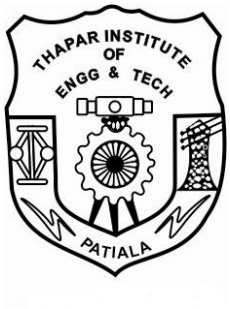
PERFORMANCE ANALYSIS OF CLUSTER BASED ROUTING PROTOCOL IN MANETs

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Software Engineering



By:
Ravi Kumar Bansal
8043118

Under the supervision of:
Mr. Anil Kumar Verma

MAY 2006

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY
(DEEMED UNIVERSITY)
PATIALA – 147004

Declaration

I hereby certify that the work which is being presented in the thesis entitled, **"Performance Analysis of Cluster Based Routing Protocol in MANETs"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in Software Engineering submitted in Computer Science and Engineering Department of Thapar Institute of Engineering and Technology (Deemed University), Patiala, is an authentic record of my own work carried out under the supervision of Mr. Anil Kumar Verma. The matter presented in this thesis has not been submitted for the award of any other degree of this or any other university.

Ravi Kumar Bansal
(8043118)

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

Mr. Anil Kumar Verma
Thapar Institute of Engineering and Technology
Patiala-147004

Countersigned by

Dr. (Mrs.) Seema Bawa
Head of Department
Computer Science & Engineering Department
Thapar Institute of Engg and Tech.
Tech Patiala.

Dr. T. P. Singh
Dean
Academic Affairs
Thapar Institute of Engg and
Patiala

The M.E. (Thesis) Viva-Voce examination of Ravi Kumar, Roll No 8043118 , M.E. (Software Engineering), Thapar Institute of Engineering and Teachnology , Patiala has been held on……..

Supervisor **External Examiner**

Acknowledgement

No volume of words is enough to express my gratitude towards my guide, Sh. Anil Kumar Verma, System Analyst cum Programmer, Computer Centre, TIET, who has been very concerned and has aided for all the material essential for the preparation of this thesis report. He has helped me 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. (Mrs.) Seema Bawa, Head, CSED and Sh. Rajesh Bhatia, P.G. Coordinator, 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 at the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis work.

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.

Ravi Kumar Bansal

8043118

Abstract

In the near future, computing environment can be expected based on the recent progresses and advances in computing and communication technologies. Next generation of mobile communications will include both prestigious infrastructured wireless networks and novel infrastructureless mobile ad hoc networks (MANETs). A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. The special features of MANET bring this technology great opportunities together with severe challenges. This thesis describes the fundamentals of ad hoc networking by giving its concept, features, and applications of MANET. Some of the technical challenges MANET poses are also presented. The routing protocols meant for wired networks can not be used for mobile ad hoc networks because of the mobility of nodes. The ad hoc routing protocols can be divided into two classes :- table-driven and on-demand. Routing in wireless mobile ad-hoc networks should be time efficient and resource saving. One approach to reduce traffic during the routing process is, to divide the network into clusters. This work mainly focuses on cluster-based routing protocol CBRP) and its comparative analysis with two other on demand routing protocols Adhoc On Demand Distance Vector(AODV) and Dynamic Source Routing (DSR) which do not use cluster based mechanism for routing .The results presented in this thesis illustrate the importance in carefully evaluating and implementing routing protocols when implementing an ad hoc network protocol.

Keywords: MANETs, Routing, CBRP, DSR, AODV

TABLE OF CONTENTS

CONTENTS

PAGE NO.

LIST OF FIGURES

CONTENTS *PAGE*

Chapter 1
Introduction

Wireless ad hoc network is a collection of mobile devices forming a network without any supporting infrastructure or prior organization. Nodes in the network should be able to sense and discover with nearby nodes .Due to the limited transmission range of wireless network interfaces, multiple network "hops" may be needed for one node to exchange data with another across the network. There are number of characteristics in wireless ad-hoc networks, such as the dynamic network topology, limited bandwidth and energy constraint in the network. Mobile ad hoc network is useful for different purpose e.g. military operation to provide communication between squads, emergency case in out-of-the-way places, medical control etc.

Routing protocol plays very important part in implementation of mobile ad hoc networks. Due to the nature of mobile ad hoc networks it is non-trivial problem to find path from source to the destination and perform the communication between nodes for a long period of time.

A number of routing protocols using a varirty of routing techniques have been proposed for use in MANETs . Adhoc On demand Distance Vector Routing (AODV) [1], Dynamic Source Routing (DSR) [2] , Temporally Ordered Routing Algorithm (TORA) [3], Location Aided Routing (LAR) [4] (in which nodes search for or maintain a route only when route is needed), and periodic (proactive) protocols such as Destination Sequence Distance Vector (DSDV) [5], Distributed Bellman Ford [6] (in which nodes periodically exchange routing information and than can always know a current route to each destination). Also, several protocols uses both reactive and proactive mechanism such as Zone Resolution Protocol (ZRP) [7], Cluster Based Routing Protocol (CBRP) [8].

The basic idea of on-demand routing protocols, is that a source node sends a route request and makes routing decision based on received route reply, which may be sent by destination or intermediate node. On-demand routing have several advantage, such as simplicity, correctness and flexibility. However, on-demand routing algorithms has the disadvantage of increasing per-packet overhead. This extra network overhead decreases the bandwidth available for transmission of data, increases the transmission

latency of each packet, and consumes extra battery power in the network transmitter and receiver hardware. Due to manner of propagation route request (flooding), it is difficult to limit dissemination of unnecessary packets.

The basic idea of proactive routing is periodically updating routing table via exchanging routing information. According to routing table, source node knows path or next hop to destination anytime when route needs. In proactive routing, route information is available when needed, resulting in little delay prior to data transmission. However proactive routing protocols are likewise not appropriate for mobile ad hoc networks, as they continuously use a large portion of the network capacity to keep the routing information current. Proactive routing protocols tend to distribute topological changes widely in the network, even though the creation/destruction of a new link at one end of the network may not be significant piece of information at the other end.

The hybrid routing protocols pretends to inherit the best parts of both reactive and proactive routing protocols. The main idea of the hybrid routing protocols is the limiting the set of forwarding nodes and using the proactive routing algorithm for nearly placed nodes which usually forward data to far placed nodes.

This thesis work invsestigates how the clustering in ad hoc networks can result in time efficient and resource saving routing. It describes the structure and working of an on demand routing protocol that is cluster based routing protocol in detail. In CBRP the nodes of a wireless network are divided into several disjoint or overlapping clusters. Each cluster elects one node as the so-called clusterhead. These special nodes are responsible for the routing process. CBRP is implemented using ns2[9] as a simulation environment and its results are compared with the protocols AODV and DSR , the protocols which don't use clustering mechanism. Advantages and disadvantages of CBRP are highlighted . Some suggestions are also made to overcome the limitations when cluster based routing is used in MANETs.

Chapter 2

Background Study

2.1 Background

Computer networks are originally developed to operate by connecting computers together with wires and transmitting data over these wires. Network sizes and occurrences increased creating a requirement for inter network communication. This led to development of the internet and suite of protocols. The use of the internet and its applications became ubiquitous. A need for providing network access to entities while not physically attached to the wired network arose. To enable this wireless networking was developed, providing devices with methods to connect to a wired network using radio wave technologies through wireless access points.
Simultaneously telephone networks were going a similar transformation. Cellular network technologies[10] were developed to allow mobile phones to connect via base stations and communicate in a circuit switched environment. In general , mobile wireless networks can be classified into two types:

2.1.1 Infrastructured networks

Wireless mobile networks have traditionally been based on the cellular concept and relied on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the fixed network infrastructure(Figure 2.1). Typical examples of this kind of wireless networks are GSM[10], UMTS[11], WLL[12], WLAN[13] , etc.

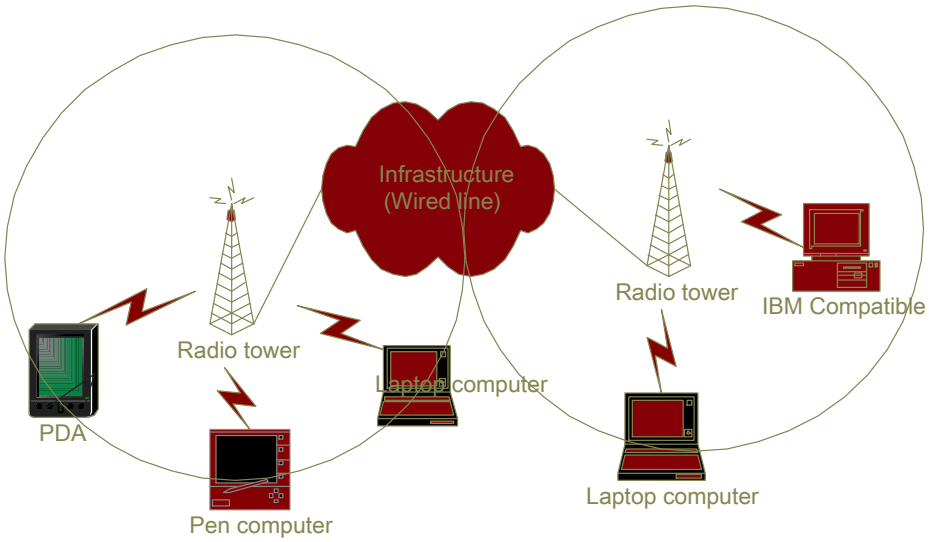


Figure 2.1: Infrastructured Network

2.1.2. Infrastructure less mobile network (Ad-hoc networks)

Wireless nodes can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure(Figure2.2) This is a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of a wireless connections on-the-fly.

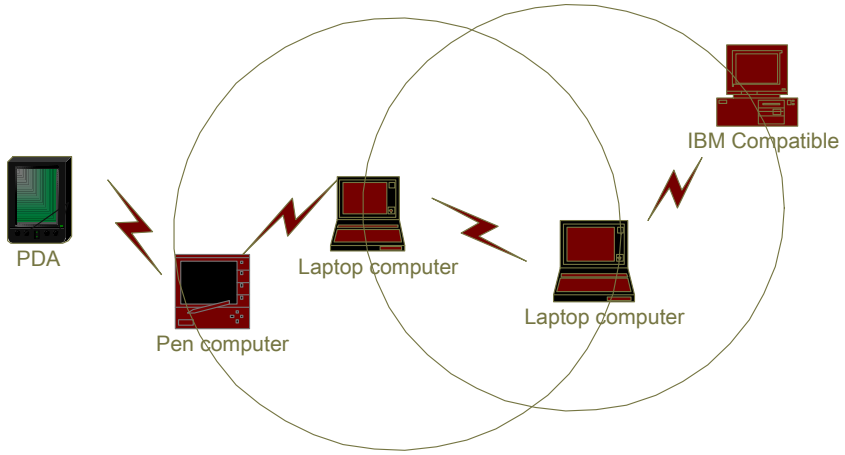


Figure 2.2 : Infrastructureless Network

2.2 Mobile Ad hoc networks

The area of mobile ad-hoc networking deals with devices equipped to perform wireless communication and networking, but without any existing infrastructure such as base stations or access points. Wireless devices form a network as they become aware of each others presence. They communicate directly with devices inside their radio range in a peer-to-peer nature. If they wish to communicate with a device outside their range, they can use an intermediate device or devices within their radio range to relay or forward communications to the device outside their range. An ad-hoc network is self-organising and adaptive. Networks are formed on-the-fly,devices can leave and join the network during its lifetime, devices can be mobile within the network, the network as a whole may be mobile and the network can be deformed on-the-fly. All this needs to be done without any system administration and without the requirement for any permanent devices within the network. Devices in mobile ad-hoc networks should be able to detect the presence of other devices and perform the necessary set-up to facilitate communications and the sharing of data and services.

2.2.1 MANET Features[14]

A MANET has the following features:

2.2.1 .1 Autonomous terminal.

In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

2.2.1.2 Distributed operation.

Since there is no background network for the central 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 relay as needed, to implement functions e.g. security and routing.

2.2.1.3 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 and applicability. 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

2.2.1.4 Dynamic network topology.

Since the nodes are mobile, the network topology may change rapidly and unpredictably 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 among themselves as they move about, forming their own network on the fly. 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).

2.2.1.5 Fluctuating link capacity.

The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.

2.2.1.6 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.

2.2.2 MANET Applications[14]

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with the increasing number of widespread applications. Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructured environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include:

2.2.2.1 Military battlefield

The modern digital battlefield demands robust and reliable communication in many forms.Most communication devices are installed in mobile vehicles ,tanks,trucks etc. Also soldieres could carry telecomm devices that could talk to a wireless base station or directly to other telecome devices if they are with in the radio range. However these forms of communication are considered to be primitive.At times when wirelses base station is destroyed by enemy, a soldier will be prohibited from communicating with other soldiers if the called party is not with in the radio range.This is the scenario where mobile ad hoc networks come into play. Adhoc networks are well known as

self organising networks since they are robust when nodes disappear due to destruction or mobility.Through multi-hop communication,soldiers can communicate to remote soldiers via data hoping and data forwarding from one radio device to another.

2.2.2.2Sensor Networks[15]

Another application of MANETs is sensor networks. This technology is a network composed of a very large number of small sensors. These can be used to detect any number of properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. Applications are the measurement of ground humidity for agriculture, forecast of earthquakes. The capabilities of each sensor are very limited, and each must rely on others in order to forward data to a central computer. Individual sensors are limited in their computing capability and are prone to failure and loss. Mobile ad-hoc sensor networks could be the key to future homeland security.

2.2.2.3 Automotive Applications

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 optimise traffic flow.

2.2.2.4 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 deployment of 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.

2.2.2.5 Personal Area Network

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, noticeable or transparently will be in close and dynamic interaction with devices in their surrounding.

2.2.3 Challenges Facing MANETs

The ad hoc networks has its own share of challenges which are listed below:

2.2.3.1 Spectrum allocation[16]

Issues such as interference, limited range, limited data throughput, device mobility and the sharing of the RF spectrum amongst devices all need addressing. Regulation Regarding the use of radio spectrum is currently under the control of FCC. Most experimental Ad hoc networks are based on the ISM band.To prevent interference Ad hoc networks must operate over some form of allowed or specified spectrum range.Most microwave ovens operate in 2.4 GHz band,which can therefore interfere with wireless LAN systems.

2.2.3.2 Energy efficiency

Energy efficiency is a concern. Most existing protocols don't consider power consumption as an issue since they assume the presence of static hosts and routes, which are powered by mains. However mobile devices today most ly operated by batteries .Battery technology is still lagging behind the microprocessor technology.The lifetime of an Li-on battery today is only 2-3 hours. Such a limitation in operating hours of a device employs a need for power conversion. In particular for

mobile ad hoc networks devices will have to perform the role of routers. Hence forwarding packets on the behalf of othetrs will consume power and this can be quite significant for nodes in mobile ad hoc networks.

2.2.3.3 Routing

Routing of data between devices outside their RF range. The routing protocols used on wired networks do not perform well on networks involving mobility and rapid membership changes. More effective routing protocols are required. In Ad Hoc networks, we need new routing protocols because of the following reasons:

- Nodes in Ad Hoc networks are mobile and topology of interconnections between them may be quite dynamic.
- Existing protocols exhibit least desirable behavior when presented with a highly dynamic interconnection topology.
- Existing routing protocols place too heavy a computational burden on each mobile computer in terms of the memory-size, processing power and power consumption.
- Existing routing protocols are not designed for dynamic and self-starting behavior as required by users wishing to utilize Ad-Hoc networks.
- Existing routing protocols like Distance Vector Protocol take a lot of time for convergence upon the failure of a link, which is very frequent in Ad Hoc networks.
- Existing routing protocols suffer from looping problems either short lived or long lived.
- Methods adopted to solve looping problems in traditional routing protocols may not be applicable to Ad Hoc networks.

2.2.3.4 Existing IP Usage

For a mobile host to be able to communicate as it moves from one location to other, one of the following of the two things have to be in place:

- Mobile Hosts must changes its IP address whenever it moves to new place
- Host specific routes must be propagated throughout Internet Routing fabric.

There are problems with either of these options. If a host has an open TCP[17] session with another host, that session will be terminated if the IP address changes. Also, if other hosts must be able to initiate communication with a mobile host, how can they do so if their IP address changes every time they move? How does the host obtain a new IP address as it joins a network?

What is also of concern and it not addressed in this IETF draft[14] or in any publications is the convergence of two separate auto configured ad-hoc networks, merging together to form one larger ad-hoc network. Depending on the amount of participating hosts in each network and given the size of the address space given to link local addressing in IPv4[18] (65,563 possible hosts), there is a possibility of hosts having duplicate addresses. The main issue with using TCP in MANETs comes from the assumption that a packet being dropped is an indication of congestion occurring, not an indication of a lossy link or a data transmission error. This is due to the observation that that packet error/ loss rates over the internet due to transmission errors are of the order of 1%. However, in a wireless network, the amount of transmission errors is of a much higher order. The factors affecting the percentage of transmission errors include interference from other radio signals, device mobility, the sharing of a wireless link with other devices. All these can affect the delivery of TCP segments to the receiver, the timely return of ACK packets from the receiver and give variations in the RTT compared to the estimated value. Any of these occurring will result in the sender assuming that congestion is occurring and will use TCP's mechanisms to drastically reduce its transmission rate.

MANETs also provide additional challenges to TCP operation. The mobility of hosts means that routes between hosts are open to change. When a route is broken due to host mobility, a route reconstruction procedure is invoked. This reconstruction results in a delay that the TCP sender is unaware of. Overall data throughput has had to suffer initially because of the route reconstruction delay, but TCP has now further drastically decreased the data throughput on false pretences.

2.2.3.5 Security and Privacy

Following are the security and privacy challenges in the area of ad hoc networks:

- Firstly, use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify

messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation.

- Secondly, nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted.
- Thirdly, an ad hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP, nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would not suffice. It is desirable for our security mechanisms to adapt on-the-fly to these changes.
- Finally, an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

2.3 Overview of Ad hoc routing protocols

Since the advent of DARPA[19] packet routing networks in the early 1970s,numerous protocols have been developed for ad hoc mobile networks ,which include high power consumption, low bandwidth and high error rates. An Ad hoc protocol is a convention or standard that controls how nodes come to agree which way route packets between computing devices in a mobile ad-hoc network .

Routing protocols in MANETs can be classified as :

- Proactive(Table driven)[20]
- Reactive (On demand)[20]
- Hybrid[20]

MANET is a dynamic network, which means node can change with time,new node can join the network and other nodes can leave the network. A MANETS is expected to be of large size than the radio range of wireless antenna ,because of this reason it could be necessary to route the traffic through a multihop.

2.3.1 Proactive protocols

These are called table driven protocols .In these protocols ,each node maintains routing information to every other node in the network.The routing information is usually kept in number of different routing tables .These tables are periodically updated if the network topology changes.The differnce between these protocols exists in the way the routing information is updated,detected and type of information kept at each routing. Some of these protocols are :

- Destination Sequenced Distance Vectored (DSDV)
- Distribtued Bellman- Ford (DBF)
- Wireless Routing Protocol (WRP)[21]
- Clusterhead Gateway Switch Routing (CGSR) [22]
- Source Tree Adaptive Routing (STAR) [23]
- Hazy Sighted Link State Routing ((HLSR)[24]
- Hierarchical Stare Routing (HSR)[25]
- Intrazone Routing Protocol (IZR)[26]

2.3.2Reactive Protocols

These are called on demand protocols. These are designed to reduce the overhead by maintaining the information for active routes only at the expense of delay due to route search. This means that routes are determined and maintained for nodes that require send data to particular destination. Route discovery occurs by flooding a route request through

the network .This scheme is significant for Ad hoc environment since the battery power is conserved both by not sending the advertisements and by not needing to receive them(A host could otherwise reduce its power consumption by putting itself into sleep or standby mode when they are not busy with other tasks.

Some of the protocols are:

- Associativity Based Routing[(ABR) [27]
- Dynamic Source Routing (DSR)
- Temporary Ordered Routing Algorithm. (TORA)
- Adhoc On Demand routing protocol (AODV)
- Cluster Based Routing Protocol (CBRP)
- Relative Distance Microdiscovery Adhoc Routing (RDMAR) [28]
- Signal Stability Routing (SSR)[29]
- Caching And Multiptath Routing (CHAMP)[30]
- Ant-based Routing Algorithm (ARA) [31]

2.3.3 Hybrid Protocols

This method combines the merits of proactive and reactive routing protocols with some additional features. The main idea of the hybrid routing protocols is the limiting the set of forwarding nodes and using the proactive routing algorithm for nearly placed nodes which usually forward data to far placed nodes. While route to nearly placed nodes is available immediately, there is no waste of bandwidth due to propagation of the local information to the far placed nodes. Also with the flexibility and correctness of the reactive routing, the overhead is greatly decreased caused by limitation of number of forwarding nodes. This is especially noticeably for high dense network. However hybrid routing algorithm does not concentrate on the route maintenance against mobility. Also imperfect balance between proactive and reactive routing causes decreasing of a data transmission performance, such as higher end to end delay, reduction of a packet delivery ratio. Protocol in this category is:

- Zone Resolution Protocol (ZRP)

Chapte
r 3

Review of State of Art

In this chapter we describe the structure and working of cluster based routing protocol (CBRP) , that is how the cluster formation and routing of packets takes place. We also give description of two other on demand routing protocols ad hoc on demand distance vector and dynamic source routing which don't clustering for routing of packets.

3.1 Cluster Based Routing Protocol (CBRP)

In recent years there have been some different approaches on cluster-based routing. The essential works that are taken into consideration here—apart from CBRP—are those of Krishna[32], Chiang [33] and Gerla and Tsai[34] . The cluster-based routing protocol (CBRP) was introduced by Jiang[8] in 1999. In CBRP the nodes of a wireless network are divided into several disjoint or overlapping clusters. Each cluster elects one node as the so-called clusterhead. These special nodes are responsible for the routing process. Neighbours of clusterheads cannot be clusterheads as well. But clusterheads are able to communicate with each other by using gateway nodes. A gateway is a node that has two or more clusterheads as its neighbours or— when the

clusters are disjoint—at least one clusterhead and another gateway node. The routing process itself is performed as source routing by flooding the network with a route request message. Due to the clustered structure there will be less traffic, because route requests will only be passed between clusterheads.

3.1.1 Cluster formation

There are two approaches of cluster formation one is identifier based clustering and other is connectivity based clustering. When using identifier-based clustering a node elects itself as the clusterhead if it has the lowest/highest ID in its neighbourhood, or a neighbour node if one has a lower ID. Connectivity-based clustering elects the node, which has the most neighbour nodes, as the clusterhead. So, whenever a clusterhead looses a neighbour node its connectivity decreases and it is most likely that another node has to be elected to act as clusterhead. While in the identifier-based approach, a new clusterhead has to be chosen only when nodes with lower/heigher ID appear. The CBRP uses a variation of the lowest-ID algorithm specified by Gerla and Tsai [34] which is an identifier-based algorithm. In order to support the cluster formation process each node uses a neighbour table, where it stores information about its neighbour nodes, such as their ID's, their role in the cluster (clusterhead or member node) and the status of the link to that node (uni-/bi-directional). The neighbour table is maintained by periodically broadcasting HELLO messages. A HELLO message contains information about one node's state, its neighbour table and its cluster adjacency table. The various states describe the clustering process depending on the current node state. These states are:-

- *Undecided*

  This means the node does not belong to any cluster: this usually occurs if a new node appears in the network. Thus, if it receives a HELLO message from a clusterhead and there is a bi-directional link between them it changes its state to be member of the cluster indicated by the clusterhead. Otherwise it looks up in its neighbour table if it has any bi-directional links. If so, it becomes itself the clusterhead of a new cluster, if not, it remains in the undecided state and tries again.

- *Clusterhead*

If a clusterhead detects that it has a bi-directional link to another clusterhead for a time period, it changes its state to member if the other clusterhead has a lower ID. Otherwise it stays the clusterhead and the other node has to change its state. This is a special case which may result in cluster re-organisation (Figure 3.1)

- *Member*

  If a member looses its clusterhead, it looks for bi-directional links to other nodes. If it detects any, it changes its state to clusterhead if it has the lowest ID, otherwise it switches to the undecided state. Each member node belongs at least to one cluster.

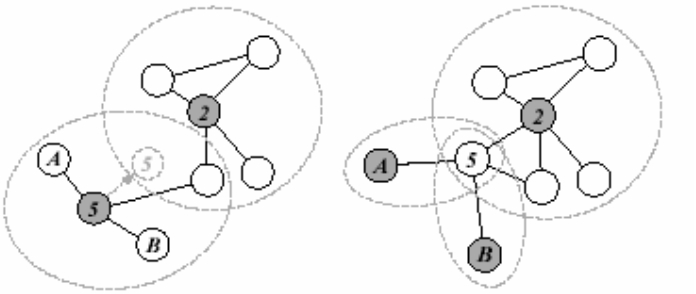


Figure 3.1[35] Clusterhead Movement : ***When clusterhead 5 moves into cluster 2 it gives up its role as clusterhead according to its higher ID. Nodes A and B which lost their clusterhead form new clusters.***

Striking for the goal to minimize cluster re-organisation, the structure of the clusters should change as seldom as possible. That means "a non-cluster head never challenges the status of an existing cluster head" , even if it has a lower ID.

3.1.2 Routing

CBRP uses two datastructures to support the routing process

1. the cluster adjacency table (CAT) and
2. the two-hop topology database.

The CAT stores information about neighbouring clusters. This is, whether they are bi-directonally or uni-directionally linked. That means, a cluster is called

- bi-directionally linked, if there is a bi-directional link between two nodes of the clusters, or if there are at least two opposite uni-directional links between two nodes (Figure 3.2)
- uni-directionally linked, if there is just one uni-directional link between them

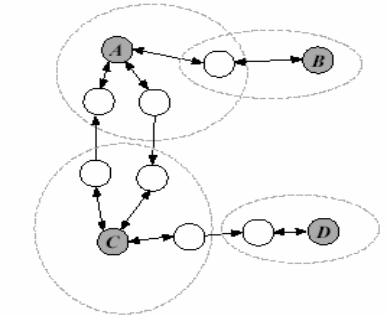


Figure3.2[35] Linking Between Clusters: Clusters A,B and A,C are bi-directionally linked, clusters C,D are unidirectionally linked

The two-hop topology database is build from the information received by HELLO messages. It contains all nodes that are at most two hops away. The routing process works in two steps. First, it discovers a route from a source node S to a destination node D, afterwards it routes the packets.

3.1.2.1 Route discovery[35]

Route discovery is done by using source routing. In the CBRP only clusterheads are flooded with route request package (RREQ). Gateway nodes receive the RREQs as well, but without broadcasting them. They forward them to the next clusterhead. This strategy reduces the network traffic.

Initially, node S broadcasts a RREQ with unique ID containing the destination's address, the neighbouring clusterhead(s)—including the gateway nodes to reach them—and the cluster address list which consists of the addresses of the clusterheads forming the route.

When a node N receives a RREQ it does the following:

```
IF N is member
     IF D is in the neighbour table
          send RREQ to D
     ELSE IF N is gateway to clusterhead C
          forward RREQ to C
     ELSE
          discard RREQ
     ENDIF
ELSE IF N is clusterhead
```

```
IF RREQ already seen
     discard RREQ
ELSE
     record ID in cluster address list of RREQ
     IF D is neighbour OR D is two hops away
          send RREQ to D
     ELSE
          FOR EACH neighbouring clusterhead C DO
               IF NOT C in address list of RREQ
                    record C in cluster address list
               of RREQ
               ENDIF
          ENDFOR
     ENDIF
     broadcast RREQ
ENDIF
ENDIF
```

If the RREQ reaches the destination node D it contains the loose source route [S,C1,C2, . . . ,Ck,D] (Figure 3.3). D sends a route reply message (RREP) back to S using the reversed loose source route [D,Ck, . . . ,C1, S]. Everytime a clusterhead receives this RREP it computes a strict source route, which then consists only of nodes that form the shortest path within each cluster.(Figure3.3)

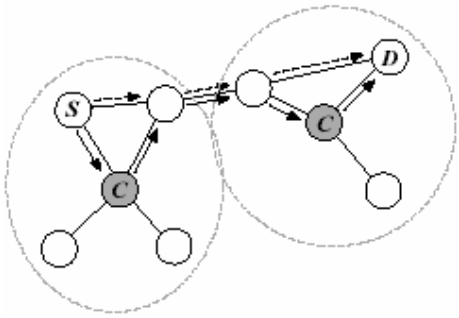


Figure 3.3[35] Source Routes: The loose source route (non-dashed arrows) and the strict source route (dashed arrows) from S to D.

3.1.2.2 Routing and route improvement

Due to node movement, (dis-)appearance of nodes or failures, the CBRP includes two mechanisms to improve a route: The first is Local Repair and the second is Route Shortening.

- *Local Repair*

If a connection between two node failes, the CBRP is able to repair the route.Therefore one of the following nodes of the route has to be in the two-hop topology database of the node, that discovered the broken link (Figure 3.4) . If the node is unable to repair the route, the route has to be recalculated.

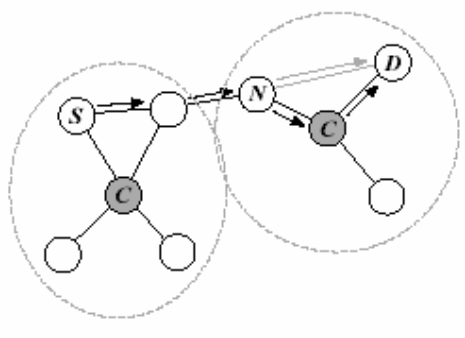


Figure 3.4 [35] Local Repair: The broken route between N and D (gray arrow) was repaired by using the clusterhead.

- *Route shortening*

Sometimes a node may discover a connection between itself and another succeeding node of the route, that is not its direct successor or a connection between two following nodes, respectively. This can be done by examening the information stored in the two-hop topology database. If so, it shortens the route by excluding the redundant node(s) from the route.

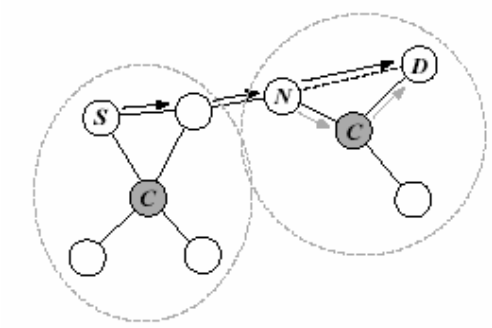


Figure 3.5 [35] Route Shortening: Node N discovered a new connection between itself and D (dashed line) and shortened the route.

In both cases, Local Repair and Route Shortening, the destination node is infomed about the changes by receiving a gratuitous route reply packet from the node, that performed the changes.

3.1.3 Problems and limitations

Like most of the other routing protocols, CBRP has some limitations and problems which are disadvantages compared to other protocols.

If a network and clusters become too big, the overhead per packet increases due to source routing. Every node of the route has to be stored in the routed packet. So the packet size raises proportional to the path length of the route. According to this, the transmission time increases as well. Also, if the cluster size grows the size of HELLO messages and stored data structures increases. According to this rise of overhead and the flat two level hierarchy the CBRP is scaleable to an extend.

Another problem of the CBRP is its support of uni-directional links. When using a network with 802.11 link layer technology these links cannot be supported, because the 802.11 protocol knows only bi-directional links. This could be solved by defining a new protocol that allows uni-directional links. From the view of the 802.11 protocol this would mean to permit that one node may forward Acknowledgement Packets. So a node would be able to send its acknowledgement back to the sender by using multiple hops.

Address resolving by using the Address Resolution Protocol (ARP)1 is also a problem. The ARP is a protocol to map netwotk IP addresses to Medium Access Control (MAC) addresses. To resolve such a mapping ARP request messages (who is IPD tell IPS) are broadcasted throughout the network. If the destination receives such a request, it replies with an ARP response message (IPD is MACD). If two nodes are uni-directionally linked one of them cannot resolve the other's MAC address by using the conventinal ARP. In this case a solution would be a modification of the protocol. So, if the uni-directional link is an intra-cluster linked, the clusterhead could inform the upstream node of the MAC address of the downstream node. In case of an inter-cluster link, the address could be resolved during the process of adjacent cluster discovery.(Figure 3.6)

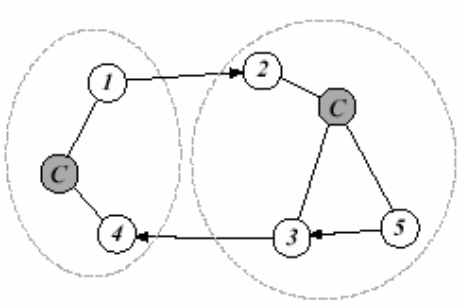


Figure3.6[35] Address Resolving: For node 3, the MAC address of 5 could be resolved by its clusterhead. For node 2, the address of 1 could be resolved during the discovery of adjacent clusters.

3.2Dynamic Source Routing(DSR)

3.2.1 Overview

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:

- *Route Discovery* is the mechanism by which a node **S** wishing to send a packet to a destination node **D** obtains a source route to **D**. Route Discovery is used only when **S** attempts to send a packet to **D** and does not already know a route to **D**.
- *Route Maintenance* is the mechanism by which node **S** is able to detect, while using a source route to **D**, if the network topology has changed such that it can no longer use its route to **D** because a link along the route no longer works. When Route Maintenance indicates a source route is broken, **S** can attempt to use any other route it happens to know to **D**, or can invoke Route Discovery again to find a new route. Route Maintenance is used only when **S** is actually sending packets to **D**.

Route Discovery and Route Maintenance each operate entirely on demand. In particular, unlike other protocols, DSR requires *no* periodic packets of any kind at any level within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and does not rely on these functions from any underlying protocols in the network. This entirely on-demand behavior and lack of periodic activity allows the number of overhead packets caused by DSR to scale all the way down to *zero*, when all nodes are approximately

stationary with respect to each other and all routes needed for current communication have already been discovered. As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use. In response to a single Route Discovery (as well as through routing information from other packets overheard), a node may learn and cache multiple routes to any destination. This allows the reaction to routing changes to be much more rapid, since a node with multiple routes to a destination can try another cached route if the one it has been using should fail. This caching of multiple routes also avoids the overhead of needing to perform a new Route Discovery each time a route in use breaks. The operation of Route Discovery and Route Maintenance in DSR are designed to allow unidirectional links and asymmetric routes to be easily supported. In wireless networks, it is possible that a link between two nodes may not work equally well in both directions, due to differing antenna or propagation patterns or sources of interference. DSR allows such unidirectional links to be used when necessary, improving overall performance and network connectivity in the system. DSR also supports internetworking between different types of wireless networks[36], allowing a source route to be composed of hops over a combination of any types of networks available For example, some nodes in the ad hoc network may have only short-range radios, while other nodes have both short-range and long-range radios; the combination of these nodes together can be considered by DSR as a single ad hoc network. In addition, the routing of DSR has been integrated into standard Internet routing, where a "gateway" node connected to the Internet also participates in the ad hoc network routing protocols; and has been integrated into Mobile IP routing, where such a gateway node also serves the role of a Mobile IP foreign agent[37]

3.2.2Basic DSR Route Discovery

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, we call **S** the initiator and **D** the target of the Route Discovery. For example, Figure 3.7 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 no de 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.

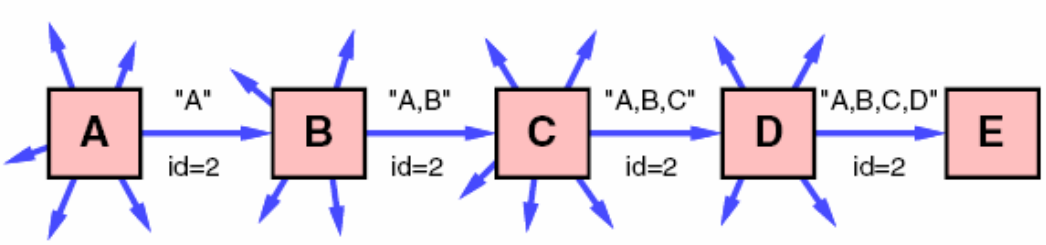


Figure 3.7 Route discovery example: Node A is initiator and node E is the target

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 3.7, 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 piggyback this ROUTE REPLY on its own ROUTE REQUEST message for **A**. It is also possible to piggyback other small data packets, such as a TCP SYN packet [38], on a ROUTE REQUEST using this same mechanism. Node **E** could also simply reverse the sequence of hops in the route record that it trying to send in the ROUTE REPLY, and use this as the source route on the packet carrying the ROUTE REPLY itself. For MAC protocols [39] such as IEEE 802.11 that require a bi-directional frame exchange as part of the MAC protocol , this route reversal is preferred as it avoids the overhead of a possible second Route Discovery, and it tests the discovered route to ensure it is bi-directional before the Route Discovery initiator begins using the route. However, this technique will prevent the discovery of routes using uni-directional links. In wireless environments where the use of uni-directional links is permitted, such routes may in some cases be more efficient than those with only bi-directional links, or they may be the only way to achieve connectivity to the target node.

When initiating a Route Discovery, the sending node saves a copy of the original packet in a local buffer called the Send Buffer. The Send Buffer contains a copy of each packet that cannot be transmitted by this node because it does not yet have a source route to the packet's destination. Each packet in the Send Buffer is stamped with the time that it was placed into the Buffer and is discarded after residing in the Send Buffer for some timeout period; if necessary for preventing the Send Buffer from overflowing, a FIFO or other replacement strategy can also be used to evict packets before they expire. While a packet remains in the Send Buffer, the node should occasionally initiate a new Route Discovery for the packet's destination address. However, the node must limit the rat e at which such new Route Discoveries for the same address are initiated, since it is possible that the destination node is not currently reachable. In

particular, due to the limited wireless transmission range and the movement of the nodes in the network, the network may at times become partitioned, meaning that there is currently no sequence of nodes through which a packet could be forwarded to reach the destination. Depending on the movement

pattern and the density of nodes in the network, such network partitions may be rare or may be common. If a new Route Discovery was initiated for each packet sent by a node in such a situation, a large number of unproductive ROUTE REQUEST packets would be propagated throughout the subset of the ad hoc network

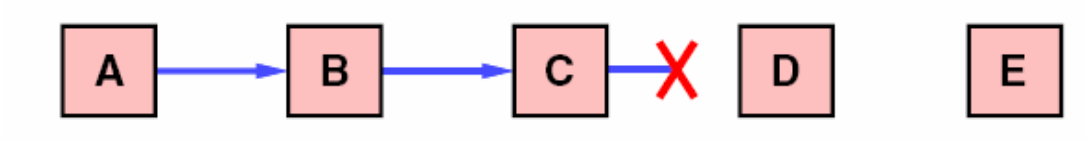


Figure 3.8 Route Maintenance example: Node **C** is unable to forward a packet from **A** to **E** over its link to next hop D

reachable from this node. In order to reduce the overhead from such Route Discoveries, we use exponential back-off to limit the rate at which new Route Discoveries may be initiated by any node for the same target. If the node attempts to send additional data packets to this same node more frequently than this limit, the subsequent packets should be buffered in the Send Buffer until a ROUTE REPLY is received, but the node must not initiate a new Route Discovery until the minimum allowable interval between new Route Discoveries for this target has been reached. This limitation on the maximum rate of Route Discoveries for the same target is similar to the mechanism required by Internet nodes to limit the rate at which ARP REQUESTs are sent for any single target IP address

3.2.3 Basic DSR Route Maintenance

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 3.8, 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**. This confirmation of receipt in many cases may be provided at no cost to DSR, either as an existing standard part of theMAC protocol in use (such as the link-level acknowledgement frame defined by IEEE 802.11 [39], or by a *passive acknowledgement* [40] (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 3.8, 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** (for example, from additional ROUTE REPLYs from its earlier Route Discovery, or from having overheard sufficient routing information from other packets), it can send the packet using the new route immediately. Otherwise, it may perform a new Route discovery for this target .

3.3 Adhoc On Demand Distance Vector Routing [41]

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes.

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. 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. A node receiving 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, nodes set up forward pointers to the destination. 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 hopcount, 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 destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

Multicast routes are set up in a similar manner. A node wishing to join a multicast group broadcasts a RREQ with the destination IP address set to that of the multicast group and with the 'J'(*join*) flag set to indicate that it would like to join the group. Any node receiving this RREQ that is a member of the multicast tree that has a fresh enough sequence number for the multicast group may send a RREP. As the RREPs propagate back to the source, the nodes forwarding the message set up pointers in their multicast route tables. As the source node receives the RREPs, it keeps track of the route with the freshest sequence number, and beyond that the smallest hop count to the next multicast group member. After the specified discovery period, the source node will unicast a Multicast Activation (MACT) message to its selected next hop. This message serves the purpose of activating the route. A node that does not receive this message that had set up a multicast route pointer will timeout and delete the pointer. If the node receiving the MACT was not already a part of the multicast tree, it will also have been keeping track of the best route from the RREPs it received. Hence it must also unicast a MACT to its next hop, and so on until a node that was previously a member of the multicast tree is reached.

AODV maintains routes for as long as the route is active. This includes maintaining a multicast tree for the life of the multicast group. Because the network nodes are mobile, it is likely that many link breakages along a route will occur during the lifetime of that route.

Chapter 4

Problem Statement

4.1 Problem motivation

Traditional routing protocols based on the *link-state* [42] or *distance-vector* [42] algorithms are aimed at finding optimal routes to every host in the network, and topological changes of the network can only be reflected through the propagation of periodic updates. These protocols are not suitable for ad hoc networks. Indeed, finding and maintaining routes to every host is too expensive and almost always not necessary as each host only communicates with a subset of the hosts in the network. Furthermore, the periodic updates cannot promptly reflect the frequent topological changes in ad hoc networks, which in turn will cause a lot of undelivered packets and undermine the quality of communication. As a consequence, a *mobile ad hoc networking* (MANET) working group has been formed within the Internet Engineering Task Force (IETF) to develop a routing framework for IP-based protocols in ad hoc networks. Today, a number of routing protocols have been proposed for ad hoc wireless networks , derived from *distance-vector* or *link-state* routing algorithms. Such protocols are classified as *proactive* or *reactive*, depending on whether they keep routes continuously updated or react on demand. While each protocol has its own advantages and disadvantages, none of them can be claimed as absolutely better than the others. Routing in wireless mobile ad-hoc networks should be time efficient and resource saving. One approach to reduce traffic during the routing process is, to divide the network into clusters.

4.2 Objectives and sub tasks.

The primary objective of this thesis is to

To analyze, implement and perform comparative analysis of cluster based routing protocol with the protocols that don't use clustering as a routing mechanism to demonstrate how the cluster based routing results in time efficient and resource saving routing as well as what are limitations of cluster based routing in mobile ad hoc networks and how these limitations can be overcome by suggesting some of the improvements in the existing protocol

Following tasks must be done to achieve primary objective.

- Get a general understanding of ad -hoc networks.
- Get a general understanding of simulation environment that could be used for analyzing ,evaluating and implementing ad hoc routing protocols
- Implement some of the routing protocols for wireless ad-hoc networks.
- Analyze the protocols theoretically and through simulation based on some parameters.
- Based on the above analysis suggest some improvements in protocols design to overcome some of the limitations in routing protocol.

Chapter 5

Analysis & Performance Evaluation

5.1 Simulation

Simulation can be defined as "Imitating or estimating how events might occur in a real situation." It can involve complex mathematical modeling, role playing without the aid of technology, or combinations. The value lies in the placing you under realistic conditions, that change as a result of behavior of others involved so you cannot anticipate the sequence of events or the final outcome.

5.1.1 Network Simulator[43]

NS is an event driven network simulator developed at University of California Berkeley that simulates variety of IP networks. It implements network protocols such as Transmission Control Protocol and Used Datagram Protocol , traffic source behavior such as File Transfer Protocol, Telne, Constant Bit Rate and Variable Bit Rate, router queue management mechanism such as DropTail, Random Early Discard. NS also implements multicasting and some of the MAC layer protocols for LAN simulations. The NS project is now a part of the VINT project[44] that develops tools for simulation results display, analysis and converters that convert network topologies generated by well-known generators to NS formats. Currently, NS (version 2) written in C++ and Otcl (Tcl script language with Object-oriented extensions) is available.

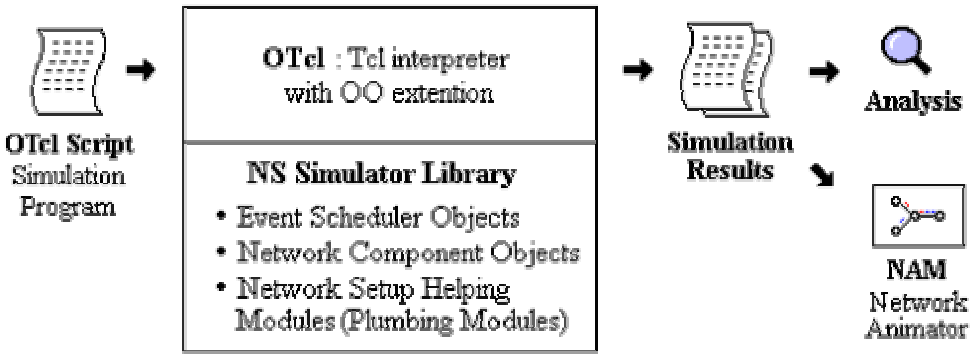


Figure 5.1 Simplified User's View of NS

As shown in Figure 5.1 , in a simplified user's view, NS is Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module libraries (actually, plumbing modules are implemented as member functions of the base simulator object). In other words, to use NS, you program in OTcl script language. To setup and run a simulation network, a user should write an OTcl script that initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler. The term "plumbing" is used for a network setup, because setting up a network is plumbing possible data paths among network objects by setting the "neighbor" pointer of an object to the address of an appropriate object. When a user wants to make a new network object, he or she can easily make an object either by writing a new object or by making a compound object from the object library, and plumb the data path through the object. This may sound like complicated job, but the plumbing OTcl modules actually make the job very easy. The power of NS comes from this plumbing.

Another major component of NS beside network objects is the event scheduler. An event in NS is a packet ID that is unique for a packet with scheduled time and the pointer to an object that handles the event. In NS, an event scheduler keeps track of simulation time and fires all the events in the event queue scheduled for the current time by invoking appropriate network components, which usually are the ones who issued the events, and let them do the appropriate action associated with packet pointed by the event. Network components communicate with one another passing packets, however this does not consume actual simulation time. All the network components that need to spend some simulation time handling a packet (i.e. need a delay) use the event scheduler by issuing an event for the packet and waiting for the event to be fired to itself before doing further action handling the packet. For example, a network switch component that simulates a switch with 20 microseconds of switching delay issues an event for a packet to be switched to the scheduler as an event 20 microsecond later. The scheduler after 20 microseconds dequeues the event and fires it to the switch component, which then passes the packet to an appropriate output link component. Another use of an event scheduler is timer. For example, TCP

needs a timer to keep track of a packet transmission time out for retransmission (transmission of a packet with the same TCP packet number but different NS packet ID). Timers use event schedulers in a similar manner that delay does. The only difference is that timer measures a time value associated with a packet and does an appropriate action related to that packet after a certain time goes by, and does not simulate a delay.

NS is written not only in OTcl but in C++ also. For efficiency reason, NS separates the data path implementation from control path implementations. In order to reduce packet and event processing time (not simulation time), the event scheduler and the basic network component objects in the data path are written and compiled using C++. These compiled objects are made available to the OTcl interpreter through an OTcl linkage that creates a matching OTcl object for each of the C++ objects and makes the control functions and the configurable variables specified by the C++ object act as member functions and member variables of the corresponding OTcl object. In this way, the controls of the C++ objects are given to OTcl. It is also possible to add member functions and variables to a C++ linked OTcl object. The objects in C++ that do not need to be controlled in a simulation or internally used by another object do not need to be linked to OTcl. Likewise, an object (not in the data path) can be entirely implemented in OTcl. Figure 5.2 shows an object hierarchy example in C++ and OTcl. One thing to note in the Figure is that for C++ objects that have an OTcl linkage forming a hierarchy, there is a matching OTcl object hierarchy very similar to that of C++.

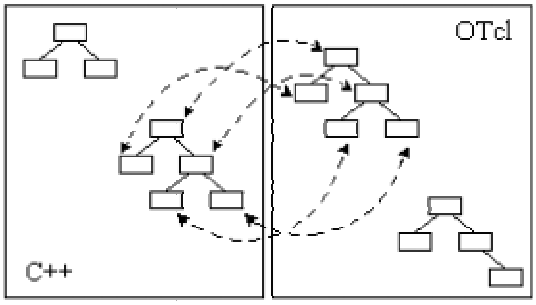


Figure 5.2 C++ and OTcl: The Duality

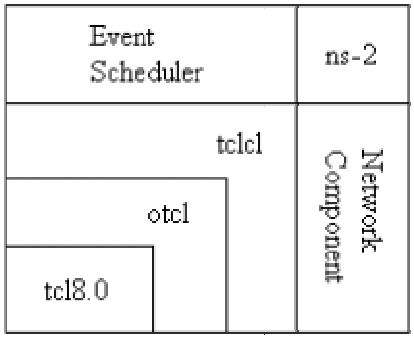


Figure 5.3 Architectural View of NS

Figure 5.3 shows the general architecture of NS. In this figure a general user (not an NS developer) can be thought of standing at the left bottom corner, designing and running simulations in Tcl using the simulator objects in the OTcl library. The event schedulers and most of the network components are implemented in C++ and available to OTcl through an OTcl linkage that is implemented using tclcl. The whole thing together makes NS, which is a OO extended Tcl interpreter with network simulator libraries. This section briefly examined the general structure and architecture of NS. At this point, one might be wondering about how to obtain NS simulation results. As shown in Figure 5.1, when a simulation is finished, NS produces one or more text-based output files that contain detailed simulation data, if specified to do so in the input Tcl (or more specifically, OTcl) script. The data can be used for simulation analysis or as an input to a graphical simulation display tool called Network Animator (NAM) that is developed as a part of VINT project. NAM has a nice graphical user interface similar to that of a CD player (play, fast forward, rewind, pause and so on), and also has a display speed controller. Furthermore, it can graphically present information such as throughput and number of packet drops at

each link, although the graphical information cannot be used for accurate simulation analysis

5.1.2 GloMoSim[45]

GloMoSim is a scalable simulation environment for wired and wireless network systems.

Currently it only supports protocols for a purely wireless network . It is also built in a layered approach such as OSI seven layer network architecture. GloMoSim is designed as a set of library modules, each of which simulates a specific wireless communication protocol in the protocol statck. The library has been developed using PARSEC, a C-based parallel simulation language. New protocols and modules can be programmed and added to the library using this language. The latest version of GloMoSim has implemented DSR. GloMoSim's source and binary code can be downloaded only by academic institutions for research purposes. Commercial users must use QualNet, the commercial version of GloMoSim

5.1.3 OPNET Modeler[46]

OPNET Modeler is commercial network simulation environment for network modeling and simulation. It allows the users to design and study communication networks, devices, protocols, and applications with flexibility and scalability. It simulates the network graphically and its graphical editors mirror the structure of actual networks and network components. The users can design the network model visually. The modeler uses object- oriented modeling approach. The nodes and protocols are modeled as classes with inheritance and specialization. The development language is C.

5.2 Simulation Model

There are different mobility models which are used for simulating the ad hoc networks in different environments . The most commonly used are

- Random waypoint mobility model[47-48]

- Reference point group mobility model[47-48]
- Freeway[49]
- MANHATTEN mobility model[49]

In this work , random waypoint mobility is considered . In random waypoint mobility model a mobile node begins the simulation by waiting a specified pause time. After this time it selects a random destination in the area and a random speed distributed uniformly between some range. After reaching its destination point, the mobile node waits again pause time seconds before choosing a new way point and speed. Traffic sources are CBR (continuous bit rate). The source destination pairs are spread randomly over the network. By changing the total number of traffic sources, we get scenarios with different traffic loads. For small traffic loads (10, 20, 30 sources), the packet rate at the source node is 4 packets/sec. For 40 sources, a smaller rate of 3 packets/sec for 50 nodes. Only 512-byte data packets are used.. Field configurations is used as 1500 m $\times$ 300 m with 50 nodes . Each node starts its journey from a random location to a random destination, with a randomly chosen speed uniformly distributed between 0 and 20 m/sec. Once the destination is reached, another random destination is targeted after a pause. Varying the pause time changes the frequency of node movement. For the set of tests with 50 nodes, the total simulation time is 900 seconds, and each data point in the following figures is the average of five runs with the same scenario configuration but different random seeds.

5.2.1 Performance Metrics

Three key performance metrics are evaluated in our experiments:

- *Throughput*—This is the ratio of the data packets delivered to the destination to those generated by the CBR sources.
- *Average end-to-end delay* of data packets—This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer time.
- *Normalized routing overhead*—This metric has two variants: *packet overhead* is the number of routing packets "transmitted" per data packet "delivered" at the destination, and *byte overhead* is the number of bytes of routing packets

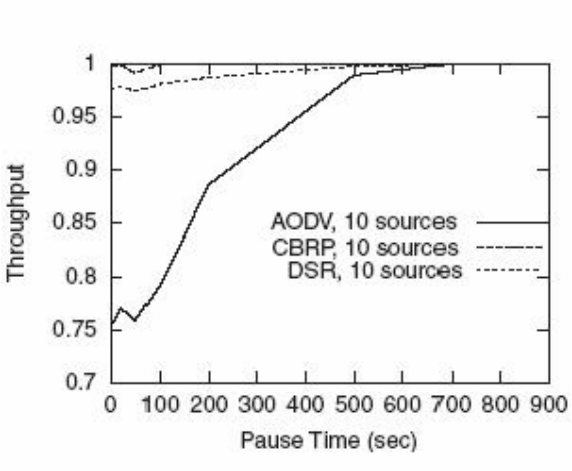
"transmitted" per data byte "delivered" at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

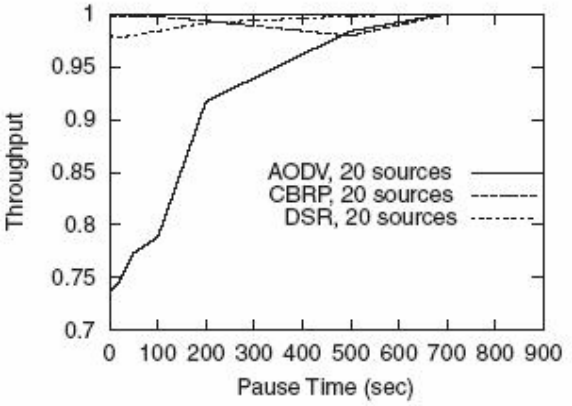
The first two metrics are the most important metrics for best-effort traffic. The routing load metric evaluates the efficiency of the routing protocol. Note that these metrics are not completely independent. For example, a larger overhead may cause lower throughput and longer delay. On the other hand, a shorter delay may not necessarily imply a higher throughput since delay is only measured on those successfully delivered packets. Also notice the scenario tested here is simply a random situation. Real-world ad hoc networks usually have special traffic and mobility models. The difficulty here is that different applications have different scenarios, and it is not very clear what the typical scenario of a specific application is.

5.3 Simulation Results:

5.3.1 Throughput

The two source routing protocols demonstrate high quality in delivering packets—more than 95% in the case of 50 nodes. AODV has difficulty when the nodes are moving fast (corresponding to smaller pause time), with a throughput less than 80%. Source routing reveals more information in one route discovery than AODV. Therefore, within the same time, more routes are discovered and so more packets can be delivered. AODV catches up when the mobility of the nodes gets lower. This is because routes become more stable, and so eventually everybody can find all the routes it ever needs. Between DSR and CBRP, CBRP has a better throughput for a larger network size. This better scalability comes from its largely reduced flooding for route discovery.


Throughput
1
0.95
0.9
0.85
0.8
0.75
0.7
0
100
200
300
400
500
600
700
800
900
Pause Time (sec)
AODV, 10 sources
CBRP, 10 sources
DSR, 10 sources


Throughput
1
0.95
0.9
0.85
0.8
0.75
0.7
0
100
200
300
400
500
600
700
800
900
Pause Time (sec)
AODV, 20 sources
CBRP, 20 sources
DSR, 20 sources

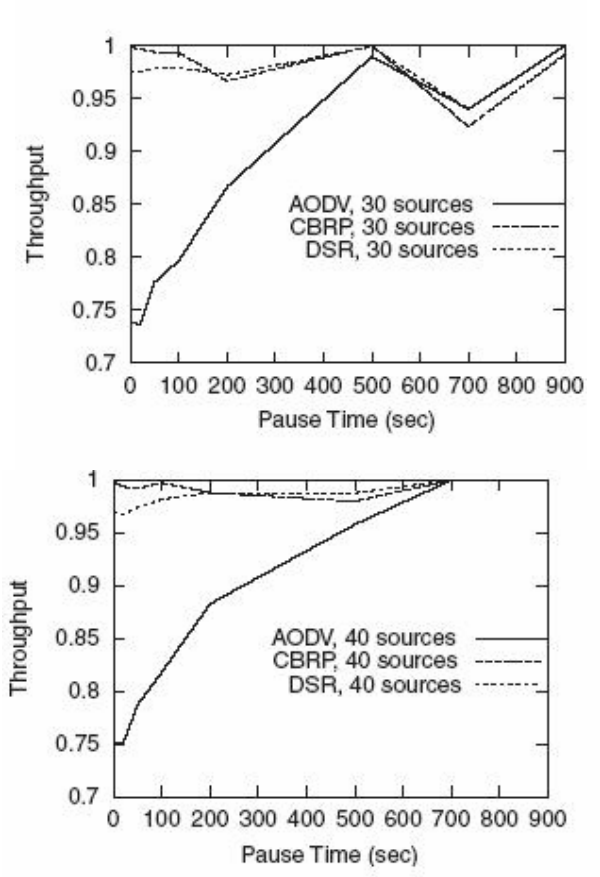
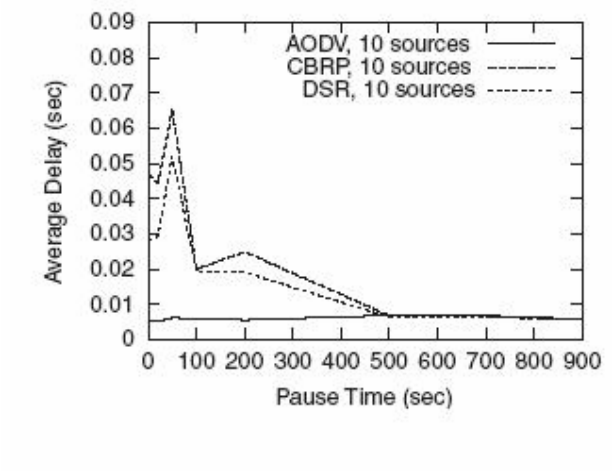


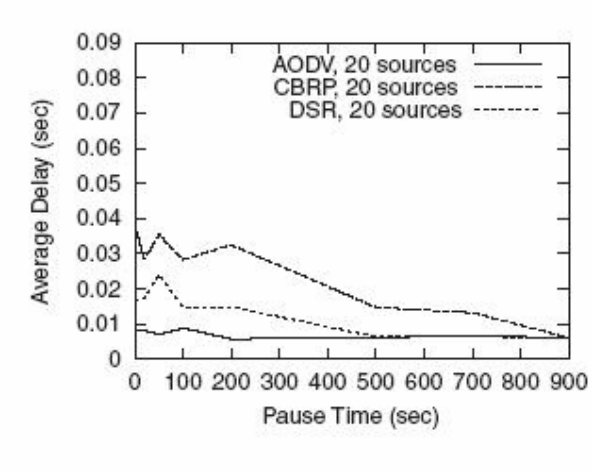
Figure 5.4 Data packet throughput: 50 node model with various no of traffic sources.

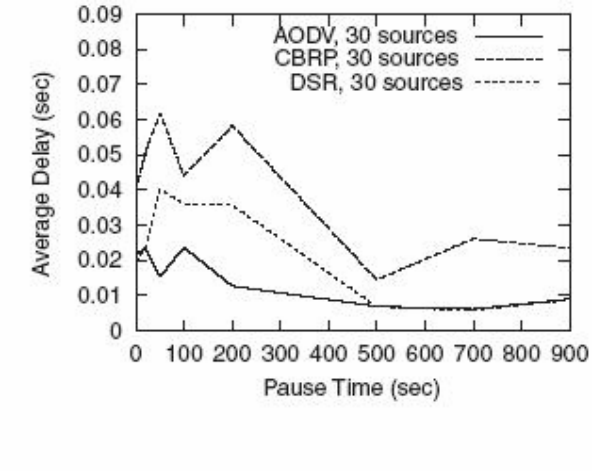
5.3.2 Delay

Among the three protocols, AODV has the shortest end-to-end delay of no more than 0.05 seconds. Besides the actual delivery of data packets, the delay time is also affected by route discovery, which is the first step to begin a communication session. The source routing protocols have a longer delay because their route discovery takes more time as every intermediate node tries to extract information before forwarding the reply. The same thing happens when a data packet is forwarded hop by hop. Hence, while source routing makes route discovery more profitable, it slows down the transmission of packets. CBRP is even more time-consuming because of its two-phase

route discovery. The task of maintaining cluster structure also takes a piece of each host's CPU time.







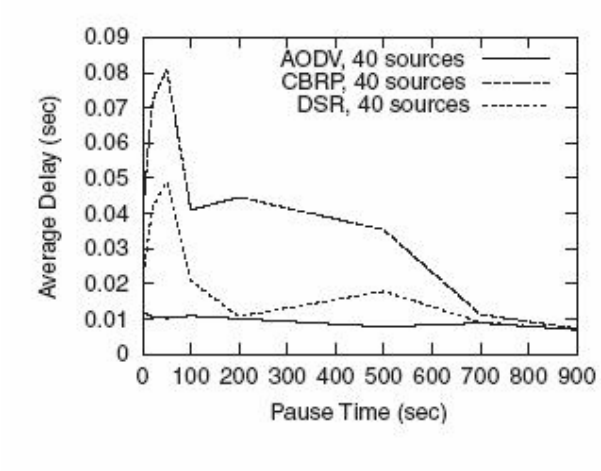
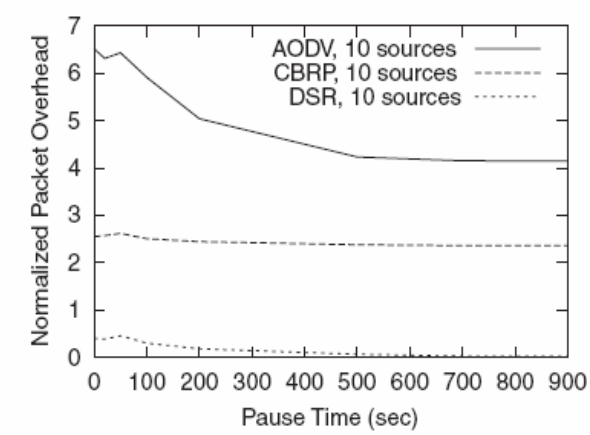
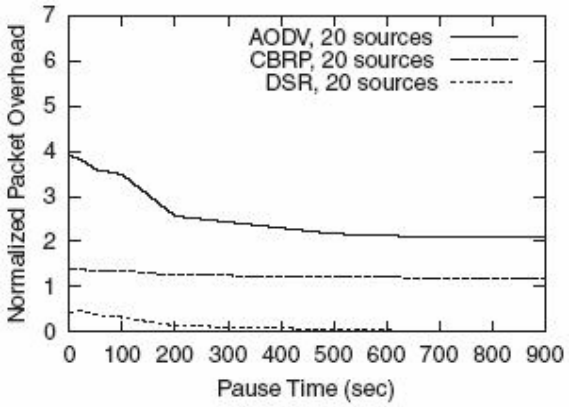


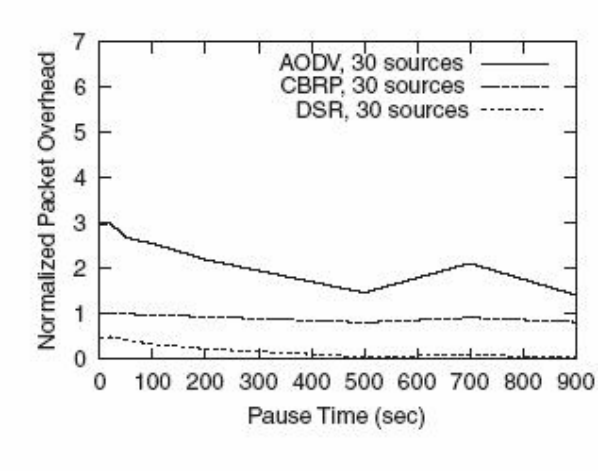
Figure 5.4 Average data packet delay : 50 node model with various no of traffic sources.

5.3.3 Overhead

Without any periodic hello messages, DSR outperforms the other two protocols in terms of overhead. In most cases, both the packet overhead and the byte overhead of DSR are less than half of the overhead of CBRP and less than a quarter of AODV's overhead. AODV has the largest routing load (in the 50-node cases, as many as 6.5 routing packets per data packet and 2 routing bytes per data byte) because the number of its route discoveries is the most, and the discovery is network-wide flooding. CBRP has a much smaller flooding range; the number of its route requests and replies is constantly half that of DSR. But its hello messages outweigh this gain. And since the size of CBRP hello messages can be large, its byte overhead is still more than DSR's (in the 50-node cases, more than twice as much as DSR's). When there are more connections, more routing is needed, and so the proportion of hello messages in the total overhead becomes smaller. As the result, CBRP and AODV get closer to DSR.


Normalized Packet Overhead
Pause Time (sec)
AODV, 10 sources
CBRP, 10 sources
DSR, 10 sources
0
1
2
3
4
5
6
7
0
100
200
300
400
500
600
700
800
900


Normalized Packet Overhead
Pause Time (sec)
AODV, 20 sources
CBRP, 20 sources
DSR, 20 sources
0
1
2
3
4
5
6
7
0
100
200
300
400
500
600
700
800
900



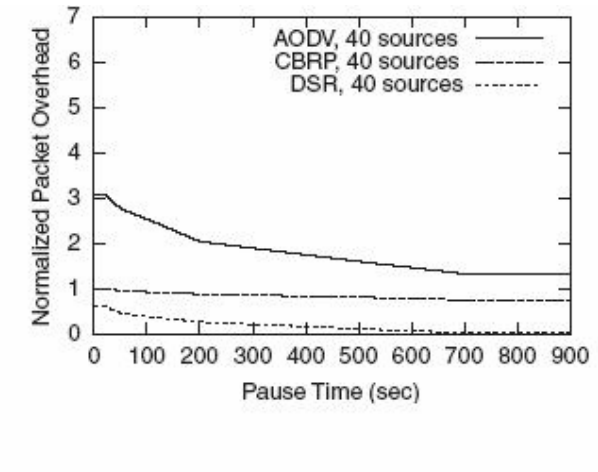


Figure 5.5 Normalized byte overhead : 50 node model with various no of traffic sources

Chapter 6

6.1 Conclusion

Ad hoc wireless networks are composed of mobile stations communicating solely through wireless channels. Such networks are expected to play an increasingly important role in future civilian and military settings, being useful for providing communication support where no fixed infrastructure exists or the deployment of a fixed infrastructure is not economically profitable and movement of communicating parties is possible. However, this creates a new set of issues and trade-offs.

In this work, we focused on the routing problem in ad hoc networks. Routing in wireless mobile ad-hoc networks should be time efficient and resource saving. One approach to reduce traffic during the routing process is, to divide the network into clusters. We have seen the structure and the working of the cluster-based routing protocol. We also described the working of two other routing protocols ad hoc on demand distance vector and dynamic source routing. We have presented an extensive simulation study to compare three on-demand ad hoc routing protocols (DSR, AODV, and CBRP), using a variety of workloads such as mobility, load, and size of the ad hoc networks. Our results indicate that the two source routing–based protocols, DSR and CBRP, have very high throughputs while the distance-vector-based protocol, AODV, exhibits a very short end-to-end delay of data packets. Furthermore, despite its improvement in reducing route request packets, CBRP has a higher routing overhead than DSR because of its periodic hello messages. DSR has much smaller routing overhead than AODV and CBRP, and AODV has the largest overhead among the three protocols.

6.2 Future Scope

- Currently the proposed work studies only one routing protocol based on clustering that is CBRP , there are other protocols which use cluster based routing such as CGSR can also be studied.
- In our simulation study only one propagation model(random way point) is used, other propagation models can also be used.
- The CBRP is a scaleable protocol and can be studied by increasing the no of nodes and results can be analyzed accordingly. Further study on superclustering can be done because currently CBRP is scaleable to only two levels of hierarchy.
- There can be some stability provided in CBRP when there is often change in clusterhead due to high mobility in the network , we can use the secondary clusterhead for the back up that is whenever primary clusterhead moves out of the network ,secondary clusterhead takes over it and no election process takes place again.
- The fact that cluster mobility is less than node mobility can be utilized to provide route maintenance against mobility by labeling each cluster to have routes which will be independent of ids of the nodes.

References

ANNEX I

- C. E. Perkins, E. M. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) Routing," RFC 3561, July 2003, work in progress *http://www.ietf.org/rfc/rfc3561.txt*
- David Johnson, David Maltz and Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," Internet Draft, draft-ietf-manet-dsr-10.txt, work in progress, July 2004
- V. Park and S.Corson "Temporally-Ordered Routing Algorithm," Internet Draft, draft-ietf-manet-tora-spec- 03.txt, work in progress, June 2001.
- Y.-B. Ko and V. N. H., "Location-Aided Routing in mobile Ad hoc networks," ACM/IEEE Mobicom, pages 66-75, October 1998.
- C. E. Perkins and P. Bhagwat , "Highly Dynamic Destination-Sequenced Distance Vector (DTDV) for Mobile Computers," Proc. of the SIGCOMM 1994 Conference on Communications Architectures, Protocols and Applications, Aug 1994, pp 234-244.
- Dimitri P. Bertsekas and Robert G. Gallager , "Distributed Asynchronous Bellman-Ford Algorithm," Data Networks, pp. 325-333, Prentice Hall, Enlgewood Cliffs, 1987, *ISBN 0-13-196825-4*
- Zygmunt J. Haas , Marc R. Pearlman and Prince Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," Internet Draft, *http://www.ietf.org/proceedings/02nov/I-D/draft-ietf-manet-zone-zrp-04.txt*, work in progress, July 2002.
- M. Jiang , J. Li and Y. C. Tay, "Cluster Based Routing Protocol (CBRP)," Functional Specification Internet Draft, draft-ietf-manet-cbrp.txt, work in progress, June 1999.
- *http://www.isi.edu/nsnam/ns*
- Jan A. Audestad. Network aspects of the GSM system. In *EUROCON 88*, June 1988.
- *http://www.iec.org/online/tutorials/umts/*
- *http://www.cdg.org/technology/cdma_technology/wll.asp*
- http://en.wikipedia.org/wiki/wlan
- IETF MANET Working Group. Mobile Ad Hoc Networks(MANET). Working Group charter, available at *http://www.ietf.org/html.charters/manet-charter.html*.
- C. Shen, C. Srisathapornphat and C. Jaikaeo, "Sensor Information Networking Architecture and Applications," IEEE Pers. Commun., pp. 52-59, Aug. 2001.
- RL Pickholtz, LB Milstein and DL Schilling, "Spread spectrum for mobile communications, " IEEE Transactions , 1991
- TCP/IP Illustrated, Volume 1: The Protocols W. Richard Stevens © 1994 / 0-201-63346-9 / Addison Wesley Professional

- P Calhoun and C Perkins, "Mobile IP Network Access Identifier Extension for IPv4**,"** RFC 2794, March 2000
- *http://www.darpa.mil*
- Royer, E.M. and Chai-Keong Toh, "A review of current routing protocols for ad hoc mobile wirelessnetworksPersonal Communications," IEEE, Apr 1999
- Shree Murthy and J.J. Garcia-Luna-Aveces , "A Routing Protocol for Packet Radio Networks," Proc. ACM International Conference on Mobile Computing and Networking, pp. 86-95, November, 1995
- Ching -Chuan Chiang, Hsiao-Kunag Wu, Winston Liu and Mario Gerla, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," IEEE Singapore International Conference on Networks, SICON'97, pp. 197-211, Singapore, 16.-17. April 1997, IEEE
- J.J. Garcia-Luna and M. Spohn, "Source Tree Adaptive Routing Internet Draft," draft-ietf-manet-star-00.txt, work in progress, October 1999. / J.J. Garcia-Luna. M Spohn, "Source-Tree Routing in Wireless Networks," Proceedings of the 7th International Conference on Network Protocols, IEEE ICNP 99, Toronto, Candada, pp. 273-282, IEEE, October 1999 *http://citeseer.ist.psu.edu/garcia-luna-aceves99sourcetree.html*
- Cesar Santivanez And Ram Ramanathan , "Hazy Sighted Link State routing protocol (HSLS)," BBN Technical Memorandum No. 1301, 31 August 2001 , *http://www.cuwireless.net/OSI/progress_report.html*
- Alan O'neill Hongyi Li , "Hierachiacal State Routing Protocol," Internet Draft, draft-oneill-li-hsr-00.txt *http://alternic.net/drafts/drafts-o-p/draft-oneill-li-hsr-00.txt*
- Zygmunt J. Hass , Marc R. Pearlman and Prince Samar , " The Intrazone Routing Protocol (IARP) for Ad Hoc Networks," Internet Draft, *http://www.ietf.org/proceedings/02nov/I-D/draft-ietf-manet-zone-iarp-02.txt*, work in progress, July 2002.
- Chai-Keong Toh , "A Novel Distributed Routing Protocol To Support Ad hoc Mobile Computing, " Proc. IEEE 15th Annual International Phoenix Conference on Computers and Communications, IEEE IPCCC 1996, 27 March-29, Phoenix, AZ, USA, pp. 480-486 / CHAI-KEONG TOH, "Long-lived Ad Hoc Routing based on the Concept of Associativity," Internet Draft, March 1999, Expired, *http://www.ietf.org/proceedings/99nov/I-D/draft-ietf-manet-longlived-adhoc-routing-00.txt*
- G. Aggelou and R. Tafazolli, " Relative Distance Micro-discovery Ad Hoc Routing (RDMAR) protocol," Internet Draft, draft-ietf-manet- rdmar-00.txt, work in progress, September 1999.
- R. dube , C. D. Rais, K. Wang and S. K. Tripathi , " Signal Stability based adaptive routing (SSR alt SSA) for ad hoc mobile networks," IEEE Personal Communication, Feb. 1997.
- Alvin C. Valera , Winston K.G. Seah and S.V. Rao "CHAMP:A Highly-Resilient and Energy-Efficient Routing Protocol for Mobile Ad hoc Networks," In Proceedings of the 5th IEEE Conference on Mobile and Wireless Communications Networks (MWCN 2002), Stockholm, Sept 9 - 11, 2002

- Mesut Günes , “the ant-colony based routing algorithm for manets,” Proceedings of the 2002 ICPP Workshop on Ad Hoc Networks (IWAHN 2002), pages 79-85, IEEE Computer Society Press, August 2002.
- P. Krishna, N. H. Vaidya, M. Chatterjee, and D. K. Pradhan, “ A cluster-based approach for routing in dynamic networks.” ACM SIGCOMM Computer Communication Review, 27:49–65, 1997.
- Ching-Chuan Chiang, Hsiao-Kuang Wu, Winston Liu, and Mario Gerla, “ Routing in clustered multihop, mobile wireless networks with fading channel,.” Proceedings of IEEE Singapore International Conference on Networks (SICON ’97), pages 197–211, April 1997
- Mario Gerla and Jack Tzu-Chieh Tsai , “Multicluster, mobile, multimedia radio network,” ACM-Baltzer Journal of Wireless Networks, 1(3):255–265,1995.
- Tim Daniel Hollerung, “The Cluster-Based Routing Protocol,” project group ‘Mobile Ad-Hoc Networks Based on Wireless LAN’ winter semester 2003/2004
- Josh Broch, David A. Maltz, and David B. Johnson.,“ Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks,” In Proceedings of The International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN’99), Workshop on Mobile Computing, Perth, Western Australia, June 1999.
- David B. Johnson. ,“Scalable Support for Transparent Mobile Host Internetworking.” Wireless Networks, 1(3):311–321, October 1995.
- J. B. Postel, “ Transmission Control Protocol,”. RFC 793, September 1981.
- IEEE Computer Society LAN MAN Standards Committee.,”Wireless LAN MediumAccess Control (MAC) and Physical Layer (PHY) Specifications,” IEEE Std 802.11-1997. The Institute of Electrical and Electronics Engineers, New York, New York, 1997.
- John Jubin and Janet D. Tornow.,” The DARPA Packet Radio Network Protocols.” *Proceedings of the IEEE*, 75(1):21–32, January 1987.
- *http://moment.cs.ucsb.edu/AODV/aodv.html*
- *http://www.cisco.com/univercd/cc/ td/doc/cisintwk/ito_doc/routing.htm*
- Ns-2 by example *http://nile.wpi.edu/NS/*
- *http://www.isi.edu/nsnam/vint/*
- R.A. Meyer. PARSEC User Manual. UCLA Parralel Computing Laboratory, *http://pcl.cs.ucla.edu*
- OPNET Users' Manual, OPNET Architecture, OV.415.*http://forums.opnet.com./*
- Broch, J., D. A. Maltz, D. B. Johnson, Y-C. Hu and J. Jetcheva. 1998, ”A performance comparison of multi-hop wireless ad hoc network routing protocols,”. Paper presented at Mobicom’98, October, Dallas, TX.
- Das, S. R., C. E. Perkins, and E. M. Royer., “Performance comparison of two on-demand routing protocols for ad hoc networks.,” Paper presented at Infocom 2000, March, Tel-Aviv, Israel.
- Bai, F. Narayanan Sadagopan and Helmy, “A framework to systematically analyze the Impact of Mobility on Performance of Routing Protocols for Adhoc Networks,” INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEEApril 2003.

List of Publications ANNEX – II

ACCEPTED

1. Ghansham Sangar, Ravi Kumar Bansal, Ripan Kumar and A.K. Verma, "A Novel Technique for Securing Bluetooth Communication", 4th International Conference on Computer Science and its Applications (ICCSA-2006), San Diego, California, June 27-29, 2006.
2. Ravi Kumar Bansal and A.K. Verma, " Review of A Stable Infrastructure Creation Protocol in MANETs", in Proceedings of National Conference on Recent Trends In Engineering And Computational Techniques (REACT-2006), BGIET Sangrur , 5-6 April,2006.