PREDICTIVE DIVERT FAILURE ROUTE PROTOCOL FOR MOBILE AD-HOC NETWORKS BASED ON AD-HOC ON DEMAND DISTANCE VECTOR

SAYID MOHAMED ABDULE

DOCTOR OF PHILOSOPHY

UNIVERSITI UTARA MALAYSIA

2012

PREDICTIVE DIVERT FAILURE ROUTE PROTOCOL FOR MOBILE AD-HOC NETWORKS BASED ON AD-HOC ON DEMAND DISTANCE VECTOR

Thesis submitted to Dean of Awang Had Salleh Graduate School of Arts and Sciences
in full fulfillment of the requirements for the degree of Doctor of Philosophy
Universiti Utara Malaysia

by

SAYID MOHAMED ABDULE

© 2012, SAYID MOHAMED ABDULE

Permission to Use

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to :

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Rangkaian Ad-hoc Bergerak (MANET) mempunyai satu ciri utama iaitu nod-nod yang boleh bergerak secara rawak. Namun, salah satu cabaran terbesar yang dihadapi MANET ialah berkaitan kegagalan pautan rangkaian. Sementara itu, Protokol Vektor Jarak Atas-Tuntutan Ad-hoc (AODV) merupakan antara protokol yang banyak digunakan dalam MANET. AODV menggunakan mekanisme pembaikan pautan setempat untuk menyelesaikan masalah kegagalan pautan. Namun, mekanisme ini hanya sesuai digunakan ketika berlakunya kegagalan pautan yang berdekatan dengan destinasi. Oleh itu, matlamat kajian ini adalah untuk memperkenalkan sebuah protokol penghalaan baru berdasarkan AODV. Protokol penghalaan baru ini dinamakan “Protokol Ramalan Ubahan Haluan Yang Gagal” (PDFRP). Protokol ini dilaksanakan dalam Penyelaku Rangkaian 2 (ns-2). Beberapa fungsi berikut telah ditambah. Antaranya ialahmekanisme Cari Laluan Baru dan mekanisme Ubahan Haluan. PDFRP menggunakan mekanisme pautan ramalan untuk mengukur kekuatan isyarat. Jika isyarat rendah daripada nilai ambang, maka mekanisme Cari Laluan Baru akan mencari haluan baru, dan kemudian mekanisme Ubahan Haluan akan mengubahkan data semasa melalui haluan baru. Gabungan teknik yang digunakan PDFRP menunjukkan prestasi hebat berbanding AODV. Walau bagaimanapun, mekanisme baru ini hanya bersesuaian untuk protokol satu laluan sahaja. Keterbatasan lain adalah ramalan salah yang terhasil apabila dua nod menghampiri satu sama lain yang menyebabkan bebanan berlebihan kepada rangkaian. Walaupun demikian, kajian ini mendapati protokol penghalaan baru ini mampu meningkatkan nisbah penghantaran bingkisan dan daya pemprosesan. Di samping itu, ianya mengurangkan kehilangan bingkisan serta lengah hujung ke hujung. Semua mekanisme baru ini membantu meningkatkan prestasi rangkaian dan kecekapan keseluruhan rangkaian ad-hoc serta memaksimumkan penggunaan sumber rangkaian. Hasil kajian menunjukkan bahawa protokol PDFRP mengungguli protokol piawaian AODV daripada aspek bebanan pasti penghalaan, kehilangan bingkisan, purata lengah, penghantaran bingkisan dan daya pemprosesan.

Kata kunci: Rangkaian ad-hoc, Kegagalan pautan, Ramalan pautan keadaan, Mengubah haluan.

Abstract

A main characteristic of Mobile Ad-hoc Network (MANET) is that its node can move randomly, and due to this, the main challenge to MANET has always been the problem of link failure. Ad-hoc On-Demand Distance Vector (AODV) protocol is one of the widely used protocols in MANET. AODV uses local repair mechanism to solve the link failure problem, but this mechanism is suitable only when the link failure occurs near the destination. The aim of this research is to present a new routing protocol based on AODV, namely the Predictive Divert Failure Route Protocol (PDFRP). The protocol has been implemented in Network Simulator 2 (ns-2) where the following functions are added: Find New Path and Divert Route mechanisms. PDFRP utilizes link prediction mechanism to measure the signal strength. If it is lower than the threshold value, the Find New Path mechanism will search a new path, and then the Divert Route mechanism diverts the current data through the new route. The combination of these techniques used by PDFRP showed superior performance to AODV. However, the new mechanism works only with the single path routing protocols. Another limitation is the false prediction when two nodes are moving closer which may cause unnecessary overhead to the network. Despite the limitations, the new routing protocol increases the packet delivery ratio and throughput. In addition, it also decreases the packet loss and delay. All these new mechanisms help to improve the network performance and overall ad-hoc network efficiency, as well as to maximize network resource utilization. The experiment results showed that the PDFRP protocol outperforms AODV in terms of routing overhead, packet loss, average delay, packet delivery and throughput.

Keywords: Ad-hoc networks, Link failure, Link state prediction, Divert route.

Declaration Associated with this Thesis

Some of the works presented in this thesis have been published as listed below.

[1] Sayid Mohamed Abdule, Suhaidi Hassan, Osman Ghazali, and Mohamed M. Kadhum, "Pause Time Optimal Setting for AODV Protocol on RPGM Mobility Model in MANETs," *International Journal of Advanced Computer Science and Applications,* vol. 1, no. 6, pp. 1–7, Dec. 2010.

[2] Sayid Mohamed Abdule, Suhaidi Hassan, and Mohamed M. Kadhum, "An Improvement of Link Failure Maintenance in Ad-hoc Wireless Network on AODV Protocol," *International Journal of Computer Science and Information Security (IJCSIS),* vol. 8, pp. 182–188, Aug. 2010, USA.

[3] Sayid Mohamed Abdule, Suhaidi Hassan, Osman Ghazali, and Mohamed M. Kadhum, "The Effect of Speed on AODV Protocol Performance Using RWP in Ad- hoc Network," *2010 International Conference on Mathematical, Physical and Engineering Sciences (MPES 2010)*, Penang, Malaysia, Nov. 2010, pp. 191.

[4] Sayid Mohamed Abdule and Suhaidi Hassan, "Divert Failure Route Protocol Based on AODV," *in Proceedings of the 2010 Second International Conference on Network Applications, Protocols and Services*, *NETAPPS '10*, Washington, DC, USA: IEEE Computer Society, Sept. 2010, pp. 67–71.

[5] Sayid Mohamed Abdule and Suhaidi Hassan, "A New Routing Protocol for Wireless Ad-hoc Networks," *in Proceedings International Conference on Network Applications, Protocols and Services (NetApps2008)*, Sintok, Kedah, Malaysia: IEEE Computer Society, Nov. 2008, pp.1-5.

Acknowledgement

In the name of ALLAH, Most Gracious, Most Merciful.

I would like to express my deep and sincere gratitude to my supervisors, Associate Professor Dr. Suhaidi Hassan and Associate Professor Dr. Osman Ghazali for their supervision and constant support. Their understanding, encouragement and personal guidance have provided a good basis for this research and for the continuous support of my PhD studies and research, for their patience, motivation, enthusiasm, and immense knowledge. Their guidance helped me in the time of research and writing of this research. I could not have imagined having a better advisor and mentor for my PhD studies.

Besides my supervisors, I would like to thank the rest of my colleagues, especially to the members of the UUM InterNetWorks Research Group, who have given me the opportunity to work with them and helped me to overcome the challenges during my research and for their encouragement, insightful comments, and hard questions. I also owe my most sincere gratitude to my sponsor (Norwegian Government) for their financial support during my study in Malaysia.

My sincere thanks also go to the Universiti Utara Malaysia for providing me good facilities to achieve my ultimate goal. My thanks also go to International Islamic University Malaysia and Universiti Kebangsaan Malaysia Library staff who were always present to help me during my study in searching for materials and related information. I would like also to thank Dr. Mohammed M. Kadhum, Postdoctoral fellow in Queen's University Kingston, Canada, Dr. Ahmed Osman Awil, Assistant Vice President, Iskandar Investment Berhad, Mr. Naseer Ali Husieen, Mr. Abdule-Aziz Tanko, Dr. Ahmed Zuki for editing this research as well as their moral support to encourage me to fulfill and accomplish my research.

Last but not the least, I owe my loving thanks to my wife Saiido, my sons, Sadiq, Subeyr, Suhayb and Abdullah, my daughters, Suaad, Sundus, Samiira, Salina, and Faduma. Without their encouragement and understanding it would have been impossible for me to finish this work.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

2HBR	-	Two Hops Backup Routing
ABR	-	Adaptive Backup Routing
ACG	-	Directed Acyclic Graph
AED	-	Average End-to-End Delay
AGT	-	Agent
AODV	-	Ad-hoc on-Demand Distance Vector
ARP	-	Address Resolution Protocol
BR	-	Backup Routing
BRRP	-	Backup Route Reply
BRRQ	-	Backup Route Request
CBR	-	Constant Bit Rate
CDMA	-	Code Division Multiple Access
C-N	-	Current Node
CTS	-	Clear To Send
CUD	-	Construct Uniform Design
CWMin, CWMax	-	Minimal and Maximal Size of Connection Window
DCF	-	Distributed Coordination Function
DES	-	Discrete Event Simulation
DM-NPM	-	Detection -Model and New Path -Model
DRMS	-	Design Research Methodology Steps
DSDV	-	Destination-Sequence Distance Vector
DSR	-	Dynamic Source Routing
DV	-	Distance Vector
DV-MP	-	Distance Vector with Mobility Prediction
ERU-REQ	-	Early Route Update Request
FWM	-	Free Way Model

GPRS	-	General Packet Radio Service
GPS	-	Global Position System
GSM	-	Global System for Mobile Communications
KBPS	-	Kilobits Per Second
LR	-	Local Repair
LRREQ	-	Local Route Request
MANET	-	Mobile Ad-Hoc Network
MG	-	Manhattan-Grid Model
MIB	-	Management Information Base
MM	-	Meshed Multipath Routing
MN	-	Mobile Nodes
NAT	-	Neighbors Activity Table
NML	-	Normalized MAC Load
NPL	-	Neighbor Power List
NRL	-	Normalized Routing Load
Ns-2	-	Network Simulator Version 2
NSR	-	Neighborhood-aware Source Routing
OLSR	-	Optimized Link State Routing
OTCL	-	Object Tool Common Language
OTCL	-	Object Tool Common Language
PDA	-	Personal Digital Assistant
PDF	-	Packet Delivery Fraction
PDFRP	-	Predictive Divert Failure Route Protocol
PDT	-	Power Difference Table
PLRR	-	Preemptive Local Route Repair
PRT	-	Packet Received Time
PSR	-	Preemptive Self Repairing
QoS	-	Quality of Service
QP	-	Query Packet
RERR	-	Route Error Packet

RPGM	-	Reference Point Group Mobility Model
RPO	-	Routing Protocol Overhead
RREP	-	Route Reply Packet
RREQ	-	Route Request Packet
RRF	-	Route Repair Fail
RROK	-	Route Repair OK
RTS	-	Request To Send
RWP	-	Random Waypoint Model
SD	-	Safe Distance
SDR	-	Shortcut Detection and Route Repair
SINR	-	Signal to Interface plus Noise Ratio
SR	-	Self Repair Algorithm
SREP	-	Shortcut Reply
SREQ	-	Shortcut Route Request
SSAR	-	Signal Stability-based Adaptive Routing
TBRPF	-	Topology Broadcast Based on Reverse Path Forwarding
TORA	-	Temporally Ordered Routing Algorithm
TTL	-	Time To Live
UMTS	-	Universal Mobile Telecommunications System
UN	-	Upstream Notification
UPD	-	Update Packet
VBR	-	Variable Bit Rate
VOIP	-	Voice over Internet Protocol
WRP	-	Wireless Routing Protocol
ZHLS	-	Hierarchical Link State
ZRP	-	Zone Routing Protocol

CHAPTER ONE

INTRODUCTION

This chapter presents a brief introduction of Mobile Ad-hoc Network (MANET). The MANET consists of a collection of nodes, which dynamically form a temporary network, without using any existing network infrastructure or centralized administration. Mobile ad-hoc infrastructure and its differentiation from other network infrastructures such as wired and infrastructure wireless like cellular network is discussed in Section 1.1. This Section also presents MANET's routing protocols and their different classes such as proactive and reactive routing protocols. Ad-hoc On-Demand Distance Vector (AODV) and the way that the AODV reacts on MANET environments in terms of suitability of processing and how it minimizes overall network resource utilization as well as its drawback is discussed in subsection 1.1.2. Research motivation and factors which inspired us to select this topic in order to conduct this research, and significance of an ad-hoc network as it can be used for both data and voice communication are presented in Section 1.2. The research problems are described in Section 1.3. The research questions, research objectives and research scope are presented in Sections 1.4, 1.5 and 1.6 respectively. The steps that the research went through such as surveying the existing AODV protocol features especially link failure as well as comprative evaluation is discussed in Section 1.7. The key contributions including empirical evaluation of the existing AODV features for disclosing the limitation and strength for the protocol present in Section 1.8 and its Subsections. Finally, Section 1.9 highlights the organization of the research.

1.1 Mobile Ad-hoc Network

Mobile Ad-hoc Networks (MANETs) can be found within many systems; wireless local networks (the IEEE 802.11 family), personal area networks (Bluetooth) or even home networks (Home-RF, etc.). The deployment capability of an ad-hoc network is simple which has been led to several applications and solutions for different environments conditions such as rescue zones, far away zones. Basically, MANET was developed for military purposes and some special conditions such as in emergency, rescue operation and military actions as shows in Figure 1.1 . However, after the demand of such wireless tool has increased, it is started to be used for conferences, airports and some social applications as written by Dhawan [1]. In the ad-hoc context, factors such as radio transmission, hidden/exposed nodes, network mobility make the traditional protocols that are designed for cellular networks insufficient. Due to this, several mechanisms and protocols are developed to address issues such as security, routing and applications. Ad-hoc networks are completely infrastructure less which makes them more complexity. Consequently, their limited resources and topology changes bring up the problem of quality of service provided at different levels of communications as described by Lin et al. [2, 3]. MANETs have a number of characteristics that drove to the development of routing protocols. These characteristics are as follows [4]:

i. *Dynamic topologies*: The arbitrary movement of nodes in an ad-hoc network leads to a quick random change in the topology of the network.

ii. *Variable throughputs and limited bandwidth:* Because of using wireless connections, the actual throughput is frequently less than the maximum transfer rate of the radio interface compared to wired communications. Limited bandwidth can lead to congestion which can be the mean reason behind this weak communication throughput.

iii. *Energy constraint function*: The energy conservation optimization can be an important solution for MANET nodes that operating on battery or on limited energy resources.

Due to the high demand and for MANET application, it is believed that, in the future, MANET is going to replace the existing wireless telephony (cellular) and each ad-hoc wireless device will be capable of receiving, storing and forwarding data packet as stated by Kioumourtzis et al. [5, 6, 7]. Routing is one of the most important issues that have a significant impact on the MANET's performance. Many routing protocols have been developed for MANET. These routing protocols fall into two broad categories: proactive and reactive routing protocols. Proactive protocols, such as Dynamic Destination-Sequenced Distance Vector routing (DSDV), Optimized Link State Routing (OLSR), and Topology Broadcast based on Reverse Path Forwarding (TBRPF), maintain a database of potential routes so it is ready when data needs to be sent as written by Pirzada et al. [8]. Reactive protocols, such as Dynamic Source Routing (DSR), Signal Stability-based Adaptive routing (SSA), mixed routing protocols such as the Zone Routing Protocol (ZRP) and Ad-hoc On-Demand Distance Vector Routing (AODV), flood the network with path request packets looking for a route when it has data to send [9]. Reactive routing protocols initiates' route computation only on demand, which leads to better performance compared to proactive routing protocols, as described by Kulkarni et al. [10]. The most common on-demand routing protocols currently used in MANET are AODV and DSR. Several studies were performed to explore the impact of these protocols on MANET performance as written by Zahary et al. [11, 12, 13]. As described earlier, ad-hoc network is more important in disaster area as well as military battlefield networks as depicted in Figure 1.1 [14].

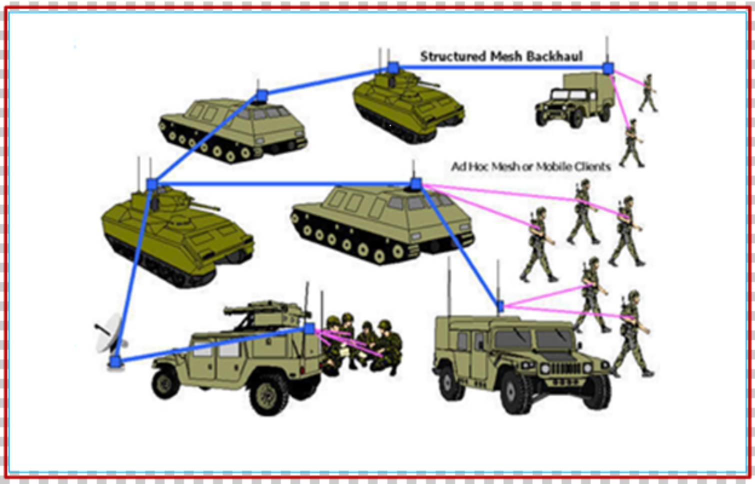


Figure 1.1: An Example of a Mobile Ad-hoc Network in a Military Action (Adopted from [14])

1.1.1 On-demand Routing Operation

To find a route to destination, MANET on demand routing protocols use different strategies. For example, DSR utilizes a source routing mechanism, in which, the source node must specify the entire route the packet should follow by putting the complete path to the destination in the message header. This means that the routed packet contains the address of each device the packet will pass through. This can result in high overhead for long paths and large addresses, especially when using IPv6 as described by Surayati and Usop [15]. On the other hand, AODV utilizes destination routing (hop by hop) mechanism, in which, the source node must specify only the destination in the message header. This means that the header of data packet should include only the next-hop information. This requires less overhead compared to DSR, as described in a standardization effort led by IETF Mobile Ad-hoc Networks (MANET) task group [16]. In addition, AODV uses sequence numbers in order to avoid any stale routes in the network to ensure the freshness of the route. Furthermore, AODV protocol scales well for large networks as well as higher traffic load and greater node mobility compared to DSR as mentioned in [17]. These advantages are the main motives behind selecting AODV for further improvement in this research.

1.1.2 Ad-hoc On-Demand Distance Vector

According to Jan et al. [17], AODV is more suitable for MANET communication as it has low processing and memory overhead. The way that AODV proceeds with ad-hoc communication is as follows: The source (sender-node) initiates route discovery through broadcasting Route Request (RREQ) packet to all nodes within the source transmission range, then the neighbor nodes will forward the RREQ to their neighbors until the packet either is reached to the destination, or it arrives at the node that has a new fresh route to the destination. When one of these requirements is taken places, a Route Reply (RREP) is returned to the source. Once the sender-node receives such RREP, it starts transmitting data using the newly constructed route. Nodes that use AODV protocol utilize link failure notification mechanism, called "Route Error (RERR)", to inform the source-node when a link to a next hop is failed. This drives the sender-node to establish a new route discovery process in order to complete the data transmission, which can reduce the overall network performance significantly. Several techniques and AODV-based protocols have been developed in order to solve such problem as written by [18, 19, 20].

However, the performance of these techniques or protocols failed to reach the optimal performance in MANET environment. This is one of the issues that motivated carrying out this research to develop a new protocol based on AODV, namely Predictive Divert Failure Route Protocol (PDFRP), to enhance the performance of MANETs.

1.2 Research Motivation

Mobile Ad-hoc Network (MANET) is recognized by the network industry in recent years as viable media. The proliferation of MANET applications has been increasing every day. Numerous applications have developed for MANET communication that serves data and voice. However, reliable mobile ad-hoc communication has been a challenge due to frequent mutability of the network topology change caused by the nodes' movement, as described by Frikha and Ghandour [21]. The mobile ad-hoc network group of the Internet Engineering Task Force (IETF) has proposed and developed numerous routing protocols to guarantee sustainable connectivity of nodes in MANETS. Nevertheless, the current routing protocols failed to maintain such requirement in most cases as they do not have the ability to scale up and down in order to adapt to network dynamics. One of the routing issues is how to select the best and shortest route to the desired destination and maintain the connectivity of the link between the source and receiver as indicated in [22]. Solution for such issue can help improving the performance of MANET significantly. Therefore, with the high demand for ad-hoc wireless application and scalable MANET architecture, it is important to develop an efficient routing protocol that meet the users' quality of service requirements.

1.3 Research Problem

Ad-hoc network is a relatively new concept in the communication industry to be accepted as an alternative medium compared to existing wired network. As mentioned earlier, in this type of network, each node moves randomly resulting in frequent route breakage. In AODV networks, when the link failure occurs, packets can be dropped because of the AODV behavior in handling link failure problem and that an alternate path is required only when the primary path is totally disconnected.

Furthermore, a new path is established by the source node instead of the intermediate node which contributes to higher end-to-end delay and overhead. The limitation of the local link failure repair mechanism in AODV led to several preemptive/predictive solutions. Unfortunately, these solutions involve large control message overhead and high latency. For example, preemptive/predictive route maintenance mechanisms come up with many implications such as high traffic overhead caused by redundant warning messages sent back to the source because of absence of warning message mechanism upon link failure. These redundant warning messages are consequences of high rate of network flood with several reinitiating route rediscovery which consumes network resources unnecessarily. Therefore, to overcome the above mentioned limitations, a new solution is needed which focuses mainly on how to prevent the number of warning messages traveling in the network before an active link (current link) fails. Thus, the research presented in this thesis includes developing a useful approach for how the packet can be diverted into a new path smoothly.

1.4 Research Questions

There are a few research questions as stated below:

i. How to overcome the link failure problem in MANETs that utilize AODV protocol in order to improve the performance and satisfy the user requirements?

ii. How to develop a new extension to AODV protocol to moderate the route rediscovery process caused by link failure?

iii. How to verify and validate the extended protocol to ensure its usability and performance?

1.5 Research Objectives

The main objective of the research is to improve the performance of MANETs by avoiding link failure phenomena that has negative impacts on these networks such as low packet delivery ratio, high end to end delay and packet loss. Therefore, the researcher comes up with the following specific objectives:

i. To perform an empirical evaluation of the AODV algorithm with different mobility models to identify the key factors that affect its performance.

ii. To develop a new extension to AODV protocol that can solve link failure problem and help improving the performance in terms of End- to-End delay, network overhead and the throughput.

iii. To evaluate the performance of the developed protocol, in comparison with available solutions, in a simulated network environment using network simulator 2 (ns-2).

iv. To verify and validate the developed protocol based on the results gained from the simulation experiments that ensure the correctness of its implementation.

1.6 Scope of the Research

This research considers routing in ad-hoc network and the problems associated with link failure that might be caused by node mobility when forwarding packets from hop to another hop on the route to the desired destination. In this particular, the research focuses on designing a new routing protocol based on AODV, namely Predictive Divert Failure Route Protocol (PDFRP), that predicts the status of an active link between two hops (nodes) and takes an action when one of these nodes is about to move away from the transmission range of the other. However, the link failure caused by sudden shutdown such as insufficient power is out of the scope of this research. The scope of the research presented in this thesis is shown in Figure 1.2 which depicts where PDFRP can actually work.

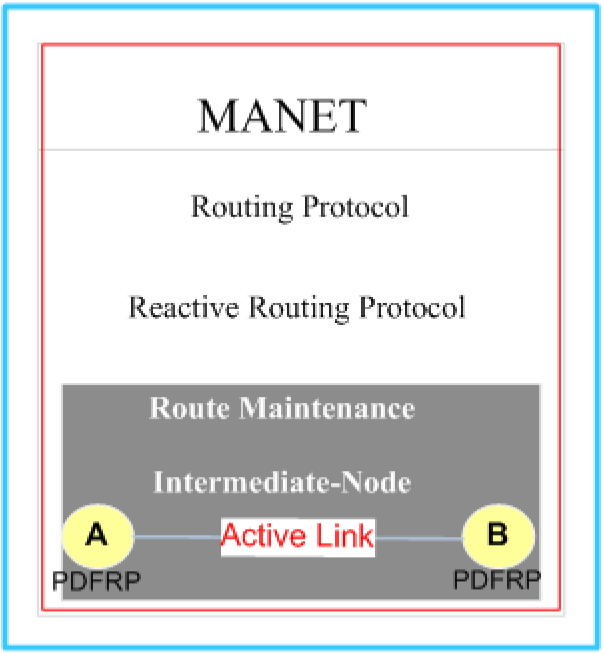


Figure 1.2: Scope of the Research (Shaded Area)

1.7 Research Steps

To complete the goal of this research, the following research steps were performed:

i. Survey of existing AODV link failure mechanisms to identify the key problem areas.

ii. Comparative performance evaluation of the existing link failure management techniques to explore their advantages and disadvantages.

iii. Design of a new extension protocol based on AODV routing protocol.

iv. Implementation of the new designed protocol in a simulation environment.

v. Performance evaluation of the new designed protocol to analyze its effect on the ad-hoc network performance regarding Packet Delivery Fraction (PDF), Normalized Routing Load (NRL), Average End-to-End Delay, Routing Overhead, Packet Loss and Throughput.

1.8 Contributions

The contributions of this research are outlined in the following sub-sections.

1.8.1 Contribution of Empirical Evaluation

The contributions include empirical evaluation of AODV algorithm where two mobility models namely Random Waypoint (RWP) and Reference Point Group Mobility (RPGM) have been tested. This pre-testing experiment presents a number of experiments aiming to figure out the optimal setting for AODV protocol in certain mobility models. However, the main contribution of this part of the research is to understand in depth the affected parameters where all main parameters have been investigated.

1.8.2 Contribution of the Developed Protocol

This research focuses on how to improve the reliability of routes in ad-hoc network in order to achieve better performance of AODV routing protocol. The research utilizes link state prediction to reduce the possibilities of data packets being dropped. The prediction mechanism is used in order to avoid the problem of the existing mechanism of routing protocol where a mobile node continues using the route until a link is broken. This research utilizes the prediction algorithm mechanism and uses the received signal power measurements to predict the link failure on an active path in order to perform a route rebuild prior to the link breakage with the aim to detect link breakage and construct a new route in advance to avoid the packet loss.

This research developed a new routing protocol which is an extension to AODV routing protocol by using the prediction algorithm. The simulation results have shown that the developed protocol performs well with high packet delivery ratio and low control message overhead. In addition, the number of data packets dropped is reduced, and its overall performance was improved compared to standard AODV protocol. Nonetheless, a new proactive routing protocol with implementation of prediction algorithm is developed where the simulation experiments have been done to analyze the accuracy and limitation of the algorithm.

In addition, this research also provides the following contributions:

i. Comprehensive evaluation of the developed protocol with prediction algorithm in terms of a specific set of performance metrics.

ii. Modification of the standard implementation of AODV in simulator ns-2 and derivation of a new routing protocol with integration of the link state prediction and developed new models of AODV routing protocol in link failure mechanism such as Detection Model, New Path-Mode and Upstream Notification (UN) Model.

iii. Comparison of the developed protocol to standard AODV protocol and four models of current related works as well.

1.8.3 Implementation of the Developed Protocol

The developed protocol has been implemented in Network Simulator 2 (ns-2). Simulations were performed to verify and validate the result of the developed protocol.

The results obtained from the simulation's experiment have shown that the developed protocol maintenance can significantly reduce total number of dropped packets as a result of link breakage reduction by the newly developed routing protocol. All results show that the developed protocol outperform AODV Protocol. For instance, PDFRP outperform AODV with 21.40%,23.26%, 30.99%,28.10% and 29.65% in terms of throughput whereas 32.63% shows that PDFRP is better than AODV in terms of Routing Overhead which indicates that the developed routing protocol comes up with a mechanism with less control messages than standard AODV protocol**.**

1.9 Organization of the Thesis

The research is organized into Eight chapters as follows:

Chapter One starts with an introduction to mobile ad-hoc network where it provides general background information of MANET with different technologies as well as different protocols used for MANET. The chapter also outlines the research motivation, problem statement, objectives of the research and scope. Finally, it presents the research steps and contributions.

Chapter Two discusses relevant literature review to the subject and framework of the research providing the in-depth background information on the development of MANET, especially ad-hoc routing protocols. In addition, the chapter outlines the overview of mobile ad-hoc network where it discusses significance of ad-hoc network communication in terms of minimizing infrastructure, MANET's features and its applications. The chapter discussed ad-hoc routing protocols illustrating different routing protocols such as Flat routing protocols, Hierarchical routing protocol and Geographical routing protocol. It presents how the AODV protocol processes the route discovery procedure such as route request broadcasting, route error message and route reply method. The chapter discusses different methods of predictive mechanisms and approaches that focus on enhancing link failure on AODV protocol. It also demonstrates different categories of mobility models such as cellular network's mobility models and ad-hoc network's mobility models.

Chapter Three introduces the methodology of the developed protocol, namely Predictive Divert Failure Route Protocol (PDFRP). The chapter illustrates the evaluation steps where it defines the details of the goals and objectives of the study. Furthermore, the chapter discusses the design of the research methodology, presenting methods and tools to improve the stages of the research correlation in a design. It highlights different simulations and their reliabilities, discussing the three most widely used simulations. Subsequently, the chapter deals with simulation setup followed by generating node mobility, data traffic and transport protocol that are used in this research.

Chapter Four presents empirical experiments of AODV protocol and mobility models for optimal setting experiments. Prior to implementing the developed protocol, studying the current behavior of AODV protocol with two different mobility models. Finally, the chapter also presents a series of experiments and examined different factors with different parameters, which can influence the performance of the protocol.

Chapter Five demonstrates the design of the developed protocol. Subsequently, the chapter gives the underlying philosophy of this research where it provides steps and details of the research design. Moreover, the chapter deals with design for the developed protocol on link failure and demonstrates the mechanisms that the developed protocol comes up with and explains how the network behaves when the link is about to be broken. In addition, the chapter explains in depth the models' design that the research has come up with, where it draws on three main models such as Detection Model, Analyzer Algorithm and New Path-Model. Finally, the chapter demonstrates link predication and its validation where it introduced the mathematical analysis through link state prediction to calculate the distance between two nodes.

Chapter Six introduces implementation of the research. The chapter gives an analysis on the simulated data as well as discussion on experiments carried out to evaluate the developed protocol. It illustrates PDFRP prediction concepts where it explains how the PDFRP main prediction concept can be implemented in simulation environments. It discusses how it is necessary to be cautious regarding ad-hoc exclusive attribute when implementing the protocol. Finally, it presents the configuration and parameters setting of PDFRP as well as the validation and verification of the developed protocol.

Chapter Seven discusses the simulation results and provides performance analysis. The chapter provides detailed performance comparison of PDFRP protocol to AODV standard algorithm based on the numerical results obtained from simulations as well as comparing the results with 4 models of current works. The chapter examines the PDFRP protocol with the different simulation scenarios with respect to varying node density, pause time and node speed.

Chapter Eight draws conclusion and recommendations based on findings of the research and summarizes the work presented in this research where it highlights the significance of the contributions made and discusses directions for future work.

CHAPTER TWO

LITERATURE REVIEW

Chapter One discusses the introduction of the thesis where it provides the general background information of Mobile Ad-hoc Network (MANET). This chapter presents relevant literature review to the topic of the research that defines the general framework of this research. The chapter provides the background information on the development of MANET in general as well as in-depth of ad-hoc routing protocols. It outlines the overview of mobile ad-hoc network where it discusses significance of ad-hoc network communication and MANET's features as well as its applications. Section 2.1 draws on the importance of MANET where it discusses the features of ad-hoc network communication in terms of minimizing infrastructure and economic perspective as well. Section 2.2 discusses ad-hoc routing protocols in general and different types of routing protocols. Link prediction mechanism and its calculation of the distance between two nodes is discussed in Section 2.3. Section 2.4 discusses current mechanisms to improve link failure on Ad-hoc On-Demand Distance Vector (AODV) protocol. The reflection of PDFRP and current mechanisms is illustrated in Section 2.5. Finally, mobility models for mobile wireless where it categories into two parts such as cellular wireless network's mobility models and for ad-hoc networks mobility models are presented in Section 2.6.

2.1 Importance of Mobile Ad-hoc Network

Ad-hoc network is decentralized network infrastructure which suitable for a variety of applications where central nodes cannot be relied on and it improves the scalability of current infrastructure wireless communication. However, ad-hoc network has become a very important communication in terms of minimal configuration, quick deployment and suitability for emergency situations like natural disasters and military conflicts as well. The purpose of ad-hoc network is the need to exchange digital information outside the typical wired in office environment. For instance, in a typical ad-hoc network, mobile nodes come together and each of the devices used by these information producers and consumers can be considered a node in an ad-hoc network. The most importance of this type of communication is that the information exchanging between network nodes is continue, while the nodes may continue to move different or same directions.

2.1.1 Mobile Ad-hoc Network Features

Mobile ad-hoc network has the following features as stated in [23].

i. *Autonomous Terminal:* Each mobile terminal in the mobile ad-hoc network presents an autonomous node, which can function either as host or router. On the other hand, besides the essential processing ability as a host, the mobile node in MANET can also act as a router.

ii. *Distributed Operation:* Since every mobile node in MANET does not rely on any base station, the control and management of the network are distributed among the terminals. All the mobile nodes in MANET should collaborate with each other in order to implement the main functions such as routing and security.

iii. *Multihop Routing:* In MANET, the routing algorithm can be classified into single hop and multihop. In case of the single hop, two mobile nodes communicate with each other directly, while for multihop, the mobile nodes communicate through intermediate nodes. Single hop routing is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When the link between two mobile nodes failed, the data packets will be forwarded through one or more intermediate nodes.

iv. *Dynamic Network Topologies:* Since the network topology of mobile ad-hoc network may change rapidly and unpredictably, the mobile nodes should adapt to the heavy traffic and congestion condition as well as the mobility patterns of the network. All the mobile nodes in the dynamic network establish routing by themselves as they are moving from one place to another place based on their movement.

v. *Light-weight Terminals:* Generally, mobile nodes in MANET need for an optimized algorithm and some mechanisms that can implement the computing and communicating function because the mobile devices normally have a small size memory, low power storage and less CPU processing capability.

2.1.2 Mobile Ad-hoc Network Applications

Development of MANET is very fast with the increasing number of extensive applications. Ad-hoc networks can be applied anytime and anywhere, where there is no infrastructure network or the high cost of infrastructure network. The basic idea of using mobile ad-hoc network is to allow the mobile devices to maintain the connections between the devices easily such as adding and removing devices from the network to transfer the data packet between the source node and destination node. The mobile ad-hoc network applications varied from large mobility- highly dynamic networks into small mobility- static networks that are controlled by power sources. The typical mobile ad-hoc network applications are as follows:

i. *Military Battlefield:* The military application is the basic technique of ad-hoc network, which contains some sort of computer equipment. In military application, the routing information is sent between the soldiers, vehicles, and military information.

ii. *Commercial Sector:* MANET uses the commercial sector with different applications' scenario such as during an emergency rescue operations for disaster relief where there is no existing infrastructure network available.

In such areas, the information can be relayed from one rescue panel part to another over a small handheld. There are other scenarios applied in the commercial sector such as ship-to- ship mobile ad-hoc network communication, law enforcement, etc. In the local level applications, mobile ad-hoc network can be separately linked to direct and temporary multimedia network using a notebook laptop in order to increase and locate information among participants at a conference or in a classroom. Another scenario is when the local level application is used in the home network where all the devices can be communicating with each other directly to exchange the information. Furthermore, the applications can be used in civilian environments like taxicabs, sports stadium, boats and small aircrafts. Personal Area Network (PAN), MANET can make the inter-communication between different mobile devices such as Personal Digital Assistant (PDA), laptop, and cellular phone simpler.

All the mobile devices in wireless ad-hoc network can be exchanged with wired cable connections. Moreover, mobile ad-hoc network can access the internet by using such as Wireless Local Area Network (WLAN), General Packet Radio Service (GPRS), and Universal Mobile Telecommunications System (UMTS). PAN is a capable application field for MANET in the future pervasive computing context. The main area that most of the researchers had emphasized on developing in ad-hoc is routing protocols. In this research, routing protocol of the mobile ad-hoc network will be emphasized in the next section.

2.2 Ad-hoc Routing Protocols in General

Generally, routing is the process of exchanging the information between a source node and destination node in the network as described by Bakht [24]. The main function of ad-hoc routing is to discover and establish a route between the pair of mobile nodes so that data packet is delivered to the destination on time using the most efficient path. Efficiency of the path is measured in various metrics like, number of hops, traffic, security, etc. Each mobile node in MANET acts as a specialized router itself. Due to the limited and shared resources in MANET, several routing protocols have been developed or proposed in order to adapt to the nature changes of wireless network such as nodes that are mobile hosts, routes that change frequently, and topology unpredictable. According to Abolhasan et al. [25], routing protocols can be classified into three different categories as shown in Figure 2.1.

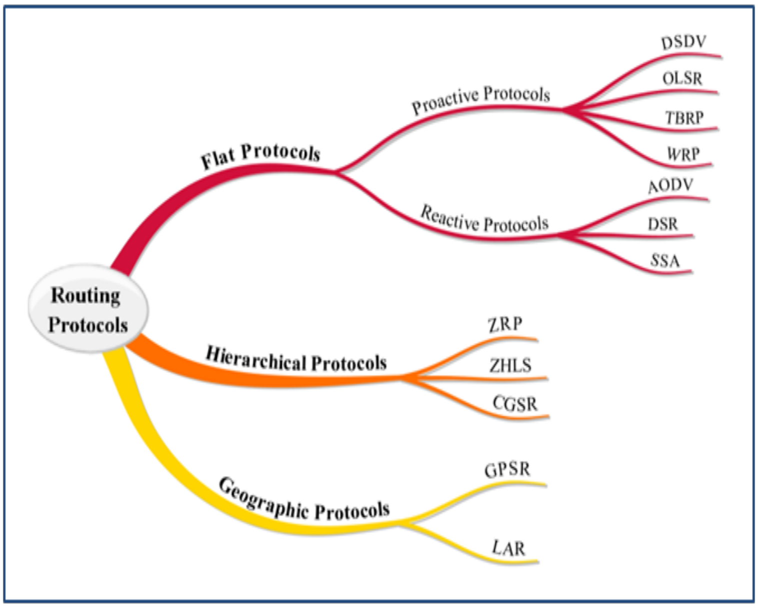


Figure 2.1: Classification of Ad-hoc Routing Protocols

Routing protocols have some difficulties during establishing the routes between the source node and destination node through intermediate node, which are as follows:

i. Limited connectivity due to transmission range of signal.

ii. Low bandwidth.

iii. Higher error rates.

iv. Vulnerable to interference.

v. Power Consumption.

vi. No specific devices to do routing.

vii. Dynamic nature - high mobility and frequent topological changes.

The following sub-sections will elaborate flat and hierarchical architecture.

2.2.1 Flat vs. Hierarchical Architecture

Hierarchical routing protocols have been developed to resolve the scalability problem of large networks as mentioned in [25]. The hierarchical network is divided into groups and at the same time a subset of nodes act as a relay-node and assigned special functionalities, and they work like a coordinator. Hierarchical network architecture topology consists of multiple layers where the top layers are more seen as the master of their lower layer nodes. There are clusters of the nodes and one gateway node among all clusters has a duty to communicate with the gateway node in another cluster in order to transfer the control messages. In this approach, the storage of network topology is based on gateway nodes, where communicating a different control message is dependent on cluster nodes as shown in Figure 2.2.

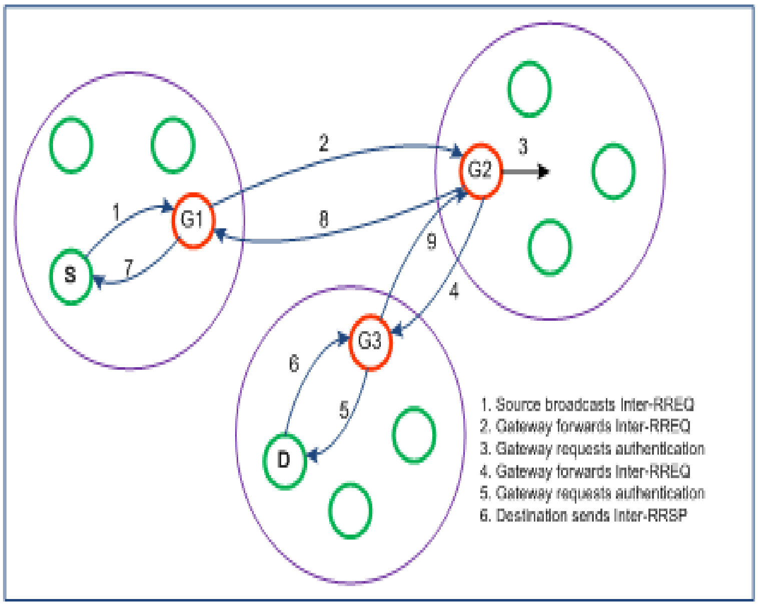


Figure 2.2: Hierarchical Architecture (Adapted from [25])

However, this architecture can be broken down when there is a single node failure (Gateway node). Gateway nodes become very critical for the successful operation of network. Examples include Zone-based Hierarchical Link State (ZHLS) routing protocol [25], where in flat architecture, there is no layering of responsibility. Each mobile node does follow the same routing algorithm as any other node in the network.

2.2.2 Proactive Unicast Routing Protocols

The proactive routing approach is also called “Table Driven” protocol. In this approach, the route is always available before sending data packets from the source to the destination. Every node updates and maintains complete routing information of the network. The routes to all destinations are calculated, and link state are maintained in node’s routing tables to compute routes in advance. All the nodes must keep the information up to date, in order to update their information periodically. The main advantage of proactive routing is when a source needs to send packets to a destination, the route is already available. On the other hand, there is no latency which can force the packet drop. The disadvantages of proactive routing approach are some routes may never be used and dissemination of routing information will consume a lot of the scarce wireless network bandwidth when the link state and network topology change fast. Examples of proactive routing protocols are: Destination Sequenced Distance Vector Routing (DSDV) as written by Perkins and Bhagwa [26]. Optimized Link State Routing Protocol Architecture (OLSR) [27], and Wireless Routing Protocol (WRP) [28].

2.2.3 Reactive Routing Protocols

Every node in the reactive routing approach maintains routing information of only active paths to the destination nodes. A route search is needed for every new destination. Therefore, the communication overhead is reduced at the expense of delay in searching the route. Rapidly changing wireless network topology may break active route and cause subsequent route search. Demand routing takes a different approach for routing than table driven protocols such as Temporally Ordered Routing Algorithm (TORA) [29], AODV [30], and DSR [31]. The routes to the destination are discovered only when actually needed. When a source node wants to send data packets to the destination, first it checks the routing table to determine whether it has a route to the destination. If there is no route, source node starts route discovery procedure in order to find a path to the destination. Reactive routing protocols are based on Distance-Vector concept (DV), which can significantly decrease routing overhead and power consumption, because on demand routing does not need to keep searching and maintaining the routes on which there is no data traffic to send as stated in [32].

For the reason mentioned earlier, proactive routing protocols may not perform efficiently due to their periodic messages for updating the routing information in the routing table. As alternative, reactive routing protocols have mostly been used in ad-hoc network research, reactive protocols can create a route to the destination and maintain it during data transmissions. Consequently, routes are not sensitive to the topology changes.

The works in [33, 34, 35, 36, 37] have evaluated the comparison of proactive and reactive with multi-hop routing protocols namely DSDV, TORA, DSR, ABR, and AODV. Through their simulation results, it has been observed that, the reactive protocols outperform proactive protocols in terms of a packet delivery ratio, routing overhead, energy efficiency and stability. Therefore, our research mainly focuses on reactive protocols. In reactive approach, when the existing route between two nodes is disconnected frequently and arbitrarily due to shifting of nodes out of the transmission range or node mobility, source node has to establish a new route. The route discovery time can be a vital factor affecting the network performance, because of the route discovery process under on demand routing approach based on broadcasting route request packet from source node. It takes considerable time to recover the whole route. The recovery of route failure is as critical as route establishment in mobile ad-hoc routing protocols.

The difference between a proactive approach and reactive approach is shown in Table 2.1.

Table 2.1: Overall Comparisons of Reactive vs. Proactive Routing Protocols

Parameters	Reactive Protocols	Proactive Protocols
Availability of routing information	Available when needed	Always available regardless of need
Routing Structure	Mostly Flat	Flat and hierarchical structure
Periodic route updates	Not required	Required
Scalability	Up to few hundred nodes depend on (traffic level, number of hops)	Up to hundred nodes
Mobility Handling	Route maintenance	Periodical updates
Communication overhead	Low	High
Signaling traffic generated	Grows with increasing mobility of active routes (as in ABR)	Greater than that on-demand routing
Quality of service support	Few can support QoS, although most support shortest path	Mainly shortest path as the QoS metric

In the next sub-section, the most common reactive routing protocols are presented.

2.2.3.1 Temporally Ordered Routing Algorithm (TORA)

TORA is reactive ad-hoc routing protocol proposed by Park et al. [38]. TORA is based on the concept of the link reversal of the Directed Acyclic Graph (DAG). TORA has the aspect of being highly adaptive and changes rapidly for route repair during link failure. These aspects make the TORA protocol suitable for a large network that is highly dynamic with dense node populations. According to Park et al. [38], TORA's reliance on synchronized clocks is important to accomplish via Global Position System (GPS) or Network Time Protocol algorithm. However, TORA protocol does not perform well if the node does not have a GPS or some external time source, or if the time source fails leading the algorithm to fail as well, because the link reversal process fails in the routing maintenance.

TORA protocol has three important mechanisms: Route Creation, Route Maintenance, and Route Erasure. The source node broadcasts a query packet (QRY) with the destination identification. Any node with a non-null height responds with an update packet (UPD) that informs its own height metric. The receiving node defines its height metric incrementing the one informed in the update packet. This process concludes with the creation of a directed acyclic graph. By following the relative height metric, possible routes can be created for any desired source/destination pair. In TORA, upon link failure of its last route to a destination, the node updates its reference level and propagates the new reference level to all neighbors. As a consequence, nodes near topological changes update their routes for adapting to such as reference level. In order to erase invalid routes, nodes flood a broadcast clear packet (CLR) overall in the network.

2.2.3.2 Dynamic Source Routing Protocol (DSR)

DSR is reactive and multihop routing protocol proposed by Johnson et al. [39]. DSR protocol has two main mechanisms, namely Route discovery, to discover the route before the source node sends data packets to the destination and route maintenance to maintain the route when a link between two nodes is broken. DSR protocol is based on the concept of source routing in which the source node knows the complete path to the destination. The intermediate nodes do not need to maintain the routing information in their route cache; all the nodes maintain a route cache that contains previously identified routes.

The main goal of using route cache in DSR protocol is to store the routes which have learned from the route discovery and to speed up the route discovery process during establishing the routes. When the source node wants to send data packets to the destination and does not have a route to the particular destination, the source node will first broadcast a Route Request Packet (RREQ) to its neighbors. The request packet contains source address, destination address, request packet ID, and route record. After intermediate nodes receive the request packet, the source node will go forward to the next hop until it reaches to the destination node. After reaching the destination node with valid route in its cache, Route Reply Packet (RREP) will be generated in the reverse path from the destination node to the source node containing the route record indentified in the route request. DSR protocol can be adopted in networks that support symmetric and asymmetric links.

The main concern of using symmetric links in DSR protocol is that, Route Reply Packets are always generated via reverse routes, which are the inverse of the routes indicated in request packets. As a consequence, Route Request Packet and Route Reply Packets establish routes in both directions. If asymmetric links exist, in order to send reply packets, mobile nodes can use any available valid route or activate a new discovery process, whereby that request packet piggybacks the reply packet. The route maintenance process in DSR protocol normally is based on monitoring all links along the routes which adopt the passive acknowledgement process. Every mobile node hears the neighbor node along the route forwarding the packet. If the mobile node does not hear such a retransmission within a specific time, it is considered as link failure which can generate a route error packet (RRER) to the source node, indicating that the route is invalid. DSR protocol can also maintain multiple routes to each destination.

2.2.3.3 Ad-hoc On-Demand Distance Vector Routing Protocol (AODV)

AODV is on-demand routing protocol developed by Perkins et al. [40] whereby all network routing information is only transmitted by mobile nodes on-demand. AODV protocol is based on DSDV protocol, and it is designed for network characterized by frequent topology changes in link connectivity. According Gupta and Saket [41], AODV is suited for MANET communication as it has low processing and memory overhead. It reduces overall network resource utilization as AODV uses loop freedom as well as sequence number mechanism for all routes. In addition, according Lee et al. [42], AODV has high scalability compared to other reactive routing protocols and AODV has an ability for quick adaptation to dynamic link environments. There are two major operation phases for AODV, namely Route Discovery and Route Maintenance operations, which are described below.

i. *Route Discovery Process:* When a source node wants to communicate with an unconnected destination node, first it has to discover a route to that particular destination in order to deliver data packets. The source node broadcasts a Route Request Packet (RREQ) to its neighbors with the RREQ message containing the source address, destination address, and unique ID to distinguish the route request. After a Route Request Packet reaches the intermediate nodes from its predecessor, the intermediate nodes will store the address of the predecessor as part of the process for building the reverse path toward to the source node, checking whether there is a route to the destination. If there is a route from the intermediate node to the destination node, the destination node will unicast Route Reply Packet (RREP) to the source node through predecessor node via the reverse path. Otherwise, the intermediate node re-forward the RREQ to their neighbors. At the same time of generation a RREQ, one of the intermediate nodes (or the destination) will unicast a Route Replay Packet back to the source node, including the complete path to the destination node. The main use of unique RREQ ID is to remove any of duplicated RREQs in the routing table of each mobile node.

ii. *Route Maintenance Process:* Route maintenance process maintains the route when the link between two mobile nodes is broken. Each mobile node in AODV protocol monitors its link to the next hop for any failure. Link failure can be detected when consecutive HELLO messages are sent periodically by the next node, or when the MAC layer fails to send data packets to the next hop. Route Error Packet (RRER) will be generated by the detected node and sends this error message to the upstream nodes towards the source node. Once the source node receives the RERR message, it starts again a new route discovery process which can cause delay and waste network resources. On the other hand, Goff et al. [43] proposed a local repair mechanism to solve link failure, which can be carried out instead of sending a RERR message to the upstream nodes. The local repair process starts at a detected node which detected the link failure by broadcasting a RREQ message to find an alternative route. If there is no route available, the detected node sends a RRER message to upstream nodes towards the source node, then the source node starts a new route discovery. However, the local repair mechanism in AODV protocol is suitable for situations where link failure occurs near to the destination node. AODV Packet information parameters are stated in Table 2.2.

Table 2.2: AODV RREQ Packet Parameters

Packet Parameters
Destination IP Address
Prefix Size
Destination Sequence Number
Next Hop IP Address
Lifetime (expiration or deletion time of the route)
Hop Count (number of hops to reach the destination)
Network Interface
Other state and routing flags (e.g., valid, invalid)

The key operations of AODV are mainly:

i. *Route Requests (RREQs)*: The source node needs to send a packet to a destination node for which it has no routing information in its table.

ii. *Route Replies (RREPs):* A node receiving the RREQ propagates RREP back to the source if it is either the destination or has a route to the destination.

iii. *Route Errors (RERRs):* When a node detects a link breakage for the next hop of an active route in its routing table, it will bring down this route, and initiate a RERR.

Figures below show the major architecture for how AODV protocol operates in terms of route discovery and route maintenance. Figure 2.3 illustrates ad-hoc network architecture that S-Source node wishes to communicate to D-destination node [44].

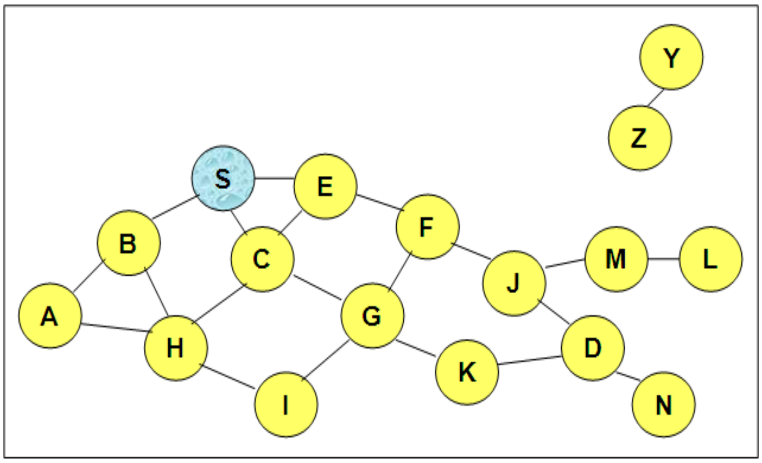


Figure 2.3: Node S Wishes to Communicate with Node D (Adapted from [44])

In Figure 2.4, the node S broadcasts enquiry in order to get a route to node D. The packet generated by node S contains: (1) node D destination address, (2) sequence number and (3) packet ID, which are then broadcasted to the neighbors.

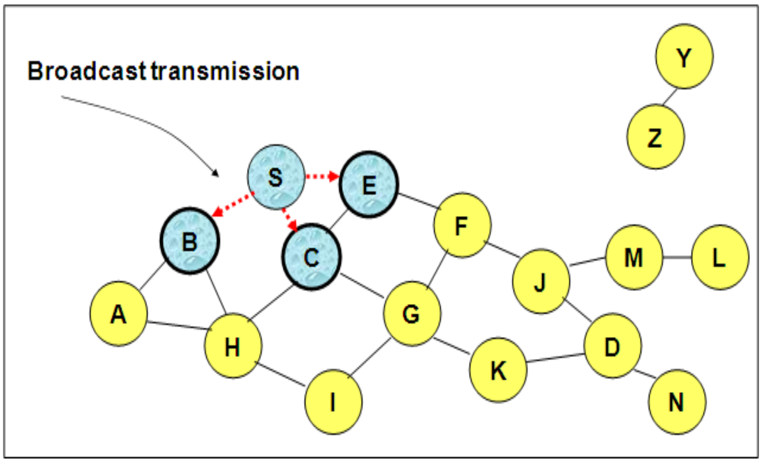


Figure 2.4: AODV Route Broadcasting Architecture (Adapted from [44])

Figure 2.5 shows when the neighbors receive the request from node S, they generate the forward path to the source node S.

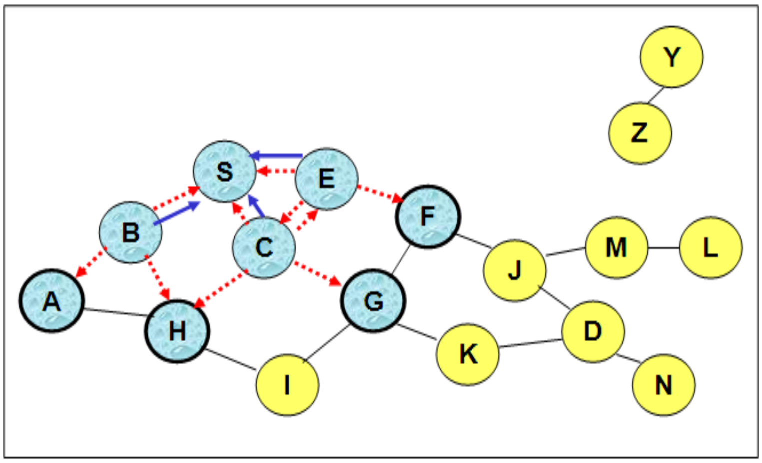


Figure 2.5: Generating a Reverse Path by Neighbors (Adapted from [44])

Figure 2.6 shows the route between the source node S and destination node D can be determined by Route Reply from destination D to the source node S.

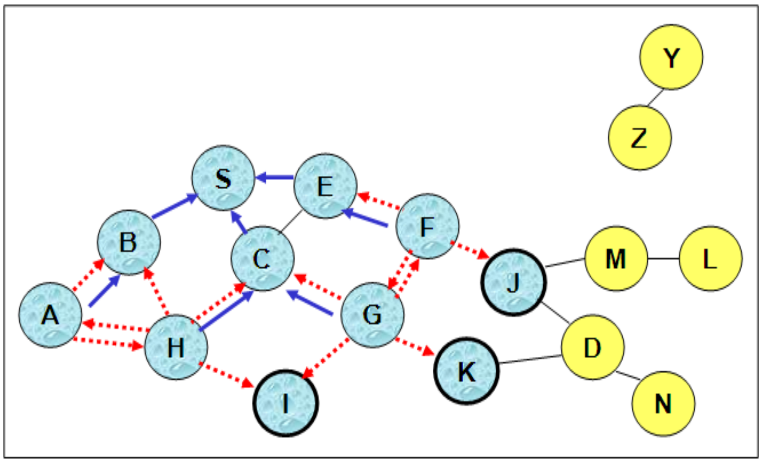


Figure 2.6: The Route Between Node S and Node D is Determined (Adapted from [44])

Figure 2.7 shows the communication between the source node S and destination node D is established.

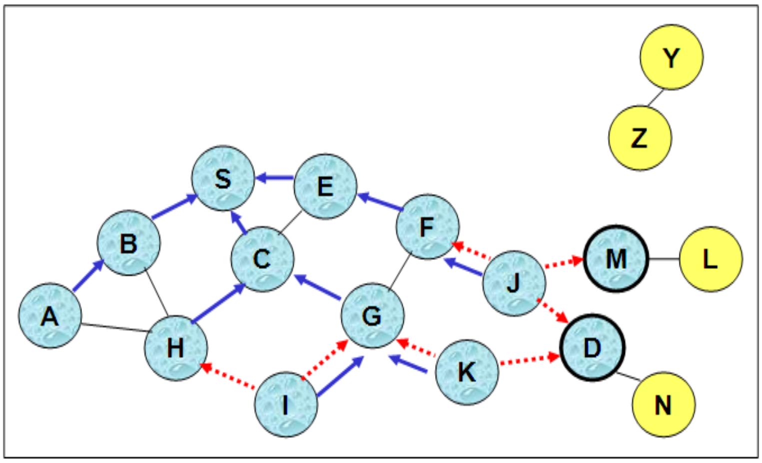


Figure 2.7: The Route Between Node S and Node D is Found (Adapted from [44])

Figure 2.8 shows the reverse path from the destination node D to the source node S.

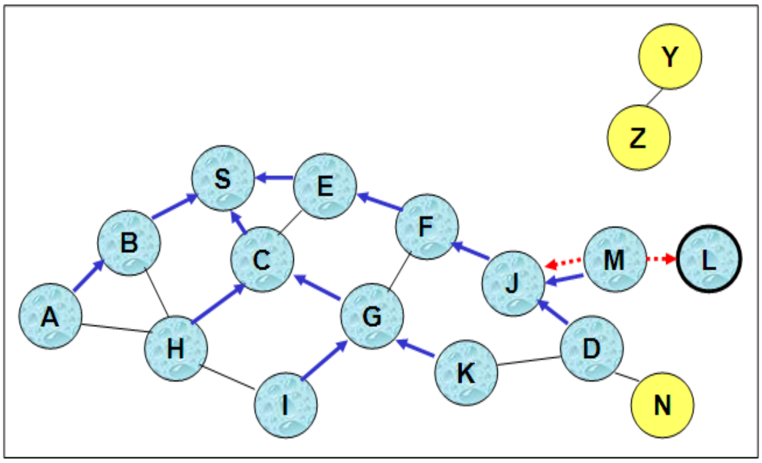


Figure 2.8: Reverse Path Setup in AODV (Adapted from [44])

Figure 2.9 shows the Route Reply Packet (RREP) from the destination node D to the source node S. To determine whether the path is known to an intermediate node is more recent, destination sequence numbers are used.

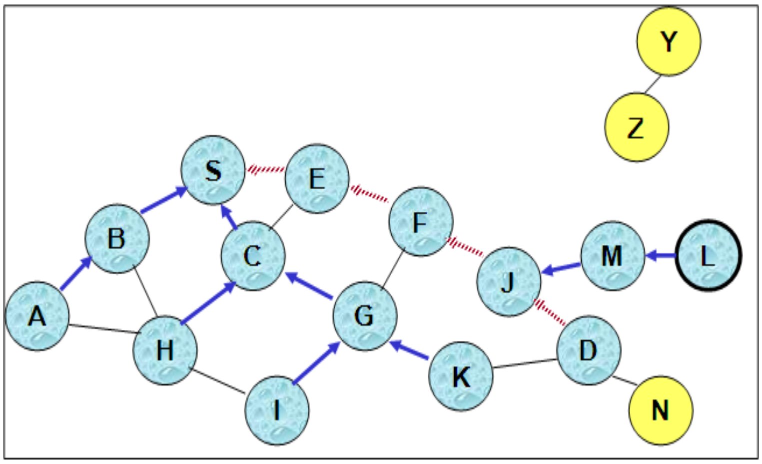


Figure 2.9: Route Reply (RREP) in AODV (Adapted from [44])

Figure 2.10 shows the forward links which are set up when the Route Reply Packet (RREP) travels along the reverse path (D-J-F-E-S).

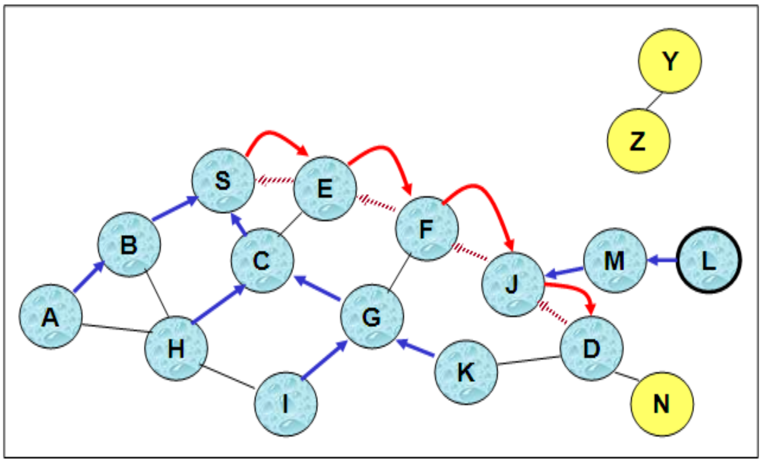


Figure 2.10: Forward Path Setup in AODV (Adapted from [44])

Figure 2.11 shows the data transmission from the source node S to the destination node D through the path (S-E-F-J-D).

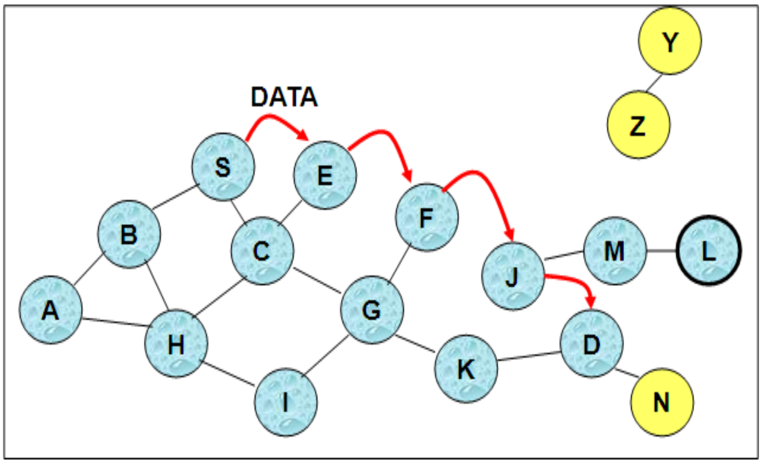


Figure 2.11: Data Delivery in AODV (Adapted from [44])

Figure 2.12 shows what happens in case a link between two hops is broken. The broken link is no more a valid route, and a RERR message is sent to other nodes. In this respect, S resends, another route requests to his neighbor nodes unless one of the nodes solves the problem on the way to the destination through local route repair as written by Perkins et al. [40].

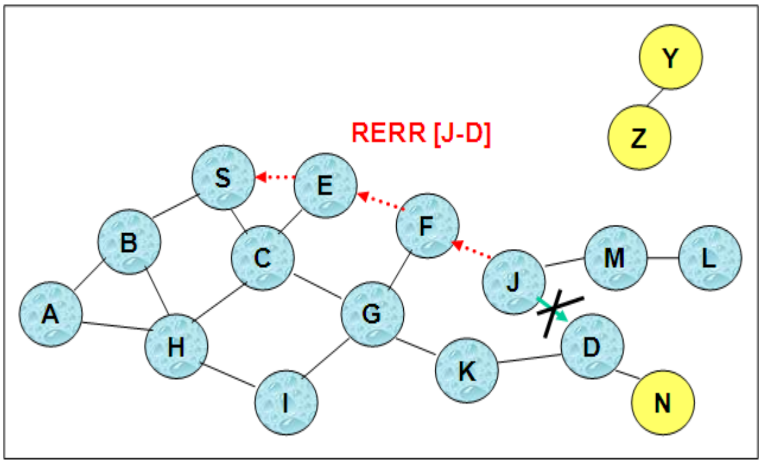


Figure 2.12: Link Break in Active Route (Adapted from [44])

The flow chart in Figure 2.13 shows the route discovery and maintenance procedures of AODV protocol where it summarizes the AODV route discovering process. AODV has two routing tables to store routing information (one for uncast and another one is for multicast). As stated in Table 2.2, these tables keep information such as destination address, next-hop address, hop count, destination sequence number, network interface, and life time as stated in [45]. In AODV routing protocol, four main messages are important for both route discovery and route maintenance, namely, RREQ, RREP, RERR and HELLO messages. The RREQ and RREP messages are used for route discovery, whereas the RERR and HELLO messages are used for route maintenance. The following flow chart (Figure 2.13) illustrates the basic AODV routing protocol route discovery.

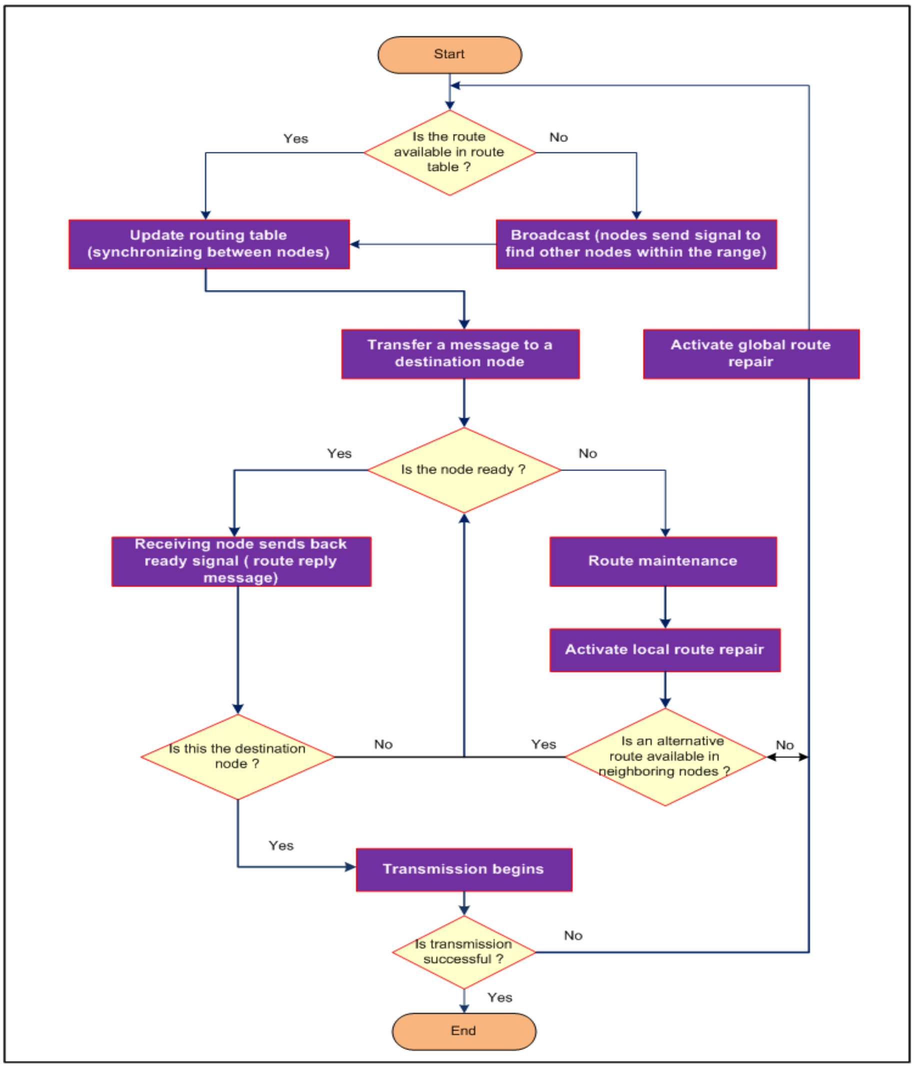


Figure 2.13: Route Discovery and Maintenance of AODV Protocol (Adapted from [45])

2.3 Link Prediction

Link prediction mechanism will be used in this research in order to calculate the distance between two nodes and link connection remaining time. It uses computation of relative movements between two mobile nodes and assumes that the nodes move with constant speeds and directions [46]. The parameters speed, direction, and positions (location) are important to calculate and predict the signal power. There are three main prediction methods in order to estimate (to predict) the link status for the near future:

i. *Signal strength based methods:* Signal strength based method: As stated in [47, 48, 49, 50], this method predicts the link breakage based on received signal strength from the upstream node. In this respect, each and every signal power is registered, then compared with a predefined threshold value. If the received signal strength is less than the threshold value, then it considers that this link will be broken soon. Each and every above mentioned method is suitable for certain environment. For instance, the signal strength method has good performance in any environment, including urban environments.

ii. *Beacon packet based methods:* The Beacon packet base method: This is another mobility prediction method. Each node broadcasts a hello packet to its one hop neighbors and it introduces itself to them and knows them. Beacon also uses signal strength method in order to check wether a signal status is of less value than the predefined threshold or not. However, this method suffers from stale routes as indicated in [51].

iii. *Position information based methods:* Positioning information based methods: This method also depends on receiving signal, in order to take action. When a node receives a packet, this packet computes its distance from the previous node. If this distance becomes larger than the allowable threshold then it considers the link between them will break soon. This method needs a positioning system like Global Positioning System (GPS) in order to estimate two consecutive nodes distance. This method is suitable only for open areas such as urban and similar environments where the estimate is not too precise, so the nodes may fail in their prediction process [52]. However, it seems that the signal strength based method is more suitable than the two other methods in terms of suitability of urban areas as well as power consumption. Thus, this research utilizes the first method (signal strength based method). Normally, these parameters (speed, direction and position) provide the Global Positioning System (GPS) [53]. But, since the GPS is not available in some places and for certain mobile device, the distance of nodes can be obtained by measuring the received signal powers.

2.4 Current Mechanisms to Improve Link Failure on AODV Protocol

When a mobile node moves from one place to another, it can change the topology of the network rapidly because of mobility network, which can cause link failure during data transmission from the source node to the destination node. The lost connectivity is a major negative impact on the overall network in terms of packet delivery ratio, packet drop, and delay. Specifically, when the detected node in AODV protocol could not find an alternative route in the routing table, it sends a RERR message to the source node which leads to re-initiating route discovery process. Because of the time elapsed between link failure discovery, alternative path connection can be high.

Therefore, several mechanisms and approaches have been focused on enhancing link failure that is related to AODV protocol. Discussion in the next sub-section, will be on the techniques and the drawback of each mechanism in order to design a new and better mechanism that can solve link failure which leads to saving the overall network resources.

2.4.1 A Preemptive on-Demand Distance Vector Routing Protocol

Boukerche and Zhang [54] proposed A Preemptive On-demand Distance Vector Routing Protocol for Mobile and Wireless Ad-hoc Networks. This is an extension to the AODV which is called P_r AODV protocol. This new extension mechanism consists of propagating the route state information which is used if the path is going to break soon. Knowing that the path will be broken soon, the preemptive mechanism finds a new path before the current path is disconnected in order to switch the data into the new path. The drawback of this approach is that the new path is created by the source where a global route rediscovery will be generated from the source whenever suspicion of route state information is received by source. In addition, initiating false warning message due to fading signal fluctuation must to be taken into consideration which loads more overhead to the network.

2.4.2 Preemptive Multicast Routing in Mobile Ad-hoc Networks

Xiong et al. [55] proposed Preemptive Multicast Routing in Mobile Ad-hoc Networks. This mechanism is similar to preemptive routing for unicast where it is also applied to multicast which is called Preemptive Multicast Routing (PMR). PMR is an extension of On-Demand Multicast Routing Protocol (ODMRP). The main idea to develop PMR is to extend the route refreshment interval mechanism that is used in ODMRP and extended the time refreshment interval from 3 seconds (where ODMRP is used) to 60 seconds. The main drawback of the route refreshment interval mechanism is control overhead caused by the flooding of route refreshment control packets to keep routes up-to-date. These flooding messages might reduce the utilization of the network bandwidth, which is expensive in a wireless environment, and causes collisions, congestion and delay due to channel contention.

2.4.3 A Preemptive Route Repair Strategy with Router Handoff for AODV Protocol

Srinath et al. [56] proposed a Preemptive Route Repair Strategy with Router Handoff for AODV protocol in order to enhance the route maintenance process. To combine a router handoff to AODV protocol, three changes have been made. First, each mobile node maintains a Neighbor Power List (NPL) that contains a table which has the last received signal strength for packets initiated from the neighbor nodes. Second, each mobile node also maintains a Power Difference Table (PDT) in which contains a table that has the rate of the power changing between a pair of the neighbor nodes. Third, each mobile node contains Hello packets, which are modified to have the neighbors' power information. The purpose of using Hello packet is when the Hello packets are sent out; each node examines its NPL and PDT in order to find neighbors with whom it has a strong link to forward the packets to the destination node.

For instance, if a current node, say A (where the link failure is happening) detects that the link to the next node, say B, is going to be broken soon by using signal power strength, it searches its Power Difference Table (PDT) in order to find another node, say C, that can connect predecessor node, say D, to the next node, say F, with a good link strength. In case a node C is found, then the current node A broadcasts a handoff message which contains the address of node C, route destination B , and node D with TTL=1. Consequently, node D will change its next node A to the new next node C. In this aspect, node C will update its routing table if required, with the information in the handoff message. The main concern of this approach is each mobile node will update its neighbor routing table using periodically broadcasted HELLO messages. However, frequently broadcasting of Hello message introduces more overhead to the network and also limits the overall network resource utilization (bandwidth).

2.4.4 Preemptive Routing Algorithm

Goff et al. [57] proposed a preemptive routing algorithm. The preemptive routing approach is based on the prediction algorithm in order to predict the link in advance before a breakdown. When the intermediate node discovers that the neighboring link is going to fail and the received packet power is weak, it sends a warning message back to the source node asking it to find an alternative route. Upon receiving the warning message from the intermediate node, the source node sends a route request (RR) message in order to find a new path. The main weakness of such a preemptive algorithm is the cost of overhead to be encountered upon false warning messages because whenever a path is assumed to be broken, this method can flood the route request packets to the whole the network, which might increase the overhead. Another weakness which conveys more overhead to the networks is ping-pong technique.

In this respect, when a node receives signal strength which is lower than predefined threshold value, the node starts pinging to the adjacent node to inform that it received a lower signal value than the threshold. So, when the adjacent node receives the ping packet, it responds with a pong packet. When the original node receives the pong from the adjacent node, it pings the adjacent node again and receives pong again. However, the number of such ping-pong responds is monitored for a while in below in order to observe whether the signal status is maintained or declined. This mechanism has three main disadvantages, (1) there is no condition to find a new route within intermediate node, (2) keeping longer ping-pong messages exchanges make tremendous network overhead and unnecessary traffic congestion and, (3) after discovering lower signal strength, global route rediscovery is generated by the source node. Moreover, generating the preemptive warning is very complicated because of the warning message may not trigger only when the signal strength falls below the threshold, but it can also be triggered even sometimes when the real signal power is above the threshold value because of false indication of signal fading caused by signal fluctuation.

2.4.5 Preemptive Route Repair

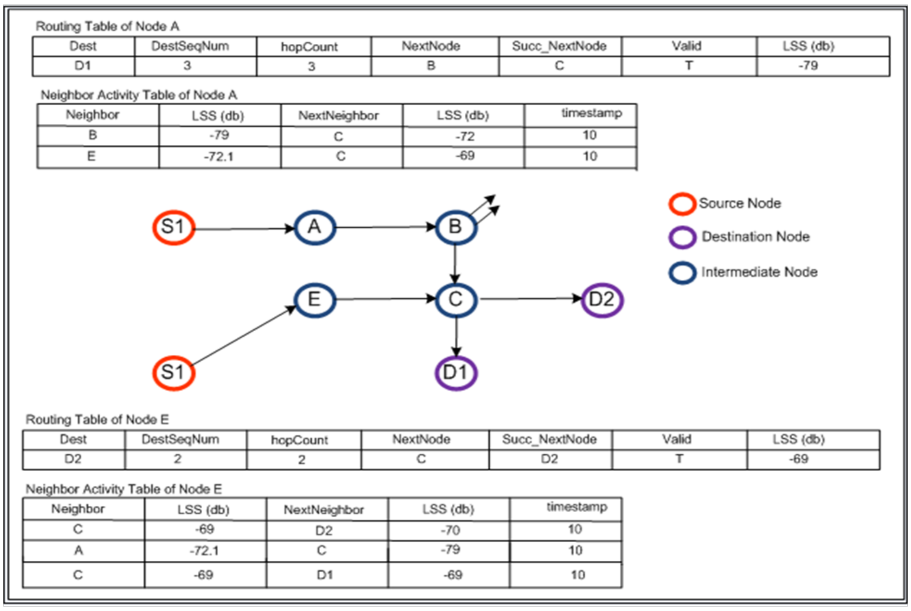
Veeraraghavan and Singh [58] proposed Preemptive Route Repair (PRR) similar to the preemptive route repair strategy with router handoff proposed in [56]. The difference between the above approaches [56] is instead of the HELLO message, the every mobile node maintains the neighbor's routing table, which is constructed during broadcasting of Route Request (RREQ) packet. When a current node discovers that the link between its link and the next node is going to break down soon, it multicasts a Handoff Request (HREQ) to its neighbors. The HREQ contains two field addresses of the next node and all previous nodes which use the failing link. After that, the current node waits for a Handoff Reply (HREP). In case if there is no HREP within a specific time, it sends a warning message to the source node to re-initiate the process of finding a new route by broadcasting Route Request (RREQ) packet. However, by frequent use of broadcasting route request packet and HREQ, it leads to increase of the routing overhead in this protocol through the handoff process.

2.4.6 Preemptive Self Repairing (AODV-PSR)

Preemptive Self Repairing protocol (AODV-PSR) is proposed by Soliman and Otaibi [59] to enhance the route maintenance phase of AODV protocol by using a preemptive approach to detect potential link failure between the mobile nodes and to find an advance alternative route in order to send the data packets to the destination node. Each mobile node in AODV-PSR maintains a Neighbor's Activity Table (NAT), where each entry contains the following fields: the neighbor's address, signal strength, the next node address, the signal strength between the neighbor and its next node, and a time stamp which recorded the last time of the signal that is overhead from that neighbor. By eliminating the use of regular and costly control messages such as route request packet, route reply packet, and route error packet, it leads to reduce the control overhead generated by a route repair process.

To achieve this goal, the Route Update Information (RUI) piggybacks over the traffic of regular data packets to perform the route repair. The RUI contains three fields: next node address, destination sequence number, and the hop count to the destination node. Figure 2.14 shows an example of AODV-PSR protocol where two source nodes (S1 and

S2) transfer data packets into two destination nodes (D1 and D2) through the routes: for (S1, D1), the route is <S1-A-B-C-D1>, and for (S2, D2), the route is <S2-E-C-D2>. When the link between node A and node B is detected to break down soon, node A looks for another route in order to send the data packets via the new route which node A has found, node E in its NAT has the best LSS to node C as shown in Figure 2.14.



Dest	DestSeqNum	hopCount	NextNode	Succ_NextNode	Valid	LSS (db)
D1	3	3	B	C	T	-79

Neighbor	LSS (db)	NextNeighbor	LSS (db)	timestamp
B	-79	C	-72	10
E	-72.1	C	-69	10

Dest	DestSeqNum	hopCount	NextNode	Succ_NextNode	Valid	LSS (db)
D2	2	2	C	D2	T	-69

Neighbor	LSS (db)	NextNeighbor	LSS (db)	timestamp
C	-69	D2	-70	10
A	-72.1	C	-79	10
C	-69	D1	-69	10

Figure 2.14: Before Link A-B Breaks (Adapted from [59])

Figure 2.15 shows the Self-Repair mechanism and how node A constructs a new RUI with node C as the new next node, destination sequence number value of 3, and hop count of 2 to be piggybacked over the D1 with node E as the next node. In this case, node A updates its routing table to D1 with node E as the next node. After the data packet is delivered to the node E, it creates a route entry for destination D1 as shown in Figure 2.15.

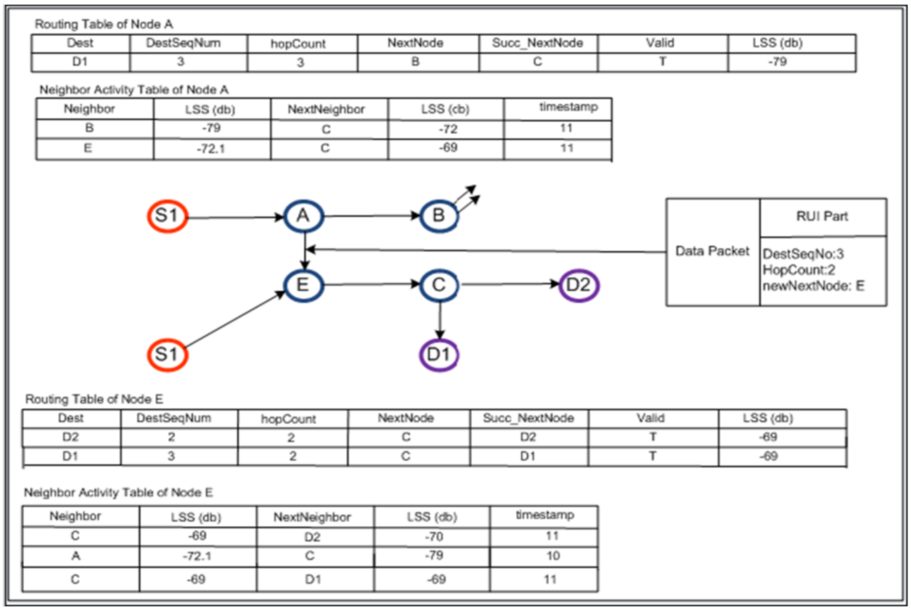


Figure 2.15: Topology after Self-Repair (Adapted from [59])

However, the maintenance of Neighbor's Activity Table (NAT) mainly depends on the nodes of an active route monitoring action of the other active routes. In this respect, it might make AODV-PSR protocol sensitive to the number of conversations. This is especially so for higher loading condition-fewer conversation-pairs, where the NAT table may not be able to settle sufficient other links for future path detouring, which leads to decreasing the performance of AODV-PSR.

2.4.7 Predictive Preemptive Approach

Hacene et al. [60] proposed Predictive Preemptive approach to improve the route maintenance in AODV protocol by avoiding link breakage in advance. The mechanism is started when a link between two mobile nodes is about to be broken instead of waiting for the break to happen. Predictive preemptive approach is used the Lagrange Interpolation Mathematical Model in order to estimate whether an active route to a neighboring node will fail. When the link failure is expected between a node and an upstream neighbor, the upstream neighbor itself attempts, first, to find a route to the destination. If such a route is not found within a discovery period, a link failure warning is propagated via upstream nodes to sources that use this link. Source node invokes the route discovery mechanism if a route to the destination is needed.

This approach has two drawbacks: (i) if the problem has happened at the upstream node and not downstream, it is going to take quite a long process to divert the route and (ii) the mechanism shows that the unnecessary warning message is still sent to the source after a certain period of time which increases the traffic in the network.

In [61], a new flooding mechanism is suggested to control route paths. The main point of the proposed scheme is to track the destination's location based on the beacon messages of the main route nodes by a directional forwarding algorithm. In other words, each node recognizes its location through Global Positioning Systems (GPS) for a one-hop neighbor node, which is at a distance of one hop from the main route, recognizing the location of the main route node through a beacon message. GPS has some issues such as the cost associated with their use, and they may not work properly because of fading. In addition, other problems with this mechanism could be the need for synchronization between the internal clocks of nodes.

In addition, there are two protocols presented by Espes et al. [62, 63] to enhance the route maintenance in the AODV routing protocol. These two protocols are similar to the original AODV protocol where the originating node can estimate the distance to the destination node by setting an initial value of the Time To Live (TTL) field in the Route Request (RREQ) packet, which depends on that estimated value. However, to achieve the goal of these protocols, modification has to be done on the TTL field technique, which may cause an unnecessarily large number of control packets traveling through the network. Many researchers have studied reactive routing protocols including AODV and DSR as well and have been proposed various schemes of preemptive/predective approaches on the subject of link failure for ad-hoc networks

[64, 65, 66, 67, 68]

2.4.8 Packet Received Time Prediction (PRT)

Packet Received Time (PRT) is proposed by Al-sharabi et al. [69] to predict the link status in order to avoid the link failure on an active route beforehand. This approach used power measurement of received packets to predict the topological change. This mechanism works as follows if the current signal of the received packet is greater than the previous one, it indicates the link is stable and does not need a prediction algorithm. However, if it is weaker than the previous received packet's signal power, then the prediction algorithm sends RERR locally to the upstream nodes to maintain the route, or to the source (initial node) to establish a new RREQ to find a fresh route to the destination node. This mechanism has a common weakness as many other mechanisms did, such as sending an unnecessary warning message propagating back to the source node which again increases the traffic in the network.

2.4.9 Distance Vector with Mobility Prediction (DV-MP)

Su et al. [70] proposed a Distance Vector with Mobility Prediction (DV-MP) routing protocol in order to perform route reconstruction proactively in unicast and multicast routing protocol. To achieve this goal, DV-MP selects a stable route based on their predicted expiration times by utilizing Global Position System (GPS) in the mobility prediction. To estimate the expiration time of the current route to the destination node, mobility information is included in the data packets of on demand routing protocols. Predicted link expiration times are joined to data packets as they move to their destination nodes. However, there is an issue with the use of Global Positioning Systems in the mobility prediction (GSP), which is the associated cost, and it may not work properly because of fading.

2.4.10 Adaptive Backup Routing Protocol (AODV-ABR)

ABR is an extension of AODV protocol proposed by Lai et al. [71]. AODV-ABR is modification of AODV-BR protocol. In AODV-ABR protocol, the alternative route will be created by overhearing not only RREP packets but also data packets. The establishment of backup routes in AODV-ABR takes advantage of overhearing Route Reply (RREP) packets with hop count to the destination node. This happens when the link between two mobile nodes detected to fail AODV-ABR starts to maintain the route by using three way handshakes. Figure 2.16 presents the handshake procedure in order to solve link failure. As in Figure 2.16 shows that after moving the node B, it discovers that the link break between itself and destination node D. Node B broadcasts Backup Route Request (BRRQ) to its one-hop nodes in order to find an available backup node.

The intermediate nodes A, X and Y received the backup route request. In this respect, node Y sends the Backup Route Reply (BRRP) because node Y is available. AODV-ABR protocol considers hop count of route and competition of multiple backup nodes. However, the control message overhead is large and there are many collisions like AODV-BR.

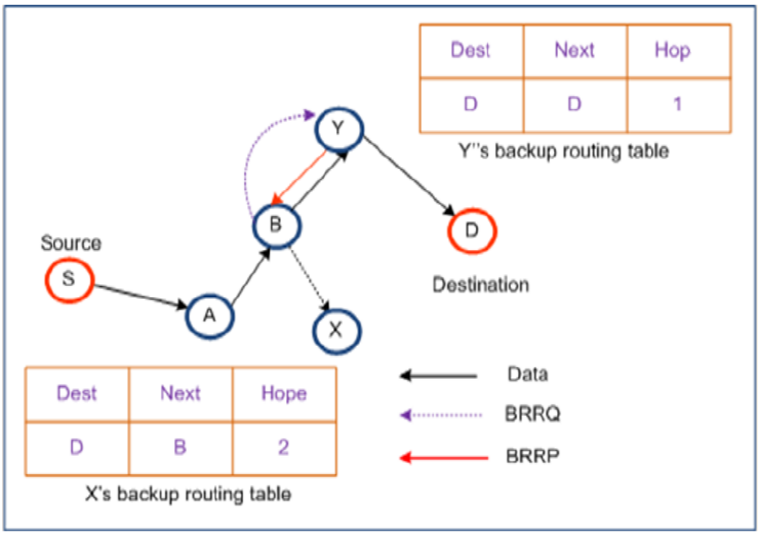


Figure 2.16: Procedure of Three Way Handshake in AODV-ABR (Adapted from [71])

2.4.11 Preemptive Local Route Repair (PLRR)

Crisostomo et al. [72] proposed as an extension to the AODV protocol namely Preemptive Local Route Repair (PLRR). PLRR aims to avoid route failure by preemptively local repairing routes when a link break is about to occur. This approach is to enhance node information concerning link stability to its neighbors resorting to HELLO messages. In this approach, the messages are attached with a new mobility extension containing the node's position, motion vector and an associated timestamp. However, the information of node mobility will be used to predict the instant link between two neighboring nodes. As Figure 2.17 shows, when a node determines that a link between the current node and its next neighbors' node is about to break, the node utilizes the information on the location and mobility patterns of both nodes. The node triggers the local repair procedure in order to find a new route to the destination or finds another node with a stable route to the destination before the previous link actually breaks.

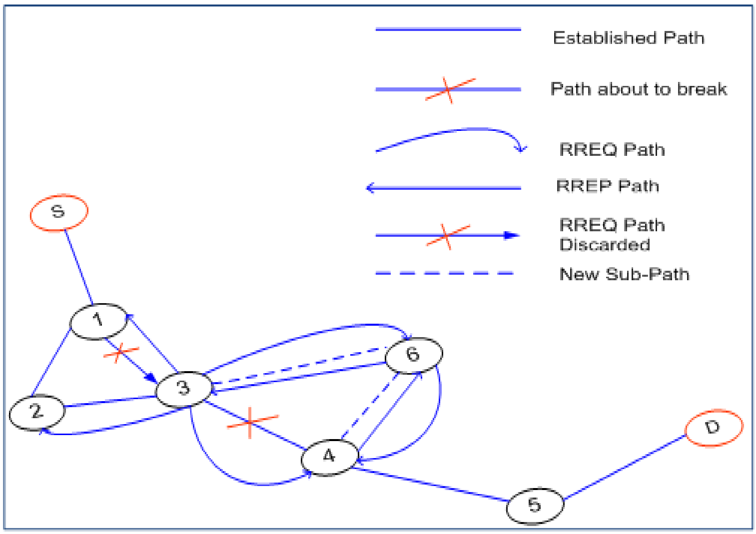


Figure 2.17: Preemptive Local Route Repair (PLRR) Illustration (Adapted from [72])

The weakness of PLRR is that it is not easy to predict that the node will divert from the link, because of the nature of ad-hoc network mobility. The device or mobile node will suddenly disappear. This is caused by either power failure (down) or the device is shut down by the user himself. It is difficult to predict whether the link has failed since one of the network devices is on high movement. The link failure might be recognized only when the link is out. As a result, an unnecessary message which makes tremendous network congestion is sent to the source. For the above mentioned reasons, PLRR is far from being the best solution for ad-hoc network route maintenance.

In addition, two independently proposed protocols in [73, 74] based on preemptive approaches can use link status information of routes, which can piggyback in the Route Reply Packet (RREP) in order to notify the source node. The main concern of piggyback in the Route Reply Packet is to plan for the right timing to route reconstruction. In the meantime, mobile nodes on the active route also need to perform link quality monitoring and confirm that with PING-PONG process for possible link breakage. Once link breakage is detected, the source node will be warned in order to preemptively initiate a route reconstruction process. However, there is always existing possibility of false identifying link breakage. In this respect, it can result in unnecessary route reconstruction and might possibly cause the broadcast storm in heavy traffic condition.

2.4.12 Way Point Routing (WPR)

Bai and Singhal [75] proposed Way Point Routing (WPR). In WPR, a number of intermediate nodes on a route are selected as waypoints and the route is divided into segments through the waypoints. In this respect, the WPR scheme used DSR as the intersegment routing protocol and AODV as the intrasegment routing protocol. This instantiation is termed DSR over AODV (DOA). In this scheme, a number of intermediate nodes on a route are selected as waypoints and the route will be fragmented. In this respect, sender and destination nodes, both are also considered as waypoints, maintain a hierarchy only for active routes. The main concept of WPR is that the route is divided into segments by selecting a number of waypoint nodes from the route, including the source and the destination nodes. The rest of the nodes on the route is termed forwarding nodes. However, the segment starts with a waypoint node called "start node" and ends with a waypoint node called "end node" and the start and end nodes of a segment are connected by a number of forwarding nodes. As illustrated in Figure 2.18, each two neighboring segments share a common waypoint node, which acts as the end node of the upstream segment and the start node of the downstream segment.

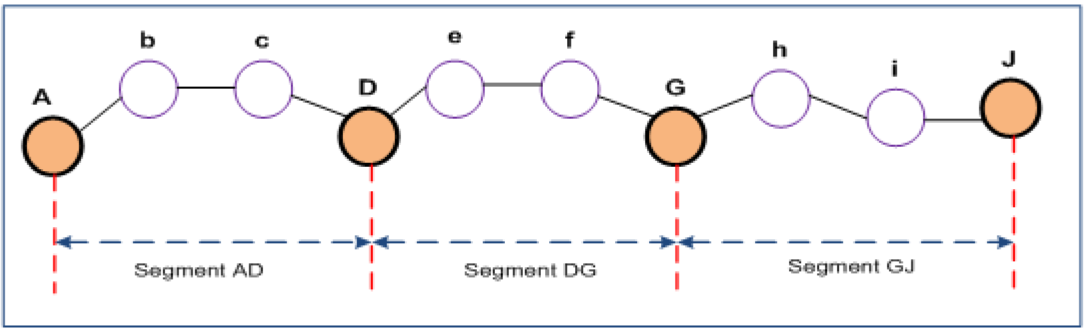


Figure 2.18: Network Divided into Segments (Adapted from [75])

In addition, as illustrated in Figure 2.19, two levels of route repairs are defined in WPR, and they are intrasegment route repair and intersegment route repair. When the original route is broken, intrasegment route repair is tried first and its repair succeeds, waypoint nodes on the source route are not changed. If intrasegment route repair fails, then intersegment or original route repair will be tried. If intersegment (original) route repair succeeds, the repaired source route is sent to the source, and the source will use the repaired route to transmit data packets thereafter. However, if both intrasegment and intersegment are failed, a route error message is sent to the source node, and as a result it may start another round of global route discovery.

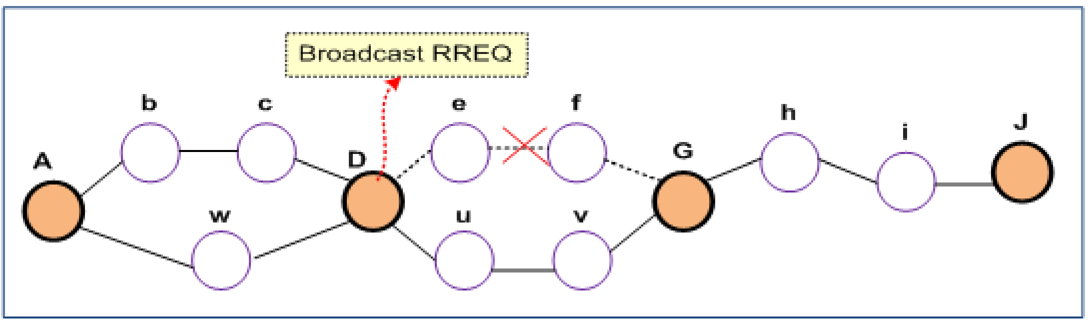


Figure 2.19: Intrasegment Route Repair and Intersegment Route Repair (Adapted from [75])

To analyze the WPR mechanism (shown in Figure 2.19), there are two segments or two routes “intersegment and intrasegment” (from D, e, f and G is intersegment and from D, u, v and G is intrasegment). As stated above, the route discovery of WPR works in the following way. If the original route is broken then intrasegment route repair is tried, if it does not succeed then intersegment or original route repair will be tried. Finally, if both intrasegment and intersegment do not succeede the waypoint node disappeare (G-Waypoint disappeared). As a result, the whole original route will be discarded, and it should initiate another round of route discovery in order to establish a new route from the source to the destination. Therefore, WPR method ignores the knowledge of the original route and it may cause a significant overhead to re-establish a new global route discovery. This is the subject matter of interest in this research and is obvious that the PDFRP outperforms WPR in terms of route maintenance mechanisms.

2.4.13 Two Hops Backup Routing (2HBR)

Chen and Lee [76] proposed Two Hops Backup Routing (2HBR) Protocol, which builds two hops alternate paths when replying to a RREP packet. This two hops backup routing scheme provides alternate routes for route maintenance procedure in AODV. Although two hops scheme can improve the packet delivery ratio for some instances, route maintenance procedure will not change much compared to the AODV protocol. If there is no alternate path to be utilized or the link on the alternate path failed, the 2HBR mechanism will be worthless. In addition, the 2HBR scheme only emphasized the route re-playing not route forwarding. In other words, it builds two hops alternate paths when replying to a RREP packet.

However, the two hops backup routing scheme is improved for route discovering with a limit margin, and it can still be improved. Furthermore, it is questionable whether the pre-established backup routes would ever be used, not to mention that these backup routes may not be available when they are actually needed due to the mobile nature of nodes in ad-hoc networks. Figure 2.20 shows the 2HBR protocol.

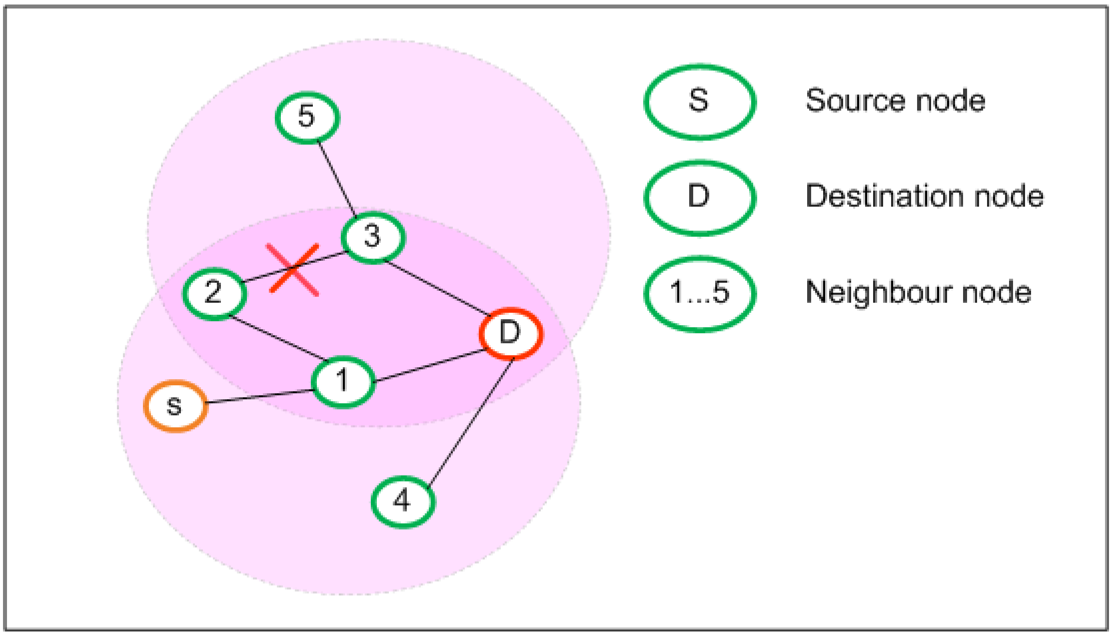


Figure 2.20: Two Hops Backup Routing (2HBR) Protocol (Adapted from [76])

2.4.14 Meshed Multipath Routing Protocol (AODV-MM)

Kuo and Liang [77] proposed AODV with meshed multipath. The route discovery process is basically the same as in AODV except that this scheme is appended with some extra information into both RREQ and RREP packets. The Route Request proceeds on receiving RREQ packets by intermediate nodes from its upstream neighbor. It will first check if this packet has been received previously or not in order either to accept or discard. In other words, if the RREQ has been received previously, the RREQ packet will be discarded, but if it is a new RREQ then the RREQ packet will add an entry in its routing table.

The route maintenance for AODV-MM protocol is not much different from the AODV. It works as follows: once a node detects link failure the node having detected link failure will check up its routing table if there is an alternate path to the desired destination or not. If it does, then the node having detected link failure will use the alternate route as the primary route to destination. Otherwise, the detected node should send an error message to the source node to restart the route discovery process. AODV-MM is basically the same as in AODV because it restarts route discovery by source node. Therefore, it needs to keep away from restarting route discovery process after the first route fails which causes heavy overhead for the network.

As illustrated in Figure 2.21, there are three reverse path routes in the routing table of node 3 namely S-1-2, S-4-5, and S-1-8. In this aspect, the route S-1-2 is used as the primary route from S to node 3. However, the primary route between nodes S and D is S-1-2-3-D. On the contrary, Figure 2.22 illustrates replying routes (RREP) while Figure 2.23 shows procedure and skeleton of multiple alternate routes.

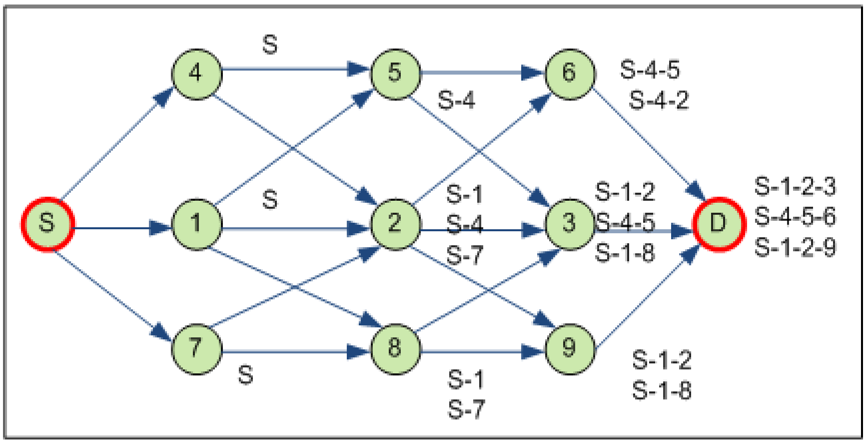


Figure 2.21: Reverse Path Routes in the Routing Table (Adapted from [77])

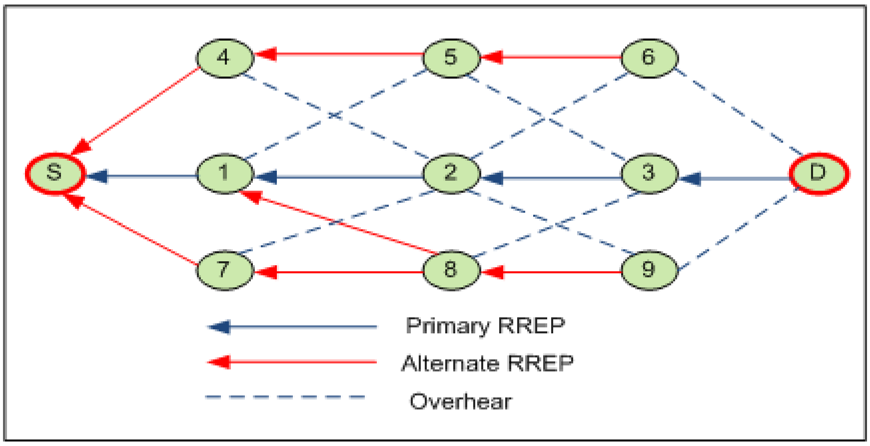


Figure 2.22: Replying Routes (Adapted from [77])

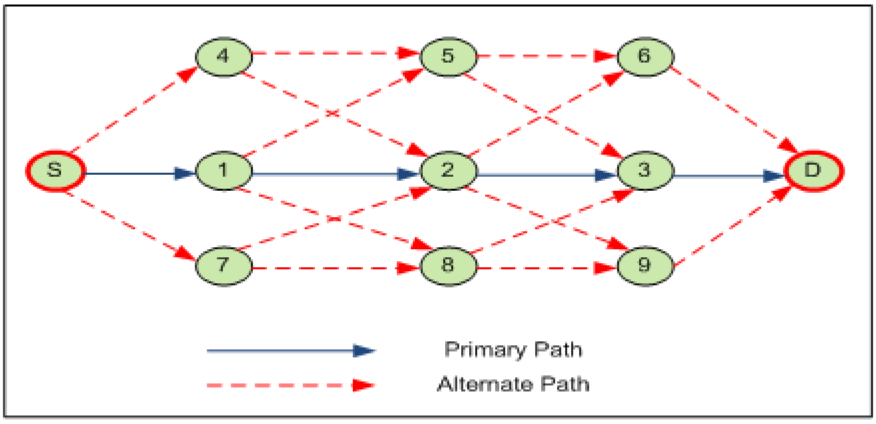


Figure 2.23: Multiple Alternate Routes Construction (Adapted from [77])

2.4.15 Backup Routing (AODV-BR)

AODV-BR is an extension of AODV protocol proposed by Lee and Gerla [78]. AODV-BR is enhanced route maintenance for AODV standard protocol by adding backup routes approached by overhearing a RREP message. Figure 2.24 (a) shows the procedure of construction backup route table. AODV-BR starts route discovery when the source node S wants to deliver data packets to the destination. It broadcasts a Route

Request (RREQ) packet to its one-hop nodes. After the RREQ packet reaches the destination node D, it sends back the Route Reply (RREP) packet to the source node S to inform the source the route has been established (D-B-A-S). When the intermediate node B receives the RREP packet, node Y creates a backup routing table because the node in the transmission range of node D can overhear the RREP packet.

After the backup route table established, node B sends a RREP to node A while nodes X and Y overhear. In this aspect, node Y does not update the backup routing table because it has already a route to destination node D. Node X creates the backup routing table. In case of link failure between two mobile nodes due to node movement, packet collision and limited battery during the data transmission, it broadcasts the data in order to find a backup node. Figure 2.24 shows link failure between node B and node D due to node B moving out of the transmission range of its next node D, in this case. Node B broadcasts the data to its one-hop nodes while nodes A, X and Y receive the packet but node A discards it after a duplicate check. In this aspect, node X as well discards it after searching its backup routing table while node Y plays the role of the backup node and it unicasts the data to destination node D, making a routing table.

Although offering a more stable connection than AODV, AODV-BR ignores the network environment. However, to establish the backup nodes, the network is very dense. In this case, there are many collisions at the node that is in the original route and receives the data from the failed link. In addition, the route recovery might increase the hop count of the route and leads to increase the end-to-end delays.

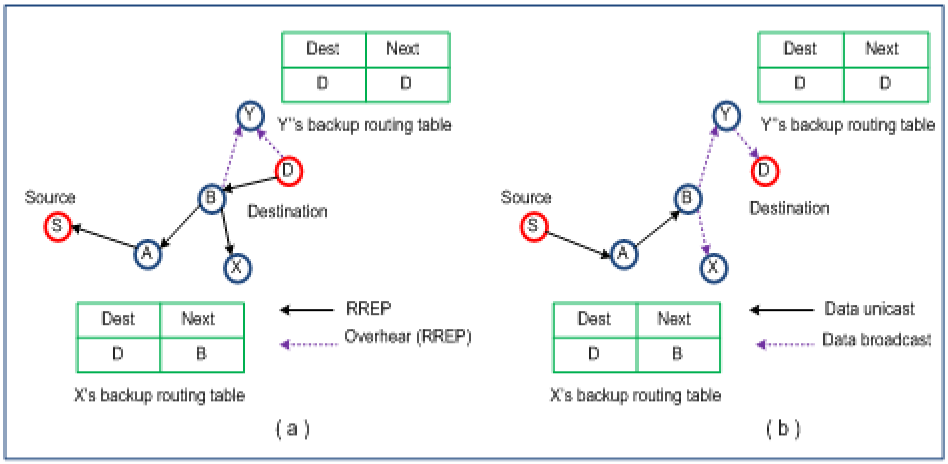


Figure 2.24: Establishment of a Backup Node and Route Recovery in AODV-BR (Adapted from [78])

2.4.16 Implicit Backup Routing Protocol AODV (IBR-AODV)

Jeon et al. [79] proposed IMPLICIT BACKUP ROUTING-AODV (IBR-AODV) which takes advantage of AODV-ABR and AODV-BR. This approach consist two mechanisms, namely, establishing backup nodes and fast route recovery. Backup nodes are established by overhearing the transmitted data of the sequent three nodes that are in the original route. Once the backup node is established, it makes a backup routing table and stores up data in the buffer. As Figure 2.25 (a) shows if any backup node cannot overhear the data, it deletes the backup routing table. The original route is S-A-C-D and node B is the backup node because node B overhears the data of nodes S, A and C. If a node that is in route tries to retransmit data to a failed link and a backup node detects it, the backup node begins fast route recovery. The backup nodes listen to the retransmission and then wait for a period of time selected by a random back-off algorithm. If backup nodes do not overhear acknowledgement during the back-off time, backup nodes send the Route Change (RC) packet to the node that tries retransmission. The node updates the routing table and sends the acknowledgement to backup node once it receives the RC. The backup node that receives the acknowledgement creates a new routing table and deletes the backup routing table. Next, the backup node transmits buffered data to the next node and the next node updates its routing table. All these procedures are shown in Figure 2.25 (b) illustrating that when the link between nodes S and A is disconnected, the backup node B conducts the route recovery. Then when the route recovery has been done, the original route (S-A-C-D) changes into the backup route (S-B-C-D).

However, one major drawback of IBR-AODV mechanism is that it coveys huge control message overhead to the network as well as many collisions happen like AODV-BR and AODV-ABR mechanisms. In addition, when a node which is in route tries to retransmit data, the link is already failed which means the packet is also dropped.

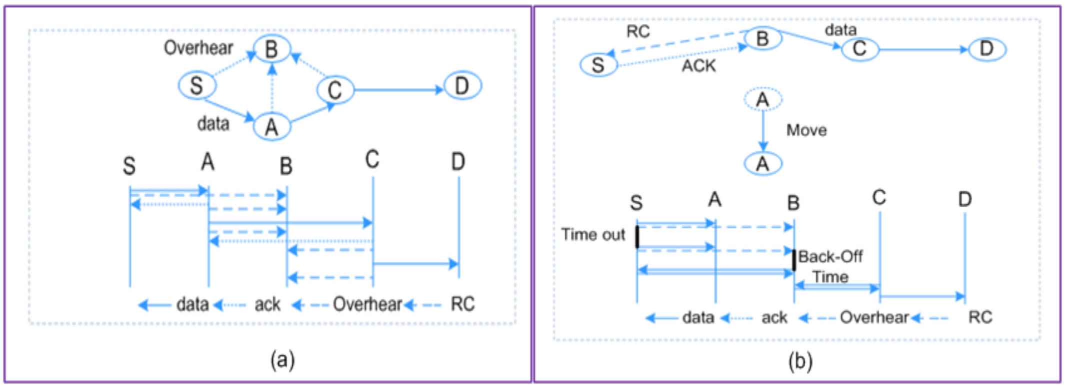


Figure 2.25: The Establishment of a Backup Node During the Data Transmission (Adapted from [79])

2.4.17 Self-Repair Algorithm (AODV-SR)

Feng and Zhou [80] proposed an AODV-SR algorithm to repair the link failure. Since the intermediate nodes are generally nearer than the source node to the destination node, the intermediate nodes on the data flow are more stable than the source node to broadcast RREQ packet in order to repair or to find a route to the destination node. In this respect, AODV-SR algorithm enhanced the AODV protocol by adopting the intermediate nodes instead of the source node in order to repair a route to the destination node. Figure 2.26 shows that the AODV-SR exchange messages when the link break occurs.

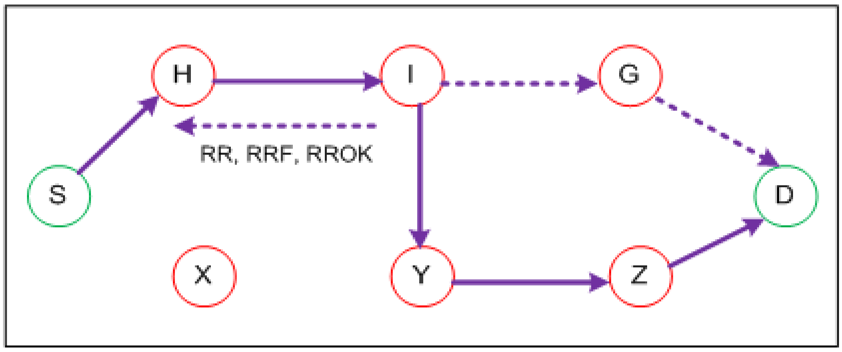


Figure 2.26: Self-Repair Algorithm Messages Exchange (Adapted from [80])

As shown in Figure 2.26, the data packet is flowing through the route <S-H-I-G-D> and a link fail is detected by the intermediate node I. In this aspect, node I does not send a Route Error (RERR) packet to the source node S. Instead, it sends a Route Repairing (RR) message back to the previous hop node H. After node H receives (RR) message, node I tends to broadcast a Route Request (RREQ) packet in order to repair the failure route. In case the node I was not able to repair the link within a specific time, it sends back a Route Repair Fail (RRF) message to the previous hop node H and at the same time node I delivers some data packages stored in the cache back to node H. Otherwise, if node I is able to repair the route on time, it sends back a Route Repair OK (RROK) message to the previous hop node H which has received a (RR) message from node I.

Upon node H receiving a (RR) message, it caches the data packages sent to the destination node D and broadcasts a Route Request (RREQ) packet in order to discover an alternative route to the destination node D. In case node H is not able to find another route to the destination node and also has received a Route Repair Fail (RRF) message from the failed node, node H sends a (RR) message back to the previous hop of itself. Alternatively, if node H receives a Route Repair OK (RROK) message, which indicates that, the route has been repaired by node I, node H will store the data packages in the cache. In contrast, node I tries to find a new route to the destination node to deliver the data packets. Whenever node I finds a route to the destination, it updates its routing table with a new route, even though the forward hop node I repairs the failed route and node H receives a RROK message from node I.

However, in highly dynamic network or worst conditions, each intermediate node is not able to repair the failed route and cannot find the alternative route to the destination node. In this respect, the source node receives a Route Repairing (RR) message. Therefore, AODV-SR algorithm might result much larger end to end delay than just sending one Route Error (RERR) packet to the source node in order to find a new route as in the traditional AODV.

2.4.18 Shortcut Detection and Route Repair (SDR-AODV)

Zapata [81] proposed an extension of AODV protocol called Shortcut Detection and Route Repair (SDR). The main concern of the SDR protocol is to find the shortest path and to repair the broken link. SDR protocol is a combination of shortcut discovery and route repair, which incorporates two different messages: Shortcut REQuest (SREQ) and Shortcut REPly (SREP). These two mechanisms work separately and lack the complementary feature. However, routing repair mechanism is started only after a link between mobile nodes has failed, which results in an extra end to end delay and increased packet loss. In addition, shortcut discovery mechanism requires mobile nodes on the current route in order to issue periodic shortcut RREQ and hence imposes an additional load on the network.

2.4.19 Neighborhood-Aware Source Routing (NSR) Protocol

Spohn and Aceves [82] proposed an extension of AODV protocol namely Neighborhood-aware Source Routing (NSR) protocol. Each mobile node in NSR has a partial topology, which can cover two hop neighborhoods as well as the links in requested paths to the destination node. NSR use link state information that is maintained by broadcasting periodic HELLO messages. In case the link between two mobile nodes has a breakdown, an intermediate node tries to maintain the route if either the link to the next hop has failed or the link headed by the next hop on the path to be traversed has failed. In this aspect, Route Error (RERR) message is generated to the source node if an intermediate node uses a totally new route to the destination node, or it has no other route to destination node. However, NSR uses periodic HELLO message in the network, which leads to introducing extreme routing overhead in order to maintain the partial topology of the network. Moreover, stale route in NSR is a big issue, which can affect the performance of the protocol.

Therefore, based on the previous work regarding solving link failure problem and its drawbacks of both current work and AODV standard protocol, is summarized in Table 2.3. From this table, it can be observed that there is a need for an efficient and reliable mechanism that can solve a link failure problem in AODV protocol during data transmission from the source node to the destination node.

More details about historical correlation of AODV initial mechanism including current weaknesses and improvement mechanisms as well as our research design departure point summarized in next section.

Table 2.3 summarizes a number of AODV extensions which tried to solve or mitigate the link failure problem using different techniques and mechanisms. Although they decrease the number of link failure problems compared to the standard one, it shows that there is still a gap which needs to be filled up. In this concept, as can be observed in

Table 2.3 especially preemptive/predictive mechanisms, unnecessary warning message is still sent to the source which makes tremendous network congestion. Thus these drawbacks indicate that there is a need for an efficient and reliable mechanism that can solve and prevent this huge number of warning messages, and this is one of the main concepts that PDFRP protocol is developed in this research.

Table 2.3: Comparison of the Previous Mechanisms Regarding Link Failure

Work	**Protocol / Mechanism**	**Technique**	**Weakness**
Soliman and Otaibi [59]	AODV-PSR	Preemptive Mechanism	NAT table may not be able to populate enough alternative links for future path detouring which leads to decreasing the performance of AODV-PSR.
Hacene et al. [61]	AODV-PP	Predictive Preemptive Approach	Unnecessary warning message is still sent to the source after a certain period of time which increases the traffic in the network.
Asenov and Hnatyshin [63]	Flooding mechanism	Global Positioning Systems (GPS)	GPS has some issues; such as the cost associated with their use and that they may not work properly due to fading.
Al-sharabi et al. [69]	AODV-PRT	Prediction Algorithm	Unnecessary warning messages propagating back to the sender node, which again increases the traffic in network.
Su et al. [70]	DV-MP	Mobility Prediction (GPS)	same as flooding mechanism weakness.
Lai et al. [72]	AODV-BR	Backup Route	Increases the end to end delay due to increase its hop count during route recovery process.
Lai et al. [71]	AODV-ABR	Adaptive Backup Routing	Control message overhead is large and there are many collisions like AODV-BR.
Crisostomo et al. [72]	AODV-PLRR	Preemptive Approach	Unnecessary data packets on position and mobility of nodes which makes tremendous network congestion is sent
Bai and Singhal [75]	AODV-WPR	Waypoint Approach	Break the whole network if the waypoint nodes break down
Kuo and Liang [77]	AODV-MM	Meshed Multipath Routing	If is no alternative are available to the desired destination, MM-AODV will re-initiate route discovery as in the standard AODV
Feng and Zhou [80]	AODV-SR	Self –Repair Algorithm	This algorithm might result in a much larger packet delay than just sending one RERR to the source to find a new route, as in the traditional AODV.
Zapata [81]	AODV-SDR	Shortcut Detection and Route Repair	Route repairing mechanism is initiated after a link is broken, which may introduce additional communication delay and packet loss.
Spohn and Aceves [82]	AODV-NSR	Neighborhood-aware Source Routing	HELLO messages in NSR incur extreme overhead to maintain the partial topology of the network. In addition, stale route is a big problem which may affect the performance of NSR.

2.5 Reflection of Current Mechanisms and PDFRP

According to [83, 84, 85, 86, 87, 88] standard unicast and multicast routing protocols in MANETs especially reactive routing protocol , an active path normally fails due to mobility when a pair of nodes are going to move beyond the range of network coverage where an alternate path is required only when the primary path is totally disconnected. Detecting link failure for traditional on-demand routing protocols involves large control message overhead and high latency because of limitation of current local link failure of repair mechanism where many retries have to time-out before a path is collapsed. In addition, a new path is established by the source node instead of intermediate node or locally [83].

However, a combination of all these constraints makes routing in ad-hoc network a big challenge. With the intention of mitigation for such drawback of MANET, beginning of last decade new ideas have emerged trying to predict the link status before the primary path totally failed. These mechanisms are mainly preemptive/predictive mechanism. The new revaluation of link failure model (the preemptive route maintenance) lets the network nodes to detect the link status and at the same time establish an alternate path before the link disconnection takes place. This may prevent an actual route break, and thus minimizes the packet loss rate as well as long delay.

Nonetheless, as Table 2.3 indicates the preemptive route maintenance mechanisms have come up with so many implications such as high traffic overhead caused by redundant warning messages due to absence of warning message mechanism. Consequences are high rate of network flood with several reinitiating route rediscovery packets which consume resources unnecessarily, causing collisions, congestion and end to end delay.

To overcome these problems (preemptive mechanism weaknesses), there must be a new design to prevent the number of warning messages traveling in the network.

Furthermore, to design and develop an algorithm for finding a new path and switching data (ongoing packets) into the new path is also of paramount importance. In order to address the above mentioned drawbacks, this research takes advantage of preemptive route maintenance and developed a new protocol, namely, Predictive Divert Failure Route Protocol (PDFRP) which provides fast route recovery with reliable connectivity and reduces the existing unnecessary huge messages upon link failure to enhance the network efficiency. PDFRP handles the competition problems between the traditional on-demand routing protocols especially AODV, and the new revaluation mechanism (preemptive) with that the PDFPR approach comes up with three main mechanisms namely, (1) to design a new mechanism to prevent various warning messages traveling in the network up on suspect link failure, (2) to develop a better mechanism for finding a new path in case the current link signal status indicates the current link breaks soon, (3) to divert data locally instead of globally.

2.6 Mobility Models

One of the most significant and difficult features of the network simulation designed for real mobile ad-hoc network situations is how to define a realistic mobility model, as stated in [89]. Because of the current scenarios which are based on the MANET environments, there are some features such as dynamically and intense uncertainties (e.g. Battlefield and Disaster). Therefore, the researcher simulates the movement pattern of mobile nodes as an alternative solution. According to Yoon et al. [90], the mobility models can be divided into two categories: the first category is for cellular wireless networks, and the second is for ad-hoc networks as shown in Figure 2.27.

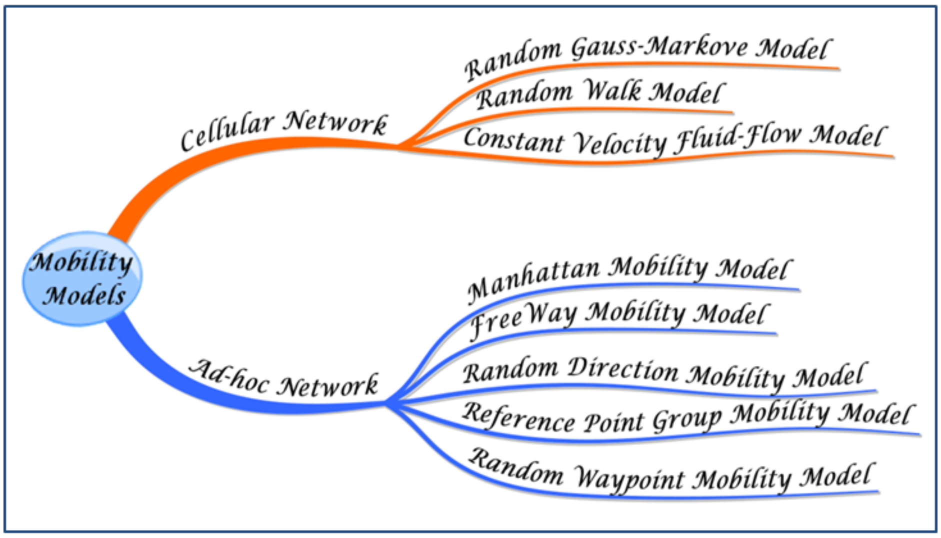


Figure 2.27: Mobility Models Classification

The mobility models in cellular wireless networks are required to use the base stations, and they are mainly concerned in the movement of individuals. In addition to including the independent movement of a single node, the mobility models in ad-hoc networks also contain group's movement of connected nodes groups. The communication in such mobility models need collaboration of two or more mobile nodes. Hence, the more realistic mobility models in ad-hoc networks such as Random Way Point (RWP) model [91]. Reference Point Group Mobility (RPGM) model [92], Free Way (FW) model [93], and Manhattan Grid (MG)model [94]. The impact of using different mobility models on the performance of mobile ad-hoc routing protocols is indicated in [93, 95, 96, 97, 98] In the next sub-sections, different mobility models in ad-hoc networks are presented.

2.6.1 Random Way Point Model (RWP)

RWP mobility model is the most widely used mobility model in both infrastructure wireless and infrastructure-less network. The way that the network traffic behaves when using this model is as follows: the mobile node begins by staying in one location for a certain period of time, called pause time. Once this time is finished, the node randomly chooses a destination in the simulation geographic area. In addition, it also randomly chooses a speed between minimum, maximum speed [91]. When pause time is long and maximum speed is small, the topology of ad-hoc network becomes stable. On the other hand, when the mobile node moves fast and the pause time is small; the topology is likely to be highly dynamic. In the RWP model, it is possible to generate various mobility scenarios with different levels of node speed.

2.6.2 Reference Point Group Mobility Model (RPGM)

Reference Point Group Mobility Model is proposed by Hong et al. [92]. RPGM model represents the movement of mobile nodes as group motion behavior, which is determined by a group leader called "logical center" where all group members have to follow the logical center in order to move from one place to the destination. The movements of the logical center follow a random way point model. These movements are independent and each mobile node can move to its way randomly with random velocity. The main idea of the logical center for RPGM model is to guide the group members continuously, which can calculate the group motion vector to identify the speeds and directions for mobile nodes in each group member. Each mobile node in the group it has its own reference point for communicating with other nodes. The reference point of the node follows the group movement. The real location of the node can be determined by its reference point plus a random motion vector that denotes its stability from the reference point. However, once the updated reference point RP (t+1) has been updated, it is shared with random motion vector values in order to represent the random motion of each mobile node around its reference point as mentioned in [93].

2.6.3 Freeway Mobility Model

FreeWay (FW) model is proposed by Bai et al. [93]. Free Way model is used to follow and track the movement's behavior in the vehicles on the highway as described by Izuan et al. [99, 100]. FW model is constrained by geographical environment, because of higher spatial dependences; the most used application used in this model is a freeway map. In this map, the freeway is divided into some specific regions called "lanes". Each node is permitted to travel only in its own path [101]. The speed of the node depends on the pervious speed of each node. For example, if the distance between two mobile nodes in one lane is less than the safe distance (SD), then the velocity of the next node is not permitted to go beyond the velocity of the front node.

2.6.4 Manhattan Grid Model (MG)

Manhattan (MG) model is proposed by Zhou et al. [94]. Manhattan Grid model is used in the urban area where the movement pattern of mobile nodes are emulated in the streets' environment. Manhattan model is similar with Free Way model in terms of having temporal dependence that can make the model constrained by geographical environments. The mobile nodes move in the horizontal and vertical streets. The mobile nodes in MG can travel right, left or move forward only with some possibility at certain levels of streets. The front and hinden nodes are similar as in the Free Way model. However, the main difference between Manhattan Grid model and Free Way model is that nodes in MG can freely select the directions of their movement, because the velocity in Manhattan Grid model depends on its velocity at the previous time. Consequently, nodes' speed will be limited by the front node in the same direction, while in Free Way model the nodes' speed is depending on the previous speed.

2.6.5 Conclusion of Mobility Models

All wireless communications are different from normal wired communications in terms of mobility where the performance of ad-hoc depends on actual environment. One of the most significant and difficult features in ad-hoc wireless is how to match an application to its suitable mobility model. Mobility Models can be divided into two categories such as Cellular Network Mobility Models which have a number of mobility models such as Random Walk Model and Random Gauss-Markov Model and so on. The second mobility model is MANET, such as RWP and RPGM and so on. This work different mobility models has been studied and tested two of these models namely, RWP and RPGM. As stated in empirical experiment chapter (Chapter Four), this work has been implemented through RWP model, which model is suitable for all ad-hoc environments. In addition it is also suitable both for infrastructure and infrastructure less environment.

2.7 Summary

This chapter has reviewed the concept of mobile ad-hoc network. Furthermore, it reviewed the mobile ad-hoc routing protocols classified as Flat routing, Hierarchical routing, and Geographic routing. It highlights the reactive routing protocols since it has shown the potential advantage over the proactive routing protocols and discusses each protocol with their techniques. It also discusses the Ad-hoc On-Demand Distance Vector (AODV) routing protocol in detail with prior work for current mechanisms to solve the link failure problem between the source and destination. It also presents the limitations of each protocol as well as suggests further enhancement for link failure to save the network resources. Finally, the chapter discussed the mobility models, which can affect the performance of routing protocols. In the next chapter, the experimental tool and the research methods for performance evaluation of the proposed protocol, namely PDFRP, will be presented.

CHAPTER THREE

RESEARCH METHODOLOGY

Chapter Two presented the background information on the development of Mobile Ad-hoc Network (MANET) providing the relevant literature review to the topic of the research and focused on link failure on Ad-hoc On-Demand Distance Vector (AODV) Protocol. This chapter, research methodology for performance evaluation of PDFRP protocol is discussed. Section 3.1 presents evaluation steps of the research and how the objectives of the research are correlated. Section 3.2 discusses the fundamental concepts of the research methodology and presents the most widely used Design Research Methodology (DRM). This section presents method stages and describes the research problem by the resulting identification of the criteria for success of the research and design of the research's conceptual idea deriving the hypothetical concept into a structural design for the developed protocol. Section 3.3 illustrates different simulations and their reliability highlighting the most common simulations such as, Continuous vs. Discrete Event, Terminating vs. Steady State and Synthetic vs. Trace-driven Simulation. Section 3.4 draws the simulation setup and a suitable environment for the developed protocol. Generation node mobility and data traffic modules, transport layer protocol and simulation software for network simulations are illustrated in Sections 3.5, 3.6 and 3.7 respectively.

3.1 Evaluation Steps

Objectives of the research have been stated and defined which the problem statement formulated, followed by the research question as well. Subsequently, has been clearly stated the goal of the research. In addition, the review of the literature and current related research topics was empirically done, pointing out and drawing the differences of this research philosophy (the gap) and existing solutions in the field. In order to realize the conceptual framework into a practice or simulation environment, the network topology, the proper parameters and the performance metrics have to set up and configured according to the research objectives. In addition, the network traffic model and suitable network mobility models have to be selected. These selections have to be done very carefully in order to simulate a system which is very near a real system. In case an incorrect traffic model according to the real environment has been selected, it can result in a worthless simulation, even if the network modeling is accurate. After selecting the network topology and parameters, then the network performance metrics (very important for the research to select a comprehensive list of performance metrics) were selected. According to Hassan and Jain [102], the metrics performance can be referred to as output of the research that will be observed at the end of simulation as stated in [102]. Selection of correct variable parameters is important: One of the main objectives of the simulation is to investigate the impact of certain variables on the performance metrics.

For instance, in the ad-hoc network, it may be interesting to study the effects of the node's pause time, speed, density, number of connections and so on. Thus, these variables can affect the network performance metrics, because if an important variable which may have a significant impact on overall network performance is left out, the result may not be significant as expected. Nonetheless, to some extent, it may not be possible to speculate the variables that have the highest impact, thus it supposes to select a large set of variables in order to start with and discard some of them later if needed. In this research, the number of variable parameters has been tested among pause time, speeds, node density, etc. According to Abdule et al. [103], the overhead is defiantly proportional to pause time and obviously the overhead will be low when the pause time is small. The experiment shows that choosing a smaller pause time gives the optimal setting for node pause time and indicates that the average performance of AODV protocol is when the node pause time is between 5 sec and 10 sec. This experiment confirms that the pause time has an impact on the network overhead results where in this case, the pause time is a variable parameter and network overhead is a performance metric. In addition, in some cases, the variable may not be a parameter, and it may be a scheme. In that situation the different simulation executions can have different versions of the algorithm. According to Abdule et al. [104], proposed Upstream Notification mechanism (UN) is an example to differentiate a variable parameter and a scheme or algorithm variable. In this case, the UN is a scheme variable because it supports PDFRP to perform better.

However, the analyst must select the variables (especially parameters) carefully in order to achieve the desired performance results. In addition, correct configuration settings and simulation software are important as well. The above mentioned different variable parameters have to be put into practice in the software model in order to verify and validate for the proposed protocol. Moreover, the software simulation has to be configured properly as it produces a relevant performance data. When the simulation is completely executed (run), the trace file data is created and stored in a disk as a file. These data have to be correct and do not contain large statistical errors. Subsequently, the raw data has to be converted into knowledge data to evaluate the impact of variables on the performance metrics [105]. Evaluation steps of the research correlations are stated in Figure 3.1.

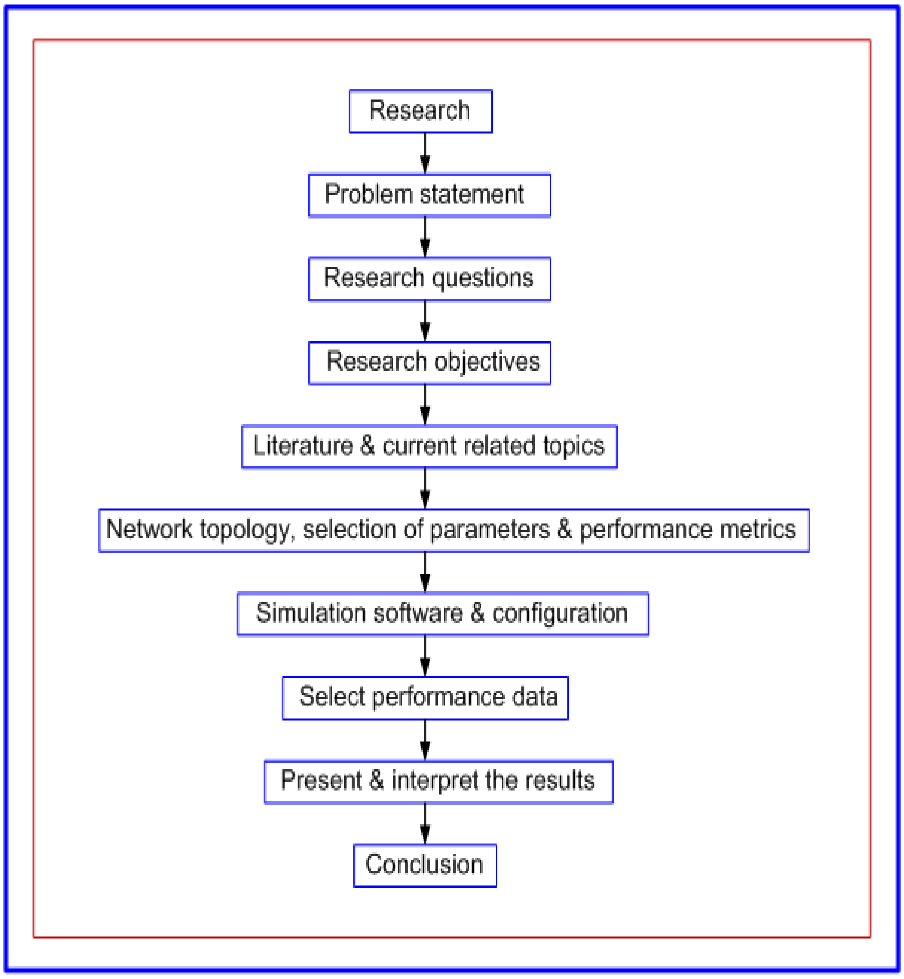


Figure 3.1: Research Strategy

3.2 Design Research Methodology (DRM)

The design of the methodology is a plan by which some undesired reality is visualized to be changed into some desired reality. It is a concept that has been designed to increase the readers' understanding of the phenomena in all its complexity and at the steps and validation of the research, methods and tools to improve the stages of the research correlation in a design. One of the main reasons to design a methodology is to improve effectiveness and efficiency of a new concept by the line of attack for research in order to support practice by developing knowledge to enhance the existing mechanism a successful into a new improved scheme (extension). The need to develop a commonly accepted research methodology as one of the main characteristics of an established area of scientific research which becomes an important topic in the research community. The design research is a fast-growing field of inquiry with significant importance in terms of helping researchers to create and improve the quality of design research as well as its academic credibility by enabling more logical, efficient and effective procedures. Figure 3.2 depicts the main stages of the Design Research Methodology. DRM has been chosen, because DRM approach studies the ways in which design research can best be undertaken to address specific questions in order to identify the aim that the research is expected to fulfill and focuses on it [106].

According to [107], DRM is an important method for both academic and industrial researchers as it is a useful and well-ordered method within a common design of research philosophy as well as a methodological framework which understands and improves the design with effective and efficient steps, thus this research used the widely accepted Design Research Methodology (DRM) [102]. According to Chakrabarti et al. [105], it can raise the following questions regarding research methodology:

i. What do we mean by a successful research?

ii. How is a successful research created?

iii. How do we improve the chances of being successful?

The first question indicates what criteria are to be used in order to judge success. In other words, what measures should be done to determine whether this research has been successful or not. The second question illustrates issues such as the influences on success and how these factors of influences cooperate. Finally, is to properly investigate these factors. The final question presents matters, which raise the translation of this understanding into design methods and tools where it indicates how the validation and verification are needed as determined by the criteria as described in [105]. All those investigating and steps increase our understanding of the design methodology to give a clear picture of the concept.

As described by Johnson and Ha [105], to address these issues in a professional and systematic method, a research methodology specific to studying and improving the design as a phenomenon is needed. To do so, there are two characteristics of design research required. First, the selection of research areas is not straightforward because of the influence of many factors and interconnectivity between them. However, it is very important to keep in mind that the methodology has to be suitable and applicable to the research topic and discipline as every field has its own research methodology design focusing on a particular discipline. For instance, social sciences, engineering science, computer science and management science and so on have to be addressed by a particular design methodology. The second characteristic of design research methodology is not only aimed at understanding the phenomenon of design, but also uses it to simplify the idea to be developed in order to change the way that the design is carried out. Figure 3.2 presents the most widely used methodology for design research where it simplifies the method stages from problem statement up to analysis, and they are as follows:

i. Research Clarification

ii. Descriptive Study I

iii. Prescriptive Study

iv. Descriptive Study II

Research Clarification-Identifying Problem: This stage describes the research problem by the resulting identification of the criteria for success of the research. The criterion for this research is going to identify a link failure due to mobile mobility.

Descriptive Study I-Design: This stage tries to understand the existing mechanism for mobile ad-hoc network on AODV protocol. Subsequently, it is going to design the research conceptual idea in order to drive the hypothetical concept into a structural design for the proposed scheme. In addition, this stage answers one of the research's objectives, namely the design objective.

Prescriptive Study- Implementation: In this stage the research implementation takes place. The prescriptive stage implements what have been designed from the descriptive stage. In this part of the stage, the simulation software is configured according to the selected variable parameters where the evaluation steps are mentioned this chapter. These variables have to be put into a practice in the software model in order to verify and validate the developed protocol. This stage and the previous stage (Descriptive study I) have to be collaborated correctly because if the software simulation is not configured according to the previous parameter setting, the outcome may not match the expected results. However, the second objective of study takes place in this stage.

Descriptive Study II-Result and Evaluation: In this stage, the support developed is applied, and a descriptive study is executed to validate the support. Descriptive study II presents the results and evaluation part of the research. This part will analyse the outcome of the simulation experiment conducted in the previous stage. The main task of this stage for this research is to collect the performance data, interpret data into understandable data, present the result as a graph, and evaluate the impact of the variables on the performance metric. Figure 3.2 is the diagram for the Design Research Methodology.

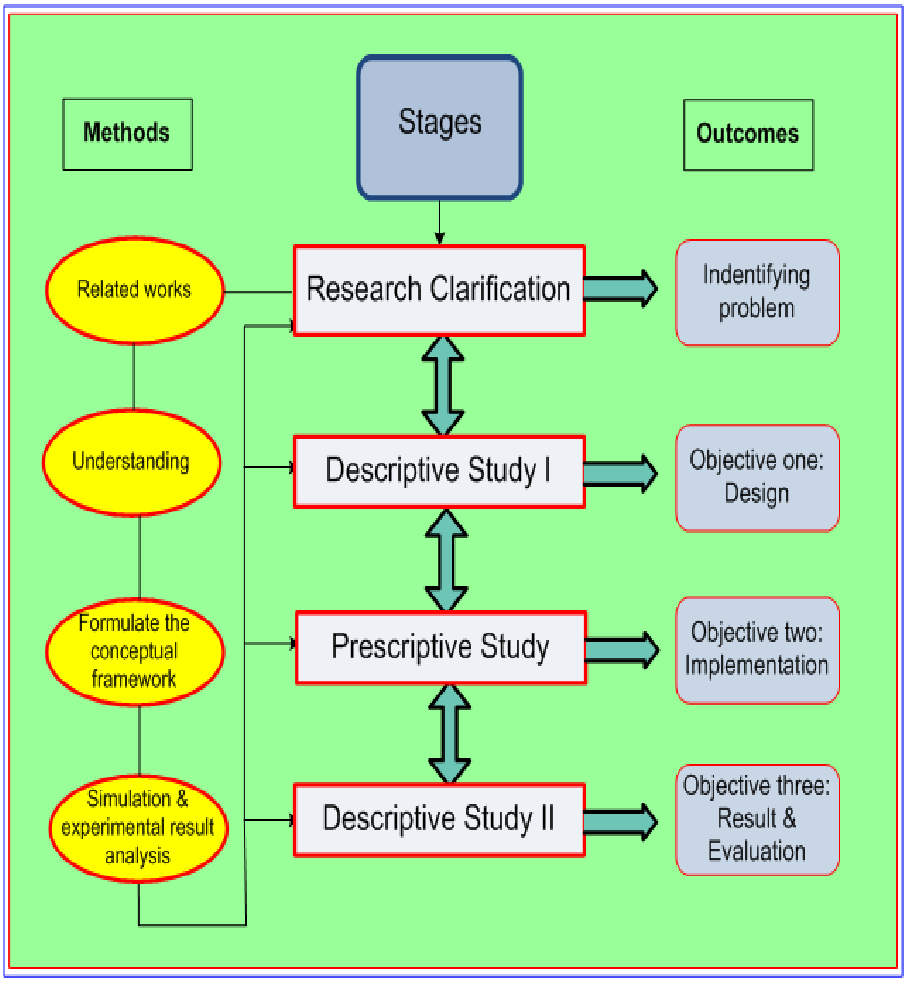


Figure 3.2: Research Methodology (Adapted from [102])

3.3 Different Simulations and Reliability

In this section, the most three widely used simulations as stated in [102] will be discussed.

i. Continuous vs. Discrete Event

ii. Terminating vs. Steady State

iii. Synthetic vs. Trace-driven Simulation

Continuous vs. Discrete Event: Simulation that uses the continuous state model is called "Continuous Event Simulation(CES)". This type of simulation is suitable in the situation where the event's execution will be continued without waiting for anything. In contrast, "a Discrete Event Simulation" (DES) uses discrete-state model of the system. The difference between these two models is the method of execution, whereby CES not depend on time in order to execute the event, whereas in the second model, each event has to adhere to specific starting times. In the latter model as the simulation progresses new events are added to the list. This model collaborates closely with the global simulation clock which is updated to the next event time.

Terminating vs. Steady State: These are two other simulation schemes different from the ones discussed above. The main difference between these two schemes is the context and the usefulness. The selection of one scheme over the other depends on how long the simulation would be run.

The steady-state simulation model is suitable in cases where one is interested in investigating the long-term packet loss rate in the congested router. In this case, the simulation must continue to run until the system reaches a steady state. Prior to reaching the steady state, the mean packet loss rate fluctuates as the system goes through a transient phase. An example of this phenomenon is illustrated in Figure 3.3. When using the steady state simulation model, the final results need to be reported with utmost care as the simulation might have terminated before the system reached the steady state. Hence it is necessary to carry out the simulation several times in order to make sure the results are valid and the system has indeed reached the steady state. In this research, simulation has been carried out at different timeslots and as indicated in Table 3.1 in section 3.5, it was finally decided for 2060 seconds to be used as the suitable simulation period based on the results obtained.

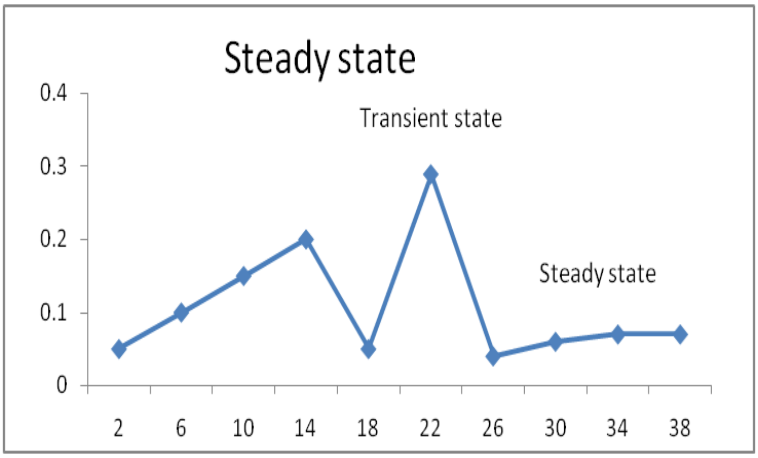


Figure 3.3: An Example of the Transient Phase in a Steady State Simulation

Synthetic vs. Trace-Driven-Simulation: Most of the experimenter who use the network simulator use the automatic traffic generator and most of these traffic generators, along with the simulators are a default package. However, in evaluating the performance of a given TCP/IP or CBR/UDP network using simulation, it has to get some input traffic pattern. The disadvantage of such input traffic is that the performance results obtained are then valid for only that specific traffic pattern. However, in many simulations input traffic is synthetically generated using random traffic generators.

According to Ariyakhajorn et al. [108], the mobility model is designed to describe the traffic pattern of mobile nodes (MNs) in addition to how their speeds and directions are changed over the time. At the moment, in Ad hoc network there are two types of mobility models used in the simulation:

- ***Traces base model:*** The traces base model obtains deterministic data from the real system.
- ***Synthetic base model:*** The synthetic base model is the imaginative model that uses statistics.

In the real world, nodes have their target destination before they decide to move. One main advantage of them choosing automatic traffic generators within a simulation it is easy for the operation due to the traffic being generated automatically. Although random traffic generation remains a popular choice network simulation, input traffic for this method never matches 100% with the actual traffic. To overcome those obstacles and achieve more credibility, many performance analysts use Trace-driven simulation. However, this study was conducted by Network Simulator version 2 (ns-2) which is a discrete event simulator. Details of ns-2 will be explained later in this chapter. Figure 3.4 shows the steps of a trace-driven simulation.

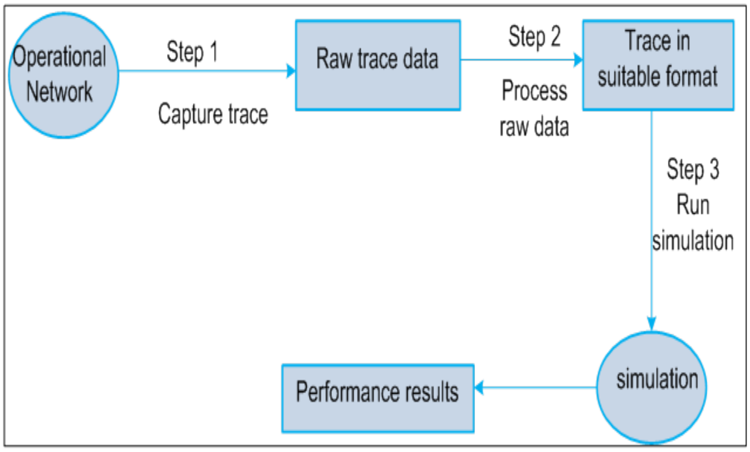


Figure 3.4: The Steps of Trace-driven Simulation (Adapted from [102])

3.4 Simulation Setup

The overall goal of simulation setup is to create a suitable environment for the developed protocol to measure its ability in order to evaluate how it reacts to the network topology changes due to node mobility. To achieve this goal, it has to be measured this ability with a variety of variable parameters, performance metrics as well as network load. Subsequently, the study simulation was set up and configured with properly selected network traffic model and network mobility model. The selection of the traffic model and mobility model that was carried out in this research has been done by a separate experiment. However, the simulation experiment's setup includes the performance metrics that is used to evaluate the overall protocol performance, number of nodes, size of topography area, node movement and data traffic patterns. According to Das et al. [109], the selection of the network performance metrics are the key metrics for this research. The following six performance metrics have been selected as a key metrics for this research.

i. Routing Overhead

ii. Packet Delivery Fraction (PDF)

iii. Normalized Routing Load (NRL)

iv. Average End-to-End Delay

v. Packet Drop

vi. Throughput

The number of nodes used in our simulation varies between 5, 20, 40, 60, 80 and 120 wireless nodes with 1000 m x 1000 m square. Lee et al. [42] conducted an experiment to investigate the ADOV scalability and tested a number of nodes from 50 up to 10,000 nodes, and found whenever the number of nodes increases the protocol performance decreases. In addition, their experiment used a specific size of the area in each number of nodes. In this case, they found that the suitable room size for 50 nodes is 1000 m x 1000 m. Since the founder's experiment shows that the AODV does not have any problem for the scalability, and they start from 50 up to 10,000 nodes, thus this research used up to 120 nodes starting from 5 to evaluate the smaller network size with 1000 m x 1000 m.

3.5 Generation Node Mobility and Data Traffic

Traffic generation module, called "Connection pattern file generator" is used for generating CBR connections (cmu-scen-gen, cbrgen.tcl, version 1.4) in ns-2 and its format is:

"ns cbrgen.tcl [-type cbr/tcp] [-nn nodes] [-seed seed] [-mc connections]"

Generated for the assigned number of nodes such as 5, 20, 40, 80 or 120 with CBR traffic sources, with a rate of 16 kbps and 4 packets are generated per second with packet size of 512 bytes. Thus, the rate will be 4*512*8 = 40 kbps. The research also used BonnMotion Tool to generate data traffic that developed by University of Bonn as presented in [110]. This Bonnmotion Tool is used for generating node mobility patterns (node-movement such as speed, pause time, node-passion etc.). More details about Bonnmotion Tool will be explained the next chapter in Section 4.2.2.

Empirical experiments have shown that choosing a smaller pause time gives the optimal setting of AODV [103]. In addition, this pre-tested experiments for node speed results indicated the speed optimal setting for AODV protocol is when the speed is less 20 m/s. This has been also shown in the experiment results for the developed protocol in Chapter Six, which indicates that the more speed grows the more protocol performance is diminished. Table 3.1 shows parameters configuration used in the research.

Table 3.1: Configuration Table of the Research

Configuration	Table
Topology Area	1000 X 1000 m
Simulator	ns-2.32
Ad-hoc Routing Protocol	PDFRP
Number of Nodes	5,20,40, 80 and 120
Simulation time	2060 seconds
Max- speed	5, 10,20 30 and 40 meter per second
Min-speed	0 m/s
Max-pause time	0,10,20,30,40 seconds
Min-pause time	0 s
Packet size	512 bytes
No. of packets	10 pkts/s
Node placement	Random Waypoint Mobility Model
Traffic model	CBR(constant bit rate)
Transport protocol	UDP
Seed	1.0
Antenna type	Omni Antenna
Mac layer	IEEE 802_11
Propagation model	Two Ray Ground & Shadow mode
Radius of node	250m
Network interface	Phy/WirelessPhy

3.6 Transport Layer Protocol

This research used Constant Bit Rate (CBR) as a transport protocol. Since TCP protocol is designed for none movement network, it will not perform well in ad-hoc network. In other words, this protocol is suitable for static node network environment. According to Bakalis and Lawal [111], different ad-hoc routing protocols including on demand and table driven protocols (proactive) have been studied analytically using TCP, CBR and Variable Bit Rate (VBR) traffic models. They found that TCP traffic models performed poorly by mis interpreting of packet loss, link failure, and late acknowledgement as a sign of network congestion. Therefore, in order to avoid mobile ad-hoc networks using TCP traffic models are congested due to the frequent topology changes. Thus, the research has been carried out by using CBR as a transport layer protocol.

3.7 Network Simulator Tools

There are a number of simulators and among them are Network Simulator 2 (ns-2), OMNeT++, OPNET Modeler, GloMoSim [112] [113]. This research has been chosen Network Simulation Tool (ns- 2) as a simulator tool. ns-2 is a discrete event simulation software for network simulations [114]. ns-2 supports simulation for many routing protocols for mobile ad-hoc networks, including AODV, DSR TORA, and DSDV and many others. The ns-2 tool is a combination of two languages, namely C++ programming language and Object Tool Common Language (OTCL) [5]. Although ns-2 can be built on a variety of platforms, this research has chosen to implement on Linux platform [115] as the Linux offers a number of programming development tools that can be used along with the simulation process. Using the ns-2 simulation software, the user must write the simulation script in OTCL and from that script get the simulation results in an output trace file. The output trace file or simulation results will be analyzed by using trace analysis program.The widely used in ns-2 trace analysis programs are AWK command and Perl scripts, but there are also available other trace analysis programs. For this research, both AWK command and Perl scripts are used for data analysis.

The reason that ns-2 is chosen as the simulation tool among the other simulation tools is because ns-2 supports both research and education while other simulation tools such as OPNET are not free and GloMoSim support only education users as stated in [116]. ns-2 simulator is more suitable for designing a new protocol and it is also suitable for comparing different protocols and traffic evaluations than among other simulators as well. This simulator is developed as a collaborative environment where it is distributed freely and it is an open source as well. Moreover, there are many versions available such as FreeBDS, Linux, Solaris, Windows and Mac OS X. In addition, as stated in [117], ns-2 has also been chosen as it contains a detailed model of the physical and link layer behavior of a wireless network based on the 802.11 specifications and allows arbitrary movement of nodes within a network area. Besides, the AODV protocol is also provided as part of the ns-2 installation. Furthermore, the ns-2 installation includes all software extensions – contributed code developed by the Monarch research group in Carnegie Mellon University (CMU) which is important in this research as it uses CMU's node-movement generator "setdest" which is used to create random waypoint node movements for mobile nodes, such as cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections][-rate rate].

3.8 Summary

This chapter introduces the research methodology and its steps. It presented the goals and objectives of the research and formulated the most widely used methodology for design research where the method is simplified by stages from the problem statement up to analyzing the level, followed by the research questions. Four clarifications of methodology steps where curried out namely Research Clarification-Identifying Problem, Descriptive Study, Prescriptive study- Implementation and Descriptive Study II-Result and Evaluating. The research design highlighted the methodology for the developed protocol, simulation setup, and type of data traffic as well. PDFRP method of steps and Simulation software that was used in this research was also illustrated. Several pre-experiment results with different mobility models will be presented in the empirical experiment chapter.

CHAPTER FOUR

EMPIRICAL EXPERIMENTS OF AODV

Chapter Three presented the research methodology and the steps of performance evaluation for the developed protocol, namely the Predictive Divert Failure Route Protocol (PDFRP). This chapter, the impact of node mobility on MANET regarding Ad-hoc On-Demand Distance Vector (AODV) Protocol and optimal setting against pause time and speed with different metrics has been studied. Empirical experiments of AODV, and mobility models for optimal setting experiment tests have been discussed. The aim of this chapter is to study the current behavior of AODV protocol prior to implementing the developed protocol. In this respect, several pre-tested experiments have been done, testing more than one mobility model with AODV standard in order to examine at least two different models' behavior with different parameters. Section 4.1 presents empirical experiments aiming to figure out the optimal setting for AODV protocol. Section 4.2 discusses experiment setup for pause time optimal setting on Random Waypoint (RWP), metrics for performance evaluation. Finally, protocol optimal setting analysis using Reference Point Group Mobility model (RPGM) is presented in Sections 4.4 and 4.5.

4.1 Empirical Experiments of Mobility Models

In this research, before it implements the developed protocol, pre-tested experiments have been done, testing two different mobility models with AODV standard in order to examine different behavior of the mobility models with different parameters. Thus, this chapter presents the number of experiments aiming to figure out the optimal setting for AODV protocol in certain mobility models. This part of the experiment is a potential for the research and it is a part of the evaluation performance of the research. In this respect, all the main parameters which can affect the performance of routing protocol have been investigated. Therefore, a number of mobility models have been tested and the results are illustrated with analysis. One of the main reasons for conducting this pre-experiment implementation is that most of ad-hoc researchers use Random Waypoint Mobility model (RWP). Due to that, the ns-2 by default provides the RWP model. This mobility model is most commonly used, but it is not suitable to be applied all ad-hoc applications.

However, there is an alternative to the use of some other mobility models, which are not provided by default in ns-2 package such as Reference Point Group Mobility model (RPGM), Manhattan Grid Model, Gauss Markov, Static, Disaster Area, Chain Scenario, etc. To implement these mobility models, a traffic generation software can be used rather than ns-2 (one example is BonnMotion Tool, which will be explained later in this chapter) which creates a file containing the movement of nodes, including the node speed, the node pause time and so on. These mobility models are applicable in special applications and has different behaviors.

In this respect, it is important to investigate which mobility model is more suitable to the developed protocol before making a final implementation. In addition, how the protocol behaves in different environments using varying metrics to evaluate the optimal setting of the developed protocol is another important issue. Hence, in this experiment several examinations regarding increasing pause time, speed and different number of nodes have been done as well. Furthermore, more mobility models where tested in order to choose the best and suitable model for the developed protocol. However, this section presents Random Waypoint Model experiment results.

This section discusses experiment results examining the optimal setting for AODV protocol using Random Way Point Model (RWP) as a model. A number of mobility models have been developed and applied with different tools. This experiment focuses on the most widely used and studied mobility model, namely Random Waypoint

Model (RWM) [118]. In this model, the movement pattern is independent of each other. The destination is chosen randomly by nodes with a random speed which follows uniform distribution between V_(min,) V_max , where V_(min,) and V_(max) representing minimum and maximum mobile nodes speed (velocity). Upon arriving at the destination, the node stops for a while according to defined "pause time", then it chooses another destination randomly and repeats the above operation. Parameters V_max and pause time are very important factors which determine the movement of the node. Choosing a smaller maximum speed with longer pause time, the topology of the ad-hoc network will be relatively stable. On the other hand, with longer maximum speed and small pause time, the topology of ad-hoc networks changes rapidly as stated in [119].

4.2 Experiment Setup for Pause Time Optimal Setting on RWP

Simulation is performed using ns-2, which CBR was used as a traffic generator. Random waypoint mobility model (RWP) was used as a mobility model in the field of 1000m x 1000m. Various network scenarios for a different number of pause times and nodes are generated. Table 4.1 shows the parameters that have been used in the simulation. This experiment executed 4 x 5 scenarios which is equivalent to 20 scenarios. Each scenario of the pause time is varying while the rest of parameters are constant. In the first scenario, node density is 10 nodes, the number of connections is 4, node speed is 20 m/s and pause time is varying (5, 10, 20, 30 and 40 s). In the second scenario, node density is increased to 20, the number of connections is 8, and node speed is 20 m/s, which the pause time of course varying. In the third and fourth scenarios, nodes and number of connections are increased to 40 nodes, 80 nodes, 30 with connections and 40 connections respectively and pause time follows as previous scenarios while the rest of the parameters are unchanged.

Table 4.1: Varying Pause Time

Parameters	Values
Simulation	ns-2
Routing Protocol	AODV
Movement Model	Random Waypoint Model
Traffic source	Constant Bit Rate (CBR)
Simulation area	1000 m x 1000 m
Simulation Time	200 s
No. of nodes	10,20,40 & 80
Pause time	5, 10, 20, 30 &40
Nodes speed	20m/s
No of sources	4 ,8, 30 & 40

4.2.1 Metrics for Performance Evaluation

The important performance metrics which were evaluated in this empirical experiment are as follows:

i. Packet Delivery Fraction (PDF)

ii. Average End-to-End Delay

iii. Routing Overhead (ROH)

iv. Packets Drop

v. Normalized Routing Load (NRL)

Packed Delivery Fraction (PDF): PDF is a vital metric overall network performance. PDF metric distinguishes the routing protocol, the completeness and correctness as well as the routing protocols' reliability as it gives the protocol's effectiveness. Packet delivery fraction is the proportion resulting from the number of exclusive data packets arriving at the destination divided by the unique data packets sent from a source.

Packet delivery fraction measures the protocol performance in the network and this performance may depend on factors such as packet size, network load, as well as the effects of frequent topological changes.

Average End-to-End Delay: This metric indicates the average time that the packets take to reach at destination. The average end-to-end delays are the summation of all end-to-end delays divided by total data packets arrived at destination. These delays include: the buffer delay, the interface queue delay, the bandwidth contention delay at the MAC, and the propagation delay. Since voice and video applications are especially dependent on low latency to perform well, end-to-end delays are important metric for routing performance. This metric is to some extent dependent on PDR and in that case if fewer packets are delivered, then the average is calculated from fewer samples. However, as path length increases between source and destination, the probability that a packet will drop also increase. On the other hand, networks with a low PDR, samples with short paths are favored and thus the delay will be low.

Routing Overhead (ROH): ROH is the total number of routing packets sent by routing protocol during the simulation time, minimizing overhead, reduces network bandwidth utilization, and in addition, saves battery power consumption to avoid large routing updates. Each time a packet is forwarded over multiple hops, routing overhead is incremented by as many packets as there are hops.

Packet Drop: This is the result of the number of data packets sent by the source from the number of data packets received at destination. There are several reasons that a packet is dropped; one common reason is that when a queue within a network router reaches its maximum length, packet drop is normally occurs.

Normalized Routing Overhead (NRL): NRL is the number of routing messages transmitted per data packet delivered to the destination. In other words, NRL is the total hops of transmitting routing control messages like Route Request, route reply and route error where each hop transmission of a routing packet is counted as one transmission Thus, the NRL metric is useful to determine the efficiency and scalability of the protocol as it can estimate how many transmitted routing messages are used for one successful data packet delivery. NRL is also highly associated with the number of route changes which occurred in the simulation. Nonetheless, the routing overhead and the normalized routing load metrics evaluate the efficiency of the routing protocol. The formulas of these metrics are stated in chapter Seven in section 7.1 (Performance Metrics).

4.2.2 Simulation Set Up

Figure 4.1 illustrated the simulation set up. This simulation set up is important for this experiment by showing how ns-2 and another Tools such as BonnMotion Tool work together in order to examine more mobility models than Random waypoint mobility model (RWP) such as Reference Point Group Mobility model (RPGM) or any other mobility model that ns-2 does not support. Normally, most of researcher those who are using ns-2 are mostly utilized RWP as mobility model because it is included in ns-2 simulator. Since the ns-2 supports only RWP, it has to be utilized another Tool, one example is BonnMotion software. BonnMotion is a Mobility Scenario Generator and Analysis Tool developed by Java software which creates mobility scenarios. In this simulation two mobility models have been tested with BonnMotion Tool. Figure 4.1 shows movement pattern created by BonnMotion and traffic pattern created by ns-2, so these two files can be integrated by using ns-2 and BonnMotion. Right side in Figure 4.1 indicates traffic pattern and left side shows movement pattern. The traffic pattern is a data traffic generation model for generating CBR connections such as number of nodes, CBR traffic sources and rate of packets that is generated per second. The movement pattern is a model to generate node mobility patterns such as speed, pause time and nodes' position.

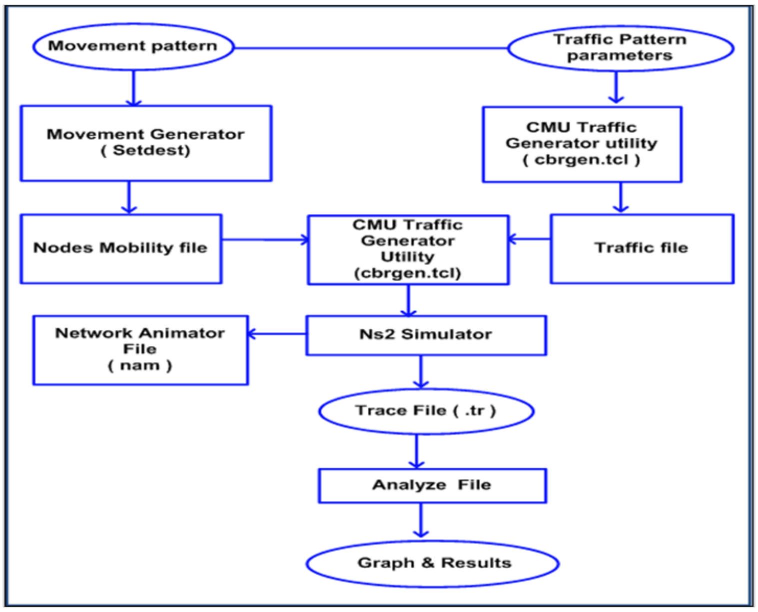


Figure 4.1: Simulation Set Up

4.2.3 Result and Discussion for Pause Time Optimal Setting on RWP

This section discusses and analyzes the results of simulation presented by graphs. The discussion focuses on four metrics that are used for measuring the protocol's performance. This simulation has taken five main scenarios where each main scenario contains 5 sub-scenarios. In each sub-scenario, the number of nodes and movement speed is constant while the pause time changes. For example, the first sub-scenario setting parameters are: 10 nodes, 4 connections, 20 m/s for movement maximum speed and 5 pause times. The next sub-scenario, all parameters remain as above except for the number of nodes and pause time, which will be increased. For instance, in the second sub-scenario, the number of nodes are doubled (20 nodes) and pause time is 10 s. For the remaining sub-scenarios, all parameters are repeated as above. When the first main scenario is tested repeatedly for 5 times with different pause time, the next main scenarios are tested similarly.

4.2.4 Result of Packet Delivery Fraction for Pause Time Optimal Setting on RWP

PDF is the ratio between the generated number of packets and the number of received packets at the destination. This metric is vital as it describes the loss rate that will be seen by the transport protocols, which in turn affects the overall network throughput that the network can support. Figure 4.2 shows that the packet delivery ratio for scenario one started lower rate and as pause time goes up, it also improves the PDF. In the second scenario, in which the pause time is a higher rate than the scenario one, there is much improvement. Finally, the third and fourth scenarios have shown the best rate of packet delivery fraction. As stated above, 5 main scenarios have been taken and each of this main contains 5 sub-scenarios which means 5x5 = 25 scenarios have been tested in this experiment. In each of these experiments of sub-scenarios, the pause time increases while other parameters are kept constant. Figure 4.2 indicates that the higher mobility environment, which network topology change rapidly, the protocol performance is lower.

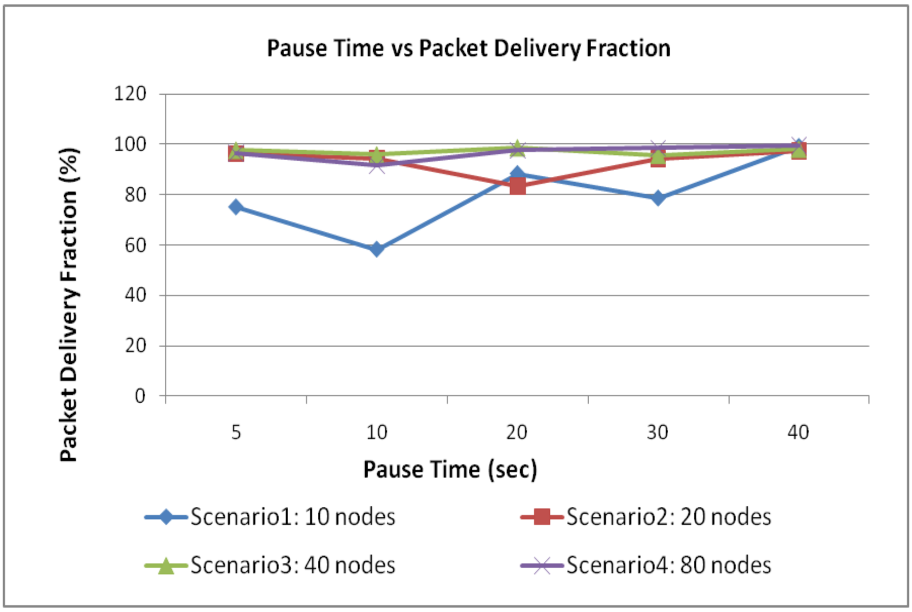


Figure 4.2: Pause Time vs. PDF on RWP

4.2.5 Result of Average End-to-End Delay for Pause Time Optimal Setting on RWP

All parameters are depending on one another and none of them is completely independent. For instance, a lower packet delivery ratio means that the delay metric is evaluated with fewer samples. On the other hand, using a longer route , the probability of a packet loss may be higher. The end to end delay may not be directly proportional to the number of hops that the packet goes through. Figure 4.3 shows that the average end to end delay of scenario one is not that much fluctuated due to less traffic, because the number of nodes for scenario one is set to 20 nodes and pause time is set to 5, which means less pause time creates high mobility. Scenario two shows very low delay which is much better than scenario one which confirms that the number of hop count and delay are no directly proportional to each other. Logically, increasing the number of nodes means the number of hop count increases, which supposedly increases the delay. Nonetheless, increasing the pause time decreases the delay in all of these scenarios.

This indicates the average performance of AODV protocol can be observed when the pause time is 40 s which is the optimal setting.

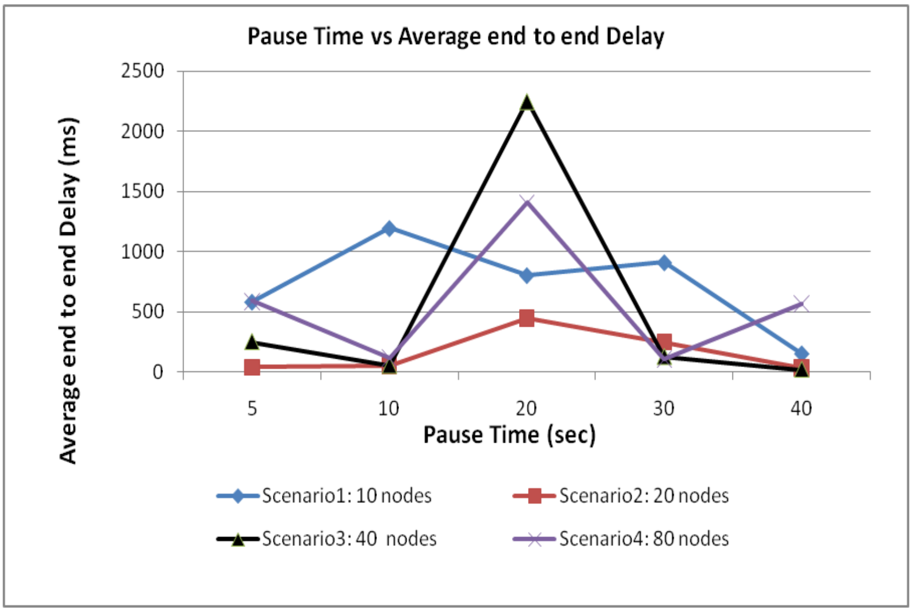


Figure 4.3: Pause Time vs. Average End-to-End Delay on RWP

4.2.6 Result of Routing Overhead for Pause Time Optimal Setting on RWP

Overhead is a vital parameter on network performance as it reduces overall network resources utilization. Routing overhead is an important metric among other metrics as it measures the scalability of the protocol as again it evaluates the degree to which the protocol will function in congested or low-bandwidth environments, and its efficiency in terms of consuming node battery power. Another important point which needs to mention is that the protocols that send large numbers of routing packets can also increase the probability of packet collisions and may delay data packets in network interface transmission queues. So it is important to reduce the overhead in the network as much as possible. Figure 4.4 presents the experiment results for routing overhead. Figure 4.4 shows that the overhead of scenario one has a low overhead and very smooth, because the load of data sent from the source node is small. As stated earlier, the sources (connections) of scenario one is four nodes which means the destinations will be less. In scenario two, the sources and destinations are both increased, and it shows that when the number of data sending resources increases, the number of routing packets will increase because there are more destinations to which the network must maintain working routes. In contrast, for the last two scenarios, it shows that the overhead is reduced whenever the pause time and number of nodes are increased. For instance, in the fourth scenario the pause time is 40 s and sources are 30 nodes; therefore, it shows that increasing pause time enhances the protocol performance.

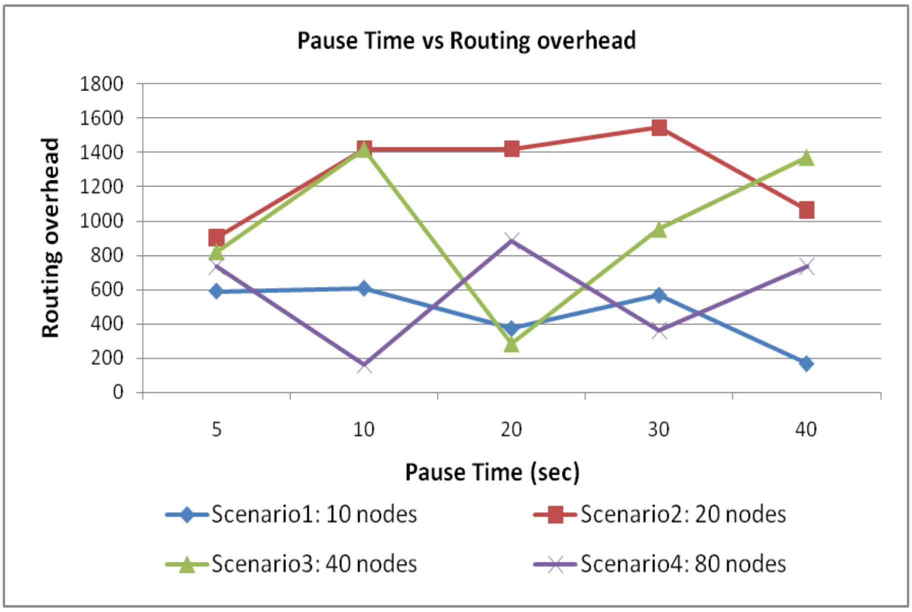


Figure 4.4: Pause Time vs. Overhead on RWP

4.2.7 Result of Packet Drop for Pause Time Optimal Setting on RWP

There are two ways that the packet is dropped: when the buffer is full, or time exceeds the limit. It means that if there is no a valid route to the destination, packet needs to be buffered for a while. However, if there is no space in the buffer, the packet has to be dropped and at the same time if the staying time exceeds the assigned time, the packet is also dropped. The experiment result for packet loss is illustrated in Figure 4.5. Figure 4.5 shows that the packets drop for both scenarios one and two more dropped packets. The packet drop and link failure are directly proportional. This case shows that in these periods more link failure has happened in the network. As shown in Figure 4.5, the remaining two scenarios indicate that the link is relatively stable. The reason for it to be stable can be because the link breakage is less than previous scenarios. It also shows that when the pause time is increased the performance of the protocol will be improved.

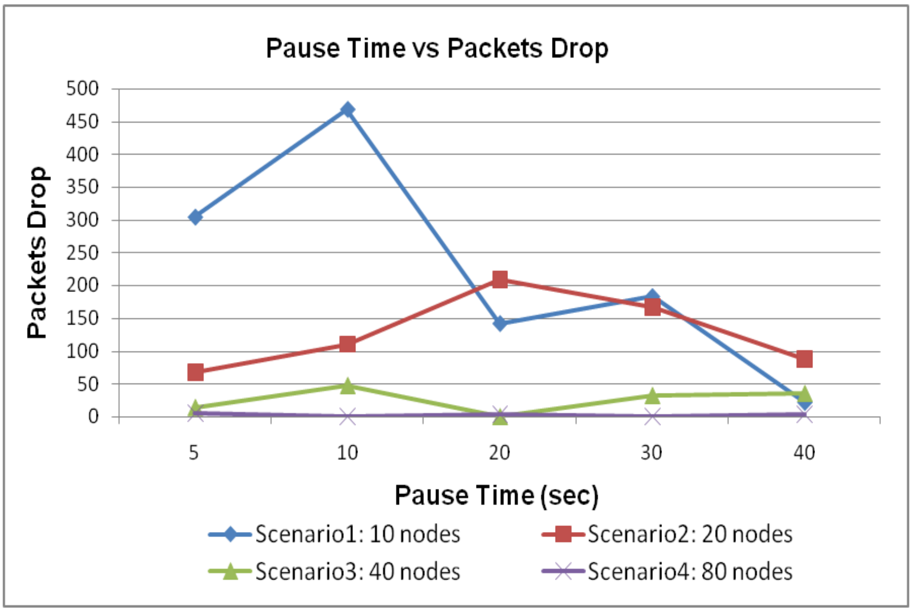


Figure 4.5: Pause Time vs. Packet Drop

4.2.8 Result of Normalizing Routing Load for Pause Time Optimal Setting on RWP

For NRL as the function of pause time, Figure 4.6 shows the results of the simulation for normalizing routing load. Scenarios one, two and three shown that the normalized routing load is fairly stable, but it does not mean the NRL is good. In contrast, scenario four shows the highest normalized routing load. In practice, NRL represents the number of routing packets transmitted per data packet delivered at the destination, and that means the result of scenario four is much better than others.

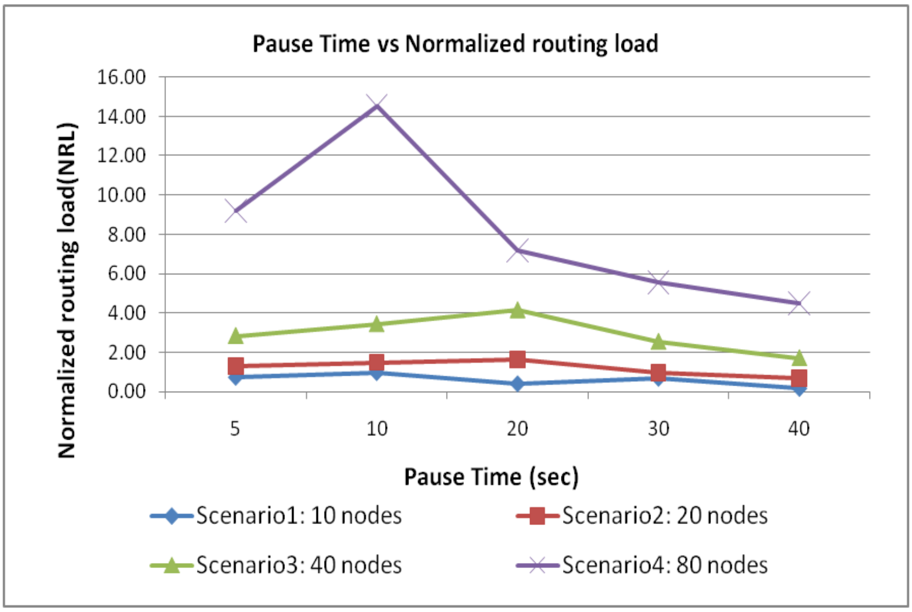


Figure 4.6: Pause Time vs. Normalized Routing Load

4.3 Experiment Setup for Speed Optimal Setting on RWP

Our experiments have been conducted using by the ns-2 simulator which is available as an open source distribution [114]. For generating the scenarios for both traffic (CBR) and movement of mobility, it uses the mobility and traffic generator tool, “cbrgen.tcl” and “setdest” scripts was used, which is provided along with the standard ns-2 distribution with the wireless protocol stack model developed by Carnegie Mellon University (CMU) [120]. This experiment utilizes CMU’s wireless extension that is based on a two-ray ground reflection model and the MAC used is the IEEE 802.11. Parameters that are used in the simulation for next experiment (speed experiment) are stated in Table 4.2.

Table 4.2: Varying Node Speed

Parameters	Values
Simulation	ns-2
Protocol	AODV
No of node	10, 20, 40 & 80
Movement Model	Random Waypoint Model
Traffic source	Constant Bit rate (CBR)
Simulation area	1000 m x 1000 m
Simulation Time	200 s
Pause time‘	40
Min-node speed	5, 10, 15, 20 m/s
Max-node speed	10, 20, 30 & 40 m/s
No of sources	4 ,8, 30 & 40

4.3.1 Motivation and Performance Metrics for Speed Optimal Setting on RWP

The motivation behind this experiment is to explore and figure out the speed affects AODV protocol. Our intention in conducting these experiments is to investigate the protocol's performance by simulation experiment under RWP model when the node speed increases. Nonetheless, in this experiment was examined five metrics such as NRL. NRL metric measures and determine the efficiency and scalability of the protocol in order to estimate how many transmitted routing messages are used for one successful data packet delivery. Network overhead is another metric that is also taken in this experiment, which is also important to minimize the network bandwidth utilization as well as saving battery power consumption to avoid large routing updates.

Packet loss is another very important vector in the network environment as it tells how the nodes communicate with each other either smoothly or overcrowding (congestion) the network. Actually, on observation of packer drop can be enough to evaluate overall network well being, thus it is always very important to include the experiment testing. The testing of average end to end delay is also included in this experiment. This delay includes processing and queuing delay in each intermediate node, which indicates the average time the packets take to reach at the destination. PDF is also included. This metric is the most important among all other metrics. This indicates the ratio of how many packets have been received at the destination according to the number of packets is sent by the source. The next sub-sections examine the speed optimal setting.

4.3.2 Simulation and Result for Speed Optimal Setting on RWP

The previous section and its sub-sections tested pause time whereas in these sub-sections test speed optical setting was tested. In this experiment, four scenarios with each containing four sub-scenarios have been tested . Actually, 16 experiments were taken where each scenario was examined 4 times. For example, the first scenario includes 10 nodes, 40 s pause time, 5 minimum speed, 10 maximum speeds, and 4 number of connections. This scenario was repeated another three times with constant for all parameters except speed where it increases in each sub-scenario.

The repeated sub-scenario speed parameters are a range of 10 m/s (minimum) and 20 m/s (maximum) , 15 m/s (minimum) and 30 m/s (maximum) and 20 m/s (minimum) and 40 m/s (maximum). In the second scenario, the number of nodes was increased up to 20, the number of connections was also increasedup to 8, the min/max speed 5 m/s and 10 m/s, while pause time in all scenarios is constant. This second scenario is also repeated another three times as well and all parameters are also constant except speed where it increases as in the previous scenario. The range of the speed parameters for the second sub-scenario is the same as the previous first sub-scenario. Third and fourth scenarios follow as the two above scenarios, just increasing the number of nodes and connections: 40 nodes, 30 connections, 80 nodes, 40 connections respectively. The results for each time that the nodes' speed increase was observed and studied the impact of the speed metric in each scenario. Figures 4.7, 4.8, 4.9, 4.10 and 4.11 show the effect of increasing the node speed.

4.3.3 Packet Delivery Fraction for Speed Optimal Setting on RWP

Here, analysis the ratio between the originated numbers of packets and the number of received packets at the receiver. Figure 4.7 shows that the packets delivery ratios where the nodes' speed is varying from 10 m/s up to 40 m/s. There are four scenarios in Figure 4.7. Scenario one shows that the packets delivery ratio is very good when the speed is 10 m/s and 20 m/s. In scenario two the highest packets delivery ratio is when the speeds are 10, 20 and 30 m/s respectively. For scenario three, the best result shows when the speed is 10 and 20 m/s where they are 81.97% and 75.73% respectively.

Finally, the fourth scenario shows the packets delivery ratio results are 62.58%, 56.92%, 50.65% 62.45% respectively, which are a little bit fluctuated compared to the other three scenarios. However, the best result in this scenario is also 10 m/s. Nonetheless, the overall results for the packets delivery ratios indicate that the low mobility environment gives the highest packet delivery ratio.

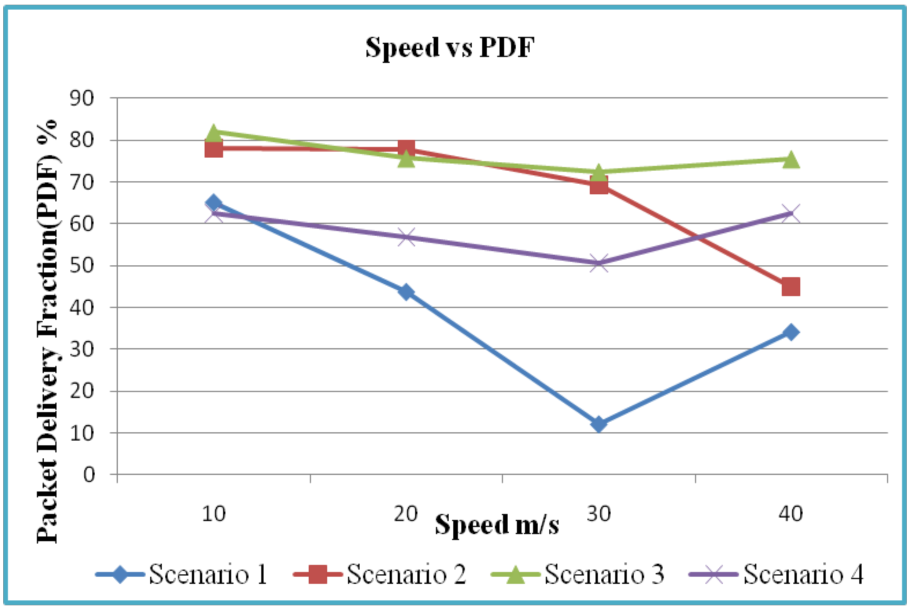


Figure 4.7: Packet Delivery Fraction for Speed on RWP

4.3.4 Routing Overhead for Speed Optimal Setting on RWP

The network overhead is an indicator of how the network routing messages are huge or small. Minimizing the network overhead is maximizing the network resources utilization with better performance. Figure 4.8 presents the experiment result for routing overhead. It shows that the overhead increases while the speed increases which means that the routing overhead is direct proportion to nodes speed. But one has to keep in mind that the number of nodes also increase from scenario to next scenario which can contribute the increasing of network overhead. For example, the number of nodes for scenario one is 10 nodes, while the number of nodes for scenario four is 80 nodes.

In addition, the number of source for scenario one is 4 connections, while scenario four is 30 connections. In order to distinguish which factors contribute more to the increase of the overhead, the graphs in the Figure 4.8 has been depth analyzed. For instance, the first scenario has tested 4 times and each time the node's speed is different (increase) while the rest of parameters are constant, and the next scenario the number of nodes and connections are increased while the speed is still the same as the previous scenario. So, from Figure 4.8 it is obvious that in every scenario, the overhead is less when the speed is lower and not when the number of nodes is increased. Because as stated in [119], the higher speed network in MANET environment, the network will be unstable where the risk of link failure will also be higher which increases the number of control signaling packets (overhead). Thus, this experiment shows that choosing a smaller speed gives the optimal setting for node mobility speed and indicates that the average performance of AODV protocol is when the node speed is between 10 m/s and 20 m/s.

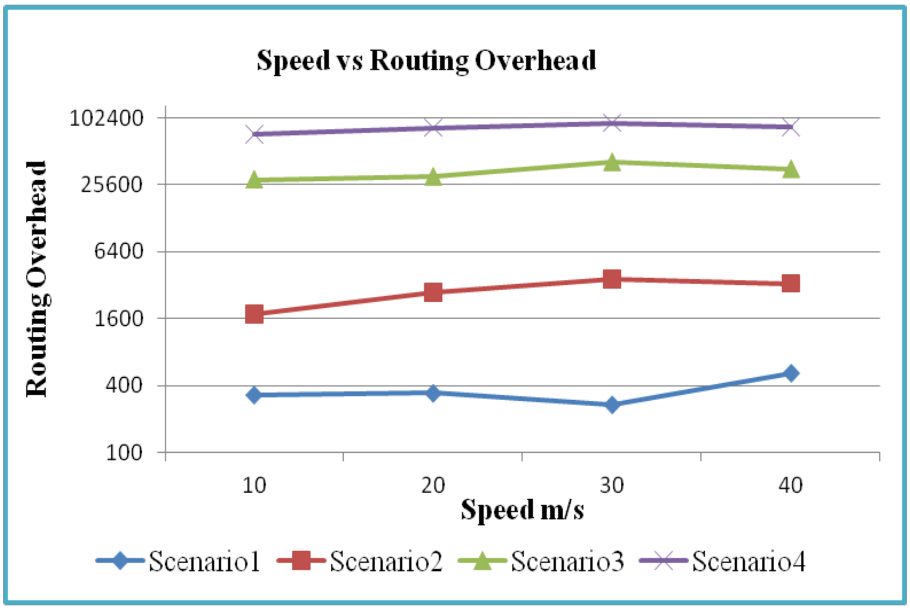


Figure 4.8: Routing Overhead for Speed on RWP

4.3.5 Average End-to-End Delay for Speed Optimal Setting on RWP

The delay metrics is an important vector for communication in general, especially in real communication (delay sensitive). The mobile ad-hoc network is a part of delay sensitive communication; thus it is a vital to minimize the delay as much as possible. Figure 4.9 shows four average end to end delays scenarios and each of these scenarios is tested four times with four different nodes speed (10, 20, 30 and 40 m/s). In scenario one, when the speed is 10 m/s the delay is 573.52 ms and when the nodes' speeds are increased up to 20 m/s, 30 m/s and 40 m/s the delays are increased up to 1160.05, 1478.58 and 3161.3 ms respectively.

In scenario two, from the speed 10 m/s up to 30 m/s the average end to end delays are also increased where 40 m/s is slightly decreased according to 30 m/s. The reason is as stated in [119], the higher the speed network in MANET environment, the network performance will be decreased. In scenario three, when nodes' speeds are 10 m/s, 20 m/s the average end to end delay are 290.79 and 512.65 ms, which indicates that the increasing of node speed, the delay will also increase. In this scenario, when the nodes' speed are 30 and 40 m/s, the delays are 435.7 and 317.54 ms. These values are in between the values for 10 and 20 m/s nodes speed. Nonetheless, the average of optimal setting of AODV protocol performance for node speed in terms of the average end to end delay is in 10 m/s in this experiment.

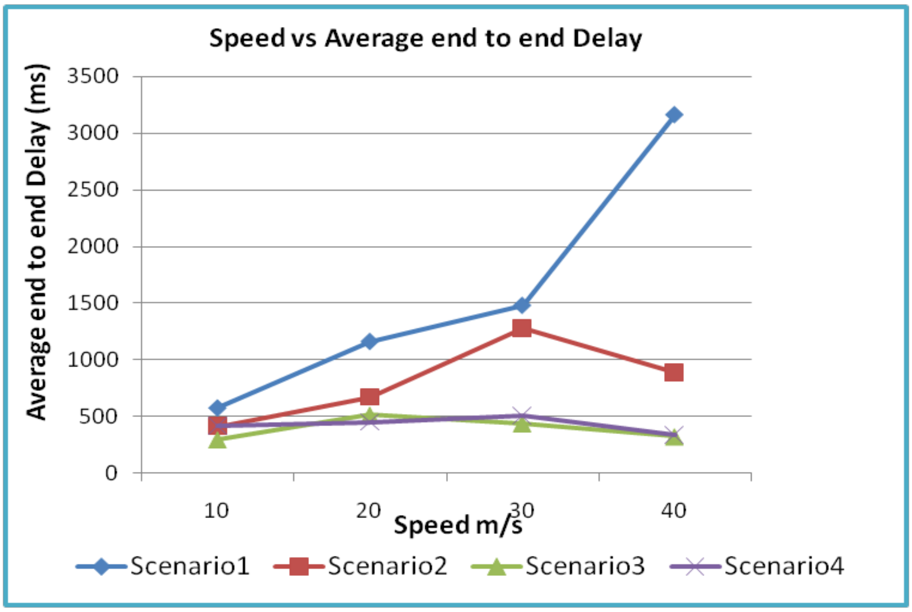


Figure 4.9: Average End-to-End Delay for Speed on RWP

4.3.6 Packets Drop for Speed Optimal Setting on RWP

Figure 4.10 illustrates packet drop vs. speed. It shows that the packets drop for both scenarios more dropped packets whenever the node speed is increased, except 40 m/s for scenario three and four which show that the packets drop decrease in this particular point. However, most of the experiment results of packets drop depicted in the Figure 4.10 shows the lower the speed, the better packets drop gained. The packet drop and link failure are directly proportional and this experiment shows that the high the mobility periods are, there are more packets drop in the network which means more link failure.

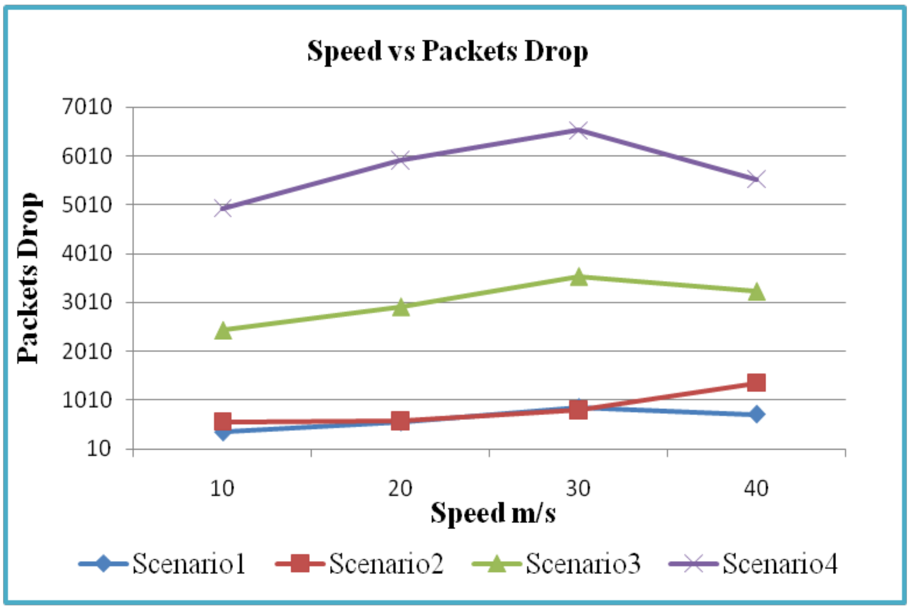


Figure 4.10: Packet Drop for Speed on RWP

4.3.7 Normalizing Routing Load for Speed Optimal Setting on RWP

Figure 4.11 illustrates the results of normalizing routing load. Figure 4.11 shows that the results for NRL are in direct proportion to the increasing node's speed. In scenario one, the results for nodes' speed 10 m/s, 20 m/s, 30 m/s and 40 m/s are 0.47, 0.72, 2.06 and 1.39 (these are ratio of packets sent and data packets received) respectively. In scenario two, the normalizing results are 0.93, 1.47, 2.19 and 3.04 (these are ratio of packets sent and data packets received) respectively. The results for scenarios three and four are also increased as node speed is increased. Nonetheless, since the NRL represents the number of routing packets transmitted per data packet delivered at the destination, the results of scenarios are much better when the node's speed is small.

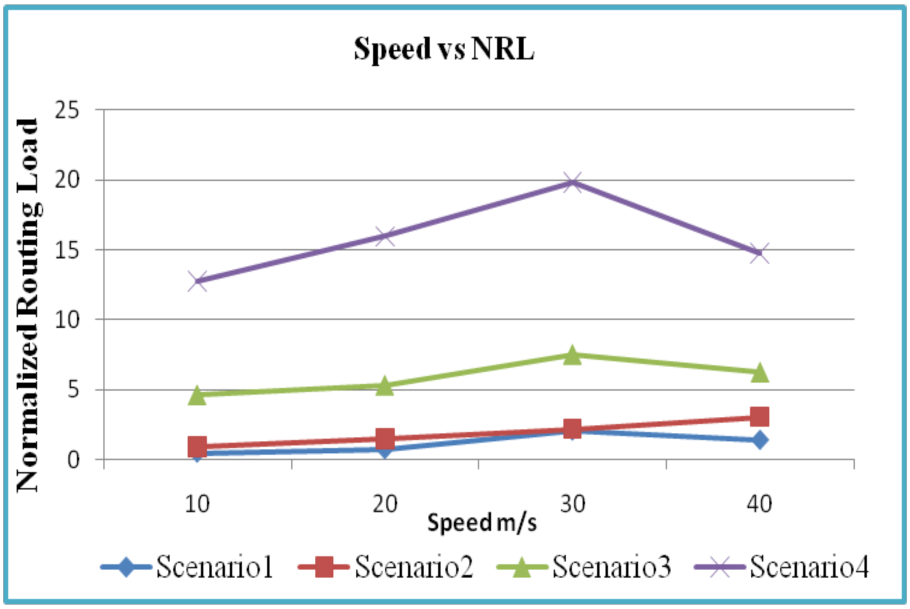


Figure 4.11: Normalized Routing Load for Speed on RWP

4.4 Protocol Optimal Setting Analyses Using RPGM

As mentioned earlier, the Random Waypoint mobility model which ns-2 provides may not be suitable for all types of simulation environment. This section examines another mobility model other than RWP, namely Reference Point Group Mobility model (RPGM) which uses the Bonnmotion-1.4 software as a data generating model as stated in [121].

RPGM is a very special and useful mobility model because it is suitable in many ad-hoc applications such as in military, Group tours, conferences, museum visits, emergency groups and rescue teams as these groups move mainly by forming clusters. RPGM is a mobility model in which mobile nodes move in clusters in the simulation area. Mobile nodes which are created by RPGM are divided into two parts: leaders and members (Cluster-heads and cluster-members). The direction of the cluster-heads is randomly chosen, and the movements of the cluster-members follow the direction of the cluster-head [122]. Figure 4.12 is a screenshot that shows a picture in the

NAM console after the end of the simulation created by RPGM and as the Figure 4.12 indicates that the nodes are clusters or groups. The simulation results for optimal setting of protocol performance using RPGM scenarios are stated below.

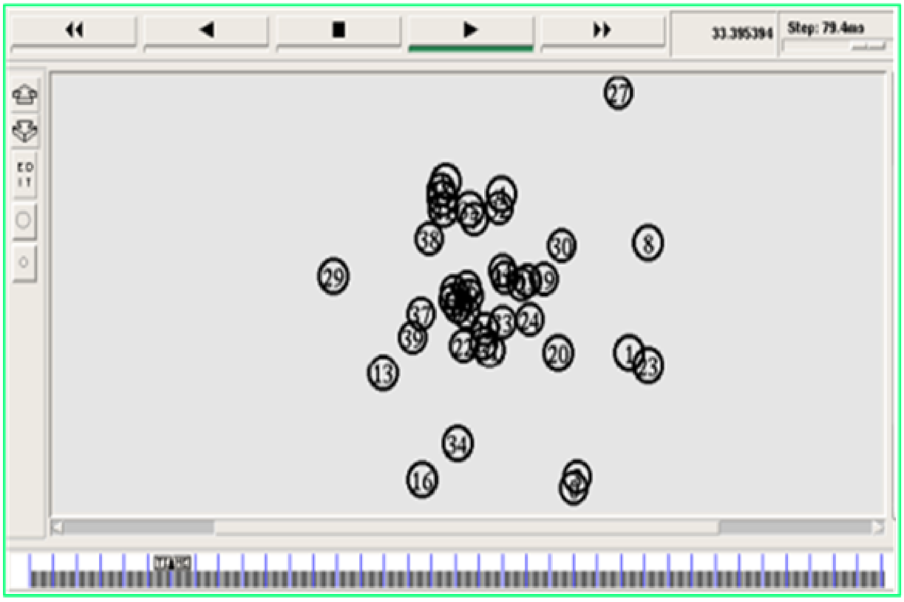


Figure 4.12: NAM Console for RPGM Model

4.5 Experiment of Pause Time Optimal Setting on RPGM

This section will analyze the performance of AODV protocol optimal setting using RPGM. These experiments have been conducted to finalize the maximum pause time optimal setting for AODV performance. In this set of simulations, our intention is to investigate the protocol's performance under RPGM when the pause time increases with varied scenarios. The results have shown that performance is very much dependent on the pause time value. The RPGM presented different results from the RWP model. RPGM results show that when the pause time is small, the protocol's performance outperforms compared to when the pause time is long.

On the contrary, the RWP results show that when the pause time is high, the protocol's performance is better. For instance, pause time optimal setting for RWP is 40 seconds while pause time optimal setting for RPGM is between 5 and 10 seconds. These different results indicate that there is no routing protocol for MANET that can provide efficient routing to any size of network. From that point of view, it is very important to run several simulations with different parameters as well as different mobility models. Thus, this research tested several mobility models in order to select the suitable mobility model for the developed protocol. However, testing with different environments informs us that there is no protocol that can be applied to all kinds of networks. In this experiment, the pause times increase from 5 up to 40 seconds and all other parameters are kept unchanged in the first scenario. What has to be kept mind is that each scenario is run five times, and these five times the pause time increases (5, 10, 20, 30 and, 40 s) while all other parameters are fixed. In the second, third and fourth scenarios, the number of nodes is doubled (from 10 to 20 nodes, 20 to 40, and 40 to 80 nodes) respectively and of course the pause time increases for all scenarios while the rest of network parameters are unchanged.

Table 4.3 indicates the scenarios that have been tested in this experiment. The following table contains four main scenarios and each of them contains five sub-scenarios. For each of these sub-scenarios, the pause time is varied (for example, pause times are 5, 10, 20, 30, and 40 s, while the number of nodes is 10 nodes only) while the rest of the parameters are constant or unchanged. When the first scenario has tested the five sub-scenarios with varying pause time, the second main scenario is continued with increasing the number of nodes and number of connection with 20 nodes and 8 connections respectively as the Table 4.3 has shown. This second scenario also tested same as tested the scenario one with five sub-scenarios except increasing the number of nodes and connections and of course the pause time is also varied. Subsequently, the third and fourth scenarios carry on with increasing the number of nodes and connections with 40 nodes and 80 nodes, with 30 and, 40 connections respectively.

Table 4.3: Varying Pause Time (RPGM model)

Parameters	**Values**
Simulation	ns-2
Protocol	AODV
No of node	10, 20, 40 & 80
Movement Model	RPGM
Traffic source	Constant Bit rate (CBR)
Simulation area	1000 m x 1000 m
Simulation Time	200 s
Pause time‘	5, 10, 20, 30, & 40
Node speed	20 m/s
No of connections	4, 8, 30 & 40
Group Size	5
Max. Distance to group	170
Group change probability	0.03
Group size deviation	1.0

4.5.1 Performance Metrics for Pause Time Optimal Setting on RPGM

As RFC 2501 describes, a number of performance metrics that can be used for evaluating the performance of a routing protocol for MANETs are four metrics. In addition, AODV developers used these four metrics [109]. Thus, in this research, was followed the general ideas described in RFC 2501, and used similar metrics such as Packet Delivery Ratio, Average End-to-End Delay, Normalized Routing Load and Routing Overhead (Normalized MAC Load). All these performance metrics are important, but the packet delivery ratio and average end to end delay are the most important for best-effort traffic. It does not mean that the other metrics are meaningless, but it means that the two first metrics have high priority than others. However, the normalized routing load is important as it will be used to evaluate the efficiency of the routing protocol.

4.5.2 Routing Overhead for Pause Time Optimal Setting on RPGM

This metric presents how the network enquiry packets control for intermediate nodes is huge. To evaluate the network efficiency, the routing overhead or Normalized MAC Load plays a significant role. Thus, it is vital for this research to figure out the factors which can be involved in the increasing of the network routing overhead. However, minimizing the network overhead is maximizing the network resources utilization with better performance. Figure 4.13 presents the experiment result for routing overhead. Figure 4.13 shows that the overhead is proportional to pause time. It indicates that the overhead increases while the pause time is increased. This experiment tested five different values of pause time, namely 5, 10, 20, 30 and 40 seconds. Figure 4.13 presents four scenarios, and each has a different value. These scenarios are analyse one by one for better overview. Look at the scenario one. When the pause time is 5 seconds the overhead is 54. When it increases the pause time to 10 s the overhead became 186, then 330, 408 (packets overhead) and finally when the pause time increase up to 40 s the overhead is worse.

The second scenario is totally different from the previous because the overhead started at 442 while in scenario one the overhead started at 54, because of varying node density in the network. However, the principle is still the same because when the pause time is increased, the overhead is also increased. Scenarios three and four are the same as these two scenarios increase the pause time, the overhead goes up. So, seeing the scenarios in Figure 4.13, the overhead is defiantly proportional to pause time and obviously the overhead will be low when the pause time is small. Thus, this experiment shows that choosing a smaller pause time gives the optimal setting for node pause time and indicates that the average performance of AODV protocol is when the node pause time is between 5 seconds and 10 seconds.

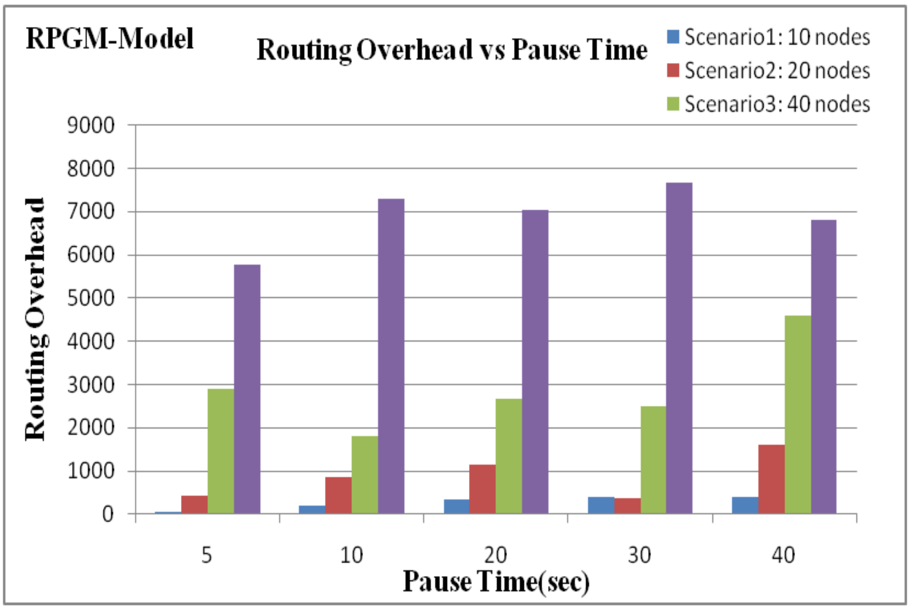


Figure 4.13: Routing Overhead Using (RPGM)

4.5.3 Packet Delivery Fraction for Pause Time Optimal Setting on RPGM

Figure 4.14 shows the result of Packet Delivery Fraction (PDF). Figure 4.14 shows that the packet delivery ratios are mostly constant whether the pause time increases or not. Only the scenario one shows a little bit of fluctuation where the pause times are 10 and 20 s, the PDF are 95.06% and 93.35% respectively. Scenarios two, three and four have shown the best result, and most values of PDF are about 98% and 99%. Nonetheless, the overall results for the packets delivery ratios based on RPGM model indicate that this model outperformed the rest of the models that have been tested in this research.

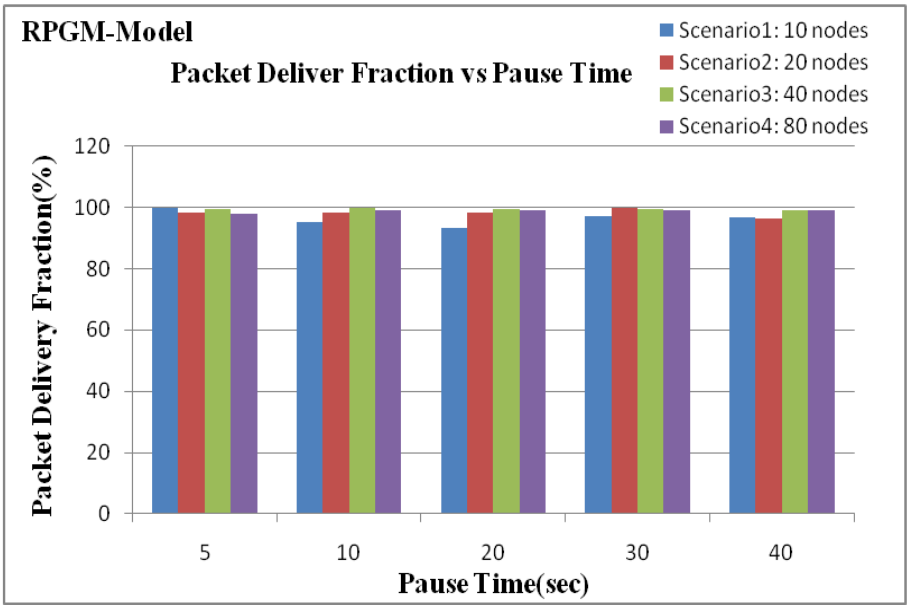


Figure 4.14: Packet Delivery Fractions (RPGM)

4.5.4 Normalized Routing Load for Pause Time Optimal Setting on RPGM

Figure 4.15 shows the simulation for Normalized Routing Load with the RPGM model. The objective of this part of analysis is to investigate the impact of the pause time on the normalizing route load in the network with the RPGM model. Figure 4.15 shows the scenarios of the simulation for normalizing routing load. It shows that as the pause time increases, the normalized routing load increases. For instance, when the pause time is 5 in scenario one the normalized routing load shows 0.05. When pause time is increased up to 10, 20, 30 and 40 s in same scenario, the results show 0.18, 0.33, 0.39 and 0.40 (these are the ratio of packets sent and data packets received) respectively. This analysis indicates that as the pause time goes up, the result gets worse which means that the network becomes more and more congested in terms of traffic load.

The rest of the scenarios are almost the same as the previous scenario (scenario one) and shows whenever the pause time increases the result of NRL increases. But scenarios two and three have shown that when the pause time is 30 and 10 the result does not follow the previous results which were increasing when the pause time increases. Instead, they decrease in this time as can be seen in Figure 4.15 whereby the results show 0.16 and 0.34 (NRL). Since most of the results have shown the same direction when the pause time is increased, it can be assumed these two cases accidentally happened because the ad-hoc network behavior is very changeable. NRL represents the number of routing packets transmitted per data packet delivered at the destination, to evaluate the efficiency of protocol's performance. However, this experiment indicates that when the pause time is between 5 and 10 seconds it is the optimal setting for AODV protocol when using RPGM model.

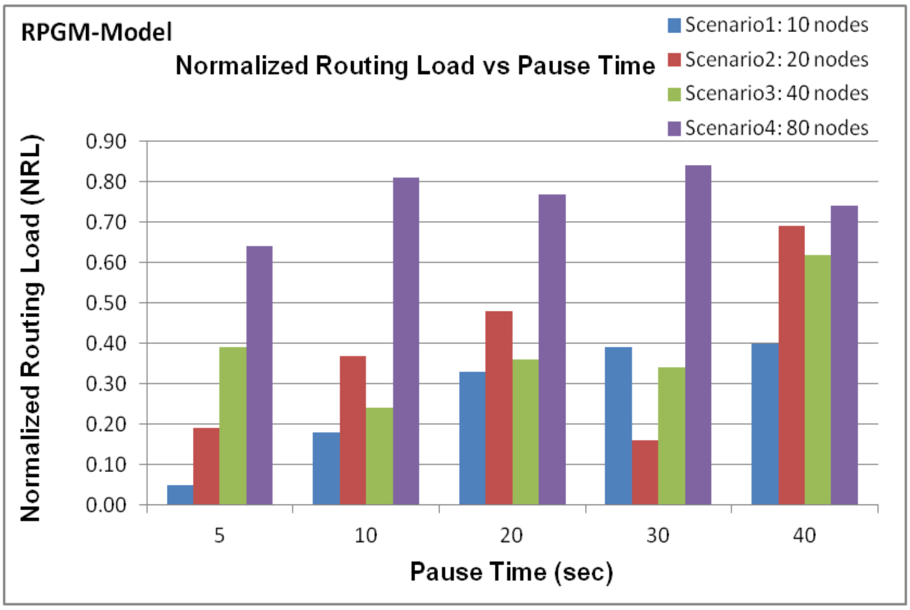


Figure 4.15: Normalized Routing Load (RPGM)

4.5.5 Average End-to-End Delay for Pause Time Optimal Setting on RPGM

Figure 4.16 illustrates the average end to end delay result for RPGM model. Figure 4.16 shows the delay of scenario one where the pause times are varying from 5, 10, 20, 30 and 40 s. It shows when the pause time becomes 30 s the average end to end delay is 11.81 ms. When the pause time is increased to 10 s the result for this scenario is also increased up to 113.23 ms. Then the pause time is increased up to 20 s, so the delay is also increased up to 204.43 ms. Again, the pause time is increased from 20 s to 30 s but as Figure 4.16 indicates in scenario one the result decreased 178.44 ms. Finally, the pause time is increased up to 40 s and the result decreased as well 135.22 ms. It seems that the average end to end delay is not that much affected by the varying of pause time. It is expected that the lower pause time will have a better performance average end to end delay than the higher pause time according to other parameters results in Figures 4.13, 4.14 and 4.15. Normally, the network parameters depend on one another, and usually there is no one parameter that cannot be affected by another vector in order to be independent completely. However, the explanation lies in that the delay can be independent to some extent.

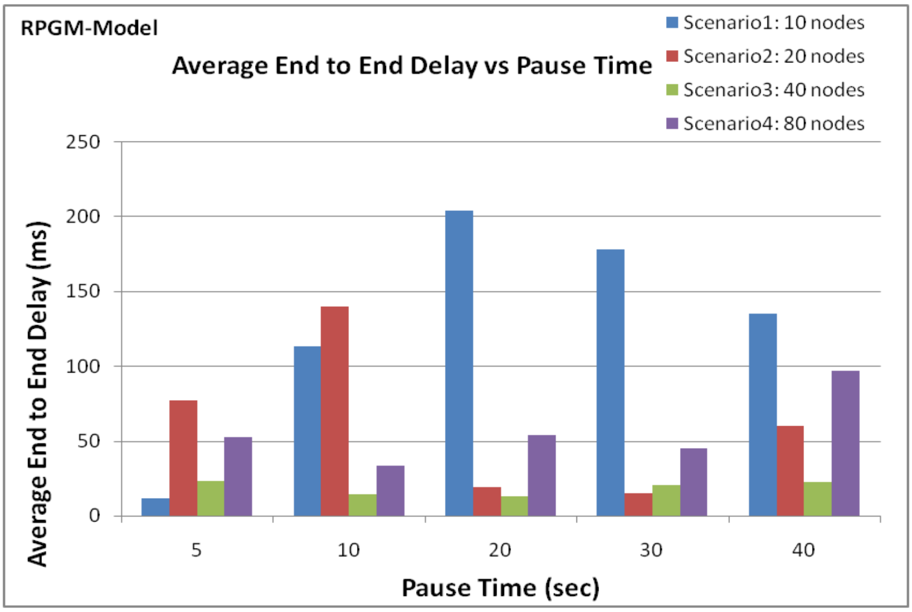


Figure 4.16: Average End-to-End Delay (RPGM)

4.5.6 Packet Loss for Pause Time Optimal Setting on RPGM

Figure 4.17 presents data packets drop. More overhead can lead to drop data packets in the network where it degrades the network performance. In terms of overhead, AODV has more overhead than other reactive routing protocols caused by AODV route query where routing overhead is proportional to the number of route queries. For instance, the source node for AODV will send a RREQ message if it does not know the route to the destination, then source waits for a while. If the source sends the second transmission of the RREQ message and does not receive RREP message within a time interval, it will drop the first packet in the queue and repeats the same procedure for the second data packet in the queue. In addition, if one of the forwarding nodes cannot succeed to find a valid route to the destination it will drop all data packets from its queue. All these things support to increase network overhead.

The results have shown that the dropped data packets in this experiment are very reasonable and much better than expected. Because, as mentioned above the AODV protocol has heavy routing overhead, which can cause a significant drop data packet. Figure 4.17 shows that dropped data packets for the scenario one are 2, 59, 90, 55 and 59 (the number of packets dropped on the way to the destination). The first experiment in this scenario has only 2 packets lost while the second, third, fourth and fifth xperiments have 59, 90, 55 and 59 packets lost respectively. Drops for scenario two are 49, 68, 83, and 158 while the third scenario results are 81, 83, 61, 170 and 167 (packets lost). However, the three first scenarios' optimal setting is when the pause times are 5 and 10 s.

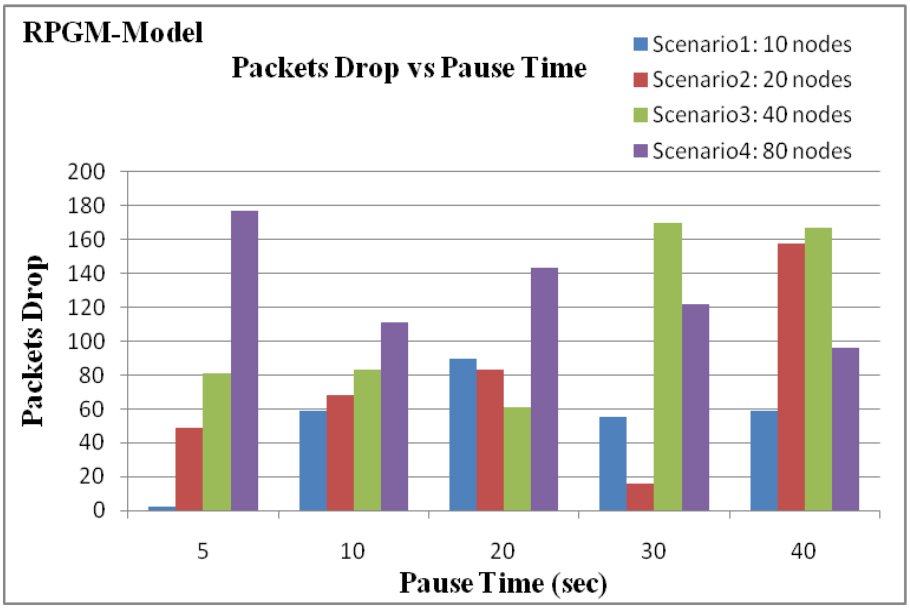


Figure 4.17: Packets Drop

4.6 Experiment and Topology Setup for Speed Optimal Setting on RPGM

In MANETs, the most common routing problem is an unpredictable topology change. This frequent topology change can lead to network partitions, especially when node density is low. This low density may affect the route discovery process and cause unnecessary rerouting because since the number of nodes is small the distance between them can be long due to mobility. MANET today are one of the leading technologies among networks, but at the same time it is also the one facing the biggest challenge. This is so especially of supporting sensitive applications, which require strict Quality of Service (QoS) such as Voice over Internet Protocol (VOIP) and video conference, which are delay sensitive due to their interactive characteristics. To evaluate the protocol's performance in terms of speed optimal setting, it has simulated various topologies with different parameters. RPGM is used in these simulations with 1000m x 1000m area. To explore the effect of speed both high mobility scenarios and low mobility scenarios with a constant pause time have been generated. The node's movement speed varied from 5, 10, 20, 30 and 40 m/s. The ad-hoc networks nodes employed in this experiment consist of 10, 20, 40 and 80 mobile nodes with 4 and 8, 30 and 40 source-destination pairs of connections. Constant bit rate (CBR) is used as the traffic generator with 512 packet size.

This experiment employed several scenarios with different parameters. The main objective of this experiment is to obtain the optimal setting of AODV protocol's performance regarding the mobile node speed. However, our ultimate goal in this experiment is beyond figuring out the optimal setting of AODV. This is a process which prepares the best path for the developed protocol to figure out the suitable future model on AODV protocol. Once the best model is known, it will be much easier than to apply all models. Thus, this experiment examines all these parameters to find out the optimal setting in these particular parameters.

Table 4.4 shows the scenarios that have generated four scenarios. Each scenario was carried out five times because the speed tests five times (5, 10, 20, 30 and 40 m/s) in each scenario with the rest of the parameters are constant. For example, the number of nodes is 10, source connections are 4 and pause time is 5 s but the speed varies from 5 up to 40 m/s the in first scenario. In the next scenario the speed varies from 5 to 40 m/s, but the number of nodes changes to 20 nodes and source connection is 8. The rest of the scenarios continue in a similar method until all five scenarios are tested.

Table 4.4: Varying Node Speed (RPGM-model)

Parameters	**Values**
Simulation	ns-2
Protocol	AODV
No of node	10, 20, 40 & 80
Movement Model	RPGM
Traffic source	Constant Bit rate (CBR)
Simulation area	1000 m x 1000 m
Simulation Time	200 s
Max. Pause time‘	5 seconds
Node speed	5, 10, 20, 30 & 4020 m/s
No of connections	4, 8, 30 & 40
Group Size	5
Max. Distance to group	170
Group change probability	0.03
Group size deviation	1.0

4.6.1 Routing Overhead for Speed Optimal Setting on RPGM

To evaluate the network efficiency, the routing overhead plays a significant role. In order to analyze the overhead more accurately, especially the AODV protocol, two main source vectors are important, namely route request (RREQ) overhead and Route reply (RREP) overhead. Figure 4.18 illustrates the experiment results for routing overhead for 4 different scenarios with various mobile node speeds. Figure 4.18 shows that whenever the mobile speed increases the overhead also increases. The overhead for scenario one are 152, 115, 38, 80 and 353 packets. These means that when the speed is 5 m/s the result for overhead shows 152 packets, but when the speed increases to 10 m/s the result for overhead is 115 packets. Subsequently, speeds of 20 m/s, 30 and 40 m/s have results 38 packets, 80 packets and 353 packets respectively. The experiment repeated five this scenario times with various speeds to figure out the speeds' optimal setting for AODV protocol performance. As illustrated in the Figure 4.18 when the speed is 20 m/s, it obtained the best result in this scenario. Thus the speed optimal setting for this scenario is 20 m/s.

This experiment indicates that when the speed increases the overhead increases as well. The explanation lies in when the network is in high mobility condition, the overhead increases due to the number of network hops is increased because of high dynamic nodes which join and disjoin in the network. As shown in the Figure 4.18 and above the number of overhead, the optimal setting of this scenario (second) is obtained when the speed is 30 m/s. The overhead for the third scenario are 2031, 1843, 2132, 6138 and 2420 packets and fourth scenarios overhead are 7705, 8975, 4369, 7217 and 6079 packets. These experiments confirm that the routing overhead is directly proportional to node speed (with network high mobility, with more network overhead). However, as indicated in the Figure 4.18 the average speeds optimal setting for AODV protocol is 20 m/s.

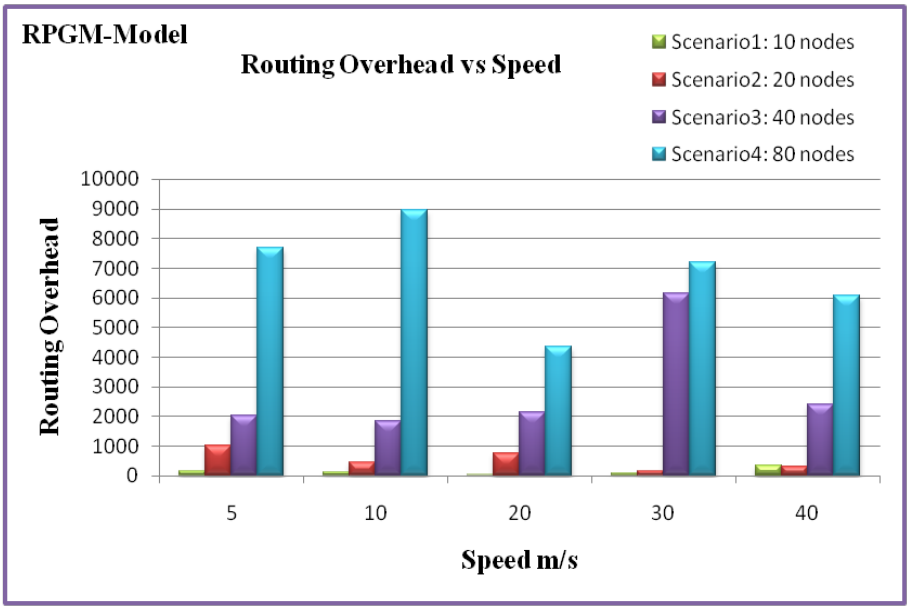


Figure 4.18: Routing Overhead for Speed Optimal Setting Using RPGM

4.6.2 Packet Delivery Fraction for Speed Optimal Setting on RPGM

This experiment focuses on speed for mobile nodes which have been varied in the range 5 - 40 m/s. Simulation results are illustrated in Figure 4.19. Since the packets delivery ratio is as a ratio of delivered and sent packets, the importance of this metric is obvious. It can be said that the overall networks well being depends on the scalability of the packets ratio. This experiment was carried out to identify the node speed's optimal setting for AODV using RPGM model. The results for packets delivery ratio of this experiment are as illustrated in Figure 4.19 where the overall ratios is very high. In order to locate the optimal setting of this particular event, it has to be analyzed one by one (scenario to scenario).

Scenario one, includes 10 nodes, 4 connections, maximum pause time 5 s and varyiing speeds, which were repeated five times. The results of this scenario for delivered and sent packets ratio are 87.32%, 99.53%, 100%, 99.63%, 85.28%. For instance, when speed is 5 m/s the ratio is 87.32% while when the mobile node speed was increased up to 10 m/s, the ratio becames 99.53% and again when the speed was increased up to 20 m/s the ratio reached the best result in this scenario, which is 100%. In this case, the optimal setting is when the speed is 20 m/s. The second scenario includes 20 nodes, 8 connections, maximum Pause continues as 5 s and varying speeds were repeated five times. In this scenario, some vectors are changed such as node density and number of connections, and these vectors may affect the result. However, the results of this scenario for packets delivered ratio are 84.00%, 99.46%, 99.21%, 100% and 98.83%.

The results of this scenario show slightly lower than previous scenarios' results and it shows that those increased vectors are effected to some extent. However, the results and mobile node speed ratios are as follows. When the speed is 5 m/s the packets delivery ratio is 84%. Then the node speed increased up to 10 m/s and the ratio is also increased to 99.46%. When the speed is again increased to 20 m/s the ratio becomes

99.21%; then the speed once again increased to 30 m/s, the ratio becomes 100%. This point is the highest rate that the ratio reached in this scenario with the optimal setting observed in this scenario is 30 m/s. Scenarios two and four are not that much different from these scenarios and therefore need not be addressed here. Nonetheless, as indicated in Figure 4.19, the average speed optimal setting for AODV using RPGM in terms of packet delivery ratio is more or less 20 m/s.

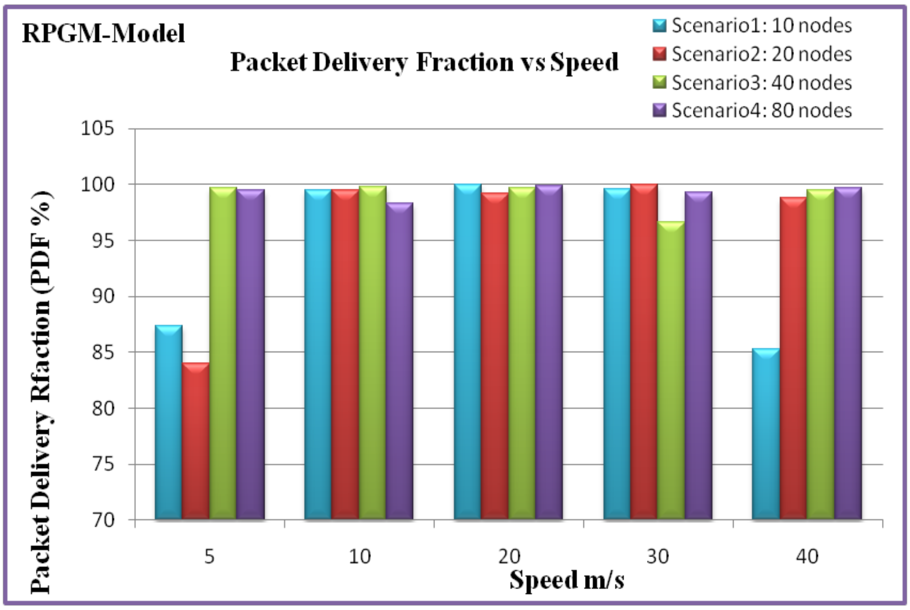


Figure 4.19: Packet Delivery Fraction for Speed Optimal Setting Using RPGM

4.6.3 Normalized Routing Load for Speed Optimal Setting on RPGM

This sub-section examines normalized routing load vs. speed using RPGM model. Figure 4.20 illustrates the experiment results for NRL for all experiments in four scenarios focusing on varying mobile node speeds to figure out the optimal setting for AODV protocol regarding RPGM model. The results in Figure 4.20 show the scenarios one and two have lower routing packets transmitted than the three and four scenarios. With scenario one, the results for NRL are 0.16 with the node speed 5 m/s, 0.11 (NRL) with the node speed 10 m/s, 0.04 (NRL) with node speed 20 m/s, 0.07 (NRL) with node speed 30 m/s and finally 0.38 (NRL) while the node speed is 40 m/s. These results show that with the increase of speed, the normalized routing load increases a bit caused by more route change because of mobile high speed. For the second and third scenarios, as illustrated in Figure 4.20, the results are also increasing when the mobile node speed is increased. Finally, scenario four shows the highest normalized routing load in these four experiments. The explanation lies in two vectors: one is that the number of mobile nodes is increased, which can contribute to the routing packets transmitted per data packet. Another reason is because AODV protocol suffers routing control message caused by mobile high speed. This happens because AODV has periodic activities in order to exchange HELLO messages information among neighbors and does not use cache to store the routes. Therefore, with the increase of speed, the routes change more frequently and there is a strong need of finding new routes. However, as presented in Figure 4.20 the optimal setting for mobile speed for AODV protocol is between 10 m/s and 20 m/s.

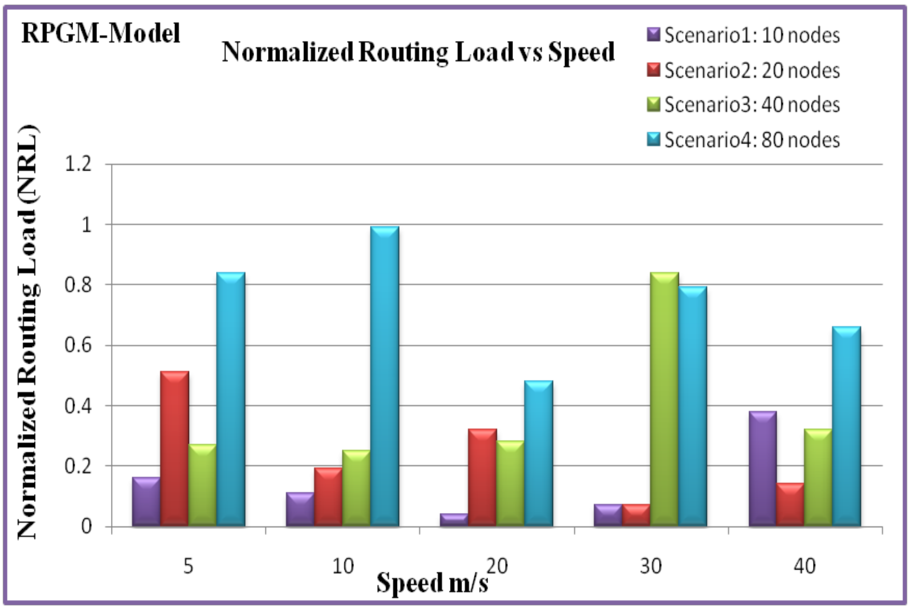


Figure 4.20: Normalized Routing Load for Speed Optimal Setting Using RPGM

4.6.4 Average End-to-End Delay for Speed Optimal Setting on RPGM

This experiment tests Average End to End Delay of data packets from source to destination. Normally when decreasing the mobile node speed for lower values, AODV suffers from higher delays, but this requirement does not always fulfil. With RPGM, the network nodes are organized as a group and each group either communicates with each other or communicates with another group. It depends on how the network topology is sets up.

This group pattern can to some extent experience that the network partitions because of groups. The mobile nodes are not always in the transmission range of each other, and there might not be enough mobile nodes to form a sequence of hops for packet forwarding. Thus, to some extent, it might result in an excessive end to end delay as it has to wait for network reconnection. Figure 4.21 illustrates the results for this experiment. Although the experiment is conducted with RPGM, the delay performance does not suffer from transient partitions that exist in the sparse network in RPGM model. In Figure 4.21, scenario one shows an excessive end to end delay when the mobile node speed is 40 m/s. The reason could be because the network becomes much sparser or is effected by mobile high speed by HELLO messages exchanging. Nonetheless, in the conventional wisdom, the longer the path lengths, the higher the probability of a packet drop which causes longer delay. On the other hand, with a lower delivery fraction, samples are usually biased in favor of short path lengths and thus have less delay [123, 124]. However, the results for these experiments are overall good, which indicate the overall network smoothness.

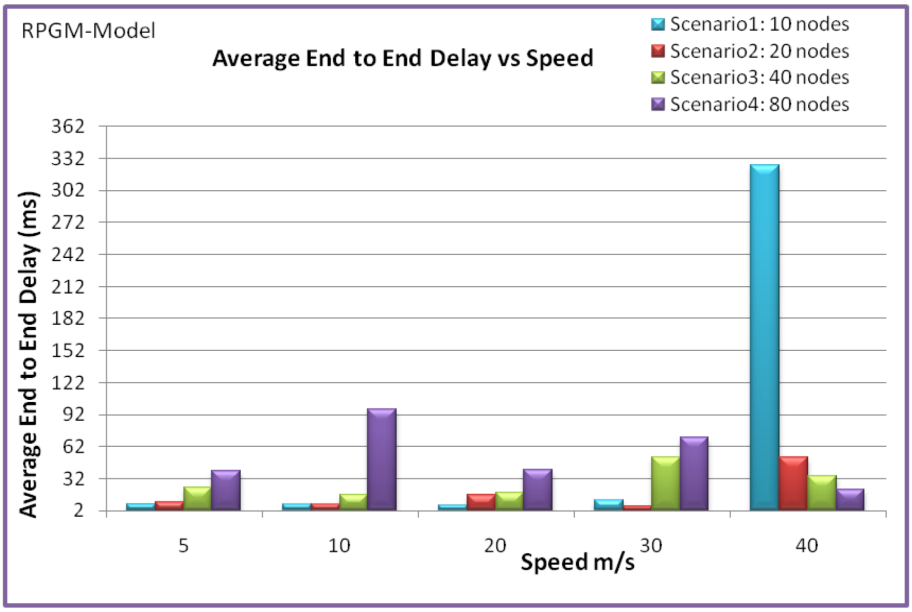


Figure 4.21: Average End-to-End to Delay for Speed Optimal Setting Using RPGM

4.6.5 Packet Loss for Speed Optimal Setting on RPGM

The rate of drop data packets is vital for network efficient or inefficient evaluation. However, three performance metrics are indirectly proportional to each other for network performance evaluation, including packet delivery ratio, the network routing overhead and drop data packets. In the case where the packets delivery ratio is high, the drop data packets rate will be small and of course the network routing overhead should be also small. Figure 4.22 illustrates the packet drop. The results show that the dropped data packets are various, sometimes dropped data packets is zero while sometimes 359 packets are dropped, which is slightly high. For instance, the results for scenario one are 120, 12, 0, 7, and 169 packets are dropped respectively. This result where a dropped data packet is zero confirms that the routing overhead, packet delivery ratio and drop data packet depend on each other. Because as indicated in Figure 4.19 (Section 4.6.2) the optimal setting for routing overhead is when the speed is 20 m/s. In addition, as indicated in Figure 4.20 the optimal setting for the packet delivery ratio is more or less 20 m/s and here in the drop packet for optimal setting is 20 m/s as shown in the Figure 4.22.

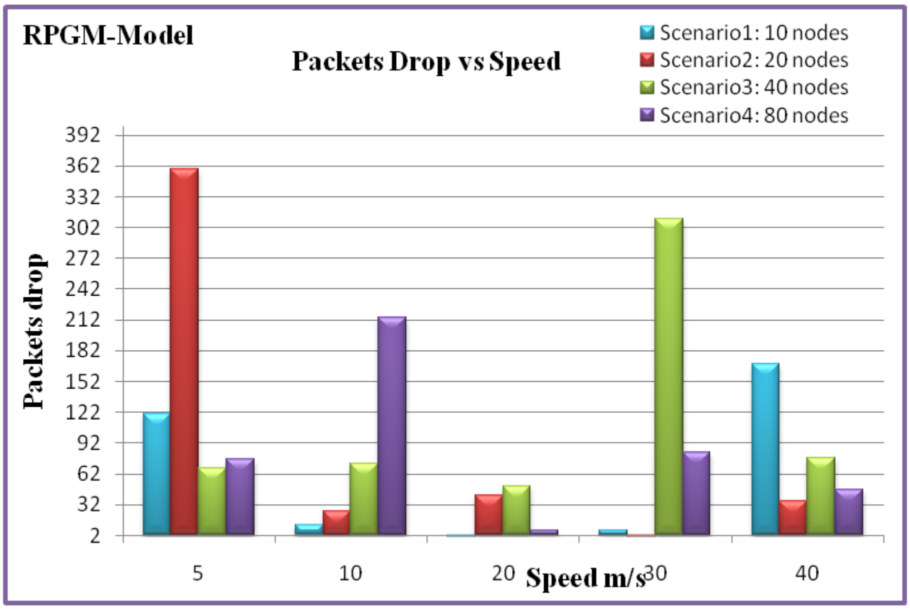


Figure 4.22: Packets Drop for Speed Optimal Setting Using RPGM

4.7 Summary

This chapter introduces empirical experiments where it draws on pre-experiment test for mobility models where it investigated pause time optimal setting for Random Waypoint (RWP) model and speed optimal setting as well. Finally, this chapter discusses different experiments with different metrics performance against pause time and speed optimal setting for Reference Point Group Mobility model (RPGM). Nonetheless, after empirical experiments of AODV with different mobility models for optimal setting have been done and specifying the optimal seting of these parameters to implement the new developed protocol in this chapter, the design issues of the Predictive Divert Failure Route Protocol (PDFRP), and its submechanisms will be presented in the next chapter.

CHAPTER FIVE

THE DESIGN OF PREDICTIVE DIVERT FAILURE ROUTE PROTOCOL (PDFRP)

Chapter Four presented empirical experiments of AODV where two mobility models for optimal setting experiment were tested. This chapter introduces the design of the new extended routing protocol developed by this research, nemaly, the Predictive Divert Failure Route Protocol (PDFRP). The chapter presents the existing obstacles regarding routing protocol on the ad-hoc network and especially how it can be overcome by the developed routing protocol that the research has come up with. Section 5.1 presents an overview of Mobile Ad-hoc Network (MANET) implementation behavior explaining distinctive communication of MANET from other networks as nodes can move randomly while communicating with each other. Section 5.2 presents the philosophy underlying the idea of this research and AODV originality namely, Destination Sequenced Distance Vector Routing (DSDV) and how it can be possible to mix up the AODV with its originality and derive a new hybrid routing protocol. Local route repair mechanism for AODV standard link failure and the solutions for link failure problem included the design of PDFRP and its submechanisms such as the Upstream Notification (UN) mechanism are presented in Sections 5.3 and 5.4. Section 5.5 including the Models' Design such as Detection Model, New Path-Model and Analyzer algorithm as well. Sections 5.6, 5.7, 5.8, 5.9, 5.10 are detailed the link prediction algorithm with various types of predictions such as distance prediction, time prediction method, signal propagation models and prediction through critical time. Finally, Section 5.11 presented UN mechanism with details followed by its sub-sections.

5.1 Overview over MANET Implementation Behavior

The distinctive feature in MANET from other networks is that the nodes can move randomly while communicating with each other with the absence of Access Point Relay (APR), which requires the routing protocols in an ad-hoc network to quickly respond that highly dynamic network topology change in order to guarantee successful data packet delivery. As a result of the limitation for radio propagation, if two hosts are not within a given transmission range of each other, they will not be able to communicate directly. In such circumstances the communication must pass through one or more other hosts in the network. Since every single host in MANET moves in an arbitrary manner, the routes are subject to frequent disconnection. Upon link failure, the period of route reconstructing, packets can be dropped, which causes significant throughput degradation for the network.

However, in reactive routing protocols such as AODV and Dynamic Source Routing (DSR) data packets can be lost in the middle of the routes constructed by reactive protocols, if the link between two mobile nodes on the route becomes broken due to an intermediate node suddenly switching off [125, 126, 127], standard on-demand ad-hoc network routing protocols such as AODV continue to use a route until a link totally breaks down. This research has designed and come up with a new method that avoids the link being completely disconnected. In the PDFRP implementation, the prediction algorithm utilizes signal power strength from the received packets to predict the link breakage time. In addition, it also utilizes signal power strength to predict the link breakage through the distance between two mobile nodes, which can also be obtained by measuring the received signal powers as well.

The aim of this research is to modify and design an existing ad-hoc network reactive routing protocol, namely Ad-hoc On-Demand Distance Vector (AODV) into a hybrid protocol by introducing PDFRP proactive behavior to improve its performance. The developed protocol route maintenance is based on the prediction algorithm to predict a link breakage caused by randomly mobile node movement. Upon the link being broken soon, the developed protocol will take action and divert the link into a new path without sending a warning message to the source node.

5.2 The Underlying Philosophy

The idea behind this study is to convert the reactive routing protocol into partially proactive routing protocol in the way that the behavior of the developed protocol acts as a uniform. The new uniform mechanism works as follows. The AODV protocol originally had been driven from proactive protocol, namely from DSDV protocol. The idea behind that the DSDV protocol to form into a reactive routing protocol was to reduce an unnecessary periodical message exchanging that frequently updates the routing tables regardless of need for proactive routing protocol. Departing from that point of view, the DSDV had modified into on demand routing protocol namely AODV. Then this new developed reactive routing protocol namely PDFRP has been able to solve that tremendous unwanted network overhead caused by unnecessary updatingn of tables leading to generating the packets on demand only. This research presents a new mechanism that combines these two different routing families and Constructs Uniform Design (CUD). In fact, the CUD acts as both reactive and proactive routing protocol mechanism in one way or another. The CUD mechanism has dual functions, which provide a new opportunity in mobile ad-hoc networks. Generally, the reactive routing protocols and proactive routing protocols differ drastically in the fact that they belong to two different routing families. As mentioned above, this new mechanism will standardize the reactive and proactive mechanism where the new mechanism works as a reactive routing protocol in terms of the route request while it works as a proactive routing protocol in terms of route maintenance. AODV protocol is reactive using routing tables with one entry per destination, which means that the information about the destination puts one time into the table and is not maintained periodically as proactive protocol does. Upon communication between two nodes, a source node initiates a route discovery process to locate the destination node. In this case, the source node broadcasts a query packet requesting a route to be set up to the destination. A Route Reply (RREP) from the destination is sent back to the source node by the destination or at the same time it may be sent by any intermediate node that has a current route to the destination node as stated in [128].

The greatest challenge in a reactive routing protocol is the route re-constructing of the link failure, because of its poor route maintenance. While a proactive routing protocol has a mechanism for route maintenance called periodically message exchange to update the routing tables. This lack of route maintenance for reactive routing protocol can cause more link failure in ad-hoc networks. From that perspective, it shows that there is a need to have a solution between the reactive and proactive world. Therefore, this research developed PDFRP protocol that includes UN mechanism to come across a uniform protocol that avoids the limitations of reactive routing protocols such as lack of information exchange among mobile nodes in the network. Sometimes it will not convey unnecessary updating information to the network which is also another limitation caused by proactive routing protocols. However, this new protocol utilizes link state prediction algorithm to maintain certain information among nodes on an active link. To avoid unnecessary network congestion and routing overhead, this updating information is active only when there is a link between at least two mobile nodes in the network, otherwise, it is switched off. Since the research is based on a new mechanism that acts as proactive and at the same time acts as a reactive upon the link establishing process, the PDFRP uses traditional reactive route establishing process. On the other hand, after the path between the source and the desired destination is established, the mechanism uses the prediction algorithm, which acts partially as proactive mechanism. This happens because the nodes that are involved with this ongoing link or the active path is predicting the link status. Therefore, this part of the mechanism can be considered as a proactive to some extent. Keeping that in mind, the nodes which are not involved in this active link are not exchanging anything. In other words, they behave as AODV standard. Figure 5.1 presents the route discovery process for AODV standard. This part of the work acts as a reactive routing protocol because the source broadcasts the route query packet to the all its neighbors which in turn rebroadcast until the request reaches the destination node.

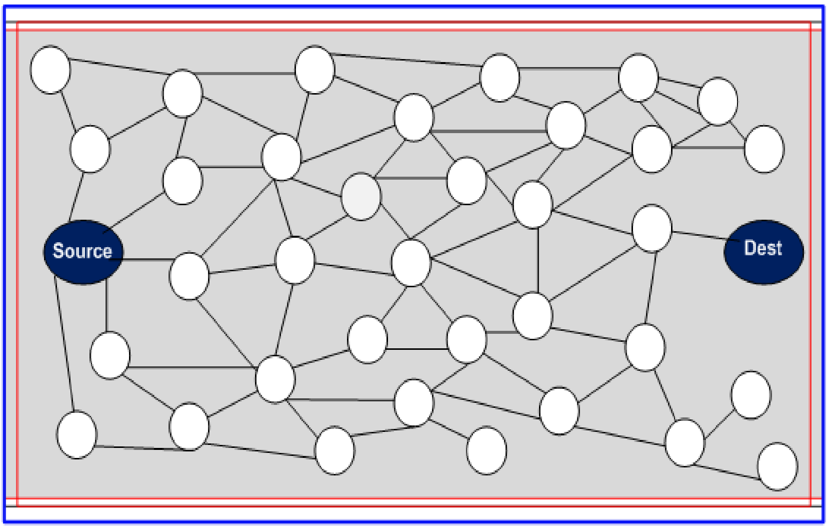


Figure 5.1: Discovery Process

Figure 5.2 illustrates the route maintenance process. The route between the source node and destination node through A, B, C, D and E have to be maintained by the prediction mechanism. The nodes (A, B, C, D and E), that go through these routes are always active in order to have the link status information of PDFRP. This information tells whether the link signal is weak or not. In case it is weaker, than an acceptable signal strength, then it takes action by diverting data through another link as explained in the next section.

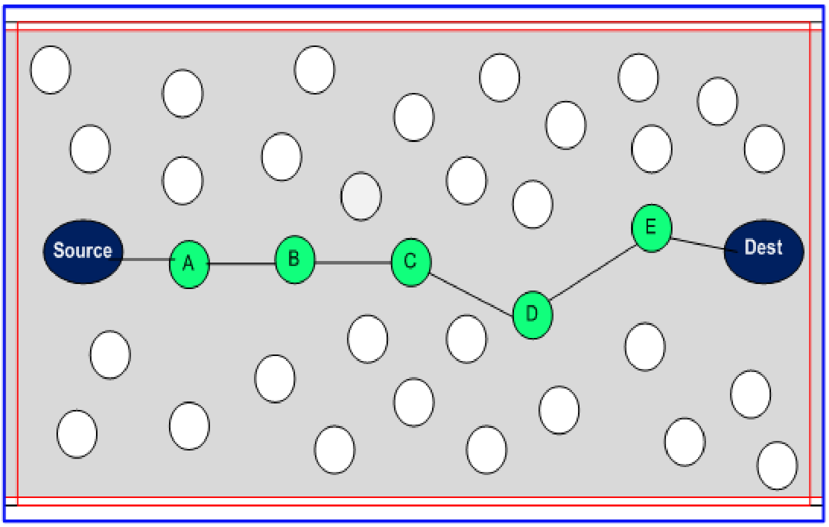


Figure 5.2: New Route Maintenance Mechanism

5.3 Link Failure in Ad-hoc On-Demand Distance Vector (AODV)

The main objective of this research is to enhance a link failure of AODV protocol by developing PDFRP protocol and UN mechanism to avoid a complete link breakdown due to the node mobility and unnecessary error message to the sender.

Figure 5.3 illustrates how AODV standard handles the link failure matter. As Figure 5.3 describes, after the link is broken, Current Node (C-N) sends an error message to the sender. Then the sender will rebroadcast a new route request throughout the network which results in congestion, delay, overhead and high normalized routing load (NRL). AODV standard has a local routoe repair mechanism, but this mechanism is suitable only in the case where the link failure occurs near the destination [129]. So the case where the link failure happens far from the destination, might not be applied by the current AODV link failure mechanism. Thus this research comes up with a mechanism as an alternative to the current mechanism, which is applicable whether the link failure happens far or near to the source or destination. As shown in Figure 5.3, the distance, where the link failure happens is far from both the source node and destination. In such a case, the current mechanism of AODV has only one option, which is the current intermediate node has to send a Route Error message back to the source node. Then, the source reinitiates a new global route discovery to all networks which causes a significant network-overhead and congestion as well.

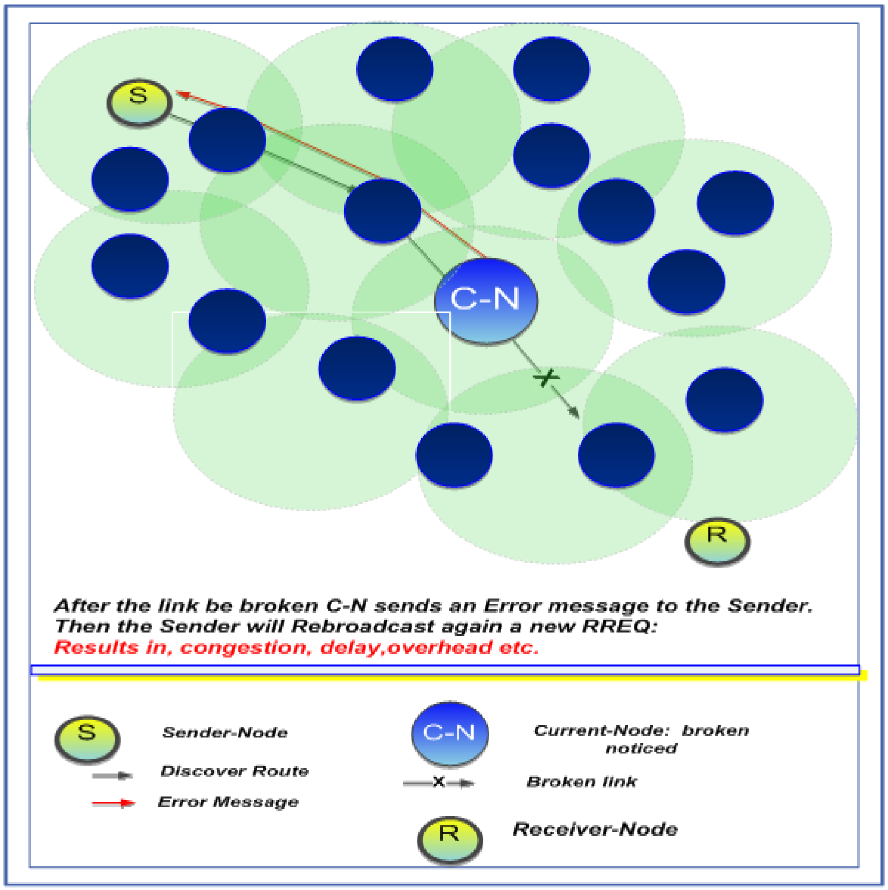


Figure 5.3: AODV Standard Link Failure

5.4 PDFRP Solutions for Link Failure

This research developed two mechanisms in order to maintain the link sustainability for mobile ad-hoc network. The first mechanism is to divert the route if the current active link is going to be broken soon. By this, it utilizes link state prediction through a signal power. In this case, the research developed a checking algorithm which monitors the link status for C-N (Current Node) neighbors where it verifies whether the C-N can find out a node that has enough signal power and at the same time has a route to the desired destination. The second mechanism, is Upstream Notification (UN) mechanism. With UN mechanism, if the first mechanism does not succeed to divert the route due to the neighbors not fulfilling the requirements, the notification signal sent to the next upstream node then takes action to monitor its neighbors.

As described by Abdule et al. [130], the developed protocol handles the link failure problem differently from the existing method. This protocol is supposed to eliminate the route regenerating by the source upon link failure on the way to the destination. Figure 5.4 demonstrates the mechanism topology and presents how the network behaves when the link is about to be broken soon. As the topology of Figure 5.4 illustrates, the link between C-N and "Moving Node" going to be broken is due to the movement of the intermediate node (Moving Node). Most likely it is going to be out of the current transmission range and this kind of limitation can be avoided or mitigated by a link prediction using equations (critical time model) from 5.13 to 5.26 stated at the end of this chapter.

As mentioned above, the research has come up with a new method for link failure problem, and it will be obtained through the prediction of signal strength of an active route diverting the data by the current node into a new path. More details about the diversion and how the new path is created can be found by referring to Models' Design and flowchart diagram as well in the next section. As illustrated in Figure 5.4, with the help of the detection of signal strength, C-N noticed that the link forwarding data to the next hop will be broken soon. The C-N node constructed a new path and diverts the data through the new path smoothly without packet loss. This method will totally avoid sending a Route Error message upon link failure. Thus, it eliminates the route discovery process initiated by the source after the link is broken. It results in minimizing congestion, delay, and overhead in addition to enhancing the overall network well-being. Nonetheless, the PDFRP protocol could function as an alternative solution for ad-hoc network, especially reactive routing protocols such as AODV and DSR as well, and it will be an acceptable mechanism for the overall wireless route discovery enhancement. Details of how the developed protocol functions will be explained in the next section.

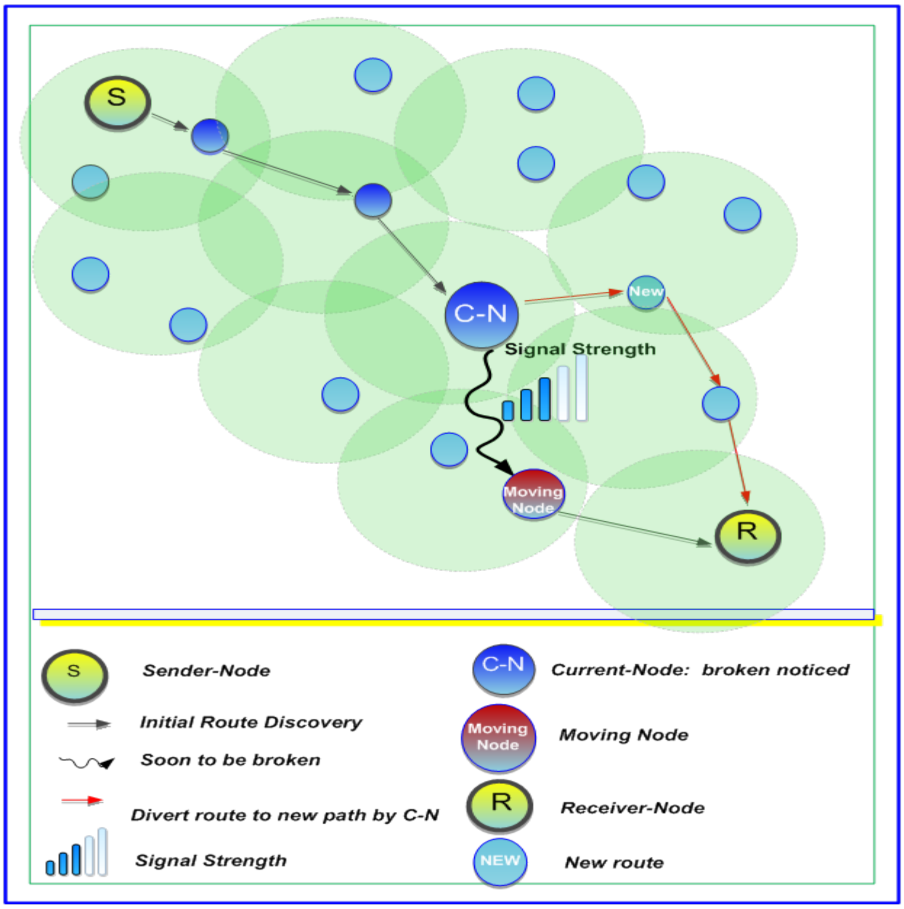


Figure 5.4: PDFRP Solutions for Link Failure

5.5 Research Models

To achieve the main goal of the study, the research has carried out very useful models in order to avoid a link failure in MANET and constructed a new direction locally (where the link failure takes place). In this respect, PDFRP has developed two main models Detection Model (DM) and New Path-Model (NPM). The main functions of these models are to predict the signal strength to determine a link status before it becomes invisible and find a new direction to the destination to divert the current link into a new route with a strong transmission. In addition, an Analyzer Algorithm is also developed to interconnect the models. Finally Upstream Notification (UN) Model is also developed as well. Figures 5.5 and 5.6 show the research models' design and Models' interconnections flowchart as well.

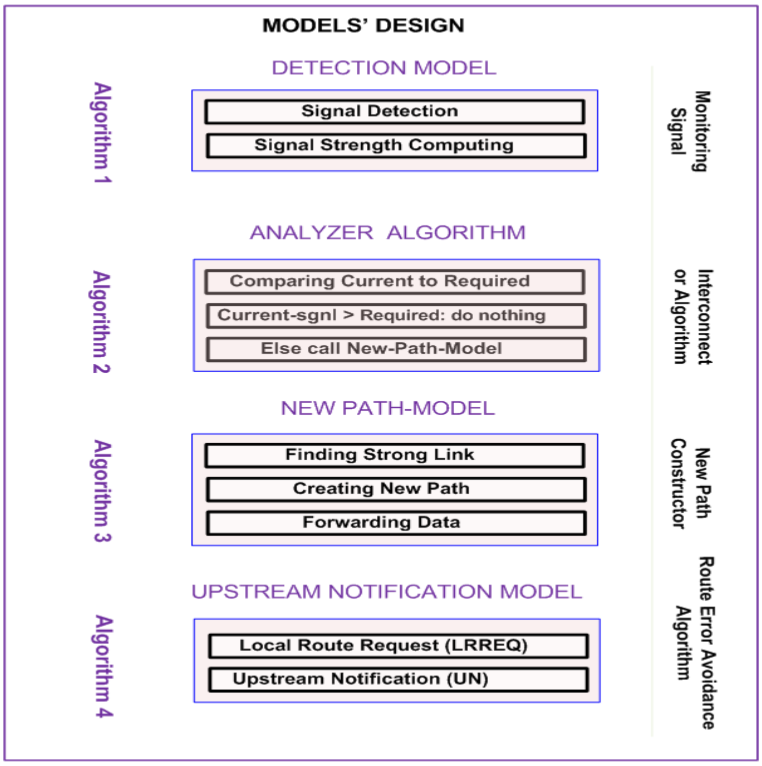


Figure 5.5: Research Models' Design

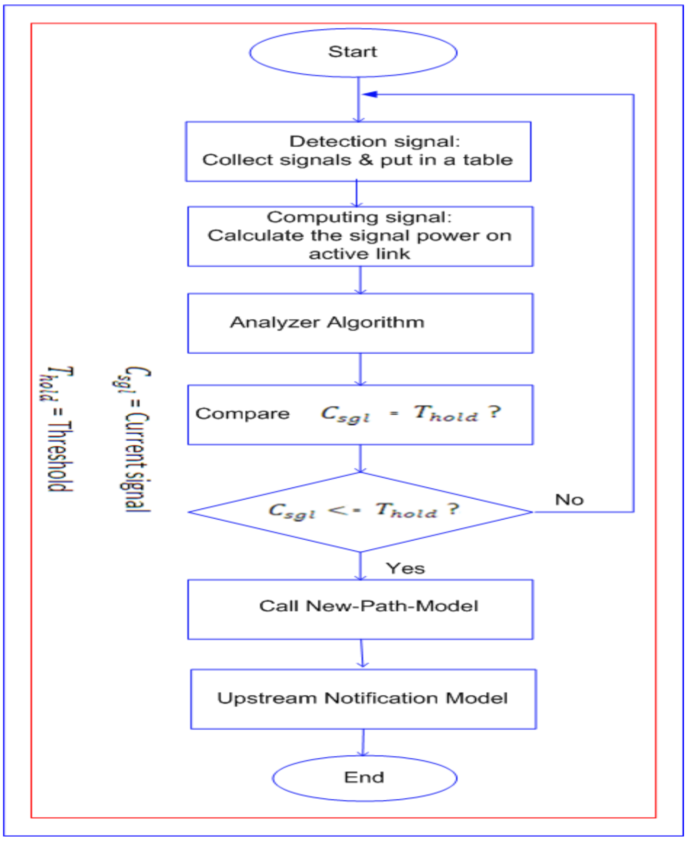


Figure 5.6: Models' Interconnections Flowchart

5.5.1 Detection Model

The detection model contains two sub-functions: detection signal function and computing signal strength.

i. *Detection Signal Function:* PDFRP utilizes the link state prediction method through the signal strength by using mathematical equations to estimate when two mobile nodes are going to disconnect each other. As described in link prediction and validation section in this chapter, there are two main ways to predict the link connectivity mathematically: distance and time. The main task of this function is to collect the current link signal status which will be used for predicting the link failure.

ii. *Computing Signal Strength:* As shown in Figure 5.6 (Models' Interconnections Flowchart), the signal status is put in a table by Detection Signal function. Thus, the Computing Signal Strength picks up the signals from that table and measures the status of the signal power and this status will be used to determine the circumstance of the current connection, whether it will be broken soon or not.

5.5.2 New Path-Model

The new path model contains three functions: finding strong link function, create new path function and forward data. They are elaborated in the following.

i. *Find Strong Link Function:* This function utilizes wireless standard receiving signal status where the initial signal power is standard (sender signal power is known). From this signal status, it determines whether it needs to take action or not. However, this action will be taken if the current link signal status is less than the signal power threshold. If this requirement is fulfilled, the current node (the node that noticed the link will fail soon) observes all available signals of neighboring nodes to find a node that has a stronger signal compared to the current connection signal strength.

ii. *Create-New-Path Function:* When the above conditions are fulfilled the Create-new-path function will construct a new path (new direction) and diverts the data through the new path as shown in Figure 5.4.

iii. *Forward Data Function:* Finally, when the new path is finalized, the Forward Data function will transfer the data through the new path. In Figure 5.6 shows more details about how the models and their algorithms are interconnected.

5.5.3 Analyzer Algorithm

The Analyzer algorithm is a decision maker of the Models. As the diagram is illustrates, the Analyzer algorithm compares the current signal to the signal power threshold ($C_{sgl} to T_{hold}$) and tests the condition ($C_{sgl} < T_{hold}$) as well. It gives an order to all actions on the models to be interconnected and interlinked with each other and interrelate them in order to unify the functions of the models.

5.5.4 Upstream Notification Model

As Chapter Two was mentioned a major negative impact and challenge of ad-hoc network is how to find an alternative route when link failure happens in an intermediate node, in order to avoid sending error message to the source node up on link failure which leads to re-initiating route discovery process. Upstream Notification (UN) Model is a route error avoidance algorithm which developed in this research and it is an alternative mechanism to solve the above mentioned drawback. The detail of UN mechanism including its functionality and how does it work is explained in Section 5.9.

The Models' interconnections flowchart illustrates how the functions of the models and the analyzer algorithm are correlated and harmonized with each other. As shown in Figure 5.6, the first task of the detection model is to monitor the signals and keep them into a place without taking any action while its second task is to compute the signal power. Then the analyzer algorithm compares the last signal power to the required transmission range. If the result is negative the New-Path-Model will operate to handle the issue and finally in case the whole operation is failed the Upstream Notification Model will take over to circulate a local route request to its neighbors as described in Figure 5.16 in Section 5.9.

5.6 Dependence of Signal Strength and Distance Experiment

This section introduces the mathematical analysis through link state prediction to calculate the distance between two nodes and link connections remaining time. As mentioned in Chapter Two as well as later in this chapter, many radio propagation and link prediction models have been proposed to calculate the received signal strength and formulas that have been used in this research are shown in Figure 5.7.

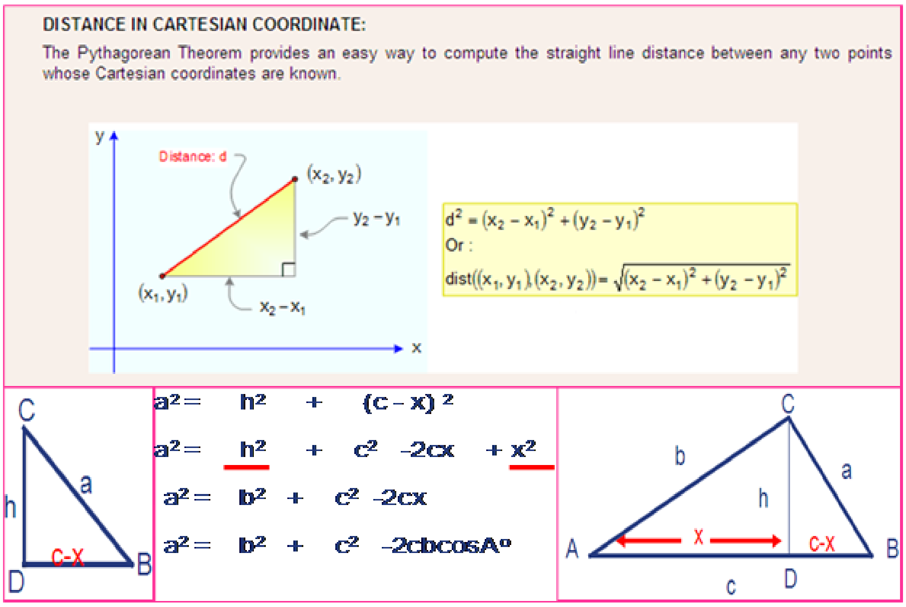


Figure 5.7: Distance in Cartesian Coordinate

The question applies Pythagoras formula to triangle CDB in Figure 5.7$a^2 = h^2 + (c-x)^2$, squaring out the bracket from above equation. Then it will be: $a^2 = h^2 + c^2$ -2cx +x^2. To integrate triangles CDB and CAB in Figure 5.7, the h^2 and x^2 should be substituted into b^2, so the result will be: $a^2 = b^2 + c^2$ -2cx. Then according to Pythagoras formula, the angle A(CAB) is equal $cosA = \frac{x}{b}$, so if "x" is the subject then the "x" will be : $x = bcosA$. From the above deriving calculations, the Cosine Rule Formula (CRF) by Pythagoras Theorem will be: $a^2 = b^2 + c^2$ -2$cbcosA$. Pythagoras formula can easily calculate an angle if one knows all sides of the triangle. An example, $a^2 = b^2 + c^2 - 2cbcosA$, if you take $b^2$and c^2 across, then $-2cbcosA = a^2 - b^2 - c^2$, then the value of the "A" for the CAB will be: $cosA = \frac{a^2-b^2-c^2}{-2cb}$, so, top and bottom are divided by -1. The positive value for the angle will be: $cosA = \frac{a^2+b^2+c^2}{2cb}$ as stated in [131].

Based on the above Pythagoras Cosine Rule Formula, an experiment using MATLAB tool for distance between two moving nodes is tested. This test has been undertaken in order to predict when the link will be disconnected as illustrated in Figure 5.8, which shows four triangles with different sizes both in length and height sides. The length side shows the varying time from t_0 when the connection was established up to the last calculation time, t_3. The altitude side shows the distance between the transmitter and receiver, $d_0 - d_3$. In that situation in mathematical point of view, it is obvious when the angle is increased, the distance of node A and node B is also increased. For instance;

$$d_0 = \sqrt{(13 - 2cos42(2)(3))} < d_1 = \sqrt{141 - 2cos60(2+8)(3+8)} \tag{5.1}$$

$$d_2 = \sqrt{525 - 2cos70(2+16)(3+16)} < d_3 = \sqrt{1165 - 2cos90(2+24)(3+24)} \tag{5.2}$$

This experiment proves that the received signal power solely depends on its distance to the transmitter, because as can be seen the graphs for the triangles in Figure 5.8 from the time t_0 to time t_3, the distance d_0 and the distance d_3 is obviously different. On the other hand, the signal power when the distance is equal to d_0 and the signal power for the distance is equal d_3 should be also different because the signal performance solely depends on the length of distance between the transmitter and the end-receiver.

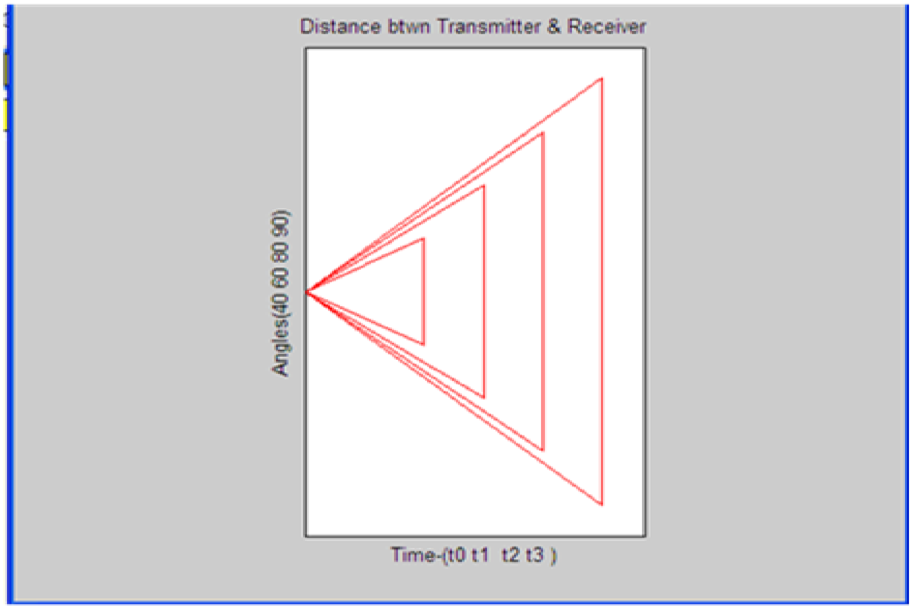


Figure 5.8: Prediction Experiment

5.7 Mobility Prediction Methods

Basically there are two methods to predict the mobile nodes' connectivity, namely, Distance and Time.

5.7.1 Prediction with Regards Distance

In the distance method, the received signal power solely depends on its distance to the transmitter. In this method, (as mentioned above) assumes that the speed, direction, and transmission range are constant. Therefore, the speeds and directions for node A and node B did not change from t_0 to t_3, where t_0 is the start point. It can calculate the distance d from A to B at time t, in order to proof the link state prediction that the research is used in correct way. It took four different calculations in four different time slots to examine the distance between two mobile nodes. In this calculation, the distance of every single point and its corresponding time slot were recorded. To simplify the calculation it is assumed that the direction and speed are constant while the time and distance are varying as described in Sections 5.7.1.1- 5.7.1.4.

As illustrated above in Figure 5.8 (Prediction Experiment) and scenarios for distance (SUB-EQ-1, SUB-EQ-1a, SUB-EQ-1b, & SUB-EQ-1c), there are four triangles with different sizes in terms of length of arc, the horizontal and elevation sides. The length of arc represents the size of angles between the transmitter and receiver because the length of arc is proportional to the angle subtended at the centre of a circle. The horizontal represents the flat area where the mobile nodes are physically supposed to move on it and finally the elevation side for the triangles represents the distance d between the mobile nodes A and B. However, from this simple calculation, the distance d when the mobile node A and B are going to be disconnected can be predicted, thus the distance can be computed as stated in [132, 133].

$$d= \sqrt{(b+v_A t)^2+(a+v_B t)^2-2cos\theta(b+v_A t)(a+v_B t) = (lt^2+mt+n)}, \tag{5.3}$$

where $l = v_A^2+v_B^2-2v_A v_B cos\theta$,

$m = 2bv_A+2av_B-2bv_B cos\theta-2av_V cos\theta$,

$n = b^2+a^2 2bacos\theta$

Alternatively, if the values of d_0, d_1 and d_2 at the time t_0, t_1 and t_2, are known but speed and direction are unknown then it can predicte the distance d_3 only at time t_3 through this equation.

$$d_3 = \sqrt{(lt_3^2)+mt_3+n}, \tag{5.4}$$

where: $l = \frac{(d_1^2 t_2 - d_2^2 t_1)-d_0^2(t_2-t_1)}{(t_1 t_2(t_1-t_2))}$, $m = \frac{(d_1^2 t_2^2 - d_2^2 t_1^2)-d_0^2(t_2^2-t_1^2)}{(t_1 t_2(t_1-t_2)}$, $n = d_0^2$

5.7.1.1 Scenario 1 for Calculating d_0

SUB-EQ-1(sub-equation 1) calculates the distance between node A and node B for the initial point. As the equation indicates, it assumes that the velocity of the mobile nodes and directions are constant. According to the above calculation and graph indicated in Figure 5.8, the initial distance d_0 is very short, and as it can be seen that the calculation of the SUB-EQ-1 the distance is not big. In mobile ad-hoc network, the short distance for two communication points presents high signal power. Thus, the connection between the transmitter node A and the receiver node B or reverse should be performed well in this case. However, it is clearly proved that this connection is powerful and signal strength is above or equal the required signal power to continue the communication for these mobile nodes. Nonetheless, when the connection establishes for two mobile nodes, the signal strength is normally stronger. This is because the distance length between them may be short. As the SUB-EQ-1 showing the distance d_0 for node A and node B is very short.

SUB-EQ-1

$$d_0^2 = (a + v_A t)^2 + (b + v_B t)^2 - 2\cos\theta(a + v_A t)(b + v_B t)$$

$$d_0^2 = (2 + 4 * 0)2 + (3 + 4 * 0)^2 - 2\cos 40(2 + 4 * 0)(3 + 4 * 0)$$

$$d_0^2 = (2)2 + (3)^2 - 2\cos 42(2)(3)$$

$$d_0 = (\sqrt{13 - 2\cos 42(2)(3)})$$

Variables	Values
a	2
b	3
v_a	4
v_b	4
t_0	0
θ	40^0

Figure 5.9: Scenario 1 for Calculating d_0

5.7.1.2 Scenario 2 for Calculating d_1

SUB-EQ-1a calculates the distance d_1 from A to B at the time t_1. In MANET, in most cases mobile nodes are moving when they are communicating, thus, the result of this scenario might differ from the previous one (SUB-EQ-1) due to node mobility. According to the equation results, the time value t_1 and the triangle graph for d_1 in Figure 5.8, the node A and node B moved from time t_0 to t_1. To prove that the nodes moved from the initial point to another new position, the graph in Figure 5.8 indicates that the d_0 and d_1 have different distances. In addition the above calculation (SUB-EQ-1a) shows a different result than SUB-EQ-1 in terms of distance d_1 between transmitter and receiver (A & B). The SUB-EQ-1 shows less value both for time and distance than the SUB- EQ-1a. These different values prove that the nodes move with constant speeds and directions. In addition it shows the nodes are not static.

SUB-EQ-1a

$$d_1^2 = (a + v_A t)^2 + (b + v_B t)^2 - 2\cos\theta(a + v_A t)(b + v_B t)$$

$$d_1^2 = (2 + 4 * 2)^2 + (3 + 4 * 2)^2 - 2\cos 60(2 + 4 * 2)(3 + 4 * 2)$$

$$d_1^2 = (2 + 8)^2 + (3 + 8)^2 - 2\cos 60(2 + 8)(3 + 8)$$

$$d_1 = \sqrt{141 - 2\cos 60(2 + 8)(3 + 8)}$$

Variables	Values
a	2
b	3
v_a	4
v_b	4
t_1	2
θ	60^0

Figure 5.10: Scenario 2 for Calculating d_1

5.7.1.3 Scenario 3 for Calculating d_2

SUB-EQ-1b investigates whether the mobile nodes come near each other or far away from each other according to the previous result obtained by SUB-EQ-1a. In implemention, when each of these calculations, takes place the result is compared to predefined threshold value in order to determine whether it needs to take action for this current connection. If the calculation algorithm makes a decision for not taking any action for an ongoing link, it means the signal is strong enough to keep maintaining this connection. The result of SUB-EQ-1b, for the calculation of the distance d_2 shows much longer according to the previous result from SUB-EQ-1a has shown. This indicates that the current signal strength is less than the recorded signal power by SUB-EQ-1a. This is a proof that shows whenever the mobile node moves from each other the signal power will reduce.

SUB-EQ-1b

$$d_2^2 = (a + v_A t)^2 + (b + v_B t)^2 - 2\cos\theta(a + v_A t)(b + v_B t)$$

$$d_2^2 = (2 + 4 * 4)^2 + (3 + 4 * 4)^2 - 2\cos 70(2 + 4 * 4)(3 + 4 * 4)$$

$$d_2^2 = (2 + 16)^2 + (3 + 16)^2 - 2\cos 70(2 + 16)(3 + 16)$$

$$d_2 = \sqrt{525 - 2\cos 70(2 + 16)(3 + 16)}$$

Variables	Values
a	2
b	3
v_a	4
v_b	4
t_2	4
θ	80^0

Figure 5.11: Scenario 3 for Calculating d_2

5.7.1.4 Scenario 4 for Calculating d_3

This scenario is the final signal captured to investigate its strength as shown in SUB-EQ-1c, and it is the time that the prediction algorithm takes an action. As mentioned earlier, this research has come up with a new method to handle the link failure on AODV routing protocol. This method is based on signal prediction to predict the status of the link between two mobile nodes in order to determine a link status before it becomes invisible. It is also to find out a new direction to the desired destination to divert the current data follow into a new path with a strong signal, respectively. According to Abdule et al. [104], if the current signal status has a lower value than the threshold (T_{hold}) the current node takes an action.

Therefore, this equation (SUB-EQ-1c) calculates the distance d_3 between node A and node B at time t_3 to measure the current signal power to test whether it fulfilled the criteria or the condition for the signal. This is made by mathematical comparison for the current signal status measured by the SUB- EQ-1c and threshold rate that is already determined and stored in a table. The longest distance for all measurements has shown in the SUB-EQ-1c. On the other hand, the smallest signal power throughout all measurements has to logically be in SUB- EQ-1c. This is to validate and prove that the prediction implementation regarding the distance between two mobile nodes for the PDFRP protocol is on the right path.

SUB-EQ-1c

$$d_3^2 = (a + v_A t)^2 + (b + v_B t)^2 - 2\cos\theta(a + v_A t)(b + v_B t)$$

$$d_3^2 = (2 + 4 * 6)^2 + (3 + 4 * 6)^2 - 2\cos 90(2 + 4 * 6)(3 + 4 * 6)$$

$$d_3^2 = (2 + 24)^2 + (3 + 24)^2 - 2\cos 90(2 + 24)(3 + 24)$$

$$d_3 = \sqrt{1165 - 2\cos 90(2 + 24)(3 + 24)}$$

Variables	Values
a	2
b	3
v_a	4
v_b	4
t_3	6
θ	90^0

Figure 5.12: Scenario 4 for Calculation d_3

5.7.2 Time Prediction Method

The time prediction method, having a knowledge of the distance d, can predict the time t when the node A and node B is going to be disconnected. In addition, it can also calculate the remaining time that the link will stay connected with known transmission range r. For example, A and B are within the transmission range r at (x_A,y_A) and (x_B,y_B) and move with speed v_A, v_B at direction θ_A, θ_B where $\theta_A$and θ_B are in the range of 0 to 2π , respectively. Therefore, as stated in [134], the remaining time of link connection is:

$$T = \frac{-(ab+cd)+\sqrt{(a^2+c^2)r^2-(ad-bc)2)}}{(a^2+c^2)}, \tag{5.5}$$

where $a = v_A cos\theta_A - vcos\theta_B$, $b = X_A - X_B$,

$c = v_A sin\theta_A - v_B sin\theta_B$ and d =$y_A - y_B$

Even though these two methods for distance prediction and time prediction method are identical and can be derived from each other for their equations, the time method prediction can be much easier than the distance prediction method if the distance d is known. However, the distance between two mobile nodes is unknown is most likly due to the MANET topology that changes frequently and hosts move randomly with unpredictable speed.

5.8 Signal Propagation Models

Global Positioning System (GPS) as mentioned by Kaplan and Hegarty [46] is a useful tool in order to locate the mobile node's direction and location. However, the GPS technology may not be always available, thus, these factors can be obtained by measuring the received signal powers at the receiver side. In order to calculate the received signal power, it uses radio propagation models. A number of radio propagation models has been developed to compute the received signal power and the most popular radio propagation models used in MANETs as follows:

- The Free Space Propagation Model
- Two-Ray Ground Reflection Model

The Free Space Propagation Model: is considered a single line-of-sight path, and it is the most popular model of radio propagation to compute the received signal powers [46] and it is calculated as follows:

$$P_r(d) = \frac{(P_t G_t G_r)}{L} * \frac{\lambda 2}{(4\pi)^2 d^2} \tag{5.6}$$

where P_t transmits signal power, G_t is the antenna gain of the transmitter, G_r is the antenna gain of the receiver, L is system loss and λ is the wavelength. The d^2 is in opposite proportion to the received signal power by receiver side where the square is the distance to the node that sent the signal.

The Two-Ray Ground Reflection Model: is more useful in terms of long distance propagation signal. In addition this model does not consider only a single line-of-sight path, it also considers a ground reflection path which gives a more clear-cut prediction at a long distance comparing with the free space propagation model [134]. The formula for the two-ray ground reflection model is

$$P_r(d) = \frac{P_t G_t G_r}{L} * \frac{h_t^2 h_r^2}{d^4} \tag{5.7}$$

This model considers the heights of the antenna because ground reflection has to be included in the calculation. Thus h_t^2 and h_r^2 are the heights of the transmission and receivers antenna respectively. This model has a disadvantage, since the signal power is inversely proportional to distance d, the receiver signal power for ground reflection model will be inversed to d^4, which double according to free space propagation model. Thus, as the distance increases the power loss is also increased.

According to the ns-2 implementation, Friss Free Space attenuation (1/r2) is used at near distance, whereas Two Ray Ground (1/r4) uses at long distance. In this case, the approximation supposes specula reflection of a flat ground plane, and the crossover point is called the reference distance which is the limit point of the transmission range. However, the reference distance in the ns-2 implementation is about 86.14 meters where the corresponding a signal power is 2.59x10-8 W at the receiver node according to ns-2 parameters.

Based on this information, this research is concerned only in the link failure caused by mobile node mobility where the nodes are going to move out of the sender transmission range. In this case, the study prediction algorithm is based on Two Ray Ground Reflection model. Thus only signals below 2.59x10-8 W will be the concern of our prediction algorithm. As described in [135], the new equation for Two Ray Ground Reflection according to the ns-2 implementation is as follows:

$$P = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4} \tag{5.8}$$

If it assumes the ground is flat where h_r and h_t will be constant and P_t is also constant, the equation (5.5) can be simplified under the conditions because of ad-hoc network:

$$P = \frac{kP_t}{d^4} \tag{5.9}$$

$$P = \frac{kP_t}{d^4}, where: k = P_t G_t G_r h_t^2 h_r^2 \tag{5.10}$$

In order to calculate and predict the signal power change, the signal powers received at the destination are measured whenever it receives data packets from a neighboring node. From that signal power samples, the rate of change for a particular neighbor's signal power level can be calculated and predict the time the transmission power level is less than the threshold [133]. For more details about received signal prediction method, refer to Figure 5.13.

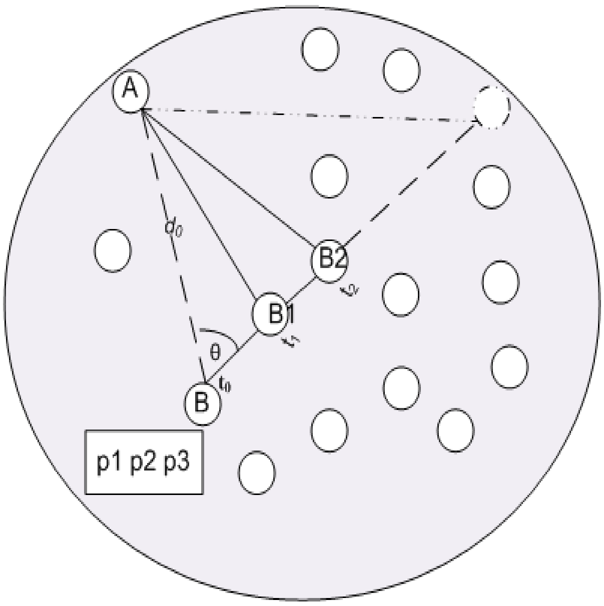


Figure 5.13: Measuring Received Signal Power (Adapted from [133])

Figure 5.13 presents how to calculate the time duration from when the third signal power was received to when the link will be broken. This prediction is related to the time prediction method because it is based on the duration time that the signal can exist. Therefore, this calculates the current time and compares the remaining time for the link live. The parameters in Figure 5.13 (p1, p2, p3) represent the signal status that node B received from node A and first three signals status is kept in an array. Each of these signals is compared with the previous signal power to evaluate either the current signal is stronger than the old one or not.

As mentioned earlier, speeds and directions for two nodes movement are assumed constant. This kind of prediction uses a calculation of relative movements between two mobile nodes and the Two-Ray Ground Reflection radio propagation [125]. The formula that can be obtained for the three received signal powers in order to calculate the time duration from when the third signal power was captured is as stated in equation 5.13.

$$T = \frac{-b+\sqrt{b^2-4ac}}{2a}, \text{ where as} = \sqrt{p_1 p_s \beta}, \tag{5.11}$$

$$b = \sqrt{p_s}((\sqrt{p_1} - \sqrt{p_2}) - t_2^2\sqrt{p_2}\beta),$$

$$c = t_2\sqrt{p_2 p_s} - t_2\sqrt{p_1 p_2}, \text{ and}$$

$$\beta = \frac{\sqrt{p_1 p_2 t_2} + \sqrt{p_2 p_3 t_3} - \sqrt{p_1 p_3 t_3} - \sqrt{p_2 p_3 t_2}}{t_2 t_3^2 - t_3 t_2^2 \sqrt{p_2 p_3}}$$

p_s is the required or threshold signal power whereas p_1, p_2 and p_3 are samples of received signal powers at time t_3, t_2 and t_3 respectively. However, the above mentioned radio propagation model, namely the Two-Ray Ground, is based on some assumptions, and if it does not fulfill these assumptions it may consider another propagation model, namely Shadow model [136, 137, 138, 139] and these assumptions are as following:

i. The radio transmission area is circular and all the radios have an equal range.

ii. Communications are bidirectional (if a node received a packet from a neighbor, then that neighbor will receive its packets to).

iii. The channel model is time-invariant (if a node can send a packet to a neighbor once, it will be possible as long as the topology does not change).

According to Aguayo et al. [140], in the absence of above assumptions the propagation model will be considered as Shadowing model. The shadowing model considers the long-term fading effects by means of a zero-mean Gaussian variable N (0,σ). Nonetheless, the received mean power $PdB(d)$ at distance d will be: $PdB(d) = PdB(d_0) - log\beta(\frac{d}{d_0}) + N$ (0, σ), where $PdB(d_0)$ is the received mean power at the first meter, while β is the path-loss exponent and σ is the shadow deviation (shadowing is another channel model than Two-Ray- Ground) (EQ-8). However, as stated in [141, 142], unlike most routing performance analysis, it takes into account the effects of both the additive thermal noise and the interferences to evaluate the signal to interface plus the noise (SINR) ratio at the receiver.

As stated in [143], in order to state if the received packet is received correctly the signal to interference plus noise ratio formula is thus used. The formula of signal-to-interference-plus-noise (SINR) is as follows:

$$SINR = 10log(\frac{p}{\sigma_n^2 + \sum_i p_i}) \tag{5.12}$$

where p is the received useful mean power and σ_n^2 is the additive noise mean power, whereas the p_i is the received interference mean power.

5.8.1 Prediction through Critical Time

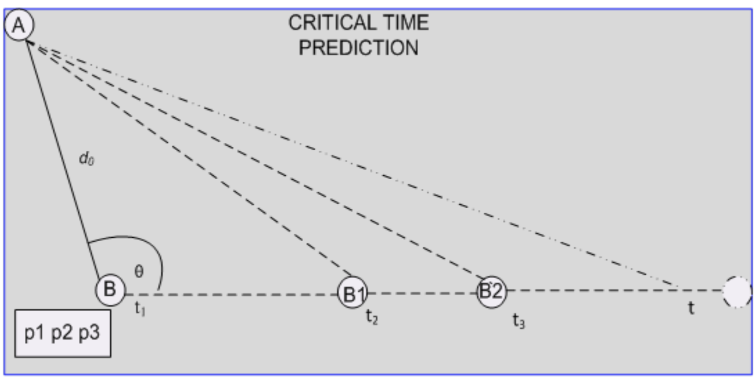


Figure 5.14: Critical Time (Adapted from [53])

According to Lee et al. [53], the threshold of signal power for a wireless network interface is constant (fixed), so if the nodes maintain their moving speed and direction the critical time will be constant. By definition, critical time is the time that two mobile nodes are moving out of the radio transmission range. Let us construct and formulate how the critical time is calculated and how the equations can be substituted with each other. As can be seen in Figure 5.14, at the time T_1, node B received a signal from node A; where it assumes that the distance between A and B is d_0. The formula for the first signal power calculated in this moment as described Lee et al. [53] is as follows:

$$P_1 = \frac{kP_t}{d^4} \tag{5.13}$$

So the next calculation for signal power will be at time T_2. Thus, node B receives the second signal from node A, where $t_2 = T_2 - T_1$. Then the second signal power calculation is:

$$p_2 = k\frac{p_t}{(d_0^2+(vt_2)^2-2d_0vt_2cos\theta)^2} \tag{5.14}$$

So, B received the third signal from node A at the time $T3$; then the time three will be: $t3 = T_3 - T_1$.

The signal power that node B has received in this moment is as follows:

$$p_3 = k\frac{p_t}{(d_0^2+(vt_3)^2-2d_0vt_3cos\theta)^2} \tag{5.15}$$

Now let us think that the node B has received a signal with power which is equivalent to the threshold signal power Ps by the time T, so let $t = T - T_1$. With that it is assumed the speed and direction for nodes A and B are maintained during the time T_1 to T. The threshold signal power calculation will be as follows:

$$p_s = k\frac{p_t}{(d_0^2+(vt)^2-2d_0vtcos\theta)^2} \tag{5.16}$$

The equation 5.13 can be simplified as follows:

$$P_1 d_0^4 = kP_t \tag{5.17}$$

Thus, the equation 5.17 can be substituted into equations 5.14, 5.15 and 5.16 and driven into new equations in order to simplify the complicity of the equations for the implementation and testing as well. The equation 5.14 can be written like:

$$p_2 = \frac{(P_1 d_0^4)}{(d_0^2+(vt_2)^2-2d_0vt_2cos\theta)^2}, \tag{5.18}$$

$$\sqrt{p_2} = \frac{\sqrt{(P_1 d_0^4)}}{\sqrt{(d_0^2+(vt_2)^2-2d_0vt_2cos\theta)^2}},$$

and $\sqrt{p_2} = \frac{\sqrt{P_1}d_0^2}{(d_0^2+(vt_2)^2-2d_0vt_2cos\theta)}$

Then the equation 5.13 is substituted again into equation 5.15:

$$p_3 = \frac{Pd_0^4}{(d_0^2+(vt_3)^2-2d_0vt_3cos\theta)^2}, \tag{5.19}$$

$$\sqrt{p_3} = \frac{\sqrt{Pd_0^4}}{\sqrt{(d_0^2+(vt_3)^2-2d_0vt_3cos\theta)^3}},$$

and $\sqrt{p_3} = \frac{\sqrt{P_1 d_0^2}}{d_0^2+(vt_3)^2-2d_0vt_3cos\theta}$

Finally, equation 5.13 is substituted into equation 5.16:

$$p_s = \frac{P_1 d_0^4}{(d_0^2+(vt)^2-2d_0vtcos\theta)^2}, \tag{5.20}$$

$\sqrt{p_s} = \frac{\sqrt{(P_1 d_0^4}}{(d_0^2+(vt)^2-2d_0vtcos\theta)^2}$, and

$\sqrt{p_s} = \frac{\sqrt{P_1 d_0^2}}{d_0^2+(vt)^2-2d_0vtcos\theta)}$

Equation 5.18 and equation 5.19 can be simplified into:

$$v^2 = \beta d_0^2, \tag{5.21}$$

where $\beta = \frac{\sqrt{p_1 p_2 t_2} + \sqrt{p_2 p_3 t_3} - \sqrt{p_1 p_3 t_3} - \sqrt{p_2 p_3 t_2}}{(t_2 t_3^2 - t_3 t_2^2)\sqrt{(p_2 p_3}}$, β is constant

Equation 5.18 and equation 5.20 can also be simplified into:

$$\sqrt{p_s} = \frac{\sqrt{P_1 P_2} d_0^2 t2}{(t_2\sqrt{p2} - t\sqrt{p_2} + t\sqrt{p_1})d_0^2 + (t2\sqrt{p_2}t^2 - t^2\sqrt{p_2}t)v^2} \tag{5.22}$$

Equation 5.21 and equation 5.22 can also be simplified and give:

$$\sqrt{ps} = \frac{\sqrt{P_1 P_2} t2}{(t_2\sqrt{p_2} - \sqrt{p2}t + \sqrt{p_1}t) + (\sqrt{p_2}t_2 t^2 - \sqrt{p_2}t_2^2 t)\beta} \tag{5.23}$$

So it gives this very simple equation which can be applied to the implementation:

$$at^2 - bt + c = 0, \tag{5.24}$$

$where : a = t_2\sqrt{P_2 Ps}\beta$, and

$c = t_2\sqrt{P_2 Ps} - \sqrt{p_2}, \; t_2\sqrt{P_1 P_2}$

Therefore, the critical time of two nodes that are approaching to cross over the border of the signal range is:

$$t = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{5.25}$$

This (5.25) equation can be written as follows because the time cannot be a negative value.

$$t = \frac{\sqrt{b^2 - 4ac} - b}{2a} \tag{5.26}$$

The concept behind of this mathematical deriving is to predict the Critical time where two mobile nodes are moving out of the radio transmission range. Thus, the equation (5.26) can be used to predict the Critical time.

5.9 Upstream Notification (UN) Model

As mentioned in Section 5.4, this research presents PDFRP protocol that includes UN mechanism. The main aim of developing UN mechanism is to avoid sending a unnecessary message back to the source because one of the major challenges in AODV protocol is error message propagating to the sender upon link failure. Abdule et al. [104] proposed a new approach to support PDFRP protocol, namely Upstream Notification mechanism (UN). However, the UN mechanism is really an improvement of PDFRP protocol. The main goal of PDFRP protocol is to predict the link status and divert it into a stable route if the signal status is below the threshold. However, after this goal has been achieved, another obstacle was found.

The PDFRP concept demonstrated in Figure 5.4 in Section 5.4 shows the link between C-N and Moving Node is going to be broken due to the movement of the intermediate node (Moving Node). Then, the C-N node constructed a new path and diverted the data into the new path smoothly without loss. This is because, as Figure 5.4 indicates, the node (new) has got both a route to the destination and enough strong signal. However, what if neither node (new) nor one of the neighbors has such facilities? For that reason, the study constructed the UN mechanism to break down the new obstacles in order to achieve the ultimate goal of the research. The UN has two mechanisms:

- Local Route Request (LRREQ)
- Upstream Notification (UN)

Before the new developed mechanisms presents (UN), a brief introduction about how the PDFRP protocol works upon a link failure in the absence of UN is provided. PDFRP protocol uses two mechanisms in order to predict the link breakage and takes action before it happens. For prediction, it utilizes the link state prediction method to collect the current link signal strength status in order to detect link breakage. When it collects the signal status it is then compared to the current connection signal strength among neighbors. Once one of those neighbors replies with a positive response and have both stronger signal and route to the destination, the current-node will divert the route into that node.

The weakness of PDFRP protocol is, if none of the neighbors has stronger signal strength than the current route, or it does not have a route to the destination at all, then the protocol will face a problem in order to process the data forwarding. However, this problem is a major challenge that all ad-hoc researchers of link failure in reactive routing protocols are facing, but this problem can be solved by UN mechanism which this research has come up with. The details about the LRREQ and UN are presented in sub sections 5.9.1 and 5.9.2. After the link state predication algorithm informs that the link between A and B will be broken soon (Figure 5.15), node A circulates a local route request to neighbors to check the signal status and whether there is a route to the destination as shown in Figure 5.16.

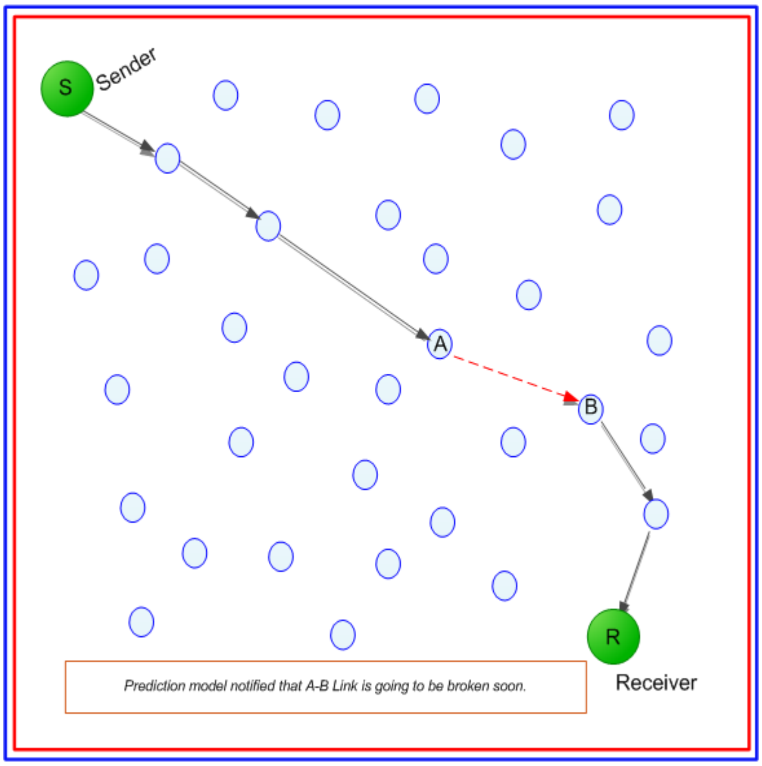


Figure 5.15: Link A-B is About to be Broken Soon

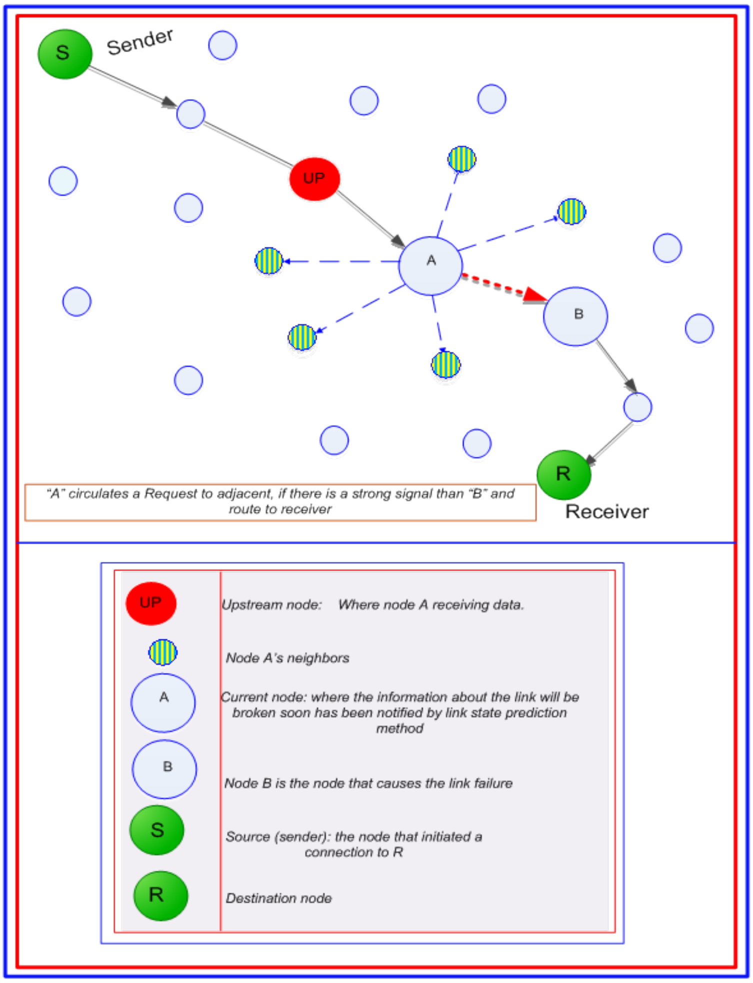


Figure 5.16: Node A Circulates a Request to Adjacent

5.9.1 Local Route Request (LRREQ)

LRREQ is a signaling packet which utilizes a current node that circulates among neighbors to investigate their signal status and route to the destination as well. The steps of this mechanism are shown in Figures 5.15- 5.19. LRREQ mechanism is used when the link state prediction model notifies that the link between two intermediate nodes on an active link will be broken soon. This means when the A-B link is about to be collapsed, node A takes action to sort out the matter instead of sending a warning message back to the sender as a AODV traditional mechanism does. In this respect, node A circulates a LRREQ-packet among its neighbors, except the node that node A is receiving from (it does not circulate to upstream node), to find out if there is a node that has a stronger signal than the current active link (in this case, link between A and B) and, at the same time, has a route to the destination (Figure 5.16).

5.9.2 Upstream Notification (UN)

If the current node (in this case, node A) could not receive a positive response from its neighbors (because no one has a route to the desired destination, or maybe they do not have a stronger signal than the current connection), the current node (A) will send a notification to the previous node (one hop to upstream) indicating the link will be broken soon. Thus, when this node (the upstream node) receives such a notification from the next hop (downstream), it circulates a (LRREQ-packet) into its neighbors except the upstream one and so on. This procedure is presented in Figure 5.17. The upstream notification continues until a new route to the desired destination, and stronger signal power are found. Figure 5.17 shows that the node A is failed to sort out the link redirection after the link state prediction informed that the A-B link will not be continued.

As mentioned earlier, in LRREQ mechanism, node A will circulate two inquiries (for the purpose of finding a stronger signal and a route to destination) to its neighbors simultaneously and if one of these inquiries is not fulfilled, the process will continue by sending a notification to the previous node to indicate that the existing link will be disconnected. This message also includes the status of the signal between nodes A and B. So, when the previous node (in this case is node-UP) receives such notification, it will circulate (LRREQ-packet) to its neighbors, as the node-A did. If UP-node successful at sorting it out, it continues sending the notification to upstream nodes until a new route to the destination is discovered.

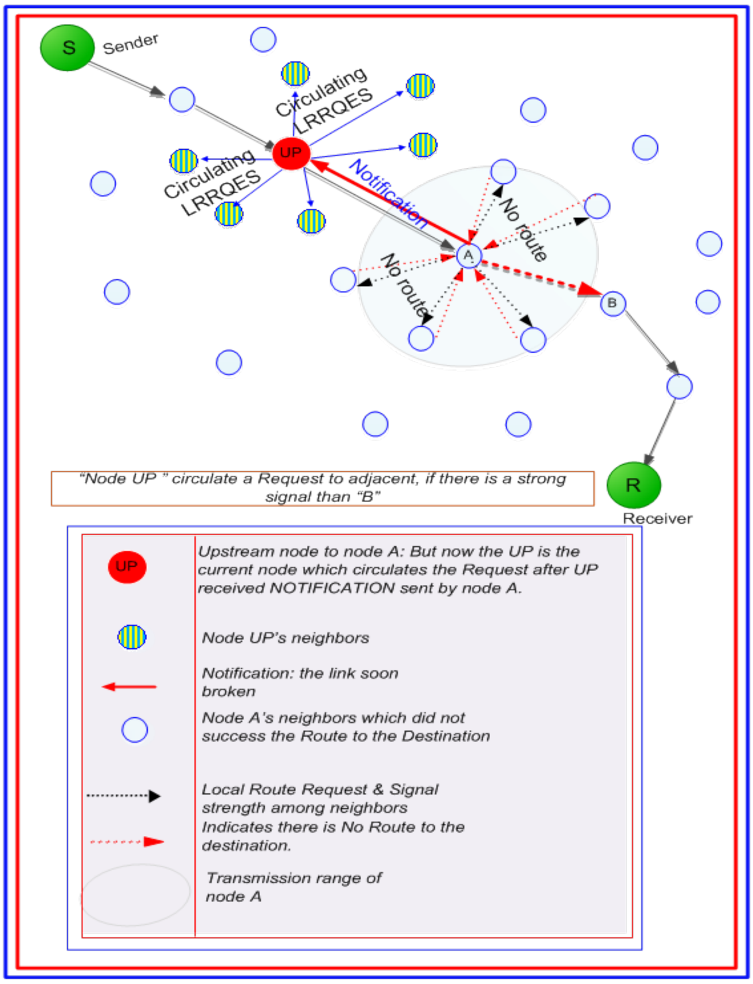


Figure 5.17: Sending Upstream Notification

However, if node C in Figure 5.18 has a stronger signal than the node A to node B, UP-node has to divert the route through node C (Figure 5.19), because A-B link is soon to be broken (because node B is moving beyond the coverage range of the node A). Intuitively, mobile ad-hoc network (as the distance between two nodes is greater than the radius of their transmission range) will not be able to communicate with each other.

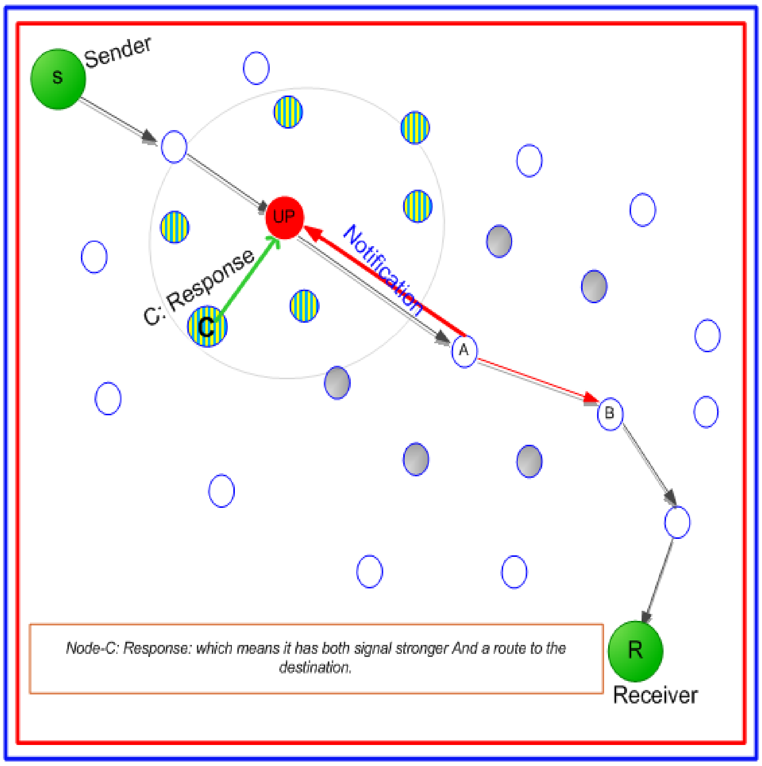


Figure 5.18: Node C Responses to Indicate That it Has Both a Stronger Signal and Route to the Destination

Figure 5.19 shows that a new route through node C is constructed. The data that flow through node A to node B will continue via the new constructed path without any loss. Nonetheless, through upstream notifications new mechanism, the research achieved the ultimate goal without obstacles.

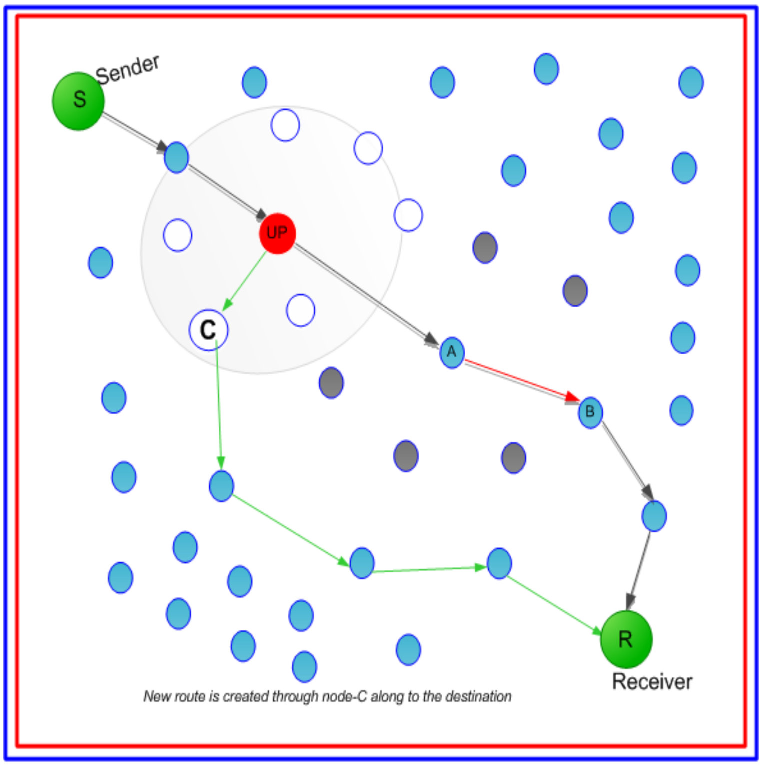


Figure 5.19: Link Diverted Through Node C

5.10 Summary

This chapter introduces the design of the hybrid developed protocol, (henceforth abbreviated as PDFRP) and UN mechanism. The chapter presents the current AODV design and how it can be migrated into a new born hybrid MANET protocol. The chapter has illustrated the philosophy behind the research explaining how the new concept is going to convert the reactive routing protocol into partially proactive routing protocol in order for the developed protocol to act as a uniform protocol. It also draws ideas of PDFRP solutions for link failure where the main objective is to enhance a link failure of AODV protocol by developing a new mechanism to avoid a complete link breakdown due to the node mobility as well as sending unnecessary message propagating to source up on link failure.

Further, the chapter discusses the developed models where it presented two main models Detection Model and New Path-Model as well as an analyzer algorithm. The chapter also discussed link prediction and validation where it introduced the mathematical analysis through link state prediction. Finally, it highlights the limitation for the PDFRP protocol and how it can be overcome by developing a new mechanism called Upstream Notification (UN). After this chapter introduces the design of the hybrid developed protocol, namely, the Predictive Divert Failure Route Protocol (PDFRP), the next chapter will discuss the PDFRP implementation.

CHAPTER SIX

IMPLEMENTATION OF PDFRP

In Chapter Five, the aim of the research and fundamental philosophy of this research as well as Predictive Divert Failure Routing Protocol (PDFRP) design are discussed. PDFRP models' design, different link predictions and signal propagation models are also presented in Chapter Five. This chapter focuses on the implementation of PDFRP protocol, illustrates PDFRP prediction concepts and how the PDFRP main prediction concept can be implemented in simulation environments. It discusses Mobile Ad-hoc Networks (MANETs) attributes and its implementation characteristics. Section 6.1 discusses ad-hoc network implementation and its complication in terms of implementation as well. Section 6.2 presents mobile ad-hoc node movement and how the mobile node randomly moves. Section 6.3 presents PDFRP algorithm and its techniques used the research implementation. Section 6.4 illustrates the PDFRP prediction concepts and explains how the PDFRP main prediction concept can be implemented in Network simulator (ns-2). Finally, configuration and parameters setting of PDFRP, validation and verification of the developed protocol are discussed in Section 6.6.

6.1 Ad-hoc Network Implementation

Mobile ad-hoc network is a unique communication network, and it has special characteristics compared to the rest of the network communications, including non ad-hoc wireless network. In such a network, it needs a unique design as it matches the real network as much as possible. One of the major phenomenona that one has to take into account is to choose the appropriate mobility model for its simulation. In the ad-hoc network, the output of any simulation, whether a good result or not is determined by the mobility model that has been chosen. Therefore, if the mobility model is chosen randomly, the simulation outcome might differ from the expected one, because the mobility model consists of some factors that can affect the network performance. Each of these factors has its own default parameter value, which has its best setting in each environment. Thus, in order to obtain the best results, the parameters of the mobility model have to be configured accordingly.

In this research, two mobility models have been tested such as Reference Point Group Mobility (RGPM), and Random Waypoint Mobility Model (RWP). Each and every model is developed in a particular environment in which it is most suitable. Of course, some of them have similar characteristics, but they may not perform in the same behaviour in all network environments. For instance, vehicle network environment is different from the city network environment, as the military or battle suitable network is different from both city and vehicle network environments. It means, the city network environment is more familiar with the vehicle network environment compared to the military network environment. However, to ensure the work has been done as it is supposed to be, all those matters have to be taken into the account, and that is why this research has spent more time for mobility models investigation as stated in Chapter Four.

As described by Sargent [144], the validation and evaluation of a protocol can be investigated with various scenarios with a different movement environment. In addition the investigation of a protocol should answer very common questions like; does the protocol correctly capture the highly dynamic network topology? and, does it choose an appropriate approach in terms of considering metrics (e.g. link failure) according to designed topology? However, it is obvious that each protocol could be the best for one network configuration whereas it might be the worst in another. Nonetheless, the network topology for mobile ad-hoc consists of two main factors which determine the overall network performance namely: Node position and Node movement. In the ad-hoc environment, node position must be dynamic, and it is determined by the movement of mobile hosts. In other words, how fast a host position is changed depends on the host speed configuration.

Therefore, one has to be very careful in such a network environment to accumulate a suitable configuration for these mobile hosts who are joining or disjoining in the network for an unpredictable way. For that reason, this research, after several examinations have been made for different mobility models as shown in Chapter Three, comes across a conclusion which decides the suitable mobility model for PDFRP is Random Waypoint Mobility Model (RWP). The RWP is the most commonly used model to generate movements for mobile hosts. According to this model, mobile hosts move independently. In addition the speed and direction of the movement have no relation to those of the previous movements.

6.2 Mobile Ad-hoc Node Movement

As described in Chapter Five, the speeds and directions for nodes movemen are assumed constant. In ad-hoc network implementation, one has to be very careful with random movement for mobile node implementation. The environments and actions of mobile ad-hoc nodes are assumed as a person or vehicle environments. In such a case, it will be difficult to estimate the speed and direction for a vehicle, (where the speed can be either high or low) as well as the direction might not be in a straight line for a while. Therefore, the implementation of mobile ad-hoc nodes assumes that the mobile node moves at a constant speed randomly and it gives maximun value to a random destination, then stops for a predefined pause time, and moves again. For instance, in our implementation, it is assumed that node B is a receiver for an ad-hoc network where node A is a sender moving at speed $\overrightarrow{v_a}$ and node B is moving at speed $\overrightarrow{v_b}$. However, $\overrightarrow{v_a}$ can be decayed to $\overrightarrow{v_{ax}}$ and $\overrightarrow{v_{ay}}$ as well as $\overrightarrow{v_b}$ to $\overrightarrow{v_{bx}}$ and $\overrightarrow{v_{by}}$ Figures 6.1

and 6.2 show directions for node A and B.

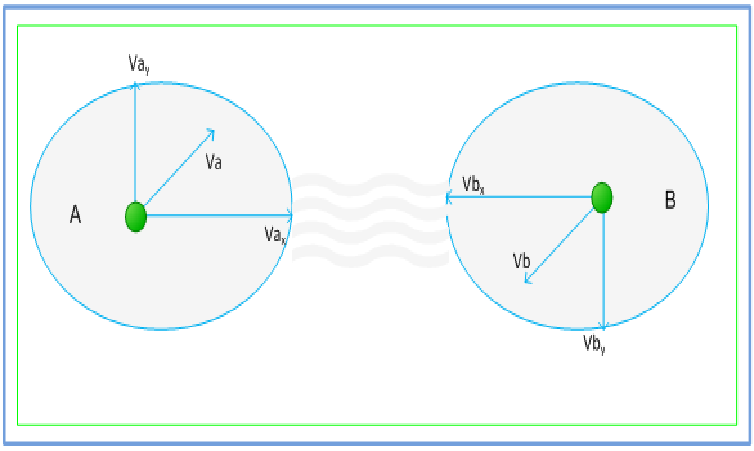


Figure 6.1: Speeds & Directions are Moving Randomly

In this respect, the relative speed of these nodes is:

$$\overrightarrow{v} = (\overrightarrow{v_{bx}} - \overrightarrow{v_{ax}}) - (\overrightarrow{v_{by}} - \overrightarrow{v_{ay}}) \tag{6.1}$$

Regarding the equation (6.1), it can be assumed that relative to node B, node A is motionless but node B is moving at the relative speed and direction is $\overrightarrow{v}$. As described in the previous chapter and illustrated in Figure 6.2 as well, in critical time prediction at a time $T1$, node B received a signal from node A. In this respect, it assumes that the distance between A and B is d_0 where the formula of signal power is calculated as follows as [145]:

$$P_1 = \frac{kP_t}{d^4} \tag{6.2}$$

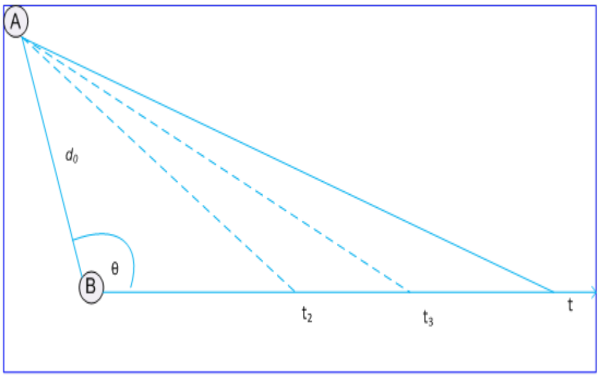


Figure 6.2: Relative Movements of Node B & Node A

6.3 Predictive Divert Failure Route Protocol (PDFRP) Algorithm

The implementation of PDFRP is based on one hop neighboring signal status where it is important to monitor the signal strength. The following explains how the concept is practically implemented. As described in Chapter Five, the PDFRP protocol comes up with several submechanism including Local Route Request (LRREQ) and Upstream Notification (UN). LRREQ used the link state prediction method, where it predicts link status for an active path between two neighboring nodes (A & B). However, the LRREQ designed one hop neighbors to collect their signal status. Upstream Notification (UN) is designed if the LRREQ fails to receive a positive response from its neighbors because of maybe a low signal status. From that perspective, it creates an array for each node to keep the signal information, called signal-status array. This array holds three packets for signal strength and their reception time. This is done by Lagrange Interpolation method, which has the following general definition as written by Hacene et al. [60].

$$L_j(x) = \prod_{0 \leqslant f \leq k, f \neq j} (\frac{x - x_f}{x_j - x_f}) = (\frac{x - x_0}{x_j - x_0}) \ldots (\frac{x - x_{j-1}}{x_j - x_{j-1}}) \tag{6.3}$$

$$p = (\frac{(t-t_1)\times(t-t_2)}{(t_0-t_1)\times(t_0-t_2)} \times p_0) + (\frac{(t-t_0)\times(t-t_2)}{(t_1-t_0)\tilde{A}\text{—}(t_1-t_2)}) \times p_1$$

The strength powers and time intervals are p_0, p_1, p_2, t_0, t_1 and t_2 respectively as stated in [60]. In this respect, as Algorithm 6.1 indicates if the signal threshold is less than the minimum requirement of signal power or there is no route to the desired destination, a warning message is sent to the upstream node. As it mentioned in Chapter Two, one of the implications of preemptive mechanisms is redundant warning messages which cause traffic overhead because of absence of warning message mechanism. Thus, PDFRP comes up with a new mechanism to prevent the number of warning messages traveling back to the source up on link failure. In this respect, as the following Algorithm 6.1 shows when UN node receives notification from downstream, it does not allow the message to propagate direct to the source. Instead, it circulates a local request. This is shown in the following Algorithm 6.1.

Algorithm 6.1 LRREQ & UN

$C_{acl-sglp}$ *******//Current active link signal power/*

T_{hold} *********// Threshold or required signal power/*

$one-hop-S-Pw$ ********//one hop neighbor's signal power/*

S_LRREQ ****//Search and checks out if there is a local route/*

$signal-status-array$[3] ******//table contains signal status/*

```
{
predict () // execute prediction in every 5 ms
        {if (C_acl-sglp < T_hold) then
      S-LRREQ (signal-power, dest-Route) //* checks one-hop-neighbor, if one them
    //*reveived stronger signal than current, plus destination, route as well */
    }
{
Response () //*one-hop-neighbors response
        signal-status-array[3] // *table contains signal status
          {if (one-hop-S-Pw > S-LRREQ (signal-power, dest-Route)) //*comparing signal
    //*power of the one hop// neighbor with the active route signal power*/
    }
}
//* Divert data into the new path

{
Divert-Data (new-path)
      Else
    Send-UN (signal-power, dest-Route) //*send natification to upstream node */
  }
}
```

6.4 Prediction Concept for PDFRP Protocol

Algorithm 6.1 explains how the PDFRPs' main prediction concept works when the two mechanisms (LRREQ and UN) are implemented. The start point in the Algorithm 6.1 indicates the prediction algorithm for main function of link state prediction is initialized called *predict()*. This prediction function is called to check whether the active link or ongoing link between A and B nodes is going to be broken soon. Using current active link signal power and threshold comparison ($C_{acl-sglP} < T_{hold}$), a local function *S_LRREQ()* is called if needed. The local function S*_LRREQ()* checks out if there is a route to the destination and the signal level according to predefined threshold value. If node A's neighbors do not meet one of these conditions, then the node sends a notification to the previous node to indicate that the downstream link will be disconnected. Then the upstream node call *response()* function and it circulates *LRREQ-Packet* to its neighbors, as node A has circulated. If node-UP does not succeed to sort it out, it continues sending the notification to the next upstream node until a new route to the destination is discovered. Finally, if the upstream-node succeeds, the data is forwarded through a new path as shown in Algorithm 6.1 (Divert-Data(new-path)).

6.5 Configuration and Parameters Setting of PDFRP

For implementating PDFRP, static network topologies have been created placing the nodes uniformly, and Random Waypoint is used as a mobility model as described by Bettstetter [146]. The ratio between operating area and nodes density plays a significant role for ad-hoc network connectivity's well-being. In this respect, the node density has been set to 4096 nodes/km2. This value has been given because it corresponds to a mean node connectivity degree of 12 and is a reasonable value to avoid the presence of network partitions [146]. Based on this connectivity number of degree, the size of the operation area was chosen. However, the calculation of node density can be obtained by following the formula in (6.4). Nodes density and expected node degree for ad-hoc network depend on the geometric distance between nodes. Let us say, geometric random graph with N nodes is represented by $G_p(r_{ij})(N)$, where $p(r_{ij})$ indicates the probability that shows there is a link between two nodes i and j at distance $r_i j$ from each other. However, the following calculation defines the expected number of links between nodes.

$$L = \sum_{i=1}^{N} \sum_{j=i+1}^{N} p(rij) \tag{6.4}$$

In order to derive the average number of connections between overall network members or possible configurations, it can denote as, $E(L)$, and assume that area Ω, is covered with $M > N$, placeholders of size $\Delta\Omega$. Moreover, it can also be assumed that N nodes are uniformly distributed over a 2-dimensional area with size Ω. Assuming that $\Delta\Omega$ is small enough to include only one node, the total number of configurations that can be formed with N nodes over the whole area will be $\frac{m}{N}$. This configuration can be simplified as: $G_1, G_2, G_3, G_4 G_{\frac{m}{N}}$. Whereas the expected number of links will be: $L_1, L_2, L_3, L_4 L_{\frac{m}{N}}$. Finally, the following equation summarises and defines the average number of links over all possible configurations where the number of links in each configuration is multiplied by the probability of occurrence of that configuration:

$$E(L)=P_r[G_1]L_1 + P_r[G_2]L_2 + P_r[G_{\frac{m}{N}}]L_{\frac{m}{N}} = \sum_{k=1}^{\frac{m}{N}} P_r(G_k)[\sum_{i=1}^{N} \sum_{j=i+1}^{N} p(|\Delta\Omega_{k,j} - \Delta\Omega_{k,j}|)] \quad (6.5)$$

Here it can be given that $\Delta\Omega_{k,x}$ which is indicated the position of the placeholder containing node x in configuration k, whereas $|\Delta\Omega_{k,i} - \Delta\Omega_{k,j}|$ is the distance between two nodes i and j in configuration k as written by[147, 148].

The simulation time for each scenario is 2060 seconds. This longer duration of time is purposely chosen to increase the accuracy of the measurements (metrics: delay, overhead, packet loss, etc.) The simulation time can be divided into two intervals; the movements' start time and data communication start time. The movement time (warming up time) is set at 950 seconds, whereas the data communication start time is set at 1000. The reason is that, according to Camp et al. [149], the random waypoint model is not representative for initial random distribution of mobile nodes themselves when moving. Thus, a warm-up period is required for the node mobility model to reach steady state. In this respect, Camp et al. [149] suggested a warm-up period of 1,000 seconds for the random waypoint model. Therefore, a warm-up or initialization period is set at 950 seconds and data communication time is set at 1000 seconds. In addition, 110 seconds is set as an extra time in order to ensure that the simulation time is not terminated before it reaches steady state.

The movement start time (warm-up time) should be started before any packets are sent, in order to achieve the steady state of the implemented mobility model. In other words, the initial time (warm-up time) is used to ensure that the routing protocol performance is well in order to reach a steady state as well. Therefore, the data traffic is modeled as a constant bit rate (CBR) through UDP protocol. Packet size is 512 kilobits per seconds (Kbps). In ns-2, the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless local area networks (WLANs) is used as the MAC layer protocol with 11Mbps as data transmission rate. Whereas, 1Mbps is used as data transmission rate for control packets such as Request To Send (RTS), Clear To Send (CTS), ACK and Broadcast and omni antenna is used as the antenna type. As mentioned in Chapter Five, there are three common radio propagation models, namely Two Ray Ground, Shadow Mode and Free Space Model. The Two Ray Ground model is valid only if the following conditions or assumptions are fulfilled, otherwise it is considered as Shadow model. These assumptions are:

i. The radio transmission area should be circular and all the radios have to be the equal range.

ii. Communications should be bidirectional.

iii. The channel model should be time-invariant as stated by Aguayo et al. [140].

So if these assumptions are not met the model is considered as Shadow model. Thus, in order to avoid a false or an unexpected result, this research has implemented both radio propagation models. Network interface type used Phy/ wirelessPhy and interface queue type used Queue/DropTail/PriQueue with max packet in the queue is 50 packets.

Moreover, the physical layer it used Management Information Base (MIB) where the minimal and maximum size of the contention window (CWMin, CWMax) was set at 31 and 1023 respectively. Geographical area network zise of PDFRP is 1000X1000 with network size: 10, 20, 40, 80 and 120 nodes are tested. The values of pause time that are used in our simulation are varying (0, 10, 20, 30 and 40 seconds), whereas the node speed (m/s) are varying with 5, 10, 20, 30 and 40. Each node involved in the traffic generator sends packets of 1000 bytes to each other in the network, deferring the subsequent transmissions of 1 second.

6.6 Validation and Verification of the PDFRP Implementation

6.6.1 Protocol Model Validation

Since, Ad-hoc On-Demand Distance Vector (AODV) Protocol had been built in ns-2, the verification and validation of the developed protocol and its models which are also implemented in ns-2 were made by comparing the results to AODV results which were obtained from actual simulation. As mentioned earlier in this chapter as well as in Chapter Four, all simulations were carried out over a period of 2060 seconds which is long enough to cover the transit state of the transmissions as well as steady state. Verification of the developed protocol was done to ensure that:

i. The developed protocol is programmed correctly.

ii. The developed protocol has been implemented properly.

iii. The developed protocol does not contain errors, mistakes, or bugs.

iv. The specification is complete and that mistakes have not been made in implementing the model.

The developed protocol was run with simple basic scenario for the purpose of verification and validation of PDFRP which included a small pause time such as 0 m/s, a small number of nodes such as 5 nodes as well as small packet size of 512 Bytes. These simple basic scenarios have been done in order to be easily analysed and the simulation results can be compared with the analysis. Subsequently, these simple basic scenarios were developed and made more complex to test the developed protocol. In addition, consistency tests were carried out to ensure that developed protocol produces similar results for input parameters values that have similar effects. Finally, in order to verify the developed protocol implementation, a script has been used to trace and filter the events that occurred during of simulation or run time**.**

Models for each of the protocols must be correct in the sense that they correctly implement the functionality described in the specification. Normally, this validation/verification is more commonly appropriate to a protocol model verification or validation. From this point of view, there are a number of standard techniques which have been used for model verification/validation as written by Bhargavan et al. [150]. These included the use of structured programming, detailed code reviews, and testing. One major validation can be tested for scenarios with known results and comparing the developed model output with the expected results, and running a detailed trace of the event sequence in a model execution to ensure that it follows the expected path. With that respect, the developed protocol has been verified and validated by a number of methods. In addition, as has been mentioned earlier since the developed protocol is an extension of AODV protocol, the AODV model had already been built in ns-2. Thus, the verification and validation of the PDFRP model were made by comparing the results to AODV results, which were obtained from actual simulation runs with more than 650 scenarios.

6.6.2 Scenario Validation of PDFRP

To verify and validate the developed protocol, 650 scenarios are examined. In this respect, 6 metrics have been tested where each metric has made 25 different experiments with different parameters. Scenario validation is one of the most basic, important tasks and fundamental to any wireless network. Our implementation scenarios were tested under a variety of parameters such as mobile node pause time, speed (m/s), node density analyzing the variety of metrics, including average end to end delay, channel throughput, number of packets dropped, packet delivery fractions, routing overhead and normalized routing load. In addition, various mobile ad-hoc communications have been deployed with correct initial placement of each device with appropriate mobility model where packets are generated and distributed in the network topology Area. Finally, the results of the above metrics are compared to the current AODV results and latest related work.

6.6.3 Formal Verification

In somehow, neither simulations nor testbed implementations can ensure the quality required for validation/verification of the protocols. According to Bhargavan [150], there is an alternative to these methods, which some researchers have already successfully investigated. The alternative is a formal verification, which it can be used as a mean to guarantee the quality of routing protocol verification. Formal verification is a technique that assures a system has, or has not given property based on a formal specification of the system under evaluation. This means that this technique can easily verify whether the model output matches with the expected results or not. However, to some extent, the other verification scenarios such as simulation or testbed might not present accurate results.

As described Zakiuddin et al. [151], basically there are three kinds of automated formal verification techniques. They are as follows:

i. *Model checking:* Model checking is a method to verify if a formal model system satisfies a given property as mentioned by Wibling et al. [152].

ii. *Theorem proving:* Theorem proving technique uses mathematical methods and applies the formula or equation and mathematical rules in order to prove the correctness of a system as described by Camara et al. [153].

iii. *Equivalence checking:* And finally, the Equivalence checking formally checks if two models at different abstraction levels are equivalent. This method is more or less a comparison between two different systems and models as written by Clarke [154].

Figure 6.3 illustrates the model checking approach, where the tool receives input from the system model then expected or not expected output be checked. The answer is represented as the output where it checks whether the system either holds or not the requested result. Nonetheless, in model checking, all the valid inputs and possibilities are verified to guarantee the correctness of the system as written by Kristensen and Jensen [155]. However, PDFRP model verification and validation were applied by theorem proving method. Thus, the mathematical equations that are presented throughout Chapter Five can be used as verification and validation for PDFRP implementation. In addition, PDFRP validation also applied equivalence checking method, where PDFRP result is compared to AODV standard result and the latest related work, which can be considered as two different models.

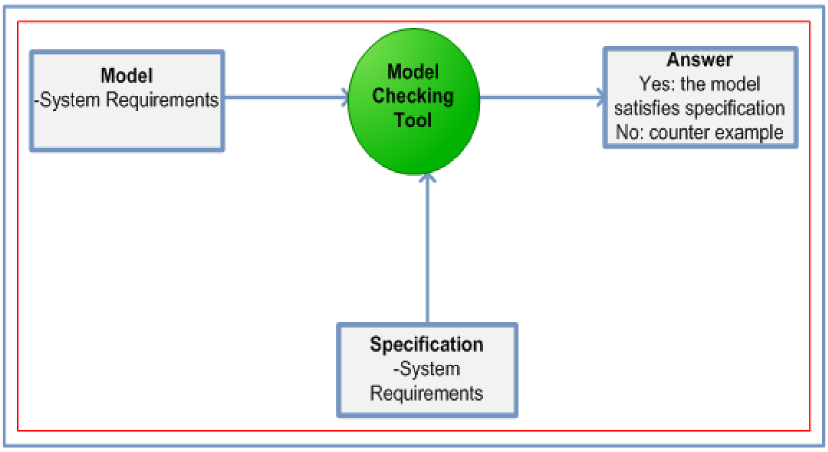


Figure 6.3: The Model Checking Approach (Adapted from [154])

6.7 Summary

This chapter presented the implementation details of the PDFRP protocol. The chapter illustrated that PDFRP can be implemented smoothly and efficiently for link state prediction to mitigate current link failure on the AODV protocol. It also discussed why Random Waypoint Mobility Model (RWP) is a suitable mobility model for this research and explained with justifications. The chapter covered mobile ad-hoc node movement and how random and uniform distributed devices can be handled presenting relevant mathematical equations. The mathematical equations simplified how in such a highly dynamic network it can be implemented by assuming that the speed and direction are constant. In addition, the chapter presented the implementation algorithm for PDFRP protocol. Moreover, it explained how the signal status is identified and collected up on about link failure. Furthermore, it showed that the PDFRP algorithm prototype flowed by loop diagram flowchart.

The chapter discussed network configuration and parameter setting of PDFRP where the implementation setup has been created. In this respect, the node density has been set to 4096 nodes/km2. It discussed the run time for the simulation setup. The chapter presented the model of data traffic such as CBR over UDP protocol with packet size 512 bytes. The chapter illustrated that the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless is utilized as the MAC layer protocol with 11Mbps as data transmission rate.

Finally, the chapter explained more about validation and verification of PDFRP protocol model validation, scenario validation as well as formal verification techniques. After presenting the implementation details of PDFRP in this chapter, the next chapter will present the performance evaluation of PDFRP based on the numerical results obtained from simulations.

CHAPTER SEVEN

RESULTS AND PERFORMANCE ANALYSIS

Chapter Six presented the implementation of Predictive Divert Failure Route Protocol (PDFRP). This chapter demonstrates the simulation results and performance analysis. It provides performance comparison of PDFRP protocol to the Ad-hoc On-Demand Distance Vector (AODV) algorithm based on the numerical results obtained from the simulations. The chapter examines the effect of different parameters of mobile ad-hoc network such as speed and pause time. Section 7.1, presents the metrics that used for measuring the protocol's performance and summarizes the metrics formulas. Section 7.1.1 outlines simulation scenarios and discuss the number of sub-scenarios which have been involved for each main scenario. Results and discussion of routing overhead, packet delivery fraction, normalized routing load, average end to end delay, packet drop and throughput against pause time parameter are presented in Sections 7.2, 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5, and 7.2.6, respectively. In Sections 7.3.1, 7.3.2, 7.3.3, 7.3.4, 7.3.5, and 7.3.6 speed effects against same metrics as mentioned above are illustrated. Results and discussion of varying node density against routing overhead, packet delivery fraction, normalized routing load, average end to end delay and packets drop are presented in Sections 7.4, 7.4.1, 7.4.2, 7.4.3, 7.4.4, and 7.4.5 respectively. Finally, Sections 7.5, and 7.5.1 discuss performance comparison of PDFRP and some of current works.

7.1 Performance Metrics

This section discusses and analyzes the results of the PDFRP protocol. The results are presented in graphs as well as comparison tables. The experiment discussion focuses on six metrics that are commonly used for measuring the protocol's performance as elaborated in Chapter Three. The aim of this Section is to show the effectiveness of the developed protocol to assess the protocol's tolerance against link failure by a performance comparison among widely used metrics which are as follows:

i. Routing Overhead
ii. Packet Delivery Fraction (PDF)
iii. Normalized Routing Load (NRL)
iv. Average End-to-End Delay
v. Packet Drop
vi. Throughput

The Transmission Control Protocol (TCP), data traffic application might cause additional packet loss and network congestion at the intermediate nodes, thus Continuous Bit Rate (CBR) is used as data traffic generation in this research. In this research, 6 metrics are implemented. Routing overhead evaluates the network efficiency where it takes into consideration how many routing messages are generated through the network channel as it evaluates network congestion. Packet delivery ratio, is concerned with the ratio of packets delivered according to the number of packets sent where it collects all received data packets from trace file, which is delivered at the destination node. Before explaining the normalized routing load, I will summarize Normalized MAC Load (NML) control packet, because it might sometimes be difficult to distinguish NML from NRL. NML metric is used for evaluating the effective utilization of the wireless medium for data traffic. NML can be defined as the fraction of all control packets (routing control packets, including Request-To-Send (RTS)) which means a request signal to the next neighbor asking if it can be ready to receive its request, Clear-To-Send (CTS) which means an acceptance for that request, Address

Resolution Protocol (ARP) requests and replies, and MAC ACKs (in case of using TCP) divide the total number of received data packets. NML metric can sometime cause confusion in packet drop calculation, because sometimes the tracing script might be exclusive or inclusive of NML packets drop. Nonetheless, NML takes into account all establishing processes for control packets in routing level but not the agent (AGT) level whereby the NRL is concerned only in received data packets at the destination. However, NRL metric is used to determine the efficiency and scalability of the protocol to estimate how many transmitted routing messages are used for one successful data packet delivery.

Average End-to-End Delay, is concerned with the transmission time for each successful data at the destination side where it includes all possible delays in the network. The packet drop metric takes into consideration the number of packet loss to observe or evaluate the protocol's delivery capacity. Throughput, evaluates the network's overall throughput capacity. However, there are two ways to represent the throughput which are, (i) the amount of data transferred over the period of time expressed in kilobits per second (Kbps), (ii) the packet delivery percentage obtained from a ratio of the number of data packets sent and the number of data packets received.

Table 7.1 summarizes the metrics formulas where the AWK – script program analyzes the calculated values of the above quantitative metrics.

Table 7.1: Metrics Derivation

Metrics	
PDF % =	Total_Data_packets_received / Total_Data_packets_sent
A_End-2-End-Delay =	Total_time_received - total time_sent / Total Data_packets_received
NRL =	Total_Routing_packets_sent / Total_Data_packets_received
Packet-Drop =	Data_sent - DataRecv
Routing overhead =	Routing packets_sent / Routing packets_received
Throughput =	Total packets_received / Total_simulation_time

To evaluate the performance of PDFRP against AODV standard, 650 scenarios are examined. In this respect, 6 metrics have been tested where each metric has made 25 different experiments with different parameters. For example, Routing Overhead is a metric among 6 metrics whereas pause time is a parameter. In the first scenario of pause time, the number of nodes set 5, while the pause time is varying from 0 to 40 seconds and the rest of the parameters in kept constant. The second scenario of pause time, the number of nodes set 20 while the pause time is varying from 0 to 40 seconds and rest of parameters are remain the same as the previous scenario.

Third, fourth, and fifth scenarios of pause time take the same concept as the first and second scenarios, but the number of nodes set 40, 80 and 120 nodes respectively. The next experiment takes into consideration the node speed which is one of the main determined variable parameters of mobile ad-hoc network performance. The speed concept is similar with the pause time scenarios,with just the speed values are varying.

The final scenario involves the node density, while the rest of variable parameters remain same. In this case, some of the variables' values are chosen deliberately. For instance, when the node density experiment scenarios were tested, the speed and pause time values were set at 5m/s and 20 seconds correspondingly. The reason that these values have been chosen is because according to Abdule et al. [108], the overhead is defiantly proportional to the pause time and obviously the overhead will be low when the pause time is small and at the same time the experiment shows that choosing a smaller pause time gives the optimal setting for node pause time. In addition, high speed causes more routing change, which causes network instability. Therefore, these values for testing the nodes' density have been chosen. Table 7.2 shows the simulation parameters where the pause time is varying.

Table 7.2: Varying Pause Time (RWM-model)

Parameters	Values
Simulator	ns-2
Routing Protocol	PDFRP, AODV
Range	1000 m x 1000 m
Pause time	0, 10, 20, 30 and 40 m/s
Simulation Time	2060 s
Packet type	Constant bit Rate (CBR)
No of Packet	10 pkts/s
Speed	20m/s
Packet size	512 Bytes
No of Nodes	5, 20, 40, 80 and 120

7.2 Results and Discussion of Varying Pause Time

This section presents the results for routing overhead against pause time.

7.2.1 Routing Overhead vs. Pause Time

Figure 7.1 presents the experiment results for routing overhead vs. duration time that the mobile node is unmoving. In Figure 7.1 illustrates 10 graphs (10 experiments) where 5 graphs present the results for PDFRP while another 5 present results of the AODV standard. In Figure 7.1, on the right side there are 10 legends: PDFRP-Pstime-0, PDFRP-Pstime-10, PDFRP-Pstime-20, PDFRP-Pstime-30, and PDFRP-Pstime-40 and AODV legends as well. These indicate different scenarios of experiments regarding routing overhead where pause time is varying. In this case, in the first set of simulations, the pause time is increased from 0 to 40 seconds, whereas the number of nodes set 5 nodes and all other parameters are unchanged. This scenario was repeated five times from 0 pause time to 40 pause time as indicated in Table 7.2. In other words, when the pause time is 0, a result of one scenario is obtained and increases the pause time up to 10 seconds and continues until pause time becomes 40 seconds; then it compares these different results. This is one scenario which contains 5 sub-scenarios. As Figure 7.1 indicating that this experiment examined 10 scenarios with 5 sub-scenarios in each. In ad-hoc networks, the routing overhead is an indicator of how huge the network routing messages through the channels are huge. In this matter, minimizing the network overhead maximizes the network resources utilization which leads to better performance for the routing protocol. Figure 7.1 illustrates the experiment results for routing overhead where it shows that the overhead decreases while the pause time increases. This is because of ad-hoc network characteristics. When the pause time increases, the network stability is also increased, and overall network performance is improved. In Figure 7.1 the overhead for scenario one (PDFRP-Pstime-0-40 with 5n) indicates a lower routing overhead when the pause time is 0. On the other hand, the value of the routing overhead is decreased by the time that the value of the pause time is increased. As indicated in Figure 7.1, whenever the pause time is headed for 30 or over pause time the routing overhead is reduced. As shown in Table 7.2 and illustrated in Figure 7.1 the pause time values begin at 0 and end 40 seconds. In this respect, the graphs were propagated from the left side in Figure 7.1, from zero pause time to right side where the graphs ended. Analyzing from that point of view, all graphs are either constant all the way or bent over by approaching the end of the edge point. In this respect, the performance of routing overhead is directly proportional to network stability.

In order to evaluate the developed protocol's performance in this respect, the outcome of the developed protocol is compared to the outcome of the AODV standard protocol. For example when pause time is 20, 30 and 40 seconds with highest traffic AODV indicating 35190, 34190 and 33130 packets are overhead whereas PDFRP shows 17370,14931 and 13995 packets are overhead. This means that PDFRP improves 50.6%, 56.30% and 57.75% in terms of packets overhead. The values of these results are illustrated in Figure 7.1, where the experiments show that the developed protocol presents the lowest routing overhead in all cases compared to AODV standard. However, routing overhead results presented in Figure 7.1 indicate that AODV performance for routing overhead drops significantly compared to PDFRP. Thus, it can be concluded that PDFRP obviously outperforms AODV standard regarding routing overhead.

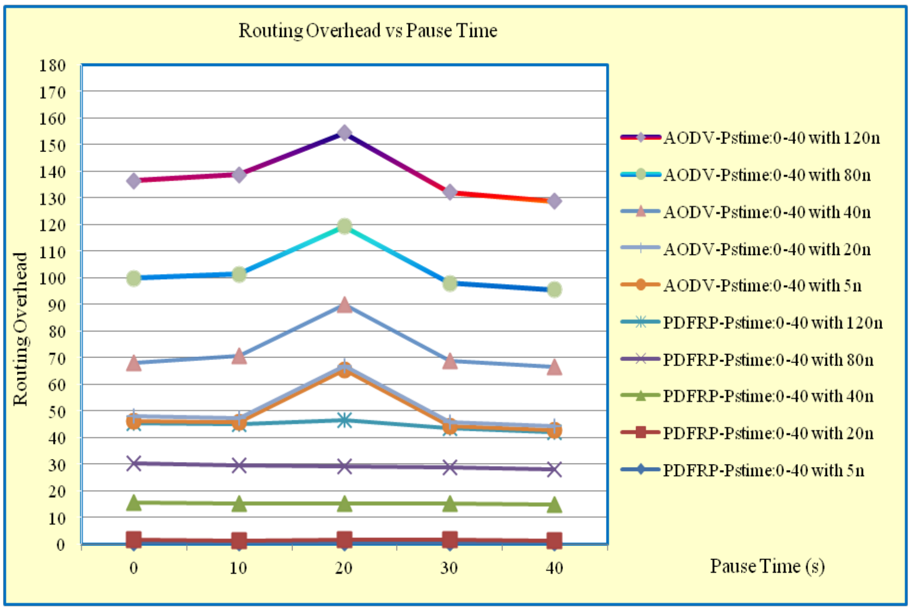


Figure 7.1: PDFRP and AODV: Routing Overhead vs. Pause Time

7.2.2 Packet Delivery Fraction vs. Pause Time

This section evaluates the effectiveness of the developed protocol by testing a widely used routing performance metric, namely the Packet Delivery Fraction (PDF). PDF is a fundamental factor for overall network efficient evaluation. This experiment focuses on pause time effects, which have been varied in the range between 0 to 40 seconds. This metric measures the performance of the whole routing process, whereas the previous metric (routing overhead) measures the signaling packets overhead only. In this experiment, the result of PDF is obtained by calculating a percentage of data packets being delivered to the total number of data packets being sent. Figure 7.2 shows the results of packet delivery fraction for both PDFRP and AODV. Figure 7.2 shown that the packet delivery ratio becomes better as the pause time increases. Figure 7.2 depicts five scenarios in each protocol (PDFRP and AODV).

As in Figure 7.2 the longer the pause time the longer the results were better. For PDFRP, last scenarios where the number of nodes is 120 (*PDFRP-Pstime:0-40 with 120n*) show the best results of the packet delivery ratio. The result values of these scenarios are 99.57%, 99.71%, 99.78%, 99.86% and 100% whereas the first scenario (*PDFRP-Pstime:0-40 with 5n*) results show 98.7%, 99.25%, 98.24%, 99.6% and 99.99% correspondingly. In the same case, the best result values for AODV standard show 68.17%, 80.32%, 77%, 77.89% and 78.53% whereas the lowest results show , 57.27%, 58.13%, 62.16%, 62.74% and 65.44% respectively. One conclusion is that the last scenario (*PDFRP-Pstime:0-40 with 120n*) gives better results whereas the first scenario (*PDFRP-Pstime:0-40 with 5n*) gives less packet delivery ratio because in the case a lower node density, there may be less chance in successfully finding an available route. This means that whenever the density of the network is sparser, there is a possibility that the nodes space distance is longer than mobile ad-hoc network signal transmission range (the number of nodes of last scenarios is 120 while the first scenario is 5 nodes).

However, both protocols present the highest result when the pause time set at 40 seconds where the conclusion shows that the ratio is higher when pause time is greater; because longer pause time indicates more stable links. As Figure 7.2 illustrates, the results generated by AODV standard are less than in PDFRP generated results. The experiment and analyses point, the developed protocol performance is better compared to AODV standard protocol. As illustrated in Figure 7.2, the experiment shows that the developed protocol presents the highest packets delivery ratio according to the AODV standard. Nonetheless, the percentage of the packet delivery ratio presented in Figure

7.2 generated by PDFRP obviously outperformed AODV.

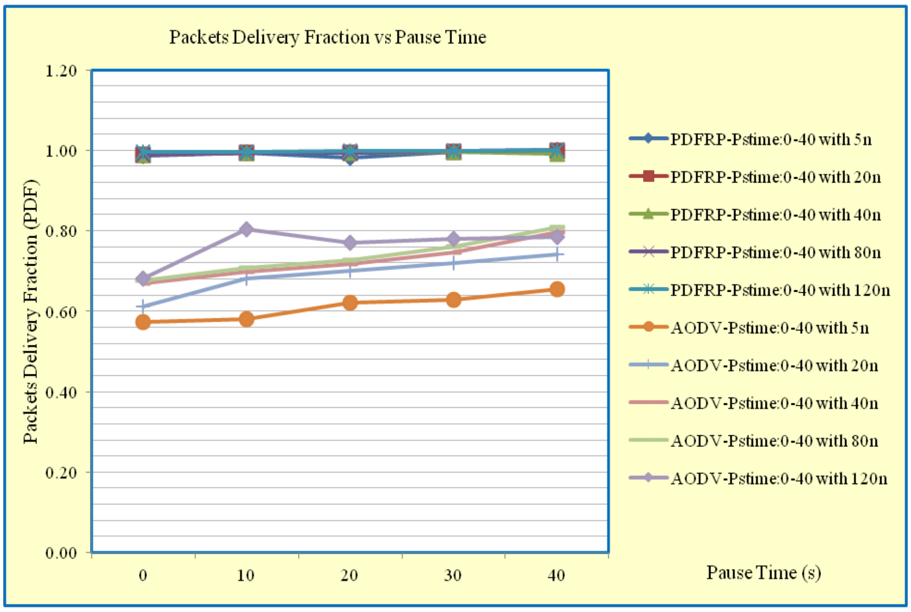


Figure 7.2: PDFRP and AODV: Packets Delivery Fraction vs. Pause Time

7.2.3 Normalized Routing Load vs. Pause Time

This sub-section presents a comparison of PDFRP to the AODV standard routing protocol regarding normalized routing load performance. As described in Table 7.1, the number of routing messages that is transmitted in one transmission is divided by the number of data packets that is delivered at the destination. In other words, it can be easily explained that the number of routing messages transmitted over the channels is the total intermediate- node-hops of transmitting routing control messages such as Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) in the AODV route discovery process. In this respect, it can be easily understood that the normalized routing load and routing overhead have similar characteristics. Because in reality, the NRL metric is actually the Routing Overhead divided by the number of delivered data packets.

However, Routing Overhead is a metric which measures the signaling packets overhead generated by the routing protocol for route broadcasting process where NRL is the ratio the number of routing messages transmitted divided by the number of data packets delivered. On the other hand, the normalized routing load is a relative metric based on the number of successful data packet delivery. In that respect, this metric has also a relation with Packet Delivery Fraction (PDF) metric because it can be used to measure the packet delivery ratio. It means, if the packet delivery ratio is quite high or low, the value of the routing overhead packets and PDF to be considered. Nonetheless, NRL metric is an instrument to measure how many transmitted routing messages are used for one successful data packet delivery by this metric to determine the efficiency and scalability of the protocol. The experiment of this sub-section focuses on normalized routing overhead effects. In other words, it analyses routing control messages per data packet delivery for each protocol (PDFRP and AODV) and compares the results.

The simulation results are presented in Figure 7.3 where each point on the graph indicates the gained ratio of normalized routing load according to the pause time value. In this respect, the x-axis denotes the duration time that the node is unmoving, whereas the y-axis denotes the ratio of the total gained routing messages transmitted through the router and number of data packets delivered at the receiver. Figure 7.3 indicates that the PDFRP control messages are much less compared to AODV control messages. Since the Normalized Routing Load (NRL) is a ratio between total routing packets sent and total data packets received at the destination, Figure 7.3 (y-axis) indicates that the PDFRP control messages are lower than 1%, where AODV control messages indicate near 2% up to 6.30%. One explanation is that the number of routing message is proportional to the link stability. According to Chang et al. [156], in the presence of link failure in AODV, when an intermediate node discovers a link failure in active route, it broadcasts a route error message to inform the source node. In this respect, the source node will re-initiate a route discovery process again if necessary.

One major drawback of AODV protocol is the source route re-initiating upon a link failure which increases the routing overhead to the network. For that reason, this research developed PDFRP protocol with a new mechanism that avoids the route re-discovery by the source upon link failure. In this respect, PDFRP reduces the routing message overhead in one hand and on the other hand it solves the link failure before the current route becomes completely disconnected utilizing link state prediction mechanism. However, the comparison of normalized routing overheads of PDFRP and AODV is given in Figure 7.3, in which PDFRP outperforms AODV in all cases where it satisfies the first objective in this thesis.

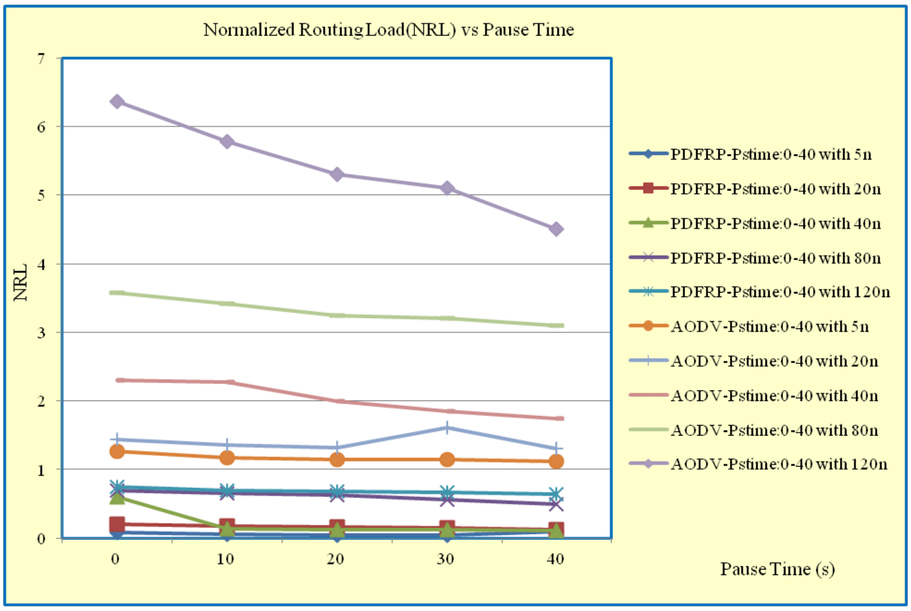


Figure 7.3: PDFRP and AODV: Normalized Routing Load vs. Pause Time

7.2.4 Average End-to-End Delay vs. Pause Time

Average End to End Delay is a useful metric in the network environment, especially in the mobile ad-hoc network. It calculates the average packet delivery time from a source to a desired destination. This means that the entire network that a particular packet goes through calculates delay separately for each hops pair. For example, in each two node that communicate with each other, an average delay for packet delivery is computed. Then the whole average delay is computed from each pair average delay. These delays include the delay in the send buffer, the delay in the interface queue, the bandwidth contention delay at the MAC, and the propagation delays. However, end to end delay metric is not completely independent of the other network performance metrics. For instance, a lower packet delivery ratio means that the delay metric is evaluated with fewer samples the dependence between these two metrics is shown. In other words, the probability of a packet loss may be higher when using a longer route where in that situation the delay will be higher.

Figure 7.4 illustrates the comparison results of PDFRP to AODV where the pause time vary from 0 to 40 seconds. As depicted in Figure 7.4, as the pause time increases, the delays are decreased which it indicates that the ratio is lower when pause time is greater, because greater pause time means more stable links. In a mobile ad-hoc network, the network stability is a major element where many researchers in the field are working on to improve it. In this drawback, two main elements mainly play a significant role, namely speed and pause time of course network density, but this is not as significant as the other two elements. As Figure 7.4 shows the left side (horizontal x-axis) denotes the pause time value from 0-40 second, whereas the right side (vertical y-axis) denotes the ratio of the total gained of the end to end delay. The number of graphs indicated in Figure 7.4 is 10 graphs: 5 belongs to PDFRP where another 5 belongs to AODV.

It can be seen in Figure 7.4 that each graph starts a deferent point (different values). In addition these values are increased as the graph moves towards the horizontal x-axis. The reason that the graphs start with different values is because each graph represents one scenario of an experiment with different node density. For example, the legend marked “PDFRP-Pstime: 0 - 40 with 5n” represents a scenario where nodes' density is five nodes and pause time is varying as mentioned earlier. The next scenario denotes (PDFRP-Pstime: 0 - 40 with 20n) and scenarios continue until 120 nodes as illustrated in Figure 7.4. The same scenarios have also been tested in AODV standard as presents in Figure 7.4. The first scenario presents the lowest average end to end delay, whereas the last scenario (PDFRP-Pstime: 0-40 with 120n) indicates the highest average end to end delay. The explanation lies by the definition: End to End Delay includes the delay in the sent buffer, the delay in the interface queue, and the bandwidth contention delay at the MAC, and the propagation delay. From this definition, it can be understood that the average end to end delay is proportional to many factors among buffer capacity, MAC type, and bandwidth availability where it can be defined as "full-buffer + low-bandwidth = network congestion".

In this respect, since the delay ratio depends on the number of network components that the data packet goes through, the delay will increase as nodes' density is increasing; thus 5 nodes, and 120 nodes are obviously two different network environments. However, this experiment is not investigating the effect of node density; it focuses only the pause time effect. The effect of nodes' density will be discussed in a later section. As illustrated in Figure 7.4, the AODV standard experiment regards the effect of pause time and is compared to the result for PDFRP with respect to pause time effect as well. Figure 7.4 shows that in all scenarios, PDFRP presented a better average end to end delay compared to AODV.

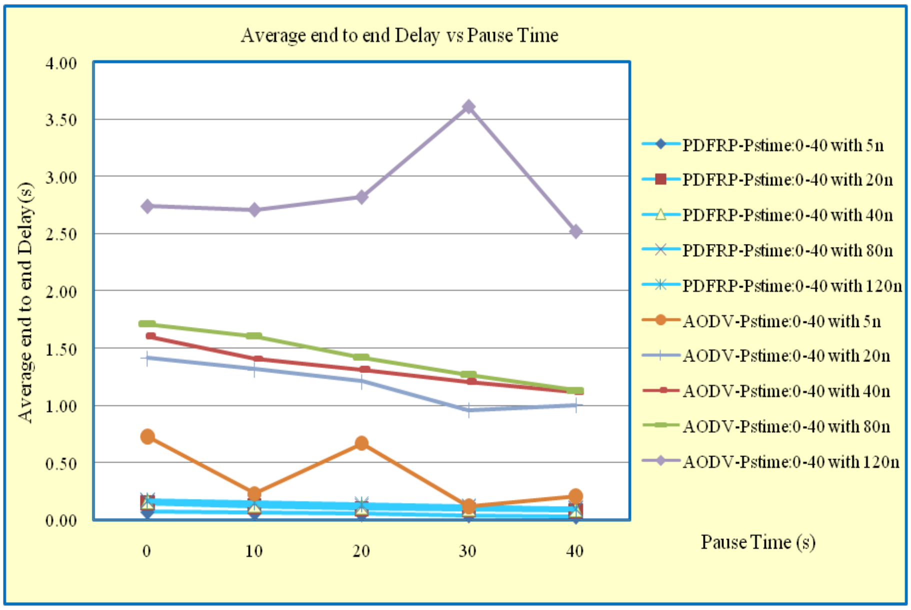


Figure 7.4: PDFRP and AODV: Average End-to-End Delay vs. Pause Time

7.2.5 Packet Drop Performance vs. Pause Time

This sub-section demonstrates the packet loss, it explains the reason behind the packet loss, where it happens and what is the solution to prevent it. The nature of AODV protocol or in general reactive routing protocols to generate packets on demand which technically reduces the routing overhead in the network environment compared to proactive routing protocol. Many factors can be involved as to why the data packet get lost before it reaches the desired destination. Sometimes a long delayed packet counts as a lost packet even though it is on the way to the destination. Such a packet is considered as a packet loss, because its delay might be beyond a predefined delay threshold. Network congestion is another issue that increases the number of packet drops', including the bandwidth limitation and network density. In addition, the wireless sends buffer with a maximum size of 64 packets containing all data packets waiting for a route to send them. The buffering is another factor for packet drop.

The packets in the buffer will be dropped if buffering is longer than the sends buffer interval time (normally within 30 s). Moreover, all packets sent by the routing layer are queued at the interface queue until the MAC layer can transmit them. However, the low priority packets are dropped at a faster rate than that for high priority packets. In AODV protocol, existing mechanism for route maintenance can cause more packets drop up on link failure, because it continues using a route until a link completely disconnected. In this case, the source will re-initiate a new route where the current data packets can be dropped. In order to avoid such a drawback, this research focuses on link failure and developed a new routing protocol to reduce the possibility of data packets being dropped. As presented in Figure 7.5, the number of packets dropped for PDFRP scenario is much lower according to the AODV standard packet drop. One reason can be that the prediction algorithm reduced the number of link breakage thus, the overall performance of packet drop is improved compared to AODV.

The main goal of this experiment is to assess the developed protocol performance and compare the result to the standard one. Figure 7.5, illustrates 10 experiments where each experiment contains five sub-scenarios. This means that each experiment is tested five times with five different pause times. The reason that each has been tested with five different pause times is to evaluate the network performance with variety of pause times.

Figure 7.5 shows that in PDFRP scenarios, the lowest packet drop indicated scenario one (*PDFRP-Pstime: 0-40 with 5n*) whereas the highest packet drop indicated scenario 5 (*PDFRP-Pstime: 0-40 with 120n*) which is logically correct. But, sometimes it may not follow the network density sequences because the packet drop depends on many factors as mentioned above and not on the scenarios' sequence. In such case, the packet drop is not proportional to the network density, but on the other hand depends on the network condition (e.g. bandwidth available, network buffering queuing setting/configuration etc.). However, the drop results indicate that the PDFRP outperform AODV, packet drop in terms of packet loss.

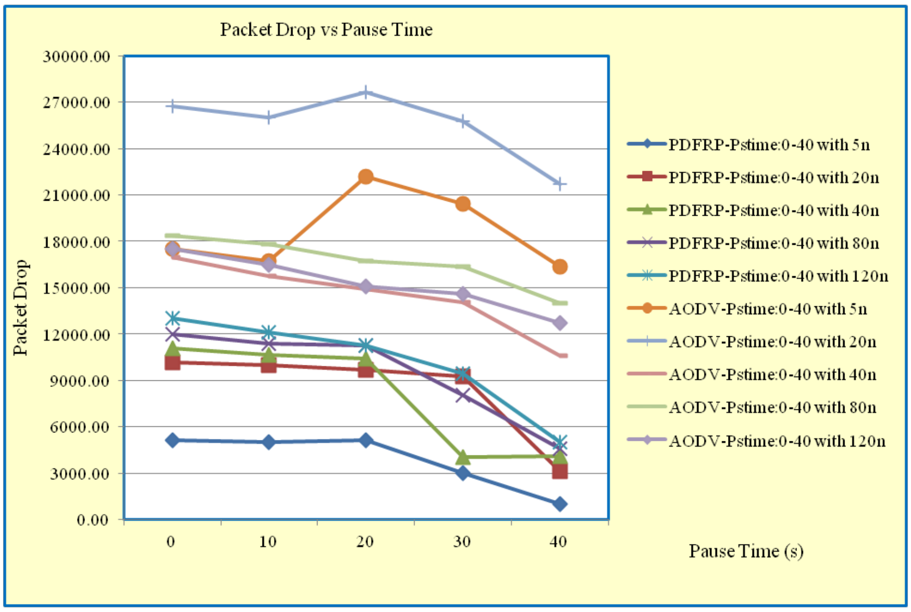


Figure 7.5: PDFRP and AODV: Packet Drop vs. Pause Time

7.2.6 Throughput vs. Pause Time

This sub-section illustrates the throughput results obtained by both PDFRP and AODV in this experiment and compares protocols' performance. Throughput metric is used to measure the effectiveness of the routing protocol performance especially to know the amount of data that is transmitted successfully from the bottleneck node (not sender node) to the destination in a given time period. In this experiment, the throughput calculated only at agent level packet (AGT level) to avoid receiving wrong calculation for the throughput because in the trace file, there are different levels of received packets such as RTS packets, CTS packets and ARP. After filtering these packets out, the agent level packets are calculated where the total agent packets received at the destination node is divided by the total simulation time. Figure 7.6 shows results for both PDFRP and AODV. All results show that the developed protocol outperforms AODV Protocol with 21.40%, 23.26%, 30.99%, 28.10% and 29.65%. All results are increasing as the pause time grows which it confirms that the longer pause time, the more mobile ad-hoc network will be stable. In this respect, the result shows that this objective is achieved because the PDFRP presented better results compared to AODV standard results.

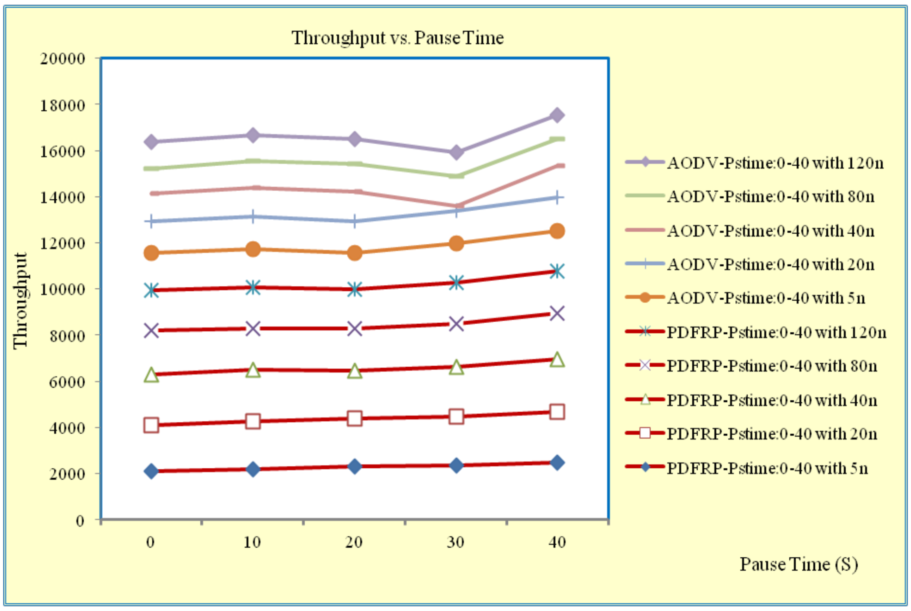


Figure 7.6: PDFRP and AODV: Throughput vs. Pause Time

7.3 Results and Discussion of Varying Speed

In this section, routing overhead experiment will be demonstrated where it emphasizes the effect of network mobility with speeds ranging over 5 to 40 m/s, then compares results of PDFRP to AODV. Table 7.3 illustrates the parameters where speed is varying. This experiment carried out 10 main scenarios with 5 sub-scenarios for both protocols where nodes' speed vary and rest of the parameters are kept constant except node density whereby each sub-scenario applies a different number of nodes.

Table 7.3: Varying Speed Parameters

Parameters	**Values**
Simulator	ns-2
Routing protocol	PDFRP and AODV
Range	1000 m x 1000 m
Max-speed	5,10, 20, 30, 40 m/s
Pause time	20 s
Simulation time	2060 s
Packet type	Constant Bit Rate (CBR)
No of packets	10 pkt/s
Packet size	512 bytes
No of nodes	5, 20, 40, 80 and 120

7.3.1 Routing Overhead vs. Speed

Figure 7.7 shows routing overhead for both protocols significantly varies and much depends on the node speed. The graph shows AODV standard presents low performance for routing overhead compared to PDFRP performance. This is because for high mobility network condition, there is a possibility that more link breakage happens for AODV. In such a case, AODV will change the route frequently and has to generate more routing packets compared to PDFRP with the link prediction mechanism expecting less link failure. In ad-hoc characteristic, when nodes are moving very fast there is a possibility that the rate of disconnections will be higher. As a result, AODV makes more route errors and frequently needs for re-initialization of the route discovery process from source.

On the other hand, this result shows that the PDFRP protocol is more efficient than the existing AODV standard protocol and performs better for routing control message. Figure 7.7 illustrates the comparison results with different scenarios. These scenarios are all investigating these two routing protocol performance with different network mobility perspective. As in Figure 7.7 depicts, each scenario presents a different result for each protocol. The resulst gained from PDFRP for the first

(*PDFRP-Pstime:0-40 with 5n*) and last scenario (*PDFRP-Pstime:0-40 with 120n*) are 400.00 and 29501.00 (Routing packets) where AODV shows similar scenarios shown by 350.00 and 39130.00 (Routing packets). At this particular point the AODV performs better than PDFRP in the beginning with 12.5%. This can be explained as follows. Due to the nature of ad-hoc mobility patterns and network environment at the moment, it shows that in this particular experiment the network has been stable and shows that the link failure does not happen frequently**.** In such a situation, the AODV protocol is suitable because it is based on demand routing protocol where it is not necessary to periodically transmit routing to update packets throughout the network as proactive routing protocol does, which makes more networks overhead. Therefore, it indicates that whenever the network is stable, the AODV standard is more preferable than PDFRP. In other words, this indicates PDFRP drawbacks and weaknesses for the developed protocol. Nonetheless, the rest of the results gained regarding PDFRP are shown in Figure 7.7, indicating better performance than ADOV standard. This happens because PDFRP link failure is less, hence it is more likely that one section of communication between source and destination is completed without changing the initial connection, while AODV changes at least one time or more for one section's communication because of lack of prediction.

In that respect, since the PDFRP implements a prediction mechanism which tries to avoid the link break in advance, the routing overhead for rebroadcast route discovery is minimized compared to AODV. This satisfies the basic idea behind the developing of PDFRP protocol to overcome the current AODV limitation by formulating a new basic model to predict the link status and divert data packets in advance.

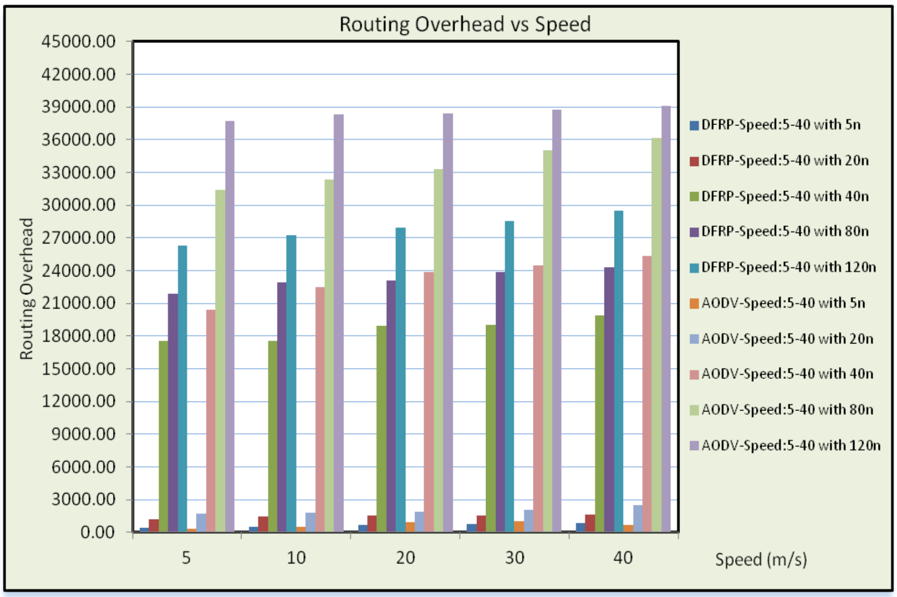


Figure 7.7: PDFRP and AODV: Routing Overhead vs. Speed

7.3.2 Packet Delivery Fraction vs. Speed

This sub-section analyses Packet Delivery Fraction (PDF) while nodes' speed is varied from 5m/s to 40 m/s; then the performance of PDFRP and AODV will be compared based on the results. Analyzing packet deliver fraction gives the overall network condition. PDR is a percentage of packets delivered out of the total number of packets sent. In that situation, if the result of the PDF is poorly performed, it means that the packet drop is also higher. In addition, it indicates that the network overhead is higher as well. Because of that the packet drop performance depends on the number of packet that has been delivered at the destination, whereas the network overhead depends on network congestion and as long as there is a packet drop, obviously, there is network congestion. On the other hand, accumulation of all mentioned above can also affect the End to End Delay.

Therefore, PDF is an important pillar among quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile ad-hoc networks. In this experiment, in order to understand how the nodes' velocity affects the routing protocol performance, the node velocity of the first scenario start, at 5 m/s (18km /h), then in subsequent scenarios the nodes' velocity was increased up to 10 m/sec (36 km/h). The third, fourth, and fifth scenarios velocity was set 20 m/s (72km/h), 30 m/s (108 km/h) and 40 m/s, (144 km/h) correspondingly. However, the intention of this particular experiment is not to investigate the network traffic loaded by nodes' density; instead, its intention is to investigate the network traffic loaded by nodes' speed. This experiment tested 10 main scenarios for each protocol, and each main scenario contains five sub-scenarios, and the total scenarios is 25 (in each protocol). In this respect, the total experiments that have been carried out for both protocol in this section was 50 scenarios.

However, in each sub-scenario, the speed varies while the rest of parameters maintain the same value. Moreover, in the subsequent sub-scenario, the number of nodes should not be same. It means that the five main scenarios each will apply a new number of nodes. For example, in the first main scenario, the number of nodes is five following the main scenario. The number of nodes will be 20 nodes for the second and third, fourth and fifth number of nodes is, 40, 80 and 120 nodes respectively. Figure 7.8 presents all scenarios and the results for both protocols as well.

Figure 7.8 shows that the packet delivery ratio performed poorly for both protocols whenever the nodes' velocity grows. The results of the first (*PDFRP-Pstime:0-40 with 5n*) and last (*PDFRP-Pstime:0-40 with 120n*) scenarios for PDFRP are 97.25%, 96.90%, 96.50%, 96.36%, and 96.10% whereas the results of the last scenario are 98.22%, 98.10%, 97.13%, 96.90% and 96.67% correspondingly. The results of the similar scenarios for AODV are 65.11%, 64.19%, 63.79%, 62.78% and 60.68% whereas the results of the last scenario are 72.53%, 71.34%, 70.75%, 70% and 68.78% respectively.

The first results of the first scenario for PDFRP shows that the number of packets that has been generated only 2.75% was not delivered, whereas the second result for the same scenario 3.10% was not delivered. Similar scenarios for AODV delivered 65.11% and 64.19% respectively (34.89% and 35.81% were not delivered). It is obvious that the results presented in Figure 7.8 satisfy the reason that the different nodes' velocity has been investigated, because, as can be seen, whenever the speed increases, the packet delivery ratio decreases. However, more clarification as to why the packet delivery ratio was inferior when the network mobility increases are explained below.

As described by Kumar [157], mobile ad-hoc network's characteristic, the high-speed movement, indicates the route might not have been maintained frequently. Because, nodes may change direction quickly and might also suddenly change the position. As a result, there is more packets loss, delays increase and networks get congested as well. Figure 7.8 shows that this drawback affects more AODV performance, because in such a high speed environment more link failures are caused which enforces that AODV protocol has to re-generate route discovery frequently upon link failure. On the other hand, this also affects PDFRP although it has much better performance compared to AODV standard. The reason that it effects PDFRP is the network is running at a very high speed. This might cause a very quick link change where the link state prediction mechanism might not be able to handle the link prediction in order to find a new route and at the same time to divert it into a new route, as it might require quite some time to handle the issue. However, the PDF results indicate that the PDFRP outperforms ADOV in terms of the packet delivery ratio.

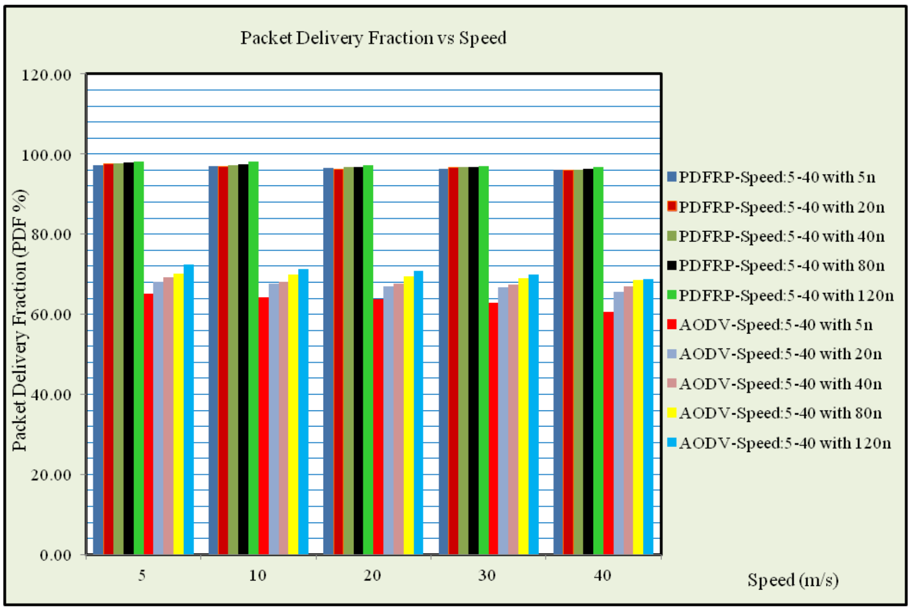


Figure 7.8: PDFRP and AODV: Packet Delivery Fraction vs. Speed

7.3.3 Normalized Routing Load vs. Speed

Normalized Routing Load (NRL) as faction of speed for PDFRP and AODV where NRL is a measurement metric for mobile ad-hoc network in order to evaluate the performance of routing protocol in terms of routing messages that have transmitted. NRL is also a metric that presents the relationship between routing packets (control message) and CBR packets (real data packet). Nevertheless, since it identifies the number of routing control messages that can be conveyed per data packet delivered at the destination, this metric is enough to determine the efficiency and scalability of the protocol performance. This sub-section focuses on normalized routing loads as faction of speed and evaluates the effect of the nodes' various velocity. Figure 7.9 shows the results of normalized routing load gained by simulation experiments. It presents the results respecting the varying of nodes' speed from 5 m/s to 40 m/s.

The main objective that the velocity increases is to investigate the performance behavior of the protocols with a low and high network environment to evaluate the dependence of network mobility and routing control message. In addition, it also investigates which protocol can adapt to either faster or delays. Figure 7.9 illustrates five main scenarios for PDFRP and five scenarios for AODV. As mentioned earlier, each protocol is divided in five sub-scenarios and athere are 50 scenarios altogether. The number of nodes used in this section and details of scenarios have been explained in the previous section. Figure 7.9 shows the results for both PDFRP and AODV whereas Table 7.4 presents comparison values.

Table 7.4: Comparison of PDFRP vs. AODV for NRL Results

PDFRP-scen1	**AODV-scen1**	**PDFRP-scen2**	**AODV-scen2**	**PDFRP-scen3**	**AODV-scen3**	**PDFRP-scen4**	**AODV-scen4**	**PDFRP-scen5**	**AODV-scen5**
0.52	1.30	0.65	3.00	0.71	3.50	0.802	5.00	0.85	6.37
0.62	1.90	0.70	3.20	0.754	3.90	0.8435	5.30	0.876	6.78
0.58	2.10	0.6786	3.40	0.767	4.00	0.8654	5.70	0.912	5.30
0.691	2.30	0.7768	3.80	0.845	4.30	0.923	6.00	0.943	7.10
0.7323	2.50	0.8213	3.95	0.887	4.80	0.9456	6.30	1.00	7.80

Table 7.4 presents the results NRL metric for both PDFRP and AODV protocols. The PDFRP-scen1 column represents the results obtained for the first 5 scenarios of PDFRP, whereas the next to right column represents the results for the similar scenarios for AODV. DFPR-scen1 shows that the first results that the first scenario gained was 0.52 (Ratio of transmitted routing messages per data packet delivered). Since the NRL by definition is the total routing packets sent divided by the total data packets received, the results indicate that the ratio for the total data packets sent and the total routing packets received are similar.

Therefore, the number of routing control packets or messages conveyed per data packet in this moment is much minimized and routing protocol performed well in terms of normalizing control message. The next value for the same scenario (DFPR-scen1) shows 0.62 (Ratio of transmitted routing messages per data packet delivered). This value is higher than the previous one. It indicates that the network condition was changed where the total routing packets sent is more compared to the previous scenario or it can also mean that the total data packets received is less than the previous one.

The values in the third row for same scenario (PDFRP-scen1) are important, because they show a value 0.58 (Ratio of transmitted routing messages per data packet delivered) which is below the previous value 0.62 (Ratio of transmitted routing messages per data packet delivered). It is logically supposed to show higher value because as the speed increases, it is expected to show a higher value than the previous value. Why is this result interesting? It is interesting for two reasons, (1) it shows an unexpected result, (2) it shows how easily mobile ad-hoc network rules can be broken. For the last two values for this column which indicate 0.691 and 0.7323 (Ratio of transmitted routing messages per data packet delivered), is followed by the previous explanations which means that whenever the speed increases the value of NRL is also increases. This is because of ad-hoc network characteristic and nodes mobility behavior, as stated in [157, 158], ad-hoc network performance mostly depends on node status in terms of mobility. However, with the above references high speed network presents low performance, but as the above results (0.58 and 0.62) indicate, because of ad-hoc behavior in some cases networks can perform well.

Now, the next right column (AODV-scen1) will be analyzed. The results of the first column for AODV-scen1 have shown 1.30, 1.90, 2.10, 2.30 and 2.50 (Ratio of transmitted routing messages per data packet delivered) respectively. These values from 1.9 up to 2.30 indicate that the data packet received is almost one third of the total routing message packets are sent. In other words, the transmitted routing messages per data packet delivery are nearly three times more than the total data packet delivered. However, the more nodes' velocity grows and of course, network density increases as well, the values of transmitted routing messages for AODV results are increasing over time.

In the last column for AODV-scen5, the RNL results indicate 6.78, 5.30, 7.10 and 7.80 (Ratio of transmitted routing messages per data packet delivered). Nonetheless, AODV failed to perform well in all scenarios, especially when the network mobility is higher and nodes density is also increased. This is because of its poor routing strategy in a network that has relatively high mobility speed. As shown in Table 7.4 and Figure 7.9, NRL results of AODV are higher than 1. This indicates that the data packets received at the destination are less than the total number of routing messages sent for AODV standard experiment scenario. On the other hand, NRL results of PDFRP are below 1. This indicates that the data packets received at the destination are more than the total number of routing messages sent for PDFRP experiment scenario. However, the overall network wellbeing for PDFRP is very good and PDFRP routing protocol performs well compared to AODV standard.

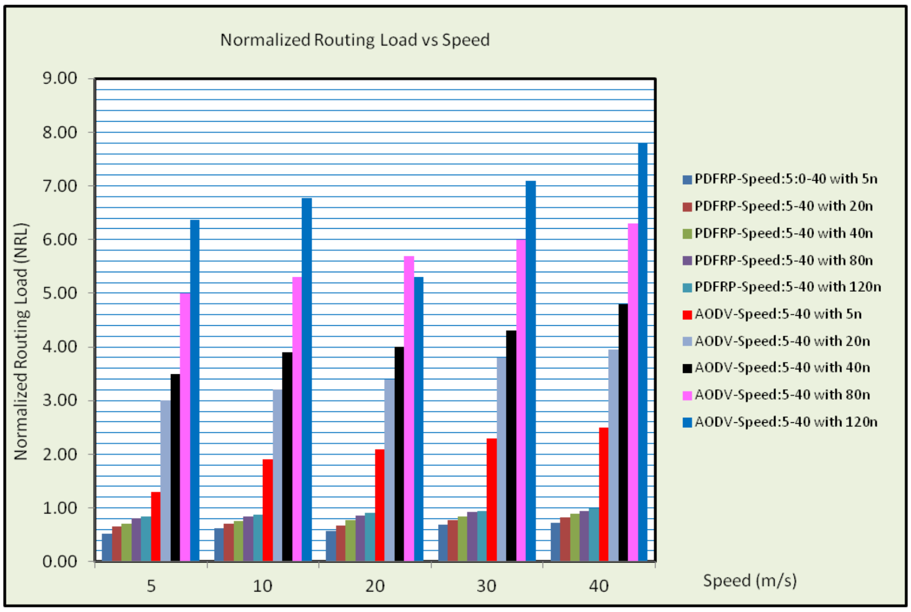


Figure 7.9: PDFRP and AODV: Normalized Routing Load vs. Speed

7.3.4 Average End-to-End Delay vs. Speed

This sub-section analyzes end to end delay with respect to nodes' speed. It focuses on how a delay parameter impacts the performance of protocol over time, especially investigating what happens the end to end delay when the speed increases and how it impacts the protocol performance. Average End-to-End Delay is among the quantitative metrics that is used for evaluating the performance of a routing protocol to measure its efficiency for packet delivery time perspective. Figure 7.10 illustrates end to end delay results for PDFRP and AODV where it has tested different scenarios with varying nodes' speed.

This sub-section, emphasizes the speed impact on two protocols, namely PDFRP and AODV standard. In that respect, several experiments with different scenarios has been examined in order to ensure and verify the accuracy of the results. Five different speeds are examined. In addition to that each is examined five times with different node density. For example, in Figure 7.10, the right side indicates (PDFRP-Speed:5-40 with 5n), where the numbers 5 to 40 represent the range of speed that was tested, whereas "5n" represents the nodes' density that is used for those varying speeds. This indicates that five times with five different speeds have been tested, and that only one node is used, namely five nodes (5n). For the next scenario, (PDFRP-Speed: 5-40 with 20n) what has been changed is the number of nodes where it indicates "20n" instead of "5n" and this continues until they reach "120n". These experiments, which have been tested, include five different nodes' density with 25 scenarios of speeds, because in each node five different speed values are tested. The scenarios for AODV have also been tested as illustrated in Figures 7.10 and Table 7.5.

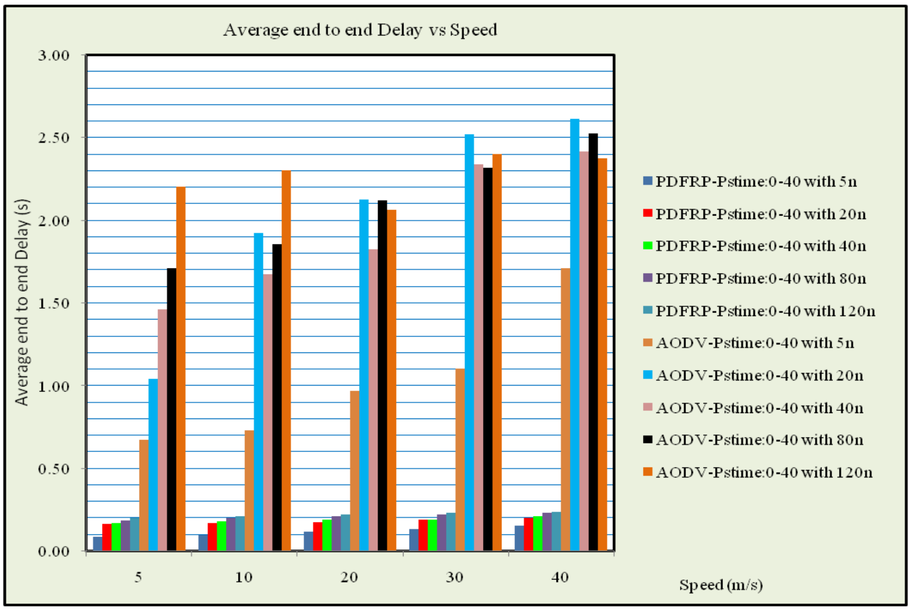


Figure 7.10: PDFRP and AODV: Average End-to-End Delay vs. Speed

Table 7.5: Comparison of PDFRP vs. AODV for Average End-to-End Delay

PDFRP-scen1	**AODV-scen1**	**PDFRP-scen2**	**AODV-scen2**	**PDFRP-scen3**	**AODV-scen3**	**PDFRP-scen4**	**AODV-scen4**	**PDFRP-scen5**	**AODV-scen5**
0.09 (s)	0.67(s)	0.16(s)	1.04(s)	0.17(s)	1.46(s)	0.19(s)	1.71(s)	0.20(s)	2.20(s)
0.10(s)	0.73(s)	0.17(s)	1.92(s)	0.18(s)	1.67(s)	0.20(s)	1.85(s)	0.21(s)	2.30(s)
0092(s)	0.97(s)	0.18(s)	2.12(s)	0.19(s)	1.82(s)	0.21(s)	2.12(s)	0.22(s)	2.06(s)
0.13(s)	1.10(s)	0.19(s)	2.52(s)	0.19(s)	2.34(s)	0.22(s)	2.32(s)	0.23(s)	2.40(s)
0.15(s)	1.71(s)	0.20(s)	2.61(s)	0.21(s)	2.41(s)	0.23(s)	2.52(s)	0.24(s)	2.37(s)

In Table 7.5, the first two columns indicate two scenarios, which were tested with the same environment for PDFRP and AODV, namely PDFRP-scen1 and AODV-scen1. The first scenarios' delay value for PDFRP shows 0.09 s. The parameters which were involved in this scenario are two, namely five nodes and 5 m/s for nodes's speed. The next value in the same column indicates 0.10 s. The parameters which were involved in this scenario are also two, namely five nodes as previous scenario and 10 m/s for nodes' speed. The third value in the same column indicates 0.12 s. The parameters which were involved in these are also two, which are five nodes and 20 m/s. The fourth and fifth values show 0.13 s and 0.15 s, correspondingly. Same as the previous scenarios, these scenarios (fourth and fifth) were also involved two parameters, which are five nodes with 30 m/s for nodes' speed (for fourth scenario) and five nodes with 40 m/s for nodes' speed (for fifth scenario). As mentioned earlier, the formula for average end to end delay is (*Total-Rt - Total-St/Total-Pr*).

The first scenario has shown a low end to end delay (0.09 s) according to the next scenarios' delay (0.10 s). This is because, as mentioned earlier, the speed is one of the factors which has the impact on mobile ad-hoc network's behavior. Thus, when the speed is increased, it affects the network's delay behavior compared to previous results. The third results (0.0921 s) can bring confusion because as mentioned above is supposed to show a higher value than previous one (0.10 s), but instead it has shown less value. This is one of the strange characteristics of ad-hoc environment, because at the same time it tests a scenario, and it gives a value, so if the same scenario is tested after 10 minutes, then it might give you a different result or unexpected value. In ad-hoc researchers, in order to overcome such an incident, each scenario needs to be run several times and the average is taken. This thesis followed this method (each scenario was tested at least five times, and the average result was taken from that average). The reason that it has been tested several times is as stated in [102], one of the standard ways to obtain a better accuracy of performance measures obtained from simulations is to take the average of several independent runs. In addition, our empirical experiment that has tested and evaluated the current algorithm of AODV in Chapter Four also experienced that the average of independent runs is more accurate because of ad-hoc unpredictable speed and node movement**.** The next two values (0.13 s and 0.15 s) have shown that the speed varying was affected and this validated that the third scenario's result (0.092 s) which was an unexpected result, as stated earlier in this chapter as well as Chapter Four. One of the ad-hoc network's attributes is when the speed is increased the performance of the network will be decreased. Thus, the two values (0.13 s and 0.15 s) indicate that the first delay is 0.13 and as the speed is increased, the next value of the delay became worse (0.15 s) than the previous delay. In this respect, the next value (0.092 s) should also become worse than previous one, but it actually became better value. Therefore, according to ad-hoc's well known theoretical background, this is an unexpected result.

Because overall scenarios which have been tested in this column were 5 and 4 provided the expected results whereas only one gave an unexpected result, the experiment was correct according to the ad-hoc characteristic. AODV-scen1 show 0.67 s, 0.73 s, 0.97 s, 1.10 s and 1.71 s. These experiment scenarios also involved two parameters, nodes density and speed. As in previous scenarios (PDFRP-scen1), each of these scenarios was tested with varying velocity (5 to 40 m/s), with a fixed number of nodes. As presented in Table 7.5, the AODV-scen1 results indicate that the average end to end delays are much different from PDFRP-scen1. It shows that the AODV delays are much higher compared to PDFRP results.

For example, PDFRP first result indicates, 0.09 s, whereas AODV presents 0.67 s, the AODV results is 10 times higher than PDFRP result. This indicates that the AODV scenario involved high delay with low data packets delivered. In other words, it shows that this scenario more routing control packets are conveyed, and many packets drop were also involved. However, when such metric values are increased, the probability of link failure will be also increased. Therefore, the reason that the AODV result becomes very high compared to PDFRP, is most likely because more link failures happened, and the AODV natural route rebroadcast mechanism made heavy routing messages, which probably affected the delays increasing for AODV results.

7.3.5 Packet Drop vs. Speed

The speed and node mobility for ad-hoc network is a key which results in packet loss as well as packet delivery. Thus, in this sub-section, the performance with different mobility patterns is illustrated. It discusses the factors which support that the packets will be dropped on the way to the desired destination. It also draws the relations between the nodes' speed and routing protocols' performance. Finally, a comparative analysis of simulation results which was achieved by this experiment is discussed and evaluated (the PDFRP and AODV performance regarding the packet drop against nodes' velocity). Nonetheless, this experiment considers performance of developed protocol (PDFRP) vs. AODV standard routing protocols with respect to speed. Factors that commonly affect the routing protocol performance are delay, routing overhead, and congestion.

However, three performance metrics are indirectly proportional to each other for network performance evaluation, including packet delivery ratio, the network routing overhead and drop data packets and all are influenced by high speed. According to Tie-yuan et al. [158], when the speed is high, there is a high probability that the node will continue moving at high speeds, and as a result generating frequent link breakdowns. On the other hand, for lower node speeds, it is very likely that the frequency of link failure is also lower. Nonetheless, in the case that the node speed is lower, the network performs better. Therefore, when the network is running at a higher speed, the network topology is more frequent and routing messages increase as well. As a result, the packet drop is increased.

Figure 7.11 presents the scenarios' results for packets drop for both PDFRP and AODV. As the previous sections explained, 10 main scenarios with five sub-scenarios in each have been taken. Figure 7.11 (*PDFRP-speed: 5-40 with 5n*) indicates the result for one main scenario, which contains another five sub-scenarios. The number 5 to 40 indicate the speed range while the "5n" stands for the number of nodes used in this scenario. The varied speeds which have been used are 5, 10, 20, 30 and 40 and five nodes in the first scenario. This means again that this experiment has been tested five times with five different speeds with five nodes only. The next experiment for PDFRP is (*PDFRP-speed: 5-40 with 20n*) which has gone through some of the previous steps; the difference is that the number of nodes was set at 20 instead of 5. The rest of the scenarios follow the same steps. In AODV scenarios, such as (*AODV-speed: 5-40 with 5n*, *AODV-speed: 5-40 with 20n, AODV-speed: 5-40 with 40n*), etc. also follow the same steps as PDFRP scenarios.

The results for AODV presented in all scenarios are very low compared to the results provided by PDFRP protocol. It indicates that the packets drop for AODV is very high, which indicates that as the speed increases, the drop is also increased. This is because, as described in [158], when the speed is increased, it is very likely that link breakage is increased as well. In other words, the PDFRP protocol performed much better than AODV.

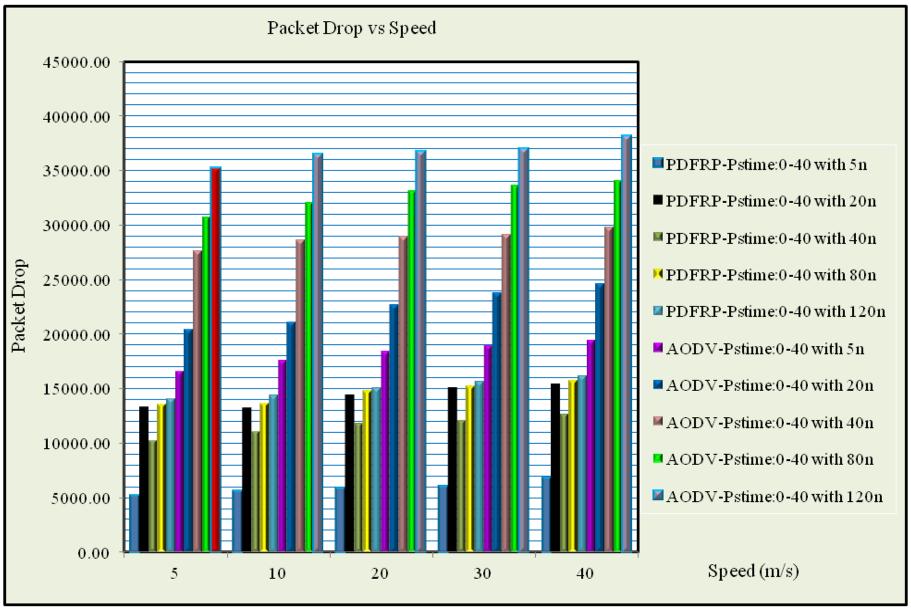


Figure 7.11: PDFRP and AODV: Packet Drop vs. Speed

7.3.6 Throughput vs. Speed

This section discusses the throughput with respect to speed and analyzes the throughput results and evaluates the protocols' performance. There are two ways to represent the throughput, and they are as follows: One is the amount of data transferred over the period of time expressed in kilobits per second (Kbps). In this case, it is calculated by summarizing the data packets received at the receiver node which is then divided by the total simulation time. The other method that represents the throughput is the packet delivery percentage achieved from a ratio of the number of data packets sent and the number of data packets received. This can be obtained through the PDR formula as defined in the previous sections. Figure 7.12 illustrates throughput vs. speed**.** The throughput for PDFRP shows relatively high throughput but on the other hand it decreases as the speed increases over time, whereas the throughput under AODV linearly increases. Table 7.6 presents throughput results comparison for both protocols.

Table 7.6: Throughput Results Comparison for Both Protocols

PDFRP-scen1	AODV-scen1	PDFRP-scen2	AODV-scen2	PDFRP-scen3	AODV-scen3	PDFRP-scen4	AODV-scen4	PDFRP-scen5	AODV-scen5
2209.11 kbps	1680 kbps	1908.48 kbps	1470.43 kbps	1500.33 kbps	1100.51 kbps	1200.33 kbps	800.32 kbps	1003.42 kbps	639.65 kbps
2120.48 kbps	1650.32 kbps	1850.6 kbps	1390.45 kbps	1450.31 kbps	1050.52 kbps	1150.36 kbps	750.27 kbps	912.82 kbps	600.24 kbps
2154.5 kbps	1590.32 kbps	1790.28 kbps	1300.45 kbps	1400.22 kbps	1000.33 kbps	1100 kbps	730.35 kbps	900.31 kbps	590.2 kbps
2054.5 kbps	1550.32 kbps	1690.23 kbps	1250.45 kbps	1360.56 kbps	900.47 kbps	1002.31 kbps	710.12 kbps	850.42 kbps	585 kbps
2054.5 kbps	1550.32 kbps	1690.23 kbps	1250.45 kbps	1360.56 kbps	900.47 kbps	1002.31 kbps	710.12 kbps	850.42 kbps	585 kbps
2000.1 kbps	1500.32 kbps	1580.24 kbps	1200.55 kbps	1250 kbps	850.33 kbps	950.61 kbps	690.32 kbps	800.31 kbps	558 kbps

PDFRP-scen1 represents the first scenario for PDFRP, while PDFRP-scen2 stands for the second scenario for PDFRP and the rest of PDFRP fields in the table 7.6 represent the rest of the scenarios. Similarly, AODV-scen1, AODV-scen2, AODV-scen3, AODV-scen4 and AODV-scen5 illustrate AODV scenarios' results. In Table 7.6, the first five scenarios (PDFRP-scen1) throughput results for PDFRP are 2209.11, 2120.48, 2154.50, 2054.50, and 2000.10 kbps respectively. In this respect, the first throughput indicates slightly higher than the following scenario's throughput, where the next throughput is a little higher than the next following scenarios' results and so on until last results which show the least value. This is because as described in Chapter Four, choosing a smaller maximum speed with longer pause time, the topology of the ad-hoc networks will be relatively stable while with longer maximum speed and small pause time, the topology of ad-hoc network changes rapidly as written by Yoon [90].

In Table 7.6, the first five scenarios (AODV-scen1) throughput results for AODV protocol are: 1680.00, 1650.32, 1590.32, 1550.32, and 1500.32 kbps correspondingly. The above values show exactly the same indications as shown in the DFPR in terms of throughput reduction as nodes' velocity increases over time. This confirms, as mentioned in the previous section with the reference, choosing a smaller speed with longer pause time presents better performance. Nonetheless, the results presented in Figure 7.12 show that the PDFRP protocol outperforms AODV in terms of throughput with 23.95%, 22.17%, 26.18%, 24.54% and 24.98% respectively.

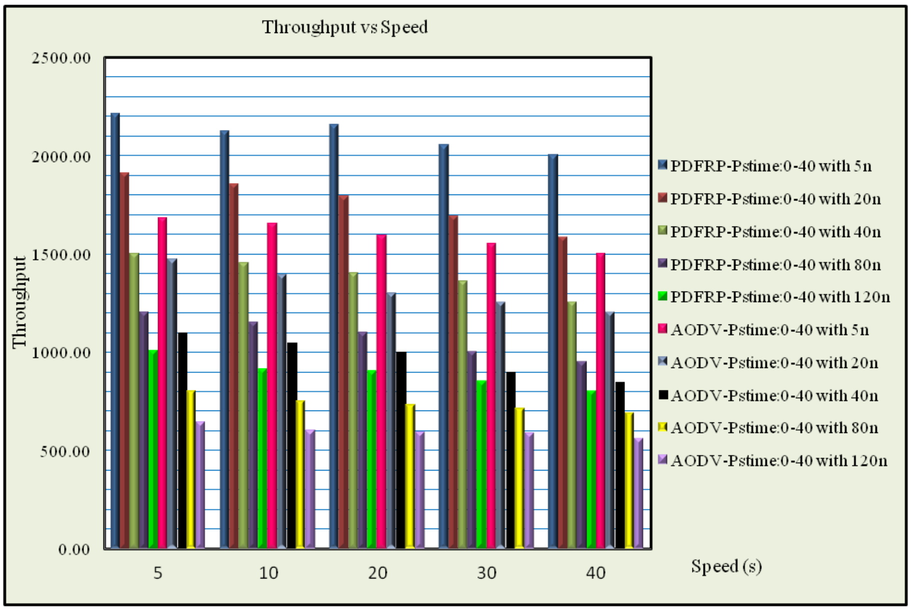


Figure 7.12: PDFRP and AODV: Throughput vs. Speed

7.4 Results and Discussion of Varying Node Density

The previous sections investigated the effect of network movement such as pause time and speed where different scenarios of node mobility and pause time have been conducted as well. In the previous sections, the number of nodes was fixed while the movements (pause time and speed) were varying in each sub-scenario. In this respect, it is not easy to identify the nodes' density effect on the network. This section discusses the effect of network density. It varies the number of nodes and analyses the protocol performance with respect to nodes' density. In other words, a fixed pause time and speed are tested with different node density. The maximum capacity of the routing protocol can be easily figured out. These scenarios consist of 5, 20, 40, 80, and 120 mobile nodes, with parameters defined in Table 7.7.

Table 7.7: Node Density Parameters

Parameters	**Values**
Simulator	ns-2
Routing protocol	PDFRP and AODV
Range	1000 m x 1000 m
Max-speed	5 m/s
Pause time	20 s
Simulation time	2060 s
Packet type	Constant (CBR)
No of packets	10 pkt/s
Packet size	512 bytes
No of nodes	5, 20, 40, 80, 120

7.4.1 Routing Overhead vs. Node Density

This sub-section discusses the results for routing overhead in relation to node density. Figure 7.13 presents the experiment results for routing overhead against node density which illustrates different network sizes for both PDFRP and AODV standard results. As depicted in Figure 7.13, the density increases from the left side to right side. In other words, as the network density is increased, the routing overhead is also increased. This experiment shows that the routing overhead for PDFRP is much less compared to the results for AODV standard. Thus, this evaluation clearly indicates that the PDFRP protocol outperformed AODV standard.

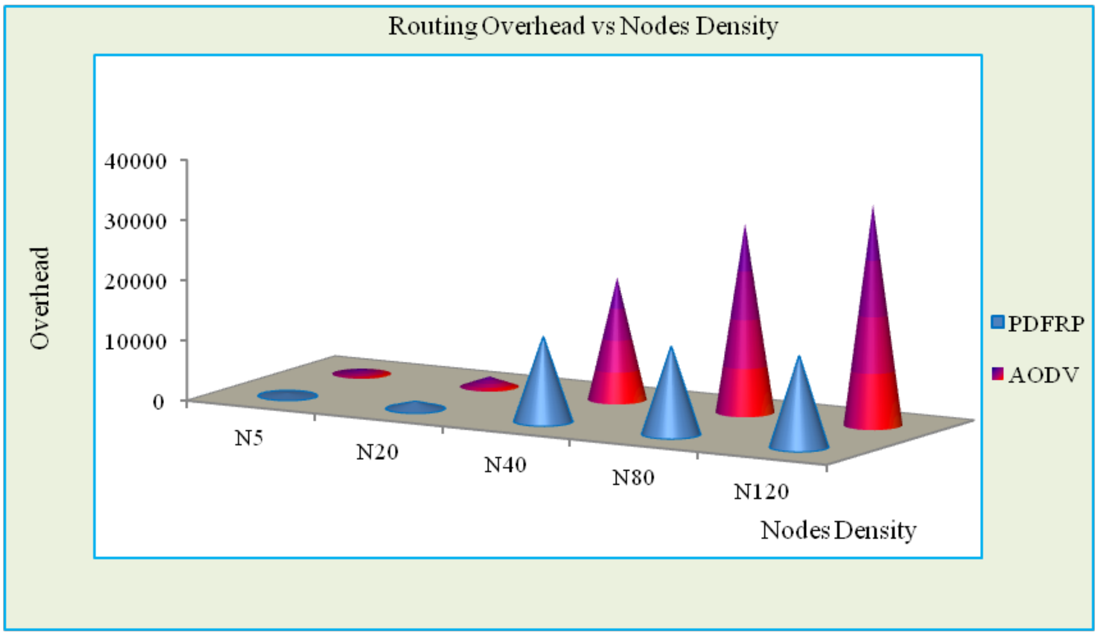


Figure 7.13: PDFRP and AODV: Routing Overhead vs. Nodes Density

7.4.2 Packet Delivery Fraction vs. Node Density

This sub-section present the results for the packet delivery fraction vs. node density. Figure 7.14 presents the results for the packet delivery fraction where the number of nodes is fraying with a range of 5 to 120 nodes. The previous results for routing overhead have shown that whenever the network is increased the overhead is also increased. However, this experiment is the opposite, as in Figure 7.14 which indicates whenever the network density increases the packet delivery fraction decreases. This is because the more network density is increased the more network is congested, which causes more link failures. In that case, the packet delivery at the destination side is also decreased. Packet delivery fraction is one of those fundamental factors to evaluate the routing protocol effectiveness as well as its efficiency.

Figure 7.14 shows that the results for AODV standard have more fluctuations according to PDFRP results. For example, the result for 20 nodes indicates less value than the result for 40 nodes' value, which is logucally not supposed to be less. Obviously more link failures happened at 20 nodes' time, whereas at the 40 nodes' time the network congestion is less. In PDFRP, the results do not show any fluctuation. When the network density is a higher, packet delivery fraction is worse, which is correct according to the ad-hoc characteristic. This experiment also show that the PDFRP protocol outperformed AODV standard.

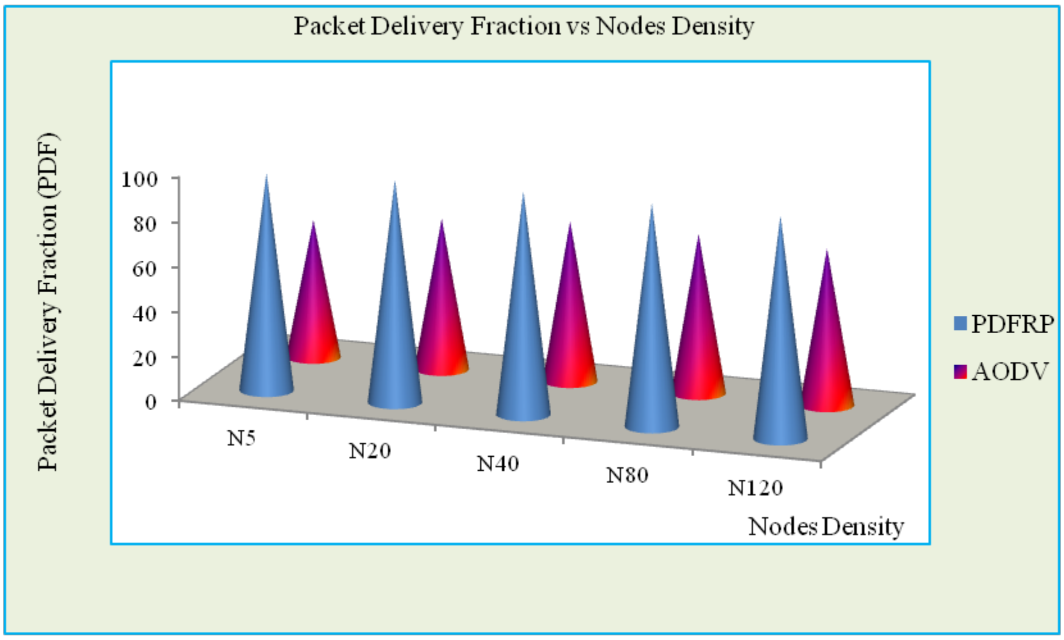


Figure 7.14: PDFRP and AODV: Packet Delivery Fraction vs. Nodes Density

7.4.3 Normalized Routing Load vs. Node Density

This sub-section presents the normalized routing load while increasing the number of nodes with a range of 5 to 120. As indicated in Figure 7.15 , for high number of nodes, AODV standard suffers higher normalized routing load than the PDFRP protocol. This is because of the characteristic of AODV standard for route maintenance upon link failure,where it will propagate a route error message back to the source node. Thus, with the increase of nodes' density, the routes change more frequently and there is a strong need of finding new routes, which causes less packet delivery as well as more link failures. On the contrary, Figure 7.15 shows that the results of PDFRP protocol are much better. This happens because PDFRP utilizes a new mechanism such as Upstream Notification (UN).

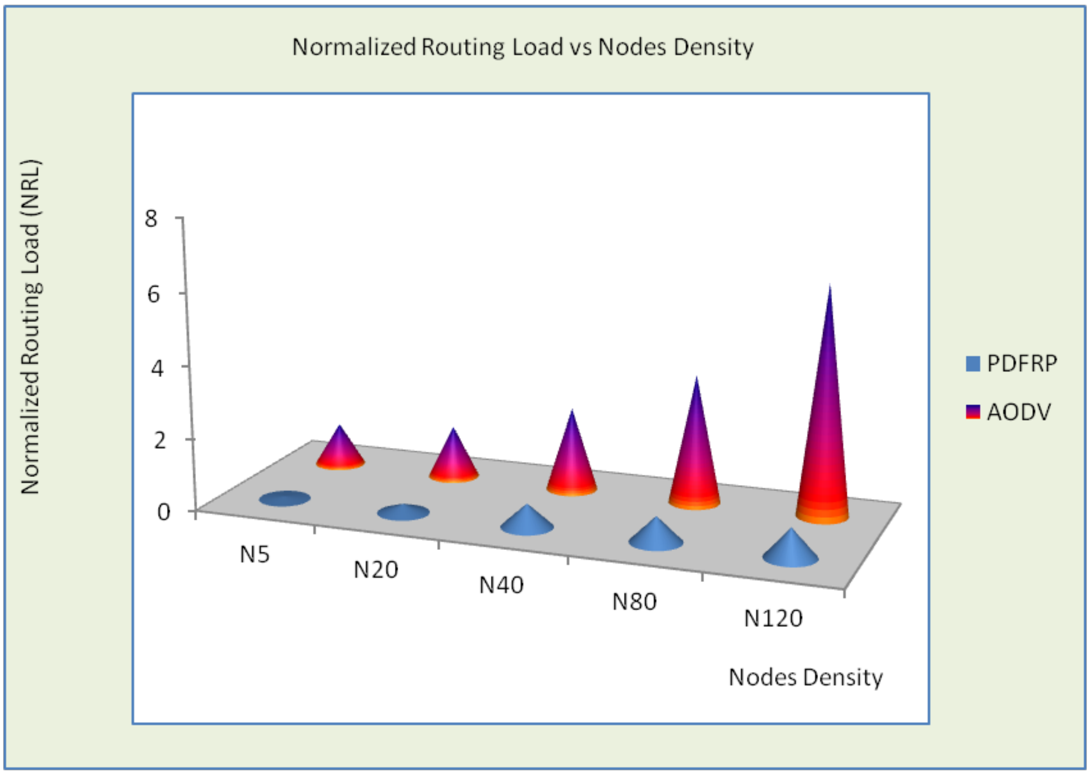


Figure 7.15: PDFRP and AODV: Normalized Routing Load vs. Nodes Density

7.4.4 Average End-to-End Delay vs. Node Density

As stated in the previous section (Section 7.1), the research evaluates the efficiency of the developed protocol by widely using metrics among delay, packet loss, packet delivery ratio, etc. The most of these metrics are depend on each other and there is no one which is completely independent from other metrics. This means that the outcome of one metric is proportional to another metric's behavior. Figure 7.16 illustrates average end to end delay with fraying node density illustrating that delay performance improves with the decrease of network size. It indicates that for a network with 20 or fewer mobile nodes, the average end to end delay is much better off compared with higher network mobile nodes. This happens because the more network traffic takes place, the more network congestion and routing overhead are involved, which contributes to a high probability of link failure. However, all these accumulation factors are donated to contribute the increase in the overall average end to end delay. The experiment indicates that the developed protocol outperformed AODV standard with 93.49% from 5 to 20 nodes while it improved with 91.99% from 80 to 120 nodes.

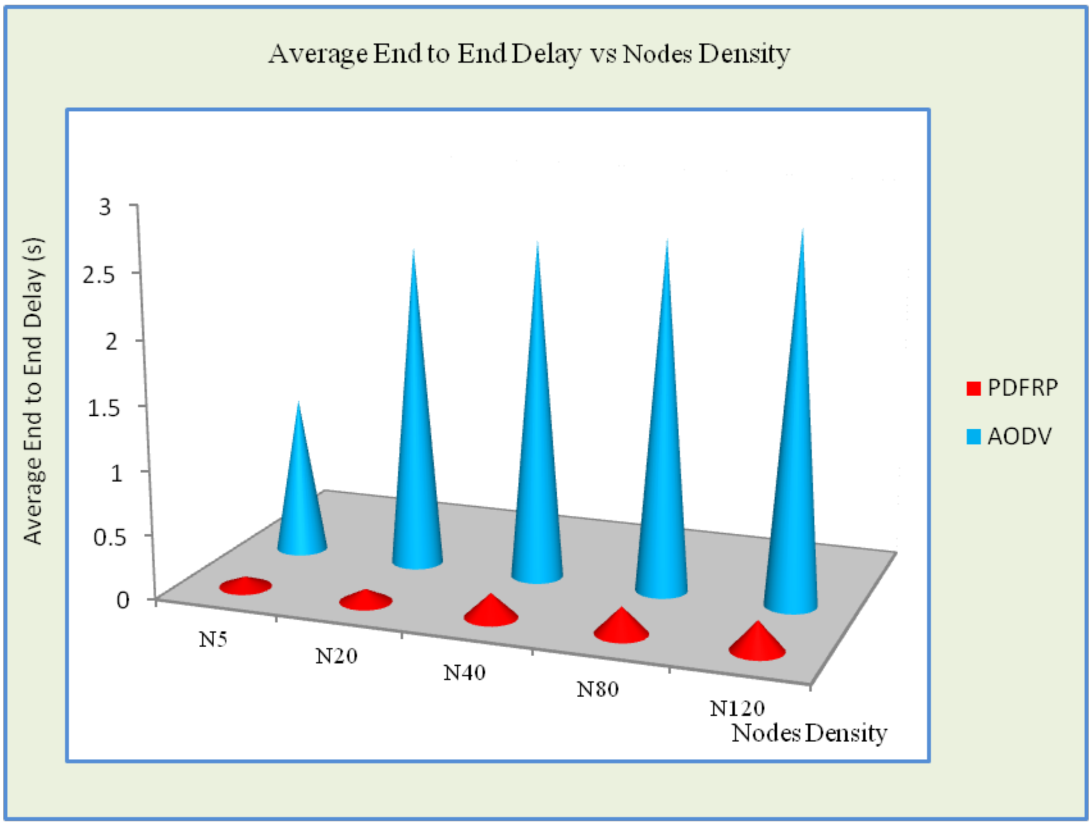


Figure 7.16: PDFRP and AODV: Average End-to-End Delay vs. Nodes Density

7.4.5 Packets Drop vs. Node Density

In this experiment, the number of packet drop within one successful data transaction in the network size with range 5 to 120 mobile nodes (Figure 7.17) is investigated. The packet drop metric is an important factor for network's overall wellbeing. In the case where the number of packet drop is higher, it might involve other factors such as the Packet Delivery Fraction (PDF) and more routing overhead. Actually, the PDF and packet loss are directly proportional, because of fewer PDF results which indicate that there is high packet loss in the network, whereas minimum packet loss indicates high PDF. In other words, more routing overhead illustrates that there is more link failures in the network because the routes change more frequently as it tries to find new routes. Figure 7.17 depicts the experiment result for packet loss. In addition, Table 7.8 shows the number of packet loss in each network size.

Table 7.8: Number of Packet Loss in Each Network Size

PDFRP-5-N	**AODV-5-N**	**PDFRP-20-N**	**AODV-20-N**	**PDFRP-40-N**	**AODV-40-N**	**PDFRP-80-N**	**AODV-80-N**	**PDFRP-120-N**	**AODV-120-N**
30513	17533	14155	26722	10100	16951	10817	18374	13614	17500

Values in the Table 7.8 indicate that the highest value of packet drop is 30513. These packets are dropped where the network size was 5 nodes in PDFRP protocol, whereas AODV standard in same network size is presented as 17533 (packets drop). In this case, since this metric depends on other factors, in this transaction it might happen more routing overhead caused by frequently link failures might happen. In such a case, there is a hypothesis in the ad-hoc network which most likely caused this accident. As described by Abdule et al. [103], the network with or fewer 20 mobile nodes are much sparser than the network with more than that number which causes a high probability of packet drop. In such a case, the packet drop performance suffers from transient partitions that exist in a sparse network. Therefore, it looks like the entire network takes place sparser or at longer distance from each other in that moment. On the other hand, as illustrated in Figure 7.17, when the number of mobile nodes increases the sparse network effect disappears, and packet drop becomes smaller. However, the rest of results shows that the fluctuation is not that much and this indicates the above theory is confirmed.

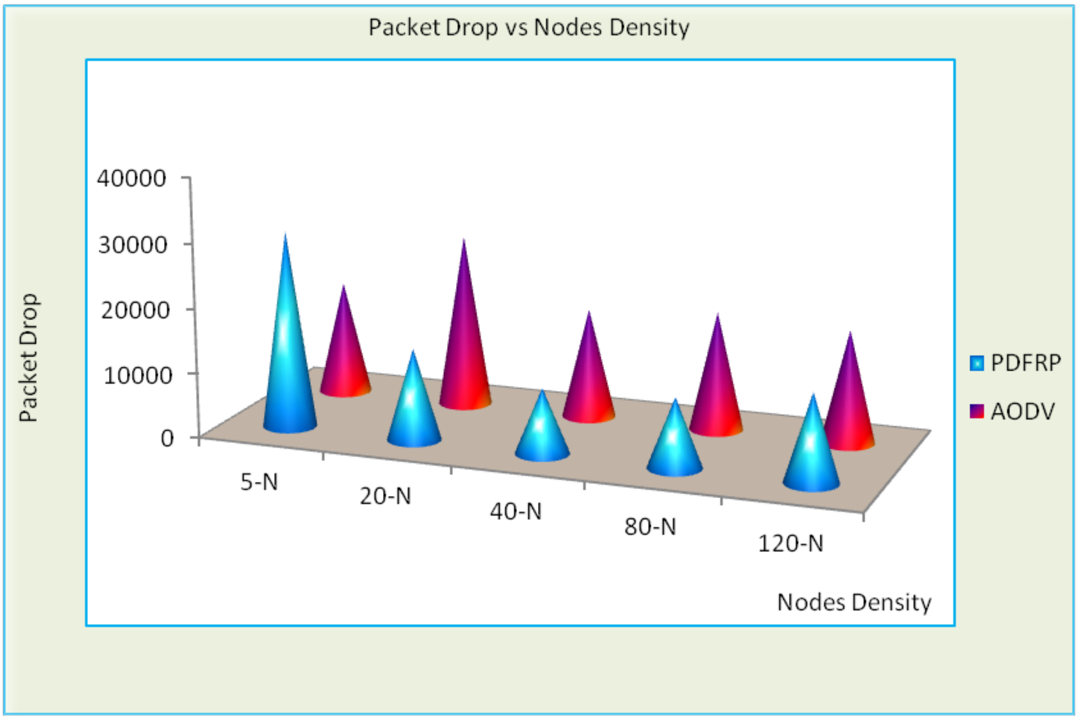


Figure 7.17: PDFRP and AODV: Packet Drop vs. Nodes Density

7.5 Performance Comparison to Current Work

7.5.1 Comparison for Model 1

This section discusses the comparison between PDFRP and one of the related current works. In our work, the result of PDFRP is compared with the current work on the theoretical and graphical framework comparing our algorithm to another algorithm that is also based on AODV. Cheng et al. [159] proposed and developed integrating preemptive link breaking avoidance and path shortening mechanisms into a modified AODV protocol. The first mechanism is a procedure that activates link breaking avoidance, called Dynamic Link Breaking Avoidance (DLBA). Besides that they initiated path shortening mechanism which they call Dynamic Path Shortening (DPS). DPS is a mechanism that is useful only if there is a shortcut available for the active route. The DLBA mechanism also utilized link state prediction mechanism where link quality is determined by signal strength upon receiving a packet. Figure 7.18 illustrates the idea behind DPS mechanism where the first packet sent from the source node, its hop count value would be set to zero and incremented by one where the term "altitude" represents the 'hop count'.

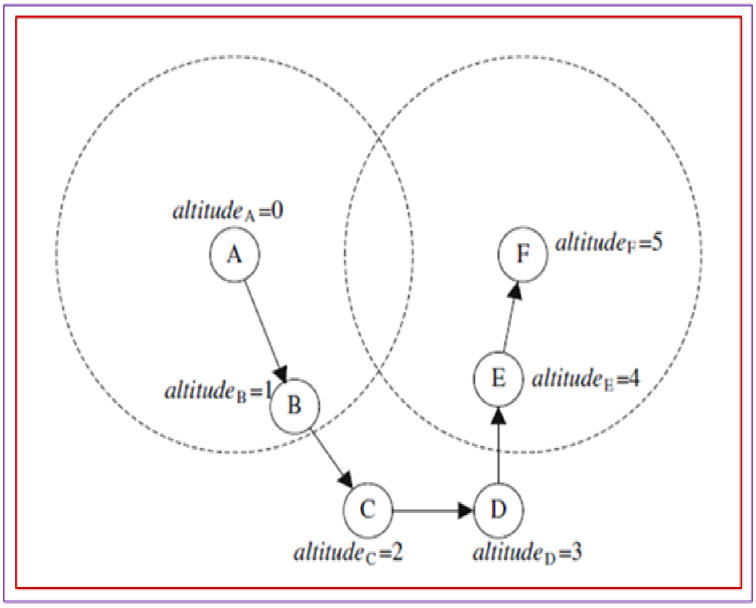


Figure 7.18: An Illustration of the Definition of DPS (altitude) (Adapted from [159])

The second mechanism that they proposed is Dynamic Link Breaking Avoidance

(DLBA) which operates by monitoring the quality of communication links (in order to avoid link breaks in advance). The DLBA mechanism inserts an intermediate node which is in between two end nodes of some breaking link. For instance, Figure 7.19 presents the link between A and B that is about to break whereas link A-B is replaced by A-C and C-B. One major drawback for this mechanism is, if there are no intermediate nodes, the link between A and B will be totally disconnected, then an error message is sent to source where the source rebroadcasts a new route request if necessary.

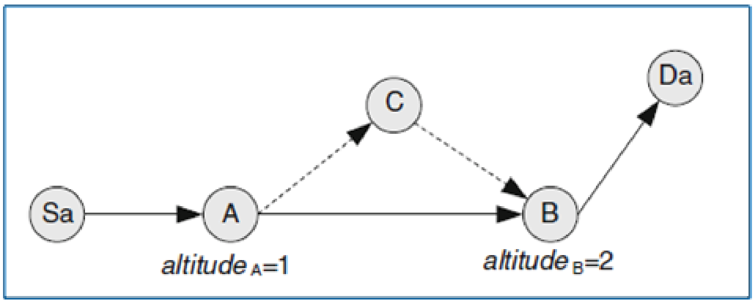


Figure 7.19: The Dynamic Link Breaking Avoidance Mechanism (indicates the link breaking soon) (Adapted from [159])

Nonetheless, the main concept of this mechanism is, if an active link between two nodes is about to break, downstream node (B) notices that the signal strength is weaker than the predefined threshold value and informs neighboring nodes to help upstream node (A) to build a new route by broadcasting a help packet. The main concept of this mechanism is partially similar to our concept but the way of problem solving is different. It seems that the DLBA mechanism considers one angle only, while our protocol looks at several angles. For instance, in PDFRP protocol, if there is no one single neighboring node between A and B that responds because of unfulfilled requirements or there is no intermediate node at all, the PDFRP comes up with a new mechanism, namely Upstream notification (UN) mechanism.

However, this mechanism (DLBA) has two major drawbacks, (1) if there is no intermediate node between A and B, the link will be disconnected, and (2) if all neighbors' signal strengths are lower than the predefined threshold value, which means not one of the intermediate nodes between A-B responds to the help packet (of course the link will be also disconnected). Thus, in the theoretical perspective, the DRFP protocol has a better approach in terms of link failure avoidance as well as providing an alternative solution in case it is not successful in the first approach.

7.5.2 Graphical Comparisons

This section compares the graphs of performance analysis and evaluation results graphically. Since, it is not easy to find the others' real code, the only option which is available in order to compare in our work to related works is to compare their theoretical concepts (their algorithm) and graphical results into our concept and graphical results. Table 7.9 show the parameters setting that DLBA used.

Table 7.9: Parameters Setting for DLBA Simulation

Parameters	**Values**
Topology size	2,200 x 600 m2
Simulator	ns-2 (version 2.1b8a)
Ad-hoc Routing Protocol	AODV, DLBA andDPS
Number of Nodes	100
Simulation time	500 s
Mobile speed	0-20 meter per second
Packet size	64 bytes
Channel capacity	2 M bits/s
Interface queue type	DropTail/PriQueue
Packet rate	3 pkts/s
Mobility model	Random Waypoint
Traffic model	CBR(constant bit rate)
Transport protocol	UDP
Number of comm. pairs	10
MAC protocol	IEEE 802_11 DCF
Path loss model	Two-ray ground
Power range (transmission rage)	250 m

Figures 7.20, 7.21, 7.22, and 7.23 present graphical results for DLBA+DPS and PDFRP which compare the protocols' performance with regards to the selected metrics. The reason that these metrics have been selected for comparison is because these metrics are tested both in our protocol (PDFRP) and their work (DLBA). Figure 7.20 shows a comparison between PDFRP (a) and DLBA (b) regarding packet delivery rate vs. pause time. Figure 7.20 (b) shows the packet delivery ratio for their work (DLBA) which indicates that the highest value for packet delivery ratio is approximately 99.3% whereas the lowest value is approximately 95.7%. Figure 7.20 (a) presents the PDFRP equivalent metrics (PDF) results which it indicates that the highest value obtained is 99.99% and lowest is 98.70%. Figure 7.21 shows the comparison between PDFRP (a) and DLBA (b) with regards to normalized control overhead vs. pause time. As indicated in Figure 7.21 (a) the PDFRP results for normalized control overhead are mostly below 0.75 whereas DLBA + DPS (b) results

are mostly between 1.0 to 4.7 (Ratio of transmitted routing messages per data packet delivered). These results which are based on the graphical comparison show that the DFPR protocol presents better results compared to DLBA in terms of the packet delivery ratio and normalized routing as well.

Figure 7.22 (b) presents the average delay time vs. pause time for their work (DLBA) where their pause time is varying as PDFRP's pause. The pause time values are very important for ad-hoc network because the longer pause time makes the network more stable and results in better performance as well. Figure 7.22 (a), presents the average delay time vs. pause time for PDFRP results where the results perform better compared to DLBA. Figures 7.23 illustrates packet delivery rate vs. number of nodes for both PDFRP and DLBA, correspondingly. These comparisons also indicate that the PDFRP present better results compared to DLBA+DPS in terms packet delivery rate vs. number of nodes. Thus, these graphical comparisons indicate that the PDFRP protocol outperforms DLBA on the subject of the tested metrics.

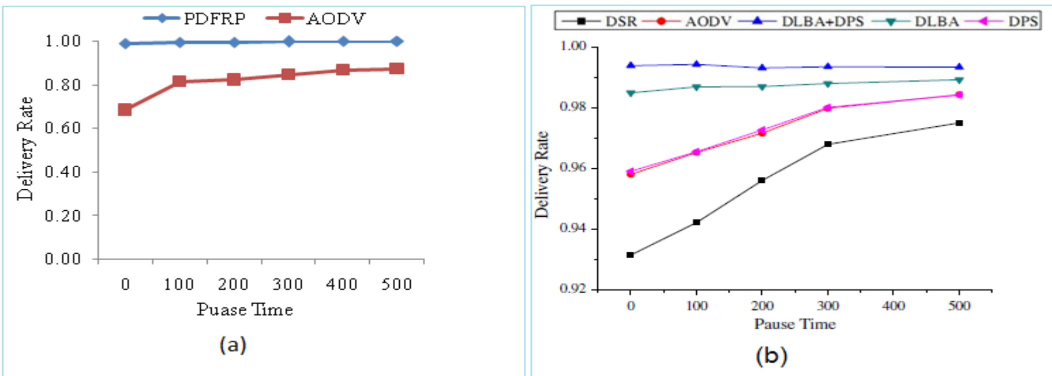


Figure 7.20: Packet Delivery Fraction vs. Pause Time of PDFRP Compared to DLBA

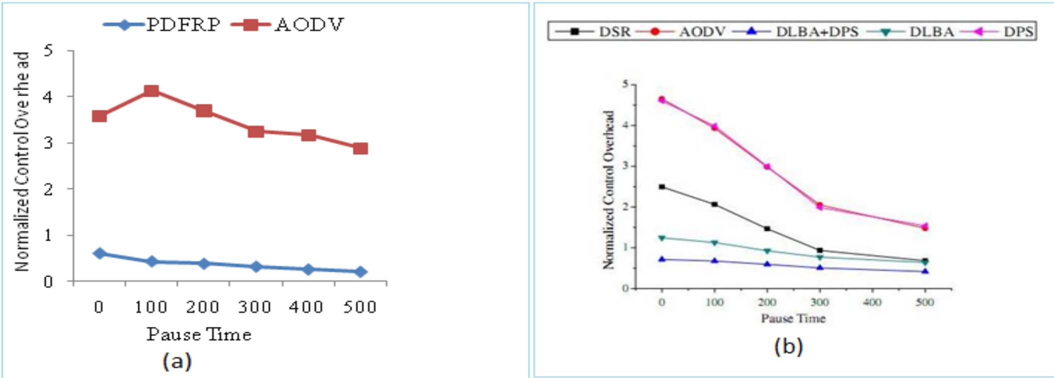


Figure 7.21: Normalized Routing Load vs. Pause Time of PDFRP Compared to DLBA

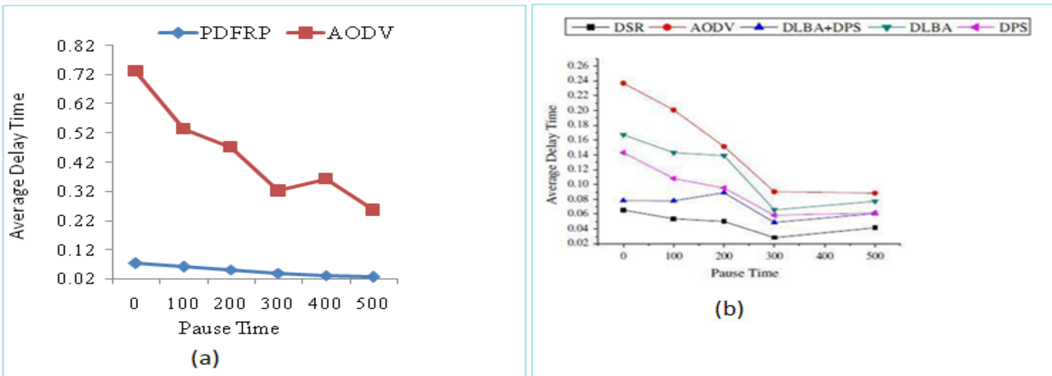


Figure 7.22: Average End-to-End Delay vs. Pause Time of PDFRP Compared to DLBA

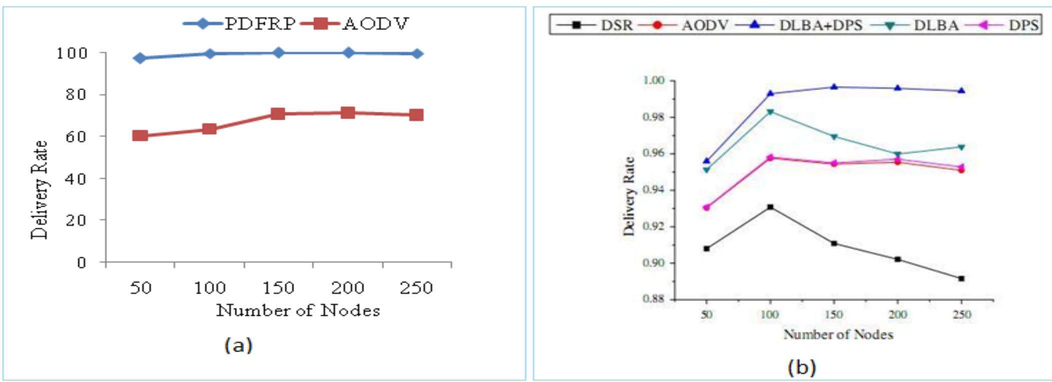


Figure 7.23: Packet Delivery Fraction vs. Node Density of DRP Compared to DLBA

7.6 Comparison for Model 2

7.6.1 Pre-emptive Zone Algorithm

This section presents the second comparison between PDFRP and Pre-emptive Zone Algorithm where it analysis specific metrics such as throughput against speed of the node as well as packet delivery time (total delay).

Link failure of Ad-hoc On-Demand Distance Vector (AODV) caused by node mobility is a common feature of wireless ad hoc networks. This leads to increased delay and routing overheads while route repair procedures are carried out. This research (Pre-emptive Zone Algorithm), proposes pre-emptive Zone and extends the definition of AODV with the ability to discover multiple routes to a host and switch between them, if an active route is becoming weak and if there is a risk that it will disappear (refer to pre-emptive mechanism). Ramesh and Subbaiah [160] proposed and developed Preemptive AOMDV Routing for Mobile Ad-Hoc Networks. They designed pre-emptive Zone model to predict the link break possibility. In practice, when the routing node considers that the link will be broken within a short period of time, the current node should find another way to the destination as soon as possible. As mentioned in Chapter Five, PDFRP has utilized link state prediction through a signal power which developed a checking algorithm which monitors the link status for current node. The difference between this mechanism (Pre-emptive Zone) and PDFRP mechanism is the PDFRP mechanism (1) verifies that if the current node could find out a node that has enough signal power and at the same time has a route to the desired destination, (2) if these two requirements are not fulfilled the operation will handover to Upstream Notification (UN) mechanism, while if this mechanism (Pre-emptive Zone) does not have such multiple options and if the current node does not succeed to find out a node with strong signal, the RERR message will propagate to the original source.

7.6.2 Concept of Pre-emptive Routing

Pre-emptive routing is to look for a new route that the node already could have, before the basic AODV protocol initiates a route discovery from source node. There are many reasons that a link can disappear, but both this work and DRFP will look into the case where mobility of nodes is the reason. In order to evaluate that a node is moving and a route is about to break, it relies on the fact that communication is based on electronic signals where it measures the quality of the signal. Figure 7.24 shows how it could look, in a network when a node (X) is moving away from another node and enters its pre-emptive zone. The concept of this Pre-emptive Zone is very simple compared to PDFRP concept in terms of conditions for alternative options to find a route in case there a sign that link failure will occur soon, in order to avoid various warning messages traveling in the network after a link completely fails. As in Algorithm 7.1 shows, that when the current node is moving and approaching the Pre-emptive Zone, RERR message propagates back to the source node to notify that the current route is going to break. Algorithm 7.1 indicates that the RERR message is reached at the source node and source node handles the issue where it checks whether there is an alternative route or not. It there is none, it initiates a new route discovery. This proves that PDFRP approach is more trustworthy in terms of protection of link failure as well as minimizing network flooding caused by reinitiating route rediscovery packets which consumes network resources unnecessarily.

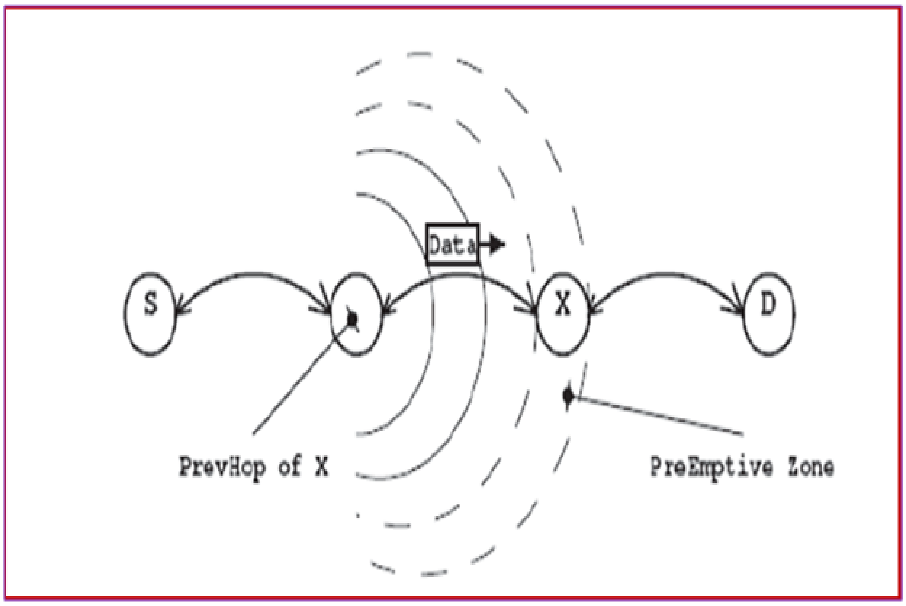


Figure 7.24: Preemptive Zone (Adapted from [160])

Algorithm 7.1 Algorithm for AOMDV with Preemptive Routing (Adapted from [161])

Algorithm 1

  Data : *IP packet*
  if *Receiving Node. isInPreemptiveZone* **then**
    send RERR to source of IP packet
  end

Algorithm 2

  if Recieve(RERR) **then**
    if Destination – this.NodeIP **then**
      if existRouteInMultioath **then**
        Change default route to destination:
     else
      Initiate a new route discovery to destination, while
      continuing using the waek link.
     end
    else
      send via next_hop to destination
   end
  end

7.6.3 Comparison of Pre-emptive Zone and PDFRP

This subsection presents evaluation performance of PDFRP and PRE-EMPTIVE ZONE. The main concern of this evaluation is to compare these two mechanisms in the line of the network reaction in terms of network topology changes caused by node mobility. A comparative analysis has been done to evaluate the tested metrics such as throughput and average end to end delay. These two metrics are vital to evaluate the network performance. For instance, throughput is the amount of data transferred over the period of time expressed in kilobits per second (Kbps) which represents the data packets received at the receiver site. Thus, the amount of data obtained at receiver site evaluates the protocol's performance with this regard. Delay is also an important metric and it is among the quantitative metrics that is used for evaluating the performance of a routing protocol to measure its efficiency for packet delivery time perspective.

Figure 7.25 illustrates Throughput Vs. Velocity. The result of throughput can be evaluated in the overall network performance as it tells how huge or small data amount is delivered. In this respect, it can also evaluate the number of packet drops. Figure 7.25 (b) illustrated the throughput result for Pre-emptive zone where it indicates that the throughput result is much lower compared to PDFRP throughput result. Figure 7.25 (b) also shows that the maximum throughput is approximately 100 kbps, which lowers the PDFRP throughput by more than 80%. Figure 7.25 (a) presents the PDFRP equivalent metric (Throughput) results where it indicates that the highest value obtained is more than 900 kbps whereas the lowest is approximately 800 kbps.

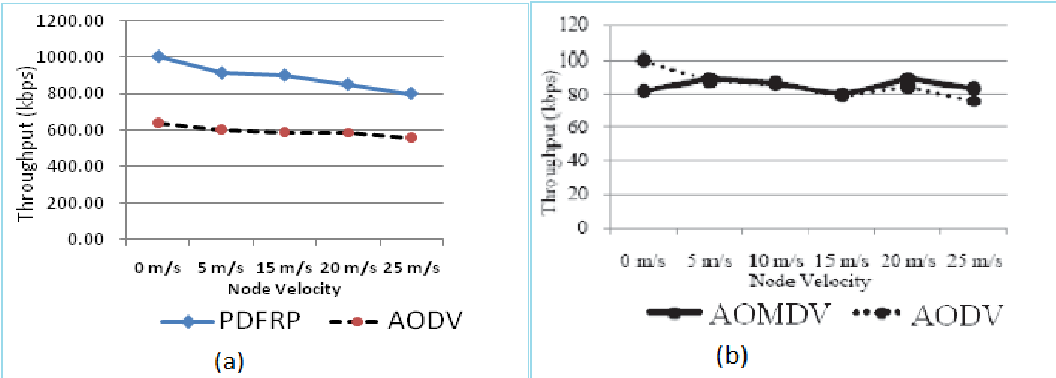


Figure 7.25: Throughput vs. Speed of PDFRP Compared to Pre-emptive Zone

Figure 7.26 shows the comparison between PDFRP and Pre-emptive Zone with respect to average delay vs. velocity. Figure 7.26 (b) presents the average delay vs. velocity for Pre-emptive Zone where its speed is varying as PDFRP's speed (0-25 m/s). In ad-hoc network, the speed effect is important as it is one of the main determining variable parameters of mobile ad-hoc network performance in terms of end to end delay. The node speed is lower as the network stability becomes more stable and produces better performance compared to high mobility network performance. As illustrated Figures 7.26 (b), the average delay for Pre-emptive Zone work indicates that the highest value for delay is approximately 0.19 s whereas the lowest value is approximately shows 0.12 s. Figure 7.26 (a), presents the average delay for PDFRP result where it shows that the highest value for delay is approximately 0.15 s and the lowest value is roughly 0.09 s which is much lower compare to pre-emptive Zone delays. However, the comparisons mentioned above indicate that the PDFRP presents better results compared to Pre-emptive Zone in terms of throughput vs. velocity as well as the average delay vs. velocity. Thus, these graphical comparisons indicate that the PDFRP protocol outperforms Pre-emptive Zone regarding the tested metrics.

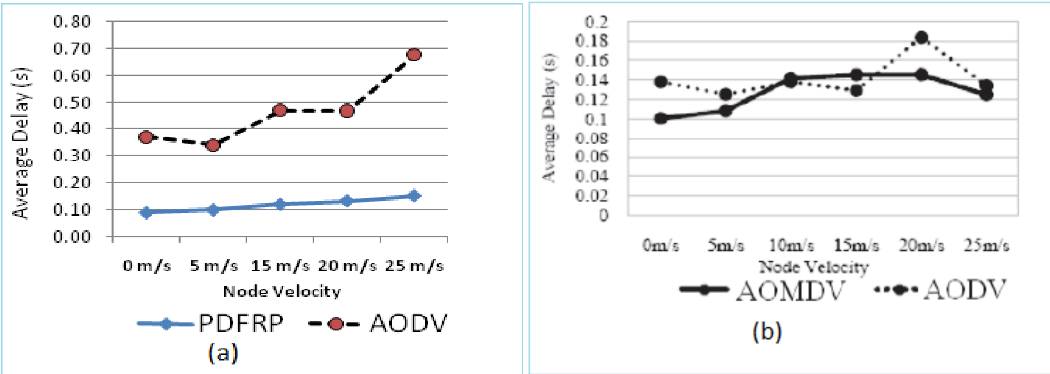


Figure 7.26: Average End-to-End Delay vs. Speed PDFRP Compared to Pre-emptive Zone

7.7 Comparison for Model 3

7.7.1 Link Stability Prediction-based Routing (LSPR) Algorithm

The third comparison discusses comparative analysis of developed protocol (PDFRP) and LSPR Algorithm with respect to packet delivery fraction and routing overhead.

One major concern for routing in mobile ad-hoc networks is how to select a stable path that can last longer since node mobility is a matter which may cause radio links to break consistently. In this work (LSPR algorithm), a link stability prediction model is proposed which uses the relative motion and the distance of nodes. In this respect, Hu et al. [161] proposed and developed a link stability prediction-based routing (LSPR) algorithm by modifying AODV routing protocol. They designed a model to predict the link stability which depends on the received signal strength of nodes. Furthermore, a forwarding rule which can reduce the number of RREQs forwarded by receding (in case a link failure happens) neighbor nodes is also designed. In LSPR algorithm, a RREQ forward delay is decided by the minimum mean link duration on the passed path which makes the destination node receive a more stable path.

7.7.2 Concept of LSPR Algorithm

As has been mentioned Chapter Five in Section 5.8, the calculation of the received signal strength always needs to get the distance and the relative motion between two neighbor nodes like A and O as indicated in Figure 7.27. However, it is complicated to evaluate the distance according to the received signal strength, in a real environment. In order to simplify it, they (LSRP) simulated with an ideal wireless transmission model which can be replaced by evaluation results with other more realistic wireless transmission model. As PDFRP was utilized, Two Ray Ground wireless transmission model was also utilized to evaluate the distance according to the received signal strength in their work as well. As the researcher (LSRP) defined **"definition 1 and definition 2"** in their paper, they assumed that there is a link L_{ao} between nodes *A* and *0* at current time *t*. Then the duration from current time *t* to the time that L_{ao} is disconnected is called the link duration of L_{ao}, denoted by D_{ao}. If both nodes of a link are mobile, such as nodes *A* and *0* of link L_{ao}, it can equivalently treat one of the nodes (node 0) as if it is kept at a fixed position, and the other node (node A) moves with the relative velocity v, and angle direction as shown in Figure 7.27.

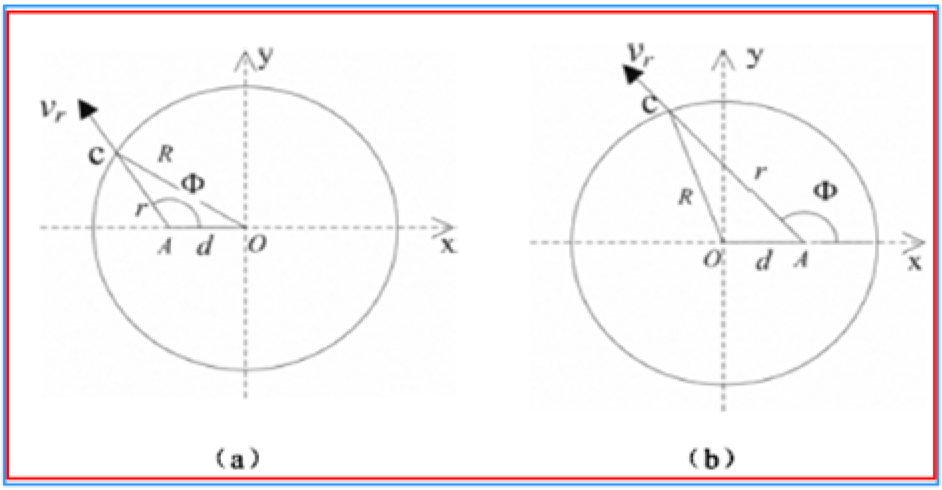


Figure 7.27: Two Categories of the Relative Motion Between Nodes A and O (a) Recede and (b) Approach adapted from [161]

7.7.3 Framework of LSPR Algorithm

Link failure caused by node mobility is a common feature with a reactive routing protocol such as AODV and overall mobile ad-hoc networks. This consequence increased delay and routing overheads while link failure is carried out. This can be avoided by extending the definition of AODV with pre-emptive/predictive mechanism to discover if an active route is becoming weak and there is a risk that it will disappear soon. The philosophy behind of pre-emptive routing is to look for a new route and divert the data into the new path at the intermediate node before the basic AODV protocol initiates a route discovery from the source after the current link disappears. A link can disappear for multiple reasons, but PDFRP and LSPR are both focusing into the case where mobility of nodes is the reason. However, LSPR algorithm and PDFRP algorithm both rely on the fact that the prediction is based on electronic received signals in order to be able to see that a node is moving and a route is about to break. This indicates that LSPR and PDFRP are intended to attack the same problem with a different approach and that is why the results obtained present different outcomes as shown in Figures 7.28 and 7.29. The main drawback of LSPR algorithm is the lack of ability to prevent unnecessary message which is normally sent by the intermediate node to the source when a link fails. In contrast, PDFRP developed Upstream Notification (UN) mechanism to prevent such a message.

7.7.4 Comparison of LSPR and PDFRP

Performance evaluation of PDFRP and LSPR is presented in this section. The main focus of this evaluation is to compare two algorithms used in the line of the network reaction when the topology changes. The rate of reaction can be measured by presenting a comparative analysis of the performance metrics of both algorithms (LSPR and PDFRP) such as packet delivery ratio and routing overhead. These two metrics are vital to evaluate the network performance. For example, lower packet delivery ratio is an indicator that shows the ratio of sent packets is much lower than the received packets at the destination. Furthermore, more routing overhead is indicative of how huge the network routing messages are through the channels. In other words, it evaluates the network efficiency where it takes into consideration how many routing messages are generated. Table 7.10 shows the parameters setting of LSRP and PDFRP.

Table 7.10: Parameters Setting for LSRP and PDFRP in this Regard

Parameters	**Value**
Transmitter Range	250 m
Mobility Model	Random waypoint mobility model
Simulation Time	500 s
Number of nodes	90
Scenario size	1000 x 1000 m2
Traffic type	Constant Bit Rate
Packet size	512 bytes
Pause Time	0,100,200,300, 400 and 500 (s)
Rate	5 packets/s

Figure 7.28 illustrates Packet delivery Fraction (PDF) Vs. Pause Time. PDF is a vital metric for overall network performance to measure the protocol's performance in the network. This performance may depend on other factors such as packet drop, network overload caused by routing overhead, as well as the effects of frequent topological changes. This metric also gives the protocol's effectiveness as well as its reliability. The result of PDF can evaluate the overall network performance as it tells how huge or small the number of packet drops, the network congestion, the throughput estimation and so on. The graph on the right side of Figure 7.28 (b) illustrates the packet delivery rate for LSPR result. Although LSRP performs well, the PDFRP results still show better perform once compared to SLRP. Figure 7.28 (a) presents the PDFRP result where it indicates that the value of PDF is maintained by achieving almost 100% packet delivery fraction. This ratio of PDFRP indicates that the number of data packets sent and the number of data packets received are nearly corresponding which is a sign that PDFRP outperforms LSPR.

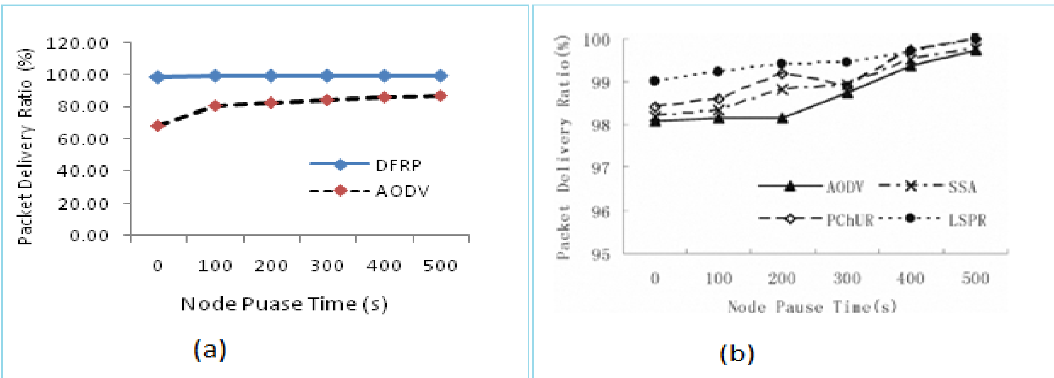


Figure 7.28: Packet Delivery Fraction vs. Pause Time of PDFRP Compared to LSPR

Figure 7.29 presents Routing Overhead Vs. Pause Time which it comprises the results of routing overhead for PDFRP and LSPR. This evaluation is important since it tells how huge signaling packets have been sent during the simulation time. Reduction of routing overhead is a sign which indicates how well the protocol performs. This includes bandwidth utilization management, battery power consumption as well as unnecessary route updating. Figure 7.29 (a) presents the experiment results for routing overhead of PDFRP. Figure7.29 shows that the overhead of PDFRP results has a low overhead compared to LSPR and one of the reasons is that (as has been mentioned in Chapter One), the main objective of this research is to enhance a link failure to develop a new extension to AODV in order to avoid entire link breakdown due to the node mobility as well as to prevent an unnecessary error warning messages traveling in the network. This is to avoid the high rate of routing overhead as it can avoid reinitiating route rediscovery by source. As in Figure 7.29, the maximum routing overhead of PDFRP is less than 52% where the LSPR presents more than 57%. However, the results show that the developed protocol outperforms LSPR.

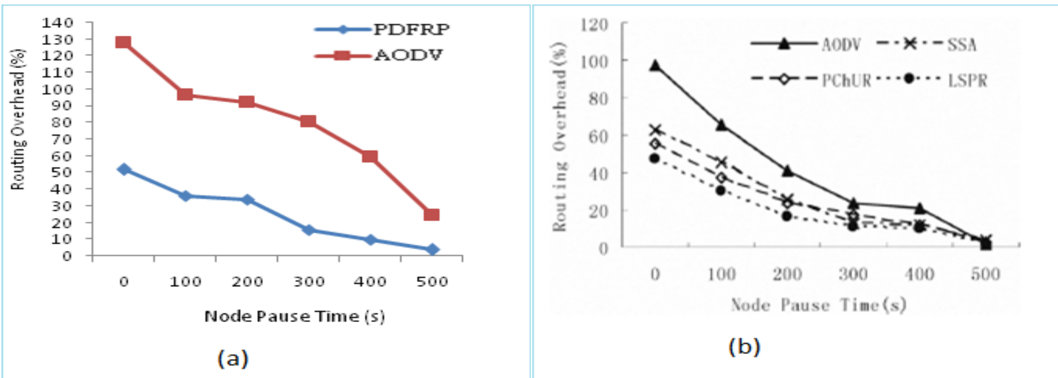


Figure 7.29: Routing Overhead vs. Pause Time of PDFRP Compared to LSPR

7.8 Comparison for Model 4

7.8.1 Enhanced Local Repair AODV (ELRAODV)

Singh et al. [162] proposed Enhanced Local Repair AODV (ELRAODV) for the original local repair strategy in AODV (LRAODV). This model is a very important model in terms of link failure improvement because it directly focuses on local repair upon link failure on an active path between a pair of nodes. But of course it has its own weaknesses for both link failure solving and preventing link failure itself and will be explained later on in this session. The current mechanism of AODV standard for local repair broadcasts RREQ upon link failure for repairing route and ELRAODV is proposed to improve this issue by using unicast approach for route repairing. The ELRAODV concept is based on an important assumption that major link failures are a singular failure as only one node is down on the route while the next node to the broken node in the route still carries route to the destination. This means that if one link is broken it normally happens between two nodes which are neighbors, but the next hop (one hop after this hop) to the destination is still alive. So this mechanism takes this opportunity to utilize the next hop which still exists and definitely it avoids unnecessary broadcasting of RREQ.

7.8.2 Fundamental of ELRAODV Concept

In AODV protocol route failure happens when a link breaks in the active route because of a node breaking down for whatever reason (battery down, switched off by user, out of coverage etc.). The concept of this mechanism is demonstrated in Figure 7.30 where it shows a few hops of an active route (shown as dark line). It shows that the route breaks when next hop to node-1 is down (shown in red in Figure 7.30). The underlying difference between the AODV standard and ELRAODV local repair strategy is that the standard one (earlier mechanism for local repairing) works like that. The node-1 (Figure 7.30) starts a local repair by broadcasting RREQ every time a node breaks while the ELARAODV takes advantage of fact that after the red node is down, node-2 still contains the route to the destination. The reason is node-1 can start repairing the same route to node-2 by finding an alternative to the broken node through neighbors of the node-1 instead of discarding the whole route. In this case, if node-1 is able to find an alternative neighbor node which has node-2 as its neighbor as well, then the link can be repaired by unicast a request (LRREQ) from node-1 to node-2 via alternative new hop (shown in green) without broadcasting any RREQ. One major drawback is that in case node-1 is not able to find any alternative neighbor for repairing route, ELRAODV must utilize the AODV standard local route repair which generates heavy traffic load.

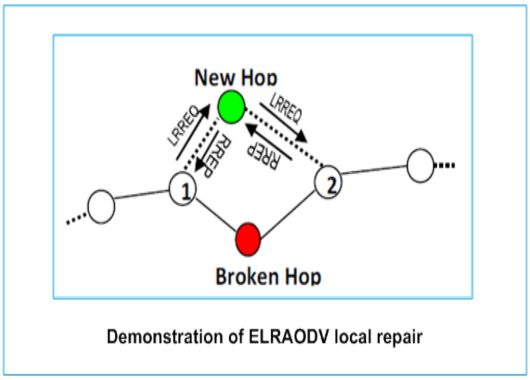


Figure 7.30: Demonstration of ELRAODV Local Repair (Adapted from [162])

7.8.3 ELRAODV and PDFRP Theoretical Framework

The main concept of ELRAODV and PDFRP is basically similar in terms of preventing unnecessary message after link failure. ELRAODV uses unicast approach for route repairing instead of broadcasting to prevent the number of warning messages traveling in the network upon link failure. PDFRP developed a number of models to repair the route at the same time to prevent this unnecessary message propagating all the way back to the source upon link failure on an active route. One of these models is Upstream Notification (UN) mechanism. As stated in Chapter Five the UN mechanism is designed to eliminate the traditional warning messages of AODV protocol upon link failure which conveys huge overhead to the network. Accordingly, both mechanisms (ELRAODV and PDFRP) are intended to attack the same problem, but in different ways and for that reason the results obtained are different, as shown Figures 7.31–7.33.

Nonetheless, the main drawback of ELRAODV mechanism is as in Figure 7.30 which shows that the route between node-1 and the red node is already broken down and must take some time until the node-1 finds a new path to divert the data. Packets are frequently arriving at node-1 from the source because there is no synchronization between node-1 and the source informing the source that the link is broken and it should stop sending until a new connection is established. So it is obvious, some packets are lost. Another major weakness in this mechanism is that if repairing the route is not successful, there is no alternative way to tackle the issue. So the only option is to propagate warning message to the source and source has to rebroadcast global route recovery.

7.8.4 Results Comparisons

This section compares the results to analyse and evaluate the performance of the two models (PDFRP and ELRAODV). This comparison is made to study how fast the models' mechanisms react to the different circumstance in network environments when the topology is going to change or already changed as in ELRAODV model (because ELRAODV mechanism as Figure 7.30 indicates that the link between node-1 and red node is already disconnected, which means the topology is already changed). The rate of reaction of the models can be measured by the results. For instance, long time propagation for packet delivery costs high end to end delay which is a sign that there are obstacles mid-way to the destination. In other words, lower packet delivery ratio indicates that the ratio of the number of packets sent is much lower than the number of those received at the destination. So, all these performance depend on how swift or slow the models' mechanism reacts to the network. Table 7.11 shows the parameters of ELRAODV as well as PDFRP in this situation.

Table 7.11: Shows the Parameters Setting of ELRAODV as Well as PDFRP in this Situation

Parameters	**Value**
Transmitter Range	250 m
Bandwidth	2Mbits/s
Simulation Time	100 s
Number of nodes	50
Scenario size	1000 x 1000 m2
Traffic type	Constant Bit Rate
Packet size	64 bytes
Flows	25
Rate	4 packets/s

Figure 7.31 illustrates average end to end delay vs. pause time where it compares PDFRP and ELRAODV performance in terms of packet time delivery. Figure 7.31 (b) shows the ELRAODV result where two legends appear, namely LRAODV and ELRAODV. The first (LRAODV) indicates the standard of ADOV local repair which is not this comparison is focusing on this legend. On the other hand, this comparison focuses on PDFRP and ELRAODV only.

Figure 7.31 (b) (ELRAODV) indicates that the result of average end to end delay is much higher compared to PDFRP result (a) in Figure 7.31. Furthermore, ELRAODV graph portrays that the ELRAODV result fluctuates up and down which indicates instability of the network whereas PDFRP results show more stability as Figure 7.31 (a) shows. These performances reflect the rate of reaction of the models' mechanism in terms of network topology's change up on link failure. In this case, PDFRP presents better results compared to ELRAODV in terms of delay average.

Figure 7.32 depicts average end to end delay vs. speed for both PDFRP and ELRAODV. This part of the analysis investigates the performance of models in terms of higher or lower nodes' speed. Such experiment is important for mobile ad-hoc environment because when the mobile node moves fast most likely network topology will change very fast which results in more link failure. According to Tie-yuan et al. [158], high speed of mobile ad-hoc network results frequently in link breakdowns. While on the other hand, lower node speed, will very likely cause the frequency of link failure to be also lower. Figure 7.32 (a) illustrates PDFRP result where it matches the above theoretical framework because as the graph indicates, as speed goes up the delay will increase which means that when the node in the network is running a higher speed, the network topology change frequently causing more link failures. This is a sign of validation and verification of the PDFRP protocol. However, the average end to end delay of ELRAODV is higher compared to PDFRP delay average which indicates that the PDFRP protocol outperforms ELRAODV on the subject of the tested metrics.

The final comparisons of these models are Packet Delivery Ration (PDR) metrics. PDR is very important in ad-hoc network or overall network environment wether wired or wireless. This metric tells not only the ration of packet delivery, but it also tells the packet drop, throughput as well as network congestion. This is because the lower ratio of packet delivery indicates the number of packet drop is higher and once the drop is higher the network congestion will be higher, meaning the amount that go through the pipe line (throughput) will be diminished.

Figure 7.33 (b) illustrates the packet delivery rate for ELRAODV result where it indicates that the highest value for packet delivery rate is approximately 80% whereas the lowest value is approximately shows 60%. Figure 7.33 (a) presents the PDFRP result where it indicates that the highest value obtained is 99.71% and lowest is 95.32%. In this respect, PDFRP protocol shows that packet delivery percentage achieved from a ratio of the number of data packets sent and the number of data packets received is not that much different, meaning PDFRP protocol reacts very fast for network topology change up on link failure. On the other hand, referring to the result obtained by ELRAODV, the gap of packet sent and packet received is relatively big. Nonetheless, the packet delivery ratio presented in Figure 7.33 shows that PDFRP protocol obviously outperformes ELRAODV.

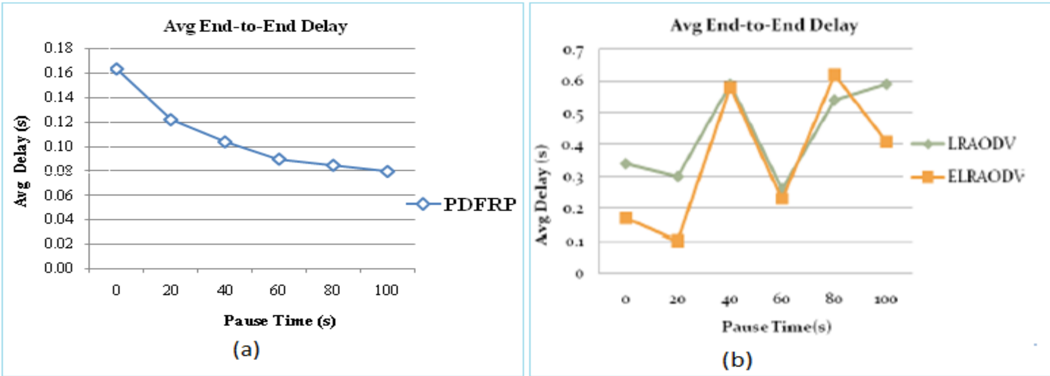


Figure 7.31: Average of End-to-End Delay vs. Pause of PDFRP Compared to ELRAODV

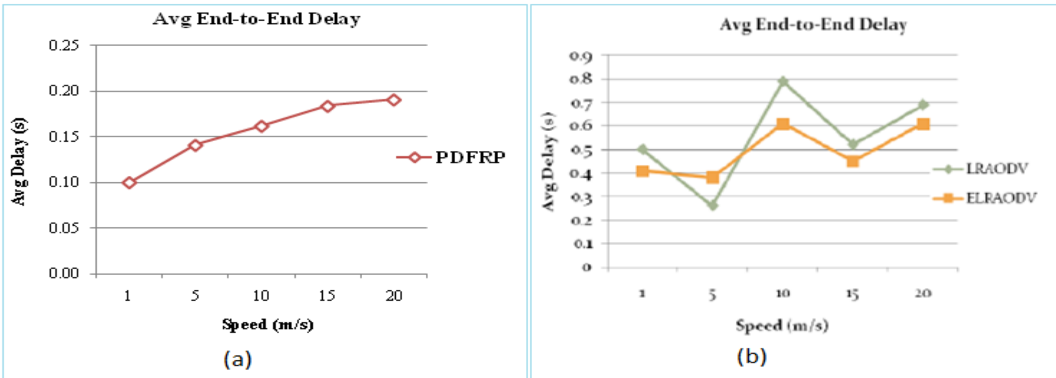


Figure 7.32: Average of End-to-End Delay vs. Speed of PDFRP Compared to ELRAODV

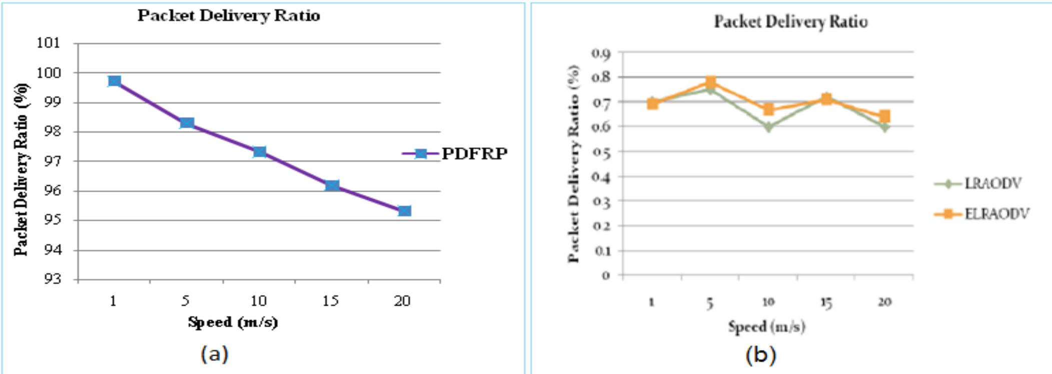


Figure 7.33: Packet Delivery Fraction vs. Speed of PDFRP Compared to ELRAODV

7.9 Summary and Observation

This chapter discusses and illustrates the detailed performance comparison of PDFRP algorithm to AODV standard algorithm based on the numerical results achieved from simulations. It analyzed and examined the effects of several parameters including speed, pause time and node density with respect to routing overhead, packet delivery ratio, normalized routing load, average end to end delay, packet drop and throughput as well. This chapter introduced the performance of PDFRP and AODV in terms of different mobility speeds as well as different pause time. The results show when the pause time is increased, the routing overhead for both protocols perform better. The experiment has shown that the PDFRP presented the lowest routing overhead in all cases compared to AODV standard. Furthermore, AODV standard suffers from more routing overhead and presents poor performance compared to PDFRP. Regarding the packet delivery fraction (PDF), the AODV standard obtained results that are less than 80% whereas the PDFRP obtained results for PDF which are all more than 98%. In addition, the results indicated that the number of packets delivered to destination increases when the pause time is more than 20 seconds, and the packet delivery ratio of both protocols reduces slightly when the pause time less than 20 seconds.

However, it has been shown that the packet delivery ratio for PDFRP is to a certain extent stable, and PDFRP performs much better than AODV standard with the improvement about 18%. The chapter illustrated also the normalized routing load with respect to the pause time where it presented the results of both protocols and compared their performances in terms of Normalized Routing Load concept. In addition, it also draws the average end to end delay, the packet drop performance, and throughput when pause time was varying with a range at 0-40 seconds.

Moreover, the chapter discussed and examined all above metrics while the speed instead of pause time was varying, such as the end to end delay, packet drop, routing overhead and throughput with varying node mobility. In addition, the chapter discussed and analyzed results while varying of nodes' density which analyzed routing overhead, packet delivery ratio, normalized routing load, average end to end delay and packet drop while increasing the number of nodes. Finally, the chapter discussed the performance comparison where the results of PDFRP are compared to different current related works.

CHAPTER EIGHT

CONCLUSION AND RECOMMENDATIONS

The previous chapter presented the performance analysis of the Predictive Divert Failure Routing Protocol (PDFRP) and numerical results obtained from simulations. This chapter provides a brief conclusion on the research. The chapter highlights the overall objectives and contributions of the research. In addition, how these contributions were achieved by the developed protocol is described. The chapter provides some recommendations for further research. Conclusion of the research where it details how Mobile Ad-hoc Network (MANET) performance depends on routing protocol's efficiency and how AODV routing protocol current mechanism deals with the link failure problem in MANETk is disussed Section 8.1. Section 8.2 presents overall objectives highlighting how these objectives were achieved by the developed protocol. The performance analysis and comparison are described in Section 8.3. The research contributions are explained in Section 8.4. Finally, the significance of the developed protocol and some suggestions for further studies are provided in Sections 8.5 and 8.6, respectively.

8.1 Conclusion

Development of ad-hoc network technology was enabled a new infrastructure-less communication and the ability for nodes to shape ad-hoc networks in the absence of infrastructure communication is a critical area of current research. There is a need of communication that ad-hoc network can meet, such as military, natural disasters as well as commercial applications. With that respect, the potential for low cost deployment and high availability, combined with the dropping costs of wireless transceivers, thus ad-hoc networks are becoming economically and technologically feasible right now. Routing protocols used in ad-hoc networks must automatically adjust to environments that can differ between the extremes of high mobility with low bandwidth, and low mobility with high bandwidth. The performance of ad-hoc network depends on how routing protocols deal with or manage the link failure problem.

AODV routing protocol works in a semi-dynamic manner, where it may establish a route on demand. The major weakness of the current AODV protocol is that the route will continue to use until it breaks. This respect, to adapt the changing network topology of high dynamic ad-hoc networks a more aggressive and adaptable routing strategy is required. This research developed Predictive Divert Failure Route Protocol (PDFRP). As a result, the PDFRP significantly improved the performance of the original AODV routing protocol and according to the simulation results, PDFRP can also adapt well in a very dynamic network environments. The new born PDFRP protocol is capable of maintaining higher link quality proactively and achieving higher data delivery rate with less average delays. On the other hand, it reduces a network overhead and packet's drop.

As mentioned in Chapter One in Section 1.4, the AODV limitation of link failure handling where an alternate path is required only when the primary route breaks. This motivates the need for developing a new link failure mechanism to improve the performance of the ad-hoc network as the current mechanism responds to link failure slowly, which results in large routing overhead, normalized routing load, less packet's delivery fraction and throughput as well. These consequences cause performance degradation due to high end to end delay with high packet loss as well. The goal of this research is to introduce a new routing protocol to modify and redesign an existing ad-hoc network reactive routing protocol namely ADOV into a hybrid protocol by introducing proactive behavior to improve its performance, where the PDFRP routing protocol is transformed into partially proactive routing protocol.

The route maintenance of the PDFRP protocol is based on a prediction algorithm which responds to link failure in a better predict compared to the existing link failure in AODV standard. Upstream Notification (UN) mechanism is a very useful algorithm developed by this research which is very unique mechanism among extended routing protocols' mechanisms for route maintenance to support communication between nodes upon suspicion of link failure in ad-hoc network which is one of the interesting aspects of our protocol scheme which significantly reduces the number of acknowledgment packets transmitted to source when link fails.

UN sends a notification message to upstream node timely to avoid current link disconnection. This happens in the case where the Current Node (C-N) does not succeed to divert the route due to none of the neighbors fulfilling the first requirement as mentioned in Chapter Five (Section 5.4). UN limits the number of link failure which reduces signaling packets overhead (more link failure, conveys more routing control messages per data packet delivered at the destination) and increases percentage of data packets being delivered to the destination.

It was observed and concluded that there is a limitation of AODV current mechanism in terms of handling link failure problems caused by dynamic natural mobile ad-hoc high mobility and frequent topological changes that have an impact on network's performance. For instance, AODV, suffers low packet delivery fraction and high routing overhead as well as low throughput, because of its poor route maintenance, being unable to handle the unresponsive connections, and having high number of consecutive drop, as explained in detail in Chapter Two. This has prompted us to develop the PDFRP that supports mobile ad-hoc network connections for next generation routing protocols to make the link connectivity more stable. According to Qin Kunz [163], who defines a link stability as the ability of a link to survive for a certain duration. The higher the link stability, the longer is the link duration. Throughout the design of PDFRP protocol (described in Chapter Five), it shows how the use of the link state prediction along with the Designed Models: Detection Model, New Path-Mode, Analyzer Algorithm and Upstream Notification Model can make the link live longer which leads to making the protocol more efficient. As stated in [164], routing efficiency can be determined by two aspects: first, the time needed to react on link failure and second, the ability to optimize to a shorter route when one is available. In that aspect, PDFRP protocol can provide better decision in terms of reaction time upon link failure compared to AODV standard.

8.2 Objectives of the Research

The objectives of this research were to investigate issues related to AODV current mechanism in terms of route maintenance and develop a new mechanism to mitigate the current AODV route maintaining shortcomings, especially its behavior to link failure.

Addressing Objective 1: First objective is empirical evaluation for the current algorithm of AODV protocol. To achieve this objective, pre-tested experiments of AODV protocol have been done. These empirical experiments aim to study the impact of the node mobility on MANET as well as to examine the behavior of two different mobility models, namely, Random Waypoint Model (RWP) and Reference Point Group Mobility Model (RPGM).

Addressing Objective 2: The second objective is to develop an extension to the Ad-hoc On-Demand Distance Vector (AODV) in link failure to address the current mechanism of the route maintenance problem of AODV standard. This objective is achieved by developed Predictive Divert Failure Route Protocol (PDFRP). As Chapter Five explained, the PDFRP encloses number of models such as *Detection Model*, *New Path-Model*, *Analyzer Algorithm* and *Upstream Notification Model (UN)*. In addition, as Chapter Six presented, link state prediction mechanism is also implemented. By using the link state prediction method, the link breakage time can be known before the link actually becomes broken. Therefore, the route will be updated in time, and the link is diverted into a new direction by *Forward Data Function* mechanism which is a sub-function of the *New Path-Mode*l. Furthermore, in case the first stage of the prediction fails, the UN Model mechanism takes place and proceeds with the link failure handling.

Addressing Objective 3: The third objective is related to implementing the developed protocol. To achieve this objective, the research implemented a very useful protocol to avoid a link failure in advance and construct a new direction locally (where the link failure takes place). It implemented three models: "*Detection Model*, *New Path-Mode* and *Upstream Notification Model*". In addition, an *Analyzer Algorithm* which interconnects the models is also developed. *Detection Model* utilizes the link state prediction method through the signal strength by using mathematical equations to estimate when two mobile nodes are about to disconnect. This objective also implemented another sub-model "*Computing Signal Strength Model*" which collaborates with *Dectection Model*. This model collects the signal and keeps it in a table by *Detection Model*. Whenever the link state prediction method needs to take action, the *Computing Signal Strength Model* picks up the signals from that table and measures the status of the signal power and this status will be used to determine the condition of the current connection, whether it will be broken soon or not.

Addressing Objective 4: The fourth objective is to evaluate and analysis the performance of the developed protocol through simulation experiments. This objective is achieved by results gained from the simulation experiments of the developed protocol and comparisons of PDFRP and related works as well.

8.3 Performance Analysis and Comparison

The experiments indicated that the PDFRP Protocol reduced routing overhead. Packets drop and average end to end delay, on the other hand, increased packet delivery fraction and throughput compared to AODV standard. In other words, the results indicate that when it deployed the new protocol (PDFRP), the routing message packets are minimized while the data packets' delivery are maximized, which indicates that the link failure per data packet transmission is reduced compared to the existing AODV standard mechanism for route maintenance.

8.4 Contributions

The important contributions of this research are presented in the following sub-sections.

8.4.1 Empirical Evaluation

Prior to implementing the developed protocol, an empirical evaluation of AODV algorithm was carried out. This experiment undertaken in order to reveal the limitation and strength of the current mechanism of AODV protocol as well as the importance of mobility models in MANET environments. This pre-test empirical evaluation is also important to disclose the optimal setting for AODV protocol with regards the sellected mobility models. Nonetheless, the empirical evaluation contribution is a potential for the research as it is a part of performance evaluation to investigate all necessary parameters which can affect the performance of routing protocol.

8.4.2 PDFRP Design Contribution

As mentioned in Chapter One, PDFRP was developed objectively to limit the link failure by designing a new protocol to the mobile ad-hoc network. The new developed protocol tries to prevent the number of warning messages traveling in the network to avoid the network flood caused by reinitiating route rediscovery up on link failure on an active link between two nodes. The developed protocol is combined with several sub-mechanisms which allow the protocol to identify the link status by checking arriving packet's signal level. One of the above mentioned mechanisms is the UN mechanism which is a part of the PDFRP protocol which uses in case the current node could not receive a positive response from its neighbor. For example, if not one of the neighbors of the current node (where the link failure is noticed) has a route to the desired destination and at the same time its signal level is below the predefined threshold value, then the UN is an alternative mechanism to overcome the traditional AODV drawback up on link failure where it (AODV) sends an unnecessary message back to the source. These combinations of mechanisms outperform the current AODV mechanism on link failure.

8.4.3 Models of PDFRP

To achieve the above objectives, the research developed three models and one analyzer algorithm, namely Detection Model, New Path-Mode, Upstream Notification Model and Analyzer algorithm. The Detection model uses (i) Detection Signal Function which detects the signal status and keeps it in a table, (ii) Computing Signal Strength, which computes the signal strength where it measures the signal power and determines the circumstance of the current connection. New Path-Mode uses three functions, namely (i) Find Strong Link Function, (ii) Create-New-Path Function, and (iii) Forward Data Function. The Find Strong Link function, based on the signal calculation by Computing Signal Strength, finds another node with a stronger signal power compared to the current connection's signal strength. The Create-New-Path Function's task depends on the response from a previous function. If the requirement is fulfilled it will create a new path (new link). Finally, the Forward Data Function forwards the data through the new path. Upstream Notification Model takes action if these two above models do not success. The Analyzer algorithm is an interconnector which interlinks the models and brings them together as they correlate with each other to unify the different functions of the models.

8.4.4 Implementation of Predictive Divert Failure Route Protocol (PDFRP)

PDFRP protocol has been implemented in Network Simulator 2 (ns-2). Simulations were performed to verify and validate the PDFRP protocol. For the results obtained from simulations, the PDFRP protocol outperformed AODV current mechanism. The experiment results have shown that the developed protocol maintenance can significantly reduce total number of dropped packets due to link breakage reduction.

8.4.5 Comparison of PDFRP to AODV and Current Work

The performance comparison of the developed protocol to AODV as well as related works have shown that PDFRP can be adjusted to achieve a higher network utilization, to effectively maximize the packet delivery fraction, minimize the signaling packet overhead, and to reduce the average end to end delay, at a lower ratio of packet loss while successfully avoiding buffer overflows by reduction of signaling overhead. The comparison study also revealed that PDFRP maximizes overall network's well-being compared to AODV standard, and achieved better throughput.

8.5 Significance of the Developed Protocol

The PDFRP protocol marks a significant step towards the enhancement of routing mechanism in ad-hoc network mobility technology. The PDFRP protocol is a reliable solution to a number of the current AODV mechanism's shortcomings. In fact, the PDFRP protocol could function as an alternative solution and indeed a readily and acceptable mechanism for the overall link failure enhancement of reactive routing protocols, especially in AODV standard mechanism. PDFRP protocol does not cause any notable side effects among tested metrics such as routing overhead, packet delivery fraction, normalized routing load, and average end to end delay, packets dropped, and throughput.

The PDFRP protocol contributes to the solving of a number of AODV outstanding limitations such as the huge number of routing messages that the current mechanism of AODV has transmitted in one successful data transaction. The overall goal for PDFRP is to propose a link failure avoidance mechanism which predicts the link status before it becomes completely disconnected and diverts it into a stable route. Moreover, the research has also come up with and developed another mechanism which eliminates sending of an unnecessary warning message upon link failure by an intermediate node back to the source, namely, Upstream Notification Model (UN). the UN mechanism is really an improvement of AODV standard protocol. In other words, the research has successfully brought a total solution through which the overall reactive routing protocols in the ad-hoc network could be improved. Nonetheless, based on experimental results, the research found that the PDFRP protocol does not cause any notable side effect on all metrics that have been tested.

8.6 Recommendation for Future Research

Mobile Ad-hoc Networks (MANETs), have received increasing research attention in recent years as a special type of network where there are many active research projects concerned with MANETs. This section discusses on future research directions based on PDFRP.

PDFRP protocol was developed and tested through ns-2 simulator environment. This suggests that the future research on PDFRP protocol be conducted in a real world environment to validate the simulation results. In addition, the protocol was tested with a reactive routing protocol environment, and thus one also suggests another environment such as proactive routing protocols is tested. PDFRP have been tested with reactive unicast protocol and have been enhanced with the link state prediction method where it achieved better performance compared to AODV as well as a number of current AODV extensions. It may also be interesting to extend the PDFRP protocol to consider protocols for multicast routing in MANETs.

Finally, it is possible to adapt the PDFRP protocol to enhance quality of service (QoS) for real time communications such as Voice over Internet Protocol (VoIP) which might limit the packet switching network routing overhead where it might save more bandwidth. However, since PDFRP protocol performs significantly towards the enhancement of routing protocol in ad-hoc network, it is also expected that it will perform well and successfully operate in a stable network as well.

REFERENCES

[1] S. Dhawan, "Analogy of Promising Wireless Technologies on Different Frequencies: Bluetooth, WiFi, and WiMAX," in *Proceedings of the The 2th International Conference on Wireless Broadband and Ultra Wideband Communications(AUSWIRELESS '07).* Washington, DC, USA: IEEE Computer Society, 2007.

[2] T. Lin, "Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications," Ph.D. dissertation, Computer Engineering, Blacksburg, Virginia, 2004.

[3] V. Timcenko, M. Stojanovic, and S. B. Rakas, "MANET Routing Protocols vs. Mobility Models: Performance Analysis and Comparison," in *Proceedings of the 9th WSEAS International Conference on Applied Informatics and Communications*, ser. AIC'09. Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS), 2009, pp. 271–276.

[4] Q. Li, C. Liu, and H. hong Jiang, "The Routing Protocol of Aodv Based on Link Failure Prediction," in *9th International Conference on Signal Processing (ICSP 2008)*, Oct. 2008, pp. 1993 –1996.

[5] G. Kioumourtzis, "Simulation and Evaluation of Routing Protocols For Mobile Ad-hoc Networks (MANETs)," Master's thesis, Naval Postgraduate School Monterey, California, Sep. 2005.

[6] R. Bin Rais, M. Mendonca, T. Turletti, and K. Obraczka, "Towards Truly Heterogeneous Internets: Bridging Infrastructure-based and Infrastructure-less Networks," in *2011 Third International Conference on Communication Systems and Networks (COMSNETS)*, Jan. 2011, pp. 1–10.

[7] K. Khan, M. Ahmed, A. Reddy, and R. Zaman, "A hybrid Architecture for Integrating Mobile Ad-hoc Network and the Internet Using Fixed and Mobile Gateways," in *1th IFIP Wireless Days, 2008 (WD '08)*, Nov. 2008, pp. 1–5.

[8] A. Pirzada, R. Wishart, and M. Portmann, "Multi-Linked AODV Routing Protocol for Wireless Mesh Networks," in *Global Telecommunications Conference, 2007(GLOBECOM '07. IEEE)*, Nov. 2007, pp. 4925–4930.

[9] S. Tang and B. Zhang, "A robust AODV Protocol with Local Update," in *The 2004 Joint Conference of the 10th Asia-Pacific Conference on Communications, 2004 and the 5th International Symposium on Multi-Dimensional Mobile Communications Proceedings*, vol. 1, 2004, pp. 418–422.

[10] N. Kulkarni, I. Gupta, and B. Raman, "On Demand Routing Protocols for Mobile Ad-hoc Networks: A Review," in *IEEE International Advance Computing Conference (IACC 2009)*, Mar. 2009, pp. 586 –591.

[11] A. Zahary and A. Ayesh, "Analytical Study to Detect Threshold Number of Efficient Routes in Multipath AODV Extensions," in *International Conference on Computer Engineering Systems, 2007, (ICCES '07)*, Nov. 2007, pp. 95–100.

[12] D. Kumar, A. Srivastava, and S. Gupta, "Performance Comparison of Pro-active and Reactive Routing Protocols for MANET," in *2012 International Conference on Computing, Communication and Applications (ICCCA)*, Feb. 2012, pp. 1–4.

[13] K. Suchdeo and D. K. Mishra, "Comparison of On-Demand Routing Protocols," in *2010 Fourth Asia International Conference on Mathematical/Analytical Modelling and Computer Simulation (AMS)*, May 2010, pp. 556–560.

[14] Online. [Online]. Available: http://www.atacwirelss.com/adhoc.html

[15] N. Surayati and M. Usop, "Performance Evaluation of AODV , DSDV and DSR Routing Protocol in Grid Environment," *Journal of Computer Science*, vol. 9, no. 7, pp. 261–268, 2009. [Online]. Available: http://paper.ijcsns.org/07_book/200907/20090737.pdf

[16] A. Boukerche, "A Simulation based Study of on-Demand Routing Protocols for Ad-hoc Wireless Networks," in *Simulation Symposium, 2001. Proceedings. 34th Annual*, 2001, pp. 85 –92.

[17] S. Jan, I. Shah, and H. Al-Raweshidy, "Performance Analysis of Proactive and Reactive Routing Protocols for Mobile Ad-hoc Grid in e-health Applications," in *International Conference on Communication Software and Networks, 2009. ICCSN '09*, Feb. 2009, pp. 484 –488.

[18] Z. Kai, W. Neng, and L. Ai-fang, "A new AODV based Clustering Routing Protocol," in *Proceedings 2005 International Conference on Wireless Communications, Networking and Mobile Computing*, vol. 2, 2005, pp. 728–731.

[19] R. Thakur, S. Sharma, and S. Sahu, "Accumulating Path Information in AODV for Ad-hoc Network," in *International Conference on Computational Intelligence and Communication Networks (CICN)*, Oct. 2011, pp. 89–94.

[20] A. Zahary and A. Ayesh, "On-Demand Multiple Route Maintenance in AODV Extensions (ORMAD)," in *International Conference on Computer Engineering Systems (ICCES 2008)*, Nov. 2008, pp. 225–230.

[21] M. Frikha and F. Ghandour, "Implementation and Performance Evaluation of an Energy Constraint Routing Protocol for Mobile Ad-hoc Networks," in *Telecommunications, 2007. AICT 2007. The Third Advanced International Conference on*, May 2007, pp. 13–17.

[22] X. Zhong, S. Mei, Y. Wang, and J. Wang, "Stable Enhancement for AODV Routing Protocol," in *14^{th} IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, PIMRC 2003*, vol. 1, 2003, pp. 201–205.

[23] J.-Z. Sun, "Mobile Ad-hoc Networking: an Essential Technology for Pervasive Computing," in *Proceedings 2001 International Conferences on Info-tech and Info-net, 2001 (ICII 2001 - Beijing)*, vol. 3, 2001, pp. 316–321.

[24] H. Bakht, "Wireless Infrastructure, Some Applications of Mobile Ad-hoc Networks," *Computing Unplugged Magazine*. [Online]. Available: http://www.computingunplugged.com/issues/issue200409/00001371001.html

[25] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-hoc Networks," *Journal of Ad-hoc Networks*, vol. 2, pp. 1 – 22, Jan. 2004.

[26] C. E. Perkins and P. Bhagwa, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers," in *in Proceeding of International Conference on Communications Architectures, ACM*, IBM, T.J. Watson Research Center, Hawthorne, NY 10562 & Computer Science Department, University of Maryland, College Park, MD 20742, 1994, pp. 234 – 244.

[27] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol for Ad-hoc Networks," in *Proceedings IEEE International Multi Topic Conference Technology for the 21th Century (2001 IEEE INMIC 2001)*, 2001, pp. 62 – 68.

[28] I. D. Aron and S. K. S. Gupta, "A Witness-Aided Routing Protocol for Mobile Ad-hoc Networks with Unidirectional Links," in *Proceedings of the First International Conference on Mobile Data Access*. London, UK.: Springer-Verlag, 1999, pp. 24 – 33. [Online]. Available: http://dl.acm.org/citation.cfm?id=648052.746196

[29] V. Park, J. Macker, and M. Corson, "Applicability of the Temporally-ordered Routing Algorithm for Use in Mobile Tactical Networks," in *Proceedings Military Communications Conference (MILCOM 98) IEEE*, vol. 2, Oct. 1998, pp. 426 –430.

[30] E. Royer and C. Perkins, "An Implementation Study of the AODV Routing Protocol," in *Wireless Communications and Networking Confernce (WCNC.2000) IEEE*, vol. 3, 2000, pp. 1003–1008.

[31] M. Tamilarasi, V. Shyam Sunder, U. Haputhanthri, C. Somathilaka, N. Babu, S. Chandramathi, and T. Palanivelu, "Scalability Improved DSR Protocol for MANETs," in *International Conference on Conference on Computational Intelligence and Multimedia Applications, 2007*, vol. 4, Dec. 2007, pp. 283–287.

[32] M. E. Royer and C. K. Toh, "A Review of Current Routing Protocols for Ad-hoc Mobile Wireless Networks," *IEEE Personal Communication*, vol. 6, no. 2, pp. 46–55, Apr. 1999. [Online]. Available: http://www.citeulike.org/user/admash/article/108493

[33] P. Kakkar and V. Singla, "Traffic Pattern based performance comparison of Reactive and Proactive protocols of Mobile Ad-hoc Networks," *International Journal of Computer Applications*, vol. 5, no. 10, pp. 16–20, Aug. 2010, published By Foundation of Computer Science.

[34] W. Lin-zhu, F. Ya-qin, and S. Min, "Performance Comparison of Two Routing Protocols for Ad Hoc Networks," in *International Conference on Information Engineering, 2009 (ICIE '09. WASE)*, vol. 1, Jul. 2009, pp. 260–262.

[35] C. Putta, K. Prasad, D. Ravilla, R. Nath, and M. Chandra, "Performance of Ad-hoc Network Routing Protocols in IEEE 802.11," in *2010 International Conference on Computer and Communication Technology (ICCCT)*, 2010, pp. 371–376.

[36] A. K. B. R. R, L. C. Reddy, and P. S. Hiremath, "Performance Comparison of Wireless Mobile Ad-hoc Network Routing Protocols," *European Journal of Scientific Research,IEEE*, vol. 8, no. 6, pp. 337–343, 2008. [Online]. Available: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1492924

[37] Y. Q. Fan, L. Z. Wang, and L. Zhou, "The Comparison and Simulation of Ad-hoc Network Routing Protocol Based on NS2," *Journal of Networks*, vol. 5, pp. 435– 442, Apr. 2010.

[38] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," in *in Proceedings of Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '97)*, vol. 3, Apr. 1997, pp. 1405 –1413. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=631180

[39] D. B. Johnson, D. Maltz, and H. Y.-C., "The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks (DSR)," http://tools.ietf.org/html/draft-ietf-manet-dsr-09, Apr. 2003, online Available.

[40] E. Perkins, E. M. B. Royer, and R. D. Samir, "Ad-hoc On-Demand Distance Vector Routing Protocol," IETF MANET Working Group, 2003, ETF MANET Working Group, 2003, online Available. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-13.txt.

[41] S. K. Gupta and R. K. Saket, "Performance Metric Comparison of AODV and DSDV Routing Protocols in MANETs Using ns-2," *International Journal of Research and Reviews in Applied Sciences (IJRRAS)*, vol. 7, no. 3, pp. 339 –350, Jun. 2011.

[42] S.-J. Lee, E. M. Belding-Royer, and C. E. Perkins, "Scalability Study of the Ad-hoc on-Demand Distance vector Routing Protocol," *International Journal of Network Management*, vol. 13, no. 2, pp. 97–114, Mar. 2003. [Online]. Available: http://dx.doi.org/10.1002/nem.463

[43] P. Manoyut and W. Suntiamorntut, "Modified Local Repair in AODV for LoWPANs," in *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication*, ser. ICUIMC '12. New York, NY, USA: ACM, 2012, pp. 1–14. [Online]. Available: http://doi.acm.org/10.1145/2184751.2184769

[44] A. Goel and A. Sharma, "Performance Analysis of Mobile Ad-hoc Network Using AODV Protocol," *International Journal of Computer Science and Security (IJCSS)*, vol. 3, no. 5, pp. 334 –343, Nov. 2009.

[45] P. Nand, S. Sharma, and R. Astya, "Simulation Based Parametric Analysis of AODV Protocol for Ad-hoc Network," *Published in International Journal of Advanced Engineering and Applications*, pp. 10 –14, Jan. 2010.

[46] E. D. Kaplan and C. Hegarty, *Understanding the GPS: Principles and Applications (Artech House Mobile Communications)*, second edition ed., C. Hegarty, Ed. Amazon, Nov. 2005. [Online]. Available: http://www.navtechgps.com/downloads/1024.pdf

[47] A. Jardosh, E. Belding-Royer, K. Almeroth, and S. Suri, "Real-World Environment Models for Mobile Network Evaluation," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 3, pp. 622 – 632, Mar. 2005.

[48] B. S. Manoj and C. S. R. Murthy, "On the Use of Out-of-Band Signaling in Ad-hoc Wireless Networks," *Computer Communications*, vol. 26, no. 12, pp. 1405–1414, 2003. [Online]. Available: http://dblp.uni-trier.de/db/journals/comcom/comcom26.html#ManojM03

[49] F. Klemm, Z. Ye, S. V. Krishnamurthy, and S. K. Tripathi, "Improving TCP Performance in Ad-hoc Networks Using Signal Strength based link Management," *Ad Hoc Netw.*, vol. 3, no. 2, pp. 175–191, Mar. 2005. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2004.07.005

[50] R.-S. Chang and S.-J. Leu, "Long-lived Path Routing with Received Signal Strength for Ad-hoc Networks," in *2006 1th International Symposium on Wireless Pervasive Computing*, Jan. 2006, p. 6.

[51] M. Heissenbuttel, T. Braun, M. Walchli, and T. Bernoulli, "Evaluating the Limitations of and Alternatives in Beaconing," *Journal of Ad-hoc Networks.*, vol. 5, no. 5, pp. 558–578, Jul. 2007. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2006.03.002

[52] H. Kaaniche and F. Kamoun, "Mobility Prediction in Wireless Ad-hoc Networks using Neural Networks," *Journal of Telecommunications (JOT)*, vol. 2, no. 1, pp. 95 –101, Apr. 2010.

[53] S.-J. Lee, W. Su, and M. Gerla, "Wireless Ad-hoc Multicast Routing with Mobility Prediction," *Mobile Networks and Applications*, vol. 6, no. 4,

pp. 351–360, Aug. 2001. [Online]. Available: http://dx.doi.org/10.1023/A:1011478628358

[54] A. Boukerche and L. Zhang, "A preemptive on-Demand Distance Vector Routing Protocol for Mobile and Wireless Ad-hoc Networks," in *36th Annual Simulation Symposium, 2003*. IEEE Computer Society, Apr. 2003, pp. 73 – 80.

[55] X. Xiong, U. T. Nguyen, and H. L. Nguyen, "Preemptive Multicast Routing in Mobile Ad-hoc Networks," in *Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, Apr. 2006, p. 68.

[56] P. Srinath, P. Abhilash, and I. Sridhar, "Router Handoff: A Preemptive Route Repair Strategy for AODV," in *Proceeding of International Communication Personal Wireless Conference (ICPWC'2002 IEEE)*, Bombay, India, Dec. 2002, pp. 168–171.

[57] T. Goff, N. Abu-Ghazaleh, D. Phatak, and R. Kahvecioglu, "Preemptive Routing in Ad-hoc Networks," *Journal of Parallel and Distributed Computing*, vol. 63, no. 2, pp. 123–140, Feb. 2003. [Online]. Available: http://dx.doi.org/10.1016/S0743-7315(02)00059-X

[58] P. Veeraraghavan and S. Singh, "An Efficient Pre-emptive Local Route Repair for AODV," in *Proceedings of International Conference on Network and Communication Systems (NCS 05)*, Krabi, Thailand, Apr. 2005, pp. 381–385.

[59] H. Soliman and M. AlOtaibi, "An Efficient Routing Approach over Mobile Wireless Ad-hoc Sensor Networks," in *Proceedings of the 6thIEEE Consumer Communications and Networking Conference (CCNC 2009)*, Jan. 2009, pp. 1 –5.

[60] S. B. Hacene, A. Lehireche, and A. Meddahi, "Predictive Preemptive Ad-hoc on-Demand Distance Vector Routing," *Malaysian Journal of Computer Science*, vol. 19, pp. 189–195, 2006.

[61] B. S. Kang and K. Young, "Effective Route Maintenance and Restoration Schemes in Mobile Ad-hoc Networks," *Journal Sensors (Switzerland)*, vol. 10, pp. 808 – 821, Jan. 2010.

[62] D. Espes and Z. Mammeri, "Adaptive Expanding Search Methods to Improve AODV Protocol," in *Proceedings of 16th IST on Mobile and Wireless Communications Summit (IEEE 2007)*, Jul. 2007, pp. 1–5.

[63] H. Asenov and V. Hnatyshin, "GPS-Enhanced AODV Routing," in *in Proceedings of the International Conference on Wireless Networks (ICWN'09)*, Las Vegas, USA, Jul. 2009, pp. 1–8.

[64] E. Amar and S. Boumerdassi, "A scalable Mobility-adaptive Location Service with Kalman-based Prediction," in *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, Mar. 2011, pp. 593 –598.

[65] M. K. Singh and B. Kumar, "Preemptive Multipath Ad-hoc on Demand Distance Vector Routing Protocol," *MIT International Journal of Computer Science and Information Technology*, vol. 1, no. 1, pp. 36 – 40, Jan. 2011.

[66] E. van den Berg, A. Cisneros, I. Hokelek, K. Parmeswaran, S. Samtani, J. Sucec, J. Simbol, A. Staikos, and G. Rucker, "Improving Link Failover Efficiency in MANETs using Modular Prediction," in *Sarn off Symposium, 2010 IEEE*, New Jersey, USA, Apr. 2010, pp. 1–6.

[67] Z. Zhao, B. Willman, S. Weber, and J. de Oliveira, "Performance Analysis of a Parallel link Network with Preemption," in *2006 40th Annual Conference on Information Sciences and Systems*, Mar. 2006, pp. 271–276.

[68] M. Chawla, J. Singhai, and J. L. Rana, "Local Repair with Handoff Approach for on Demand Routing Protocols in Ad-hoc Networks," *International Journal of Computer Science and Communication (IJCSC)*, vol. 1, no. 2, pp. 33 –40, Jul. 2010.

[69] N. Al-Sharabi, Y. P. Lin, and W. Rajeh, "Avoid Link Breakage in On-Demand Ad-hoc Network Using Packet's Received Time Prediction," in *Proceeding of 19th European Conference on Modeling and Simulation*, Jun. 2005, pp. 802–807.

[70] W. Su, S.-J. Lee, and M. Gerla, "Mobility Prediction and Routing in Ad-hoc Wireless Networks," *In International Journal of Network Management*, vol. 11, no. 1, pp. 3–30, Jan. 2001. [Online]. Available: http://dx.doi.org/10.1002/nem.386

[71] W. K. Lai, S.-Y. Hsiao, and Y.-C. Lin, "Adaptive Backup Routing for Ad-hoc Networks," *Journal of Computer Communications*, vol. 30, no. 2, pp. 453–464, Jan. 2007. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2006.09.011

[72] S. Crisostomo, S. Sargento, P. Brandao, and R. Prior, "Improving AODV with Preemptive Local Route Repair," in *International Workshop on Wireless Ad-hoc Networks (2004 IEEE)*, Jun. 2004, pp. 223–227.

[73] A. Boukerche and L. Zhang, "A Performance Evaluation of a Rre-emptive on-Demand Distance Vector Routing Protocol for Mobile Ad-hoc Networks," *Wireless Communications and Mobile Computing*, vol. 4, no. 1, pp. 99–108, 2004.

[74] W. Zhu, X. Zhang, Y. Liu, and N. Li, "Improve Preemptive Routing Performance in Mobile Ad-hoc Networks with Cache-enabled Method," in

Third International Conference on Communications and Networking in China, (ChinaCom 2008), Aug. 2008, pp. 732–736.

[75] R. Bai and M. Singhal, "DOA: DSR over AODV Routing for Mobile Ad-hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 10, pp. 1403 –1416, Oct. 2006.

[76] H.-L. Chen and C.-H. Lee, "Two Hops Backup Routing Protocol in Mobile Ad-hoc Networks," in *Proceedings of 11^{th} International Conference on Parallel and Distributed Systems (IEEE-2005)*, vol. 2, Jul. 2005, pp. 600–604.

[77] C.-T. Kuo and C.-K. Liang, "A Meshed Multipath Routing Protocol in Mobile Ad-hoc Networks," in *Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (2006. PDCAT '06)*, Dec. 2006, pp. 306 –310.

[78] S.-J. Lee and M. Gerla, "AODV-BR: Backup Routing in Ad-hoc Networks," in *Wireless Communications and Networking Confernce (WCNC. 2000 IEEE)*, vol. 3, 2000, pp. 1311–1316.

[79] J. Jeon, K. Lee, and C. Kim, "Fast Route Recovery Scheme for Mobile Ad -Hoc Networks," in *2011 International Conference on Information Networking (ICOIN)*, Jan. 2011, pp. 419–423.

[80] J. Feng and H. Zhou, "A Self-Repair Algorithm for Ad-hoc On-Demand Distance Vector Routing," in *International Conference on Wireless Communications, Networking and Mobile Computing, 2006 (WiCOM 2006)*, 2006, pp. 1–4.

[81] M. Zapata, "Shortcut Detection and Route Repair in Ad-hoc Networks," in *Third IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom 2005 Workshops*, Mar. 2005, pp. 237–242.

[82] M. Spohn and J. J. Garcia-Luna-Aceves, "Neighborhood Aware Source Routing," in *Proceedings of the 2^{th} ACM International Symposium on Mobile Ad-hoc Networking and Computing*, ser. MobiHoc '01. New York, NY, USA: ACM, 2001, pp. 11–21. [Online]. Available: http://doi.acm.org/10.1145/501417.501419

[83] J. Thriveni, V. Alekhya, N. Deepa, B. Uma, A. Alice, G. Prakash, K. Venugopal, and L. Patnaik, "QoS Preemptive Routing with Bandwidth Estimation for Improved Performance in Ad-hoc Networks," in *4^{th} International Conference on Information and Automation for Sustainability, 2008. ICIAFS 2008*, Dec. 2008, pp. 443–448.

[84] 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, Jul. 2007.

[85] N. Javaid, A. Bibi, A. Javaid, and S. Malik, "Modeling Routing Overhead Generated by Wireless Reactive Routing Protocols," in *2011 17th Asia-Pacific Conference on Communications (APCC)*, Oct. 2011, pp. 631–636.

[86] J. Hemmes, M. Fisher, and K. Hopkinson, "Predictive Routing in Mobile Ad-Hoc Networks," in *2011 5th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST)*, 2011, pp. 117–122.

[87] S. Wang, Q. Song, J. Feng, and X. Wang, "Predicting the Link Stability based on Link Connectivity Changes in Mobile Ad-hoc Networks," in *IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010*, Jun. 2010, pp. 409–414.

[88] P. Singh and D. Lobiyal, "DSR with Link Prediction using Pareto Distribution," in *2010 International Conference on Networking and Information Technology (ICNIT)*, Jun. 2010, pp. 29 –33.

[89] P. Prabhakaran and R. Sankar, "Impact of Realistic Mobility Models on Wireless Networks Performance," in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2006. (WiMob'2006)*, Jun. 2006, pp. 329 –334.

[90] J. Yoon, M. Liu, and B. Noble, "Random Waypoint Considered Harmful," in *Proceeding of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies (INFOCOM 2003)*, vol. 2, Apr. 2003, pp. 1312–1321.

[91] R. de Moraes, F. de Araú andjo, and A. Pontes, "A Proposal to Stabilize the Random Waypoint Mobility Model for Ad-hoc Network Simulation," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, Apr. 2010, pp. 1 –6.

[92] X. Hong, M. Gerla, G. Pei, and C.-C. Chiang, "A Group Mobility Model for Ad-hoc Wireless Networks," in *Proceedings of the 2th ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems*, ser. MSWiM '99. New York, NY, USA: ACM, 1999, pp. 53–60. [Online]. Available: http://doi.acm.org/10.1145/313237.313248

[93] F. Bai, N. Sadagopan, and A. Helmy, "IMPORTANT: a Framework to Systematically Analyze the Impact of Mobility on Performance of Routing Protocols for Ad-hoc Networks," in *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications IEEE Societies (INFOCOM 2003)*, vol. 2, Apr. 2003, pp. 825 – 835.

[94] B. Zhou, K. Xu, and M. Gerla, "Group and Swarm Mobility Models for Ad-hoc Network Scenarios Using virtual Tracks," in *Military Communications Conference, (MILCOM 2004 IEEE)*, vol. 1, Nov. 2004, pp. 289–294.

[95] B. Divecha, A. Abraham, C. Grosan, and S. Sanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility Models," in *First Asia International Conference on Modelling Simulation, 2007 (AMS '07)*, Mar. 2007, pp. 224 –229.

[96] M. Singh, S.-G. Lee, D. Singh, and H. J. Lee, "Impact and Performance of Mobility Models in Wireless Ad-hoc Networks," in *Fourth International Conference on Computer Sciences and Convergence Information Technology, (2009. ICCIT '09)*, Nov. 2009, pp. 139–143.

[97] G. Jayakumar and G. Gopinath, "Performance Comparison of Two On-demand Routing Protocols for Ad-hoc Networks based on Random Waypoint Mobility Model," *American Journal of Applied Sciences*, vol. 5, no. 6, pp. 659 – 664, 2008. [Online]. Available: http://thescipub.com/abstract/10.3844/ajassp.2008.659.664

[98] N. Cooper and N. Meghanathan, "Impact of Mobility Models on Multi-Path Routing in Mobile Ad-hoc Networks," *International Journal Of Computer Networks and Communications (IJCNC)*, vol. 2, pp. 185 –194, Jan. 2010.

[99] M. Izuan and M. Saad, "Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol," *European Journal of Scientific Research*, vol. 32, no. 4, pp. 444–454, 2009. [Online]. Available: http://www.eurojournals.com/ejsr_32_4_01.pdf

[100] L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, P. Huang, S. McCanne, K. Varadhan, Y. Xu, and H. Yu, "Advances in Network Simulation," *Computer*, vol. 33, no. 5, pp. 59 –67, May 2000.

[101] B. Liang and Z. Haas, "Predictive Distance-based Mobility Management for Pcs Networks," in *Proceedings IEEE Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '99)*, vol. 3, Mar. 1999, pp. 1377–1384.

[102] M. Hassan and R. Jain, *High Performance TCP/IP Networking: Concepts, Issues, and Solutions*. Pearson Prentice Hall, 2004.

[103] S. Abdule, S. M.and Hassan, O. Ghazali, and M. M. Kadhum, "Pause Time Optimal Setting for AODV Protocol on RPGM Mobility Model in MANETs," *International Journal of Advanced Computer Science and Applications*, vol. 1, no. 6, pp. 1–7, Dec. 2010.

[104] S. Abdule, S. M.and Hassan and M. M. Kadhum, "An Improvement of Link Failure Maintenance in Ad-hoc Wireless Network on AODV Protocol," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 8, pp. 182–188, Aug. 2010.

[105] E. Johnson and J. Ha, "PDATS Lossless Address Trace Compression For Reducing File Size And Access Time," in *1994. IEEE 13th Annual International Phoenix Conference on Computers and Communications*, Apr. 1994, p. 213.

[106] L. Blessing, "DRM: A Design Research Methodology," Konstruktionstechnik Und Entwicklungsmethodik, Fakultät V-Verkehrs- und Maschinensysteme Technische Universität Berlin, Berlin, Tech. Rep., Jun. 2004.

[107] L. T. Blessing and A. Chakrabarti, "DRM, A Design Research Methodology," *Springer*, Jun. 2009.

[108] J. Ariyakhajorn, P. Wannawilai, and C. Sathitwiriyawong, "A Comparative Study of Random Waypoint and Gauss-Markov Mobility Models in the Performance Evaluation of MANET," in *International Symposium on Communications and Information Technologies (ISCIT '06)*, 2006, pp. 894 –899.

[109] S. Das, C. Perkins, and E. Royer, "Performance Comparison of Two on-Demand Routing Protocols for Ad-hoc Networks," in *in Proceedings IEEE Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM 2000)*, vol. 1, 2000, p. 3 –12.

[110] N. Aschenbruc, "BonnMotion Mobility Generator."

[111] P. Bakalis and B. Lawal, "Performance Evaluation of CBR and TCP Traffic Models on MANET Using DSR Routing Protocol," in *IEEE 2010 International Conference on Communications and Mobile Computing (CMC)*, vol. 3, Apr. 2010, pp. 318–322.

[112] A. Varga, "The OMNeT++ Discrete Event Simulation System," in *In the Proceedings of the European Simulation Multiconference, (ESM'2001)*, Prague, Czech Republic, Jun. 2001.

[113] J. Cai and B. Jia, "Network Simulation Based on OPNTE and Application," in *First International Workshop on Education Technology and Computer Science, 2009 (ETCS '09)*, vol. 1, Mar. 2009, pp. 199 –202.

[114] P. Meeneghan and D. Delaney, "An Introduction to NS, Nam and OTcl Scripting," http://www.cs.nuim.ie/research/reports/2004/nuim-cs-tr-2004-05.pdf. [Online]. Available: http://www.cs.nuim.ie/research/reports/2004/nuim-cs-tr-2004-05.pdf

[115] L. Presage Technologies, *CentOS Desktop*, 2008.

[116] J. Wang, "Ns-2 Tutorial (1)," Multimedia Networking Group,The Department of Computer Science, Tech. Rep., 2004. [Online]. Available: http://www.cs.virginia.edu/~cs757/slidespdf/cs757-ns2-tutorial1.pdf

[117] G. L. Pore, “A Performance Analysis of Routing Protocols for Ad-hoc Networks,” Master’s thesis, Master Thesis, Naval Postgraduate School Monterey, CALIFORNIA, Mar. 2006.

[118] C. Bettstetter, G. Resta, and P. Santi, “The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad-hoc Networks,” *IEEE Transactions on Mobile Computing*, vol. 2, no. 3, pp. 257 – 269, 2003.

[119] Y. Huan, J. Hong, and L. Lei, “Performance Analysis of Mobility Models in Sparse Ad-Hoc Networks,” in *Control Conference, 2008. CCC 2008, 27th Chinese*, Jul. 2008, pp. 216 –220.

[120] Y. Zhang and W. Li, “An Integrated Environment for Testing Mobile Ad-hoc Networks,” in *Proceedings of the 3th ACM International Symposium on Mobile Ad-hoc Networking and Computing*, ser. MobiHoc ’02. New York, NY, USA: ACM, 2002, pp. 104 –111. [Online]. Available: http://doi.acm.org/10.1145/513800.513813

[121] C. Waal and M. Gerharz, “Bonnmotion: A Mobility Scenario Generation and Analysis Tool,” Communication Systems Group, Institute of Computer Science IV, University of Bonn, 2003.

[122] A. Pal, J. Singh, P. Dutta, P. Basu, and D. Basu, “A Study on the Effect of Traffic Patterns on Routing Protocols in Ad-hoc Network Following RPGM Mobility Model,” in *2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN)*, Jul. 2011, pp. 233 –237.

[123] S. Das, R. Castaneda, J. Yan, and R. Sengupta, “Comparative Performance Evaluation of Routing Protocols for Mobile, Ad-hoc Networks,” in *Proceedings the 7th International Conference on Computer Communications and Networks(1998)*, Oct. 1998, pp. 153–161.

[124] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, “A Performance Comparison of Multi-hop Wireless Ad-hoc Retwork Routing Protocols,” in *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, ser. MobiCom ’98. New York, NY, USA: ACM, 1998, pp. 85–97. [Online]. Available: http://doi.acm.org/10.1145/288235.288256

[125] L. Qin, “Proactive Route Maintenance in DSR,” M. Sc Thesis, Ottawa-Carleton Institute of Computer Science, Canada, Aug. 2001.

[126] S. Azzuhri, M. Portmann, and W. L. Tan, “Evaluation of Parameterised Route Repair in AODV,” in *4th International Conference on Signal Processing and Communication Systems (ICSPCS)*, Dec. 2010, pp. 1–7.

[127] N. Pereira and R. de Moraes, "A Comparative Analysis of Aodv Route Recovery Mechanisms in Wireless Ad-hoc Networks," in *IEEE Latin-American Conference on Communications, 2009 (LATINCOM '09)*, 2009, pp. 1 –6.

[128] D. Arora, E. Millman, and S. Neville, "Assessing the Performance of AODV, DYMO, and OLSR Routing Protocols in the Context of Larger-scale Denser MANETs," in *2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, Aug. 2011, pp. 675–679.

[129] M. Pan, S.-Y. Chuang, and S.-D. Wang, "Local Repair Mechanisms for on-Demand Routing in Mobile Ad-hoc Networks," in *Proceedings 11th Pacific Rim International Symposium on Dependable Computing 2005*, Dec. 2005, p. 8.

[130] S. M. Abdule and S. Hassan, "Divert Failure Route Protocol Based on AODV," in *Proceedings of the 2010 Second International Conference on Network Applications, Protocols and Services*, ser. NETAPPS '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 67–71. [Online]. Available: http://dx.doi.org/10.1109/NETAPPS.2010.19

[131] Pythagoras, "Pythagoras' Theorem," http://www.ibmaths.com/free/stnotes/trig.pdf.

[132] R. Ghanbarzadeh and M. Meybodi, "Reducing Message Overhead of AODV Routing Protocol in Urban Area by Using Link Availability Prediction," in *Computer Research and Development, 2010 Second International Conference on*, May 2010, pp. 274 –279.

[133] C. Chunling, H. Jingbo, and Z. Dengyin, "An Expanding Ring Prediction and Location Aided AODV Routing Algorithm," in *2011 International Conference on Information Technology, Computer Engineering and Management Sciences (ICM)*, vol. 2, 2011, pp. 61–64.

[134] T. S. Rappaport, *Wireless Communications Principles and Practice*. Prentice Hall, 2002.

[135] T. Henderson, "The VINT Project," Available: http://www.isi.edu/nsnam/ns/doc/index.html, A Collaboratoin Between Researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC., Tech. Rep., 2011, kevin Fall and Kannan Varadhan (Editors). [Online]. Available: Available:http://www.isi.edu/nsnam/ns/doc/index.html

[136] J. Eriksson, M. Faloutsos, and S. V. Krishnamurthy, "DART: Dynamic Address RouTing for Scalable Ad-hoc and Mesh Networks," *IEEE/ACM Transactions on Networking*, vol. 15, no. 1, pp. 119 –132, Feb. 2007.

[137] F. Martinez, C.-K. Toh, J.-C. Cano, C. Calafate, and P. Manzoni, "Realistic Radio Propagation Models (RPMs) for VANET Simulations," in *Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE*, 2009, pp. 1–6.

[138] B. Qi and F. Shen, "Propagation Models for Multi-hop Wireless Networks in Ns-2 Simulator," in *Eighth International Conference on Information Technology: New Generations (ITNG)*, Apr. 2011, pp. 701–706.

[139] C. Hossain, M. Hossain, and M. Tarique, "Effects of Shadowing on the Performances of Mobile Ad-hoc Networks," in *2011 International Conference on Computational Intelligence and Communication Networks (CICN)*, Oct. 2011, pp. 319 –322.

[140] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris, "Link-level Measurements from an 802.11b Mesh Network," *In SIGCOMM*, pp. 121–132, 2004. [Online]. Available: http://citeseer.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.5380

[141] D. Kotz, C. Newport, and C. Elliott, "The Mistaken Axioms of Wireless Network Research," Technical Report TR2003-467, Tech. Rep., 2003.

[142] M. Takai, J. Martin, and R. Bagrodia, "Effects of Wireless Physical Layer Modeling in Mobile Ad-hoc Networks," in *Proceedings of the 2^th ACM International Symposium on Mobile Ad-hoc Networking and Computing*, ser. MobiHoc '01. New York, NY, USA: ACM, 2001, pp. 87–94. [Online]. Available: http://doi.acm.org/10.1145/501426.501429

[143] W. Xiuchao and A. Ananda, "Link Characteristics Estimation for IEEE 802.11 DCF based WLAN," in *29^th Annual IEEE International Conference on Local Computer Networks, 2004*, Nov. 2004, pp. 302–309.

[144] R. Sargent, "Validation and Verification of Simulation Models," in *Simulation Conference Proceedings, 1999 Winter*, vol. 1, 1999, pp. 39–48.

[145] F. de Renesse and A. Aghvami, "Formal Verification of Ad-hoc Routing Protocols using SPIN Model Checker," in *Proceedings of the 12^th IEEE Mediterranean Electrotechnical Conference, 2004 (MELECON 2004)*, vol. 3, May 2004, pp. 1177–1182.

[146] C. Bettstetter, "On the Minimum Node Degree and Connectivity of a Wireless Multihop Network," in *Proceedings of the 3^th ACM International Symposium on Mobile Ad-hoc Networking and Computing*, ser. MobiHoc '02. New York, NY, USA: ACM, 2002, pp. 80–91. [Online]. Available: http://doi.acm.org/10.1145/513800.513811

[147] R. Hekmat, *Ad-hoc Networks: Fundamental Properties and Network Topologies*. Springer, 2006.

[148] K. Manousakis, K. Young, C. Graff, and M. Patel, "On the Design of Power and Delay Aware k-Connected Topologies," in *The 2010 Military Communications Conference - Unclassified Program - Networking Protocols and Performance Track*, USA, 2010, pp. 1403–1408.

[149] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad-hoc Network Research," *Wireless Communications and Mobile Computing (WCMC): Special Issue on Mobile Ad-hoc Networking: Research, Trends And Applications*, vol. 2, pp. 483–502, 2002.

[150] K. Bhargavan, D. Obradovic, and C. A. Gunter, "Formal Verification of Standards for Distance Vector Routing Protocols," *The Journal of the Association for Computing Machinery (ACM)*, vol. 49, no. 4, pp. 538–576, Jul. 2002. [Online]. Available: http://doi.acm.org/10.1145/581771.581775

[151] I. Zakiuddin, M. Goldsmith, P. Whittaker, and P. Gardiner, *A Methodology for Model-Checking Ad-hoc Networks*, ser. SPIN'03. Berlin, Heidelberg: Springer-Verlag, 2003. [Online]. Available: http://dl.acm.org/citation.cfm?id=1767111.1767123

[152] O. Wibling, J. Parrow, and A. Pears, "Ad-hoc Routing Protocol Verification through Broadcast Abstraction," in *in Proceeding of 25th International Federation for Information (IFIP)*, Taiwan, 2005, pp. 128 –142.

[153] D. Camara, A. Loureiro, and F. Filali, "Methodology for Formal Verification of Routing Protocols for Ad-hoc Wireless Networks," in *Global Telecommunications Conference,IEEE (2007. GLOBECOM '07)*, Nov. 2007, pp. 705–709.

[154] E. M. Clarke, "Model Checking — My 27-Year Quest to Overcome the State Explosion Problem," in *Proceedings of the 15th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning*, ser. LPAR '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 182–182. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-89439-1_13

[155] L. M. Kristensen and K. Jensen, "Specification and Validation of an Edge Router Discovery Protocol for Mobile Ad-hoc Networks," *Springer-Verlag*, pp. 248–269, 2004.

[156] Z. Chang, G. Gaydadjiev, and S. Vassiliadis, "Routing Protocols for Mobile Ad-hoc Networks: Current Development and Evaluations," in *16th Annual Workshop on Circuits, Systems and Signal Processing, ProRisc 2005*, Nov. 2005, pp. 489–494. [Online]. Available: http://ce.et.tudelft.nl/publicationfiles/1104_536_chang_TUD_IST_Summit_2005.pdf

[157] V. Kumar, "Simulation and Comparison of AODV and DSR Routing Protocols in MANETs," M. Sc Thesis, Dept. of Computer Science and Engineering, Thapar University, 2009.

[158] L. Tie-yuan, C. Liang, and G. Tian-long, "Analyzing the Impact of Entity Mobility Models on the Performance of Routing Protocols in the MANET," in *3th International Conference on Genetic and Evolutionary Computing, 2009, (WGEC '09)*, Oct. 2009, pp. 56–59.

[159] R.-H. Cheng, T.-K. Wu, and C. W. Yu, "A Highly Topology Adaptable Ad-hoc Routing Protocol with Complementary Preemptive Link Breaking Avoidance and Path Shortening Mechanisms," *Wireless Networks*, vol. 16, no. 5, pp. 1289 –1311, Jul. 2010. [Online]. Available: http://dx.doi.org/10.1007/s11276-009-0203-0

[160] V. Ramesh and P. Subbaiah, "Preemptive AOMDV Routing for Mobile Ad-hoc Networks," in *International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2011)*, Jul. 2011, pp. 622–625.

[161] X. Hu, J. Wang, and C. Wang, "Link Stability Prediction and its Application to Routing in Mobile Ad-hoc Networks," in *2th International Conference on Power Electronics and Intelligent Transportation System (PEITS), 2009*, vol. 1, Dec. 2009, pp. 141–144.

[162] J. Singh, P. Singh, and S. Rani, "Enhanced Local Repair AODV (ELRAODV)," in *International Conference on Advances in Computing, Control, Telecommunication Technologies, (2009. ACT '09)*, Dec. 2009, pp. 787–791.

[163] L. Qin and T. Kunz, "Increasing Packet Delivery Ratio in DSR by Link Prediction," in *Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003*, Jan. 2003, p. 10.

[164] E. Nordström, P. Gunningberg, and C. Rohner, "A Comprehensive Comparison of MANET Routing Protocols in Simulation, Emulation and the Real World," in *Uppsala University*. Sweden: Osker Wibling, May 2006, pp. 1–12.

Appendix A

CREATING CBR TRAFFIC AND MOVEMENT PATTERN SCENARIO FILES

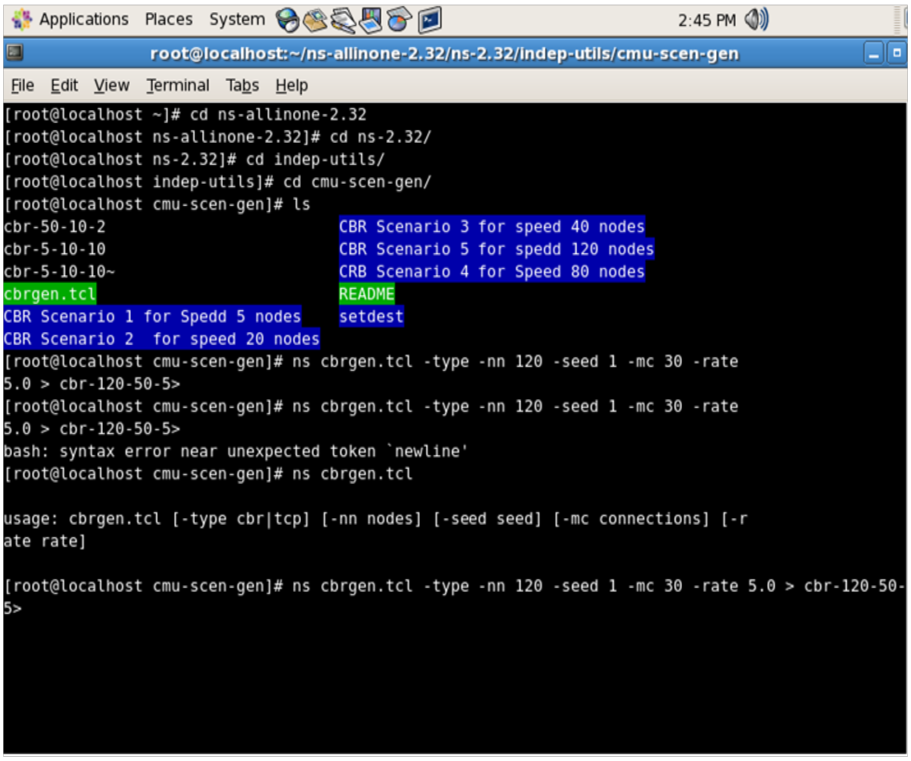
Before running TCL code in ns2 simulator, it has to be generated the traffic and scenario patterns using either ns-2 or any other traffic generator tools. In this research, it has been used ns-2 and BonnMotion as a traffic and mobility generator. It can be used only ns-2 to generate both traffic pattern and scenario pattern utilizing "~ns\indep-utils\cmu-scen-gen: ns cbrgen. tcl and /setdest in ns-2 tool. In this scenario can be used if the mobility model that utilizes in the simulation is only Random Waypoint Mobility Model. As it has been mentioned earlier, this research has been also tested RPGM model therefore utilized another additional tool such as BonnMotion. How to generate both traffic pattern and scenario pattern by ns-2 and BonnMotion tools is as flows:

Creating CBR Traffic Pattern Scenario Files Using ns-2 Tool, under the Below Directories

i. Go directories: ns-allinone-2.32/ns-2.32/indep-utils/cmu-scen-gen,

ii. Run: ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections] [-rate packet/second for one connection]>[output-file].

Next snapshot is an example for traffic generating by Random Waypoint Mobility Model in ns-2 were generated for 120 nodes with CBR traffic sources, with maximum connections of 30 at a rate of 20 kbps, App-A-Figure 1 shows one example of screenshot for CBR traffic.



App-A-Figure 1

The Flowing is the Command CBR Traffic for Above Screenshot

nodes: 120, max conn: 30, send rate: 0.5, seed: 1

1 connecting to 2 at time 2.5568388786897245

set udp_(0) [new Agent/UDP]

$ns_ attach-agent $node_(1) $udp_(0)

set null_(0) [new Agent/Null] $ns_ attach-agent $node_(2) $null_(0)

set cbr_(0) [new Application/Traffic/CBR] $cbr_(0)

set packetSize_ 512 $cbr_(0) set interval_ 0.5 $cbr_(0)

set random_ 1 $cbr_(0)

set maxpkts_ 10000 $cbr_(0) attach-agent $udp_(0)

$ns_ connect $udp_(0) $null_(0)

$ns_ at 2.5568388786897245 "$cbr_(0) start"

4 connecting to 5 at time 56.333118917575632

set udp_(1) [new Agent/UDP] $ns_ attach-agent

$cbr_(1) attach-agent $udp_(1)

$ns_ connect $udp_(1) $null_(1)

$ns_ at 56.333118917575632 "$cbr_(1) start"

4 connecting to 6 at time 146.96568928983328

#Total sources/connections: 20/30

Packet Delivery Fraction

PDR % Pause Time: 0 10 20 30 40

DFRP-Pstime:0-40 with 5n : 98.70 99.25 98.24 99.60 99.99

DFRP-Pstime:0-40 with 20n : 98.76 99.28 99.33 99.68 99.90

DFRP-Pstime:0-40 with 40n : 98.82 99.30 99.38 99.70 99.00

DFRP-Pstime:0-40 with 80n : 98.80 99.37 99.42 99.78 99.97

DFRP-Pstime:0-40 with 120n :99.57 99.71 99.78 99.86 99.98

AODV-Pstime:0-40 with 5n : 57.27 58.13 62.16 62.74 65.44

AODV-Pstime:0-40 with 20n : 61.19 68.04 69.95 72.05 74.13

AODV-Pstime:0-40 with 40n : 66.94 69.87 71.70 74.67 79.77

AODV-Pstime:0-40 with 80n : 67.61 70.68 72.65 76.10 80.94

AODV-Pstime:0-40 with 120n : 68.17 80.32 77.00 77.89 78.53

Appendix B

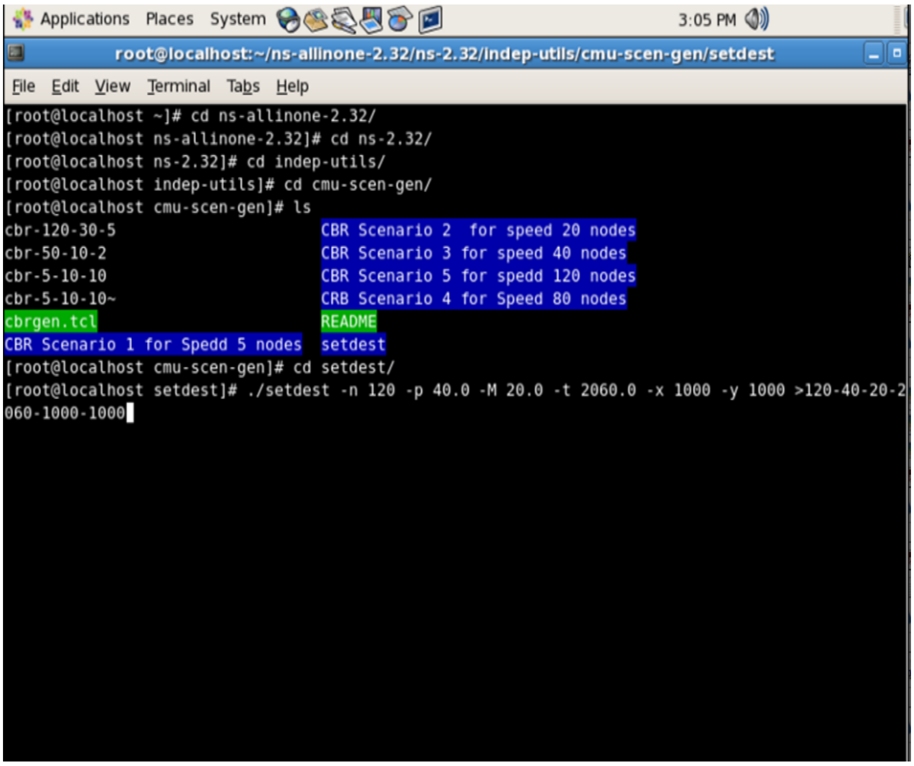
Creating Node Mobility Movement Scenario Files Using ns-2 Tool

i. ns-allinone-2.32/ns-2.32/indep-utils/cmu-scen-gen/setdest,

ii. run: ./setdest [-n num_of_nodes] [-p pausetime] [-s maxspeed] [-t simtime] [-x maxx] [-y maxy] > [output-file].

This is another example for creating node movement scenario files for the simulation using 120 nodes, with pause time of 40 seconds, maximum speed of 20m/s, topology boundary of 1000x1000 and simulation time of 2060 secs as in App-B-Figure 1 presented.

This is an example for mobility movement scenario that is created for the simulations as shown the below screenshot.



App-B-Figure 1

The Flowing is a Part of the Movement Scenario traffic Command for Above Screenshot

nodes: 10, speed type: 1, min speed: 15.00, max speed: 30.00

avg speed: 8.14, pause type: 1, pause: 40.00, max x: 1000.00, max y: 1000.00

$node_(0) set X_ 708.378426577596

$node_(0) set Y_ 616.223586763839

set Y_ 292.418053798134 $node_(2)

set Z_ 0.000000000000 $node_(3)

set X_ 595.631696025700 $node_(3)

set Y_ 3.414293683640 $node_(3)

set Z_ 0.000000000000 $node_(4)

et Z_ 0.000000000000

$ns at 36.874856680504 "$node_(5) setdest 37.457577835577 748.298657509992 0.000000000000"

$ns at 40.000000000000 "$node_(1) setdest 729.671082871870 833.336985282156 18.935853180861"

$ns at 40.000000000000 "$node_(6) setdest 449.104474720948 92.056609026104 20.804497054158"

Destination Unreachables: 196

Route Changes: 417

Link Changes: 101

#**Node**:0|1|2|3|4|5|6|7|8|9

| **Route Changes:**105|87|101|101|85|47|69|63|76|100

| **Link Changes:**22|23|21|25|17|9|13|24|23

Appendix C

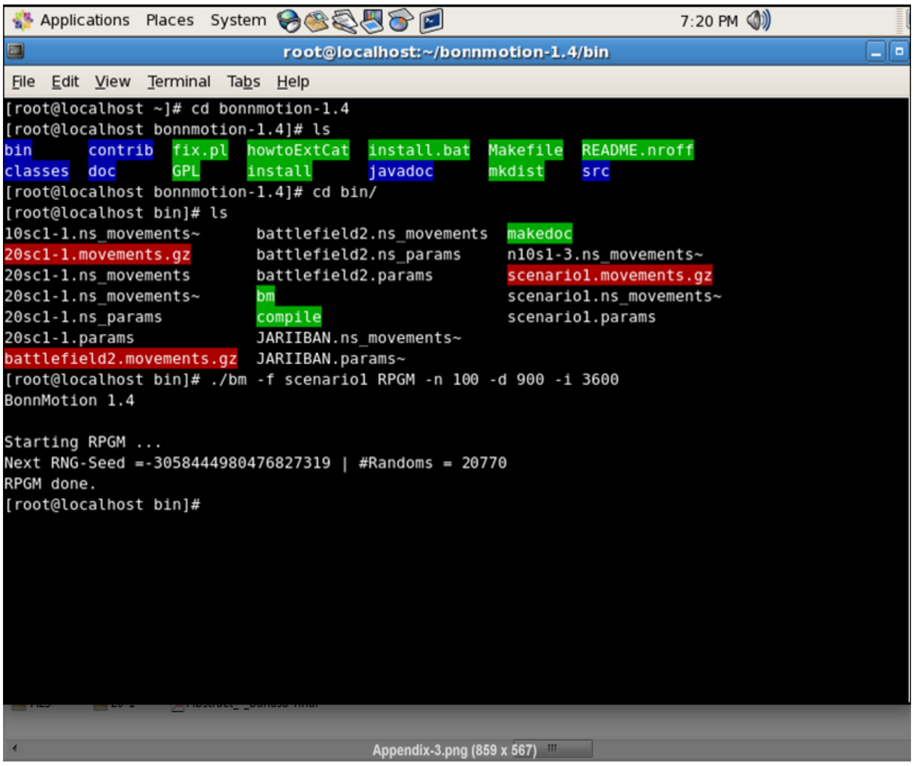
Bonnmotion Tool

As mentioned earlier, to test any other mobility model than Random Waypoint Model, needs separate traffic generator rather than **"setdest and cbrgen.tcl "** which built in ns-2 Tool. In this research, BONNMOTION TOOL was used in order to test RPGM Model where utilized Linux (Centos 5.3) as a platform. Flowing command was used in order to create node mobility movement scenario files for BONNMOTION TOOL: **"./bm -f scenario1 RPGM -n 100 -d 900 -i 3600".** This command will create a RPGM scenario file with 100 nodes, with duration of 900 seconds and initial phase cutoff of 3600 seconds. This command will produce 2 files: "scenario1.params": which has complete set of parameters used for the simulation and the second file is "scenario1.movements.gz", which is a compressed file containing the movement data. These two files cannot be directly used in ns-2, an application called "NSFILE" is provided with BonnMotion package which is used to transform these files so that they can be integrated to TCL in ns-2. It opens the dos prompt again, and navigates to the bin directory location of Bonnmotion and types the following command **"bm nsfile -f scenario1"** This command will generate two files:

i. Scenario1.ns_params containing the parameters for running simulations in ns-2

ii. Scenario1.ns_movements which contains the movements data essential for ns-2

App-C-Figure 1 shows the screenshot for BonnMotion tool which can be seen more practically and details about command and scenarios.



App-C-Figure 1

The Prediction Algorithm Implemented in PDFRP

In ns-2 .**{h, cc}; wireless-phy.cc:** In wirless-phy.cc, in this class normally receives and sends packets, so that when a node receives a unicast packet, and it is the next hop of the packet, it then it adds (previous hop address, receive time, signal power strength) to the nodes relevant table in order to help nods predict the link breakage time. In node, **{h, cc}**, the link breakage is predicted where the math equation is implemented to calculate the link breakage time.

```
#ifdef PREDICTION

double breakTime = 2000.0;

if (ch->num_forwards() != 0 && ch->next_hop_ == index){

Node *currentNode = Node::get_node_by_address(index);

breakTime = currentNode->getTime(ch->prev_hop_);

if (breakTime < 2000.0 && breakTime > CURRENT_TIME

&& (breakTime - CURRENT_TIME < PREDICTION_TIME_FOR_UNICAST)
```

```
&& (rt->rt_prevnode_warning == 0)){
//printf("\nPREDICTION:: at %.9f on node %d prev node %d , dst %d,
will break at %.9f\n", CURRENT_TIME,
index, ch->prev_hop_, ih->daddr(), breakTime);
sendLPW(ch->prev_hop_, breakTime); rt->rt_prevnode_warning ++; }
}#endif
########################################
Forward (rt, p, NO_DELAY) ;}
// PDFRP code - could it be removed? #handle_link_failure(prediction_nbr);
// PDFRP code
#ifdef PDFRP_PACKET_DIVERT
if ( !DATA_PACKET(ch->ptype()) )
UN(p, UN_RTR_MAC_CALLBACK);
else { // diverting the packet using an alternate path if available.
pdfrp_rt_entry *rt = rtable.rt_lookup(ih->daddr());
if ( rt && (rt->rt_flags == RTF_UP) &&(ch->pdfrp_divert_count_ < PDFRP_MAX_divert_COUNT)
)
{ch->pdfrp_divert_count_ += 1;
forward (rt, p, NO_PDFRP_DELAY); }
else UN(p, UN_RTR_MAC_CALLBACK);
}
while((p = PDFRPifqueue->filter(prediction_nbr)))
{ struct hdr_cmn *ch = HDR_CMN(p);
struct hdr_ip *ih = HDR_IP(p);
if ( !DATA_PACKET(ch->ptype()) ) UN(p, UN_RTR_MAC_CALLBACK);
else { // Divert the packet using an alternate path if available.
pdfrp_rt_entry *rt = rtable.rt_lookup(ih->daddr());
if ( rt && (rt->rt_flags == RTF_UP) &&
```

(ch->pdfrp_divert_count_ < PDFRP_MAX_divert_COUNT))

{ch->pdfrp_divert_count_ += 1;

forward (rt, p, NO_PDFRP_DELAY); }

else UN(p, UN_RTR_MAC_CALLBACK); }

}

#else // NO PACKET Divert, call Upstream Notification

UN(p, UN_RTR_MAC_CALLBACK); // Do the same thing for other packets in the interface queue using the

// CN-node not success to divert data,

while ((p = PDFRPifqueue->filter(No_Fil_ Rqment_nbr))

{ UN(p, UN_RTR_MAC_CALLBACK);

}

nb_delete(prediction_nbr);

// PDFRP code #endif

// NO PACKET Divert, call Upstream Notification

}

#endif // LINK LAYER DETECTION

} Packet *rerr = Packet::alloc();

struct hdr_PDFRP_error *re = HDR_PDFRP_ERROR(rerr);

/* * For now, no drop the packet and send error upstream Notification (UN), then the route request is broadcast UN-node neighbors.