COMPARISON OF ENERGY EFFICIENT ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS

Thesis submitted in partial fulfillment of the requirements

for the award of degree of

Masters in Engineering

in

Computer Science and Engineering

Submitted By

Sushate Sandal

(Roll No.: 801032028)

Under the supervision of

Mr. Karun Verma

Assistant Professor, CSED

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA -147004

JUNE 2012

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Comparison of Energy Efficient Routing Protocols in Mobile Ad-Hoc Networks"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Computer Science and Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of ***Mr. Karun. Verma*** and refers other researcher's works which are duly listed in the reference section.

The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

(**Sushate Sandal**)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(**Mr. Karun. Verma**)
Assistant Professor
Computer Science and Engineering Department
Thapar University
Patiala.

Countersigned by:

(**Dr. Maninder Singh**)
Assoc. Professor & Head
Computer Science & Engineering Department,
Thapar University,
Patiala.

(**Dr. S.K. Mohapatra**)
Dean (Academic Affairs)
Thapar University,
Patiala.

Acknowledgement

No volume of words is enough to express my gratitude towards my guide, ***Mr. Karun. Verma****, Assistant. Professor and also the P.G. Coordinator, Computer Science and Engineering Department, Thapar University, who has been very concerned and has aided for all the material essential for the preparation of this thesis report. He has helped me to explore this vast topic in an organized manner and provided me with all the ideas on how to work towards a research-oriented venture.*

I am also thankful to ***Dr. Maninder Singh****, Head of Department, CSEDr, for the motivation and inspiration that triggered me for the thesis work.*

I would also like to thank the staff members and my colleagues who were always there in the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis.

Most importantly, I would like to thank my parents and the Almighty for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.

Sushate Sandal

801032028

Abstract

Mobile ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. These nodes change positions frequently. To accommodate the changing topology special routing algorithms are needed. The main classes of routing protocols are Flat Routing, Hierarchical Routing and Geographic Position assisted Routing.

For relatively small network flat routing protocols may be sufficient. However in large network either hierarchical or geographic routing protocols are best. There is not any single protocol that fits in all type of networks perfectly. The protocols have been chosen according to network characteristics, such as density, size, mobility of nodes and the application area.

In this work an attempt has been made to compare the energy awareness of three prominent routing protocols for MANETs:-Destination Sequenced Distance Vector Routing Protocol (DSDV), Ad hoc On Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols. The performance of these protocols has been analyzed on different parameters with varying simulation time. These simulations are carried out using the ns-2 network simulator.

Keywords: MANETS, DSDV, DSR, AODV.

Table of Contents

Certificate……………………………………………………………………...i

Acknowledgement……………………………………………………………ii

Abstract………………………………………………………………………iii

Table of Contents……………………………………………………………iv

List of Figures.. viii

List of Tables viii

CHAPTER 1 1

INTRODUCTION...1

1.1. MANETs 1

1.1.1. History...2

1.1.2. Mobile Ad hoc Network Communication Architecture: Protocol Stack .2

1.1.3. Features of MANET 3

1.1.4. Application of mobile Ad hoc network 4

1.1.5. Challenges facing MANET..5

1.2. Routing in Mobile Ad Hoc Network 6

1.2.1. Problem in routing with mobile Ad Hoc Network...................................7

1.3. Classification of Routing Protocol 7

1.3.1. Flat Routing 8

1.3.1a. Proactive Routing Protocol 8

1.3.1b. Reactive Routing Protocol 9

1.3.2. Hierarchical Routing 9

1.3.3. Geographic Position Assisted Routing 9

CHAPTER 2 11

LITERATURE REVIEW 11

2.1. Power in wireless Network 11

2.2. Routing Protocol 11

2.2.1. Table Driven Routing Protocols 12
2.2.2. On Demand Routing Protocols 12
2.3. Destination Sequence Distance Vector Routing Protocol 12
2.3.1. Packet Routing and Routing Table Management in DSDV [17, 16] 13
2.4. Dynamic Source Routing protocol 16
2.4.1. Important Properties of the Protocol 16
2.4.1a. DSR Route Discovery [18, 19] 16
2.4.1b. DSR Route Maintenance [18, 19] 18
2.5. Ad Hoc on Demand Distance Vector Routing Protocol 19
2.5.1. RREQ 19
2.5.2. RREP 20
2.5.3. RERR 20
CHAPTER 3 23
OBJECTIVE & METHODOLOGY 23
3.1. Objective 23
3.2. Methodology 24
3.3. Simulation Environment 24
3.3.1. Ubuntu-10.04 24
3.3.2. The Network Simulator (NS2) 24
3.3.3. NS2 installation steps on Linux 25
3.3.4. Tool Command Language (Tcl) 26
3.3.5. The Network Animation (NAM) 26
3.3.6. The Trace File 27
3.3.7. Energy Model API 28
3.3.8. Energy Analysis through Trace Files 28
CHAPTER 4 30
RESULTS, PERFORMANCE EVALUATION AND ANALYSIS 30
4.1. Residual Energy Vs Time 30
4.2. Dropped Packet Vs Time Due to decrease in energy 32
4.3. Packet Delivery Fraction (ratio of packet sent/packet received) 35

CHAPTER 5 .... **36**

CONCLUSION AND FUTURE SCOPE **36**

References **37**

List of Publications **40**

Published 40

List of Figures

Figure 1.1 Mobile ad hoc network (MANETs)…………………………………1
Figure 1.2 Models of protocol stack ……………………………………………3
Figure 1.3 Classification of Routing Protocol in Mobile Ad hoc Network…….8
Figure 2.1 Power Consumption in IEEE 802 based networks…………………11
Figure 2.2 Example of Ad hoc network………………………………………..13
Figure 2.3 DSDV packet routing example……………………………………..15
Figure 2.4 Route Discovery example…………………………………………..17
Figure 2.5 Route Maintenance example………………………………………..18
Figure 2.6 A possible path for a route replies……………………………….....20
Figure 3.1 Running NS2 programs……………………………………………..25
Figure 3.2 Installation of NS2………………………………………………….26
Figure 3.3 Contents of .tr file…………………………………………………..29
Figure 4.1 Residual energy Vs time in DSDV…………………………………31
Figure 4.2 Residual energy Vs time in DSR…………………………………...31
Figure 4.3 Residual energy Vs time in AODV………………………………...32
Figure 4.4 Dropped Packet Vs Time in DSDV………………………………...33
Figure 4.5 Dropped Packet Vs Time in DSR…………………………………..33
Figure 4.6 Dropped Packet Vs Time in AODV………………………………..34
Figure 4.7 Packet Delivery Fraction in MANET’s…………………………….35

List of Tables

Table 1.1 Application of MANET’s……………………………………………….4
Table 2.1 Routing table of node H6 at one instant ……………………………14
Table 2.2 A route request message……………………………………………..20
Table 4.1 Description of Trace file……………………………………………..27
Table 5.1 Packet Delivery Fraction of various routing protocols in MANET...35

CHAPTER 1

INTRODUCTION

1.1. MANETs

A mobile ad hoc network (MANETs) consists of mobile hosts prepared with wireless communication devices. Each node participating in the network acts both as host and a router and are able to forward packets for other nodes. It is a self-configuring network of mobile nodes connected by wireless links with no access point [1, 2]. In other words, ad hoc network do not rely on any fixed infrastructure. The Communication in MANET takes place by using multi-hop paths. The density of nodes and the number of nodes are depends on the applications in which it is being used.

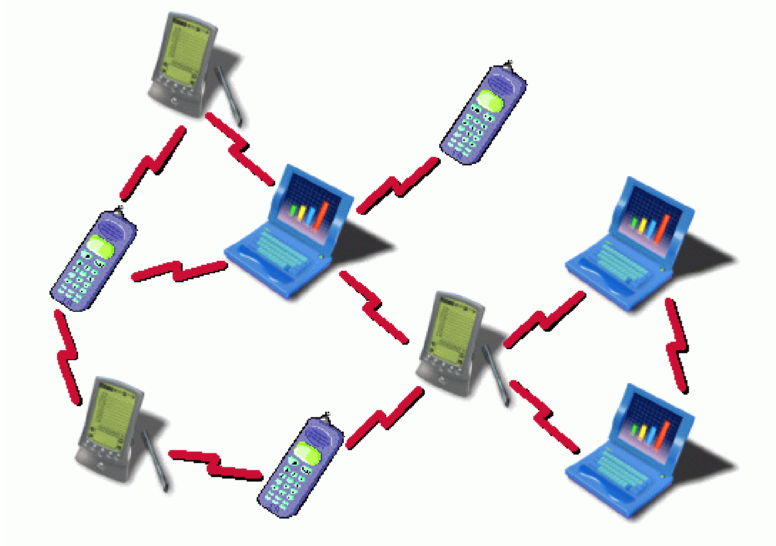


Figure 1.1 A mobile ad hoc network (MANETs) [2].

Nodes in the MANET share the wireless medium and the topology of the network changes irregularly and dynamically. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication [1]. In MANET, breaking of communication link is very frequent, as nodes are free to move to anywhere. The mobile hosts can move randomly and can be turned on or off without notifying other hosts. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts placed between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area.

1.1.1. History

The life cycle of mobile ad hoc network can be characterized into first, second and third generation. Present ad hoc network are considered the third generation [3]. The first generation of ad hoc network can be traced back to 1970's. In 1970's, these are called Packet Radio Network (PRNET) [4]. The Defence Advanced Research Project Agency (DARPA) initiated research of using packet switched radio communication to provide reliable communication between computers and PRNET.

The PRNET is then evolved into the Survivable Adaptive Radio Network (SURAN) in the early 1980's. By the growing interest in the ad hoc networks, a various other great developments takes place in 1990's.

The working group of MANET is born in [4] Internet Engineering Task Force (IETF) who worked to standardized routing protocols for MANET and gives rise to the development of various mobile devices like PDA's, palmtops, notebooks, etc. Meanwhile the Development of Standard IEEE 802.11 (i.e. WLAN's) benefited the ad hoc network. Some other standards are also developed that provide benefits to the MANET like Bluetooth and HIPERLAN.

1.1.2. Mobile Ad hoc Network Communication Architecture: Protocol Stack

This section describe that the Protocol stack of the mobile ad hoc network. This gives a complete picture and helps to understand mobile ad hoc network. Figure 1.2 shows the protocol stack which consist of five layers: physical layer, data link layer, network layer, transport layer and application layer. It is similar to TCP/IP protocol suite. In the left the figure of TCP/IP suite is illustrated.

On the right side, the MANET protocol stack is shown. The main difference between these two protocol stack is in network layer. Mobile nodes (hosts and routers) use an ad hoc routing protocol to route packets. In the physical and data link layer, mobile nodes run protocol that has been designed for wireless channel. Some options are the IEEE standard for wireless LAN, IEEE 802.11, the European ETSI stands for high speed wireless LAN, [5] and finally an industry approach towards wireless personal area network, i.e. wireless LAN at an even small range, Bluetooth.

<table>
<tr><th>TCP/IP SUIET</th><th colspan="2">MANET PROTOCOL STACK</th></tr>
<tr><td>APPLICATION</td><td colspan="2">APPLICATION</td></tr>
<tr><td>TRANSPORT</td><td colspan="2">TRANSPORT</td></tr>
<tr><td>NETWORK</td><td>NETWORK</td><td>AD-HOC ROUTING</td></tr>
<tr><td>DATALINK</td><td colspan="2">DATALINK</td></tr>
<tr><td>PHYSICAL</td><td colspan="2">PHYSICAL</td></tr>
</table>

Figure 1.2 Models of protocol stack.

This thesis focuses on an ad hoc routing which is held by network layer. The network layer is divided into two parts: Network and Ad Hoc Routing. The protocol used in the network part is Internet Protocol (IP) and the protocols which can be used in the ad hoc routing are Destination Sequence Distance Vector (DSDV).

1.1.3. Features of MANET

A Mobile Ad hoc Network has the following features [6]:

- *Autonomous terminal:* In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, working as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are the same in MANET.
- *Distributed operation:* In MANETs there is no control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a receiver and transmitter as needed, to implement functions e.g. security and routing.
- *Multihop routing:* Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with

the cost of lesser functionality. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

- *Dynamic network topology:* Since the nodes are mobile, the network topology may change rapidly and randomly and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing between themselves as they move and, forming their own network. Moreover, a user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network (e.g. Internet).
- *Light-weight terminals:* In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions [6].

1.1.4. Application of mobile Ad hoc network

A Mobile Ad hoc Network has the following application [2]

Table 1.1 Application of MANET's

Application	**Possible scenarios/services**
Tactical networks	• Military communication and operations • Automated battlefields
Emergency services	• Search and rescue operations • Disaster recovery • Policing and fire fighting • Supporting doctors and nurses in hospitals
Commercial and civilian environment	• E-commerce: electronic payments anytime and anywhere • Business: dynamic database access, mobile offices • Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks • Sports stadiums, trade fairs, shopping malls • Networks of visitors at airports

Home and enterprise networking	• Home/office wireless networking • Conferences, meeting rooms • Personal area networks (PAN), Personal networks (PN) • Networks at construction sites
Education	• Universities and campus settings • Virtual classrooms • Ad hoc communications during meetings or lectures
Sensor networks	• Home applications: smart sensors and actuators embedded in consumer electronics • Body area networks (BAN) • Data tracking of environmental conditions, animal movements, chemical/biological detection
Coverage extension	• Extending cellular network access • Linking up with the Internet, intranets, etc.
Entertainment	• Multi-user games • Wireless P2P networking • Outdoor Internet access • Robotic pets

1.1.5. Challenges facing MANET

The following list of challenges shows the inefficiencies and limitations that have to be overcome in a MANET environment [7]:

- *Limited wireless transmission range*: In wireless networks the radio band will be limited and the data rates it can offer are much lesser than what a wired network. This requires the routing protocols in wireless networks to use the bandwidth in a finest way by keeping the overhead as low as possible. Especially in MANET's due to frequent changes in topology, maintaining the topological information at all nodes involves more control over head, which in turn results in more bandwidth wastage [8].
- *Broadcast nature of the wireless medium*: The broadcast nature of the radio channel is that in which transmissions made by a node are received by all nodes within its direct transmission range. When a node is receiving data, no other node in its neighbor hood, except sender, should transmit. A node should get access to

the shared medium only when its transmissions do not affect any ongoing session. Even the network is vulnerable to hidden terminal problem and broadcast storms [7]. The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver [8].

- *Packet losses due to transmission errors*: In ad hoc wireless networks large amount of packet loss due to factors such as high bit error rate (BER) in the wireless channel, increased collisions due to the presence of hidden terminals, presence of interference, unidirectional links and frequent path breaks due to mobility of nodes [8].
- *Mobility-induced route changes*: The network topology in an ad hoc wireless network is extremely dynamic due to the movement of nodes. So an on-going session suffers frequent path breaks. This situation some time results to changes the route frequent. Communication in an ad hoc network is unstable such that running conventional protocols for MANET's over a high loss rate will degrade the performance. However, with high error rate, it is very difficult to deliver a packet to its destination.
- *Battery constraints*: This is one of the limited resources that form a major constraint for the nodes in an ad hoc network. So conservation of power and power-aware routing must be taken into consideration.
- *Potentially frequent network partitions*: The randomly moving nodes in an ad hoc network can lead to network partitions. In major cases, the intermediate nodes are the one which are highly affected by this partitioning. Ease of snooping on wireless transmissions (security issues). The radio channel used for ad hoc networks is broadcast in nature and is shared by all the nodes in the network. Data transmitted by a node is received by all the nodes within its direct transmission range. So an attacker can easily snoop the data being transmitted in the network [8].

1.2. Routing in Mobile Ad Hoc Network

A MANET can be defined as a system of independent mobile nodes that communicate over wireless links without any preinstalled infrastructure. This is due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engage them in multihop forwarding. Nodes in the network will act as host but also act as router to route data to/from other nodes [9].

Routing is the process of information exchange from one host to the other host in a network [1]. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc.

1.2.1. Problem in routing with mobile Ad Hoc Network

- *Asymmetric links:* Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad hoc networks as the nodes are mobile and constantly changing their position within network. For example consider a MANET where node X sends a signal to node Y but this does not tell anything about the quality of the connection in the reverse direction [10].
- *Routing overhead:* In wireless ad hoc networks, nodes often change their location within network. So, some slate routes are generated in the routing table which leads to unnecessary routing overhead.
- *Interference*: This is the major problem with mobile ad hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other node and corrupt the total transmission.
- *Dynamic Topology:* This is also the major problem with the ad hoc routing since the topology is not constant. The mobile node might move or medium characteristics might change. In ad hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. For example in a fixed network routing table updating takes place for every 30 second [10]. This updating frequency might be very low for ad hoc networks.

1.3. Classification of Routing Protocol

Classification of routing protocol in Mobile Ad Hoc Networks can be done in many ways. Most of these are depending on the strategy and network structure [11]. According to routing strategy the routing protocols can be characterized as Table-driven and Source initiated. While depending on the network structure these are classified as Flat routing, Hierarchical routing and Geographic position assisted routing [9]. Both the table driven and source initiated protocols comes under the flat routing which can be shown in figure 1.3.

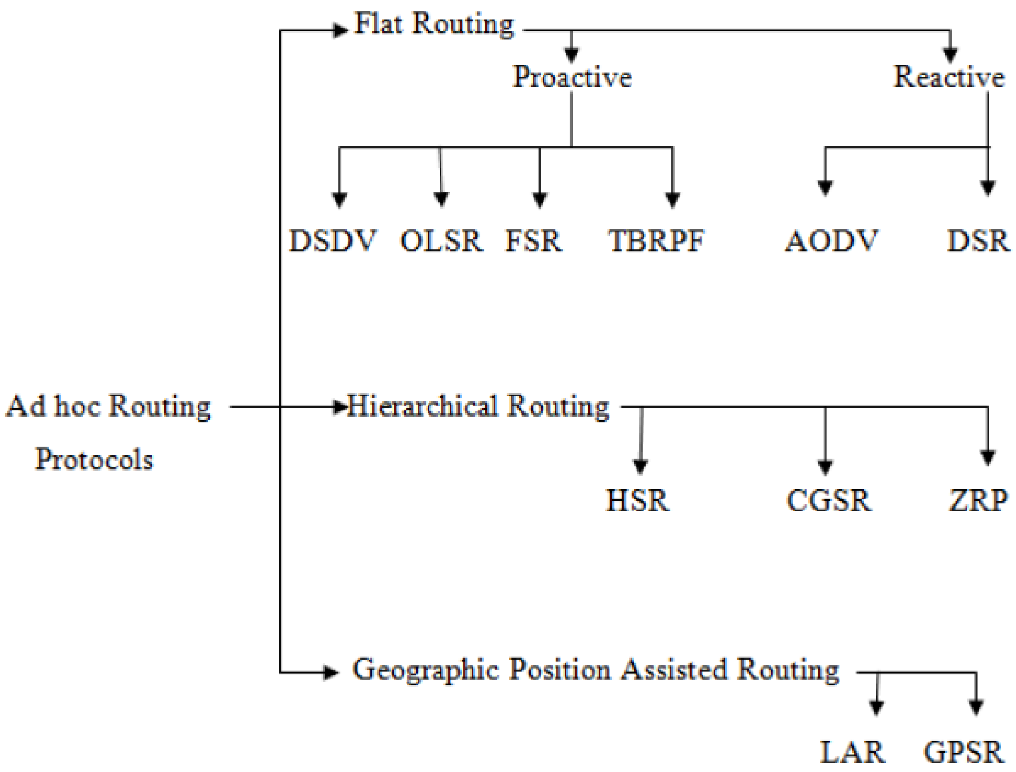


Figure 1.3 Classification of Routing Protocol in Mobile Ad hoc Network

1.3.1. Flat Routing

In the flat routing infrastructure, each network ID is represented individually in the routing table. The network IDs have no network/subnet structure and cannot be summarized. No effort is made to organize the network or its traffic, only to discover the best route hop by hop to a destination by any path. Think of this as all routers sitting on a flat geometric plane. Flat routing protocols are divided into [11] two classes: *Proactive Routing (Table Driven) Protocol and Reactive Routing (On-demand) Protocols.* In both protocol classes all nodes participating in routing play an equal role. They have been further classified after their design principles. Proactive Routing is mostly based on Linked State (LS) and On-demand routing is based on Distance-vector (DV).

1.3.1a. Proactive Routing Protocol

In proactive routing scheme every node continuously maintains complete routing information of the network. This is achieved by flooding network periodically with network status information to find out any possible change in network topology. Current routing protocol like Link State Routing (LSR) protocol (open shortest path first) and the Distance Vector Routing Protocol (Bellman-Ford algorithm) are not suitable to be used in mobile environment. Destination Sequenced Distance Vector Routing Protocol (DSDV) and Wireless routing protocols were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm [1].Examples of Proactive routing protocols are:

- Destination Sequenced Distance Vector Routing (DSDV).
- Optimized Link State Routing (OLSR).
- Fish-eye State Routing (FSR).
- Topology Broadcast Based on Reverse Path Forwarding (TBRPF).

1.3.1b. Reactive Routing Protocol

Every node in this routing protocol maintains information of only active paths to the destination nodes. A route search is needed for every new destination therefore the communication overhead is reduced at the expense of delay to search the route. Rapidly changing wireless network topology may break active route and cause subsequent route search [1].Examples of Reactive routing protocols are:

- Ad hoc On-demand Distance Vector Routing (AODV).
- Dynamic Source Routing (DSR).
- Temporally Ordered Routing Algorithm (TORA).

1.3.2. Hierarchical Routing

As the size of the wireless network increases, flat routing protocols will produced much more overhead for the MANET. In this case Hierarchical Routing may be preferred. Hierarchical routing has different solutions to the organization of the routing nodes in MANET [11].Examples of Hierarchical routing protocol are:

- Cluster head-Gateway Switch Routing (CGSR).
- Zone Routing Protocol (ZRP).
- Hierarchical State Routing (HSR).

1.3.3. Geographic Position Assisted Routing

The geographical position of a mobile node can be used to improve the performance of routing algorithms. The global positioning system (GPS) can be used for acquiring position information. Location-aided routing (LAR) is similar to DSR but limits route discovery to certain geographical regions. Examples of Geographic Position Assisted Routing:

- Location-Aided Routing (LAR).
- Geographic Addressing and Routing (GeoCast).

CHAPTER 2

LITERATURE REVIEW

2.1. Power in wireless Network

A Mobile Ad Hoc network (MANET) is a collection of digital data terminals that can communicate with one another without any fixed networking infrastructure [12]. Since the nodes in a MANET are mobile, the routing and power management become critical issues. Wireless communication has the advantage of allowing untethered communication, which implies trust on portable power sources such as batteries. However, due to the slow advancement in battery technology, battery power continues to be a constrained resource and so power management in wireless networks remains to be an important issue.

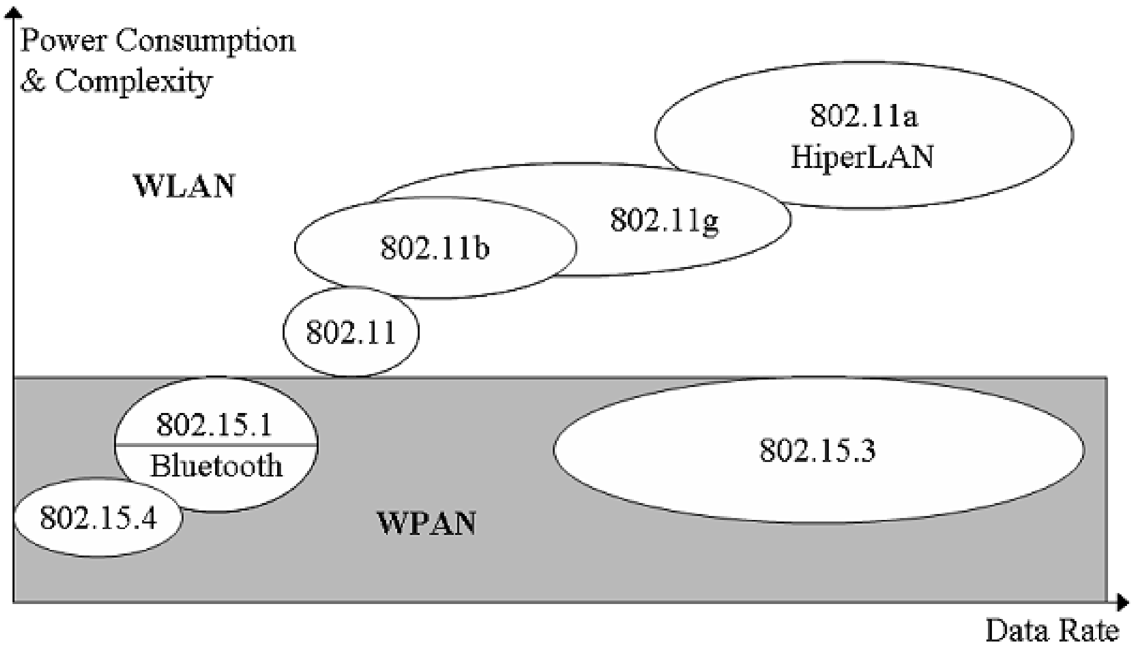


Figure 2.1 Power Consumption in IEEE 802 based networks [13].

2.2. Routing Protocol

Mobile Ad-hoc Network is a composition of a group of mobile, wireless nodes which cooperate in forwarding packets in a multi-hop fashion without any centralized administration. In MANET, each mobile node acts as a router as well as an end node which is either source or destination because the structure of the network changes dynamically [15]. Mobile Ad-Hoc Networks are characterized by a dynamic, multi-hop, rapid changing topology. The classification of routing protocol is:

2.2.1. Table Driven Routing Protocols

These protocols are also called as proactive protocols since they maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. The advantage is that routes to any destination are always available without the overhead of a route discovery. Example protocols are DSDV (17), OLSR, and CGSR etc.

2.2.2. On Demand Routing Protocols

These protocols are also called as reactive protocols[14] since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network. Example protocols are AODV [21], DSR [1 8], and TORA etc.

2.3. Destination Sequence Distance Vector Routing Protocol

Destination Sequence Distance Vector Routing(DSDV) is a hop-by-hop distance vector routing protocol. It is a proactive protocol in which each network node maintains a routing table that contains the distance of next-hop and the number of hops to all reachable destinations. Periodical broadcasts of routing updates keeps the routing table completely updated at all times [14]. To maintain the consistency of routing tables in a changing topology, each station periodically transmits updates, immediately when significant new information is available.

To guarantee loop free DSDV uses a concept of sequence numbers to indicate the freshness of a route. DSDV is adapted from the conventional Routing Information Protocol (RIP) to ad hoc network routing[16]. It adds a new attribute, sequence number, to each route table entry of the conventional RIP. Using the newly added sequence number, the mobile nodes can distinguish old route information from the new and thus prevent the formation of routing loops.

2.3.1. Packet Routing and Routing Table Management in DSDV[17, 16]

In DSDV, each mobile node of an ad hoc network maintains a routing table, which lists all available destinations, the metric and next hop to each destination and a sequence number generated by the destination node. Using such routing table stored in each mobile node, the packets are transmitted between the nodes of an ad hoc network.

When network topology changes are detected, each mobile node advertises routing information using broadcasting or multicasting a routing table update packet. The update packet starts out with a metric of one to direct connected nodes. This indicates that each receiving neighbor is one metric (hop) away from the node. It is different from that of the conventional routing algorithms. After receiving the update packet, the neighbors update their routing table with incrementing the metric by one and retransmit the update packet to the corresponding neighbors of each of them. The process will be repeated until all the nodes in the ad hoc network have received a copy of the update packet with a corresponding metric.

The elements in the routing table of each mobile node change dynamically, so to keep consistency with dynamically changing topology of an ad hoc network. To reach this consistency, the routing information advertisement must be frequent or quick. Receiving the updated routing information, each node has to transmit data packet to other nodes upon request in the dynamically created ad hoc network.

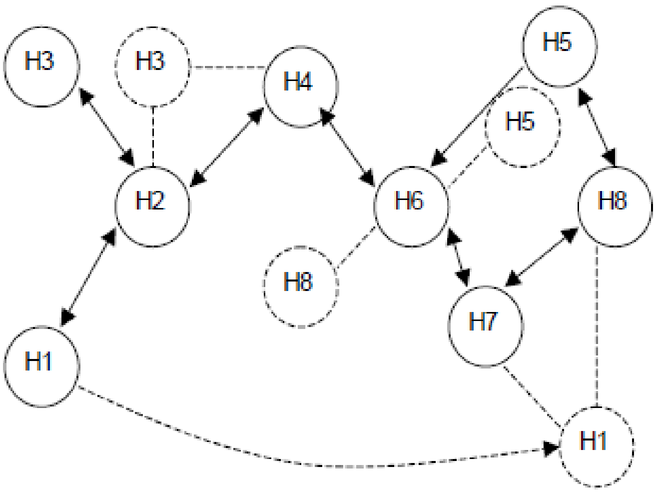
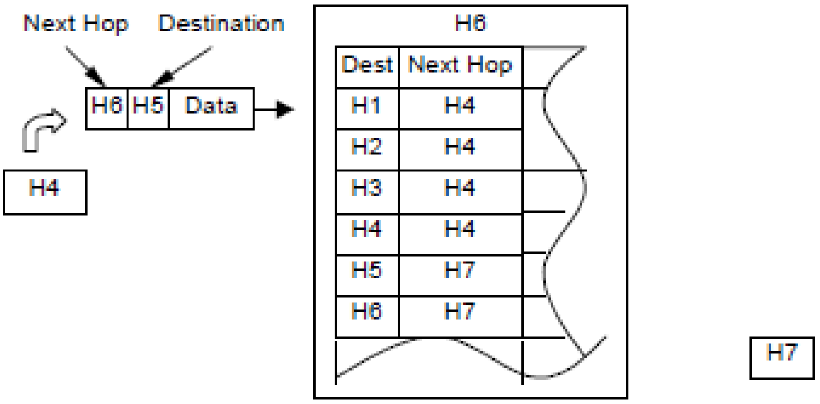


Figure 2.2Example of Ad hoc network [17].

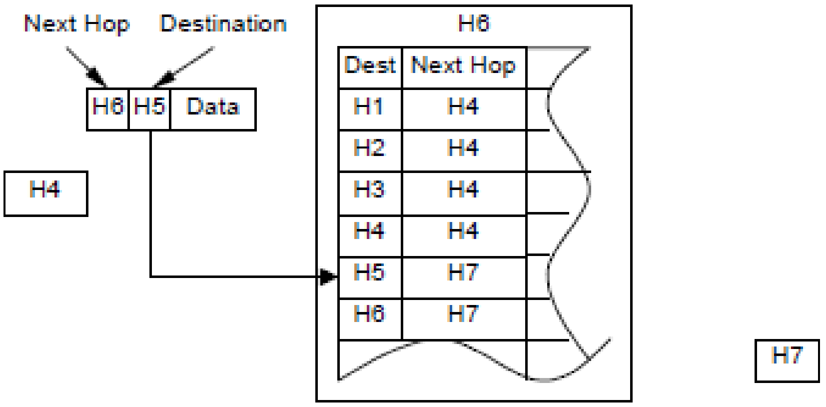
Figure 2.2 shows an example of an ad hoc network before and after the movement of the mobile nodes. Table 2.1 is the routing table of the node H6 at the moment before the movement of the nodes. The Install time field in the routing table helps to determine when to delete old routes.

Dest	Next Hop	Metric	Seq.No.	Install
H1	H4	3	S406_H1	T001_H6
H2	H4	2	S128_H2	T001_H6
H3	H4	3	S564_H3	T001_H6
H4	H4	1	S710_H4	T002_H6
H5	H7	3	S392_H5	T001_H6
H6	H6	0	S076_H6	T001_H6
H7	H7	1	S128_H7	T002_H6
H8	H7	2	S050_H8	T002_H6

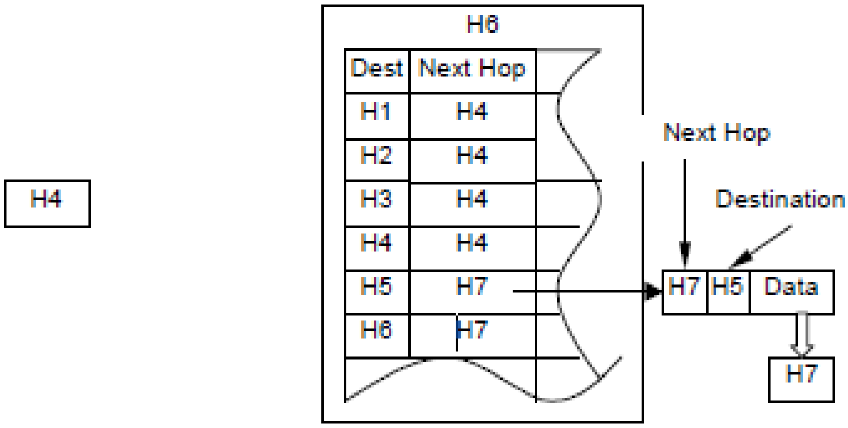
Table 2.1Routing table of node H6 at one instant [17].



a) Node H4 transmits a packet to node H6 for forwarding



b) Node H6 looks up the destination and route for forwarding the packet in its routing table



a) Node H6 forwards the packet to the next hop

Figure 2.3: DSDV packet routing example [17]

Figure 2.3 shows an example of packet routing procedure in DSDV. Node H4 wants to send a packet to the node H5 as shown in Figure 2.2. The node H4 checks its routing table and locates that the next hop for routing the packet is node H6. Then H4 sends the packet to H6 as shown in Figure 2.3a. Node H6 looks up the next hop for the destination node H5 in its routing table when it receives the packet (Figure 2.3b). Node H6 then forwards the packet to the next hop H7 as specified in the routing table as shown in Figure 2.3c. The routing procedure repeated along the path until the packet finally arrives its destination H5.

Advantages of DSDV [14]

• DSDV protocol guarantees loop free paths.

• Count to infinity problem is reduced in DSDV.

• Extra traffic can be reduced with incremental updates instead of full dump updates.

• Path Selection: DSDV maintains only the best path instead of maintaining multiple paths to every destination. With this, the amount of space in routing table is reduced.

Limitations of DSDV [14]

• Wastage of bandwidth due to unnecessary advertising of routing information even if there is no change in the network topology.

• DSDV doesn't support Multi path Routing.

• It is difficult to determine a time delay for the advertisement of routes.

• It is difficult to maintain the routing table's advertisement for larger network.

2.4. Dynamic Source Routing protocol

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. As nodes in the network move or join or leave the network [18], and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR routing protocol. Since the number or sequence of intermediate hops needed to reach any destination may change at any time, the resulting network topology may be quite rich and rapidly changing.

The protocol [18] is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network.

Assumptions [20]

- All nodes in the MANETs are willing to participate fully in the DSR protocol.
- The diameter of the MANET will often be small (5 to 10 hops).
- The speed with which node moves, is moderate with respect to the packet transmission latency.
- Nodes may be able to enable “promiscuous” receive mode on their wireless network interface.
- DSR operate with unidirectional link.
- Each node selects a single IP address.

2.4.1. Important Properties of the Protocol

The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network:

2.4.1a. DSR Route Discovery [18, 19]

When some node **S** originates a new packet destined to some other node **D**, it places in the header of the packet a *source route* giving the sequence of hops that the packet should follow on its way to **D**. Normally, **S** will obtain a suitable source route by searching its *Route Cache* of routes previously learned, but if no route is found in its cache, it will initiate the Route Discovery protocol to dynamically find a new route to **D**. In this case,**S** is called the *initiator* and **D** the *target* of the Route Discovery.

For example, figure 2.4 illustrates an example Route Discovery, in which a node **A** is attempting to discover a route to node **E**. To initiate the Route Discovery, **A** transmits a ROUTE REQUEST message as a single local broadcast packet, which is received by (approximately) all nodes currently within wireless transmission range of **A**. Each ROUTE REQUEST message identifies the initiator and target of the Route Discovery, and also contains a unique *request id*, determined by the initiator of the REQUEST. Each ROUTE REQUEST also contains a record listing the address of each intermediate node through which this particular copy of the ROUTE REQUEST message has been forwarded. This route record is initialized to an empty list by the initiator of the Route Discovery.

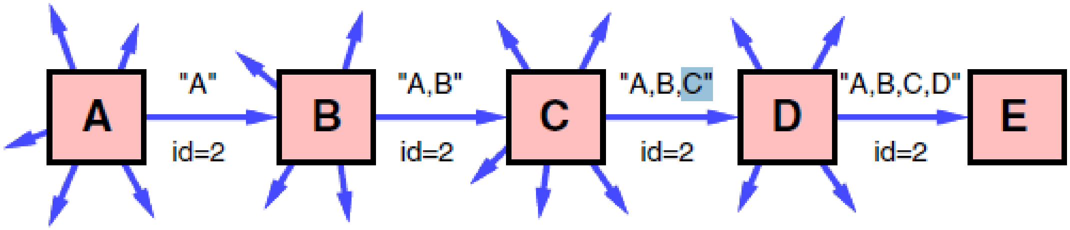


Figure 2.4 Route Discovery example: Node **A** is the initiator, and node **E** is the target [18].

When another node receives a ROUTE REQUEST, if it is the target of the Route Discovery, it returns a ROUTE REPLY message to the initiator of the Route Discovery, giving a copy of the accumulated route record from the ROUTE REQUEST. When the initiator receives this ROUTE REPLY, it caches this route in its Route Cache for use in sending subsequent packets to this destination. Otherwise, if this node receiving the ROUTE REQUEST has recently seen another ROUTE REQUEST message from this initiator bearing this same request id, or if it finds that its own address is already listed in the route record in the ROUTE REQUEST message, it discards the REQUEST. Otherwise, this node appends its own address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet (with the same request id).

In returning the ROUTE REPLY to the initiator of the Route Discovery, such as node **E** replying back to **A.** In Figure 2.4, node **E** will typically examine its own Route Cache for a route back to **A**, and if found, will use it for the source route for delivery of the packet containing the ROUTE REPLY. Otherwise, **E** may perform its own Route Discovery for target node **A**, but to avoid possible infinite recursion of Route

Discoveries, it must piggy back this ROUTE REPLY on its own ROUTE REQUEST message for **A**.

2.4.1b. DSR Route Maintenance [18, 19]

When originating or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that the packet has been received by the next hop along the source route. The packet is retransmitted (up to a maximum number of attempts) until this confirmation of receipt is received. For example, in the situation illustrated in Figure 2.5, node **A** has originated a packet for **E** using a source route through intermediate nodes **B**, **C**, and **D**. In this case, node **A** is responsible for receipt of the packet at **B**, node **B** is responsible for receipt at **C**, node **C** is responsible for receipt at **D**, and node **D** is responsible for receipt finally at the destination **E**.

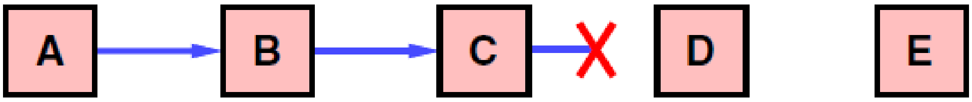


Figure 2.5 Route Maintenance example: Node **C** is unable to forward a packet from **A** to **E** over its link to next hop **D**[18].

This confirmation of receipt in many cases may be provided at no cost to DSR, either as an existing standard part of the MAC protocol in use (such as the link-level acknowledgement frame defined by IEEE 802.11), or by a *passive acknowledgement*(in which, for example, **B** confirms receipt at **C** by overhearing **C** transmit the packet to forward it on to **D**). If neither of these confirmation mechanisms are available, the node transmitting the packet may set a bit in the packet's header to request a DSR specific software acknowledgement be returned by the next hop, this software acknowledgement will normally be transmitted directly to the sending node, but if the link between these two nodes is uni-directional, this software acknowledgement may travel over a different, multi-hop path.

If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet, identifying the link over which the packet could not be forwarded. For example, in Figure 2.5, if **C** is unable to deliver the packet to the next hop **D**, then **C** returns a ROUTE ERROR to **A**, stating that the link from **C** to **D**is currently "broken". Node **A** then removes this broken link from its cache. Any retransmission of the original packet is a function for upper layer protocols such as

TCP. For sending such a retransmission or other packets to this same destination **E**, if **A** has in its Route Cache another route to **E** or it can send the packet using the new route immediately. Otherwise, it may perform a new Route Discovery for this target.

Advantages of DSR [19]

• Routes maintained only between nodes that need to communicate

• Route caching can further reduce route discovery overhead

• A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches.

Disadvantages of DSR [19]

• Packet header size grows with route length due to source routing

• Flood of route requests may potentially reach all nodes in the network

• Potential collisions between route requests propagated by neighboring nodes

• Old caches will lead to increased overhead.

2.5. Ad Hoc on Demand Distance Vector Routing Protocol

The AODV routing protocol is a reactive routing protocol, therefore routes are determined only when needed. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand. AODV is capable of both unicast and multicast routing [21]. It keeps these routes as long as they are desirable by the sources. Additionally, AODV creates trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. The sequence numbers are used by AODV to ensure the freshness of routes. It is loop-free, self-starting, and balance to large numbers of mobile nodes [21, 25]. AODV defines three types of control messages for route maintenance:

2.5.1. RREQ

A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Every node maintains two separate counters: a node sequence number and a broadcast id. The RREQ contains the following fields [21]:

Table 2.2 A route request message

Source address	Broadcast ID	Source sequence no.	Destination address	Destination sequence no.	Hop count

The pair <source address, broadcast ID> uniquely identifies a RREQ. Broadcast ID is incremented whenever the source issues a new RREQ.

2.5.2. RREP

A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

2.5.3. RERR

Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting originator list, containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

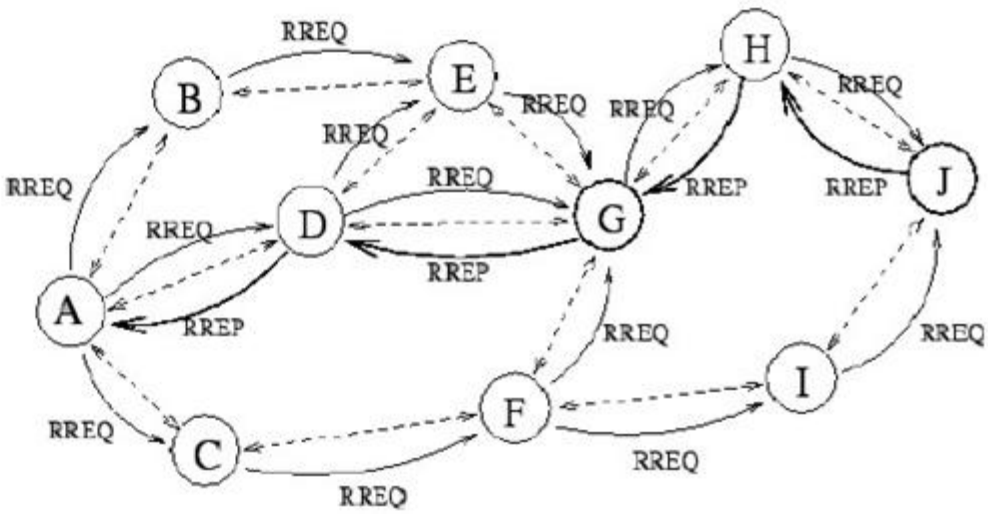


Figure 2.6 A possible path for a route replies: If A wishes to find a route to J [24]

The above Figure 2.6 illustrates an AODV route lookup session. Node **A** wants to initiate traffic to node **J** for which it has no route. **A** transmit of a RREQ has been done, which is flooded to all nodes in the network. When this request is forwarded to

J from **H**, **J** generates a RREP. This RREP is then unicasted back to **A** using the cached entries in nodes **H**, **G** and **D**.

AODV builds routes using a route request/route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network [23]. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware[25]. A node getting the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it.

As the RREP propagates back to the source, node set up forward pointers to the destination [22]. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destinations. After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

Advantages of AODV [14]

• Because of its reactive nature, AODV can handle highly dynamic behavior of Vehicle Ad-hoc networks.

• It used for both uncast and multicast using the ’J’ (Join multicast group) flag in the packets.

Limitations AODV [14]

• Requirement on broadcast medium: The algorithm expects/requires that the nodes in the broadcast medium can detect each other's broadcasts.

• Overhead on the bandwidth: Overhead on bandwidth will be occurred when an RREQ travels from node to node in the process of discovering the route.

• The routing info is always obtained on demand, including for common case traffic.

• It is vulnerable to misuse: The messages can be misused for insider attacks including route disruption, route invasion, node isolation, and resource consumption.

• AODV is designed to support the shortest hop count metric.

CHAPTER 3

OBJECTIVE&METHODOLOGY

3.1. Objective

A mobile ad-hoc network (MANET) is a type of wireless network which is a self-configured network of mobile nodes or routers, connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily, thus the network's wireless topology may change rapidly and unpredictably.

Routing is the task of moving information from a source to a destination in an internetwork. During this process, at least one intermediate node within the internetwork is encontered. The routing concept basically involves two activities : one is to determine optimal routing path and another is, transferring the information through an internetwork. Routing protocols use several metrics to calculate the best path for routing the packet to its destination. The process of path determination is that, routing algorithms initialize and maintain routing tables, which contain the total route information for the packet. This route information varies from one routing algorithm to another.

Energy is the most vital resource in mobile ad-hoc network, as recharging or replacing the battery is always not possible and it is very much costly. So,in routing protocols, energy should be considered as an important parameter. There are various routing protocols in MANET's such as Destination Sequence Distance Vector Routing (DSDV), Dynamic Source Routing (DSR) and Ad-Hoc On Demand Distance Vector (AODV) which are studied in this thesis.

Therefore, the objective of this work can be outlined as:

- To study and analyze these protocols.
- To simulate the protocol on a discrete event simulator.
- To perform a comparitive study on the basis of energy parameters.

3.2. Methodology

For this thesis work, the methodology that has been followed has been discussed in following steps:

- The DSDV, DSR and AODV protocols were studied.
- Linux as an Operating System was opted to work on.
- NS2 tool was installed for simulation and analysis.

3.3. Simulation Environment

3.3.1. Ubuntu-10.04

Ubuntu is a free operating system base on Linux. It provide simple and stylish interface. Ubuntu is based on Debian, sharing many of its packages, tools and techniques with that project. Ubuntu is confident that your files and data will stay protected. A built-in firewall and virus protection are available. Ubuntu is fast and loads quickly on any computer.

3.3.2. The Network Simulator (NS2)

Network simulator is a discrete event simulator targeted at networking research. Simulation can be defined as estimating how events might occur in the support of technology. NS2 provides large support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks [26].

There are two languages [27] used in NS2 C++ and OTcl (an object oriented extension of Tcl). The compiled C++ programming hierarchy makes the simulation efficient and execution times faster. The OTcl script which written by the users the network models with their own specific topology, protocols and all requirements need. The form of output produce by the simulator also can be set using OTcl. The OTcl script is written which creating an event scheduler objects and network component object with network setup helping modules. The simulation results produce after running the scripts can be use either for simulation analysis or as an input to graphical software called Network Animation (NAM) [27].

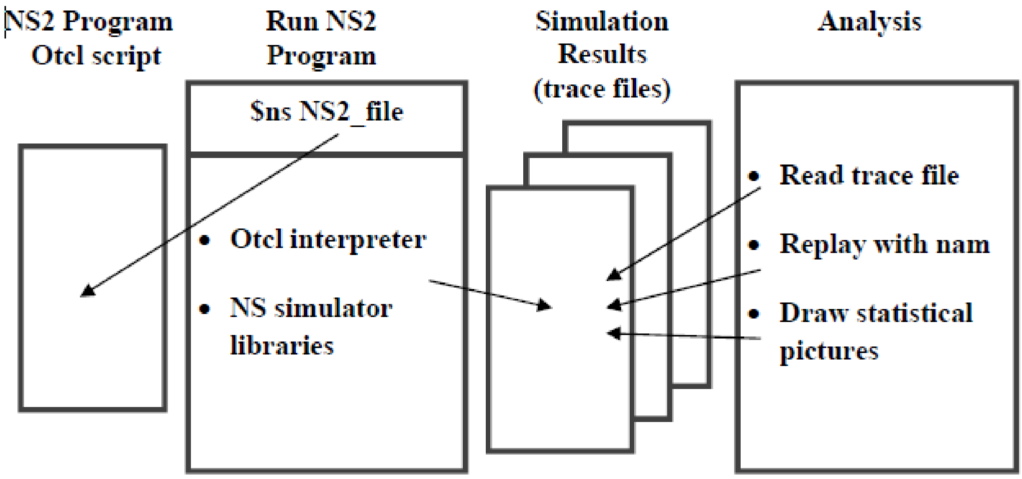


Figure 3.1 Running NS2 programs [27]

NS2 is an event driven network simulator, which can be implemented in Linux-based platform. This report will explain on how to install NS2 in Ubuntu platform. It is not recommend logging in as a root because installation at root may interfere with any important Linux files.

3.3.3. NS2 installation steps on Linux

NS2 is a popular discrete event simulator for simulating different types of networks. This article will show the steps to install NS2.34 on Linux.

Before installing NS2 on Linux, following package should be installed like tcl, tk, gcc, g++ and other required packages. If not, install it using the following command.

- *sudo apt-get install build-essential autoconf automake libxmu-dev*

Follow these simple steps one by one:

- *NS2 can be download by this command - ns-allinone-withpath-2.34.tbz.*
- *Then it can be copied it to the /usr/local directory by using a command - sudocp /tmp/ns-allinone-withpath-2.34.tbz /usr/local/*
- *After that change directory to /usr/local by using a command - cd /usr/local/*
- *Extract it using the following command - sudo tar -jxvf ns-allinone-withpath-2.34.tbz*
- *Again change the directory to ns-allinone-2.34 by using a command - cd ns-allinone-2.34/*

- *Now Install ns2 by using a command - sudo ./install*

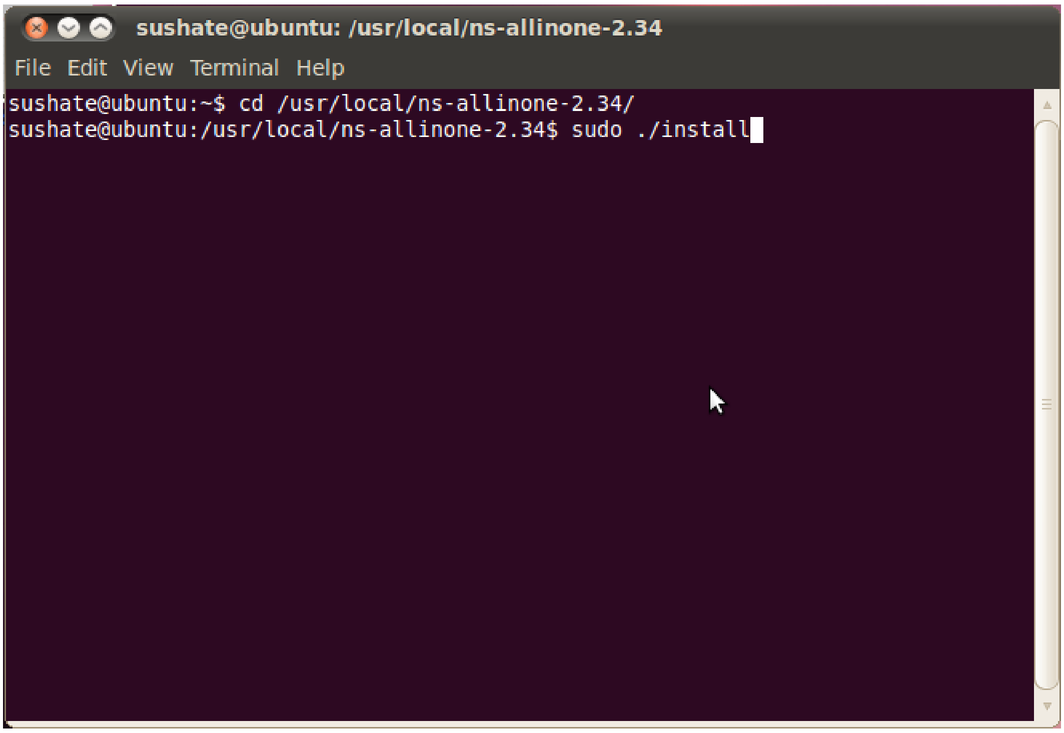


Figure 3.2 Installation of NS2.

3.3.4. Tool Command Language (Tcl)

Short for Tool Command Language, Tcl [28] is a powerful interpreted programming language developed by John Ouster out at the University of California, Berkeley. Tcl is a very powerful and dynamic programming language. It has a wide range of usage, including web and desktop applications, networking, administration, testing etc. Tcl is a truly cross platform, easily deployed and highly extensible. The most significant advantage of Tcl language is that it is fully compatible with the C programming language and Tcl libraries can be interoperated directly into C programs

3.3.5. The Network Animation (NAM)

The network animator [29] began in 1990 as a simple tool for animating packet trace data. This trace data is typically derived as output from a network simulator like ns or from real network measurements, e.g., using tcp dump. Steven McCanne wrote the original version as a member of the Network Research Group at the Lawrence Berkeley National Laboratory, and has occasionally improved the design, as he's needed it in his research. Marylou Orayani improved it further and used it for her Master's research over summer 1995 and into spring 1996. The nam development effort was an ongoing collaboration with the VINT project. Currently, it is being developed at ISI by the SAMAN and Conser projects.

3.3.6. The Trace File

After running the script, a trace file named '.tr' is generated. The trace file is an ASCII code files and the trace is organized in 12 fields as in figure 4.3 below. The format of the trace file is the following:

r 0.519 0 1 cbr 500 ------- 0 0.0 1.0 1 1
+ 0.52 0 1 cbr 500 ------- 0 0.0 1.0 4 4
- 0.52 0 1 cbr 500 ------- 0 0.0 1.0 4 4

Table 3.1 Description of Trace file

Event	The first field is ○ r receive at dest ○ + enqueue ○ - dequeue ○ d drop
Time	The second field is the time when event occurs
Source	The third field is input node at which event takes place
Destination	The fourth field is output node where the event takes place
Pkt. Type	The fifth field is the packet type such as continuous bit rate (cbr) or transmission control protocol (tcp).
Pkt. Size	The sixth field is the size of the packet such as 500 in our example
Flags	Seventh field are flags
Fid	The eighth field is the flow identity of IPv6, which can specify stream color of the NAM display and can be use for further analyze purposes.
Srce add.	The ninth field is the source address of the node in the form of node.port (e.g., 0.1 means node 0 port 1)
Dest. add.	The tenth field is the destination address of the node in the form of node.port (e.g., 2.3 means node 2 port 3)
Seq. no.	The eleventh is the network layer protocol's packet sequence number.

	NS keeps track of UDP packet sequence number for the analysis purposes.
PktId	The twelfth, which is the last field, is the unique identity of the packet.

3.3.7. Energy Model API

The energy model is used through the node-config API. The following parameters are generally there.

```
$ns node-config -adhocRouting $val(rp) \
        -llType $val(ll) \
        -macType $val(mac) \
        -ifqType $val(ifq) \
        -ifqLen $val(ifqlen) \
        -antType $val(ant) \
        -propType $val(prop) \
        -phyType $val(netif) \
        -channelType $val(chan) \
        -topoInstance $topo \
        -agentTrace ON \
        -routerTrace ON \
        -macTrace OFF \
        -movementTrace ON \
        -energyModel $opt(energymodel) \
        -idlePower 1.0 \
        -rxPower 1.0 \
        -txPower 2.0 \
        -sleepPower 0.001 \
        -transitionPower 0.2 \
        -transitionTime 0.005 \
        -initialEnergy $opt(initialenergy)
```

3.3.8. Energy Analysis through Trace Files

We have added energy breakdown in each state in the traces to support detailed energy analysis [49]. In addition to the total energy, now users will be able to see the energy consumption in different states at a given time. Following is an example from a trace file on energy as shown in figure 3.3.

[energy 979.917000 ei 20.074 es 0.000 et 0.003 er 0.006]

The meaning of each item is as follows:

Energy: total remaining energy

ei: energy consumption in IDLE state

es: energy consumption in SLEEP state

et: energy consumed in transmitting packets

er: energy consumed in receiving

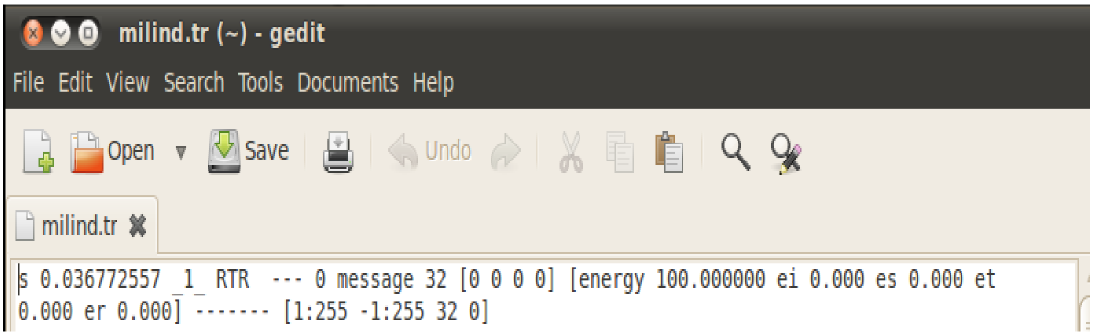


Figure 3.3 Contents of .tr file.

CHAPTER 4

RESULTS, PERFORMANCE EVALUATION AND ANALYSIS

In this chapter, the results of the simulation of the various protocols are analyzed on the bases of *.tr file. A comparison has been performed to analyze the energy efficiency among different routing protocols such as:

- Destination-Sequenced Distance-Vector (DSDV)
- Dynamic Source Routing (DSR)
- Ad-Hoc On-Demand Distance Vector (AODV)

The following parameters were use of for the analysis of various routing protocols:

- Residual Energy Vs Time
- Dropped Packet Vs Time Due to decrease in energy
- Packet Deliver Fraction (ratio of packet received/ packet sent)

4.1. Residual Energy Vs Time

After transmitting or receiving data to /from neighbors, some energy of nodes gets dissipated. So along with the passage of time the remaining energy or residual energy of nodes decreases.

The figure 4.1 shows the relationship between Residual Energy along y-axis and Time at x-axis for Destination-Sequenced Distance-Vector (DSDV) Routing Protocol.

It can be analyzed from the graph that the energy gets reduced gradually along with the time. Because DSDV is a proactive routing protocol in which each node maintains its routing table to forward packet to its neighbors. But at the end of the simulation, the energy of the node varies due to the addition of new nodes in the path because the MANET's do not have fixed infrastructure.

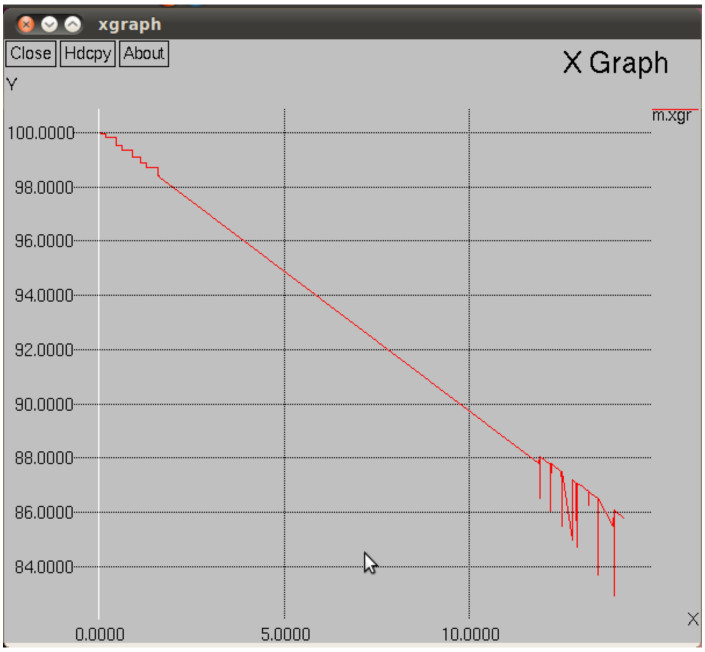


Figure 4.1 Residual energy Vs time in DSDV

The figure 4.2 shows the relationship between Residual Energy at y-axis and Time at x-axis for Dynamic Source Routing (DSR) Protocol.

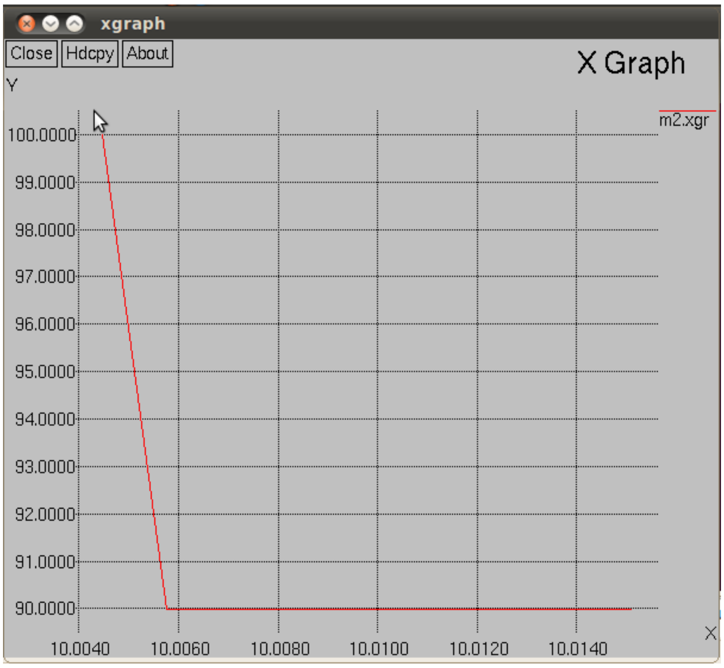


Figure 4.2 Residual energy Vs time in DSR

This graph show's that initially the reduction of energy is more. It happens because in DSR, initially route gets discovered from source to destination before sending a packet. After completing the route discovery, the packet gets transmitted from source to destination by using the same path.

The figure 4.3 shows the relationship between Residual Energy at y-axis and Time at x-axis for Ad Hoc on Demand Distance Vector(AODV) Routing Protocol.

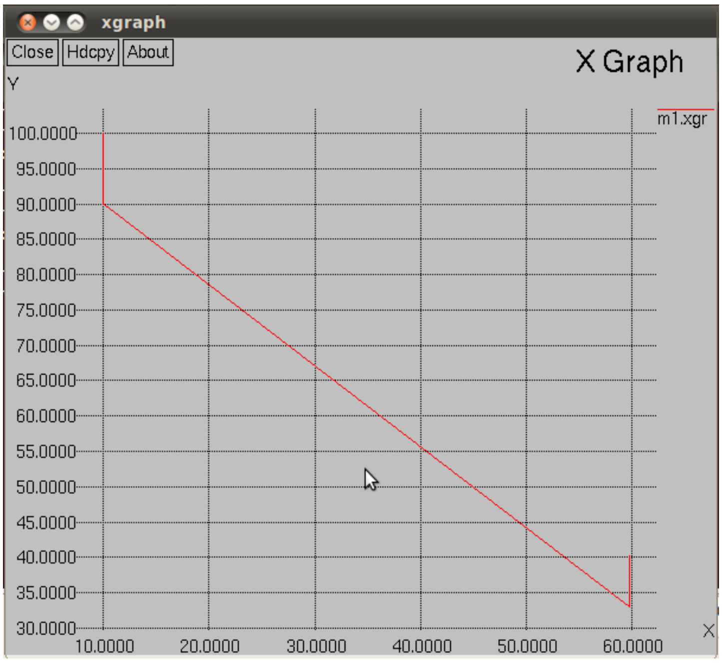


Figure 4.3 Residual energy Vs time in AODV

It can be analyzed from the graph that initially the energy loss is very fast.This is because of the REQUEST/REPLY mechanism in the protocols which require a large number of data packets to be transmitted. Due to varying network infrastructure, the energy increases at the end with the addition of new nodes.

4.2. Dropped Packet Vs Time Due to decrease in energy

As energy level decreases, destination nodes become unreachable or die, due to which some packets will be dropped. As the passage of time, energy decreases and number of dropped packets will be increased depending upon the routing algorithms.

Figure 4.4 shows the relation between the Packets dropped at y-axis and time, at x-axis for Time in Destination Sequence Distance Vector (DSDV) Routing protocol.

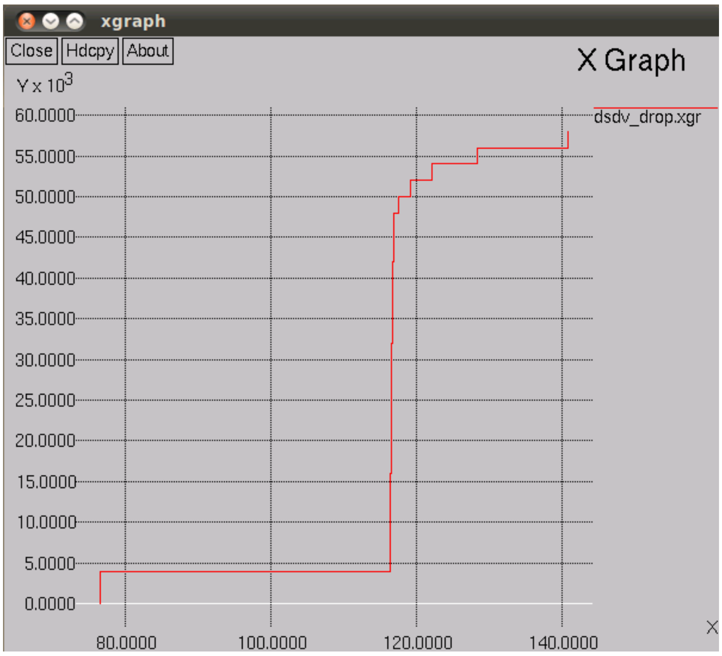


Figure 4.4.Dropped Packet Vs Time in DSDV

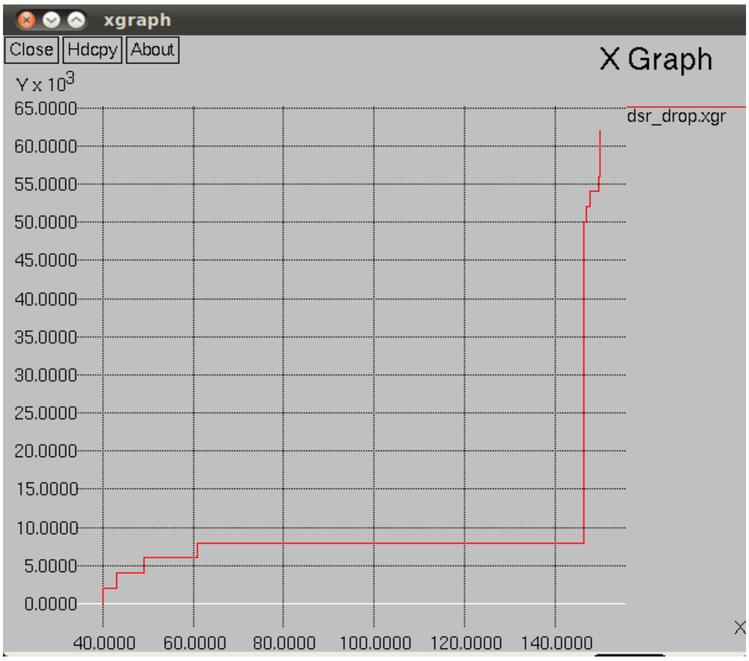


Figure 4.5.Dropped Packet Vs Time in DSR

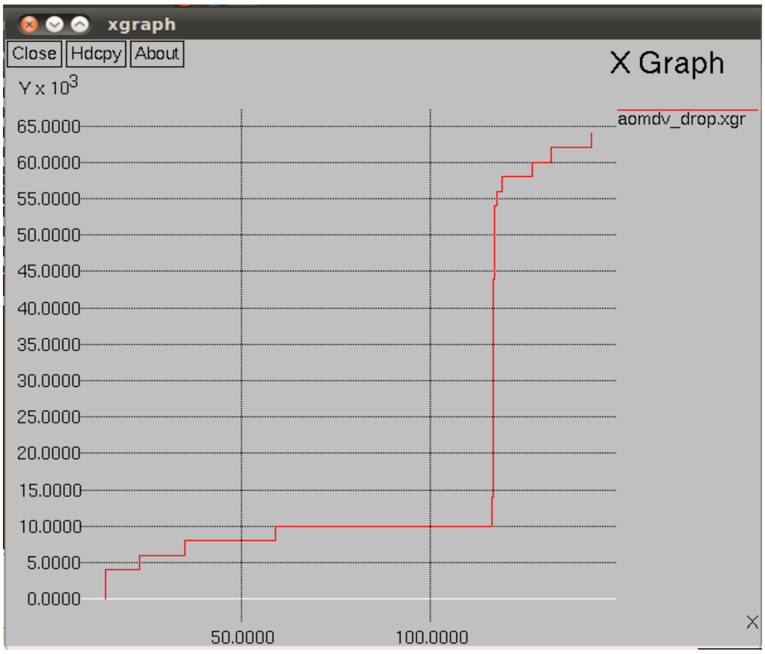


Figure 4.6 Dropped Packet Vs Time in AODV

As shown in figure 4.4, 4.5 and 4.6 in initial phase some packets are dropped. Then after some time, number of packets dropped increases due to lack of energy. DSR performs fine as compare to other two routing protocols. In DSR, packets get dropped only in the beginning and then for a long period of time, the drop rate becomes zero in figure 4.5. And then there is a rapid increase in number of packets that get dropped due to loss of energy.

In Flooding, number of packets dropped with respect to time increases very rapidly because in flooding packet is broadcasted to all neighbors, as shown in figure 4.4 and 4.6, energy decreases very rapidly and some nodes become dead very soon.

4.3. Packet Delivery Fraction (ratio of packet sent/packet received)

This is the ratio of the number of packets send to the number of packets received to the destination to those generated by the traffic source.

Table 4.1 Packet Delivery Fraction of various routing protocols in MANET's

Routing Protocol	No. of packets Send	No. of packets Received	PDF
DSDV	6474	6444	0.9954
DSR	7493	7470	0.9969
AODV	2236	2205	0.9861

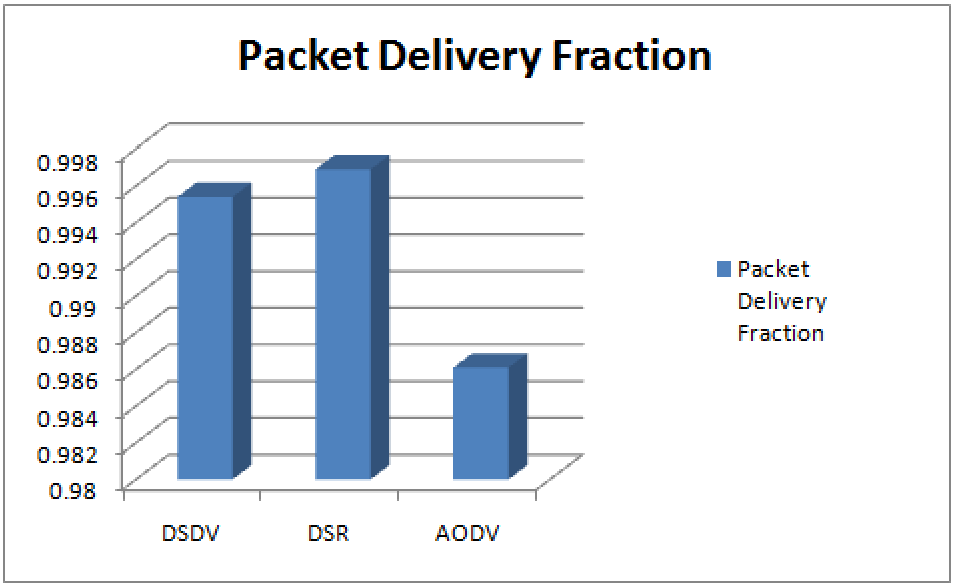


Figure 4.7 Packed Delivery Fraction.

As shown in figure 4.7 in term of Packet Delivery Fraction, AODV perform better than DSDV and DSR.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

Routing in MANET's is an interesting research area that has been growing in recent years. The main difficulty in MANET is faced because of the continuous change in the environment. With this changing environment a routing protocol is used to decide the best suitable route for sending data to the sink from a source node. One of the major concerns is to send this data on a route which consumes less power, because the power is a limited resource in mobile ad hoc networks. So to make our communication energy efficient, we have to choose a routing protocol which considers energy as an important parameter.

In this work, the performance of three protocols are studied against various parameters such as, residue energy, packet drop and packet deliver fraction. The three protocols Destination-Sequenced Distance-Vector (DSDV), Dynamic Source Routing (DSR) and Ad-Hoc On-Demand Distance Vector (AODV) have been compared using simulation. We conclude that initially in DSR the energy consumption is high as compare to DSDV or AODV. And if the MANET has to be set for small amount of time then DSDV and AODV should be preferred due to low initial packet loss and DSR should not be preferred to setup a MANET for small amount of time because initially there is a high packet loss.

It would be interesting to note the behavior of these protocols when the number of packets sends/ receive and the numbers of nodes in the network are increased. And also interesting to note the behavior of these protocols on a real life test.

References

[1] Amit Shrivastava, Nitin Chander, Prashanth Patlolla and Vivek Yadlapalli, "Overview of Routing Protocols in MANET's and Enhancements in Reactive Protocols", pp 1-8.

[2] Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester, "An Overview of Mobile ad hoc Networks: Applications &Challenges", Journal of the Communications **Network**, Vol. 3, July 2004, pp. 60-66.

[3] Vikaram Patal and Sonali Mote, "Mobile Ad hoc Networks: Opportunities and Future",pp 1-4.

[4] Humayun Bakht, "History of Mobile Ad hoc Networks" http://www.oocities.org/humayunbakht/HMANET.pdf, accessed on April 2012.

[5] M. S. Corson, J. P. Maker and G. H. Cirincione, "Internet Based Mobile Ad Hoc Networking", IEEE Internet Computing, Vol. 3, No. 4, July-August 1999, pp. 63-70.

[6] Jun-Zhao Sun, "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing", Info- tech and Info-net, vol.3, 2001, pp316 – 321.

[7] G. S. Mamatha and Dr. S. C. Sharma, "Analyzing the MANET Variations, Challenges, Capacity and Protocol Issues", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010.

[8] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Second Edition, Pearson Education, 2007.

[9] Laura Marie Feeney, "A taxonomy for routing protocols in mobile ad hoc networks", Technical report, Swedish Institute of Computer Science, Sweden, 1999.

[10] Charles E. Perkins and Pravin Bhagwat, "DSDV routing over a multi hop wireless network of mobile computers", Technical report, IBM Research and University of Maryland, USA, 29 Nov 2000.

[11] Ankur Khetrapal, “Routing techniques for Mobile Ad Hoc Networks Classification and Qualitative/Quantitative Analysis”, 2006, pp 1-7.

[12] M. Tamilarasi, S. Chandramathi and T.G. Palanivelu, “Efficient Energy Management for Mobile Ad Hoc Networks”, Ubiquitous Computing and Communication Journal, Vol. 3 No. 5, pp 1-8.

[13] Kevin Klues, “Power Management in Wireless Networks”, 24 Apr 2006, pp 1-24.

[14]P. Parvathi, “Comparative Analysis of CBRP, AODV, DSDV Routing Protocols in Mobile Ad-hoc Networks”, Computing Communication and Application (ICCCA), 2012, pp 1-4.

[15] Md. Monzur Morshed, Franz I. S. Ko, Dongwook Lim, Md. Habibur Rahman, Md. Rezaur Rahman Mazumder and Jyotirmoy Ghosh “Performance Evaluation of DSDV and AODV Routing Protocols in Mobile Ad-hoc Networks”, New Trends in Information Science and Service Science (NISS), 2010 , pp 399 – 403.

[16] C. E. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers”, Proceedings of ACM SIGCOMM, 1994, pp, 34–244.

[17] Guoyou He, “Destination-Sequenced Distance Vector (DSDV) Protocol”, pp 1-9.

[18] David B. Johnson, David A. Maltz and Josh Broch, “DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks”, 2001, pp 1-25.

[19] Sangeeta Biswal, Suneeta Mohanty and Dambarudhar Seth, “Study of DSR Routing Protocol in Mobile Adhoc Network”, International Conference on Information and Network Technology (IPCSIT), vol.4, Singapore 2011, pp 1-5.

[20] David B. Johnson and David A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”, Kluwer Academic Publishers, 1996, pp 1-18.

[21] C.E. Perkins and E.M. Royer, Ad-hoc On-Demand Distance Vector Routing, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.

[22] Charles E. Perkins, “Ad Hoc on Demand Distance Vector (AODV) Routing”, Internet draft, draft-ietf-manetaodv, August 1998.

[23] Per Johansson, Tony Larsson, Nicklas Hedman, Bartosz Mielczarek Mikael Degermark, “Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks”, Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, ACM New York, NY, USA, 1999, pp195-206.

[24]Ad-hoc distance vector Protocol for Mobile ad Hoc network http://www.olsr.org/docs/report_html/node16.html#adhoc_aodv#adhoc_aodv accessed on April 2012.

[25] Abdul Hadi AbdRahman, Zuriati Ahmad Zukarnain, “Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks”, European Journal of Scientific Research (ISSN), Vol.31, No.4, pp.566-576, 2009.

[26] Marc Greis, Ns Tutorial, http://www.isi.edu/nsnam/ns/tutorial/, accessed on March 2012

[27] Network Simulator, http://www.isi.edu/nsnam/ns/, accessed on March 2012.

[28] TCL Tutorial, http://www.tcl.tk/man/tcl/tutorial/tcltutorial.html, accessed on March 2012.

[29] Network Animation, http://csis.bits-pilani.ac.in/faculty/murali/resources/tutorials/ns2.htm, accessed on May 2012.

List of Publications

Published

Sushate Sandal and Karun Verma, "Power management techniques in Wireless Sensor Network", International Journal of Advances in Computing and Information Technology (IJACIT), Volume 1 Issue 2, 2012 - April Issue.