“Classification and Comparative Study of Routing Techniques in Adhoc Wireless Networks”

Dissertation

Submitted to the faculty of

Applied Sciences and technology

University Of Kashmir.

For the Award of the degree of

Masters of Philosophy

In

Computer Science

By

BILAL MAQBOOL BEIGH

Under Supervision of

Prof. M . A . PEER

Co-Supervisor

Dr. Mehraj-u-Din Dar

Post Graduate Department of Computer Science,

Faculty of Applied Sciences and Technology

University of Kashmir

2011

"In the name of Allah, the most beneficial and merciful"

Dedicated to

My Mom and Dad

University Of Kashmir

Hazratbal Srinagar Kashmir 190006

Certificate

This is to certify that the work embodied in this dissertation entitled "Classification and Comparative Study of Routing Techniques in Adhoc Wireless Networks" is original work carried out by Mr.BILAL MAQBOOL BEIGH, Department of Computer Science, University of Kashmir, Srinagar under my supervision and is suitable for the submission for the award of the Masters of Philosophy in computer Science.

This Work has not previously been submitted for award of any degree or fellowship.

Co-Supervisor	Supervisor
(Dr. Mehraj-u-din Dar)	(Prof. M. A. Peer)
Director IT&SS	Chairman J&K BOPEE

Acknowledgment

This owes a great many thanks to a great many people who helped and supported me during the writing of this dissertation. Apart from the efforts of me, the success of this dissertation depends largely on the encouragement and guidelines of many others. I take this opportunity to express my gratitude to the people who have been directly or indirectly involved in the successful completion of this dissertation.

My deepest thanks to my guide and my mentor **Prof. Mushtaq Ahmad Peer**, for guiding me through whole M.Phill course and for correcting various documents of mine with attention and care. He has taken pain to go through the dissertation and make necessary correction as and when needed. I would like to thanks my Co-supervisor **Dr. Mehraj-u-din Dar** for guiding me during the whole course.

I express my thanks to **Dr. S. M. K. Quadri**, Head Department of Computer Sciences University of Kashmir, for his support and valuable advices.

My deep sense of gratitude to **Mr. Mohmmad Shafi, Mr. Mohmmad Shafique, Mr. Sajad Ahmad Khan , Dr. Rana Hashmi, Mr. Manzoor Ahmad, Mr. Mohmmad Younis** for support and guidance. Thanks and appreciation to the helpful people at University of Kashmir for their support.

I would also like to thank my Institution and whole faculty members without whose advices this work would have been a distant reality. I also extend my heartfelt thanks to my family, friends(**Sameer ,Manzoor, Bilal, Wasim ,Irsahd, Suhail, Umar and Khalid**) and all well wishers.

(BILAL MAQBOOL BEIGH)

Abbreviation Used

AP	Access Point
SSID	service set identifier.
WLAN	Wireless Local Area Network
BS	Base Station
dB	Decibel
PAN	Personal Area Network
DSDV	Destination Sequence Distance vector.
WRP	Wireless Routing Protocols.
CGSR	Cluster head Gateway switch Routing
STAR	Source-Tree Adaptive Routing
OLSR	Optimized Link State Routing
FSR	Fisheye State Routing
MRL	Message Retransmission List
AODV	Ad hoc On Demand Distance Vector
DSR	Dynamic Source routing protocol
TORA	Temporally ordered routing algorithm
ABR	Associativity Based routing
SSR	Signal Stability-Based Adaptive Routing
RReq	Repeat request
RRep	Request Reply
RRC	Route reconstruction
LSP	Link State Packet
HSR	Hierarchical State Routing
CBRP	Cluster Based Routing Protocol
LAR	Location aided routing
DREAM	Distance routing effect algorithm for mobility
TCL	Tool Command Language

List of Figures

List of Tables

Preface

Chapter 1: Introduction

This chapter provides an introduction about the network in general and particularly the Adhoc networks. In this chapter, the fundamentals of the Adhoc network i.e. the desirable properties of the Adhoc networks, advantages and disadvantages of Adhoc networks, Characteristics of radio transmission and Adhoc networks and the propagation mechanisms have been discussed.

Chapter 2: Classification and theoretical study of Routing Protocols

This chapter provides the classification of the routing protocols, by choosing different parameters. During classification, brief overview of routing protocols has been undertaken. The protocol has been discussed on some parameters according to category wise. The categories are as Pro-active Based routing, Re-active Based Routing ,Hybrid Based Routing ,Hierarchical Based Routing, Geographical Based Routing, Power Based Routing.

Chapter 3: Propagation models

This chapter provides an overview of the propagation models for the wireless Adhoc networks. The Propagation model that have discussed in this chapter are fading models and non-fading models. In fading models, the Rician model, Shadowing model and the Rayleigh Model and in non- fading model i discussed the free space model and the Two-Ray Ground model have been discussed.

Chapter 4: Network Simulator 2(NS2) and its implications

This chapter provides an overview of the network simulator. This chapter provides the idea of defining basic installation steps of network simulator .This also provide an example, how to define Ns/Nam trace and Traffic and movement models for the network simulator NS2.

Chapter 5: Performance / comparative study of Routing Protocols using Simulation.

This chapter provides us the comparative study of various types (Categories) of routing protocols (as per defined in the classification chapter). This chapter provide the performance analysis of the routing protocols according to the category wise, thus suggests the user/ researchers which among the group of protocols is best suited for which conditions.

Chapter 6: Conclusion and Future Scope

This chapter provides us the main conclusion of the thesis. This is also not possible to develop / enhancement / security of the routing protocol without analyzing the performance of the existing routing protocols. Thus provides us the idea what should be in best suited protocol and what not.

Chapter 7: Publications.

This chapter shows the list of publications, which have been published during the course of M.Phill.

Abstract

Wireless systems have been in use since 1980s. We have seen their evolutions to first, second and third generation's wireless systems. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other.

The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the Infrastructured wireless systems.

Recent advancements such as Bluetooth introduced a new type of wireless systems known as ad-hoc networks. Ad-hoc networks or "short live" networks operate in the absence of fixed infrastructure. They offer quick and easy network deployment in situations where it is not possible otherwise. Ad-hoc is a Latin word, which means "for this or for this only." Mobile ad-hoc network is an autonomous system of mobile nodes connected by wireless links; each node operates as an end system and a router for all other nodes in the network.

Nodes in ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network.
A mobile ad-hoc network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective. The popular IEEE 802.11 "WI-FI" protocol is capable of providing ad-hoc network facilities at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Ad-hoc networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet.

An ad-hoc network has certain characteristics, which imposes new demands on the routing protocol. The most important characteristic is the dynamic topology, which is a consequence of node mobility. Nodes can change position quite frequently; the nodes in an ad-hoc network can consist of laptops and personal digital assistants and are often very limited in resources such as CPU power, storage capacity, battery power and bandwidth. This means that the routing protocol should try to minimize control traffic, such as periodic update messages. The Internet Engineering Task Force currently has a working group named Mobile

Ad-hoc Networks that is working on routing specifications for ad-hoc networks. This M.Phill thesis evaluates some of the protocols put forth by the working group. This evaluation is done by means of simulation using Network simulator 2 from Berkeley.

This work aims at classification of the existing routing protocols of adhoc wireless networks using some definite parameters. After classification of routing protocols of adhoc wireless network, their comparative study was undertaken in order to yield category wise distribution. Furthermore performance evaluation of these protocols was carried out by employing different parameters like fading models, mobility models, traffic patterns etc using the network simulator NS-2

Hence I explore and evaluate different methods for validation of ad hoc routing protocols which are used to set up forwarding paths in spontaneous networks of mobile/Adhoc devices to accomplish the above mentioned comparative study and classification.

Keywords: Adhoc networks, Routing, Simulation, NS-2, Protocols, Classification, Comparison, Performance, Mobile, Networks.

Contents

Chapter 1

Introduction of Networks

Chapter 1

Introduction of Networks

A computer network is an interconnected collection of independent computers, which aids communication in numerous ways. Apart from providing a good communication medium, sharing of availability resources, improved reliability of service and cost effectiveness are some of the advantages of computer networking,

In general computer networks can be categorised into two types.

1. Wired networks
2. Wireless Networks

1.1 Wired networks

These networks are generally connected with the help of wires and cables. Generally the cables being used in this type of networks are CAT5 or CAT6 cables. The connection is usually established with the help of physical devices like Switches and Hubs in between to increase the strength of the connection. These networks are usually more efficient, less expensive and much faster than wireless networks. Once the connection is set there is a very little chance of getting disconnected.

Advantages of Wired networks

1. A wired network offer connection speeds of 100Mbps to 1000Mbps

2. Physical, fixed wired connections are not prone to interference and fluctuations in available bandwidth, which can affect some wireless networking connections.

Disadvantages over wireless networks

1. Expensive to maintain the network due to many cables between computer systems and even if a failure in the cables occur then it will be very hard to replace that particular cable as it involved more and more costs.
2. When using a laptop which is required to be connected to the network, a wired network will limit the logical reason of purchasing a laptop in the first place.

1.2 Wireless Networks

Wireless networks use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The most admiring fact in these networks is that it eliminates the need for laying out expensive cables and maintenance costs.

Advantages of Wireless Networks

1. Mobile users are provided with access to real-time information even when they are away from their home or office.
2. Setting up a wireless system is easy and fast and it eliminates the need for pulling out the cables through walls and ceilings.
3. Network can be extended to places which cannot be wired.
4. Wireless networks offer more flexibility and adapt easily to changes in the configuration of the network.

Disadvantages of Wireless Networks

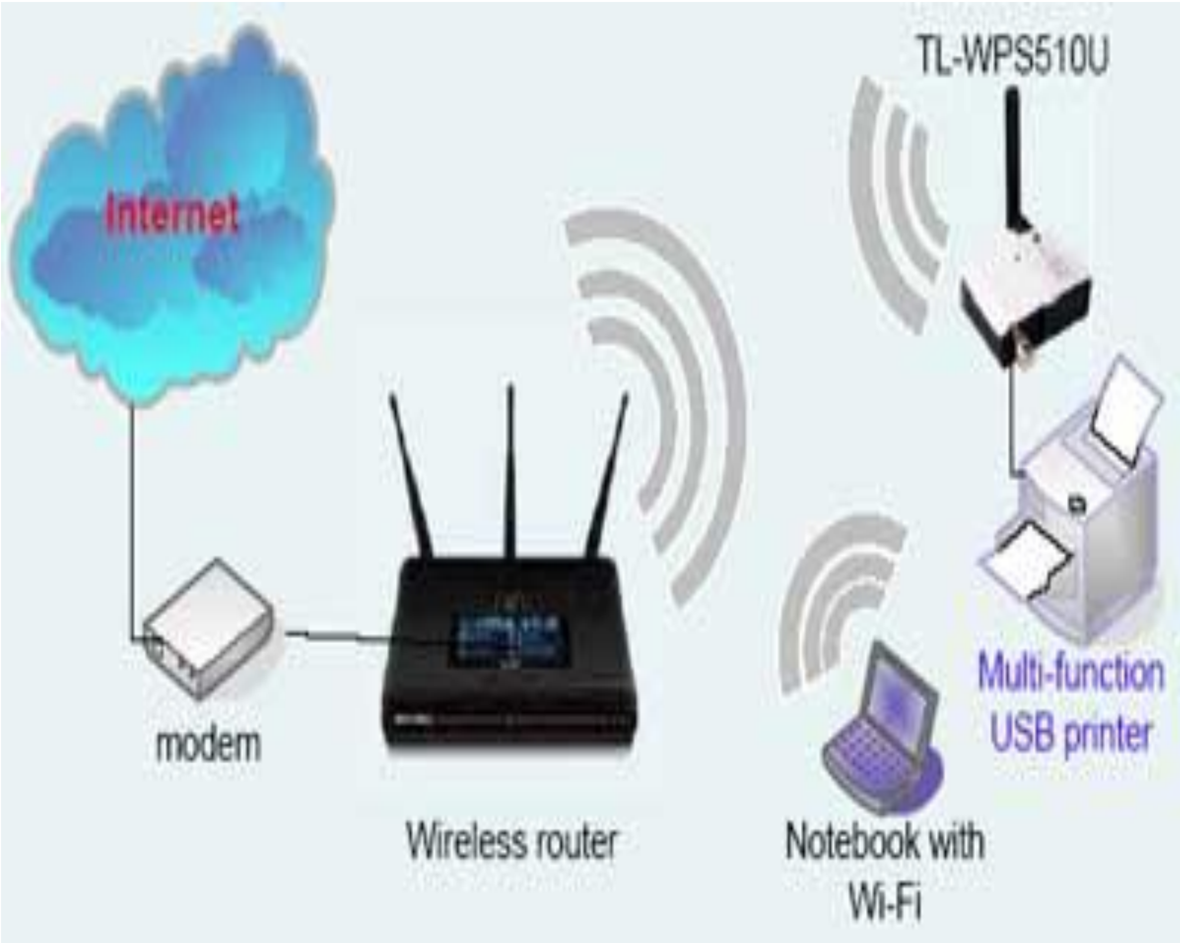
1. Interference due to weather, other radio frequency devices, or obstructions like walls.
2. The total Throughput is affected when multiple connections exists.

Further there are two types of wireless networks.

a) Infrastructure wireless network
b) Infrastructure- less wireless network also known as wireless Adhoc networks.

1.1.3 Infrastructure Wireless networks:

Infrastructure mode wireless networking bridges (joins) a wireless network to a wired Ethernet network. Infrastructure mode wireless also supports central connection points for WLAN clients. A wireless access point (AP) is required for infrastructure mode wireless networking. To join the WLAN, the AP and all wireless clients must be configured to use the same service set identifier (SSID). The AP is then cabled to the wired network to allow wireless clients access. For example, Internet connections or printers. Additional APs can be added to the WLAN to increase the reach of the infrastructure and support any number of wireless clients. Compared to the alternative, ad-hoc wireless networks, infrastructure mode networks offer the advantage of scalability, centralized security management and improved reach. The disadvantage of infrastructure wireless networks is simply the additional cost to purchase AP hardware. Note that home wireless routers have a built-in AP to support infrastructure mode.



Infrastructed wireless networks

1.1.4 Infrastructured-less Wireless/Adhoc networks

A wireless ad-hoc network is a collection of mobile/semi-mobile nodes with no pre-established infrastructure, forming a temporary network. Each of the nodes has a wireless interface and communicates with each other over either radio or infrared. Laptop computers and personal digital assistants that communicate directly with each other are some examples of nodes in an ad-hoc network. Nodes in the ad- hoc network are often mobile, but can also consist of stationary nodes, such as access points to the Internet. Semi mobile nodes can be used to deploy relay points in areas where relay points might be needed temporarily

Figure 2 shows a simple ad-hoc network with three nodes. The outermost nodes are not within transmitter range of each other. However the middle node can be used to forward packets between the outermost nodes. The middle node is acting as a router and the three nodes have formed an ad-hoc network.

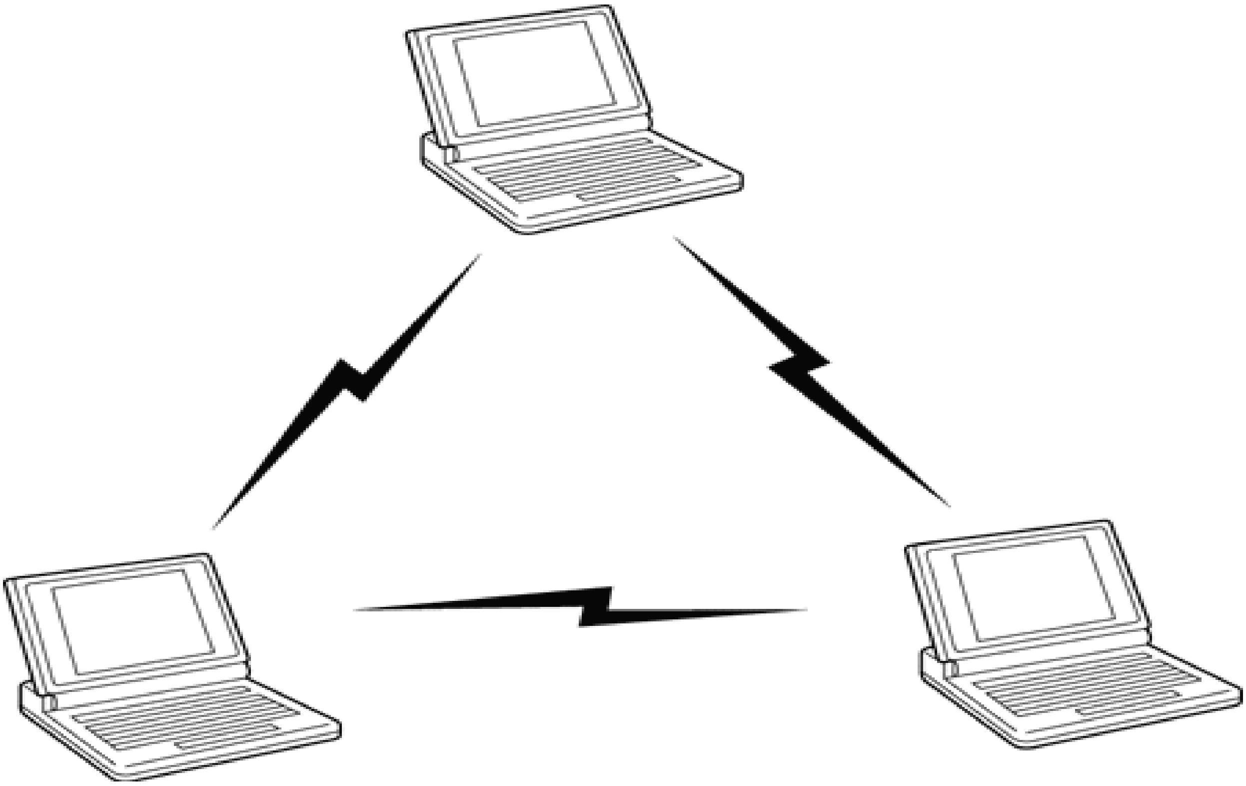


Figure 2 . Adhoc Wireless networks

1.1.5 Advantages of Adhoc networks

The principal advantages of an ad hoc network include the following:

1. Independence from central network administration
2. Self-configuring, nodes are also routers
3. Self-healing through continuous re-configuration
4. Scalable—accommodates the addition of more nodes
5. Flexible—similar to being able to access the Internet from many different locations

1.1.6 Dis-advantages of Adhoc networks

While ad hoc networks are typically used where they have the greatest emphasis on its advantages, there are some limitations:

1. Each node must have full performance
2. Throughput is affected by system loading
3. Reliability requires a sufficient number of available nodes. Sparse networks can have Problems
4. Large networks can have excessive latency (time delay), which affects some applications, some of these limitations also apply to conventional hub-and-spoke

based networks, or cannot be addressed by alternate configurations. For example, all networks are affected by system loading, and networks with few nodes are difficult to justify in hard-wired solutions.

1.2 Characteristics of Adhoc networks

Ad-hoc networks are often characterized by a dynamic topology due to the fact that nodes change their physical location by moving around. This favours routing protocols that dynamically discover routes over conventional routing algorithms like distant vector and link state [1] etc. Another characteristic is that a host/node has very limited CPU power, storage capacity, battery power and bandwidth, also referred to as a “thin client”. This means that the power usage must be limited thus leading to a limited transmitter range. The access media, the radio environment, also has special characteristics that must be considered when designing protocols for ad-hoc networks. One example of this may be unidirectional links. These links arise when for example two nodes have different strength on their transmitters, allowing only one of the hosts to hear the other, but can also arise from disturbances from the surroundings. Multihop in a radio environment may result in an overall transmit capacity gain and power gain, due to the squared relation between coverage and required output power. By using multihop, nodes can transmit the packets with a much lower output power.

1.3 Radio Propagation Mechanisms

Heinrich Rudolf Hertz observed in 1886 [96] the transmission of electromagnetic waves and, hence, realized the long-debated Maxwell’s predictions of wave propagation. The first milestone on the road to wireless communications, however, was realized by Guglielmo Marconi who conducted his famous experiments from 1894 to 1901. Marconi demonstrated in 1901 that the radio wave could provide continuous contact with ships sailing the English Channel [97]. After that, two-way radio communications and broadcasting systems were developed in the 1930s and 1940s. In the 1960s and 1970s, the cellular concept was developed in Bell Laboratories, Holmdel, NJ [98].

The selection of propagation model plays a very important role in wireless communication systems, thus before implementing designs and confirming planning of wireless communication systems, accurate propagation characteristics of the environment should be known. Propagation prediction usually provides two types of parameters corresponding to the large-scale path loss and small-scale fading statistics. The path-loss information is vital for the determination of coverage of a base-station (BS) placement and in optimizing it. The small-scale parameters usually provide statistical information on local field variations and this, in turn, leads to the calculation of important parameters that help improve receiver (Rx) designs and combat the multipath fading. Without propagation predictions, these parameter estimations can only be obtained by field measurements which are time consuming and expensive. The following subsections provide a brief description of propagation models and challenges facing the development of accurate and sufficiently general propagation prediction models. The mechanism which radio wave generally experiences are as under [8]:

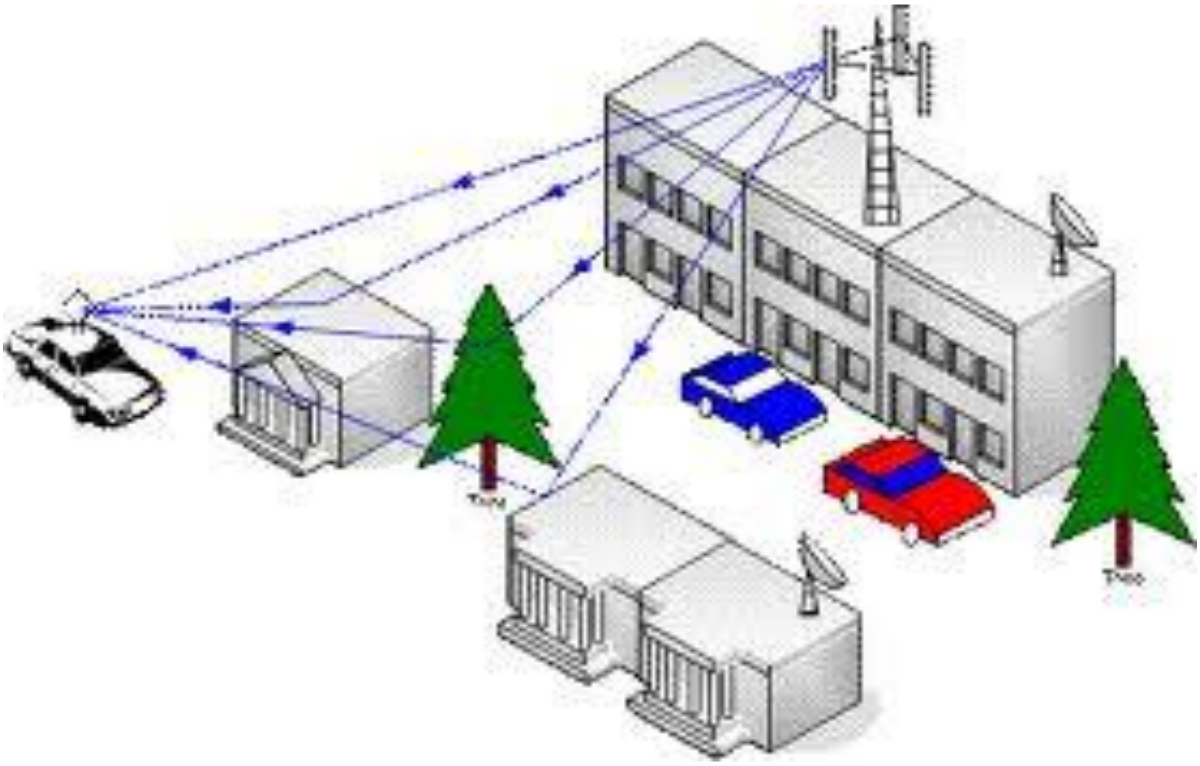


Figure 3. Radio propagation mechanism

1.3.1 Reflection:

When the propagating radio wave hits an object which is very large compared to its wavelength (such as the surface of earth, or tall building), the wave gets reflected by that object. Reflection causes a phase shift of 180 degree between incident and the reflected rays.

1.3.2 Diffraction:

This propagation effect is undergone by a wave when it hits an impenetrable object. The wave bends at the degree of the object, thereby propagating in different directions. This phenomenon is termed as diffraction. The dimensions of the object causing diffraction are comparable to the wavelength of the wave being diffracted. The bending causes by the wave to reach places behind the object which generally cannot be reached by the line of sight transmission. The amount of diffraction is frequency-dependent, with the lower frequency wave diffraction is more.

1.3.3 Scattering:

Is the mechanism in which the direction of the wave is changed when wave encounters propagation medium discontinuous smaller than the wave length, which results in a random change in the energy distribution.

1.3.4 Reflection:

Refraction is redirection of a wave front passing through a medium having a refractive index that is a continuous function of position or through a boundary between two dissimilar media.

1.3.5 Absorption:

Absorption is the conversion of the transmitted electromagnetic energy into another form, usually thermal. The conversion takes place as a result of interaction between the incident energy and the material medium.

1.4 Characteristics of Wireless channels:

The wireless channel (transmission medium) is susceptible to a varity of transmission impediments such as path loss, interference and blockage. These factors restrict the range, data rate and the reliability of the wireless transmission. The extent to which these factors affect the transmission depends upon the environment conditions and the mobility of the transmitter and reviver. The various characteristics of wireless channel are:

1. Path Loss
2. Fading
3. Interference
4. Doppler Shift.
5. Transmission rate constraints.

1.4.1 Path Loss:

Path loss can be expressed as the ratio of the power of transmitted signal to the power of sine signal received by the receiver, on a given path. It is a function of the propagation distance. Path loss is dependent on a number of factors such as radio frequency and the nature of the terrain. The path loss is usually expressed in decibels (dB) as follows:

$$L_{db} = 10 \ \log_{10} \frac{Pr}{Pt}$$

where *Pt* and *Pr* are the transmitted and received signal power, respectively.

1.4.2 Fading:

Fading refers to the fluctuations in signal strength when received at the receiver. Fading can be classified onto two types: fast fading / small-scale fading and slow fading / large-scale fading.

Fast fading refers to the rapid fluctuations in the amplitude, phase or multipath delays of the received signal, due to the interference between multiple versions (copies) of the same transmitted signal arriving at the receiver at slightly different times. The time between the reception of the first version of the signal and the last echoed signal is called delay spread. The multipath propagation of the transmitted signal, which causes fast fading, is because of the three propagation mechanisms described previously, namely reflection, diffraction and scattering. The multipath signal paths may sometimes add constructively or sometimes destructively at the receiver, causing a variation in the power level of the received signal [21]. Slow fading occurs when objects that partially absorb the transmission lie between the transmitter and the receiver. Slow fading is so called because the duration of the fading may last for multiple seconds or minutes. Slow fading may occur when the receiver is inside a building and the radio wave must pass through the walls of a building. The obstruction objects cause a random variation in the received signal power. Slow fading may cause the received power to vary, though the distance between the transmitter and the receiver remains same.

1.4.3 Interference:

Wireless transmissions have to counter interference from a wide varity of sources. Two main forms of interference are adjacent channel interference and co channel interference. In the adjacent channel interference case, signals in nearby frequencies have components outside their allocated range, and these components may interfere with ongoing transmission in the adjacent frequencies. It can be avoided by carefully introducing guard bands between the allocated frequency ranges. Co-channel interference, sometimes also referred to as narrow band interference, is due to other nearby system (say AM/FM broadcast) using the same transmission frequency.

Inter-symbol interference is another type of interference, where distortion in the received signal is caused by the temporal spreading and the consequent overlapping of individual pluses in the signal. When this temporal spreading of individual pluses (delay spread) goes above a certain limit (symbol detection time) the receiver becomes unable to reliably distinguish between changes of the state in the signal, that is, the bit pattern interpreted by the receiver is not same as that by the sender. Adaptive equalization is a commonly used technique for combating inter-symbol interference. Adaptive equalization involves mechanisms for gathering the dispersed symbol energy into its original time interval. Complex digital processing algorithm is used in the equalization process. The main principle behind adaptive equalization is the estimate of the channel pulse response to periodically transmitted well-known bit pattern, known as training sequence. This would enable a receiver to determine the time dispersed of the channel and compensate accordingly.

1.4.4 Doppler Shift:

The Doppler shift is defined as the change / shift in the frequency of the received signal when the transmitted and the received are mobile with respect to each other. If they are moving towards each other, then the frequency of the received signal will be higher than that of the transmitted signal, and if they are moving away from each other, the frequency of the signal at the receiver will be lower than that at the transmitter. The Doppler shift

$$f_d = \frac{\nu}{\lambda}$$

Where ν is the relative velocity between the transmitter and the receiver, and λ is the wavelength of the signal.

1.4.5 Transmission Rate Constraints:

Two important constraints that determines the maximum rate of data transmission on a channel are Nyquist’s theorem and Shannon’s theorem. The two theorems are presented below.

Nyquist’s Theorem:

The signalling speed of a transmitted signal denotes the number of times per second the signal changes its value / voltage. The number of changes per second is measured in terms of baud. The baud rate is not same as the bit rate /date rate of the signal since value may be used to convey multiple bits. The nyquist theorem gives the maximum data rate possible on a channel. If B is the bandwidth of the channel (in Hz) and L is the number of discrete signal levels/voltage values used, then the maximum channel capacity C according to Nyquist theorem.

$$C = 2 \text{ x } B \text{ x } \log_2 2\, L$$

The above theorem is valid for noiseless channels only

Shannon’s Theorem:

Noise level in the channel is represented by the SNR. It is the ratio of signal power(S) to noise power (N), specified in decibels, that is, SNR = 10 $log_{10}(S/N)$. One of the most important contributions of Shannon was his theorem on the maximum data rate possible on a noisy channel. According to Shannon’s theorem, the maximum data rate C is given by

$$C = B \text{ x } \log_2(1 + (S/N)) \quad \text{bits/sec}$$

Where B is the bandwidth of the channel(in Hz).

1.5 Applications of Adhoc networks

There are a number of application areas for ad-hoc networks. The cover theme articles in this issue will provide insights into a few selected application areas and research activities. The following overview should give you an idea of the wide range of application areas:

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

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

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

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

5. Military battlefield. Military equipment now routinely contains some sort of computer equipment. Ad hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarters. The basic techniques of ad hoc network came from this field.

6. Commercial sector. Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deploymentof a communication network is needed. Information is relayed from one rescue team member to another over a small handheld. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

7. Local level. Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.


Headquarter

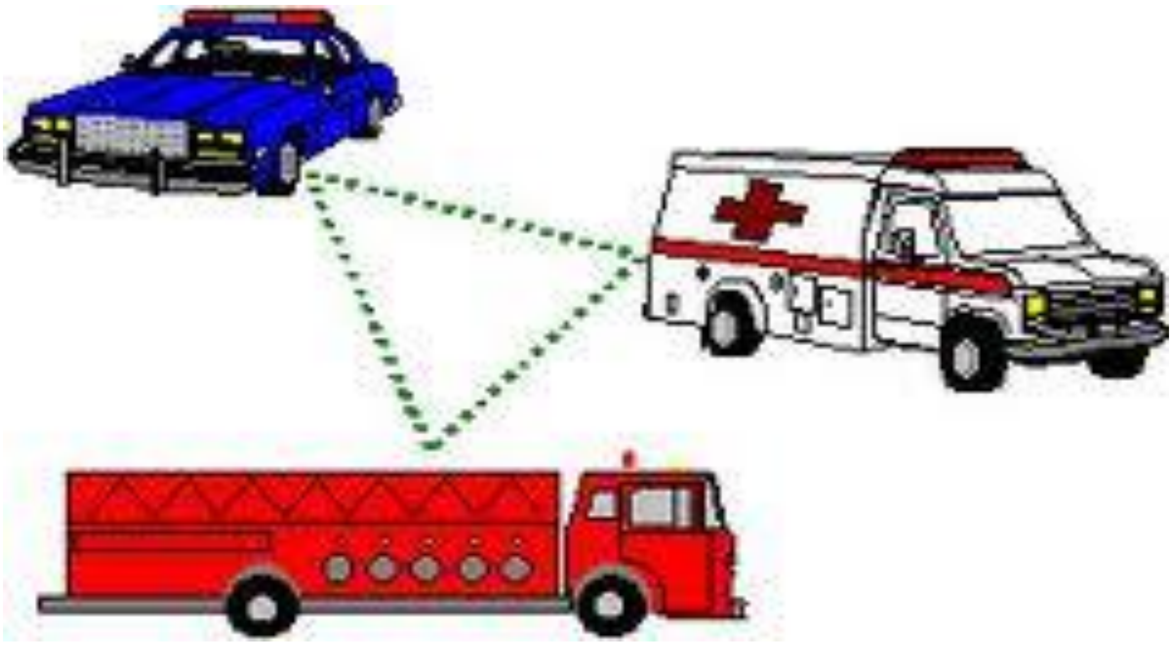


Figure 4: Application of Adhoc networks

1.6 Goal of Thesis.

The area of routing in wireless Adhoc networks is abuzz with research activity for obvious advantages of transmitting data over a communication link. Owing to a huge commercial market for new routing techniques, the area is wide open for further research in order to develop new algorithms and techniques aiming at routing of Adhoc networks, This thesis will aim at the classification and comparative study of wireless routing protocols for wireless Adhoc networks. The comparative study has been carried out on the basis of practical work done during M.Phill research program using some network simulator. The work to be carried out during this programme will attempt at:

1. Classification of existing routing techniques in wireless Ad hoc networks

2. Comparative Study / performance analysis of existing routing techniques in wireless Ad hoc networks using different network simulators.

3. The performance evaluation of the existing protocols will be carried out under different parameters (e.g. Fading models, Mobility models, traffic pattern) etc.

Chapter 2 Classification and Theoretical comparision of Routing Protocols

Chapter 2

Classification and Theoretical Comparision of Routing Protocols

2.1 Routing Protocols:

Routing protocols can be defined as formula used by routers to determine the appropriate path onto which data should be forwarded. The routing protocol also specifies how routers report changes and share information with the other routers in the network that they can reach. A routing protocol allows the network to dynamically adjust to changing conditions, otherwise all routing decisions have to be predetermined and remain static. There are some desirable properties or characteristics which every routing protocol should have.

2.2 Desirable Properties of Routing Protocols for Wireless Adhoc Networks:

There are some desirable properties of routing protocols for wireless Adhoc networks, the properties that are desirable in Ad-Hoc Routing protocols are as under [2][4][5][6][7].

2.2.1 Distributed operation:

The protocol should be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The difference is that the nodes in an ad-hoc network can enter or leave the network very easily and because of mobility the network can be partitioned.

2.2.2 Routing overhead:

Tracking changes of the network topology requires exchange of control packets amongst the mobile nodes. These control packets must carry various types of information, such as node identities, neighbor lists, distance metrics, etc., which consume additional bandwidth for transmission. Since wireless channel bandwidth is at a premium, it is desirable that the routing protocol minimizes the number and size of control packets for tracking the variations of the network.

2.2.3 Loop freedom:

Since the routes are maintained in a distributed fashion, the possibility of loops within a route is a serious concern. The routing protocol must incorporate special features so that the routes remain free of loops.

2.2.4 Timeliness:

Since link breakages occur at random times, it is hard to predict when an existing route will expire. The timeliness of adaptation of the routing protocol is crucial. A broken route causes interruption in an ongoing communication until a new route is established. Often the newly rediscovered route may be largely disjoint from the older route, which creates problems in rerouting the packets that were already transferred along the route and could not be delivered to the destination. Ideally, a new route should be determined before the existing one is broken, which may not be possible. Alternatively, a new route should be established with minimum delay.

2.2.5 Path optimality:

With constraints on the routing overhead, routing protocols for mobile ad hoc networks are more concerned with avoiding interruptions of communication between source and destination nodes rather than the optimality of the routes. Hence, in order to avoid excess transmission of control packets, the network may be allowed to operate with suboptimal (which are not necessarily the shortest) routes until they break. However, a good routing protocol should minimize overhead as well as the path lengths. Otherwise, it will lead to excessive transmission delays and wastage of power.

2.2.6 Demand based operation:

To minimize the control overhead in the network and thus not waste the network resources the protocol should be reactive. This means that the protocol should react only when needed and that the protocol should not periodically broadcast control information.

2.2.7 Unidirectional link support:

The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

2.2.8 Security:

The radio environment is especially vulnerable to impersonation attacks, so to ensure the desired behaviour of the routing protocol, we need some sort of security measures. Authentication and encryption is the way to go and problem here lies within distributing the keys among the nodes in the ad-hoc network.

2.2.9 Power conservation:

The nodes in the ad-hoc network can be laptops and thin clients such as PDA's that are limited in battery power and therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for these sleep modes.

2.2.10 Multiple routes:

To reduce the number of reactions to topological changes and congestion multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.

2.2.11 Quality of Service Support:

Some sort of Quality of service is necessary to incorporate into the routing protocol. This helps to find what these networks will be used for. It could be for instance real time traffic support. It should be noted that none of the proposed protocols have all these properties, but it is necessary to remember that the protocols are still under development and are probably extended with more functionality.

2.2.12 Storage complexity:

Another problem of distributed routing architectures is the amount of storage space utilized for routing. Ad hoc networks may be applied to small portable devices, such as sensors, which have severe constraints in memory and hardware. Hence, it is desirable that the routing protocol be designed to require low storage complexity.

2.2.13 Scalability:

Routing protocols should be able to function efficiently even if the size of the network becomes large. This is not very easy to achieve, as determining an unknown route between a pair of mobile nodes becomes more costly in terms of the required time, number of operations, and expended bandwidth when the number of nodes increases.

2.3 Taxonomy of Routing Protocols

There are number of routing protocols currently available in Adhoc networks. To compare and analyze mobile ad hoc network routing protocols, appropriate classification methods are important. Classification methods help researchers and designers to understand distinct characteristics of a routing protocol and find its relationship with others [3]. Traditionally classification was done by dividing protocols to table driven and to source initiated [3]. Table Driven routing protocols attempts to maintain consistent up to date routing information for each and every node in the network. These protocols require to maintain a consistent view. The areas in which they differ are the number of necessary routing related tables and the methods by which changes in network structure are broadcast. A very different approach from table driven routing scheme is source initiated routing. This type of routing creates routes only when needed by the source node. When a node needs a route to a destination, it initiates a route discovery process with in the network. This process is completed once route is found or all possible route permutations has been established, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or until the route is no longer required. In this thesis, an effective classification has been introduced, based on that classification protocols will be divided in groups according to following criteria, reflecting fundamental, design and implementation choices.

1. Pro-active Based routing.
2. Re-active Based Routing.
3. Hybrid Based Routing.
4. Hierarchical Based Routing.
5. Geographical Based Routing.
6. Power Based Routing.

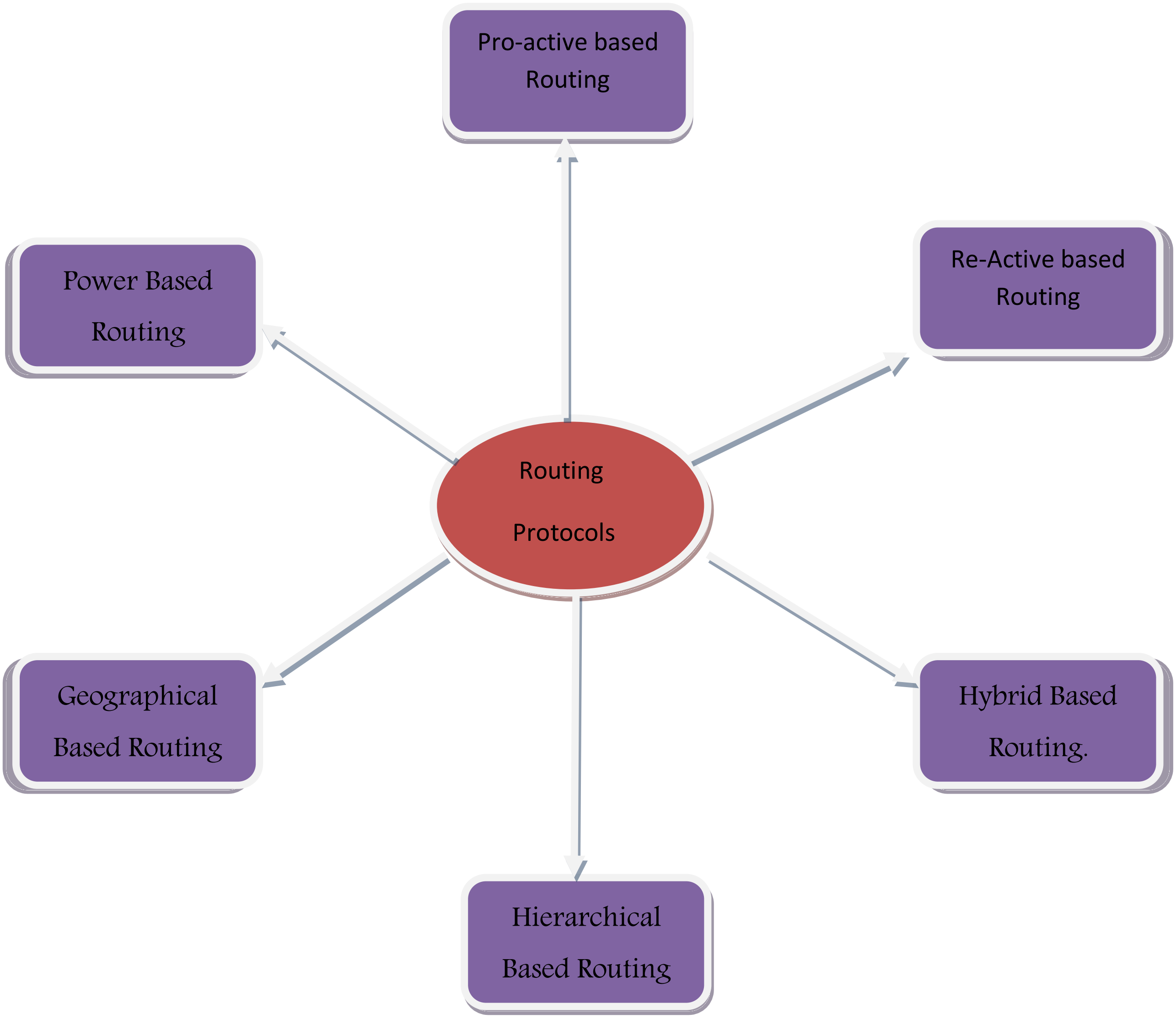


Figure 5: classification of routing protocols

2.3.1 Proactive based Routing:

Proactive protocols perform routing operations between all source destination pairs periodically, irrespective of the need of such routes. These protocols stem from conventional link state or distance vector routing algorithms, and attempt to maintain shortest-path routes by using periodically updated views of the network topology. These are typically maintained in routing tables in each node and updated with the acquisition of new information. Proactive protocols have advantages of providing lower latency in data delivery and the possibility of supporting applications that have quality-of-service constraints. Their main disadvantage is due to the wastage of bandwidth in sending update packets periodically even when they are not necessary, such as when there are no link breakages, or when only a few routes are needed.

Issues in Proactive Routing:

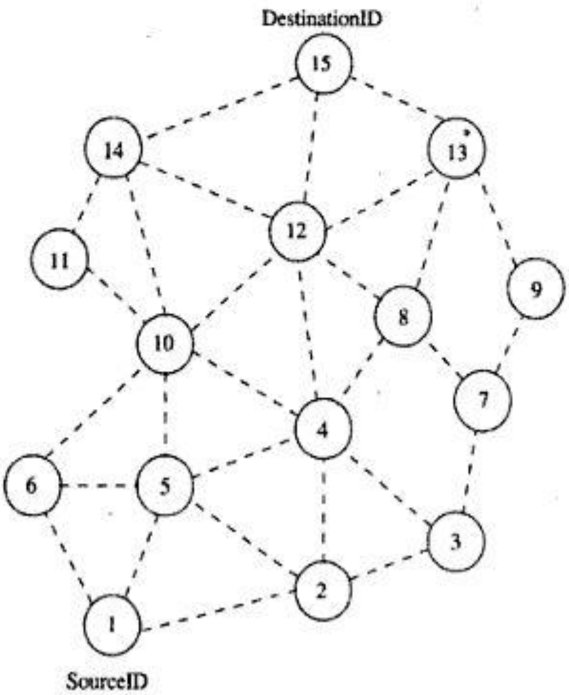
The key characteristic of proactive routing protocols is that updates are sent periodically irrespective of need. Another issue is that they are table-driven. These two properties cause serious problems for making proactive routing protocols scale with network size. However, these protocols work well under heavy traffic and high mobility conditions as they try to maintain fresh routing information continuously.

Some of the Proactive based routing algorithm are discussed below. I am going to discuss some protocols in this chapter and rest protocols will be explained in the coming chapters.

1. Distanation Sequence Distance vector.(DSDV)
2. Wireless Routing Protocols.(WRP)
3. Cluster head Gateway switch Routing (CGSR)
4. Source-Tree Adaptive Routing (STAR)
5. Optimized Link State Routing (OLSR)
6. Fisheye State Routing (FSR)

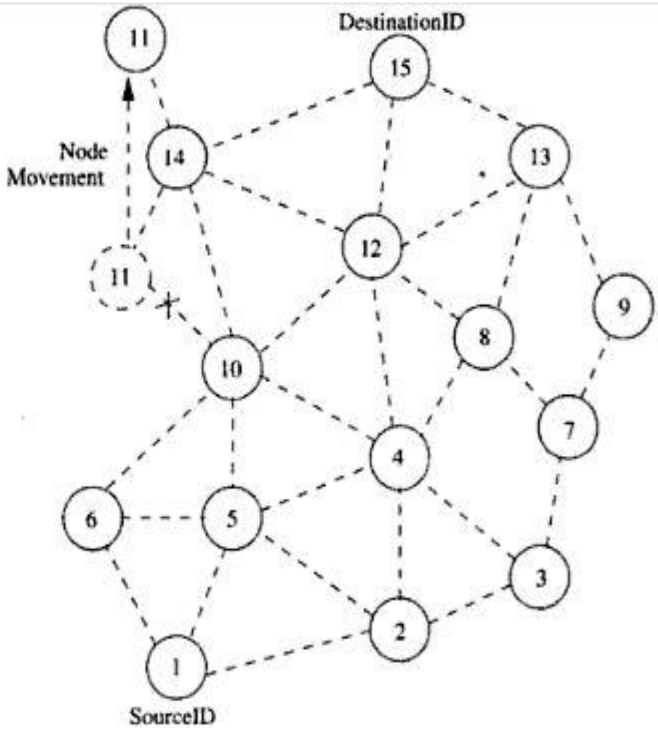
2.3.1.1 Destination-Sequenced Distance-Vector Routing (DSDV) :

This protocol is based on classical Bellman-Ford routing algorithm designed for MANETS. Each node maintains a list of all destinations and number of hops to each destination. Each entry is marked with a sequence number. It uses full dump or incremental update to reduce network traffic generated by route updates. The broadcast of route updates is delayed by settling time. The only improvement made here is avoidance of routing loops in a mobile network of routers. With this improvement, routing information can always be readily available, regardless of whether the source node requires the information or not. DSDV solve the problem of routing loops and count to infinity by associating each route entry with a sequence number indicating its freshness. In DSDV, a sequence number is linked to a destination node, and usually is originated by that node (the owner). The only case that a non-owner node updates a sequence number of a route is when it detects a link break on that route. An owner node always uses even-numbers as sequence numbers, and a non-owner node always uses odd-numbers. With the addition of sequence numbers, routes for the same destination are selected based on the following rules: 1) a route with a newer sequence number is preferred; 2) in the case that two routes have a same sequence number, the one with a better cost metric is preferred [22]. The list which is maintained is called routing table.



Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

Route Establishment Routing table for node 1



Routing table of node 1

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

Route maintenance

Figure 6: DSDV

The routing table contains the following:
(1) All available destinations' IP address

(2) Next hop IP address

(3) Number of hops to reach the destination

(4) Sequence number assigned by the destination node

(5) Install time.

The sequence number is used to distinguish stale routes from new ones and thus avoid the formation of loops. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven.

As stated above one of "full dump" or an incremental update is used to send routing table updates for reducing network traffic. A full dump sends the full routing table to the neighbors and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. If there is space in the incremental update packet then those entries may be included whose sequence number has changed. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps will be more frequent. [22]

Each route update packet, in addition to the routing table information, also contains a unique sequence number assigned by the transmitter. The route labelled with the highest (i.e. most recent) sequence number is used. If two routes have the same sequence number then the route with the best metric (i.e. shortest route) is used. Based on the past history, the stations estimate the settling time of routes. The stations delay the transmission of a routing update by settling time so as to eliminate those updates that would occur if a better route were found very soon. Each row of the update send is of the following form: <Destination IP address, Destination sequence number, Hop count> After receiving an update neighboring nodes utilizes it to compute the routing table entries. To damp the routing fluctuations due to unsynchronized nature of periodic updates, routing updates for a given destination can propagate along different paths at different rates. To prevent a node from announcing a routing path change for a given destination while another better update for that destination is still in route, DSDV requires node to wait a settling time before announcing a new route with higher metric for a destination.

2.3.1.2 Wireless routing protocol (WRP):

Wireless routing protocol was proposed by Murthy [31]. Wireless routing protocol (WRP) [30] is distance vector based protocol designed for Adhoc networks. Wireless routing protocol modifies and enhances distance vector during vector routing in the following three ways.

1. When there are no link changes, WRP periodically exchanges a simple HELLO packet rather than exchanging the whole route table. If topology changes are perceived, only the 'path-vector tuples' that reflect the updates are sent. These path-

vector tuples contain the destination, distance, and the predecessor (second-to-last hop) node ID.

2. To improve reliability in delivering update messages, every neighbor is required to send acknowledgments for update packets received. Retransmissions are sent if no positive acknowledgments are received within the timeout period.

3. The predecessor node ID information allows the protocol to recursively calculate the entire path from source to destination. With this information, WRP substantially reduces looping situations, speeds up the convergence, and is less prone to the 'count-to-infinity' problem. Still, temporary loops do exist and update messages are triggered frequently in networks with highly mobile hosts.

Since WRP, like DSDV, maintains an up to date view of network, every node has a readily available route to every destination node in the network. It differs from DSDV maintains only one topology table, WRP uses a set of tables to maintain more accurate information. The tables that are maintained by a node are the following.

1. Link Cost Table:

This table contains the cost of the link to each immediate neighbor node and information about the status of the link to each immediate neighbor.

2. Distance Table:

The distance table of a node contains a list of all the possible destination nodes and their distances beyond the immediate neighbors.

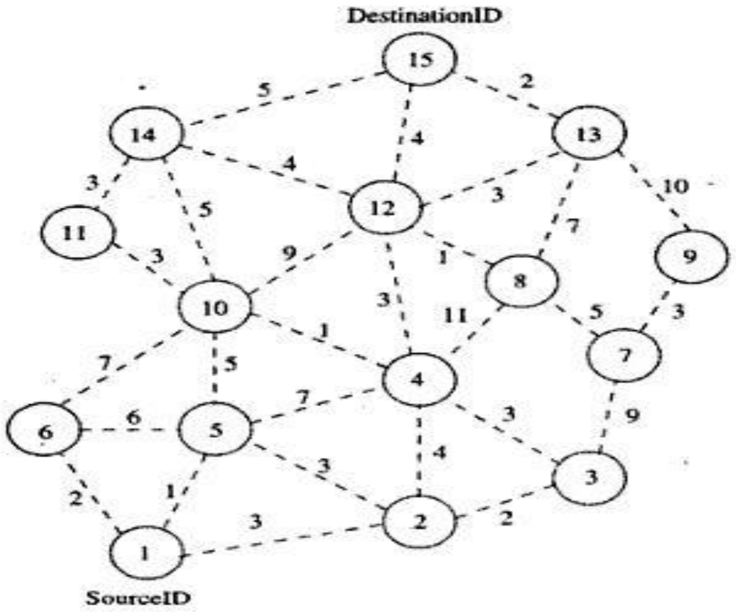
3. Routing Table:

The routing table contains a list of paths to a destination via different neighbors. If a valid path exists between a source and a destination node, its distance is recorded in the routing table along with information about the next-hop node to reach the destination node.

4. Message Retransmission List (MRL):

The MRL of a node contains information about acknowledgement (ACK) messages from its neighbors. If a neighbor doesn't reply with an ACK for a hello message within a certain time, then this information is kept in its MRL and an update is sent only to the non-responding neighbors.

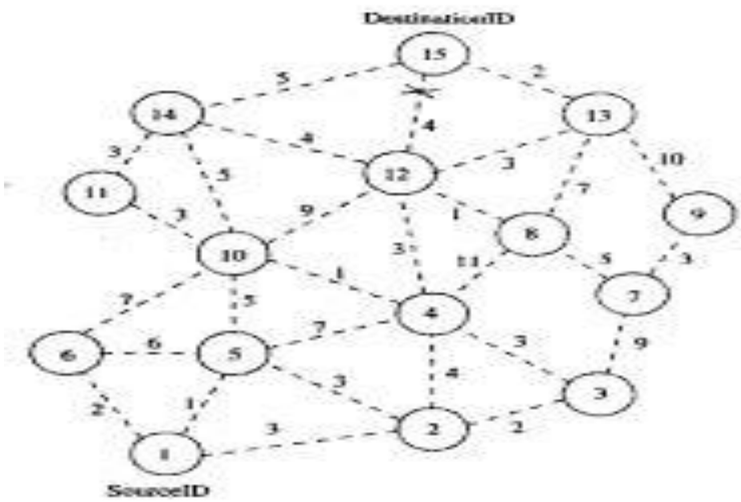
WRP works by requiring each node to send an update message periodically. This update message could be new routing information or a simple "hello" if the routing information hasn't changed from the previous update. After sending an update message to its all neighbors, a node expects to receive an ACK from all of them. If an ACK message does not come back from a particular neighbor, the node will record the non-responding neighbor in MRL and will send another update to the neighbor node later.



Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	12	4
11	14	14	8
10	4	12	8
9	13	13	12
8	12	12	5
7	8	12	10
6	10	12	15
5	10	12	13
4	12	12	10
3	4	12	7

Route Establishment



Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	13	5
11	14	14	8
10	4	13	9
9	13	13	12
8	12	13	6
7	8	13	11
6	10	13	16
5	10	13	14
4	12	13	8
3	4	13	11
2	4	13	12
1	2	13	15

Route Maintenance

Figure 7: WRP

The nodes receiving the update messages look at the new information in the update message and then update their own routing table and link cost table by finding the best path to a destination. This best path information is then relayed to all the other nodes so that they can update their routing tables. WRP avoids routing loops by checking the status of all the direct links of a node with its direct neighbors, each time a node updates any of its routing information.

2.3.1.3 Cluster head Gateway Switch Routing Protocol (CGSR):

Cluster head Gateway switch Routing Protocol [32], the nodes are divided into clusters. To form the cluster the following algorithm is used.

When a node comes up, it enters the "undecided" state, starts a timer and broadcasts a Hello message. When a cluster-head gets this hello message it responds with a triggered hello message immediately. When the undecided node gets this message it sets its state to "member". If the undecided node times out, then it makes itself the cluster-head if it has bi-directional link to some neighbor otherwise it remains in undecided state and repeats the procedure again. Cluster heads are changed as infrequently as possible. Each node maintains a neighbor table. For each neighbor, the neighbor table of a node contains the status of the link (uni- or bi-directional) and the state of the neighbor (cluster-head or member). A cluster-head keeps information about the members of its cluster and also maintains a cluster adjacency table that contains information about the neighboring clusters. For each neighbor cluster, the table has entry that contains the gateway through which the cluster can be reached and the cluster-head of the cluster. When a source has to send data to destination, it floods route request packets (but only to the neighboring cluster-heads). On receiving the request a cluster-head checks to see if the destination is in its cluster. If yes, then it sends the request directly to the destination else it sends it to all its adjacent cluster-heads. The cluster-heads address is recorded in the packet so a cluster-head discards a request packet that it has already seen. When the destination receives the request packet, it replies back with the route that had been recorded in the request packet. If the source does not receive a reply within a time period, it backs off exponentially before trying to send route request again. In CBRP, routing is done using source routing. It also uses route shortening that is on receiving a source route packet, the node tries to find the farthest node in the route that is its neighbor (this could have happened due to a topology change) and sends the packet to that node thus reducing the route. While forwarding the packet if a node detects a broken link it sends back an error message to the source and then uses local repair mechanism. In local repair mechanism, when a node finds the next hop is unreachable, it checks to see if the next hop can be reached through any of its neighbor or if hop after next hop can be reached through any other neighbor. If any of the two works, the packet can be sent out over the repaired path.

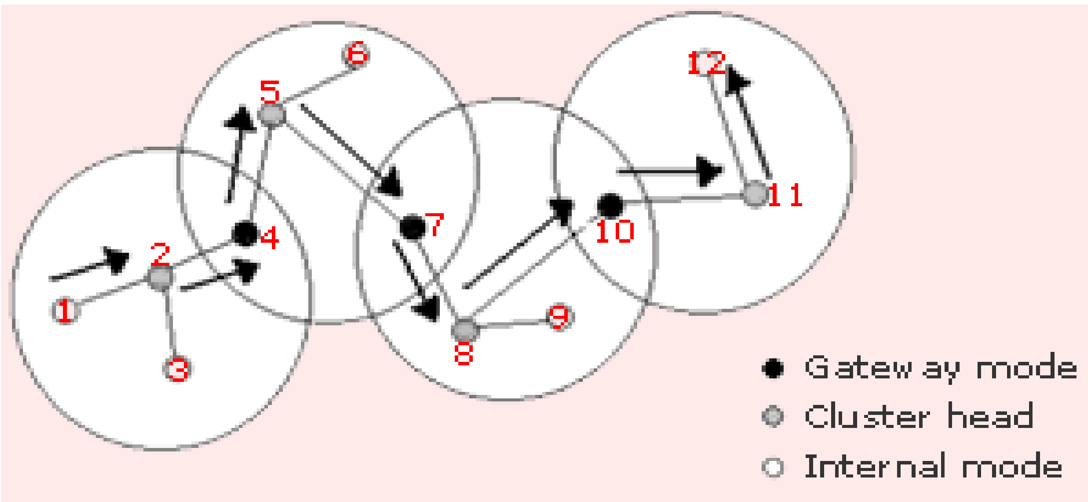


Figure 8: CGSR

2.3.1.4 Source tree adaptive routing protocol (STAR):

Source tree adaptive routing protocol(STAR) [9Book] proposed by Garcia-Luna-Aceves and Spohn is a table-driven routing protocol. Each node discovers and maintains topology information of the network, and builds a shortest path tree (source tree) to store preferred paths to destinations. The basic mechanisms in STAR include the detection of neighbors and exchange of topology information (update message) among nodes. For STAR, there are mainly two alternative mechanisms to discover neighbors:

1. Hello Messages: Hello messages are sent by each node periodically to inform neighbors of its existence. Such messages can be small packets, not needing to contain any routing information. When a node receives a hello message from another node that it does not know previously, it discovers a new neighbor. If a node does not receive any message (update or hello) from a neighbor for a certain period of time, it determines that this neighbor is broken or out of its range.
2. Neighbor Protocol: A neighbor protocol can be implemented at the link layer. It notifies STAR of the existence of new neighbors or the loss of connectivity to an existing neighbor. With the support of a neighbor protocol, no hello messages are needed.

By adopting the Least-Overhead Routing Approach (LORA), STAR greatly reduces control overhead in ad hoc network environment. Under LORA, a source node does not need to maintain shortest paths to destinations. A node running STAR does not send update messages after every change of topology. It only sends updates in the event of unreachable destinations, new destinations, the possibility of permanent routing loops, or cost of paths exceeding a given threshold. These situations are defined by the three basic LORA rules in STAR. Four LORA rules are further defined for the case when the underlying MAC protocol does not support reliable transmission. These rules introduce periodic update messages, repair messages and query messages. Query messages give some ondemand characteristic to STAR, but they are used much less aggressively than in such on-demand protocols as AODV and DSR. The basic information unit in STAR is the representation of a link, which indicates the two adjacent neighbors, the cost of the link, and the time stamp reflecting the freshness of the link. Accordingly, for communicating topology information, the basic information unit transmitted is a LSU (Link State Update). The set of links used by a node in its preferred paths to destinations form the source tree of the node. The set of LSUs form the topology information being exchanged.

2.3.1.5 The Fisheye State Routing (FSR):

The Fisheye State Routing (FSR) [33] is a proactive unicast routing protocol based on Link State routing algorithm with effectively reduced overhead to maintain network topology information. As indicated in its name, FSR utilizes a function similar to a fish eye. The eyes of fishes catch the pixels near the focal with high detail, and the detail decreases as the distance from the focal point increases. Similar to fish eyes, FSR maintains the accurate distance and path quality information about the immediate neighboring nodes, and progressively reduces detail as the distance increases.

In Link State routing algorithm used for wired networks, link state updates are generated and flooded through the network whenever a node detects a topology change. In FSR, however, nodes exchange link state information only with the neighboring nodes to maintain up-to-date topology information. Link state updates are exchanged periodically in FSR, and each node keeps a full topology map of the network. To reduce the size of link state update messages, the key improvement in FSR is to use different update periods for different entries in the routing table. Link state updates corresponding to the nodes within a smaller scope are propagated with higher frequency.

FSR exhibits a better scalability concerning the network size compared to other link state protocols because it doesn't strive for keeping all nodes in the network on the same knowledge level about link states. Instead, the accuracy of topology information is reverse proportional to the distance. This reduces the traffic overhead caused by exchanging link state information because this information is exchanged more frequently with node nearby than with nodes far away. Adapting the frequency of exchanging link state information according to the FSR

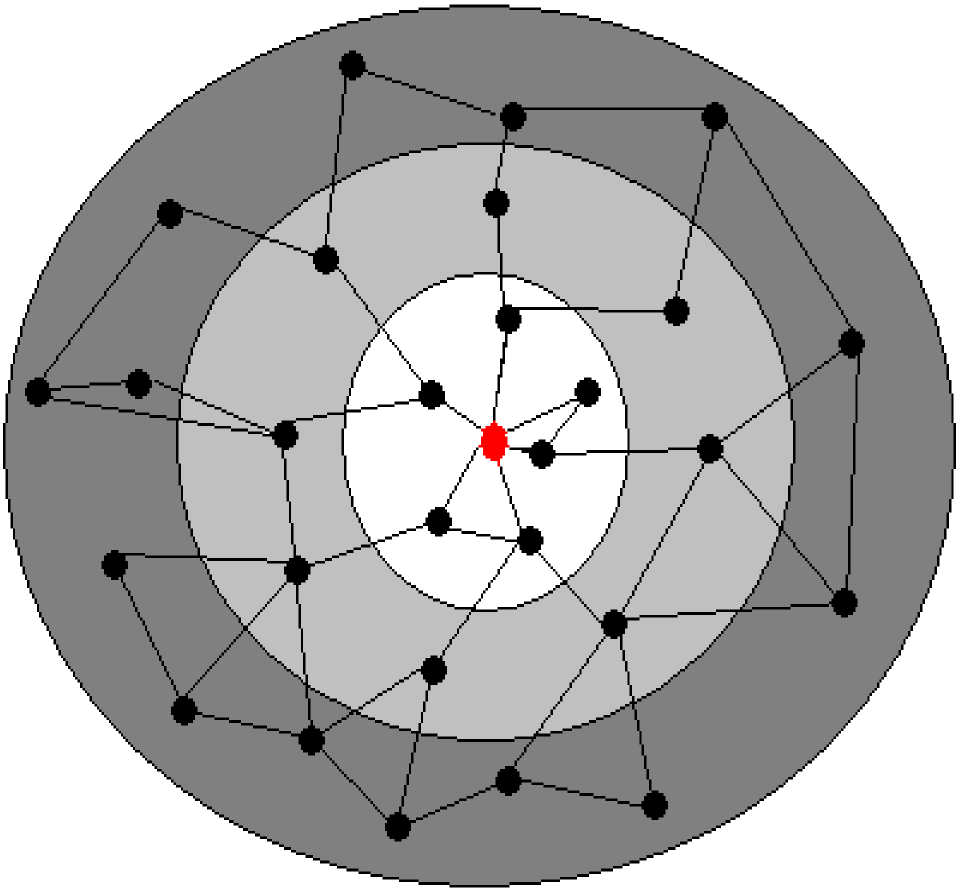


Figure 9: Fisheye State Routing (FSR)

2.3.1.6 Theoretical Comparison of Proactive Routing Protocols

Control traffic overhead and loop-free property are two important issues when applying proactive routing to mobile ad hoc networks. The proactive routing protocols used for wired networks normally have predictable control traffic overhead because topology of wired networks change rarely and most routing updates are periodically propagated. However, periodic routing information updates are not enough for mobile ad hoc routing protocols. The proactive routing in mobile ad hoc networks needs mechanisms that dynamically collect network topology changes and send routing updates in an event-triggered style.

Although belonging to the same routing category for mobile ad hoc networks, WRP, DSDV,OSLR and FSR have distinct features. Both WRP and DSDV exploited event-triggered updates to maintain up-to-date and consistent routing information for mobile nodes. In contrast to using event-triggered updates, the updates in FSR are exchanged between neighboring nodes and the update frequency is dependend on the distance between nodes. In this way, update overhead is reduced and the far-reaching effect of Link State routing is restricted.

Different mechanisms are used in WRP, DSDV , OSLR and FSR for loop-free guarantee. WPR records the predecessor and the successor along a path in its routing table and introduces consistence-checking mechanism. In this way, WRP avoids forming temporary route loops but incurs additional overhead. Every node needs to maintain more information and execute more operations. In DSDV, a destination sequence number is introduced to avoid route loops. FSR is a modification of traditional Link State routing and its loop-free property is inherited from Link State routing algorithm.

WRP, DSDV and FSR have the same time and communication complexity. Whereas WRP has a large storage complexity compared to DSDV because more information is required in WRP to guarantee reliable transmission and loop-free paths. Both periodic and triggered updates are utilized in WRP and DSDV; therefore, their performance is tightly related with the network size and mobility pattern. As a Link State routing protocol, FSR has high storage complexity, but it has potentiality to support multiple-path routing and QoS routing.

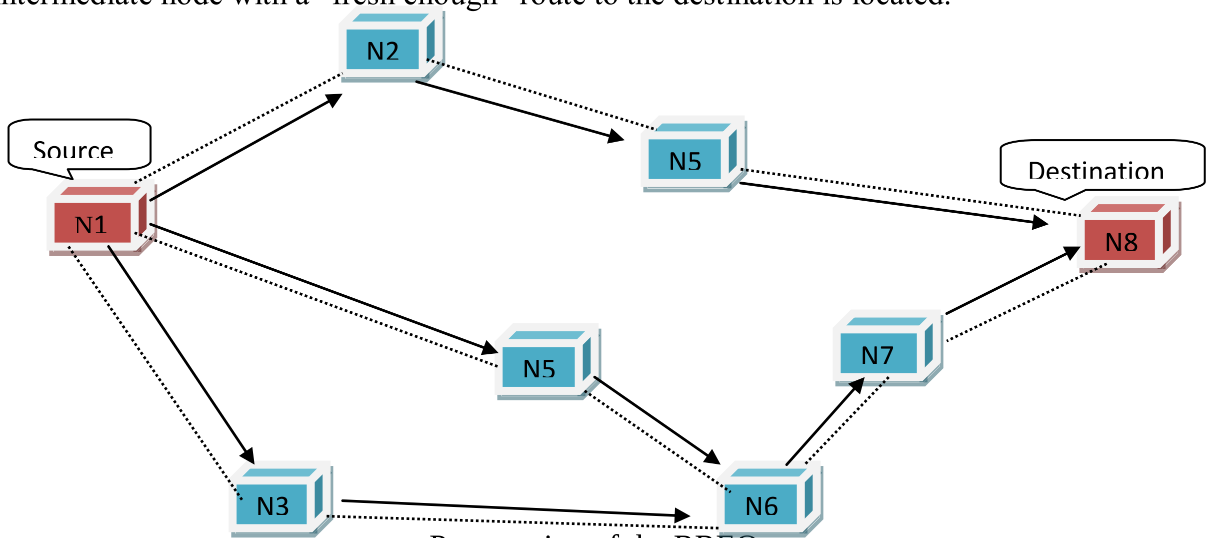
2.3.2 Reactive Based Routing:

As its name suggests, this type of protocols discovers a route only when actual data transmission takes place. When a node wants to send information to another node in a network, a source node initiates a route-discovery process. Once a route is discovered, it is maintained in the temporary cache at a source node unless it is expired or unless some event happens (e.g., a link failure) that requires another route discovery to start over again. Reactive protocols require less amount of routing information at each node, compared to proactive protocols, as there is no need to obtain and maintain the routing information for all the nodes in a network. Another advantage in reactive protocols is that intermediate nodes do not have to make routing decisions. An obvious disadvantage in reactive protocols is delay due to route discovery, called route acquisition delay. Furthermore, if routing information changes frequently, as it is the case in Adhoc networks , and if route discoveries are needed for those changed routes, reactive protocols may result in a large volume of messaging overhead, since route recoveries require global broadcasts. The protocols which comes reactive routing are as under. Some of them will be explained here and others are explained in coming chapters.

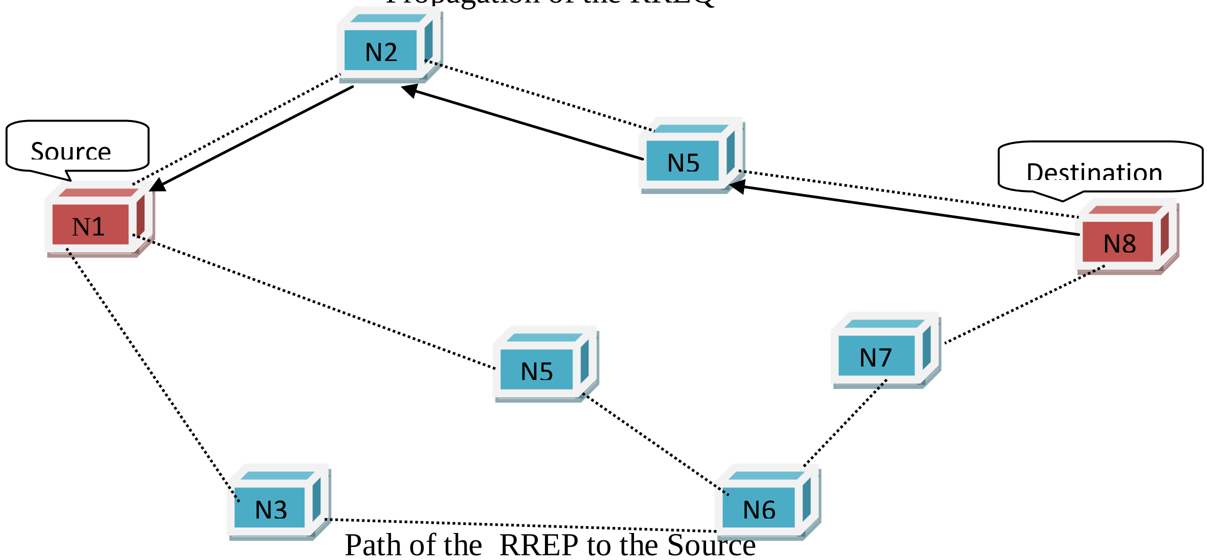
1. Ad hoc On Demand Distance Vector (AODV)
2. Dynamic Source routing protocol (DSR)
3. Temporally ordered routing algorithm (TORA)
4. Associativity Based routing (ABR)
5. Signal Stability-Based Adaptive Routing (SSR)

2.3.2.1 Ad hoc On Demand Distance Vector (AODV):

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol described in [34] builds on the DSDV algorithm previously described. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, since nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges [34]. When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbors, which then forward the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located.



Propagation of the RREQ



Path of the RREP to the Source

Figure10: AODV

Figure illustrates the propagation of the broadcast RREQs across the network. AODV utilizes destination sequence numbers to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies an RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ. During the process of forwarding the RREQ, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination/intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ. As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forwarded along the path established by the RREQ, AODV only supports the use of symmetric links. Routes are maintained as follows. If a source node moves, it is able to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbor notices the move and propagates a link failure notification message (an RREP with infinite metric) to each of its active upstream neighbors to inform them of the erasure of that part of the route [34]. These nodes in turn propagate the link failure notification to their upstream neighbors, and so on until the source node is reached. The source node may then choose to reinitiate route discovery for that destination if a route is still desired. An additional aspect of the protocol is the use of hello messages, periodic local broadcasts by a node to inform each mobile node of other nodes in its neighborhood. Hello messages can be used to maintain the local connectivity of a node. However, the use of hello messages is not required. Nodes listen for retransmission of data packets to ensure that the next hop is still within reach. If such a retransmission is not heard, the node may use any one of a number of techniques, including the reception of hello messages, to determine whether the next hop is within communication range. The hello messages may list the other nodes from which a mobile has heard, thereby yielding greater knowledge of network connectivity.

2.3.2.2 Dynamic Source Routing Protocol (DSR)

Dynamic Source Routing (DSR) protocol [40]: Dynamic Source Routing protocol, as its name implies, is a source routing protocol: a complete sequence of intermediate nodes from a source to a destination will be determined at a source node and all packets transmitted by a source node to a destination follow the same path. Every packet header contains the complete sequence of nodes to reach a destination. DSR protocol is a reactive protocol and its primary motivations are, (1) to avoid periodic announcements of link states required in proactive protocols, by separating route discovery from route maintenance, (2) to avoid long convergence time of routing information and (3) to eliminate a large routing table for forwarding packets at intermediate nodes. The routing table, in a sense that it is the data structure to always hold routing information to reach every possible destination in a network, is not used in DSR protocol. In DSR, routes are discovered on demand and route cache is used to hold routes that are currently in use. As most of the reactive protocols do, DSR consists of two procedures: route discovery and route maintenance.

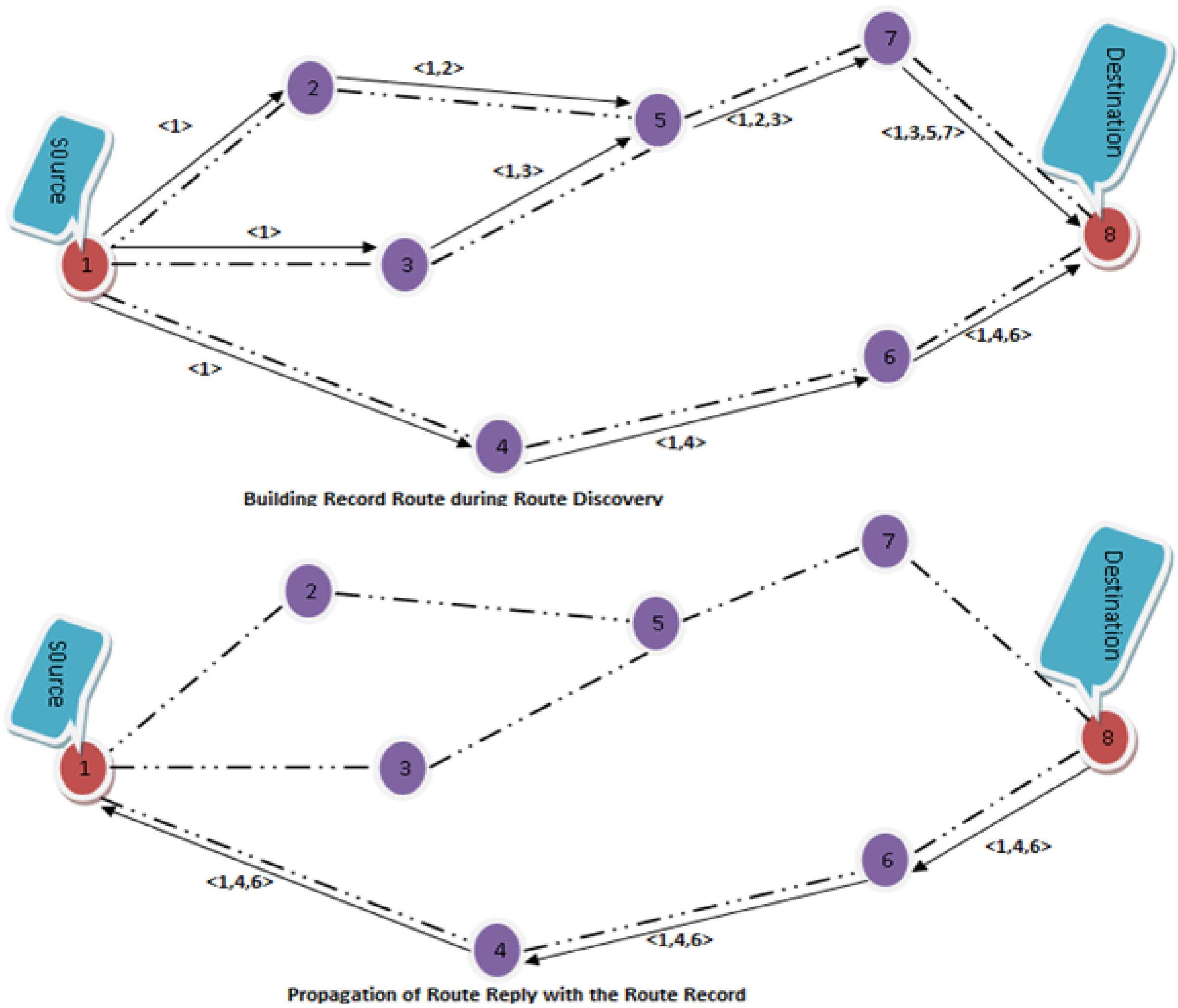


Figure11: DSR

Route Discovery:

Every node in a network maintains a route cache that contains a list of hop-by-hop routes to each destination node currently active and its expiration time (i.e., the time after which a route is considered stale and discarded). Before a source node starts transmitting data to a destination node, it first looks up its route cache to see if a valid route to that destination exists. If such a route exists, then the route discovery process ends and the source starts transmitting data using the route found in its route cache. Otherwise, a source node broadcasts a route request packet (RRP) to find a route to reach the destination. This broadcast is a global broadcast, which floods RRP in a network through all alternative paths to reach a destination. While a RRP is being broadcast and propagated to the destination, a RRP adds the address of every node it encounters to its list. If the same address appears more than once in the list, a RRP drops itself to avoid a routing loop. When a RRP reaches the destination node, the destination returns the learned path extracted from the RRP to the source node. For wireless networks that consist of asymmetric links, the destination node can send that path information back to the source node as a global broadcast, which allows DSR to work for asymmetric links.

Route Maintenance:

Route maintenance in DSR is a mechanism to inform network failures to all nodes in a network. Its primary motivation is to expedite detection of network failures by explicitly announcing them to every node in a network using global broadcasts. No matter if it is a link or node failure, a node that is connected to the other end of a failed link is responsible for detecting a failure in DSR. On detecting a network failure, the detecting node broadcasts an error message, called error packet, to all the other nodes in a network to inform the failure. When other nodes receive an error packet, they will disable the paths that go through the failed link in their route cache. An obvious advantage in DSR is that source nodes are aware of existence of alternative paths, which implies that recovery from a link failure will be easy and quick. Another advantage is that there will not be a chance of a routing loop (or it is easy to detect and avoid one). Furthermore, nodes do not have to maintain routing table, which is an advantage especially for a large network where nodes continue to move. Being a reactive protocol also means that a route is stored in the route cache only when one is needed, which implies low maintenance overhead. Since most routes are short-lived and network topology frequently changes in MANETs, on-demand routing will make more sense than proactive protocols in terms of maintenance overhead for routing information at each node (this is because a node does not have to modify anything if a failed and/or changed link is not a part of any active path from this node).

The disadvantage in DSR is long route acquisition delay due to route discovery if short transmission delay is a significant factor. Long route acquisition delay may not be acceptable in certain situations, such as mobile communication at a battlefield. It is also quite possible that the path between a source and a destination may not be the shortest path (this is because resumed links will not be explicitly advertised in DSR), resulting paths with in suboptimal end-to-end delay. Another disadvantage is that messaging overhead of the protocol will be high during busy time, when many connections must be established in a short time since broadcast is used in route discovery. Large packet header will also cause low payload utilization, since each packet has to contain a list of all the intermediate routers to reach a destination.

2.3.2.3 **Signal Stability-Based Adaptive Routing protocol** (SSR)

Another on-demand protocol is the Signal Stability-Based Adaptive Routing protocol (SSR) presented in [41]. Unlike the algorithms described so far, SSR selects routes based on the signal strength between nodes and a node’s location stability. This route selection criteria has the effect of choosing routes that have “stronger” connectivity. SSR can be divided into two cooperative protocols: the Dynamic Routing Protocol (DRP) and the Static Routing Protocol (SRP). The DRP is responsible for the maintenance of the Signal Stability Table (SST) and Routing Table (RT). The SST records the signal strength of neighboring nodes, which is obtained by periodic beacons from the link layer of each neighboring node. Signal strength may be recorded as either a strong or weak channel. All transmissions are received by, and processed in, the DRP. After updating all appropriate table entries, the DRP passes a received packet to the SRP. The SRP processes packets by passing the packet up the stack if it is the intended receiver or looking up the destination in the RT and then forwarding the packet if it is not. If no entry is found in the RT for the destination, a route-search process is initiated to find a route. Route requests are propagated throughout the network, but are only forwarded to the next hop if they are received over strong channels and have not been previously processed (to prevent looping). The destination chooses the first arriving route-search packet to send back because it is most probable that the packet arrived over the shortest and/or least congested path. The DRP then reverses the selected route and sends a route-reply message back to the initiator. The DRP of the nodes along the path update their RTs accordingly. Route-search packets arriving at the destination have necessarily chosen the path of strongest signal stability, since the packets are dropped at a node if they have arrived over a weak channel. If there is no route-reply message received at the source within a specific timeout period, the source changes the PREF field in the header to indicate that weak channels are acceptable, since these may be the only links over which the packet can be propagated. When a failed link is detected within the network, the intermediate nodes send an error message to the source indicating which channel has failed. The source then initiates another route-search process to find a new path to the destination. The source also sends an erase message to notify all nodes of the broken link.

2.3.2.4 The Associativity-Based Routing (ABR)

A totally different approach in mobile routing is proposed in [43]. The Associativity-Based Routing (ABR) protocol is free from loops, deadlock, and packet duplicates, and defines a new routing metric for ad hoc mobile networks. This metric is known as the degree of association stability. In ABR, a route is selected based on the degree of association stability of mobile nodes. Each node periodically generates a beacon to signify its existence. When received by neighboring nodes, this beacon causes their associativity tables to be updated. For each beacon received, the associativity tick of the current node with respect to the beaconing node is incremented. Association stability is defined by connection stability of one node with respect to another node over time and space. A high degree of association stability may indicate a low state of node mobility, while a low degree may indicate a high state of node mobility. Associativity ticks are reset when the neighbors of a node or the node itself move out of proximity. A fundamental objective of ABR is to derive longer-lived routes for ad hoc mobile networks. The three phases of ABR are:

- Route discovery
- Route reconstruction (RRC)
- Route deletion

The route discovery phase is accomplished by a broadcast query and await-reply (BQ-REPLY) cycle. A node desiring a route broadcasts a BQ message in search of mobiles that have a route to the destination. All nodes receiving the query (that are not the destination) append their addresses and their associativity ticks with their neighbors along with QoS information to the query packet. A successor node erases its upstream node neighbors' Associativity tick entries and retains only the entry concerned with itself and its upstream node. In this way, each resultant packet arriving at the destination will contain the Associativity ticks of the nodes along the route to the destination. The destination is then able to select the best route by examining the associativity ticks along each of the paths. When multiple paths have the same overall degree of association stability, the route with the minimum number of hops is selected. The destination then sends a REPLY packet back to the source along this path. Nodes propagating the REPLY mark their routes as valid. All other routes remain inactive, and the possibility of duplicate packets arriving at the destination is avoided. RRC may consist of partial route discovery, invalid route erasure, valid route updates, and new route discovery, depending on which node(s) along the route move. Movement by the source results in a new BQ-REPLY process, as shown in Fig. 6a. The RN[42] message is a route notification used to erase the route entries associated with downstream nodes. When the destination moves, the immediate upstream node erases its route and determines if the node is still reachable by a localized query (LQ[H]) process, where H refers to the hop count from the upstream node to the destination (Fig. 6b) the destination receives the LQ packet, it REPLYs with the best partial route; otherwise, the initiating node times out and the process backtracks to the next upstream node. Here an RN[0] message is sent to the next upstream node to erase the invalid route and inform this node that it should invoke the LQ[H] process. If this process results in backtracking more than halfway to the source, the LQ process is discontinued and a new BQ process is initiated at the source. When a discovered route is no longer desired, the source node initiates a route delete (RD) broadcast so that all nodes along the route update their routing tables. The RD message is propagated by a full broadcast, as opposed to a directed broadcast, because the source node may not be aware of any route node changes that occurred during RRCs.

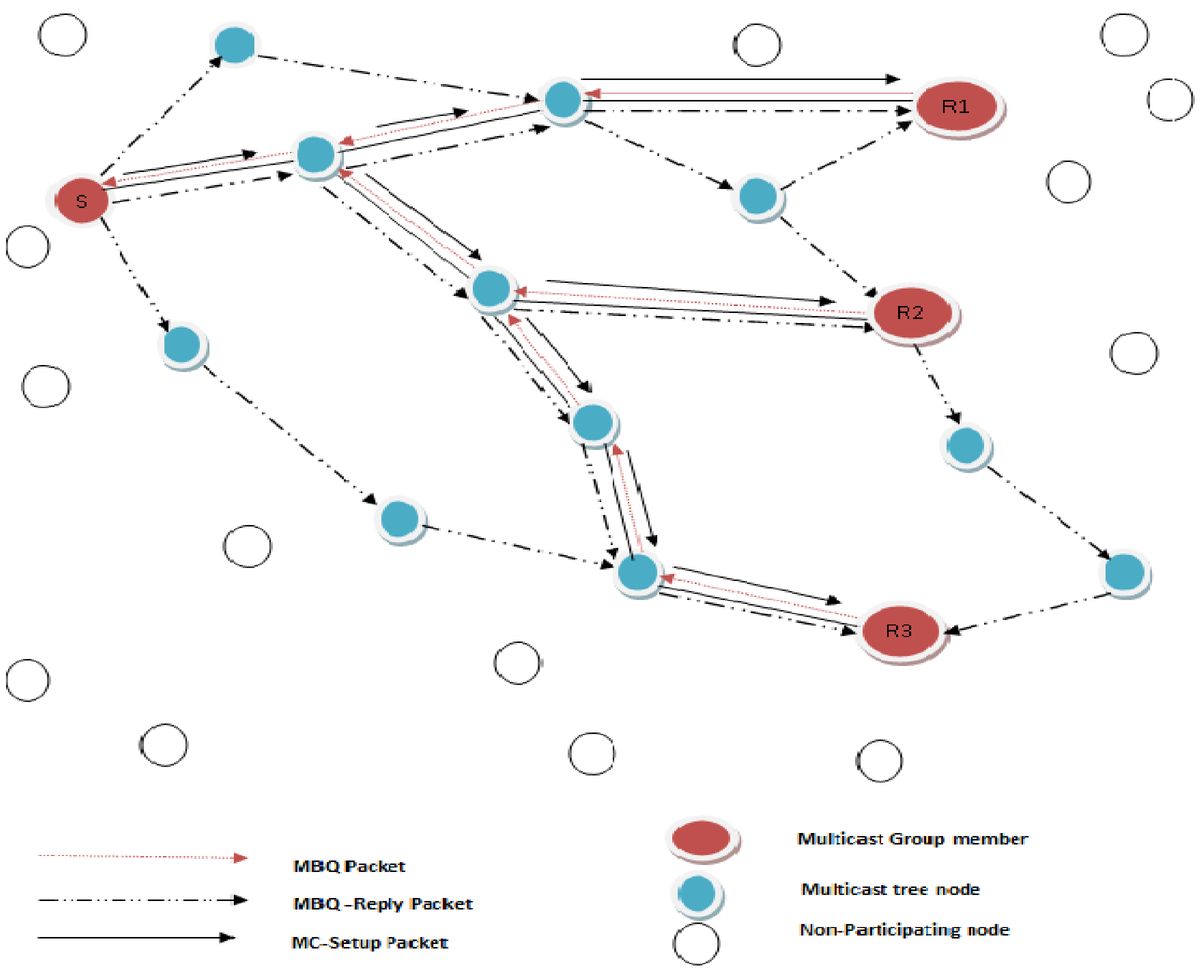


Figure 11: ABR

2.3.2.5 Theoretical Comparison of Reactive Routing Protocols:

AODV employs a route discovery procedure similar to DSR; however, there are a couple of important distinctions. The most notable of these is that the overhead of DSR is potentially larger than that of AODV since each DSR packet must carry full routing information, whereas in AODV packets need only contain the destination address. Similarly, the route replies in DSR are larger because they contain the address of every node along the route, whereas in AODV route replies need only carry the destination IP address and sequence number. Also, the memory overhead may be slightly greater in DSR because of the need to remember full routes, as opposed to only next hop information in AODV. A further advantage of AODV is its support for multicast [36]. None of the other algorithms considered in this article currently incorporate multicast communication. On the downside, AODV requires symmetric links between nodes, and hence cannot utilize routes with asymmetric links. In this aspect DSR is superior, since it does not require the use of such links and can utilize asymmetric links when symmetric links are not available. The DSR algorithm is intended for networks in which the mobiles move at moderate speed with respect to packet transmission latency [35]. Assumptions the algorithm makes for operation are that the network diameter is relatively small and that the mobile nodes can enable a promiscuous receive mode, whereby every received packet is delivered to the network driver software without filtering by destination address. An advantage of DSR over some of the other ondemand protocols is that DSR does not make use of periodic routing advertisements, thereby saving bandwidth and reducing power consumption.

Hence, the protocol does not incur any overhead when there are no changes in network topology. Additionally, DSR allows nodes to keep multiple routes to a destination in their cache. Hence, when a link on a route is broken, the source node can check its cache for another valid route. If such a route is found, route reconstruction does not need to be reinvoked. In this case, route recovery is faster than in many of the other ondemand protocols. However, if there are no additional routes to the destination in the source node’s cache, route discovery must be reinitiated, as in AODV, if the route is still required. On the other hand, because of the small diameter assumption and the source routing requirement, DSR is not scalable to large networks. Furthermore, as previously stated, the need to place the entire route in both route replies and data packets causes greater control overhead than in AODV. TORA is a “link reversal” algorithm that is best suited for networks with large dense populations of nodes [39]. Part of the novelty of TORA stems from its creation of DAGs to aid route establishment. One of the advantages of TORA is its support for multiple routes. TORA and DSR are the only on-demand protocols considered here which retain multiple route possibilities for a single source/destination pair. Route reconstruction is not necessary until all known routes to a destination are deemed invalid, and hence bandwidth can potentially be conserved because of the necessity for fewer route rebuilding. Another advantage of TORA is its support for multicast. Although, unlike AODV, TORA does not incorporate multicast into its basic operation, it functions as the underlying protocol for the Lightweight Adaptive Multicast Algorithm (LAM), and together the two protocols provide multicast capability [37]. TORA’s reliance on synchronized clocks, while a novel idea, inherently limits its applicability. If a node does not have GPS or some other external time source, it cannot use the algorithm. Additionally, if the external time source fails, the algorithm will cease to operate. Furthermore, route rebuilding in TORA may not occur as quickly as in the other algorithms due to the potential for oscillations during this period. This can lead to potentially lengthy delays while waiting for the new routes to be determined.

ABR is a compromise between broadcast and point-to-point routing, and uses the connection-oriented packet forwarding approach. Route selection is primarily based on the aggregated associativity ticks of nodes along the path. Hence, although the resulting path does not necessarily result in the smallest possible number of hops, the path tends to be longerlived than other routes. A long-lived route requires fewer route reconstructions and therefore yields higher throughput. Another benefit of ABR is that, like the other protocols, it is guaranteed to be free of packet duplicates. The reason is that only the best route is marked valid, while all other possible routes remain passive. ABR, however, relies on the fact that each node is beaconing periodically. The beaconing interval must be short enough to accurately reflect the spatial, temporal, and connectivity state of the mobile hosts. This beaconing requirement may result in additional power consumption. However, experimental results obtained in [38] reveal that the inclusion of periodic beaconing has a minute influence on the overall battery power consumption. Unlike DSR, ABR does not utilize route caches. The SSR algorithm is a logical descendant of ABR. It utilizes a new technique of selecting routes based on the signal strength and location stability of nodes along the path. As in ABR, while the paths selected by this algorithm are not necessarily shortest in hop count, they do tend to be more stable and longer-lived, resulting in fewer route reconstructions. One of the major drawbacks of the SSR protocol is that, unlike in AODV and DSR, intermediate nodes cannot reply to route requests sent toward a destination; this results in potentially long delays before a route can be discovered. Additionally, when a link failure occurs along a path, the route discovery algorithm must be reinvoked from the source to find a new path to the destination. No attempt is made to use partial route recovery (unlike ABR), that is, to allow intermediate nodes to attempt to rebuild the route themselves. AODV and DSR also do not specify intermediate node rebuilding. While this may lead to longer route reconstruction times since link failures cannot be resolved locally without the intervention of the source node, the attempt and failure of an intermediate node to rebuild a route will cause a longer delay than if the source node had attempted the rebuilding as soon as the broken link was noticed. Thus, it remains to be seen whether intermediate node route rebuilding is more optimal than source node route rebuilding.

Parameters	AODV	DSR	TORA
Source Routing	No	Yes	No
Topology	Full	Full	Reduced
Broadcast	Full	Full	Local
Update Information	Route Error	Route Error	Node’s Height
Update Destination	Source	Source	Neighbour
Methods	Unicast	Unicast	Broadcast
Storage Complexity	O(E)	O(E)	O(Dd*A)

Abbreviations:
Dd - Number of maximum desired destination.
E – Communication Pairs.
A – Average Numbers of Adjacent nodes.

Table 1: Comparison of reactive routing protocols

2.3.3 Hybrid Based Routing Protocol :

Because of the initial delay due to route discovery and high control overhead in reactive protocols, a pure reactive protocol may not be the best solution for routing in Adhoc networks. On the other hand, a pure proactive protocol used for a large network may not be feasible because of the need to keep a large routing table at all times. A protocol that uses the best features of both reactive and proactive protocol may be a better solution for routing in Adhoc networks. This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for one or the other method requires predetermination for typical cases.

2.3.3.1 Zone Routing Protocol:

ZRP ([25], [26]) is a zone or cluster-based routing protocol that is a hybrid between proactive and reactive routing. Since the advantages of either approach depend on the characteristics of the network, such as degree of mobility and node density, it could be beneficial to combine them. ZRP introduces the concept of a routing zone which is a set of nodes within the local neighborhood. In practice, each zone defines a maximum number of hops, and a node within the zone may be distant from the centre node of the zone. Each node maintains routing information actively within its zone. The scheme used is called Intra-zone Routing Protocol (IARP), which is essentially an adapted form of a basic link state algorithm. For route discovery outside the local routing zone, a reactive protocol, namely, Inter-zone Routing Protocol (IERP) is used. For this purpose, a border cast of a request message is used. Border cast is a technique where the packets are forwarded only to the defined peripheral nodes of the zone. The receiver of border cast can check if the target is within their own zone, or it may continue to border cast. The border cast process is able to identify and reject repeated packets which are already propagated in the same region through recording queries for some pre-defined time at the relaying nodes. ZRP uses a special technique for this, called Advanced Query Detection and Early Termination [26]. Route caching and local repair are also possible.

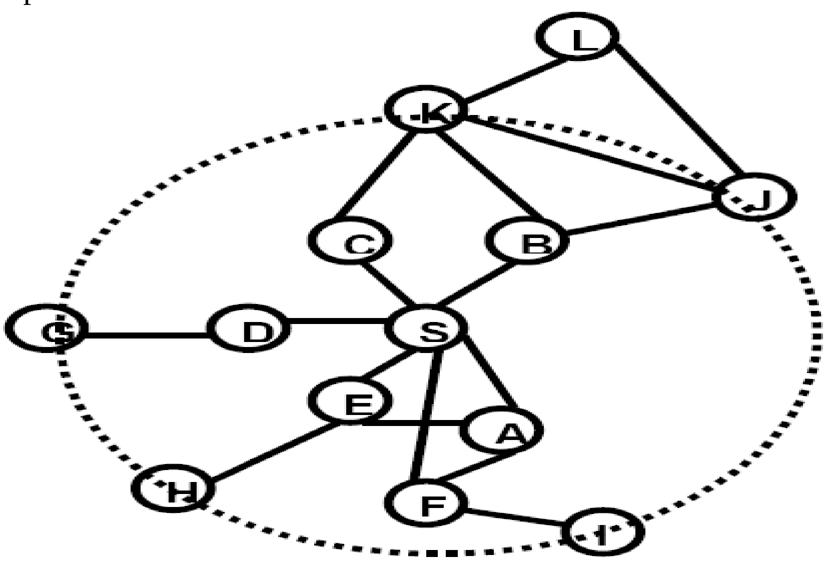


Figure 12. A routing zone with radius of 2 hops (Ref. from [26]).

ZRP is targeted for very large and dense networks, typically in the order of a few hundred nodes, where it is logical to divide the network into zones or clusters of nodes [27]. Such cluster-based routing is not new. A number of cluster-based approaches have appeared in the past [28] [29].

2.3.3.2 The Hybrid Ad hoc Routing Protocol (HARP)

The Hybrid Ad hoc Routing Protocol (HARP) [44] is a hybrid routing scheme, which exploits a two-level zone based hierarchical network structure. Different routing approaches are utilized in two levels, for intra-zone routing and inter-zone routing, respectively.

The Distributed Dynamic Routing (DDR) [44] algorithm is exploited by HARP to provide underlying supports. In DDR, nodes periodically exchange topology messages with their neighbors. A forest is constructed from the network topology by DDR in a distributed way. Each tree of the forest forms a zone. Therefore, the network is divided into a set of non-overlapping dynamic zones.

A mobile node keeps routing information for all other nodes in the same zone. The nodes belonging to different zones but are within the direct transmission range are defined as gateway nodes. Gateway nodes have the responsibility forwarding packets to neighboring zones. In addition to routing information for nodes in the local zone, each node also maintains those of neighboring zones.

As in ZRP, the intra-zone routing of HARP relies on an existing proactive scheme and a reactive scheme is used for inter-zone communication. Depending on whether the forwarding and the destination node are inside the same zone, the respective routing scheme will be applied.

2.3.3.3 The Zone-based Hierarchical Link State routing (ZHLS)

The Zone-based Hierarchical Link State routing (ZHLS) [45] is a hybrid routing protocol. In ZHLS, mobile nodes are assumed to know their physical locations with assistance from a locating system like GPS. The network is divided into non-overlapping zones based on geographical information.

ZHLS uses a hierarchical addressing scheme that contains zone ID and node ID. A node determines its zone ID according to its location and the pre-defined zone map is well known to all nodes in the network. It is assumed that a virtual link connects two zones if there exists at least one physical link between the zones. A two-level network topology structure is defined in ZHLS, the node level topology and the zone level topology. Respectively, there are two kinds of link state updates, the node level LSP (Link State Packet) and the zone level LSP. A node level LSP contains the node IDs of its neighbors in the same zone and the zone IDs of all other zones. A node periodically broadcast its node level LSP to all other nodes in the same zone. Therefore, through periodic node level LSP exchanges, all nodes in a zone keep identical node level link state information. In ZHLS, gateway nodes broadcast the zone LSP throughout the network whenever a virtual link is broken or created. Consequently, every node knows the current zone level topology of the network.

Before sending packets, a source firstly checks its intra-zone routing table. If the destination is in the same zone as the source, the routing information is already there. Otherwise, the source sends a location request to all other zones through gateway nodes. After a gateway node of the zone, in which the destination node resides, receives the location request, it replies with a location response containing the zone ID of the destination. The zone ID and the node ID of the destination node will be specified in the header of the data packets originated from the source. During the packet forwarding procedure, intermediate nodes except nodes in the destination zone will use inter-zone routing table, and when the packet arrives the destination zone, an intra-zone routing table will be used.

2.3.3.4 Comparison of ZRP, HARP and ZHLS

As zone based mobile ad hoc network routing protocols, ZRP, HARP and ZHLS use different zone construction methods, which have critical effect on their performance.

In ZRP, the network is divided into overlapping zones according to the topology knowledge for neighboring nodes of each node. In HARP, the network is divided into non-overlapping zones dynamically by DDR through mapping the network topology to a forest. For each node in HARP, the topology knowledge for neighboring nodes is also needed and the zone level stability is used as a QoS parameter to select more stable route. ZHLS assumes that each node has a location system such as GPS and the geographical information is well known, and the network is geographically divided into non-overlapping zones. The performance of a zone based routing protocol is tightly related to the dynamics and size of the network and parameters for zone construction. However, because zones heavily overlap, ZRP in general will incur more overhead than ZHLS and HARP.

All three zone-based routing protocols presented in this subsection use proactive routing for intra-zone communication and reactive routing for inter-zone packet forwarding. Performance of a zone based routing protocol is decided by the performance of respective proactive and reactive routing protocols chosen and how they cooperate each other.

2.3.4 Hierarchical Based Routing protocol:

In this type of protocols the choice of proactive and of reactive routing depends on the hierarchic level where a node resides. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The choice for one or the other method requires proper attributation for respective levels. HSR. CBRP, CEDAR

2.3.4 Hierarchical State Routing (HSR):

The Hierarchical State Routing (HSR) [47] is a multi-level cluster-based hierarchical routing protocol. In HSR, mobile nodes are grouped into clusters and a clusterhead is elected for each cluster. The clusterheads of low level clusters again organize themselves into upper level clusters, and so on. Inside a cluster, nodes broadcast their link state information to all others. The clusterhead summarizes link state information of its cluster and sends the information to its neighboring clusterheads via gateway nodes. Nodes in upper level hierarchical clusters flood the network topology information they have obtained to the nodes in the lower level clusters.

In HSR, a hierarchical address is assigned to every node. The hierarchical address reflects the network topology and provides enough information for packet deliveries in the network. Mobile nodes are also partitioned into logical subnetworks corresponding to different user groups. Each node also has a logical address in the form of <subnet, host>. For each subnetwork, there is a location management server (LMS) which records the logical addresses of all nodes in the subnetwork. LMSs advertise their hierarchical addresses to the top level of hierarchical clusters. The routing information, which contains LMSs' hierarchical addresses, is sent down to all LMSs too. If a source node only knows the logical address of the destination node, before sending a packet, the source node firstly checks its LMS and tries to find the hierarchical address of the destination's LMS. Then the source sends the packet to the destination's LMS, and the destination's LMS forwards the packet to the destination. Once the source knows the hierarchical address of the destination, it sends packets directly to the destination without consulting LMSs.

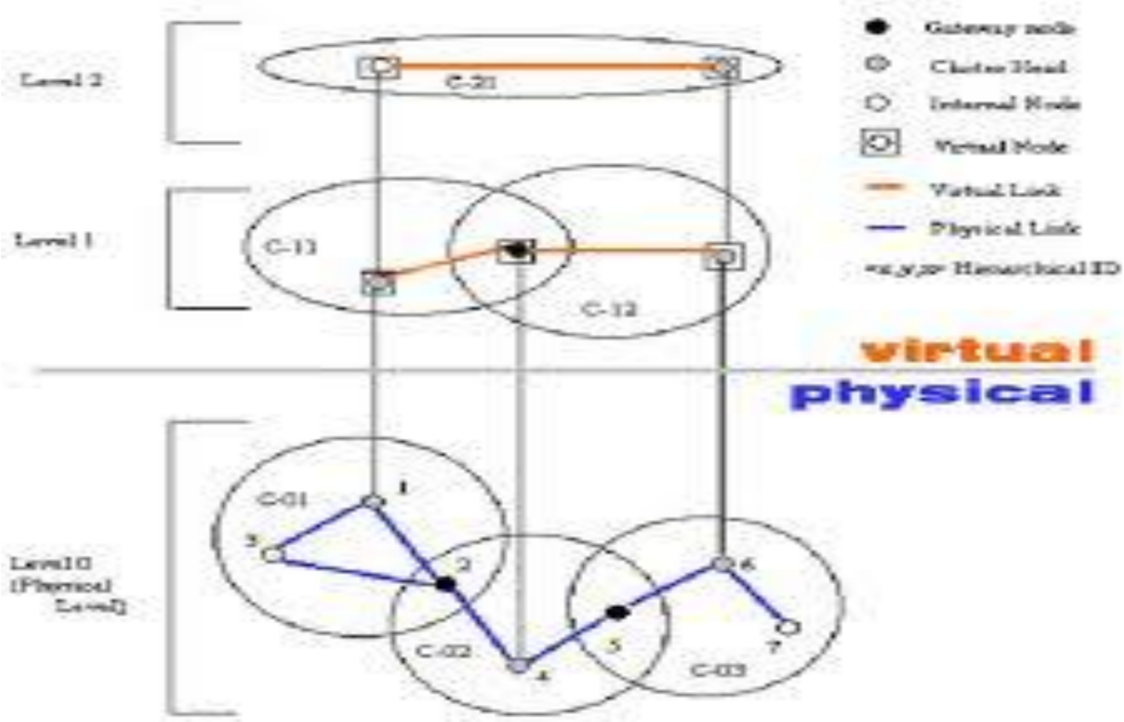


Figure 13: HSR routing Protocol

In HSR, logical addresses reflect the group property of mobile nodes and hierarchical addresses reflect their physical locations. Combining these addressing schemes can improve adaptability of the routing algorithm.

2.3.4.2 Cluster Based Routing Protocol (CBRP)

In the Cluster Based Routing Protocol (CBRP) [46], nodes are divided into clusters and the clustering algorithm is performed when a node joins the network. Before joining, a node is in the "undecided" state. The "undecided" node initiates the joining operation by setting a timer and broadcasts a Hello message. If a clusterhead receives the Hello message, it replies with a triggered Hello message. Receiving the triggered Hello message, the "undecided" node changes its state to "member" state. If the "undecided" node has bi-directional links to some neighbors but does not receive a message from a clusterhead before the local timer generates a timeout, it makes itself a clusterhead. Otherwise, the node remains in "undecided" mode and repeats the joining operation later.

In CBRP, every node maintains a neighbor table in which it stores the information about link states (uni-directional or bi-directional) and the state of its neighbors. In addition to the information of all members in its cluster, a clusterhead keeps information of its neighboring clusters, which includes the clusterheads of neighboring clusters and gateway nodes connecting it to neighboring clusters.

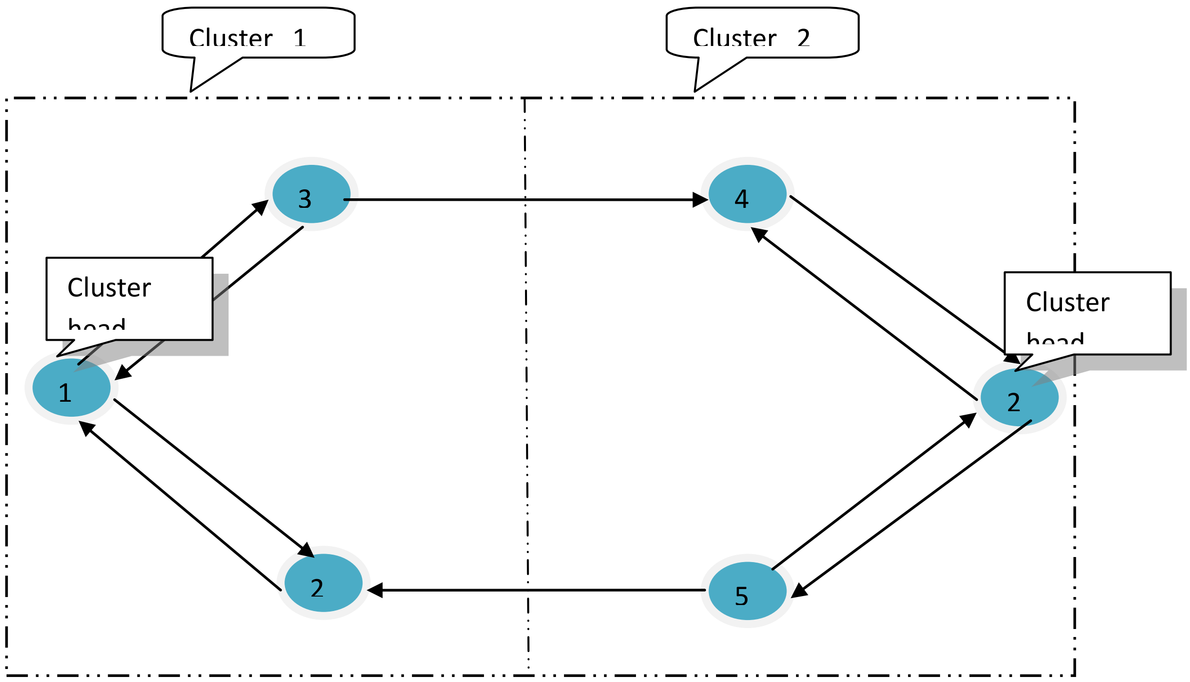


Figure 14: CBRP

If a source node wants to send a packet but has no active route which can be used, it floods route request to clusterhead of its own and all neighboring clusters. If a clusterhead receives a request it has seen before, it discards the request. Otherwise, the clusterhead checks if the destination of the request is in its cluster. If the destination is in the same cluster, the clusterhead sends the request to the destination, or it floods the request to its neighboring clusterheads. Source routing is used during the route search procedure and only the addresses of clusterheads on the route are recorded. The destination sends a reply including the route information recorded in the request if it successfully receives a route request. If the source doesn't receive a reply in the specified time period, it starts an exponentially backoff algorithm and sends the request later.

The shortening route is proposed in CBRP for performance optimization. Because CBRP uses a source routing scheme, a node gets all information about the route when receiving a packet. To reduce the hop number and adapt to network topology changes, nodes exploit route shortening to choose the most distant neighboring node in a route as next hop. Another optimization method exploited by CBRP is local repair. Whenever a node has a packet to forward and the next hop is not reachable, it checks the routing information contained in the packet. If the next hop or the hop after next hop in the route is reachable through one of its neighbors, the packet is forwarded through the new route.

2.3.4.3 Comparison of cluster based hierarchical routing protocols

This comparison presents Different clustering algorithms have been introduced to group mobile nodes and elect clusterheads in cluster based routing protocols. In HSR, hierarchical addressing is used and the network may have a recursive multi-level cluster structure. Moreover, a location management mechanism is used in HSR to map the logical address to the physical address. In CBRP, every node keeps information about its neighbors and a clusterhead maintains information about its members and its neighboring clusterheads. CBRP exploits the source routing scheme and the addresses of clusterheads along a route are recorded in the data packets.

2.3.5 Geographical Based Routing Protocols:

This type of protocols acknowledges the influence of physical distances and distribution of nodes to areas as significant to network performance. The protocols which comes under this type of category are as under:[76,83,87]

i. Location aided routing (LAR)
ii. Distance routing effect algorithm for mobility (DREAM)
iii. LANMAR

2.3.5.1 Location Aided Routing:

Like DSR, LAR is also on demand routing protocol. But it came with in the category of geographical/location aided on demand routing protocols. The main differences between LAR and DSR is that LAR sends location information in all packets to decrease the overhead of a future route performance of routing protocols, thus using location information for MNs to flood a route request packets for destination in a forwarding zone instead of the entire adhoc network. A node says x, on receiving a route request message, compares the desired destination with its own identifier. If there is a match, it means that the request is for a route to itself (i.e. node x). Otherwise, node x broadcast the request to its neighbour to avoid redundant transmission of route request once (repeated reception of a route request is detected using sequence numbers). The author of [48] purposes two methods used by the intermediate nodes between source S and destination D to determine the forwarding zone of a route request packet.

Method 1:

Our first scheme uses a request zone that is rectangular in shape. Assume that node S knows that node D was at location (Xd, Yd) at time t0. At time t1, node S initiates a new route discovery for destination D. We assume that node S also knows the average speed v with which D can move. Using this, node S defines the expected zone at time t1 to be the circle of radius R = v(t1 - t0) cantered at location (Xd, Yd). (As stated before, instead of the average speed, v may be chosen to be the maximum speed or some other function of the speed distribution.) In our first LAR algorithm, we define the request zone to be the smallest rectangle that includes current location of S and the expected zone (the circular region defined above), such that the sides of the rectangle are parallel to the X and Y axes. In figure 1(a), the request zone is the rectangle whose corners are S, A, B and C, whereas in figure 1(b), the rectangle has corners at point A, B, C and G – note that, in this figure, current location of node S is denoted as (Xs, Ys). The source node S can, thus, determine the four corners of the request zone. S includes their coordinates with the route request message transmitted when initiating route discovery. When a node receives a route request, it discards the request if the node is not within the rectangle specified by the four corners included in the route request. For instance, in figure 1(a), if node I receives the route request from another node, node I forwards the request to its neighbours, because I determines that it is within the rectangular request zone. However, when node J receives the route request, node J discards the request, as node J is not within the request zone (see figure 1(a). When node D receives the route request message, it replies by sending a route reply message (as in the flooding algorithm). However, in case of LAR, node D includes its current location and current time in the route reply message. When node S receives this route reply message (ending its route discovery), it records the location of node D. Node S can use this information to determine the request zone for a future route discovery. (It is also possible for D to include its current speed, or average speed over a recent time interval, with the route reply message. This information could be used in a future route discovery. In our simulations, we assume that all nodes know each other's average speed.)

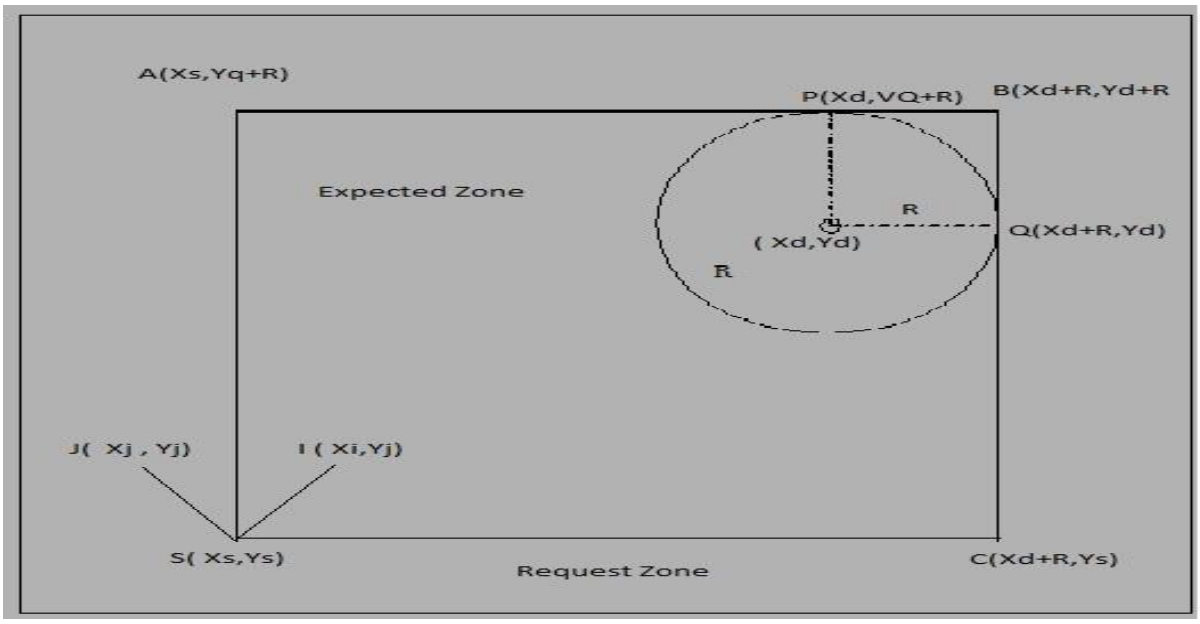


Figure 15(a)

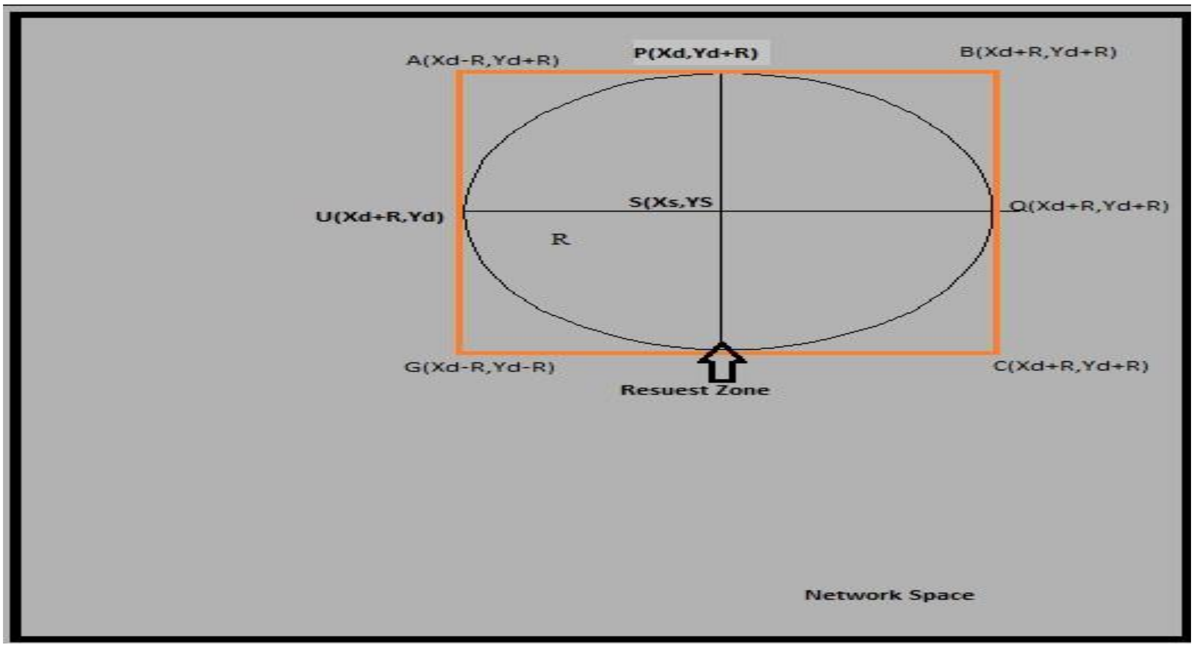


Figure 15(b)

Method 2:

In In LAR scheme 1, source S explicitly specifies the request zone in its route request message. In scheme 2, node S includes two pieces of information with its route request:

1. Assume that node S knows the location (Xd, Yd) of node D at some time t0 – the time at which route discovery is initiated by node S is t1, where t1 > t0. Node S calculates its distance from location (Xd, Yd), denoted as DISTs, and includes this distance with the route request message.

2. The coordinates (Xd, Yd) are also included with the route request.

When a node I receives the route request from sender node S, node I calculates its distance from location (Xd, Yd), denoted as DISTi, and:

1. For some parameters $\propto$ and , if σ (DISTs)+ β > DISTi, then node I forwards the request to its neighbors. When node I forwards the route request, it now includes DISTi and (Xd, Yd) in the route request (i.e., it replaces the DISTs value received in the route request by DISTi, before forwarding the route request).
2. Else $\propto$(DISTs)+ β< DISTi. In this case, node I discards the route request.

When some node J receives the route request (originated by node S) from node I, it applies a criteria similar to above: if node J has received this request previously, it discards the request. Otherwise, node J calculates its distance from (Xd, Yd), denoted as DISTj. Now,

1. Else $\propto$ (DISTi)+ $\beta <$ DISTj. In this case, node J discards the request.

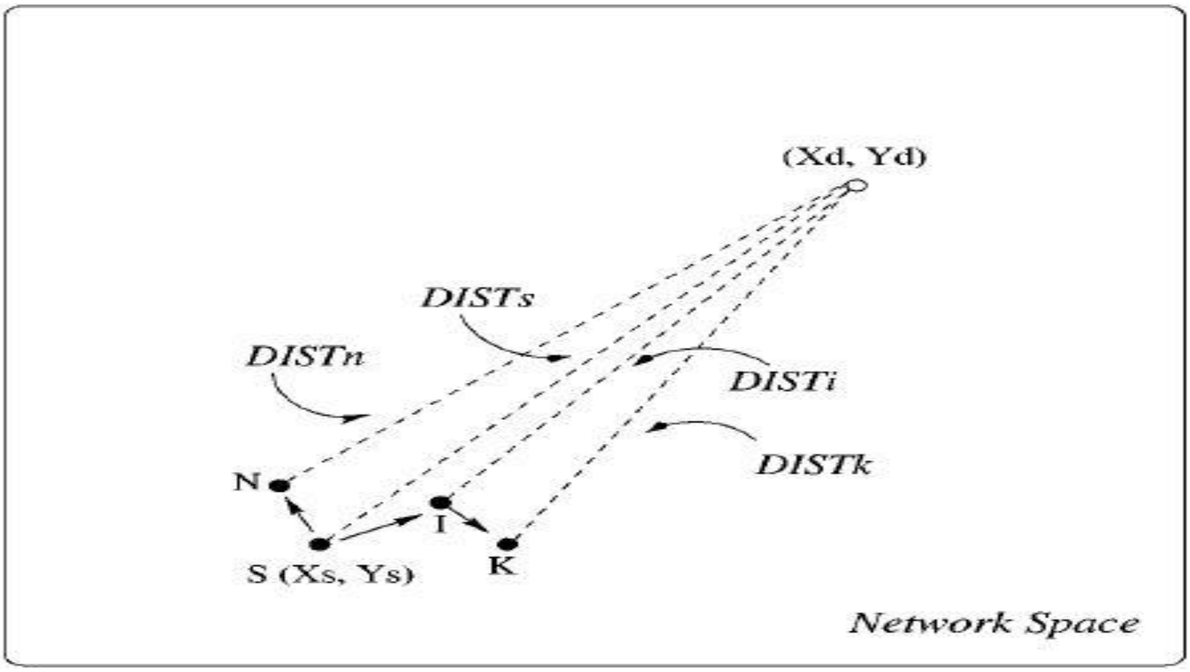


Figure 16: Location Aided Routing

2. The route request received from node I includes DISTi. If $\propto$ (DISTi) + β > DISTj, then node J forwards the request to its neighbors (unless node J is the destination for the route request). Before forwarding the request, J replaces the DISTi value in the route request by DISTj.

Thus, a node J forwards a route request forwarded by I(originated by node S), if J is "closer" to or "not much farther" from (Xd, Yd) than node I. For the purpose of performance evaluation, initially we use $\propto$ = 1 and β = 0 in the next section. Nonzero $\propto$ and β may be used to trade-off the probability of finding a route on the first attempt with the cost of finding the route. Nonzero $\propto$ and β may also be appropriate when location error is nonzero, or when the hosts are likely to move significant distances during the time required to perform route discovery. To see how the parameters of $\propto$ and β affect the routing overhead. Figure above illustrates the difference between the two LAR schemes. Consider figure (a) for LAR scheme 1. When nodes I and K receive the route request for node D (originated by node S), they forward the route request, as both I and K are within the rectangular request zone. On the other hand, when node N receives the route request, it discards the request, as N is outside the rectangular request zone. Now consider figure (b) for LAR scheme 2 (assume $\propto$ = 1 and β = 0). When nodes N and I receive the route request from node S, both forward the route request to their neighbors, because N and I are both closer to (Xd, Yd) than node S. When node K receives the route request from node I, node K discards the route request, as K is farther from (Xd, Yd) than node I. Observe that nodes N and K take different actions when using the two LAR schemes.

2.3.5.2 Distance routing effect algorithm for mobility (DREAM):

Distance routing effect algorithm for mobility (DREAM), one of the improved algorithms based on node position information, was suggested in Basagni et al., (1998). According to DREAM, the position information obtained by GPS of whole nodes in the network is stored in every node's routing table. This algorithm is a table driven algorithm since it holds information belonging to whole nodes. DREAM protocol [49,50,51,52] is a restricted flooding communication protocol used in unstructured architectures. Each node may maintain a location table about the position of all nodes of the network and frequently floods a location packet, called control packet, to update the position information maintained by its neighbours. Each location packet submitted by a node A to other nodes to update their location tables contains A's coordinates along with its speed and the time the location packet was transmitted. DREAM uses the principle of distance effect in which the location tables update frequency is determined by the distance of the registered nodes. In other words, the closer to another node, the more updates sent to this node. The frequency of sending a control packet is adjusted based on the moving speed of the source node S [52]. When the source node S wishes to send a message to a destination node D, it starts by looking for its location table and retrieves information about its geographical position. If the direction of D is valid, S sends the message to the all one hop neighbours in the forwarding zone determined by that direction. If no location information is available for D, then a recovery procedure must be executed by flooding partially or entirely the network in order to reach D. When a node A receives the message, it checks first if it is the node destination. If this is the case, it sends an acknowledgement to the source node. Otherwise, A repeats the same process by sending it to all one hop neighbours that are in the direction of D. Each of these nodes, in turn, repeats this process, if possible, until D is reached. To determine the forwarding zone in the direction of the node D, the source node S calculates the expected zone which contains D. Figure 3 shows an example of expected zone, i.e., the circle around the position of D. The radius r of this zone is set to (t1 − t0) vmax , where t0 is the timestamp of the position information that S has about D, t1 is the current time, and vmax is the local known speed that the node D may travel in ad hoc network. After determining the expected zone, the node S defines its forwarding zone which is the region enclosed by an angle whose vertex is at S and whose sides are tangent to the expected zone calculated for D and then sends the packet, destined for D, to all its neighbours in the forwarding zone [51]. In DREAM, exchanging nodes' coordinates instead of exchanging complete link state or distance vector information helps reducing the occupied bandwidth. Moreover, since DREAM uses the distance effect principle described above, it can perform well in dynamic mobile ad hoc networks.

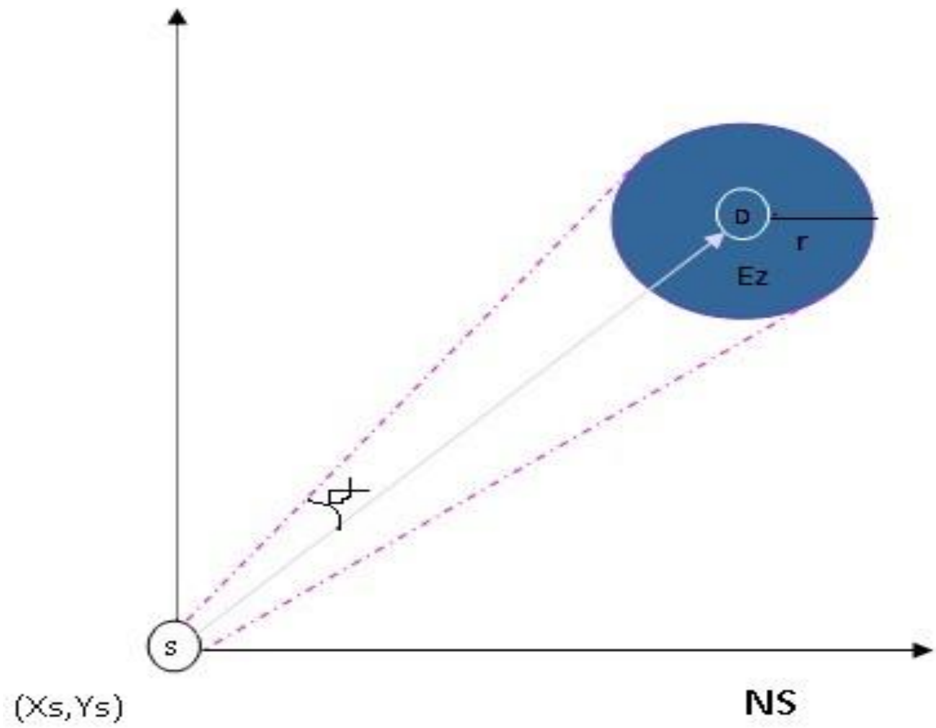


Figure 17: DREAM

2.3.5.3 LANMAR:

In the original landmark scheme for wired networks proposed in [53], the predefined hierarchical address of each node reflects its position within the hierarchy and helps find a route to it. Each node knows the routes to all the nodes within it hierarchical partition. Moreover, each node knows the routes to various "landmarks" at different hierarchical levels. Packet forwarding is consistent with the landmark hierarchy and the path is gradually refined from top level hierarchy to lower levels as a packet approaches destination. LANMAR borrows from [53] the notion of landmarks to keep track of logical subnets. A subnet consists of members which have a commonality of interests and are likely to move as a "group" (e.g., brigade in the battlefield, colleagues in the same organization, or a group of students from same class). A "landmark" node is elected in each subnet. The routing scheme itself is modified version of FSR. The main difference is that the FSR routing table contains “all” nodes in the network, while the LANMAR routing table includes only the nodes within the scope and the landmark nodes. This feature greatly improves scalability by reducing routing table size and update traffic O/H. When a node needs to relay a packet, if the destination is within its neighbour scope, the address is found in the routing table and the packet is forwarded directly. Otherwise, the logical subnet field of the destination is searched and the packet is routed towards the landmark for that logical subnet. The packet however does not need to pass through the landmark. Rather, once the packet gets within the scope of the destination, it is routed to it directly. The routing update exchange in LANMAR routing is similar to FSR. Each node periodically exchanges topology information with its immediate neighbours. In each update, the node sends entries within its fisheye scope. It also piggy-backs a distance vector with size equal to the number of logical subnets and thus landmark nodes. Through this exchange process, the table entries with larger sequence numbers replace the ones with smaller sequence numbers.

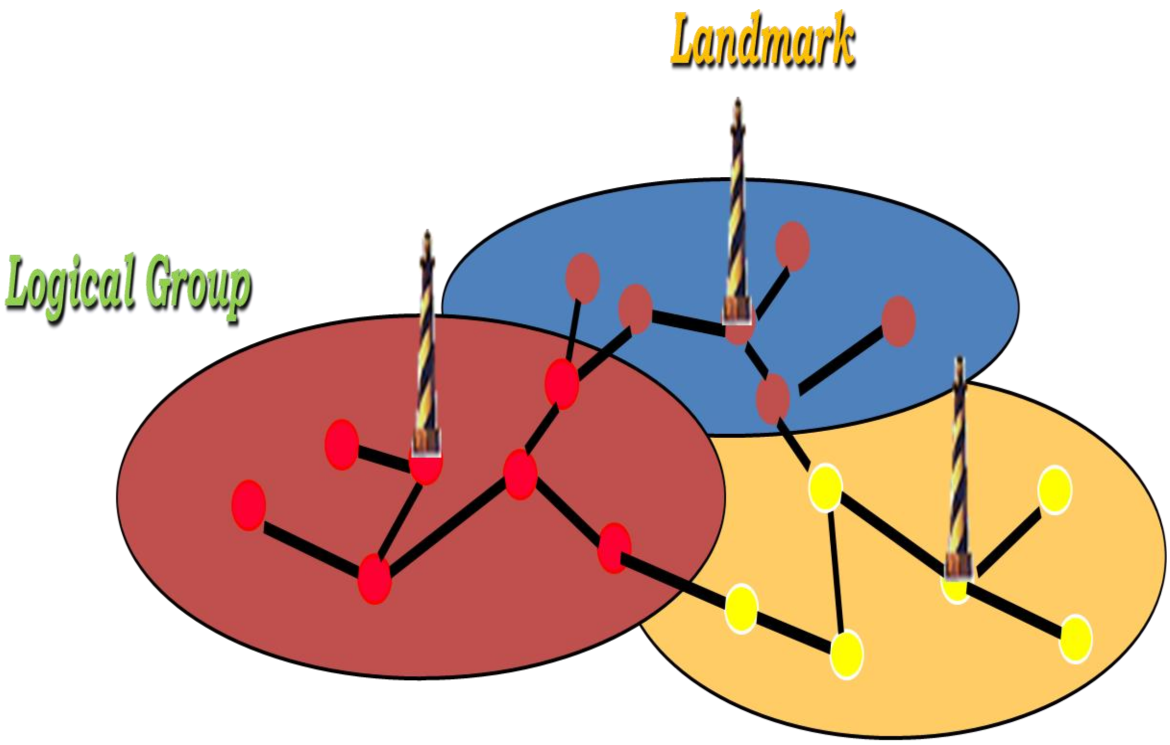


Figure 18: LANMAR

2.3.6 Power Based Routing Protocols:

Energy required to transmit a signal is approximately proportional to d∝, where d is the distance and is the attenuation factor or path loss exponent, which depends on the transmission medium. When ∝ = 2 (which is the optimal case), transmitting a signal half the distance requires one fourth of the energy and if there is a node in the middle willing spend another fourth of its energy for the second half, data would be transmitted for half of the energy than through a direct transmission - a fact that follows directly from the inverse square law of physics.

2.3.6.1 Power Aware Controlled Routing Protocol:

PCAR is a power controlled routing protocol. It consists of two parts: Bellman-Ford routing and proportion- integral power control.

1) Bellman-Ford Routing: PCAR constructs routing tables through the classical distributed Bellman-Ford algorithm. As with DSDV [5], the PCAR protocol utilizes sequence numbers to avoid the formation of loops. PCAR can forward a packet along the shortest path in the sense of number of hops, since each PCAR node stores the next hop of the shortest path for each destination

2) Proportion-Integral Power Control: We implement PIPC [4] in PCAR for power control. The power control algorithm accepts the routing table as its input. The derived topology is of course also reflected in the routing table, i.e., the derived topology is fed back to the input of the power control algorithm. PCAR adjusts the transmission power such that the derived topology is between RNG and GG.

Routing Table and Forwarding Algorithm The routing table of each node u has the format RTu = {(destID, destP os, transPower, hops, nextHop, entryStatus, seqNum, routeChanged, lastModified), where RTu denotes the routing table of node u, destID is the identification of a destination node, destP os is the position of that destination, transPower is the transmission powerof that destination, hops is the number of hops from node u to that node, nextHop is the next hop on the shortest path, entryStatus is used to handle the asymmetry problem, seqNum is the sequence number indicating timeliness, routeChanged indicates whether the route is changed or not, and lastModified records the last time the entry was modified. It is important to note that lastModified is node u’s time, and hence PCAR does not require that the network should be synchronized.

The forwarding algorithm at each node u is described as follows.

1. ForwardPacket(packet, u){
2. if (u is the destination of packet)
3. Send packet to the upper layer;
4. else{
5. Find the entry e in RTu such that e.destID is the destination of packet;
6. Forward packet to e.nextHop;
7. }
8. }

Each usable data link should be symmetric, i.e., node u is a neighbor of v if and only if node v is a neighbor of u. Asymmetric communication links are impractical, because many communication primitives become unacceptably complicated. In PCAR, the transmission power may differ significantly from one node to another, which generates a great number of unidirectional links. Even if all nodes use a common transmission power, there may still exist many unidirectional links due to asymmetry of radio path loss in the real-world environment. It is well known that some MAC protocols have taken care of the asymmetry problem. For example, IEEE 802.11 solves the problem through the RTS/CTS handshake for unicast. However, to the best of our knowledge, no MAC protocols take asymmetry into account for the case of broadcasting. PCAR constructs routing tables through broadcasts, which may well result in asymmetric links. To handle that problem, PCAR utilizes entryStatus whose value may be one of LOST, INLINKED, BICONNECTED, and INLINKED MULTIHOP BICONNECTED. Suppose that there is an entry with respect to node v in u's routing table. LOST indicates that node u cannot hear anything of node v. INLINKED implies a unidirectional link from v to u (whether bidirectional is not known as yet). BICONNECTED means that each link on the established path from u to v is bidirectional. INLINKED MULTIHOP BICONNECTED represents that u and v are BICONNECTED through two or more hops and there exists a unidirectional link from v to u. Therefore, only those BICONNECTED and INLINKED MULTIHOP BICONNECTED entries are available when forwarding packets. Suppose node u has received the routing table of node v, the asymmetry problem at each node u is handled as follows.

```
HandleAsymmetry  (RTu,RTB v ){
if (there exists an entry in RTB v whose destID is u, and ((entryStatus ==INLINKED or INLINKED MULTIHOP BICONNECTED) or (entryStatus ==BICONNECTED and hops == 1))){
 /* Link (v, u) is bidirectional.*/
 for (each BICONNECTED or INLINKED MULTIHOP BICONNECTED entry of RTB v )
 Update RTu as ConstructRoutingTable() does;
 }
 else{
 /* Link (v, u) is unidirectional.*/
 Add the INLINKED property to the entry with respect to v in RTu;
 Update other properties of that entry.
 }
 }
```

Line 10 includes a process that is something like ConstructRoutingTable. It is important to note that the handling-asymmetry algorithm should be integrated into the procedure of constructing routing tables. But here, we introduce them separately; otherwise, one is so easily confused.

Power Control

PCAR employs the PIPC algorithm to adjust transmission power such that the derived topology is between RNG and GG. The RNG derived from a given graph G = (V,E) consists of all links (u, v) ∈ E such that the intersection of the two circular areas centered at u and v and with radius d(u, v) does not contain any node w from V , where d(u, v) is the Euclidean distance between u and v. The GG contains link (u, v) if and only if disk(u, v) contains no other nodes of V , where disk(u, v) is the disk with edge (u, v) as its diameter. For each node, the transmission radius in RNG and GG is denoted by rngRadius and ggRadius, respectively. The transmission power of each node is adjusted such that the transmission radius is in the range of [rngRadius, ggRadius]. The PIPC algorithm at each node u is described as follows.

```
PIPC(RTu(i)){
Compute rngRadius(i) and ggRadius(i);
Estimate control error e(i);
Determine parameters KP (i), KI (i), and ζ(i);
 Δp(i) = KP (i)(e(i) − e(i − 1)) + KI (i)e(i) + ζ(i);
Add Δp(i) to u.transPower;
```

}

In the PIPC algorithm, RTu(i) is the routing table of node u at digital time i, e is the control error, KP is the proportion gain, KI is the integral gain, and ζ is a modification term.

2.3.6.2 PARO

Prior to transmitting a packet, a node updates its packet header to indicate the power required to transmit the packet. A node overhearing another node's transmission can then use this information plus, a localized measure of the received power, to compute (using a propagation model) the minimum transmission power necessary to reach the overheard node. In this simple manner, nodes can learn the minimum transmission power toward neighboring nodes. PARO does not, however, maintain routes to other nodes in the network in advance but discovers them on a per-node on-demand basis. This approach has the benefit that signalling packets, if any, are transmitted only when an unknown route to another node is required prior to data transmission, thus reducing the overall power consumption in the network. At first the operation of PARO may seem counter-intuitive because in the first iteration of PARO the source node communicates with the destination node directly without involving any packet forwarding by intermediate nodes (i.e., redirectors). Any node capable of overhearing both source and destination nodes can compute whether packet forwarding can reduce the transmission power in comparison to the original direct exchange between source and destination nodes. When this is the case an intermediate node may elect to become a redirector and send a route-redirect message to the source and destination nodes to inform them about the existence of a more power efficient route to communicate with each other. This optimization can also be applied to any pair of communicating nodes; thus, more redirectors can be added to a route after each iteration of PARO with the result of further reducing the end-to-end transmission power. PARO requires several iterations to converge toward a final route that achieves the minimum transmission power, as defined below equation.

$$P_k = \sum_{i=0}^{nk} \frac{T_{i,i+1}L + T_{i+1,i}L}{C}$$

.

Where The factor Ti,j in equation is the minimum transmission power at node i such that the receiver node j along route k is still able to receive the packet correctly , while Nk is the number of times a data packet is forwarded along route k including the source node. The PARO model comprises three core algorithms that support overhearing, redirecting and route-maintenance, as shown in figure. The overhearing algorithm receives packets overheard by the MAC and creates information about the current range of neighboring nodes. Overheard packets are then passed to the redirecting algorithm, which computes whether route optimization through the intermediate node would result in power savings. If this is the case, the node elects to become a potential redirector, transmits route redirect messages to the communicating nodes involved and creates appropriate entries in its redirect table. The overheard packet is then processed by the packet classifier module with the result that one of the following actions is taken: (i) the packet is passed to the higher layers if both MAC and IP addresses match; (ii) the packet is dropped if neither MAC nor IP addresses match; or (iii) the packet is forwarded to another node when only the MAC addresses match. In the latter case, PARO searches the redirect table to find the next node en route and then searches the overhear table to adjust the transmission power to reach that node. When PARO receives a data packet from the higher layers it searches the redirect table to determine if a route toward the destination node exists. If this is not the case, PARO searches the overhear table to determine if there is any transmission power information related to the destination node available. If this is not the case, PARO transmits the packet using the maximum transmission power anticipating that the receiving node is located somewhere in the neighborhood. Once the destination node replies with a packet of its own then PARO's route optimization follows as described previously. PARO relies on data packets as the main source of routing information in the network. When nodes are mobile and no data packets are available for transmission, a source node may be required to transmit explicit signalling packets to maintain a route. The role of the route maintenance algorithm is to make sure that a minimum flow of packets is transmitted in order to maintain a route when there are no data packets available to send at the transmitter.

Chapter 3

Propagation Models

Chapter 3

Propagation Models

3.1 Propagation Models:

The transmission path between the transmitter and receiver can vary from a direct line-of-sight to the one that is heavily obstructed by towers, buildings and mountains. More obstruction along the propagation path causes more reflection, diffraction and scattering of the signal being transmitted which deteriorates the network performance. Also, due to mobility, propagation characteristics of a Ad hoc networks vary from place to place, and from time to time. The diverse nature of radio channel causes a fundamental limitation on the performance of the network. While methods exist to closely model exact nature of propagation phenomenon, these methods require a large amount of detailed information specific to its terrain, time and operating environment specific data[11] [10], limiting general applications of the model to certain types. An alternative, statistical propagation models are more commonly in use for the evaluation of mobile radio channels. Radio wave propagation is largely attributed to reflection, diffraction and scattering. The transceiver antennas of mobile devices are small and provide a low clearance. As a result, direct line-of-sight (LOS) path is usually absent causing the propagated wave to suffer from a diffraction loss. Due to multiple reflections, the received signal becomes the superimposition of direct signal as well as reflected, scattered and diffracted signal characterizing multipath reception[10][9] also called as multipath propagation. The signals received are called as the multipath waves or multipath signal. The strength of the wave decreases as the distance between the transmitter (T) and receiver (R) increases.

The propagation models are usually characterized as: non-fading and fading. The non-fading propagation models account for the fact that a radio wave has to cover a growing area when the distance to the sender is increasing. Examples are free-space and two ray ground [11, 12]. On the other hand, fading propagation models calculate the signal strength depending on node's movements or small time frames. There is signal attenuation due to different objects (large scale fading) as well as variability due to multipath (small scale fading).Large scale fading is characterized by a large distance separating transmitter and receiver, while in small scale fading, the receiver gets multiple copies of a signal which interfere with each other and causes fluctuation is signal strength over a short distance [11]. Several statistical models are used to describe fading in wireless environments and the most frequently used distribution for large scale fading is shadowing, while for small scale fading, Rayleigh, and Ricean [14, 15] can be used. In these models, the instantaneous received power of a given signal may be treated as a stochastic random variable that varies with distance and the selection of a particular model associates a known probability distribution with this random variable.

3.2 Non Fading Model:

In non-fading models, the received signal power Pr is calculated for every transmission between two nodes with the chosen propagation model. The channel model distinguishes primarily between three cases. In case Pr is greater than the receiving threshold RXThresh, the transmission has enough power to allow proper reception at the receiver side. Other simultaneous transmissions with reasonable transmission powers may certainly interfere with this transmission and make a correct reception impossible. If Pr is below RXThresh but greater than the carrier sense threshold CSThresh, the receiving node must drop the packet. However, the receiving power of this transmission is still strong enough to interfere with other simultaneous transmissions. Consequently, these interfered packets are also invalid and nodes must drop them as well. Transmissions with receiving powers Pr smaller than CSThresh do not even obstruct other simultaneous transmissions at the same node. Two different propagation models are considered as non-fading: the free space model and the two ray ground models [12, 15, 18].

3.2.1 Free Space Model:

The Free Space model represents by equation (1) a signal propagating through open space, with no environmental effects. It has one parameter, called "line of sight". With this parameter off, terrain has no effect on propagation. With it on, the model uses terrain data solely to determine if a line-of-sight (LOS) exists between the transmitting and receiving antennas. If there is no LOS, the signal is blocked entirely and no communication takes place.

$$Pr = \frac{Pt \,.\, Gt \,.\, Gr.\, \lambda^2}{(4\pi)^2 d^2\, L} \qquad (1)$$

Pr the received signal is power (in Watt), Pt Where receiving and the transmitting antennas respectively. λ is the wave length, L is the system loss, and d is the distance between the transmitter and the receiver. According to [14], a single direct path between the communicating partners exists seldom at larger distances.

3.2.2 Two ray model:

The free space model described above assumes that there is only one signal pat from the transmitter to the receiver. But in reality, the signal reaches the receiver through multiple paths (because of reflection, refraction and scattering) the two path model tries to capture this phenomenon. The model assumes that the signal reaches the receiver through two paths, one line of sight path, and the other the path through which the reflected (or refracted, or scattered) wave is received. According to the two path model, the received power is given by

$$Pr = \frac{P_t \,.\, G_t \,.G_r}{d^2} .(h_t \; h_r)^2 \qquad (2)$$

Where Pt is the transmitted power, Gt and Gr represent the antenna gain at the transmitter and the receiver respectively, d is the distance between the transmitter and the receiver, and ht and hr are the heights of the transmitter and the receiver, respectively.

3.3 Non-Fading Models:

Statistical models are used to accurately predict the fading effect. In large scale fading, the shadowing model shows how the signal strength fades with distance according to power law and reflects the variation of power at a distance. In small scale fading, a fading in which the reflected signal components reaching the receiver are of almost equal strength is called a Rayleigh fading and the one in which there is one principal component that has higher contribution towards signal reception is called Ricean fading. The following is based on [19,20].

3.3.1 Rician model:

For fast fading, random variable descriptions are obtained through consideration of the behaviours of the total received fields. Fast fading results due to interference among signals propagating over many paths between transmitter and receiver. Two distinct cases involving fast fading occur: situations in which a dominant line-of-sight path exists between Transmitter and receiver, and situations in which a dominant line-of-site path does not exist. In the former case, multipath reflected fields are added to the direct line-of-sight path, while in the latter, only the multipath signals are received. In both cases we will assume that the number of multipath signals received becomes large, so that the received field, which is a sum of contributions from these paths, approaches a Gaussian random variable. Using time harmonic analysis, we can represent the received field in terms of its real and imaginary components, both of which will be Gaussian random variables. In addition, for a sufficiently large number of multipath terms, the phase of the total of the multipath contributions will be random (excluding the line-of-sight path), so that the real and imaginary field components of the multipath field are independent of one another. The random phase behaviour of the multipath fields implies that the average multipath field received is zero, although significant variations can be observed in a given measurement. Fast fading effects are most conveniently modeled by treating the received power, and not the path loss, as the random variable of interest. In the case with a dominant line-of sight path, we describe the average received power in the absence of fast fading effects as Pm (in Watts, not decibels). The empirical path loss methods along with a statistical model of slow fading (if desired) combined with the Friis formula can be utilized to estimate Pm in a given problem. To model fast fading effects, we assume that an additional fast fading power Pf is added to Pm to obtain the mean power received:

$$P\ rec,\ mean = Pf + Pm \qquad ...... (3)$$

again in Watts. It was shown by Rice in 1944 that the appropriate pdf for the total power received is

$$f_p(P) = 1/P_f e^{-(Pm+P)/Pf}\ I_0(2\sqrt{PmP\ /pf})$$

Which of course applies for p > 0 only. The quantity I_0 represents the modified Bessel function of zeroth order; routines and tables for computing this function are widely available. For Pf = 1 Watt and for varying values of Pm in Watts, indicated in the legend. It is not surprising the pdfs are cantered around the value of Pm specified. It is somewhat surprising that the width of the pdf's increases for fixed Pf as Pm is increased. Given the above pdf, the standard deviation of the receiver power can be found to be

$$\sigma P = Pf\,(Pf + 2Pm) \qquad (5)$$

The inclusion of Pm in this equation confirms the increasing width of the pdf functions as Pm is increased.

3.3.2 Rayleigh fading model:

The phase of each path can change by 2π radian when the delay $\tau_n(t)$ changes by 1/fc. If f_c is large, relative small motions in the medium can cause change of 2π radians. Since the distance between the devices are much larger than the wavelength of the carrier frequency, it is reasonable to assume that the phase is uniformly distributed between 0 and 2π radians and the phases of each path are independent .When there are large number of paths, applying Central Limit Theorem, each path can be modeled as circularly symmetric complex Gaussian random variable with time as the variable. This model is called Rayleigh fading model. A circularly symmetric complex Gaussian random variable is of the form,

$$Z= X+jY$$

Where real and imaginary parts are zero mean independent and identically distributed (iid) Gaussian random variables. For a circularly symmetric complex random variable Z,

$$E[Z] = E[\ e^{j\theta}Z] = e^{j\theta}E[Z]$$

The statistics of a circularly symmetric complex Gaussian random variable is completely specified by the variance,

$$\sigma^2 = E[Z^2]$$

The magnitude $|Z|$ which has a probability density is called a Rayleigh random variable.

$$P(z) = \frac{z}{\sigma^2}\, e^{\frac{-x^2}{2\sigma^2}} \quad , x>0$$

This model, called Rayleigh fading model, is reasonable for an environment where there are large number of reflectors.

3.3.3 Shadowing fading Model:

The free space model and the two-ray model predict the received power as a deterministic function of distance. They both represent the communication range as an ideal circle and predict the mean received power at distance “d”. In reality, the received power at certain distance is a random variable due to multipath propagation effects, which is also known as fading effects. A more general and widely-used model is the shadowing model. The shadowing model consists of two parts. The first one is known as path loss model, which predicts the mean received power at distance “d”. It uses a close-in distance “d0“as a reference. Mean received power is computed relative to Pr(d0) as shown below:

$$\frac{P_r(d_0)}{P_r(d)} = (\frac{d}{d_0})^{\beta} \quad \text{…. Equation 4}$$

Where β is called the path loss exponent and is usually empirically determined by field measurement. From Equation 4 we know that β = 2 for Free space propagation model. Following table gives some values of β. Larger values correspond to more obstructions and hence faster decrease in average received power as distance becomes larger. Pr(d0) can be computed from Equation 1.

Environment		β
Outdoor	Free space	2
	Shadowed urban area	2.7 to 5
Indoor	Line-of-sight	1.6 to 1.8
	Obstructed	4 to 6

Table 2 : Values of path loss exponent β

The path loss is usually measured in dB. So from Equation 4 we have

$$\left[\frac{P_r(d)}{P_r(d_0)}\right] = \text{-}10\beta\log\left(\frac{d}{d_0}\right) \quad \text{….} \quad \text{equation 5.}$$

The second part of the shadowing is known as log-normal shadowing model. It reflects the variation of the received power at certain distance. It is a log-normal random variable, that is, it is of Gaussian distribution if measured in dB. The overall shadowing model is represented by Equation 6

$$\left[\frac{P_r(d)}{P_r(d)}\right]_{\beta} = \text{-}10\beta\log\left(\frac{d}{d_0}\right) + X_{dB} \quad \text{....... equation 6}$$

Where XdB is a Gaussian random variable with zero mean and standard deviation σdB. σdB is called the shadowing deviation and is obtained by measurement. Following table shows some values of σdB.

Environment	σdB
Outdoor Office	4 to 12
Office, hard partition	7
Office,	9.6

hard partition	
Factory, line-of-sight	3 to 6
Factory, obstructed	6.8

Table 3: Values of shadowing deviation σdB

The shadowing model extends the ideal circle model to a richer statistic model: nodes can only probabilistically communicate when they are near the edge of the communication range. Before using the shadowing model the user should select the values of path loss exponent β and the shadowing deviation σdB according to the simulated environment.[17]

Chapter 4

Ns-2 and its implications

Chapter 4

Ns-2 and its Implications

NS is a discrete event simulator targeted at networking research. It provides substantial support for TCP routing and multicast protocols over wired and wireless networks. Using Xgraph (A plotting program) we can create graphical representation of simulation results. All the work is done under Linux and windows platforms. The windows platform uses Cygwin for the support.

4.1 ABOUT NS 2

ns is an object oriented simulator, written in C++, with an OTcl interpreter as a frontend. ns uses two languages because simulator has two different kinds of things it needs to do. On one hand, detailed simulations of protocols require a systems programming language which can efficiently manipulate bytes, packet headers, and implement algorithms that run over large data sets. For these tasks run-time speed is important and turn-around time (run simulation, find bug, fix bug, recompile, re-run) is less important. On the other hand, a large part of network research involves slightly varying parameters or configurations, or quickly exploring a number of scenarios. In these cases, iteration time (change the model and re-run) is more important. Since configuration runs once (at the beginning of the simulation), run-time of this part of the task is less important. ns meets both of these needs with two languages, C++ and OTcl .C++ is fast to run but slower to change, making it suitable for detailed protocol implementation. OTcl runs much slower but can be changed very quickly (and interactively), making it ideal for simulation configuration.

In NS-2, the frontend of the program is written in TCL(Tool Command Language). The backend of NS-2 simulator is written in C++ and when the tcl program is compiled, a trace file and nam file are created which define the movement pattern of the nodes and keeps track of the number of packets sent, number of hops between 2 nodes, connection type etc at each instance of time. In addition to these, a scenario file defining the destination of mobile nodes along with their speeds and a connection pattern file(CBR file) defining the connection pattern, topology and packet type are also used to create the trace files and nam files which are then used by the simulator to simulate the network. [23][24] Also the network parameters can be explicitly mentioned during the creation of the scenario and connection-pattern files using the library functions of the simulator.

4.2 BASIC INSTALLATION STEPS

(1) NS-2.31 is extracted in the home folder or folder in which it is to be installed
(2) Then TCL and TK packages are installed using the following command.
(i) Sudo apt-get install tcl 8.4-dev tk 8.4-dev
(ii) sudo apt-get install build-essential autoconf automake libxmu-dev
(3) Now NS-2.31 is ready to be installed
(4) “bashrc” file is edited by adding the following variables and their attributes.

```
# LD_LIBRARY_PATH
OTCL_LIB=/your/path/ns-allinone-2.31/otcl-1.13
NS2_LIB=/your/path/ns-allinone-2.31/lib
X11_LIB=/usr/X11R6/lib
USR_LOCAL_LIB=/usr/local/lib
export
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$OTCL_LIB:$NS2_LIB:$X11_LIB:$USR
_LOCAL_LIB
# TCL_LIBRARY
TCL_LIB=/your/path/ns-allinone-2.31/tcl8.4.14/library
USR_LIB=/usr/lib
export TCL_LIBRARY=$TCL_LIB:$USR_LIB
# PATH
XGRAPH=/your/path/ns-allinone-2.31/bin:/your/path/ns-allinone-
2.31/tcl8.4.14/unix:/your/path/ns-allinone-2.31/tk8.4.14/unix
NS=/your/path/ns-allinone-2.31/ns-2.31/
NAM=/your/path/ns-allinone-2.31/nam-1.13/
PATH=$PATH:$XGRAPH:$NS:$NAM
```

(5) It is immediately made effective by the command ” $ source ~/.bashrc”
(6) To confirm NS is installed ns is typed on konsole which gives a “%” symbol
(7) It is validated by the command

```
$ cd ns-2.31
$ ./validate
```

[24]

4.3 DEFINING GLOBAL VARIABLES

```
set ns_ [new Simulator] #creates a new simulator instance
set topo [new Topography] #creates a new topology
$topo load_flatgrid 670 670 #defines it in 670X670 area
```

Here set command is used to create a global variable. The first argument is the variable name (ns_, topo, etc.). the second argument is used to get the value of the variable. It may be a constant or a function whose return value is assigned to the variable. To access a variable we use $var_name, where var_name is the name of the variable.[24]

4.4 DEFINING STANDARD NS/NAM TRACE

To run the output of the program in an animator we need a nam file, and to analyze the output we need trace file. So the program must output certain files called nam file and trace file. We can do so by the following commands:

```
Set tracefd [open demo.tr w]
$ns_ trace-all $tracefd
Set namtrace [open demo.nam w]
$ns_ namtrace-all-wireless
$namtrace 670 670
```

The above commands opens two files called demo.tr and demo.nam and initialize them. [24]

Example for mobile node configuration

We can configure a mobile node by following codes.

```
$ns_node-config -adhocRouting [choose protocol]\
-llType LL \
-macType Mac/802_11\
-ifqLen 50 \
-ifqType Queue/DropTail/PriQueue \
-antType Antenna/OmniAntenna \
-propType Propagation/TwoRayGround \
-phyType Phy/WirelessPhy \
-channelType Channel/WirelessChannel \
-topoInstance $topo
-agentTrace ON \
-routerTrace OFF \
-macTrace OFF
```

[23][24]

4.5 TRAFFIC AND MOVEMENT

We can also define the traffic and movement pattern in separate files called CBR file and scenario file respectively. Cbr file can be created by using a tcl program called cbrgen.tcl which is present in the directory "ns-2/indep-utils/cmu-scen-gen/". To define the movement we use an exe file called setdest present in the folder "ns-2/indep-utils/cmu-scen-gen/setdest/". The scenario and cbr files are generated by using the following commands in the appropriate directory respectively.

```
./setdest -n <num_of_nodes> -p pausetime -s <maxspeed> -t <simtime> -x <maxx> -y
<maxy>
ns cbrgen.tcl [-type cbf|tcp] [-nn nodes] [-seed seed] [-mc connections] [-rate rate]
```

[23][24].

4.6 Simulation in NS2

In this section, we have taken a protocol OFSP and have shown how we can implement the OFSP with different varying parameter in NS2.

4.6.1 Setting network topology

The OTcl code to set up the required network topology is shown in Listing 1 and shown as seen in NAM in Figure 4.2.1.(1111)

```
set ns_ [new Simulator]

set node(0) [$ns_ node];

set node(1) [$ns_ node];

set node(2) [$ns_ node];

set node(3) [$ns_ node];

set node(4) [$ns_ node];

set node(5) [$ns_ node];

set node(6) [$ns_ node];

set node(7) [$ns_ node];

set node(8) [$ns_ node];


# Set some aliases

set voip1 $node(0)

set voip2 $node(1)

set httpuser $node(2)

set server $node(3)


# labels and colours for nam

$node(4) label "LER_0"

$node(5) label "LER_1"

$node(6) label "LSR_2"

$node(7) label "LSR_3"

$node(8) label "LSR_4"

$voip1 color red

$voip1 label "VoIPUser1"
```

$voip2 color red

$voip2 label "VoIPUser2"

$httpuser color blue

$httpuser label "HttpUser"

$server color blue

$server label "Server"

Create links

ns_ duplex-link $node(0) $node(4) 44.736Mb 1ms DropTail

$ns_ duplex-link $node(1) $node(5) 44.763Mb 1ms DropTail

$ns_ duplex-link $node(2) $node(4) 44.763Mb 1ms DropTail

$ns_ duplex-link $node(3) $node(5) 44.763Mb 1ms DropTail

$ns_ duplex-link $node(4) $node(6) 1.544Mb 1ms DropTail

$ns_ duplex-link $node(4) $node(7) 1.544Mb 1ms DropTail

$ns_ duplex-link $node(5) $node(6) 1.544Mb 1ms DropTail

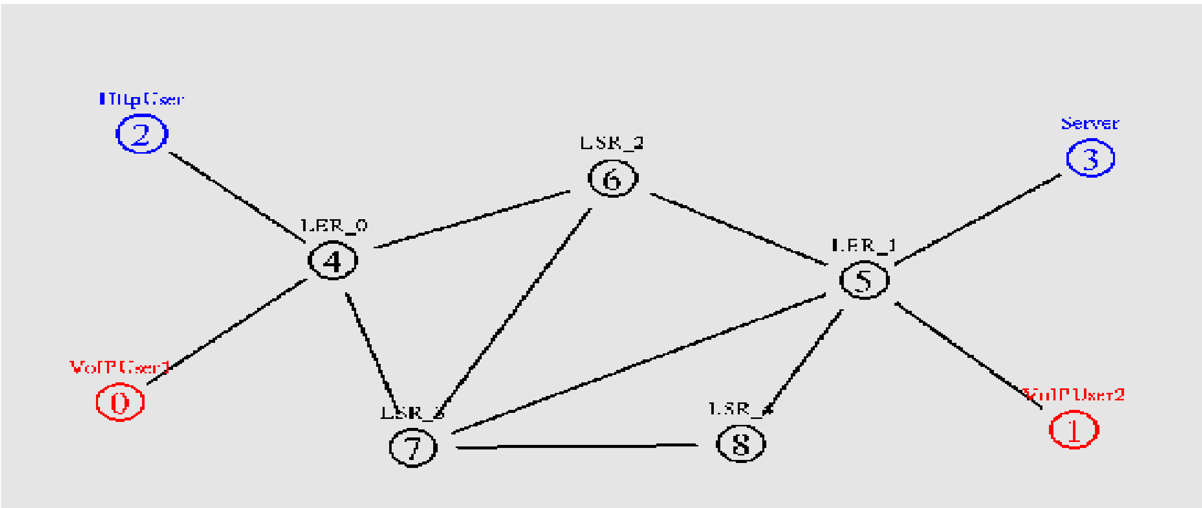
$ns_ duplex-link $node(5) $node(7) 1.544Mb 1ms DropTail

$ns_ duplex-link $node(5) $node(8) 1.544Mb 1ms DropTail

$ns_ duplex-link $node(6) $node(7) 1.544Mb 1ms DropTail

$ns_ duplex-link $node(7) $node(8) 1.544Mb 1ms DropTail

Listing 1



4.6.2 Introducing explicit traffic

It is very convenient to set up different traffic demand between nodes, see Listing 2 below

```
#VoIP traffic
#sink attach to the node $voip2
        set vsink0_ [new Agent/Null]
        $ns_ attach-agent $voip2 $vsink0_
#source
        set vudp [new Agent/UDP]
        $ns_ attach-agent $voip1 $vudp
#traffic
        set vtraffic [new Application/Traffic/CBR]
        $vtraffic set packetSize_ 100
        $vtraffic set burst_time_ 0
        $vtraffic set idle_time_ 0
        $vtraffic set rate_ 64k
        $vtraffic attach-agent $vudp
#connect
        $ns_ connect $vudp $vsink0_
        set vsrc0 $vtraffic
        $ns_ at 1.0 "$vsrc0 start"
```

Listing 2 Traffic demand for VoIP

4.6.3 Introducing background traffic

The traffic is set up in the previous section, see the traffic comment and the vtraffic variable

4.6.4 Running OSPF protocol (with load balancing)

To use an OSPF-like routing protocol, the LS (link state) RtProto Object is set up, as in Listing 2.

```
$ns_ rtproto LS
```

Listing 2 Configure OSPF

4.6.5 MPLS setup and LSP configuration

Each node has to be configured with MPLS, and the static RSVP-TE paths and defaults need to be set up. All the link Queue types where changed to the Classifier Based Queues (CBQ) for RSVP-TE and MPLS to work correctly. A number of other small changes were made to make it run which should not be necessary in future (such as turning off LS routing and turning on static routing). The MPLS and RSVP-TE parts of the changes are shown in Listing 3

```
$ns_ node-config -MPLS ON

set node(0) [$ns_ node];

$ns_ add-to-mpls-list $node(0)

...

#MPLS Settings


# RSVPTE Settings

$ns_ PATH-color "purple"

$ns_ PATHERR-color "red"

$ns_ PATHTEAR-color "red"

$ns_ RESV-color "grey"

$ns_ RESVERR-color "red"

$ns_ RESVCONF-color "red"

$ns_ color 1002 green

Agent/RSVP set noisy_ 255
```

```
Agent/RSVP set refresh_ 30

Agent/RSVP set lifetime_factor_ 3

Agent/RSVP set ip6_ 0

Agent/RSVP set nam_ 1


# One RSVP-TE Agent on each MPLS Node

$ns_ configure-rsvpte-on-all-mpls-nodes

$ns_ cfg-cbq-for-SBTS 10 DropTail 990000.000000 0.010000

auto 0

$ns_ cfg-cbq-for-HBTS 10 DropTail 0.000000 0.000000 auto

0.0000

$ns_ cfg-cbq-for-STS 10 DropTail 0.000000 0.000000 auto

0.000000

$ns_ cfg-cbq-for-RTS 2040 DropTail 0.000000 0.990000 auto

0.0000

$ns_ bind-rsvpte-to-SBTS

set LSR(4) [eval $node(4) get-module "MPLS"]

set ses(1) [$LSR(4) session $node(5) 1]

set LSR(5) [eval $node(5) get-module "MPLS"]

set ses(2) [$LSR(5) session $node(4) 1]

$ns_ at 0.500000 "$LSR(4) PATH-resv-er $ses(1) 1000.000000

50 \

 50    $node(5) 1001 5 5 6_5"

$ns_ at 0.600000 "$LSR(5) PATH-resv-er $ses(2) 1000.000000

50 \

 50 $node(4) 1002 5 5 8_7_4"
```

Listing 3 Setting up MPLS and RSVP-TE

The code in Listing 4 was put in each flow of network traffic to identify the flow and what class of service it used. The value 7 was changed each time to uniquely identify each flow.

```
$vudp set fid_ 7
$ns_ bind-flowid-to-SBTS 7
```

Listing 4 Per-traffic flow changes

4.6.6 Configure egress/ ingress LER nodes

Some bugs were found in the NS2 patch which caused the packets not to get routed into the MPLS paths, but the simulation set up for it should look like Listing 5. It is hoped that the bugs will be fixed in the next version of the patch due in the next few months.

```
$ns_ at 0.800000 "$LSR(4) bind-flow-erlsp 5 7 1001"
$ns_ at 0.900000 "$LSR(5) bind-flow-erlsp 4 8 1002"
```

Listing 5 Configure LER ingress and egress

4.6.7 Introducing a failure condition

In NS2, we can configure failure event as shown in Listing 6. The restoration event is similar with a different time and —up" instead of —down".

```
$ns_ rtmodel-at 2.0015 down $node(4) $node(6)
```

Listing 6 Configure Failure Event

4.6.8 Collect results and compare performance

The simulation file creates two trace files, a NAM file and a tr file. Both these files are ASCII text and can easily be parsed to find the information or statistics or run through animation and graphing programs (nam and xgraph or tracegraph) respectfully The simulation file can itself calculate statistics and values, and display them in any way it wishes, as it is a full general purpose programming language. NS2 can be used with the Akaroa2 simulation controller which runs the simulation credible results with low statistical error.

Chapter 5

Performance Evaluation & Comparative Study of Routing Protocols using Simulation

Chapter 5

Performance Evaluation & Comparative Study of Routing Protocols using Simulation

In this chapter of my thesis, I am going to analyze the comparative study of some category of routing protocols which i have discussed in the chapter 2 of this thesis using the network simulator (NS2). The main of this comparative study is that, i will be able to put forward the routing protocol from each category, i.e. which is best among each category. The analysis will give the idea, which protocol is best suited for which conditions. The comparative study as per group wise is discussed as under.

5.1 Simulation Matrices

The performance analysis of the routing protocols can be done with the help of network simulator. As there are matrices available, with the help of these matrices, I can analyze the comparative study of the routing protocols, Such types of matrices which we have used in our results are as under:

End to End Delay:

The concept "end-to-end" is used as a relative comparison with "hop-by-hop". Data transmission seldom occurs only between two adjacent nodes, but via a path which may include many intermediate nodes. End-to-end delay is the sum of delays experienced at each hop from the source to the destination. The delay at each intermediate node has two components: a fixed delay which includes the transmission at sender node and the propagation over the link to the next node, and a variable delay which includes the processing and queuing at sender node. The propagation delay is the delay in transmitting the data packet along a physical link.

$$\text{E.E.Delay} = \sum_{1}^{n}(\text{CBRsent} - \text{CBRreciv})$$

Packet Delivery Fraction (PDF):

PDF also known as the ratio of the data packets delivered to the destinations to those generated by the CBR sources. The PDF shows how successful a protocol performs delivering packets from source to destination. The higher for the value give use the better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness.

$$\text{PktDelivery\%} = \frac{\sum_{1}^{n} \text{CBR recived}}{\sum_{1}^{n} \text{CBR recived}} \text{x } 100$$

Routing Overhead:

It is the total number of control or routing (RTR) packets generated by routing protocol during the simulation. All packets sent or forwarded at network layer is consider routing overhead.

$$\text{Overhead} = \text{Number of RTR packets}$$

5.2 Performance / Comparative Study of Routing Protocols:

The Comparative study of the routing protocols provides us an idea, how much a routing protocol is better under which conditions. Here i am presenting comparative study of routing protocols using simulation. The simulation results are shown as under:

5.2.1 Empirical Evaluation of Proactive Routing Protocols:

Proactive protocols perform routing operations between all source destination pairs periodically, irrespective of the need of such routes. These protocols stem from conventional link state or distance vector routing algorithms, and attempt to maintain shortest-path routes by using periodically updated views of the network topology. These are typically maintained in routing tables in each node and updated with the acquisition of new information.

5.2.1.1 Simulation Parameters:

Here in this chapter, I am considering the parameter as propagation model for performance analysis of proactive routing protocols. As already discussed in above chapters, we have two types of propagation models first non-fading model and fading model that we discuss above. We are going to evaluate the performance of proactive routing protocols first under non-fading models and then under fading models. In fading models we change the node's mobility and the result is evaluated under two scenarios. The result simulation has been taken from my paper published in international journal of engineering science and technology[54].

1. With varying node's speed
2. With node's pause time.

The node will move randomly varying their speed from minimum to maximum. Also one more thing is considered to be random that is traffic pattern. The movement model will define the active route throughout the entire evaluation simulation time. In each simulation there are 25 source nodes, 25 receiver nodes and the transmission rate is 512 bytes and the simulation time is 200 s. This is necessary in order to enable fair comparisons among the routing protocols and to expose them to identical environmental conditions.

5.2.1.2 Simulation Results.

The goal of this simulation is to evaluate the impact of different propagation model on the performance of two proactive based routing protocols, while evaluating the performance; we introduce fading effects so that we can get real time environment evaluation. In this simulation, we are comparing the results of non-fading model with fading models. The result of the simulation performed is based on the three previously defined matrices. Simulation is carried out on two scenarios.

1. Varying node's pause time.
2. Varying pause time.

Scenario 1: Performance with varying node's maximum speed.

DSDV and OSLR show different behaviours at different levels , As speed increases, DSDV delivers less packets and exhibits more delay and more routing overhead than OSLR, as shown in the following figures.

Packet delivery ratio:

The packet delivery ratio decreases with the increase of speed, which implies that the links are relatively stable and more reliable at lower speed. OSLR delivers more packets than DSDV as shown in Figure below. The main reason for packet drops in wireless ad hoc routing protocols are mobility, congestion, and characteristics of wireless channel. Free space, shadowing and two ray ground models deliver more packets than Rayleigh and Ricean models when packet delivery ratio is considered as metric. The fading models deteriorate the network performance significantly, with Rayleigh and Ricean exhibiting the worst performance. This is due to a random drop in signal strength which causes packets being lost on reliable links, falsely indicating that links have failed, leading to interruption and the need for establishment of new route. This would also increase both delay and routing overhead. As speed increases, DSDV exhibits more delay and more routing overhead than OSLR.

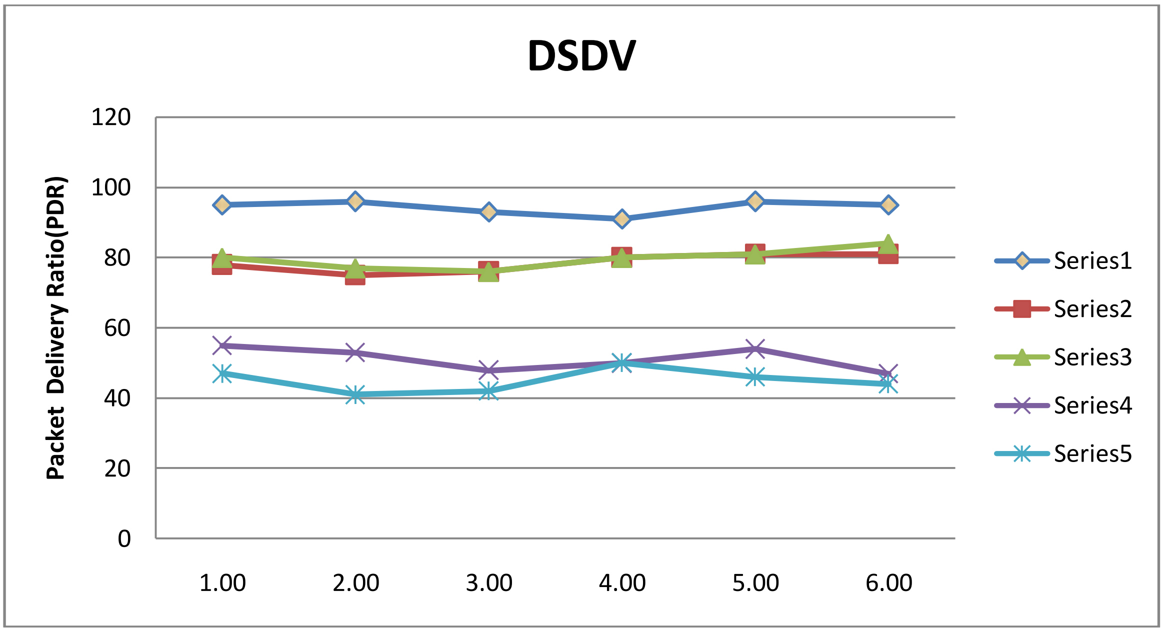


Figure 19

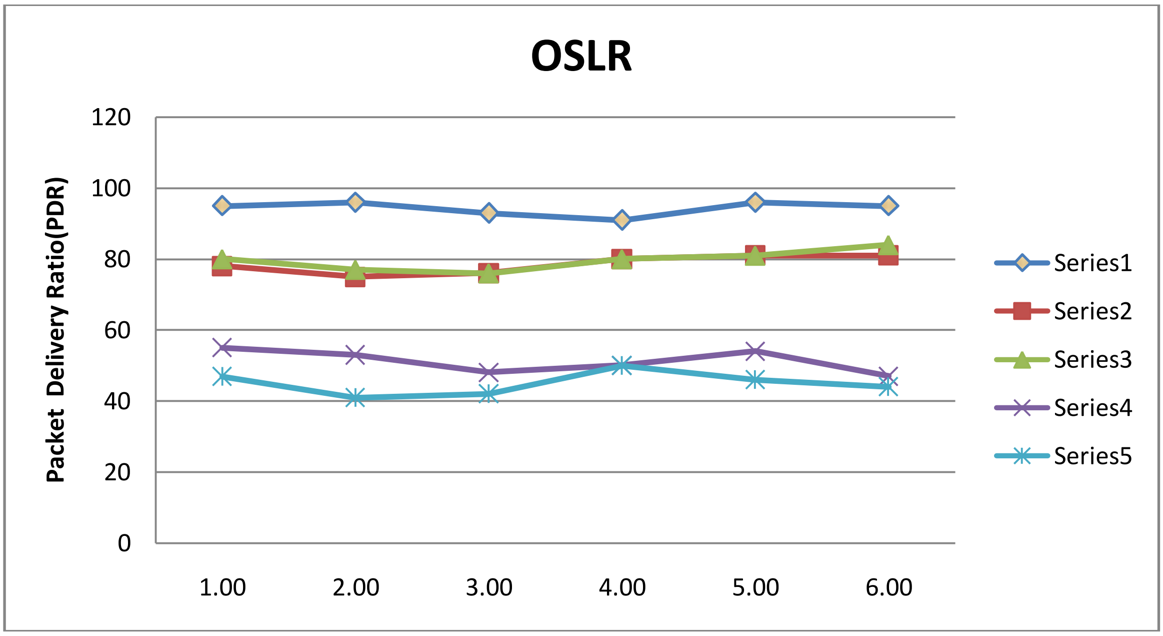


Figure 20

End-to-end delay

DSDV exhibits more delay than OSLR under all speed variations and delay increases with the increase of speed as indicated in Figure below. In comparison to free space and shadowing, the two ray ground, Rayleigh and Ricean models show higher delay. As expected Ricean model and Rayleigh exhibit more delay than the non-fading models. The abnormality of graphs may be due to higher congestion and increased MAC retries caused by unreliable routes that enforce on demand routing protocols to spend a significant number of their time performing route updates.

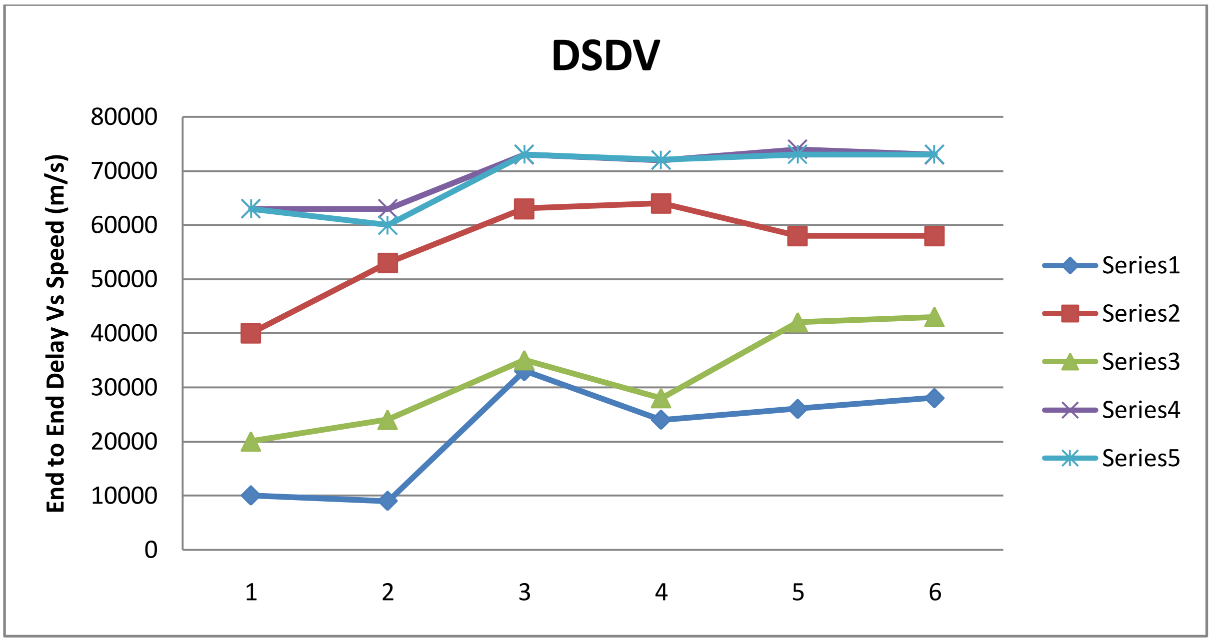


Figure 21

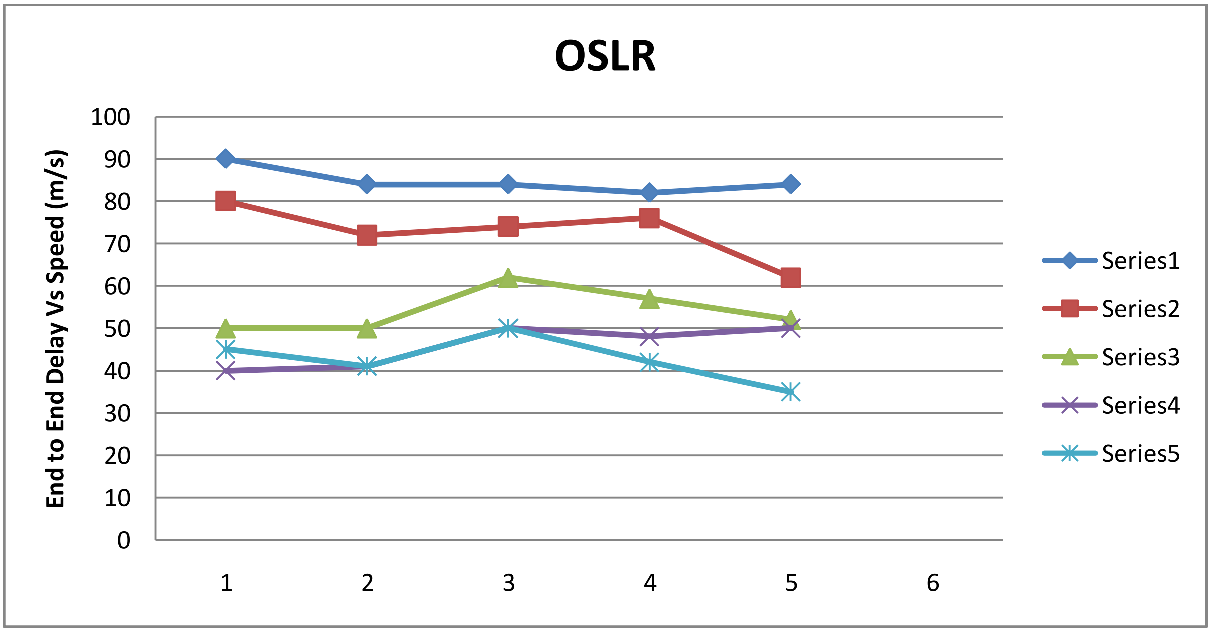


Figure 22

Routing overhead:

In general, the DSDV Shows increase in the routing overhead when compared with OSLR. Furthermore, much increase is observed under high speed as compared to low speed condition. Increase in the routing overhead is due to local connectivity through hello packets. Under all propagation models DSDV shows a higher increase in the routing overhead with increasing speed which can be attributed to ineffective usage of the routing packets. A lot of packets are dropped and updated each time the topology changes. This can be attributed to the constructive interference phenomena due to multipath signal propagation. In free space model, a sharp increase was observed in the routing overhead as the speed increases and this is essentially due to frequent link breaks. A similar behaviour was obtained for two ray ground model, with OSLR performing better than DSDV. In fading model, the two protocols have higher routing overhead compared with non-fading models as indicated in Figure below. This can be attributed to higher congestion and high inter-nodal interference.

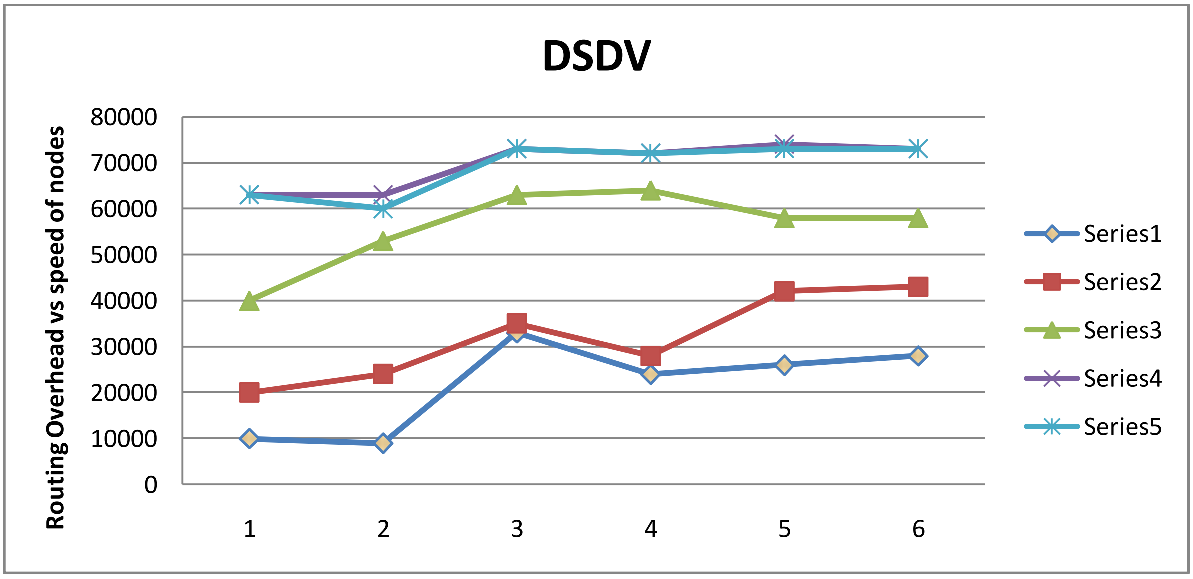


Figure 23

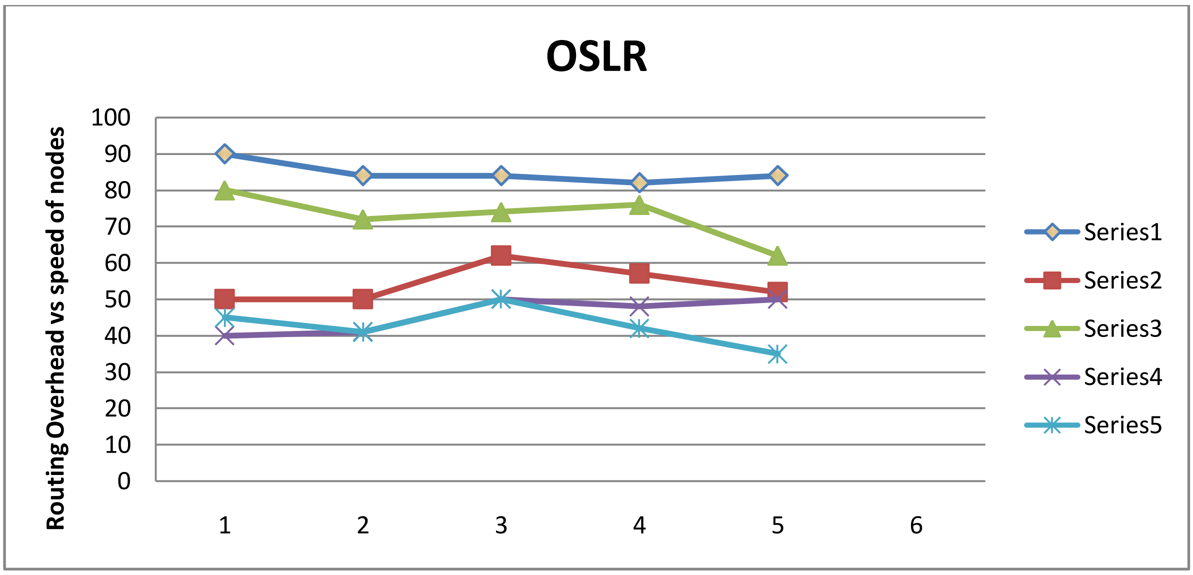


Figure 24

Scenario 2: Performance with varying node's pause time.

OSLR and DSDV show an approximately similar behaviour at different levels of pause time when considering packet delivery ratio. As pause time increases, DSDV exhibits more delay and more routing overhead than OSLR as shown in the following figures.

Packet delivery ratio

The two protocols relatively do the same performance when packet delivery ratio over a variety of pause time, for two ray ground, Rayleigh and Ricean models, while free space model exhibits the highest packet delivery ratio as presented in figure below. The lowest delivery ratio is for Ricean model, it is a consequence of the random variations in received signal strength. Packets are lost on a reliable link, falsely indicating that the link has failed leading to the interruption in protocol operation and initiates the need for a new path which would also increase delay and routing overhead. The results indicate that under Ricean and Rayleigh models, DSDV drops more packets than OSLR over a variety of pause times.

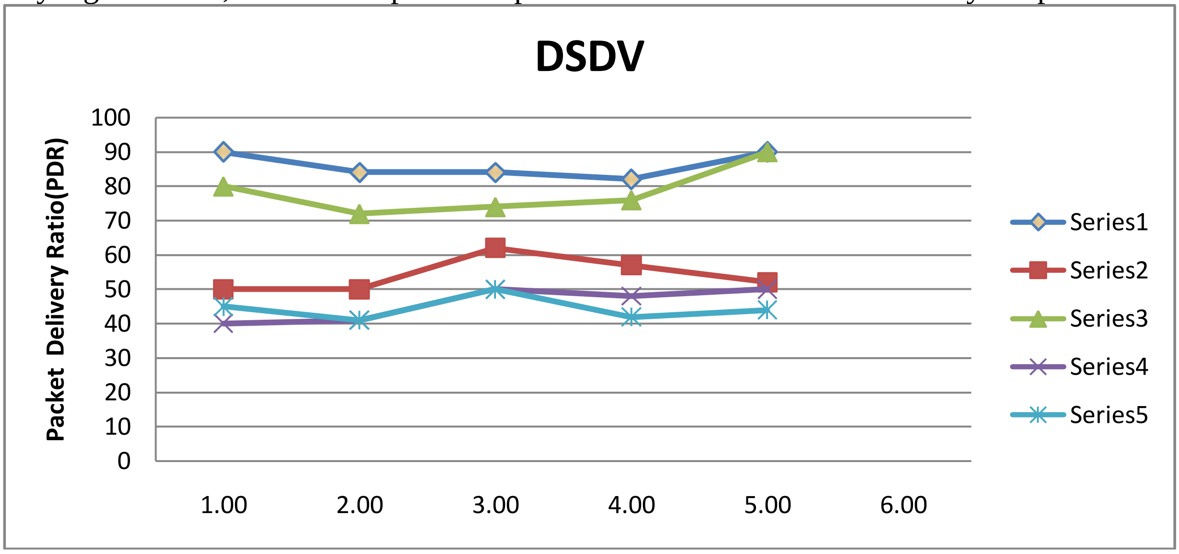


Figure 25

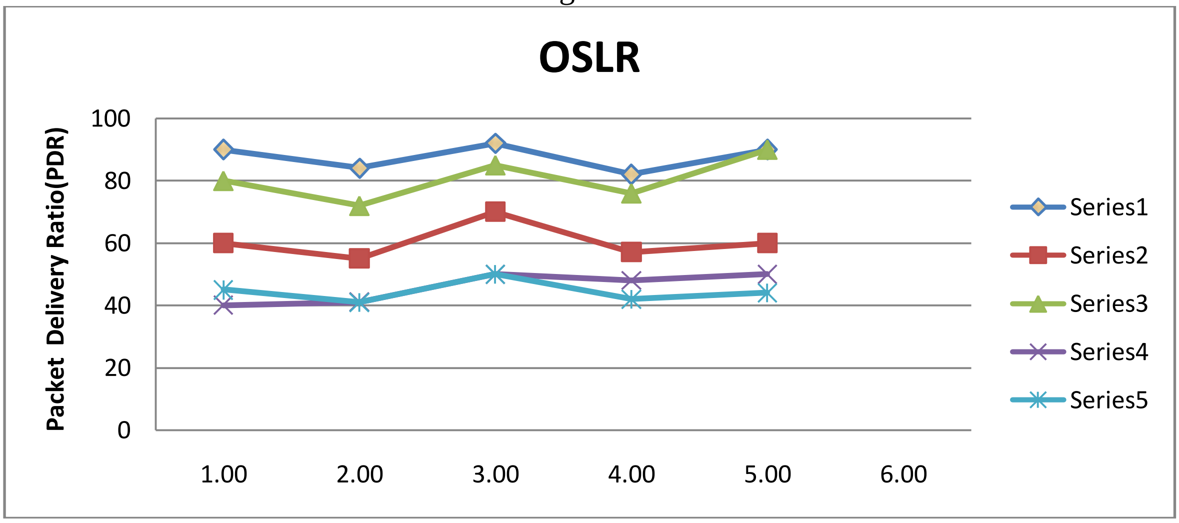


Figure 26

End-to-end delay

The two protocols show similar results with DSDV showing higher delay than OSLR as presented in Figure below. As expected the highest delay is for fading propagation models.

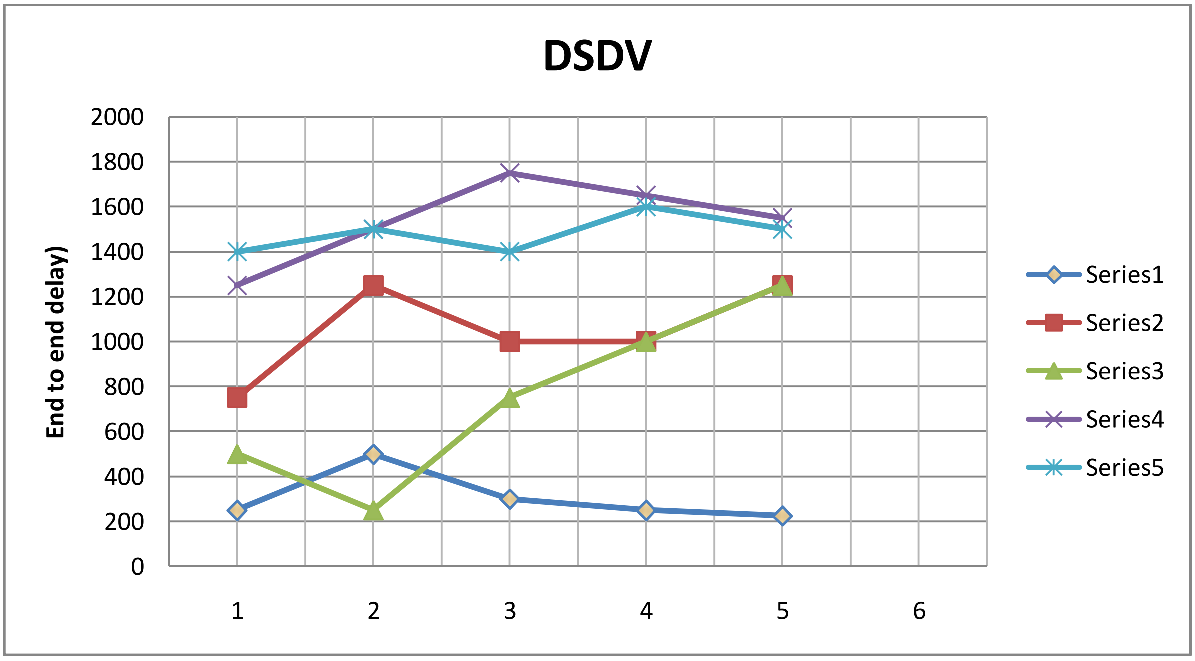


Figure 27

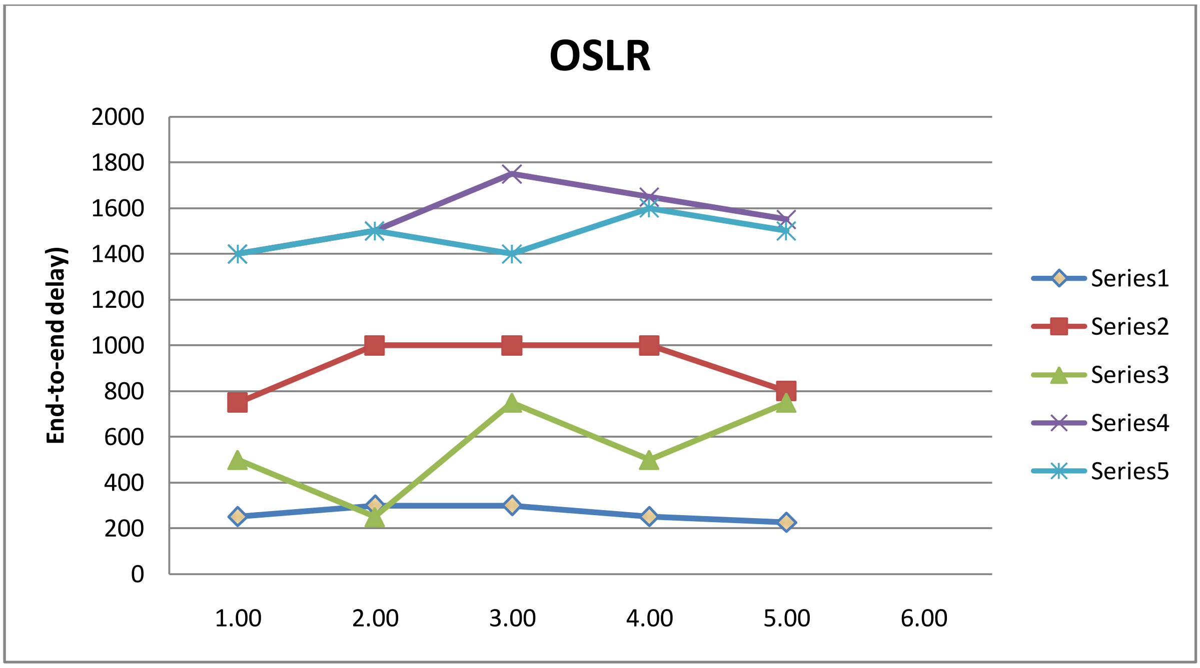


Figure 28

Routing overhead

The routing overhead for Ricean and Rayleigh is high compared to other models with free space which exhibited lowest routing overhead. As pause time increases, the routing overhead decreases, however, under higher pause time the routing overhead starts to increase. When modelled under the Ricean and Rayleigh fading, two protocols show an approximately similar behaviour at different levels of pause time with DSDV performing worse than OSLR as indicated in Figure below

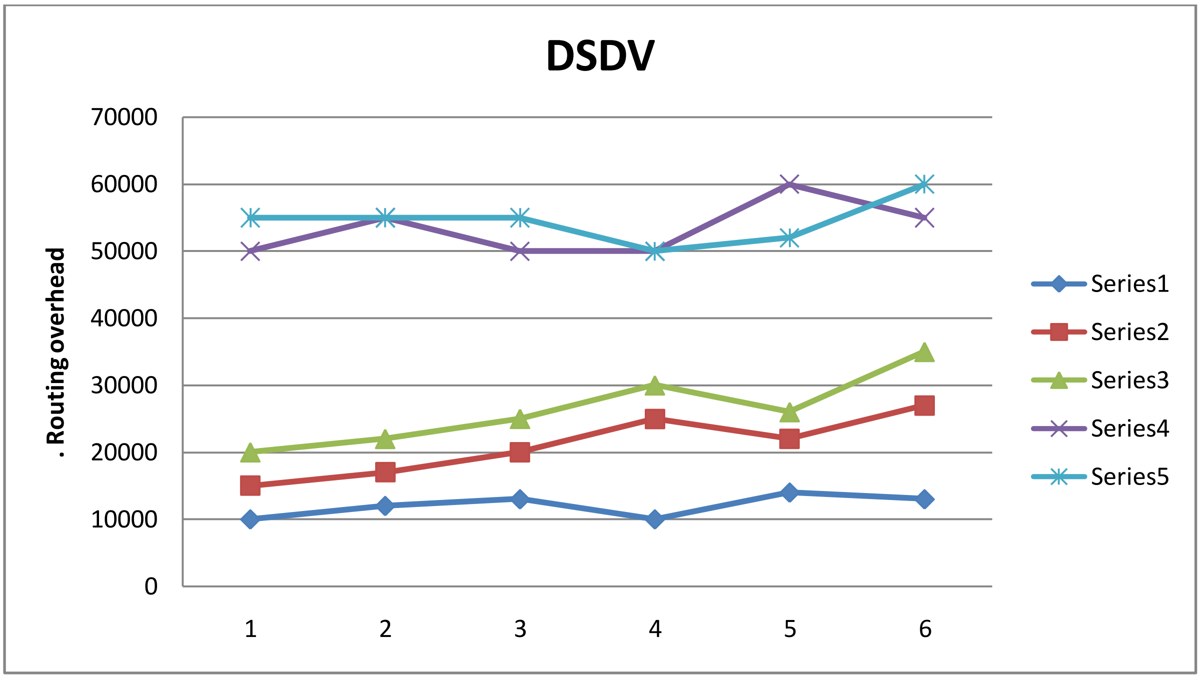


Figure 29

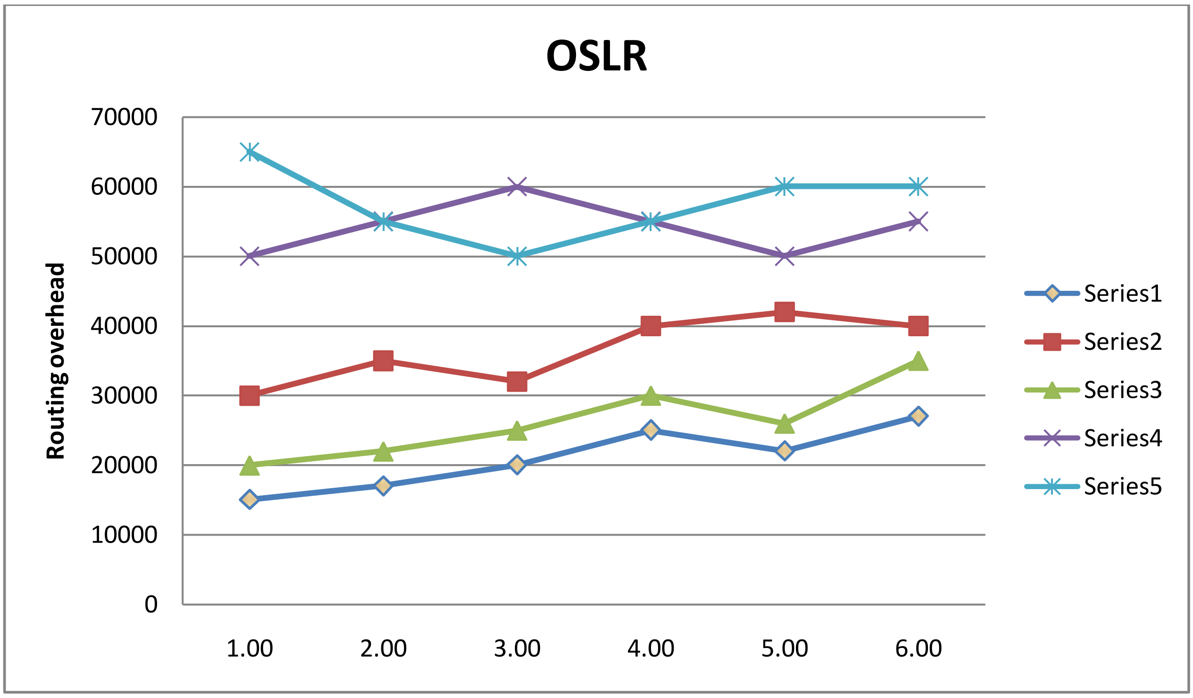


Figure 30

5.2.1.3 Conclusion:

In this paper, the effects of different propagation models on the performance of ad hoc networks have been investigated From the simulation results, the choice of propagation models have a great impact on performance of the routing protocol, so realistic and representative propagation models are necessary as far as the accurate Evaluation of the performance of routing protocols is concerned. The simulation results revealed that the different propagation models affected the performance of the mobile ad hoc network considerably. Consequently, different performance evaluation results were obtained. The performance has deteriorated very quickly when fading models were taken into account; for shadowing, Rayleigh, and Ricean models. The main reasons for this deterioration resulted from the large variation of the received signal strength.

5.2.2 Empirical evaluation of Reactive Routing Protocols:

On-demand (reactive) protocols will build the routes when required by the source node, in order for the network topology to be detected as needed (on-demand). When a node needs to send packets to several destinations but has no routes to the destination, it will start a route detection process within the network. When a route is recognized, it will be sustained by a route maintenance procedure until the destination becomes unreachable or till the route is not wanted anymore.

5.2.2.1 Simulation Parameters:

The simulations of above mentioned three reactive routing protocols I.e. AODV, DSR, TORA[55] are being carried out through Ns-2.3.1, under our assumed benchmark. The parameters are chosen in such a way, so that it fulfils the goal of our proposed benchmark. The Network size chosen is of 1000 m x 1000 m, with a transmission range of 270 m. The transmission speed for transmitting data is 11 Mbps. The Transmission power is fixed to 20 dbm with received thrush hold as -90 dbm. The antenna type is Omni directional with height gain and antenna height as 1 and 1.5 m respectively.

In this simulation processes the traffic parameter used is CBR (Continuous bit rate), because TCP offers a confirm load to network. The data rate is fixed to 4 packets per second. The simulation is performed by changing the node’s mobility with respect to node’s pause time .The nodes move according to a random waypoint model with velocity that allows a uniform distribution that form a minimum speed to maximum speed. The fading model used which are being used in simulation is Rician model .The other parameters which are being varied to acquire the results are mentioned in table below.

Ns-2 Simulation Parameters	
Network Simulator	Ns-2.3.1
Examined Protocols	AODV, DSR, TORA
Simulation Area	1000 m x1000m
Simulation Time	4 min
Transmission Range	260 m

Traffic Pattern	CBR(UDP)
Bandwidth	11 Mbps
Transmission Power	20 dbm
Packet rate	4 packets /sec
Data Payload	512 bytes
Send Buffer	64 packets
Number of nodes	30 nodes
Mobility Model	Random Way Point
Path loss Exponent	2
Antenna height	1.5 m
Antenna Gain	1
Antenna Type	Omni Directional
System loss Coefficient	1
Transmission speed	11 Mbps
Receive Thrush Hold	-90 dbm
Fading Model	Ricien Model
Ricien Factor	6
Channel Type	Channel/WirelessChannel
Network interface model	Phy/WirelessPhy
MAC Type	Mac/802.11
Link Layer type	LL

Table 4: Parameters of reactive routing protocols

5.2.2.2 Simulation Results:

The results of the simulation based on the above mentioned parameters are as under :

Packet Ratio Delivery:

The results show that as the speed of node's speed gets increased, the packet delivery ratio decreases. The main reason for packet drop in wireless adhoc is mobility, congestion and characteristics of wireless channel. While using the Rician model as fading model, its packet delivery ratio get decreased from that of packet ratio delivery of without fading models. DSR performs high than AODV and then TORA. The fading model declines the performance of network significantly. Fig below shows the comparison between the routing protocols on the basis of pause time. From the results it is clear that packet ratio delivery decreases as the increase in mobility. DSR & AODV drops a considerable number of packets during the route discovery phase, as the route acquisition takes time proportional to the distance between the source and destination. The situation is similar to TORA, in this case AODV ahs slightly lower packet delivery ratio than DSR because of higher drop rate, and TORA's performance is not very competitive with the other two routing protocols. Although the TORA performs good when pause time is increased.

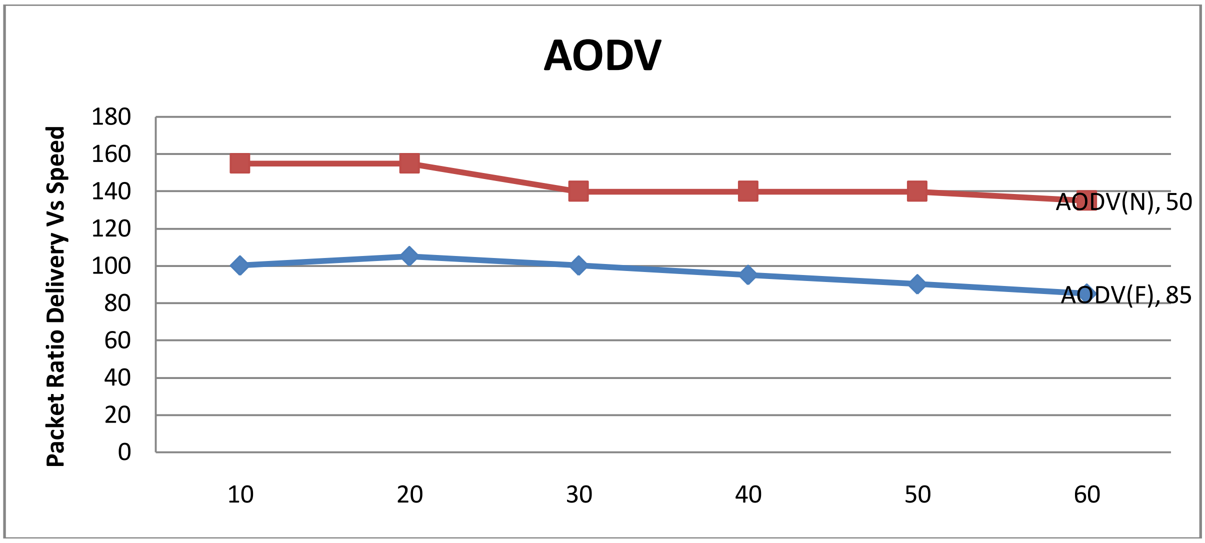


Figure 31

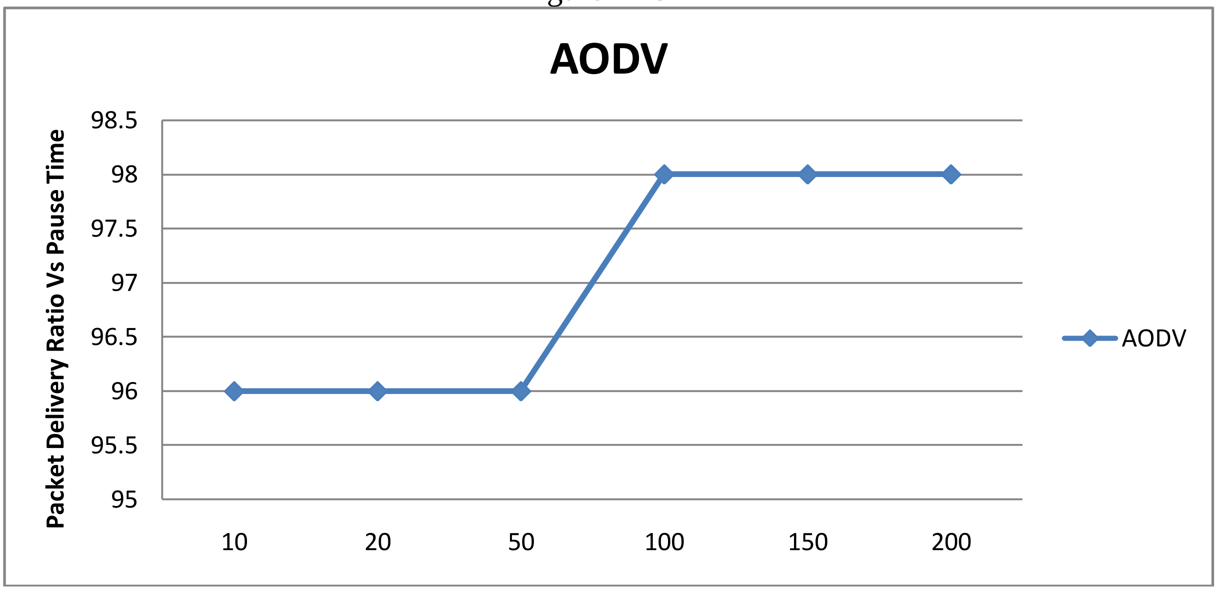


Figure 32

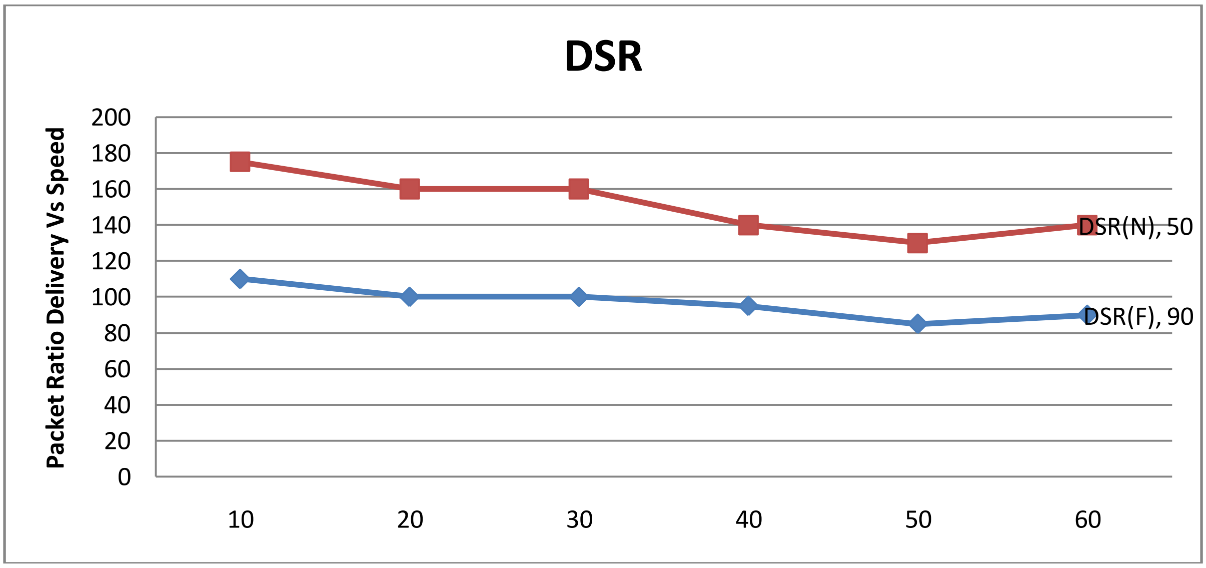


Figure 33

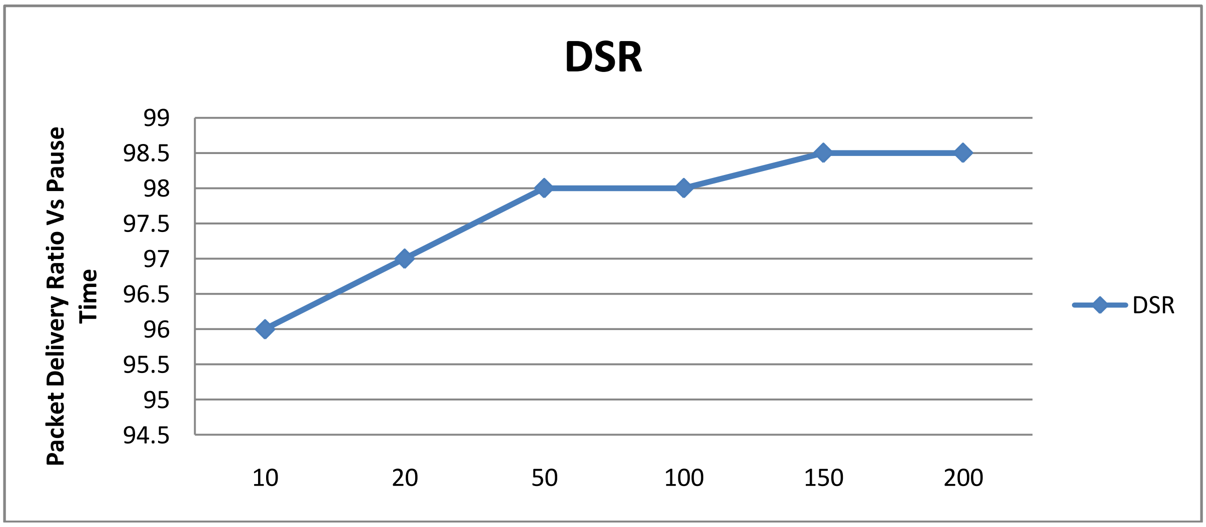


Figure 34

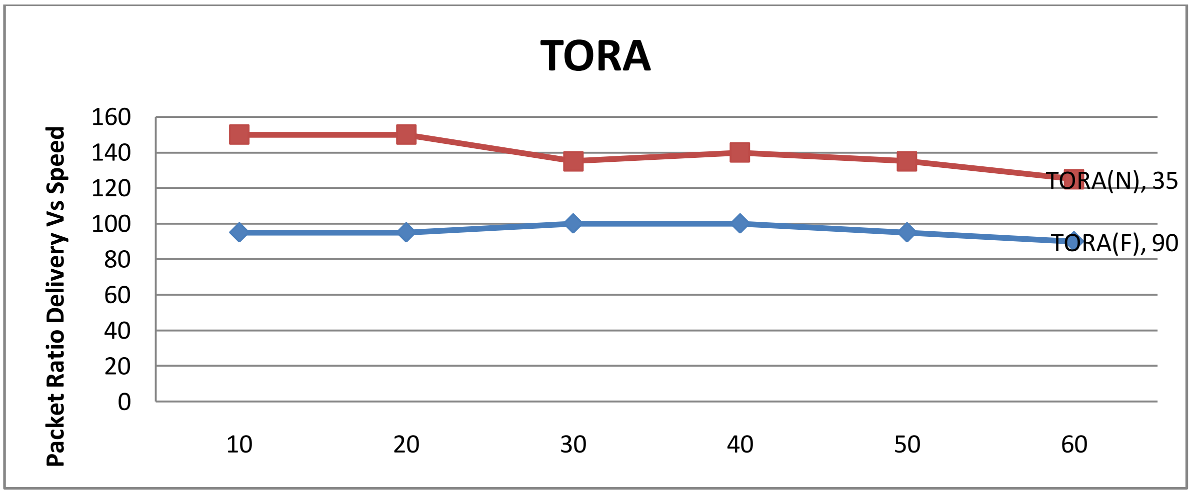


Figure 35

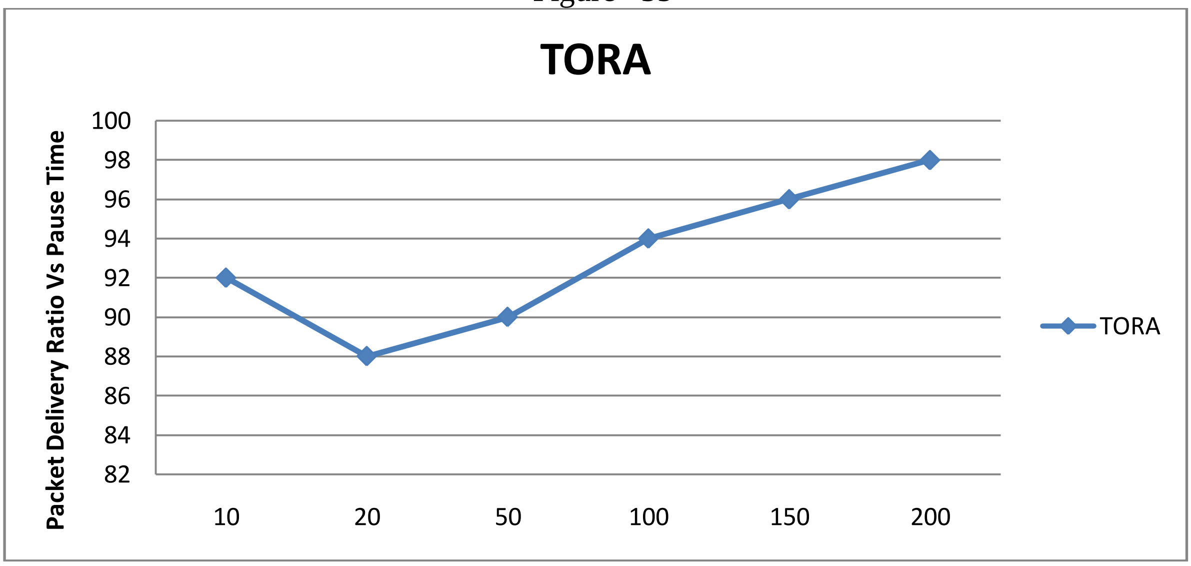


Figure 36

End To End Delay:

While calculating this parameter, the results shows that as the speed of node's get increased, the end to end delay increases. The main reason for packet drop in wireless adhoc is mobility, congestion and characteristics of wireless channel. While using the Rician model as fading model, its End to end delay get increased as that of normal i.e. without using fading models. AODV shows higher delay than TORA and then DSR. I.e. DSR have least end to end delay. Fig below shows the comparison between the routing protocols on the basis of pause time. From the below results AODV shows higher delay than TORA which in turn shows higher delay than DSR.

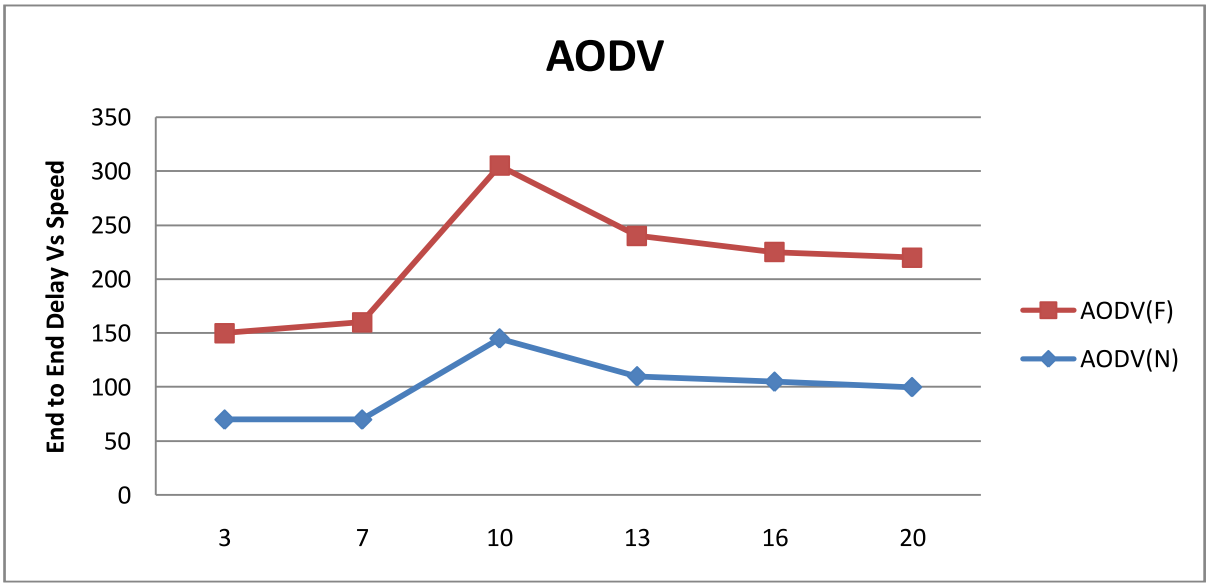


Figure 37

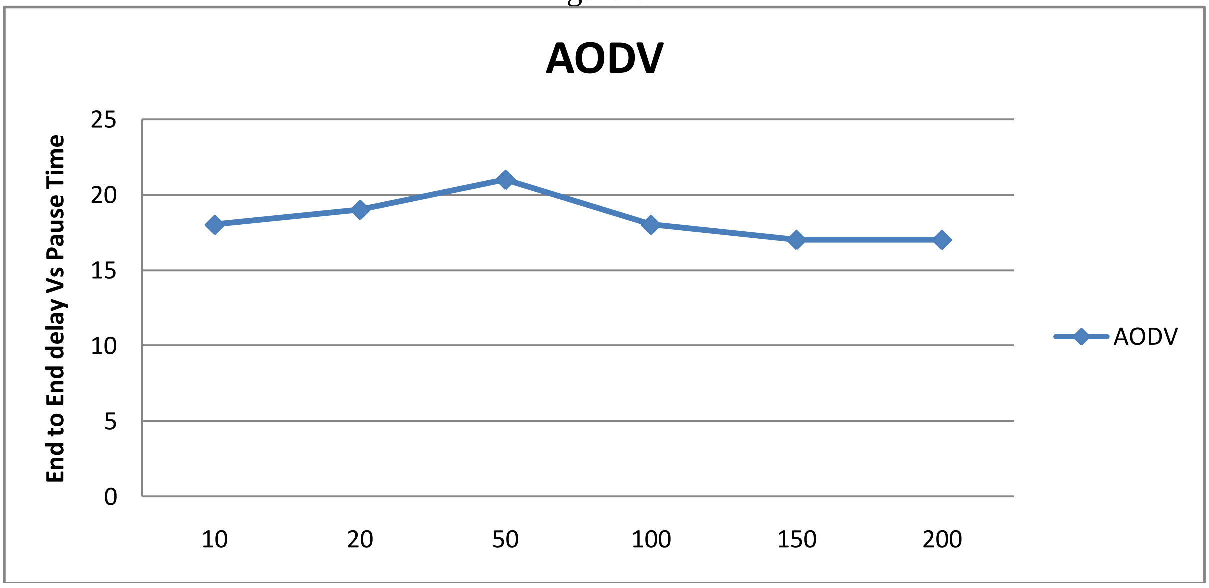


Figure 38

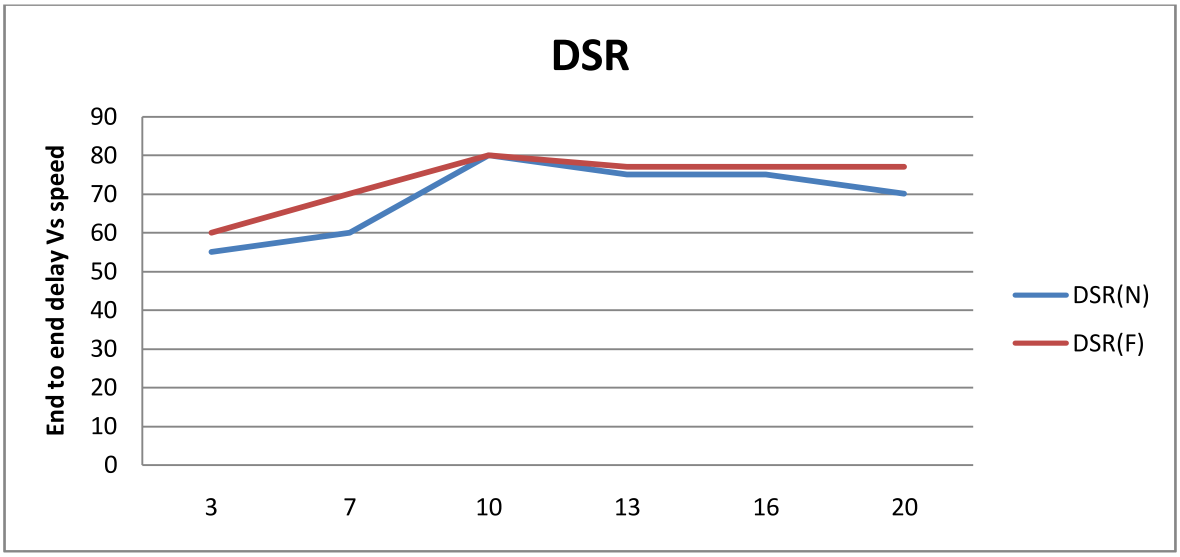


Figure 39

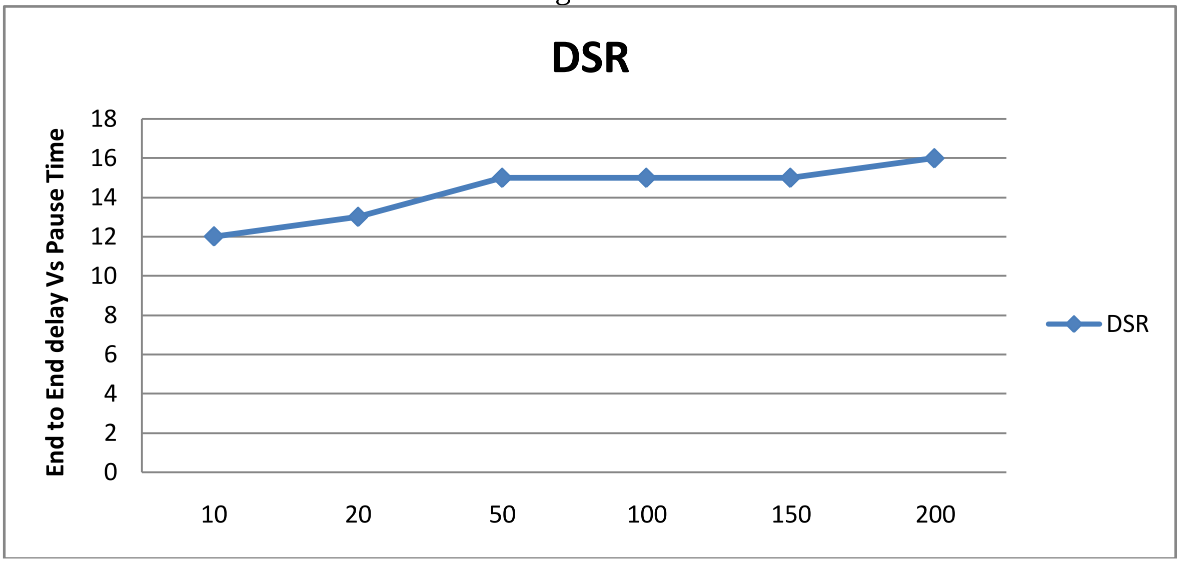


Figure 40

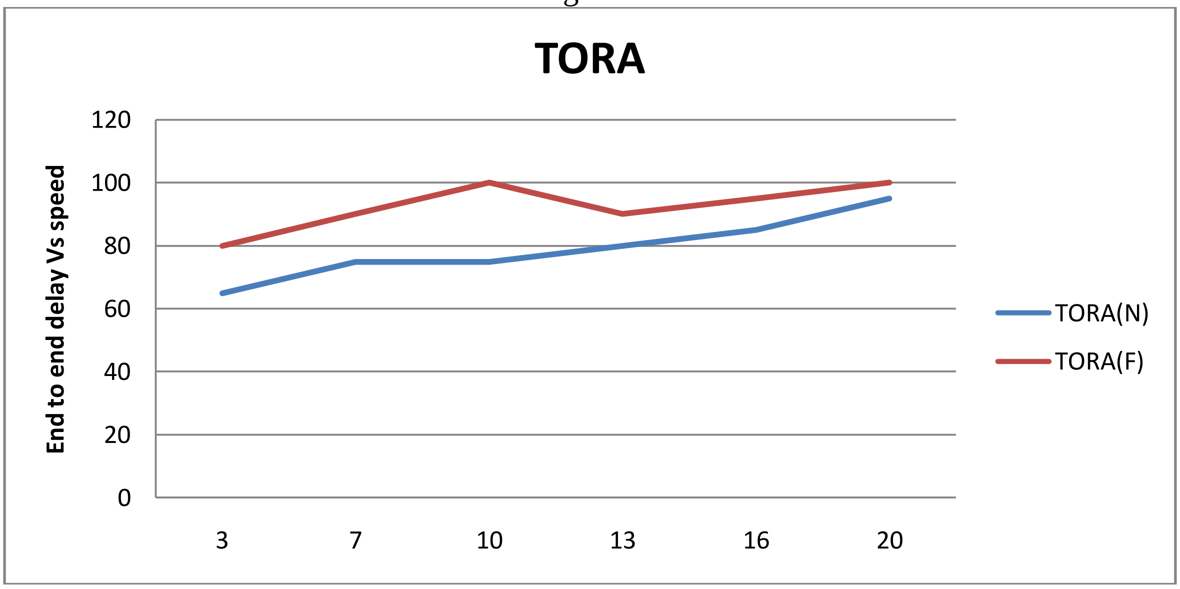


Figure 41

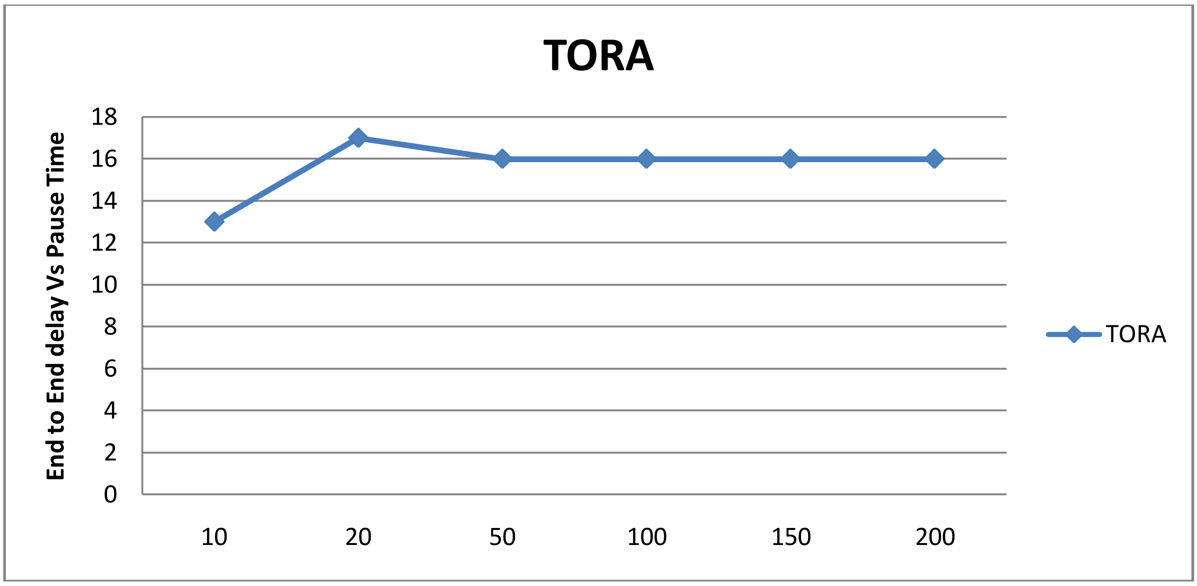


Figure 42

Routing Overhead:

While calculating this parameter, the results shows that as the speed of node’s get increased, the routing over head increases. The main reason for packet drop in wireless adhoc is mobility, congestion and characteristics of wireless channel. While using the Rician model as fading model, its routing overhead get increased as that of normal i.e. without using fading models. TORA shows higher routing overhead than DSR and then AODV. I.e. AODV have least routing overhead. Fig below shows the comparison between the routing protocols on the basis of pause time. From the below results TORA shows higher delay than DSR which in turn shows higher delay than AODV.

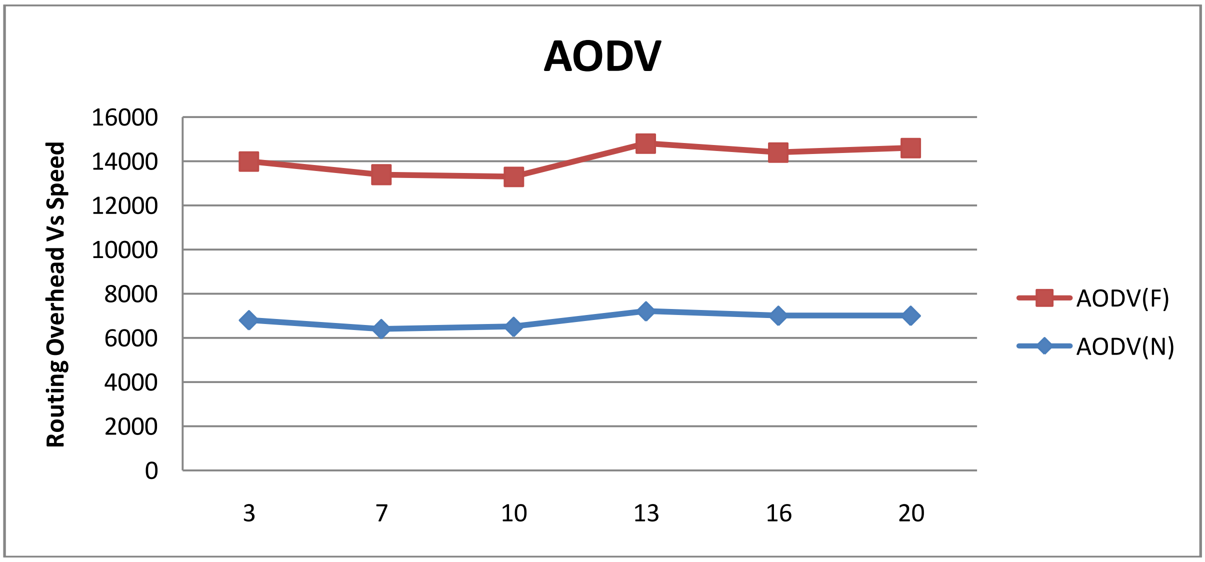


Figure 43

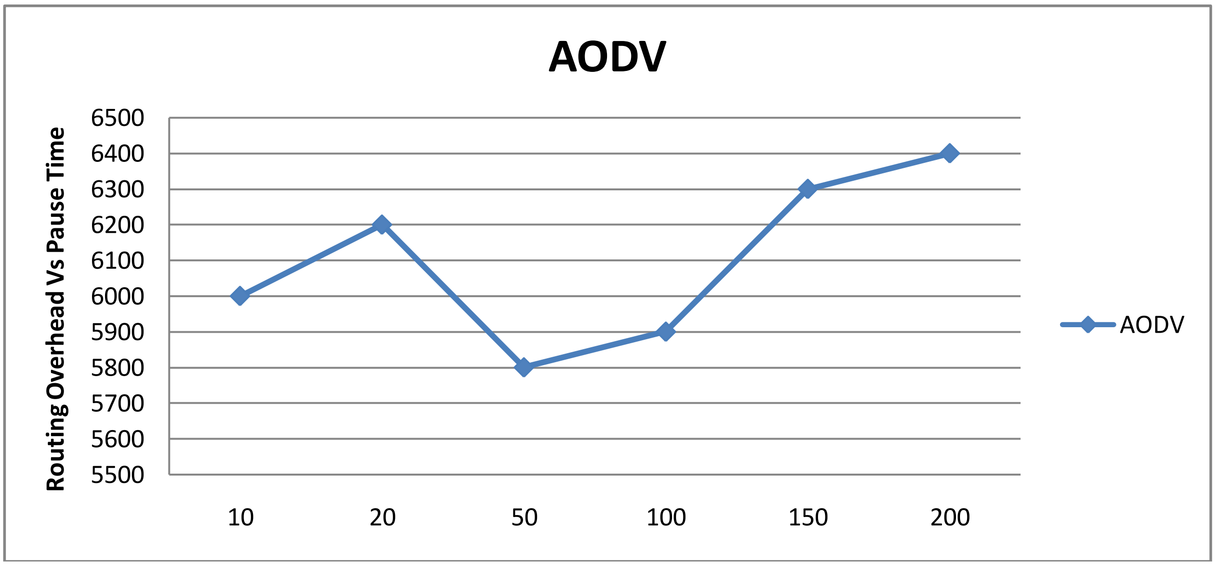


Figure 44

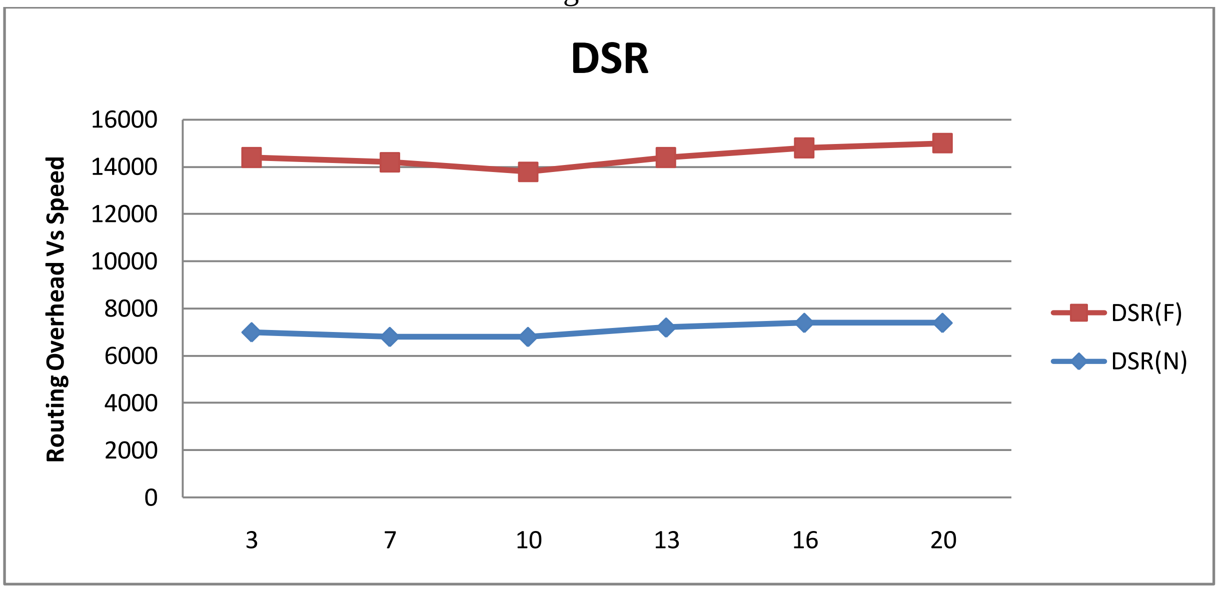


Figure 45

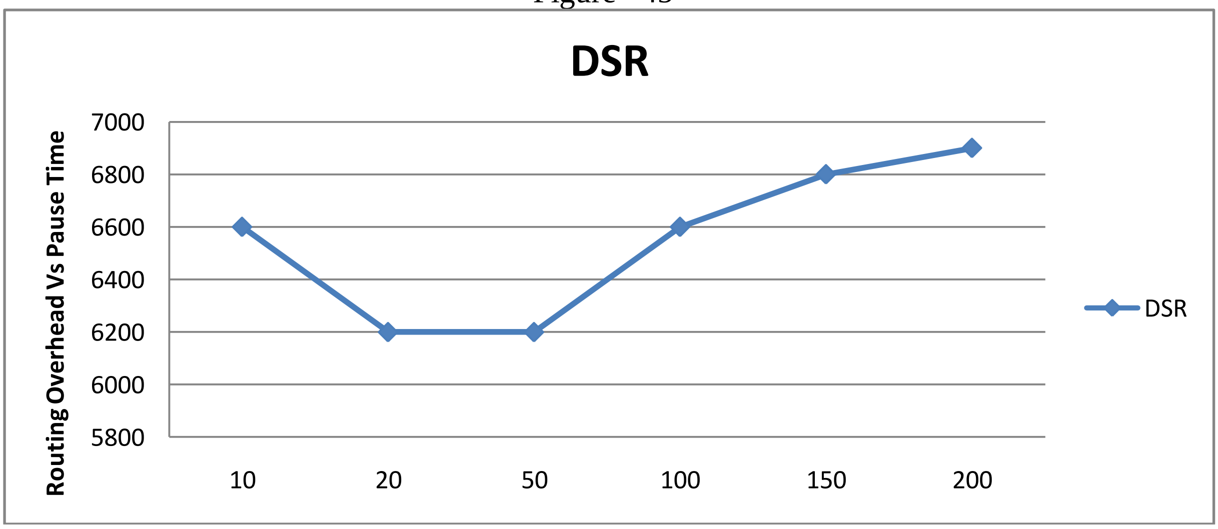


Figure 46

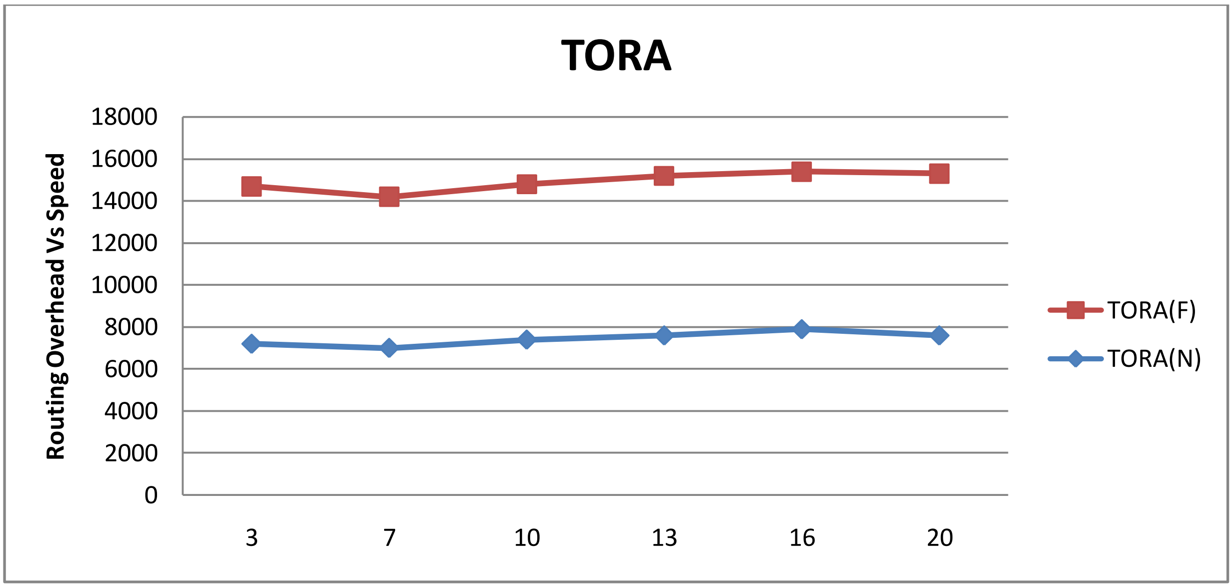


Figure 47

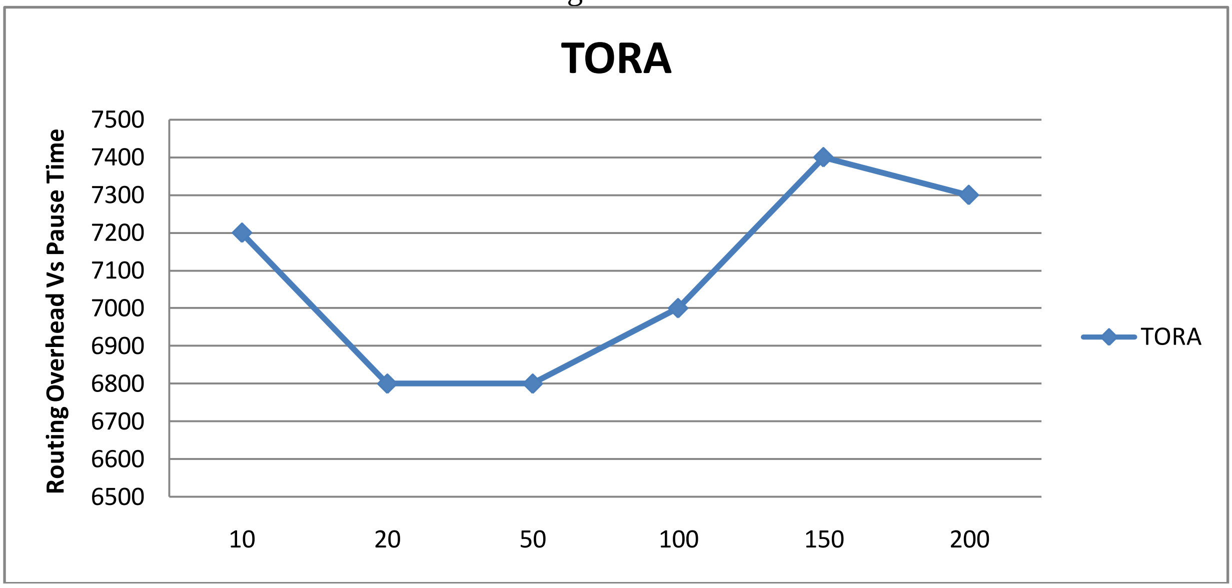


Figure 48

5.2.2.3 Conclusion:

Adhoc network receives vary much attention in recent years. Mobile adhoc networks are wireless networks that use multihop routing instead of static network infrastructure to provide network connectivity. Researchers are designing new routing protocols, comparing and improving existing ones.

This work provides an attempt towards the performance evaluation of routing protocols under the assumed benchmark. The performance matrices we evaluate are packet ratio delivery, end to end delay and routing overhead. In our paper the simulations show that DSR have more packet delivery ratio than AODV which in turn shows more PDR than TORA. While as in end to end delay AODV shows higher delay than TORA and DSR. In routing overhead TORA shows higher routing overhead than DSR and AODV. Thus in average the performance of DSR is better than TORA and AODV.

5.2.3 Empirical Evaluation of Geographical Based Routing:

5.2.3.1 Simulation Parameters:

Network simulator Ns-2.9 allinone is discrete simulator used for research. Ns-2 allows researchers to study Internet protocols and large-scale systems in a controlled environment [xx]. Here in this paper, Network simulator Ns-2 is used to analyze the effects performances of Location / Geographical based routing protocols. The simulation incorporated common values, with a setting of physical specification as indicated in table below.Other network performance are varied in accordingly. The Simulation of routing protocols has been carried out in this paper. The simulation parameters are given in table below.

Parameter	Value
Simulator	Ns2
Simulation Area	1000x1000
Simulation Time	900 s
Transmission Range	250 m
Nodes	40
Movement Model	Random Waypoint
Mobility Group Min Speed	2
Mobility Group Max Speed	2
Mobility Group INTERNAL Min Speed	10
Group Node Placement	UNIFORM
Propagation Channel Frequency	2.4e9
Path Loss model	Two Ray
Phy Data Rate	11 MBPS
Phy Power Transmission	15.0
Mac Protocol	802.11
Simulation Time	20 m
Traffic Pattern	UDP
Pause Time	0,20,40,80,160,350,700,900 s
CBR Source	10,20,30
Data Payload	64 bytes
Traffic Pattern	Random

Table 5: Parameters of Geograhical routing protocols

5.2.3.2 Results and Discussion:

The detailed discussion after acquiring the results is as under. The discussion is based on the result output produced by the simulations.

Packet Ratio Delivery:

As per results acquired after doing simulation, the data packet delivery ratio varies according to change in speed and increase in pause time. The packet ratio delivery is lower for

DREAM. We have chosen two parameters into consideration, speed and pause time. While using first parameter, I.e. Speed, all three routing protocols shows the decrease in packet ratio delivery. The DREAM protocol shows largest decrease in packet delivery ratio than other ones. The DREAM shows decrease due to limited buffer size and the contention and congestion in the network caused by flooding nature of the protocol. When calculating for our second parameter I.e. pause time, all three routing protocols tend to decrease their packet ratio delivery. The most deviated curve for packet delivery ratio is for DREAM .I.e. the DREAM has lowest packet delivery ratio then LAR and at the top for packet ratio delivery is LANMAR.The LANMAR has highest packet ratio delivery because of keeping accurate routes to "landmark" nodes rather than blurred routes to all nodes.

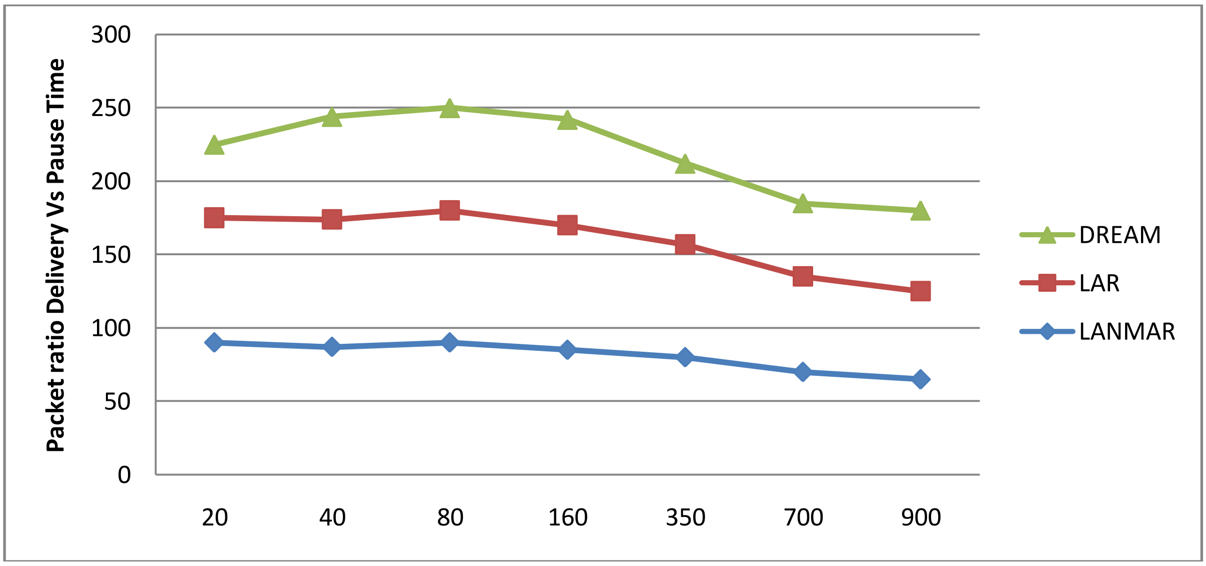
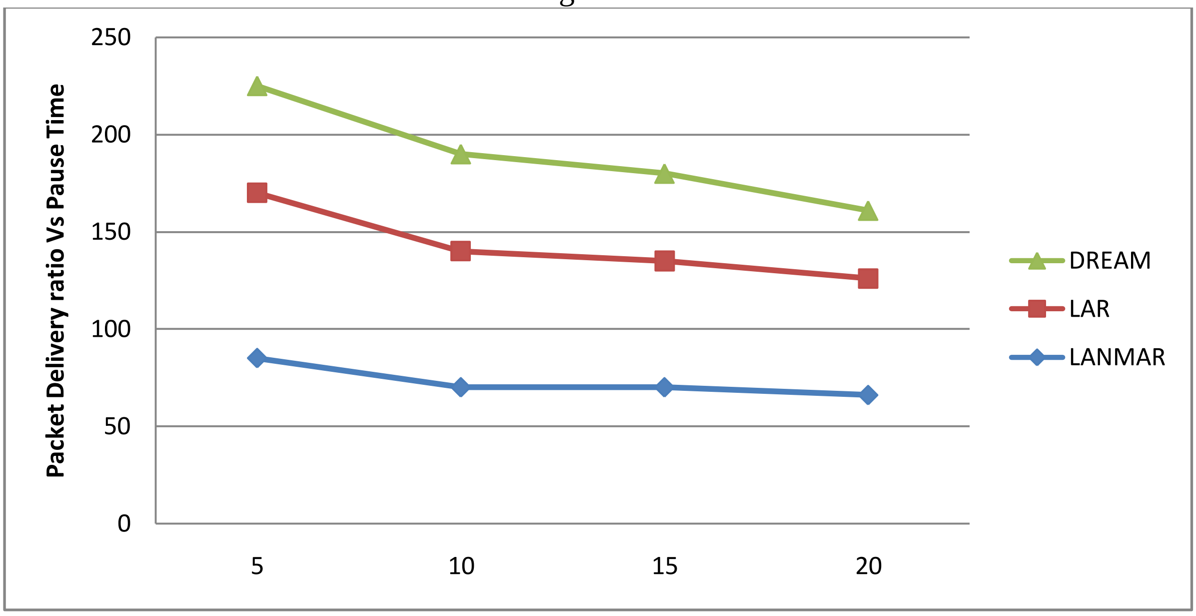


Figure 49



Packet Ratio delivery a) Vs Pause Time b) Vs Speed

Figure 50

End to End Delay:

As per results acquired after simulation, the LANMAR shows lower delay from that of LAR, which in turn shows lower delay than DREAM. After acquiring the results for the speed parameter, which shows that the end to end delay increases as we go on increasing the speed. The LANMAR has the lowest delay under the increased speed. On using the second constraint i.e. pause time, the observation are like as, when we go on increasing the pause time of nodes, the end to end delay also increases. The observation shows that the DREAM has highest end to end delay than that of LAR, which in turn has high delay than LANMAR.

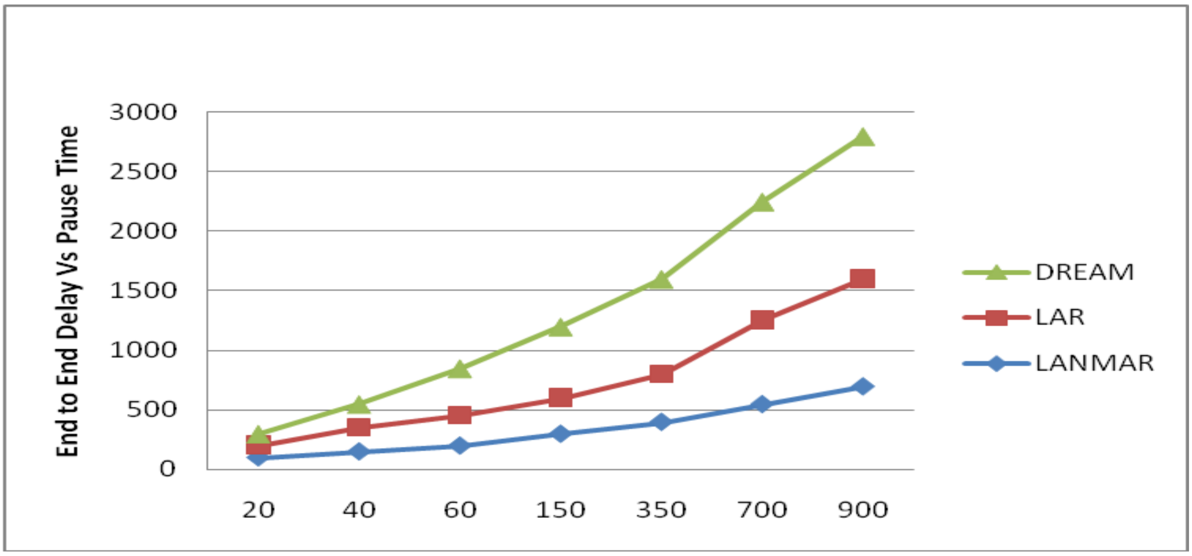


Figure 51

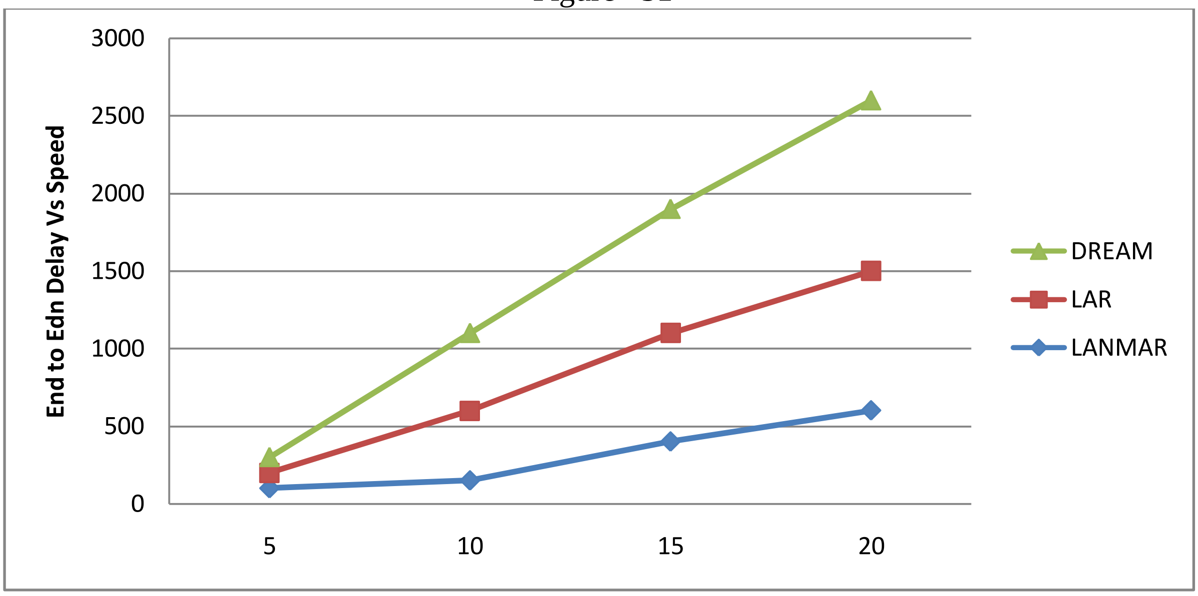


Figure 52

Routing Overhead:

As per results acquired from simulation, the routing protocols increased as we go on increasing speed and pause time of the nodes. The LANMAR has got the lowest routing overhead, Thus LANMAR outperforms the other two protocol in every field.When we go on increasing the speed of the nodes , the routing overhead go on increasing thus we have LAR at the highest routing overhead ,after that we have DREAM and the LANMAR.Also for the pause time the hierarchy is same as that of speed i.e LAR has high routing overhead then DREAM and at the last LANMAR.

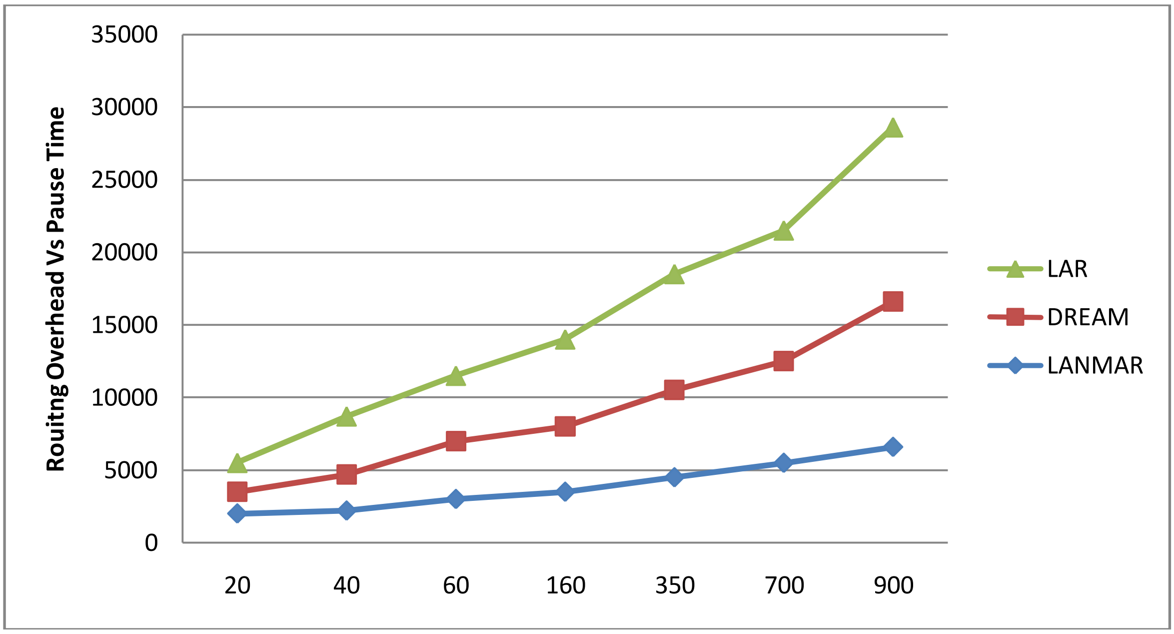


Figure 53

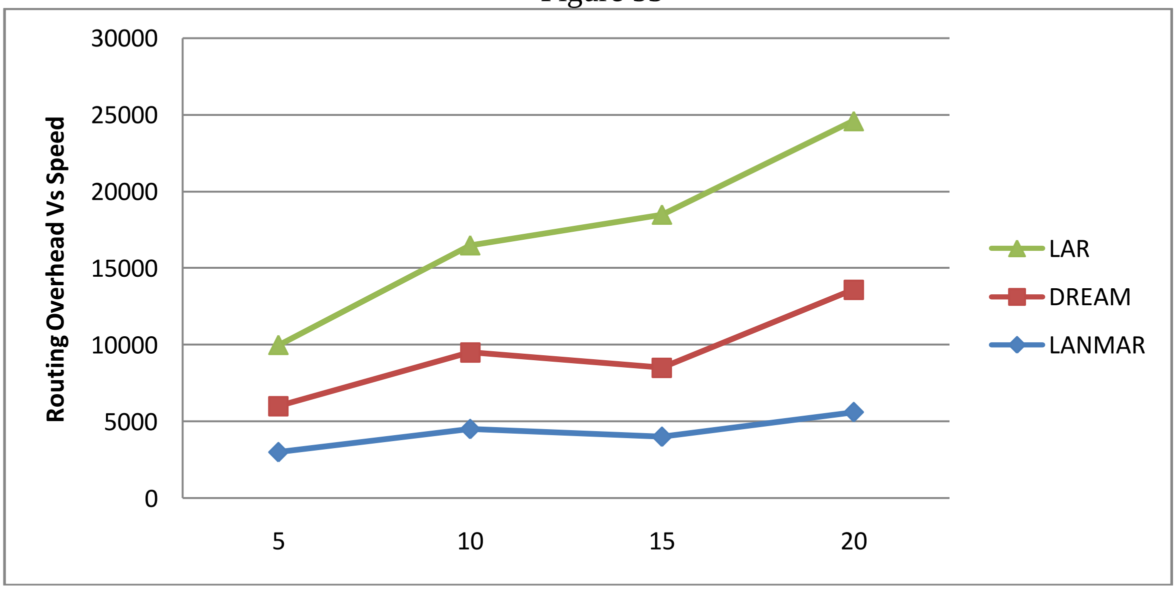


Figure 54

5.2.3.3 Conclusion :

Adhoc network receives vary much attention in recent years. Mobile Adhoc networks are wireless networks that use multihop routing instead of static network infrastructure to provide network connectivity. Researchers are designing new routing protocols, comparing and improving existing ones.

This work provides an attempt towards the performance evaluation of routing protocols under the assumed parameters. The performance matrices we evaluate are packet ratio delivery, end to end delay and routing overhead. In our paper the simulations show that LANMAR have more packet delivery ratio than LAR which in turn shows more PDR than DREAM. Also end to end delay of LANMAR, LAR and DREAM are same as packet ratio. But routing overhead LAR shows higher routing overhead than DREAM and LANMAR. Thus in average the performance of LANMAR is better than LAR and DREAM.

Chapter 6

Conclusion

Chapter 6

Conclusion

Ad-hoc networks are an emerging area of mobile computing. Ad-hoc network is a self-supporting collection of mobile nodes that happen to exist within a close proximity in an interval of time. The adhoc networks use a set of rules for transforming the data from one wireless station to another wireless station which we call as routing protocols. There are number of routing protocols available for wireless adhoc networks, we make an attempt to provide descriptions of several routing schemes proposed for ad hoc wireless networks. We also provide a classification of these schemes according to the routing strategy. The presented classification model of routing protocols is a meaningful attempt to clarify the vast field of adhoc routing protocols. It is so because it tries to reveal the main design and implementation principles behind protocols. The classification is a little bit complicated and it is not always an easy task to classify a protocol according to that taxonomy, but the meaning of classifying is try to get some rough basis for protocol's performance evaluation.

Here in this work, we have made an attempt to analyze the performance of different category of routing protocols as described in the classification of this thesis. The categories are Proactive, Reactive and Geographical based routing protocols. The results conclude for the above mentioned are as under:

1. Proactive Based Routing Protocols:
   OSLR have more packet deliver ratio than DSDV under all the condition(fading models and mobility etc), also as the speed increases the routing overhead and delay increases for both OSLR and DSDV , but DSDV shows higher overhead and delay than OSLR.Thus in general OSLR outperforms the DSDV.

2. Reactive Based Routing Protocols:
   DSR have more packet delivery ratio than AODV which in turn shows more PDR than TORA. While as in end to end delay AODV shows higher delay than TORA and DSR. In routing overhead TORA shows higher routing overhead than DSR and AODV. Thus in average the performance of DSR is better than TORA and AODV.

3. Geographical Based Routing Protocols:
   LANMAR have more packet delivery ratio than LAR which in turn shows more PDR than DREAM. Also end to end delay of LANMAR, LAR and DREAM are same as packet ratio. But routing overhead LAR shows higher routing overhead than DREAM and LANMAR. Thus in average the performance of LANMAR is better than LAR and DREAM.

In recent years many routing protocols have been developed but there are various challenges that are faced in the Ad-hoc environment. These are mostly due to the resource poorness of these networks. They are usually set up in situations of emergency, for temporary operations or simply if there are no resources to set up elaborate networks. Ad-hoc networks therefore throw up new requirements and problems in all areas of networking. The solutions for conventional networks are usually not sufficient to provide efficient Ad-hoc operations. The wireless nature of communication and lack of any security infrastructure raise several security problems. In future work an attempt will taken on the security of routing protocols that is an enhancement will be done on existing protocols in terms of security or a new protocols will be designed , which will be secure.

Chapter 7

Publications

Chapter 7

Publications

Paper Published in National and International Journals

1. Bilal Maqbool Beigh, Prof.M.A.Peer." Classification of Current Routing Protocols for Ad Hoc Networks - A Review". International Journal of Computer Applications (0975 – 8887) Volume 7– No.8, October 2010.

2. Bilal Maqbool Beigh, Prof.M.A.Peer," Performance Evaluation of Pro-Active Routing Protocols with Fading Models: An Empirical Evaluation using Ns-2". International Journal of Engineering science and Technology Volume 3 issue 1, January2011.

3. Bilal Maqbool, Suhail Qadir Mir et.al "Information availability: components, threats and protection mechanisms ", JGRC, March 2011.

4. Bilal Maqbool Beigh, Prof.M.A.Peer, "Towards the Benchmarking of Routing Protocols in Wireless Adhoc networks", International Journal of Science and technology., March 2011.

5. Bilal Maqbool Beigh, Prof.M.A.Peer, " Performance Evaluation of Geographical Routing Protocols: An Empirical Study communicated to IEEExplore transaction on communication.

Paper Published in Conferences

6. Bilal Maqbool Beigh, Prof.M.A.Peer, "Taxonomy of routing protocols in wireless adhoc networks", 6th JK Science Congress University of Kashmir 2010.

7. Bilal Maqbool Beigh, Prof.M.A.Peer, " A comparative study of open source and commercial network Simulators:OPNet and OMNet++, Open source software systems University of Kashmir 2011.

References

References

1. Larry L. Peterson and Bruce S. Davie, “Computer Networks - A Systems Approach”. San Francisco, Morgan Kaufmann Publishers Inc. ISBN 1-55860-368-9.

2. Bilal Maqbool Beigh, Prof.M.A.Peer, ”Classification of routing protocols for wireless Adhoc networks- A Review”, International Journal of Computer Applications (0975 – 8887)Volume 7– No.8, October 2010.

3. Bilal Maqbool Beigh, Prof. M.A Peer, “Taxonomy of routing protocols for wireless Adhoc networks” , 6th J&k Science congress conference , university of Kashmir 2010.

4. J. Broch, D. A. Maltz, D. B. Johnson, Y-C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In Proceedings of the 4th International Conference on Mobile Computing and Networking(ACM MOBICOM’98), October 1998.

5. S.R. Das, R. Castaneda, J. Yan, and R. Sengupta. Comparative performance evaluation of routing protocols for mobile, ad hoc networks. In 7th Int. Conf. on Computer Communications and Networks (IC3N), October 1998.

6. X. Hong, K. Xu, and M. Gerla. Scalable routing for mobile ad hoc networks. IEEE Network, 2002.

7. E. M. Royer and C. K. Toh. A reivew of current routing protocols for ad hoc mobile wireless networks. IEEE Pers.Comm., pages 46–55, April 1999.

8. C.Siva Ram Murthy and B.S.Manoj, “ Ad hoc Wireless Networks Architecture and protocols” Pearson Publication.

9. A. Neskovic, N. Neskovic, and G. Paunovic, “Modern Approaches in Modeling of Mobile Radio Systems Propagation Environment,” IEEE Communications Surveys, Third Quarter 2000.(1)

10. J-P. Linnartz, “Narrowband Land-Mobile Radio Networks,” Artech House, 1993(6)

11. T. Rappaport, “Wireless Communications: Principles and Practices (2nd edition),” Prentice Hall, 2002(15)

12. Guardiola IG, Matis TI. Fast-fading, an additional mistaken axiom of wireless-network research. Int J Mobile Network Des Innovation 2007; 2(3–4):153–8.(4)

13. Puccinelli D, Haengi M.Multipath fading in wireless sensor network: measurements and interpretation IEE/ACM international wireless communication and mobile computing conference (IWCMC 06) 2006.(11)

14. Punnoose NR, Stancil D. Efficient simulation of Ricean fading within a packet simulator. In: Proceedings of IEEE vehicular technology conference; 2000. p. 764–767.

15. Schmitz A, Wenig M. The effect of the radio wave propagation model in mobile ad hoc networks. In: Proceedings of ACM MSWiM; 2006.

16. T. Rappaport, “Wireless Communications: Principles and Practices (2nd edition),” Prentice Hall, 2002

17. Exploring Network simulator 2 by Manasa S.Mohit P. Tahiliani

18. Hasti AhleHagh. Techniques for communications and geolocation using wireless adhoc networks. Master of science thesis, Worcester Polytechnique institute; 2004

19. Lenders, Wagner J, May M. Analyzing the impact of mobility in adhoc networks.ACM/Sigmobile Workshop on Multi-hop Ad Hoc Networks: from Theory to Reality (REALMAN), Italy; 2006.

20. Nasri Amir, Schober Robert, Ma Yao. Unified asymptotic analysis of linearly modulated signals in fading, non-Gaussian noise, and interference. IEEE Trans Commun 2008; 56(6):980–90.

21. T. S . Rappaport, Wireless communication: Principles and Practice , Prentice Hall PTR, New Jersey, 2001

22. C.E. Perkins & P. Bhagwat, “Highly Dynamic Destination Sequence-Vector Routing (DSDV) for Mobile Computers”, Computer Communication Review, vol. 24, no.4, 1994, pp. 234-244.

23. www.isi.edu/nsnam/ns/tutorial Marc Greis tutorial on ns2

24. Matthias Transier “ Ns2 tutorial running simulations ”

25. Z.J. Haas, M.R. Pearlman and Prince Samar, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks”, IETF Internet draft, Jul 2002, http://www.ietf.org/internetdrafts/draft-ietf-manet-zone-zrp-04.txt, last accessed on Jan 2006

26. Zygmund J. Haas and Marc R. Pearlman, “The performance of query control schemes for the zone routing protocol”, IEEE/ACM Transactions on Networking,Vol. 9, No. 4, pp. 427–438, Aug 2001.

27. Samir, Das, Robert, Castaneda, Jiangtao Yan, “Simulation-Based Performance Evaluation of Routing Protocols for Mobile Ad Hoc Networks”, Mobile Networks and Applications, May 2000, pp. 179–189, www.csee.umbc.edu/~krishna/cs628/Papers/p179-das.pdf, last accessed on Jan 2006.

28. M. Gerla and J.T.-C. Tsai, “Multicluster, mobile, multimedia radio network”, ACM/Baltzer Journal of Wireless Networks. vol. 1, (no. 3), pp. 255–265, 1995.

29. P. Krishna, N.H. Vaidya, M. Chatterjee and D.K. Pradhan, “A clusterbased approach for routing in dynamic networks”, ACM SIGCOMM Computer Communication Review, pp. 49–65, Apr 1997.

30. S. Murthy, J.J. Garcia-Luna-Aceves, An efficient routing protocol for wireless networks, ACM/Baltzer Mobile Networks and Applications 1(2) (1996) 183–197.

31. Murthy S. and Gracia-Luna-Aceves JJ. An Efficient Routing Protocol for Wireless Networks. ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communications Networks 1996; 183-197.

32. C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel" Proc. IEEE SICON'97, Apr.1997, pp.197-211 http:// www.ics.uci .edu/`~atm/adhoc/ paper -collection/gerla-routing-clustered sicon97.pdf

33. G. Pei, M. Gerla and T.-W. Chen, Fisheye State Routing in Mobile Ad Hoc Networks. In Proceedings of the 2000 ICDCS Workshops, Taipei, Taiwan, Apr. 2000, pp. D71-D78

34. C. E. Perkins and E. M. Royer, “Ad-hoc On-Demand Distance Vector Routing,” Proc. 2nd IEEE Wksp. Mobile Comp. Sys. and Apps., Feb. 1999, pp. 90–100.

35. D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad-Hoc Wireless Networks,” Mobile Computing, T. Imielinski and H. Korth, Eds.,Kluwer, 1996, pp. 153–81.

36. C. E. Perkins and E. M. Royer, “Ad Hoc On Demand Distance Vector (AODV) Routing,” IETF Internet draft, draft-ietf-manet-aodv-02.txt, Nov.1998

37. L. Ji and M. S. Corson, “A Lightweight Adaptive Multicast Algorithm,”Proc. GLOBECOM ’98, Nov. 1998, pp. 1036–42.

38. C.-K. Toh and George Lin, "Implementing Associativity-Based Routing for Ad Hoc Mobile Wireless Networks," Unpublished article, Mar. 1998.

39. V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. INFOCOM '97, Apr. 1997.

40. Johnson DB. and Maltz DA. Dynamic Source Routing in Ad-Hoc Wireless Networking,Mobile Computing; Kluwer Academic Publishing: New York, 1996.

41. R. Dube et al., "Signal Stability based Adaptive Routing (SSA) for Ad-Hoc Mobile Networks," IEEE Pers. Commun., Feb. 1997, pp. 36–45.

42. J. Jubin and J. Tornow, "The DARPA Packet Radio Network Protocols,"Proc. IEEE, vol. 75, no. 1, 1987, pp. 21–32.

43. C-K. Toh, "A Novel Distributed Routing Protocol To Support Ad-Hoc Mobile Computing," Proc. 1996 IEEE 15th Annual Int'l. Phoenix Conf. Comp. and Commun., Mar. 1996, pp. 480–86.

44. Navid Nikaein, Christian Bonnet and Neda Nikaein, HARP - Hybrid Ad Hoc Routing Protocol, in proceeding of IST 2001: International Symposium on Telecommunications, Iran/Tehran 2001.

45. M. Joa-Ng and I-Tai Lu, A peer-to-peer zone-based two-level link state routing for mobile ad hoc net-works, IEEE on Selected Areas in Communications, vol. 17, no. 8, pp. 1415 1425, 1999.

46. Mingliang Jiang, Jinyang Li and Y. C. Tay. Cluster Based Routing Protocol (CBRP), Internet draft,draft-ietf-manet-cbrp-spec-01.txt.

47. A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, Scalable routing strategies for ad hoc wireless networks. IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks, August 1999, p1369-p1379

48. Y.ko and N.H.Vaidya,"Location aided routing(LAR) in mobile adhoc network, In proceedings of ACM/IEEE international conference in mobile computing and networking(MobiCom), 1998,pp 66-75.

49. M. Bakhouya and A. Nait-Sidi-Moh, "Localisation et Routage Géographique dans les Réseaux Mobiles Ad Hoc à Large Echelle", Book Chapter, Geopositionement et Mobilité, PPUR-UTBM, to appear,2009.

50. S. Basagni, I. Chlamtac, V.R. Syrotiuk, and B.A. Woodward, "A Distance Routing Effect Algorithm for Mobility (DREAM)", MOBICOM'9, 1999.

51. T. Camp, J. Boleng, B. Williams, L. Wilcox, and W. Navidi, "Performance Comparision of Two Location Based Routing Protocols for Ad Hoc Networks", Proceedings of the IEEE INFOCOM, pp. 1678- 1687, 2002.

52. X. Hong; K. Xu, and M. Gerla, "Scalable Routing Protocols for Mobile Ad hoc Networks", IEEE Network, Vol. 16, Issue 4, pp. 11-21, 2002.

53. P. F. Tsuchiya, "The Landmark Hierarchy: a new hierarchy for routing in very large networks," In Computer Communication Review, vol.18, no.4, Aug. 1988, pp. 35-42.

54. Bilal Maqbool Beigh, Prof.M.A.Peer, "Performance Evaluation of Pro-Active Routing Protocols with Fading Models: An Empirical Evaluation using Ns-2" International Journal of Engineering science and Technology Volume 3 issue 1, January2011.

55. Bilal Maqbool Begh, Prof M.A.Peer and Dr.S.M.K.Quadri ," Benchmarking for Performance Analysis of Routing Protocols for Adhoc Wireless Networks.", International journal of computer science and technology, volume 1 issue 2, March 2011.

56. Ge M, Lam K-Y, Gollmann D, Chung S-L, Chang C-C, Li J-B. A robust certification service for highly dynamic MANET in emergency tasks. International Journal of Communication Systems; 2009.

57. Haas P-J. Stochastic petri nets: modelling, stability, simulation. Springer series in operations research; 2002.

58. Bertocchi, F et.al, "Performance Comparison of Routing Protocols for Ad hoc networks", In proceedings of Global Telecommunications Conference, 2003, pp 1033-1037.

59. Bertocchi, F et.al, "Performance Comparison of Routing Protocols for Ad hoc networks", In proceedings of Global Telecommunications Conference, 2003, pp 1033-1037.

60. Bai, Fan; Helmy, Ahmed (2006). A Survey of Mobility Models in Wireless Adhoc Networks. (Chapter 1 in Wireless Ad-Hoc Networks. Kluwer Academic. 2006).

61. C.Perkins, E.B.Royer and S.Das,"AdHoc On-Demand Distance Vector (AODV) Routing", RFC 3561, IETF Network Working Group,July 2003

62. Cooperation stimulating mechanism for MANETs using hash chains. Future Generation Computer Systems 2009

63. Efficient certification path discovery for MANET. EURASIP Journal on Wireless Communications and Networking 2010.

64. Liu Y, Lia K. A novel reputation computation model based on subjective logic for mobile ad hoc networks. Future Generation Computer Systems 2010

65. Luoa J, Liu X, Fana M. A trust model based on fuzzy recommendation for mobile ad-hoc networks. Computer Networks 2009

66. Marchanga N, Dattab R. Collaborative techniques for intrusion detection in mobile ad-hoc networks. Ad Hoc Networks 2008.

67. Merwe J-V-D, Dawoud D, McDonald S. A survey on peer-to-peer key management for mobile ad hoc networks. ACM Computing Surveys 2007.

68. Marias G-F, Georgiadis P, Flitzanis D, Mandalas K. Cooperation enforcement schemes for MANETs: a survey. In: Wireless communication and mobile computing; 2006.

69. Zouridaki C, Mark B-L, Hejmo M, Thomas R-K. E-Hermes: a robust cooperative trust establishment scheme for mobile ad hoc networks. Ad Hoc Networks 2009.

70. Verma Amandeep, (2011), “A Study of Performance Comparisons of Simulated Ad hoc Network Routing Protocols,” International Journal of Computer Technology and Applications, pp. 565-569.

71. Zhiyuan Li, (2009), “Geographic Routing Protocol and Simulation”, Proceedings of International workshop on Computer Science and Engineering, pp. 404-407

72. Evaluation of a Hybrid Sensor and Vehicular Network to Improve Road Safety”, 7th ACM PEWASUN 2010, Bodrum, Turkey.

73. R.S. Raw, S. Kumar, S. Das, (2010) “An Efficient Position-Based Routing Protocol for Vehicular Ad Hoc Network in City Traffic Scenarios”, RISTEP-2010, NIT Srinagar, India.

74. Kuo C., Pang A., Chan S.: Dynamic Routing with Security Considerations. IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 1, pp. 48-58. (2009).

75. T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, L. Viennot, Optimized link state routing protocol for ad hoc networks, in: Proceedings of the IEEE INMIC, 2001, pp. 62-68.

76. C. Chiang, H. Wu, W. Liu, M. Gerla, Routing in clustered multihop, mobile wireless networks, in: Proceedings of IEEE SICON, 1997, pp. 197-211.

77. S. Murthy, J. Garcia-Luna-Aceves, An efficient routing protocol for wireless networks, MONET 1 (2)(1996) 183-197.

78. J. Garcia-Luna-Aceves, M. Spohn, Source-tree routing in wireless networks, in: Proceedings of the IEEEICNP, 1999, pp. 273-282.

79. S. Roy, J. Garcia-Luna-Aceves, Using minimal source trees for on-demand routing in ad hoc networks,in: Proceedings of the IEEE INFOCOM, 2001, pp. 1172-1181.

80. P. Samar, M. Pearlman, S. Haas, Independent zone routing: an adaptive hybrid routing framework forad hoc wireless networks, IEEE/ACM Transactions on Networking 12 (4) (2004) 595-608.

81. G. Pei, M. Gerla, T.-W. Chen, Fisheye state routing in mobile ad hoc networks, in: Proceedings of ICDCS Workshop on Wireless Networks and Mobile Computing, 2000, pp. D71-D78.

82. L. Kleinrock, K. Stevens, Fisheye: A lenslike computer display transformation, Tech. rep., Dept. Of Computer Science, UCLA (1971).

83. G. Pei, M. Gerla, X. Hong, LANMAR: landmark routing for large scale wireless ad hoc networks with group mobility, in: Proceedings of the ACM MobiHoc, 2000, pp. 11-18.

84. G. N. Aggelou, R. Tafazolli, RDMAR: a bandwidth-e±cient routing protocol for mobile ad hoc networks,in: Proceedings of the IEEE WoWMoM, 1999, pp. 26-33.

85. S.-C. Woo, S. Singh, Scalable routing protocol for ad hoc networks, Wireless Networks 7 (5) (2001) 513-529.

86. G. Wang, Y. Ji, D. C. Marinescu, D. Turgut, A routing protocol for power constrained networks with asymmetric links, in: Proceedings of the ACM Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN), 2004, pp. 69-76.

87. Y. Ko, N. Vaidya, Location-Aided Routing (LAR) in mobile ad hoc networks, in: Proceedings of the ACM MOBICOM, 1998, pp. 66-75.

88. Y. Ko, N. Vaidya, Location-Aided Routing (LAR) in mobile ad hoc networks, Wireless Networks 6 (4) (2000) 307-321.

89. S. Basagni, I. Chlamtac, V. Syrotiuk, B. Woodward, A distance routing algorithm for mobility (DREAM), in: Proceedings of the ACM MOBICOM, 1998, pp. 76-84.

90. B. Karp, H. Kung, GPSR: greedy perimeter stateless routing for wireless networks, in: Proceedings of the ACM MOBICOM, 2000, pp. 243-254.

91. J. Li, P. Mohapatra, LAKER: location aided knowledge extraction routing for mobile ad hoc networks, in: Proceedings of the IEEE WCNC, 2003, pp. 1180-1184.

92. L. Blazevic, S. Giordano, J.-Y. L. Boudec, Self organized routing in wide area mobile ad-hoc network, in: Proceedings of the IEEE GLOBECOM, 2001, pp. 2814-2818.

93. G. Boato, F. Granelli, MORA: a movement-based routing algorithm for vehicle ad hoc networks, in: Proceedings of the International Conference on Distributed Multimedia Systems (DMS), 2004, pp. 171-174.

94. A. Valera, W. K. G. Seah, S. V. Rao, Cooperative packet caching and shortest multipath routing in mobile ad hoc networks, in: Proceedings of the IEEE INFOCOM, Vol. 1, 2003, pp. 260-269.

95. M. K. Marina, S. Das, On-demand multi path distance vector routing in ad hoc networks, in: Proceeding of the IEEE ICNP, 2001, pp. 14-23.

96. A. J. Schwab and P. Fischer, "Maxwell, Hertz, and German radio-wave history," *Proc. IEEE*, vol. 86, pp. 1312–1318, July 1998.

97. G. C. Corazza, "Marconi's history," *Proc. IEEE*, vol. 86, pp. 1307–1311, July 1998.

98. Q. Bi, G. I. Zysman, and H. Menkes, "Wireless mobile communications at the start of the 21st century," *IEEE Commun. Mag.*, vol. 39, pp. 110–116, Jan. 2001