On-Demand Routing with Unidirectional Link Support for Mobile Ad hoc Networks

Megat Farez Azril Zuhairi

A thesis submitted for the degree of Doctor of Philosophy to the
Centre for Intelligent Dynamic Communications
Department of Electronic and Electrical Engineering
University of Strathclyde, Glasgow, UK

August 2012

Declaration

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has lead to the award of a degree.

Megat Farez Azril Zuhairi August 2012

Acknowledgements

First, I would like to thank my supervisor, Dr. David Harle, who has given me the opportunity to work on this project and has assisted me in any way possible. He provided me with endless source of ideas and encouragement throughout my study. His insights and suggestions to the thesis have given me invaluable guidance in various stages of my work. His directions with regard to the developments of my academic thinking, problem solving and technical writing were inspiring and will be very helpful in my future work and study.

Then, I want to thank my colleagues, Dr. Christos Tachtatzis and Dr. Mohammad Haseeb Zafar, whom were very supportive throughout this project. I am also grateful for the support and assistance from all current and former members of the Centre for Intelligent Dynamic Communications (CIDCOM) who helped me in many ways and given me a sense of belonging as a group.

I would like to extend my sincere gratitude to my employer and sponsor Universiti Kuala Lumpur, Malaysia, for giving me the opportunity to pursue my PhD at University of Strathclyde.

Last but not least, my family members deserve special recognitions for their endless support during the past years. My deepest and sincere thanks are always to my parents, parent-in-laws, brothers, sisters, brother-in-laws and sister-in-laws for their constant support and prayers. I am grateful to my lovely wife Dewi Malinda Putri and son Megat Afiq Luqman without their understanding, patience and encouragement it would have been impossible for me to finish this work.

Abstract

The development and growth of wireless communication for multi-hop communication, has led to many research works particularly in the area of Mobile Ad hoc Networks (MANETs). Despite a large number of investigative and development works on the subject, the research on MANET is considered premature and therefore, many issues need to be addressed. Naturally, the topology of MANETs is frequently changing, where nodes having different attributes and transmission capability, forming connections using limited resources. Such characteristic causes the network to be heterogeneous and as a result, routing paths between nodes can be formed via links that are both symmetrical and asymmetrical. The design of efficient and reliable routing schemes that can exploit and utilise all types of link is therefore, a major challenge in MANET. The key works on this research are to investigate the impact of unidirectional links on the routing path construction and to develop schemes to improve the performance. In the first part of the thesis, an investigative work using the AODV routing protocol is made. The link and routing path connectivity is thoroughly analysed with different propagation and mobility models. The second part of the thesis presents the first proposed scheme, referred to as Dynamic Reverse Route (DRR), built upon the AODV routing protocol. Fundamentally, the DRR operation follows the base protocol but enhanced the routing mechanism in the presence of unidirectional links. The DRR is able to minimise the routing overhead incurred due to multiple route request broadcast and also rapidly constructs the routing path construction by allowing control packets to be propagated via unidirectional links. The third part of the thesis presents a new routing metric, formulated using the combination of three parameters; the highest received signal strength, the lowest path loss, and smallest number of hop count. Subsequently, the routing metric is implemented on the second proposed scheme referred to as AODV with path loss (AODV-PL) estimation technique. Unlike the first scheme, AODV-PL is a mechanism that addresses the unidirectional link problem by detecting and avoiding links that are potentially unidirectional. A new performance metric is also developed known as the probability of route connectivity, which complements the analysis of link connectivity. Based on such metric, the routing performance can be measured in terms of the number of success to construct routing path. Typical routing performance analysis using packet delivery ratio, average delay, and routing load are also presented in addition to the probability of route connectivity. The performance differentials of each scheme are analysed using Network Simulator 2 (NS-2). Results from the simulation experiment show the superiority of the proposed schemes compared to the base protocol under varying cases of network scenario.

Publications

The following lists the author's publications in chronological order.

Journal Publications

[J1] M. Zuhairi, H. Zafar and D. Harle, "Wireless Machine-to-Machine Routing Protocol with Unidirectional Links", *Smart Computing Review*, vol. 1, no. 1, pp. 58–68, October 2011.

[J2] M. Zuhairi, H. Zafar and D. Harle, "Dynamic Reverse Route for On-Demand Routing Protocol in MANET", *KSII Transactions on Internet and Information Systems*, vol. 6, no. 5, pp. 1354–1372, May 2012.

[J3] H. Zafar, M. Zuhairi, D. Harle and I. Andonovic, "A Review of Techniques for the Analysis of Simulation Output", *IETE Technical Review*, vol. 29, no. 3, pp. 223–228, May-June 2012.

[J4] M. Zuhairi, H. Zafar and D. Harle, "The Impact of Mobility Models on the Performance of MANET Routing Protocol", (in press) *IETE Technical Review*, vol. 29, no. 5, September-October 2012.

Conference Publications

[C1] M. Zuhairi, D. Harle, "AODV Routing Protocol in Heterogeneous Network", *Proc. 11th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet)*, Liverpool, UK, pp. 9–12, June 2010.

[C2] M. Zuhairi, D. Harle, "Dynamic Reverse Route in Ad hoc on Demand Distance Vector Routing Protocol", *Proc. 6th International Conference on Wireless and*

Mobile Communications (ICWMC), Valencia, Spain, pp. 139–144, September 2010.

[C3] M. Zuhairi, D. Harle, "A Simulation Study on the Impact of Mobility Models on Routing Protocol Performance with Unidirectional Link Presence", *Proc. 25th IEEE International Conference on Information Networking (ICOIN)*, Kuala Lumpur, Malaysia, pp. 335–340, January 2011.

[C4] M. Zuhairi, H. Zafar and D. Harle, "On-Demand Routing with Unidirectional Link Using Path Loss Estimation Technique", *Proc. Wireless Telecommunications Symposium (WTS)*, London, UK, April 2012.

Contents

List of Figures

List of Tables

Abbreviations

ACK	Acknowledgement
AODV	Ad hoc On-demand Distance Vector
AODV-PL	Ad hoc On-Demand Distance Vector-Path Loss
AOMDV	Ad hoc On-demand Multipath Distance Vector
AP	Access Point
APE	Ad hoc Protocol Evaluation
API	Application Programming Interface
ARP	Address Resolution Protocol
AOZDV	An Enhanced AODV Protocol based on Zone Routing
BMT	Batch Means Test
BRA	Bidirectional Routing Abstraction
BRREP	Backtrack Route Reply
BSS	Basic Service Set
CBM	Content Based Multicast
CBR	Constant Bit Rate
CDMA	Code Division Multiple Access
CEDAR	Core Extraction Distributed Ad hoc Routing
CGSR	Clusterhead Gateway Switched Routing
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CTS	Clear To Send
DBLAR	Distance-based Location Aided Routing
DCF	Distributed Coordination Function
DIFS	DCF Inter Frame Spacing
DQPSK	Differential Quadrature Phase Shift Keying
DRR	Dynamic Reverse Route
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum

DTN	Delay Tolerant Network
ESS	Extended Service Set
ETT	Expected Transmission Time
ETX	Expected Transmission Count
EUDA	Early Unidirectional Link Detection and Avoidance
FDMA	Frequency Division Multiple Access
GDB	GNU Debugger
GloMoSim	Global Mobile Information Systems Simulation Library
GM	Gauss Markov
GPS	Global Positioning System
HRRP	Hybrid Reactive Routing Protocol
IBSS	Independent Basic Service Set
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IFQ	InterFace Queue
IFS	Inter Frame Spacing
LBSR	Loop Based Source Routing
LL	Link Layer
LOS	Line of Sight
LPS	Local Positioning System
MAC	Medium Access Control
MANET	Mobile Ad hoc NETwork
MAODV	Multicast Ad hoc On Demand Distance Vector
MPDU	MAC Protocol Data Unit
MPR	Multi Point Relay
NAV	Network Allocation Vector
NetIF	Network InterFace
NIC	Network Interface Card
NLOS	Non-LOS
NS-2	Network Simulator 2
OLSR	Optimised Link State Routing
OMNeT++	Objective Modular Network Testbed in C++

OPNET	Optimized Network Engineering Tool
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTcl	Object Tool command language
PHY	Physical
PL	Path Loss
QoS	Quality of Service
RAODV	Reverse-AODV
RERR	Route Error
RF	Radio Frequency
RFC	Request for Comments
RPG	Reference Point Group
RPS	Reverse Path Search
RREP	Route Reply
RREQ	Route Request
RSS	Received Signal Strength
RTS	Request To Send
RTT	Round Trip Time
RWP	Random Waypoint
SCF	Store-Carry-Forward
SIFS	Short Inter Frame Spacing
SINR	Signal to Interference and Noise Ratio
SWIM	Shared Wireless Infostation Model
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TLRP	Tree-shape Location-based Routing Protocol
TTL	Time-to-Live
UDP	User Datagram Protocol
VANET	Vehicular Network
WiFi	Wireless fidelity
WiMax	Worldwide Inter-operability for Microwave Access
WLAN	Wireless Local Area Network

WMN	Wireless Mesh Network
WSN	Wireless Sensor Network
WUSB	Wireless Universal Serial Bus
ZigBee	Zonal Intercommunication Global-standard

1. Introduction

The rapid development in wireless communication technologies and the increasingly cheaper costs of manufacturing radio components have led to a high surge of interest in wireless communication within the unlicensed frequency spectrum. Traditional wireless network such as Wireless Local Area Networks (WLANs) [1] have proven to be more reliable than MANET in providing high capacity network access via radio signal. Nevertheless, a particular shortcoming of WLAN is the need to have a centralised coordination function for assisting nodes with link setup and communication maintenance. Such restriction reduces flexibility. For this reason, an autonomous system is preferred, leading to the formation of wireless ad hoc networks. Such networks enable the communication path to be self-created by wireless devices[1] using a set of protocols specifically design to adapt to the dynamic nature of the topology. Nonetheless, a key challenge in such a network is to devise efficient methods to ensure high route availability while incurring minimal disruption to packet transmission. The typical single-hop communication technique used in WLANs is no longer relevant in this situation and in turn leads to a new form, referred as multi-hop relay messaging. Data is propagated using successive cooperation between devices, allowing a source node located outside the transmission range of the destination node to communicate via multiple hops (links). Such technique is possible if nodes are equipped with an ad hoc routing protocol, where each node can serve as a router to forward packet on behalf of others. Such protocols effectively construct routing paths and also spontaneously detect broken links caused by wireless interference, nodes mobility, and radio propagation phenomenon. Many research project, which utilises ad hoc network approach have been undertaken. Examples of application are the Green Sensor Network for Structural

[1] Wireless devices, users, nodes, and mobile nodes are used interchangeably in this thesis.

Monitoring (GENESI) [2] and FLORA [3], which is a wireless sensor system for monitoring natural resources.

1.1 Characteristics of Wireless Multi-hop Ad Hoc Network

Indeed, there are many reasons wireless multi-hop ad hoc network should be explored as an alternative to the traditional network type. First, ad hoc networks can avoid bottleneck forming within cells and at gateways, a typical occurrence in WLANs when there is a sudden increase in the number of wireless devices. Therefore, expecting every node to exchange information over the infrastructure is not feasible. Second, the freedom to create and distribute information in an infrastructure-based network can be severely limited. Many centralised networks are subject to restrictions, where contents to be shared and published are filtered through the firewall. Third, the backbone devices in the infrastructure network are continuously consuming resources to disseminate network updates. Thus, energy utilisation is highly inefficient, particularly when the network load is low, i.e. when a small number of nodes are connected to the network. Finally, constant reliance on the infrastructure network to communicate reduces the flexibility for nodes to be mobile. In light of these points, the wireless multi-hop ad hoc network is clearly an appropriate choice for future wireless communication. The network offers flexibility and alleviates the issues as previously mentioned.

1.2 Challenges in Wireless Multi-hop Ad Hoc Network

The unique operation of wireless multi-hop ad hoc network presents several challenges. The flexibility of the network compromises the routing reliability and end-to-end services because of the dynamic network topology. When nodes are mobile, the impact to the network performance is more severe. The state of the link may constantly fluctuate, which mitigating against a stable communication path persisting for an extended period of time. The node’s movement pattern can also affects the network connectivity. For instance, nodal movement of a random fashion may result in a dynamic topologies, thus creating a non-durable communication sessions. By contrast, in a network where nodes move in groups, the links are relatively unchanged, and as a consequence, the creation of long-lived clusters may occur. Additionally, a common set of protocols which nodes employ to establish communication may only be effective in particular scenarios but not others, resulting in performance inconsistencies. Furthermore, the wireless network extremely depends on the availability of radio signal to setup path. Severe interference, obstruction, and other environmental phenomenon are additional complicating factors to the network's operation.

1.3 Wireless Multi-hop Ad hoc Support

Despite the challenges previously presented, a variety of current technologies exist that may provide a platform for wireless multi-hop ad hoc networking. The ad hoc mode, which is part of the service protocol offered by IEEE802.11b, can be exploited to operate multi-hop. Originally designed to setup point-to-point communication, the ad hoc mode can provide a service for future multi-hop communication. Another existing technology is the Bluetooth, which perhaps have a design that is more compatible with wireless multi-hop ad hoc approach. Other protocols such as ZigBee [4] are also available but these technologies do not attract as much attention from the research community.

1.4 Research Motivation

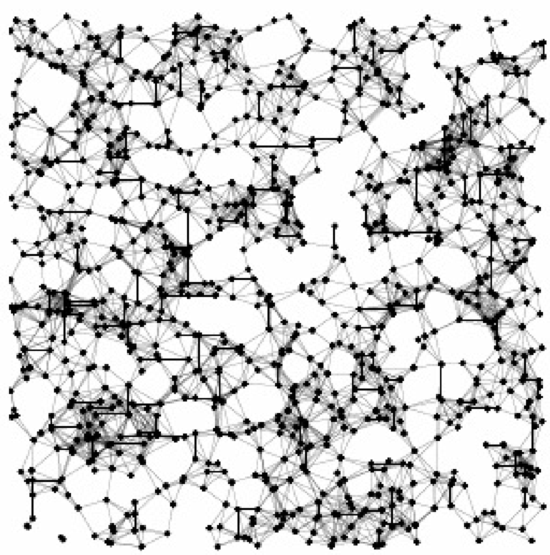
In light of the previously addressed issues and challenges, the focus of this thesis is to design and improve routing protocols for wireless multi-hop ad hoc networks, specifically the Mobile Ad Hoc Network (MANET). The routing protocol should be able to adapt to the limitations while providing reliable network performance under severe network conditions.

Due to the broadcast nature of wireless communication, nodes within transmission range of each other compete for the available channels. Furthermore, the effective available bandwidth in this network is significantly lower compared to the nominal bandwidth offered by the network hardware. The signal strength of packets received by a node is also significantly affected by changes in the signal to interference and noise ratio (SINR); a results of concurrent transmission by adjacent nodes and variations in signal propagation. These lead to packet loss, which is more severe when the receiver's signal and the source of noise overlap in terms of frequency. Based on such constraints and other common issues on MANET, the general requirements for the design of routing protocol in this thesis are summarised as follows:

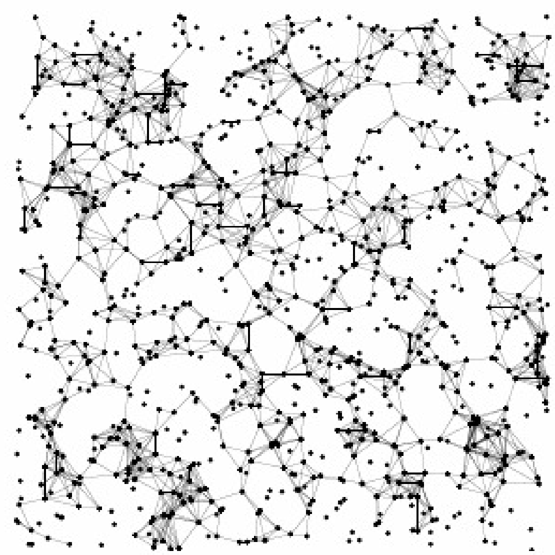
- *Low overhead*: The routing protocol needs be able to reduce the routing overhead, particularly the number and the size of control packets. In addition, it is also important to minimise the number of times nodes forward data packets (by having shorter path), to conserve bandwidth and energy.
- *Adaptiveness*: To enable efficient operation over various ranges of network conditions, the routing protocol needs to dynamically adapt to different network topologies and propagation conditions.
- *Resilience to loss*: In the event of packet loss, the correct operation of routing protocol must be maintained. The probability of packet loss in the ad hoc network environment may be high, particularly when subject to broadcast packets. In addition, due to frequent link flaps, standard control flow mechanisms within the link layer may not be able provide sufficient reliability.

Specifically, the research work in this thesis focuses on designing a routing scheme capable of efficiently handling unidirectional links. Underpinned by the principles that radio signal in wireless multi-hop ad hoc network is subject to severe SINR, nodes mobility, and non-homogeneous nodes properties, the link between nodes may not always be bidirectional. Surprisingly, many simulation studies fail to consider such a key issue and subsequently draw conclusions on the basis that a network is homogeneous. Furthermore, it is often conjectured typically, that every node uses a single type of networking technology, e.g. IEEE 802.11b, and that radio signals all have the same strength. Such assumptions are not true. In fact, an important characteristic of wireless communication is the heterogeneity. Different wireless technology may interoperate by using a bridge access point, for instance between ZigBee and WiFi [5]. Perhaps in the near future interoperability between technologies may also include other wireless technologies such as Wireless USB (WUSB) [6] and WiMax [7].

The effect of heterogeneity in a network leads to irregular connectivity between nodes, causing the formation of unidirectional link. Figure 1.1 shows the difference in link distribution between *homogeneous* and *non-homogeneous* network in terms of transmission power. Although the node distribution is varied (due to different seed), the node density in both Figure 1.1a and Figure 1.1b are similar. Clearly, the network in which the property of radio signal is varied (Figure 1.1b), exhibits more isolated node compared to those that are set with identical radio power (Figure 1.1a). The lines connecting the points, i.e. nodes, refers to link establishment. Therefore, when multiple connections are created between the nodes, the line intensity increases.



(a) Equal transmission power



(b) Non-equal transmission power

Figure 1.1: Network connectivity [8]

As a consequence of high costs and the inherent difficulty (and lack of flexibility) to build a real-scale wireless multi-hop network, the research work in this thesis is based upon network simulations. It is shown in some papers that network simulations packages are the most commonly used option to study the performance of such networks [9]. Indeed, simulators may not be always able to evaluate the network performance, but with careful selection of model and parameter settings, the credibility of simulation output can be improved. For instance, most studies on mobile ad hoc networking use the random waypoint as a reference for node mobility [10]. But recent studies have shown that the random waypoint mobility model fails in reproducing human mobility in realistic manner [11][12][13]. Moreover, the simulation settings generally used in experimentation often favour the execution of protocols. When using other realistic models, which will be presented in Chapter 4, the protocols behave differently.

1.5 Research Contributions

In this thesis, two different routing schemes capable of forming routing path in severe network connectivity caused by unidirectional links are presented. Each scheme has a unique approach to handling such links. The mobility and radio propagation could affect network connectivity, therefore, prior to the evaluation of the proposed schemes, several models are studied and compared by simulation. Models that are deemed relevant for the analysis of unidirectional link are selected and used for simulation experiment in subsequent chapters of the thesis. The following summarises the major contributions in the research work:

- A comprehensive analysis of network connectivity by way of simulation is presented. The quantification of network connectivity is conducted over several types of mobility pattern and different signal propagation, which generate sufficient variation of network scenarios. A new performance metric referred as the probability of route connectivity is introduced to enhance the analysis of network connectivity. Such a performance metric further facilitates a routing protocol's evaluation complimenting to typical link connectivity analysis.

- A Dynamic Reverse Route (DRR) routing scheme is proposed that enables node to rapidly compute routing path despite the presence of unidirectional link on the network. The proposed scheme is protocol independent, which can be adopted by other routing protocols that share similar properties with the base protocol. DRR reduces the frequency of route discovery while locally dealing with the unidirectional link at the affected node.
- An Ad hoc On Demand Distance Vector routing protocol based on path loss (AODV-PL) estimation technique is proposed. The proposed scheme eliminates the traditional dependency on shortest route computation based only on hop count. A new cost function is proposed for the link selection process that is built upon the combination of path loss, received signal strength, and hop count. In effect, the proposed scheme maintains routing every packet via symmetrical routes. Each link along the routing path is successively determined by using the proactive path loss estimation technique.

1.6 Thesis Organisation

The outline of the thesis indicating the relationships is shown on Figure 1.2.

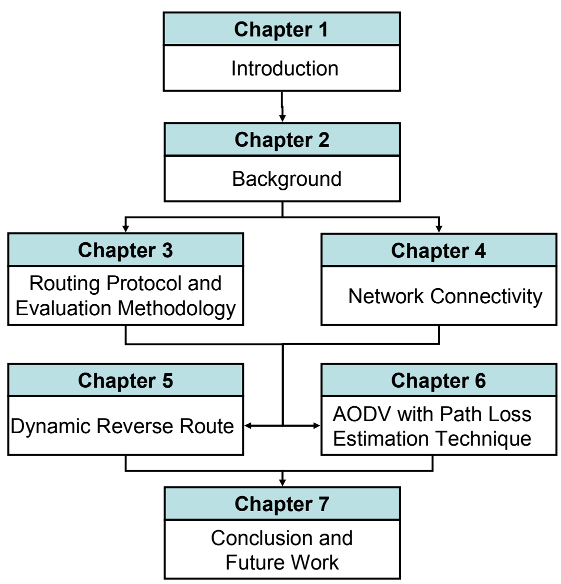


Figure 1.2: Flowchart of thesis

2. Background

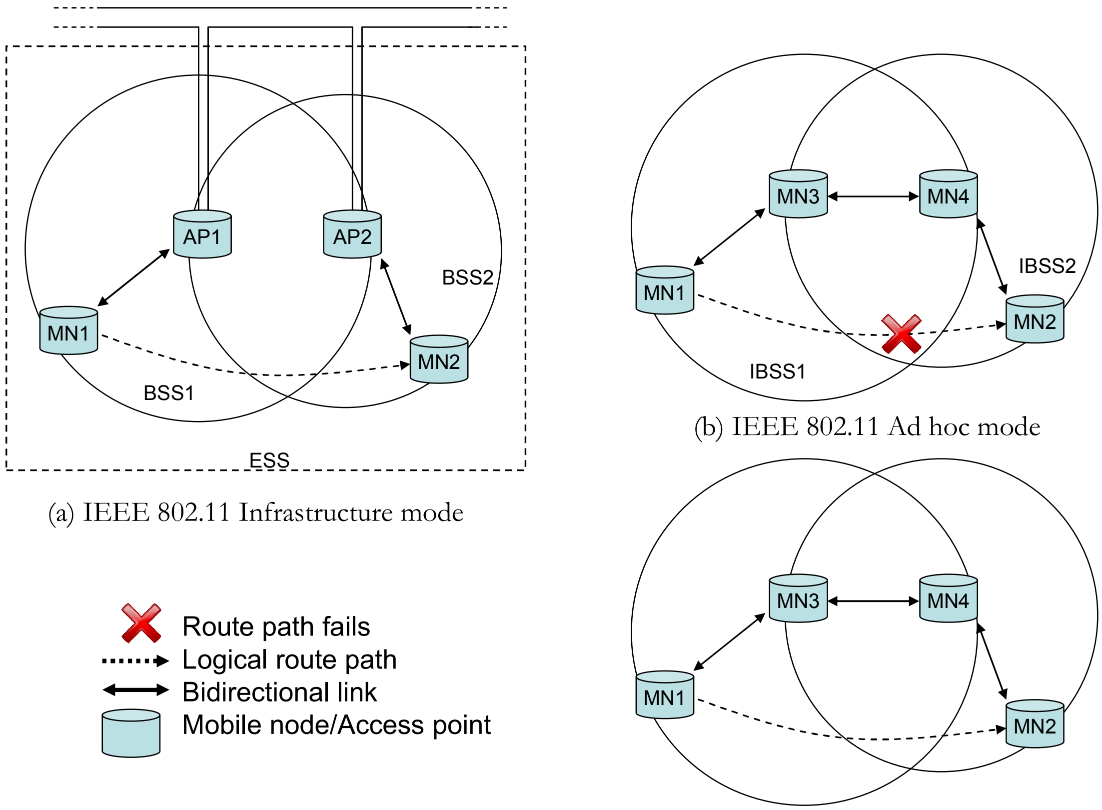
2.1 Introduction

This chapter presents a discussion of Mobile Ad Hoc Networks (MANETs) along with a review of several types of MANET routing protocols. Section 2.2 introduces the underlying concept of wireless multi-hop networks and their important properties. Subsequently, section 2.3 discusses the various types of wireless multi-hop networks, highlighting the similarities and the differences. Section 2.4 presents the key properties of MANETs that form the basic building blocks unique to such networks. The section further discusses about the constraints, which result from using conventional protocols designed for traditional wireless network. Next, section 2.5 presents the classification of MANET routing protocols, including the foundation protocol from which the work proposed in this thesis is derived. Finally, section 2.6 summarises this chapter.

2.2 Wireless Multi-hop Networks

It is not until recently, following the birth of Wireless Local Area Networks (WLAN) in the early 1990's that wireless communication has really began to be develop rapidly. The technology for wireless data transportation has been around for many years. However, the growing demand for mobile internet connectivity in recent years and the ease at which such related services are available has increased the need for wireless network connectivity. The IEEE 802.11 [1] standard for WLAN was released in 1997 and has been accepted for widespread application in many wireless products, such that communication with existing infrastructure is now possible without complex configuration. To that end, wireless users are able to access the network by connecting to a fixed gateway station inside a specific radio area. However, the downside of such architecture is that it lacks flexibility. The network coverage offered is limited to a particular radio range specified by the Basic Service Set (BSS) and users may experience intermittent connectivity particularly when moving between different radio domains at a relatively high velocity.

Consequently, the IEEE 802.11 standard has been extended to support mobility and multi-hop services, increasing connection flexibility and robustness to network changes [14][15] . Generally, this will result in performance gains for end-users in system who do not have a direct line-of sight (LOS) between the source and destination. The new technology relies on routing cooperation among wireless devices to forward data from one point to another. As shown in Figure 2.1, three different forms of communications is possible using the IEEE 802.11 standard. Figure 2.1a shows the communication setup in an infrastructure mode known as Extended Service Set (ESS). Note that the access point 1 (**AP1**) and access point 2 (**AP2**) communicates via the cable infrastructure, although both APs are within the range of each other. In addition, the BSS is the area of network coverage associated with each AP. As shown in Figure 2.1a, mobile node 1 (**MN1**) and mobile node 2 (**MN2**) are located in different BSS. Therefore, any communication between **MN1** and **MN2** has to be routed via **AP1** and **AP2**. Figure 2.1b is the Ad Hoc mode, where nodes basically communicate peer-to-peer in an Independent BSS (IBSS). In this method, nodes are not configured to relay messages to other node. As such **MN1** is unable to send data to **MN2** because both are outside the transmission range of each other. However, with a proper MANET routing technique set within each MN, a routing path can be constructed that follows the path <**MN1-MN3-MN4-MN2**>. This is known as multi-hop relay technique, shown by Figure 2.1c. A set of these devices forms a multi-hop relay message exchange, leading to a unique configuration of a network known as a wireless multi-hop network.



(a) IEEE 802.11 Infrastructure mode

(b) IEEE 802.11 Ad hoc mode

(c) IEEE 802.11 Multi-hop relay mode

Figure 2.1: Three different forms of IEEE 802.11-based communication

In this section, three different wireless multi-hop networks are presented, although one in particular, the MANET [16], will remain to be the *focus* of this thesis. Generally, wireless multi-hop networks are decentralised, deployed based on request, where devices communicate using radio links, and forward information through multiple hops from source to destination nodes. The requirement of planning for connection setup is minimal and changes to the network, i.e. nodes joining or leaving the network, are immediately detectable by the system and dealt rapidly to reduce disruption to network performance.

Many of the underlying protocols for multi-hop relay mode, e.g., media access control (MAC), follows the model from the infrastructure and ad hoc modes. However, the effects to the network operations are significant. Despite the lack of infrastructure support provided in traditional WLANs, nodes in wireless multi-hop networks are able to coordinate themselves according to the current state of network topology and mobility. Four pertinent characteristics of wireless multi-hop network compared to others are:

- *Dynamic Topology:* Node connectivity is extremely dynamic, the results of operating in a boundary-less network with few restrictions on nodes joining and leaving the network. This is, perhaps, the most important characteristic of ad hoc wireless networks compared to traditional wireless networks, resulting in compatibility issues with the IEEE 802.11 standard.
- *Infrastructure-less*: Nodes are independent of backbone infrastructure, relying exclusively on radio links. As a consequence, data will be unreliably transported over a network with constrained capacity, i.e. fixed bandwidth shared among nodes.
- *Resource Constraints*: Nodes are typically small and therefore, have limited internal system resources such as memory, processing power, and battery power supply.
- *Scalability*: Finally, increasing numbers of nodes, i.e. users, connected to the network will have a substantial impact on the performance of wireless multi-hop network, leading to scalability issues.

As a consequence of the points raised above, protocols designed for traditional wireless network may not perform as well in wireless multi-hop network environment. These new approaches have to be developed or improved, based on the current algorithms, to adapt to the network characteristics.

2.3 Classification of Ad hoc Wireless Multi-hop Networks

The emergence of ad hoc wireless network over the past few years has attracted a lot of attention from researchers, resulting in the development of new concepts and applications [17][18]. This section provides an overview of three types of multi-hop wireless networks, highlighting the similarities and the differences. First is the Mobile

Ad hoc Network (MANET), which is one of the earliest ad hoc wireless multi-hop notions established after the idea was proposed in two conferences [19][20] in the early 1990's. It describes the self-organising ability of nodes in a network, where the network is formed on demand, irrespective of a node's mobility condition. MANETs can also be categorised as a subset of a larger Wireless Mesh Network (WMN) [21], leading to the formation of the second type of wireless multi-hop networks. Basically, WMN refers to the connectivity within any wireless network that is 'mesh' in nature. Finally, a discussion of wireless multi-hop network known by the wireless sensor network (WSN) [22] is presented. Figure 2.2 provides a general comparison between the previously mentioned multi-hop wireless networks and other network types. The differences between each network types are illustrated as a function of infrastructure and connectivity.

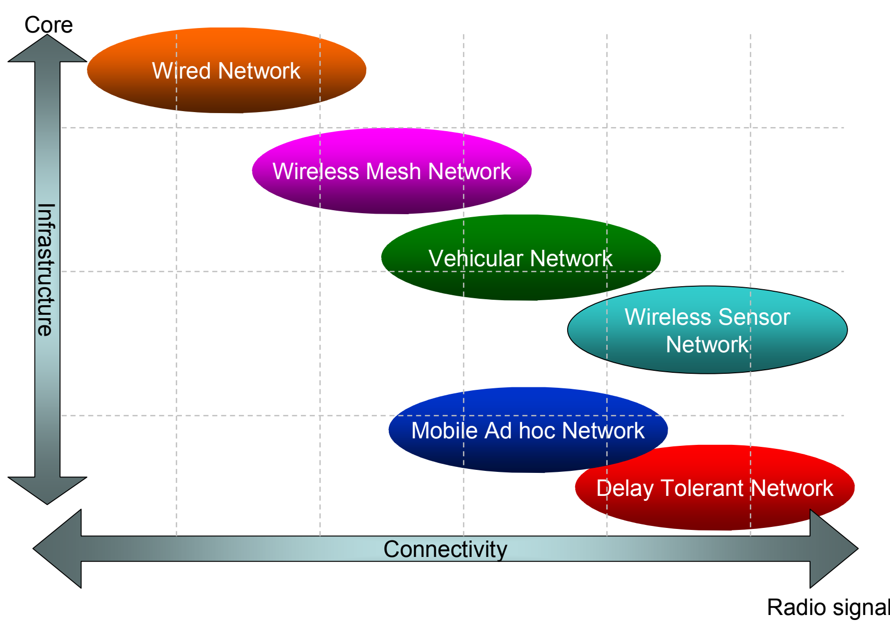


Figure 2.2: Classification of networks

2.3.1 Mobile Ad Hoc Networks (MANET)

A MANET is different from other types of wireless multi-hop network in that nodes communicate without relying on any predefined connection while in motion. Therefore, connections between nodes are highly flexible, significantly influenced by the variability of network topologies. To accommodate this dynamic nature, connections among nodes must rely solely on the availability of radio link. In order to guarantee end-to-end communication, nodal functionalities as end stations and routers must be interchangeable. For instance, in a room occupied by a group of students, where each person is equipped with a device capable of wireless communication, a MANET may form. Messages from the source device, i.e. end station, can be forwarded to another device acting as a router, in a relay fashion. Although some students may move into or out of the room, the communication path is sustained. In addition, the devices may run out of battery, which eventually being powered off, causing link breaks. Such challenges predicate robust algorithms so nodes are able to rapidly adapt to changes and maintain network connectivity. Nonetheless, data transmission in wireless ad hoc is not as reliable as in traditional wireless network [15]; since nodes are typically operate with limited network resources, i.e. bandwidth, battery power, and etc.

In view of the challenges mentioned above, much work has already been accomplished to address such problems. However, there are still quite a number of issues that remain and these include the physical access scheme, transport layer, energy management and, particularly, routing efficiency which is of principal interest in this thesis.

2.3.2 Wireless Mesh Networks (WMN)

WMNs refer to the type of connections formed in wireless multi-hop network by means of a mesh topology. In contrast to MANETs, nodes on a WMN communicate in organised fashion. A group of nodes are typically set with low or null mobility which, in effect, forms the network backbone supporting other mobile nodes for building a reliable communication path. These dominant nodes are comparable to access points on WLAN, responsible of routing and forwarding data through the network. Essentially, the backbone nodes are known as mesh routers, whereas mobile nodes are known as mesh clients. In addition, mesh routers are typically equipped with a stable power supply, e.g. external power source from alternate current input, capable of higher processing and decision routing, and able to provide a longer reach of radio coverage for mobile nodes. On the other hand, mesh clients are more mobile with limited energy resources, i.e. battery-powered, compared to mesh routers.

The backbone structure in WMN provides stability and the support required by mesh client to forward data through the wireless network. Data packets are primarily propagated through backbone links which have higher bandwidth capacity, reducing the probability of link congestion and link breakages. There are some well-known WMN test-bed projects that have been deployed by academic researchers and other independent group for experimentation purposes. Examples include Berlin RoofNet [23], QuRiNet [24], and QUMESH [25].

2.3.3 Wireless Sensor Networks (WSN)

The wireless sensor networks (WSN) are a sub-class of wireless multi-hop network, typically formed by a group of sensor nodes to provide robust communication infrastructure over a specific geographical area. Generally, sensor nodes are small in size equipped with limited amount of energy and processing power designed to collect certain physical parameters of the environment (or even the nodes itself), and forward the gathered data to a central monitoring station for recording and measurement purposes. Examples of applications include remote environment observation, measurement of physiological data of patient and habitat monitoring [3][17][26]. In many cases, sensor nodes are constrained by battery power; therefore sensing activities are usually irregular, although some specific applications may require periodic data collection.

Similar to MANETs, sensor networks are ad hoc in nature and require minimal planning prior to connection setup. Nevertheless, sensor networks suffer from several issues and challenges related to its operation and maintenance. The fact that nodes carry a limited and typically irreplaceable battery power often leads to WSN design that is efficient in power consumption, storage and transmission capability. In contrast to traditional wireless networks, which aim to offer the best quality of service (QoS), wireless sensor networks focus primarily only on vital sensing operations. For instance, sensor nodes deployed in a harsh environment such as in a region with high volcanic activity will require minimum or no human intervention. As such, the power source, i.e. battery, is not possible to be replenished causing deterioration of nodes sensing capability. In addition, this may affect nodal radio transmission range, reducing the number of potential connections and increasing the probability of unidirectional link creation. Sensor networks also have restricted bandwidth resources. Therefore, data propagation must be effectively distributed through several connections towards the central monitoring station. In fact, applications that demand high redundancy such as military applications will require multiple connections to be established in order to increase stability and removing a single point of failure.

2.4 MANET properties and constraints

This section focuses on identifying several important MANET properties and its constraints that may affect their network performance and in particular, routing operations. Four MANET attributes relevant to the scope of this thesis are identified: network topology, node mobility, physical layer, and data link layer operations.

2.4.1 Network topology

Generally, path setup in MANET is a product of instantaneous wireless association by a group of nodes located adjacent to each other without the need for configuration prior to connection establishment. The network topology is unpredictable, in that it constantly changes over time in ad hoc fashion. One particular property of the network topology affecting the system performance is node density, defined by number of nodes per unit area. Such a characteristic influences the number of potential links that can be established for routing, where a high nodal density, i.e. dense networks, leads to greater connectivity and low node density, i.e. sparse networks, results in lower connectivity.

Although a densely connected network can improve robustness through multiple links, it may also cause severe co-channel and adjacent channel interference.

Interference in a densely connected network topology is not uncommon, and the standard IEEE 802.11 protocol has been designed to naturally overcome the issue. A typical interference management is the hold-off and retransmission mechanism. With such scheme, a node that is about to transmit a packet when it senses the wireless medium is busy will defer access to the channel for a time duration, i.e. silent period, specified by the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) [27] protocol. In another example, a node is in the middle of transmission when it detects severe interference, thus preventing the receiver node from correctly receiving a packet. As a result, the packet is not acknowledged and the sender subsequently invokes a retransmission procedure. Although packets may eventually be received, the throughput however, is significantly impacted, as shown by Stamatiou [28].

On the positive side, a network topology with high node density may benefit from higher network capacity provisioning. This is achieved by allowing the spatial reuse of the spectrum. Research work by Fengji [29] demonstrates that the capacity of a wireless multi-hop network is proportional to the number of concurrent connections established. In other words, a densely connected network provides higher network capacity compared to sparse networks, assuming that both scenarios adopt the same transmission range setting. On the other hand, a network that accommodates low node density may be efficient in terms of reducing severe interference but higher connectivity is compromised. For this reason, evaluation on the effect of network density is paramount, which is analysed in Chapter 6.

2.4.2 Node Mobility

As mentioned earlier, one of the main characteristic of MANET that distinguishes them from other types of wireless network is the fact that nodes are frequently in motion. In addition, nodes are allowed to intermittently join and leave the network affecting the routing path stability. In light of this, three issues commonly considered as the direct consequences of node mobility are: path breakages, traffic overhead, and path lifetime.

Of the three issues, the most common effect of node mobility on MANET is perhaps path breakage. Naturally, much research work has shown the negative impact of nodes mobility on the network performance [12][13], where the number of packets delivered drops when nodes are set with high mobility compared to nodes with low or null mobility. However, such relationship may not be true if external factors are considered such as network area, node density and radio transmission range. For instance, a network with high number of nodes confined within a small network area may produce lower path breakage even in the event of high node mobility.

There are several general techniques discussed in the literature that deal with path breakages [30][31]:

- *Prevention method*: This method is achieved by computing the link duration to determine when the primary path will break. Based on that knowledge, the route can be instantly avoided or switched to alternative path before disconnection. Depending on the technique used, the time can be computed based on various links metric. This may include links with the lowest delay, highest route expiration time, and strongest received signal strength. Following this idea, the technique proposed in Chapter 6 utilises the path loss as a metric to compute stable routes, resulting in a stronger link connection. This way, the probability of path breakage occurrences is reduced and the number of control packets, i.e. traffic overhead, generated can be significantly minimised.
- *Frequency of updates*: The second method to alleviate the impact of node mobility is to increase the frequency of periodic topology updates. This approach is common for proactive routing protocol. Although effective in combating against path breakages, frequent exchange of control packets typically leads to the degradation of system performance, caused by severe routing overhead.

- *Routing mechanism*: The final method is to completely change the routing mechanism so that it can tolerate extremely low propagation delays and high packet loss that result from mobility. An example is the Store-Carry-Forward (SCF) technique in the Delay Tolerant Network (DTN) [32]. In this system, upon a link breakage, the packet that is about to be transmitted is stored for a substantial amount of time and forwarded only when links are re-established. However, such a method is not practical for applications that require continuous connectivity and low propagation delay such as MANET and, thus, is beyond the scope of this thesis.

2.4.3 Physical Layer

The physical layer properties of MANETs define the physical transmission of data/control packet among nodes. Generally, communication is carried over radio signals using IEEE 802.11 protocol, similar to traditional wireless network. Although the protocol operates effectively for WLANs, it may not be as efficient for MANETs. This is because nodal capabilities are rather limited in terms transmitting power due to the key requirement for energy conservation. Consequently, nodes may be configured with lower transmitting power to improve energy utilisation. One implication of such a setup is the formation of heterogeneous paths by which a routing path is constructed of a combination of *bidirectional* and *unidirectional links*.

2.4.3.1 Unidirectional Links

In addition to physical layer constraints as discussed above, unidirectional links may also arise from various combinatorial factors affecting wireless device transmission range. Since links are radio signals, connectivity is substantially influenced by the external noise sources that impact wireless signal strength. As a result, links become asymmetric in nature and communication between source and destination pairs may follow paths which are in fact unidirectional. A typical example is unequal SINR experienced by adjacent nodes. Unidirectional links may also be caused by unequal transmitting power configured at each device. For instance, a network which employs a power-aware routing scheme will attempt to control the awake and/or sleep scheduling of a node to conserve energy. Consequently, power link budget in the forward direction may not be equal to those in the opposite direction, resulting in a unidirectional link.

To date, many proposed routing algorithms assume that nodes are homogeneous and possess similar characteristics. As a consequence, such schemes may not perform as effectively in real life situations. However, a substantive amount of research has investigated the use of unidirectional links and removing the assumption of an inherent symmetrical network; these results indicate there is a potential gain in terms of network performance [33][34][35].

2.4.4 Data Link Layer

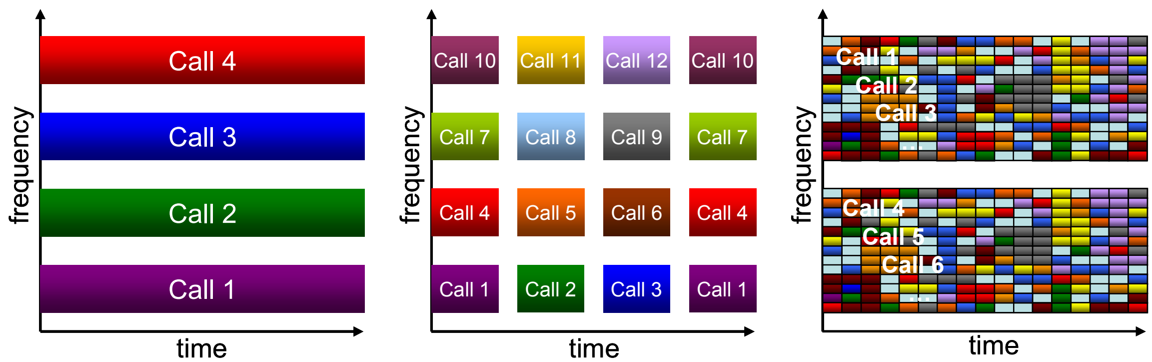
The data link layer is concerned with the coordination of medium and data transmission between two nodes. The main function of this layer is to provide node access to the shared medium, controlled primarily by its sub-layer component, the MAC. Two categories of MAC's scheme are presented in the following discussion, followed by the constraints against MANET operation.

The contention-free MAC protocols are organised access schemes, where transmission from each node is scheduled sequentially to ensure a collision-free access to the channel. Some examples of these schemes are Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA). As shown in Figure 2.3a, the FDMA separates each transmission into different frequency slots. The scheme tends to be inefficient when the MANET becomes densely populated. On the other hand, the TDMA shown in Figure 2.3b requires time synchronisation among the nodes on the network, which is not practicable for MANET that is highly decentralised. Figure 2.3c shows the CDMA, which is a highly advanced MAC scheme capable of transmitting data at high capacity. However the issue of CDMA with MANET is that nodes need to keep track of frequency hopping patterns and/or spreading codes of the time-varying neighbour. Each MAC scheme previously discussed can be considered as a circuit based approach. They require a dedicated point-to-point connection between the source and destination nodes. Generally, the idea is the same: to divide the medium into several different frames and slots, which is then reserved by every node. As such, simultaneous transmissions can be effectively supported with fewer collisions.

Nonetheless, such schemes may not be practical for system used in MANET, where communications are packet based. Data is typically fragmented into several packages, numbered in sequence, and then separately sent to the destination. Although every packet may follow a different route to destination and arrive out of order, each packet will be reassembled in the proper sequence.

On the other hand, the contention-based protocols (IEEE 802.11[2]) are typical for MANETs, which is also the key scheme employed in this thesis. The operation does not require coordination among nodes contending for the channel and nodes are free to randomly access the channel. Consequently, packet collision frequently occurs, causing nodes to back-off and re-attempt channel access again. For this reason, collisions are substantially higher than the contention-free MAC protocol leading to a lower throughput. Pure ALOHA [36] and Slotted ALOHA [37] were the first protocols taking such an approach. Further refinement was then made to significantly improve the throughput by the introduction of CSMA scheme [38]. Later, the Collision Avoidance (CA) and Request-to-Send/Clear-to-Send (RTS/CTS) mechanisms were added, to further enhance system performance.

[2] IEEE 802.11 DCF and IEEE 802.11 are used interchangeably for simplicity.



(a) FDMA (b) TDMA (c) CDMA

Figure 2.3: Contention-free Media Access Control

2.4.4.1 Hidden and Exposed Node Problem

The hidden and exposed node problem is described in the following example. In Figure 2.4, four wireless nodes are located in a simple chain network topology, where each node is assumed to be placed at the edge of other nodes transmission range. The hidden node problem arises when node **A** is in the middle of transmission with node **B** but **C** is attempting to communicate with **D**. Node **C** senses that the medium is idle (because node **C** is outside of node **A** transmission range) and begins to send data. Naturally, since data is broadcast, packet transmission from node **C** interferes with packet reception, which causes disruption and decreases the SINR of node **B**. By way of contrast, the exposed terminal problem is the reverse of hidden node problem, shown by Figure 2.5. In fact, the exposed node problem is more detrimental to the network performance. The reason being is that nodes are unnecessarily restrained from transmitting packet even if doing so will not cause any interference. For instance, when node **C** is sending to **D**, node **B** is attempting to communicate with node **A**. Since node **B** can hear the signal from **C**, and deemed that the medium is busy, node **B** will not be able to transmit packet to **A**. As a result, network capacity is not fully utilised.

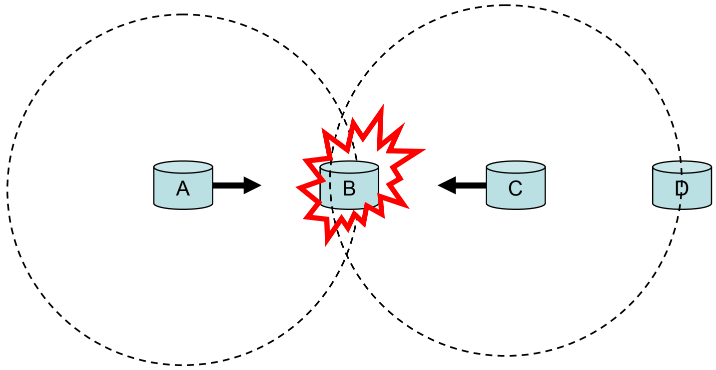


Figure 2.4: The hidden node problem

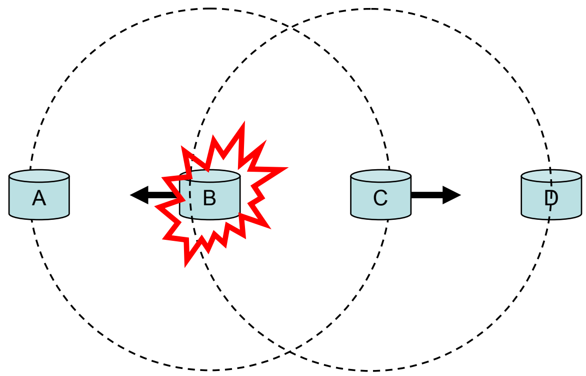


Figure 2.5: The exposed node problem

2.4.4.2 Distributed Coordination Function (DCF)

The contention-based algorithm, i.e., CSMA/CA with RTS/CTS support, provide some level of tolerance to packet collisions without compromising MANET performance. Basically, the main component of distributed coordination function (DCF) that helps to reduce interference is the exchange of RTS/CTS control packet prior to data transmission between adjacent nodes. As shown in Figure 2.6, the source node listens to the medium by using CSMA and, if it senses that the medium is not occupied, starts to send the RTS packet. Subsequently, if the intended destination is free to start a new conversation, it responds with a CTS packet back to the source. Based on such information, other node can maintain the Network Allocation Vector (NAV), which indicates the remaining time of the on-going communication. For instance, in Figure 2.7, node **A** and **D** receives RTS and CTS respectively, and set their NAV accordingly to refrain themselves from accessing the medium during **B**-**C** communication. Upon completion of data transmission, an acknowledgement (ACK) packet is sent by the destination node to inform the source that transmission is successful and the medium can then be freed.

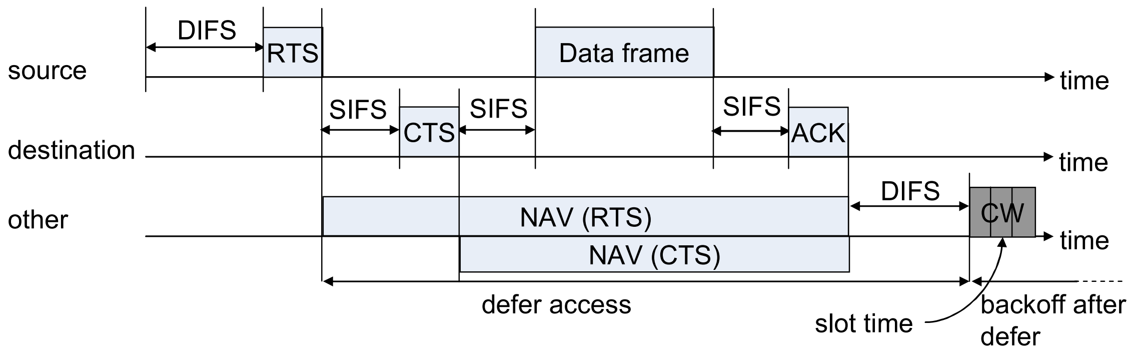


Figure 2.6: Basic Access with RTS/CTS scheme

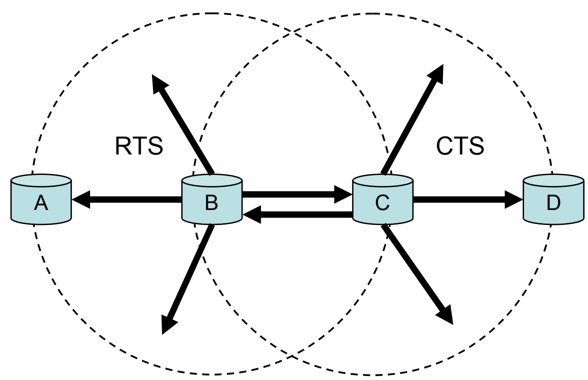


Figure 2.7: Network Allocation Vector

The DCF Inter Frame Spacing (DIFS[3]) is the time period which denotes the link is idle and therefore nodes may attempt to transmit data. The Short Inter Frame Spacing (SIFS) is a fixed value and considered to be the shortest Inter Frame Spacing. It is used as a time reservation, which prioritised a particular session and allows a pair of nodes to complete the frame exchange sequence uninterrupted. Typically, the SIFS is used prior

[3] DIFS denotes the longest waiting time and has the lowest priority for medium access.

to ACK, CTS, and MPDU (MAC Protocol Data Unit). Table 2.1 shows data rate and the time interval between frames in different IEEE 802.11 [1] PHY layers standards. Like SIFS, the Slot Time[4] is a fixed value defined in each standard. Most 802.11-based networks generally use two Slot Time values, i.e., 9 and 20 microseconds. In addition, equation 2.1 presents the mathematical derivation of the DIFS, which depends on the parameters shown in Table 2.1.

$$DIFS = SIFS + (2 \times SlotTime) \qquad 2.1$$

The implementation of DCF mechanism has been proven to be successful for traditional wireless networks, which does not significantly rely on broadcasting messages. Generally, nodes are configured with an address that points to the gateway node, which usually located one hop away from itself. In this way, packets from end nodes can be immediately unicast to the gateway node, e.g. access point, rather than broadcast. On the contrary, nodes in MANET are not typically preconfigured with gateway address. As a result, in order to determine the potential next hop node to which data must be forwarded to, nodes rely on frequent route discovery by way of broadcast packets. Consequently, the RTS/CTS mechanism in such networks can be extremely affected by the interference range [39], resulting in RTS/CTS packet loss. In addition, the reduction in collision occurs at the expense of increased control overhead involved with the exchange of RTS and CTS. The problem is more significant in a short frame transmission [40]. According to previous research work [41], it is recommended that the RTS/CTS packet is exchanged only for a transmission of MAC Protocol Data Unit (MPDU) with a size of greater than 200 byes. The packet size employed in this research work is 512 bytes and as such, the RTS/CTS mechanism can be used without compromising the network throughput.

[4] This is defined as the sum of Receiver-to-Transmitter turnaround time, MAC processing, clear channel assessment (CCA) detect time and air propagation time. The value of slot time for different IEEE 802.11 specification is shown in Table 2.1.

Table 2.1: Inter Frame Spacing (IFS) in different IEEE 802.11 standards [1][42]

Parameters	802.11a	802.11 (Freq. Hopping)	802.11b (Direct Sequence)	802.11b (High rate)
Slot Time (μs)	9	50	20	20
SIFS (μs)	16	28	10	10
DIFS (μs)	34	128	50	50
Data rate (Mbps)	6 to 54	1 and 2	1 and 2	1, 2, 5.5, and 11

2.5 Classification of Routing Protocols in Wireless Ad hoc Networks

This section discusses the main functionality of the network layer; the *routing operation* that is central to this research work. The primary objective of this mechanism is to ensure that data is carried over paths that are predetermined beforehand by routing control packets. In traditional wireless networks, the backbone nodes, i.e. access points, are responsible for directing data from one station to another in a topology that is not really affected by frequent link changes. Unfortunately, the same set of algorithms may not perform as efficiently for wireless multi-hop ad hoc network. Routing in such networks requires flexibility in order to accommodate for constant link breakage, higher nodal mobility and insufficient knowledge of the network topology. For this reason, some protocols require nodes to frequently exchange update messages with the neighbours to maintain connectivity. Others may employ different strategies. Nevertheless, many routing protocols developed for MANETs are typically derived from predecessor protocols and therefore may perhaps share some similar principles and properties.

To date, many routing protocols has been proposed and developed for MANET and therefore, it is not possible to classify all of them based upon a single characteristic. In the following discussion, four typical forms of routing approach are presented along with the examples. As such, the difference between routing protocols can be clearly distinguished. Figure 2.8 shows the classification of routing protocols based four different attributes.

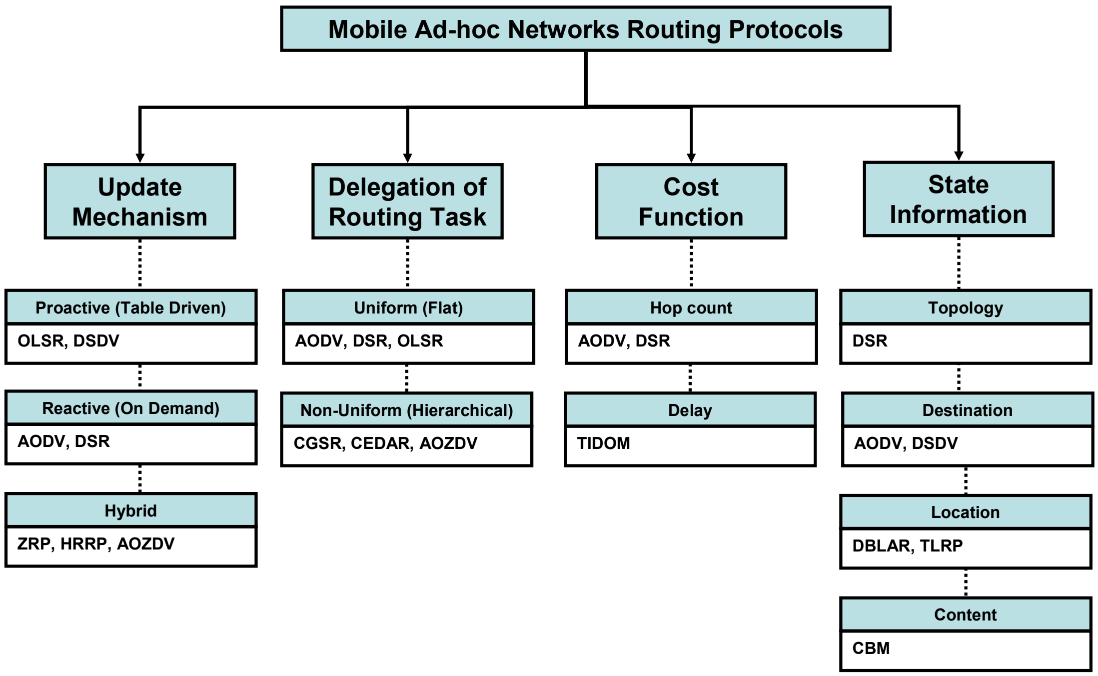


Figure 2.8: Classification of MANET routing protocols

2.5.1 Routing Information Scheduling (Update Mechanism) Based Scheme

A popular way to differentiate routing protocols for MANET is by classifying them according to the routing information scheduling. Generally, routing algorithms are responsible for acquiring and maintaining the routing information gathered by the nodes. Therefore, based on this attribute, routing protocols can be further divided into proactive, reactive and hybrid routing.

A proactive routing protocol is also known as a table-driven approach. With proactive routing, nodes in the network consistently update the path to the destination and/or source nodes. The absence of up-to-date information leads to the disruption of routing path, which triggers the route repair mechanism. In this method, fresh routing paths are maintained by the routing table that stores vital information such as the next hop node, destination node, link expiration, and etc. Consequently, when data is to be transported to destination, a routing path can be rapidly established using the current information obtained from the routing table. In addition, changes to the status of a link can be immediately identified and a new routing path is advertised promptly to all nodes. As a result, route breakage is quickly recovered, leading to minimum data losses. However, the advantages of such technique are at the expense of higher routing overheads. Control packets are disseminated frequently on the network, which consume a large amount of resources, i.e. bandwidth and battery power. Furthermore, the benefits of acquiring the complete network topology by excessive control packets exchanges may not justify the small amount of data packet transported. The proactive method is also severely affected when topology changes occur more frequently and nodes are moving at much higher velocity. Two examples of proactive routing protocols are the Optimised Link State Routing (OLSR) [43] and Destination Sequence Distance Vector (DSDV) [19].

On the contrary, the reactive routing protocol is a less demanding approach compared to the proactive method. The path to the destination node is not known to the sender prior to data transmission. In this technique, nodes collect less routing information, just sufficient to propagate the data packets between the source and destination. Typically, the process of seeking a routing path is by broadcast, performed only if the source node does not have a valid path to forward the data packet. As such, the number of control packets, i.e. routing overhead, is significantly reduced, increasing the network's performance efficiency. However, on the negative side, the reactive approach may not be as responsive as the proactive method. The method may cause a slightly higher delay for the routing path construction. Two types of reactive routing protocol are the Dynamic Source Routing (DSR) [44] and Ad hoc On Demand Distance Vector (AODV) [45].

Finally, a hybrid routing protocol is the combination of attributes from both proactive and reactive routing approaches. The idea is to alleviate the shortcomings of proactive and reactive method by exploiting the hierarchical network architectures. The combination however, resulted in a more complex approach, which may not be feasible for a resource constrained networks such as MANETs. Examples of hybrid routing protocols include An Enhanced AODV Protocol based on Zone Routing (AOZDV) [46] and Hybrid Reactive Routing Protocol (HRRP) [47].

2.5.2 Routing Task Structure and Delegation

MANET routing can also be classified based on the routing structure and routing responsibility. Routing structure can either be *non-uniform* or *uniform*. A non-uniform routing protocol operates differently compared to uniform routing. Some of the nodes may assume explicit routing and management functions, distinguishing them from others. This approach is typically related with a hierarchical network structure, which facilitates node organisation and management. The AOZDV, Cluster-Head Gateway Switch Routing (CGSR) [48] and Core-Extraction Distributed Ad Hoc Routing (CEDAR) [49] are some examples of non-uniform routing protocols.

The AOZDV is a zone based routing protocol, where the network is virtually separated into different zones and each zone is associated with autonomous routing decision. Depending on the design, zones may overlap, allowing nodes to reside in multiple zones. This approach effectively reduces routing overhead because the control packets can be disseminated locally. In order for nodes to reach outside its zone, packets are forwarded to specific node acting as gateway for the inter-zone communication. As such, a node is able to connect to other nodes within the zone at the lowest possible cost compared to the uniform routing approach. CGSR is a cluster based routing protocol. In this approach, the algorithm performs an election process to select the cluster head that is responsible for the membership management and routing function within its cluster. The cluster is a set of mobile nodes grouped together that is similar to the zone based routing protocols. CEDAR is another non-uniform routing protocol that is core-based. The core is typically a set of selected nodes that forms the network backbone. The nodes that are designated as core perform special functions such as routing path construction and control/data packet dissemination.

On the contrary, a uniform routing typically operates over a flat network structure, i.e. single hierarchy network structure. The AODV and DSR are examples of routing protocols that operate using a uniform routing approach.

2.5.3 Cost Function (Routing Metrics)

Routing protocols can also be classified according to the routing metrics used for the routing path computation. A study presented by Baumann [50] provides a comprehensive discussion on the classification of routing metrics. Two common choices of routing metric associated with MANET are hop count and delay. The hop count metric provides a stable and less complex approach for routing decisions, which is practical for a small network. In some cases, the resulting routing path constructed using a hop count metric may not be the optimal. This is a result of the nature of the algorithm, where paths are chosen based on the 'lowest cost[5]' rather than the quality of the link. It is shown previously [51] that the hop count metric tends to choose a routing path which consists of longer hops. As a consequence, the path is more liable to be broken as a result of node movement. Two examples of routing protocols that are reliant on such a metric are AODV and DSR. By contrast, the delay metric is more sophisticated, where delay information is acquired by a passive or active monitoring process using probing packets. Although the metric shows a positive effect in reducing delay [50], such metric however, may not suitable for routing path computation in a network with a high proportion of asymmetrical links. For instance, the unidirectional link delay metric is unable to offer the support to identify unidirectional link and subsequently avoid computing a routing path via such links. Other examples of metric employed by routing protocols are based on the number of periodic messages received, power aware routing, and expected transmission time.

---

[5] The lowest cost of route is calculated based on the routing metrics. Depending on the routing metric, the lowest cost of a route may be represented by the lowest hop count, lowest delay, etc.

2.5.4 State Information

Another classification of routing protocols is based upon the state information. Four routing strategies under this category are topology based, destination based, location based, and content based.

In topology based schemes, nodes continuously collect network information in order to generate a complete network topology. When data needs to be sent, routing decisions can be executed quickly to construct path from source to destination. On the contrary, nodes using a destination based routing strategy have access only to valid next hop nodes when relaying packet to destination. DSR is an example of a topology based scheme, whereas AODV and DSDV are destination based routing schemes. Location based routing typically depends on the availability of location positioning system such as Global Positioning System (GPS) or Local Positioning System (LPS). Thus, nodes are able to access the geographical information from positioning system in order to assist routing. In this approach, the relative distance and velocity of a sender node to a receiver can be accurately computed. Two examples of location based routing are Distance-based Location Aided Routing (DBLAR) [52] and Tree-shape Location-based Routing Protocol (TLRP) [53]. In the former, nodes send packets based solely on the location information without the need for any additional information from the nodes. The latter scheme uses both location information and topology information to assist routing operation. Finally, routing can also be constructed based on the content, i.e., content based routing. The technique is typically employed in some mobile network that conveniently supports anonymous communication. An example of this scheme is Content Based Multicast (CBM) [54].

Table 2.2 shows the summary of routing protocols previously discussed in this section. The subsequent sections introduce four routing protocols frequently discussed in connection with MANETs; each being a unique or having a common characteristics shared between the categories as shown in Figure 2.8. The routing protocols considered are OLSR, DSR, and AODV with the latter forming the basis for the development of the proposed scheme in this work.

Table 2.2: Summary of the characteristics of routing protocols

Routing protocol	Main attribute
OLSR (Optimised Link State Routing) [43]	Some of the nodes are designated as a MPR (multipoint relay), providing support for message forwarding between mobile stations.
DSDV (Destination Sequenced Distance Vector) [19]	The DSDV reduces the routing loop problem by using destination sequence number.
AODV (Ad hoc On-demand Distance Vector) [45]	AODV shares the DSDV's sequence numbering but reactively maintains the routing table, i.e. on-demand routing.
DSR (Dynamic Source Routing) [44]	DSR is based on the concept of source routing and mobile nodes are required to maintain route caches that contain the source routes of which the mobile is aware.
AOZDV (An Enhanced AODV Protocol based on Zone Routing) [46]	The AOZDV creates a zone using traffic and power information, and it utilizes a destination-vector table for internal-zone routing.
HRRP (Hybrid Reactive Routing Protocol) [47]	HRRP combines the attribute of AODV and Epidemic routing.
CGSR (Cluster-head Gateway Switch Routing) [48]	CGSR elects cluster-heads that are responsible for membership management and routing within the cluster.
CEDAR (Core-Extraction Distributed Ad hoc Routing) [49]	CEDAR forms a core network, which requires a special role for the nodes, which are part of the core.
DBLAR (Distance-based Location Aided Routing) [52]	The DBLAR relies on location information computed based on the distance to reduce the request zone, leading to a smaller routing overhead.
TLRP (Tree-shape Location-based Routing Protocol) [53]	An important element in TLRP is the tree shape approach to make decision for route request forwarding.
CBM (Content Based Multicast) [54]	In CBM, the content of the multicast data determines the set of destination nodes, which can be dynamically varied as the content of the multicast changes.

The following sections discuss three commonly used routing protocols: AODV, DSR, and OLSR. The AODV and DSR are reactive schemes whereas OLSR is proactive. A summary of comparison between proactive and reactive approaches is presented in Table 2.3.

Table 2.3: Summary of differences between proactive and reactive schemes

Parameters	Proactive (table-driven)	Reactive (on-demand)
Route availability	Always available irrespective of need	Computed when needed
Routing philosophy	Flat	Flat
Periodic updates	Always required	Not required
Handling mobility	Updates occur at regular intervals	Use localised route discovery
Control traffic generated	Usually higher than on-demand	Increases with mobility of active routes
Storage requirements	Higher than on-demand	Depends on the number of routes maintained or needed
Delay	Small as routes are predetermined	High as routes are computed when needed
Scalability	Usually up to 100 nodes	Usually higher than table-driven

2.5.5 Optimised Link State Routing (OLSR)

The OLSR is a proactive routing protocol and the key mechanisms in its operation rely on the link state and the uniform approaches. Indeed, the traditional link state method such as in Open Shortest Path First (OSPF) [55] can cause a protocol in MANET to incur a higher communication overhead. To reduce such impact, the link state process in OLSR is optimised by using the multipoint relay (MPR) strategy, as shown in Figure 2.9. The optimisation is two-stage. Firstly, the size of link state message is minimised by including only the MPR selectors (nodes) in the advertised control packet. Secondly, nodes that are not designated as MPR is prevented from generating link state messages, resulting in fewer broadcast packet transmissions.

During the initial topology update, each node detects its neighbours via the HELLO message; periodically sent to other nodes in the network. The neighbour nodes respond by broadcasting another HELLO message that includes the information about its neighbours and their link status. The HELLO message propagates to all nodes that are within a distance of one-hop from the sender, where it then terminates. Based upon the routing information in the HELLO messages, each node updates the knowledge about its one-hop and two-hop neighbours, which then is recorded in the node's neighbour table. Subsequently, the node computes a set of one-hop neighbour nodes, called the MPR nodes, which offers the best access (shortest path) to its two-hop neighbour nodes. As a result, every two-hop neighbours' node information is aggregated into the neighbour table of the MPRs. The node then declares the MPRs to its neighbours in the subsequent HELLO messages.

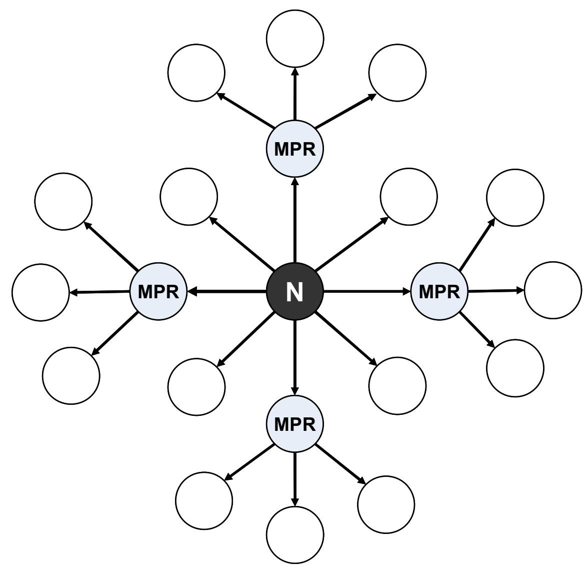


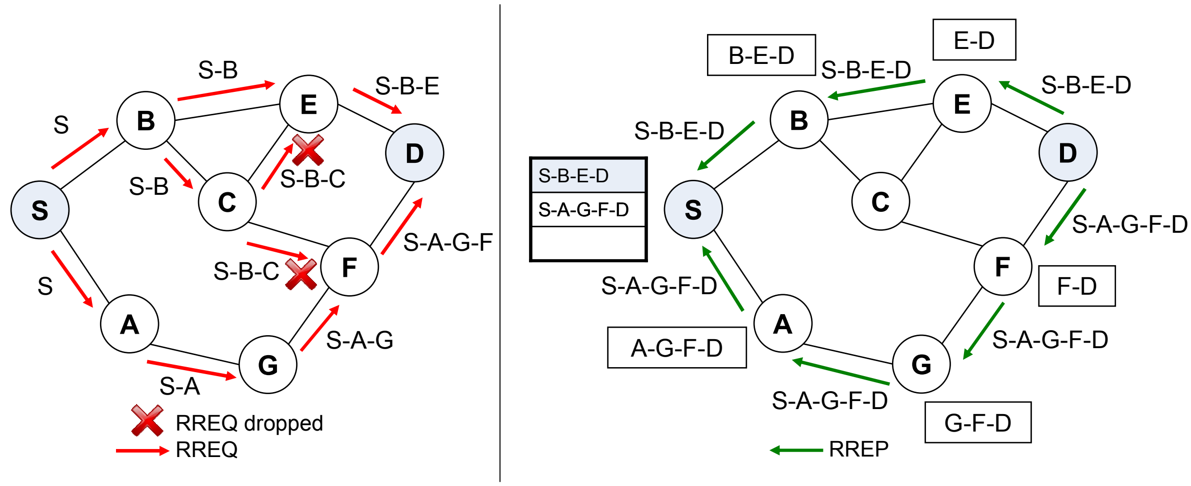
Figure 2.9: Multi point relay in OLSR

Nonetheless, the MPR selection strategy strictly requires bidirectional connectivity between the source and the neighbours and therefore, may not perform as expected in a network with a high unidirectional link presence. As such, the OLSR protocol is deemed efficient only when operated in a densely connected network and that has a sufficient capacity in order to send and receive the topology updates messages. Another downside of OLSR pertains to the size of routing table it must maintain. As a proactive approach, each node must record and update all possible routes in the routing table, including the routes to node that are not needed. The impact of routing overhead may not be noticeable for a small network. However, as the network expands, the number of control messages increases, which in turn constraints the network's scalability.

2.5.6 Dynamic Source Routing (DSR)

The DSR is a reactive routing protocol but differs to AODV in many ways. As shown in Figure 2.8, DSR can be further categorised as topology based as opposed to AODV, which is destination based. In DSR routing, the source node appends the complete routing path to each data packet before transmitting. Additionally, each node uses a caching technique to maintain the route information. Generally, routing construction in DSR comprises two major phases; the route discovery and the route maintenance. Prior to sending data packets, a source node consults the route cache to determine the path availability to the destination. If a valid routing path exists, it will be included inside the data packet, and if not, the source node invokes the route discovery by broadcast a route request (RREQ) packet as shown in Figure 2.10a. A RREQ packet is distinguished by using a unique number along with the address of both the source and destination. At every intermediate node, the received RREQ packet is compared against the route cache to match the route information for the destination. If such information is not available or has not been previously determined, the node appends its own address to the route record field of the RREQ before forwarding to its neighbours.

The communication overhead is reduced by removing duplicate RREQ packet and concatenating route information at intermediate nodes. Duplicate packets are prevented from being propagated if the RREQ contents matches the destination address appeared in the node's route cache. When the RREQ packet reaches the intended destination or an intermediate node that has valid path to the destination, a route reply (RREP) packet is generated and returned, as shown in Figure 2.10b. The content of a RREP packet typically comprises the complete list of address in which the RREQ packet has traversed through. If the source of RREP is an intermediate node instead of the destination node, the address installed in the RREP is the list of nodes address traversed concatenated with the address from the intermediate node's cache.



(a) Route discovery (b) Route reply

Figure 2.10: Dynamic Source Routing route construction procedure

There are three possible paths that can be followed by the RREP packet back to the source node. The first case is the destination or intermediate node already has a predetermined route to the source node in its route cache. Second and the most common method is in a reverse manner, to follow the path list in the route record field, assuming that the path between the pair of source and destination consists solely of symmetrical links. The third possibility is that there may be potential asymmetrical links along the routing path. In such cases, the RREP packet propagation is lost and a new route discovery is initiated to find another route to the source by the destination node. The RREP packet is piggybacked on the RREQ (by the destination node) and broadcast to the neighbours. During route maintenance, a routing path breakage is typically handled by the source node. When the data link layer detects link disconnection, a ROUTE_ERROR packet that reversely follows the list of path in the route cache is unicast back to the source node. At each node, all routes associated with the broken links are removed from the route cache.

The DSR routing protocol is extremely efficient in a small network. However, as the network expands, i.e. by increasing the number of nodes, the routing's performance can be substantially affected [56]. The degradation occurs because each node includes in every transmitted packet the complete routing path to the destination; leading to overall higher packet sizes.

2.5.7 Ad hoc On Demand Distance Vector Routing Protocol (AODV)

AODV is a reactive unicast routing protocol that is simple, and efficiently handles packet propagation in a dynamic MANET environment. The algorithm is motivated by bandwidth deficiency and frequent mobility in wireless communications. Many of its advantageous concepts are borrowed from DSR and DSDV. The on-demand route discovery is based on hop-by-hop routing that follows the DSR approach, whereas the route maintenance and topology updates use a sequence number, similar to DSDV.

In this protocol, the algorithm maintains the routing information only about the active paths, stored in the routing table at each node. Every node looks up the routing table to determine the next hop node towards the destination before forwarding a packet. Vital information that keeps the routing table valid is the route entry expiry timer. If the route towards the destination has not been used or reactivated before the timer expires, that particular route entry is deemed invalid and removed from the node's routing table. Furthermore, the destination sequence number is utilised as on-demand, unlike DSDV where it is received regularly by every node at every interval and when the topology changes.

Another important feature for AODV is the route management through caching scheme. A node maintains cache information in order to keep track of the RREQ packets it has received and as well as to store the paths pointing back to the originator of RREQ packet. A RREQ packet is deemed fresh if the new destination sequence number is at least equal or greater than the value indicated in previous RREQ packet. A node (either the destination or intermediate node) that receives a fresh RREQ packet replies with a RREP packet. The RREP packet is propagated in reverse, along the forward path created by the RREQ packet, resulting in symmetrical routing path between the source and destination.

Along the reverse path, each intermediate node updates its routing table entry, adding information such as next-hop node and hop count with respect to the destination node.

The neighbour status update in AODV is either periodically sent or on demand. As for periodic update, a HELLO message is sent from a node to neighbours to notify its existence. This way, the status of link to the next hop is actively monitored although it generates more traffic packet. On the other hand, the AODV also allows a node to passively monitor the link using the data link layer message feedback. When a particular node discovers that an active link along the route has been disconnected or unavailable for communication, it either repairs the route locally or broadcasts a route error (RERR) packet. The local repair is invoked if it is deemed that the point of failure along the route is closer to the destination than to the source. Otherwise, the node releases a broadcast RERR packet to its neighbours. As a result, every node that receives the RERR propagates the packet (by way of unicast) to all intermediate nodes whose routes may be affected by the disconnected link. Upon reception of RERR, the source node will then reinitiate another route discovery operation if it still has data to be transmitted.

2.6 Summary

In this chapter, a review of three different wireless multi-hop network are presented, where the MANET in particular, being the focus of the research work. Despite the differences, these networks share common attributes that includes dynamic topology, infrastructure-less, resource constraints, and scalability issue. Four MANET properties pertinent to the scope of this research are also discussed, which is the network topology, nodal mobility, physical layer, and data link layer. These are basically the major elements in MANET that must be considered in the design of routing protocol. Chapter 3 presents more detail on the network topology and nodal mobility using several different mobility models. A brief introduction on the unidirectional link is provided, which subsequently forms the major discussion in the subsequent sections.

Several types of MANET routing protocols are presented and categorised according to different their approaches. The classification of routing protocols can be based on routing information scheduling, routing task structure and delegation, cost function, and state information. The key operation of each routing protocols are discussed in relation to the classification presented, with AODV being the candidate as the reference protocol that will be compared to the proposed scheme in this work. Chapter 3 presents more details on AODV routing protocol and evaluation methodology used in the simulation experiment.

3. Routing Protocols and Evaluation Methodology

3.1 Introduction

The wireless ad hoc networks of today can be considered as *heterogeneous* networks, where every node may not have identical radio interface specification. The nodes are wireless-enabled devices and can carry data, voice and video over unreliable and with bandwidth constraint links [57]. Each network can be seen as an autonomous system designed and configured with a particular routing protocol that operates under exclusive network conditions. In a densely connected network, most routing protocols typically incur low transmission delay, higher success of packet transmission and low link breakages. On the other hand, routing in a sparsely connected network is more complex, which requires the routing algorithm to be more efficient in order to adapt to low link connectivity. The underlying research work focuses on two extreme cases of network topologies, which are the bidirectional and unidirectional link routing strategies.

In many cases, routing on ad hoc wireless network is based on the availability of bidirectional and symmetrical links. Therefore, the absence of such links may prohibit the proper operation of a routing protocol, particularly the reactive routing method. It is because nodes in such routing schemes typically discover routes by broadcasting and the failure to setup routing path via bidirectional links can cause multiple broadcasts. In addition, nodes in a non topology-based routing protocol such as AODV, typically possesses little information about the complete topology. As such, broadcast packets may follow asymmetrical paths, and consequently a routing path that is unidirectional may be constructed.

Chapter 3 is organised as follows. Section 3.2 introduces the operation of AODV routing protocol. First, the basic mechanism of routing construction is discussed, followed by the overview of the unidirectional link avoidance mechanism, known as AODV with blacklist [45] technique. Section 3.3 highlights the benefit and presents the common techniques employed by routing protocols to handle unidirectional links. Some of the techniques are also briefly explained in the related work. Section 3.4 discusses the performance evaluation methodology and the description of simulation tool is presented in section 3.5. Comprehensive simulation modelling is discussed in section 3.6.

3.2 Route Establishment with Bidirectional Link

This section provides detailed discussion of AODV to enhance section 2.5.7, which simply presented a general description of the routing operation. Two cases of routing operations are presented, first is the basic routing mechanism and second, the operation with unidirectional link detection. Typically, AODV relies upon the bidirectional link availability between nodes, an important property that ensures the correct operation of the routing protocol. At least one single bidirectional path between the source and the destination must exist, otherwise the routing protocol may not function properly and connections between node pairs will not be able to be made.

3.2.1 Basic AODV Routing Technique

As shown in Figure 2.1b, the IEEE 802.11 architecture supports an ad hoc mode, facilitated by the IBSS. In this mode, devices that perform a specific AP function are eliminated and replaced by mobile stations, where each station communicates directly with each other, i.e. single-hop communication within a limited range. To enable multi-hop communication, shown in Figure 2.1c, every node in the network must be enabled with a MANET routing protocol, e.g., AODV. Despite the differences in terms of routing functionality, the same set of underlying link layer protocols, i.e. CSMA/CA and RTS/CTS, typically remain unchanged.

In AODV, a source node first will attempt to communicate with an identified destination by comparing the destination address with the content of its routing table. If a match is found and the address is valid, the source node immediately forwards the data packets through the wireless interface. However, if a matching address is not available or has been stored but the state information is invalid, the source node initiates a route discovery by using the *expanding ring search* algorithm. In this algorithm, the source node searches for the destination node using the multiple ring method, as opposed to the simple flooding technique. The ring radius is set by the time-to-live (TTL) value, which in return defines the distance, i.e. number of hops, the packet propagates away from the source node. In this technique, the TTL value is set to an initial start value of 3[6] with increment of 2, resulting in a linear expansion of the ring radius. Nevertheless, in a worst case scenario, wherein the searches exceeded the threshold value (7), the AODV simply reverts to the simple flooding method. The default limit of flooding attempts is 3 [45]. If a node fails to obtain a RREP up to the maximum threshold, the source node timeouts with MAX_RREQ_TIMEOUT, after which the route discovery process is repeated. In this way, the number of broadcast packets is significantly reduced, leading to lower communication overheads.

The RREQ packet contains information such as source node ID, hop-count towards source node, sequence number to identify the freshness of packet, packet lifetime and a time-stamp to compute the route latency. RREQ packet is forwarded (using broadcast) towards its destination, where each node along the path caches the first copy of received RREQ by recording the Broadcast ID (BID) and Source ID (SID). If any subsequent RREQ received matches the cache, that RREQ packet will be dropped. Each node maintains a routing table, which records only the most recent information from RREQs by comparing them to the stored sequence number and hop count. The algorithm in Figure 3.1 shows the process flow at every node that checks for route freshness and eliminates duplicate received RREQ packet.

[6] The value is specified by the parameter TTL_START in *RFC 3561*, which have initial value of 1. The value 3 is selected in this thesis to minimise the number of RREQ attempt.

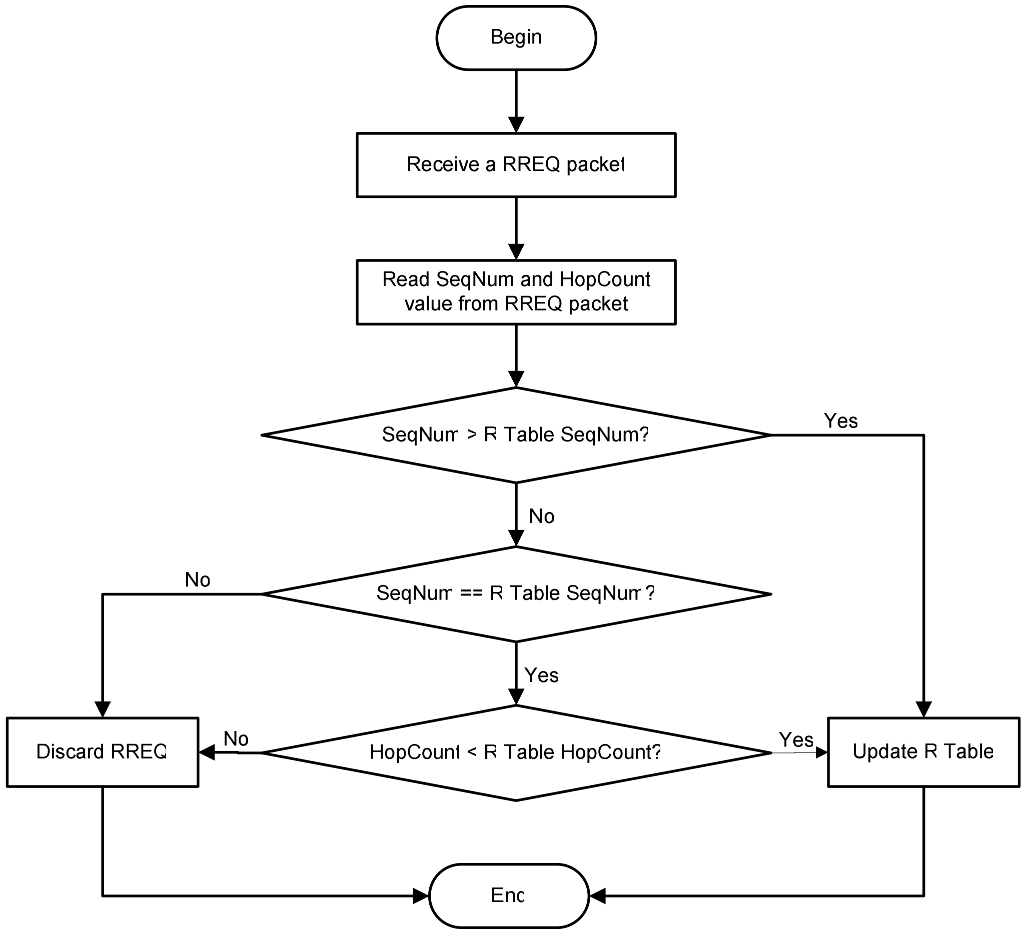


Figure 3.1: RREQ route freshness inspection procedure

If all links in the network are bidirectional, AODV guarantees that, based on the above algorithm, the routing path created between the source and the destination will be the shortest hop with lowest delay. However, depending on network condition, constructing routes solely through bidirectional link may not be possible. As such, if nodes are unable to find at least a single bidirectional link between the source and destination pair, the AODV scheme may fail to function.

3.2.2 Unidirectional Link Detection and Avoidance (AODV-Blacklist)

In the presence of unidirectional links, the basic AODV routing path construction can produce a sub-optimal network performance. For example, a network with low nodal density and a large number of unidirectional links may possess a higher probability of setting up a forward route, i.e. from source to destination, through unidirectional links. As a result, the RREP packet may fail to reach the source node using the reverse of the forward route created by RREQ.

Refer to Figure 3.2, where node **S** is the source and node **D** is the destination. The RREQ packet from **S** is assumed to reach **D** through path **S-A-E-D**. The link (**A-E**) is unidirectional, pointing to node **E**. Assuming that nodes are moving at a relatively low speed, route discovery may fail to constructs a reverse route from **D** to **S**. This is because node **E** is able to receive packets from **A**, but not vice versa, even though **E** has established a reverse route with **A** as the next hop candidate to reach **S**. Further attempts of RREQ broadcast by the source node will likely produce a similar result, hence increasing the overall routing overhead.

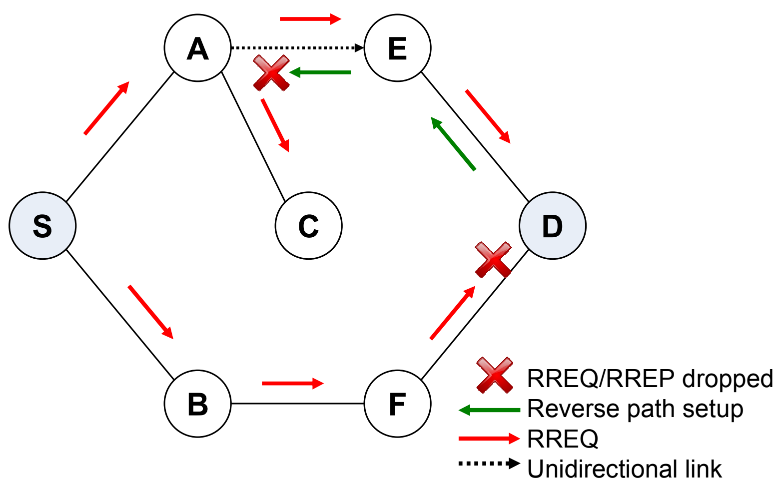


Figure 3.2: Unidirectional link facing to node **E** from **A**

On the contrary, the AODV-Blacklist routing scheme implements a unidirectional link detection and avoidance mechanism. In this scheme, a network ACK packet is returned for each RREP received, i.e. originated or forwarded by a node. For instance, in Figure 3.2, as soon as node **E** transmits a RREP packet to node **A**, it expects an immediate reply of ACK packet. However, a failure to receive an ACK packet, upon timeout, will cause node **E** to cache **A** in its blacklist set and remove the current entry towards **A** from its routing table. The system then waits for further attempts of RREQ discovery by the source. Node **E**, upon receiving another fresh copy of RREQ from node **A**, will discard the packet because the node has been blacklisted. This allows the forward route to be constructed via a different path, e.g. **S-B-F-D**, after another route discovery process.

The AODV-Blacklist scheme is an efficient unidirectional link avoidance technique when there are only a few unidirectional links within the network. However, when the number of nodes increases along with the number of link connections between them, the system may generate more unidirectional links. As such, the chances of creating a forward path via such link is high, which can lead to a failure on the first route discovery attempt. The source node then may have to perform several rounds of route broadcast until all bidirectional links are found. Consequently, a higher routing overhead is incurred and the route acquisition delay is substantially increased, leading to deterioration in network performance.

3.3 Routing Operation in the Presence of Unidirectional Link

Routing schemes that support control and data packet forwarding over unidirectional links [58][59][60] have been shown to alleviate the problems associated with routing exclusively with bidirectional links. Some researchers, however, implied that routing data packets along asymmetrical and unidirectional links between a pair of source and destination nodes is inefficient and the gain from such approach is small [35][61]. This is typically caused by the additional control packets required for route discovery, leading to a higher routing overhead. Taking this into account, one of the schemes proposed in this thesis (Chapter 5) are designed to allow routes to be discovered by means of unidirectional link but at the same time, constrain data forwarding to solely using bidirectional and symmetrical connections. Additionally, the proposed schemes are protocol independent and, as such, can be integrated with any routing protocol that shares general principles associated with the root underlying AODV protocol.

3.3.1 Occurrence and the Impact of Unidirectional Link

There are many reasons for occurrences of unidirectional links and their presence in the network may substantially affect the performance of a system that relies exclusively on the availability of bidirectional link.

The characteristics of radio links in wireless communication are typically a manifestation of the effects of signal propagation. Transmitter-receiver separation distance, transmitting power, antenna gain and SINR sensitivity affect the link connectivity. Ideally, a wireless communication path should be symmetrical and bidirectional between the two end stations, however, this is not always the case in MANETs. At the data link layer, the presence of unidirectional link causes problem for efficient path construction. Consequently, when a node establishes a unidirectional path to a neighbour node through a unidirectional link, the acknowledgement packet is not possible to be returned back to the sender node via the reverse route. As a result, conventional methods of packet flow control and reliability mechanism to avoid hidden nodes, such as RTS/CTS, lose effectiveness. The problem is more severe on a sparsely connected network compared to a dense network. Although increasing the distribution of nodes over the network may potentially reduce the impact of unidirectional links, the approach could, however, result in looping and broadcast storms.

Two common causes of the occurrences of unidirectional link are discussed. The first is the hidden node problem, which is illustrated in Figure 2.4. Typically, unidirectional links caused by such a phenomenon is often transient, and may disappear as soon as the high interference surrounding the sender node is reduced. However, irrespective of whether the condition is temporary or persistent, the path is asymmetrical and the formed routing path may be unidirectional.

Secondly, unidirectional links can be the result of the radio transmission power difference between adjacent nodes. In Figure 3.3, the transmitting power of node **Y** and **X** is initially set to a higher radio transmission energy level. However, due to excessive local utilisation, i.e., caused by frequent routing and forwarding processing, the energy level at node **X** is significantly decreased. In addition, if node **X** operates on a power-aware routing technique, the impact of energy depletion can cause a substantial decrease in transmitting power. Therefore, in order to conserve the energy, node **X** may choose to transmit packets with a lower radio energy level and the packets emitted from node **X** may not reach node **Y**. As a result, a unidirectional link facing to node **X** is created. In this example, the creation of such link, which is the main focus of discussion in this work, may be permanent.

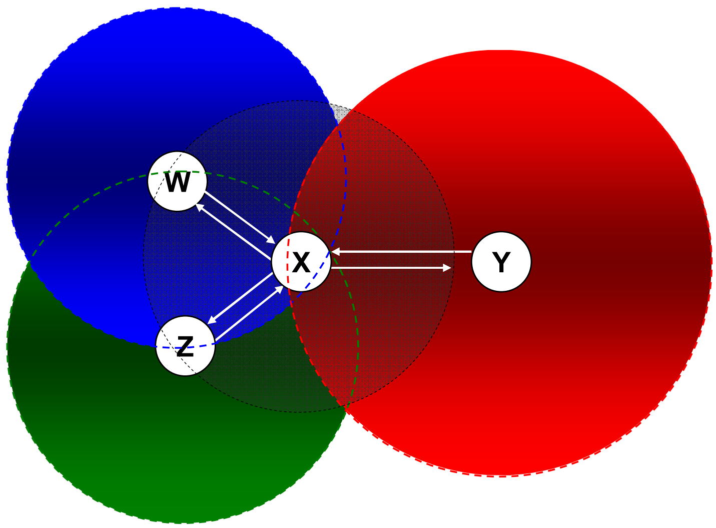


Figure 3.3: Permanent unidirectional link between node **X** and **Y**

3.3.2 Components of Routing with Unidirectional Link

This section discusses the main processes that are commonly adopted to handle unidirectional links.

3.3.2.1 Detection

The most basic component that constitutes any routing protocol to deal with unidirectional link is the detection method. For AODV, unidirectional link detection is implemented by the network layer. Each node broadcasts a HELLO message at every specific interval set by the AODV parameters. This control packet is exchanged only between adjacent nodes, controlled by TTL set to 1. The HELLO message typically contains the list of neighbours from which the node is currently receiving HELLO messages. Subsequently, based on the information gathered, if the node ID is not present within the neighbour list received from the other node, the node may safely assume that it is on the receiving side of a unidirectional link. Another detection approach is to use the ACK packet as a response for each RREP packet sent. For every ACK packet returned by the receiver, the sender node concludes that the link is bidirectional and symmetrical. On the other hand, the absence of ACK packet is an indication that the link is potentially unidirectional. The failure to receive ACK packet may also signify that the link is severely congested. The method is simple and does not significantly affect the routing overhead since an ACK packet is generated only in respond to the unicast RREP packet.

3.3.2.2 Avoidance

The next step after detection process is to decide whether to avoid or utilise the unidirectional link to advantage. The former method (avoid) completely prohibits forwarding any packet (control and data packet) via unidirectional link, which is the common method used by most routing protocols [35][45][62][63]. For instance, AODV-Blacklist avoids using unidirectional link, achieved by storing such links in a blacklist database. The content of blacklist database is retained only for a very short duration; typically only until the current route discovery cycle is completed. Nodes that are stored in the blacklist database are consulted by a receiver node each time a RREQ packet is to be forwarded to the next hop node. If the node ID stored in the blacklist database matches the next hop node ID field in the current RREQ packet, the packet is dropped. The system then waits for the source node to timeout before another round of route discovery is attempted. Although the technique enables AODV nodes to correctly identify paths that are unidirectional and avoids them, it has drawbacks. With the blacklist method, the number of possible link connections for routing construction is limited, when it excludes communication to nodes that can be reached via only unidirectional links. In addition, the method may introduce additional latency for route discovery since the RREPs sent over the partially constructed routes can be potentially dropped and cause timeouts at the source node.

3.3.2.3 Exploit

The exploit approach differs from the above method, where unidirectional link is utilised to advantage. Generally, there are two ways to utilise such link. First, the routing protocol temporarily allows the control/routing packet to be forwarded through all links, irrespective of whether the link is unidirectional or not. For instance, in the reverse path search (RPS) [35] scheme; when a link is detected unidirectional, the propagation of RREP packet through the reverse path is not dropped. Alternatively, the packet is forwarded via alternate paths and if such a route is not present in the node cache, a broadcast packet called backtrack route reply (BRREP) is transmitted to the upstream nodes, i.e. facing destination node. Subsequently, the upstream node removes the current reverse link and attempts to re-route the RREP through other available links. Figure 3.4, Figure 3.5, and Figure 3.6 illustrate the process of RPS.

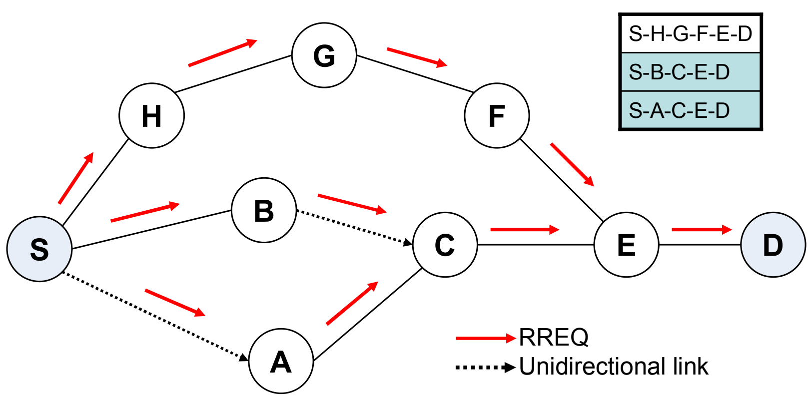


Figure 3.4: Paths are created via unidirectional links at **B-C** and **S-A**

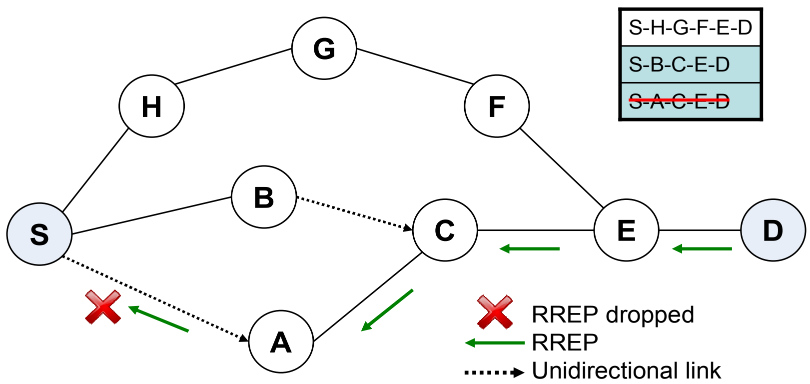


Figure 3.5: The first reverse path creation fails via **D-E-C-A-S**

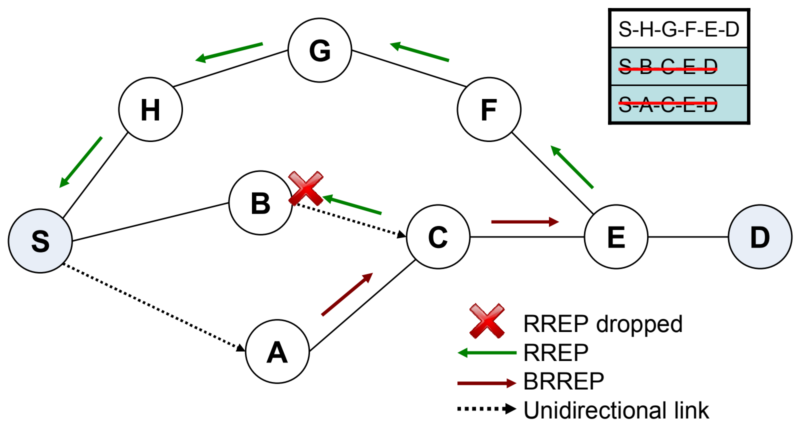


Figure 3.6: The second reverse path creation fails via **D-E-C-B-S**

The second approach allows the unidirectional link to be fully exploited during route discovery and these links then also utilised for data packet transmission. This approach is able to handle the asymmetrical characteristics of the network. An example of such an approach is the Bidirectional Routing Abstraction (BRA) [58]. Although the scheme is protocol independent, significant changes to the underlying routing principles must be made to any routing protocol before such technique can be adopted. In addition, the scheme optimises the routing efficiency by supporting asymmetric links only in the area of network where the connectivity is poor.

3.3.3 Related Work

A wide variety of routing protocols have been proposed for MANETs. However, many simply ignore the presence of unidirectional links in the network. As such, the implementation of these schemes often exhibits connectivity issues, affecting the network performance. To counter the inherently unreliable effect of unidirectional links, several schemes have been proposed.

3.3.3.1 Early Unidirectional Link Detection and Avoidance (EUDA)

In contrast to the blacklist method, the Early Unidirectional Link Detection and Avoidance (EUDA) [63] is a proactive technique. A node detects unidirectional link as soon as it receives a RREQ packet during the route discovery phase. Basically, when a node receives a RREQ from a neighbour, the node computes an estimated distance towards the sender using the information carried within the RREQ packets. The estimated distance is then compared against the radio transmission range, which is set at the highest radio signal strength. If the distance between the sender and receiver is greater than the maximum transmission range, the link is considered unidirectional. As a result, the received RREQ packet is dropped. On the other hand, the link is considered bidirectional if the estimated distance is equal to or smaller than the receiver nodes transmission range. Like AODV, this scheme detects duplicate RREQ packets. On receiving a RREQ packet, a node compares the sequence number attached to the packet and compares it to the current sequence number recorded in its entries. If the node has previously forwarded the packet with a match <*source, sequence number*> entry, the packet is immediately discarded.

The scheme can be described using the network scenario in Figure 3.2. When node **E** receives a RREQ packet from node **A**, the scheme provides an estimated distance of node **A** relative to node **E**. Based on the computed distance, node **E** realises that node **A** lies outside its radio transmission range. As a result, the RREQ packet from node **A** is dropped. Subsequently, node **E** may receives another copy of RREQ packet from node

C and by using similar approach, the link is immediately determined as bidirectional. The packet is then forwarded to the final destination node **D**, which responds with a RREP packet that follows the reverse path <**D-E-C-A-S**>. The scheme can rapidly construct routes by using paths that are solely bidirectional; only if there exists at least one such route between the source and destination node. Nevertheless, if the condition is not met, the scheme may not able to construct the route and the source re-broadcasts the RREQ with new sequence number.

The scheme is built upon the typical theoretical two-ray ground wireless channel propagation model to compute the estimated distance, e.g., distance **A-E**. The received power is given by equation 3.1.

$$P_r = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4} \tag{3.1}$$

Based on the equation, the arbitrary transmitter-receiver separation distance, d, can be calculated if the transmitted and received power, P_t and P_r, is known, along with all other variables in the equation 3.2. The G_t and G_r are the transmitter and receiver gain, while h_t and h_r are the transmitter and receiver height, respectively.

$$d = \sqrt[4]{\frac{P_t G_t G_r h_t^2 h_r^2}{P_r}} \tag{3.2}$$

To enable the receiver node to compute the distance, the sender node includes specific information into the RREQ packet field, i.e. P_t and *RXThresh*. Other parameters, i.e. G_t, G_r, h_t, and h_r, are assumed identical across the system and therefore not significant for the purpose of distance computation. An issue with EUDA approach is that nodes are assumed to operate at highest radio power, which results in a maximum transmission range. Such conditions are rarely possible in real world scenarios. Several factors may significantly vary the node's communication range such as obstacles, fading, and interference. The scheme also attempts to improve the accuracy of distance estimation, by considering more realistic parameters such as channel gain, receiver sensitivity, and the receiver's SINR in the unidirectional link detection process. The parameters are shown in equations 3.3 and 3.4.

$$G_{x,y} = \frac{P_r(y)}{P_t(x)} \tag{3.3}$$

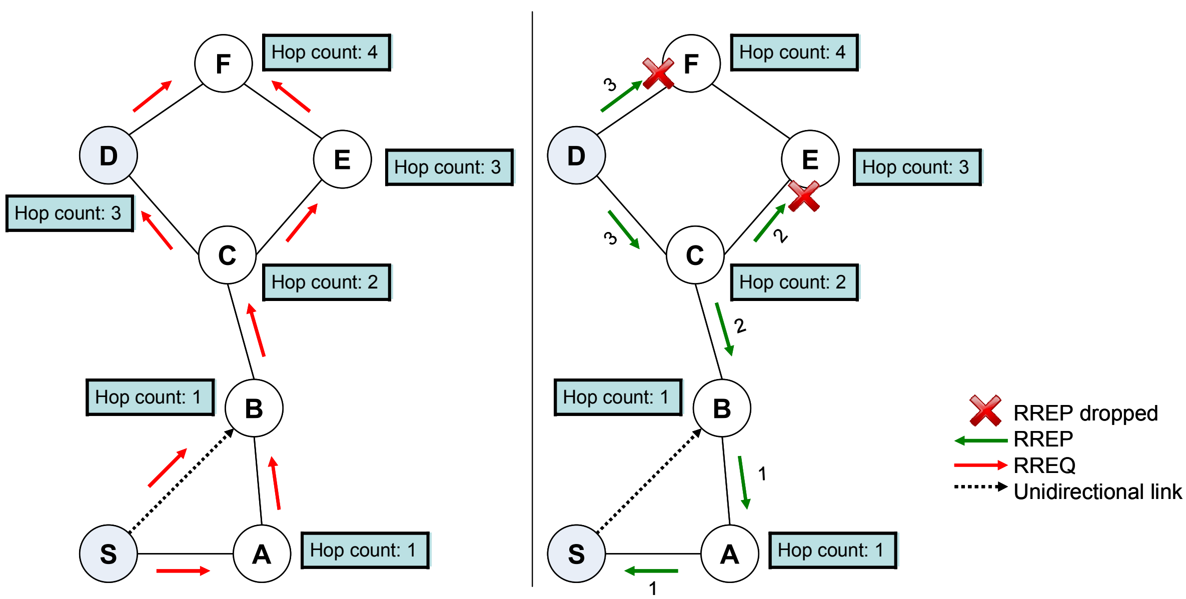
$$SINR_x = \frac{G_{x,y} \times P_t(y)}{P_n(x)} > SINR\_Thresh_x \tag{3.4}$$

Assume that node *y* is the receiver and node *x* is the sender. Three additional fields are introduced in the RREQ packet, i.e., $P_t(x)$, the accumulated noise observed at node x, $P_n(x)$, and $SINR\_Thresh_x$. Based on equation 3.3, node *y* computes the gain $G_{x,y}$, where $P_r(y)$ is measured by the node's physical layer. Assuming identical gain on both the receiver and sender sides, the computed SINR at node *x* is compared against the $SINR\_Thresh_x$. Basically, when a node receives a RREQ packet and the information advertised satisfies equation 3.4, the link is considered bidirectional. Despite the rapid detection of unidirectional link compared to the AODV-Blacklist, the scheme suffers from higher routing overheads as a result of the RREQ packet size increase.

3.3.3.2 Ad hoc Routing Protocol with Flooding Control using Unidirectional Links

The scheme [64] is based on DSR routing protocol that employs a two-way broadcast system, i.e. forward and reverse discovery. On the contrary, the AODV routing protocol broadcast employs a one-way control packet broadcast, which floods RREQ only during the forward path discovery. During the forward path broadcast discovery, each node records the number of hops it is from the source. On the reverse broadcast discovery phase, the recorded hop count is compared against the reverse hop count, where each node then decides whether to allow the propagation of packet or to discard them. Results shown in the paper indicate that the scheme is able to find routes around the unidirectional link and consistently reduces the number of control packets in all experiments. The scheme achieves this by restricting the flooding area of RREP packets during the backward path discovery.

The scheme's general operation can be illustrated by Figure 3.7. Initially, the source node, **S**, does not have a path to the destination node, **D**, and it searches for the best route by broadcast the RREQ packet. The route discovered between **S** and **D** includes a unidirectional link, facing to node **B** from **S**. The area of broadcast by the RREQ packet shown in the Figure 3.7a is similar to any traditional on-demand routing protocols that rely on packet flooding technique, e.g., AODV, DSDV, and DSR. At each node along the path, the hop count information from the source is recorded; extracted from the TTL associated with the RREQ packet.



(a) Route discovery (b) Route reply

Figure 3.7: Unidirectional link (**S-B**) is avoided on reverse route computation

Upon completion of the forward broadcast phase, the first RREQ packet reaches **D** from path (**S-B-C-D**) with 3 hop counts. Instead of being reversely unicast, the RREP packet is broadcast back to the source (Figure 3.7b). As such, the reverse route followed by the

RREP packet may be different than the previously constructed forward route and may forms an asymmetrical route. However, before broadcast, node **D** includes the recorded hop count, i.e. 3, in the RREP packet. Subsequently, node **F** and **C** receives the RREP packet, where each node compares the hop count advertised by the RREP against the recorded hop count in its cache. If the advertised hop count is higher, the packet is relayed, otherwise it is dropped. As shown in Figure 3.7b, node **C** replaces the advertised hop count (3) with its recorded hop count value (2), whereas node **F** drops the RREP. At node **C**, the RREP is rebroadcast and subsequently received by node **E** and **B**. The same process is then repeated. When the advertised hop count is equal to the recorded value, i.e. at node **A**, the RREP propagation is paused for a short duration of time. The waiting time is necessary to allow for other RREP packet with shorter hops to reach **S** ahead of the RREP packet from node **A**. For instance, if the link (**S-B**) changes to bidirectional, the RREP packet relayed by node **B** to **S** will have a higher priority. After the time-out, the RREP is finally broadcast to **S**. The final route constructed by the scheme follows the path (**D-C-B-A-S**).

The proposed scheme is able to reduce the control packet traffic by limiting the area of broadcasts, resulting in lower routing overheads compared to DSR. However, routes formed between the source and destination pairs may be asymmetrical, which is not feasible for routing protocols that inherently rely on symmetrical two-way communication. For instance, some protocols such as AODV and DSDV prohibit asymmetrical route and supports only symmetrical route, where both source and destination pairs should follow only the same route between them.

3.3.3.3 Loop Based Source Routing (LBSR)

The Loop Based Source Routing (LBSR) [59] scheme provides inherent support for asymmetrical routing. It is derived from DSR and most of its operation follows the original scheme in addition to unidirectional link support. The scheme reactively discovers routing path using a single flooding technique. In addition, several unicast packets are sent by the source, which propagate in a loop back to the source node. The cache mechanism is superior compared to DSR, as it performs better in the presence of unidirectional links.

Although DSR routing protocol provide supports for asymmetrical connection, it employs two independent route broadcasts. As such, the routing overhead incurred is twice that of AODV. The LBSR reduces such impact by removing the need for broadcast in the reverse direction. This is done by allowing the broadcast packet to discover all possible paths throughout the network using a single flooding technique. The scheme ensures that all nodes, including the destination, relay non-duplicate request packet to their neighbours. As a result, the reverse route constructed follows a completely different path back to the source node. The operation of LBSR is illustrated by Figure 3.8.

Initially, the source node **S** broadcast a control message known by *Lreq (*Loop request), which is received by nodes within its transmission range. Subsequently, the *Lreq* is rebroadcast and will eventually reach the destination node **D**. However, unlike DSR, where the packet propagation stops as soon as it reaches the destination node, the *Lreq* packet continues to be broadcast. The transmission of *Lreq* packet results in multiple loops, as shown in Figure 3.8. To reduce the impact of routing overhead, a node that is identified as part of the loop does not rebroadcast the *Lreq*, but instead, unicast. Assume that node **F** is part of the loop constructed around the nodes (**S-A-B-F-S**). If subsequent *Lreq* packet, e.g. from loop (**S-A-B-D-F-S**), is received by **F**, the packet propagated between **(F-S)** is unicast. As such, the number of broadcast packet generation is minimised. As shown in Figure 3.8, multiple loops are detected by using the LBSR scheme. To communicate with destination node **D**, node **S** follows the forward path (**S-A-B-D**). On the reverse, node **D** chooses the path (**D-F-S**) to return to the source node. The path (**D-E-G-S**) is not selected because it is not the shortest path, i.e. in terms of hop count.

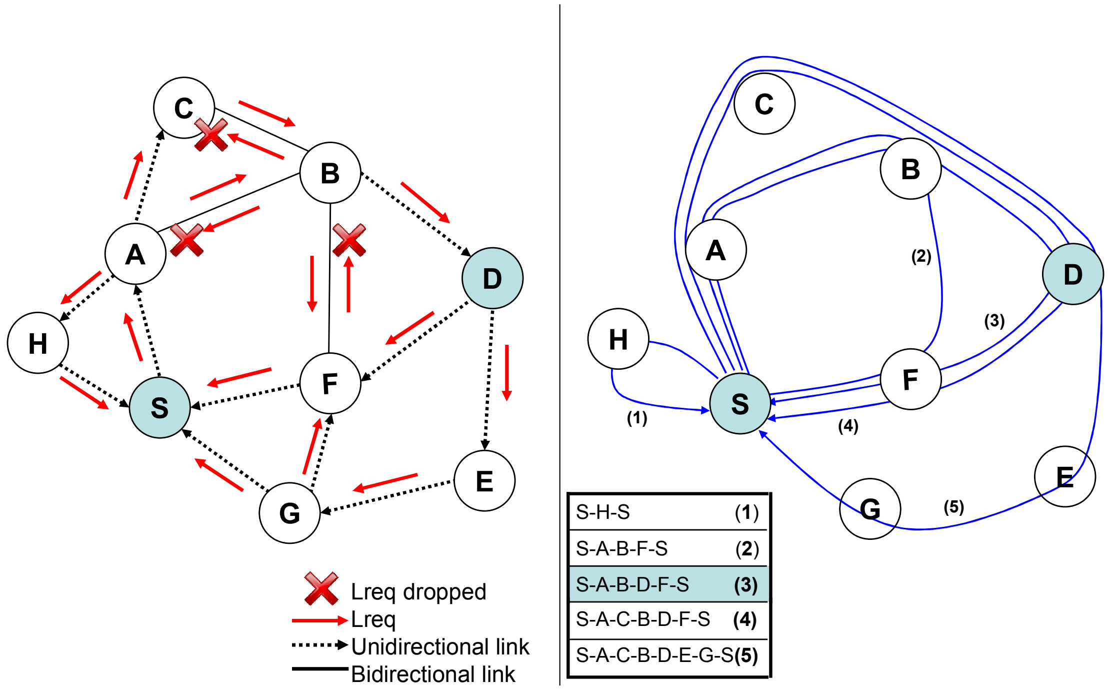


Figure 3.8: Loop based source routing (LBSR)

3.3.4 Comparison Table

Table 3.1 presents the summary and comparison of the schemes previously discussed. One particular element that is common among all the schemes is the routing metric, i.e. hop count. Although the metric provides a simple mechanism to calculate the shortest path, the path may not be reliable and can be detrimental in the presence of unidirectional links. In Chapter 6, it is shown by the simulation results; the performance of AODV based only on hop count is inferior compared to when using path loss.

Table 3.1: Summary of routing schemes

	BRA [58]	**LBSR [59]**	**RPS [35]**	**EUDA [63]**	**Flooding [64]**
Base protocol	AODV	DSR	AODV	AODV	AODV
Multicast support	No	No	No	No	No
Routing path selection	Destination	Source	Source	Source	Source
Unidirectional link handling	Utilising	Utilising	Avoidance	Avoidance	Avoidance

	BRA [58]	LBSR [59]	RPS [35]	EUDA [63]	Flooding [64]
Routing Metric	Hop count	Hop count	Hop count	Hop count	Hop count
Multipath routes	No	Yes	Yes	No	No
Route discoveries	Single	Single (back to source)	Single	Single	Two-way
Asymmetrical route	Yes	Yes	No	No	No
Detection phase	Forward path	Forward and reverse path	Reverse path	Forward path	Reverse path
Protocol independent technique	Yes	No	No	No	No
Power routing control	No	No	No	No	No
Motivation and the impact on routing performance	Discovers route using the reverse of Bellman Ford algorithm	Multiple routes detection. Improves reliability	Rely on multipath for reverse route constructio n	Immediate detection of unidirectio nal link during route discovery	Increases routing overhead compared to base protocol

3.4 Performance Evaluation Methodology

This section discusses the performance evaluation methodology between the schemes proposed in this thesis and the base routing protocols. Initial results of an extensive set of experiments are shown, where comparison in terms of various performance metric are presented against different types of network scenarios. To quantify the performance of routing protocols, several methods can be employed. This research adopts the simulation method. To justify the chosen methodology, a brief comparison with other techniques is presented.

Firstly, a routing protocol can be *empirically* measured in laboratory environments or on a site that covers a particular geographical area. The test-bed typically consists of several wireless devices distributed randomly or evenly, which are configured to communicate using a common protocol. There are many existing test-beds currently deployed for MANETs [65][66][67][68][69]. Although practical experiments can provide accurate information about the performance of the protocol being investigated, the major downside is that the results from experiments are difficult to reproduce. It is because a wireless mobile network is sensitive to external effects, particularly when small changes to the environment may severely impact the experiment results. Therefore, it is a common practice that results obtained from field work are compared to the simulation or analytical modelling, hence, increasing the results credibility. Nevertheless, empirical methods typically require a high number of participants to simulate mobility, which in turn incur high costs and require extensive amount of time and resource management.

The second approach to evaluate the protocol performance is through the use of *analytical* or *mathematical* modelling. In this method, the area of network considered is often small with few number of interconnecting nodes. As noted by a research work [70], nodes movement in wireless network is complex; hence the limited studies using analytical approach. Typically, only a small-scale network is considered, which can be represented using a simple set of algebraic equations in the computer systems. There are several analytical research works on both single-hop and multi-hop 802.11 wireless network [71][72][73][74][75]. Many of the studies however, are based on a specific assumption such as a network with saturated traffic load, a homogeneous network, and a network that operates using a global scheduling. Basically, these assumptions are made to simplify the analysis, which may have an effect on the simulation outcome. For instance, a mathematical model can be used to represent the simple activity of a queuing system at a certain instance. This is achieved by averaging the system's performance output over several sets of experiments. Despite the fact, that such method can provide rapid results, numerical computation may increasingly become complex with introduction of additional elements. Other factors such as nodal mobility characteristic and signal propagation are often neglected or simplified in the analysis. Therefore, in a dynamic network, which has varying workload volume distributed over the network, the mathematical modelling can be very complex.

The third approach is *simulation* and this is the primary evaluation technique employed by this research. The simulation tool described in section 3.4.1 provides several models structured according to the Open System Interconnection (OSI) layers. The system's operation is clearly defined and integration with new models is reasonably simple. Unlike the analytical method, the simulation computation technique is more comprehensive, where it considers the workload distributions across the network. In addition, if the simulation is an event tracing technique, each state transition the node experiences is successively recorded. The post-processing analysis then can be used to comprehensively analyse the output. The simulation method is often considered to be time consuming; requiring significant computer processing resources to execute. However, the benefits of simulation far outweigh the analytical method; particularly when handling multiple transactions on a densely connected network. Often, it required that only a particular layer of the network is to be investigated and thus, a correctly constructed simulation model can provide efficient method for independent layers to be evaluated. Based on this argument, the simulation technique is opted for network performance evaluation throughout the work.

3.4.1 Simulation Tools

Several choices of simulation tools are widely available for simulation experiment work. A review over a five-year-period of wireless network research papers [9] indicates that 76% of the works are based on network simulation. The extensive application of network simulation for wireless research continues to grow with Network Simulator 2 (NS-2) as the most popular simulation tools for such research. Based on the above-mentioned review, 44% of researchers choose NS-2 over other simulation tools. In principle, each tool is inherently differs from others and a precise selection of packages that best suit the simulation work needs to be determined. Tools that include a properly built model and debugging package are critical to ensure output obtained is credible and can support various conditions and network scenarios. There are several simulation tools that can be used for the simulation of MANETs such as NS-2 [76][77], GloMoSim [78], QualNet [79], OPNET [80] and OMNeT++ [81]. Table 3.2 summarises the shows the comparison between the simulators, highlighting the capabilities, strengths, and weaknesses. Previous studies [82][83] have also present a detail comparison between these tools. Basically, the choice of simulator is driven by the research work requirements and the following criteria provide the basis of selection:

- Open source
- Free license
- Well established with complete manuals and community support
- Widely used for research in MANETs domain
- Support cross platform installation
- Easy access to new extensions and modifications can be easily included

Table 3.2: Summary of simulation tools

	NS2 [77]	**GloMoSim [78]**	**QualNet [79]**	**OPNET [80]**	**OMNET++ [81]**
Interface	C++/OTcl	Parsec	Parsec	C or C++	C++/NED
Available Modules	TCP/IP, Ethernet, Propagation model, IEEE 802.11, ad-hoc, Zigbee, and energy model	TCP/IP, Ethernet, Propagation model, IEEE 802.11, and ad-hoc model	TCP/IP, Ethernet, Propagation model, IEEE 802.11, ad-hoc, Zigbee, and energy model	TCP/IP, Ethernet, Propagation model, IEEE 802.11, ad-hoc, S-MAC, and direct diffusion model	TCP/IP, Ethernet, Propagation model, IEEE 802.11, and ad-hoc model
Mobility	Support	Support	Support	Support	No
Graphical Support	Limited visual aid	Limited visual aid	Good graphical support for debugging	Excellent graphical support and to facilitate debugging	Good visualisation and excellent facility for debugging
License	Open source	Open source	Commercial	Free academic license for limited use	Free for academic and educational use
Scalability	Medium	Large	Very Large	Medium	Large
Documentation and user support	Excellent	Poor	Good	Excellent	Good
Extendibility	Excellent	Excellent	Excellent	Excellent	Excellent

Based on Table 3.2, NS-2 is selected as the simulation tools because it satisfies the criteria previously mentioned. Although it provides limited support for visualisation, such requirement is not critical in this research work. The excellent documentation and user support adds to the fact that NS-2 is the best choice for this research work.

3.5 NS-2 Overview

Throughout the years, NS-2 has been significantly improved by the open source community and its current release, the NS-3 was introduced in 2008. This new release is a replacement for the popular NS-2 simulator but it is not considered as an extension for NS-2. Despite the fact that both versions are based on C++, the NS-3 does not support the NS-2 Application Programming Interfaces (APIs). Although research work in this thesis coincides with the new release, i.e., NS-3, it is still new and very little support is available from the author and community to address issues that may arise. For this reason, the NS-2, which has been widely used in MANET work, is selected for this research work.

The NS-2 is developed by University California Berkeley. It is an object-oriented tool and is designed for discrete event driven networks. The tool is suitable for a variety of communication research. It includes the support for simulation of wired and wireless network functions and protocols such as physical layer, link layer and routing. Generally, NS-2 users are allowed to simulate a network by specifying the features included in the tools. In addition, the modular structure of NS-2 enable users the ability to focus the study on a specific protocol by simulating their corresponding behaviours.

In addition to the C++ object oriented programming language, NS-2 includes the Massachusetts Institute of Technology (MIT)'s Object extension Tool command language (OTcl) [84]. The tool is intended to assists users for simulation, which allows them to specify values for parameters that can be passed to the C++ object. The main purpose of OTcl is to expedite the simulation process. It reduces the time required to build and recompile the code after every changes made to the simulation parameter. In this way, the core structure of the protocol, i.e., coded in C++, is retained and various results can be output much faster. In general, the implementation and simulation of NS-2 can be summarised by Figure 3.9.

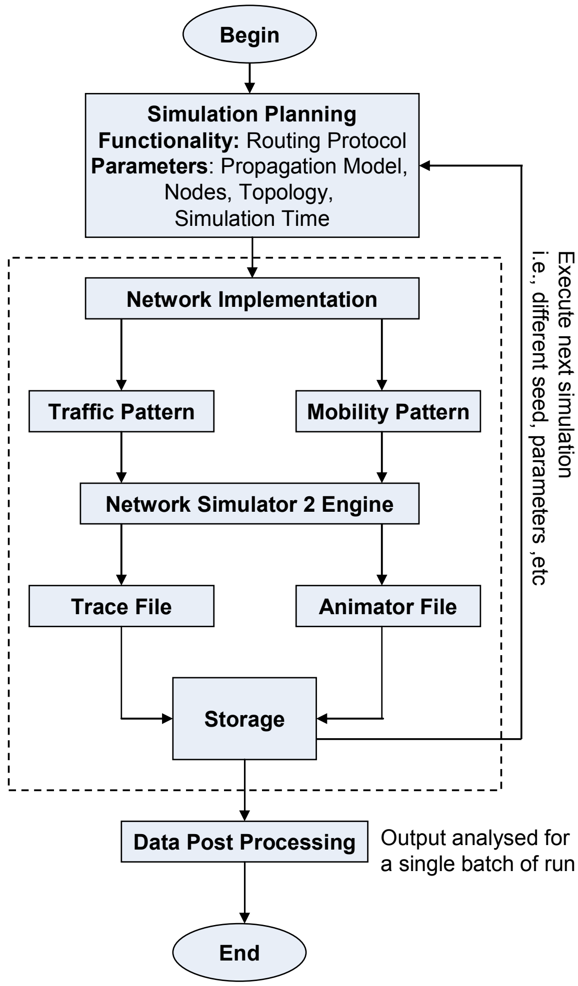


Figure 3.9: Simulation process [85]

3.6 Simulation Modelling

As previously described, the primary work of this research is done through simulation and therefore, it is essential that all the techniques involved are fully discussed. The key protocol is AODV, as it underpins the proposed scheme in this work. A comprehensive protocol validation and verification is also presented, evaluated using the same set of model assumption and network scenario followed by other researchers [56][86]. AODV is chosen for several reasons; outlined below:

- AODV is an enhanced version of DSDV routing protocol, which significantly improves the performance for on-demand based ad hoc network. Many research works, particularly for on-demand based routing have widely accepted AODV as the basis for comparison with a new routing protocol design [35][56][86][87]. In addition, the AODV routing protocol is also used in some research experiment to empirically determine the routing performance. The work of Perkins et al. [56] shows that the AODV routing protocol is typically more efficient than other on-demand routing protocols, e.g., DSR, over a range of scenarios.
- The AODV's routing method has been designed to specifically facilitate wireless communication that requires low communication overhead and where data is only sent on-demand. The routing path is not actively maintained outside data transmission, conserving node's power and bandwidth. In addition, the AODV's performance has been shown to be reliable under mobility conditions. Previous study [86] shows that AODV delivers over 95% of the packets regardless of mobility rate.
- Validated implementations of AODV are available with NS-2 [56][86].

The following sections outline the NS-2 model components, in particular those that are important for the implementation of the proposed scheme. The NS-2 distribution discussed within this thesis is the NS-allinone version 2.32.

3.6.1 Mobile Node Model

Nodes are the most fundamental element among all other components of NS-2. They are modelled to perform the basic functionality of network-enabled devices; including processing and forwarding of packets. The internal architecture of a node differs, depending on whether the node is mobile or stationary. NS-2 supports two types of nodes; wired and mobile. Typically, a mobile node is a wired node equipped with extra functionality to model the behaviours of mobile networking. In addition, mobile nodes are allowed to move within a certain area of the network, as opposed to wired nodes which remain stationary. The mobile node itself is a compound object, built from the several components. Figure 3.10 shows the internal structure of such node:

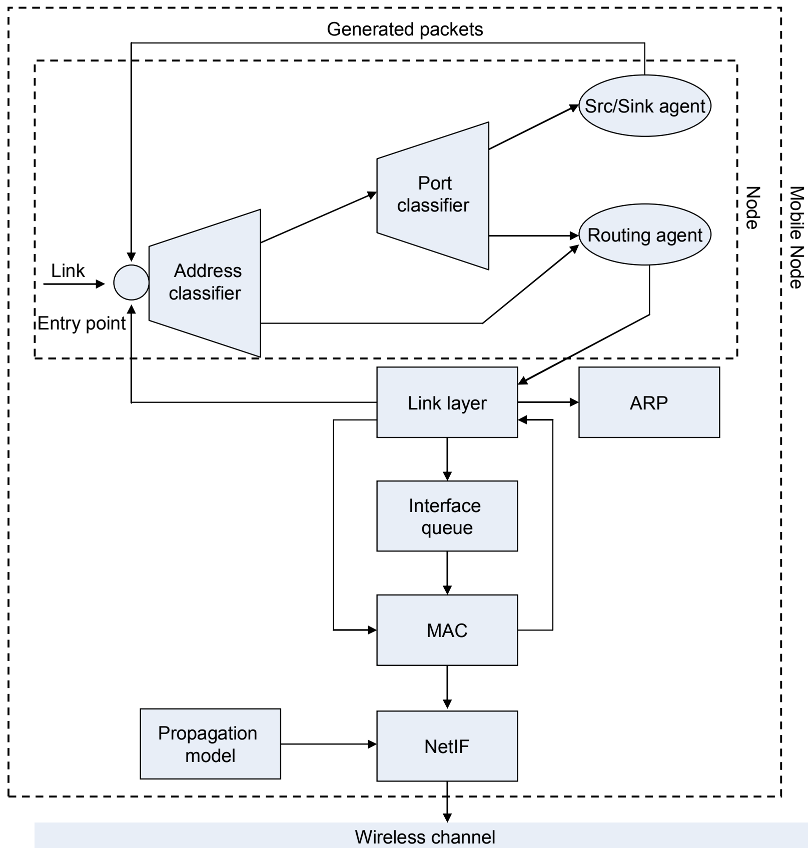


Figure 3.10: Components of mobile node model in NS-2 [77]

- *Src/Sink agent*: every packet that is sent by the source node (Src) is handled at the entry point, which is then forwarded either to the unicast or multicast classifier. Consequently, the packet is relayed through the routing agent before being sent to the immediate lower layers. The sink agent only receives packets through the classifier if the packet is addressed to the node.
- *Routing agent*: the main function of this agent is to perform routing. An incoming packet from an application is processed using the specified routing

algorithm and forwarded to the entry point. The classifier appends an address and the packet is sent to the link, which is then received by the receiver node's entry point. In the event that the incoming packet is not for the mobile node itself, the packet is handed to the routing agent, which assigns the routing information and sends it down to the link layer (LL). A port number of 255 is set by the receiver's classifier to attach the routing agent to a mobile node.

- *Link layer* and *ARP* module: the function of LL class is to simulate the data link protocol. Similar to the IEEE 802.3 standard specification [88], the LL class employs the Address Resolution Protocol (ARP) to determine the hardware address of neighbouring nodes and map Internet Protocol (IP) addresses to their correct interfaces.
- *Interface Queue* class: prior to transmission, all outbound packets are queued using the interface queue (IFq) class. Although the IFq has been defined by default to hold a maximum size of 50 packets, it is possible to change the value. Packets are placed according to their priority before being delivered to the MAC. Basically, there are four different priority queues available, in which packets are stored in accordance to priority level.
- *MAC* module: this module is an implementation of the IEEE 802.11 standard. It is a common protocol used by the MANET's modelling community and, as such, an appropriate candidate protocol to be used in this analysis.
- Radio *propagation model*: the two-ray ground reflection model [89] and the log-normal shadowing model are selected for the simulation in this work. The log-normal shadowing model is crucial for the study of routing protocol that highly depends on the channel condition for routing path construction. The omni-directional antenna's gain is assumed unity, i.e., 0 dBm, which used for the transmitters and receivers. Node's antenna is placed at an equal height of 1.5 m above the ground.
- *Network interface* model: In the evaluation work, the wireless network interface (NetIF) is set to follow the specification of the Cisco Aironet 350 Client Adapter [90], operating at 2.4 GHz. However, for the purpose of the model validation, the

Lucent WaveLAN [91] is used. This is consistent with the previous studies. The WaveLAN is a shared media radio with nominal bit rate of 2 Mbps and nominal radio range of 250 m. Table 3.3 shows the detail configuration parameters for the WaveLAN network interface.

Table 3.3: Lucent WaveLAN network interface parameters

Parameter Name	Parameter variable	Parameter Value
Raw bit rate (bps)	Rb_	2*1e6
Power of transmission (W)	Pt_	0.2818
Frequency (Hz)	freq_	914e+6
System loss factor	L_	1.0
Carrier sense threshold (W): min power required to detect another node's transmission	CSThresh_	1.559e-11
Receive threshold (W): min power required to receive a packet	RXThresh_	3.652e-10
Capture threshold (dBm): signal ratio required to maintain receiver capture of incoming packet in face of collision	CPThresh_	10.0

3.6.2 Network and Mobility Model

Different network scenarios are generated to evaluate the performance of the proposed scheme various link conditions. Each network scenario produces a different set of node movements and as such, the effect of link connection/disconnection to the routing performance can be thoroughly investigated. On the other hand, a variety of network simulation parameters are used, including the physical network size, node density, the number of source and destination nodes and the node's average moving speed. The packet size and the transmission frequency are also considered in order to observe the impact of traffic load on the routing protocols. For the combination of 2 routing protocols, i.e. AODV and AODV-Blacklist, a total of more than 500 simulation runs are carried out. This includes 2 physical network sizes (1500x300m^2, 575x575m^2) with a maximum of 20 pairs traffic connections, a maximum of 50 simulation repetitions, 5 maximum speeds (0m/s, 5m/s, 10m/s, 15m/s, 20m/s), varying pause time between 0 to 900s, packet size of 512 bytes, and a packet transmission frequency of 4 packets/second.

The mobility model used in this chapter is the Random Waypoint (RWP) [86], which can be described by using a simple mobility process shown in Figure 3.11.

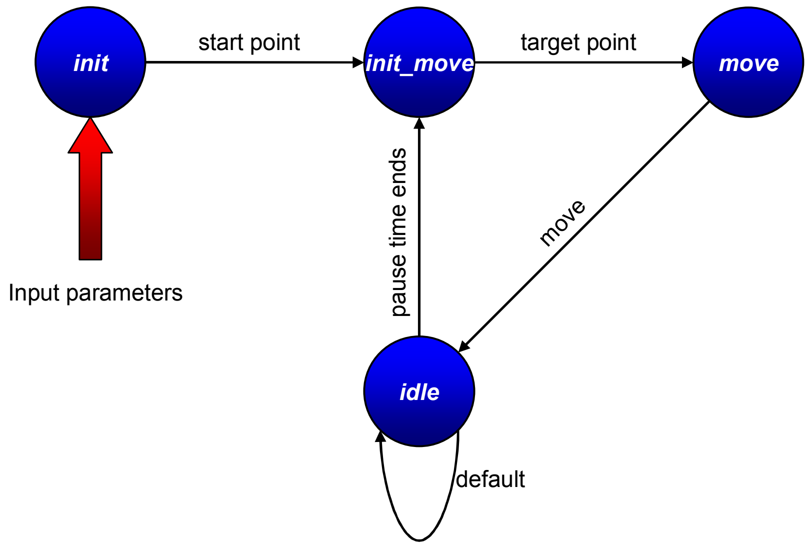


Figure 3.11: RWP mobility process model

Generally, this mobility model has been adopted by many research works in ad hoc network [33][35][44][45][56][62]. Basically, the input parameters for the model are the network area, maximum speed, and pause time. Initially, in the *init* state a node chooses a random location specified on any point on the network area. Later, the current node transits to the *init_move* state, where the node selects a random destination along with the speed, chosen from a uniform distribution between 0 and the maximum speed. In the *move* state, a node travels along a straight line to the destination at the selected speed. At the destination position, the node transits to *idle* and pauses for a duration time specified by the input parameter, i.e. pause time. When the pause time period finishes, the current node returns to the *init_move*, and cycle repeats.

3.7 Simulation Results Analysis

This section presents the approach in the analysis of results obtained from the simulation experiment. It may not be possible to guarantee the accuracy of results by using only independent simulation replications. Issues such as fluctuations can affect the simulation outcome, causing ambiguous and inconsistent result. Generally, there are two forms of simulations; terminating simulations and *steady-state* simulations. The simulation experiment used in this research work can be considered as steady-state. As such, a common problem associated with this type of simulation is the transient output during the warm up period.

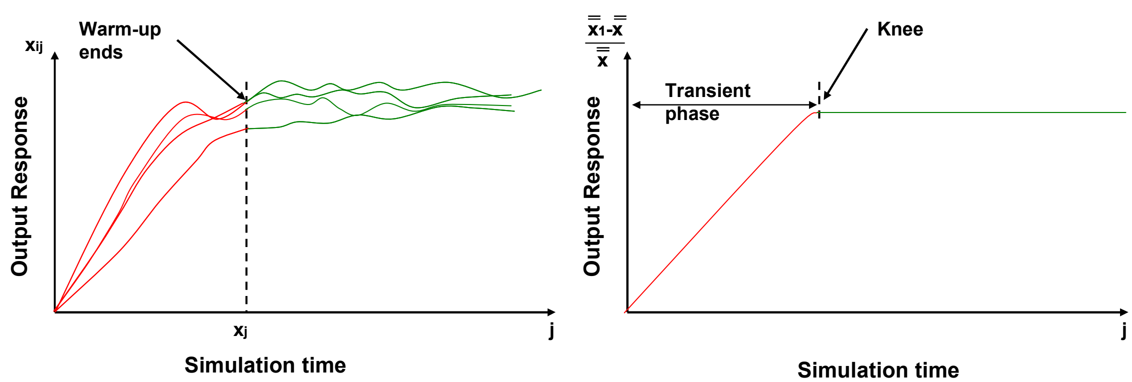
3.7.1 Simulation Control and Independent Replications

In the terminating simulation model, the starting and stopping conditions of the simulation are specified as a natural reflection of the target system's operation. The system's flow is terminating according to some conditions, where all operations occur within the pre-determined start and stop time. On the other hand, the steady state simulation is a method where the system's performance is measured in a theoretically infinite time frame [92]. The initial parameter conditions and simulation time period is pre-determined and the measure of interest is defined within a specified time frame, as the simulation theoretically run to infinity.

In this research work, the latter approach is adopted for the simulation experiment since it enables the performance of routing protocol to be observed in long-run. Essentially, two typical issues arises in the steady-state simulation; first the detection of initial transient period and second, the analysis of concurrent data. An important attribute of steady-state simulation is the time period between the start of the simulation until the time the simulation enter a stationary state. Such period is defined as the transient period or the warm-up period, where the system converges to a stable state. The simulation output obtained during such period is inconsistent and therefore, is not of use. As such, the data need to be discarded because it can severely affect the analysis of the routing performance. The following section discusses the methods to determine the initial transient period and subsequently the data elimination process.

3.7.1.1 Initial Data Deletion

The initial data deletion (IDD) [93] method requires analysis of the overall average after some of the initial output is deleted from the sample. A steady state is achieved when the average output of the simulation shows only a small variation. Nevertheless, due to the randomness of the simulation, which may be caused by random seeds, the average can slightly changed during the steady state. To reduce the effect of randomness, it is essential that the simulation output is averaged across several replications. Each replication is run using the same parameter settings, which differs only in terms of the seed values used in the random-number generators. The averaging technique causes the simulation to produce a smoother trajectory. Figure 3.12a shows the result of several simulation runs with different seeds, whereas the average run in Figure 3.12b shows a smooth curve.



(a) Multiple independent runs (b) Smoother average runs

Figure 3.12: Initial data deletion method

Assume that there are m replications of size n each. Let x_{ij} denote the j_{th} observation in the i_{th} replication. The value of j varies from 1 to n along the time axis, while i vary from 1 to m across the replications. The method consists of the steps summarises by Table 3.4.

Table 3.4: Initial data deletion method [93]

Step	Description	Equation
1.	Compute the mean trajectory by averaging *n* replications.	$\bar{x}_j = \frac{1}{m}\sum_{i=1}^{m} x_{ij}$ for $j = 1,2,\ldots,n$
2.	Compute the overall mean.	$\bar{\bar{x}} = \frac{1}{n}\sum_{j=1}^{n} \bar{x}_j$
3.	Assume transient state duration is *l* long. Delete the first *l* observations from the mean trajectory and compute the overall mean from the remaining (*n–l)* observations.	$\bar{\bar{x}}_l = \frac{1}{n-1}\sum_{j=l+1}^{n} \overline{x_j}$
4.	Compute the relative change of the mean.	$\frac{(\bar{\bar{x}}_l) - (\bar{\bar{x}})}{\bar{\bar{x}}}$
5.	Repeat step 3 and 4 by increasing *l* to n-*l* until the relative change stabilises. Plot the curve, after certain value of *l* the relative change stabilises. This point is known as the knee, which indicates the end of the transient period.	

3.7.1.2 Batch-Means Test

The Batch-Means Test (BMT) is a simulation test [94] on running a simulation over a long period of time. Subsequently, the simulation is divided into several partitions, each of equal duration known as batch. Each batch is computed for its individual batch mean. The variance of the batch means is then analysed as a function of the batch size. As shown in Figure 3.13, *N* number of observations is divided into *m* batch, each with *n* size, where $m = N/\text{n}$. Similar to the IDD method, let x_{ij} denote the j_{th} observation in the i_{th} batch. The sequence of steps for the BMT is illustrated in Table 3.5.

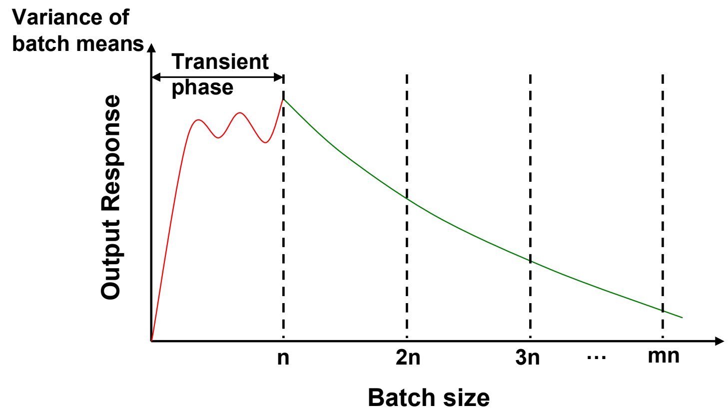


Figure 3.13: Batch means analysis

Table 3.5: Batch means test [94]

Step	Description	Equation
1.	For each batch, compute a batch mean.	$\bar{x}_i = \frac{1}{n}\sum_{j=1}^{n} x_{ij}$ for $i = 1,2,\ldots, m$
2.	Compute the overall mean.	$\bar{\bar{x}} = \frac{1}{m}\sum_{i=1}^{m} \bar{x}_i$
3.	Compute the variance of the batch means.	$Var(\bar{x}) = \frac{1}{m-1}\sum_{i=1}^{m} (\bar{x}_i - \bar{\bar{x}})^2$
4.	Repeat steps 1 to 3 for increasing batch size *n*.	
5.	Plot the variance as a function of batch size *n*.	
6.	The transient interval is the value of *n* for which the variance starts decreasing.	

The advantage of BMT is that only one transient interval needs to be removed. On the contrary, the IDD requires multiple transient intervals, *l*, to be deleted prior to output stabilisation (knee). Another issue with IDD is that randomness can cause some fluctuations during steady state. This may lead to unexpected deletion of steady state data. Multiple runs with high variations of seed can reduce such problem. On the other hand, the BMT approach requires large batch sizes to ensure output is significantly correlated between successive batches. Nevertheless, the BMT technique is adopted in thesis and is used with the confidence estimation measures discussed in the next section. On the other hand, the IDD is employed to determine the cut-off point, for which the nodal movement stabilises in each mobility model. Unless specified, the cut-off point for each simulation in subsequent chapters is set at 1100 seconds.

3.7.1.3 Independent Replications

The other aspect of the simulation control in this work is the replications method [95]. To produce a credible simulations output, a sufficient number of independent replications must be made for the analysis of the correlated data.

It is important that the number of replications is carefully chosen to produce simulation output that can guarantee the accuracy of the final results. Based on the methods previously discussed, the transient output can be effectively discarded, and the remaining results are sufficient for the analysis. However, the method does not specify the number of independent repetitions needed for a particular simulation. Therefore, the following points outline the steps required to achieve a confidence interval of 95%:

- The same set of initial parameters is set for each replication.
- The initial transient detection scheme is applied for each replication
- The simulation is repeated with different random number generator seed value for each replication. A total of 25 replications is considered with the size of each replication is $m - l$, where l is the size of discarded observations due to transient state.
- Each replication is run over a long simulation time to ensure the number of observations is significantly larger than the portion that is discarded due to transient period. If the simulation is too short, the results may be highly variable.
- The overall mean is calculated across the replications. Based on the variance of the replicated means, the confidence intervals can be computed. The upper and lower bound of the confidence interval are identified by the vertical bars across

the mean value. The confidence interval limits can be found by using the Student's t-distribution table [95][96]. In this work, the simulation output has been set to a confidence interval of 95%, i.e. a confidence level α of 0.05.

A detail step of the confidence interval calculation for the simulation output is presented in Table 3.6.

Table 3.6: Independent replications [95]

Step	Description	Equation
1.	Compute the mean for each replication.	$\bar{x}_i = \frac{1}{n}\sum_{j=n_t+1}^{n_t+n} xij$ for $i = 1,2,\ldots,m$
2.	Compute the overall mean for all replication.	$\bar{\bar{x}} = \frac{1}{m}\sum_{i=1}^{m}\bar{x}_i$
3.	Calculate the variance of the replicate means.	$Var(\bar{x}) = \frac{1}{m-1}\sum_{i=1}^{m}(\bar{x}_i - \bar{\bar{x}})^2$
4.	An approximate 100(1-*a*)% confidence interval for the mean response is:	$C = \bar{\bar{x}} \mp t\sqrt{\frac{Var(\bar{x})}{m}}$ (where $t \equiv t_{\frac{\alpha}{2},m-1}$ is chosen such that $P\{T_{m-1} \le t\} = \frac{\alpha}{2}$ and T_{m-1} is a Student-*t* random variable with *m*-1 degrees of freedom)

3.8 Validation Methodology

This section discusses the validation methodology. The comparison method is selected for validation, which is one of the techniques presented by Sargent [97]. Simulation results of the base routing protocols are reproduced and compared against the results obtained by previous researchers. To do this, similar network scenarios are recreated with parameters set to match as close as possible to the studies [35][86][56]. In order to ensure that the results obtained are credible, the simulation control and replications method as discussed in section 3.7.1 are applied. For this reason, the simulation outputs in this validation may not be identical to the compared simulation results. A slight difference is observed, as shown by the results in this section.

3.8.1 Comparison to Other Simulation Model

A comparison to a benchmark results from a 'valid' simulation work is the approach used to validate the simulation model in this research. Based on the comparison, a degree of similarity can be observed, which may indicate that the simulation settings and network scenarios are valid in comparison to other research work. The baseline results [35][86][56], which is run by authors of the routing protocol are considered faithful. Similar network parameters settings are followed and the value is summarised in Table 3.7. Naturally, the output of the simulation results may not be identical to the compared work. This is due to undocumented parameters and for that reason, some simulation settings are assumed similar to the parameters commonly used in earlier NS-2 simulation work. The NS-2 simulation software models all network layers in great detail, and may results in complex calculations and high resource consumptions, i.e., memory and computing time.

Table 3.7: Simulation parameters for model validation

Parameter	**Perkins [56]**	**Marina [35]**
	Physical and Data Link Model	
Propagation model	Two-Ray Ground	Two-Ray Ground
Radio frequency	914MHz	914MHz
Transmission range	250 meters	250 and 150 meters
Data bit rate	2Mb/s	2Mb/s
Antenna height	1.5 meter	1.5 meters
Interface queue	50	50
Link layer	IEEE802.11 standard	IEEE802.11 standard
	Routing Model	
Link breakage detection	MAC layer feedback	MAC layer feedback

Parameter	Perkins [56]	Marina [35]
Active route time	300 seconds[7]	300 seconds
Route reply lifetime	600 seconds	600 seconds
Route request attempt	3	3
Route request timeout	6 seconds	6 seconds
Broadcast ID timeout	3 seconds	3 seconds
Reverse route timeout	3 seconds	3 seconds
Broken link timeout	3 seconds	3 seconds
Movement Model		
Mobility model	Random Waypoint	Random Waypoint
Number of nodes	50	100
Pause time	0 to 900 seconds	0 second
Network area	1500 x 300 m/sq	575 x 575 m/sq
Maximum node speed	20 m/s	0 to 20 m/s
Simulation time	900 seconds	500 seconds
Ave. runs for each data point	25[8]	50
Traffic Model		
Traffic source	Constant Bit Rate	Constant Bit Rate
Traffic load	4 packets/sec	4 packets/sec
Number of sources	20	20
Packet size	512 bytes[9]	512 bytes

3.8.2 AODV Model Validation

The AODV model is validated using NS2, which follows most of the parameters stated by Broch and Perkins. Table 3.7 shows the parameters used in this validation. Generally, the simulation parameters in Perkins's work are identical to Broch's except for the packet size and the number of repetitions. The differences can slightly affect the results, which can be observed in Figure 3.14 specifically at 300 and 600 seconds.

Basically, Figure 3.14 and Figure 3.15 shows the packet delivery ratio (the ratio of number of data packets delivered to destination to those generated by the sources) and

[7] The routing parameters are not explicitly specified but are referred to Broch [86].
[8] The average runs by Perkins [56] and Broch [86] are 5 and 70 respectively.
[9] The packet size defined in Broch [86] is 64 bytes.

routing overhead (the total number of routing packets sent and forwarded) as a function of pause time, with maximum node speed of 20 m/s. Each point on the graphs represents a repetition of 25 independent simulation runs, varied only by the node movement patterns. The results of AODV, obtained from the simulation (represented by the square symbol) are nearly identical to Broch's and Perkins's (represented by the bar charts). There are some slight differences, particularly when compared to the Perkins's result. As indicated by Table 3.7, the average number of runs on Perkin's is small, i.e. 5, which can be the reason for the small discrepancy. Nonetheless, as expected, at a pause time of 900, the packet delivery ratio for every result is nearly identical. Nodes set with such pause time are virtually stationary for the entire time period of simulation. Figure 3.15 shows the routing overhead output obtained by simulation compared to the results reported by Broch. At pause time 0, the routing overhead shown obtained by the simulation is the highest, which slowly decreasing as the pause time increases towards 900. Again, there are some slight differences in the results, which may be due to the fact the packet size used in Broch's work is much smaller, i.e. 64 bytes. Figure 3.16, shows the normalised routing load (the number of routing packets sent and forwarded to the number of data packets received). It shows a similar trend to Figure 3.15, where each point on the graphs slowly decreasing as the pause time increases.

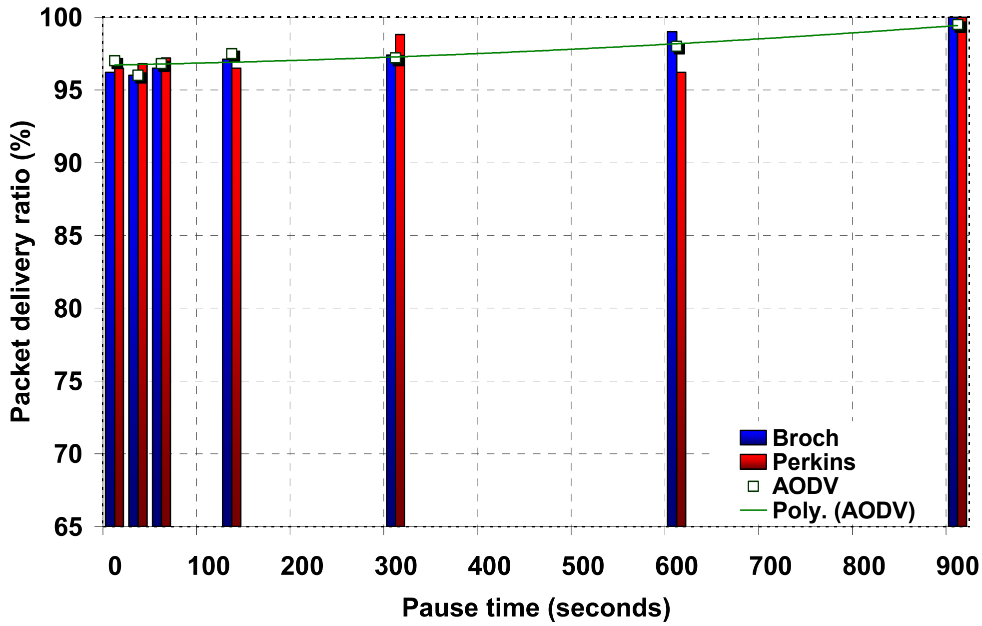


Figure 3.14: Packet delivery ratio

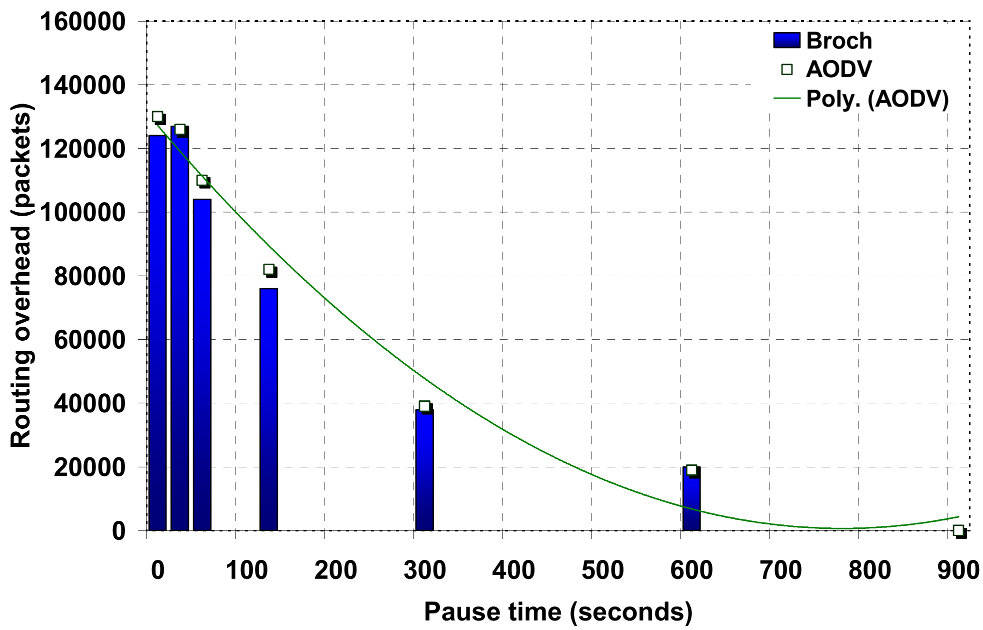


Figure 3.15: Routing overhead

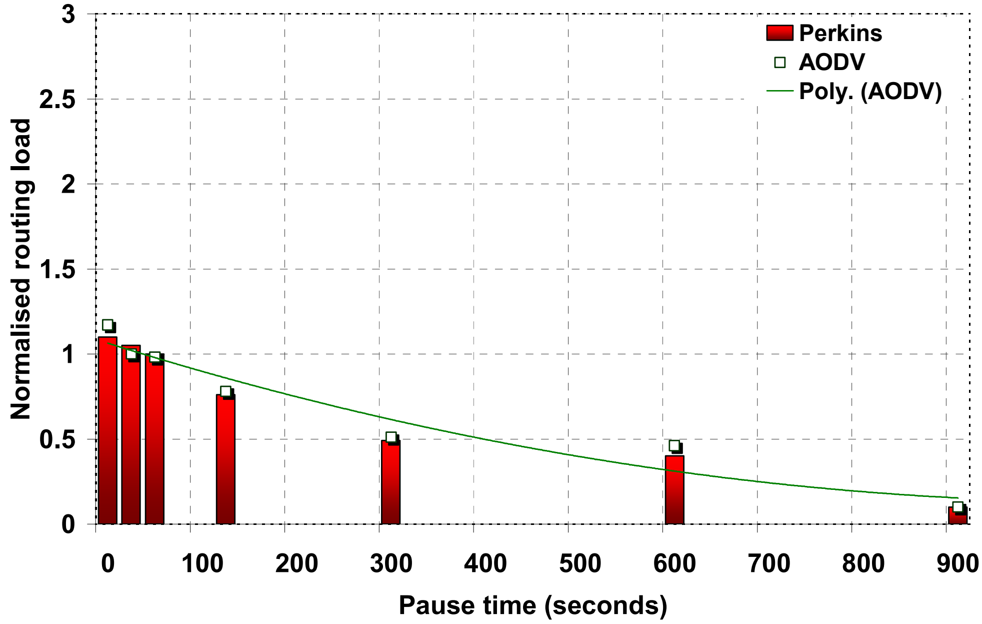


Figure 3.16: Normalised routing load

3.8.3 AODV-Blacklist Model Validation

The AODV-Blacklist scheme is validated with the simulation parameters stated by Marina, shown in Table 3.7. Nodes on the network are equally separated into two groups that are set with two different transmitted powers, i.e., 0.2818 and 0.0176 W. Ideally, the reduction in the transmitting power causes the transmission range to drop by two-fold. The complete radio interface specifications are as outlined in Table 3.3. Figure 3.17 compares the packet delivery ratio of AODV-Blacklist obtained by simulation to the results reported by Marina. In contrary to the previous section, the network area for the AODV-Blacklist validation is smaller, 575 x 575 m^2 on a flat space. In addition, the number of nodes is significantly higher, which is twice as much as in the research works [86][56]. Such settings cause the network to be highly congested, which explains the reason for the low packet delivery ratio. For instance, at speed of 20 m/s, the packet delivery ratio shown by Marina is 70%, which is low compared to more than 95% shown by Broch and Perkins. Figure 3.18 shows the normalised routing load. As expected, the normalised routing load increases with the increase of nodal speed.

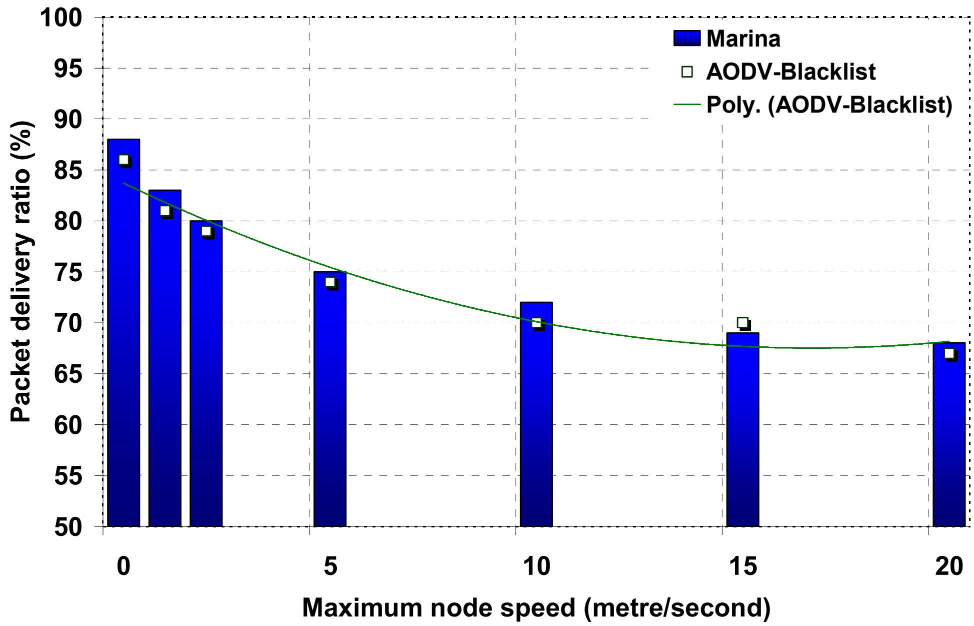


Figure 3.17: Packet delivery ratio

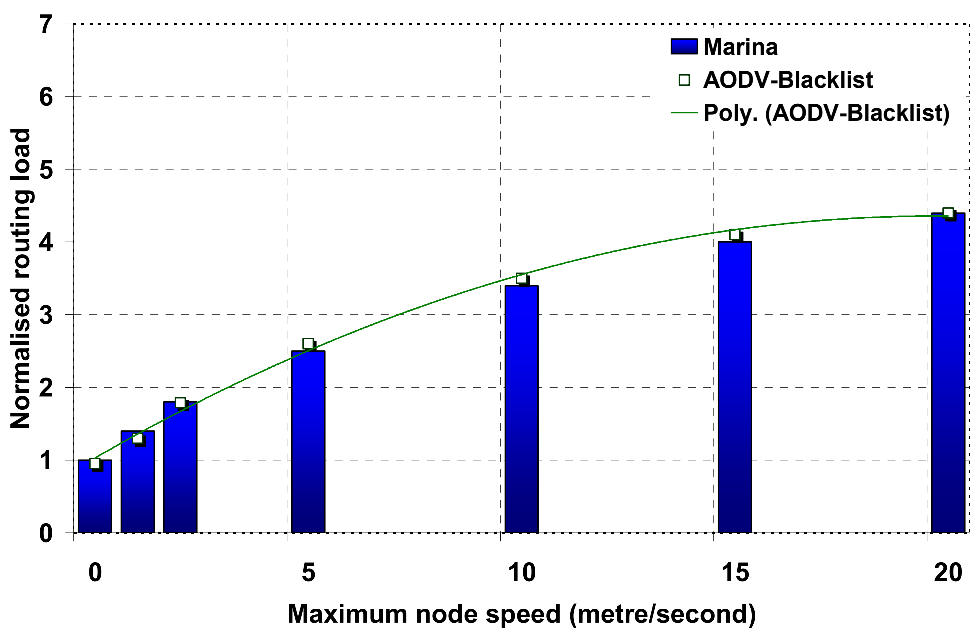


Figure 3.18: Normalised routing load

3.9 Summary

In this chapter, the concept of routing with using bidirectional link is presented using the AODV routing protocol. Many routing protocols inherently rely on the availability of bidirectional link and symmetrical path to form end-to-end communication between a pair of source and destination nodes. The occurrence of unidirectional link and the effect it has on the routing protocol operation is also described. A number of schemes have been developed to deal with such link. The common technique is to avoid but there are also a few schemes choosing to utilise the unidirectional link for data transportation. A list of schemes described in this chapter is summarised with their strength and weaknesses highlighted. There are three essential components to handle unidirectional link; the detection, avoidance, and/or exploit.

This chapter also presents the evaluation methodology employed for the evaluation of every routing scheme used in this thesis. In addition, the simulation modelling is also described, including network model, node model, and mobility model. An important element in any simulation experiment, which is the simulation control, is also discussed. Finally, this chapter presents the validation process, where results obtained by simulation are compared to the benchmark results reported by other authors. Such is essential to increase the credibility of the simulation model used in the subsequent chapters.

In the next chapter, a discussion on network connectivity is presented. This includes simulating unidirectional links and observing the impact on the performance of routing protocol. To increase variation in terms of network topology, i.e., nodes movement and connection, four different mobility models are considered, namely Random Waypoint (RWP), Gauss Markov (GM), Reference Point Group (RPG), and Manhattan. The next chapter also proposed a new performance metric referred to the probability of route connectivity, which is designed to supplement the evaluation of a routing protocol's performance, particularly in Chapter 6.

4. Network Connectivity

4.1 Introduction

This chapter presents the investigation on the impact of unidirectional link formation to the performance of MANET's routing protocol. Several network models are varied and the simulation results are exhaustively analysed. Based on observations, the occurrences of unidirectional link have shown to significantly impact the proper operation of MANET routing protocol. Chapter 4 is organised as follows. Section 4.2 presents a review of research works, which investigate the effect of unidirectional link on the network connectivity. Section 4.3 describes the definitions used in the subsequent simulation model. Section 4.4 introduces the analysis of link connectivity and the formulation of routing path connectivity. Section 4.5 presents the simulation setup along with the results analysis, using different network performance metrics.

4.2 Review of Unidirectional Links

This section presents an extended review of unidirectional link, which was briefly discussed in section 2.4.3.1. A unidirectional link can result from various combinatorial factors affecting the wireless device transmission range. Since links are radio signals, connectivity is significantly influenced by the variation of noise, signal propagation, and the heterogeneity of nodes transmission range. As a result, links become asymmetric in nature and the communication between a pair of source and destination nodes may follow paths which are in fact unidirectional. A typical example is unequal SINR experienced by adjacent wireless devices [98]. Unidirectional links may also be caused by unequal transmitting power (P_t) configured at each device. For instance, a network which employs a power-aware routing scheme will attempt to control the awake and/or sleep scheduling of a node to conserve energy. Consequently, power link budget in the forward direction may not be equal to that in the opposite direction thus resulting in a unidirectional link. Generally, such links can be represented by using a Boolean reachability function shown by equation 4.1. If node **X** is able to successfully transmit a packet to **Y** at time t but not vice versa, the link is considered unidirectional [99].

$$R(X,Y,t) \neq R(Y,X,t) \tag{4.1}$$

The existence of unidirectional link in wireless communication is not generally favourable because they can severely affect the network performance. A wireless network is extremely dependent on the availability of radio links to communicate; each link typically shared among several devices on a particular network segment. Basically, in a multi-hop wireless ad hoc network such as MANET, communications between nodes are characterised by a low control traffic exchanges [100][101]. Wireless devices often compete for network access, which may be limited in terms of bandwidth. By using a particular medium reservation scheme, e.g. MAC, nodes rapidly exchange control packets to build a routing path on-demand. The medium is then released as soon as the session is complete. Furthermore, the network topology changes dynamically as a consequence of nodal movement and signal interference, causing the link to fluctuate. Consequently, it is not feasible to monitor the state of the link, i.e., unidirectional or bi-directional, by nodes using a frequent exchange of control messages. Nodes in MANETs are also typically limited by power, memory, and computation capabilities. Due to such constraints, it may not be feasible to actively probe the status of a link prior to a packet transmission. Such a deficiency causes a source node to discover routing paths that can be detrimental to the network performance. In addition, many routing schemes in MANETs operate with the assumption that every wireless link is symmetrical. The lack of proper unidirectional link management can further deteriorate the protocol's performance. Therefore, it is crucial for a routing scheme to be able to alleviate this problem and subsequently form routing paths that are reliable and capable of increasing the network efficiency.

As previously mentioned, many routing protocols in MANET typically operate on the basis that every node has homogenous properties and therefore, the links between adjacent nodes are deemed bidirectional. However, such an assumption is inaccurate; in fact, the occurrences of unidirectional link in MANET are quite common, as shown by a research work [102]. Despite such findings, many existing routing schemes are restricted to using only equal bidirectional links and symmetrical paths are implicit in their operation. In other research work [103][104], it is shown that routing schemes finding unidirectional link can increase the end-to-end delay and the resulting performance advantage may be negligible. On the contrary, utilising unidirectional links in addition to the existing bidirectional links can also significantly improve MANET routing performance, as shown by previous researchers [35][58][62]. As discussed in section 3.3.2, two main approaches to handle routing operation with unidirectional links exist. The first explicitly avoids and eliminates routing a packet through such link, where all packets must be routed solely using bidirectional link. In the second approach, both bidirectional and unidirectional links are utilised, where nodes are able to exploit full network connectivity and build the shortest route from source to destination.

4.3 Unidirectional Link and Network Connectivity

The presence of unidirectional links can severely affect the proper operation of a network. As such, it is important to investigate and analyse the impact of such link on the performance of MANET routing protocol. One particular effect commonly associated with unidirectional link is the system's declining ability to form an effective routing path in the network. At the MAC layer, such link causes the congestion control and link sensing services to be hampered. The MAC functionality is typically important for unicast routing, where packet transmission specifically requires a bidirectional link connection to perform the RTS/CTS handshaking. In such event, the link layer ACK is prevented from being directly returned to the node which originates the packet. On the other hand, at the network layer, the efficiency of routing operation is also significantly impaired. When a routing path fails to be formed, additional route discoveries are needed to find alternative paths to the destination node. Consequently, a protocol's performance such as AODV, which operates naturally using only bidirectional links, is substantially degraded. Other routing protocols such DSR and Reverse-AODV [62] may avoid unidirectional links. However, the two-way broadcast mechanism employed by these protocols is expensive and can incur additional routing overhead. Figure 4.1 shows the two-way broadcast approach in DSR and R-AODV to avoid the unidirectional link, **A-E**. Although the approach can setup a route from **S** to node **D**, via **S-B-F-D**, the reverse path is invalid. As shown in Figure 4.1, node D has recorded the path **D-E-A-S** to node S, via the unidirectional link **A-E**. Hence, in order for node **D** to be able to communicate with **S**, it has to perform another route discovery broadcast, causing the routing overhead to increase by as much as three times.

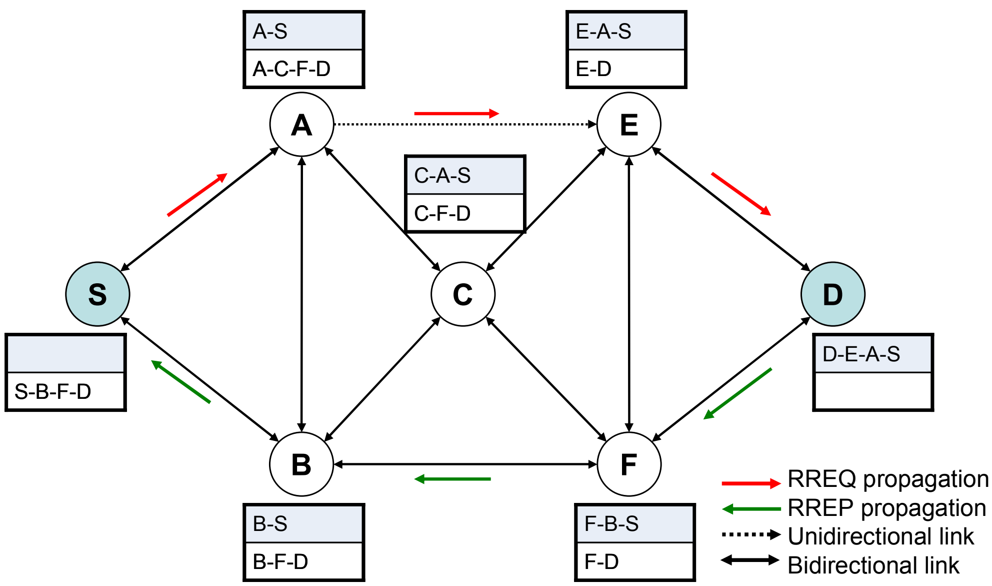


Figure 4.1: Two-way broadcast

Several research studies exist [35][61][106][107] that analyse the impact of unidirectional link on the network connectivity. However, the observations made by these studies are not particularly comprehensive, where important attributes such as nodal mobility and the variation of radio propagation are not fully considered. Research work by Prakash [61], examines mathematically the impact of unidirectional link on a network that operates with distance vector routing protocol. The study shows an increase of routing messages when packets are routed via unidirectional link. In particular, the study observed the order of routing overhead growth, O, in the system. As a function of network size, the routing overhead can increase from between $O(n)$ to $O(n^2)$, where n is the size of the network [61]. Although a higher routing overhead can be alleviated by increasing the node's storage capacity, such methods can lead to more complex systems. In addition, substantive growth in routing overhead causes the network to become saturated. Such situation can hinder the chances for new nodes to join and reserve the channel. Other research work [35] presents a discussion on network connectivity, which analyses unidirectional link using random graphs that are fully connected using bidirectional links. The simulation study is based on the assumption that the radio range is perfect, i.e. having a circular shape disk, where each point equidistant from the source has the same signal strength. In reality, the strength of radio signal encompassing a node is not equal in every direction; mainly a result of power fluctuations and shadowing effects [108][109][110]. Figure 4.2 illustrates the variation of signal strength around a node in a real-world scenario in comparison to a perfect radio model.

Two important components of MANET that has not been fully considered in the previous work are path loss and mobility. In a University of California, Los Angeles (UCLA) study [106], it is shown that a node's received signal is vulnerable to losses even when nodes are not in motion. The experimental study is conducted on the UCLA campus with large wireless multi-hop network. The number of wireless nodes deployed is 185 uniformly distributed in a grid-like fashion, where each node is set with identical radio setting. Although nodes are distributed in such an organised network, the ratio of unidirectional link to the total link is surprisingly high, i.e. up to 15%. In real network, however, it is uncommon to have nodes located equally separated between each other. Furthermore, each node may be equipped with non-identical radio interfaces. As a result, the number of unidirectional link formed can substantially increases, leading to a much higher impact on the network performance.

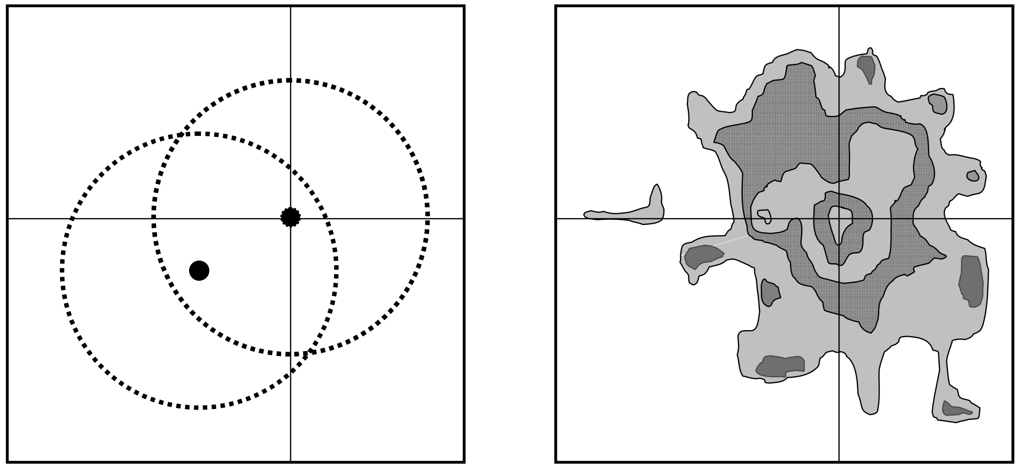


Figure 4.2: Theoretical and empirical transmission area [110]

To address these shortcomings, the simulation work in this chapter considers using various network topologies generated using two different radio propagation models, i.e., two-ray ground and log-normal shadowing. The study is conducted by simulation and the analysis is restricted only to the quantification of unidirectional link, which resulted from the difference of transmission power. A wider range of scenarios is also generated using several mobility patterns, i.e., *Random Waypoint* (RWP), *Gauss Markov* (GM), *Reference Point Group* (RPG), and *Manhattan*, to enhance the investigation of network connectivity. The results obtained from each model are compared and analysed using several performance metrics.

4.3.1 Propagation Models

In real-world, the exact behaviour of radio waves is not possible to be determined. Nevertheless, there exist many models that can statistically represent the environmental effects such as refraction, reflection and fading. Such models may accurately predict the transmission losses, received power, and etc. A number of models have been developed [111][112][113][114], many of which differ dominantly in terms of the path loss factor between the transmitter and the receiver. These radio models have been widely validated against a sufficiently large set of data collected by empirical measurement. For instance, Sugimoto and Sato [115] have indicated that their theoretical results are comparable to the empirical data.

In the next sections, a discussion of two radio propagation models is presented, i.e., *two-ray ground* and *log-normal shadowing* models, which underpin the simulation experiments described in this chapter.

4.3.1.1 Two-Ray Ground Model

The two-ray ground model, as discussed by Lee [116] , describes radio propagation over extended range. This model considers a signal reflected off the ground in addition to the direct signal path. The reflected signals are assumed to have approximately the same strength to the signal of the direct path, but with some delay. In this model, the received signal strength is shown by equation 4.2, where d is the transmitter and receiver separation distance, h_t is transmitter antenna height, h_r is receiver antenna height, G_t, is the transmitter gain, and G_r is the receiver gain.

$$P_r = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4} \tag{4.2}$$

Assuming a unity gain and small antenna height, which is a typical case in network simulation, the path loss, *PL* decays with the fourth power of distance, which is faster than the free space propagation model. Equation 4.3 shows path loss (*PL*) as a function of distance.

$$PL = \frac{P_r}{P_t} = \left(\frac{1}{d^4}\right) \tag{4.3}$$

Radio wavelength, which is a ratio of speed of light (c) and frequency (f), is a less important factor in this model due to the assumption of large transmitter-receiver separation. This model along with the shadowing effect (discussed in next section) is used for the network simulation in this thesis. Nonetheless, previous research work [117] presented results of experiments based on the two-ray ground and log-normal shadowing (discussed in the next section). The results clearly show many differences. It also indicates that the two-ray tracing can overestimate the quality of radio channel and thus, a more realistic radio model incorporating shadowing is more likely to produce a credible result.

4.3.1.2 Log-normal Shadowing Model

The log-normal shadowing model provides a further element on the deterministic propagation model, which accounts for the random variations in the received power observed over distances. Also known as slow-fading, the model adds a random component to the received power in order to reproduce random variability typical of wireless links. The log-normal shadowing model consists of two components, the mean loss and the shadowing element. Mean loss is the deterministic path loss mathematically modelled using a single power-law model (in dB), which predicts the received power at a distance between the transmitter and receiver. Shadowing reflects the variation of received power at a particular distance. The model is mathematically shown by the equation 4.4.

$$PL(d) = PL(d_o) + 10n\log_{10}\left(\frac{d}{d_0}\right) + X_\sigma \tag{4.4}$$

The mean loss *PL(d)* is a function of distance *d*, $PL(d_o)$ is the mean loss at a reference distance d_o, and *n* is the path loss exponent. These parameters depend on factors such as antenna height and radio frequency. The loss computation follows the log-normal distribution, varied about the zero-mean Gaussian random variable, X_σ with standard deviation σ.

4.3.2 Mobility Model

The impact of node movement to the creation of unidirectional link is the other aspect of network connectivity investigated in this section. A mobility model represents the nodal motion relative to others in a designated network area. Nodal movement, always, to a degree, restricts node's ability to make effective routing decisions and consequently reduces the probability of success in forming routing paths. Most importantly, each mobility model generates a different connectivity pattern, which can substantially affect the simulation output. Therefore, a mobility model selected without consideration to be used for a simulation may not behave as expected, and this can lead to inconclusive results. For this reason, it is crucial that the routing protocol is analysed with various mobility models prior to data collection. Although much research work [118][119][120] have shown the effect of nodal mobility on the protocols' performance, however, it is not the aim of this thesis to exhaustively observe such effects on the routing protocol's performance. The aim is to show that different models have different attributes and their use can significantly change the simulation output. An assessment that is solely based on a randomly chosen model may lead to inconclusive judgments. Thus, to improve the credibility of simulation results, it is important to determine which particular model is the most relevant for simulation experiment in this thesis.

Indeed, when measuring the performance differential, many researchers have often failed to take into consideration that simulators are based on discrete event or incomplete models and therefore, the results obtained may be imprecise compared to the reality. The problem arises particularly when a routing protocol being evaluated is highly dependent on nodal mobility behaviour. Therefore, in this research work, four different mobility models are investigated. Results obtained from these models are compared and subsequently only one is adopted as foundation for representing nodal movement.

4.3.3 Mobility Characteristics

A mobility model, from a network simulator perspective, is a model designed to recreate the movement pattern of nodes that follows as close as possible, the actual node behaviour in the real world. For instance, in a vehicular wireless network, the mobility model should be able to provide the simulator with a realistic representation of the vehicular movement such as moving in a specific path, vehicle to vehicle interaction and also the effect of traffic rule enforcement.

Generally, every mobility model possesses four intrinsic properties, resulting in variations of network topology. First, the speed and space distribution of nodes in the network can directly influence the path availability among nodes. The speed and spatial distribution of nodes in some models, such as RWP is not uniform, as indicated in the research work [10][121]. As a result, the performance measurement of a routing protocol may not be similar to the performance outcome in a different environment. Second, a mobility model is strongly characterised by the path duration between nodes. Nodes in proximity of each other, e.g. in a group mobility model, produce a higher number of available paths with fewer chances of disconnection over a short period of time. Such attributes significantly affect the network protocol performance, which must be taken into consideration when performing the simulation. Third is the node density, which is an extremely important parameter for the measurement of a routing protocol's performance. Finally, a mobility model is also characterised by the number of neighbour nodes, which affects the degree distribution of the node in a particular area.

There are basically two general approaches of modelling mobility in MANET, trace based and stochastic based. In what follows, the differences between the two approaches are presented.

4.3.4 Trace Based Mobility Model

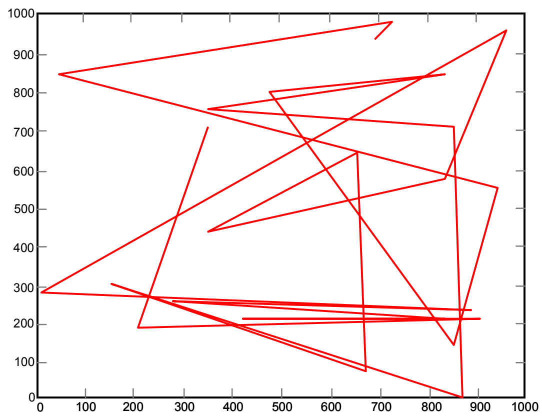
In this approach, the mobility model is designed with deterministic value, where nodal movement is the result of real data traces of the motion of pedestrians, vehicles and etc. In such models, a substantial amount of data is collected on a designated geographical area with long observation over a period of time. Although such data is difficult to obtain, some works [122][123] on real-traces collection exists and the data acquired has been published. Nonetheless, such models lack arbitrariness and may not be suitable for applications on a different MANET environment. For instance, traces for bus movement

[122] are not sufficient to represent the movement of cars in the city centre, since routes taken to a specific destination by the public transports may be shorter and consist of more frequent stops compared to private vehicles. Another example is the study at Dartmouth College campus [124], which observes the user mobility characteristics from the wireless network traces. The study discovers that the speed and pause distribution of the mobility characteristics closely follows the log-normal distribution. Students choose to frequently follow popular roads and walkways on the campus and thus, create a non-uniform distribution of direction of movement across the campus.

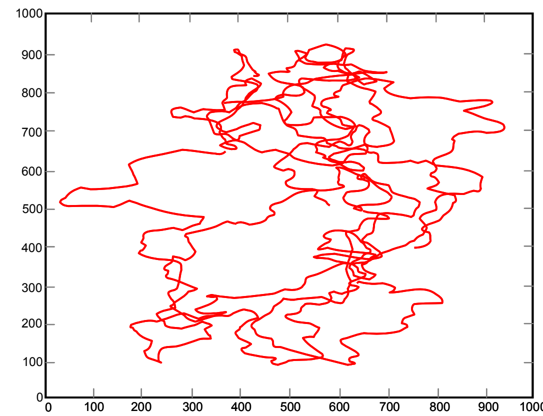
4.3.5 Stochastic Based Mobility Models

By contrast, a stochastic based mobility model is derived from mathematical modelling, which mimics the nodal movement in real world. In such a form, the nodal mobility is modelled as close as possible to the characteristics of a real node in MANET scenario, to the effect that it can influence the outcome of the simulated protocol. The stochastic mobility model can be categorised into two types based on the randomness [121]. The first is characterised by total randomness, where the nodal speed and direction are only restricted to a predefined upper and lower limit. In addition, nodes are not restricted to moving only a particular path between any two points. The second type is the constrained topology-based, where nodes are constrained to move within restricted areas or along paths. Such nodal mobility may represent a vehicle moving along the roads or a person walking in an office building.

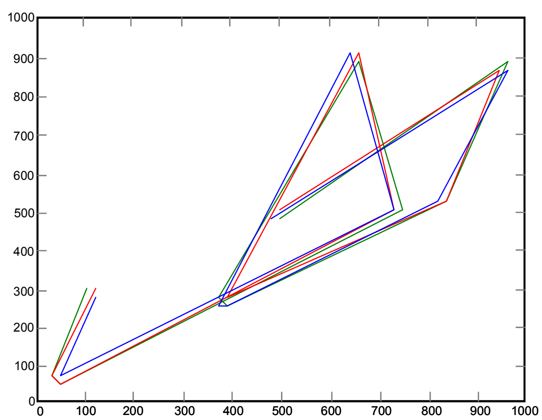
To demonstrate that a particular routing protocol is robust across various types of nodal mobility behaviour, the simulations performed in the subsequent chapters in the thesis are underpinned by four distinct mobility models: RWP [86], GM [125], RPG [126] and Manhattan [127]. The RWP and GM model are both categorised as total randomness, whereas RPG and Manhattan mobility models belong to the group of constrained-topology. Based on the mobility characteristics, nodal movement in the RWP model are fully randomised with the speed and direction of travel uncorrelated. On the other hand, the GM model is derived from a controlled random process. The nodal mobility is typically characterised by temporal dependency of speed and direction based on historical record of nodes movement. In the RPG model, nodes tend to move collectively and alongside each other. Such a mobility pattern is termed as mobility model with spatial dependency. And lastly, the Manhattan is a model that represents nodes moving in a restricted geographical condition. Figure 4.3 illustrates the basic nodes movement in each mobility model and the discussion and comparison between them is presented in the following section.



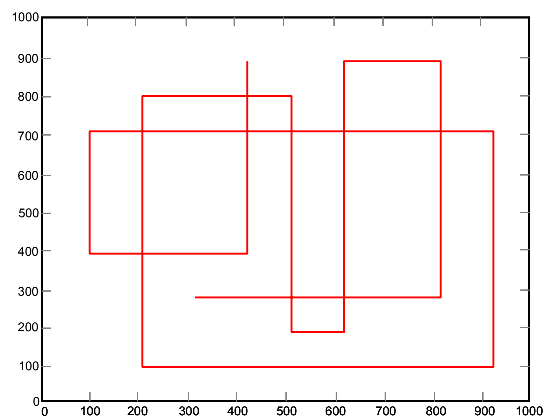
(a) Random WayPoint



(b) Gauss Markov



(c) Reference Point Group



(d) Manhattan

Figure 4.3: Nodes movement in mobility model

4.3.5.1 Random WayPoint Model (RWP)

The RWP model was first modelled by Johnson and Maltz for the simulation of DSR protocol. Several studies on the accuracy of the randomised mobility models have been presented [118][119][121], where researchers discussed the harmful impact of random stochastic mobility patterns on the simulation process. Nevertheless, the RWP is the most common mobility model for the simulation of MANET. In this elementary model, each node moves unnaturally under a wide range of mobility patterns. Additionally, nodal movement is independent of the previous speed and direction, i.e. memory-less. As such, a node travelling in a straight line may instantaneously switch direction during its course, causing sharp turns and sudden stops. The model is considered unrealistic and may generate an extremely hostile topology condition. Nodes can move in a zigzag fashion at constant speed, causing severe performance degradation of the routing protocol. Despite the fact that the nodal motion in RWP is harmful [121], it is ultimately beneficial to be used in simulation analysis as it can provide valuable insights into the robustness of a routing protocol.

In principle, each node is set with a random initial position (x,y), with x and y is distributed over $[0,X_{max}]$ and $[0,Y_{max}]$, respectively. The X_{max} and Y_{max} represent the upper bound of the network area. Similarly, the destination point (x',y') for each node is chosen using similar procedure as (x,y). The speed, v, is then determined from a uniformly distributed interval between (V_{min}), which is usually a null speed, and the maximum allowable speed (V_{max}). From this initial position, the node travels along a straight path at a constant v, and upon reaching the destination, pauses for a time set by the pause_time, *(pt),* parameter. The pt can be either a constant value or randomly selected from a set of distribution. Once the pt expires, nodes move to the next predetermined destination by the same process, and is repeated until the simulation ends.

Despite the fact that RWP is frequently used in many MANET simulations, results based on the model may not always be credible. Simulation outcomes are typically affected by the average speed steady state issue, caused by some nodes moving at a very low speed.

This is shown previously [121], where it was found that a collection of nodes in the model tends to gradually move more slowly as the simulated time progresses. In order to eliminate any ambiguity in results, each RWP-based simulation run must be subject to steady state detection analysis. Chapter 3 provides a detail discussion of the methods used for the steady state process (transient removal).

4.3.5.2 Gauss Markov (GM)

The GM mobility model is proposed to overcome the drawbacks of RWP model. In this model, trace generation is autoregressive and it produces a more realistic model, where nodes determine their next vector to future locations based on the historical speed and direction. Nevertheless, GM model is not particularly common in MANET simulation studies due to its complexity in mobility computation; it has a larger size model, i.e. trace file, when compared to the RWP model. To define a GM mobility model, consider that nodes are initially placed at random locations in the network. Every node is then assigned with an initial mean speed and mean direction to determine their future movement. At each predetermined time interval, the node computes its next movement based on past speed and direction along with different seed to provide a certain degree of randomness. The value of speed and direction at the n^{th} instance can be calculated by the equation 4.5 and 4.6.

$$s_n = \alpha s_{n-1}(1-\alpha)\bar{s} + \sqrt{(1-\alpha^2)}s_{x_{n-1}} \tag{4.5}$$

$$d_n = \alpha d_{n-1} + (1-\alpha)\bar{d} + \sqrt{(1-\alpha^2)}d_{x_{n-1}} \tag{4.6}$$

The instance of past speed (s_{n-1}) and past direction (d_{n-1}) at $(n-1)^{\text{th}}$ time interval influence the computation of current speed (s_n) and direction (d_n), where $0 \leq \alpha \leq 1$. The value of $\alpha = 0$ sets the mobility to be completely random whereas $\alpha = 1$ generates linear nodal mobility. The parameters $\bar{s}$ and $\bar{d}$ are constants representing the mean value of speed and direction as $n \to \infty$; where $s_{x_{n-1}}$ and $d_{x_{n-1}}$ are random variables from Gaussian distribution. In addition, a node's next location is calculated based on the current position, speed and direction of travel. Both equation 4.7 and 4.8 compute node's future location at n^{th} time interval based on the node position at $(n\text{-}1)^{th}$ time interval.

$$x_n = x_{n-1} + s_{n-1} \cos.d_{n-1} \tag{4.7}$$

$$y_n = y_{n-1} + s_{n-1} \sin.d_{n-1} \tag{4.8}$$

4.3.5.3 Reference Point Group (RPG)

The RPG mobility model is based on the assumption that group motion occurs frequently in MANETs. This model may represent the group movement of several rescue teams in a disaster area such as earthquake, where each team movement is directly associated with the group leader movement.

The RPG model is a different entity compared to other models discussed in this section. In this model, individual node movement is influenced by the group movement pattern. Nodes are clustered into groups and their random speed ($V_{node}(t)$) and random direction ($\theta_{node}(t)$) revolve around a predefined individual reference point, i.e. group leader. Subsequently, the group leader is set with a group motion vector ($V_{group}(t)$, $\theta_{group}(t)$). In order to control the deviation value of individual node's speed and direction, a speed standard deviation (*SSD*) and angle standard deviation (*ASD*) are used. Based on the deviation value, the node's movement can be calculated by equation 4.9 and 4.10.

$$|V_{node}| = |V_{group}| + rand.*SSD*V_{\max} \tag{4.9}$$

$$|\theta_{node}| = |\theta_{group}| + rand.*ASD*\theta_{\max} \tag{4.10}$$

The V_{max} is the maximum limit of allowable speed and θ_{max} is the turning angle for each node.

4.3.5.4 Manhattan

For quite some time, simulations of MANETs are based on movement of nodes with randomised waypoints. However, in recent years, particularly with the development of Vehicular Network (VANET), researchers are more aware on the impact of such model to the output of simulation. It has been discussed [128] that an overly simplified model such as RWP does not offer sufficient mobility pattern to satisfy vehicular movement characteristics. Consequently, Manhattan mobility model is developed to overcome the shortcomings of random mobility model. In this model, the path of travel is depicted as roadways in a grid-like fashion of a city, representing an urban area in which nodes move in a constrained area. The model is also ideal for simulating scenarios such as campus environment with pathways, where pedestrians, i.e. students, are allowed to move only within the region in both directions with a velocity set to equal to the human walking speed.

The mobile nodes are assumed to be uniformly distributed with restricted travelling directions. Although this model has high spatial and temporal independence, it has some limitations in that nodes move specifically in a straight line and at a constant speed, which is not as realistic compared to the GM model. However, one particular attribute that this model offers is the nodal ability to decide, with certain probability, the direction to follow at each intersection, i.e. turn left, right or straight on. Such attributes provide some degree of variation in motion pattern compared to the other mobility model previously mentioned, which is essential to take into consideration for protocol measurement.

In summary, each distinct mobility model can effectively represent the movement of a vehicle or a person. Table 4.1 shows the possible applications for the mobility models discussed.

Table 4.1: Summary of possible application for mobility models

Environment	RWP [86]	GM [115]	RPG [126]	Manhattan [127]
Airport	✗	✓	✗	✗
Battle field	✗	✓	✓	✗
Campus	✗	✓	✗	✓
City Section	✗	✓	✗	✓
Freeway	✗	✗	✗	✓
Conference room	✗	✓	✓	✓
Farmed animals	✓	✓	✗	✓

4.4 Network Connectivity Analysis

This section presents the simulation analysis of unidirectional links in wireless multi-hop network. Many researchers investigate network connectivity by using a random graph technique [129][130]. However, such approach does not provide sufficient information of the performance of a routing protocol. Hence, a new performance metric is developed and used along with other existing method. The technique quantifies the probability of success to create a routing path and can provide a more precise way to analyse the efficiency of a particular routing mechanism. Several random topologies with two different radio propagation model, i.e., two-ray ground and log-normal shadowing, are generated with link connectivity formed using a high power and low power nodes. A high power node is typically set with a radio power that is twice as much as the low power node. The wireless interface model in the simulation follows the specification of Cisco Aironet 350 [90], which is also quite similar radio interface chosen in previous empirical work [106]. Based on such interface, the transmitter power can be varied between six different levels, shown in Table 4.2

Table 4.2: Radio transmitter power

Parameter	Parameter Value
Available transmit power settings	100 mW (20 dBm) 50 mW (17 dBm) 30 mW (15 dBm) 20 mW (13 dBm) 5 mW (7 dBm) 1 mW (0 dBm)

4.4.1 Definition of Connectivity and Topology Model

Consider a connectivity model denoted by a set of nodes defined by $V = \{v_1, v_2, ..., v_n\}$, with initial node placement randomly distributed within a heterogeneous multi-hop wireless ad hoc network. Each node is set with an omni-directional antenna that can be adjusted to vary the strength of transmission power. As such, depending on separation distance between adjacent nodes, a link between each node can be either unidirectional or bidirectional. Let P_v be a node's transmission power, then $P_v^{\max}$ is the maximum allowable transmit power by the interface specification. Typically, if adjacent nodes v_x and v_y, $(x \neq y) \in V$, can form a symmetrical link, then the required transmission power for node v_1 to reach node v_2 is $P_{v_1 v_2}$ which is equal to $P_{v_2 v_1}$. However, when $P_{v_1}^{\max}$ is not equal to $P_{v_2}^{\max}$ for which $v_1 \neq v_2$, then a formation of asymmetrical link can occur if $P_{v_1}^{\max} \geq P_{v_1 v_2} \geq P_{v_2}^{\max}$. In such case, node v_1 can reach v_2 using $P_{v_1}^{\max}$ but node v_2 is unable to reach v_1 using $P_{v_2}^{\max}$.

The topology of the network can be modelled as an undirected graph, $G = (V, E)$ where each node is assumed to transmit at $P_v^{\max}$. V is the set of nodes in the wireless network and E is the set of edges or directed links. An edge $E_{v_x v_y} \in E$, if node v_y is within the transmission range of node v_x. The Euclidean distance between the nodes can be denoted by $d(v_x, v_y) = D_{xy}$. Subsequently, if a network topology G is bidirectionally connected, it implies that the distance between each pair of adjacent nodes is within the transmission power of each other. Denoting transmission power as a function of distance, the network can be represented by $P(D_{xy}) = P(D_{yx})$. On the other hand, a unidirectionally connected network implies that a network topology may have some degree of unidirectional links. As such, $P(D_{xy}) = K \cdot P(D_{yx})$, where $0 \le K \le 1$. K is a constant which denotes the number of unidirectional links to the total amount of links in the network. Therefore, when $K = 0$, the network can be considered fully unidirectional, where each node is completely isolated to each other. On the contrary, when $K = 1$, all links are bidirectional and nodes form a fully connected network.

In the next section, a typical network performance analysis using link connectivity is presented. Then, a new performance metric is proposed in section 4.4.3, which will be compared in the simulation works in the subsequent section.

4.4.2 Link Connectivity

A statistical research study by Bettsetter [129] presented an analysis of *link connectivity* based on undirected graphs. The work investigates a fundamental characteristic of MANET; the minimum node degree essential for multi-hop communication. Node degree, *d*, is defined by the number of neighbours associated with a particular node. In other words, a node with a degree $d = 0$ is an isolated node and therefore has no neighbours. To achieve a connected network, the minimum requirement for any MANET is $d \geq 1$. In this case, every node in the network is presumed to have at least one link connecting to its neighbour. Analytically, the paper derived a mathematical expression to determine the probability of link connectivity, given by the equation 4.11.

$$P_{lc} = (1 - e^{-\rho \pi r^2})^n \tag{4.11}$$

The P_{lc} is the probability of link connectivity, ρ is node density, r is node transmission range, and n is the number of nodes in the network. The P_{lc} simulation results presented in the section 4.6.3 consider only the minimum node connectivity (i.e. $d \geq 1$).

4.4.3 Routing Connectivity

This section proposes a new routing performance metric referred as the probability of *route connectivity*, P_{rc}. In contrast to link connectivity, P_{rc} measures the number of successfully constructed routes over a random set of network topologies. The link connectivity, P_{lc}, analysis on a network provides an incomplete view on the connection between a pair of source and destination nodes. A high value of link connectivity or a network with node degree, $d \geq 1$, is not sufficient by itself to suggest that a routing protocol may perhaps be able to effectively construct a routing path. Hence, by using P_{rc} as a performance metric, the analysis of network connectivity on a particular routing protocol can be supplemented. The P_{rc} is measured based on a network topology that can be expressed by undirected graph, $G = (V, E)$, as previously discussed. A bidirectional link between any two nodes exists if they lie within the transmission radius of each other. Also, the routing path between a pair of source and destination nodes can only be set up if there are sufficient links to complete the connection. Since nodes are mobile, the paths (E), change randomly over time and therefore, the analytical based performance evaluation is not generally feasible. For this reason, a very large number of repetitions are made on the simulation experiments, where each run is associated with a different network topology. At any instance, the total number of routing path in a network topology can be defined as E_t. Assuming all nodes (V) have sufficient energy to remain active throughout the simulation and they are kept bounded within the network region; the undirected graph at instance t can be given by equation 4.12, where G_t is a subset of G.

$$G_t = (V, E_t) \tag{4.12}$$

Node mobility is an important factor which affects the computation of route construction, where routing paths continuously form and break. For instance, a network scenario in which the nodal mobility is not null, i.e. constantly mobile, the number of routes established will have to be computed and averaged over several snapshots. For instance, in Figure 4.4, the m^{th} scenario is equally partitioned with 18 snapshots within 900 s of simulation time. The effective number of routes established throughout a single simulation run is computed 18 times in succession of the snapshots. The number of snapshots, n, can be of any real number, and setting n to a higher value will increase result accuracy.

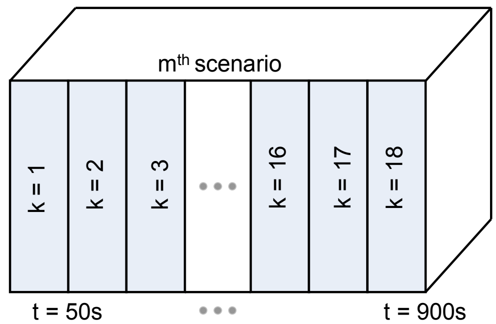


Figure 4.4: A scenario with 18 snapshots

Mathematically, the average success of route construction in a particular network scenario (a single simulation run) can be expressed by equation 4.13.

$$\overline{E_t} = \overline{E_1 + E_2 + E_3 + \ldots + E_n} \qquad (4.13)$$

The simulation is then repeated over large set of scenarios, which results in equation 4.14.

$$P_{rc} = \frac{\sum_{j=1}^{j=m} \sum_{k=1}^{k=n} \overline{E_{k,j}}}{m} \qquad (4.14)$$

The P_{rc} is the probability of route connectivity success, m is the total number of scenarios, and n is the number snapshots obtained from the m^{th} scenario. A unique case for which n = 1, i.e. a singe simulation run without partitioning, can be represented using equation 4.15.

$$P_{rc} = \frac{\sum_{j=1}^{j=m} (\overline{E_j})}{m} \tag{4.15}$$

Equation 4.15 is equivalent to a measurement of P_{rc} over an average of m^{th} scenario without partitioning throughout the entire simulation time.

The performance metric, P_{rc}, is employed for routing performance analysis in this chapter and then later in Chapter 6 for the mobility model investigation purposes.

4.5 Simulation Framework

In essence, the simulation experiments are used to investigate the effect of unidirectional links on node connectivity. The AODV routing protocol is chosen as the case study because it forms the basis of the proposed scheme (to be discussed in Chapter 5 and 6). The simulation experiments consist of three parts. Firstly, to quantify the routing performance with varying radio power. Different levels of radio signal strength are employed using the parameters shown in Table 4.2. Secondly, the propagation model is varied to observe the impact of power fluctuations on the routing path setup. The final part of the experiment is to analyse the impact of mobility models on the network performance. Each set of experiments are assigned with four mobility models as previously mentioned; the RWP, GM, RPG, and Manhattan. The experiments conducted are extensive, which involves a lot of computing resources. Appendix-A shows the estimated time required to undertake each simulation experiment in this thesis.

4.5.1 Mobility and Traffic Model

The nodal movement pattern is generated using the BonnMotion [131] scenario generator tool. This tool is able to provide several mobility models including the RWP, similar to the model generated by using the *setdest* [77] script included within NS-2. A simple AODV routing protocol's performance using RWP nodes movement generated from both tools were conducted, and results shown an acceptable level of consistency.

This step is to ensure that the scenario produced by BonnMotion is compatible with the NS-2 simulation engine. Nonetheless, many studies [132][133][134][135] have also used BonnMotion to evaluate the protocol's performance.

The traffic pattern is generated using connection pattern generator script *cbrgen.tcl* [77]. Random constant bit rate (CBR) traffic is chosen as it is widely used in MANET simulation. The CBR is transport with user datagram protocol (UDP) instead of Transport Control Protocol (TCP). There are several reasons TCP is not used in this evaluation. First the TCP adopts several mechanisms to control the data flow, and as such, it can cause the simulation to behave in unforeseen ways. Thus, it is more difficult to fairly evaluate the performance of routing protocols. Secondly, TCP requires an acknowledgement to be sent back to source, for each data packet received by the destination node. This goes in conflict with the typically low capacity of ad hoc networks. On the other hand, the CBR traffic can effectively stresses a network as there are no control mechanisms to consider when flows are delayed or a packet is lost. Traffic sources are CBR nodes chosen randomly from the full set of nodes generating 512 bytes data packets at a rate of 4 packets per second. Simulations are run for 900 seconds of real time[10]. Each data point represents an average from twenty five runs each using different seeds, with a corresponding confidence interval of 95%.

4.5.2 Radio Transmitting Power

The simulation employs a different radio interface specification from the validation work in Chapter 3, which adopts the Lucent WaveLAN 914MHz wireless card (Table 3.3). However, in this section the nodal interface is set to follow the settings used in previous empirical work [136]. This reflects a more practical network interface for a non-line-of-sight (NLOS) wireless communication operating at 2.4 GHz frequency. The wireless interface is based on Cisco Aironet 350 Client Series Data Sheet [90]. Table 4.3 shows the difference between the two radio interfaces specifications.

[10] The total simulation time is set to 2000 seconds and due to steady state issue only the final 900 seconds of data is recorded. The steady state is discussed in section 3.7.1.1.

Table 4.3: Comparison of radio interface specifications

Parameter	Lucent WaveLAN	Cisco Aironet 350
Data rates	2 Mbps	2 Mbps
Network standard	IEEE 802.11b	IEEE 802.11b
Frequency band	914 MHz	2.4 GHz
Wireless medium	Direct Sequence Spread Spectrum (DSSS)	Direct Sequence Spread Spectrum (DSSS)
Media Access Protocol	CSMA/CA	CSMA/CA
Modulation	Differential Quadrature Phase Shift Keying (DQPSK)	Differential Quadrature Phase Shift Keying (DQPSK)
Receiver Sensitivity	-80 dBm	-91 dBm
Transmitter power	24.5 dBm	0 dBm to 20 dBm
Power consumption	Tx: 3 W Rx: 1.48 W Sleep: 0.18 W	Tx: 450 mA Rx: 270 mA Sleep: 15 mA
Antenna	Omnidirectional	Omnidirectional

To enable the investigation of routing performance in network scenarios with different intensity of unidirectional links, different sets of nodes are generated. Each set comprises a mixture of nodes assigned with two different levels of transmitter power, P_t (*Two-power*). Intuitively, this approach is sufficient to vary the number of unidirectional links in the network. The two levels of P_t refer to high power nodes assigned with P_{thigh} and a set of low power nodes, with P_{tlow}. The receiver sensitivity, *RXThresh*, for all nodes are set to -91 dBm. Although nodes are set to transmit at low data rate, i.e. 4 packets/second, such a rate is sufficient to monitor the impact of packet loss due to unidirectional link. Nevertheless, the number of source and destination pairs is quite large, where half of the nodes are set to transmit data packets throughout the simulation. Therefore, increasing the packet rate will only increase the simulation output time without any significant benefits for the results. Table 4.4 shows the variation of high power and low power nodes combinations. For example, Set 1 indicates 10% of the nodes are designated with P_{tlow} while the remaining 90% are set with P_{thigh}.

Table 4.4: Ratio of P_{tlow} to total number of nodes

Set No.	**Set 0**	**Set 1**	**Set 2**	**Set 3**	**Set4**	**Set 5**
Ratio of low power nodes(P_{tlow})	0	0.1	0.2	0.3	0.4	0.5

In addition to the two different level of transmitter power, the radio interface is also changed between 0 and 20 dBm to reflect a random variation of transmission range. Such method enables the study of link and routing path connectivity, which can show the ability of a routing protocol to correctly perform routing operation under various transmitter powers.

4.5.3 Performance Metrics

The analysis of AODV routing protocol is subject to four performance metrics:

- *Average RREQ packet sent:* The average number of RREQ packet transmitted in each connection by every source node. When route discovery fails to setup a routing path, perhaps due to unidirectional link, the source rebroadcast the route using the network wide broadcast, which can cause congestion. Thus, the average route request is an important metric, as it can show the effect of network routing overhead.
- *Normalised unidirectional link:* The normalised unidirectional link is calculated based on the total number of unidirectional links to the number of RREP packet received by source node for each routing path constructed. Essentially, a lower value of normalised unidirectional link indicates efficient route handling. In such cases, the number of routing path is sufficiently high to overcome impact of unidirectional link on the network.
- *Probability of link connectivity:* The probability of success to create a fully connected network, where the minimum degree, $d \geq 1$. When there is at least one node isolated in network, the connectivity is incomplete, reducing the probability of link connectivity.

- *Probability of route connectivity:* The average number of successful routing path construction, repeated over several scenarios. Nodes that are not part of the routing path do not affect the probability of routing connectivity. An isolated node that neither assigned as the source or destination, nor does not participate in the routing path computation is ignored.

4.6 Simulation Results and Discussion

The first objective of the simulation is to confirm that the radio setup used in the experiment can correctly produce the appropriate number of unidirectional links. As it is quite difficult, by simulation, to generate precise numbers of unidirectional link throughout the simulation time, the two-power approach is adopted. Second objective is to investigate the impact of mobility and propagation models on the outcome of unidirectional link in the network. Each performance metric is quantified according to the following models:

- Two-ray ground model
- Log-normal shadowing model
- Random Waypoint mobility model
- Gauss Markov mobility model
- Reference Point Group mobility model
- Manhattan mobility model

In each model, there are a range of parameters to be configured. Table 4.5 shows the variation of parameter values for power model, Table 4.6 shows the settings used in the propagation model, and Table 4.7 shows the parameters for mobility models. A common set of parameters used for every experiments are shown in Table 4.8

Table 4.5: Propagation model parameters

Parameter	Two-ray ground	Log-normal shadowing
Path loss exponent	n.a	3
Gaussian random variable ($X\sigma$)	n.a	0 mean with shadowing deviation 4dB
Reference distance	n.a	1 m
Antenna height	1.5 m	1.5 m
Loss	1	1
Gain	1	1

Table 4.6: Radio model parameters

Parameter	Two power	Multiple power
Transmit power (P_{thigh})	15 dBm	20 dBm – 13dBm
Transmit power (P_{tlow})	7dBm	13 dBm – 0 dBm
Receiver sensitivity	-91 dBm	-91 dBm

Table 4.7: Mobility model parameters

Parameter	RWP	GM	RPG	Manhattan
Speed update frequency	n.a	2.5 s	n.a	n.a
Angle std deviation	n.a	45 degree	n.a	n.a
Speed deviation	n.a	1.5 m/s	n.a	n.a
Group size	n.a	n.a	10 groups	n.a
Maximum node distance from group centre	n.a	n.a	100 m	n.a
Probability change group	n.a	n.a	0.1	n.a
Group deviation	n.a	n.a	2	n.a
Pause time	0 s	n.a	0 s	0 s
Number of blocks (x,y)	n.a	n.a.	n.a	(5,5)
Cut off time	0-1100 s	0-1100 s	0-1100 s	0-1100 s

Table 4.8:Common simulation parameters

Parameter	Parameter value
Simulation network area	1000 x 1000 m^2
Number of nodes	50
Simulation time	900 seconds
Source-destination pair	25
Maximum node speed	20 m/s

4.6.1 Average RREQ packet

The number of RREQ packets generated in the network is an important characteristic affecting the routing operation, particularly for protocols that rely on request broadcast approach such as AODV, DSR, and DSDV. Frequent dissemination of RREQ packets can cause severe congestion, and consequently affects the number of data packet transmitted to the destination. Other external elements such as path loss and non-uniform transmission range may also cause links to fluctuate, leading to a formation of a transient or permanent unidirectional links.

The average number of RREQ packets sent by each source is shown in Figure 4.5 and Figure 4.6. The simulation output based on two-ray ground model is shown in Figure 4.5 while Figure 4.6 shows the output when the propagation model is changed to log-normal shadowing. Based on observations, the impact of path loss, as a result of varying the propagation model is quite obvious. As discussed in section 4.3.1.1, the two-ray ground model considers only two forms of signal propagation; the main signal and the reflected signal. For this reason, there is lower variation of received signal at any point around the node when compared to the log-normal shadowing model. The log-normal shadowing model generates a more realistic signal propagation approach, where the received strength is non-identical for each packet received by a node. Therefore, the probability of link failure increases, leading to increased route discovery attempts by the source node.

Generally, as the ratio of low power nodes increases, the number of RREQ packets sent by each source increases. The main reason for the increasing number of RREQ packets is because of the failure to construct routing path. This causes the source node to rebroadcast the RREQ packet several times before it succeeds. As the low power node ratio increases, the average number of RREQ packet increases. Clearly, such results indicate that the number of unidirectional link for each set was appropriately generated by using the two power level approach.

Another important observation is the effect of varying the mobility model. Four different mobility patterns are investigated, each with their unique characteristics. The GM mobility model produces a smooth node trajectory; where a nodes move in a more natural way as shown previously in Figure 4.3b. As such, the occurrences of link breakage are lower compared to the RWP and Manhattan. The probability of forming a routing path is also higher, reflected by the lower average number of RREQ packets sent by source node, shown by Figure 4.5 and Figure 4.6. On the other hand, in the RWP mobility model, nodes are constantly moving (due to 0 sec pause time) in a straight line before abruptly turns into another direction. In such cases, a connection between a pair of source and destination can be easily disrupted, leading to route breakage. In addition to the abnormal nodes movement, the variation of signal strength can also causes a slight increase of RREQ packet. The RPG is a group-based mobility model; hence, nodes are tightly bound together in a restricted area around the group leader. Nodes are in proximity and as such, the link connectivity is more stable compared to other models. The average RREQ packet sent by every source is the lowest, which indicate that route breakages are significantly lower. Finally, the Manhattan mobility model generates the highest number of RREQ packets shown by Figure 4.5 and Figure 4.6. The reason is because link connectivity is more severe, caused by the non-uniform distribution of nodes, which is a consequences of having an area with spaced blocks throughout the topology. Nodal movement is also directionally restricted, where nodes move in a straight line. At an intersection, the nodes are able to turn right, left or move straight on with certain probability.

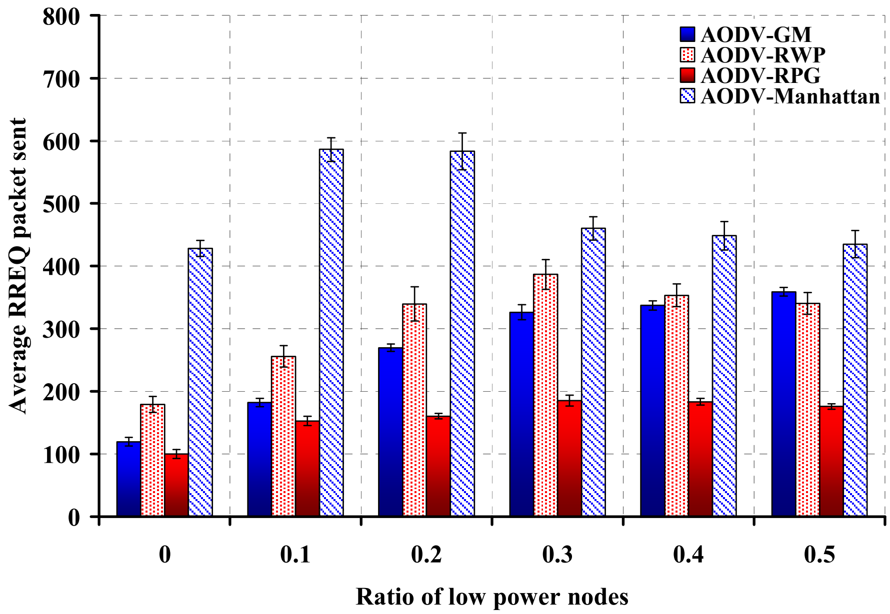


Figure 4.5: Average RREQ packets (Two-ray ground)

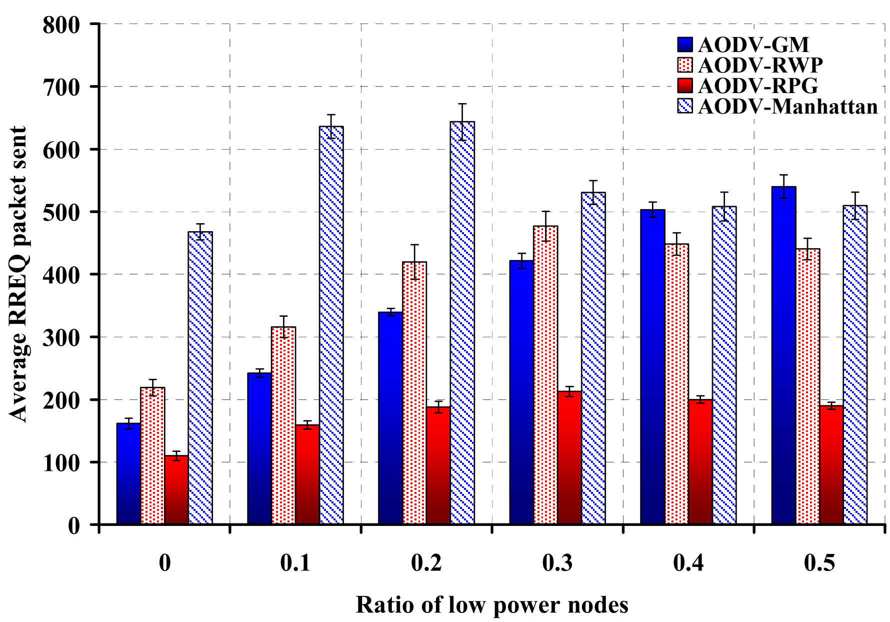


Figure 4.6: Average RREQ packets (Log-normal shadowing)

4.6.2 Normalised Unidirectional Link

Figure 4.7 and Figure 4.8 show the normalised unidirectional link, computed based on the total number of unidirectional link detected to the number of RREP packet received by source. Essentially, a lower normalised unidirectional link indicates better performance. The accumulated number of unidirectional links for a session could be high, but if the source node receives a sufficiently high number of RREP packets, the routing mechanism is considered reliable. This metric provides greater details compared to only computing the total number of unidirectional links. Both figures show the normalised unidirectional link in the GM model slowly increases as the ratio of low power nodes increases. In contrast, the RWP model exhibits an increasing normalised unidirectional link but remain relatively flat after 0.3. The RPG model shows the lowest normalised unidirectional link. Since a large number of nodes are within proximity, only a small number of unidirectional links may exist in the network. On the other hand, the Manhattan model produces a slightly lower normalised number of unidirectional links compared to GM and RWP model, perhaps because of the high number of RREP received by the source node. Nonetheless, the results obtained from Manhattan model indicate a high variation of error interval and this may be due to the significant constraint imposed on the nodal movement. On average, the AODV routing protocol exhibits a higher normalised unidirectional link in log-normal shadowing model compared to the two-ray ground. This behaviour is consistent with the observations made in the previous section (4.6.1).

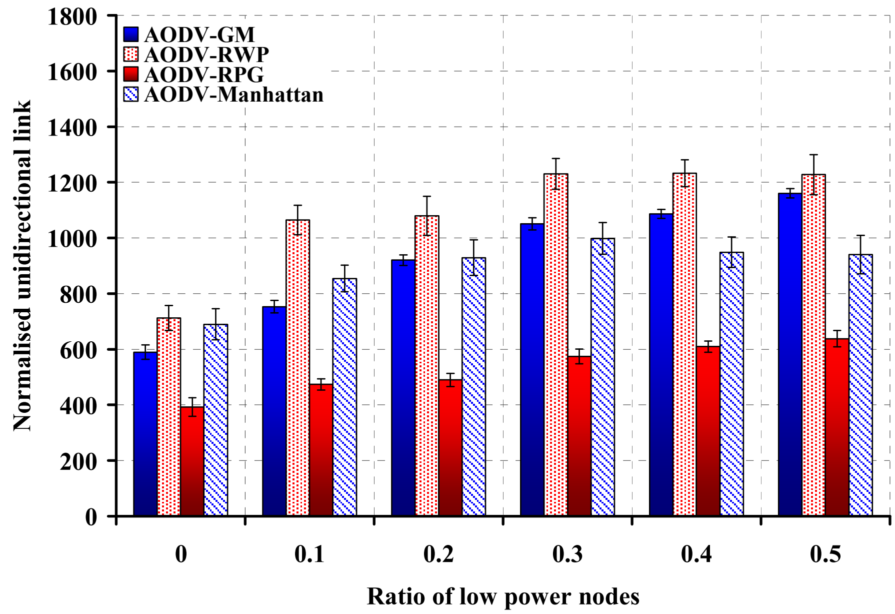


Figure 4.7: Normalised number of unidirectional links (Two-ray ground)

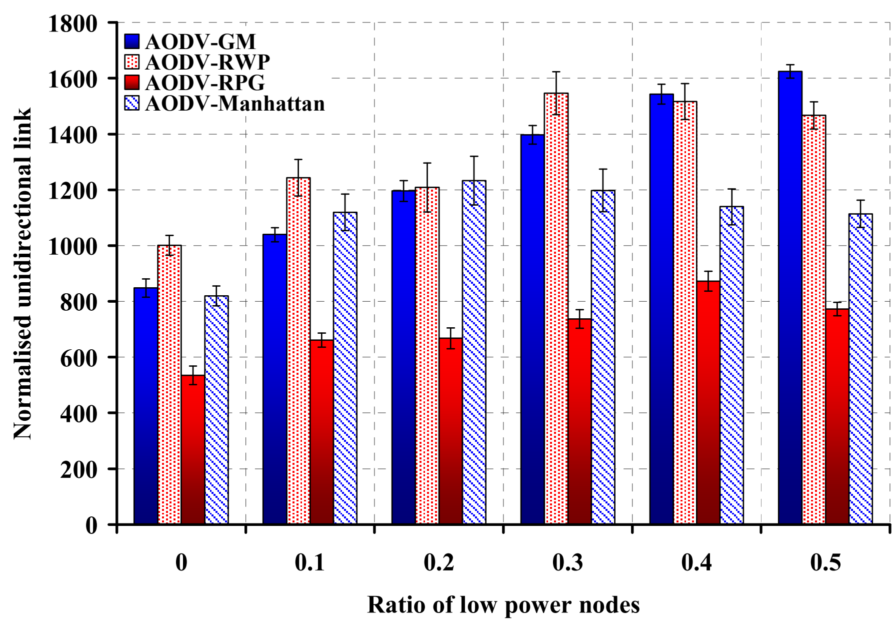


Figure 4.8: Normalised number of unidirectional links (Log-normal shadowing)

4.6.3 Probability of Link Connectivity

As shown in Figure 4.9 through to 4.12, the probability of link connectivity, P_{lc}, varies significantly for different transmission ranges. Each point on the graphs represents a repetition of 25 simulation runs, for which the ratio of low power nodes are set to 0, 0.3, and 0.5 as reported in Table 4.4. At a typical transmission range of 250 m, the GM and RWP model in Figure 4.9 and Figure 4.10 are able to provide the highest percentage of P_{lc} (80%) for set 0, where every node has equal transmitting power. Such a setting is expected to create a higher number of bidirectional links. In contrast, the P_{lc} obtained from the RPG model is only 38% (Figure 4.11) while the Manhattan mobility model achieves a P_{lc} of 70% (Figure 4.12). Nevertheless, when the number of nodes assigned with P_{tlow} increases, the three models demonstrate a steady decrease in P_{lc}, shown by set 0.3 and 0.5 in every graph. This is because nodal reachability has been reduced due to the increase of unidirectional links. As shown in Figure 4.9, at transmission range of 250 m, the P_{lc} drops by as much as 37.5% between set 0 and 0.3. The result implies that, at such theoretical transmission range, even the presence of only bidirectional links between the neighbouring nodes may not always guarantee a fully connected network. A further increase in the number of low power nodes, i.e. set 0.5, has resulted in much lower percentage of P_{lc}; a decrease of almost 76%. In such a condition, in order to achieve a value equivalent to the P_{lc} of set 0, nodal transmission power (P_t) must be increased slightly. For instance, as shown in Figure 4.12, a network assigned with set 5 will have to increase the nodal transmission range by as much as 40 m to gain a comparable performance to set 0, i.e. at transmission range of 250 m, the P_{lc} is 70%). Based on results, the RPG shows the lowest link connectivity compared to GM, RWP, and Manhattan mobility model. It is also shown that at the nominal transmission range, i.e. 250 m, which is specified in many NS-2 simulation works, the presence of unidirectional links can severely impact the MANET's performance. Expanding transmission range beyond this value may potentially increase link connectivity but such a change may only result in severe channel interference; an effect that is not desirable.

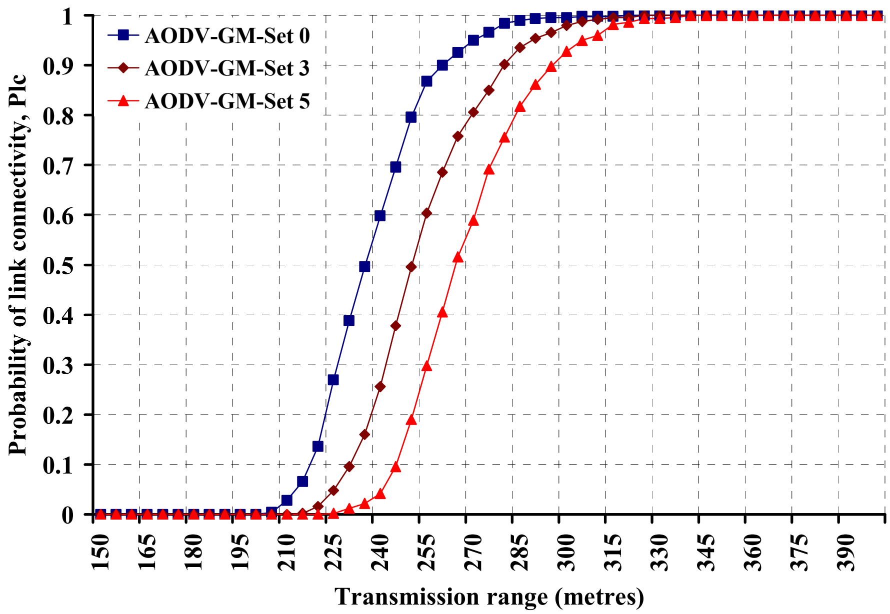


Figure 4.9: Probability of link connectivity (Gauss Markov)

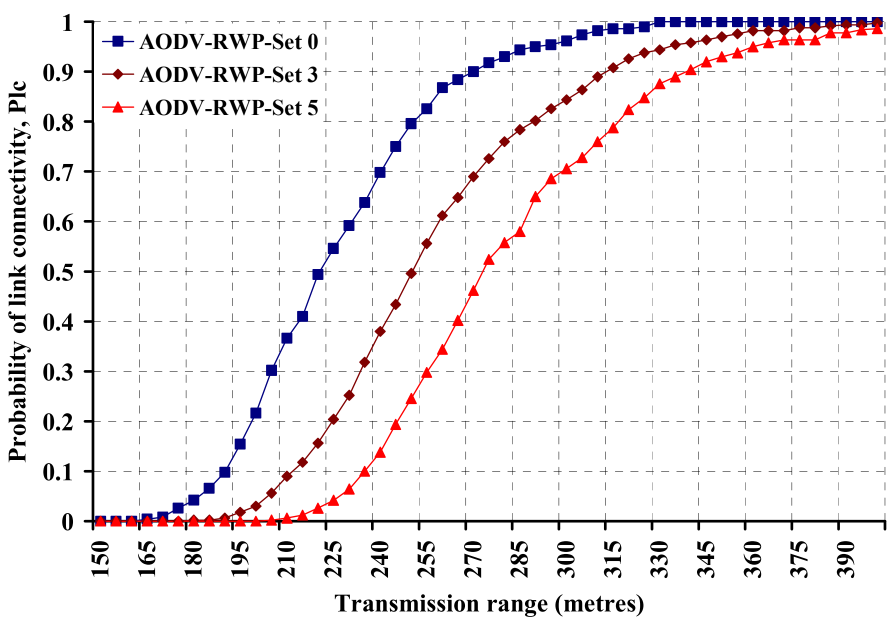


Figure 4.10: Probability of link connectivity (Random Waypoint)

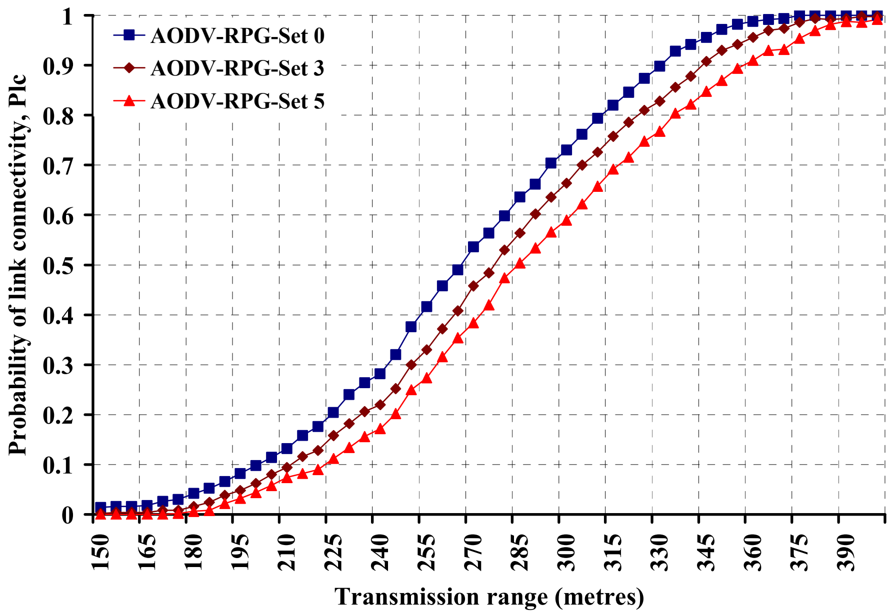


Figure 4.11: Probability of link connectivity (Reference Point Group)

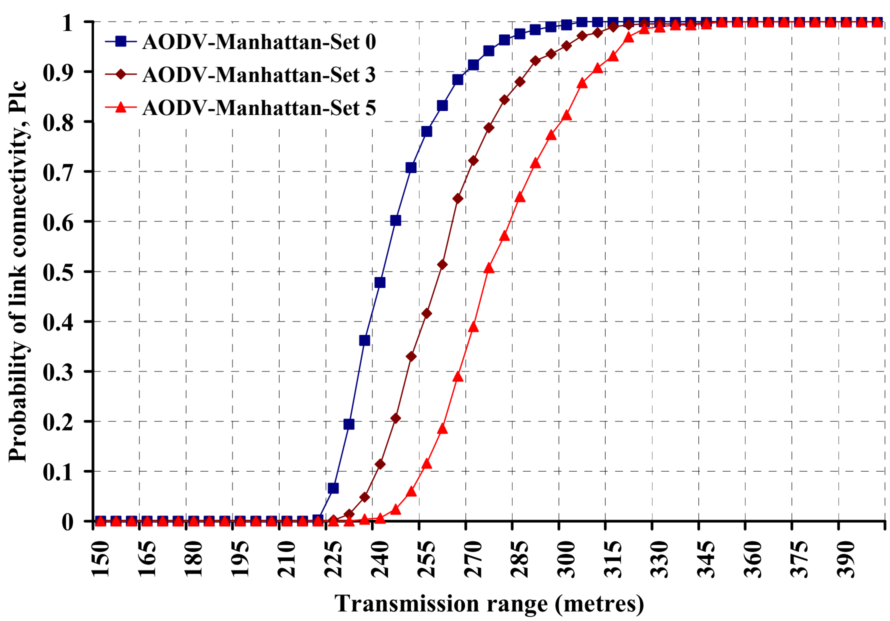


Figure 4.12: Probability of link connectivity (Manhattan)

4.6.4 Probability of Route Connectivity

The results in terms of P_{rc} are shown in Figure 4.13 through to 4.16. P_{rc} is quantified by the number of successful route established. A RREP packet received by the source node indicates that the destination nodes have successfully captured the RREQ packet, thus creating the routing path. Figure 4.13 shows the P_{rc} of the GM mobility model, where each point corresponds to 450 small scenarios (25 repetitions each with 18 partitions) repeated for node's transmission range varied between 150 m to 400 m. The computation of P_{rc} further enhances the analysis of P_{lc}, which can show the precise impact of unidirectional links on routing protocol performance. As expected, the P_{rc} for set 0 nodes show higher performance compared to set 0.3 and 0.5 in every experiment. In Figure 4.13, it is shown that when nodal movement is based on the GM model, AODV can successfully establish a routing path in 435 out of 450 trials when node P_t is homogeneous; transmitting at 250 m. In contrast, the RWP mobility model in Figure 4.14 has shown the highest P_{rc} values across all values of transmission range. In Figure 4.15, the RPG's P_{rc} is comparatively lower than GM's. On the other hand, the Manhattan's P_{rc} is almost identical to GM at P_t greater than 250 m. Generally, the performance of AODV routing protocol drops significantly for set 0.3 and 0.5 across all mobility models. On average, the P_{rc} decreases by as much as 60% between set 0 and 0.5. The significantly low values result from high number of unidirectional links in the network. Consequently, since basic AODV has no unidirectional link detection mechanism, more routing paths will not able to be established, resulting in a lower P_{rc}.

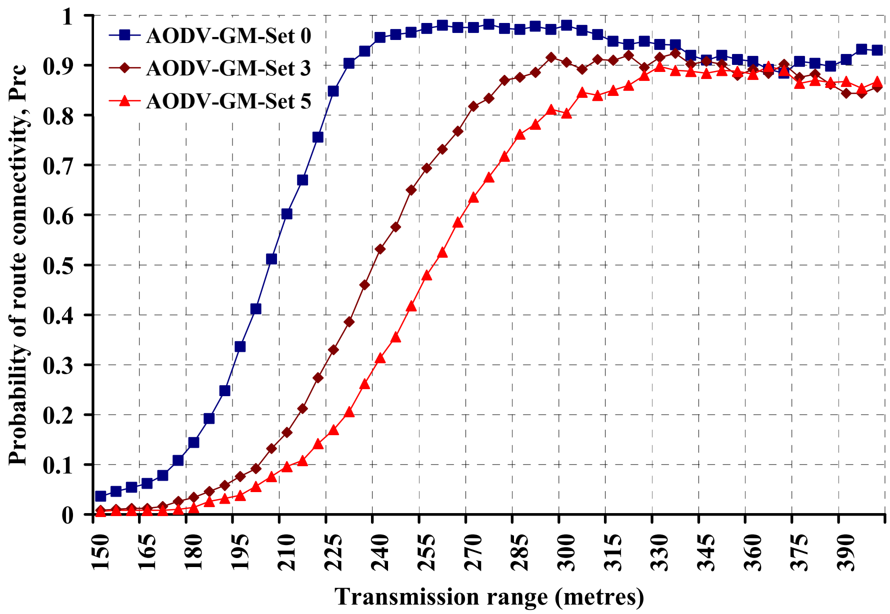


Figure 4.13: Probability of route connectivity (Gauss Markov)

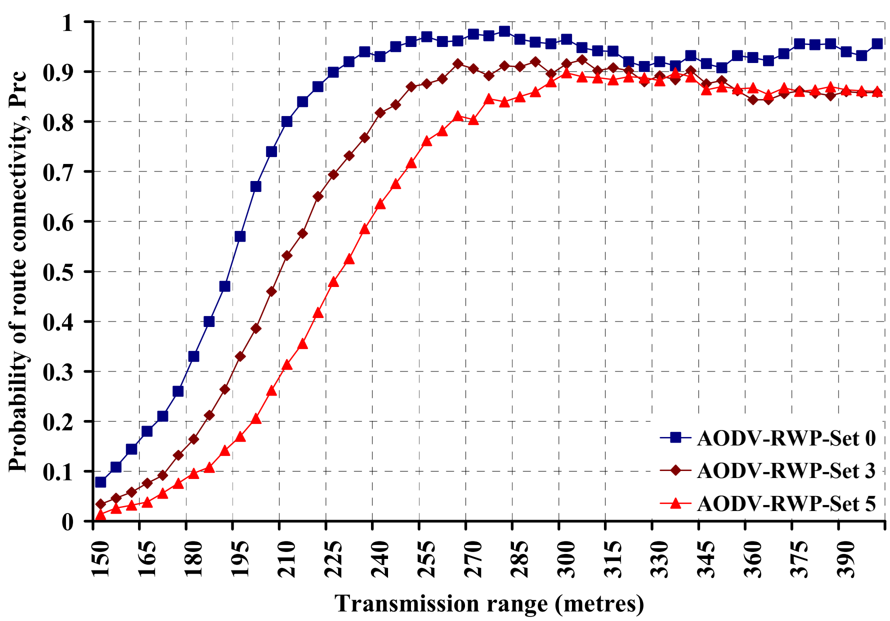


Figure 4.14: Probability of route connectivity (Random Waypoint)

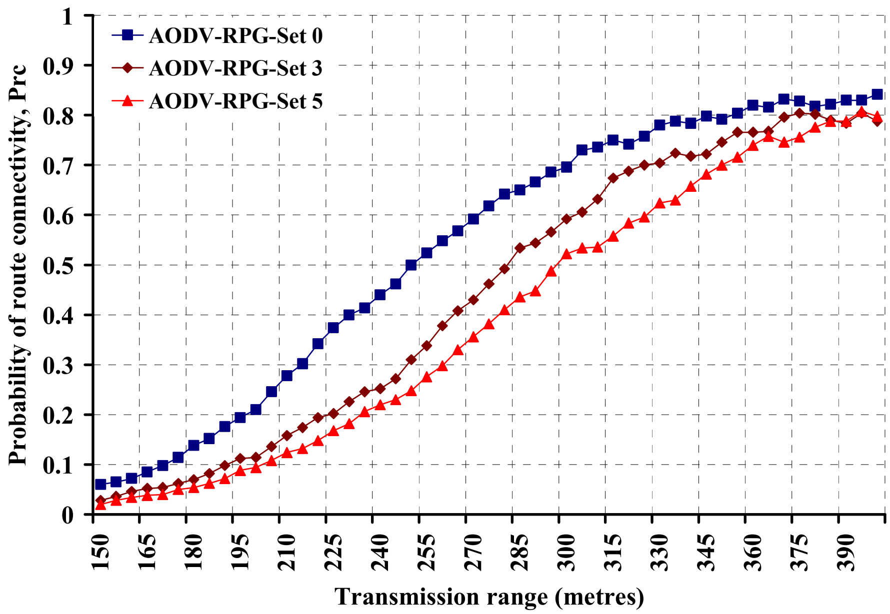


Figure 4.15: Probability of route connectivity (Reference Point Group)

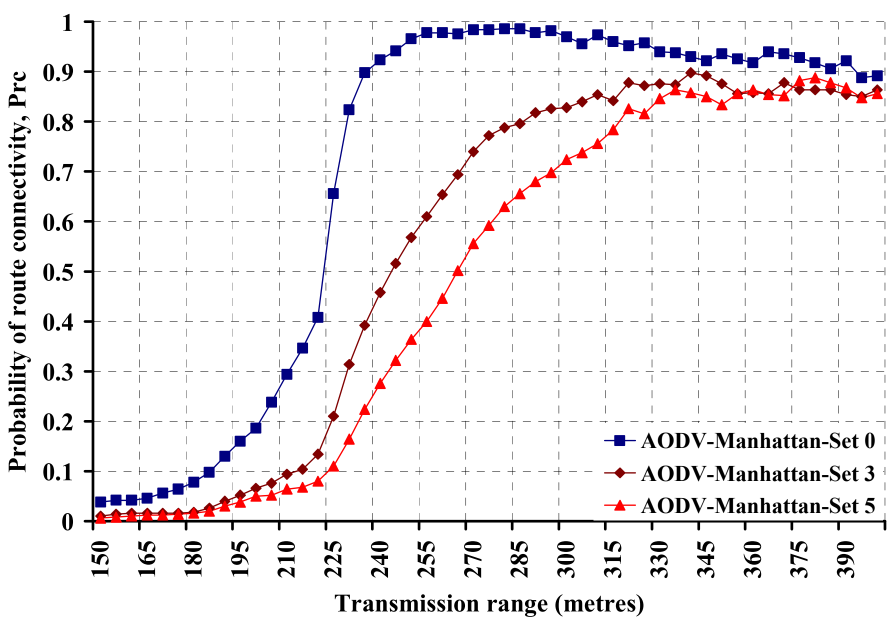


Figure 4.16: Probability of route connectivity (Manhattan)

4.7 Summary

In this chapter, the basic concepts of unidirectional link and the effect it has on the performance of routing protocol were discussed. Much research exists, which has analysed the impact of such links on the network's link connectivity for a specific models. Clearly, the simulation results in this chapter have shown that the choice of system model can significantly affect the output. Four mobility models and two propagation models with unique attributes are highlighted. The RWP mobility model has shown a slightly better performance in terms of probability of link and route connectivity (section 4.6.3 and 4.6.4). Total randomness of RWP mobility model causes nodes to frequently changes position, leading to more short-lived links to be created. Additionally, the nodal movement in RWP is typically unrealistic and results obtained from such model may *not be sufficiently credible*. Thus, the GM mobility model with shadowing effect is chosen to form the system model for the remaining part of experiments within the main body of this thesis. The choice is based on the fact that both the GM and log-normal shadowing model offers a more complex model, which may correctly represent the real-world scenario. In addition, a new performance metric to complement the analyses of link connectivity, referred as the probability of route connectivity is proposed. The metric provides a comprehensive approach to analyse networks impacted by unidirectional links.

5. Dynamic Reverse Route

5.1 Introduction

This chapter presents a novel and practical routing scheme called Dynamic Reverse Route (DRR), implemented over the prominent AODV [45] routing protocol. To setup a routing path, the scheme follows the fundamental operation of AODV. However, the main feature of the algorithm is the ability to build a routing path as efficiently as possible on a network with high number of unidirectional links. The scheme reduces additional routing overhead incurred by the routing construction while rapidly re-computing alternative paths around the nodes that are blocked by unidirectional links. The routing performances are quantified using several performance metrics, which are; packet delivery ratio, normalised routing load, packet loss, and average delay. The scheme and other competing protocols are investigated under various numbers of unidirectional links, nodal speeds, and offered load. The scheme's principles of operation are discussed in section 5.2. The verification of the DRR scheme is presented in section 5.3. Section 5.4 presents the simulation setup. Simulation results and the analysis are discussed in section 5.5. Finally, section 5.6 concludes this chapter.

5.2 Dynamic Reverse Route (DRR) Routing Scheme

In Chapter 4, the analysis of network connectivity has been discussed in detail. The simulation output shows that the presence of unidirectional links within MANETs is significant in various models and may affect the proper operation of many routing protocols. In light of this, a practical scheme, known as the Dynamic Reverse Route (DRR) that can efficiently handle unidirectional links is proposed. The scheme is protocol independent, which can be easily incorporated into other on-demand routing protocols that share similar characteristics with the AODV routing protocol. The scheme is capable of minimising routing overhead and efficiently avoids multiple route request discovery, caused by the lost of RREP packet during reverse path construction.

5.2.1 Routing Operation

Most on-demand routing protocols depend on the bidirectional link availability between nodes. The two-way communication over symmetrical link ensures that the routing protocols are able to correctly exchange control packets to establish and maintain the routing path. However, in some network scenarios, routing packets may be forwarded via paths that are unidirectional. As such, the reply packet is unable to retrace the forward path created, causing the routing path to be partially completed. In the event that a reverse path fails, a typical routing protocol such as AODV and DSDV performs another route discovery broadcast. This increases the delay to form the routing path, caused by route rediscovery. In the following section, the scheme's routing operation is presented.

5.2.1.1 Route Discovery

The route discovery is the phase initiated by a node when its routing entry, i.e. a valid next hop node pointing to the destination, does not exist within the routing table. As such, the node's system moves to the next process state, which is the route discovery phase. At this point, a RREQ packet is formed by including the information that is unique to that particular session. Figure 5.1 shows the formation of a RREQ packet before broadcast. The IP header contains the address of the source and destination nodes, which remain the same throughout the route discovery phase. On the other hand, the request packet header stores the information related to RREQ packet, i.e. timestamp, hop count, sequence number, broadcast ID, packet type, and the request packet address. The information within the request packet header such as hop count and request packet address, changes with every hop visited by the packet.

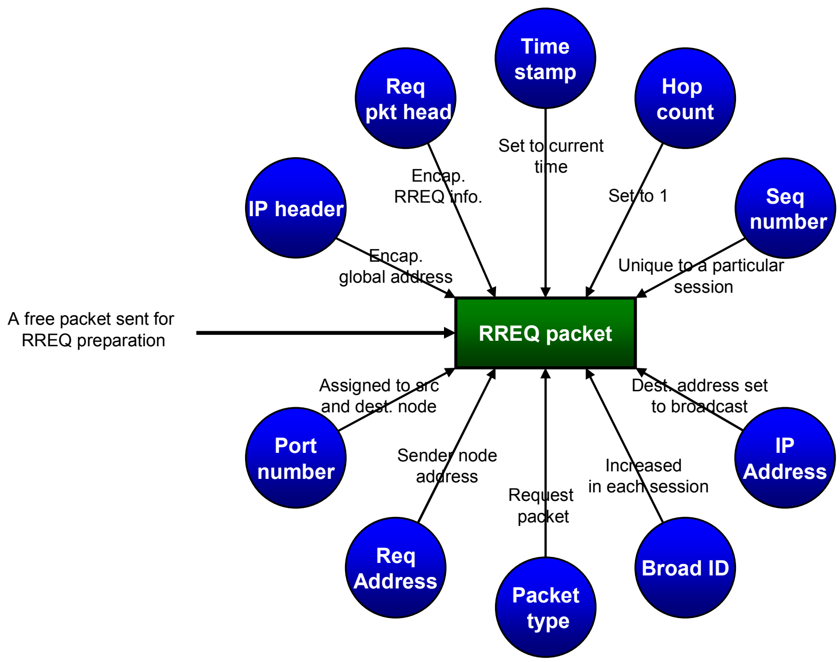


Figure 5.1: RREQ packet formation

To form a routing path, the source node seeks to find the address of destination node by broadcasting the RREQ packet to adjacent nodes. A broadcast packet is identified by the destination IP address set to IP_BROADCAST. Upon receiving such a packet, each node compares the contents of RREQ, i.e. broadcast ID and sequence number, with the stored information in its cache. A packet is deemed fresh if the value of the RREQ's sequence number is higher than the entry stored in the routing table. The broadcast ID along with the source request packet address forms a unique combination for a particular broadcast session. Additionally, for every route discovery phase, the broadcast ID is increased by 1 unit. Such increment is essential in order for every node to differentiate between a new and obsolete RREQ packet. For instance, when a source node fails to construct the routing path on the first route discovery, a new RREQ packet is rebroadcast. As such, an intermediate node may receive multiple RREQs from different route discovery sessions. Therefore, by increasing the value of broadcast ID for each route request transmission, nodes can ensure that only the current RREQ is processed. A maximum of three route discovery attempts (RREQ_RETRIES) is allowed for a particular transmission. The number of attempts is set to three as shown in Table 5.1, which follows the AODV specification as reported by Perkins [45]. The process is then repeated until the routing path is finally established. The parameters corresponding to the route discovery process and the RREQ packet preparation flow are shown in Table 5.1 and Figure 5.2, respectively.

Table 5.1: Route discovery parameters

Parameter	Value
RCAST_WAIT_TIME	1.5 seconds
HELLO interval	1 second
NODE_TRAVERSAL_TIME	0.03 seconds
RREQ_RETRIES	3
MAX_RREQ_TIMEOUT	10 seconds
RREP_WAIT_TIME	1 second
NETWORK DIAMETER	30
ACK_WAIT_TIME	0.5 second
TTL_START	3[11]
TTL threshold	7
BCAST_ID_SAVE	6 seconds

In addition to the highest sequence number, each forwarding node also seeks the lowest hop count. In some cases, if a RREQ's packet hop count is identical to the content of routing table, the highest sequence number takes precedence. However, if the hop count advertised by the RREQ packet is lower than the entry on the routing table, the packet is considered fresh. Subsequently, the route entry is replaced by the information as advertised by the RREQ packet. The mechanism ensures that a node always maintains the shortest routing path while effectively eliminates the duplicate packets. Figure 5.3 illustrates the process of route freshness inspection. Such an algorithm ensures that a node computes the shortest routing path with using only bidirectional links. Nonetheless, constructing routes exclusively through bidirectional links may not be practicable, since

[11] TTL_START is consistent with the value discussed in section 3.2.1.

link conditions frequently vary. Therefore, if the system is unable to find at least a single bidirectional link between the source and destination node pair such algorithm may fail to function.

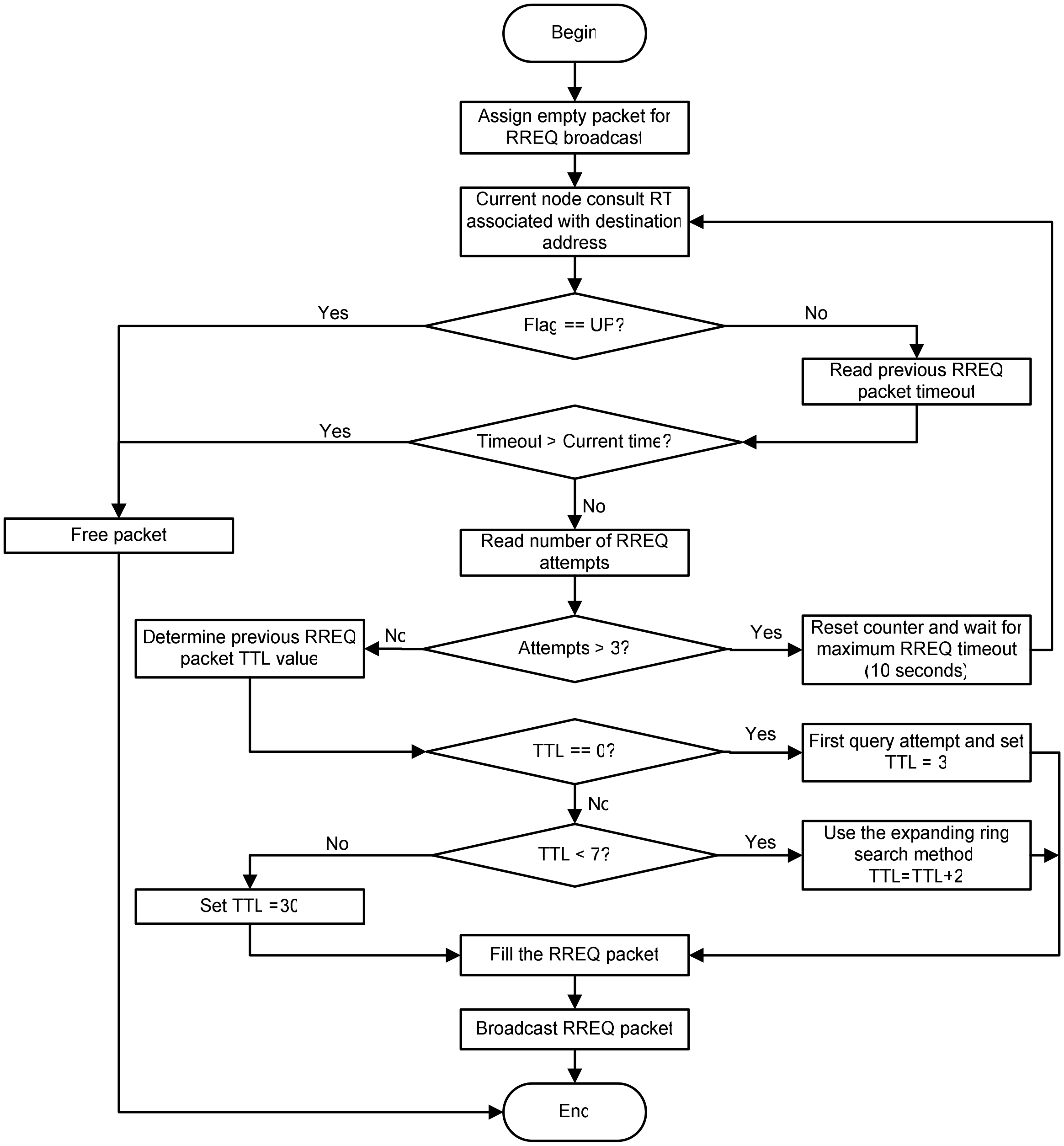


Figure 5.2: Flowchart of route request preparation

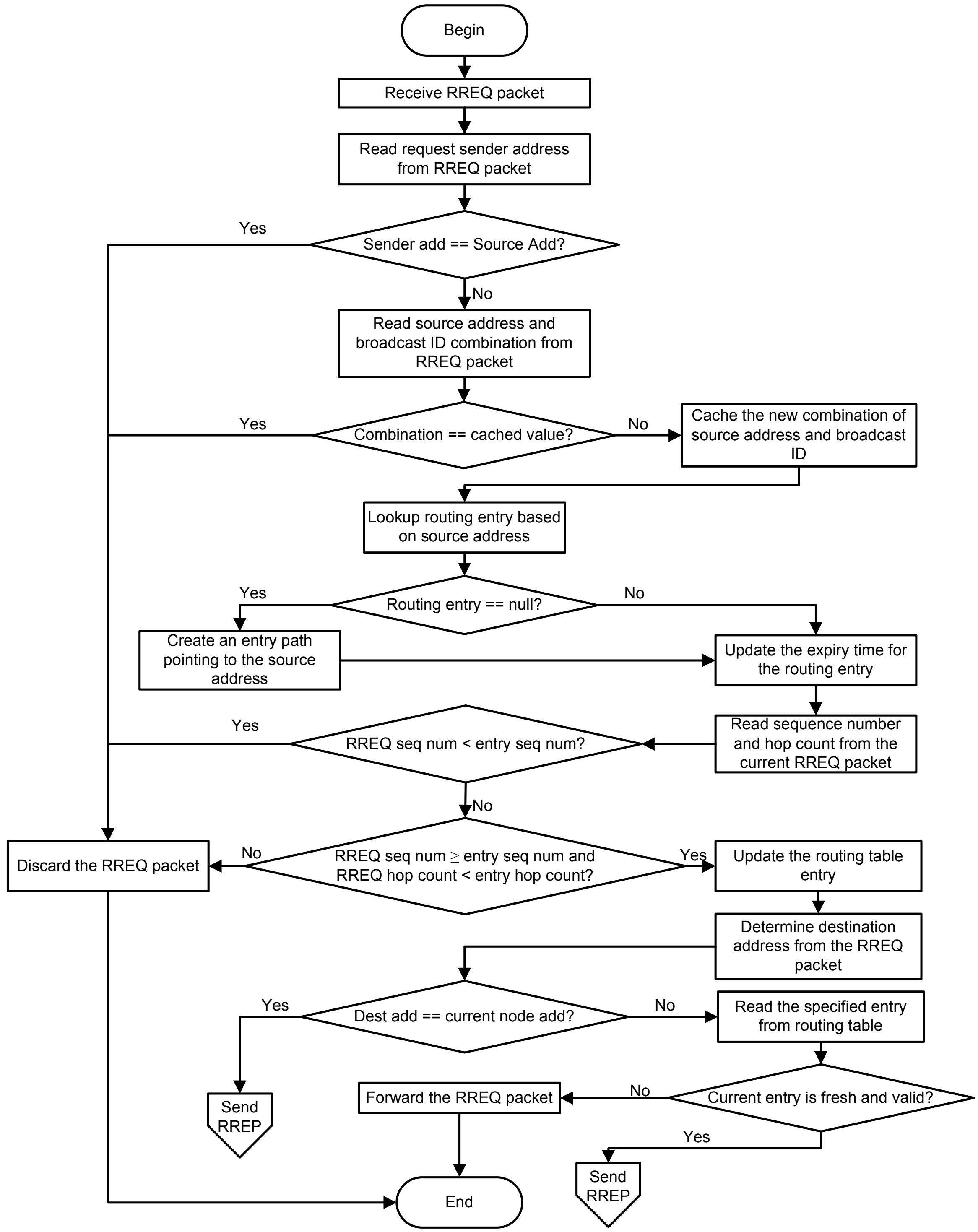


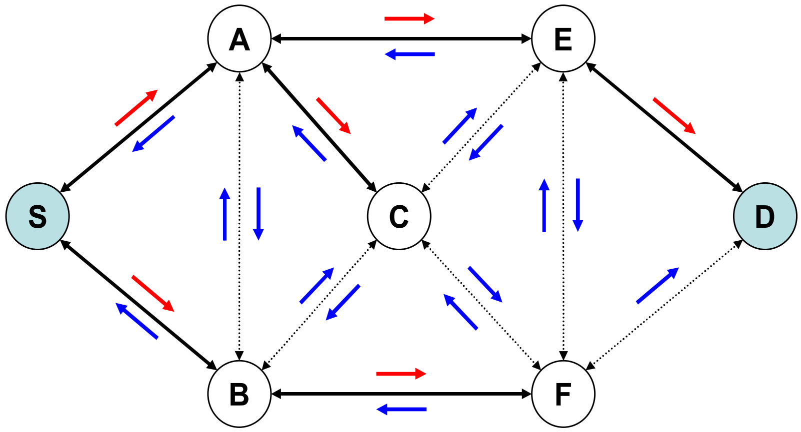
Figure 5.3: Flowchart of route freshness inspection

In the AODV routing protocol, the hop count provides a simple solution for nodes to select route with the shortest distance. However, it may not be as effective when a large number of links within the network are unidirectional. As a result, the routing overhead and delay are increased because additional time is required by a source node to perform new route discoveries.

5.2.1.2 Route Establishment

In the route establishment phase, a node responds to the first RREQ packet received by sending a RREP packet back to the source node. Similar to intermediate nodes, the destination node records only the freshest RREQ packet using the sequence of process described by Figure 5.3. Figure 5.4 shows the initial content of routing table at each node after the first route request discovery. The red line shows the propagated RREQ packets and the blue line shows the dropped RREQ packets, which have been determined to be redundant. At the destination node **D**, the RREQ propagation is terminated.

After receiving the first RREQ packet, the destination node **D**, responds by preparing the RREP packet. The destination and source IP addresses is swapped and the next hop node is included within the RREP packet's field. The next hop node follows the ID of the node from which the RREQ is received. For instance, as shown by Figure 5.4, assuming the first RREQ packet received is from link **E**-**D**, node **D** elects **E** as the next hop node. The RREP packet is then unicast via each node, which forwards to the next destination based on its routing table. The reverse path **D**-**E**-**A**-**S** is created.



Summary of routing table

Node	Next hop	Hop count
S	-	-
A	S	1
B	S	1
C	A	2
E	A	2
F	B	2
D	E	3

Figure 5.4: Forward route creation and routing table

5.2.1.3 Unidirectional Link Detection

On a network with high concentration of unidirectional links, the process of routing path selection using the RREQ-RREP combination approach can be detrimental. Assuming link **A-E** is now unidirectional; pointing to node **E**. As shown in Figure 5.4, after node **D** receives a RREQ packet it immediately assumes that node **S** can be reached via next hop node **E**. However, such a response is not possible because the link **A-E** is unidirectional. In such a case, the typical AODV scheme with unidirectional link detection mechanism (AODV-Blacklist) can detect and avoid such links. The scheme reads every RREP received, i.e. originated or forwarded by a node, and responded by returning a network layer ACK packet. As soon as node **E** transmits a RREP packet to the next hop node **A**, it expects an immediate ACK packet reply. In the event that node **E** fails to receive the ACK packet, it identifies the link pointing to node **A** as unidirectional and subsequently blacklisted. All current routing entries to node **A** are then removed and the system waits for another round of RREQ discovery. Later, node **E** discards every RREQ packet forwarded by node **A**. As a result, a new forward route can be constructed via a different path, e.g., **S-B-F-D**.

However, the DRR scheme employs a different approach compared to the AODV-Blacklist. Instead of avoiding, the proposed scheme utilises the unidirectional link to advantage during forward route construction. In the event of ACK reception failure, the identified unidirectional link is not blacklisted. Instead, a new reverse route is computed immediately, which can be used to potentially propagate the RREP packet back the source node. In order to find such a route, the downstream node affected by the unidirectional link invokes a *one-hop local reply broadcast* packet. Basically, the packet is an exact copy of the dropped RREP packet, and differs only in terms of packet type, i.e., broadcast instead of unicast. The local reply broadcast mechanism takes advantage of the unused route entries recorded by intermediate nodes after the route discovery phase, illustrated by the summary of routing entries in Figure 5.4. The details of reverse route construction for the DRR scheme are presented in the following section.

5.2.1.4 Reverse Route Reconstruction

As shown in Figure 5.4, the initial broadcast of RREQ packets has established a forward route through link **S**-**A**-**E**-**D**. In addition to the active nodes (**S**, **A**, **E**, **D**) along the forward route, other nodes such as **C**, **B** and **F** also record the RREQ entries pointing to the source node. As previously discussed, these nodes may be able to provide alternative routes to the RREP packet blocked by the unidirectional link **A**-**E**. After receiving the RREQ packet, node **D** responds by unicasting a RREP packet with RREP_NO_FLAG bit set. Additionally, prior to every RREP unicast transmission, each node, including the destination, stores a copy of the packet along with its contents. Such information can later be used by the local reply broadcast transmission if the preceding RREP forwarding fails. At node **E** the RREP packet is forwarded and, in return, node **E** expects to receive an ACK packet. To avoid high delay, node **E** waits for a short duration of time indicated by ACK_WAIT_TIME. If node **E** fails to receive the ACK packet, it results in node **A** being cached as unreachable. As such, node **E** promptly invokes the one-hop local reply broadcast mechanism. A copy of the previously stored RREP packet is broadcast to the adjacent nodes with TTL set to 1 and the flag is set to OHR (one-hop-broadcast).

Node **C**, **F**, and **D** receives the broadcast RREP because they are within node's **E** radio transmitting power (P_t). Node **D** drops the packet because it is the originator, whereas both node **C** and **F** receive the RREP packet. Upon reception, both nodes restore the packet's flag from OHR to RREP_NO_FLAG, before forwarding it to the next hop node. RREP packets recovered using this approach may slightly increase the routing overhead. To minimise such an effect, each node along the RREP packet propagation path records, in its cache, a unique combination list of source address, destination address, and sequence number <*Src ID, Dest ID, seq_num*>. Therefore, if a RREP packet that matches the combination is later received by the node, the packet propagation is terminated. This causes the RREP packet to reversely follow, as far as possible, the forward route created, and diverted to the alternative route only when the primary forward path is blocked.

5.2.1.5 Network Layer Feedback (Acknowledgement)

The introduction of ACK packets in the DRR scheme can cause a slight increase in terms of the overall system's routing overhead. Therefore, a necessary countermeasure has been implemented in the scheme, to minimise such effects. The operation of ACK packet exchange can be significantly reduced if nodes are set to respond correctly to different type of RREP packet. In the scheme, the ACK packet can only be returned by the receiver node for a RREP packet with the flag bit set to RREP_NO_FLAG. Alternatively, an ACK packet is not returned when the flag bit is set to OHR. As a result, control packet exchange is minimised, leading to more efficient use of bandwidth.

In addition to the ACK message exchange reduction, the DRR scheme can also substantially reduce the number of RREQs in the system. Previous work [137] shows that the number of RREQ packet transmitted by source nodes may dominate the total number of control packet in the routing protocol. Such an issue is inherent in routing protocols such as AODV and AODV-Blacklist which operate "on-demand". Slight route breaks can cause the source node to flood multiple RREQ packets into the system. By using the DRR scheme that locally restores the routing path, such issues can be effectively avoided.

5.2.1.6 Reverse Path and Local Reply Broadcast

As previously mentioned, when the propagation of RREP packet is blocked by a unidirectional link, DRR allows a node to rediscover alternative reverse paths. As a result, multiple copies of RREP packets may be received by the source node over several different paths. Such problem can be avoided by comparing the current and previous RREP broadcast packet. For instance, after the local broadcast reply by node **E**, the recovered RREP packet will propagates via the two reverse paths towards node **S**, e.g. **E**-**C**-**A**-**S** and **E**-**F**-**B**-**S**. Assuming the first RREP packet arrives from path **E**-**C**-**A**-**S**, node **A** then immediately records the packet information, i.e. <*node **S**, Node **D**, seq_num*>. Later, when the second RREP packet arrives from path **E**-**F**-**B**-**S**, the packet is discarded because the content of the packet matches the stored information. In addition, the recorded RREP packet is cached for only a short period of time set by RCAST_WAIT_TIME. The value must not exceed the roundtrip time of RREQ-RREP packet; the time difference between sending the RREQ and receiving the RREP at the source node. An estimation of the roundtrip can be computed by equation 5.1.

$$3 * \textit{Network Diameter} * \textit{Node Traversal Time} \qquad (5.1)$$

The *Network Diameter* is set to 30, in accordance to the maximum hop allowed in AODV. On the other hand, the *Node Traversal Time* is set to 0.03 seconds, based on the estimated time for a packet to traverse one-hop, which includes the queue, transmission, propagation and all other delays.

The reverse link created by the local reply broadcast enables the source node to reach the destination node via an alternative reverse path. However, when using such paths, data packet can be transmitted only from the source node to the destination node, but not vice versa. This may not be an issue for some applications, which typically rely on fast data transfer and best effort delivery with using UDP. For instance, sending updates on stock markets, news, and bulletins to customers requires fast data dissemination but may compensate for unreliable communication. Nonetheless, a two-way communication can be enabled with the proposed scheme. Upon unidirectional link detection, an additional flag called RREPAIR is included to the RREP packet advertised by the local broadcast mechanism. The RREPAIR is set to indicate to the source node that the RREP packet has been recovered by one of the nodes along the reverse path. Therefore, when the source node receives a RREP packet with the flag set to RREPAIR, it reconstructs the forward path by propagating downstream a unicast RREQ packet towards the destination node. The packet follows the reverse path created, where details such as hop count and sequence number at each node's routing table are updated. Note that as soon as the RREQ packet is unicast, the source node can start sending the data packets.

5.3 DRR Model Verification

This section discusses the verification of the simulation model and the implementation of the DRR scheme. This is imperative to ensure that every step involved in the routing operation is correctly performed. Using a small scale network, each routing table generated by nodes are checked thoroughly. The sequence of control packet propagation is observed and the corresponding sequence number, hop count, and routing path is ensured to be processed correctly. In a more complex network, the debugging tool, GNU Debugger (GDB) with Eclipse as the integrated development environment (IDE) is utilised. The tool provides easy verification process that is able to perform fast code compilation and immediate build status. The routing process transition and outcome can be shown at any breakpoints set on the code. In addition, a set of verification codes is also provided in the Table 5.2. Each step shown in the verification rules are followed and tested multiple times to confirm results consistency.

Table 5.2: DRR model verification rules

Verification steps	Verification rules
1.	A data packet is allocated and forwarded to the routing layer. The current node attempt to resolve the path to the destination based on the corresponding address stated in the data packet.
2.	The RREQ packet is broadcast to adjacent nodes.
3.	If no valid route exists the node prepares the RREQ packet by allocating the packet fields with information, e.g., timeout, route request count, TTL, and etc.
4.	Nodes that are within the transmission range of the sender node receive the packet. The packet is filtered according to its type, where a packet with DRR header is subsequently processed.
5.	If the source address advertised by the RREQ packet matches the current node address, the packet is discarded. The broadcast ID along with the source address is compared with the node's cache and if a match is not found the source address and broadcast ID is stored in the node's cache.
6.	The destination address advertised by the RREQ packet is compared against the address of intermediate node. If not matched, the RREQ packet is forwarded with the hop count increases by 1 and the sender address is changed to the current node address.
7.	A node replies to the RREQ packet only if the destination address matches to its address or if it has a fresh route pointing to the destination node.
8.	The intermediate node or destination node prepares to respond by sending RREP packet. The hop count is increased by 1 and the source address, destination address, sequence number and current time is copied into the RREP packet.
9.	RREP packet is prepared and a copy of RREP packet state is stored in the node's cache. The RREP packet is unicast to the address of next hop node.
10.	The node waits for ACK packet to be returned by the next hop node for duration of time set to ACK_WAIT_TIME. If ACK is not received after timer expires, the same copy of RREP packet is broadcast with TTL set to 1 and packet flag set to OHR.
11.	Every adjacent node except the destination node receives the RREP broadcast. Each node removes the OHR flag to RREP_NO_FLAG and the packet is unicast to its next hop node upstream to the source node.
12.	For each node the recovered RREP packet passes, a unique combination of source address, destination address and sequence number is recorded. Every RREP packet received that matches such combination is deemed redundant and therefore dropped.
13.	If the RREP packet is received by the source node, the packet propagation is terminated. The source node checks the RREP flag field and if it is marked as ALT, a repair packet is sent.

14.	The repair packet called RREPAIR is propagated downstream along the reverse route to provide update on the hop count and next hop node pointing to the source node.
15.	Data packet is transmitted from the source node.

5.4 Simulation Framework

The performance of DRR scheme is quantified using the NS-2 tool, which also provides the routing model for the AODV routing protocol and some basic components of AODV-Blacklist. The two protocols are ideal comparisons for the DRR scheme because both offer extreme mechanism to handle unidirectional links. At one end, the AODV routing performance can highlight the severe effect of ignoring the presence of unidirectional links. At the other end, the AODV-Blacklist shows the impact of improper handling of unidirectional link by blacklisting.

5.4.1 Mobility and Traffic Model

To observe the scheme's robustness to mobility, different nodal speeds are used within the mobility pattern. As discussed in Chapter 4, the GM mobility model is selected as it provides more realistic nodal movement compared to the classical RWP model. Generally, as shown by the comparison results in Chapter 4, a routing protocol's path connectivity using GM model is slightly higher compared to other models. It is because the movement of nodes in this model are more human-like, which avoids sharp turns and sudden stops when travelling from one point to another. As such, the number of route breakages is small.

As shown in Table 5.3, the random traffic model is set as CBR, established between several randomly selected source and destination node pairs. The start of the CBR session between any pair of nodes is also randomised to avoid immediate bursts of data traffic being sent simultaneously by every source node. The size of each packet is 512 bytes set at a rate 4 packets/second; values commonly used in many previous MANET simulation work [12][34][35][56][63]. The simulation time is set to be 900 seconds, where each point plotted on the graph corresponds to 25 repetitions of the same simulation setting with different network scenario. The resulting confidence interval is set to be 95%.

Table 5.3: Mobility and traffic parameters

Parameter	Value
Simulation time	900sec
Number of nodes	50
Terrain size	700x500 m^2
Traffic type	CBR
Packet rate	4 packets/sec
Packet size	512 bytes
Number of sources	25
Maximum speed	0, 2, 4, 8, 12, 16, 20 m/s
Speed update frequency	2.5 s
Angle of std deviation	45 degree
Speed deviation	1.5 m/s

5.4.2 Transmission Power

The radio interface equipped for each node on the network follows the settings of Cisco Aironet 350 [90] wireless interface card. Two distinct transmitting powers are set to different numbers of nodes, similar to the approach discussed previous chapters. Table 5.4 shows the radio settings used in the simulation.

Table 5.4: Simulation parameter – radio settings

Parameter	Value
Transmitter range	~ 250 meter
Transmit power (P_{thigh})	15 dBm
Transmit power (P_{tlow})	7dBm
Receiver sensitivity	-91 dBm
Nominal channel bandwidth	2 Mbps

5.4.3 Performance Metrics

Several key performance metrics are used to evaluate the schemes performance:

- *Packet delivery ratio:* The average ratio of accumulated data packets delivered to destinations compared to those generated by data sources. Such metric shows the general performance of the scheme in terms of its capability to transmit as much data as possible to the destination. It may also represent the number of loss packet, which can be used to show the scheme's efficiency.
- *Normalised routing load:* This value is calculated based on the number of routing packets sent and forwarded by each node compared to the number of data packets received by the sink nodes, i.e., destination nodes. Essentially, a low normalised routing load indicates an efficient network, where the number of data packets received is higher than the number of routing packets generated for a particular connection. Nonetheless, the normalised routing load is also affected by the number of nodes participating in the routing packet exchange. Hence, a low number of nodes participating in route propagation can result in low normalised routing loads.
- *Packet loss:* The failure of one or more transmitted packets to arrive at their destination. The packet loss metric is an absolute number of packets dropped in the network, which quantifies the analysis of packet propagation in the network.
- *Average delay:* Average delay includes all possible end-to-end delays caused by buffering during route discovery, queuing at the interface queue, re-transmission delays at the MAC, propagation time, and transfer time.

5.5 Simulation Results and Discussion

The simulation experiments investigate the ability of the routing mechanisms to react to the changes of link connectivity while successfully delivering data packets to their destinations. To measure this ability, the performance of routing protocols are evaluated and compared under a range of scenarios. The performance metrics are measured against the attributes that may occur in the network, which are:

- Ratio of nodes with low transmitting power (ratio of P_{tlow} to the total number of nodes).
- Mobility (speed of the nodes)
- Offered Load (number of sources)

In each simulation, there are a several parameters that are configured; these are:

- *Speed:* The speed of node is set between a minimum and a maximum possible setting.
- *Number of nodes*: A consistent number of nodes is set in every experiments.
- *Terrain size:* A medium-sized, rectangular network area is selected for experiments in this chapter.
- *Simulation time:* The duration over which the simulation are run.

5.5.1 Varying Unidirectional Link

A node's transmitting power and its corresponding transmission range are important characteristics that determine whether or not a node can establish a path with its neighbours. By using two power levels the number of unidirectional links can be varied and the impact upon the relevant performance metrics can be investigated. Nonetheless, the effect may be temporary but may still affect the routing path computation. The number of unidirectional links (varied by using two power levels) is employed to investigate the impact it has on the metrics being used. The ratio of nodes, as reported in Table 4.4 shows 6 sets, where each ends of the table represent two extreme cases of unidirectional link intensity. Set 0 represents a network where all links are virtually bidirectional; although some links may become unidirectional link due to interference, mobility, and etc. On the other hand, set 5 signifies a network, where half of the nodes are low-powered. Such an extreme network scenario is useful to evaluate the robustness of routing protocols, although this may not be a realistic case. Nonetheless, increasing the low power nodes to set 5 is essential to ensure that a significant number of unidirectional links is created on the network. The summary of parameters used in the simulation is shown in Table 5.5.

Table 5.5: Simulation parameters – Varying number of low power nodes

Parameter	Value
Transmitting power (P_{thigh})	15 dBm
Transmitting power (P_{tlow})	7d Bm
Simulation time	900 sec
Number of nodes	50
Terrain size	700x500 m^2
Traffic type	CBR
Packet rate	4 packets/sec
Packet size	512 bytes
Number of sources	25
Maximum speed	20 m/s

5.5.1.1 Packet Delivery Ratio

The variation of packet delivery ratio as a function of low power nodes is shown in Figure 5.5. As the number of low power nodes increases, the probability of links created unidirectional also increases. Hence, every routing protocol exhibits rapid deterioration of packet delivery ratio. In the case of set 0, which illustrates a homogenous group of nodes in terms of transmitting power, the performance of each scheme is quite close to each other. In fact, this is an ideal situation where every node to performs effectively, because packets have higher probability of being forwarded via bidirectional links. Nonetheless, a slight difference can be observed within set 0. Since nodes are set to move at a maximum speed of 20 m/s, some RREP packets may be dropped. This causes the DRR scheme to invoke the unidirectional link detection mechanism. At set 0, the packet delivery ratio in DRR scheme is improved by 6% compared to the AODV routing protocol. Although the AODV-Blacklist offers nodes a protection from unidirectional links, the scheme relies on the source node re-broadcasting the RREQ packet which may increase delay and routing overhead. As such, the performance of AODV-Blacklist degrades; in particular after set 0.1. The inefficiency of AODV-Blacklist is also heightened by the fact that the network is saturated with the data traffic; a consequence of 25 simultaneous active data sessions. The congestion increases the competition for channel access, causing more packets to collide and subsequently be dropped. The AODV scheme exhibits the worst performance. Specifically, at set 0.3, the AODV's packet delivery ratio drops as much as 66% compared to the DRR scheme. The absence of any unidirectional link detection mechanism causes the RREP packet propagation to fail and the source has to wait for the timer to expire before it is able to identify any problems. Generally, the DRR scheme exhibits a significant improvement compared to the AODV-Blacklist and AODV scheme.

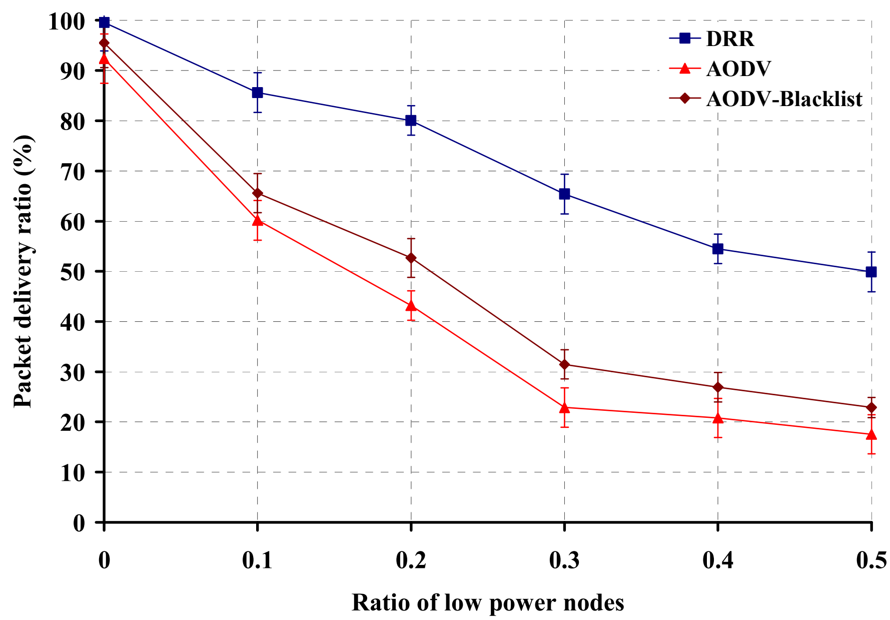


Figure 5.5: Packet delivery ratio as a function of node power variables

5.5.1.2 Normalised Routing Load

The normalised routing load metric characterises the ability of a routing scheme to perform in low bandwidth and highly dense network conditions. Protocols that operate on-demand typically rely on a high degree of routing packet dissemination to discover routes. Such mechanisms can potentially increase the probability of packet collisions and subsequently cause retransmissions. In essence, an efficient scheme should be able to minimise routing packets as far as possible while maintaining a high number of successful data packet transmissions. Figure 5.6 presents the normalised routing load for a network consisting of 50 nodes. The normalised routing load in DRR is much lower than AODV and AODV-Blacklist across all sets. Between set 0 and 0.1, the performance of AODV and AODV-Blacklist is nearly identical; however, as the ratio of low power nodes increases beyond set 0.1, the DRR's normalised routing load is significantly lower compared to the competing protocols.

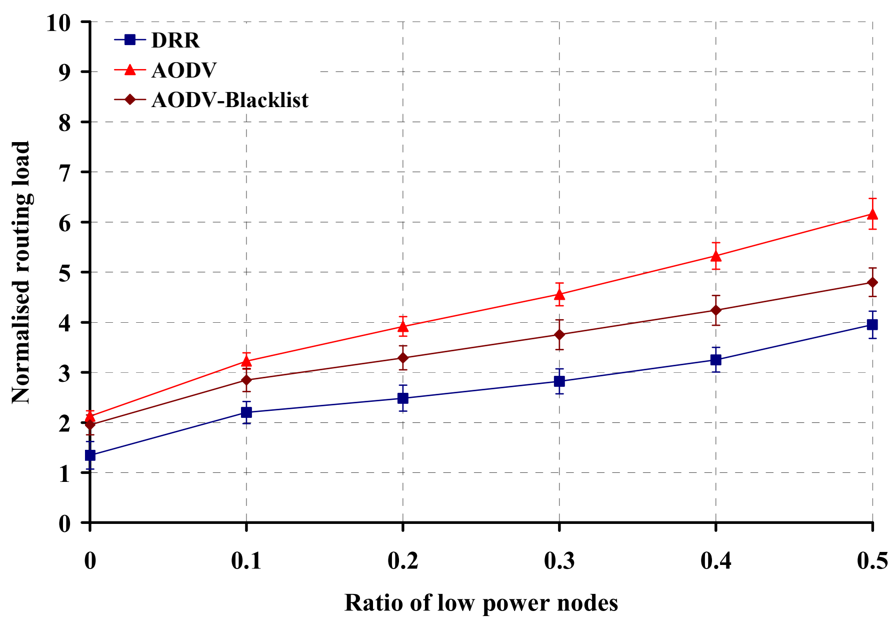


Figure 5.6: Normalised routing load as a function of node power variables

5.5.1.3 Packet Loss

The packet loss of the three schemes as a function of low power nodes is shown in Figure 5.7. In this simulation experiment, a sequence of packets are generated and transmitted according to the rate parameter. The data packet size is fixed to 512 bytes and, therefore, the total size of the accumulated loss packet can be easily computed. However, the packet loss quantification in a real network may be a more complex process. Transmitted packets arrive in different size and forms and as such, the total amount of traffic loss can significantly vary. In this simulation, the packet loss is quantified based on the total count of the packet, instead of the total accumulated packet size. As the number of nodes with P_{tlow} increases, more packets are dropped as a consequence of the increase number of unidirectional links present in the network. The packet loss in DRR is lower, simply because it enables routing packets to be partially propagated around the unidirectional link.

5.5.1.4 Average Delay

The average delay presents the cumulative holding time for a packet. It includes all possible delays from the moment the packet is generated, transmitted, and received by the destination node. Generally, the length of the routing path is a constituent part of the metric. Thus, a longer routing path generates a higher delay, since data packets take more time to reach the destination node. Figure 5.8 depicts a variation of the average delay as a function of low power nodes. Every scheme shows a significant increase of average delay with the increase of the low power nodes. Such a phenomenon is a result of bidirectional link shortage in the network. The probability of successfully constructing a routing path is reduced, causing the number of route rediscoveries to increase. As such, the data packets are delayed in the queue until a new routing path is found. As shown in Figure 5.8, the DRR's delay is substantially lower compared to the AODV-Blacklist and AODV routing protocols. Clearly, the DRR mechanism is effective when subject to unidirectional links. A routing path is promptly constructed by the affected node, thus avoiding the route discovery and buffering delay.

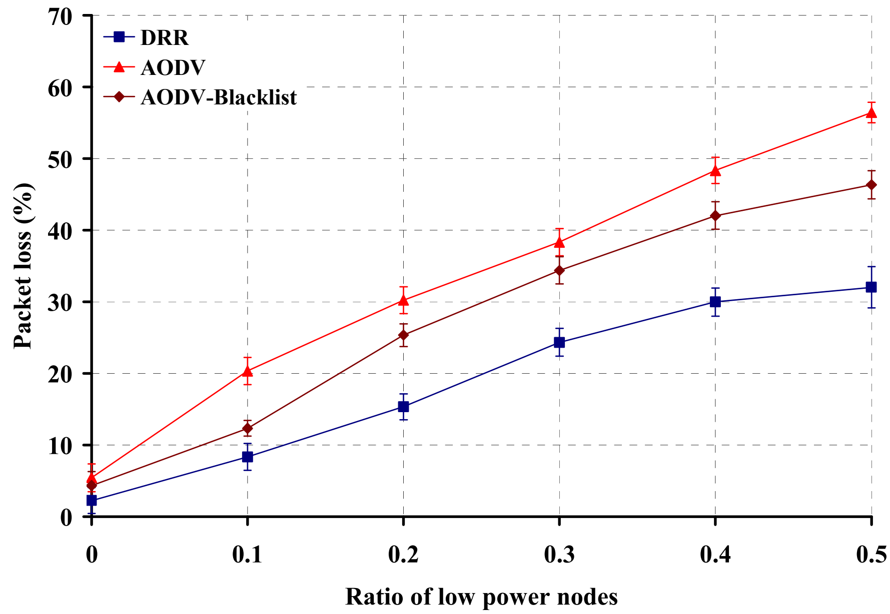


Figure 5.7: Packet loss as a function of node power variables

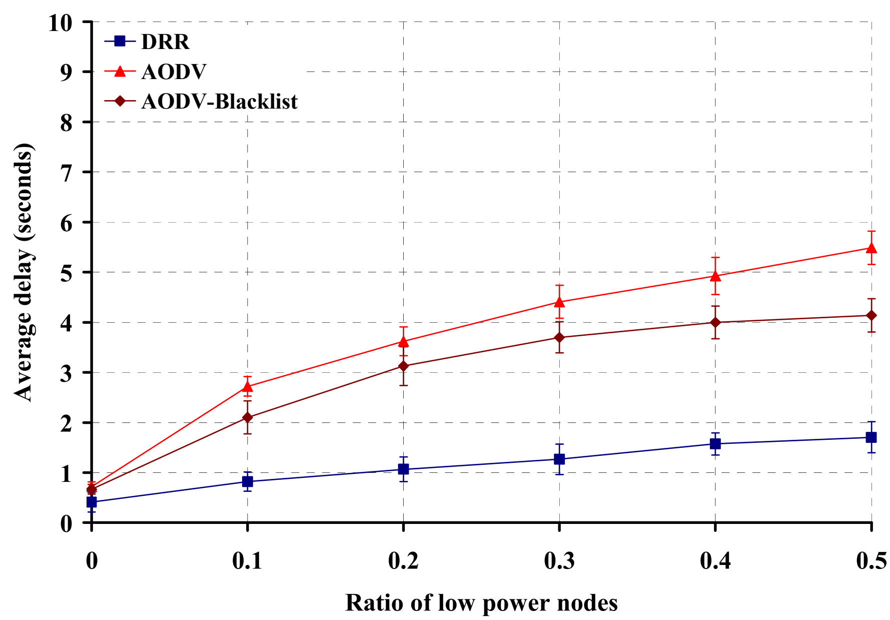


Figure 5.8: Average delay as a function of node power variables

5.5.2 Varying Mobility

An important attribute that is commonly associated with MANET is mobility, which causes link state to change in a more dynamic fashion than a stationary system thus further impacting network performance. To investigate such an effect, the GM mobility model is selected to generate nodal movement pattern. The model presents a realistic model compared to the RWP model. To ensure consistency, the same set of model parameters as reported in Table 4.7 is used. Every node is mobile and the maximum speed is varied to increase a node's average speed. Typically, a static network corresponds to the speed of 0 m/s while a high mobility corresponds to a speed of 20 m/s. The simulation parameters used for the mobility simulations are similar to the experimental work listed in Table 5.5 but with minor changes. The changes made are shown in Table 5.6. Nodes are set with 7 different speeds while the ratio of low power nodes is set to 0.3. Such ratio is chosen because it gives a good compromise between bidirectional and unidirectional links.

Table 5.6: Simulation parameters – Varying nodes maximum speed

Parameter	Value
Maximum speed (m/s)	0, 2, 4 , 8, 12, 16, 20
Ratio of low power nodes (P_{tlow})	0.3

5.5.2.1 Packet Delivery Ratio

The packet delivery ratio is shown in Figure 5.9. The three schemes exhibit a gradual decrease as the maximum speed increases. At null mobility, i.e. 0 m/s, the packet delivery ratio of DRR scheme is approximately 29% better compared to the AODV scheme. At higher speed, the DRR's packet delivery ratio is twice as much as AODV's. Such performances indicate the effectiveness of DRR in handling the routing construction despite significant nodal movement. The AODV-Blacklist scheme indicates only a slight increase of packet delivery ratio compared to the AODV routing protocol. On average, the performance increase compared to AODV offered by AODV-Blacklist scheme is only 20%, which is about less than half of the performance gained by the DRR scheme.

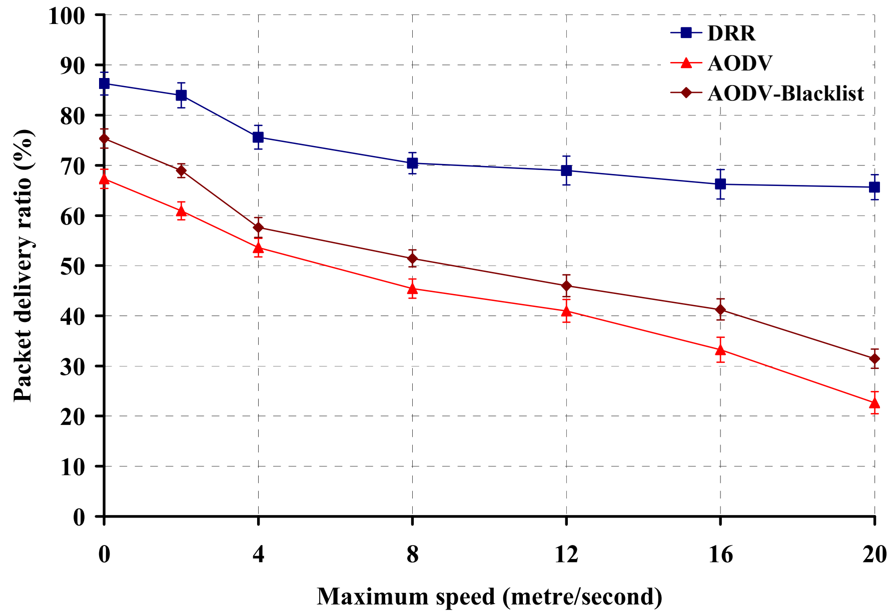


Figure 5.9: Packet delivery ratio as a function of mobility

5.5.2.2 Normalised Routing Load

The normalised routing load performance metric is computed based on the number of control and data packet transmitted and forwarded by the protocol per successfully delivered data packet. Essentially, this metric quantifies the amount of effort consumed by the protocol for the delivery of each data packet. For instance, a normalised routing packet of 10 indicates an average of 10 packet transmissions attempts for each data packet delivered to a destination node. Hence, a normalised routing load of smaller than 1 signifies a very efficient network, where the number of data packets received is higher than the number of routing packets generated for that particular connection. Nonetheless the normalised routing load can be affected by many factors such as the frequency of data packets sent, and the number of nodes participating in the routing packet exchange. Since the computation of this metric is based on a large number of nodes, i.e., 50 nodes, this explains the reason for the extremely high value of normalised routing load in every simulation output. In Figure 5.10, the normalised routing load incurred by the DRR scheme is the lowest despite the presence of unidirectional links. Although the AODV-Blacklist scheme is able to detect and avoid unidirectional links, route construction may not be as efficient as the DRR scheme. Further analysis on AODV scheme indicates an excessive number of routing packets being generated, a consequence of multiple RREQ flooding by the source node.

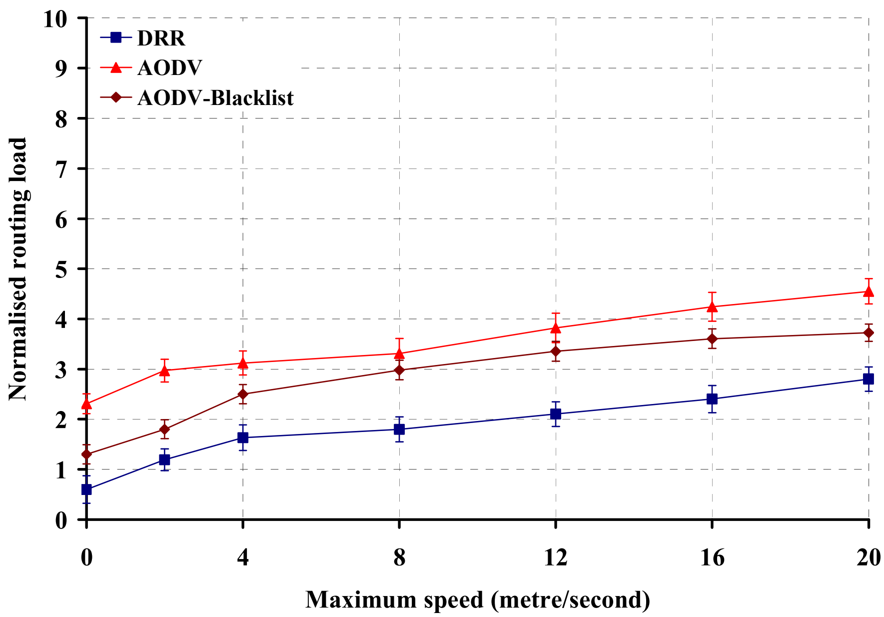


Figure 5.10: Normalised routing load as a function of mobility

5.5.2.3 Packet Loss

Figure 5.11 presents the packet loss for the three schemes. The DRR scheme achieves the lowest packet loss, a consequence of prompt avoidance of unidirectional links during the recovery of routing path breakage. Generally, every scheme exhibits a gradual increase of packet loss as nodal maximum speed increases. This is expected because, at higher nodal mobility, the links become more unstable, causing more packets to be dropped. At null mobility, a proportion of the links are unidirectional due to the non-identical transmitting power. As such, the packet loss is much higher compared to homogeneous radio power, shown by set 0 previously in Figure 5.7.

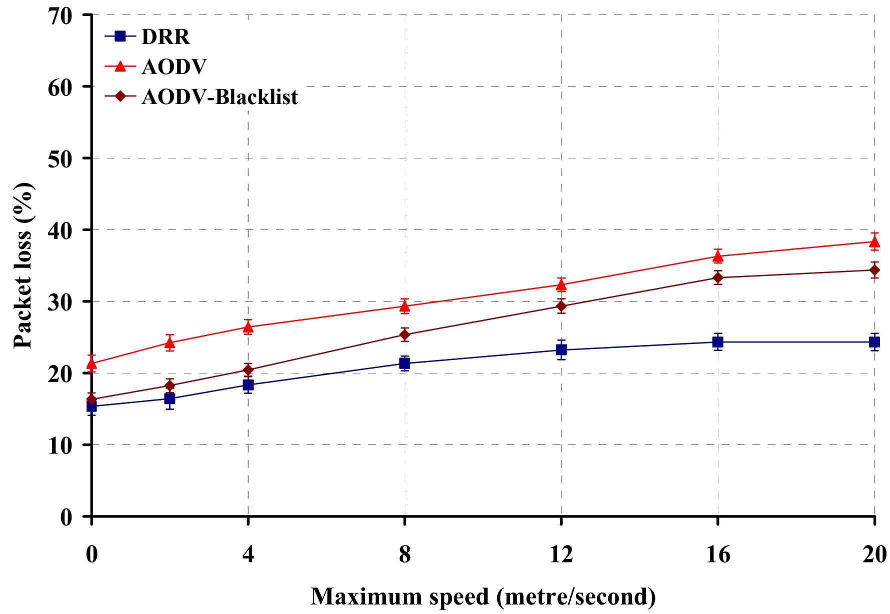


Figure 5.11: Packet loss as a function of mobility

5.5.2.4 Average Delay

The average end-to-end delay as a function of the number of sources is shown in Figure 5.12 and illustrates that DRR has a lower average delay across all different maximum speeds. Typically, the delay to construct a routing path may dominate the overall delay incurred in the system. The DRR scheme experiences the lowest average delay simply as a result of lower route discovery latency. The effect of increasing the maximum node speed is clear when comparing the DRR to the competing schemes. The DRR scheme is least affected by the mobility because of the rapid procedure to recover packets and find alternative paths around the unidirectional link. In general, the three schemes show an increasing average delay as the maximum node speed increases. Between 0 and 20 m/s, the DRR scheme exhibit an increase of average delay by as much as 83%. Nonetheless, its performance is still better than that of AODV and AODV-Blacklist. Both these schemes incur an average delay (at 20 m/s) that is approximately 300% higher compared to when nodes are static.

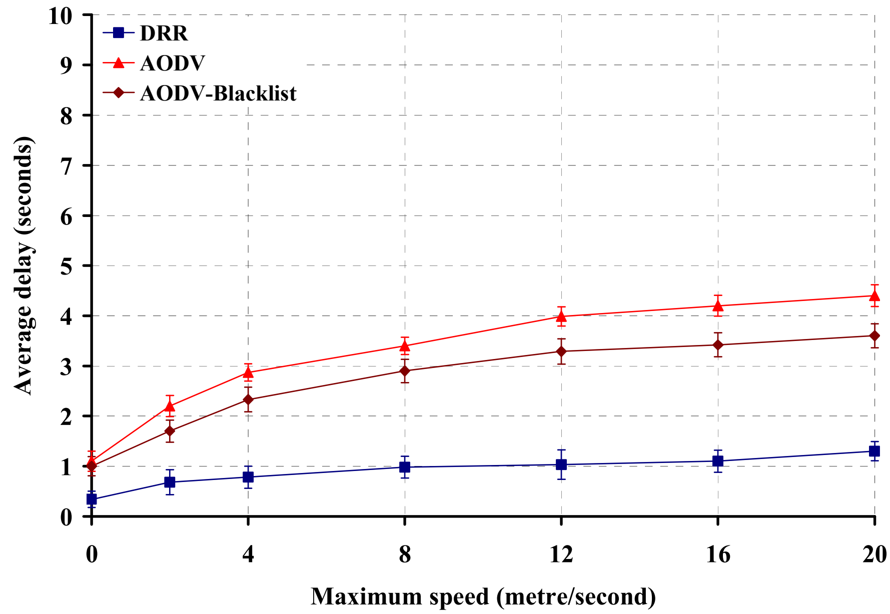


Figure 5.12: Average delay as a function of mobility

5.5.3 Varying Offered Load

The final simulation experiment varies the offered load to investigate its impact on routing scheme performance. Essentially, the offered load is characterised by three parameters; the number of active connections, packet size, and the frequency of packet transmission. In this experiment, the number of active connections is varied while the packet size and its sending rate is fixed at 512 bytes and 4 packets/second, respectively. Subsequently, the number of random active connections (sources) is varied between 15 and 40. The simulation parameters used in this experiment is similar to the settings in section 5.5.1 but with changes as shown in Table 5.7.

Table 5.7: Simulation parameters – Varying number of sources

Parameter	Value
Number of sources	15, 20, 25, 30, 35, 40
Ratio of low power nodes (P_{tlow})	0.3

5.5.3.1 Packet Delivery Ratio

The packet delivery ratio shown in Figure 5.13 is a function of number of active sources. As the number of sources increases, the packet delivery ratio for the three schemes drops. Specifically, when 30% of the nodes are set with P_{tlow}, the DRR scheme outperforms the AODV and AODV-Blacklist. Even at higher loads, i.e., 40 sources, DRR is able to offer more than twice the packet delivery ratio in AODV. In contrast, the AODV-Blacklist scheme, which simply detects and avoids communication through unidirectional link, can offer only a slight improvement. The results show that the unidirectional link avoidance technique of AODV-Blacklist is not as efficient as the DRR. It is because the routing path construction process has been restricted to only using bidirectional links, hence limiting the number of forward routes which the scheme can utilise.

5.5.3.2 Normalised Routing Load

Figure 5.14 shows the normalised routing load for the three schemes. At a maximum mobility of 20 m/s, the AODV and AODV-Blacklist offers a higher routing load compared to the DRR scheme. The high increase in routing load for both schemes is caused by the RREQ rebroadcast, which dominates the total number of routing packets transmitted by the nodes. Despite the fact that DRR uses a local RREP broadcast packet for rerouting, the additional overhead of such control packets is clearly significant when the network is subjected to a high presence of unidirectional links. Although as many as 30% of nodes in the network have a reduced transmission range, DRR scheme still, on average, outperforms AODV and AODV-Blacklist by over 30%. The result shows that the DRR protocol is highly efficient and as such, is capable of handling unidirectional links despite the highly saturated network characteristics.

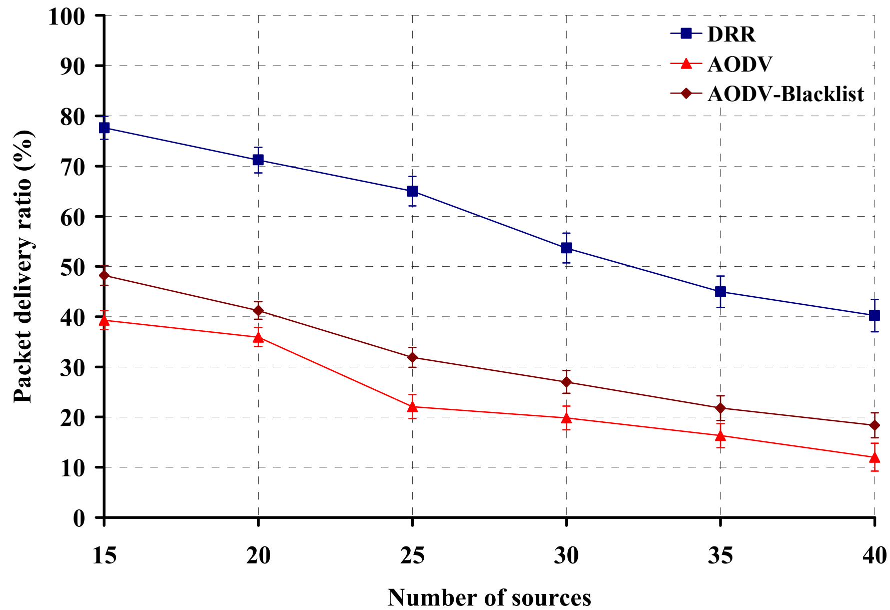


Figure 5.13: Packet delivery ratio as a function of the number of sources

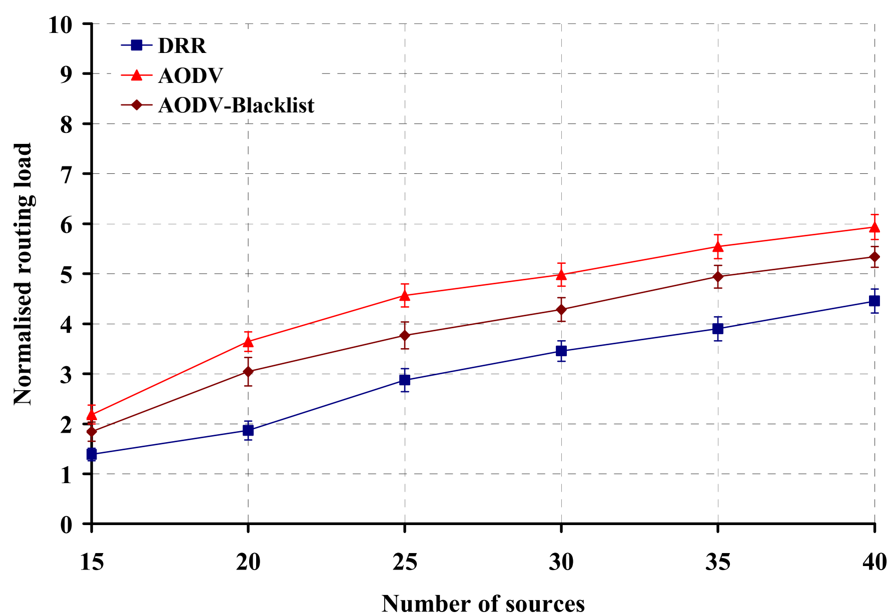


Figure 5.14: Normalised routing load a function of the number of sources

5.5.3.3 Packet Loss

Packet loss for the three schemes is shown in Figure 5.15. Generally, every scheme has a lower packet loss when sources are set to 15. However, as the number of source nodes increases, more packets are transmitted via the active connections. The network becomes congested and as a result, more packets are dropped. The DRR scheme exhibits better performance because it can rapidly construct the routing path. Therefore, the probability of buffered data packet being dropped is minimised, resulting in a lower packet loss.

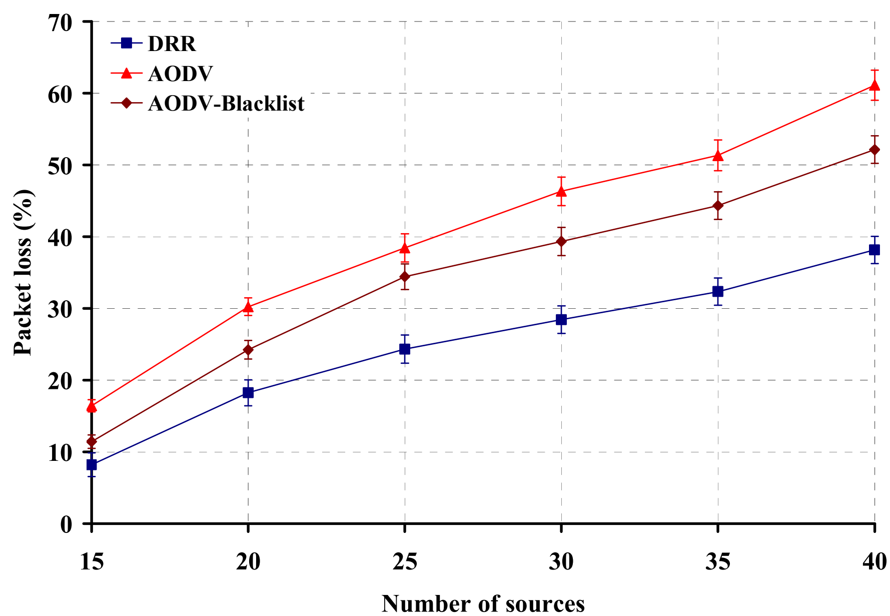


Figure 5.15: Packet loss as a function of the number of sources

5.5.3.4 Average Delay

Figure 5.16 shows the average delay in a network scenario where 30% of the nodes are set with P_{tlow}. The DRR scheme shows only a small increase in average delay compared to AODV and AODV-Blacklist. Such an effect is due to DRR utilising unidirectional link to propagate RREQ packet towards the destination. It is also observed that, the average delay of AODV and AODV-Blacklist schemes remain at a level that is consistently higher than the DRR throughout the entire experiment. This is expected since both schemes restrict routing from using unidirectional links. Such a constraint therefore prevents a forward route being formed over unidirectional links, causing a significant delay to create the routing path. On the contrary, the DRR scheme utilises the unidirectional links by slightly compromising a RREP packet drop on the reverse path, therefore improved overall routing performance can be achieved. With a high unidirectional link presence, the DRR average delay is nearly four times lower than AODV.

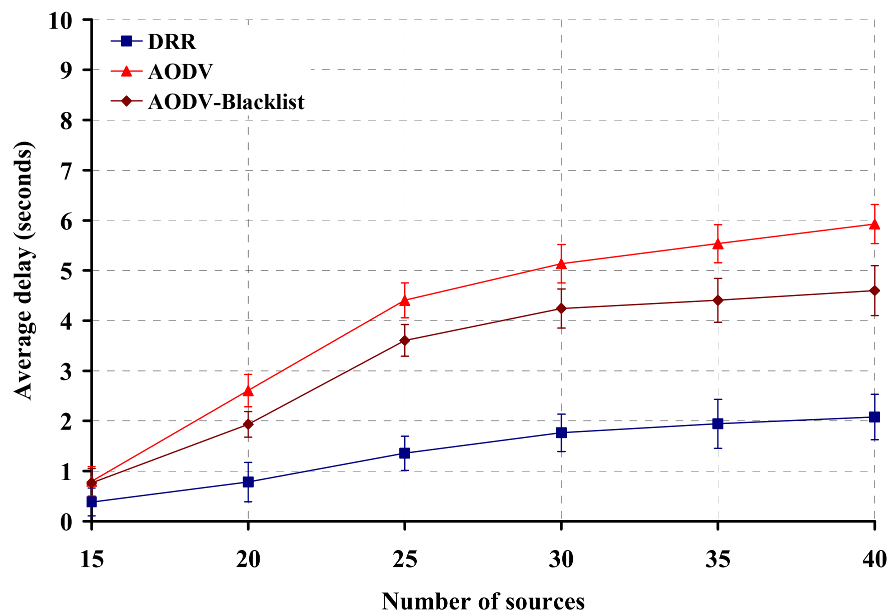


Figure 5.16: Average delay as a function of the number of sources

5.6 Summary

This chapter presents a scheme referred as the Dynamic Reverse Route (DRR), proposed for mobile ad hoc networks. The main feature of the scheme is the ability to efficiently construct routing paths despite high numbers of unidirectional links present in the network. As shown by the simulation results, the DDR scheme is able to reduce delays and routing overhead. The scheme enables nodes to exploit a neighbour node's unused route entries and rapidly compute alternative paths around the blocked path, caused by unidirectional link. Despite the introduction of additional control packets, the degree of routing overhead is lower compared to other competing protocols. Network Simulator 2 (NS2) is used as the simulator tool to perform the simulation experiment. The performance of DRR scheme is compared with AODV and AODV-Blacklist routing protocols. The mechanisms used to handle unidirectional links in these two protocols have been shown to be inferior in terms of performance of network. The AODV scheme does not offer explicit node detection of unidirectional link and therefore causes the system to wait for source node to timeout. As a result, a higher delay is incurred. On the other hand, AODV-Blacklist provides a detection and avoidance mechanism but fails to utilise all available links for its routing path construction. The DRR scheme outperforms both protocols due to its flexibility in using such links. By compromising a few lost packets, the scheme allows the forward route to be discovered via unidirectional links. If there are sufficient alternative paths around the blocked links, the scheme can be guaranteed to construct routing path on the first route discovery attempt. Performance evaluation of the schemes shows that DRR performs better than both AODV and AODV-Blacklist when considering a variety of metrics. As expected, with an increase in mobility, offered load and network size, the performance of DRR will slowly degrade but consistently shows superior performance when compared to the competing protocols.

Despite the superiority of DRR, improvements in performance can be sought. The DRR scheme can be considered as a reactive scheme, where the detection process is invoked only after the failure to received acknowledgement packet. Such behaviour may prevent the proper operation of applications that require lower delay and minimal performance degradation. Thus, it is important for nodes in a wireless multi-hop network to be able to form reliable routing paths with the least possible loss. Building upon this idea, the next chapter presents a scheme capable of reducing losses while proactively detecting unidirectional links using the path loss estimation technique.

A possible application for the proposed scheme is for data tracking of environmental conditions, animal movements, and chemical or biological detection, where nodes are equipped with small wireless tracking devices that are typically limited in terms of battery power. In such a case, it can be difficult to replenish the battery power and thus, the radio transmission range can be severely affected. Consequently, a high number of unidirectional links may be formed, causing the significant degradation of network performance. Other possible applications include information/bulletin aware services in theme parks, outdoor network access using ad hoc wireless network, and ad hoc communication during meetings or lectures in campus. Nonetheless, despite the significant reduction of delay, the proposed scheme may not be suitable for vehicle-to-vehicle network applications, which require a scheme that can provide route stability with high nodal mobility.

6. AODV with Path Loss Estimation Technique

6.1 Introduction

The connection between wireless mobile devices via radio signals is susceptible to numerous changes during the signal propagation. Link conditions can be unstable, thus affecting the broadcasting transmission pattern and the SINR at a particular node. For this reason, the communication path established by MANETs routing protocol is generally more unpredictable compared to the infrastructure-based wireless network. The concept of distance vector routing, which is quite prominent in wired network has been widely adopted in MANET due to its simplicity and light-weight mechanism. In the typical distance vector routing method, the shortest distance is defined as the lowest hop count. Previous research work [138] has indicated that using hop count can improve the route life-time. However, the metric performs poorly over transient links that lead to frequent disconnection mirroring the effects of mobility. Although regarded as the simplest and primitive routing metric, hop count approach may not be suitable for MANETs. Thus, forwarding packets via paths that are computed based on the lowest number of accumulated hops is often not practicable and does not offer the best routing performance.

Research work [139] has shown that other radio metrics such as round-trip-time (RTT), expected transmission count (ETX) and expected transmission time (ETT), may provide a better solution to hop count. The link conditions such as delay, loss, and the available bandwidth are continuously monitored by nodes to support routing path computation. Despite the advantages, these metrics often fail to alleviate the fundamental problem in heterogeneous wireless communication, which is the unidirectional link.

In light of such deficiency, the scheme proposed in this section is designed to enable nodes to effectively determine the unidirectional link and subsequently computes the best routing path for data transportation. The proposed routing mechanism is referred as AODV with path loss (AODV-PL). It offers rapid routing path construction in a network with high presence of unidirectional link and minimises the routing overhead. In addition to finding the shortest path, the scheme also takes into account the path loss and received signal strength (RSS) for the routing path construction. Based on simulation results, the probability of routing paths being established using the AODV-PL is significantly improved, despite the decrease in the number of nodes per unit area (low node density). The remaining chapter is organised as follows. Section 6.2 discusses the routing metric formation while section 6.3 presents the unidirectional link detection scheme for AODV-PL. Section 6.4 discusses the simulation results and is separated into two parts. The first part presents the simulation results of the comparison of proposed metric with traditional hop count and RSS. The second part compares routing performances of AODV-PL, DRR and AODV-Blacklist routing protocol. Section 6.5 discusses the comparison of routing performance with difference mobility models. Finally, section 6.6 summarises the chapter.

6.2 Routing Metric and AODV-PL Operation

The AODV-PL is a novel and practical routing scheme capable of proactively constructing forward routes through unidirectional links. The underlying protocol is on-demand distance vector and, as such, the prime objective of discovering the shortest distance remains. The addition of *path loss* and *RSS* metric to the AODV route computation substantially improves the link selection process. Such technique extends the traditional distance vector approach and allows a node to avoid links that are deemed unreliable for routing packets. Based on the new routing metric, the state of the links can be efficiently predicted. Links that are considered unreliable are avoided; these include those that are potentially unidirectional or perhaps a link that may be susceptible to breakage. The following section discusses the proposed routing metrics, i.e., the combination of path loss, RSS, and hop count.

6.2.1 Routing Metric

An important constituent in wireless ad hoc multi-hop routing protocol is the mechanism to select the optimal routing path from a set of available links between a pair of source and destination nodes. A scheme may choose a route with the lowest delay to accommodate a real-time traffic. However, the created path may not be able to offer the lowest power consumption. Other schemes can offer high route-lifetime but lower values in terms of throughput. Hence, there is no absolute best route. The routing metrics such as delay, bandwidth, and energy can be regarded as the second-order routing costs. On the other hand, the primary or the first-order routing metric is the availability of radio signal, which is considered as the principal element to form a connection between wireless nodes.

As discussed in previous chapters, node radio power can be non-homogeneous, an effect caused by different transmission power capability, SINR, etc. The packet propagation encounters several environmental issues, reducing the received signal strength. Typically, a low received signal power indicates the link is unreliable, where the transmitter-receiver separation distance is high. However, such assumption is not always true when the network is non-homogeneous. Basically, the received signal is also a function of the transmitting radio power (as shown by equation 4.2). As such, nodes with low received signal strength could also imply that the sender node is transmitting with low radio power while in proximity with the receiver. The propagation can also be affected by interference and losses due to environment, which may deteriorate the absolute signal strength of the received packet. Thus, using the highest received signal strength by itself is not sufficient to indicate that the link is reliable. A more accurate way is to add path loss to the route computation, which distinguishes between transmitted power and the received signal power.

To choose the best routing path, the destination node typically responds to the freshest RREQ packet. This is determined by inspecting a set of parameter values, referred as the routing metric included within the packet. In the proposed method, a simple mathematical expression is used to form the routing metric. At every node, a reverse link pointing to the source is computed based on the metric, where the lowest value is preferred.

6.2.2 Routing Metric Formation

The parameters considered in the proposed metric are path loss, RSS and the hop count. As RREQ packet travels towards the destination, each link cost pointing to the source node is computed and updated. The process repeats until the packet arrived at the destination node, where a RREP packet is returned to complete the routing path construction. The routing path is updated as needed when changes occur on the system. Generally, the parameters used for the routing computation are considered restrictive, which depends on a *minimum* or maximum value. Assume M is the minimum metric, measured based on the three parameters P_1, P_2, and P_3, which corresponds to path loss, RSS, and hop count respectively. Intuitively, P_1 and P_3 should be minimised whereas P_2 is maximised. A simple approach to form the metric M is shown in equation 6.1.

$$M_{\min} = \frac{P_1 \cdot P_3}{P_2} \tag{6.1}$$

There are no specific or formal rules for developing such cost function and they can be as simple or complex as required. In this work, the simple approach is taken and the cost function shown by equation 6.1, based upon simplicity intuition, is deployed. The multiplication operation is an effective method to combine the P_1 and P_3 metrics, because they both represent a means of quantifying propagational losses. Furthermore, the metric M's applicability will be evaluated based upon extensive simulations in section 6.4.1. It is possible to adopt more complex approaches to refine the scheme and this is considered for future works.

6.2.3 Intermediate Cost Along a Path

The operation of AODV scheme using the cost function shown by equation 6.1 is described in this section. Figure 6.1 illustrates the parameter values associated with each receiver node (node at the end of the arrow line). These parameters are consistently used in this section to demonstrate the routing path selection using 1) the proposed routing metric, and 2) using independent parameters, i.e., path loss and RSS.

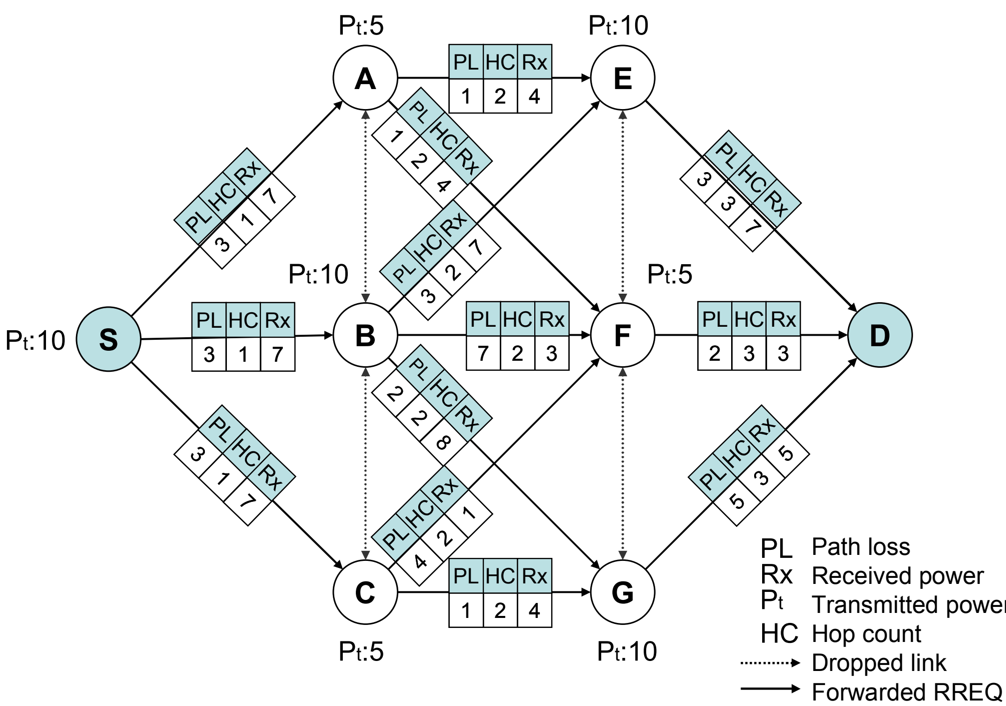


Figure 6.1: Parameters at each link between nodes

A numerical example shown in Figure 6.1 is a simple network with 8 nodes, where two different levels of transmission powers, i.e., 10 and 5, are assigned to different nodes. The corresponding path loss for each link, hop count and RSS are shown in the small table along the link. In this example, path loss is simply considered as the difference between P_t and Rx. The dotted lines represent dropped links that are caused by the obsolete RREQ packet, which advertises a hop count higher than the value stored by the receiving node.

6.2.3.1 Path Computation Using RSS

Based on Figure 6.1, the routing path computed between node **S** and **D** using only the strongest RSS have resulted in a best route of **S**-**B**-**E**-**D**. The total loss accumulated along the routing path is 9, which accounts for 30% loss compared to the total transmitted power, i.e. 30. The result of the routing path computation is shown in Figure 6.2.

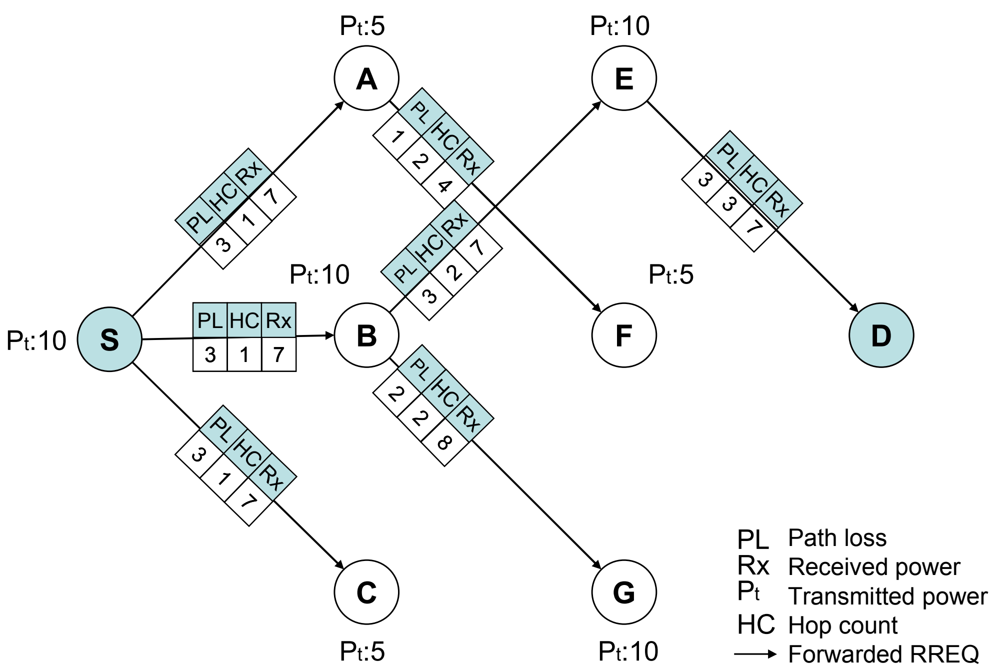


Figure 6.2: Routing path computation using strongest RSS

6.2.3.2 Path Computation Using Path Loss

A routing path formed using only the lowest path loss as the cost function results in the path **S-A-F-D**. The total loss is slightly lower compared to the RSS metric, i.e., 6, however, the resultant efficiency is identical, i.e. 30%. It is because the total radio power used by the nodes along the path is much lower, i.e. 20. Figure 6.3 shows the routing path computed with path loss as the cost function.

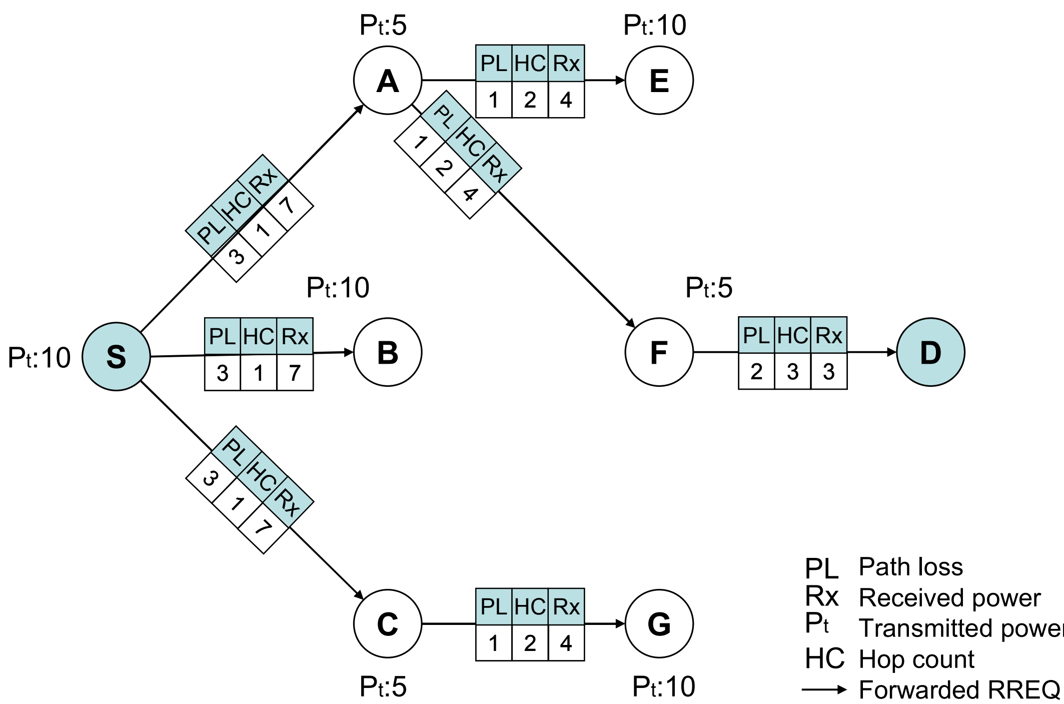


Figure 6.3: Routing path computation using lowest path loss

6.2.3.3 Path Computation Using the Proposed Routing Metric

In contrast to the metrics previously discussed, the proposed metric considers the highest RSS, the lowest path loss and hop count along the path. Such a technique can optimise the network performance by choosing upstream nodes that can transmit the signal along the path with the lowest loss. In addition, the total transmitted power can be significantly reduced, leading to efficient use of node energy. Based on the proposed metric, the transmitted packet from source to destination creates the path **S-A-E-D**. Although the accumulated path loss is 7, the efficiency is increased, where loss is only 28%. The following figure shows the routing paths.

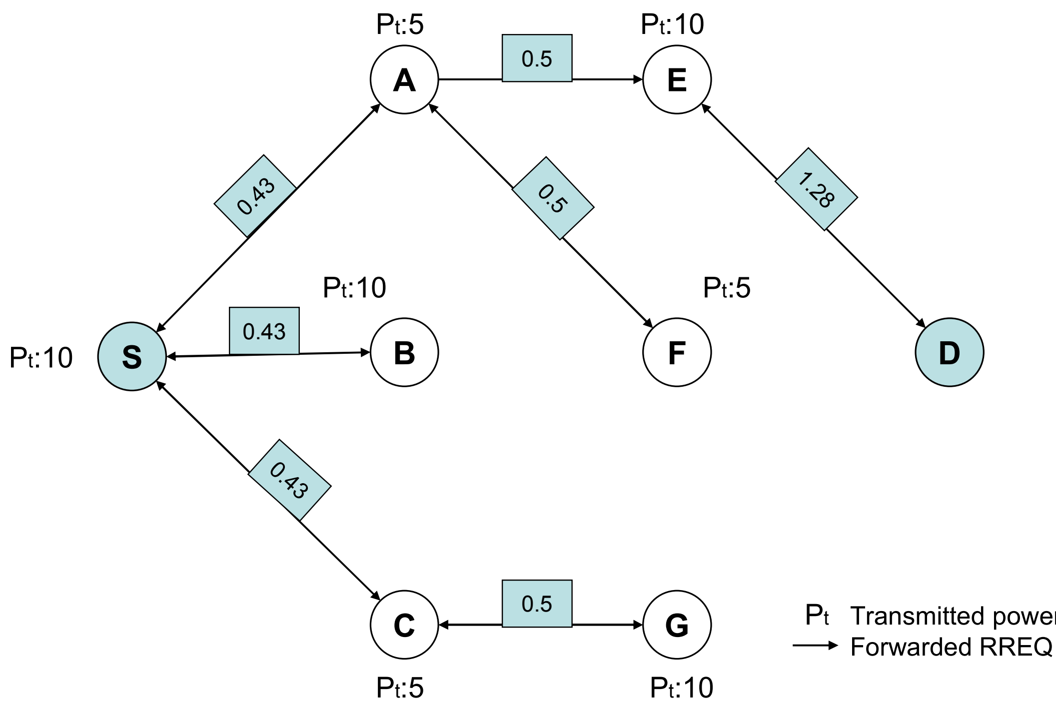


Figure 6.4: Routing path computation using the proposed routing metric

6.3 AODV-PL Routing Operation

This section discusses the proposed scheme's unidirectional link detection mechanism, which include the proposed routing metric discussed in section 6.2.2. In research work [63], Ko proposed a scheme to proactively avoid a unidirectional link during route discovery phase. The scheme, however, relies only on the traditional hop count metric to compute the routing path. Despite computing the shortest distance (in terms of hop), the hop count metric does not offer sufficient information for nodes to avoid links with unidirectional link. Such an issue frequently arises when nodes in the network are assigned with non-identical transmission power. By contrast, the advantages of the proposed scheme are two-fold. First, it uses a cost function that enables nodes better able to avoid links with high losses. Secondly, the proposed scheme implements a path loss measurement technique, where nodes can rapidly identify unidirectional link and subsequently removed from the route selection process. As shown Judd et al., the path loss can be used effectively as a routing metric to improve the routing path selection [140]. The work proposed an algorithm that enables the receiver to reversely predict the RSS at sender side by using the path loss measured between them. Other parameters such as bandwidth and delay are options for path computation. However, such metrics may not be as effective, since the information provided is less able to indicate if the link is unidirectional.

6.3.1 Path Loss and Received Signal Strength

The main objectives of the proposed scheme are to proactively avoid unidirectional links during route discovery phase and to choose paths that are reachable only via the shortest bidirectional links.

The fundamental property that ensures correct operation of the proposed scheme relies on the path loss measurement between the sender and receiver node. In typical wireless operation, the RSS is measured only on the receiving side. However, the AODV-PL scheme enables the RSS to be pre-computed on the sender side by using the information collected from the received packet. This technique allows the sender node to predict whether the link facing the receiver node is reachable, hence bidirectional. Although path loss can vary over a period of time, the instantaneous path loss in both directions is quite similar and therefore will not affect prediction accuracy. Theoretically, a path loss is a function of distance, frequency and the path loss exponent. As such, the direction in which the signal travels is not significant and therefore, does not affect the path loss properties. The path loss can be represented by the Reciprocity Theorem [141], as previously discussed [140], which states: "*As path loss is entirely determined by the signal transfer function, the instantaneous path loss between two nodes is the same in both directions and a transmitter can obtain the path loss to a receiver by measuring the* *path loss from the receiver to the transmitter*". In other words, for adjacent nodes, the instantaneous path loss in either direction, i.e., towards sender or receiver, is equal.

In light of this, it is possible for a node to determine the instantaneous path loss in the reverse direction given that sufficient information can be gathered from the receiver (the node which sends the RREQ packet). Nevertheless, the RSS value can also be slightly affected by interference, which mostly results from the hidden node terminal problem. The results from experimental work [140] show that the effect of interference on RSS in most cases is typically under 1dB. Therefore, in order to compensate for the effect of SINR at the receiver, a maximum reduction of 1dB is added to the RSS prediction in the proposed scheme. Consequently, with the impact of SINR being compensated, the path loss computation will be more reliable.

6.3.2 Propagation Model

As described in Chapter 4, radio signals may be affected by many factors such as transmitter-receiver separation distance, antenna transmitting power, antenna gain, multi-path transmission due to reflection and diffraction, fading, obstruction, etc. [115]. Radio propagation is also influenced by the type of environment, e.g. free-space, LOS or NLOS, urban area, indoor and outdoor. Although radio transmission is not always predictable, the characteristics and external factors affecting them can be reasonably well represented using an appropriate but specific model. To show the effectiveness of the proposed scheme, the AODV-PL scheme is built upon a more realistic propagation model, the log-normal shadowing, as discussed in section 4.3.1.2. Such model, used in many research work [111][112], effectively describes the NLOS signal propagation in a cell of up to 1 kilometre in radius.

Figure 6.5 summarises the algorithm in AODV-PL scheme. Each node constantly seeks for fresh routes advertised by adjacent nodes. At the destination node, a fresh route is computed from the parameters included within the received RREQ packet, which results in the lowest metric shown by equation 6.1. In the simulation model, the path loss is computed using the log-normal shadowing model, as shown by equation 6.2.

$$L(d) = P_t - P_r = L(d_o) + 10\mu_{pl} \log_{10}(\frac{d}{d_o}) + X_g \tag{6.2}$$

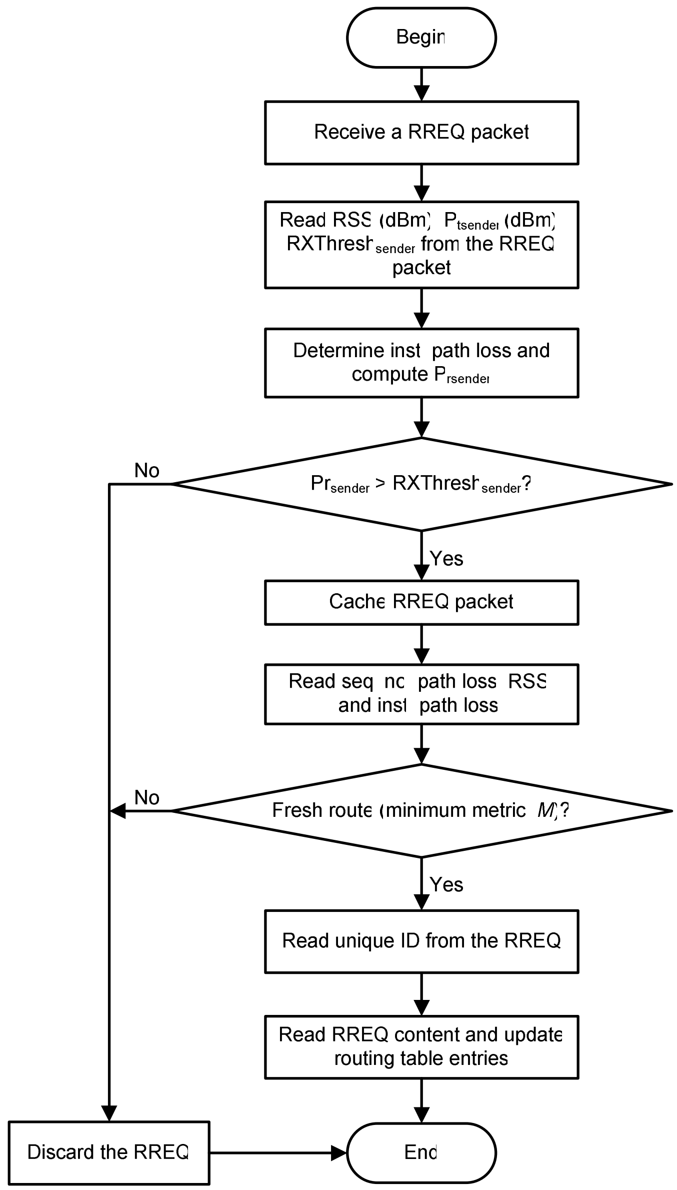


Figure 6.5: Unidirectional link detection and fresh route update mechanism

In equation 6.2, the normal distribution represented by X_g, accounts for the shadowing effect, which may be encountered in an area with many buildings. The transmitter-receiver separation is d, in meters while d_o is the reference distance, typically set to 1 meter [114][142]. Table 6.1 provides the typical path loss exponent μ_{pl} in different type of environment. The value of μ_{pl}, particularly for the shadowed urban area is within the range of the empirical results obtained by Souza and Lins [114]. The model described in equation 6.2 theoretically approximates the node's received power (affected by shadowing) at a specific distance from the source node.

Table 6.1: Path loss exponent values

Environment		μ_{pl}
Outdoor	Free space	2
	Shadowed Urban Area	2.7 to 2.5
In building	Line of sight	1.6 to 1.8
	Obstructed	4 to 6

6.3.3 Received Signal Strength Prediction

The received signal power can be measured by node's interface and has been formally defined in standard 802.11 [1]. This describes a mechanism in which the circuitry on a wireless network interface card (NIC) can measure the radio frequency (RF) energy received by the antenna. As previously discussed, based on RSS and the P_t advertised by the source, it is possible for receiver node to estimate the reverse RSS. However, for such method to be successful, every packet sent by the source must be appended with the sender's P_t and the minimum receiver sensitivity value, *RXThresh*. As shown in Figure 6.6, source **Y** appends P_{tY} and $RXThresh_Y$ to RREQ and propagates the packet over a distance of R_Y. Assuming node **X** is idle, the RREQ packet from node **Y** is captured and the path loss is computed by using the difference of P_t and P_r given by equation 6.2. Consequently, node **Y**'s RSS (P_{rssY}, in dBm) can be predicted at node **X** using equation 6.3.

$$P_{rssY} = P_{tY} - L(d) \tag{6.3}$$

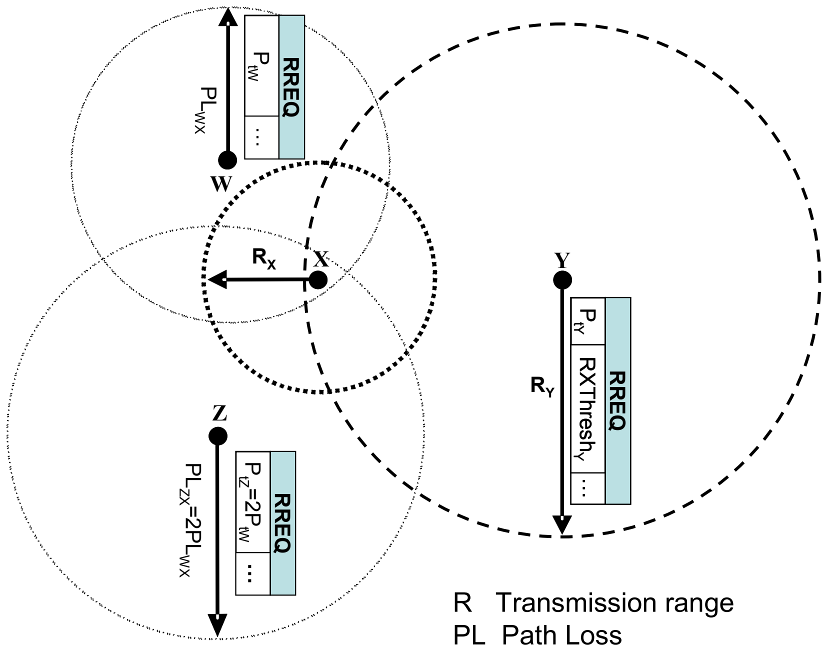


Figure 6.6: A unidirectional link between node **Y** and node **X**

The AODV-PL mechanism involves two steps; first the detection and removal of unidirectional link, and secondly, route freshness inspection. As shown by Figure 6.5, when a node receives a copy of RREQ packet, the RSS along with the P_t and *RXThresh* of the sender is cached. Later, the instantaneous path loss is determined, which can be used to predict the sender's RSS (Pr_{sender}). The Pr_{sender} is then reduced by 1dB and compared with the sender's received signal threshold, $RXThresh_{sender}$. If Pr_{sender} is greater than $RXThresh_{sender}$, the link is considered to be bidirectional. The fixed value of 1dB is sufficiently high to mimic the effect of interference on RSS measurement [140]. Multiple interference measurement can be used to slightly improve the computation accuracy of Pr_{sender}. The link is then further inspected for reliability using the metric M (equation 6.1).

The AODV-PL is more reliable than the RSS index [143][144] method for choosing the better routing path. The routing technique [143] actively collects the RSS from the HELLO packets, which are then stored in the neighbour's table. Such a method introduces additional system overhead, since the nodes have to constantly monitor the RSS value even when data is not routed on the network. In addition, for every RREQ broadcast received, the destination node responds with the RREP packet, thus increasing the routing overhead by two-fold. On the other hand, Chang and Leu proposal [144] in effect remove the possibility a routing path to be formed by asymmetrical links. Routes are selected based on the highest link uptime, computed from the RSS rate of change. However, the scheme does not consider P_t in route computation, which is an extremely important component that can affect the receiver's RSS level. Routing protocols that choose links solely based on the strongest RSS typically fail to perform correctly. This can be explained by considering Figure 6.6. Assume that node **Z** and **W** are set with different level of P_t, where $P_{t\mathbf{Z}} = 2P_{t\mathbf{W}}$. However, if the path loss $PL_{\mathbf{ZX}}$, i.e. path loss of link **Z-X**, is twice as high as $PL_{\mathbf{WX}}$, the RSS from both nodes may be detected to be identical at node **X**, i.e., $RSS_{\mathbf{Z}} = RSS_{\mathbf{W}}$. In such a scenario, the RSS scheme [144] may not be able to differentiate the two links based only on the RSS. As a result, node **X** may potentially select a link that is more lossy. On the other hand, the proposed scheme in this thesis can effectively avoid such an issue and chooses the packet from path $PL_{\mathbf{WX}}$, which has a lower path loss compared to the other link.

6.3.4 Proactive Unidirectional Link Detection

In contrary to AODV-Blacklist, the proposed scheme promptly detects unidirectional links during route discovery rather than waiting to fail to receive an ACK packet. As such, the routing construction delay can be significantly minimised. As shown in Figure 6.6, as soon as node **X** receives a RREQ packet from **Y**, the node immediately detects the unidirectional link and prevents the current RREQ packet to be propagated to other nodes. Node **X** computes the expected signal strength at node **Y**, i.e., $Pr_{rss\mathbf{Y}}$ and compares against $RXThresh_{\mathbf{Y}}$, advertised by node **Y**. If $ExPr_{rssY} < RXThresh_Y$, than the

RREQ packet is dropped, otherwise it will be checked for route freshness before being forwarded to a valid next hop node.

6.4 Performance Evaluation and Simulation Setup

Two key sets of experiment were conducted to evaluate the routing metrics and the proposed scheme. The first set applies to the evaluation of routing metrics in random static scenarios, while the second considers the quantification of proposed scheme in different mobilities and network densities.

6.4.1 Evaluation of Metric in Static Scenarios

The first set is conducted over random static topologies of 50 nodes homogeneously distributed in 6 square network areas as shown in Table 6.2.

Table 6.2: Square network area

Network Area (m^2)					
500 x 500	600 x 600	700 x 700	800 x 800	900 x 900	1000 x 1000

Node communication ranges are set to one of 10 different transmitting powers between the range of 0 to 20 dBm. 25 data connections are scheduled and the duration of each simulation run is 900 seconds. The connection duration is selected from a uniform distribution of 0 – 10 seconds. Each individual connection is represented by a CBR source transmitting packets of 512 bytes at a rate of 4 packets/second. Each point on the graph represents a repetition of 25 random network scenarios and the load applied to the network is constant throughout each simulation. The corresponding confidence interval is set to 95% as discussed in Chapter 3. The proposed metric is compared to the traditional hop count and the RSS-based metric. Each metric is compared in terms of the resultant path length, accumulative path loss, average transmitted power, and average received power.

6.4.1.1 Path Length

Figure 6.7 shows the path length (the number of nodes each packet traverse from source to destination) versus the network area. The number of nodes is fixed in each network (50 nodes). Thus, by expanding the network area, the sender-receiver separation distance increases (lower node density). As the number of links to exploit decreases, the performance of each metric to compute the best routing path is significantly affected. It can be clearly seen that routing schemes based on hop count can construct routes with lowest path length (number of hops). On the contrary, the proposed metric suffers a slightly higher path length but performs significantly better compared to the RSS method. Generally, as the network size increases from 500 x 500 m^2 to 1000 x 1000 m^2, the path length discovered by the every routing metric increases. The RSS metric shows a substantially longer path in every network. This is a consequence of nodes seeking to find path with strongest received signal, which results in shorter distance.

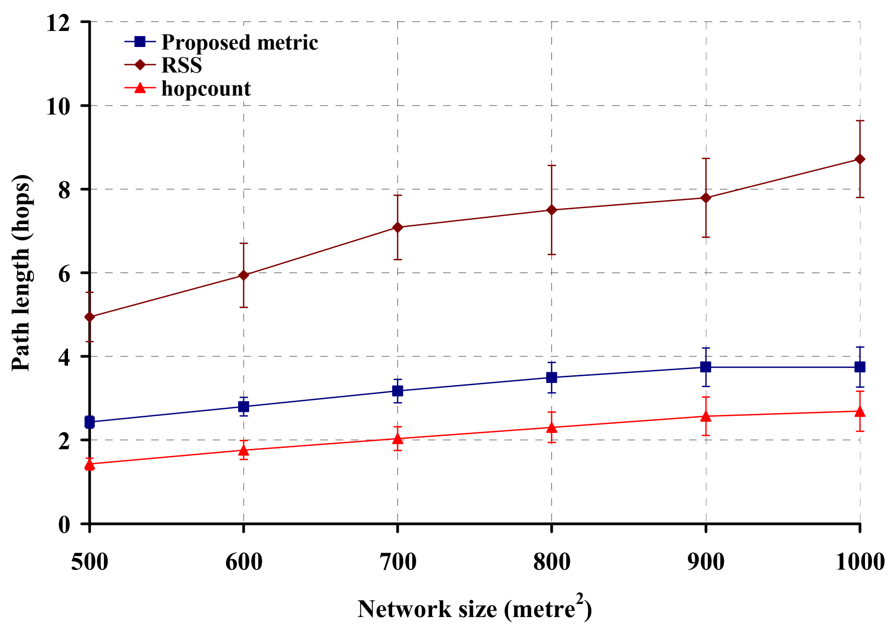


Figure 6.7: Path length comparison

6.4.1.2 Path loss

Figure 6.8 shows the performance of three metrics in terms of the average path loss. The average path loss shown by the RSS is significantly lower compared to the hop count and the proposed metric. This behaviour is expected, because RSS discovers routes based only on the strength of received signal. Typically, a shorter distance between sender and receiver results in a higher received signal strength and this justifies the longer path length accumulated by the RSS method (Figure 6.7). The shorter distance between nodes along the routing path also causes the path loss in the RSS metric to decrease. Nonetheless, such behaviour is not practicable because longer path lengths can cause higher delay and routes are susceptible to breakage. In order to minimise such an effect, the proposed metric compromises a slightly higher path loss with a shorter path length compared to the RSS method. On average, the path loss in the proposed metric is increased by only 6% compared to the RSS.

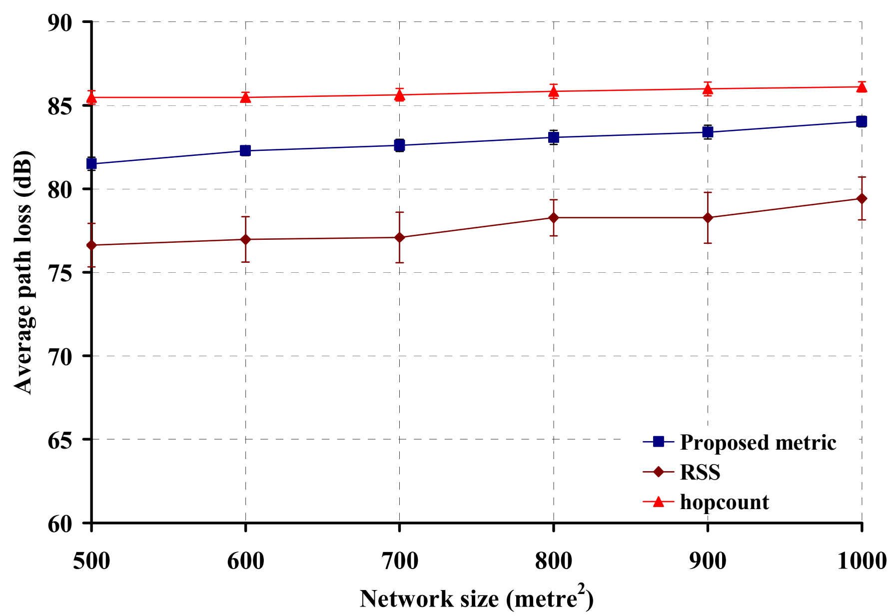


Figure 6.8: Average path loss

6.4.1.3 Average Transmitted Power

Another metric of interest is the average transmitted power consumed by nodes in the network. Figure 6.9 shows how the average transmitted power varies against the increasing network size. Previously, it is shown that the hop count method computes the lowest routing path length compared to RSS and the proposed metric. It is because links with longer communication ranges are utilised, hence the high transmitted power. This is clearly shown when network is densely connected, i.e., area with the size of 500 x 500 m^2. In such a scenario, the distance between nodes is low that it may result in a point-to-point connection between a pair of source and destination nodes. This argument is supported by Figure 6.7, where it shows the path length is close to 1. Once the network area is further increased, the average transmitted power slowly decreases because routing packets are propagated via longer paths that may include nodes with low transmitter power. On the other hand, the proposed metric exhibits the lowest consumption of transmitter power although the network is densely connected, i.e., 500 x 500 m^2. The average transmitter power is conserved by as much as 11% compared to the hop count method. Such performance indicate the effectiveness of the proposed metric, where nodes are able to exploits links with low transmitter power utilisation regardless of the separation distance between the sender and receiver. In the RSS method, the transmitter power utilisation is higher compared to the proposed metric. The RSS method filters the inbound packet based only on the highest received signal strength. Therefore, when the network is densely connected (as in the case of 500 x 500 m^2), the receiver nodes have several potential links to choose from for the routing path construction. Typically, a node with high transmitting power causes the receiver nodes to detect packets with high signal strength. However, the links can also comprise of sender nodes with low transmitting power but still in proximity with the receiver. Due to such phenomenon, the number of hops the packet traverse to destination increases (Figure 6.7), causing the average transmitter power to be slightly reduced compared to the hop count method.

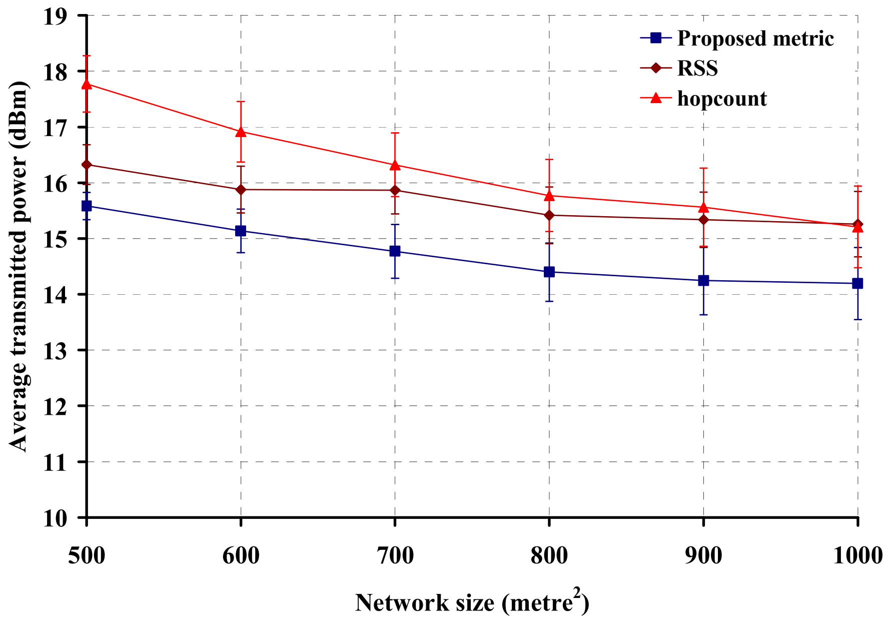


Figure 6.9: Average transmitted power

6.4.1.4 Average Received Power

Figure 6.10 shows the average received power versus the network size. As expected, the RSS method which discovers routing path based on the strongest received signal strength shows the lowest average received power. Observing the results for the proposed metric, the average power received by each node along the routing path is significantly higher compared to the hop count, which indicate the link is reliable (less likely to cause breakage). Indeed, the path length computed using the traditional hop count is lower than the proposed metric. However, the shorter path length represents a higher separation distance, which can results is higher path loss (Figure 6.8) and route breakage.

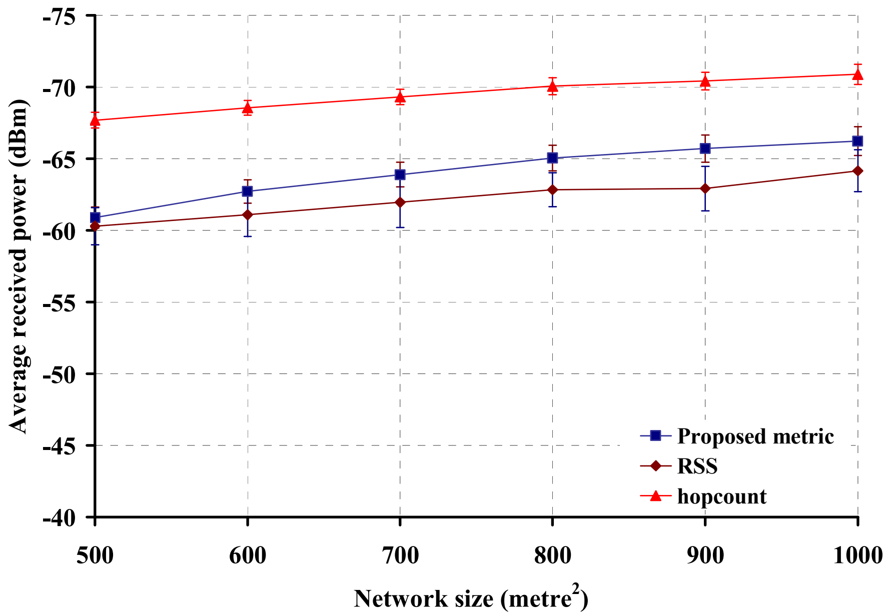


Figure 6.10: Average received power

6.4.2 Evaluation of Schemes in Mobile Scenarios

In this section, the performance of the AODV-PL (implemented with the proposed metric as described in section 6.2.2) is compared with the DRR and the AODV-Blacklist scheme. The objectives are to investigate the scalability and adaptability of the proposed scheme to the variation of network topology and nodal mobility while delivering data packets to their destinations. To assess this ability, each routing mechanism is evaluated with using the performance metrics as described in section 5.3.4 under three network parameters:

- Network density
- Mobility density
- Transmission range

6.4.3 Network Size

In this evaluation section, the number of nodes in each topology is varied according to the area of network such that the nodal density is *approximately constant*, i.e. 1.42×10^{-4} nodes/m^2. The corresponding network area and number of nodes for the simulation is shown in Table 6.3.

Table 6.3: Network size

Network area (m^2)	700 x 500	780 x 540	850 x 580	910 x 620	950 x 670	1000 x 700
Number of nodes (*N*)	50	60	70	80	90	100
Node density (*N*/m^2)	1.42×10^{-4}	1.42×10^{-4}	1.42×10^{-4}	1.42×10^{-4}	1.42×10^{-4}	1.42×10^{-4}

The performance of routing schemes is computed by increasing the number of nodes in the network from 50 to 100 nodes. The area of the network is also changed to reflect the scalability issue. Such evaluation differs from section 6.4.1, where node density is varied (fixed number of nodes and varying network area) to see the effect of transmission range on the network metrics. In this section, a large area with many nodes means that a source node may construct a longer routing path to destination nodes than for a smaller area with a lower number of nodes. Such scalability performance is also consistent with previous work [86][145]. As shown by Lee [145], the scalability of networks can be analysed by holding the node density constant. The corresponding node population and network area can be slowly increased while keeping the node density unchanged. This method is effective in assessing the scalability of the schemes in terms of increasing network area. Investigation of scenarios with more than 100 nodes does not appear worthwhile since the performance of all schemes drops significantly for larger setups. The summary simulation parameters for this section are shown in Table 6.4.

Table 6.4: Network size simulation parameters

Parameter	Value
Transmitting power (P_{thigh})	15 dBm
Transmitting power (P_{tlow})	7dBm
Simulation time	900sec
Propagation model	Log-normal shadowing
Mobility model	Gauss Markov
Ratio of low power nodes	0.3
Traffic type	CBR
Packet rate	4 packets/sec
Packet size	512 bytes
Number of sources	25
Nodal speed	0 – 20 m/s

6.4.3.1 Packet Delivery Ratio

The packet delivery ratio for the three schemes is shown in Figure 6.11. The results show the efficiency of routing mechanisms to deliver packets to the destination as the network size increases. In a large network area, each scheme computes a longer routing path compared to a small network area. As such, the paths are more prone to breakage, particularly when nodes are mobile. This is clearly shown by the results, where packet delivery ratio slowly decreases as the network grows in terms of area and nodes population. The AODV-PL exhibits the highest packet delivery ratio because the probability of link disconnection is lower compared to the competing schemes. It is because the AODV-PL computes routing path based on a combination of radio parameters that considers the lowest path loss, highest RSS, and lowest hop count. On the contrary, the DRR and AODV-Blacklist rely only on hop count and thus, routing path computed may not be as reliable. In addition, the proactive detection mechanism offered by the AODV-PL can more rapidly avoid links that are unidirectional when compared to the DRR and AODV-Blacklist schemes. As such, the number of packets dropped as a result of overloaded buffers and routing construction delay is minimised.

6.4.3.2 Normalised Routing Load

Figure 6.12 depicts the normalised routing load as a function of node size. It shows the AODV-PL scheme suffers the lowest number of routing overhead per total number of data packet transmitted to the destination nodes. The scheme adapts to the increasing network density by maintaining links that have the highest probability route lifetime. As a result, the AODV-PL scheme reduces the number of route reconstructions that results from link disconnection. On the other hand, the DRR scheme, which compromises a slightly higher RREP packet drop to detect unidirectional links, offers better performance compared to the AODV-Blacklist. The DRR scheme employs a similar network metric, i.e., hop count, as the AODV-Blacklist scheme. However, the DRR scheme is able to off-set the inherent effect of traditional hop count by temporarily utilising unidirectional links for routing path construction. Nonetheless, the major obstacle of such an approach, i.e., compute routing path based on hop count, is that the sender-receiver separation distance is high. In a highly mobile network, such links have the potential to cause more frequent route disconnections.

6.4.3.3 Packet Loss

Figure 6.13 shows the relationship between the node size and the packet loss of the schemes indicating the degree of reliability of each protocol. Generally, packet loss of the three schemes increases with node size due to wireless link transmission errors, mobility and congestion. The AODV-PL scheme shows the lowest percentage of packet loss, a result of more efficient discovery of reliable links that prolong the lifetime of routing paths. The rapid increase of path loss for every scheme may be due to transmission errors caused the physical condition of the channel or the terrain where networks are deployed. A packet may be dropped at the source if a route to the destination is not available or if the buffer that stores pending packets is full. The lower value packet loss for the AODV-PL scheme also shows that the links between active nodes along the routing path remaining paired for longer as compared to the nodes in the competing schemes.

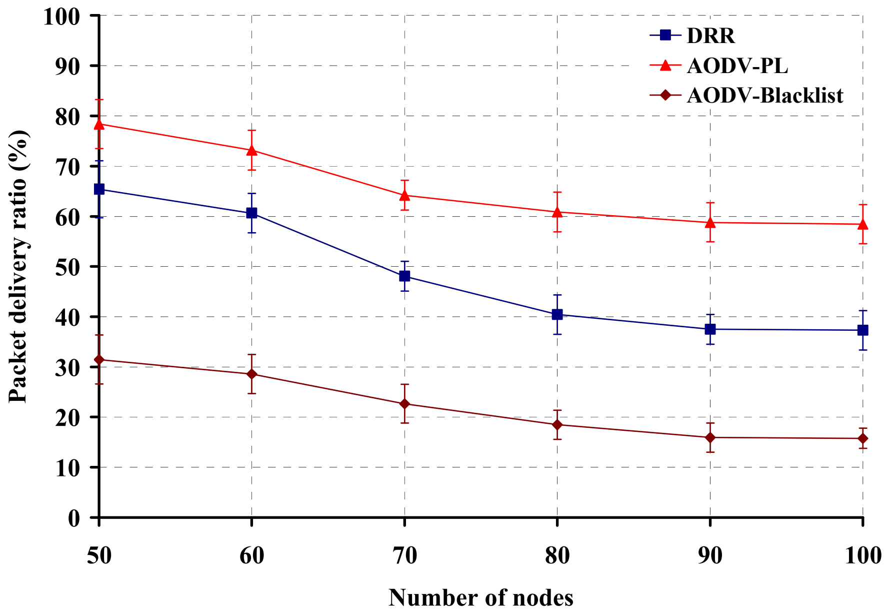


Figure 6.11: Packet delivery ratio as a function of node size

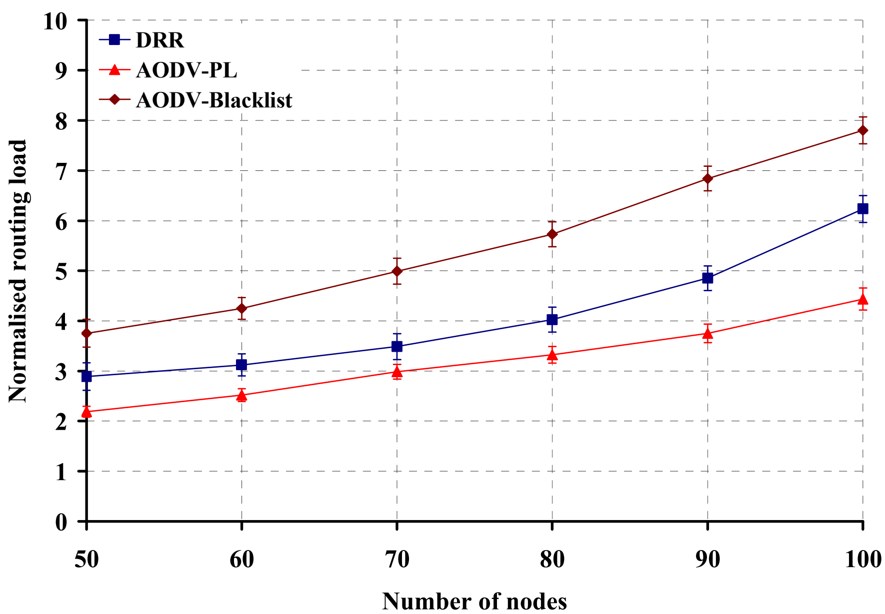


Figure 6.12: Normalised routing load as a function of node size

6.4.3.4 Average Delay

As can be seen in Figure 6.14, the average delay of AODV-PL is lower than both DRR and AODV-Blacklist delay. Typically, the average delay in this simulation is dominated by the waiting time at the source node to re-compute the reverse route blocked by the unidirectional link. The average delay can also include the time incurred in resuming the connections after route breaks have occurred. The delay is higher for AODV-Blacklist when compared to DRR and AODV-PL because AODV-Blacklist has to re-initiate the route discovery process at the source node in order to resume the session. Additionally, in large networks, the time needed for broken paths to be detected by AODV-Blacklist is significantly higher. This is because such notification is delayed as a consequence the longer path over which the route error packet is propagated back to the source node. The AODV-PL has the lowest delay value, as it minimises the impact of route re-discovery due to fewer route disconnections compared to the other two schemes.

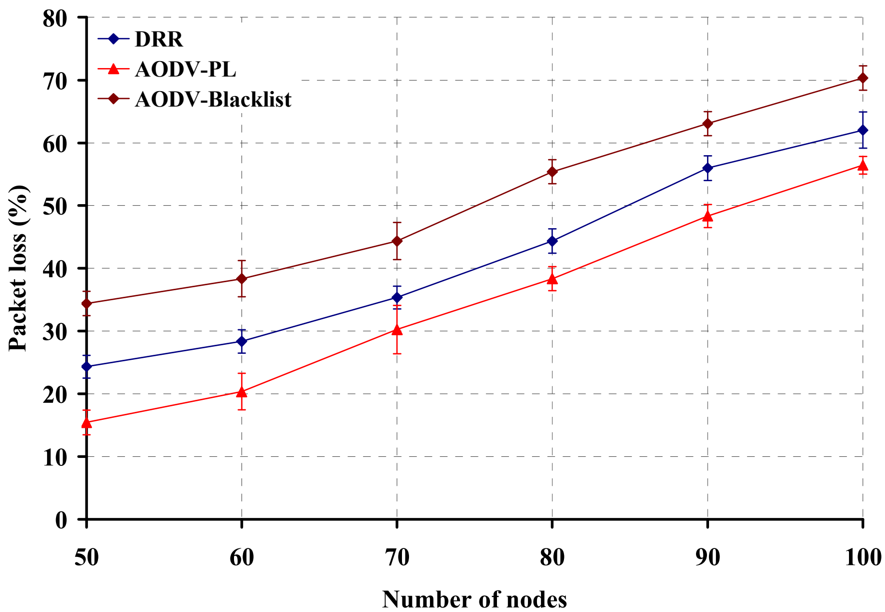


Figure 6.13: Packet loss as a function of node size

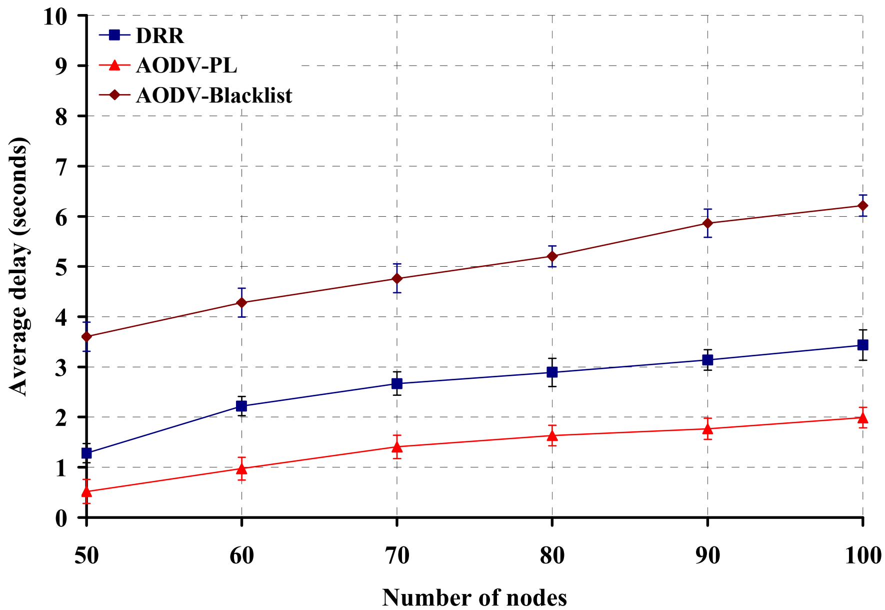


Figure 6.14: Average delay as a function of node size

6.4.4 Mobility Density

In this section, the performance of routing schemes is evaluated with using different network mobility density. For each scenario, the number of mobile nodes is varied while the remaining nodes on the network are set with null mobility (fixed nodes). The aim is observe the ability of routing protocols to perform under the increased stress of route breakages and link fluctuation (due to nodal movement). Such evaluation is also important to investigate the ability of routing schemes to compute and select reliable links for routing path construction. The number of nodes is 50 and the network area is fixed to 700 x 500 m^2. Table 6.5 shows the ratio of mobile nodes against the total number of nodes in the network scenarios. Each mobile node has a maximum nodal speed of 20 m/s.

Table 6.5: Network mobility density

Mobility density ratio	0	0.2	0.4	0.6	0.8	1.0
Number of mobile nodes	0	10	20	30	40	50

6.4.4.1 Packet Delivery Ratio

Figure 6.15 shows the packet delivery ratio versus the ratio of mobile nodes while the maximum speed of each mobile node is varied between 0 to 20 m/s. As the percentage of mobile node increases, the packet delivery ratio for the three protocols slowly drops. In all cases, the performance of AODV-PL is higher compared to the competing schemes. Between a static network and when all nodes are mobile, the packet delivery ratio drops for the AODV-Blacklist scheme is the highest, i.e., 60%. However, the AODV-PL, in all cases, achieves higher packet delivery ratio than the competing protocols.

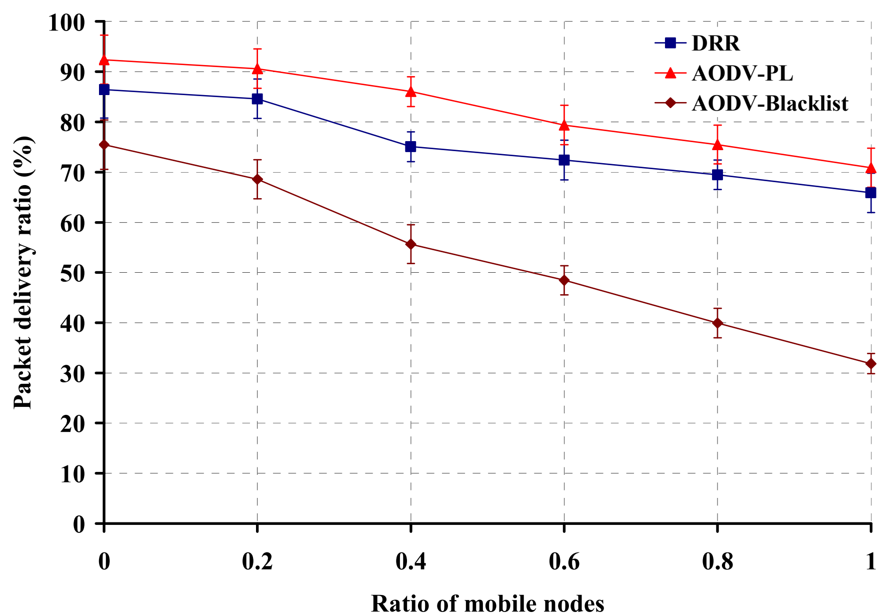


Figure 6.15: Packet delivery ratio as a function of mobility density

6.4.4.2 Normalised Routing Load

Figure 6.16 shows the normalised routing load. As expected, increasing the mobile intensities result in more frequent route failures, which, in turn, trigger route discoveries and the protocol efficiency drops (higher normalised routing load). Comparing the scheme's performance with the results shown in Figure 6.12, it is clear that the impact of varying mobility density is not as severe as when the size of the network is increased. Perhaps, this is due to the limit of maximum speed set to every node, thus, causing the rate change for the links to be nearly identical in each scenario. The normalised routing load may significantly increase if the schemes are evaluated under increasing nodes speed. Although such evaluation is possible, the extremely high value of normalised routing caused by higher nodal speed (and frequent route breakage) would render the simulation output insignificant. Thus, by gradually increasing the number of mobile nodes, the effect of mobility can be more appropriately observed. The rate of increase is lowest with AODV-PL followed by DRR and AODV-Blacklist.

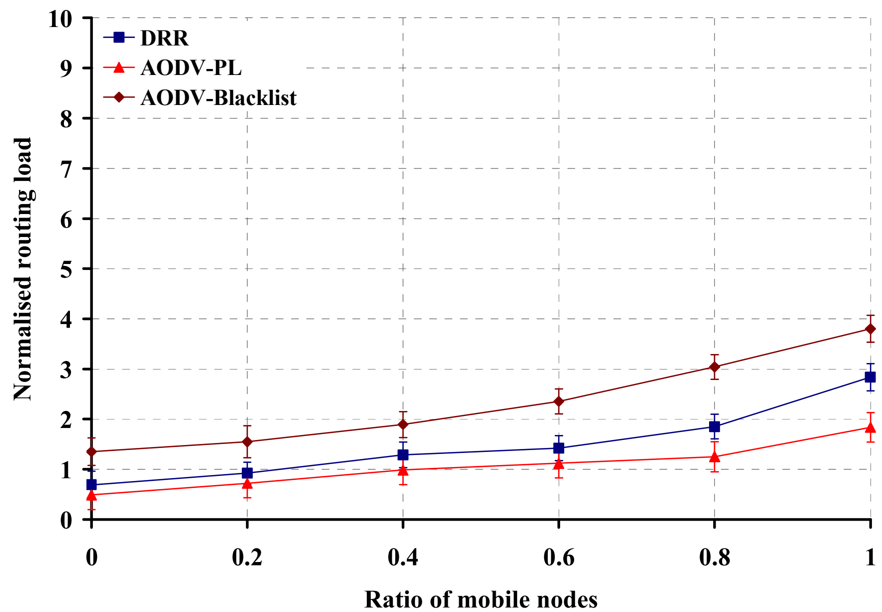


Figure 6.16: Normalised routing load as a function of mobility density

6.4.4.3 Packet Loss

Figure 6.17 shows the packet loss versus the ratio of mobile nodes in the network. The packet loss shown the AODV-PL is the lowest, which indicate the improvement offered by the proposed metric. The packet loss exhibited by DRR and AODV-Blacklist is consistent with previous results, where the routing performance of DRR is better compared with AODV-Blacklist.

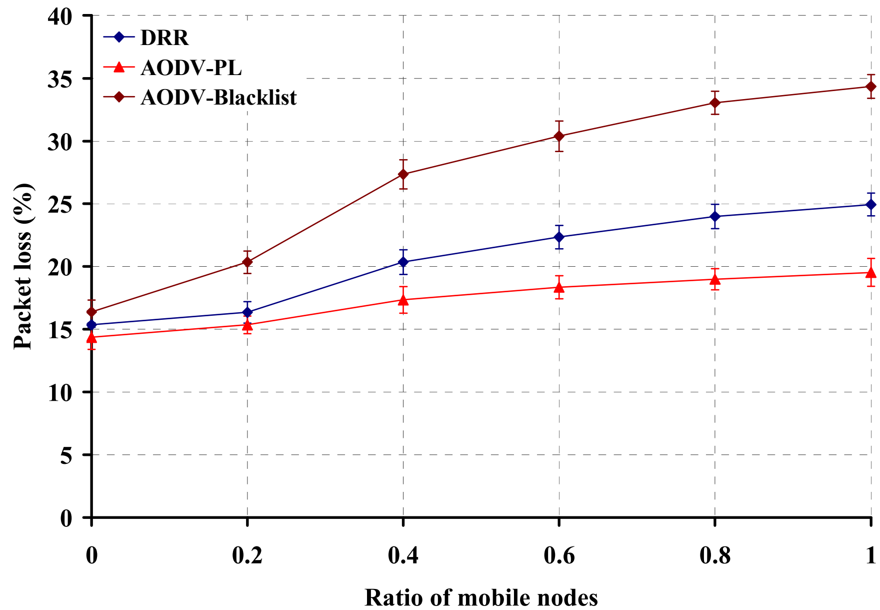


Figure 6.17: Packet loss as a function of mobility density

6.4.4.4 Average Delay

Figure 6.18 shows the average delay versus ratio of mobile nodes for the three schemes. Indeed, when comparing the average delay between AODV-PL and DRR schemes, the difference is small. However, the general performance improvement offered by the AODV-PL is significant considering the fact that its packet delivery ratio (Figure 6.15) and packet loss (Figure 6.17) is higher compared to the DRR. As discussed in section 6.3.3.4, the computed average delay can be affected by the waiting time at the source node to detect the unidirectional link. Both DRR and AODV-PL offers rapid recovery of link blocked by such links. On the contrary, the AODV-Blacklist does not offer protection for a RREP packet drop. Such behaviour causes the source node to wait until the timer expires before sensing that the initial route discovery has failed. This explains the higher average delay incurred by the AODV-Blacklist scheme, particularly for mobility density ratio between 0.4 and 1.

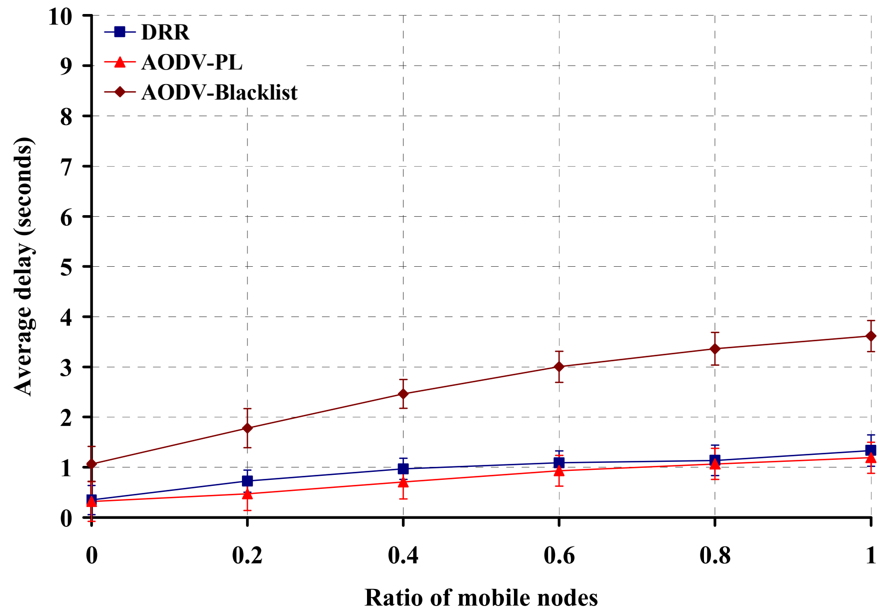


Figure 6.18: Average delay as a function of mobility density

6.5 Routing Performance with Varying Mobility Behaviour

As discussed in Chapter 4, the GM mobility model has been selected as the *reference model* to represent nodal mobility behaviour in this thesis. Typically, a node in the GM mobility model follows a smooth trajectory from one location to another. The model considers historical nodal movement to determine the next vector to future locations. In essence, the GM is a statistical model which is sufficiently complex, that can mimic nodal movement in the real world, e.g., pedestrian, vehicle, etc.

As presented in previous chapters, the proposed schemes have been shown to outperform the reference routing protocol, i.e. AODV, when using the GM mobility model. Indeed, quantifying the proposed schemes based only on a single model may not be sufficient and can lead to inappropriate judgements. Chapter 4 has shown that different mobility models generate different connectivity patterns, which can then impact the simulation output. Therefore, further analysis on the proposed schemes with respect to various mobility models is essential to ensure the *credibility* of results.

The probability of route connectivity, P_{rc}, presented in Chapter 4 is used to characterise the scheme performance in this section. The general simulation parameters employed in this section follow the settings reported in section 4.6. The radio transmission range is varied by adjusting the level of radio power within the range shown in Table 4.2. Additionally, each scheme is measured with different P_{tlow}, which is assigned to mobility models as shown Table 6.6.

Table 6.6: Ratio of P_{tlow} and mobility models

Parameters	**Set 0**	**Set 1**	**Set 2**	**Set 3**	**Set 4**	**Set 5**
Ratio of low power nodes(P_{tlow})	**0**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**
Mobility model	Gauss Markov	-	Random Waypoint	Reference Point Group	-	Manhattan

6.5.1 Transmission Range

This section discusses the performance comparison between AODV-PL, DRR, and AODV with varying transmission range. The probability of route connectivity is used as the performance metric.

6.5.1.1 Probability of Route Connectivity

As shown in Figure 6.19 through 6.22, at low radio transmission range, nodes are less likely to be connected and as a result, the chances of a node being isolated in the network are higher. This is because the number of available links between nodes is relatively small at low transmission ranges and thus, the number of routing path constructed is impacted. As shown in each simulation result, the probability of route connectivity (P_{rc}) approaches zero as the transmission range decreases, which indicates that the number of potential routing paths being created is low. On the contrary, as the transmission range increases, nodes link connectivity improves, causing more links to become available for route establishment. As a consequence, the P_{rc} sharply increases, as illustrated by Figure 6.19, Figure 6.20 and Figure 6.22. However, it is also observed that, nodes in the RPG mobility model (Figure 6.21), exhibits a slower rate of increase in P_{rc}; a consequence of the distinct nature of nodal movement compared to other models. Nodes in this model are formed into groups and, as such, are in proximity of each other. Nevertheless, the separation between groups can be quite distant, which can lead to poor link connectivity and hence decreasing the P_{rc}.

As mentioned in section 2.4.1, a network that is well connected may provide higher network capacity. This required density can be achieved by increasing the transmission range. However, such an approach may cause severe interference, particularly when the network is highly saturated with nodes. The simulation results have shown that, even with low nodal density (50 nodes in 1000x1000 m^2), the effect of interference is obvious. For instance, the P_{rc} in the GM and RWP mobility models are slightly degraded when nodal transmission range is increased above 295 metres. This shows that the nodal connectivity in such models is affected by signal interference. On the other hand, the impact of signal interference is less severe in the RPG and Manhattan model. This may be due to the high nodal separation in such models, which reduces the possibility of signal interference between adjacent nodes.

In addition, it is also observed that, with increasing number of unidirectional links (depicted by the increasing set value from 0 to 5), the performance of each routing protocol is typically degraded. This is expected because the number of available links between nodes drops slowly. The P_{rc} in RWP mobility model (Figure 6.20) is an exceptional case. Routing performance in the RWP model remains significantly better compared to other mobility models. For instance, in set 2 (where 20% of the nodes are assigned with P_{tlow}), the P_{rc} of AODV-PL scheme at 160 metres is as much as 85%. By contrast, with the GM model (Figure 6.19), where all nodes are set with P_{thigh}, the AODV-PL scheme achieves a P_{rc} of only 60%. This results show that the performance of the routing protocol is impacted by the nature of nodal movement. Hence, quantifying the performance of routing protocols based only on a particular mobility mode, e.g. RWP, may be limited and not conclusive.

Nonetheless, for all mobility models, P_{rc} of the DRR scheme is superior compared to the AODV routing protocol. Although the number of unidirectional links is high, the DRR scheme is able to compute alternative paths around any path that is blocked by the unidirectional link. The performance of DRR scheme significantly relies on the availability of potential reverse paths. As such, at low transmission ranges (less than 100 metres), the DRR's P_{rc} is comparable to the AODV routing protocol. However, as the transmission range increases, the DRR unidirectional link detection technique becomes more effective, leading to a significant increase of routing performance.

In the second proposed scheme, i.e. AODV-PL, the P_{rc} is further improved compared to DRR. This is shown by the simulation results illustrated by Figure 6.19 through 6.22. As previously discussed, the AODV-PL scheme is able to improve routing performance by computing paths using a combination of metrics rather than using only hop count. Similar to DRR, when the number of available links between nodes is high, the AODV-PL's routing mechanism becomes more efficient. This is due to the fact that the AODV-PL scheme is able to choose the best path with the lowest path loss to establish end-to-end communication. As shown in these results, the AODV-PL scheme indicates a better performance compared to DRR. For instance, in Figure 6.19, the AODV-PL achieves 90% success of route construction when nodes are set at 190 metres transmission range. On the other hand, DRR and AODV require an additional 30 and 45 metres to achieve the same level of route success probability. In addition, this also indicates that nodes can be configured with lower radio power setting, hence reducing the energy consumption.

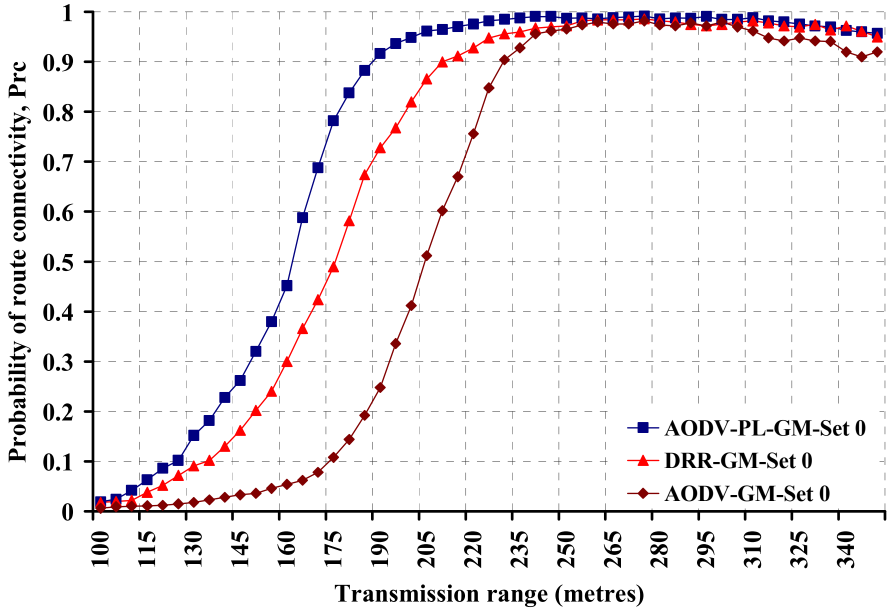


Figure 6.19: Probability of route connectivity (Gauss Markov)

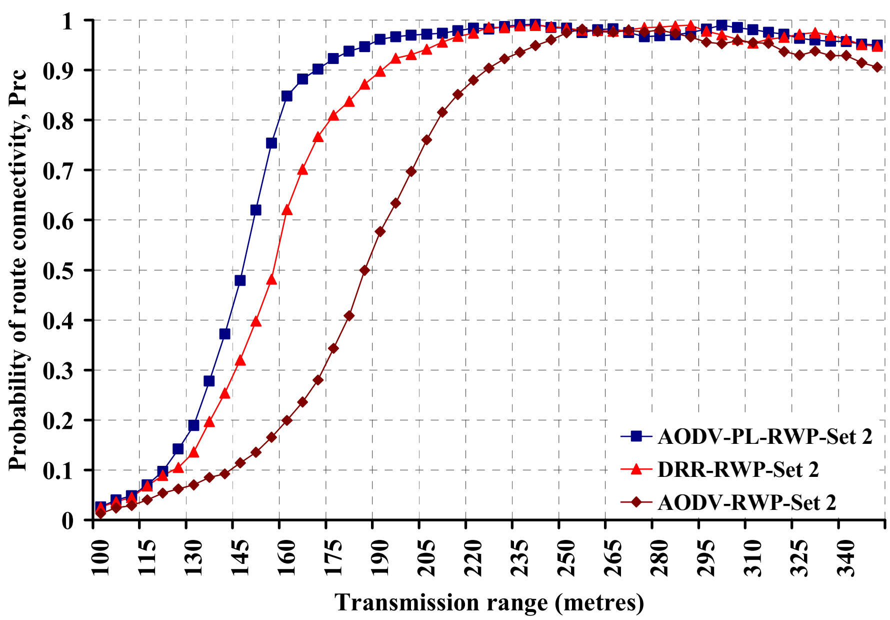


Figure 6.20: Probability of route connectivity (Random Waypoint)

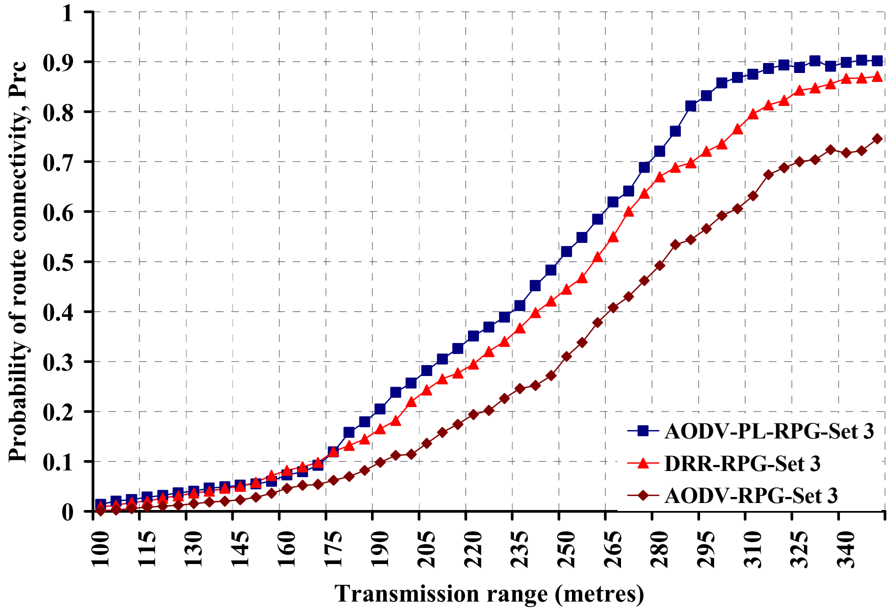


Figure 6.21: Probability of route connectivity (Reference Point Group)

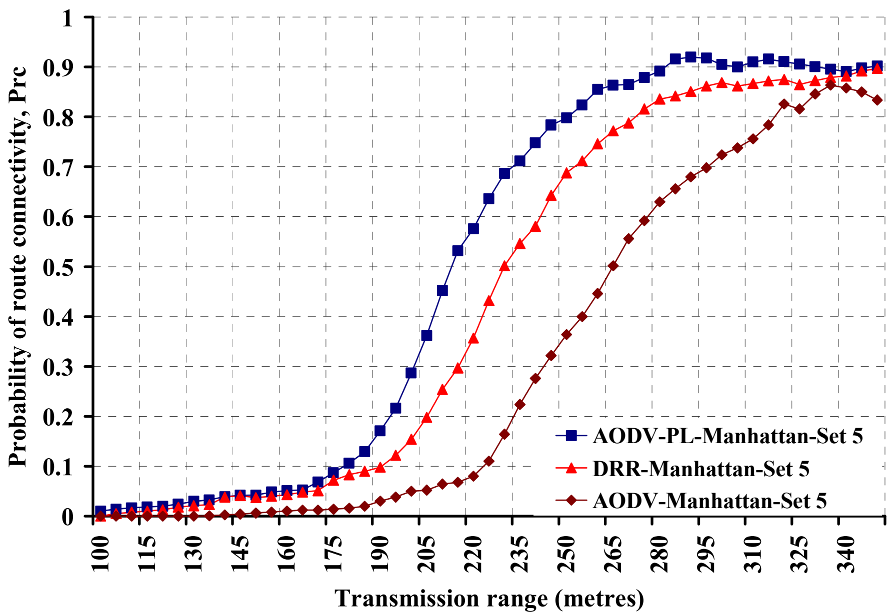


Figure 6.22: Probability of route connectivity (Manhattan)

6.6 Summary

The proposed routing scheme, AODV with Path Loss Estimation Technique (AODV-PL) offers improved performance in terms of packet delivery ratio, normalised routing load, packet loss, and average delay by exploiting links with the lowest path loss and highest received signal in addition to the traditional hop count method. The probability of route breakage is reduced, shown by the lower packet loss and normalised routing load achieved by the proposed scheme. The merits of the proposed scheme are quantified for varying number of network density and mobility density. AODV-PL offers clear improvement over the DRR that temporarily offers routing packet forwarding via unidirectional link. The impact of RREP packet drops resulting from the absence of ACK packet is effectively removed by the AODV-PL scheme. The scheme computes reliable links during route discovery and the unidirectional link can be avoided promptly rather than waiting for the ACK packet to be received from the receiver node.

The performance of the proposed metric under random static scenarios also demonstrated the additional merits of the AODV-PL scheme. It is shown that by using the hop count method, links are not reliable and may be prone to breakage. This behaviour is expected since the hop count metric does not offer sufficient information to indicate that the link can remain connected for a longer period of time. In contrast, the proposed metric explicitly considers the fundamental component of connectivity, which is path loss, transmitter power, and received signal strength. Although the path length is longer compared to hop count, the resultant routing paths are more stable and have longer route lifetimes.

The section also investigates the effect of mobility models on the performance of routing schemes. The proposed schemes are compared against the base protocol under four different mobility models, each with distinct nodal behaviour. Simulation results show a high routing performance differential between mobility models. Nonetheless, the performances of the proposed schemes are consistently higher compared to AODV, which indicate high degree of resilient to network topology changes.

7. Conclusion and Future Work

Routing protocols for wireless ad hoc networks, particularly the reactive approach is significantly affected when unidirectional links are present in the network. Although many routing protocols have been proposed, most of the schemes typically assume operation over symmetrical and bidirectional routing paths, which are not feasible due to the inherent heterogeneous properties of wireless devices. Radio links between a set of wireless devices may be asymmetrical and unidirectional as a result of factors such as high mobility, packet collisions due to interference and the difference in terms of transmission power assigned to the devices. Such an issue should not be ignored because there are many real-world scenarios in which unidirectional links can exist. In this thesis, the effect of unidirectional links on the performance of routing protocol is explored in the context of a reactive and uniform routing approach. Two efficient routing schemes based local reply broadcast and path loss estimation technique were presented. The proposed schemes effectively reduce the routing overhead, which is typically incurred by reactive routing protocol when subject to unidirectional link. Additionally, a new performance metric referred as the probability of routing connectivity is presented, which enhances the analysis of network connectivity for MANET.

7.1 Summary and Conclusion

Chapter 2 presents an overview of MANET and also includes comparison to other forms of wireless ad hoc network technologies. The chapter also provides technical background on the characteristics of MANET, its constraints and protocols that are considered essential for the discussion in the subsequent chapters.

Chapter 3 consist of two parts. The first section discusses various number of routing protocols that exhibit different techniques to handle unidirectional link in the network.

Generally, two main approaches to handle routing operation with unidirectional links exist. The first explicitly avoids and eliminates routing a packet through such link, where all packets must be routed solely using bidirectional link. In the second approach, both bidirectional and unidirectional links are utilised, where nodes are able to exploit full network connectivity and build the shortest route from source to destination. Typically, when the number of unidirectional links on the network is high, the latter approach causes the path between the source and destination nodes to be asymmetrically connected. Researchers have shown that such an approach is inefficient and the improvement is negligible [35][61]. To ensure data is transported via symmetrical routing paths, the schemes proposed in this thesis adopt the former approach. The second part of the chapter presents the evaluation methodology, where detailed explanation of the simulation control is presented. Two existing routing schemes are chosen for the validation purposes, i.e., AODV and AODV-Blacklist, which form the basis of comparison to the proposed scheme in the subsequent simulation experiments.

Chapter 4 presents the network connectivity, which is a paramount component to consider in designing schemes for wireless communication. Since nodes extremely depend on the availability of radio signal, a slight change of mobility and radio propagation can cause disconnection. Many sets of simulation are conducted to observe the behaviour of routing protocols under different mobility and propagation model. Based on the simulation output, two models suitable for the unidirectional link simulation are identified and adopted for the remaining experiments in this thesis. This chapter also presents a new performance metric referred as the probability of route connectivity. The metric enhances the analysis of routing protocols in terms of the success of route construction in addition to the standard performance metrics such as packet delivery ratio, average delay, etc. When nodes are subject to different transmission range, a significant variation is observed between the probability of route connectivity and the link connectivity. Although the network is fully connected, a routing path is not guaranteed to be formed and this is shown by the results obtained by using the probability of route connectivity metrics.

In chapter 5, a practical Dynamic Reverse Route (DRR) based on AODV is proposed. The scheme is proposed to mitigate the network performance issues caused by unidirectional links. The scheme partially allows the routing protocols to be forwarded via unidirectional link but maintain the data propagation via bidirectional path. The scheme reacts to the unidirectional link by employing a passive detection scheme using ACK packet. The failure to receive such packet triggers the local reply broadcast, which utilises the temporary route entries stored in the neighbour nodes. Subsequently, alternative paths can be rapidly built, which results in lower delay and lower routing overhead. The advantages of the DRR scheme compared to the existing approaches are a) simplicity b) ability to minimise the routing overhead and delay incurred as a result of multiple route broadcast, and c) rapid recovery from the failure of reverse route breaks by utilising all possible links pointing to the source node. The proposed scheme is comprehensively evaluated using NS-2 and its advantages are illustrated over the competing protocols. Based on the models selected from Chapter 4, the DRR scheme is analysed under wide range of scenarios with varying ratio of unidirectional links, mobility, and offered load.

Chapter 6 presents the next proposed scheme referred as AODV with Path Loss Technique (AODV-PL). The key operational principle of AODV-PL is to avoid choosing links that are deemed unreliable. The inherent heterogeneous properties of wireless networks render the state of each link to be different. The scheme prioritised link selection based on a proposed metric that is form by combining path loss, RSS, and hop count. The proposed metric is compared against the traditional hop count and RSS method to ensure that it performs as expected. Despite the slight increase in terms of routing path length, results show that the proposed metric is able to discover links with high received signal power and low transmitted power. The number of packet loss is lower compared to other competing schemes, which shows that the routing path is more stable, i.e., remain connected longer. In addition, the AODV-PL effectively reduces the chance to create path via unidirectional links by predicting the symmetrical properties of the link. The RSS in the reverse direction is estimated at the receiver side, which provides a practicable approach to indicate whether the link is unidirectional link or not.

7.2 Future Work

The unidirectional link extension based on AODV offers improvements in terms of packet delivery ratio, average delay, and increases the probability of route connectivity. Nonetheless, there are some areas within the proposed schemes where improvements can be further made.

Although the DRR scheme performs significantly better compared to AODV and AODV-Blacklist, the average delay exhibits by the scheme may not be feasible for applications that require extremely low latency such as real-time traffic. To further decrease the delay, the proposed scheme can be modified to have a lower ACK waiting time. To do this, the parameter ACK_WAIT_TIME should be evaluated for every possible value, which would result in optimum delay for the transmission of real-time packet. The question then becomes, how low the waiting time can be set without causing any issue with the delivery of ACK packet. The time needed for the receiver nodes to return the ACK packet may vary and as such, a definite value may not be practicable to be set for the parameter. A possible alternative is to introduce a lower and upper bound, for which the packet can be successfully delivered. However, such a technique needs to be comprehensively investigated by using simulation. Once the modification is made, the scheme can be evaluated in a network with the nodes set to transmit packets carrying real-time traffic.

Additional analysis work can also be done to investigate the impact of further increasing the size of the network, as discussed in section 6.4.3. Based on the simulation results, the number of nodes assigned is not sufficient to indicate the performance of network for nodes greater than 100. Further analysis on this parameter is possible; however, a significant amount of computing resources may be required in order to reduce the simulation time.

The AODV-PL scheme uses a routing metric based on the combination of path loss, received signal strength, and hop count to detect reliable links. This routing metric reflects the ‘real’ condition of the links and has been shown to perform well compared to the traditional hop count and schemes that are based solely on RSS. Nonetheless, the scheme can be further improved to support high reliability traffic such as TCP. Therefore, additional parameters may be included, such as the round trip time (RTT) value measured by the TCP. The RTT can be implemented on per-hop basis or end-to-end between the source and destination nodes. The RTT enables the source node to determine the level of congestion in the network and subsequently modifies the link selection process. Each parameter can be associated with different weight, which can be varied according the aspect of network that needs to be optimised, i.e., shorter path length, lower loss, less congestion, etc.

Another potential area that can be investigated is the network lifetime, in particular, when nodes are battery powered. As shown by the simulation results, the AODV-PL scheme can operate effectively while the radio transmission range is reduced. Such a performance indicates that a lower radio power can be set for each node, thus leading to lower energy consumption. As a result, nodal lifetime in the network improves.

Other areas of MANET that can be further explored are the multicast and multi-path network. There exists extension of AODV for both type of networks that are referred as the Multicast Ad hoc On Demand Distance Vector (MAODV) and Ad hoc On Demand Multipath Distance Vector (AOMDV) routing protocols. To date, none of the technique described by the proposed schemes for unidirectional detection has been designed for both routing protocols. Furthermore, since the basic routing operation is quite similar to AODV, the same parameters applied in the proposed schemes may be applicable to its multicast and multipath counterparts.

References

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

[2] L. Benini, D. Brunelli, C. Petrioli, S. Silvestri, "GENESI: Green Sensor Networks for Structural Monitoring", *IEEE 7th Communication Society Conference on Sensor Mesh and Ad Hoc Communication and Networks*, Boston, USA, June 2010.

[3] F. Resquin, et. al., "A Low Power Routing and Topology Control Protocol for Cluster-based Environmental Wireless Sensor Networks: The FLORA Project Case", *IEEE 8th International Conference on Mobile Adhoc and Sensor Systems*, Valencia, Spain, October 2011, pp. 132-134.

[4] B. Yan, Z. Jianjun, "The Design of ZigBee Protocol Based Mobile Node in Wireless Sensor Network", *2012 2nd International Conference on Consumer Electronics, Communications and Networks,* Yichang, China, April 2012, pp. 652-655.

[5] J. Tao, G. Noubir, S. Bo, "WiZi-Cloud: Application-transparent Dual ZigBee-WiFi Radios for Low Power Internet Access", *IEEE 30th International Conference on Computer Communications*, Shanghai, China, April 2011, pp. 1593-1601.

[6] "Wireless Universal Serial Bus", http://www.usb.org/developers/wusb/docs

[7] "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems", *IEEE 802.16*, July 2004.

[8] L. Hogie, "Mobile Ad Hoc Networks: Modelling, Simulation and Broadcast-based Applications", *PhD Thesis*, University of Le Havre, April 2007.

[9] S. Kurkowski, T. Camp, M. Colagrosso, "MANET Simulation Studies: The

Incredibles", *Special Issue on Medium Access and Call Admission Control Algorithms for Next Generation Wireless Networks: Mobile Computing and Communications Review*, 2005.

[10] C. Bettstetter, G. Resta, P. Santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad hoc Networks", *IEEE Transactions on Mobile Computing*, 2003, pp. 257-269.

[11] A. Munjal, T. Camp, W. Navidi, "Constructing rigorous MANET simulation scenarios with realistic mobility", *European Wireless Conference*, Lucca, Italy, April 2010, pp. 817-824.

[12] J. Ariyakajorn, "A Comparative Study of Random Way Point and Gauss Markov Mobility Models in the Performance Evaluation of MANET", *International Symposium on Communications and Information Technologies*, September 2006, pp. 894-899.

[13] L. Tie-yuan, C. Liang, G. Tian-long, "Analyzing the Impact of Entity Mobility Models on the Performance of Routing Protocols in the MANET", *International Conference on Genetic and Evolutionary Computing*, October 2009, pp. 56-59.

[14] S. Narayanan, L. Pei, S. Panwar, "On the Advantages of Multi-hop Extensions to the IEEE 802.11 Infrastructure", *IEEE Wireless Communications and Networking Conference*, March 2005, pp. 132-138.

[15] K. Sundaresan, H. Hsieh, R. Sivakumar, "IEEE 802.11 Over Multi-hop Wireless Networks: Problems and New Perspectives", *Ad hoc Networks 2*, 2004, pp. 109-132.

[16] "IETF Mobile Ad hoc Networks (MANET) Working Group", http://www.ietf.org/html.charters/manet-charter.html.

[17] N. Zulkifli, F. Harun, N. Azahar, "Centralized Heart Rate Monitoring Telemetry System Using ZigBee Wireless Sensor Network", *IEEE-EMBS International Conference on Biomedical and Health Informatics,* Hong Kong, China, Jan 2012,

pp. 265-268.

[18] J. Pojda, A. Wolff, M. Sbeiti, C. Wietfeld, "Performance analysis of mesh routing protocols for UAV swarming applications", *8th International Symposium on Wireless Communication Systems*, Aachen, Germany, November 2011, pp. 317-321.

[19] C.E. Perkins, P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance Vector (DSDV) for Mobile Computers", *ACM SIGCOMM Computer Communication Review,* October 1994, pp 234–244.

[20] D. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts", *Workshop on Mobile Computing Systems and Applications*, December 1994, pp. 158-163.

[21] D. Benyamina, A. Hafid, M. Gendreau, "Wireless Mesh Networks Design-A Survey", *IEEE Communications Surveys & Tutorials*, vol 14 (2), 2012, pp. 299-310.

[22] D. Goyal, M. Tripathy, "Routing Protocols in Wireless Sensor Networks: A Survey", *2nd International Conference on Advanced Computing & Communication Technologies*, January 2012, pp. 474-480.

[23] R. Sombrutzki, A. Zubow, M. Kurth, J.-P. Redlich, "Self-Organization in Community Mesh Networks The Berlin RoofNet", *1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks,* Berlin, Germany, September 2006, pp. 1-11.

[24] D. Wu, P. Mohapatra, "QuRiNet: A Wide-area Wireless Mesh Testbed for Research and Experimental Evaluations", *2nd International Conference on Communication Systems and Networks*, Bangalore, India, January 2010, pp. 1- 10.

[25] L. Romdhani, A. Mohamed, T.M. Elfouly, S. Raeisi, "QUMESH: Wireless Mesh Network Deployment and Configuration in Harsh Environment", *IEEE Wireless Communications and Networking Conference*, Shanghai, China, April 2012, pp. 3328-3333.

[26] T. Naumowicz, "Wireless Sensor Network for Habitat Monitoring on Skomer Island", *IEEE Conference on Local Computer Networks*, October 2010, pp. 882-889.

[27] C.S. Murthy, B.S. Manoj, *Ad hoc Wireless Networks Architectures and Protocols*, Prentice Hall, NJ, USA, 2004.

[28] K. Stamatiou, M. Haenggi, "Optimal Spatial Reuse in Poisson Multi-Hop Networks", *IEEE Global Telecommunications Conference,* Miami, USA, December 2010, pp. 1-6.

[29] Y. Fengji, B. Sikdar, "Evaluation of Spatial Reuse in Wireless Multi-hop Networks", *IEEE Vehicular Technology Conference*, September 2004, pp. 4315-4319.

[30] A. Yuste, A. J.Triviño, E. Casilari, F.D. Trujillo, "Adaptive Gateway Discovery for Mobile Ad Hoc Networks Based on the Characterisation of the Link Lifetime", *IET Communications*, vol. 5 (15), October 2011, pp. 2241-2249.

[31] T. Shahin, F. Ghazal, Z. Sadan, "Performance of Modified AODV (waiting AODV) Protocol in Mobile Ad-hoc Networks", *2nd International Conference on Ubiquitous and Future Networks,* Jeju Island, South Korea, June 2010, pp. 160-164.

[32] F. Nordemann, R. Tonjes, "Transparent and Autonomous Store-Carry-Forward Communication in Delay Tolerant Networks (DTNs)", *International Conference on Computing, Networking and Communications*, February 2012, pp. 761-765.

[33] Jorjeta J., David J., "Routing Characteristics of Ad Hoc Networks with Unidirectional Links", *Journal Ad hoc Networks*, May 2006, pp. 303-325.

[34] A. Huda, A. Mehran, W. Tadeusz, "Scalability of MANET Routing Protocols for Heterogeneous and Homogenous Networks", *Journal of Computer and Electrical Engineering*, July 2010, pp. 752-765.

[35] M. Marina, S. Das, "Routing Performance in the Presence of Unidirectional Links

in Multihop Wireless Networks", *International Symposium on Mobile Ad Hoc Networking and Computing,* Lausanne, Switzerland, June 2002.

[36] N. Abramson, "The ALOHA System - Another Alternative for Computer Communications", *Proceedings of Fall Joint Computer Conference*, 1970, pp. 281-285.

[37] L. Kleinrock, S. Lam, "Packet-switching in a Slotted Satellite Channel", *Proceedings of American Federation of Information Processing Societies*, 1973, pp. 703-710.

[38] L. Kleinrock, F. Tobagi, "Packet Switching in Radio Channels: Part I--Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics", *IEEE Transactions on Communications*, 1975, pp. 1400-1416.

[39] K. Xu, M. Gerla, S. Bae, "How Effective is the IEEE 802.11 RTS/CTS Handshake in Ad Hoc Networks", *IEEE Global Telecommunications Conference*, 2002, pp. 72-76.

[40] C. Yu, B. Lee, S. Kalubandi, M. Kim, "Medium Access Control Mechanisms in Mobile Ad Hoc Networks", *Mobile Computing Handbook*, 2004.

[41] J. Weinmiller, H. Woesner, J. Ebert, A. Wolisz, "Analysing and Tuning the Distributed Coordination Function in the IEEE 802.11 DFWMAC Draft Standard", *IEEE/ACM International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*, San Jose, USA, February 1996.

[42] M. Burton, "802.11 Arbitration", White paper, September 2009.

[43] T. Clausen, C. Dearlove, P. Jacquet, "The Optimized Link State Routing Protocol version 2", *Internet Draft <draft-ietf-manet-olsrv2-07>,* July 2008.

[44] D.B. Johnson, Y. Hu, D.A. Maltz, "Dynamic Source Routing in Ad hoc Wireless Networks", *RFC 4728*, February 2007.

[45] C.E. Perkins, E.M. Royer, S. Das, “Ad hoc On-demand Distance Vector (AODV) Routing”, *RFC 3561*, July 2003.

[46] H.K. Lee, Y.W. Kim, J.S. Song, “AOZDV: An Enhanced AODV Protocol based on Zone Routing in MANET”, *International Conference on Wireless Communications, Networking and Mobile*, Shanghai, China, September 2007, pp. 1685-1688.

[47] T. Kathiravelu, S. Sivasuthan, “A Hybrid Reactive Routing Protocol for Mobile Ad-hoc Networks”, *IEEE 6th International Conference on Industrial and Information Systems*, Kandy, Sri Lanka, August 2011, pp. 222-227.

[48] C.S. Murthy, B.S. Manoj, “AdHoc Wireless Networks”, *Pearson*, 2004, pp. 336-338 and 627.

[49] R. Sivakumar, P. Sinha, V. Bharghavan, “CEDAR: A Core-Extraction Distributed Ad hoc Routing Algorithm”, *IEEE Journal on Selected Areas in Communications*, August 1999, pp. 1454–1465.

[50] R. Baumann, S. Heimlicher, M. Strasser, A. Weibel, “A Survey on Routing Metrics”, *TIK Report 262*, 2007.

[51] R. Draves, J. Padhye, B. Zill, “Comparison of Routing Metrics for Static Multi-Hop Wireless Networks”, *Proceedings on Applications, Technologies, Architectures, and Protocols for Computer Communications*, October 2004, pp. 133-144.

[52] K. Wang, M. Wu, L. Weifeng, X. Pengrui, S. Shen, “A Novel Location-Aided Routing Algorithm for MANETs”, *5th International Conference on Information Technology: New Generations*, Las Vegas, USA, April 2008, pp. 1162-1163.

[53] G. Deng, X. Zhang, J. Zhang, F. Liu, “TLRP: Tree-shape Location-based Routing Protocol in Mobile Ad Hoc”, *6th International Conference on ITS Telecommunications Proceedings,* Chengdu, China, June 2006, pp. 646-649.

[54] N. Wang, B. Dong, “Fast failure recovery for reliable multicast-based content

delivery", *International Conference on Network and Service Management*, Niagara Falls, USA, October 2010, pp. 505-510.

[55] J. Moy, "OSPF Version 2", *RFC 2328*, April 1998.

[56] C. Perkins, M. Royer, S. Das, M. Marina, "Performance Comparison of Two On-demand Routing Protocols for Ad hoc Networks", *IEEE Personal Communications*, February 2001, pp. 16-28.

[57] C. Calafate, R. Garcia, P. Manzoni, "Optimizing the Implementation of a MANET Routing Protocol in a Heterogeneous Environment", *IEEE International Symposium on Computers and Communication*, 2003, pp. 217-222.

[58] V. Ramasubramanian, D. Mosse, "BRA: A Bidirectional Routing Abstraction for Asymmetric Mobile Ad Hoc Networks", *IEEE Transactions on Networking*, 2008, pp. 116-129.

[59] H. Higaki, "LBSR: Routing Protocol for MANETs with Unidirectional Links", *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, October 2007, pp. 84.

[60] Z. Wang, J. Lu, J. Tang, "Neighbour Monitoring Mechanism to Solve Unidirectional Link Problem in MANET", *International Conference on Wireless and Mobile Communications*, March 2007, pp. 72.

[61] R. Prakash, "Unidirectional Links Prove Costly in Wireless Ad-hoc Networks", *International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, 1999, pp. 15-22.

[62] C. Kim, E. Talipov, B. Ahn, "A Reverse AODV Routing Protocol in Ad hoc Mobile Networks", *Lecture Notes on Computer Science*, 2006, pp. 522-531.

[63] Y. Ko, S. Lee, J. Lee, "Ad-hoc Routing with Early Unidirectional Detection and Avoidance", *International Symposium on Mobile Ad hoc Networking and Computing*, Tokyo, Japan, May 2004.

[64] S. Terada, T. Miyoshi, H. Morino, M. Ogawa, K. Sezaki, "Ad Hoc Routing Protocol with Flooding Control Using Unidirectional Links", *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, September 2007, pp. 1-5.

[65] L. Barolli, M. Ikeda, F. Xhafa, A. Duresi, "A Testbed for MANETs: Implementation, Experiences and Learned", *IEEE Systems Journal,* vol 4 (2), June 2010, pp. 243-252.

[66] E. Kulla, M. Ikeda, M. Hiyama, L. Barolli, "Evaluation of a MANET Testbed in Indoor Stairs Environment Considering OLSR Protocol", *International Conference on Complex, Intelligent and Software Intensive Systems*, Seoul, Korea, July 2011, pp. 160-167.

[67] W. Wang B. Soong, Y. Chan, "Design and Implementation of Audio Conferencing Testbed based on Wi-Fi MANET", *IEEE Wireless Communications and Networking*, Budapest, Hungary, April 2009, pp. 1-6.

[68] E. Kulla, M. Ikeda, T. Oda, L. Barolli, F. Xhafa, M. Takizawa, "Multimedia Transmissions over a MANET Testbed: Problems and Issues", *6^{th} International Complex, Intelligent and Software Intensive Systems*, Palermo, Italy, July 2012, pp. 141-147.

[69] X. Zhang, W. Wang, L. Huang, "Testbed for Multi-Hop Ad hoc Network in IEEE 802.11 Wireless Environment", *6^{th} International Conference on Wireless Communications Networking and Mobile Computing*, Chengdu, China, September 2010, pp. 1-5.

[70] M. Zhao, Y. Li, W. Wang, "Modeling and Analytical Study of Link Properties in Multihop Wireless Networks", *IEEE Transactions on Communications*, February 2012.

[71] Y. Panlong, Q. Guangcheng, T. Chang, C. Guihai, "A Principle Component Analysis Based Method on Evaluating Wireless Mobile Ad Hoc Network Routing Protocols", 2^{nd} *International Symposium on Intelligent Information Technology*

and Security Informatics, Moscow, Russia, January 2009, pp. 106-109.

[72] H. Mansouri, M. Pakravan, B. Khalaj, "Analytical Modeling and Performance Analysis of Flooding in CSMA-Based Wireless Networks", *IEEE Transactions on Vehicular Technology,* vol. 60 (2), February 2011, pp. 664-679.

[73] M. Rusli, R. Harris, A. Punchihewa, "Markov Chain-based Analytical Model of Opportunistic Routing Protocol for Wireless Sensor Networks", *IEEE Region 10 Conference TENCON*, Fukuoka, Japan, November 2010, pp. 257–262.

[74] Z. Ming, L. Yujin W. Wang, "Modeling and Analytical Study of Link Properties in Multihop Wireless Networks", *IEEE Transactions on Communications*, vol. 60 (2), February 2012, pp. 445-455.

[75] K. Kashiki, A. Yamaguchi, "Experimental and analytical study regarding transmission quality of Wireless LAN system - For implementation of heterogeneous wireless network", *IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications,* Toronto, USA, September 2011, pp. 685-689.

[76] "The CMU Monarch Project's Wireless and Mobility Extensions to NS", August 1998, http://www.monarch.cs.rice.edu/cmu-ns.html

[77] "NS-2 (The Network Simulator 2)", http://www.isi.edu/nsnam/ns/

[78] "GloMoSim (Global Mobile Information Systems Simulation Library)", http://pcl.cs.ucla.edu/projects/glomosim/

[79] "QualNet, Scalable Network Technologies", http://www.scalable-networks.com/

[80] "OPNET (Optimized Network Engineering Tool)", http://www.opnet.com/

[81] "OMNeT++ (Objective Modular Network Testbed in C++) Community Site", http://www.omnetpp.org

[82] M. Halvardsson, P. Lindberg, "Reliable Group Communication in Military Ad hoc Network", *Technical Report*, 2004.

[83] L. Begg, W. Liu, K. Pawlikowski, S. Perera, H. Sirisena, "Survey of Simulators of Next Generation Networks for Studying Service Availability and Resilience", *Technical Report* , University of Canterbury, New Zealand, February 2006.

[84] "OTcl-Object Tcl Extensions", http://bmrc.berkeley.edu/research/cmt/cmtdoc/otcl

[85] T. Wu, "Design of Implicit Routing Protocols for Large Scale Mobile Wireless Sensor Networks", *PhD Thesis*, Univ. of Strathclyde, April 2011.

[86] J. Broch, D.A. Maltz, D.B. Johnson, Y. Hu, J. Jetcheva, "A Performance Comparison of Multi-hop Wireless Ad hoc Network Routing Protocols", *ACM/IEEE International Conference on Mobile Computing and Networking*, Dallas, USA, October 1998, pp. 85–97.

[87] R. Yang, Z.Y. Li, "A Stablity Routing Protocols Base on Reverse AODV," *International Conference on Computer Science and Network Technology*, Harbin, China, December 2011, pp. 2419-2423.

[88] "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks--Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", *IEEE 802.3*, 2005.

[89] I. Glover; P. Grant, *Digital Communications 2/e*, Pearson Education Ltd., 2004.

[90] "Cisco Aironet 350 Client Adapter", http://www.cisco.com/

[91] B. Tuch, "Development of WaveLAN, an ISM Band Wireless LAN", *AT&T Technical Journal*, 1993, pp. 27–33.

[92] W. Kelton, R. Sadowski, D. Sadowski, "Simulation with Arena", *McGraw-Hill*, 2002.

[93] W. D. Kelton, "Simulation Analysis", *Conference on Winter Simulation*, Berlin, Germany, December 1983.

[94] D. Goldsman, G. Tokol, “Output Analysis Procedure for Computer Simulations”, *Winter Simulation Conference*, Orlando, USA, December 2000, pp. 39-45.

[95] M.K. Nakayama, “Statistical Analysis of Simulation Output”, *Winter Simulation Conference*, December 2008, pp. 62–72.

[96] R. Jain, “The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modelling”, *Wiley-Interscience*, April 1991.

[97] R. Sargent, “Verification and Validation of Simulation Models”, *Proceedings of the Winter Simulation Conference*, Phoenix, USA, December 2011, pp. 183-198.

[98] S. Nesargi, R. Prakash, “A Tunneling Approach to Routing with Unidirectional Links in Mobile Ad-hoc Networks”, *Conference on Computer Communications and Networks*, 2000, pp. 522-527.

[99] G.Wang, D.Turgut, “A MAC Layer Protocol for Wireless Networks with Asymmetric Links”, *Ad Hoc Networks*, 2008, pp. 424-440.

[100] K. Khan, R. Zaman, A. Reddy, “Performance Comparison of On-Demand and Table Driven Ad-hoc Routing Protocols Using NCTUns”, *Conference on Computer Modelling and Simulation*, April 2008, pp. 336-341.

[101] M. Morshed, M. Rahman, “Performance Evaluation of DSDV and AODV Routing Protocols in Mobile Ad-hoc Networks”, *International Conference on National Information Systems Security*, May 2010, pp. 399-403.

[102] S. Mank,R. Karnapke, J. Nolte, "MAC Protocols for Wireless Sensor Networks: Tackling the Problem of Unidirectional Links", *International Journal on Advances in Networks and Services*, vol. 2(4), 2009.

[103] R. Prakash, “A Routing Algorithm for Wireless Ad Hoc Networks with Unidirectional Links,” *ACM/Kluwer Wireless Networks*, 2001.

[104] M. Gerla, L. Kleinrock, Y. Afek, “A Distributed Routing Algorithm for

Unidirectional Networks", *IEEE Global Communication Conference, Exhibition and Industry Forum*, 1983.

[105] T. Le, P. Sinha, D. Xuan, "Turning Heterogeneity Into an Advantage in Wireless Ad-hoc Network Routing," *Ad Hoc Networks*, January 2010.

[106] D. Ganesan, B. Krishnamachari, A. Woo, D. Culler, D. Estrin, S. Wicker, "An Empirical Study of Epidemic Algorithms in Large Scale Multihop Wireless Networks", *UCLA Computer Science Technical Report UCLA/CSD-TR 02-0013*.

[107] V. Ramasubramaniam, D Mosse, "Statistical Analysis of Connectivity in Unidirectional Ad Hoc Networks", *International Conference on Parallel Processings Workshops*, Vancouver, Canada, August 2002.

[108] C.A. Hossain, M.A. Hossain, M. Tarique, "Effects of Shadowing on the Performances of Mobile Ad Hoc Networks", *International Conference on Computational Intelligence and Communication Networks*, Gwalior, India, October 2011, pp. 319-322.

[109] G. Marco, M. Longo, F. Postiglione, "Connectivity of Ad Hoc Networks with Link Asymmetries Induced by Shadowing", *IEEE Communications Letters*, June 2007.

[110] P. Stuedi, O. Chinellato, G. Alonso, "Connectivity in the Presence of Shadowing in 802.11 Ad Hoc Networks", *IEEE Wireless Communications and Networking Conference*, 2005, pp. 2225-2230.

[111] J. Lloret, "A Fast Design Model for Indoor Radio Coverage in the 2.4 GHz Wireless LAN", *International Symposium on Wireless Communications Systems*, Mauritius, 2004.

[112] L. C. Liechty, E. Reifsnider, G. Durgin, "Developing the Best 2.4 GHz Propagation Model from Active Network Measurements", *IEEE Vehicular Conference*, Baltimore, USA, 2007, pp. 894-896.

[113] S. Yoon, "A Radio Propagation Model for Wireless Underground Sensor Networks", *IEEE Global Telecommunications Conference*, December 2011, pp. 1-

5.

[114] R. Souza, R. Lins, "A New Propagation Model for 2.4 GHz Wireless LAN", *Proceedings of Asia Pacific Conference on Communications*, October 2008.

[115] H. Sugimoto, T. Sato, "Experimental Results of 2.45, 3.5, 5, and 10GHz Radio Propagation Characteristics", *IEEE Vehicular Technology Conference*, 2007, pp. 339-343.

[116] Lee, C. Y. William. "Mobile Communications Engineering", *NY: Mc-Graw-Hill*, 1982, pp. 564.

[117] L.F. Zang, G.B. Row, "Improved Modelling for Mobile Ad-hoc Networks", *Electronics Letters*, October 2007.

[118] A. Alshanyour, U. Baroudi, "Random and Realistic Mobility Models Impact on the Performance of Bypass-AODV Routing Protocol", *IEEE/IFIP Wireless Days*, Dubai, November 2008, pp. 1-5.

[119] J. Ariyakhajorn, P. Wannawilai, C. Sathitwiriyawong, "A Comparative Study of Random Waypoint and Gauss-Markov Mobility Models in the Performance Evaluation of MANET", *International Symposium on Communications and Information Technologies*, Bangkok, Thailand, September 2006, pp. 894-899.

[120] I. Stepanov, K. Rothermel, "On the Impact of a More Realistic Physical Layer on MANET Simulations Results", *Ad Hoc Networks*, January 2008, pp. 61-78.

[121] J. Yoon, M. Liu, B. Noble, "Random Waypoint Considered Harmful", IEEE *Conference on Computer Communications*, April 2003, pp. 1312-1321.

[122] J. Jetcheva, Y. Hu, S. PalChaudhuri, A. Saha, D. Johnson, "CRAWDAD Data Set Rice Ad hoc City (v. 2003-09-11)", http://crawdad.cs.dartmouth.edu/rice/ad hoc city, 2003.

[123] "UMass-Trace-Repository", http://traces.cs.umass.edu/index.php/Network/Network

[124] M. Kim, D. Kotz, S. Kim, "Extracting a Mobility Model from Real User Traces", *International Conference of Computer Communications*, 2006, pp. 1-13.

[125] L. Ben, H. Zygmunt, "Predictive Distance-based Mobility Management for PCS Networks", *IEEE Conference on Computer Communications,* New York, USA, March 1999, pp. 1377-1384.

[126] H. Xiaoyan, G. Mario, P. Guangyu, C. Chuan, "A Group Mobility Model for Ad Hoc Wireless Networks", *International Workshop on Modelling and Simulation of Wireless and Mobile System*, New York, USA, 1999.

[127] "Universal Mobile Telecommunications System (UMTS)–Selection Procedures for the Choice of Radio Transmission Technologies of the UMTS", *European Telecommunications Standard* Institute, 1998.

[128] M. Boban, T. Vinhoza, "Modelling and Simulation of Vehicular Networks: Towards Realistic and Efficient Models", *Mobile Ad-Hoc Networks: Applications*, InTech Publishers, 2011.

[129] C. Bettsetter, "On the Minimum Node Degree and Connectivity of a Wireless Multihop Network", *International Symposium on Mobile Ad hoc Networking and Computing*, Lausanne, Switzerland, June 2002, pp. 80 – 91.

[130] Q. Ling, Z. Thian, "Minimum Node Degree and k-Connectivity of a Wireless Multihop Network in Bounded Area", *IEEE Global Telecommunications Conference*, November 2007, pp. 1296-1301.

[131] "BonnMotion: A mobility scenario generation and analysis tool", http://net.cs.uni-bonn.de/

[132] N. Aschenbruck, "Evaluation of Wireless Multi-hop Networks in Tactical Scenarios Using BonnMotion", *European Wireless Conference*, April 2010, pp. 810-816.

[133] C.P. Agrawal, M.K. Tiwari, O.P. Vyas, "Evaluation of AODV Protocol for Varying Mobility Models of MANET for Ubiquitous Computing", *International*

Conference on Convergence and Hybrid Information Technology, November 2008, pp. 769-774.

[134] A. Pal, J.P. Singh, P. Dutta, P. Basu, D. Basu, “Study on The Effect of Traffic Patterns on Routing protocols in Ad-hoc Network Following RPG Mobility Model”, *International Conference on Signal Processing, Communication, Computing, and Networking Technologies*, July 2011, pp. 233-237.

[135] E. Zola, A. F. Barcelo-Arroyo, “Impact of Mobility Models on the Cell Residence Time in WLAN Networks”, *IEEE Sarnoff Symposium*, March 30 – April 1 2009, pp. 1-5.

[136] D. Faria, “Modeling Signal Attenuation in IEEE 802.11 Wireless LANs – Vol 1”, *Technical Report TRKP06-0118*, Kiwi Project, July 2005.

[137] W. Xu, Y. Zhang, W. Liang, “Overhead Analysis of Query Localization Optimization and Routing”, *International Conference on Ubiquitous Information Management and Communication*, Seoul, Korean, February 2011, pp. 21- 23.

[138] K. Chin, “The Behavior of MANET Routing Protocols in Realistic Environments”, *Asia-Pacific Conference on Communications*, October 2005.

[139] R. Draves, J. Padhye, B. Zill, “Comparison of Routing Metrics for Static Multi-Hop Wireless Networks”, *Special Interest Group on Data Communication*, Portland, USA, August 30 – Sept. 3, 2004.

[140] G. Judd, X. Wang, P. Steenkiste, "Efficient Channel-aware Rate Adaptation in Dynamic Environments," *International Conference on Mobile Systems, Applications, and Services*, June 2008.

[141] C. Tai, “Complementary Reciprocity Theorems in Electromagnetic Theory”, *IEEE Transactions on Antennas and Propagation*, 1992, pp. 675–681.

[142] N. Ahmed, S. Kanhere, S. Jha, “Probabilistic Coverage in Wireless Sensor Networks”, *IEEE Conference on Local Computer Networks*, 2005.

[143] Y. Yang, W. Han, “A QoS Routing Protocol For Mobile Ad-hoc Networked Control Systems,” *International Conference on Networks Security, Wireless Communications and Trusted Computing*, April 2010, pp. 89-92.

[144] R. Chang, S. Leu, “Long-lived Path Routing with Received Signal Strength for Ad hoc Network,” *International Symposium on Wireless Pervasive Computing*, January 2006.

[145] S.J. Lee, E.M. Belding-Royer, C.E. Perkins, “Scalability Study of the Ad hoc On-demand Distance Vector Routing Protocol”, *International Journal of Network Management*, 2003, pp. 97–114.

Appendix-A

This section explains the computational resources needed for the simulation experiments in this thesis. Indeed the time computed for each simulation work varies with different hardware architectures and the configuration parameters. Nonetheless, an approximate timings is presented, as shown in Table A.1, based on a machine equipped with 8-core "Intel® Xeon™ CPU 2.40GHz processor. As a comparison, the timings are compared against a slower machine, i.e., Intel® Core™2 Duo CPU 2.33GHz, which is used in the event that all cores on the former machine are fully utilised (Table A.2). The results presented in Table A.1 and Table A.2 shows the approximate total time taken to compute the experiments in section 6.4.4 and section 6.5.1.

Table A.1: Computation resources for Intel® Xeon™ CPU 2.40GHz

Description	Simulation section 6.4.4	Simulation section 6.5.1
Simulation time for each run of routing protocol	8 minutes	1 minute (with 18 partitioning)
Post processing run for each protocol	2 minutes	0.5 minute
Number of repetition for each point on the graph	25	25
Simulation time for each run of routing protocol	(8 + 2) x 25 = 250 minutes	(1+0.5) x 25 = 37.5 minutes
Number of points for each graph	6	251
Simulation time for each graph of routing protocol	6 x 250 minutes = 1500 minutes	251 x 37.5 minutes = 9412.5 minutes
Number of routing protocol	3	3
Total simulation time	3 x 1500 minutes = 3.125 days	3 x 9412.5 minutes = 19.6 days

Table A.2: Computation resources for Intel® Core™2 Duo CPU 2.33GHz

Description	Simulation section 6.4.4	Simulation section 6.5.1
Simulation time for each run of routing protocol	12 minutes	1.5 minute (with 18 partitioning)
Post processing run for each protocol	4 minutes	1 minute
Number of repetition for each point on the graph	25	25
Simulation time for each run of routing protocol	(12 + 4) x 25 = 400 minutes	(1.5+1) x 25 = 62.5 minutes
Number of points for each graph	6	251
Simulation time for each graph of routing protocol	6 x 400 minutes = 2400 minutes	251 x 62.5 minutes =15687.5 minutes
Number of routing protocol	3	3
Total simulation time	3 x 2400 minutes = 5 days	3 x 15687.5 minutes = 32.7 days