CHAPTER 2
LITERATURE SURVEY

2.1 INTRODUCTION

Various multicast protocols in MANETs along with the challenges and issues existing in the MANETs are discussed. The advancements in computing [30] and the use of mobile devices in computing made mobile and wireless networking important. The main confront lies in applying multicast communication to the scenario in which mobility is unlimited and also where frequently failures occur.

2.2 PUBLISH–SUBSCRIBE MECHANISM

It is a messaging pattern where senders of messages, called publishers, do not program the messages to be sent directly to specific receivers, called subscribers. Published messages are characterized into classes, without knowledge of what, if any, subscribers there may be. A subscriber expresses interest in one or more classes, and only receives messages that are of interest, without knowledge of what, if any, publishers there are. Pub/sub is a sibling of the message queue paradigm, and is typically one part of a larger message oriented middleware system. Most messaging systems support both the pub/sub and message queue models in their API, e.g. Java Message Service (JMS). This pattern provides greater network scalability and a more dynamic network topology.

2.3 TOPOLOGIES

In many pub/sub systems, publishers post messages to an intermediary message broker and subscribers register subscriptions with that broker, letting the broker perform the filtering. The broker normally performs a store and forward function to route messages from publishers to subscribers.
2.4 DESCRIPTION OF WORKING GROUP

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing applications within the static and dynamic topologies with increased dynamics due to node motion or other factors. The working group will develop two Standards track routing protocol specifications:

- Reactive MANET Protocol (RMP)
- Proactive MANET Protocol (PMP)

The multicast service is critical in applications characterized by the close collaboration of teams (e.g. rescue patrol, battalion, scientists, etc) with requirements for audio and video conferencing and sharing of text and images. In the Internet (IPv4), multicasting facilities were introduced via the Multicast Backbone (MBone), a virtual overlay network on top of the Internet. This overlay network consists of multicast-capable islands connected by tunnels. These routers manage group membership and cooperate to route data to all hosts wishing to participate in a multicast group. IP multicast groups are identified by special IP addresses. Support for multicasting is an integral component of IPv6, so it can be assumed that multicasting applications will become even more popular with the increased popularity and acceptance of IPv6. Hosts may join and leave groups any time. A permanent group has a well known, administratively assigned address.

There is no assumption of an underlying fixed infrastructure. To provide communication through the whole network, a source-to-destination path could pass through several intermediate neighbor nodes. The majority of nodes will rely on batteries, thus routing protocols must limit the amount of control information that is passed between nodes. The main use of the MANET is necessary where the wire line network is not available.
2.5 MOBILE AD HOC NETWORKS (MANETS)

A wireless network is that which transmits data in packets from computer to computer. Instead of using a central base station (access point) to which all computers must communicate, this peer-to-peer mode of operation can greatly extend the distance of the wireless network. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. MANET is a particular type of Wireless Mesh Network (WMN). A MANET is a collection of mobile users that communicate using wireless links. In MANET, nodes are mobile and energy constrained. Issues in Ad Hoc Networks

- Bandwidth Constraints
- Frequent Topology changes
- Limited Battery power

Fig. 2.1: Working of a general Ad Hoc Network
2.6 MULTICASTING IN AD HOC NETWORKS

Many of these potential applications of MANETs involve point-to-multipoint communication, and thus would benefit from multicasting [16] support in the network layer.

In the case of IP [29] Multicasting, for example, the packet is not definite to arrive to all nodes of the destination group or in the same order relative to other packets. Multicasting is intended for group-oriented computing and its use within a network has many benefits. Most of the applications require one-to-many or many-to-many dissemination which is an essential task.

While many applications, such as audio/video distribution, can tolerate loss of data content, many other applications cannot. In addition, even loss-tolerant applications will suffer a performance penalty: an audio stream may experience a short gap or lower fidelity in the presence of loss. The original goal of this work is to design an efficient protocol that delivers packets from one or multiple senders to many receptions with high probability.

We started this effort by exploring the performance of a number of best effort protocols: two unicast protocols, three multicast protocols, and two broadcast protocols. The extensive simulation results show that broadcast protocols perform surprisingly well. So we decided to use the more efficient broadcast protocol, BCAST, as starting point for the next step. After exploring a number of design alternatives, the simulation results reported demonstrates that this mechanism indeed increases the packet delivery ratio. The experiments also show that a high degree of mobility is actually advantageous: as network partitions are potentially short lived, our retransmission scheme is more likely to successfully recover from packet losses during such partitions. In contrast, in networks with longer lived partitions, the amount of
packets buffered at nodes needs to be increased substantially to recover in these cases. Finally, the results show that implementing any reliability mechanism has to be done with care. As the network capacity is limited, flooding the network with NACKs and the ensuing packet retransmission attempts will have a detrimental impact on the protocol performance when the network is experiencing congestion.

In the reliable BCAST protocol, each node monitors the local network traffic and suppresses NACKs when it observed too much traffic in the recent past. In a last step, we explored the impact of the MAC layer on the concert of both best effort and reliable BCAST. Varying the user traffic load and the MAC layer we can find insights in relationship between MAC and ROUTING layer.

Problems with Current Multicast Routing Protocols:

- They have a tree based structure, so as the node connectivity changes, the tree structures changes accordingly.
- Multicast trees require a global routing substructure involving excessive Channel and processing overhead

The Reliable Broadcast Protocol [7] explains the problem of reliable delivery of messages. It [8] uses solely local recovery from nearby members for error control. Different MANET multicast protocols are available and some of them are: ODMRP [21], MAODV [3], CAMP [22], MCEDAR [4], [23]. Anyone of these protocols could be used in a brute force, “flat” approach by treating each node in the team as an individual unit without exploiting the group mobility feature. However, these schemes require periodic or event-driven control packet updates for each member in the multicast group in order to maintain the multicast structure (e.g., membership information, routes, etc.). Those protocols work effectively with small scale multicast groups (e.g., less than 100 nodes). However, they suffer from severe communication
overhead caused by control packet floods (e.g., Join Query or Request packet flooding in ODMRP and MAODV) in a large-scale network with a large number of multicast groups. Such overhead would be unsustainable in a battlefield scenario with multicast groups consisting of dozen of teams, where each team includes hundreds of units.

Achieving reliable packet delivery in a MANET is not trivial. A few simulation studies have explored the performance of MANET multicast routing protocols such as the multicast extensions for AODV and ODMRP [7, 8, and 9]. These studies commonly simulated an area of usually 1000 x 1000 meters, populated by 50 mobile nodes. Nodes move according to the “random waypoint” mobility model: initially, nodes are placed randomly within the area. Each node picks a destination and moves to that destination based on a speed that is uniformly distributed between 0 and MAX. Once a node reaches to the destination, it pauses for PAUSE seconds, after which the process repeats itself. In all these studies, Congestion controlled Adaptive Lightweight Multicast (CALM) [10] is a multicast transport protocol that tries to achieve reliable delivery strictly through congestion control. The Reliable Adaptive Lightweight Multicast protocol [11] uses a congestion control scheme similar to that of CALM and recovers from losses using source based retransmissions. It requires multicast group member information to perform congestion control and error recovery. In an extended version of RALM [12], we do maintain group membership information at the source.

A major source of network dynamics is node mobility and node failure.

i) Reliance on More Nodes

ii) Reliance on Fewer Nodes

iii) Reliance on No Nodes

iv) Reliance on Stable Nodes

v) Reliance on an Overlay Layer
The mobile Ad Hoc network has the following typical features [18]:

• There is Unreliability of wireless links between nodes.
• Dynamic change of topology.
• Lack of security features

2.7 USE OF MULTICAST IN MANETs

There are applications such military battlefields, emergency in rescue sites, classrooms, and conventions where participants share information dynamically using their mobile devices that lend themselves well to multicast operations

• Multicasting can improve the efficiency of the wireless links,
• Improved transmission efficiency can reduce energy consumption, which is an important consideration in MANETs

2.8 CHALLENGES IN MANET ROUTING

i). The MANETs need dynamic routing because of the following reasons

• Possibility of frequent topological changes.
• It is very different from dynamic routing in the Internet.
• It is Potential of network partitions.

ii). Routing overhead must be kept minimal due to the following reasons

• Wireless $\rightarrow$ low bandwidth
• Mobile $\rightarrow$ low power

Minimize # of routing control messages - Minimize routing state at each node

Other major challenges are given below

a). Auto configuration issues like

• Address assignment
• Service discovery
b). Security issues like

- Ease of denial-of-service attack
- Misbehaving nodes difficult to identify
- Nodes can be easily compromised

c). New Applications/services like

- Location based: Distribute some information to all nodes in a geographic area (geo cast).
- Content based: Query all sensors that sensed something particular in the past hour.

2.9 VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

The main reasons for vulnerabilities [20] are mentioned below.

- Lack of Secure Boundaries
- Threats from Compromised nodes inside the Network
- Lack of Centralized Management Facility
- Restricted Power Supply
- Scalability

MANETs are insecure by its nature due to mobility of nodes, lack of centralized management, restricted power supply and other factors.

2.10 ATTACK TYPES IN MOBILE AD HOC NETWORKS

There are numerous kinds of attacks in the mobile Ad Hoc network, and are classified in to two types [19, 20]:

i). External attacks.

ii). Internal attacks,

The main attack types are mentioned below.

Denial of Service (DoS)
i) Impersonation

ii) Eavesdropping

iii) Attacks Against Routing

2.11 VARIOUS MANET PROTOCOLS

The protocols used for Topology based routing are given below

- Proactive approach, e.g., DSDV. --Reactive approach, e.g., DSR, AODV, TORA.
- Hybrid approach, e.g., Cluster, ZRP.

Position based routing are given below

- Location Based Services:
  - DREAM, Quorum-based, GLS, Home Zone etc.

Forwarding Strategy

- Greedy, GPSR, RDF, Hierarchical, etc.

2.12 ON-DEMAND MULTICAST ROUTING PROTOCOL IN MULTI-HOP WIRELESS MOBILE NETWORKS (ODMRP)

ODMRP [31] is On-Demand and mesh based protocol [17, 20, 47] that sends data packets from source to destination with creating mesh. One of the important metrics in QOS of forwarding packets is Packet Delivery Ratio (PDR). PDR may be affected by mobility, Group Size, Packet Size and action range. Since ODMRP use single route for forwarding packets, if this route fails the packet is lost and cause to PDR reduction in destination.

ODMRP is based on mesh (instead of tree) forwarding. It applies on demand (as opposed to periodic) multicast route construction and membership maintenance. Simulation results show that ODMRP is effective and efficient in dynamic environments and scales well to a large number of multicast members.
The advantages of ODMRP are:

- Low channel and storage overhead
- Usage of up-to-date and shortest routes
- Robustness to host mobility
- Maintenance and exploitation of multiple redundant paths
- Scalability to a large number of nodes

ODMRP applies on-demand routing techniques to avoid channel overhead and improve scalability. It uses the concept of forwarding group (a set of nodes responsible for forwarding multicast data on shortest paths between any member pairs) to build a forwarding mesh for each multicast group. It works on mesh network instead of tree structure network.

2.12.1 ODMRP Operation

1. On demand Route and Mesh Network Creation
2. Multicast Route and Membership Maintenance
3. Data Forwarding
4. Soft State
5. Selection of Timer Values
6. Unicast Capability
2.12.2 ODMRP Route and Mesh Creation Operation

1. \( S \) floods a **Join Query** to entire network to refresh membership.

2. Receiving node stores the backward learning into routing table and rebroadcasts the packet.

3. Finally when query reaches a receiver creates a **Join Reply** and broadcasts it’s to its neighbors.

4. Node receiving the **Join Reply** checks whether the next node id in **Join Reply** matches it own. If yes, it is a part of the forwarding group, sets its **FG_FLAG** and broadcasts its **Join Reply** built upon matched entries.

5. **Join Reply** is propagated by each forwarding group member until it reaches source via a shortest path.

6. Routes from sources to receivers build a mesh of nodes called “**Forwarding Group (FG)**”.

2.12.3 Multicast Route and Membership Maintenance

**Member Table**

Each multicast receiver stores the source information in the Member Table. For each multicast group the node is participating in, the source ID and the time when the last Join Query is received from the source is recorded. If no Join Query is received from a source within the refresh period, that entry is removed from the Member Table.

**Route Table**

A Route Table is created on demand and is maintained by each node. An entry is inserted or updated when a non-duplicate Join Query is received. The node stores the destination (i.e., the source of the Join Query) and the next hop to the destination (i.e., the last node that propagated the Join Query). The Route Table provides the next hop information when transmitting Join Replies.
Forwarding Group Table

When a node is a forwarding group node of the multicast group, it maintains the group information in the Forwarding Group Table. The multicast group ID and the time when the node was last refreshed are recorded.

Message Cache

The Message Cache is maintained by each node to detect duplicates. When a node receives a new Join Query or data, it stores the source ID and the sequence number of the packet. Note that entries in the Message Cache need not be maintained permanently. Schemes such as LRU (Least Recently Used) or FIFO (First In First Out) can be employed to expire and remove old entries and prevent the size of the Message Cache to be extensive.

2.12.4 Data Forwarding

After the group establishment and route construction process, a multicast source can transmit packets to receivers via selected routes and forwarding groups. Periodic control packets are sent only when outgoing data packets are still present. When receiving a multicast data packet, a node forwards it only if it is not a duplicate and the setting of the FG_FLAG for the multicast group has not expired. This procedure minimizes traffic overhead and prevents sending packets through stale routes.

2.12.5 Soft State

In ODMRP, no explicit control packets need to be sent to join or leave the group. If a multicast source wants to leave the group, it simply stops sending Join Query packets since it does not have any multicast data to send to the group. If a receiver no longer wants to receive from a particular multicast group, it removes the corresponding entries from its Member Table and does not transmit the Join Reply for
that group. Nodes in the forwarding group are demoted to non-forwarding nodes if not
refreshed (no Join Replies received) before they timeout.

2.12.6 Selection of Timer values

Timer values for route refresh interval and forwarding group timeout interval can
have impacts on ODMRP performance. The selection of these soft state timers should
be adaptive to network environment like traffic type, traffic load, mobility pattern,
mobility speed, channel capacity, etc.

For Route Refresh Interval

-- Small Route Refresh Interval used Fresh route Information and membership
information obtained. Flow of more packets causes network congestion.

-- Large Route Refresh Interval used Up to date information about the nodes in the
network is not known. Less control traffic generated.

For Forwarding group timeout Interval

-- In heavy network load, timeout values should be small so that unnecessary nodes
can timeout quickly and create excessive redundancy.

-- In network with high mobility, the forwarding group timeout value must be larger so
that alternate paths can be provided.

Generally forwarding group timeout value must be 3 to 5 times larger than the route
refresh Interval.

2.12.7 Unicast Capability

One of the major strengths of ODMRP is its unicast routing capability. Not only
can ODMRP coexist with any unicast routing protocol, it can also operate efficiently
as a unicast routing protocol. Thus, a network equipped with ODMRP does not require
a separate unicast protocol.
2.12.8 Drawbacks of ODMRP

**Mesh is very flexible to:**

-- Short term disruptions (jamming, fading, obstacles).

-- Medium term (connectivity) disruptions, e.g. FG node moving out of field.

**FG maintenance**

-- To overcome connectivity disruptions, need frequent mesh refresh.

-- Short refresh interval (proportional to FG node longevity) needed to keep connectivity in the face of motion.

Due to high flexibility and short refresh interval leads to high overhead, which is a drawback in ODMRP as refresh rate is a key performance parameter.

When small route refresh interval values are used, fresh route and membership information can be obtained frequently at the expense of producing more packets and causing network congestion. On the other hand, when large route refresh values are selected, even though less control traffic will be generated, nodes may not know up-to-date route and multicast membership. Thus in highly mobile networks, using large route refresh interval values yield poor protocol performance.

2.13 PERFORMANCE DIFFERENCES OF ODMRP & MAODV PROTOCOLS

The MAODV and ODMRP protocols [32] uses on-demand route discovery, but have different routing mechanisms. In general, ODMRP outperforms in packet delivery ratio than the MAODV. But ODMRP doesn’t have good scalability when there is increase in the group size or number of senders.

2.14 RELIABLE ADAPTIVE LIGHTWEIGHT MULTICAST (RALM) TRANSPORT PROTOCOL

The Reliable Adaptive Lightweight Multicast (RALM) [24] transport protocol provides reliability and congestion control over throughput. For example, an operation
commander disseminating mission critical data to his troops in a covert operation is more interested in reliably delivering the commands rather than obtaining high throughput (assuming adequate throughput is obtained). In such a scenario, any data loss can be fatal to the success of the entire operation. RALM is a reliable, rate-based, congestion controlled protocol that targets small group operation scenarios ranging from special military operations to civilian emergency rescue applications. When there is no packet loss, RALM sends packets at the specified application sending rate. Once loss is detected, RALM recovers by initiating a modified send and wait procedure. Send and wait is performed with each multicast receiver that experiences losses, one at a time in a round-robin fashion. Once all receivers have up-to-date packets, RALM reverts to the application sending rate. In our previous work [6], we assumed that the multicast sources know the receiver information ahead of time and were able to use a window based congestion control approach. In this paper, we do not make such an assumption and hence use a send and wait procedure.

2.15 PURPOSES OF VARIOUS SIMULATORS

GloMoSim [92] is a scalable simulation environment build to address wireless and wired network systems. It is designed for the parallel discrete-event simulation capability provided by Parsec. It supports protocols for wireless network. New design is developed to support wired as well as a hybrid network with both wired and wireless capabilities. Most of the networking systems are currently built using a layered approach similar to the existing layered network architecture. Many of the regular APIs will be used among different simulation layers. This helps fast growth in integration of different models developed by different people in different layers. To run GloMoSim, the latest Parsec compiler is required. If we want to develop our own protocols in GloMoSim, one should use Parsec and it doesn’t require an expert.
Knowledge on C code is sufficient for the developers. Each network node is initialized as a separate parsec entity. These are considered to be separate logical processes in the simulating environment.

Fig. 2.2: Basic Structure of GLOMOSIM

Fig. 2.3: GLOMOSIM simulator GUI editor screen shot
Parsec code is used extensively in the GloMoSim kernel. It can run on different operating systems environments like Linux, Fedora and Windows Network (NT). The tool was considered for running the protocols.

Different MANETs simulators [28] exhibit different features and models. Depending upon the requirements, choice of the simulator will be decided. The key factor is to find required details. If high precision PHY layers are needed, then ns-2 [25], [27] is clearly the wisest choice. If the wireless technology has not impact on the targeted protocol, recent simulators which propose high level abstractions and polished object-oriented designs will be more adapted.

The number of nodes targeted also determines the choice of the simulation tool. Sequential simulators should not be expected to run more that 1,000 nodes. If larger scales are needed, then parallel simulators are a wise choice. One can also consider highly optimized simulators like ns-2 coupled with stage simulation. Most of the non-commercial simulators do not have good documentation and technical support. In case of trouble the commercial tool is the right choice. Many commercial simulators usually feature extensive lists of supported protocols, while open source solutions give full empowerment.

2.16 DESIGN CONFLICTS OF MULTICAST

The two conflicting design goals of multicasting are:

• The length of the paths (usually in terms hops) to the individual destinations should be minimum, and

• The total number of hops to forward the packet to all the destinations should be as small as possible.

To overcome the conflicts it uses local information. Two distinct cases can occur when forwarding node. The first part denotes the number of neighbors that the packet
is transmitted to and the second part calculates the remaining distance to all the
destinations.

\[ f(w) = \lambda \frac{|w|}{|N|} + (1 - \lambda) \frac{\sum_{z \in Z} \min_{m \in W} d(m, z)}{\sum_{z \in Z} d(k, z)} \]  

(1)

In the above equation symbols have following meaning:

k: Current forwarding node  
N : The set of all neighbors of k  
W: The set of all subsets of NZ : The set of all destinations, and  
d(x, y) : A function that measures the distance between nodes x and y.

Given a set of next hop nodes w \(\in\) W, the normalized number of next hop nodes is
determined in first part and while in second part the overall distance to all the
destinations is normalized to the distance from the current node to all the destinations.

These values are linearly combined using a Parameter \(\lambda\) \(\in\) [0, 1]. Multicast packet will
split early if \(\lambda\) is closer to 0.

In greedy multicast forwarding, there may be a situation where a packet arrives at a
node that does not have neighbors offering progress to one or more destinations. This
situation can be handled by applying a modification of the right hand rule, e.g. Face
routing. The key idea is to traverse the boundaries of the gap until greedy can be
resumed.

2.17 MULTICAST TOPOLOGY - GROUP-SHARED TREE

The properties of Group-shared tree are mentioned below

- It constructs one single tree for a multicast group even if there is more than
  one source
- It uses less memory
- It introduces possibly extra delay
- It gets possibly sub-optimal paths from a source to receivers
2.18 MULTICAST TOPOLOGY — SOURCE BASED TREE

The features of Source based tree are given below.

- It constructs an individual tree for each sender in a multicast group
- It gets optimal paths from a source to receivers
- It minimizes delay
- It uses more memory

2.19 CAMP MULTICAST PROTOCOLS

It is [22] is used in MANETs. FGMP [33, 35] requires for control packets to be flooded in an Ad Hoc network. This approach is acceptable only in small networks. In contrast, the use of cores in CAMP eliminates the need for flooding, unless all cores are unreachable from a connected component. CAMP uses a scheme based on the transmission of heartbeat messages to ensure that the mesh contains all the reverse shortest paths. Each mesh member temporarily keeps track of traffic sources whose packets come through members other than their respective reverse shortest paths to the sources. Whenever such situation arises, a heartbeat is sent to the successor in the reverse shortest path to the source given by the unicast routing table. That heartbeat message triggers a push join message when the successor is not a mesh member. The push join forces that specific successor and all routers in the path to the traffic source to join the mesh. Mesh components merge together by means of similar push joins sent towards cores. The mappings of multicast addresses to (one or more) core addresses are disseminated from each core out to the network as part of group membership reports.

It is the first multicast routing protocol based on a routing structure other than trees that does not require flooding an entire network to set up its routing structure. CAMP consists of the maintenance of multicast meshes and loops less packet forwarding over
such meshes. Within the multicast mesh of a group, packets from any source in the group are forwarded along the shortest paths defined with the mesh from the source to the receivers. CAMP guarantees that, within a finite time, every receiver of a multicast group has a reverse shortest path to each source of the multicast group, which is used to reduce the sub-optimality of the paths traversed within a mesh compared to the true shortest paths, which could include nodes that are not part of the mesh.

CAMP scales very well, because it does not require sources or receivers to flood the entire network with control or data packets as long as there are cores available. Simulation experiments show that CAMP easily outperforms tree-based multicast protocol in dynamic networks.

**2.20 SURVEY ON MULTICAST ROUTING**

There are three main categories based on the routing strategy [44]. Firstly, there are protocols, which use a proactive approach to find routes between all source destination pairs regardless of the need of such routes. Examples of this approach are [36, 26] Destination Sequence Distance Vector (DSDV) protocol, Wireless Routing Protocol (WRP), Global State Routing (GSR) protocol, Fishey State Routing (FSR) protocol, Landmark Ad Hoc Routing (LANMAR) and Optimized Link State (OLSR) protocols recently proposed by the MANET group also falls in this category. Secondly, there are the reactive (on demand) routing protocols suggested with the key motivation of reducing routing load. DSR follows this approach. Other examples of this approach are [36] Signal stability Routing (SSR), Associativity Based Routing (ABR), and Temporally Order Routing Algorithm (TORA). In addition to the above mentioned protocols, hybrid protocols combine reactive and proactive characteristics, which enable them to adapt efficiently to the environment evolution. This approach comprises Zone Routing Protocol (ZRP) [36]. Routing protocols can also be classified
in terms of an architectural view. A third classification is according to the location characteristics. Multipoint communication has emerged as one of the most research areas in the field of networking. As the technology and popularity of Internet grow, applications, such as video conferencing, that require multicast support are becoming more widespread. Multicast protocols used in static networks as Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), Core Based Trees (CBT)[34], and Protocol Independent Multicast (PIM) do not perform well in wireless Ad Hoc networks due to the fragile multicast tree structures, which must be readjusted as connectivity changes. Furthermore, multicast trees usually require a global routing substructure such as link state or distance vector. The frequent exchange of routing vectors or link state tables that are triggered by continuous topology changes yields excessive channel and processing overhead. Hence, the tree structures used in static networks must be modified, or a different topology between group members need to be deployed for efficient multicasting in wireless Ad Hoc networks [37]. To provide efficient multicast routing in MANETs, a different kind of protocols should be designed. These protocols should modify the conventional tree structure, or deploy a different topology between group members [38]. There are three general purpose On-Demand multicast protocols, namely Adaptive Demand Driven Multicast Routing protocol (ADMR), the Multicast Ad Hoc On-Demand Distance Vector protocol (MAODV), and the On-Demand Multicast Routing Protocol (ODMRP). Some technical challenges of multicast routing are as follows [39]: minimizing network load, providing basic support for reliable transmission, designing optimal routes, providing robustness, efficiency, active adaptability, and unlimited mobility.
Because of the complexity of multicast routing in Ad Hoc networks, only a few propositions have been made. Globally, we notice two main categories, tree-based protocols (e.g. MAODV, ABAM, MZR [36], and SMBP [36]) and mesh based protocols (e.g. ODMRP, Patch ODMRP). The multicast extension of Ad Hoc On-Demand Distance Vector (MAODV) routing protocol [40] uses destination sequence number for each multicast entry requiring a lot of control messages. The On-Demand Multicast Routing Protocol (ODMRP) [41] is based on a mesh structure for connecting multicast members using the concept of forwarding group nodes. ODMRP uses shortest path as a criteria to select forwarding group nodes, which is not the optimal route in a dynamic network as Ad Hoc network. Patch ODMRP [42, 43] extends the ODMRP.

Multicasting [45] is employed when the nodes in MANETs need one-to-many or many-to-many communication. The two best multicast protocols are MAODV (Multicast Ad-hoc On-Demand Distance Vector Routing Protocol) and ODMRP (On-Demand Multicast Routing Protocol). To compare these protocols, performance measures to be evaluated are the PDR (Packet Delivery Ratio). MAODV performs better for high traffic. ODMRP performs better for large areas and high node speeds and poorer for small antenna ranges. MAODV is one among the most discussed tree based protocol where as ODMRP is the best mesh based protocol.

2.21 COMPARATIVE RESULTS OF ADMR, MAODV AND ODMRP

Performance comparison of ADMR, MAODV, and ODMRP in a variety of simulation scenarios were summarized below [46]. Consider the mobile networks composed of 100 or 200 nodes, with both a single active multicast group, and multiple active multicast groups in the network, along with a variety of multicast scenarios such as conferencing and single-source vs. multi-source groups. All protocols perform well
in terms of packet delivery ratio, and the differences in behavior are in their efficiency. ADMR is the most efficient across all scenarios and typically generates 3 to 5 times less normalized packet overhead than MAODV and ODMRP, because it scales its overhead to meet existing communication demands. MAODV incurs a high level of packet overhead due to its use of periodic Hello packets and because it uses a shared group tree, which enables it to localize multicast group joins but results in longer data forwarding paths.

Due to its use of longer forwarding paths, MAODV performs more data packet transmissions, suffers from more packet losses and collisions, and higher end-to-end delay, compared to ADMR and ODMRP. ODMRP uses the shortest paths among the three protocols, and overall incurs the smallest end-to-end delay, because it performs frequent periodic state discovery floods. These floods also result in the creation of a large amount of forwarding state within the network, which improves the robustness of the protocol against mesh disconnection or packet loss, but at the cost of significantly increasing network load.

Investigated the performance on control overheads generated, access channel efficiency and the retransmissions required to deliver packets for ODMRP (mesh based multicasting approach) and ADMR (tree based multicasting approach). ODMRP is an Ad Hoc routing protocol that is capable of routing both unicast and multicast data. ODMRP unicast operation was described in detail and its performance is evaluated by comparing it with other Ad Hoc unicast routing protocols. The impact of the mobility prediction on ODMRP performance to evaluate its effectiveness was examined. Simulation results indicate that ODMRP is a competitive unicast protocol. The use of mobility prediction proved to be valuable and enhanced ODMRP
performance. With mobility prediction, more data packets were delivered to
destinations and the control packets were utilized more efficiently.

Performance of the various routing protocols such as ODMRP, AODV and FSR were
evaluated in this study [48]. The following conclusions were found.

- Both under varying number of nodes and differing values of mobility Average
  throughput is higher for the routing protocol ODMRP. The maximum throughput
  of ODMRP is 43% higher than the maximum of AODV and FSR under varying
  nodes condition.

- AODV has a higher ratio of legitimate packet delivery as compared with the other
  routing protocols evaluated, ODMRP and FSR. The maximum packet delivery of
  AODV is 38% higher than the maximum of ODMRP and FSR under varying
  nodes condition.

- ODRMP performs better in avoiding network congestion as compared to AODV
  and FSR.

A performance comparison of several multicast routing protocols (ODMRP, CAMP, AMRIS, AMRoute, and flooding) was conducted in [49, 50]. Generally speaking, mesh-based multicast routing protocols outperform tree-based counterparts in the terms of packet delivery ratio in the scenario of high mobility because of redundancy of multiple paths among group members. However, the overhead of the former is greater than the latter for the same reason. Within tree-based routing protocols, AMRoute performs the worst due to temporary loop formed in the tree creation and inefficiency of delivery tree composed of virtual links.

Generally, reactive protocols performed better for our (relatively) large number of
nodes and our modest traffic load, with ODMRP outperforming AODV [51] due its
inclusion of the original message in the flooded route discovery packets. Interestingly,
however, the performance of ODMRP dropped precipitously (and the performance of AODV improved by a similar amount) when the nodes were indoors and could all hear each other, in both cases due to the different levels of contention and packet loss. Indoor experiments on real hardware clearly cannot predict the outdoor performance of common routing protocols. On the other hand, the indoor performance does suggest that contention may play a larger role outdoors than might be expected, with results changing dramatically depending on the “clustering” of the network. Finally, the simulation results indicate that simulation, with an appropriate choice of models, can accurately predict outdoor performance.