadcast the RREQ (C-

CNRR). In this proposed protocol, the forwarding node, X, selects the CL set within each zone as follows. All the nodes neighbouring the forwarding node are placed in the appropriate zones in accordance with Algorithm 1, shown in Table 3-1. To select the CL within each zone, the forwarding node selects only those nodes that are at a distance greater than 20% of its transmission distance.

As shown in Figure 3-2, the nodes inside the inner circle are excluded from the CL set in each zone as they located within 20% of the transmission range of the forwarding node, X. In this proposed protocol, the Candidate Neighbours in each CL are selected based on their distances from the forwarding node.

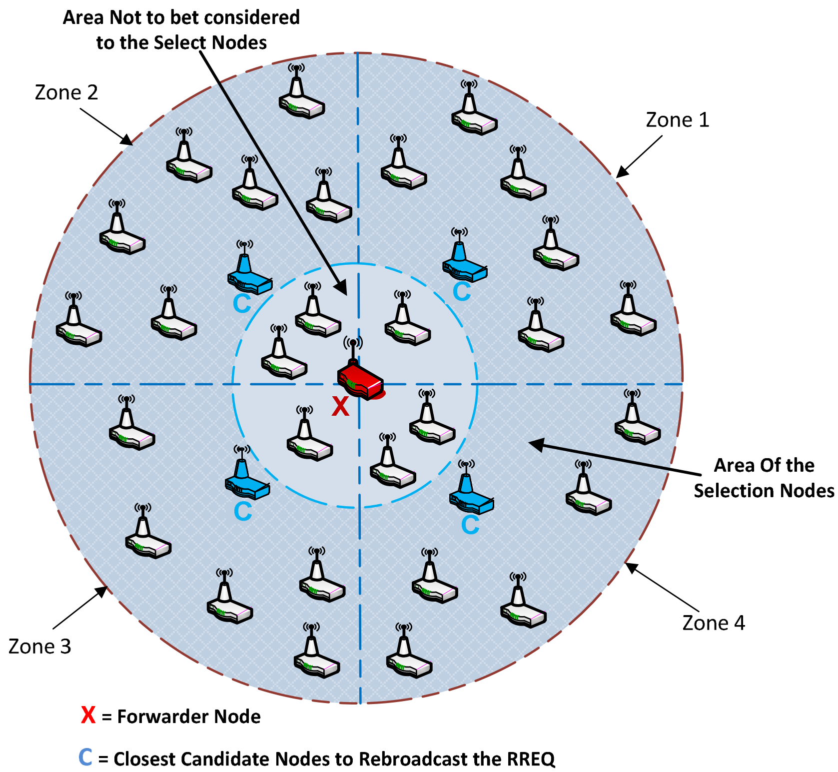

Figure 3-12: Closest Candidate Neighbours to Rebroadcast the RREQ

The forwarding node selects the Candidate Neighbour within each zone based on the smallest distance away from it. The CL for this mechanism is selected in accordance with Algorithm 2 of the Table 3-2 by taking $\beta = 20\%$ and changing line 3 to "if D(S,n)$> \beta$".

Similarly, the Candidate Neighbours within each CL set are selected in accordance with Algorithm 3 in Table 3-4 by changing line 8 to “if D(S,nk) < D (S, nk +1)”.

Figure 3-3 shows the whole proposed F-CNRR and C-CNRR procedure for the sending of an RREQ by the sender/source and its rebroadcasting by intermediate forwarding nodes. In the case of the source node, when a route to a particular destination is required, the source locates each of its neighbours in the correct zone and calculates their distances away from itself. Further, the source node selects the furthest nodes when F-CNRR is running as a routing protocol, or selects the closest nodes if C-CNRR is running as a routing protocol. After the four candidate nodes are selected, the RREQ is sent uniquely to them by means of inserting their network addresses in the CNRR field of the modified RREQ packet. The receiving Candidate Neighbour, upon reception of the RREQ packet, first if it has a valid route to the destination, a RREP packet will be sends to the source. If the receiving Candidate Neighbour haven’t a valid route to the destination it checks the CNRR field. If it finds its own network address in that field, it applies the F-CNRR or C-CNRR algorithms that have been applied. If any neighbouring node does not find its address inside the RREQ, the packet is simply discarded.

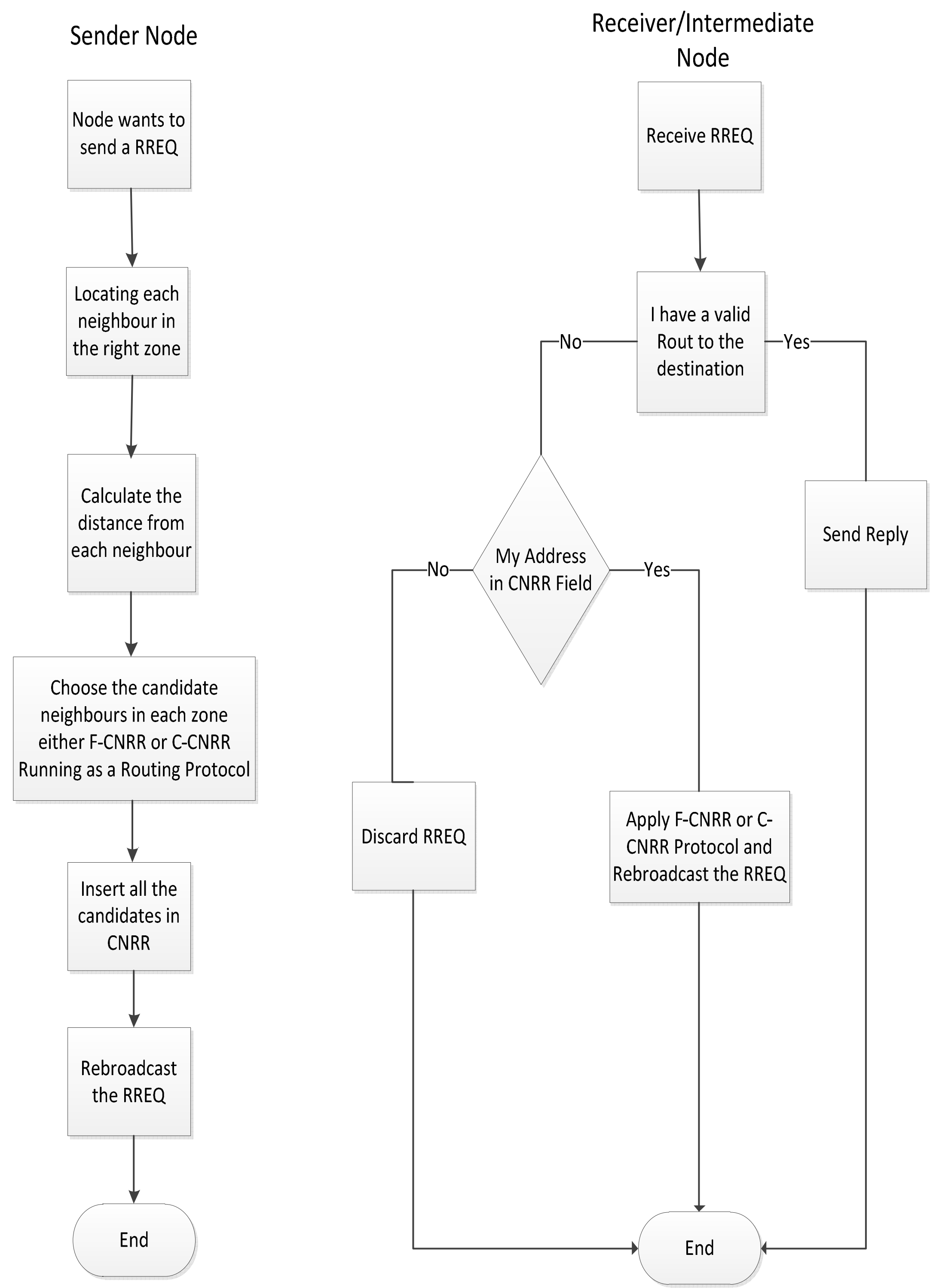

Figure 3-13: Flow chart presents the processes of a new RREQ packet for the Sender and Receiver nodes

3.4 Performance Evaluation

In order to evaluate the performance of the proposed protocols, the F-CNRR and C-CNRR mechanisms were simulated using Network Simulator NS2 [22]. The simulation environment, performance metrics and results are discussed in the subsequent sections.

3.4.1 Simulation Environment

In the simulations, the Distributed Coordination Function DCF [23] was selected and run on the IEEE 802.11 MAC layer. The transmission range and bandwidth were set to 250m and 2 Mbps, respectively. Evaluations of the network's performance were conducted for 100 mobile nodes that were randomly propagated in an area of 600 x 600 metres^2. The Random Waypoint Model [24] was used to simulate the nodes' mobility, whereby any mobile node in the network starts to move from a current location to a random location with a randomly chosen speed between a minimum speed equal to 5 m/h and a maximum speed equal to 30 m/h. The packet size was set to 1000 bytes and the packets were generated at a fixed interval rate of 5 packets per second using Constant Bit Rate (CBR) as the flow type. 20 flows were configured to choose a random source and destination during the simulation, which ran for 500 seconds. After running the simulation, the average results were gathered and plotted as shown in Section 3.4.3.

3.4.2 Performance Metrics

- **Packet Delivery Ratio:** the ratio of data packets that were successfully delivered to the destination nodes to those generated by the source nodes.
- **Total End-to-End Delay:** the delay to the packets for the entire network, computed by considering the time elapsing between when the packet was generated and when the destination node received it. This includes all possible delays caused by queuing, retransmission and propagation.
- **Total Overhead:** the number of control packets transmitted in the network, including the RREQ, RREP, Rerr and hello messages.

- **Total Throughout:** the total amount, in bits, of data successfully transmitted in the network per second.
- **Data Drop:** the total amount of data dropped during the simulation time for specific reasons such as error detection and collision.

3.4.3 Results and Discussion

This section analyses and compares the performances of the F-CNRR and C-CNRR protocols with that of the AODV on-demand routing protocol. The results of the simulation experiments demonstrate that C-CNRR does indeed have more advantages in most cases and improves network performance.

3.4.3.1 Data Drop

Figure 3-4 illustrates data drop rates in the AODV, F-CNRR and C-CNRR routing protocols.

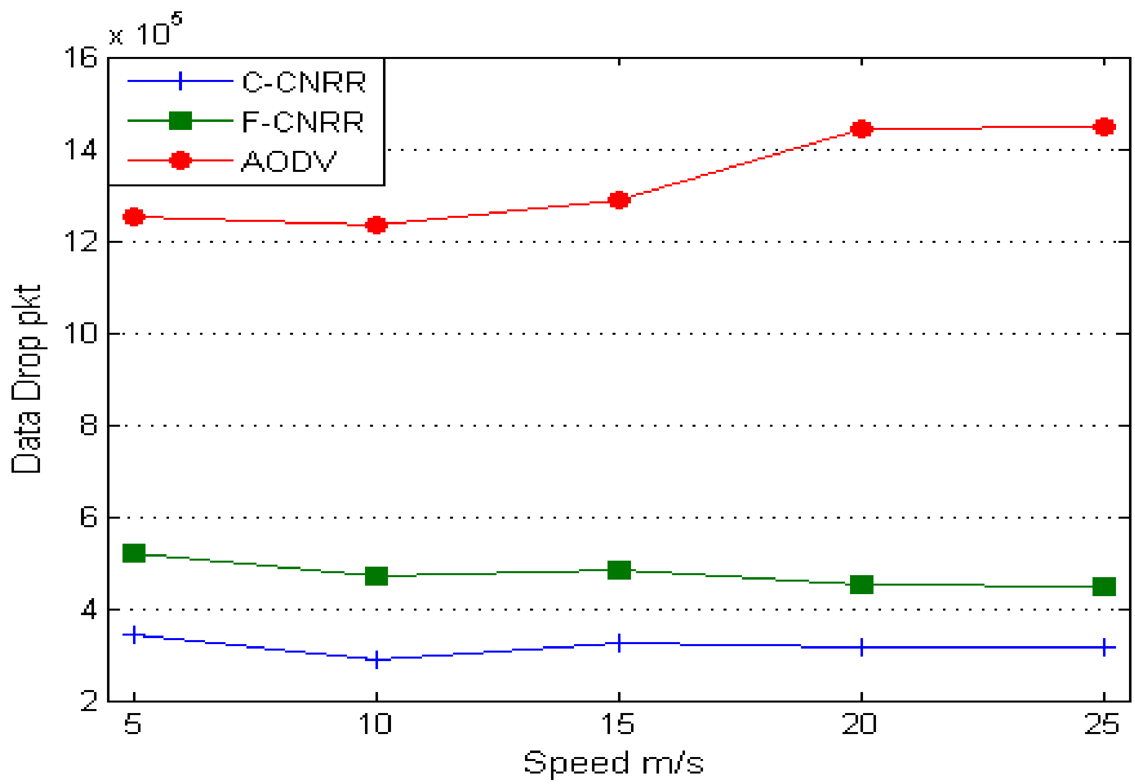

Figure 3-14: Data Drops vs. Speed

The figure shows that there are fewer data drops in both F-CNRR and C-CNRR in comparison to the AODV. This shows that F-CNRR and C-CNRR have better flooding mechanisms than the classic AODV. Furthermore, C-CNRR achieves a better performance than F-CNRR. This is because the end-to-end path selected by C-CNRR considers only those nodes that are close to each other, thus providing better channel quality, while the end-to-end path selected by the F-CNRR considers only how far nodes are from each other, thus increasing the chances of collisions and error detections that lead to more dropping of packets.

3.4.3.2 Throughput

Figure 3-5 illustrates the average throughput that was gathered from the simulation. It shows that throughput decreases when node mobility increases. Generally, the movements of mobile nodes break already established routes and result in the discovery of a new route.

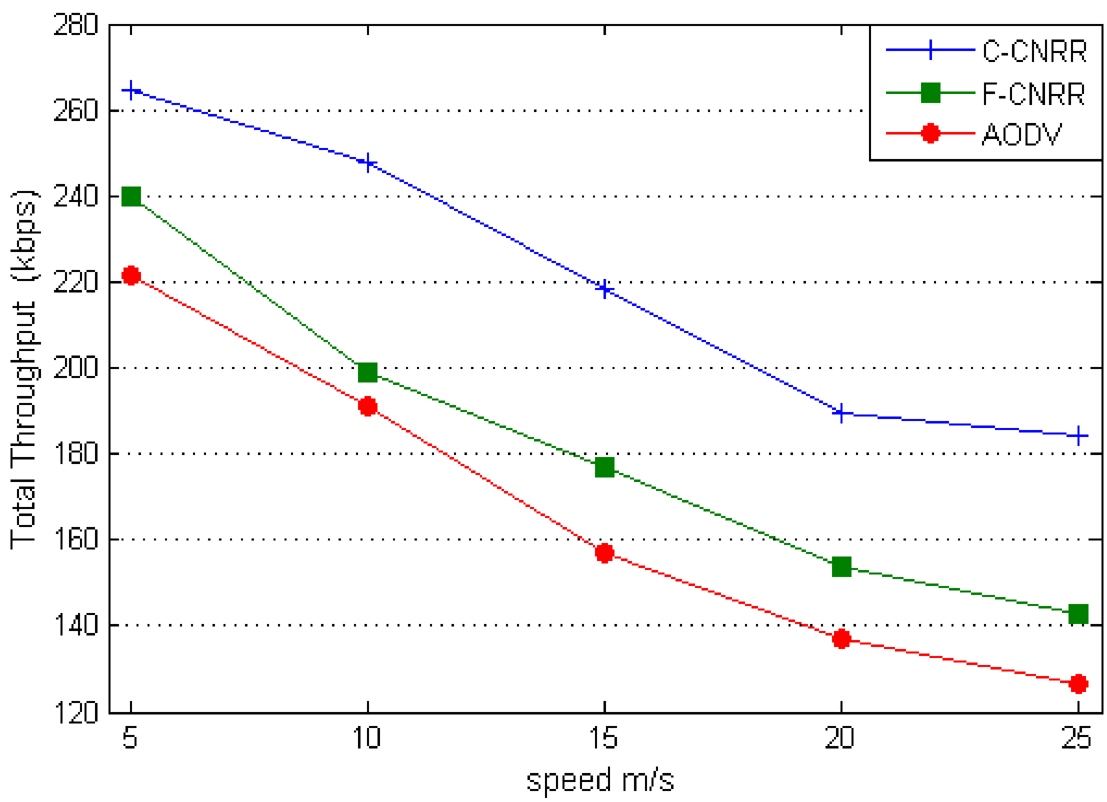

Figure 3-15: Throughput (kb/s) vs. Speed

As mentioned in Section 3.3.2, the throughput improvement in C-CNRR is due to a reduction in rebroadcasting, which gives real data a higher chance of transmission. C-CNRR rebroadcasts fewer RREQs than F-CNRR because when further nodes are selected as Candidate Neighbours, as in the case of F-CNRR, the links are likely to be unavailable or weaker owing to them being at a greater distance from the source/forwarding node. In contrast, when Candidate Nodes are selected, as in the case of C-CNRR, these are at short, appropriate distances from the source/forwarder node. Fewer rebroadcasts result in less bandwidth consumption by redundant RREQ packets. Furthermore, this also reduces collisions and computations among the nodes when accessing a channel.

3.4.3.3 Delay

In Figure 3-6, the average delay in each packet between its sent and received times has been recorded to illustrate the end-to-end delay.

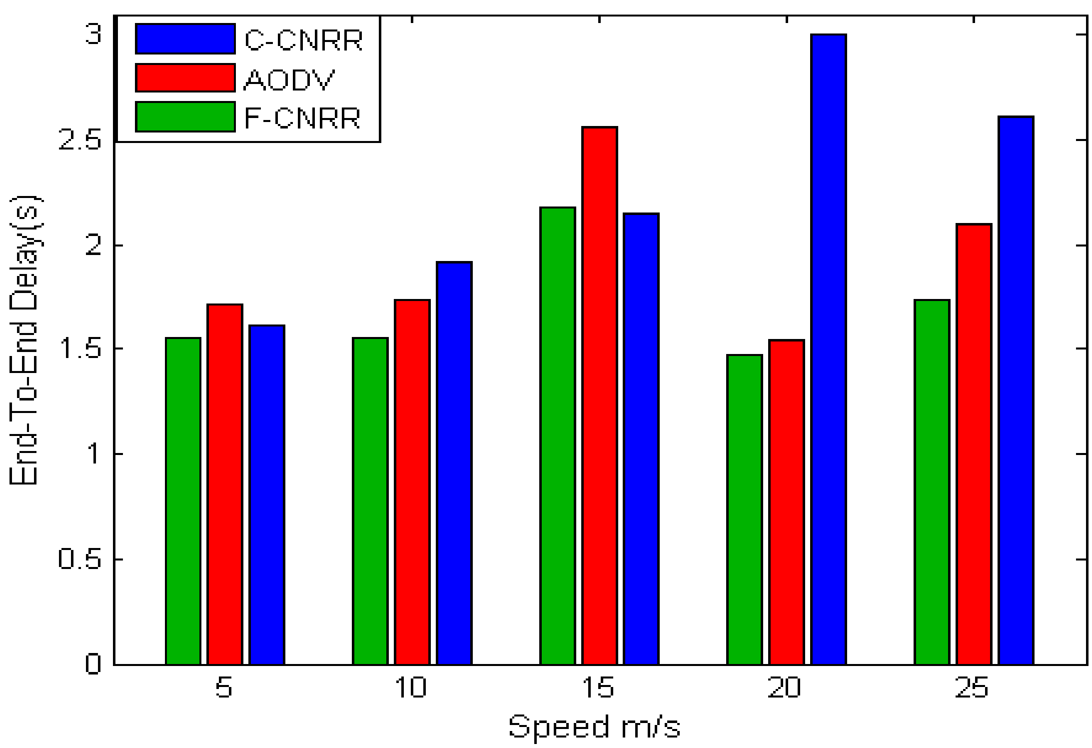

Figure 3-16: Total End-To-End Delay vs Speed

The end-to-end delay result broke the tenet of C-CNRR having better performance in all metrics. In MANET routing protocols, bandwidth availability is not a vital decision metric and the choice of end-to-end route is based simply on the hop-count. Selecting paths with fewer hop-counts can make packets arrive more quickly than selecting a path with more hops. It can clearly be seen from Figure 3-6 that F-CNRR has a lower level of delay compared to C-CNRR and AODV. F-CNRR always uses the furthest forwarder nodes to rebroadcast RREQ packets and creates an end-to-end path with a lower hop count than those of AODV and C-CNRR. This ultimately leads to less network delay overall. Figure 3-6 also shows that AODV performs better than C-CNRR in terms of causing less delay in the network. This is because the C-CNRR protocol creates an end-to end path using the closest nodes, resulting in a greater hop count, whereas in AODV the end-to-end path is selected from both the closest nodes (like C-CNRR) and more distant nodes at random. This is why AODV performs better in some cases than C-CNRR and vice versa. The conclusion obtained from the end-to-end delay results is that the F-CNRR protocol is a better choice among the three protocols under observation for delay-sensitive applications where delay is a vital deterministic parameter, e.g., video and audio streaming, than C-CNRR or AODV.

3.4.3.4 RREQ Rebroadcasts

In AODV, a received RREQ will be rebroadcasted by the mobile node if it has no valid route to the destination in the routing table and the RREQ is not a duplicate. However, in F-CNRR and C-CNRR each node decides to rebroadcast or not in accordance with the proposed algorithms, while maintaining the desired level of connectivity and reachability. Hence, a node running F-CNRR or C-CNRR routing protocols definitely rebroadcasts smaller numbers of RREQs than those running the AODV routing protocol. Figure 3-7 shows that more route requests are generated when the nodes' mobility increases, especially in the case of AODV. The end-to-end path established by C-CNRR will last longer than those selected by F-CNRR and AODV. This is due to the algorithm used by C-CNRR creating a path between nodes that are close to each other, leading to less rediscovering of routes as a result of less route breakage, which in turn leads to lower numbers of RREQs having to be propagated in the network to discover a end-to-end path.

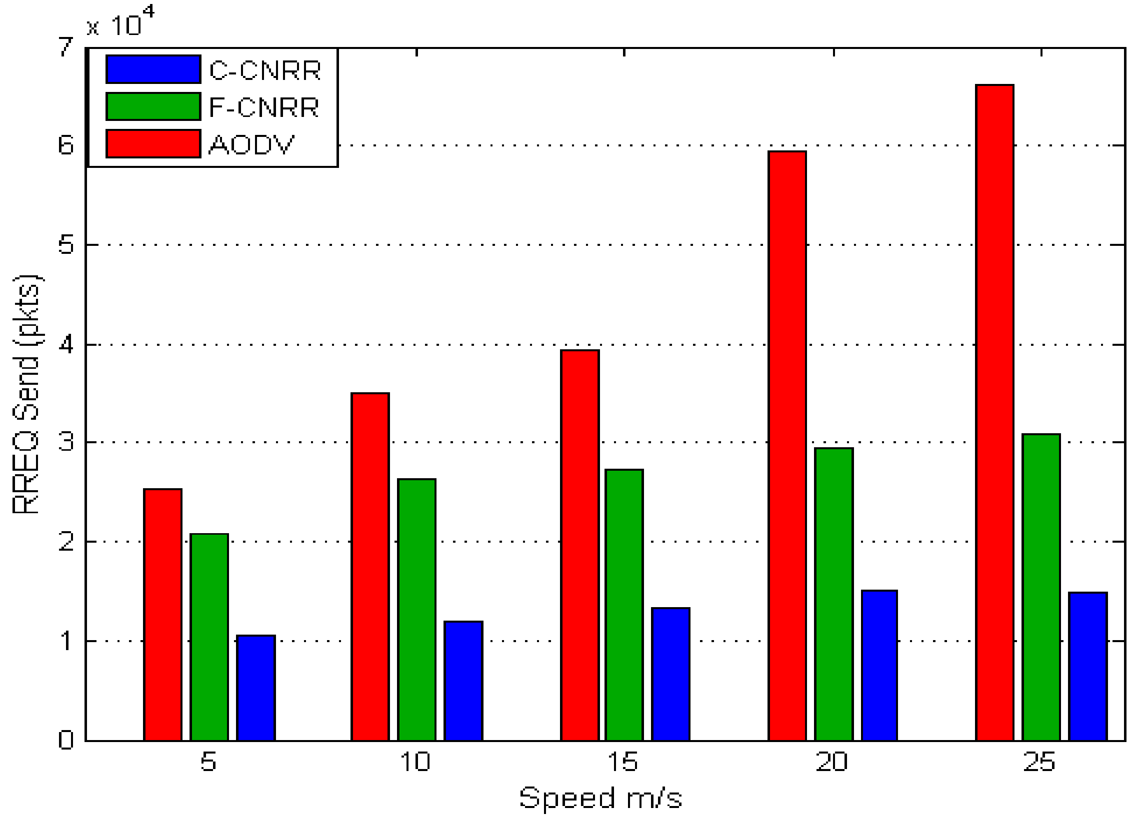

Figure 3-17: Number of Rebroadcast RREQs vs. Speed

Also, with high mobility the proposed approach has the advantage of rebroadcasting fewer RREQs than AODV. When comparing the two proposed algorithms, F-CNRR and C-CNRR, the latter can be seen as better than the former because the link is more stable in the case of C-CNRR and there is no need to reinitiate the RREQ process again and again.

3.4.3.5 Overhead

Figure 3-8 shows that the routing overhead for AODV increases linearly with increases in the nodes' mobility, while the overhead is almost equal for F-CNRR and C-CNRR. This is because AODV sends RREQs without any knowledge of which neighbours are best-suited to rebroadcasting the RREQ packets. Figure 3-8 also shows that C-CNRR performs better than

AODV and F-CNRR due to having less rebroadcasting of RREQ packets, as shown in Figure 3-7.

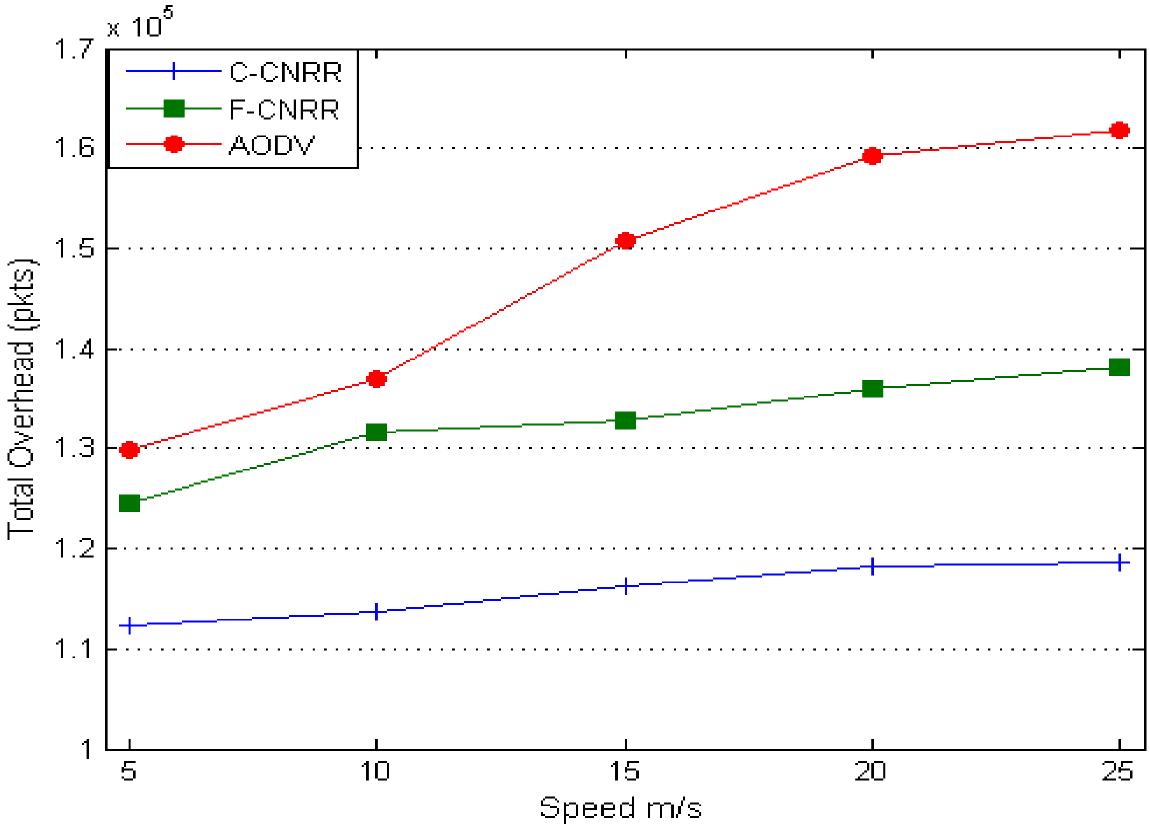

Figure 3-18: Total Overhead vs. Speed

3.4.3.6 Packet Delivery Ratio

Figure 3-9 depicts a comparison of the performance of the three protocols under observation in terms of their packet delivery ratios. C-CNRR and F-CNRR outperform AODV in all cases. This is because as node mobility increases, C-CNRR and F-CNRR update the positions of the nodes by exchanging hello messages and the four candidate nodes in the CNRR field are updated accordingly. In contrast, AODV creates end-to-end routes without knowing the positions of neighbours and, as a result, all neighbours rebroadcast the RREQ, which leads to redundant RREQs. The redundancy of RREQs affects the performance of the whole network in terms of the packet delivery ratio, throughput, delays and overhead.

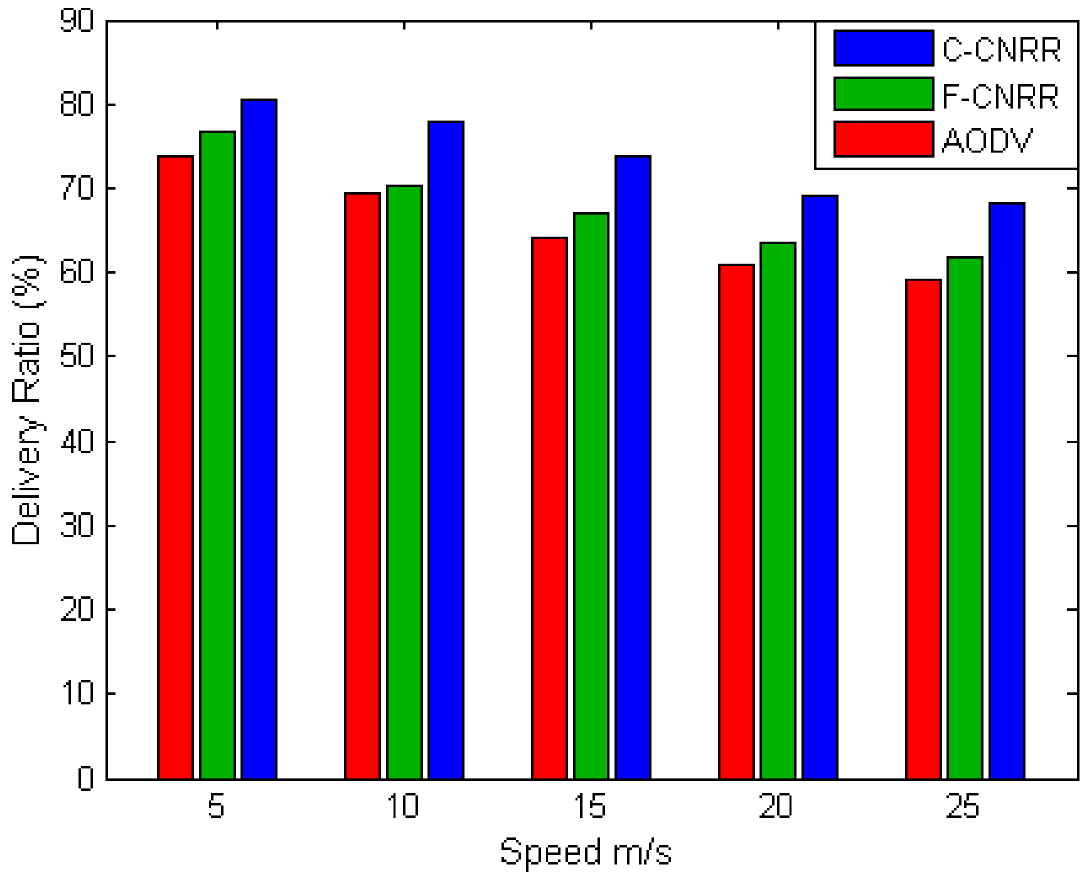

Figure 3-19: Packet Delivery Ratio vs. Speed

3.5 Conclusion

The Candidate Neighbours to Rebroadcast the Route Request (CNRR) method has been proposed to reduce the deleterious impact, known as the broadcast storm, of RREQ packets flooding traditional on-demand routing protocols. The main concept behind CNRR is dividing the transmission range of any node that would like to originate/rebroadcast the RREQ into four equal zones and selecting node per zone, called a candidate neighbour, to rebroadcast the RREQ packet. A Sender node selects its candidate neighbours, being potentially the best nodes to forward the RREQ, based on their distances from it. Two methods, *i.e.* F-CNRR and C-CNRR, have been investigated in relation to selecting these four candidate nodes. F-CNRR selects the furthest nodes from the sender, while the C-CNRR selection of candidate neighbours is based on the closest nodes to the sender. The AODV 'HELLO' message, which is exchanged frequently between neighbours, has been modified to carry the (*x, y*) coordinates of the node and inform all its neighbours about its current location. Further, the RREQ has been modified by adding the *cnrr* field to carry the four addresses of the candidate nodes. This *cnrr* field is checked by all the nodes and the RREQ's forwarding/rebroadcasting decision is based on the inclusion of its address by the sender in the additional field. The proposed techniques for RREQ discovery demonstrate higher performance as compared to the AODV routing protocol.

Although it is impossible to guarantee that there will be no redundant RREQs, however by adopting the C-CNRR and F-CNRR protocols, it has been possible to reduce the number of redundant RREQs and the simulation results show the possibility of better throughput, low end-to-end delay, high packet delivery ratios and low levels of data drops. The C-CNRR and F-CNRR algorithms can be implementing in all on-demand routing protocols that initiate the RREQ process to find the path to a destination.

The simulation results show that the proposed algorithms have a significant effect as they reduce the routing overhead of the AODV protocol by up to 28% compared to the C-CNRR, and by up to 17.5% compared to the F-CNRR. Notably, the proposed protocols simultaneously achieve better throughput and less data dropping.

3.6 References

[1] Akyildiz, I.F., Wang, X. and Wang, W. "Wireless mesh networks: a survey", Computer networks, vol. 47, no. 4, pp. 445-487, 2005.

[2] Abdulai, J., Ould-Khaoua, M. and Mackenzie, L. "Improving probabilistic route discovery in mobile ad hoc networks", Local Computer Networks 32nd IEEE Conference, pp. 739, 2007.

[3] Perkins, C.E. and Bhagwat, P. "Highly Dynamic Destination-Sequenced distance-vector routing (DSDV) for mobile computers", ACM SIGCOMM Computer Communication Review, vol. 24, no. 4, pp. 234-244, 1994.

[4] Qayyum, A., Jacquet, P. and Muhlethaler, P. "Optimized Link State Routing Protocol (OLSR)", 2003.

[5] Ogier, R., Templin, F. and Lewis, M. Topology dissemination based on reverse-path forwarding (TBRPF), 2004.

[6] Das, S., Perkins, C. and Royer, E. "Ad hoc on demand distance vector (AODV) routing", Mobile Ad-hoc Network (MANET) Working Group, IETF, 2002.

[7] Johnson, D.B., Maltz, D.A. and Broch, J. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks", Ad hoc networking, vol. 5, pp. 139-172, 2001.

[8] Z. J. Haas, M. R. Pearlman, and P. Samar, "The Zone Routing Protocol (ZRP) for ad hoc networks," IETF Internet Draft, draft-ietf-manet-zonezrp- 04.txt., July 2002.

[9] Tseng, Y.C., Ni, S.Y., Chen, Y.S. and Sheu, J.P. "The broadcast storm problem in a mobile ad hoc network", Wireless networks, vol. 8, no. 2, pp. 153-167, 2002.

[10] Y.-C. Tseng, S.-Y.Ni, and E.-Y. Shih, "Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc networks," Proceedings of IEEE Transactions on Computers, vol. 52, pp. 545--557, May 2003.

[11] Abdulai, J. "Probabilistic route discovery for Wireless Mobile Ad Hoc Networks (MANETs)", Glasgow University 2009.

[12] Basagni, S., Chlamtac, I. and Syrotiuk, V.R. "Dynamic source routing for ad hoc networks using the global positioning system", Wireless Communications and Networking Conference WCNC, 1999 IEEE, pp. 301, 1999.

[13] Abolhasan, M., Wysocki, T. and Dutkiewicz, E. "A review of routing protocols for mobile ad hoc networks", Ad hoc networks, vol. 2, no. 1, pp. 1-22, 2004.

[14] Kaplan, E.D. and Hegarty, C.J. Understanding GPS: principles and applications, Artech House Publishers, ISBN 1-58053-894-0, 2006.

[15] A. Nasipuri, J. Mandava, H. Manchala, and R. E. Hiromoto, "On-Demand Routing Using Directional Antennas in Mobile Ad Hoc Networks," Proceedings of the IEEE International Conference on Computer Communication and Networks (ICCCN 2000), pp. 535-541, October 2000.

[16] J. Wu and F. Dai, "Broadcasting in ad hoc networks based on self-pruning," International Journal of Foundations of Computer Science, vol. 14, pp. 201-221, April 2003.

[17] Zhang, X., Wang, E., Xia, J. and Sung, D. "An Estimated Distance based Routing Protocol for Mobile Ad hoc Networks", Vehicular Technology, IEEE Transactions on, , no. 99, pp. 1-1, 2011.

[18] Hanashi, A.M., Siddique, A., Awan, I. and Woodward, M. "Performance evaluation of dynamic probabilistic broadcasting for flooding in mobile ad hoc networks", Simulation Modelling Practice and Theory, vol. 17, no. 2, pp. 364-375, 2009.

[19] Jisha, G. and Samuel, P. "Coverage based route maintenance in MANET routing protocol", Intelligent Systems Design and Applications (ISDA), 12th International Conference on IEEE, , pp. 398, 2012.

[20] Sofian Hamad, Noureddine, H., Radhi, N., Shah, I. and Al-Raweshidy, H. "Efficient flooding based on node position for mobile ad hoc network", Innovations in Information Technology (IIT) on IEEE International Conference, pp. 162, 2011.

[21] De Morais Cordeiro, C. and Agrawal, D.P. "Mobile ad hoc networking", Center for Distributed and Mobile Computing, ECECS, University of Cincinnati, 2002.

[22] Simulator, NS2. ns-2, http://www.isi.edu/nsnam/ns. 1989. Retrieved in *July 2012.*

[23] Bianchi, G. "Performance analysis of the IEEE 802.11 distributed coordination function", Selected Areas in Communications, IEEE Journal on, vol. 18, no. 3, pp. 535-547, 2000.

[24] http://www.netlab.tkk.fi/~esa/java/rwp/rwp-model.html. Retrieved in *August 2012*.

CHAPTER 4

Link **S**tability and **E**nergy-**A**ware Protocol for Reactive Routing in MANETs

4.1 Introduction and Motivation

In reactive routing protocols, the path to a destination is discovered before data packets are exchanged between communication pairs [1]. The routing operation in MANETs requires mobile nodes to cooperate with each other to successfully direct traffic amongst communication peers [2]. Node availability is essential for the enforcement of such cooperation and affects the status of all live connections in the vicinity of the node. Several factors can cause link breakages in MANETs, including obstacles, nodes' residual energy, mobility and interference in the network. This chapter considers two factors that are seen as having the greatest impact on link breakages in MANETs. The two factors are:

A) Nodes' residual energy (battery lifetime)

B) Nodes' mobility.

Since MANET nodes are mobile devices and their power supplies are not permanent, the mobility factor makes these nodes energy-constrained devices. Further, the control messages introduced into the network for route management consume considerable amounts of node energy. This factor dramatically affects nodes' availability and consequently the network's lifetime [3]. In addition, node mobility is one of the main characteristics of MANETS that leads to frequent topological changes and to a subsequent increase in the probability of link failures and route breakages. Link failures then lead nodes into a process of route maintenance, where the aim is to find alternative paths or discover new links. However, the route maintenance process is bandwidth intensive, wastes the nodes' battery power and affects the network's performance by introducing an additional routing overhead and re-routing delays. Therefore, consideration of the nodes' mobility, as well as the residual energy in the routing operation, is essential for limiting route discovery to the most stable and durable routes.

This chapter proposes a new route discovery mechanism that uses the Link Lifetime (LLT) and the nodes' Residual Energy (RE) in the discovery process. The key concept behind the proposed mechanism is to forward Route Request (RREQ) messages over stable links via nodes which have sufficient RE and a good LLT in relation to the previous sender/forwarder. The proposed protocol can be easily implemented with most on-demand routing protocols, e.g., the Ad-hoc On-demand Distance Vector (AODV)[4] and the Dynamic Routing Protocol (DSR) [5].

4.2 Related Work

There are several existing methods for estimating LLTs in MANETs. Some of these methods rely on Received Signal Strength (RSS), such as in [6], while others make use of the location information of the nodes composing the links to predict the LLT. In addition, many routing algorithms use both the LLT and nodes' RE as routing metrics to allow the most stable and energy efficient end-to-end route to be selected for data transmission. In this section, we highlight the existing routing protocols that involve LLTs and nodes' RE in the routing process.

4.2.1 Signal Strength-Based Routing Protocols

The authors of [6] used signal strength as a link quality metric that varies according to a predefined signal strength threshold. The link quality between two mobile nodes increases when the signal strength between them is above a set threshold and decreases otherwise. Moreover, [7] proposes Signal Stability-based Adaptive Routing (SSA), which classifies links into groups according to the signal strength metric. During the path-discovery phase, each mobile node divides its connections with neighbouring nodes into Strongly Connected (SC) and Weakly Connected (WC) groups. This grouping is performed by the receiving nodes based on the signal strength of those neighbours from whom they receive the Route Request (RREQ) packet. However, SSA can suffer from path breakages during data transmission because the path may contain WC links. In [8], the authors proposed a signal strength-based routing protocol for MANET that first uses the earliest established path to forward packets and then changes to the strongest signal strength path for longer transmissions. In [9], the authors proposed a link management technique for an Optimized Link State Routing Protocol (OLSR) [10] in order to manage links locally. The proposed mechanism uses a cross-layer technique based on signal strength. The quality of the link, including whether it is improving or degrading, is determined by the signal strength. Further, the hysteresis method as given in the OLSR RFC is used for handling packet losses. This proposed mechanism makes link management more robust and improves network performance by anticipating link breakages.

4.2.2 Location Information Routing Protocols

All Location Information Routing Protocols make use of geographical positioning systems (GPS) [11] to get information such as the (x, y) coordinates, speed and direction of nodes in a network. A method of predicting link and route lifetimes based on nodes' location and movement information was proposed in [12]. The authors assumed that all the nodes in a network have their clocks synchronized, using the GPS clock itself. Therefore, if the motion parameters of two neighbours (such as direction, speed and (x, y) coordinates) are known, the length of time for which two nodes will remain connected can be determined by using Equation (4-1). The routing concept introduced in [12] predicts the Link Expiration Time (LET) at each hop of the route, which provides a prediction of the end-to-end Route Expiration Time (RET). RET is defined as the minimum LET of the links that are involved in an end-to-end route. Then, the path which has the highest RET is selected as the best route.

$$LET = \frac{-(a+b)+\sqrt{(a^2+c^2)r^2-(\mathrm{ad}-\mathrm{bc})}}{a^2+c^2} \qquad (4\text{-}1)$$

Where,
$a = v_i \cos\theta_i - v_j \cos\theta_j$,
$b = x_i - x_j$
$c = v_i \sin\theta_i - v_j \sin\theta_j$,
$d = y_i - y_j$

The parameters ϑi, v_i, ϑj, v_j are the movement directions and speeds of the nodes *i* and *j* , respectively.

Three schemes, grouped together under the term Heading-direction Angles Routing Protocol (HARP 1, HARP 2 and HARP 3), were proposed in [13]. In all these schemes, Equation (4-1) was applied to get the LET, although the authors used a different concept from that in [12] to get the angle (ϑ). Location Prediction-Based Routing (LPBR) was suggested in [14]. The key concept behind the LPBR routing protocol is that each node attaches its own mobility and location information to the RREQ message before sending it. When the RREQ reaches the destination node, it stores all the information gathered about mobility and direction in the routing table. The destination node will use this information when any route fails to predict the intended node's current location from the information gathered previously.

4.2.3 Energy-Aware Routing Protocols

The main goal of energy-aware routing protocols is to minimize the energy consumed by mobile nodes and to maximize overall network lifetimes. Minimum Battery Cost Routing (MBCR) is proposed in [15]. In the MBCR routing protocol, an end-to-end path is selected based on the criterion of summing the residual energies of the individual path participant nodes. The problem with this approach is that it might select an end-to-end path containing nodes with low residual energy. These low-energy mobile nodes may then cause frequent path breakages. Max-Min Battery Cost Routing (MMBCR) has been proposed, in which the inherent problems of MBCR are addressed by selecting a path consisting of nodes having maximum residual energy compared to other nodes in the network. Each MMBCR path is evaluated using the values of the minimum residual energy of the mobile nodes. Then the destination node selects the maximum value of each path and returns the RREP to the source. Conditional Maximum Battery Capacity Routing (CMMBCR) was proposed in [16] in an attempt to extend the lifetimes of nodes by avoiding any route/path that contains nodes having battery power below a predefined threshold. [17] introduced the Improved-AODV to cover situations where selfish nodes exist in the network. I-AODV used a new technique for recording those probability nodes agreeing to help to relay data. Furthermore, to prolong the lifetime of the network, I-AODV considers the RE of the nodes in a network. This results in the I-AODV selecting nodes having a high RE and hence a high probability of relaying data. The authors of [18] proposed a bandwidth-based energy-aware routing protocol that reduces energy consumption and prolongs network lifetimes. Their proposed algorithm detects the received signal strength and uses it to compute the transmission bandwidth by looking at a dB-to-bandwidth table. Further, the authors proposed the use of a Received Signal Strength (RSS) variation for computing LLTs and predicting the amount of data that could potentially be transmitted.

Most of the research works in the literature have addressed LLTs and energy information as routing metrics to improve the route selection mechanisms of routing protocols. Their methods was attaching the nodes' LLT and RE values in the RREQ packet prior to send, then the destination node on receiving the RREQ will select the best path based on the aggregate values of the LLT and RE attached to the RREQ. To the best of our knowledge, this is the first work that introduces LLTs and nodes' RE as ways to enhance the route discovery process. The proposed route discovery mechanism selects only those routes that satisfy LLT and energy requirements. In the Link Stability and Energy Aware (LSEA) routing protocol [19] we proposed a Fixed-LSEA (F-LSEA). In this protocol, the RREQ message would not be sent if it could not satisfy the LLT and RE requirements for the sender/forwarder nodes based on their fixed thresholds.

4.3 The Proposed Protocol

This section presents the proposed protocols and their variants in detail.

4.3.1 Problem Definition

As previously mentioned, there are two important factors that cause link breakages: a node moving out of the radio range of its neighbouring node, and a node dying due to energy exhaustion. For instance, consider the example shown in Figure 4-1, where the effects of link lifetimes on the network have been shown. As can be seen from this figure, there are six nodes in the network, where 'D' is the destination node and 'S' is source node. The numerical values on each link show the quality of the communication link between any two nodes in the network in terms of link lifetimes. When node S broadcasts a RREQ, nodes 1 and 2 receive this RREQ from it. Accordingly, nodes 1 and 2 record node S on the routing table as a reverse path for S . After this, nodes 1 and 2 broadcast the RREQ packet as it is assumed that they do not have a valid route to D. Nodes 3 and 4 receive the RREQ from nodes 1 and 2, respectively. Accordingly, nodes 3 and 4 record nodes 1 and 2 on the routing table as a reverse path for S. Then 3 and 4 broadcast the RREQs accordingly. Further, node D receives the RREQ packet from node 3 and, at the same time, node 3 receives a duplicated RREQ from 4. Node 3 will simply discard the duplicated RREQ from node 4. Finally, node D prepares to reply with the RREP packet.

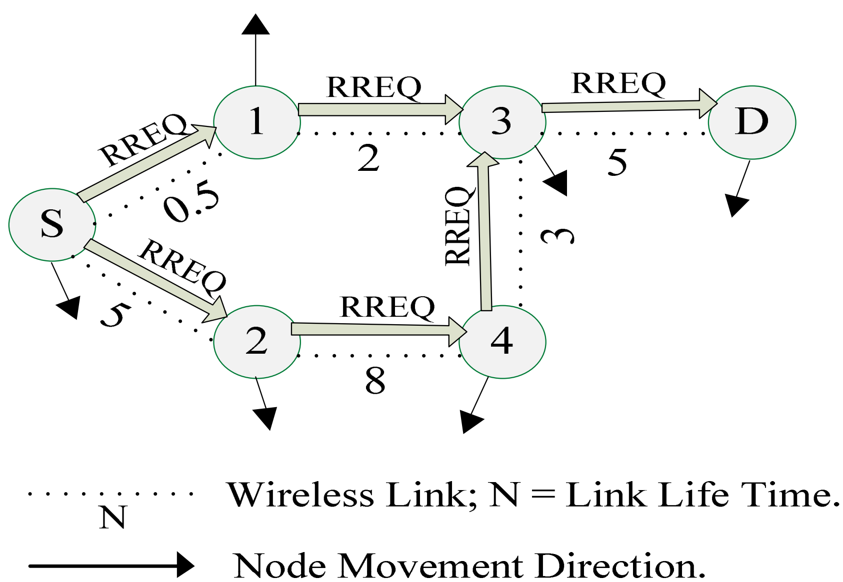

Figure 4-20: Illustration of the effect of Link Lifetimes (LLT)

Now there is a reverse path from D to S as (D, 3, 1, S). Node 3 will successfully receive the RREP sent by node D as there is a good link lifetime between them, which is equal to 5. Similarly, node 1 will successfully receive the RREP sent by node 3 as there is a good link lifetime between them, which is equal to 2. However, a problem may appear when node 1 tries to send the RREP to node S as the link might be broken (Weak Link = 0.5) even if node S successfully receives the RREP from node 1. The link will definitely break after a few data packets have been sent through it due to the weak link between nodes S and 1, which is equal to 0.5 seconds at the time of receiving the RREQ, and because the nodes are moving in different directions.

Moreover, in Figure 4-2 we exemplify the same network shown in Figure 4-1 and take into account the effect of node energy levels on the network. If node S chooses path S, 3, 4, D to send data through, then the path will quickly break because node 3 will consume all the residual energy after a few data packets have been sent through it due to there being a low energy level.

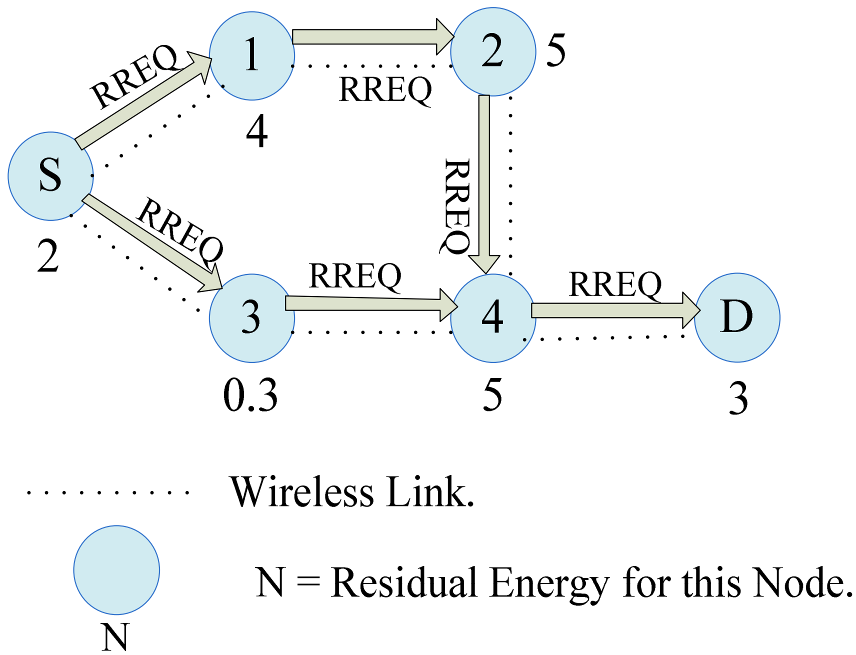

Figure 4-21: Illustration of the effect of Residual Energy (RE)

4.3.2 Preliminaries

Two protocols have been proposed as ways to improve the route discovery process by allowing only those nodes which can verify specific requirements. The two protocols are the:

1- Fixed Link Stability and Energy Aware (F-LSEA) routing protocol

2- Average Link Stability and Energy Aware (A-LSEA) routing protocol.

Our protocol satisfies pure on-demand routing protocols rules in that it discovers a path when it is needed, unlike pro-active routing protocols, which must have routing information for all the nodes in the network. Equation (4-1) in Section 4.2.2 has been used to get the Link Lifetimes (LLT) in both the proposed protocols. In these protocols, we followed the method in [12] to predict LLTs and the same assumptions were applied with regard to the prediction method (*see Section 4.2.2*). For the RE, any node can easily get its residual energy. For instance, when the LLT between any two nodes is equal to 1, this implies that after 1 second the link between those two nodes will be unavailable.

4.3.3 Fixed Link Stability and Energy-Aware (F-LSEA) routing protocol

In this chapter, our focus is mainly on improving the end-to-end route discovery process whenever a source node attempts to communicate with a destination node for which it has maintained no previous routing information. The LLT and RE thresholds have been fixed at specific values, as shown in the simulation setup in Section 4.4.1. In the Fixed Link Stability and Energy Aware (F-LSEA) protocol, when a node that has no prior route information seeks a path to a specific destination, the source node broadcasts a RREQ message to all of its neighbours. On receiving the RREQ message, any neighbouring node must carry out two necessary checks. First, it will compare its RE with the fixed RE threshold. If it is above the threshold then the node will go to the second necessary check; otherwise, the current RREQ packet will be discarded. Secondly, if the node passes the first necessary check, it will compare its LLT with the fixed LLT threshold. If it is above the threshold, the RREQ packet will be re-broadcasted; otherwise, it will discard the RREQ packet. The two conditions must be verified before the neighbouring node forwards the received RREQ packet. In essence, simplicity combined with effectiveness is one of the major goals of the proposed routing protocol. The F-LSEA is different from all previous work in that upon receiving an RREQ at any node it immediately decides whether or not to forward the RREQ based on both its RE and the LLT in relation to the RREQ sender. In contrast, in earlier work all nodes forward all received RREQs and allow the destination to select a path based on the received RREQ. Such a path contains nodes having a good link lifetime among them, where link lifetimes are used as a metric, or that contain nodes having a good residual energy where energy is used as a metric. Hence, in the proposed F-LSEA we tackled the fundamental question of why a node must forward a RREQ when the link lifetime with the RREQ sender is going to end and the RREP cannot reach the RREQ sender that is sent back by the destination node. In addition, sending any RREQs will incur more overhead and, in the end, only one path created by one RREQ will be selected. F-LSEA eliminates redundant paths at the beginning by selecting/reserving the best paths, in contrast to earlier relevant works.

For a better understanding of the concept of the proposed F-LSEA, consider the topology presented in Figure 4-3. In this network topology, the numbers inside the circles represent the node numbers (identity or address). The numbers below each node represent their respective REs, while the number below the connecting links shows the LLT between any two nodes sharing that link. Let the LLT and RE threshold be set to 3. As can be seen from the figure, let node S be the source node which wants to communicate with the destination, D, through intermediate nodes (nodes 1, 2 and 3) in an ad-hoc network. Let us assume that node S has no prior routing information for the destination, D, in its routing table. In this case, S broadcasts a RREQ packet and all its neighbours receive it. In conventional AODV, nodes 1, 2 and 3 will rebroadcast the RREQ if they do not have a valid fresh route to the intended destination, D. However, in our proposed scheme (F-LSEA), node 1 will check its link lifetime with S. If node 1 finds that its link lifetime is good (supposing the threshold is equal to 3 seconds), then it will go on to check the second necessary condition, which is the residual energy level. If node 1 finds that it has very low residual energy or a level below the set threshold, it will discard the received RREQ packet under our scheme. The same process is involved for the intermediate nodes, 3 and 2. Upon RREQ reception from node S at nodes 1, 2 and 3, node 3 finds that its energy level is very good (above the set threshold of 3). However, during the second necessary check it discovers that its LLT with node S is very weak, and therefore it discards the RREQ packet. In the given example, the only node that rebroadcasts the RREQ is node 2, as it satisfies the set necessary requirements for energy level and link lifetime.

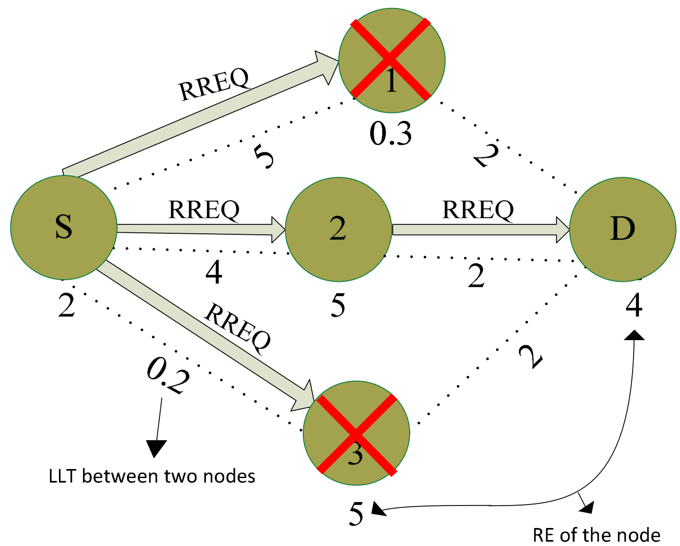

Figure 4-22: Instance of the F-LSEA operation

Each RREQ recipient node decision is based on the algorithm shown in Table 4-1.

Table 4-1: The F-LSEA operation algorithm

Algorithm 1

1. *Let S be the RREQ source/forwarding node.*

2. *Let N={n_1, n_2, n_3,…, $n_{|N|}$} be the neighbour nodes of S*

3. *Let L= {L_1, L_2,…, $L_{|N|}$} be the links between S and all its' neighbours* | $L_n \in L$ is a link between S and the *neighbouring node n_n,∀ $n_n \in N$.*

4. *Let LLT be the link life time associated with each link ⍰$_n$∈L.*

5. *Let RE be the residual energy of each neighbour $n_n \in N$.*

6. *Let α and β be the threshold LLT and RE for any link $L_n \in N$, for any neighbor $n_n \in N$.*

7. *for i= 1 to |N|*

//at each RREQ recipient neighbouring node

8. *if* (LLT ≥ α) and (RE ≥ β)

9. Forward RREQ

10. *else*

11. Drop RREQ

12. *end if*

13. *next i*

As can be seen in Algorithm 1 in Table 4-1, upon receiving the RREQ all nodes check their LLT and RE against the set defined thresholds at line 8 and the RREQ is forwarded if both the thresholds are met; otherwise, it is discarded. The same mechanism is also shown in the flow chart in Figure 4-4.

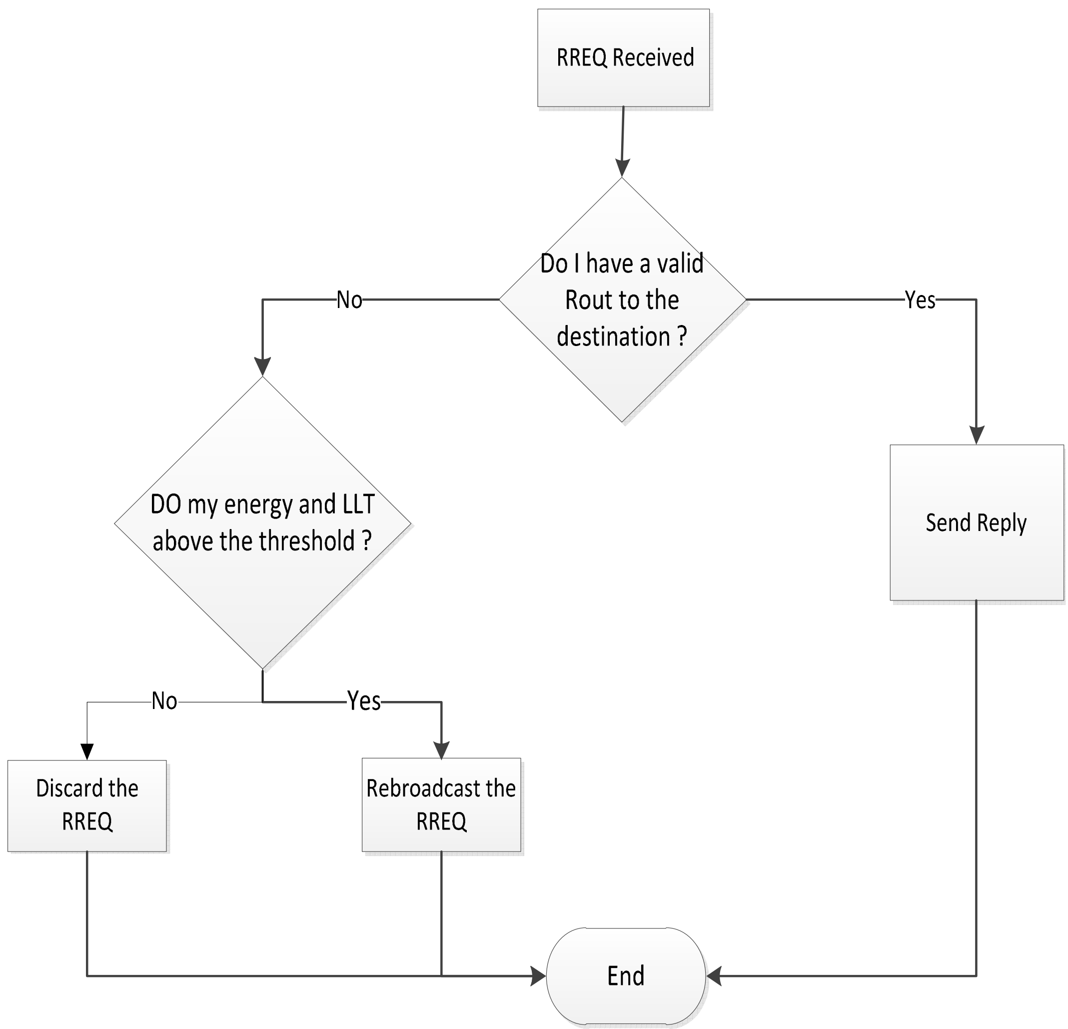

Figure 4-23: Flow Chart illustrates the processes of receiving a RREQ at any node.

4.3.4 Average Link Stability and Energy Aware (A-LSEA)routing protocol

The proposed F-LSEA algorithm provides link stability at each hop in the sense that each receiver in a communication link makes a forwarding decision. However, the forwarding of an RREQ is based on a fixed node residual energy and link lifetime threshold. The assumed fixed threshold does not prove to be flexible enough, and the receiver's decision-making is not flexible enough under these fixed threshold parameters. The inflexibility arises for two main reasons. First, there may be a case where all the neighbours of the receiver node have parameters below the fixed set threshold. In this case, as depicted in Figure 4-5, the receiver node becomes isolated as no node is able to forward the RREQ to the next hop. For instance, as in Figure 4-5, node S is the source node and A, B and F are the neighbour nodes of S. When nodes A, B and F receive an RREQ message, they should check the routing information for the destination (D) node. If there is any information available, they will send back a Route Reply (RREP) message to node S; otherwise, they will enter into decision mode concerning whether or not to forward the RREQ to their neighbours. In this case nodes, A,B and F check their RE and LLT with node S (the node from which the RREQ has been received). Let us assume that all the neighbour nodes of S have one parameter, *i.e.*RE or LLT, below the fixed set threshold. In this scenario, there is no way for node S to get its RREQ through the network. This problem arises in the proposed F-LSEA.

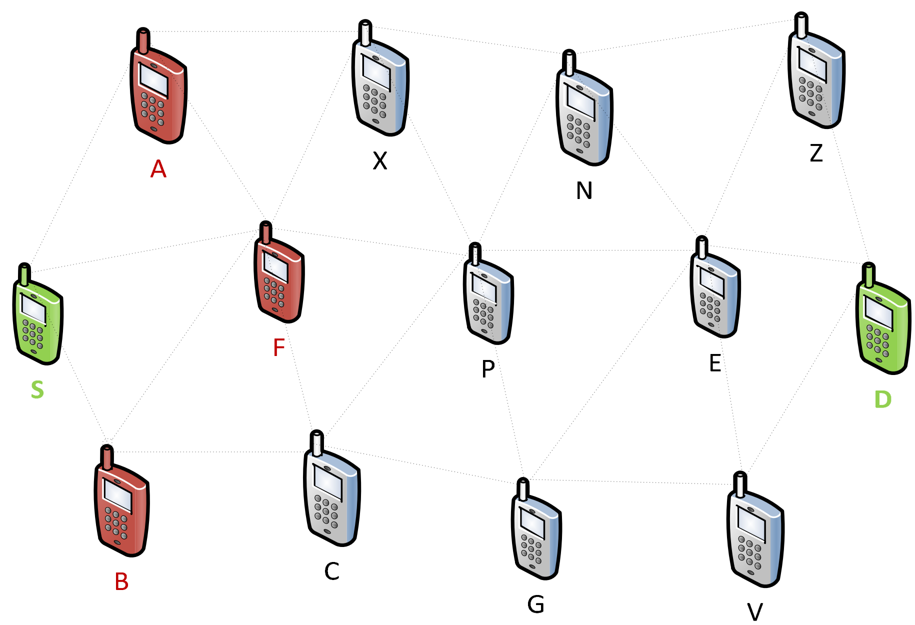

Figure 4-24: Instance of an isolated node

To overcome this drawback in the F-LSEA protocol, a new protocol has been proposed called the Average Link Stability and Energy Aware (A-LSEA) routing protocol.

In contrast to F-LSEA, the A-LSEA protocol works on the basis of average energies and average link lifetimes, and this information is gathered in the following way:

- A node sends periodic "hello" messages to its neighbours. Each node must append its Residual Energy level to the "hello" message, as shown in Figure 4-6. By doing this, any node can aggregate the RE of its neighbours to calculate the Average Energy (RE_{avg}), as shown in Equation (4-2). The (x,y) coordinates for the node are also attached to the "hello" message to allow the receiver node calculate the LLT value.
- Any node in the network can obtain LLT information on all its neighbouring nodes. To get the Average LLT(LLT_{avg}), the node aggregates its LLT with each neighbour and divides the total by the number of neighbours, as shown in Equation (4-3).

IP Address	Sequence Number
Hop Count	Lifetime
Pos $_x$	Pos $_y$
Residual Energy	

Figure 4-25: The modified 'Hello' message

A-LSEA works as follows. Once the RREQ message has been received at any node, the node follows the normal process, *i.e.* looking for routing information for the current request in its routing table. If the receiving node does not have fresh route information for the current request, it will calculate the RE_{avg} and the LLT_{avg} of all the neighbouring nodes. Further, the current node compares its own RE and LLT with the RE_{avg} and LLT_{avg}, respectively. If the RE and LLT are equal to or greater than RE_{avg} and LLT_{avg} respectively, the current node will re-broadcast the RREQ; otherwise, the node simply drops it.

Consider, for instance, the scenario in Figure 4-5, where the source node, 'S', wants to find an end-to-end path to the destination, 'D'. Node 'S' will broadcast the RREQ to its neighbours. It should be noted that the source, ‘S’, being the originator of the RREQ, will always broadcast the RREQ to all of its neighbours. This means that the RREQ originator node (*i.e*. the end-to-end path’s source node) is excluded from the A-LSEA algorithm. This means the originator node will always perform according to the route discovery process of the reactive routing protocols, i.e. AODV. All the onward nodes in the network topology will perform RREQ forwarding according to the A-LSEA as follows. Let node ‘F’ be the candidate node that has to make a decision regarding RREQ forwarding in accordance with the A-LSEA protocol. To generalize for the sake of clear understanding, let N = {N_1, N_2, N_3,…., $N_{|N|}$} be the neighbour nodes of node ‘F’. Let T = {N} U S be the set of all neighbouring nodes and the source/forwarding node. Further, let RE= {RE_1, RE_2, RE_3, …., $RE_{|N|}$} be the residual energies of the neighbouring nodes, accordingly. The average residual energy of all the neighbouring nodes is represented by Equation (4-2), as below:

$$RE_{Avg} = \sum_{i=1}^{|T|} \frac{RE_i}{|T|} \qquad (4-2)$$

Similarly, let LLT_1, LLT_2, $LLT_{3,}$…., $LLT_{|N|}$ be the link lifetimes between node ‘F’ and its corresponding neighbours. The average LLT is calculated as in Equation (4-3),below:

$$LLT_{Avg} = \sum_{i=1}^{|N|} \frac{LLT_i}{|N|} \qquad (4-3)$$

Let $LLT_{(S-F)}$ be the link lifetime between the current node, ‘F’, and node ‘S’ under the consideration that the RREQ has been received at node ‘F’ from node ‘S’, as shown in Figure 4-5. Node ‘F’ compares its own residual energy with that of its neighbours’ average level and its link lifetime, $LLT_{(S-F),}$ with that of the average, LLT_{avg}. As shown in Algorithm 2, Table 4-2, if the $LLT_{(S-F)}$ and RE_F are greater than the LLT_{avg} and $RE_{avg,}$ as calculated in Equations (4-3) and (4-2), the RREQ will be re-broadcasted by node ‘F’; otherwise, it will be dropped.

Table 4-1: The A-LSEA operation Algorithm

Algorithm 2

Input: Local information on neighbours' RE and LLT.

Output: A stable end-to-end routing path.

1. *Let S be the RREQ source/forwarding node.*
2. *Let N={n_1, n_2, n_3,..., $n_{|N|}$} be the neighbour nodes of S*
3. *Let L= {λ_1, λ_2,...,$\lambda_{|N|}$} be the links between S and all its neighbours* | $\lambda_n \in L$ is a link between S and the *neighbouring node n_n, $\forall n_n \in N$.*
4. *Let LLT_{Avg} be the averaged link lifetime associated with all neighbouring node links and the set threshold.*
5. *Let RE_{Avg} be the averaged residual energy of all neighbouring nodes, including source S..*
6. *for i= 1 to |N|*
   //at each RREQ recipient neighbouring node
7. *if* (LLT≥ LLT_{Avg}) and (RE ≥ RE_{Avg})
8. Forward RREQ to all neighbours.
9. *else*
10. Drop RREQ
11. *end if*
12. *next i*

The algorithm presented in Table 4-2 is localized and distributed in the sense that global knowledge is not required during end-to-end path computation. As opposed to previous relevant work, where the destination node decides on the best/most stable path, our proposed approach only needs localized information about the residual energy and link lifetimes of neighbouring nodes.

4.4 Performance Evaluation

In order to evaluate the performance of the F-LSEA and A-LSEA protocols, we simulated the proposed mechanisms using the NS2 Simulator [20]. The simulation environment, performance metrics and results are discussed in the subsequent sections.

4.4.1 Simulation Environment

In our simulations, the MAC layer runs on the IEEE 802.11 Distributed Coordination Function (DCF). The bandwidth is set to 2 Mbps and the transmission range is set to 250 m. The evaluations are conducted using 100 nodes that are randomly distributed in an area covering 600m x 600m. Random Waypoint was used to simulate the nodes' mobility. In the Random Waypoint model, each node starts to move from its location to a random location with a randomly chosen speed from a minimum speed equal to 5 m/s and maximum speed equal to 30 m/s. In each test, the simulation lasts for 600 seconds. The size of each Constant Bit Rate (CBR) packet is 1000 bytes and packets are generated at a fixed interval rate of 4 packets per second. 15 flows were configured to choose a random source and destination during the simulation.

For the proposed F-LSEA protocol, the LLT was fixed at 2 seconds and the RE initial values varied from 1 to 4 joule.

4.4.2 Performance Metrics

The following metrics were used to evaluate the proposed protocols:

- ***Packet Delivery Ratio*****:** the ratio of those data packets successfully delivered to the destinations to those generated by the CBR sources.
- ***Total End-to-End Delay:*** the total delay, which includes all possible delays caused by buffering during the route discovery and link recovery phases, queuing at the interface queues and retransmission delays at the MAC layer.
- ***Total Overhead:*** the number of control packets transmitted in the network, including the RREQ, RREP, Rerr and hello messages.

- ***Network Life Time:*** the aggregate time before all nodes die due to battery exhaustion.
- ***Total Data Sent:*** the total amount of data sent in the network before the nodes are unable to participate in the network due to battery exhaustion.
- ***Total Data Received:*** the total amount of data received in the network before the node is unable to receive data due to battery exhaustion.
- ***Total Data Dropped:*** the total amount of data dropped in the network.

4.4.3 Results and Discussion

In this sub-section, the obtained results are analysed and a comparative discussion is presented in terms of the parameters shown in Section 4.4.2.

4.4.3.1 Total Overhead

As shown in Figure 4-7, we compared the total overhead of the proposed schemes with that of AODV. As can be seen from the figure, the overhead increases with increases in mobility for both the AODV and F-LSEA protocols, while it remains at the same level in the case of A-LSEA. This is because the AODV protocol floods any received RREQs if no routing information is available in the routing table of the request recipient; whereas in both of the proposed protocols (A-LSEA and F-LSEA), any node first checks its link lifetime with the RREQ sender as well as its own energy level before forwarding any RREQs. This reduces the number of forwarding nodes and ultimately the number of RREQ packets in the network. The proposed mechanisms increase path stability because the returned path consists of those nodes with better link lifetimes and high residual energy levels. Moreover, when the residual energy threshold increases (*i.e.* from 1 to 4), the overhead decreases due to there being few nodes which satisfy this value. When the threshold value is high, the routing overhead is low and vice versa. In addition, it is clear that A-LSEA outperforms F-LSEA and AODV because the inflexibility of the F-LSEA protocol threshold does not assist the protocol to be aware of network conditions and parameters. There may not be any available nodes with the predefined fixed threshold (LLT or RE), so no node can participate in the end-to-end path. In contrast, the flexibility in the A-LSEA protocol provides more accurate knowledge of network conditions and parameters.

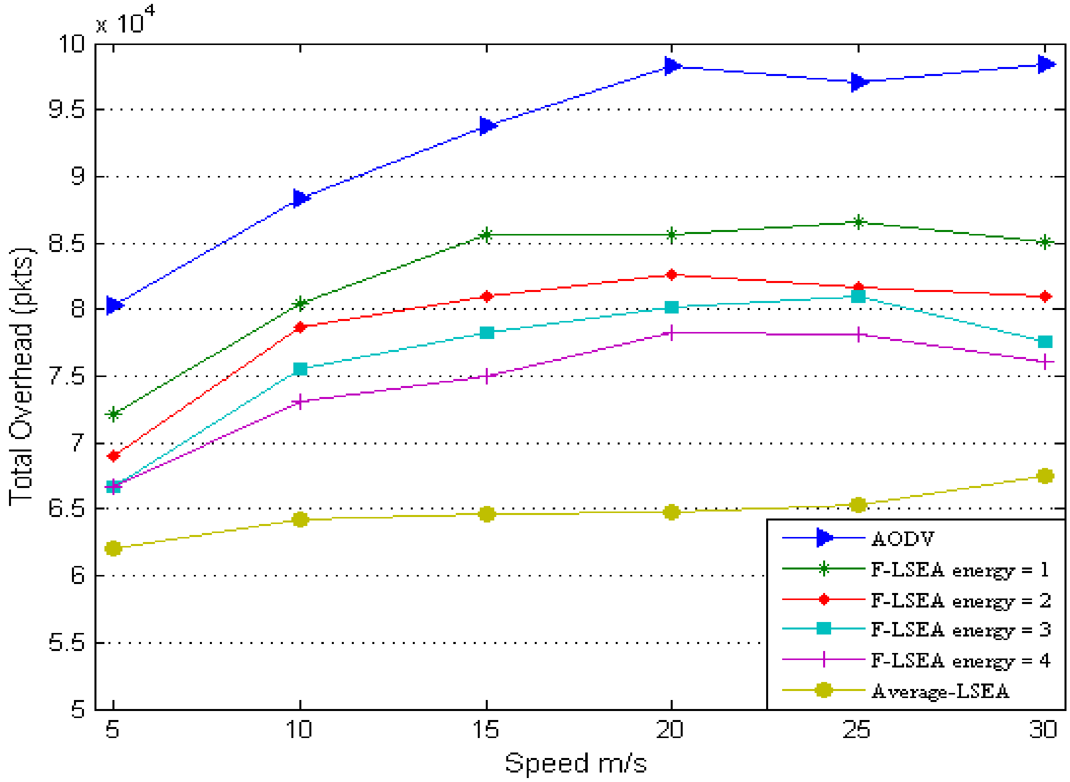

Figure 4-26: Overhead vs. Speed

4.4.3.2 Delivery Ratio

The data delivery ratio of the proposed schemes was compared with that of the AODV protocol. The results show that the combined effects of residual energy and link lifetimes affect the delivery ratio, as shown in Figure 4-8. This figure shows that F-LSEA and A-LSEA both give a better average packet delivery ratio than the AODV protocol. The reason for this is that the end-to-end paths returned by F-LSEA and A-LSEA are stable and have higher path lifetimes in comparison with AODV. These protocols consider paths with nodes that have the highest residual energy levels and good link lifetimes by running localized and distributed algorithms. These are shown as Algorithms 1 and 2 of Table 1 and 2, respectively. In the case of AODV, the network nodes are not capable of capturing the RE and LLTs of their neighbouring nodes, and hence cannot distinguish between the best and worst links. Thus, AODV blindly disseminates RREQs in the network and may return paths that have bad individual links, leading to more data drops. Furthermore, A-LSEA performs better than F-LSEA because the average values taken for LLT and RE are flexible in relation to the nodes' condition and the status of the network.

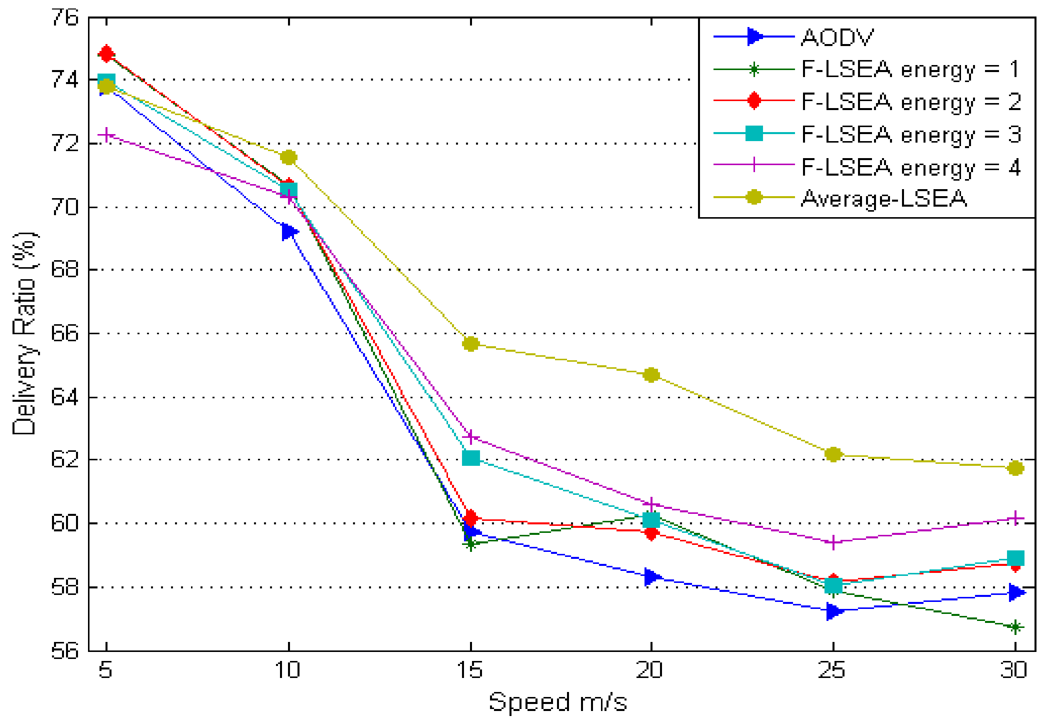

Figure 4-27: Delivery Ratio vs. Speed

4.4.3.3 Network life time

Figure 4-9 shows the network lifetime and presents a comparative analysis. It can be seen from Figure 4-9 that the network lifetime increases with increases in the energy threshold level in the case of the F-LSEA protocol. When the energy threshold is increased (1 to 4), any node can be prevented from forwarding the RREQ if its energy is below this level. This can eliminate many nodes from RREQ forwarding and ultimately lead to energy saving for nodes and hence a better network lifetime. Sending and receiving more RREQs at the same time actually causes nodes to die earlier, and they are then no longer able to be part of the network. The F-LSEA protocol's elimination of nodes, however, helps with saving energy from a global viewpoint by saving nodes' energy through cutting off them from the transmission and reception of RREQ packets. Moreover, the selection of more stable paths in the case of F-LSEA means that fewer control packets are needed for path maintenance and thus less energy is consumed.

Some RREQ messages can be considered unnecessary if the route/path created by those RREQs breaks and hence quickly becomes unavailable due to weak link quality or lower battery energy levels. Reducing the number of unnecessary RREQ messages being transmitted in the network helps the nodes to save power, which in turn leads to increases in the network's overall lifetime. The A-LSEA protocol performed better than the F-LSEA (RE =1, 2, 3, 4 with LLT = 2 in all cases) due to the fact that very flexible averaged threshold values were taken, whereas in the case of F-LSEA the threshold values are fixed. This flexibility in A-LSEA leads to more stable paths in comparison with F-LSEA and hence the total network lifetime increases.

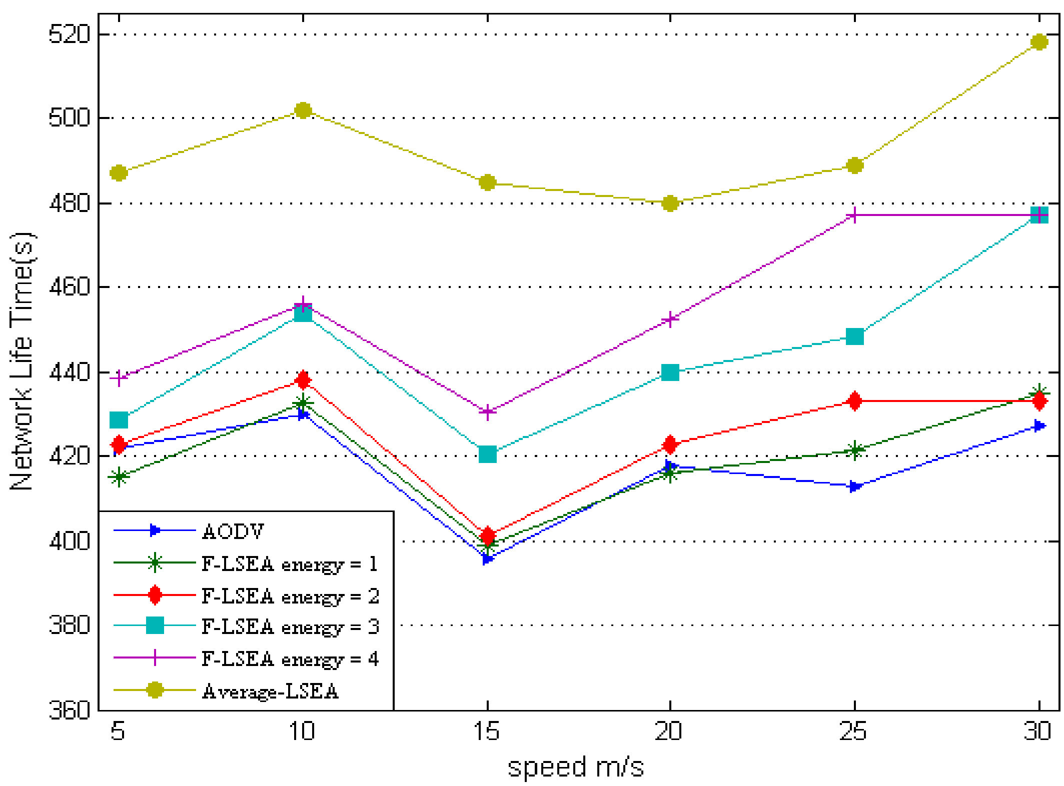

Figure 4-28: Network lifetime vs. Speed

4.4.3.4 End-To-End Delay

Figure 4-10 compares the average end-to-end delay of the proposed schemes with that of the AODV. As can be seen from the figure, the average delay experienced by the packets is greater in the case of AODV than in the proposed schemes. However, in some cases the delay in the proposed schemes (*i.e.* A-LSEA and F-LSEA) is greater, as can be seen in Figure 4-10. This is because the proposed protocols select a path based on the link quality and residual battery life of the nodes. Since the end-to-end route returned by these proposed schemes may have more hops in comparison to the AODV, more delays may be experienced by the packets due to there being more transmission and queuing delays on the path.

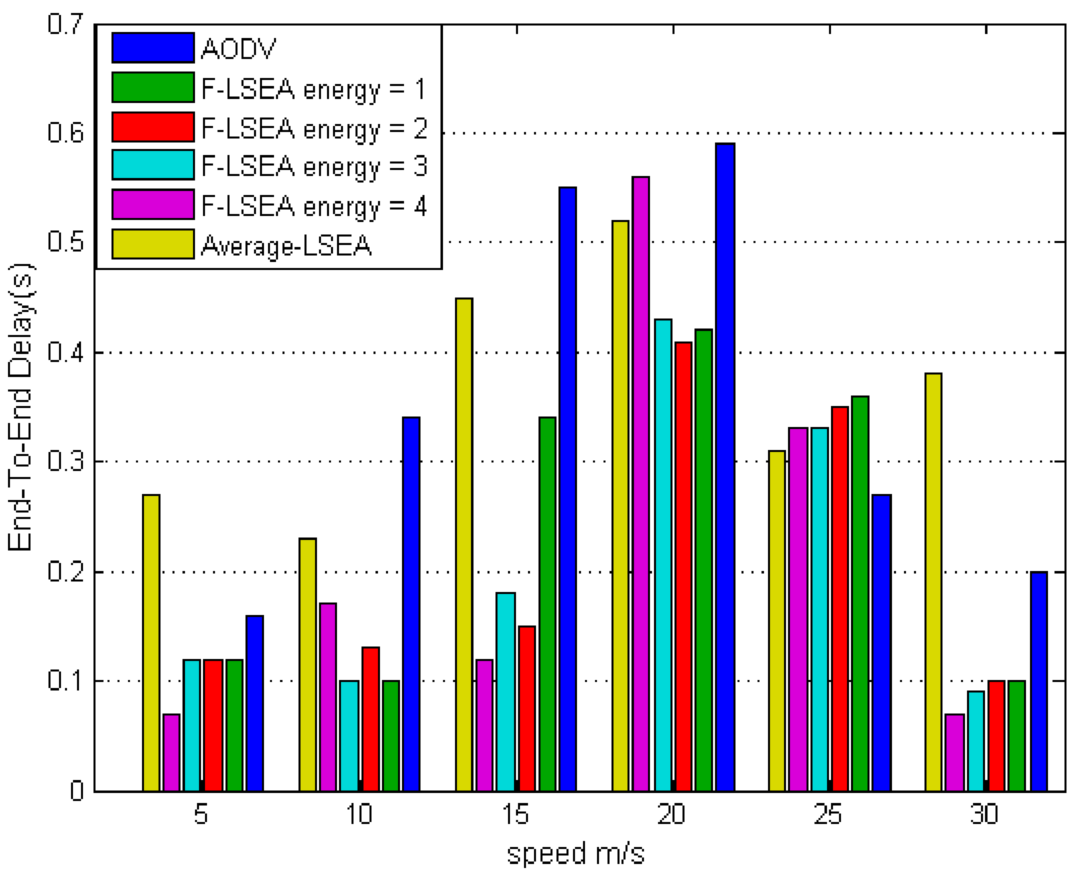

Figure 4-29: End-To-End Delay vs. Speed

4.4.3.5 Total Data Sent

Figure 4-11 shows a comparison between AODV and the proposed schemes in different settings. As can be seen from the figure, A-LSEA outperforms both the F-LSEA and the AODV protocols. This is because during the route discovery process A-LSEA applies a more sophisticated method for capturing the links' quality and residual energy by taking their averages. This more stable path selection leads to fewer route breaks and hence the total amount of data sent in this case is greater than in the other two protocols. Furthermore, F-LSEA (with a variable RE between 1 and 4) performs better than AODV for the same reason as that mentioned above (*section 4.4.3.3*). Similarly, when the RE threshold is increased, more RREQs are eliminated, and this results in more real data transfer (by energy conservation that should have been used to send the un-necessary RREQs).

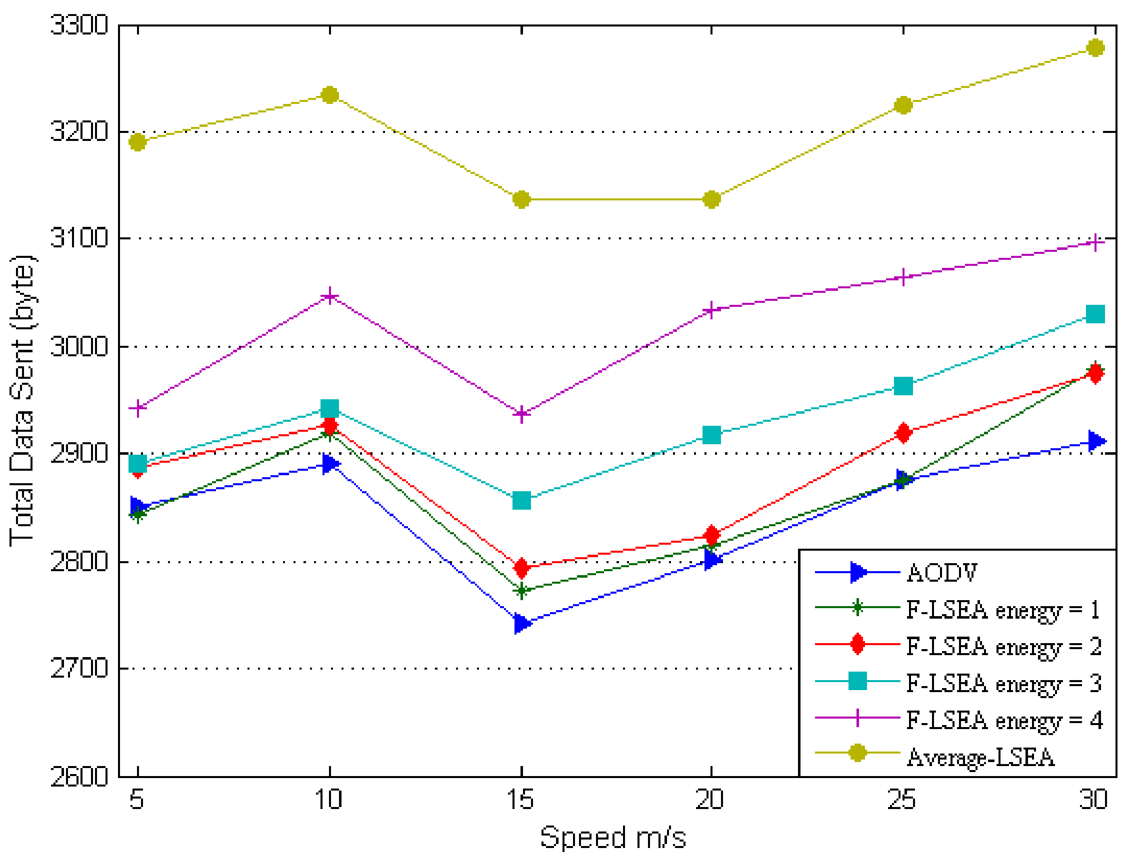

Figure 4-30: Total Data Sent vs. Speed

4.4.3.6 Total Data Received

Any node in the network will consume energy while receiving data and, at the same time, energy consumption will increase when the distance between the sender and the receiver is great. Due to these facts and the algorithm applied in A-LSEA, A-LSEA outperforms F-LSEA and AODV, as shown in Figure 4-12. A-LSEA returns those end-to-end paths that are capable of maintaining route stability and providing reasonable distances between the nodes; similarly, the most important factors in calculating the LLT between two nodes and good RE among the nodes are involved in the route computation. Obviously, the total amount of data received decreases for all the protocols under observation when the mobility of the nodes increases, as shown in Figure 4-12. In addition, F-LSEA (with a variable RE from 1 to 4) performs better than the AODV in terms of the total amount of data received for the same simulation parameters. As can be seen in the figure, an increase in the fixed threshold for RE leads to fewer RREQ packets which satisfy the requirements of the fixed threshold being sent, and this directly affects the number of RREQs received (fewer RREQs being sent means fewer RREQs being received),leading to more real data being received.

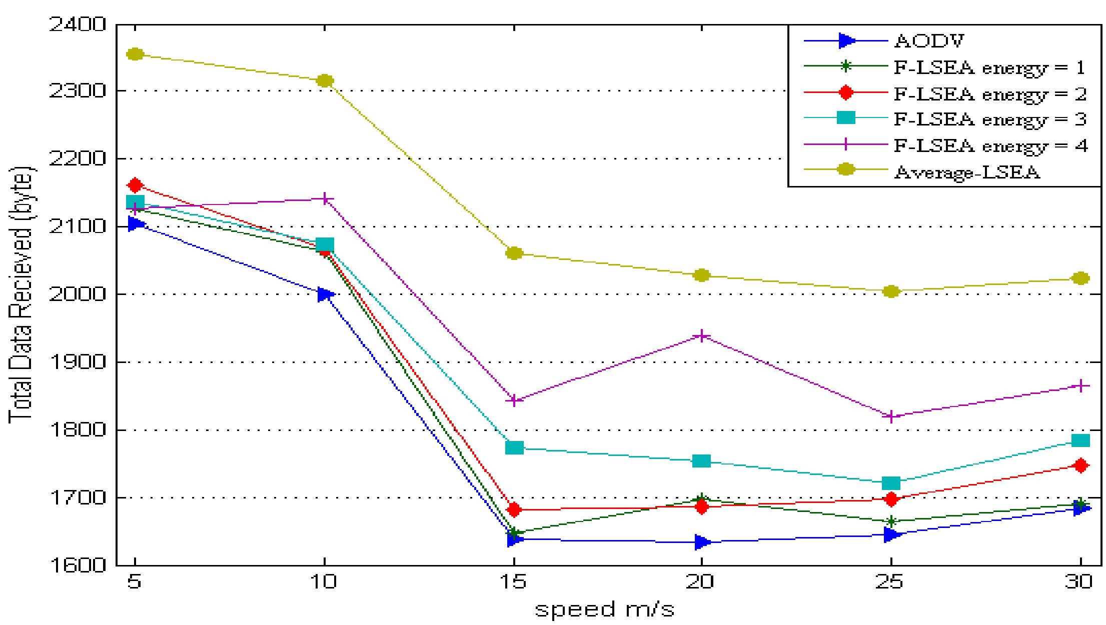

Figure 4-31: Total Data Received vs. Speed

4.4.3.7 Total Data Drop

Figure 4-13 compares the proposed F-LSEA (in various settings), A-LSEA and AODV protocols in terms of total data drops during communication. As demonstrated in Figure 4-13, A-LSEA shows a low rate of data drop in comparison to those under the F-LSEA and AODV methods. This is because A-LSEA provides more stable paths and hence less congestion. When congestion occurs in a network, it is likely that the nodes will drop more data than under normal network conditions. Furthermore, interference between the nodes while sending data, collisions and queuing lengths have the highest impacts on data packet dropping.

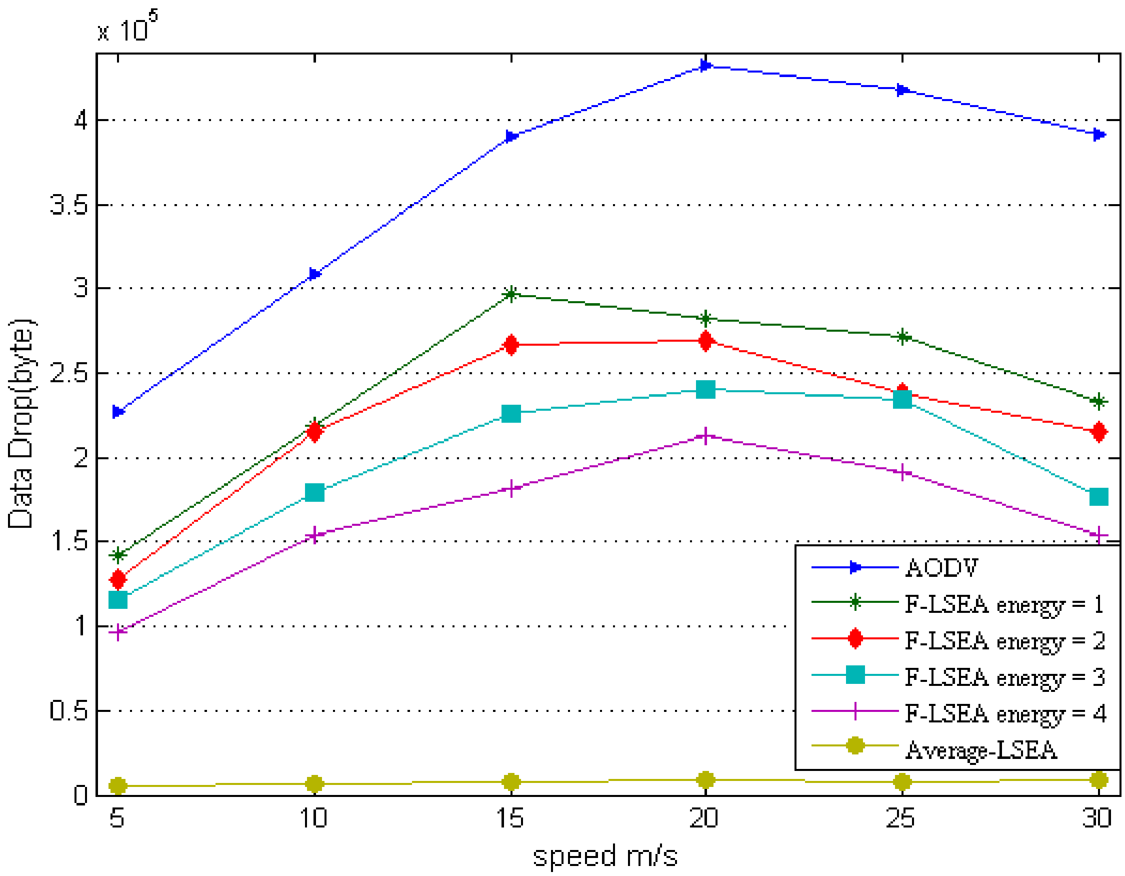

Figure 4-32: Total Data Drop vs. Speed

Moreover, a small increase in A-LSEA behaviour can be observed in comparison to F-LSEA and AODV as the mobility of the network nodes increases. The steady increase in data loss in the A-LSEA is due to the fact that it incurs fewer RREQs in the network, resulting in more free channel time, shorter queue lengths and less interference in the network, leading to less overhead. Ultimately, A-LSEA provides more stable routes than AODV and F-LSEA and it is more likely that the routes will remain for a long time before a new route needs to be discovered, resulting in less overhead in the network. On the other hand, routes created by AODV do not last for long and it is soon necessary to discover a new route, which results in more overhead in the network. Similarly, in the F-LSEA (with a variable RE of 1 to 4) a route will last only for the predefined fixed threshold before a new route needs to be discovered, which results in more overhead. It can be noted that when the predefined threshold increases in the F-LSEA protocol the overhead decreases due to there being less RREQ packet forwarding.

4.4.3.8 Number of RREQs sent

The number of RREQs sent, as shown in Figure 4-14, has a significant impact on the performance of all the routing protocols discussed in this chapter (AODV, F-LSEA and A-LSEA). An increase in the number of RREQs in the network leads to busier and more occupied channels. In addition, the nodes consume more energy in receiving and sending these RREQs, which is reflected in the Network Lifetime, Overhead, Real Data Sent, Real Data Received and Delivery Ratio for real data sent. Figure 4-14 shows that A-LSEA outperforms both the F-LSEA (with a variable RE of 1 to 4) and AODV protocols. Furthermore, the fixed set threshold RE for the F-LSEA protocol plays a major role in reducing the number of RREQs sent/forwarded through the network; increasing the threshold decreases RREQ forwarding and vice versa.

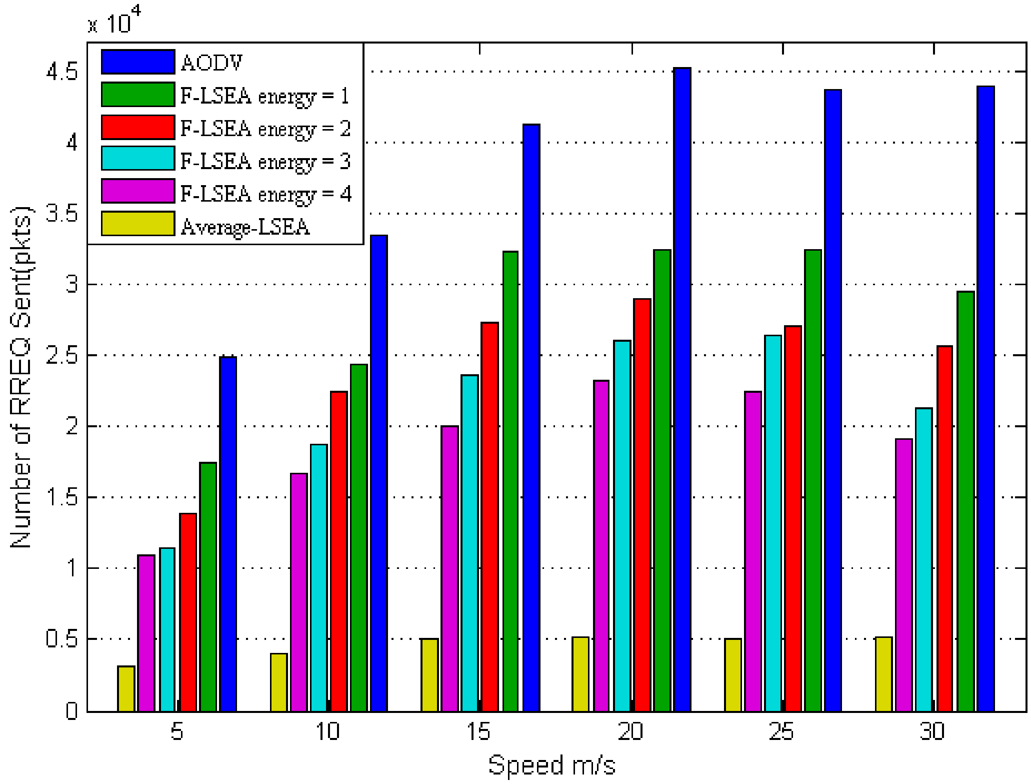

Figure 4-33: RREQ Sent vs. Speed

4.4.3.9 Average Throughput

Figure 4-15 shows the comparative average throughput of both the proposed schemes and the AODV protocol. It can be observed that the throughput of all the schemes decreases with increases in mobility. This is obviously because the mobility of the nodes affects link breakages and hence leads to more re-initiation of end-to-end routes, resulting in reduced throughput. Comparatively, the average throughput is equal in the AODV, F-LSEA and A-LSEA routing protocols. Hence, the proposed schemes improved the other metrics while, at the same time, obtaining convergent average throughputs.

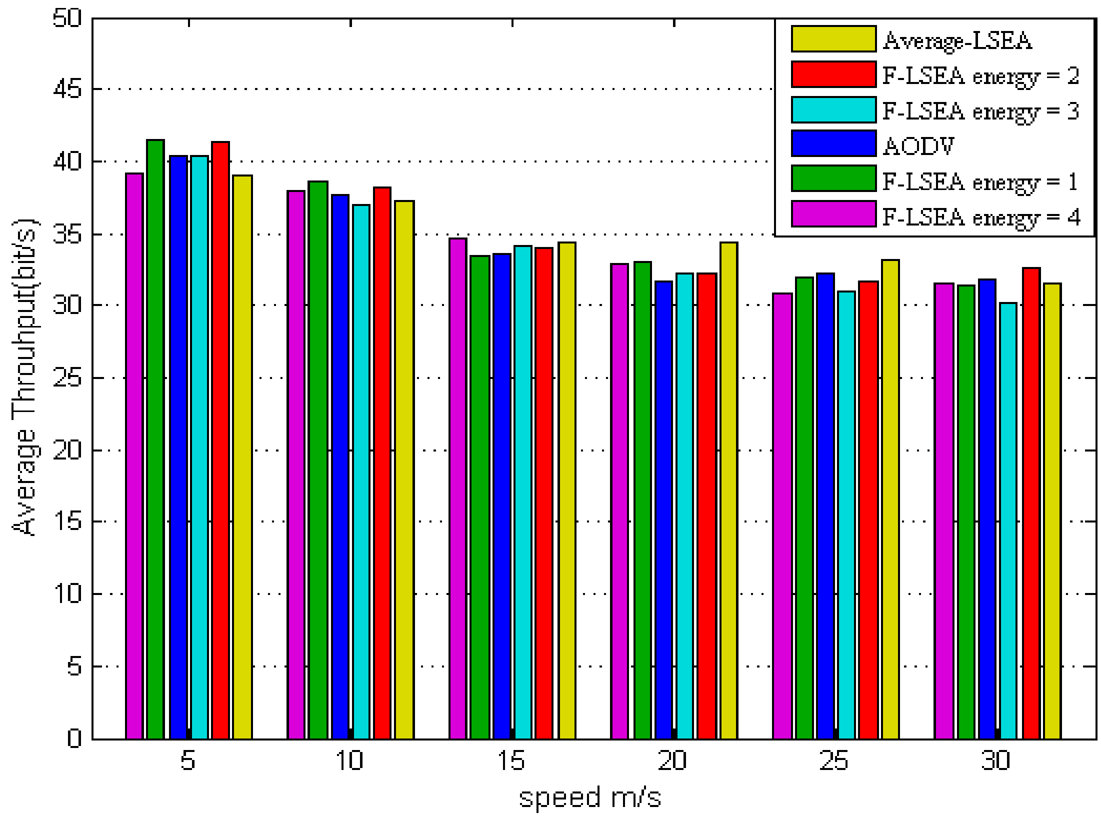

Figure 4-34: Throughput vs. Speed

4.5 Conclusion

Route discovery process in the reactive routing protocols can consume enormous amounts of network resources due to the dissemination of RREQ packets into the network. Further, MANET nodes are energy-constrained devices due to the extreme mobility in these types of networks. The number of control messages transferred and received in the network dramatically affects the nodes' availability and consequently the network lifetime. Furthermore, the MANET topology changes frequently and the links among the nodes are likely to break after a while. Any node that forwards RREQ packets involves itself in the end-to-end route established. However, the participation of nodes with insufficient Residual Energy (RE) and bad Link Life Time (LLT) affects the route quality. Accordingly, the Link Stability and Energy Aware protocol (LSEA) has been developed to improve the network's lifetime. The proposed protocol helps to control the global dissemination of RREQs in the network by eliminating those nodes with residual energy below a specific threshold value from participating in the end-to-end route.

The key concept behind LSEA is that a node must have enough RE before forwarding the RREQ and advertise itself as a participant node in the end-to-end path. Furthermore, in the LSEA protocol the LLT between the RREQ sender and RREQ receiver has been measured and the receiver node must have a good LLT with the RREQ sender before forwarding the RREQ. So only those nodes that have a good RE and LLT will be allowed to forward the received RREQ further if no routing information was available in their routing table. Combining these two conditions gives the route more stability and less frequent route breakages. The proposed LSEA protocol significantly increases the network's life time by up to 19% compared to other on-demand routing protocols, while obtaining the same level of packet delivery ratios and network throughput.

4.6 References

[1] M. Abolhasan, T. Wysocki, E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks“, Ad Hoc Networks 2 (1), pp. 1 – 22, 2004.

[2] De MoraisCordeiro, C. and Agrawal, D.P. "Mobile ad hoc networking", Center for Distributed and Mobile Computing, ECECS, University of Cincinnati, 2002.

[3] Maleki, M., Dantu, K. and Pedram, M. "Lifetime prediction routing in mobile ad hoc networks", IEEE Wireless Communications and Networking WCNC, pp. 1185, 2003.

[4] C. Perkins, E. Royer, “Ad-hoc on-demand distance vector routing“, in: Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100, 1999.

[5] D. B. Johnson, Y. Hu, D. A. Maltz, IETF Request for Comments: 4728, “The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4“, February 2007.

[6] H. M. Ali, A. Busson, “Network Layer Link Management using Signal Strength for Ad-hoc Networks”. Proc. of IEEE on Communication, Network-ing& Broadcasting, pp. 141 – 146, Sousse , July 2009.

[7] Dube, R., Rais, C.D., Wang, K.-Y., Tripathi, S.K., “Signal stability based adaptive routing (SSA) for ad hoc networks”. IEEE Personal Communications 4, pp. 36–45, February 1997.

[8] Wang, S.Y., Liu, J.Y., Huang, C.C., Kao, M.Y. and Li, Y.H. "Signal strength-based routing protocol for mobile ad hoc networks", Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference onIEEE, , pp. 17.

[9] Ali, H.M., Naimi, A.M., Busson, A. and Vèque, V. (2007) "An efficient link management algorithm for high mobility mesh networks", Proceedings of the 5th

ACM international workshop on Mobility management and wireless access ACM, , pp. 42, 2005.

[10] Qayyum, A., Jacquet, P. and Muhlethaler, P. "Optimized Link State Routing Protocol (OLSR)", 2003.

[11] Kaplan, E.D. and Hegarty, C.J. Understanding GPS: principles and applications, Artech House Publishers, ISBN 1-58053-894-0, 2006.

[12] W. Su, S.-J. Lee, and M. Gerla, "Mobility Prediction and Routing in Ad Hoc Wire-less Networks," Int'l J. Network Management, vol. 11, no. 1, pp. 3-30, Feb. 2001.

[13] [11] M. Al-Akaidi, and M. Alchaita, "Link stability and mobility in ad hoc wireless networks," IET Communications, vol. 1, pp. 173-178, April 2007.

[14] Meghanathan, N. "A location prediction-based reactive routing protocol to minimize the number of route discoveries and hop count per path in mobile ad hoc networks", The Computer Journal 52 (4): 461-82, 2009.

[15] Singh, S., Woo, M., Raghavendra, C.S., "Power-aware routing in mobile ad hoc networks". In: Proc. of 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 181–190, 1998.

[16] Toh, C.-K. "Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks". IEEE Communications Magazine 39, 138–147 June 2001.

[17] Feng, D., Zhu, Y. "An Improved AODV routing protocol based on remaining power and fame". Proc of International Conference on Electronic Computer Technology, pp. 117–121, February 2009.

[18] Chen, C.W., Weng, C.C. and Kuo, Y.C. "Signal strength based routing for power saving in mobile ad hoc networks", Journal of Systems and Software, vol. 83, no. 8, pp. 1373-1386. 2010.

[19] Hamad, S., Noureddine, H. and Al-Raweshidy, H. "LSEA: Link Stability and Energy Aware for efficient routing in Mobile Ad Hoc Network", Wireless Personal Multimedia Communications (WPMC), 14th International Symposium on IEEE, pp. 1, 2011.

[20] http://www.isi.edu/nsnam/ns/ns-build.html, Retrieved in July 2012.

CHAPTER 5

Position-based Selective Neighbours

5.1 Introduction

Wireless telecommunication has undergone intensive research attention during the last decade from both the academic and industrial sectors due to the facilities provided by this form of media. Wireless access is now preferred to wired technologies because it gives more freedom to move around. Mobile Ad-hoc Networks (MANETs) have attracted the research community's interest in terms of finding ways to enhance their operation and performance. MANETs consist of mobile nodes connected to each other via wireless links with no existing access points or any kind of permanent infrastructure. Furthermore, much work has been carried out across all the Open Systems Interconnection (OSI) layers from the application to Medium Access Control (MAC). In particular, numerous routing algorithms have been proposed in order to provide end-to-end routes that are reliable and robust against node mobility.

In wireless networks, neighbouring nodes share the wireless medium and the nodes have to compete with other to get access to the medium (channel). The Medium Access Control (MAC) layer controls this operation. The main goal of an MAC protocol is to regulate wireless devices' access to a shared wireless medium. In the process, several timing constraints are imposed by the MAC protocol in order to better regulate the shared resource and avoid collisions. Collisions can occur, as illustrated in Figure 5-1, where node A is not aware that node B is currently busy receiving some data from node C and therefore may start its own transmission, causing a collision at node B. These collisions and interference from neighbouring nodes, as well as the presence of the hidden nodes and the distances between senders and receivers, greatly affect wireless network performance.

MANETs can suffer from all these above mentioned problems, especially when there is a high level of data and control packet traffic and the topology is highly mobile.

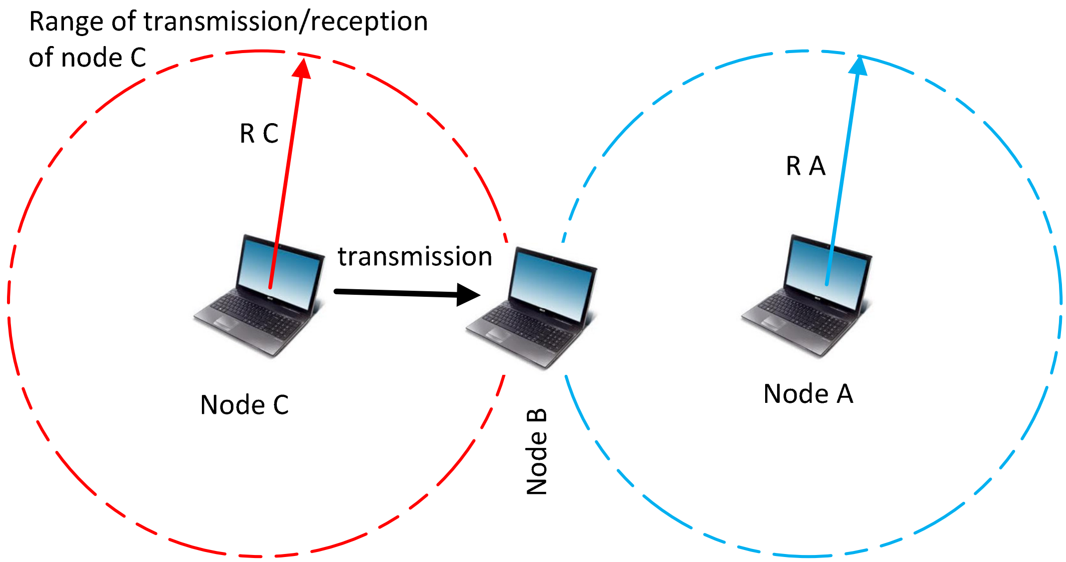

Figure 5-35: Instance of the Hidden Node Problem

Due to the highly mobile topology of MANETs, and the nodes acting as data generating as well as forwarding entities in the network, the designing of efficient and robust routing protocols is a crucial task that requires more effort. Recently, many routing protocols have been proposed for MANETs for establishing end-to-end paths between data-generating sources and sink destination nodes in multi-hop scenarios [1-6]. In conventional on-demand routing protocols [4-5], a node discovers routes to a particular destination by broadcasting a Route Request packet (RREQ). Upon receiving the RREQ, the node checks whether the packet has previously been received. If the packet has already been received, the node will drop it; otherwise, it will send a Route Reply (RREP) back to the source node if the route is available. In either case, the node will rebroadcast the RREQ to its immediate neighbours until the destination is found. This method of route discovery is referred to as blind flooding. Every mobile node rebroadcasts one copy of the received RREQ, so the maximum number of rebroadcasts is equal to N – 2 in the global network, where N is the number of nodes in the network. This can potentially lead to excessive redundant retransmissions and therefore high channel contention, causing excessive packet collisions in dense networks. Such a phenomenon is referred to as the broadcast storm problem [7] and significantly increases network communication overhead and end-to-end delay, while increasing bandwidth loss [7,9].

Many approaches attempt to resolve the flooding problem by reducing the number of redundant messages. However, this leads to a low degree of coverage and connectivity. This interdependency between the two phenomena poses the challenge of balancing message overhead (*i.e*., the level of redundancy) and coverage [8].

Reducing collisions in the network can improve network performance. This is especially the case in MANETs, where the nodes are supposed to cooperate with each other in order to connect to those nodes that are out of their transmission range. Furthermore, duplicate messages generated by broadcasting RREQ messages across the entire network while seeking an end-to-end path increase the chances of potential collisions. Eliminating unnecessary RREQ packets can reduce the number of packet collisions and hence improve network performance.

This chapter discusses a new algorithm that reduces RREQ propagation in the global network to a minimum while preserving network connectivity. The proposed algorithm assumes that all nodes are aware of their own (x, y) coordinates as well as those of their neighbours. Based on these positions, a node selects the best neighbours from its own perspective to rebroadcast RREQs further. The transmission range of the source node is divided into four equal zones ($Zone_1$, $Zone_2$, $Zone_3$ and $Zone_4$) in a set M= {M_1, M_2, M_3, M_4}. Further, four neighbour nodes are selected from the zones based on their residual energy levels and the quality of their links with the source node.

The aim of this chapter is to outline an efficient routing protocol that tackles the flooding problem and reduces the propagation of RREQs to the minimum while maintaining comparable reachability among the nodes in a global network.

5.2 The Flooding Problem in MANET Reactive Routing Protocols

Flooding is a reactive routing operation whereby a source node sends the same RREQ message to all its neighbours. Intermediate nodes then forward the same message to all their neighbours. This process continues until the RREQ message reaches its destination or one of the intermediate nodes returns a valid route. Therefore, broadcasting seems to reduce network performance by increasing the number of unnecessary RREQs in the network and utilizing the bandwidth while causing collisions among the nodes. Hence, it is important to show caution when choosing which intermediate nodes will rebroadcast the RREQ message so as to avoid packet redundancy in the route discovery dissemination process.

Flooding, or broadcasting, is very costly and should be used with care. In the following, we will present the analysis proposed by Tseng and Ni [7], who have discussed the greater coverage area that can be provided by rebroadcasting received RREQ messages. For instance, in Figure 5-2, node N sends a broadcast, which is received by its neighbouring node A. Node A further rebroadcasts this message. Let us assume that T_N and T_A represent the areas of the circles covered by N's and A's transmission ranges, respectively. Rebroadcasting by node A provides an additional coverage area, denoted by $S_{A\text{-}N}$ in Figure 5-2. Equation (5-1) is used to calculate the intersection area between the two nodes, assuming that the transmission area is represented by a circle for each node, as follows:

$$\text{INTC}(d) = 4\int_{d/2}^{r} \sqrt{r^2 + x^2}\; dx. \qquad (5\text{-}1)$$

Where INTC = the intersection between the transmission of the two nodes

r = radii for nodes T_N and T_A

d = distance between the two nodes.

Then,

$$\pi r^2 - \text{INTC}(r) = r^2\left(\frac{\pi}{3} + \frac{\sqrt{3}}{2}\right) \approx 0.61\ \pi r^2 \qquad (5\text{-}2)$$

Equation (5-2) illustrates that message rebroadcasting by node A provides only 0-61% more coverage (previously covered by transmission from node N). Furthermore, to calculate the average value of $\pi r2$ − INTC*(d)*, let node **A** be randomly located in any part of **N**'s transmission range. Then, integrating the above value over the circle of radius *x* centred at N for *x* in [0*, r*] gives an average acquired value, as in Equation (5-3):

$$\int_0^r \frac{\pi r^2 \, . \, [\pi r^2 - INCT(x)]}{\pi r^2} dx \approx 0.41 \;\; \pi r^2 \qquad (5\text{-}3)$$

Therefore, rebroadcasting by node A can provide only 41% more additional coverage area than the previous broadcast. Furthermore, if node A waits to receive the same message from different neighbours, the additional coverage area will shrink and, in some cases, rebroadcasting the received RREQ will not provide any additional coverage area.

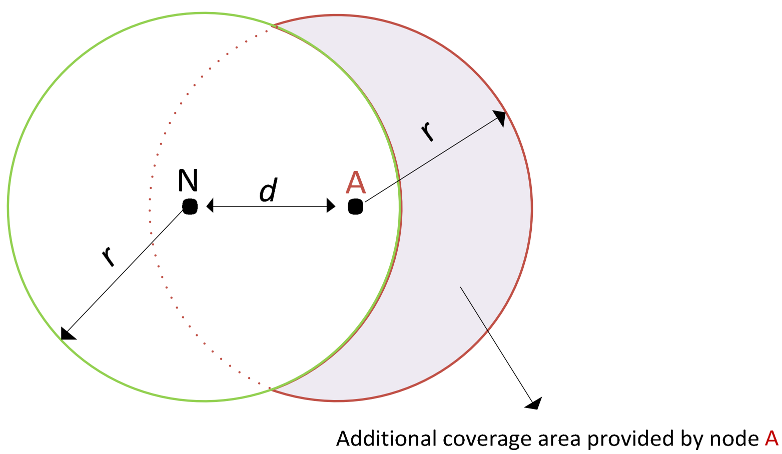

Figure 5-36: Intersection of the transmission ranges of two nodes (N, A)

5.3 Related Work

Recently, several approaches have suggested ways to decrease the effect of the broadcast storm caused by simple flooding [7-10]. These approaches can be classified into five categories [8]: simple flooding, position-based methods, probability-based approach, neighbour knowledge methods and various other approaches using different techniques.

5.3.1 Simple Flooding

Simple or "blind" flooding is a technique used by reactive/on-demand routing protocols for the propagation of Route Request (RREQ) packets among the nodes in a network. One of the most popular reactive routing protocols, AODV [4], applies this blind flooding technique for route discovery between any source and destination; the source simply broadcasts the RREQ, and the intermediate nodes rebroadcast the same RREQ if they have not seen it before. Blind flooding is a simple technique in which each node receives and then re-transmits messages to all its neighbours. This technique applies only one condition to the nodes: to discard messages they have received before [9]. However, straightforward flooding of the network with broadcast messages is usually costly and results in serious redundancy and collisions in the network; such a scenario has often been referred to as the broadcast storm problem.

In MANETs, nodes are energy-constrained devices due to the extreme mobility in these types of networks. The number of control messages transmitted and received in the network dramatically affects the nodes' availability and consequently the network's lifetime. Therefore, nodes in MANET networks should conserve their energy by sending and receiving only important packets and discarding other (repetitive) messages.

5.3.2 Neighbour Knowledge Methods

The key concept for this method is expansion of information about node' neighbours; this allows each node to send one-hop or two-hop neighbour node addresses to their neighbours. The node utilizes existing "hello" messages to send this information periodically. Through doing this, each node can know implicitly which nodes it has in common with other nodes. The authors of [11] proposed the concept of 2-hop backward neighbour information, to be used for minimizing the number of forwarding nodes and reducing collisions in the network. Their proposed mechanism requires the exchange of 1-hop hello messages. In [12], the authors proposed a novel joint 1-hop neighbour information-based flooding scheme that consists of two sub-algorithms, *i.e.*, sender-phase and receiver-phase algorithms. The sender-phase algorithm helps a node to select a subset of its 1-hop neighbours for forwarding flooding messages. This algorithm selects forwarding nodes which can make the greatest contribution to flooding message dissemination. In [13] the authors proposed an Efficient Flooding Scheme Based on 1-hop Information in Mobile Ad Hoc Networks. The basic idea behind their protocol is that each node uses its one-hop neighbour's information. Each node which is seeking a new route determines a subset of its neighbours as candidate neighbours to rebroadcast this message if they receive it; this is done by attaching those nodes' addresses to the RREQ message. Upon receiving the RREQ, the node will look for its address. If the receiving node finds its address, the sending node provides candidates from a new subset of its neighbours and rebroadcasts the RREQ. Otherwise, the node will drop the RREQ.

Neighbour knowledge methods succeed in reducing redundant RREQs in the network. However, the periodic hello messages carry all the neighbouring nodes' addresses and thus utilize the available bandwidth and, in some cases, may increase the overhead. Furthermore, due to the mobility of the nodes, the one-hop or two-hop information gathered is not always accurate.

5.3.3 Position-Based Methods

Area-based methods consist of distance-based and location-based schemes. They emphasize how much more area (than that covered by the previous broadcast) a node can offer if it rebroadcasts the same received message. Within a node's transmission range, the greater the distance from the previous broadcasting node, the more additional coverage can be acquired, resulting in more opportunities to reach more nodes. In [14], the authors proposed an approach called **F**looding based on **O**ne-hop **N**eighbour **I**nformation and **A**daptive **H**olding (FONIAH). They assumed that nodes are able to know their geographical location (*x, y* coordinates). In addition, sharing positions among the nodes requires each node to send hello messages containing location information continuously. The key concept of FONIAH is that the node selects the furthest nodes in its transmission range and then calculates the distance between itself and the furthest nodes; this distance is referred to as the Maximum Distance D_{max} . D_{max} is used to calculate the waiting time at the receiver node.

In [15], the authors proposed Position-based Selective Flooding (PSF), in which they applied a new strategy to selecting forwarding nodes. The key concept of PSF is that, first, the source node broadcasts the RREQ packet just like a normal AODV route discovery operation. The receiving nodes will rebroadcast the received RREQ if, and only if, they fall in the Forwarding Region (FR) area, shaded grey in Figure 5-3. The authors stated that this is the best position for neighbours to rebroadcast RREQs from as the signal will probably be strong and this will result in a greater coverage area. However, this method can fail to find the requested destination because the destination node may be in the opposite direction to the forwarder.

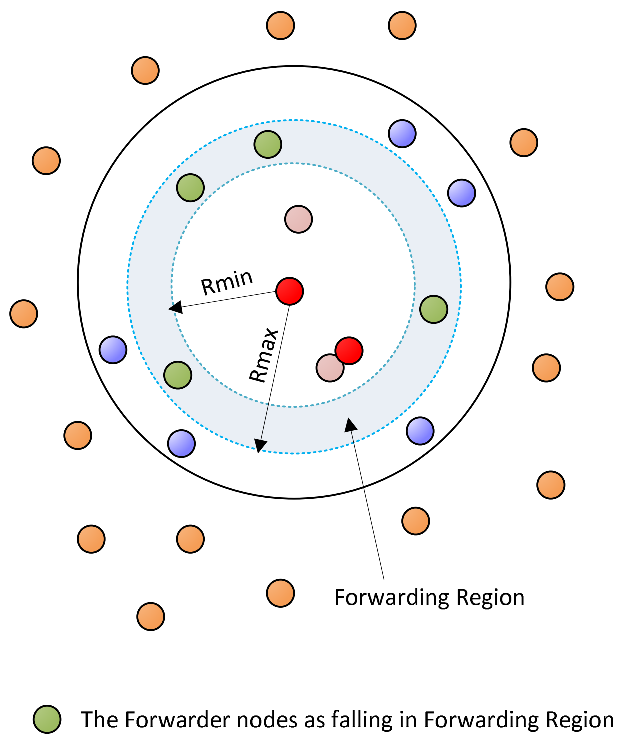

Figure 5-37: Illustration of the Forwarding Region (FR) in the PSF method

In [16], we proposed a new algorithm to reduce the overhead generated by redundant RREQ messages. Candidate Neighbours to Rebroadcast the RREQ (CNRR) divides the transmission ranges for nodes that would like to send/rebroadcast RREQs into four equal zones ($Zone_1$, $Zone_2$, $Zone_3$ and $Zone_4$). Then one node per zone is selected to rebroadcast the RREQ. The node selection in each zone is based on the distance between the node and its neighbours.

5.3.4 Probability-Based Approaches

Probability-based approaches depend on assigning different probabilities of node participation in the network. This probability is a sign to nodes to rebroadcast or discard the received RREQ. Probability values can vary for different algorithms and node conditions. The authors of [17] proposed a new probabilistic flooding algorithm which is able to raise the threshold value when a node has a high density of neighbours; in this case the node is not permitted to rebroadcast the received RREQ. In contrast, the node will have a high probability of rebroadcasting the received RREQ if it has a low number of neighbour nodes. [18] proposes the Dynamic Adjusted Probabilistic Flooding algorithm (DAPF). The key idea in this method is to rebroadcast a message with probability function that is adjusted dynamically with passing time and local observations such as network density and the number of duplicate received messages. In [19], the authors proposed a dynamic probabilistic broadcasting approach, which can be classified as a combination of two methods (probabilistic and position-based methods). Probabilities are assigned to nodes based on their distances from the RREQ sender. Thus, if the receiver node is closer to the sender node, then the probability of rebroadcasting the RREQ is low; otherwise, the probability of rebroadcasting the RREQ is high and significantly more coverage area is achieved.

5.3.5 Other Approaches

The research community has also considered various other approaches to tackling the broadcast storm problem. In some of these research studies [20-21], the authors have considered node speed as a condition for rebroadcasting RREQs. The authors of [20] proposed two approaches to enhancing the route discovery phase and increasing overall routing performance. They considered node speed as a condition for the node's participation in the route discovery phase; node mobility is periodically computed (low or high) and then a decision to forward the received RREQ message or not is made based on that computation. The two approaches are 1- Per-Hop Mobility Aware (PH-MA-AODV) and 2- Aggregate-AODV (Agg-AODV). In the both approaches, the node keeps track of its speed.

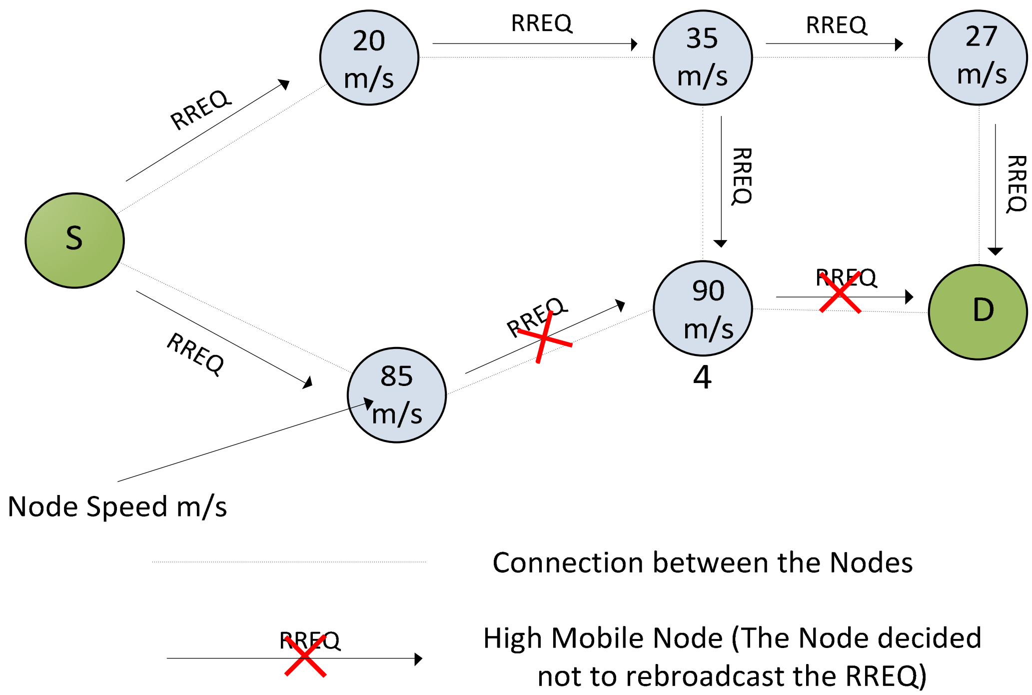

Figure 5-38: RREQ propagation in the PH-MA-AODV Method

In the first approach, upon receiving the RREQ the node will decide whether to forward the RREQ based on its speed. If its speed is high, the node will decide to discard the received RREQ, assuming that the link between it and the sender node will break soon because of its mobility. If the speed is low, the node will decide to participate in the route and forward the received RREQ. Figure 5-4 illustrates those nodes with a speed greater than 80 m /s and which will discard the received RREQs. In the second approach, a node attaches its speed and then forwards the received RREQ. The destination node will select the best route to the source node based on the low aggregate speed of the nodes from which it has received the RREQ.

5.4 The Proposed Position-based Selective Neighbours (PSN) Protocol

This section discusses the Position-based Selective Neighbours (PSN) routing protocol. As mentioned in the previous chapters, on-demand routing protocols, e.g. AODV, follow a blind flooding mechanism to disseminate route discovery packets in a global network. This mechanism works well in situations where reachability is the only concern among the nodes of the network. However, as these protocols use hop counts as the only metric for end-to-end route selection, unstable paths can be returned owing to the extremely mobile environment of MANETs. To tackle this problem, we proposed two solutions in the previous chapters. For example, Chapter-3 outlines the mechanism of placing the neighbours of the sending/forwarding node into different zones. Further, Chapter-4 takes link stability into account by explicitly looking into the quality of links and the residual battery energy of neighbouring nodes. These proposed protocols reduce network-wide RREQ dissemination to a minimum while preserving the desired connectivity. However, the proposed mechanisms presented in the previous chapters suffer from their own problems when considered in isolation. For example, the CNRR protocol, discussed in Chapter-3, only considers the locations of the neighbouring nodes, and hence RREQ forwarding decisions are made based solely on distance. Although this method reduces RREQ dissemination to a considerable extent, it ignores link quality and the remaining nodes' energies. Therefore, the routes returned may not be stable over a long period. The LSEA protocols presented in Chapter-4 do consider the link quality and residual energies of the nodes during the route discovery phase. This method returns stable paths; these are live for more time in the sense that the nodes in the end-to-end paths have more energy and are comparatively less mobile. This stability in the paths results in high throughput and fewer delays. However, since this method does not consider the nodes' positions during RREQ dissemination, connectivity can be compromised.

5.4.1 PSN Route Discovery Mechanism

The proposed PSN protocol's route discovery process consists of three phases, as given below.

First, a node, 'S', which intends to send an RREQ, divides all of its neighbours into four zones. Dividing the neighbouring nodes into four zones is exactly the same mechanism as that presented in Chapter-3. The (x,y) coordinates of each neighbour are made known to a node with the assistance of a specialized positioning device such as GPS [22]. In the second phase, each node 'S' compares the average Link Lifetime (LLT) of each node in a specific zone with the averaged Link Lifetime (LLT_{avg}) taken from the specific times of all the nodes sharing links with the current node 'S'. Similarly, node 'S' compares the residual energies of all its neighbours in the specific zone with the average RE (RE_{avg}). In the third phase, node 'S' selects a Candidate Node (CN) from among the neighbours in a specific zone based on specific conditions. The CN is the node in the specific zone which is selected by the current node 'S' for forwarding the current RREQ. Node 'S' will select the CN based on two conditions. First, if the LLTs and the REs of the neighbouring nodes are higher than the LLT_{avg} and RE_{avg}, then the current node is selected as a Potential Candidate Neighbour (PCN) and added to node 'S' 's Potential Candidate List (PCL). The same process is performed by node 'S' for all of its neighbours in the specific zone, and the nodes are either placed in the PCL or dropped, according to the conditions mentioned earlier. In the next phase, node 'S' selects CNs from the already existing PCL based on their LLTs and REs. One node is selected from the PCL set on the basis that it has more LLT and RE in comparison to other nodes in the PCL. However, if there is a node neighbouring node 'S' in the specific zone which can meet the LLT_{avg} and RE_{avg} conditions for consideration for the PCL, that node which has the most LLT and RE in the specific zone is selected as the CN. The same process is continued for all the zones, and in this way node 'S' selects four neighbours to use for RREQ forwarding.

For instance, consider the MANET topology shown in Figure 5-5. As can be seen from the figure, node X aims to send a RREQ to its neighbours. First, it divides its transmission range into four zones, as discussed earlier and shown here in Figure 5-5. Let us assume that node X compares the LLTs and REs of all its neighbours with the LLT_{avg} and RE_{avg} in Zone1. Assume that, based on the checks, nodes A, B and C are selected as the Potential Candidate Neighbours and are put in the PCL list. So, in this case, the PCL of node X in Zone1 = {A, B and C}. Next, node X selects the best node for forwarding the RREQ based on a comparison of the LLTs and REs within the PCL list. Let (LLT_C and RE_C) > (LLT_B and RE_B) > (LLT_A and RE_A);

then node X will select node C as its CN in Zone1. Similarly, CNs are selected in all the remaining three zones, following the procedure discussed above, and node X will attach the addresses of all the selected CNs in the respective zones to the RREQ packet. All the neighbours of node X in all the zones will, upon receiving the RREQ packet, check if their address is included in the address list. Only those nodes which find their addresses in the list will forward the RREQ to their neighbours, in accordance with the PNS procedure, while the others will simply drop it.

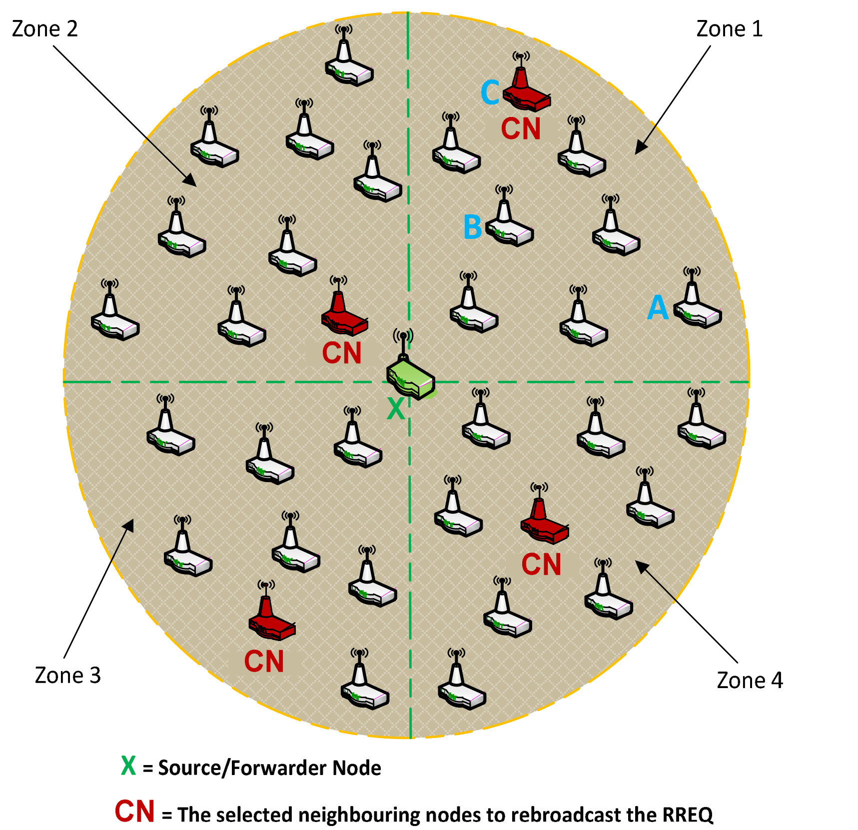

Figure 5-39: Instance of dividing the transmission range into four zones and selecting the CNs in each zone

To understand the concept presented so far for the PSN route discovery mechanism, consider Figure 5-6, which presents Zone1 only, for simplicity. The interactions of node 'S' with all its neighbours are shown in the specific zone. The links of the neighbouring nodes (A, B, C, D, E, G) with node 'S' are L_{S-A} , L_{S-B} , L_{S-D} , L_{S-E} , L_{S-G}, respectively. The LLT of each node is shown above the link, while the RE is shown below each individual node. It should be noted that each node knows the LLT and RE of each of its neighbours.

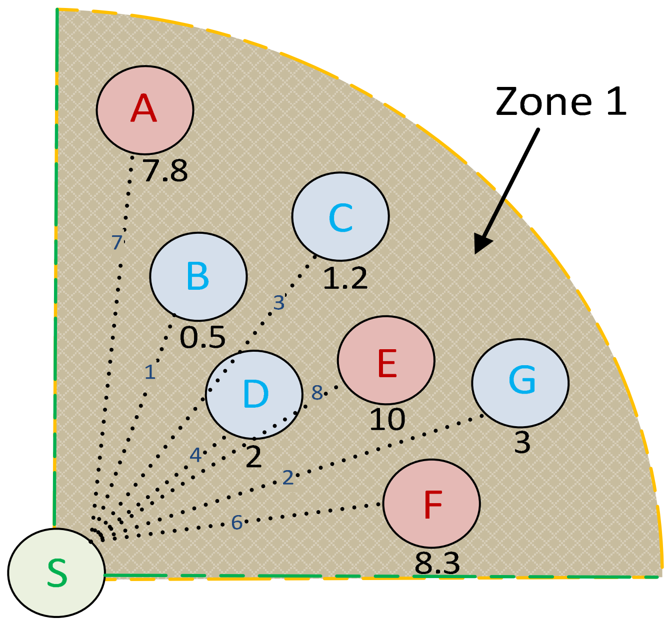

Figure 5-40: Instance of selecting the best CN from the PCL List in a specific zone

As has been discussed earlier, in Chapter-4, each node knows the LLTs and the REs of all its neighbour nodes through the exchanging of 'hello' messages. Similarly, in the proposed PSN protocol, the 'hello' message has been modified to convey the (x, y) coordinates and RE of the current node to all its neighbours. This frequent exchanging of 'hello' messages helps each node to gain fresh information about the link quality and residual energy of its neighbours. As shown in Figure 5-6, node 'S' intends to send a RREQ packet to its neighbours. After computing the LLT_{avg} (of all the neighbouring nodes), and similarly computing the RE_{avg}, node 'S' will compare these values with each node's LLT and RE values to find out which nodes have LLTs and REs above the LLT_{avg} and RE_{avg}. It is clear that only nodes A, E and F are eligible for inclusion in the Potential Candidates List (PCL) here.

The other nodes in Zone1, i.e., nodes B, C, D and G, are excluded from the PCL as their LLTs or REs or both are below the LLT_{avg} and RE_{avg}. Further, looking at Figure 5-6, among the

PCNs in the PCL, node E is the best candidate for selection as the CN. Therefore, based on its better LLT and RE, node E is selected as the CN. Node 'S' repeats this process for all the zones and one node in each zone is selected as the CN. In the final phase, node 'S' includes the addresses of all the CNs in the modified RREQ packet and broadcasts it. All the nodes in all the zones receive the same RREQ. Those who see their addresses in the address list rebroadcast the current RREQ following the method mentioned above. The rest of the neighbouring nodes just drop it.

Algorithm 1, as shown in Table 5-1, selects four CNs to forward the RREQ as follows. First, the whole area around node 'S' is divided into four separate zones represented by the set M = {M_1, M_2, M_3, M_4}. Each member of set M represents the set of nodes inside each zone, *i.e.,* $M_1 = \{n_{1-\mathrm{M1}}\ ,\ n_{2-\mathrm{M1}}\ , \ldots.\ , n_{|\mathrm{M1}|-\mathrm{M1}}\}$, $M_2=\{n_{1-\mathrm{M2}}\ ,\ n_{2-\mathrm{M2}}\ , \ldots.\ , n_{|\mathrm{M2}|-\mathrm{M2}}\}$, $M_3=\{n_{1-\mathrm{M3}}\ ,\ n_{2-\mathrm{M3}}\ , \ldots.\ , n_{|\mathrm{M3}|-\mathrm{M3}}\}$, $M_4=\{n_{1-\mathrm{M4}}\ ,\ n_{2-\mathrm{M4}}\ , \ldots.\ , n_{|\mathrm{M4}|-\mathrm{M4}}\}$. Next, it iterates through each node of the specific zone and selects the PCL set and hence the CN in that zone. Finally, node 'S' sends the RREQ packet to the selected Candidate Nodes.

Table 5-1: PSN algorithm

Algorithm 1

Input: Set of nodes N= {n_1, n_2, n_3, ….,$n_{|N|}$} $\in$ *the transmission range of sender* S.

Output: Selection of four CNs to transmit the RREQ.

// Divides the nodes in the transmission range of 'S' into four zones represented by M={M_1, M_2, M_3, M_4}, where each represents a set of nodes in their respective zones.

for i= 1 to |N|
  If $n[i]_x \geq S_x$ & $n[i]_y \geq S_y$
  $n[i] \in M_1$
  else if $n[i]_x < S_x$ & $n[i]_y \geq S_y$
  $n[i] \in M_2$
  else if $n[i]_x \leq S_x$ & $n[i]_y > S_y$
  $n[i] \in M_3$
  else if $n[i]_x \leq S_x$ & $n[i]_y < S_y$
  $n[i] \in M_4$

end if

next i

// Selects the PCL and the four CNs from the PCL in each zone $M_n \in \mathrm{M}$.

for j= 1 to 4

for k= 1 to $|M_j|$

//Node ‘S’ selects the PCL and CN in Zone M_j

if ($LLT_k \geq LLT_{Avg}$) and ($RE_k \geq RE_{Avg}$)

$PCL\_M_j = PCL\_M_j \cup \{n_{k\text{-}Mj}\}$

else

next k

end if

Select CN in the PCL M_j based on the maximum RE and LLT in the set PCL_M_j .

next j

5.4.2 Percentage of RREQ Reception by Neighbor Nodes

As discussed previously, in Section 5.2, the rebroadcasting of RREQs can only offer 61% more coverage area across the whole network [7]. PSN offers further improvement and enhancement with an additional algorithm that causes CNs to make further checks for optimized RREQ dissemination. For instance, when any sender/forwarder node ‘S’ chooses to run Algorithm 1, as shown in Table 5-1, the result is that it selects four CNs from among its neighbours. Further, node ‘S’ attaches the selected CNs’ addresses to the RREQ packet and broadcasts it. Only the attached CNs are allowed to further process the received RREQ, when they find their addresses inside the modified field (address list) of the RREQ. All CNs have to check how many of their neighbours have received the same RREQ by checking the distance between each of its own neighbours and the sender, ‘S’. if the distance is less than the transmission range of ‘S’, then the CN will assume that this neighbour has already received the same RREQ as itself. This way, any CN can get the percentage of how many neighbours have received the same RREQ. Through extensive simulation, we have found that the percentage that improves the network’s performance is 75%.This indicates that if more than 75% of the CN’s neighbours have already received the same RREQ, the CN should not rebroadcast the received RREQ as most of its neighbours have received it and there is no need for rebroadcasting. If less than 75% of the CN's neighbours have received the same RREQ, the CN will rebroadcast it. Figure 5-7 shows the relationship with the overhead added into the network when CNs have a predefined percentage for rebroadcasting received RREQs.

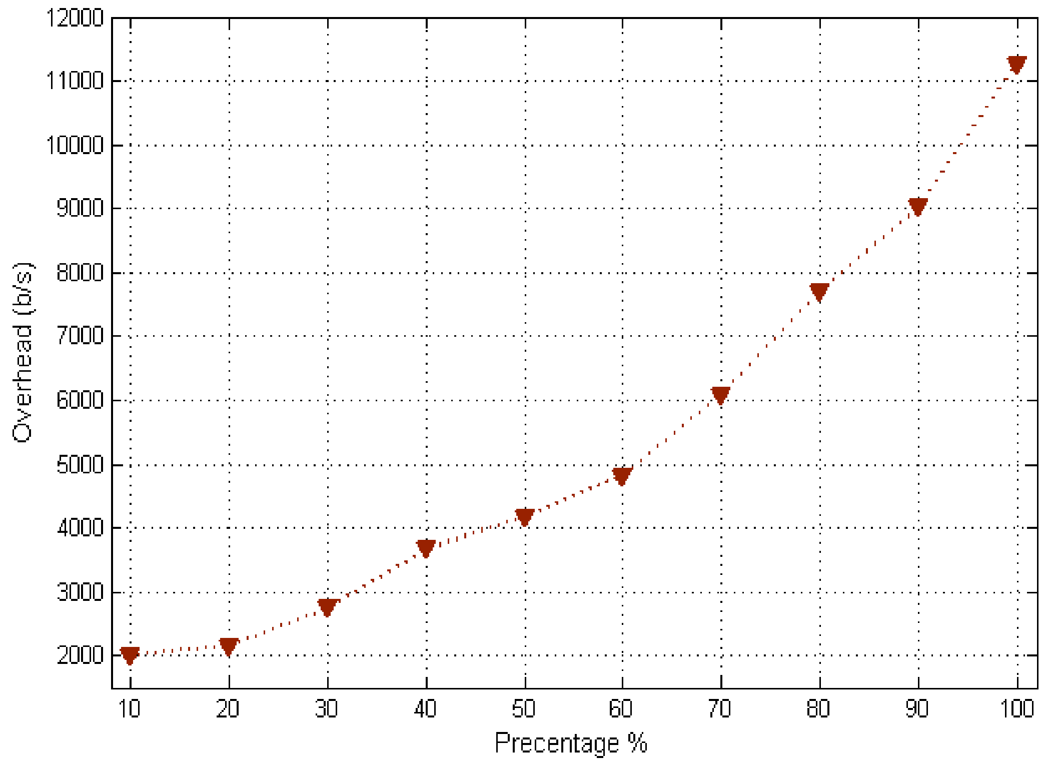

Figure 5-41: CN rebroadcasting effect

The results presented in Figure 5-7 show that when the percentage is low, the relevant overhead is low and vice versa. This essentially means that when fewer CN neighbours receive the same RREQ, the CN node rebroadcasts the received RREQ and more overhead is therefore added to the network. Bear in mind the fact that if the percentage is set to a low degree most of the CNs will not rebroadcast the RREQ, which reduces the chances of finding the intended destination because few nodes will receive the RREQ. Hence, a balance between the overhead added into the network and reachability (disseminating a minimum number of RREQs to find the intended destination) is struck by setting the percentage at 75%.

5.5 PSN Performance Evaluation and Results Analysis

5.5.1 Network Simulator (NS2)

The PSN protocol was implemented in the NS2 modeller [23], version 2.34. Ns2 is one of the most widely used discrete event network simulator tools when simulating real network scenarios. NS2 is freely available and was originally designed to simulate wired networks. However, it has been extended to simulate wireless networks including wireless sensor networks, wireless LANs and MANETs. In addition, NS2 is organized according to the OSI reference model [24]. Recent research [25] shows that 57% of all published simulation-based papers have used NS2 as a simulation tool, which provides evidence that NS2 is a powerful and trusted network simulator.

5.5.2 Simulation Environment and Parameters

The proposed PSN protocol has been thoroughly analysed by comparing it with our previous proposed schemes, *i.e.* C-CNRR and A-LSEA. The benchmark selection was based on C-CNRR and A-LSEA showing comparatively better performance than F-CNRR and F-LSEA, respectively. Section 5.5.4 discusses the results obtained from the comparison of AODV, C-CNRR, A-LSEA and PSN using the parameters provided in Table 5-2. Random Way Point has been used to simulate the mobile nodes, whereby each node moves randomly at a consistent speed [5 – 30 m/s], as shown in Table 5-2. When any node reaches a certain random destination, it pauses for only 2 seconds and then starts moving again to another random destination.

Table 5-1: Simulation Parameters for Comparing AODV, C-CNRR, A-LSEA and PSN

Simulation Area	**600 x 600 M^2**
Nodes number	100
Data rate	2 Mbps

Transmission Range	250 m
Mac protocol	802.11
Traffic Type	CBR
Packet size	1000 bits
Traffic	5 packets/sec
Simulation time	600 sec
Speed	[5 m/s - 30 m/s]

5.5.3 Performance Metrics

The following metrics were used to evaluate the proposed protocols:

- ***Packet Delivery Ratio*****:** the ratio of those data packets successfully delivered at destination nodes to those generated by source nodes.
- ***Total Overhead:*** the number of control packets transmitted in the network that include the RREQ, RREP, Rerr and hello messages.
- ***Network Life Time:*** the aggregate time before all nodes dies due to battery exhaustion.
- ***Total Data Sent:*** the total amount of data sent in the network before nodes are unable to participate in the network due to battery exhaustion.
- ***Total Data Received:*** the total amount of data received in the network before the nodes are unable to receive data due to battery exhaustion.
- ***Total Data Dropped:*** the total amount of data dropped in the network due to error detection, collision, queue lengths*etc*.
- ***Sent and Received RREQ:*** the total number of sent and received RREQ packets in the network.
- ***Average Throughput:*** the total number of application layer data bits successfully transmitted in the network per second.

5.5.4 Results and Discussion for the First Simulation

This sub-section analyses the obtained results and presents a comparative discussion.

5.5.4.1 Total Overhead

As shown in Figure 5-8, we compared the total overhead of the proposed schemes with those of AODV, C-CNRR and A-LSEA. The figure shows that the overhead increases strongly with increases in mobility in the case of AODV. However, this increase is very steady for the proposed schemes, *i.e.* C-CNRR, A-LSEA and PSN. This is because the AODV protocol floods any received RREQs without any constraints (*i.e.* Link Quality and Energy Level). Comparing the other three schemes, PSN outperforms A-LSEA and C-CNRR. The reason for this is that PSN considers the LLT_{AVG} and RE_{AVG} and selects a particular set of nodes (CNs) to rebroadcast a RREQ. Furthermore, the PSN routing protocol reduces the overhead to a minimum by forcing the CNs to check how many of their own neighbours have received the same RREQ before sending it. In contrast, C-CNRR considers only the distance, while A-LSEA considers both constraints but without a zoning concept or a further check of how many neighbours have received the same RREQ.

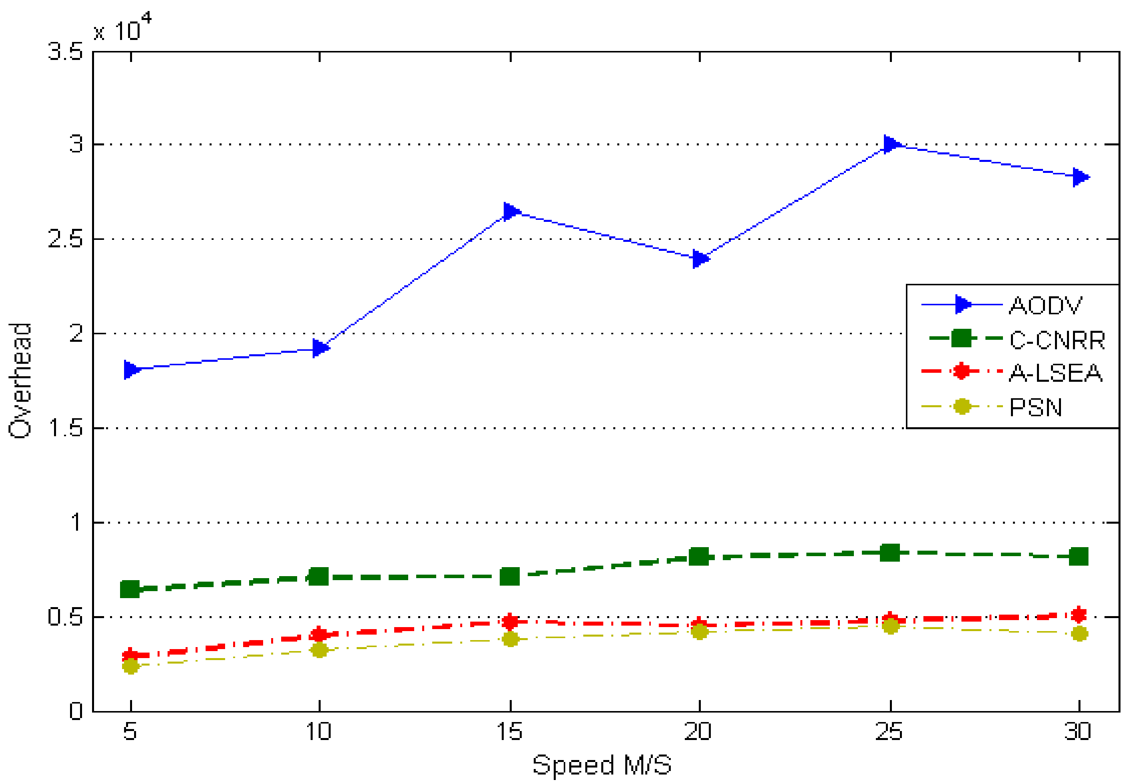

Figure 5-42: Overhead vs. Speed

5.5.4.2 Sent and Received RREQs

Figure 5-9 shows the number of RREQs sent and received in the entire network. In general, a node sends a broadcast RREQ and then all its neighbours receive it. There is a correlation between the number of sent and received RREQs (sending a lot, receiving a lot and vice versa). PSN outperforms all the other protocols because the proposed algorithm selects CNs not only based on link quality and energy levels but also in terms of what percentage of a node's neighbours have received an RREQ. When a certain percentage of node 'S' neighbours have received an RREQ, the RREQ is not flooded in the network. This gives more control over RREQ dissemination across the entire network. A-LSEA performs better than C-CNRR because A-LSEA's path selection is more stable (as it considers the RE and LLT) than C-CNRR's (which considers only the distances between nodes).

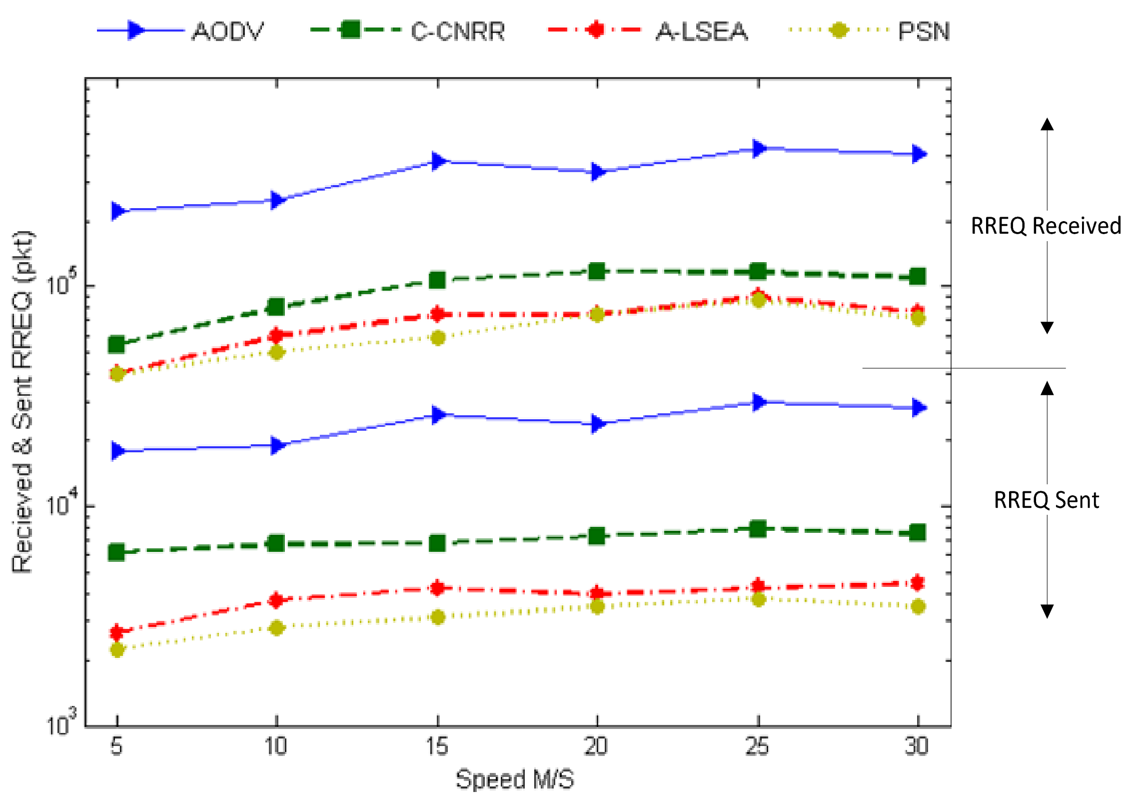

Figure 5-43: Received and Sent RREQs vs. Speed

5.5.4.3 Average Throughput

Figure 5-10 demonstrates the average throughput for the PSN routing protocol as compared to the other routing protocols (AODV, C-CNRR and A-LSEA). It shows that, generally, throughput decreases with increases in the mobility of the nodes for all the protocols under analysis. Furthermore, PSN performs better than the other protocols in most cases because the paths selected by PSN last for longer than those selected by the other protocols. This gives PSN an edge over the other protocols (AODV, C-CNRR and A-LSEA) as it is able to send more data due to better path lifetimes.

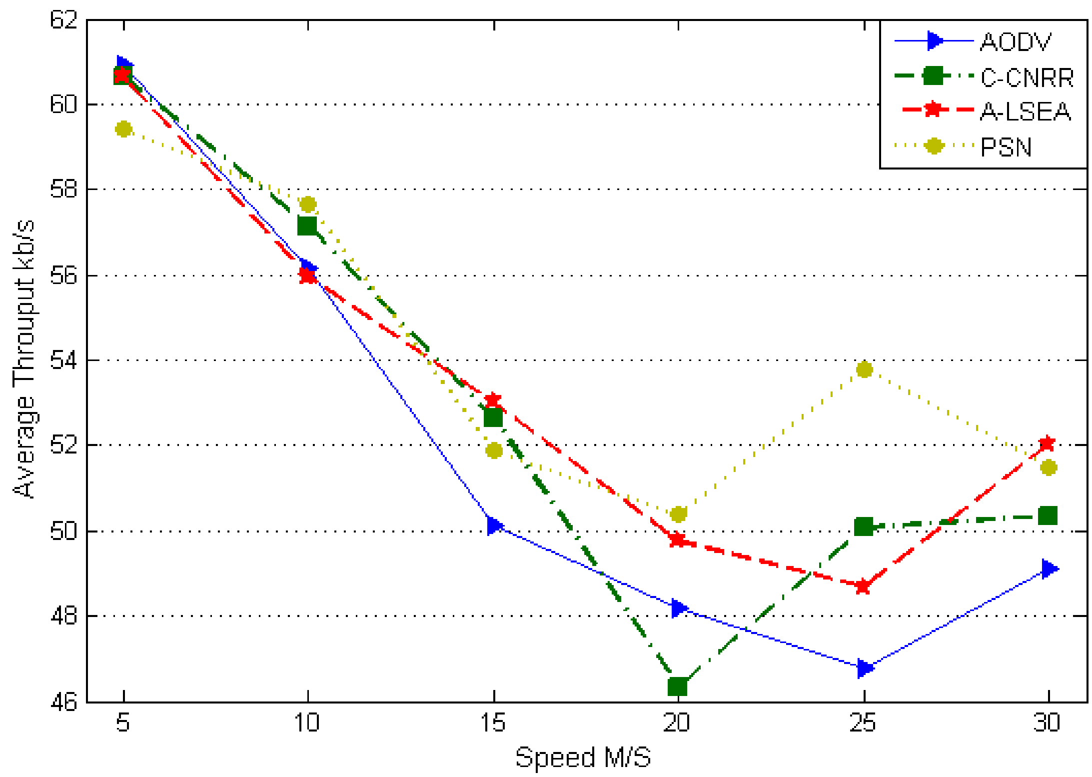

Figure 5-44: Throughput vs. Speed

5.5.4.4 Data Sent

Figure 5-11 illustrates the amount of the data that was successfully sent during the simulation. In MANETs, node power supplies are not permanent due to their mobile nature; therefore, any data transmitted to or received by the node will reduce energy levels. In

Figure 5-9, we saw that AODV was the worst protocol in terms of sending and receiving RREQs. A high number of unnecessarily received and sent RREQs dramatically reduces the battery life of the nodes. The extra energy that nodes spend on sending and receiving RREQs could instead be used for actual data sending and reception. PSN has proven to be a better protocol than the other routing protocols because it sends fewer RREQs while, at the same time, successfully sending more data.

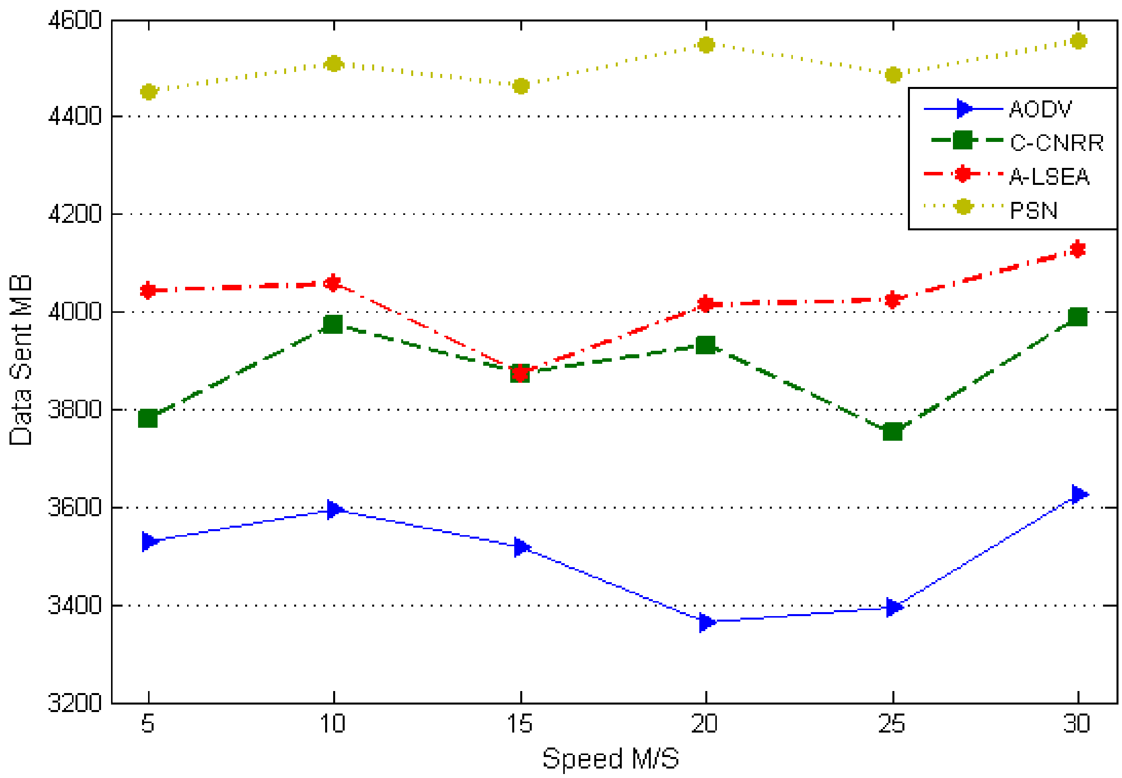

Figure 5-45: Data Sent vs. Speed

5.5.4.5 Data Received

Figure 5-12 shows the data received for PSN and other routing protocols (AODV, C-CNRR and A-LSEA). For AODV, C-CNRR and A-LSEA, the figure shows that the amount of data received decreases when mobility increases. This affects the established routes and links, which need to be re-established whenever breakages occur. However, in the PSN routing protocol, the amount of received data decreases when the speed increases from 5 m/s to 15 m/s but stays at approximately the same level above 15 m/s. This is because the links established by the PSN algorithm estimate Link Lifetimes and Residual Energy, easing the impact of high speeds by involving only those nodes that have been selected through the developed algorithm (selecting the best node in each zone) in the end-to-end path.

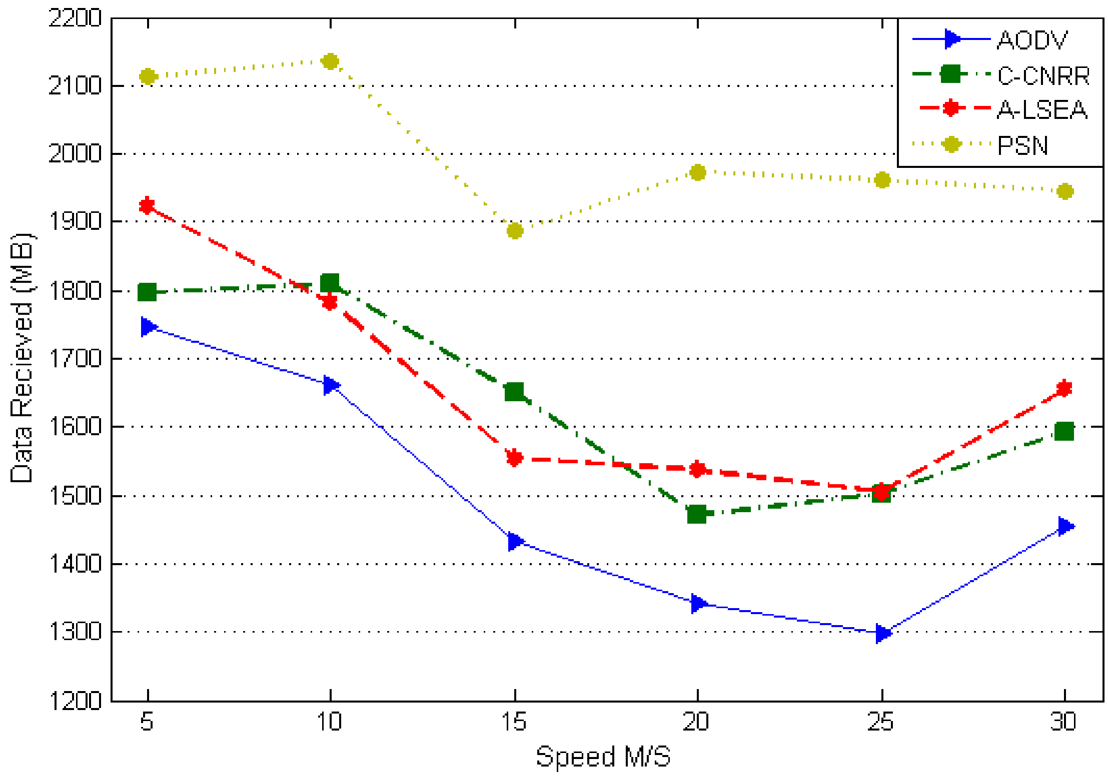

Figure 5-46: Data Received vs. Speed

5.5.4.6 Network Lifetime

Figure 5-13 illustrates the Network Lifetime results for AODV, C-CNRR, A-LSEA and proposed PSN. The figure shows that PSN outperforms all the other routing protocols, giving better Network Lifetime results. This is because the PSN routing protocol selects only four nodes to rebroadcast received RREQs. Further, the selected CN nodes run an advanced algorithm to eliminate RREQ redundancy by checking how many of their neighbours have received the same one. Based on that calculation, CN nodes will decide to rebroadcast or discard received RREQs. Saving energy by not sending and receiving unnecessarily will conserve node energy and lead to network lifetime increases.

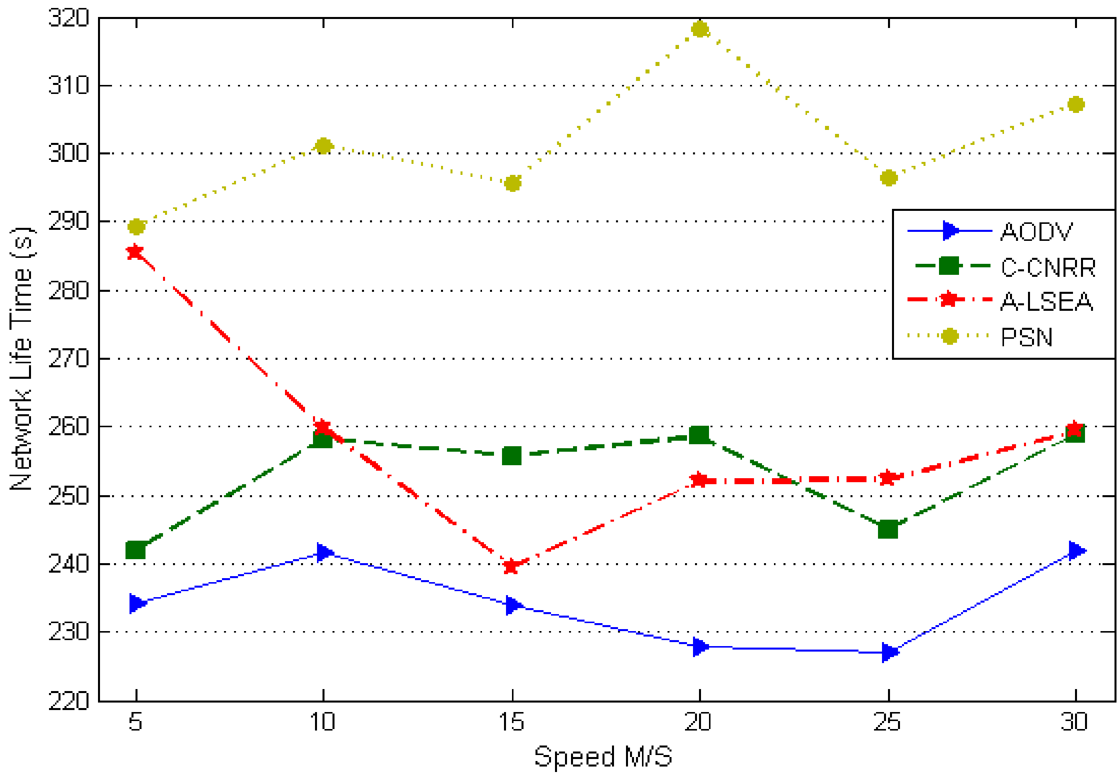

Figure 5-47: Network Life Time vs. Speed

5.5.4.7 Data Drop

Figure 5-14 shows the amount of data dropping (in packets) during the simulation for the AODV, C-CNRR, A-LSEA and proposed PSN protocols. The PSN routing protocol prevailed over all other routing protocols in all the previous performance metrics. However, Figure 5-14 shows that C-CNRR outperforms all the other routing protocols in terms of data dropping. Although PSN selects better paths than the other routing protocols, this does not give it the advantage of performing better in term of dropped data packets in the network, as shown in the figure. After deeply analysing the reason for the observed result, it is concluded that C-CNRR's selection of an end-to-end path based on the distance between the nodes involved in the route gives it an advantage. This is because the strength of the signal on which the data are sent and received is stronger, due to the smaller distances involved, than in the other routing protocols.

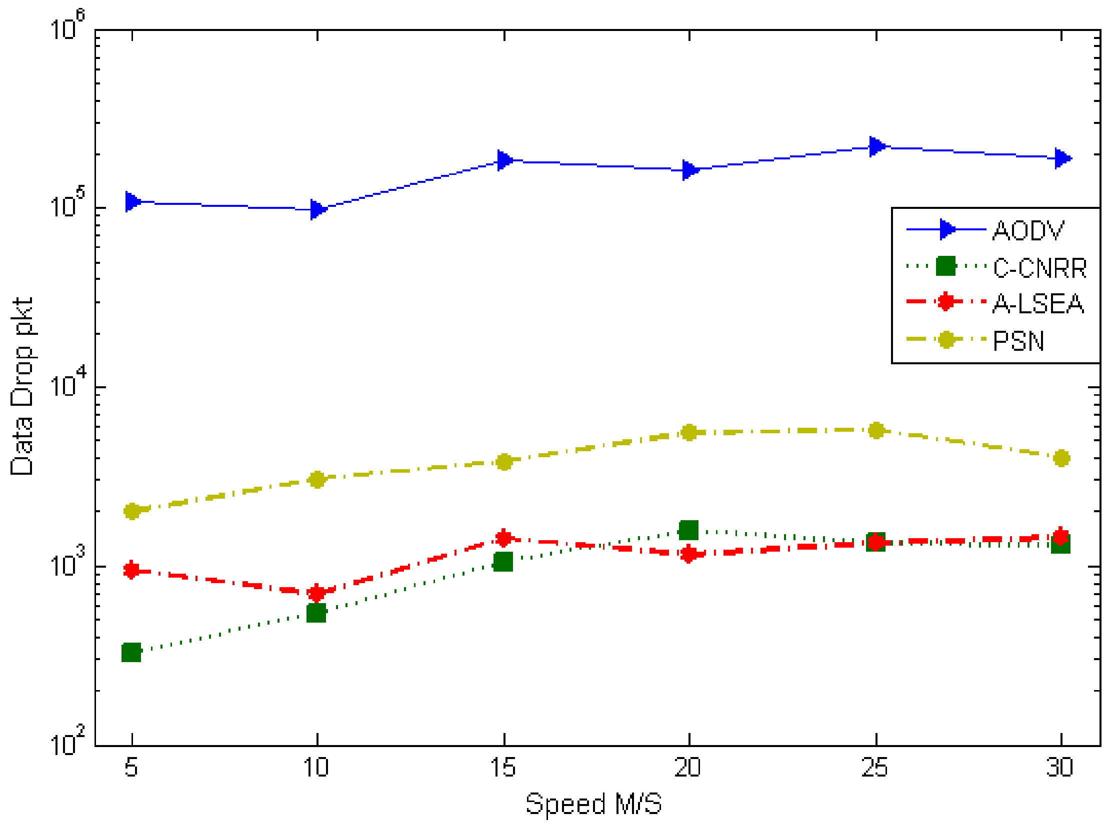

Figure 5-48: Data Drop vs. Speed

5.5.5 Results and Discussion for the Second Simulation

Mobility-Aware AODV [20] was implemented in NS2 for further verification and validation, and to compare it with the proposed Position-based Selective Neighbour (PSN) approach. In Section 5.5.4, PSN was seen to achieve a better performance as compared to our previously introduced routing protocols (C-CNRR and A-LSEA) and the standard AODV. For this reason, PSN is considered the best routing protocol proposed in this thesis, and it has thus been selected for comparison with the work proposed in [20] and AODV. All the schemes have been compared using the same simulation parameters, as shown in Table 5-3.

Table 5-1: Simulation Parameters for comparing AODV, MA-AODV and PSN

Simulation Area	**700 x 700 M^2**
Nodes number	100
Data rate	2 Mbps

Transmission Range	250 m
Mac protocol	802.11
Traffic Type	CBR
Trafic Number	15 flows
Packet size	1000 bits
Traffic	5 packets/sec
Simulation time	700 sec
Pause Time	[2 s – 12 s]

Figures 5-15 to 5-21 show the comparisons between AODV, MA-AODV and PSN for different metrics, as explained in Section 5.5.3.

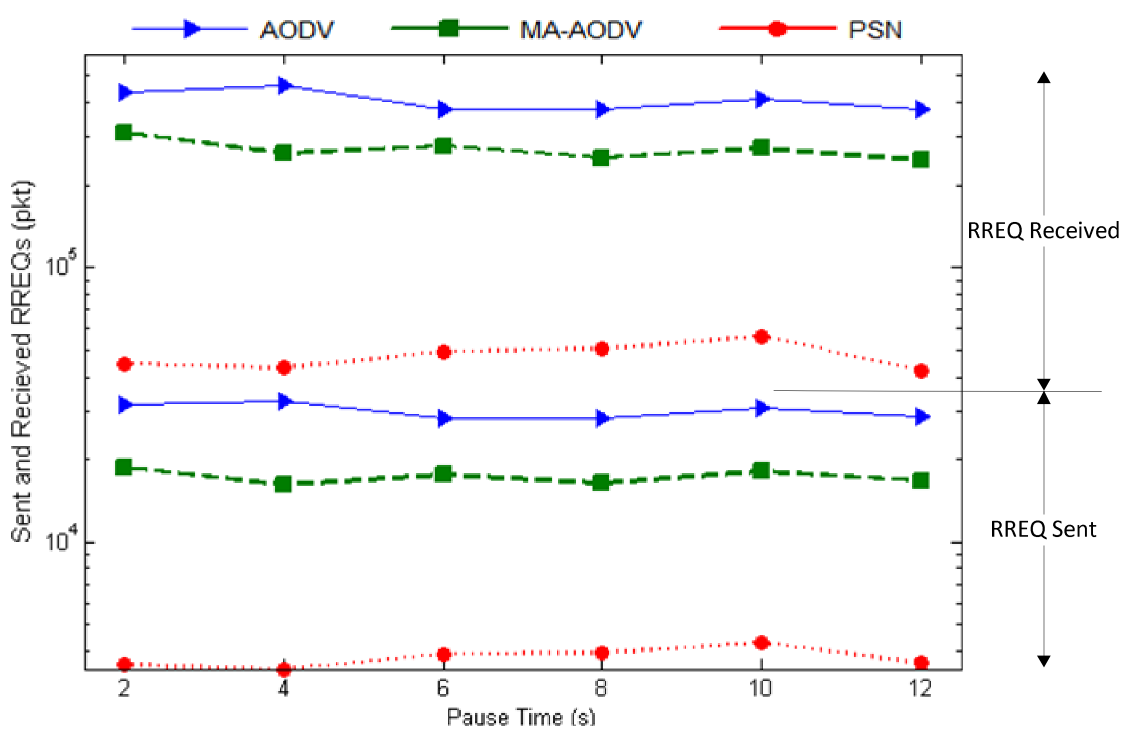

Figure 5-49: Sent and Received RREQs vs. Pause Time

As can be seen from Figure 5-15, the PSN routing protocol sent and received fewer RREQ packets in the network. This is because PSN selects end-to-end routes based on the LLT and RE factors, while the MA-AODV selects routes based only on node speeds. These two factors give PSN an edge over MA-AODV because the route selected by PSN will last longer than that selected by MA-AODV. In addition, the routes selected by MA-AODV will last for shorter times in most cases and the nodes then have to establish a new path by initiating a new RREQ discovery process. This leads to more RREQs being sent and received and more overhead in total, as shown in Figure 5-16.

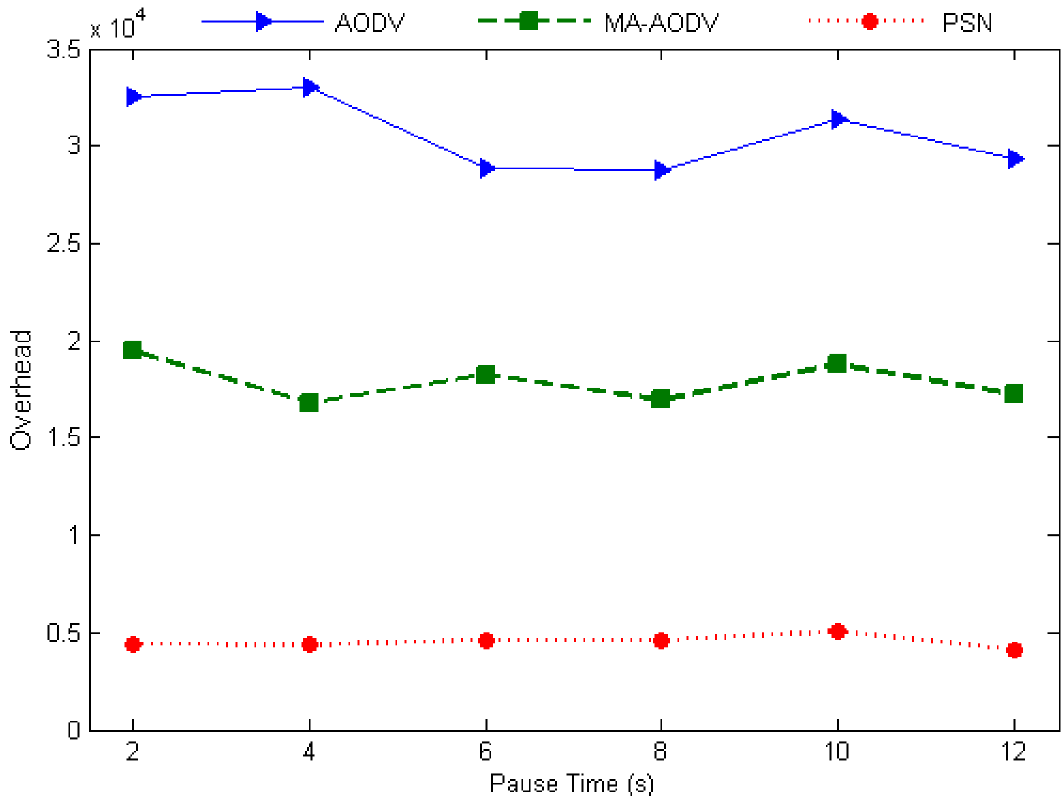

Figure 5-50: Average Overhead vs. Pause Time

Figure 5-17 illustrates the average Delivery Ratio for the PSN, MA-AODV and AODV routing protocols. As is clear from the results shown in Figure 5-17, all routing protocol delivery ratios increase when the pause time increases due to stillness in the mobile nodes. Furthermore, the PSN routing protocol performs better than the MA-AODV and AODV routing protocols. This is because PSN selects paths which last longer than those selected by MA-AODV as the PSN's selected end-to-end paths are based on the Link Lifeitmes (LLT) and Residual Energy (RE) of the nodes involved in the route. On the other hand, MA-AODV forwards RREQs based on node speeds. Thus, the MA-AODV algorithm results in end-to-end routes that all have low-speed nodes along the path. This approach, however, does not guarantee better paths as far as the MANETs are concerned for two obvious reasons, as follows. First, there might be two nodes with low speeds but moving in opposite directions.

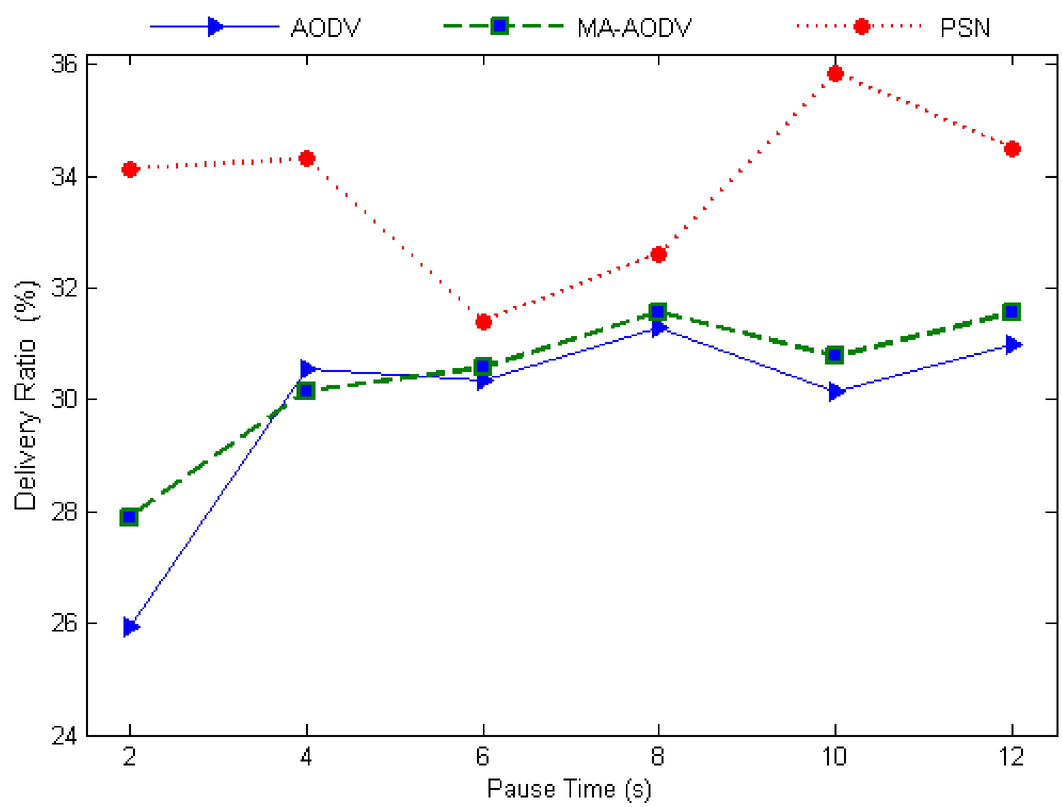

Figure 5-51: Delivery Ratio vs. Pause Time

This essentially means that the link lifetime for these two nodes will break due to their moving apart. Furthermore, imagine two neighbouring nodes moving at high speed in the same direction; here, the link lifetime between these two nodes will stay valid for longer than between the two low-speed nodes moving in opposite directions. MA-AODV only considers the speed of the node as a condition for forwarding a received RREQ, while PSN considers both speed and direction and calculates the link lifetimes of any two neighbour nodes. Secondly, PSN provides a stronger Packet Delivery Ratio because of the way it considers the nodes' Residual Energies during the route selection decision.

Furthermore, as can be seen in Figure 5-18, the proposed PSN successfully runs the network longer than MA-AODV routing protocol for two reasons. Firstly, PSN considers the Residual Energies and the Link Lifetimes of the nodes involved in end-to-end routes that return stable paths. Secondly, discontinuing the sending/receiving of unnecessary RREQ packets that consume non-negligible amounts of the node energy conserves energy.

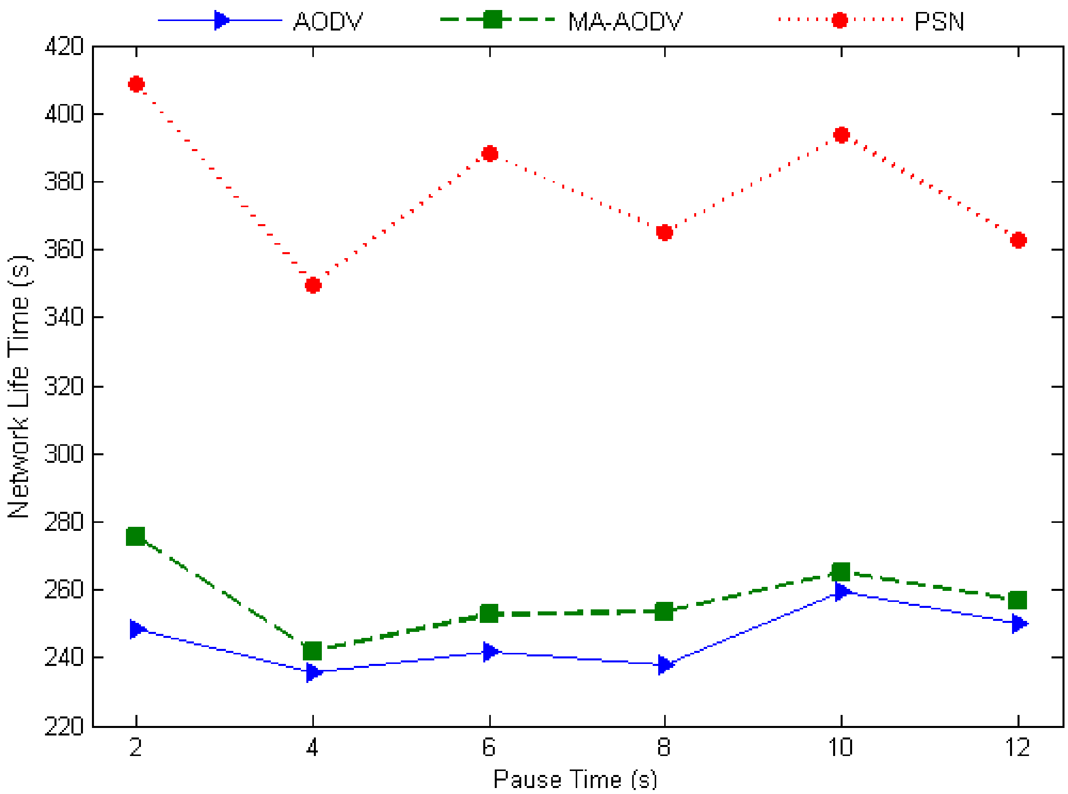

Figure 5-52: Network Life Time vs. Pause Time

Also, MA-AODV considers only the speed of the nodes and this is not an accurate parameter for selecting stable paths. Running a network for a long time gives the nodes the ability to send and receive more data, as shown in the next Figure 5-19; thus, PSN outperforms MA-AODV by sending and receiving more data packets.

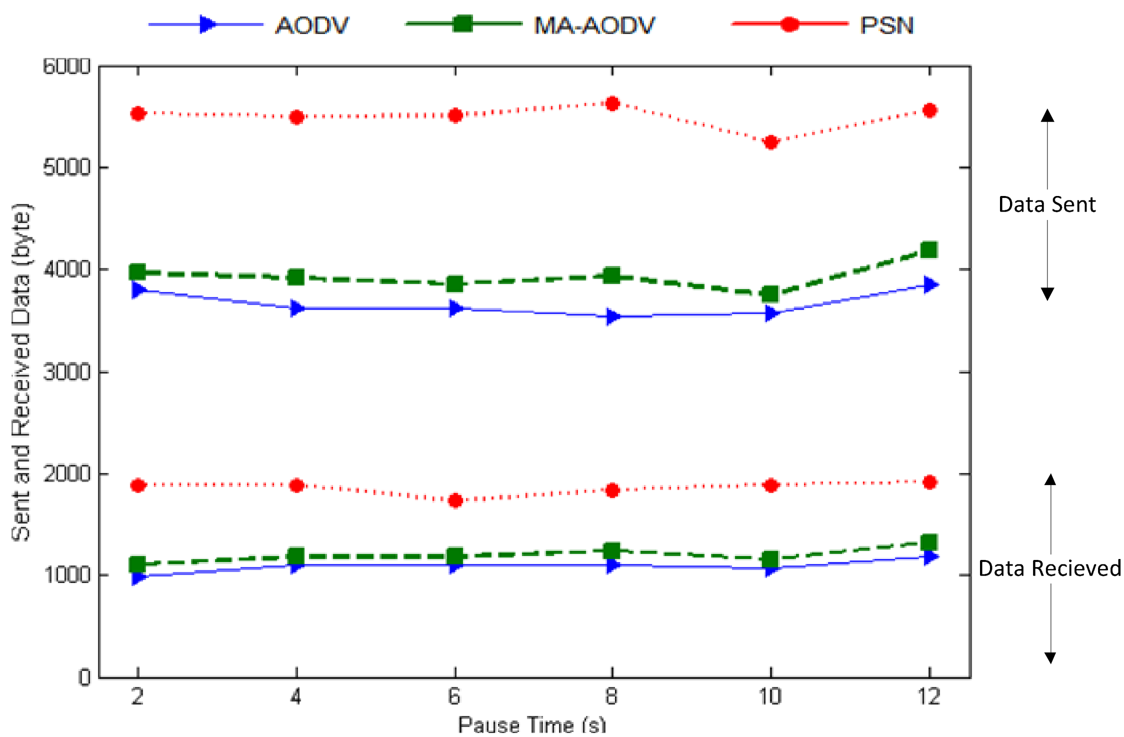

Figure 5-53: Sent and Received RREQs vs. Pause Time

Figure 5-20 shows a throughput comparison of the PSN, MA-AODV and AODV routing protocols. It is obvious from the figure that PSN outperforms MA-AODV in most cases due to the improved algorithm applied in the PSN routing protocol, which returns better and more stable end-to-end paths.

It is also noticeable that the general curve of the throughput rate has an incremental shape as the pause times increases, despite some fluctuations that are due to the randomness of the nodes' mobility. In theory, the throughput rate for a scenario with a4-second pause time should be higher than for a scenario with a 6-second pause time, given that the trajectories travelled by the nodes during the simulation are identical. However, under the Random Waypoint mobility model, the positions to which the nodes move are randomly selected and differ from one scenario to another.

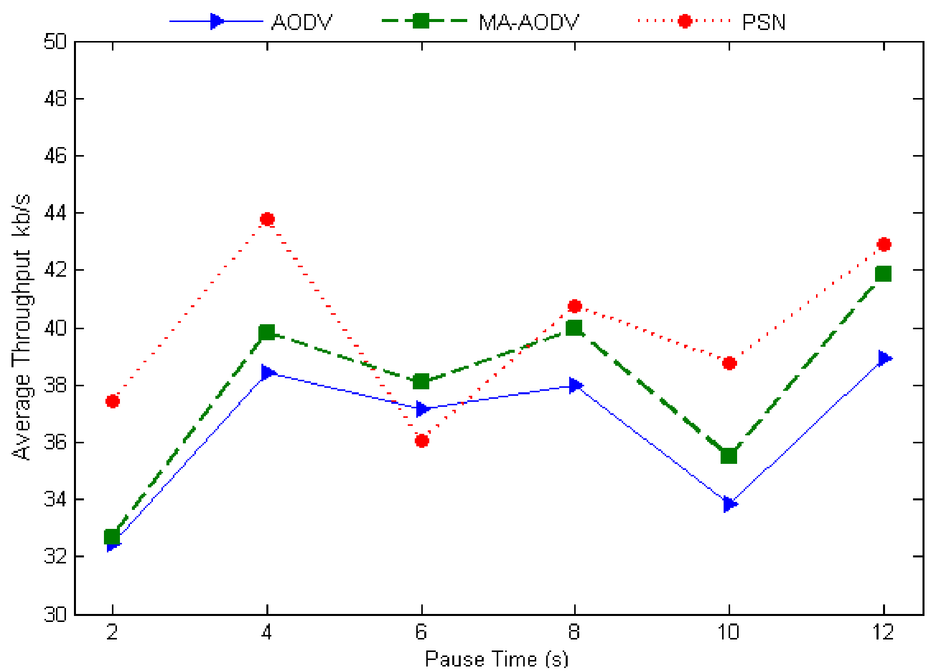

Figure 5-54: Average Throughput vs. Pause Time

Last but not least, PSN has outperformed the MA-AODV routing protocol with regard to data drop packets, as shown in Figure 5-21. This is due to the abovementioned reasons.

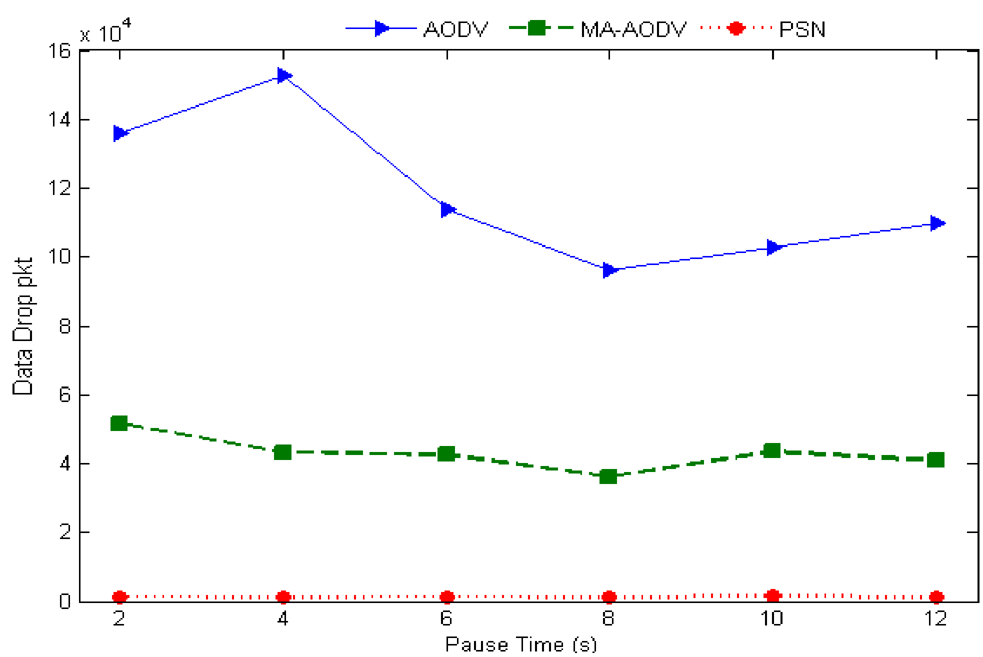

Figure 5-55: Data Drop vs. Pause Time

5.6 Conclusion

This chapter has presented the Position-based Selective Neighbours (PSN) protocol. The proposed routing protocol aims to control RREQ propagation in the network, resulting in the selection of better end-to-end paths with regard to Link Lifetimes (LLT) and Residual Energy (RE). PSN gains advantages from combining these two important factors. In addition, merging the LSEA and CNRR concepts further reduces the dissemination of RREQs into a network without causing loss of reachability among the nodes, increasing the network life time, reducing the overhead and improves the amount of data sent and received. The proposed mechanism combines the advantages of zoning and link stability by selecting the four candidates nodes based on their RE and LLT (with the source/forwarder).

Upon RREQ message reception, the node first checks the CNRR field for inclusion of its address. Upon finding its address in the CNNR field, a node will understand its inclusion in the sender's candidacy list and should rebroadcast the RREQ. For greater enhancements, we apply the Sender/Receiver approaches; the sender will select four nodes as candidates to rebroadcast the RREQ and the receiver node checks the reception of the same RREQ by its neighbours. Based on this calculation the node will make a decision to forward the RREQ or discard it. The results show that the proposed technique improves the delivery ratio by 24.6% to 18.8%, as compared to the AODV and MA-AODV, respectively.

The proposed routing protocol gives advantages over previously introduced routing protocols by reducing unnecessary RREQs and hence their dissemination in the global network. This provides increased network lifetimes, obtains better throughput, and enables more data to be sent and received. The proposed scheme combines both the Link Lifetime (LLT) and Residual Energy (RE) factors in the routing management process, rather than using only a single factor, such as in the studies of [20, 26].

5.7 References

[1] Perkins, C.E. and Bhagwat, P. "Highly Dynamic Destination-Sequenced distance-vector routing (DSDV) for mobile computers", ACMSIGCOMM Computer Communication Review, vol. 24, no. 4, pp. 234-244, 1994.

[2] Qayyum, A., Jacquet, P. and Muhlethaler, P. "Optimized Link State Routing Protocol (OLSR)", 2003.

[3] Ogier, R., Templin, F. and Lewis, M. (2004) Topology dissemination based on reverse-path forwarding (TBRPF), 2004.

[4] Das, S., Perkins, C. and Royer, E. "Ad hoc on demand distance vector (AODV) routing", Mobile Ad-hoc Network (MANET) Working Group, IETF, 2002 .

[5] Johnson, D.B., Maltz, D.A. and Broch, J. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks", Ad hoc networking, vol. 5, pp. 139-172, 2001.

[6] Z. J. Haas, M. R. Pearlman, and P. Samar, "The Zone Routing Protocol (ZRP) for ad hoc networks," IETF Internet Draft, draft-ietf-manet-zonezrp-04.txt., July 2002.

[7] Tseng, Y.C., Ni, S.Y., Chen, Y.S. and Sheu, J.P. "The broadcast storm problem in a mobile ad hoc network", Wireless networks, vol. 8, no. 2, pp. 153-167, 2002.

[8] Abdulai, J., Ould-Khaoua, M. and Mackenzie, L. "Improving probabilistic route discovery in mobile ad hoc networks", Local Computer Networks,. 32nd IEEE Conference, pp. 739, 2007.

[9] Y.-C. Tseng, S.-Y.Ni, and E.-Y. Shih, "Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc networks," Proceedings of IEEE Transactions on Computers, vol. 52, pp. 545--557, May 2003.

[10] B. Williams and T. Camp, "Comparison of broadcasting techniques for mobile ad hoc networks," Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, MOBIHOC, pp. 194 - 205, June 2002.

[11] Le, T.D. and Choo, H. "Efficient flooding scheme based on 2-hop backward information in ad hoc networks", IEEE ICC'08 International Conference on Communications, pp. 2443, 2008.

[12] Yang, S.R., Chiu, C.W. and Yen, W.T. "A novel convex hull-based flooding scheme using 1-hop neighbour information for mobile ad hoc networks", Wireless Networks, vol. 17, no. 7, pp. 1715-1729, 2011.

[13] Liu, H., Wan, P., Jia, X., Liu, X. and Yao, F. "Efficient flooding scheme based on 1-hop information in mobile ad hoc networks", Proc. IEEE INFOCOM, 2006.

[14] Lee, S.H. and Ko, Y.B. "An Efficient Neighbor Knowledge Based Broadcasting for Mobile Ad Hoc Networks", Computational Science–ICCS, pp. 1097-1100, 2006.

[15] Abolhasan, M. and Wysocki, T. "GPS-based route discovery algorithms for on-demand routing protocols in MANETs", Wireless On-Demand Network Systems, pp. 144-157, 2004.

[16] Hamad, S., Noureddine, H., Radhi, N., Shah, I. and Al-Raweshidy, H. "Efficient flooding based on node position for mobile ad hoc network", IEEE Innovations in Information Technology (IIT), pp. 162, 2011.

[17] Yassein, M.B., Khaoua, M.O., Mackenzie, L. and Papanastasiou, S. "Improving the performance of probabilistic flooding in manets", In Proc. of International Workshop on Wireless Ad-hoc Networks (IWWAN), 2005.

[18] Nourazar, F. and Sabaei, M. "DAPF: An Efficient Flooding Algorithm for Mobile Ad-hoc Networks", 2009 International Conference on Signal Processing Systems IEEE, pp. 594, 2009.

[19] Kim J, Zhang Q, Agrawal DP. In: Probabilistic broadcasting based on coverage area and neighbor confirmation in mobile ad hoc networks. Global telecommunications conference workshops, GlobeCom workshops, p. 96-101, 2004.

[20] Khamayseh Y, Darwish OM, Wedian SA. “Ma-aodv: Mobility aware routing protocols for mobile ad hoc networks”, IEEE ICSNC'09 fourth international conference on Systems and networks communications, p. 25-29, 2009.

[21] Hamad S, Noureddine H, Al-Raweshidy H. In: Link stability and energy aware for reactive routing protocol in mobile ad hoc network. Proceedings of the 9th ACM international symposium on mobility management and wireless access; ACM; p. 195-8, 2011.

[22] Kaplan, E.D. and Hegarty, C.J. Understanding GPS: principles and applications, Artech House PublishersK, ISBN 1-58053-894-0, 2006.

[23] "The Network Simulator Ns-2-the VINT pro,"http://www.isi.edu/nsnam/ns/ns-build.html; Retrieved in July 2012.

[24] Lewan, D. and Long, H. "The OSI file service", Proceedings of the IEEE, vol. 71, no. 12, pp. 1414-1419, 1983.

[25] Gast, M. 802.11 wireless networks: the definitive guide, O'Reilly Media, ISBN 0-596-10052-3, 2005.

[26] Xie, F., Du, L., Bai, Y. and Chen, L. "Energy aware reliable routing protocol for mobile ad hoc networks", IEEE Wireless Communications and Networking Conference WCNC, pp. 4313, 2007.

CHAPTER 6

Conclusions and Future Work

This chapter summarises the major contributions of this thesis and presents the main conclusions. The future work section highlights those research areas where the findings of this research could be further investigated in new research directions.

6.1 Conclusion

The most important feature of MANETs is the mobility support that allows mobile nodes to move freely within a network's geographical area. The nodes' movements have varying speeds and patterns and these can cause link and route disconnections. In turn, this can significantly degrade an employed routing protocol's performance. In addition, mobile nodes in MANETs suffer from limited power supplies and any receiving or transmitting of data affects their battery levels. Therefore, mobile nodes must conserve their batteries for necessary communications and should not waste them on duplicate processes such as flooding in the network.

The aim of this thesis was to resolve some of the issues found in Mobile Wireless Ad-hoc Networks, especially in on-demand routing protocols such as AODV and DSR that find end-to-end routes between network nodes to enable communication. This work introduced three new route discovery techniques that improve the overall level of overhead and offer a better experience during communication with regard to Network Lifetime, Throughput, Data Drop and Delivery Ratio.

The three techniques are summarised in the following sections.

6.1.1 Candidate Neighbours to Rebroadcast the RREQ Protocol

The Candidate Neighbours to Rebroadcast the RREQ (CNRR) approach was proposed as a way to reduce the overhead in MANETs. The CNRR routing protocol utilizes the nodes' location information to select four neighbour nodes for rebroadcasting received RREQ messages when there is no information in the routing table for the intended destination in the RREQ packet. CNRR applies a source routing strategy in which the source node selects four neighbours based on their distances. This source strategy has rarely been used in geographical routing protocols to improve the route discovery phase. Two versions of CNRR were introduced and labelled:

- Further Candidate Neighbours to Rebroadcast the RREQ (F-CNRR).
- Closest Neighbours to Rebroadcast the RREQ (C-CNRR).

In order to implement these two versions, we selected the AODV routing protocol for modification. The standard AODV 'hello' message was modified in both versions of the above-mentioned protocols to enable the (x, y) coordinates of each node to be carried/shared. Furthermore, the RREQ message was modified with the addition of a *cnrr* field to carry the four candidate nodes' addresses. In addition, the proposed work made two assumptions. The first was that the node could get its position using specific technology such as a Geographical Positioning System (GPS). The second was that the network should be deployed in such a way that there were no obstacles to GPS reception and therefore to network performance (Outdoor Network).

In F-CNRR, the selection of the four candidate nodes was based on the distances between the sender and its neighbours, *i.e.* the furthest nodes from the source were selected as long as the distance did not exceed the 80% transmission range threshold of the source/forwarder node. The 80% threshold was important as the signal becomes very weak after this point and it is then highly likely that the transmission/reception will be unclear and that data might be dropped. On the other hand, C-CNRR selects those nodes that are closest to the sender/forwarder but not falling within the first 20% of its transmission range. This provides a greater coverage area, good channel quality and reduces redundancy because very close nodes will have similar coverage areas.

6.1.2 Link Stability and Energy Aware Protocol

A new Link Stability and Energy-Aware (LSEA) routing protocol was introduced in this thesis. It considered the Link Lifetime (LLT) between the source/forwarder node and the node receiving an RREQ packet. In addition, the protocol simultaneously considered the Residual Energy (RE) of any node in the process of receiving or sending an RREQ message. Considering these two parameters when establishing a route can help with solving MANETs' problems with mobility and energy constraints. Applying this protocol to MANETs guarantees that the selected route will be the best available route in the network with respect to the LLT and RE parameters. LSEA was developed to increase the stability of selected routes and reduce broken links, which arise from selecting an end-to-end route without any knowledge of how long the links will remain valid. LSEA was developed into two phases:

- Fixed Link Stability and Energy-Aware (F-LSEA).
- Average Link Stability and Energy-Aware (A-LSEA).

The LSEA *routing protocol concepts can be summarized as follows:*

- Upon receiving an RREQ, all recipients must check the LLT (with the sender of the RREQ) and its own RE parameters.
- If F-LSEA has been applied as a routing protocol in the network, then both parameters must be above the previously determined fixed thresholds before the receiver node can forward the received RREQ packet in cases where there is no available information in the routing table. If one or both of the parameters are below the fixed threshold, the node will discard the received RREQ.

  The fixed threshold parameters (LLT, RE) are pre-defined in the F-LSEA routing protocol. A-LSEA is designed to overcome the fixed thresholds for both the parameters in the F-LSEA routing protocol as these two parameters should be flexible in relation to the network's condition and status. Applying A-LSEA as a routing protocol in the network, a node gathers all its neighbours' REs through a modified hello message. Furthermore, the receiver node will gather its LLTs with all its neighbours through the same hello message, which has also been changed to share LLT information between neighbours. Once the LLT_{avg} and RE_{avg} are available, the receiver node must compare its RE and LLT (the LLT between the sender of the RREQ and the node processing the RREQ) with the RE_{avg} and LLT_{avg} , respectively. If the receiver node's RE and LLT are above the RE_{avg} and LLT_{avg}, respectively, then it will rebroadcast the received RREQ. Otherwise, the receiver node discards the received RREQ.

6.1.3 Position-based Selective Neighbours

Finally, the last contribution took advantage of both of the proposed CNRR and LSEA routing protocols. Position-based Selective Neighbours (PSN) is an intelligent routing protocol that can reduce overhead in the network to a minimum without losing reachability among the nodes. The advantages of LSEA and CNRR have been improved upon even more to achieve better routing paths that can apply a zoning concept and select four candidate nodes from each zone based on their REs and LLTs with respect to the sender/forwarder node. The key concepts of the PSN routing protocol can be summarised as follows:

- Any source/forwarder node in the process of sending a RREQ should divide the transmission range into four equal zones and select one node per zone based on its RE and LLT.
- The source/forwarder node will gather all the available information collected by the 'hello' message about its neighbours' REs and LLTs. Then, the source/forwarder node will select the best node in each zone as a Candidate Node (CN) to rebroadcast the received RREQ based on the RE

and LLT parameters. These selected CNs will be attached to the RREQ packets in the new *cnrr* field.

- Upon receiving the RREQ, all neighbours look to see if they are included in the *cnrr* field in the received RREQ. If an address belonging to them is found, this means that this node has been selected by the source/forwarder node as a CN to rebroadcast the RREQ. Otherwise, the node will understand that the source/forwarder did not select it as a CN and will simply discard the received RREQ.
- Furthermore, the CN runs an advanced algorithm to discover the number of nodes in its neighbourhood that have already received the same copy of this RREQ. Even though the CN has been selected by the source node, this check is very important to eliminate RREQ redundancy in the network. The candidate node will forward the RREQ if less than 75% of its neighbouring nodes have received the same one. The RREQ packet is discarded if more than 75% of the neighbouring nodes have already received it. This helps reduce RREQ flooding caused by dissemination inside the global network.

6.2 Directions of Future Research

6.2.1 Thesis' Future Research

Several issues and unsolved problems in this thesis' research require further study. Possible future research is outlined below.

6.2.1.1 Improving the CNRR Routing Protocol

The zoning partitioning concept in the CNRR protocol could be investigated further. The four zones could be increased to six or eight to see the effects of increasing the zones and how the overhead might change in turn.

Furthermore, there needs to be more investigation of the method of selecting candidate neighbours to rebroadcast RREQs for both F-CNRR and C-CNRR. In some cases, the closest node can reduce the coverage area and increase the overhead because of the closeness of the nodes, which increases RREQ redundancy in the network. Furthermore, in some cases the furthest node can lead to frequent link breakages because the furthest nodes always located at the edge of the source node when they are selected. Hence, the distance may be determined by averaging neighbours distance to the source node and select the candidate nodes based of the average distance.

6.2.1.2 Optimization of the LSEA Routing Protocol

An important challenge that the LSEA has to face is balancing the Link Lifetime and Residual Energy parameters. In the F-LSEA and A-LSEA routing protocols, the threshold parameters that tell the node when to rebroadcast or discard received RREQs need further research and development. The proposed routing protocols cannot distinguish between degrees of priority for each parameter (RE and LLT) and both of the nodes' parameters must pass the condition or be above the fixed or average threshold to allow the node to forward/rebroadcast the received RREQ rather than discarding it. Combining these two parameters based on their priorities for an optimized solution in the route discovery process could be a very interesting area for future research.

6.2.1.3 Flexible Percentages for the PSN Routing Protocol

In the PSN routing protocol, when the Candidate Node (CN) receives an RREQ, the CN must calculate the percentage of its neighbours that have received the same RREQ before making a decision. This percentage plays a vital role in the decision to rebroadcast or discard the received RREQ. As mentioned previously, the best percentage for improving network performance is 75% under the PSN routing protocol. This indicates that if more than 75% of the CN's neighbours have already received the same RREQ, then the CN should not rebroadcast it. If less than 75% of the CN's neighbours have received the same RREQ, the CN will rebroadcast it. The effect of this percentage has been shown in relation to the overhead and the number of neighbours who have received the same RREQ. When the percentage is low, the relevant overhead is low and vice versa. This essentially means that when fewer CN neighbours receive the same RREQ, the CN node rebroadcasts it, thus adding more overhead to the overall network traffic.

Determining this percentage needs further investigation as the CN should be aware of the network's status and what the average number of neighbours is for each node. CNs should decide whether to rebroadcast or discard RREQs carefully, based on a flexible rather than fixed percentage. This is because the decisions taken by CNs will affect connectivity among the nodes, as well as path discovery. If all the CNs decide not to rebroadcast a received RREQ it is likely that it will not find its intended destination. Hence, this percentage should be flexible and based on other parameters and the status of the network, including the average number of neighbours.

PSN Functions

```
void
PSN::recvRequest(Packet *p) {
struct hdr_ip *ih = HDR_IP(p);
struct hdr_PSN_request *rq = HDR_PSN_REQUEST(p);
PSN_rt_entry *rt;

  /*
   * Drop if:
   *      - I'm the source
   *      - I recently heard this request.
   */

  if(rq->rq_src == index) {
#ifdef DEBUG
    fprintf(stderr, "%s: got my own REQUEST\n", __FUNCTION__);
#endif // DEBUG
    Packet::free(p);
    return;
  }

 if (id_lookup(rq->rq_src, rq->rq_bcast_id)) {

#ifdef DEBUG
   fprintf(stderr, "%s: discarding request\n", __FUNCTION__);
#endif // DEBUG

   Packet::free(p);
   return;
 }

 /*
  * Cache the broadcast ID
  */
/*
 else
     {
       double link_life;
       link_life = get_link_life_time(ih->saddr());
       if (link_life > 2)
       id_insert(rq->rq_src, rq->rq_bcast_id);
       else {
       Packet::free(p);
       return; }
     }
*/
       id_insert(rq->rq_src, rq->rq_bcast_id);
```

```
/*
 * We are either going to forward the REQUEST or generate a
 * REPLY. Before we do anything, we make sure that the REVERSE
 * route is in the route table.
 */
PSN_rt_entry *rt0; // rt0 is the reverse route

  rt0 = rtable.rt_lookup(rq->rq_src);
  if(rt0 == 0) { /* if not in the route table */
  // create an entry for the reverse route.
    rt0 = rtable.rt_add(rq->rq_src);
  }

  rt0->rt_expire = max(rt0->rt_expire, (CURRENT_TIME + REV_ROUTE_LIFE));

  if ( (rq->rq_src_seqno > rt0->rt_seqno ) ||
       ((rq->rq_src_seqno == rt0->rt_seqno) &&
        (rq->rq_hop_count < rt0->rt_hops)) ) {
  // If we have a fresher seq no. or lesser #hops for the
  // same seq no., update the rt entry. Else don't bother.
   rt_update(rt0, rq->rq_src_seqno, rq->rq_hop_count, ih->saddr(),
             max(rt0->rt_expire, (CURRENT_TIME + REV_ROUTE_LIFE)) );
    if (rt0->rt_req_timeout > 0.0) {
    // Reset the soft state and
    // Set expiry time to CURRENT_TIME + ACTIVE_ROUTE_TIMEOUT
    // This is because route is used in the forward direction,
    // but only sources get benefited by this change
      rt0->rt_req_cnt = 0;
      rt0->rt_req_timeout = 0.0;
      rt0->rt_req_last_ttl = rq->rq_hop_count;
      rt0->rt_expire = CURRENT_TIME + ACTIVE_ROUTE_TIMEOUT;
    }

    /* Find out whether any buffered packet can benefit from the
     * reverse route.
     * May need some change in the following code - Mahesh 09/11/99
     */
    assert (rt0->rt_flags == RTF_UP);
    Packet *buffered_pkt;
    while ((buffered_pkt = rqueue.deque(rt0->rt_dst))) {
      if (rt0 && (rt0->rt_flags == RTF_UP)) {
       assert(rt0->rt_hops != INFINITY2);
        forward(rt0, buffered_pkt, NO_DELAY);
      }
    }
  }
  // End for putting reverse route in rt table
```

```
/*
 * We have taken care of the reverse route stuff.
 * Now see whether we can send a route reply.
 */

rt = rtable.rt_lookup(rq->rq_dst);

// First check if I am the destination ..

if(rq->rq_dst == index) {

#ifdef DEBUG
  fprintf(stderr, "%d - %s: destination sending reply\n",
                  index, __FUNCTION__);
#endif // DEBUG

  // Just to be safe, I use the max. Somebody may have
  // incremented the dst seqno.
  seqno = max(seqno, rq->rq_dst_seqno)+1;
  if (seqno%2) seqno++;

  sendReply(rq->rq_src,           // IP Destination
            1,                    // Hop Count
            index,                // Dest IP Address
            seqno,                // Dest Sequence Num
            MY_ROUTE_TIMEOUT,     // Lifetime
            rq->rq_timestamp);    // timestamp

  Packet::free(p);
}

// I am not the destination, but I may have a fresh enough route.

else if (rt && (rt->rt_hops != INFINITY2) &&
              (rt->rt_seqno >= rq->rq_dst_seqno) ) {
//assert (rt->rt_flags == RTF_UP);
  assert(rq->rq_dst == rt->rt_dst);
  //assert ((rt->rt_seqno%2) == 0);  // is the seqno even?
  sendReply(rq->rq_src,
            rt->rt_hops + 1,
            rq->rq_dst,
            rt->rt_seqno,
            (u_int32_t) (rt->rt_expire - CURRENT_TIME),
            //              rt->rt_expire - CURRENT_TIME,
            rq->rq_timestamp);

  // Insert nexthops to RREQ source and RREQ destination in the
```

```
   // precursor lists of destination and source respectively
   rt->pc_insert(rt0->rt_nexthop); // nexthop to RREQ source
   rt0->pc_insert(rt->rt_nexthop); // nexthop to RREQ destination

#ifdef RREQ_GRAT_RREP

   sendReply(rq->rq_dst,
             rq->rq_hop_count,
             rq->rq_src,
             rq->rq_src_seqno,
             (u_int32_t) (rt->rt_expire - CURRENT_TIME),
             //             rt->rt_expire - CURRENT_TIME,
             rq->rq_timestamp);
#endif

// TODO: send grat RREP to dst if G flag set in RREQ using rq->rq_src_seqno, rq->rq_hop_counT

       Packet::free(p);
    }

 /*
  * Can't reply. So forward the  Route Request
  */

else if ( (rq->NCRR[0]) or (rq->NCRR[1]) or (rq->NCRR[2]) or (rq->NCRR[3])  == index )
{
int all_nbr = 0;
int nbr_rcv= 0;
       nb_purge();

       PSN_Neighbor *nb = nbhead.lh_first;

       for(; nb; nb = nb->nb_link.le_next) {

              all_nbr = all_nbr + 1;

              iNode = (MobileNode *) (Node::get_node_by_address(ih->saddr()));
// for the sender of the RREQ
               nbr = (MobileNode *) (Node::get_node_by_address(nb->nb_addr));
 // for the neighbour of this node

              double distance = calculate_distance(nbr->X(), nbr->Y(), iNode->X(), iNode->X() );

              if ( distance < 250)
              nbr_rcv = nbr_rcv + 1 ;
         }
```

```
if (nbr_rcv or all_nbr == 0 )
         return;

else if(((nbr_rcv/all_nbr)*100)<25){ // to check how many of its neighbour recieved this RREQ

             identifyzone();

             rq->NCRR[0] = NCRR[0];
             rq->NCRR[1] = NCRR[1];
             rq->NCRR[2] = NCRR[2];
              rq->NCRR[3] = NCRR[3];
             ih->saddr() = index;
             ih->daddr() = IP_BROADCAST;
              rq->rq_hop_count += 1;
             // Maximum sequence number seen en route
             if (rt) rq->rq_dst_seqno = max(rt->rt_seqno, rq->rq_dst_seqno);
              forward((PSN_rt_entry*) 0, p, DELAY);
             //   Packet::free(p);

        }
 }

else
Packet::free(p);

}
---------------------------------------------------------------------------------------

void
PSN::sendRequest(nsaddr_t dst) {
// Allocate a RREQ packet
Packet *p = Packet::alloc();
struct hdr_cmn *ch = HDR_CMN(p);
struct hdr_ip *ih = HDR_IP(p);
struct hdr_PSN_request *rq = HDR_PSN_REQUEST(p);
PSN_rt_entry *rt = rtable.rt_lookup(dst);

 assert(rt);

 /*
  *  Rate limit sending of Route Requests. We are very conservative
  *  about sending out route requests.
  */

 if (rt->rt_flags == RTF_UP) {
   assert(rt->rt_hops != INFINITY2);
```

```
  Packet::free((Packet *)p);
  return;
 }

 if (rt->rt_req_timeout > CURRENT_TIME) {
  Packet::free((Packet *)p);
  return;
 }

 // rt_req_cnt is the no. of times we did network-wide broadcast
 // RREQ_RETRIES is the maximum number we will allow before
 // going to a long timeout.

 if (rt->rt_req_cnt > RREQ_RETRIES) {
  rt->rt_req_timeout = CURRENT_TIME + MAX_RREQ_TIMEOUT;
  rt->rt_req_cnt = 0;
 Packet *buf_pkt;
  while ((buf_pkt = rqueue.deque(rt->rt_dst))) {
      drop(buf_pkt, DROP_RTR_NO_ROUTE);
  }
  Packet::free((Packet *)p);
  return;
 }

#ifdef DEBUG
   fprintf(stderr, "(%2d) - %2d sending Route Request, dst: %d\n",
                    ++route_request, index, rt->rt_dst);
#endif // DEBUG

 // Determine the TTL to be used this time.
 // Dynamic TTL evaluation - SRD

 rt->rt_req_last_ttl = max(rt->rt_req_last_ttl,rt->rt_last_hop_count);

 if (0 == rt->rt_req_last_ttl) {
 // first time query broadcast
  ih->ttl_ = TTL_START;
 }
 else {
 // Expanding ring search.
  if (rt->rt_req_last_ttl < TTL_THRESHOLD)
    ih->ttl_ = rt->rt_req_last_ttl + TTL_INCREMENT;
  else {
  // network-wide broadcast
    ih->ttl_ = NETWORK_DIAMETER;
    rt->rt_req_cnt += 1;
  }
 }
```

```
 // remember the TTL used  for the next time
 rt->rt_req_last_ttl = ih->ttl_;

 // PerHopTime is the roundtrip time per hop for route requests.
 // The factor 2.0 is just to be safe .. SRD 5/22/99
 // Also note that we are making timeouts to be larger if we have
 // done network wide broadcast before.

 rt->rt_req_timeout = 2.0 * (double) ih->ttl_ * PerHopTime(rt);
 if (rt->rt_req_cnt > 0)
   rt->rt_req_timeout *= rt->rt_req_cnt;
 rt->rt_req_timeout += CURRENT_TIME;

 // Don't let the timeout to be too large, however .. SRD 6/8/99
 if (rt->rt_req_timeout > CURRENT_TIME + MAX_RREQ_TIMEOUT)
   rt->rt_req_timeout = CURRENT_TIME + MAX_RREQ_TIMEOUT;
 rt->rt_expire = 0;

#ifdef DEBUG
 fprintf(stderr, "(%2d) - %2d sending Route Request, dst: %d, tout %f ms\n",
                 ++route_request,
                index, rt->rt_dst,
                rt->rt_req_timeout - CURRENT_TIME);
#endif  // DEBUG//

 // Fill out the RREQ packet
 // ch->uid() = 0;
 ch->ptype() = PT_PSN;
 ch->size() = IP_HDR_LEN + rq->size();
 ch->iface() = -2;
 ch->error() = 0;
 ch->addr_type() = NS_AF_NONE;
 ch->prev_hop_ = index;          // PSN hack

 ih->saddr() = index;
 ih->daddr() = IP_BROADCAST;
 ih->sport() = RT_PORT;
 ih->dport() = RT_PORT;

identifyzone(); // call this funtion to execute the funtion and bulid up the CNRR to
attach it                                      in the RREQ

 rq->NCRR[0] = NCRR[0];
 rq->NCRR[1] = NCRR[1];
 rq->NCRR[2] = NCRR[2];                      // attach the NCRR array in the RREQ
 rq->NCRR[3] = NCRR[3];
```

```
 // Fill up some more fields.
 rq->rq_type = PSNTYPE_RREQ;
 rq->rq_hop_count = 1;
 rq->rq_bcast_id = bid++;
 rq->rq_dst = dst;
 rq->rq_dst_seqno = (rt ? rt->rt_seqno : 0);
 rq->rq_src = index;
 seqno += 2;
 assert ((seqno%2) == 0);
 rq->rq_src_seqno = seqno;
 rq->rq_timestamp = CURRENT_TIME;

 Scheduler::instance().schedule(target_, p, 0.);

}
---------------------------------------------------------------------------------------

double
PSN::get_link_life_time(nsaddr_t source) {
//Packet *p = Packet::alloc();
//struct hdr_cmn *ch = HDR_CMN(p);
//struct hdr_ip *ih = HDR_IP(p);
double x,y,sx,sy; //direction index and source
double angle_index, angle_source; // angle index and source
double a,b,c,d,k;
double A,B,C,K,R,F,N;
double source_speed, current_speed;
double link_life; // link life time

MobileNode *current_node;
MobileNode *source_node;
current_node = (MobileNode *) (Node::get_node_by_address(index));
source_node = (MobileNode *) (Node::get_node_by_address(source));

source_node->update_position();
current_node->update_position();

if ( (current_node->X() == priv_x) && (current_node->Y() == priv_y) ) {

        current_speed = 0;
        angle_index = 0;
        x = 0;  y = 0;
        }
        else
        {
        x = current_node->dX();
        y = current_node->dY();
        angle_index = calculate_direction(x,y);
```

```
        current_speed = current_node->speed();
        }

if ( (source_node->X() == source_priv_x) && (source_node->Y() == source_priv_y) ) {

        source_speed = 0;
        angle_source = 0;
        sx = 0; sy = 0;
        }
        else
        {
        sx= source_node->dX();
        sy= source_node->dY();
        angle_source = calculate_direction(sx,sy);
        source_speed = source_node->speed();
        }

priv_x = current_node->X();
priv_y = current_node->Y();
source_priv_x = source_node->X();
source_priv_y = source_node->Y();

a = ( current_speed * cos(angle_index) ) - ( source_speed * cos(angle_source) );

b = current_node->X()- source_node->X();

c = ( current_speed * sin(angle_index) ) - ( source_speed * sin(angle_source) );

d = current_node->Y() - source_node->Y();

k = ((a*d))-((b*c)); // * ( (a*d)-(b*c) );   // (ad-bc)*(ad-bc)

A = a*a;
B = b*b;
C = c*c;

K = k*k;
R = 250*250;

if (A == 0 && C == 0 )
return(1000);

if ((((A+C) * R )-K ) > 0) {
F = sqrt( ((A+C) * R )-K );
}
else {
F =  (((A+C) * R )-K ) * -1;
F = sqrt(F);
```

```
F = F * -1;
}

N = -1 * ((a*b)+(c*d));
link_life = (N+F)/(A+C);

if (link_life<0)
return(0);
else
return (link_life);

}
--------------------------------------------------------------------------------------

double
PSN::calculate_direction(double x, double y)
{
  double dir;

if (x == 0 && y == 0)
return(0);

else if (y == 0) {
        if ( x > 0 )
        return(0);
        else
        return(180);
        }
else if (x == 0) {
        if (y < 0 )
        return(270);
        else
        return(90);
        }

else if (x != 0)
        {
        dir = atan(y/x);

        if(dir > 0) {
        if (x > 0 )
        dir = dir;
        else
        return ( 180 + (dir*(180/PI)));
        }


        else if (dir < 0) {
```

```
        if ( x < 0){
        dir = PI+dir;
        }
        else
        dir = 2*PI + dir;
        }
        }
       return (dir*(180/PI));

}
```

```
double
PSN::calculate_distance(double x1, double y1, double x2, double y2)
{
double distance;
distance = sqrt(((x1 - x2)*(x1 - x2)) + ((y1 - y2)*(y1 - y2)));
return (distance);
}
```

```
double
PSN::avg_energy() {

nb_purge();

double avg_energy_value = 0; int nbor_n = 0;

PSN_Neighbor *nb = nbhead.lh_first;

        for(; nb; nb = nb->nb_link.le_next) {
nb_purge();
               iNode = (MobileNode *) (Node::get_node_by_address(nb->nb_addr));
               avg_energy_value = avg_energy_value + iNode->energy_model()->energy();

               nbor_n = nbor_n + 1;
        }
                       if  ( (avg_energy_value == 0)  or  (nbor_n == 0)  ) {
                       }
                       else
                       {
                       return (avg_energy_value/nbor_n);
                       }

}
```

```
double
PSN::avg_link() {
nb_purge();
double avg_link_value = 0; int nbor_n = 0; //double link_life = 0;
PSN_Neighbor *nb = nbhead.lh_first;
//PSN_Neighbor *nbn;
        for(; nb; nb = nb->nb_link.le_next) {
                avg_link_value = avg_link_value + nb->nb_llt;
                nbor_n = nbor_n + 1;
                }
                        if  ( (avg_link_value == 0)  or (nbor_n == 0)  ) {
                            return 0;
                        }
                        else
                        {
                        return (avg_link_value/nbor_n);
                        }
}
```

List of Publications

Published Papers

1- Sofian Hamad, H. Noureddine and Hamed Al-Raweshidy "Link stability and energy aware for reactive routing protocol in mobile ad hoc network", *Proceedings of the 9th ACM international symposium on Mobility management and wireless access* ACM, pp. 195, 2011.

2- Sofian Hamad, H. Noureddine, N. Radhi, I. Shah and Hamed Al-Raweshidy, "Efficient flooding based on node position for mobile ad hoc network", *Innovations in Information Technology (IIT), International Conference on* IEEE, pp. 162, 2011.

3- Sofian Hamad, H. Noureddine and Hamed Al-Raweshidy "LSEA: Link Stability and Energy Aware for efficient routing in Mobile Ad Hoc Network", *Wireless Personal Multimedia Communications (WPMC), 14th International Symposium on* IEEE, pp. 1, 2011.

4- Sofian Hamad, N. Radhi and Hamed Al-Raweshidy, "Candidate Neighbours to Rebroadcast the RREQ for efficient flooding in mobile ad hoc network", *Wireless Advanced (WiAd),* IEEE, pp. 26, 2011.

5- N. Radhi, K. Aziz, Sofian Hamad and Hamed AL-Raweshidy, "Estimate primary user localization using cognitive radio networks", *Innovations in Information Technology (IIT), International Conference on* IEEE, pp. 381, 2011.

6- N. Radhi, Sofian Hamad and Hamed AL-Raweshidy, "Implementation of Spectrum Sensing Methods for UWB-Cognitive Radio System", *Next Generation Mobile Applications, Services and Technologies (NGMAST), 5th International Conference on* IEEE, pp. 142, 2011.

7- I. Shah, Sofian Hamad and Hamed Al-Raweshidy, "Multi-Radio Multi-Channel assignment games in non-cooperative Wireless Mesh Networks with end user bargaining", *Fuzzy Systems and Knowledge Discovery (FSKD), Eighth International Conference on* IEEE, pp. 2679, 2011.

Papers under review

1- Sofian Hamad, I. Shah, Sadaqat Khan and Hamed AL-Raweshidy, " Route Discovery by Candidate Neighbours to Rebroadcast the RREQ in Mobile Ad-Hoc Network", Wireless Communications and Mobile Computing Journal-Wiley, under revision since August 2012.

2- Sofian Hamad, I. Shah, Sadaqat Khan and Hamed AL-Raweshidy, "Link Stability and Energy-Aware in Mobile Ad-hoc Network", Submitted to IET Journal in Communications, under revision since August 2012.