An Efficient Non Periodic PIM-DM for Multicast over LAN and Integrated LAN-WLAN

Mohammad Rajib Ullah Ibne Bashir

A Thesis

in

The Department

of

Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements

for the Degree of Master of Applied Science (Electrical Engineering) at

Concordia University

Montréal, Québec, Canada

August 2004

Your file Votre référence
ISBN: 0-612-94692-4
Our file Notre référence
ISBN: 0-612-94692-4

ABSTRACT

Efficient Non Periodic PIM-DM for Multicast Over LAN and Integrated LAN-WLAN

Mohammad Rajib Ullah Ibne Bashir

General multicast protocols suitable for internet level deployment may not be very efficient for corporate level small scale deployment. On the basis of our needs and goals, one needs to optimize those multicast protocols or to create new multicast protocols amenable to specific environments. In this thesis, a new multicast routing protocol has been proposed, that is efficient especially for corporate level closed network multicasting. This protocol is better suited where the number of multicast receivers is higher, wired network links are relatively more reliable and closed LAN multicast is widely used.

PIM-DM is more efficient for these purposes compared to other available multicast protocols. But PIM-DM is not efficient in terms of network bandwidth, processor and memory utilization because of its periodic flooding nature. In this thesis a PIM-DM based multicast routing protocol has been proposed that is free from periodic flooding. The proposed protocol is more efficient in terms of bandwidth, processor and memory utilization than that of PIM-DM. This thesis also briefly describes the proposed protocol for an infrastructured integrated LAN-Wireless LAN with some slow speed mobile users. Simulations results support the advantages and applicability of the new protocol.

Acknowledgments

First and foremost, I would like to express my solemn gratitude to all mighty Allah, most glorious and most merciful. I could not have finished my thesis without the help of Allah.

I am very fortunate that, from the very beginning of my research work, I was under the supervision of Dr. A. K. Elhakeem. His vast experience, immense knowledge, friendly attitude, guidance and encouragement throughout my research work directed me to achieve my goal. I also like to acknowledge the financial support that he provided me during my research work.

I would also like to thank all of my friends who have ever helped me during my research work. Specially, Mahmud Hossain, Sahidul Haq Akond, Hafizur Rahman, Joydeep Dhar and Salekul Islam.

Finally, I would like to express my appreciation to my parents, brother and sister-in-law for their unlimited encouragement and support. They are always beside me and helping me with their support, love and encouragement.

Table of Contents

Chapter 3 Proposed PIM-DM for Closed LAN Multicast

LIST OF FIGURES

LIST OF ACRONYMS

ACK	Acknowledgement
AIFS	Arbitration Inter Frame Space (802.11e)
AP	Access Point
CA	Collision Avoidance
CBT	Core Based trees
CFP	Contention Free Period
CP	Contention Period
CSMA	Carrier Sense Multiple Access
DCF	Distributed Coordination Function
DVMRP	Distance Vector Multicast Routing Protocol
FA	Foreign Agent
HA	Home Agent
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ISM	Industrial, Science, Medical
LAN	Local Area Network
MAC	Medium Access Control
MOSPF	Multicast Open Shortest Path First
NAV	Network Allocation Vector

OSPF	Open Shortest Path First
PC	Point Coordinator
PCF	Point Coordination Function
PDU	Protocol Data Unit
PIFS	PCF Inter Frame Space
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast Dense Mode
PIM-SM	Protocol Independent Multicast Sparse Mode
RIP	Routing Information Protocol
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RTS/CTS	Request to Send/Clear to Send
SDU	Service Data Unit
SPT	Shortest Path Tree
SIFS	Short Inter Frame Space
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network

Chapter 1

Introduction

1.1 Motivation and Scope

With the development of multicasting routing protocols, many multicasting protocols have been developed and deployed. But all of them are general purpose multicast routing protocols and suitable for internet level deployment. These general multicast protocols may not be very efficient for corporate level small scale deployment. Because the corporate level network architecture and internet level network architecture are different and so their requirements are also different. Sometimes, general multicasting protocols developed with an aim for internet level or wide scale deployment includes many additional features. These additional features are not required by the small scale corporate level deployment. Moreover, these additional unnecessary features will cost extra network resources and thus waste valuable network resources for small scale deployment.

Corporate level networks generally consist of wired LANs. However, infrastructured integrated LAN-Wireless LANs models will also become very popular in the near future for corporate networks, because of their flexibilities.

Infra-structured integrated LAN-WLAN includes routers, APs (generally with built in routers) and a fixed backbone, with both fixed and mobile users. The rapid growth of wireless technology has attracted interest in the integration of WLAN with wired LAN. Lots of works have been done in the field of AD-HOC WLAN regarding multicast algorithms. But there is no significant development on the multicasting algorithm of Infra-structured integrated LAN-WLAN for mobility support. That's why a multicasting routing algorithm that can ensure fast and smooth handovers of mobile users with fewer control signals would be highly desired.

The above mentioned scenarios are the motivation of this thesis.

The objectives of this thesis are as follows:

1. To design a simple multicast routing protocol for efficient corporate level multicasting without making extra overhead to the network or wasting valuable network resources.
2. Ensuring reliability of the multicast protocol for corporate level multicasting.
3. Ensuring corporate level multicast confidentiality.
4. Facilitate user mobility support, when the corporate network is an integrated infrastructured LAN-WLAN.
5. Study on various performance criterions of the proposed multicast routing protocol.
6. Vary input parameters, and perform studies and comparisons with the inherent protocols.

1.2 Thesis Organization

In chapter 2, IP multicast is introduced with its definition, necessity and applications. Important IP multicast techniques like group management, addressing and distribution tree constructions are covered. Moreover, most important multicast protocols are described with their advantages and disadvantage. Finally, the chapter describes the micro mobility protocols.

In chapter 3, inherent PIM-DM problems for corporate multicast are discussed and then the solution was given mainly by introducing multicast session end message. Moreover, the proposed protocol's reliability issues are also described. Additionally, the chapter describes the corporate level multicast confidentiality technique. This chapter also includes simulations results on different performance criterions and their corresponding discussions.

In chapter 4, at first the problems of other multicasting routing protocols, including inherent PIM-DM for integrated infrastructured LAN-WLAN are defined. Solutions are given by describing proposed protocol for corporate level integrated infrastructured LAN-WLAN. Mobility support mechanism has been described in the view of both sender and receiver movements. Simulations results on performance criterions of mobility issues are also described in this chapter.

In chapter 5, the thesis summarizes the contributions and conclusions and suggests necessary future works.

Chapter 2

Review of IP Multicast, WLAN and Micro Mobility

This chapter introduces the IP Multicast concept and covers the definition of IP multicast, the advantages and disadvantages of IP multicast, multicast group management, IP multicast addressing and routing algorithms. Furthermore, this chapter describes the WLANs and micromobility technology.

2.1 Overview of IP Multicast

2.1.1 What is IP Multicast?

IP Multicast is mentioned as "the transmission of an IP datagram to a 'host group', a set of zero or more hosts identified by a single IP destination address" [1].

In general IP communication a host (sender) sends datagrams to a single host (Unicast), to all hosts (Broadcast) [2] or to a particular host in a group (Anycast) [3]. But IP multicast gives the fourth option to send the datagrams to all hosts in a group or groups.

Multicast provides efficient group communications. Transmission of these datagrams can be from one to many or many to many. Which means multiple sources and multiple groups are allowed.

2.1.2 Why IP Multicast?

For efficient group communications unicast and broadcast will cause the following problems-

1. Inefficient bandwidth utilization.
2. Too much processing load on routers.
3. Receiver's addresses are needed.

Anycast will not complete the group communication process. As with anycast, packets are transmitted to a particular receiver and from there the packets need to be collected by the receivers.

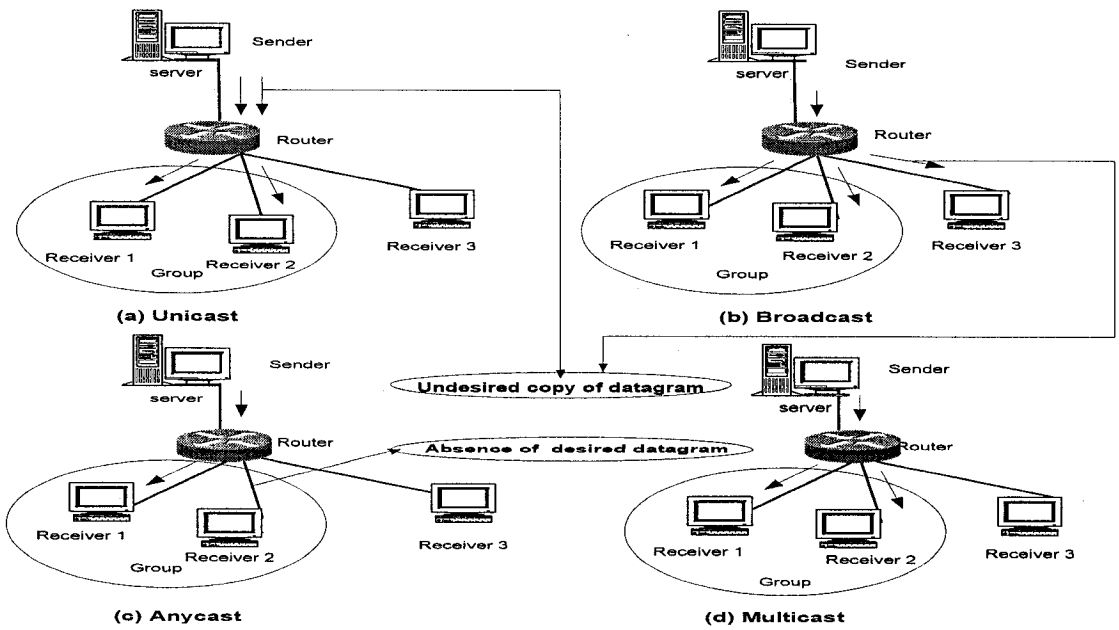


Figure 2.1: Concept of Unicast, Broadcast, Anycast and Multicast

In Figure 2.1 we have a Group, whose members are Receiver 1 and Receiver 2. If we want to send datagrams to this group, we can do one of the following:

-Using unicast the sender needs to send one personal copy to every receiver.

-By using broadcast, the sender needs to send one copy to its designated router and the router broadcasts it through out the network. Packets are received by all connected receivers, regardless a receiver needs it or not.

-By using anycast, the sender will send a personal copy to any particular receiver (generally to the nearest receiver) in the group. This receiver becomes the mirror (server) for the other group members.

-Finally when we use multicast, sender sends a single packet to the router and the multicast router multicasts the packet to the desired receivers by using various algorithms. So, we see that multicast efficiently controls traffic and reduces server and router loads by removing redundancy of datagrams. Thus multicast enables efficient multi point group communications. [4]

2.1.3 Multicast Disadvantages [4]

Main multicast disadvantages are as follows-

• Multicast applications are UDP based. Best effort delivery sometimes causes packet drops. Many real time multicast applications may be disturbed by these losses. Again too many retransmissions of the lost data are not desired for real-time applications.

• Too much drops on voice applications may cause missed speech patterns.

• For video, moderate to heavy drops are often better tolerated by human eyes or

video application softwares. However, some compression algorithms used in video transmission can be severely impacted. This can make the picture noisy and become frozen for several seconds.

• With the change of network topology, duplicate packets may be generated for multicast.

2.1.4 Some Multicast Applications [4]

Most common multicast applications are as follows-

Sdr (session directory)

- Lists view of available advertised sessions.

- Launches multicast applications on click.

Vat (audio conferencing)

-Various compression algorithms based audio conferencing.

VIc (video conferencing)

-Video conferencing based on various video compression algorithms.

Wb (white board)

-Shared drawing tool.

-PostScript images can be imported.

-Uses Reliable Multicast.

2.2 Multicast Group Management

Multicast group concept is described as "the membership of a host group is dynamic; that is, hosts may join and leave groups at any time. There is no restriction on

the location or number or members in a host group. A host may be a member of more than one group at any time." [1].

Group membership protocol is used by routers to know about the present group members on their directly connected sub networks. It is used by the multicast clients to subscribe particular event and thus a particular group. When a host wants to join a Multicast group, it sends a join message for the group and waits to receive multicast packets from the group. This is accomplished by the IGMP (Internet Group Membership Protocol). The router periodically queries the receivers to know, who still need the traffic. This periodic query comes in every 60 seconds.

IGMP version 2 [5], allows "leave the group" message from the user. So, the router does not need to make any periodic query message in every 60 seconds. However, the router still queries every time a user leave a group to know if there are any more interested users. Because the router is never tracking how many subscriptions it has at a certain time.

IGMP version 3 [6], allows "source specific" multicast. It allows the clients to specify the desired source. In Figure 2.2 basic IGMP mechanisms has been shown.

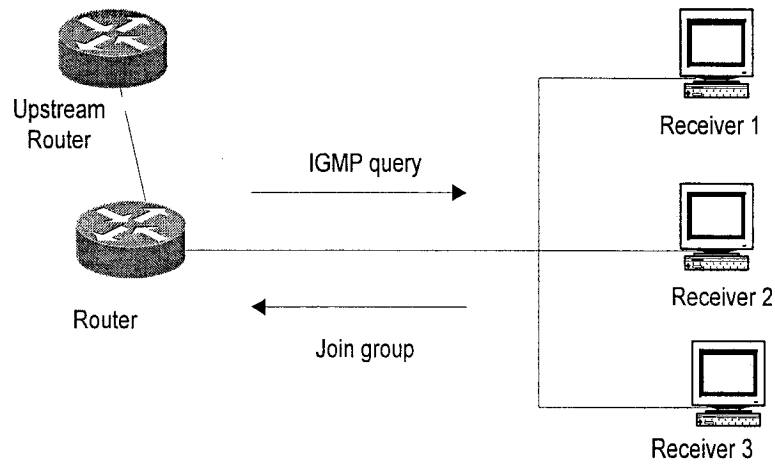


Figure 2.2: IGMP v1 query and join

Generally, we do not enable or disable IGMP on our PC. It comes as a built in function into the viewer/listener/client software [7].

2.3 IP Multicast Addressing Format

There are five classes of IPv4 addressing. First three (class A to C) are for unicasting purposes. Fourth (class D) is for multicasting purposes. Last one (class E) is reserved for experimental purposes. Each address consists of four octets separated by a decimal. Table 2.1 shows different classes of IP address.

Class	Range	Purpose
A	0.0.0.0 to127.255.255.255	Unicast
B	128.0.0.0 to 191.255.255.255	Unicast
C	192.0.0.0 to 223.255.255.255	Unicast
D	224.0.0.0 to 239.255.255.255	Multicast
E	240.0.0.0 to 247.255.255.255	Experimental

Table 2.1: Different classes of IP address

The (IPv4) addressing format is shown in Figure 2.3. The first 4 bits specify it as a multicast address and the remaining 28 bits specify a particular group.

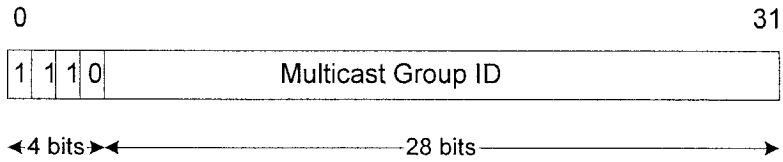


Figure 2.3: Multicast IP address format

Well known addresses designated by "The Internet Assigned Numbers Authority (IANA)" [8] are-

224.0.0.0 through 224.0.0.255 for reserved use, 224.0.0.1 for all multicast systems on subnet and 224.0.0.2 for all routers on subnet.

When a multicast session is going to be started then the source selects a destination address (class D). This address corresponds to a particular multicast group. Receivers join and leave a group using IGMP. So, we see that in multicast, the source does not recognize the receivers individually; rather the source only recognizes the groups.

2.4 Multicast Packet Distribution Trees

Multicast packet distribution tree defines the path down which traffic flows from source to receiver(s). Two types of multicast distribution trees are - source tree and shared tree.

2.4.1 Source Trees

Source tree is the simplest form of multicasting tree. Source tree has its root at the source and branches form the spanning tree towards the receivers. This is often called as shortest path tree (SPT) as the tree uses the shortest path through out the network.

A Shortest path is a minimum spanning tree with the lowest cost from the source to all leaves of the tree.

Packets are forwarded on the Shortest Path Tree according to both the Source address (S) that the packets originated from and the Group address (G) that the packets are addressed to. This is the reason the forwarding state on the Spanning tree is denoted by the notation (S,G).

Where:

- "S" is the address of the source.
- "G" is the multicast group address
- (S,G) means Source – Group pair or a state.

For multiple sources and multiple groups many (S,G) states are created in the routers. As an example (S1,G7) means the state of source1 and Group 7 pair.

In Figures 2.4 & 2.5 -

The shortest path between Source 1 and Receiver 1 is via Routers A and C, and shortest path to Receiver 2 is one additional hop via Router E. Each SPT is routed from the source. That implies that there is a corresponding SPT for every source sending towards a group. [4]

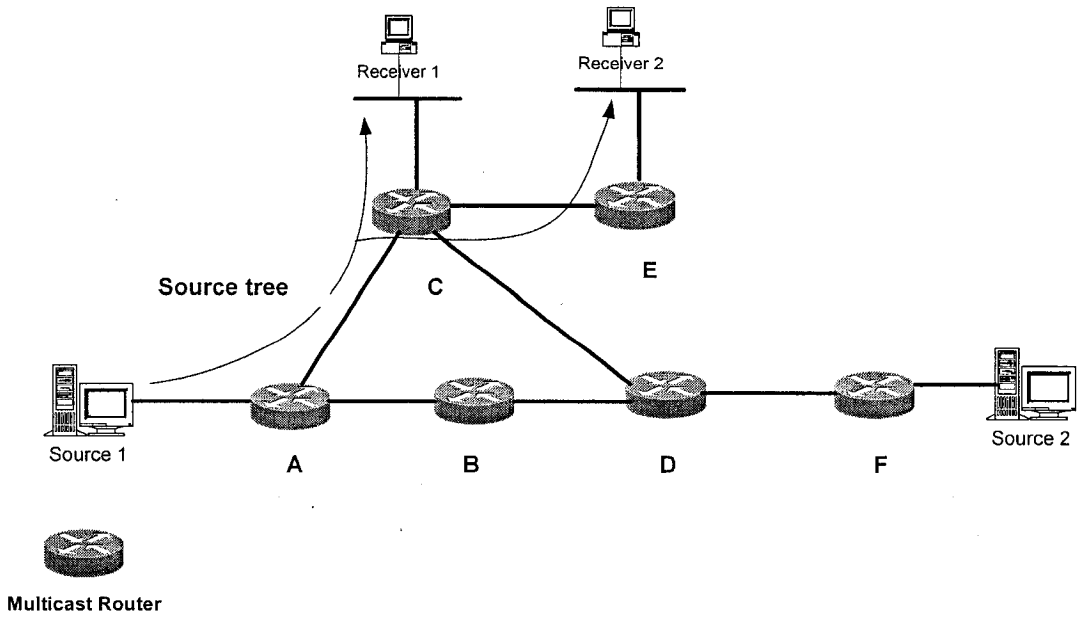


Figure 2.4: Source tree for source 1

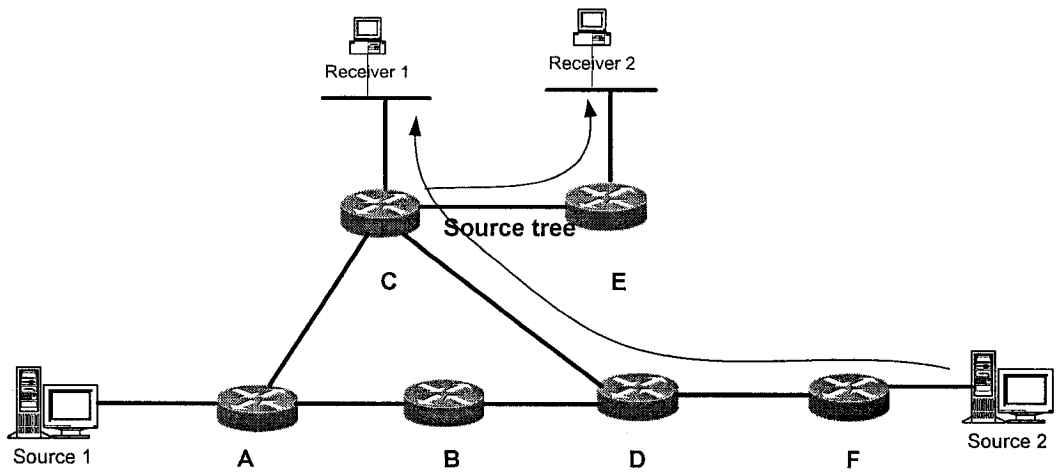


Figure 2.5: Source tree for source 2

The shortest path between Source 2 and Receiver 1 is via Routers F, D and C, and shortest path to Receiver 2 is one additional hop via Router E.

Shortest path tree has the advantage of creating the optimal path between the source and the receiver. This ensures the least network latency for the forwarding of multicast packets. But the main drawback is that every router must maintain path information for every source. In a huge network where there may be thousands of sources and groups, this can create an overhead for the routers and can become a scalability issue. Because, the memory consumption due to the size of the multicast routing table will increase with the increase of source-group pairs. [9]

2.4.2 Shared Trees

On the shared distribution tree the root is a shared point in the network. Multicast data flows downwards to reach the receivers in the network. Multicast traffic is forwarded down the Shared Tree according to just the Group address G that the packets are addressed to, regardless of source address. For this, the forwarding state on the shared tree is denoted by the notation (*,G)

Where:

- "*" means any source
- "G" is the group address

Before traffic can be sent down the Shared Tree it must somehow be sent to the Root of the tree. Rendezvous Point (RP) joins the Shortest Path Tree back to each source and the traffic flows to the RP and from RP down through the shared tree. In order to trigger the RP to take this action, it must somehow be notified when a source goes active in the network.

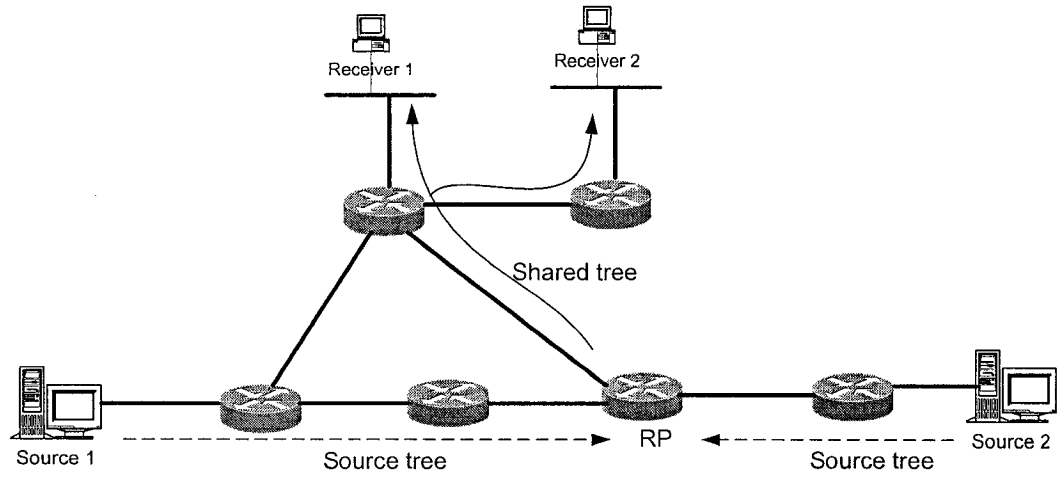


Figure 2.6: Shared tree

In the Figure 2.6, the RP has been informed of Sources 1 and 2 being active and has subsequently joined the SPT to these sources. [4]

Shared tree needs minimum amount of states in routers. This saves memory consumption. The main disadvantages are:

- It may get sub-optimal paths from source to all receivers and thus may introduce extra delay.
- Shared trees may create traffic concentration near the RP.
- If the core router (RP) is down then whole multicast process may be affected. [9]

2.4.3 Multicast Routing Protocols and the Ways of Creating Distribution Trees

In this section, ways of creating multicasting distribution trees of different multicast routing protocols will be described briefly. Details of the different multicast protocols will be described in section 2.5.

PIM [10] & [11] utilizes the underlying unicasting routing table and the following messages-

Join: Join messages are sent to upstream routers by the downstream router to establish themselves as branches of the tree when they have interested receivers attached with them.

Prune: Prune messages are generated by the routers to send PRUNE messages towards upstream routers and thus removing themselves from the distribution tree when they no longer have any interested receiver.

Graft: Graft messages are generated by already pruned router to get back the multicast traffic. When a router gets an IGMP join message and if it does not have the requested traffic then the router creates Graft. By the Graft, a router re-establishes itself as a branch of the distribution tree.

DVMRP [12] utilizes a special RIP -like multicast routing table, special metric of Infinity (Poison-Reversea) and the originally received metric to make the distribution tree. Routers also send Prunes and Grafts similar to PIM-DM.

MOSPF [13] utilizes the underlying OSPF (Open shortest path first) unicast routing protocol to build (S,G) trees. Each router has to maintain an up-to-date image of entire network topology all the time.

CBT [14] utilizes the existing unicast routing protocol and the Join/Prune/Graft

mechanisms to build the distribution tree. [4]

2.5 Routing Protocols for IP Multicast

Multicast routing protocols are not as simple as unicast routing protocols. Because multicast routing protocols have to take care of the changes in the network topology as well as group memberships. On the basis of receiver's distribution through out the network, multicasting routing protocols are classified into two main classes-

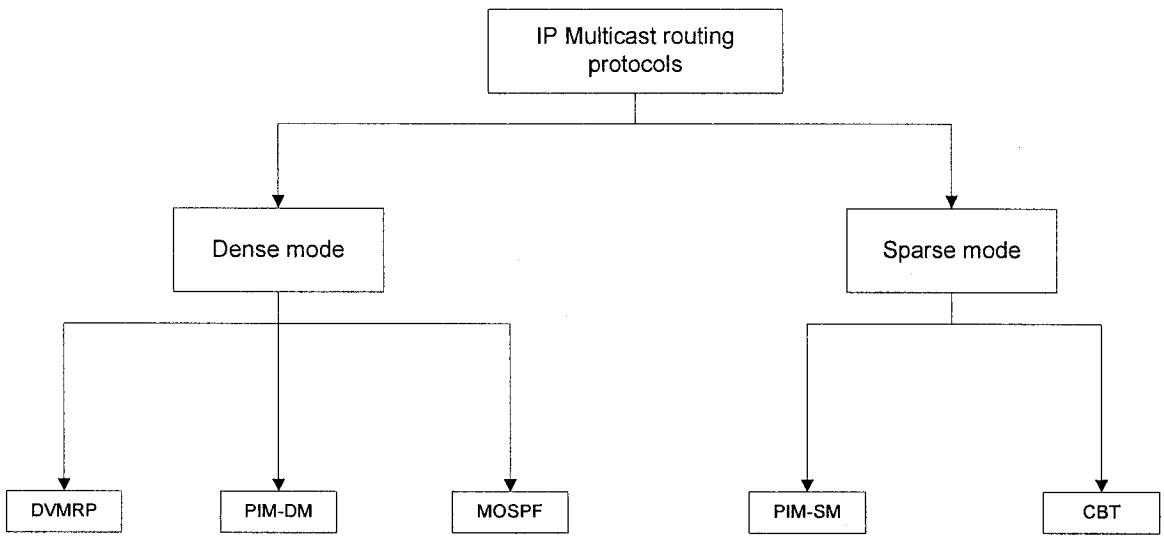


Figure 2.7: IP multicast routing family tree

The Dense mode and the Sparse mode [15]. Figure 2.7 describes the multicast family tree. The Dense mode assumes that the multicast group members are densely distributed through out the network. While sparse mode assumes that receivers are sparsely distributed. Both modes of multicast routing protocols are widely chosen depending on the distribution of multicast group members, processing efficiency, speed, simplicity, band-width availability of the network etc.

2.5.1 Protocol Independent Multicast (PIM)

2.5.1.1 PIM Dense Mode (PIM-DM)

PIM-DM [10] uses a very simple way for IP multicast routing. PIM-DM assumes multicast packet stream has receivers at most locations. A very common example of this might be a company announcement by the president of the company.

PIM-DM starts by flooding the multicast traffic and then stops this at every link where there is no interested receiver by using Prune messages.

PIM-DM v1 re-floods all the multicast traffic in every 3 minutes. This may not be good for high volume multicast. However PIM-DM v2 includes a new message called "State-refresh" This feature uses a PIM state refresh messages to refresh the Prune state on outgoing interfaces. This message also can detect topology changes more quickly. In general, state refresh messages are sent every 60 seconds. Details of this message will be described on chapter 3.

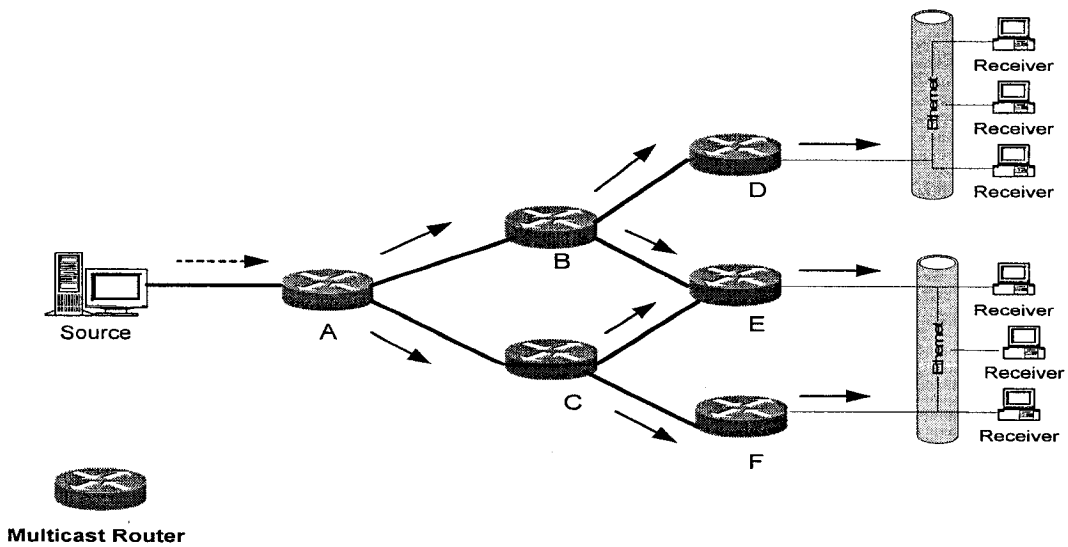


Figure 2.8: PIM Dense mode

In Figure 2.8, consider the case of router E and F. When there are more than one PIM-DM routers connected to a LAN, they will see the multicast packets from each other. One should forward packets to the LAN while the other must stop. Both of them create Assert messages at this situation. Best routing metric wins, with higher IP address as a tie-breaker.

Prune delay ensures one leaf node in an Ethernet to keep continue with the session while other leaf node sends a prune message to the upstream router. When a prune message is heard by the other leaf node, it creates a join message. Whenever an upstream router gets a prune message from any Ethernet leaf node it waits for 3 seconds. By this time the upstream router gets a join message from the interested leaf node and the interface remains open. Suppose a router was Pruned previously and some time later a receiver requests the multicast stream using IGMP join message. Then a Graft message is created by the router. This Graft message manages desired traffic for the receiver.

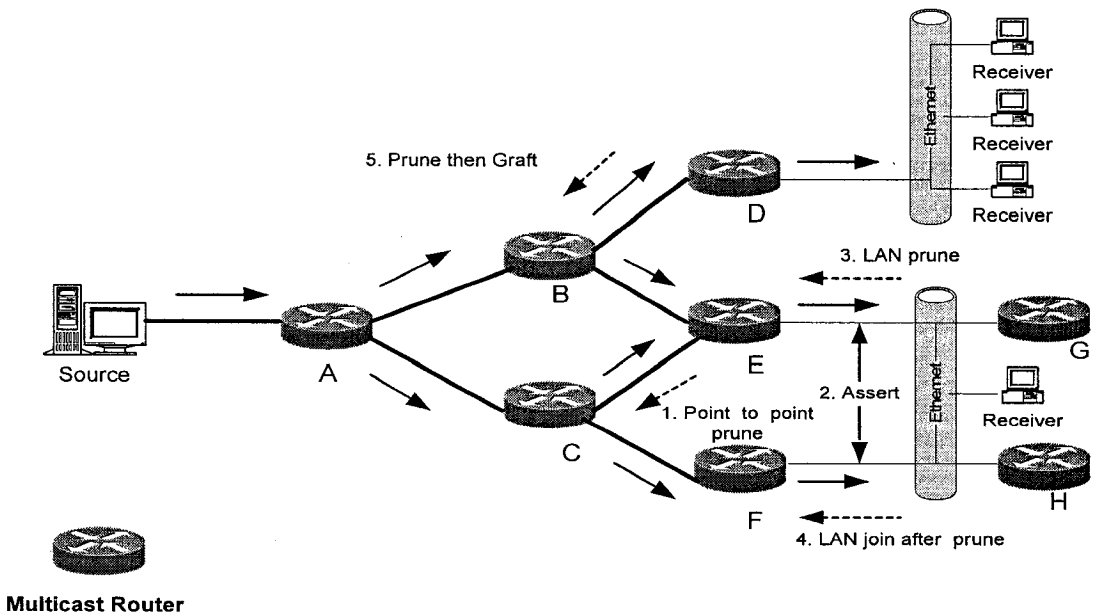


Figure 2.9: PIM-DM messages

In Figure 2.9, Router E chooses B as its RPF neighbour on the basis of unicast routing back to the source. E receives a multicast packet through the point-to-point interface from C. It sends a Prune to C.

When E and F notice duplicate packets they exchange Assert messages. Suppose E wins on the basis of unicast routing metric or address. Then F will not forward multicast packets on the LAN. Router G and H are not involved in assert mechanism because the Ethernet is their RPF interface.

When router G has no downstream receivers, it generates a LAN Prune to router E.

Whenever router H has local or downstream receiver(s), it generates Join that overrides the prune.

Suppose router D had no downstream or local receivers and previously sent a Prune to the router B. Sometime later a receiver to its right become interested to get the multicast traffic then it sends an IGMP message for the same multicast group. Router D then generates and sends a Graft message to B. Then B starts sending multicast traffic to router D and eventually to the receiver. [15]

2.5.1.1.1 Advantages of PIM-DM

- Most simple technique.
- Independent of underlying unicast routing protocol.
- Uses optimal path.
- Suitable for Dense mode.

2.5.1.1.2 Disadvantages of PIM-DM

- Periodic flooding causes Bandwidth wastage.
- No support for shared tree.

2.5.1.2 PIM Sparse Mode (PIM-SM)

PIM Sparse Mode (PIM-SM) [11] assumes relatively fewer receivers. An example would be the initial orientation video for new employees. This difference shows up in the initial behaviour and mechanisms of the two protocols. In PIM-SM multicast packets are sent only when there is a request.

PIM-SM uses a Rendezvous Point (RP) to connect source and receivers. There can be only one RP per multicast group, and the simplest implementation uses one RP for all the multicast groups. RP gives a way of using the Shared Tree and thus controlling the excessive creation of state information in routers, when too many receivers join at the same time.

There is no protocol for registering sources with IP multicast. When the multicast source starts sending, it sends up to the neighbouring router(s). In PIM-SM the neighbouring router knows about the RP. The neighbouring router forwards the multicast data to the RP by encapsulating it in the form of a unicast Register message or messages. Normal routing delivers this message to the RP. RP de-encapsulates the message and forwards copies down any Shared Tree. If receivers exist, the RP sends a PIM Join back towards the Source. This connects the Source to the RP and makes the Source Tree (S, G), Shortest Path Tree (SPT). Once the RP receives multicasts along this SPT, it sends a

Register-Stop to tell the router of the Source to stop sending Register packets. This behaviour ensures no loss of multicast packets, if receivers are already present.

However, if there are no receivers present, the Register-Stop message is sent. Later on if a receiver subsequently shows up then the RP sends the PIM Join to the Source at that time. Figure 2.10 assumes there is a source and active receivers (not shown). The receiver sends an IGMP report to router D. Router D then sends a Join towards the RP. If there are other receivers, the RP is already joined to the Source Tree and is receiving the multicast flow. It passes the Source Tree flow packets on via the Shared Tree.

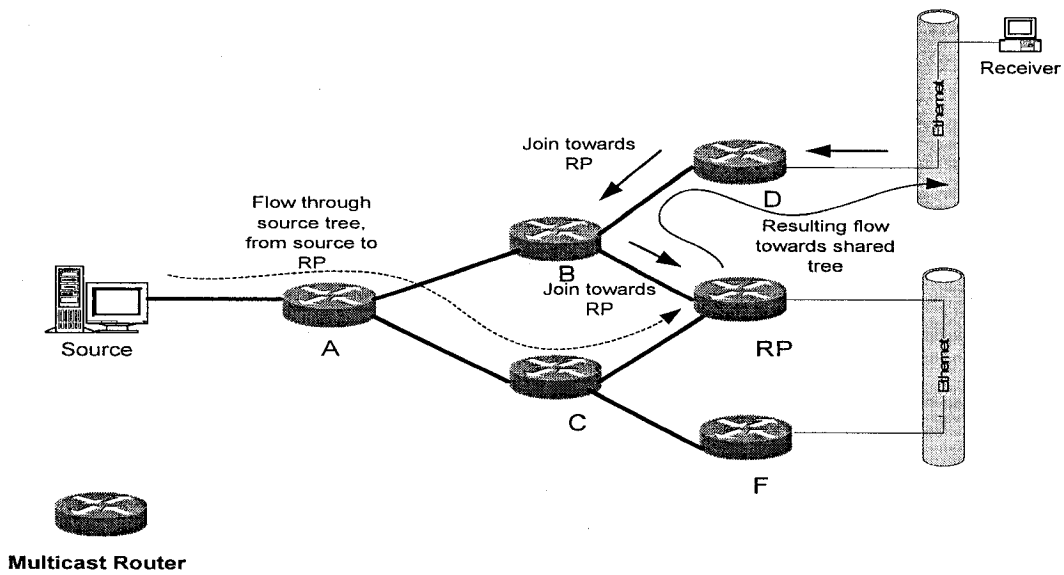


Figure 2.10: PIM Sparse Mode

So, we have two paths and thus two types of trees. Packets going from the Source to the RP along the Source Tree (Shortest Path Tree, SPT). And from the RP to the receiver along the Shared Tree. When the total packet bit rate from all sources exceeds a threshold in bit rate then this triggers the router nearest the receiver to try to join the Source Tree.

And it sends a Join towards the source of the multicast flow. Previously Join message was sent towards the RP. Now, the Join towards the source goes router by router towards the Source until it reaches a router that is already in the Source Tree. This adds the receiver's router to the Source Tree. As soon as a packet is received along that tree, a Prune is sent towards the RP. Figure 2.11 shows, how this works.

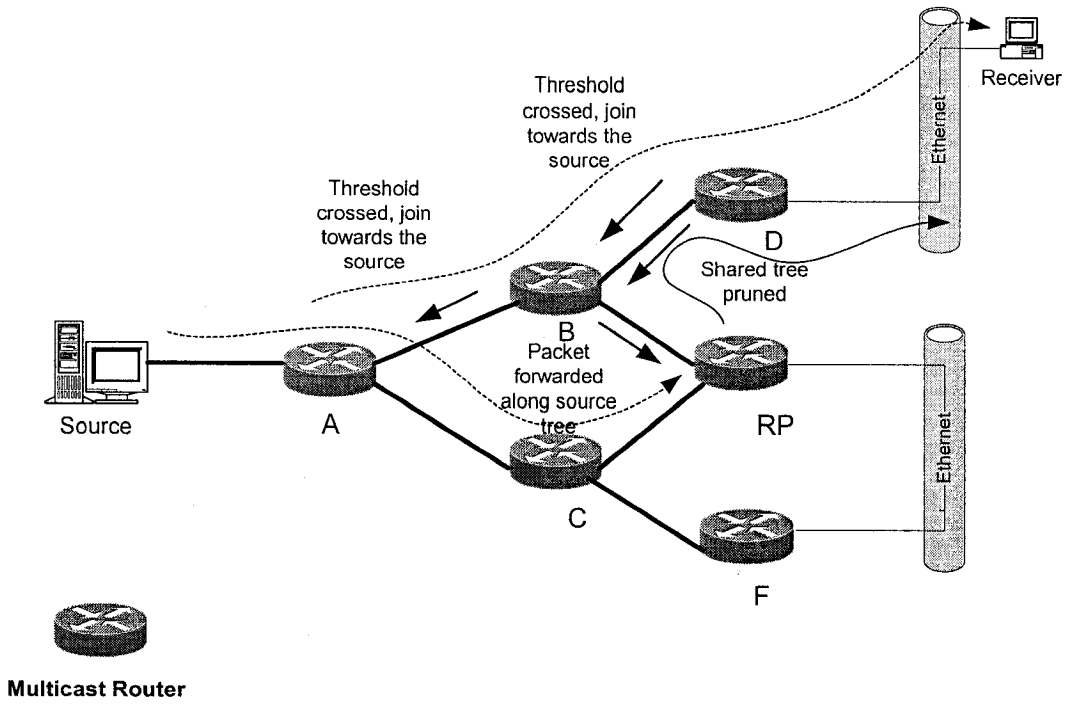


Figure 2.11: PIM-SM tree transfer mechanism

By the way, the threshold is controllable on the basis of bit rate. But the default is zero Kbps. If we have many sources for a particular multicast group then there is a (S, G) Source Tree entry for each one. If the threshold is set to be never activated, then all packets go through the RP using only the Shared Tree. Low rate (S, G) Source Trees are

switched back over to the Shared Tree to maintain the quality. The volume of traffic is checked every minute.

If a receiver wishes to join while its neighbour router is on the Source Tree, then the outgoing interface Shared Tree entry is copied to the Source Tree entry. This protects traffic to be send to the RP and then transferred to the router on the source tree. [16]

2.5.1.2.1 Advantages of PIM-SM

- No flooding required.
- Users join explicitly.
- Can use shared tree and move to source tree dynamically.
- Independent of underlying unicast routing protocol.
- Suitable for wide scale sparse mode deployment.

2.5.1.2.2 Disadvantages of PIM-SM

- May use sub optimal path for some time.
- Too much bottlenecks towards RP.
- When RP is down, the whole process is disturbed.
- Relatively complex algorithm.
- Needs many control messages.

2.5.2 Distance Vector Multicast Routing Protocol (DVMRP)

The Distance Vector Multicast Routing Protocol (DVMRP) [12] was driven from the Routing Information Protocol (RIP) [17]. The difference is that RIP forwards the packets toward the destination based on next-hop information, while DVMRP makes transmission trees based on the previous-hop backward to the source. This destination may be a single host, single subnetwork, or a group of sub networks.

The first packet of multicast from a particular source to a particular multicast group is flooded through out the network. Then, uninterested routers create "Prune" messages. Prune messages are used to cut off the branches with no multicast group members. Prune messages are forwarded hop by hop. "Graft" message grafts a previously pruned branch of the delivery tree when a new host on that branch joins the multicast group. Like the prune messages graft messages are sent back hop by hop until they reach a node which is on the multicast delivery tree. DVMRP needs periodical floodings. [19]

2.5.2.1 DVMRP Source Tree Building

The concept of "Truncated Broadcast trees" is used to build DVMRP Source tree. Truncated Broadcast Tree (TBT) for source subnet "T1" represents a shortest path spanning tree started at subnet "T2" to all other routers in the network. In DVMRP, the TBT's for all sub-networks are built by exchanging the periodic DVMRP routing updates between all DVMRP routers in the network. Just like unicasting protocol, RIPv2, DVMRP updates contain network prefixes along with route metrics in the form of hop number). This describes the path cost of reaching different subnets in the network.

A downstream DVMRP router signals an upstream router that this link is on the TBT for

source subnet S1 by using Poison-Reverse advertisement. This Poison-Reverse is constructed by adding 32 with the advertised metric and finally sending it back to the upstream router.

2.5.2.2 DVMRP Forwarding to Multi-Access Network

When there is more than one router present in a subnetwork, then the router which is closest to the source is selected to forward multicast packets. Others will simply discard the multicast packets from that source. When there are two or more routers in a subnetwork with the same distance from the source, the router with lowest IP address will forward the multicast packets.

In DVMRP each source has its own TBT. So, there is only one TBT for each source network in a DVMRP net work. [4]

2.5.2.3 Advantages of DVMRP

On TBT the initial flooding of multicast traffic all over the DVMRP network is limited to flowing down the branches of the TBT. This ensures no duplicate packets sent as a result of parallel paths in the network.

2.5.2.4 Disadvantages of DVMRP

• TBT requires DVMRP routing information to be exchanged throughout the entire network. (Unlike PIM that make use of the existing unicast routing table and do not have to exchange additional multicast routing data).

• DVMRP is based on RIP model and thus it is not unicast protocol independent.

• Efficient unicast protocol like OSPF has superseded RIP long ago in terms of robustness and scalability. So, RIP is not widely used and thus DVMRP becomes obsolete. [4]

2.5.3 Multicast Extension to OSPF (MOSPF)

MOSPF [13] is an extension to OSPF (Open shortest path first) unicast routing protocol. MOSPF requires OSPF as an underlying unicast routing protocol. MOSPF uses "Group-Membership LSA" (Group-Membership Link State Advertisement) to advertise the existence of Group members on networks.

Group-Membership LSA's are periodically flooded throughout an area in the same fashion as other OSPF LSAs. MOSPF uses shortest-path tree for every source network. MOSPF uses Dijkstra algorithm to compute this shortest-path.

MOSPF supports hierarchical routing. All hosts in the internet are considered into some "Autonomous Systems" (AS). Every AS is further divided into subgroups named as "areas". The following sections describes MOSPF multicast routing in these levels.

2.5.3.1 Intra-Area Routing of MOSPF

OSPF is a link-state based routing protocol. OSPF splits AS into areas. OSPF link state database provides the complete map of an area. This database is kept at each router. Using link state advertisement, the information about the location of members of multicast groups can be obtained and kept in the database. Using Dijkstra algorithm shortest-path delivery trees rooted at the source nodes are constructed. Group

membership information is used to prune the links not belonging to a group member. All area routers have the complete map of the topology of the area and group membership database. As long as source and all group members are in the same area, all the routers will follow the same delivery tree for a given (source, group) pair. These delivery trees are constructed on demand. When a router receives the first multicast packet of a (source, group) pair, it will build the delivery tree. On the basis of delivery tree the router decide the interface it should expect to receive multicast messages (of a particular (source, group) pair and towards which interface(s) it should forward the packets. There will be separate "forwarding cache" in every router for every (source, group) pair. This is created on the arrival of multicast packets. This cache contains the interface on which the packets are expected to be received from and the interfaces the packets should be forwarded through. MOSPF do not need the first packet to be flooded in an area.

2.5.3.2 Inter-Area Routing of MOSPF

When the source and/or some of the group members are in different areas of an AS .The intra area routing mechanism won't be enough for forwarding multicast packets. For this situation area border routers (Bars) are elected to work as the inter-area multicast forwarders. Inter-area multicast forwarders are responsible for forwarding a summarized version of group membership information of their attached areas using a new type of group membership LSAs. However, this information is not flooded into non-backbone areas.

"Wild-card multicast receiver" is also used in MOSPF. This wild-card multicast receiver gets all the multicast packets originated in their areas. All the inter-area multicast

forwarders in non-backbone areas are wild-card multicast receivers. This ensures all the multicast packets originated in a non-backbone area to reach the inter-area multicast forwarders. For this reason, these packets can be forwarded to the backbone area if it is necessary. Multicast packets can be forwarded to the appropriate areas in AS because the backbone has complete information about group memberships in different areas.

2.5.3.3 Inter-AS Routing of MOSPF

When source and/or some of the destination multicast group members are in different Autonomous Systems (AS), then MOSPF uses Inter-AS routing. Inter-AS routing is very similar to that of inter-area routing. Some of the AS Boundary Routers (ASBRs) are configures as "inter-AS multicast forwarders". Inter-AS multicast forwarders are also wildcard multicast receivers in their attached areas. That ensures these routers to remain on all multicast delivery trees and receive all multicast packets. [4]

2.5.3.4 Advantages of MOSPF

- MOSPF uses the optimum path and thus ensures efficient routing in terms of path cost.
- MOSPF does not need any flooding.

2.5.3.4 Disadvantages of MOSPF

- MOSPF is protocol dependent. It needs OSPF to work.
- Dijkstra algorithm needs to be run for every (S,G) pair.
- Dijkstra algorithm need to be rerun when group membership changes.
- MOSPF does not support shared-trees. [4]

2.5.4 Core-Based Trees (CBT)

Core-based tree (CBT) [14] has a centralized router that coordinates all transmissions for a particular group. A node wishing to join a new multicast group issues an IGMP host membership report. As soon as a multicast router receives a request to join a new group, the CBT uses a mechanism in which all memberships are directed towards a centralized router. Every CBT router keeps a cache of multicast routing information.

In CBT a single core router is used to coordinate multicast traffic through a particular region of a network. Every multicast-capable router willing to participate in a multicast (through IGMP host membership reports) will direct a CBT join request towards the centralized router. When the join request reaches another multicast router (MRX) that is already participating in a desired group then the membership is granted by that router. The join message does not need to go up to a centralized router. Every multicast router maintains a list of group participation as well as the particular interface that the multicast traffic is to be forwarded through.

When a multicast packet is received by any CBT router, it searches the local routing cache to determine the interfaces for which the particular multicast group is registered. Then the router will forward the multicast packet to all interfaces except the interface on which the packet was received.

Messages used by CBT for signalling purposes are-

• Join request is generated by a leaf router towards the core router when it needs to join a new group. This message isn't always sent unicast to the core router. The message is

forwarded through the intermediate multicast routers (MRX) towards the core. If the message reaches an intermediate router, which is already a member of the desired group then the intermediate router will process the request and the join message is stopped. It will not travel anymore towards the centralized router.

• Join acknowledge works as acknowledging messages after successful processing of the Join request message. As soon as a router receives the Join ack message that means the multicast route is fully established. And from then multicast packets follow the path guided by this route.

• Quit notification message is sent when a router decides that it no longer needs multicast from a particular multicast group. Unlike the join request, there is no explicit acknowledgement message for Quit notification. Quit notification is generally sent couple of times.

• Child routers periodically send Echo request messages to monitor the availability of parent routers. It is much like "Hello" messages. Whenever an upstream router receives this message it starts a timer. The router will issue an Echo reply message upon the expiration of the timer. When Echo reply is not received, corresponding cached route needs to be updated.

• When a router losses connectivity to its parent for a particular group then it floods Flush tree message to all downstream routers. This message will contain references to the groups that must be disabled due to lost connectivity [20].

2.5.4.1 Advantages of CBT

• Suitable for widely distributed multicast.

• Reverse path multicast (RPM) protocols need to continuously check the actual flow of multicast transmissions while CBT routers only maintain forwarding caches for the multicasting of packets.

2.5.4.2 Disadvantages of CBT

• CBT has no capability to switch to SPT and thus may use the suboptimal path.

• CBT can suffer from latency problems as all traffics need to flow through the core router.

• CBT Core routers can become bottlenecks when senders and receivers are very far apart from each other. [4]

2.6 Review of Wireless LAN (WLAN)

In Wireless LAN technology, the wires of LAN have been eliminated by digital radio or infrared transmission. WLAN simplify the installation and can give wireless communication between two nodes. WLANs are getting very popular due to their flexibility and the inherent possibility of wireless nodes to be mobile. There are some other standards similar to WLAN such as HiperLan/2 [21] and HomeRF [22], but they are not very popular.

2.6.1. Topologies of Wireless LANs

Wireless LANs (IEEE 802.11) [23] allow for more flexible communications. There are two types of wireless LANs: infrastructure WLAN and Ad Hoc (Peer-to-peer) WLAN.

2.6.1.1 Infrastructure Wireless LANs

The infrastructure WLAN consists of Access points (AP) and mobile receivers. Access Points are fixed and connected to the wired Backbone network. APs act as gateways between the mobile users and the wired backbone. APs are analogous to the Base stations of cellular networks.

The basic service set (BSS) is the basic building block of the Infrastructured WLAN,

"A BSS is defined as a group of stations that coordinate their access to the medium under a given instance." [24]

Each BSS has an AP. The geographic area of BSS is known as basic service area (BSA), analogous to the cell area of the cellular network.

BSSs interconnected by the distribution system form an extended service set (ESS) [24]. Figure 2.12 illustrates an example of the infrastructure WLAN.

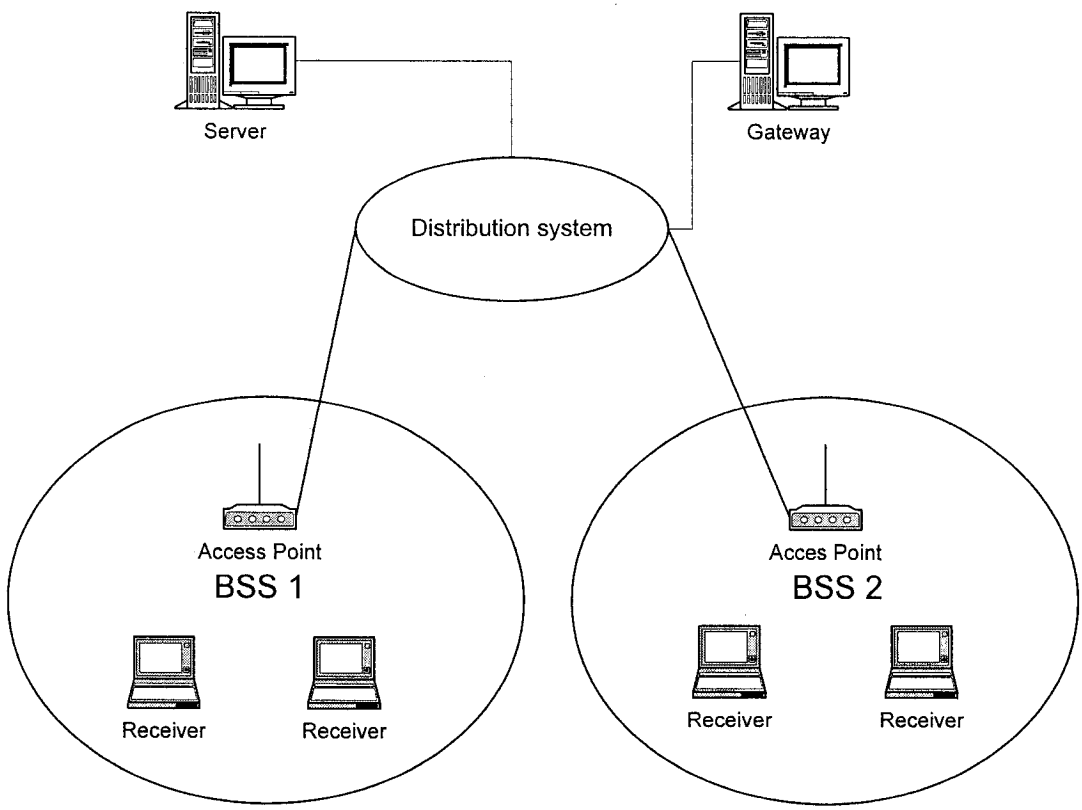


Figure 2.12: Infrastructure Wireless LANs

In an infrastructure integrated LAN-WLAN the WLAN is connected with the regular LAN. And this is the most common environment and widely used. Figure 2.13 illustrates an example of the infrastructure integrated LAN-WLAN.

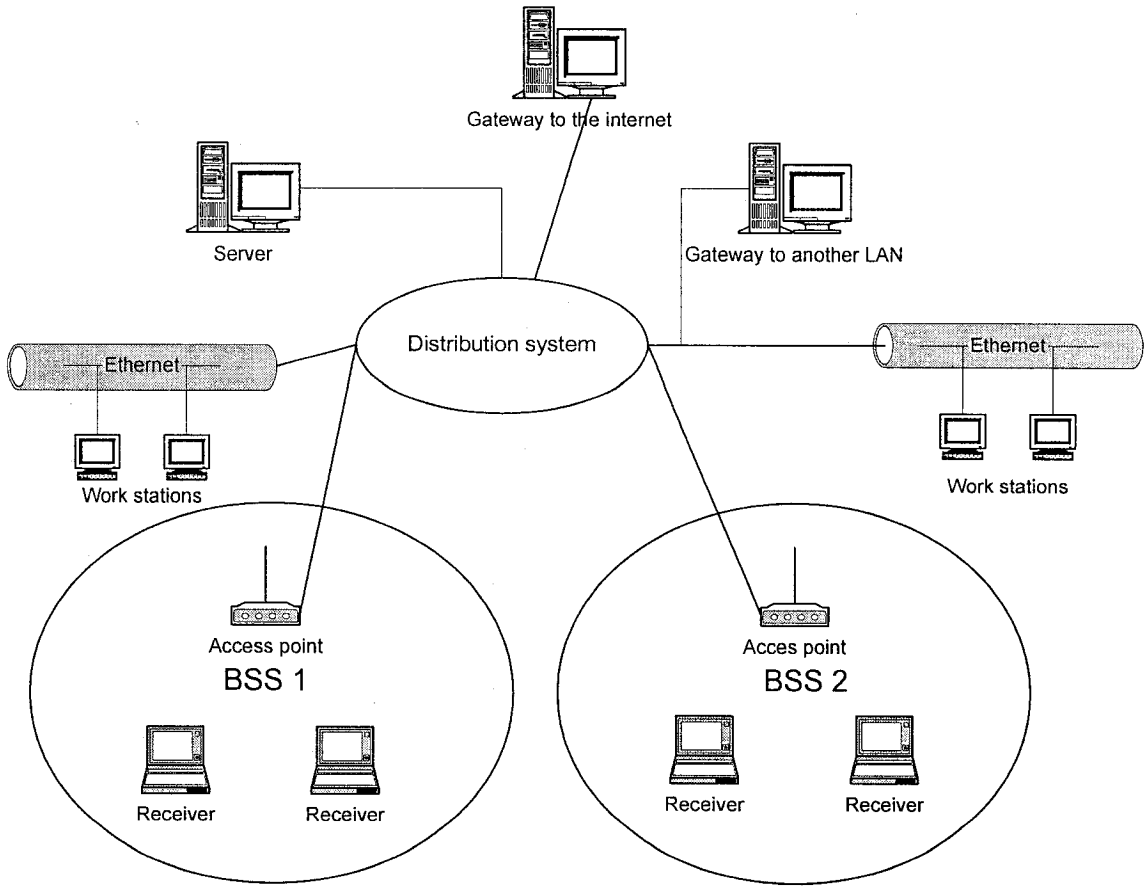


Figure 2.13: Infrastructure Integrated LAN-WLAN

2.6.1.2. Ad Hoc (Peer-to-Peer) Wireless LANs

Ad Hoc WLAN [25] consists of only mobile nodes within range of each other. They build a peer to peer network without the need of any Access Point (AP) and wired backbone.

Ad Hoc WLAN can be formed spontaneously anywhere and be disbanded at any time. Even two stations can make an ad-hoc network.

Wireless communication in ad-hoc is a multi-hop communication. Figure 1.2 gives an example of Ad Hoc WLAN.

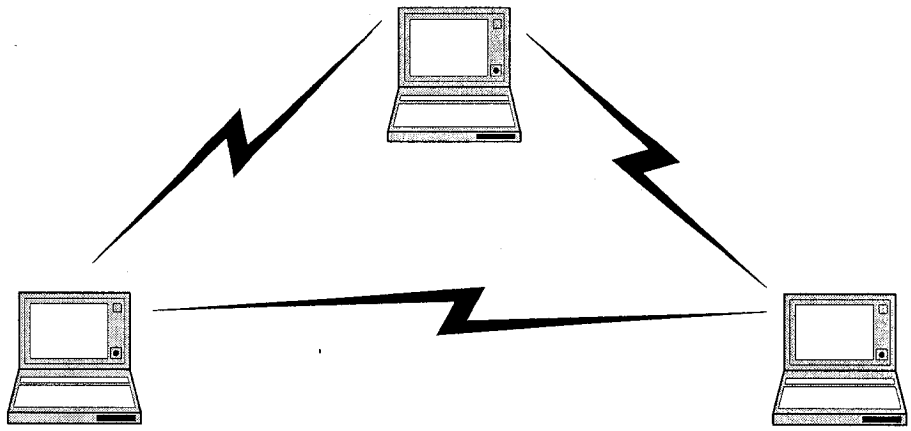


Figure 2.14: Ad Hoc (Peer-to-Peer) Wireless LANs

2.6.2 WLAN Transmission Technology

WLANs categorized as per the transmission techniques are-

Spread Spectrum: This type of LAN uses spread spectrum transmission technology and is the most common type.

Infrared (IR): This is suitable for limited range, especially for a single room. As infrared can not penetrate through opaque walls.

Narrowband: These LANs uses narrowband microwave frequencies.

Carrier Current: This technology uses power lines as a medium for the transport of data.

2.6.2.1 Spread Spectrum

Spread spectrum was invented for use by the military because it uses wideband

signals those are difficult to detect and are jamming proof. Now a days researchers are more interested for applying spread spectrum processes for commercial purposes, especially in Wireless LANs.

Currently, the most popular type of WLANs use spread spectrum techniques. In spread Spectrum systems the signal power is spread over a wider band of frequencies. It is a digital modulation technique that takes a data signal of certain bit rate and modulates it with a signal that has a very large bandwidth. This costs bandwidth but improves signal-to-noise ratio. Spreading process makes the signal less susceptible to different noise than conventional radio modulation techniques [26]. Figure 2.15 illustrates an example of a spread spectrum.

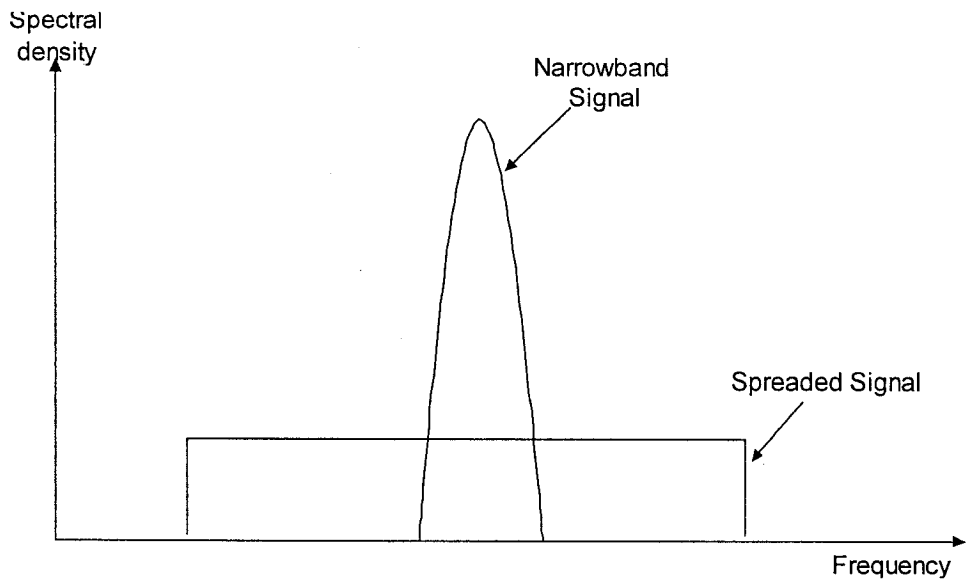


Figure 2.15 Spreading of narrowband signal (Spread spectrum)

2.6.2.1.1 Frequency Hopping Spread Spectrum (FHSS)

In Frequency Hopping Spread Spectrum (FHSS), the data signal is modulated with different frequency bands as the transmission goes on. Figure 2.16 illustrates an example of the spreading technique of a frequency hopping spread spectrum signal.

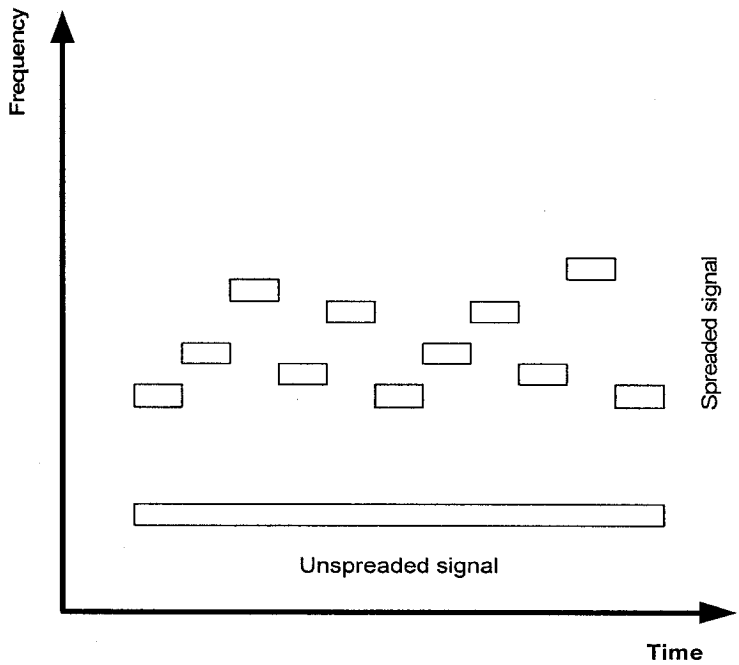


Figure 2.16: Frequency hopping spread spectrum

Channel hopping sequence is not arbitrary. It is determined by the use of a pseudo random sequence. On the other side the receiver can reproduce the identical hopping sequence and thus decode the original signal. Channel switching rate can be thousands of times a second, so the time spent on each channel is very tiny.

If the radio faces interference on a particular frequency then forward error correction can cancel the resulting bit errors. Added, not all frequency channels have interference all the time.

In frequency hopping spread spectrum technique, interfering signal from a narrowband system will affect the spread spectrum signal only. As both are transmitting at the same frequency at the same time. Therefore the average interference will be very low.

So, frequency hopping is the most cost-effective for WLAN as network bandwidth is 2 Mbps or less [27].

Multipath fading through affects narrow frequency bands and thus some of the channels provides very low quality signal. Frequency hopping reduces time spent on each channel and thus quality is not hampered that much.

2.6.2.2 Direct Sequence Spread Spectrum (DSSS)

Direct sequence spread spectrum is another approach to spread spectrum modulation for digital signal transmission over the air interface. In direct sequence spread spectrum, the stream of information to be transmitted is divided into small pieces and each one is allocated a frequency channel across the spectrum. At the point of transmission data signal is combined with a higher data-rate bit sequence that divides the data according to a spreading ratio, this is also known as a chipping code. Redundant chipping code helps the signal to get rid of the interference and also data recovery if the original data is altered by any means. DSSS represents each data 0 and 1 by the symbols -1 and +1 and multiplies every symbol by a binary pattern of +1 and -1s to obtain a digital

signal that varies more frequently and thus occupies a larger bandwidth. [24]. Figure 2.17 illustrates an example of a direct sequence spread spectrum signal.

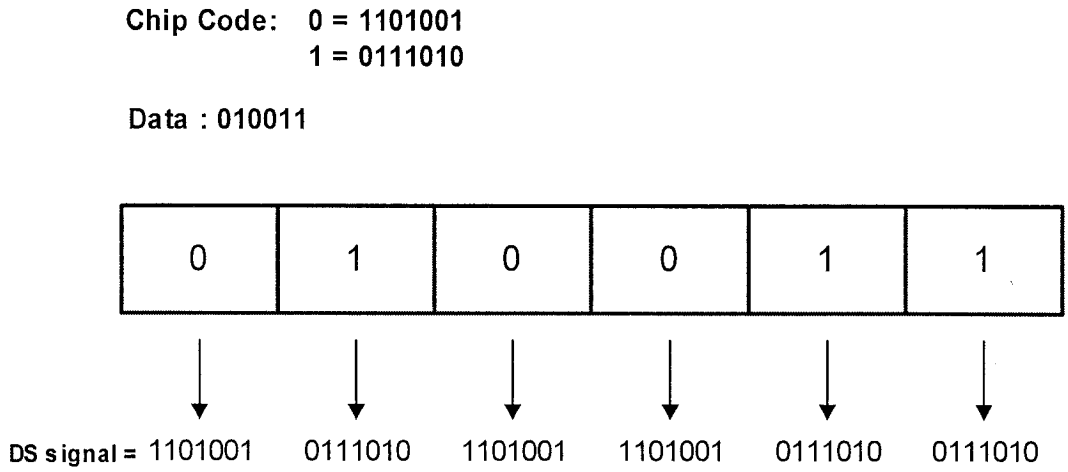


Figure 2.17: Direct Sequence Spread Spectrum (DSSS)

2.6.3 Frequency Bands

WLANs operate in unlicensed bands, popularly known as Industrial, Scientific, and Medical (ISM) bands. WLAN suffers more interference as many of the industrial equipments operate on the same band. Figure 2.18 describes ISM band.

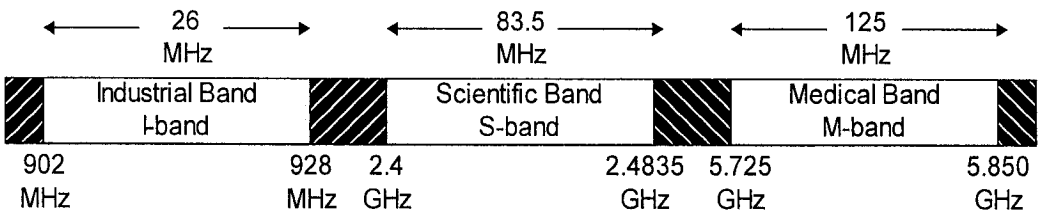


Figure 2.18: ISM band

2.6.4. Medium Access Control

IEEE 802.11 MAC protocol is specified in terms of coordinate functions. These functions determine when a station under a BSS is allowed to transmit and when it will receive PDUs (Protocol data unit) using the wireless interface. Two types of coordinate functions are:

2.6.4.1 Distributed Coordination Function (DCF)

DCF uses Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) protocol. DCF allows for asynchronous data transfer of MAC SDUs using best effort criteria.

In DCF the transmission medium is controlled in a contention mode. So, each station must contend for the channel for each packet transmitted.

When a station has a frame to transmit, it listens to the medium first. If it finds that the medium is idle then it may transmit; otherwise the station must follow a back off algorithm and needs to wait until the current transmission has been completed.

To ensure the smooth functioning of this algorithm, all stations are obliged to remain quiet for a certain minimum period after their transmission has been done. This is called the interframe space (IFS).

Different IFS intervals are described as follows-

Short IFS (SIFS): SIFS is the shortest IFS. It provides the highest priority level by allowing some frames wait up to SIFS period before contending for the channel.

PCF IFS (PIFS): The PIFS is intermediate in duration. PIFS is used under the PCF use to gain access to the medium at the beginning of contention free period.

DCF IFS (DIFS): Stations operating under for transmitting data and management frames. This is the longest IFS [24]. Figure 2.19 shows a time diagram that describes DCF contention.

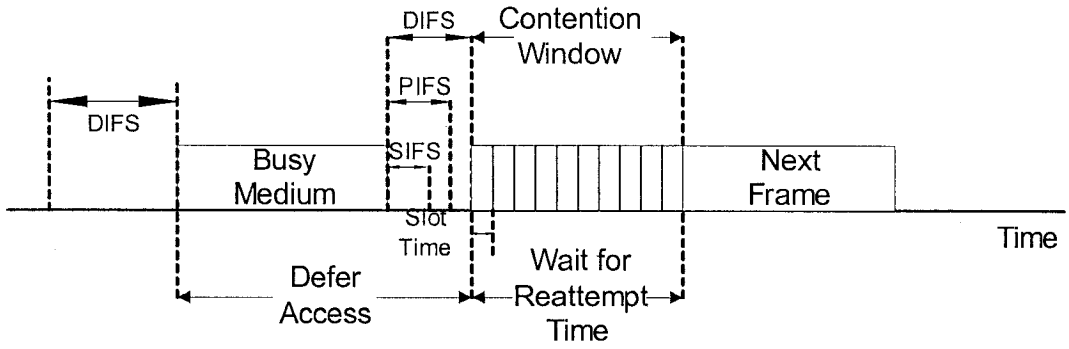


Figure 2.19: Distributed Coordination Function (DCF) [24]

2.6.4.2 Point Coordination Function (PCF)

The PCF is an additional capability that can be used to provide connection-oriented, contention-free services. In PCF, polled stations can transmit without contending for the channel. PCF uses PIFS at the time of issuing polls.

PCF must coexist with the DCF and built on the top of DCF. PCF uses features of DCF.

At the beginning of every CFP repetition interval every station in the BSS updates its Network Allocation Vector (NAV) to the maximum length.

RTS/CTS (Request to Send/Clear to Send) frames are not used by point coordinator or by the CF-aware stations when contention free period is on going [24]. Figure 2.20 describes the CFP repetition interval.

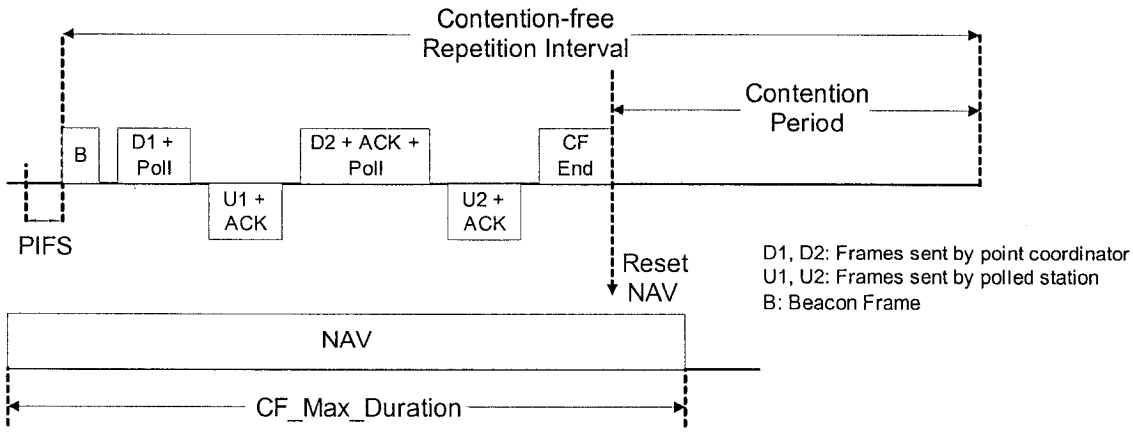


Figure 2.20: Point Coordination Function (PCF) [24]

2.7 Review of Micro Mobility

For the last few years a number of IP micromobility protocols [28] have been proposed, that complement the basic Mobile IP protocol [29] by providing fast and seamless handovers.

IP micromobility protocols are basically for environments where mobile hosts change their point of attachment very frequently. For these environments the basic Mobile IP mechanism faces problems in terms of increased delay and packet loss. Many real-time wireless applications (e.g., voice over IP) will face noticeable degradation of service with the basic Mobile IP for these environments.

Micromobility protocols are based on local movement (e.g., within a domain) of mobile hosts. This reduces delay and packet loss during handoff. Moreover, this eliminates registration between mobile hosts and possibly distant Home agents (HAs), as mobile hosts remain inside their local coverage areas. This reduces signaling in the network due to handoffs [30].

The three most important IP micromobility protocols are-

a. Hierarchical Mobile IP [31].

b. Cellular IP [32].

c. Hawaii [33].

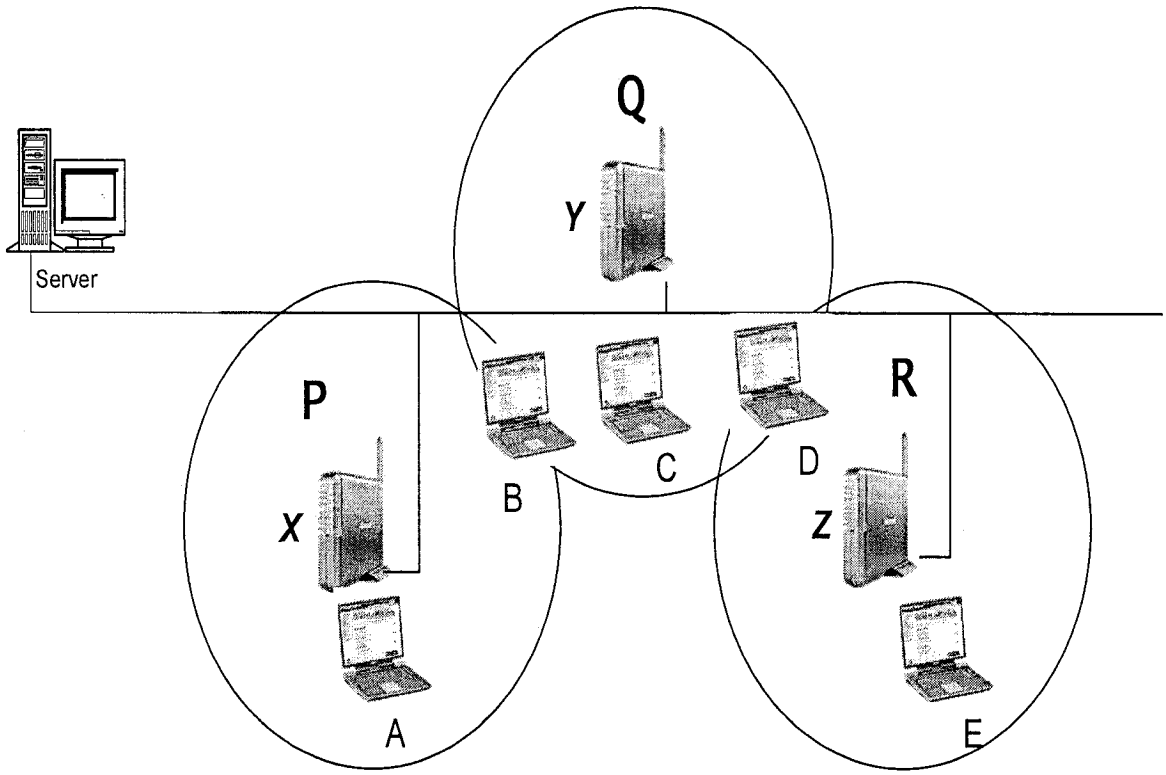


Figure 2.21: IP micromobility

In the figure 2.21, there are 3 APs- X, Y, Z and their corresponding coverage areas are P, Q, and R with radius 100 meter each. Suppose a user wants to move from point A to E. At point A, the user is under the coverage of access point X. He starts moving from point A, at point B handover occurs and he comes under access point Y. At point C, he is under access point Y. At point D, second handover occurs and finally he reaches point E. Where he is under access point Z. Thus the user maintains seamless communication with the network while moving around.

2.7.1 Difference between Classical Mobile IP and Hierarchical Mobile IP

The Hierarchical Mobile IP protocol from Ericsson and Nokia employs a hierarchy in which FAs can locally manage Mobile IP registration.

When using classical Mobile IP, a mobile node registers with its home agent every time it changes the care-of address. When the distance between the visited network and the home network of the mobile node is very large, the signaling delay for these registrations may increase a lot.

In hierarchical mobile IP, mobile station registers locally to the visited domain. Regional registration reduces the number of signaling messages to the home network, and reduces the signaling delay when a mobile node moves from one foreign agent to another, within the same visited domain.

When HA receives a packet addressed to a mobile host located in a foreign network, it tunnels the packet to the paging FA. FA pages the mobile host to reestablish with the current point of attachment.

The idle mobile station remains in idle battery saving mode. This is similar to the concept of paging found in the second-generation cellular systems [30].

However, all these micro mobility protocols are still under intensive research and none of these have been implemented yet.

Chapter 3

Proposed PIM-DM for Closed LAN Multicast

This chapter first presents the inherent PIM-DM problems for LAN and integrated infrastructured LAN-WLAN, and then it shows ways to overcome those problems by introducing different new approaches. Furthermore, the chapter presents the detailed description of the proposed multicast routing protocol and its advantages over the inherent PIM-DM. Finally it describes the simulation details and results of the proposed multicast routing protocol for LAN and integrated infrastructured LAN-WLAN.

3.1 Classical PIM-DM Problems

Some potential problems faced when considering PIM- DM for corporate level multicasting are:

1. The periodic flood and prune nature of PIM dense mode is a problem for networks. As it is a bandwidth hungry procedure. Classical PIM-DM uses the push model and the

traffic is initially flooded to all PIM neighbors and finite life time (S,G) states are created in every router. Branches not needing data are pruned and multicast forwarding states are created. But this pruned finite states times out every 3 minutes and thus it causes a new flood every 3 minutes. However, in order to overcome the bandwidth consumption problem "state-refresh" message has been introduced in PIM-DM V2 by the PIM research group of Internet engineering task force (IETF). This State Refresh feature prevents the pruned states from timing out by p eriodically flooding a c ontrol message down the source-based distribution tree. This control messages reset the timers of prune states and thus prevent prune states from timing out. It is a signaling by control packets, created usually every 60 seconds. This control message overcomes the "massive flood" created by multicast data packets of PIM –DM, which occurs in every 3 minutes.
However, this message creates some overheads as it is periodic in nature and very frequent.

2. If we stop the periodic flooding process, that has some side effects. As without periodic flooding (S,G) -Source tree in multicast routers will expire. And without (S,G) state a new user can not join the existing multicast session.

3. In PIM-DM there should be one timer for every (S,G) in every router. Thus it will cause significant processor load as the number of (S,G) increases.

3.2 Proposed PIM-DM

The following sections describe how our proposed modified PIM –DM overcomes all these problems.

• Routers initially flood multicast traffic over all interfaces, same like the classical PIM-DM. But Infinite life time (S,G) state is created instead of finite life time (S,G) state.

• Branches with no interested members send Prune messages toward the source to prune off the unwanted traffic. These pruned branches never become active (dense-forwarded) except for Join or Graft messages. But in PIM-DM this pruned branches times out every 3 minutes. So, In order to keep the states alive, PIM-DM needs re-flooding.

• Multicast states (S,G) are created by multicast data arrival at different routers and will be deleted only with the arrival of proposed "Multicast session end" message. But in PIM-DM, a (S,G) state will be deleted automatically after 3 minutes if there is no multicast data flow available for the state.

• Topology changes are managed by the Prune, Graft and IGMP join and leave messages.

3.2.1 Multicast Session End Message

(S,G) table is used to forward multicast traffic sent by the source (S) to the group (G). (S,G) state is created by the arrival of (S,G) multicast traffic. We introduced a new message called "Multicast session end" message. There is no multicast session end message available in PIM-DM as PIM-DM is timer controlled and a (S,G) state will be deleted automatically after 3 minutes, if there is no multicast data flow available for the state. In the proposed approach, when the router serving the source will finish forwarding the last packet from the multicast source or there is no (S,G) data from the source for

more than a particular time (Usually 5 minutes) then this router will assume that the source has finished or has been discontinued the multicast session. This router will then flood the proposed "Multicast session end" message for the particular (S,G), through out the network and all those particular (S,G) states in different routers will be deleted. However, users will not get this message as it will end up at the router level. This solves problems 1 and 2 and makes the PIM- DM non periodic in true sense.

3.2.1.1 Advantages of Proposed Multicast Session End Message over the State Refresh Message

1. In PIM-DM version1, there was a massive flood in every 3 minutes. It was overcome by version2's "state re-fresh" message that appears in every 60 seconds and resets the clocks. But in version2, in order to overcome a periodic massive flood, a new periodic signaling has been introduced with the state refresh message. Multicast session end message also introduces a signaling like PIM-DM version2's state refresh. But multicast session end will signal the network only 1 time, when the multicast session is over. But version2's state refresh will create a signaling in every 60 seconds.

So if there is a 60 minute multicast session, PIM- DM version2 with state refresh needs

1 (massive flood at the beginning) + 60 (signaling due to state refresh)

and with multicast session end message, PIM-DM needs-

1 (massive flood at the beginning) + 1 (signaling at the end of session)

So, for longer session duration PIM-DM version2 with state refresh message faces more overhead in terms of the number of signaling compared to the proposed protocol.

2. Again what happens if the number of (S,G) states increases ? As an example, if there are 70 (S,G) states in a network and all the multicast sessions are of 60 minutes of duration or greater. Then for a 60 minutes time period- with state refresh message, a network will face-

{1 (massive flood at the beginning) + 60 (signaling due to state refresh)} X 70 numbers of floodings.

This huge number of signaling will increase the overhead for the network.

But the networks with the proposed multicast session end will face only-

{1 (massive flood at the beginning) + 1 (signaling at the end of session)} x 70 numbers of floodings.

This is much smaller and more tolerable.

So, again with the increase of the number of (S,G) states PIM-DM version2 with state refresh message faces more overhead than the proposed protocol.

So, we see that in version2, the number of control signaling increases and still it is periodic in nature. Although it overcomes the problem of massive flooding in every 3 minutes. While the proposed protocol with multicast session end message is non periodic in true sense.

3. Thirdly, when there are no periodic timers, this will lead to less processor load. A router may be associated with 70-80 different (S,G) states and if there is one timer for every state, definitely it will cause too much processor load.

4. Proposed protocol cleans up the specific (S,G) state immediately with the multicast session end message but PIM-DM is controlled by timers and waits for 3 minutes before

deleting the (S,G) state. And thus the proposed protocol ensures efficient memory utilization.

5. Finally, the proposed protocol with multicast session end is simpler than PIM-DM or PIM-DM with state refresh technique.

3.2.2 Graft Message

Basic graft mechanism of PIM-DM remains unchanged in the proposed protocol. Additionally, in the proposed protocol, Graft message will also be used for mobile users to join the multicast session after the successful handover.

So, in the proposed protocol Graft message is used for the following two cases-

a. When a new member joins a group and there is no (S,G) data on its router.

b. When a mobile user has been handover to a new AP and the router of the AP does not have the desired (S,G) data. Details on this have been described in chapter 4.

3.2.3 Asserts Message

Basic assert mechanism of PIM-DM remains unchanged in the proposed protocol. In addition, in the proposed protocol, if the multicast source is in a multi access LAN then multicast session end message will be generated by the router that has been selected by assert process. The basic assert mechanism is described below.

Duplicate traffic is generated when two routers both forward the same (S,G) multicast traffic to a common multi-access LAN. PIM-DM solves this by assert mechanism. Assert messages are generated by both routers to determine which router should continue

forwarding on the LAN and other router(s) should be pruned. Assert mechanism remains unchanged in our proposed protocol [34].

3.2.4. RPF Check

RPF check mechanism of PIM-DM remains totally unchanged in the proposed protocol. An RPF (Reverse Path Forwarding) check is always performed for IP multicast forwarding. RPF check prevents multicast packet forwarding loop in an efficient way. For every multicast packet the multicast router check the source address on the packet. It then looks for the sender in the unicasting routing table, and determines the interface it would use to send unicast packets to the multicast source. This interface is selected as the RPF interface. This is the only authorized interface to receive multicast packets. The router stores this RPF interface to make (S,G) state entry.

When a packet is received on the RPF verified interface, the packet is copied and forwarded to every outgoing interface listed in the Outgoing interface list (OIL).When a packet is received on a non-RPF interface, it is deleted and a prune message is sent on that interface to stop the stream [16].

3.2.5. Prune Delay

Prune delay mechanism of PIM-DM remains totally unchanged in the proposed protocol. Prune delay ensures one leaf node in an Ethernet to keep continue with the session while other leaf node sends a prune message to the upstream router. When a prune message is heard by the other leaf node, it creates a join message. Whenever an

upstream router gets a prune message from any Ethernet leaf node, it waits for 3 seconds. By this time the upstream router gets a join message from the interested leaf node and the interface remains open [34].

3.2.6 Reliability Issues of the Proposed Protocol

3.2.6.1 Acknowledge Messages

In the proposed protocol some new acknowledging messages has been introduced. There will be acknowledging messages for prune, graft and newly introduced multicast session end messages in the proposed protocol. These acknowledging messages are absent in PIM-DM. These acknowledging messages will increase the reliability of the multicast. It may be possible that the corresponding acknowledge messages are also lost. In such case, the router will generate corresponding prune, graft and multicast session end message n times before getting the corresponding acknowledging message. Even though if any acknowledging message is not found then the router will create an error log entry.

When the multicast session end message is forwarded, the upstream routers have to get an acknowledge back from each of the downstream routers, i.e. every PIM neighbor. This will ensure the reliable signaling of multicast session end message.

3.2.6.2 Remedy of First Hop Router Failure and Infinite States

A very unusual but potential problem may occur only in the proposed protocol, when the first hop router that is serving the multicast source fails before the multicast

session ends. Thus, the router is not getting any opportunity to transmit the multicast session end message. This will cause the particular (S,G) state to remain in the router memory for infinite time. This problem can be overcome as follows-

Whenever a new (S,G) state is created in the router, the state table will make an entry for the state creation time. Once in a week or a month a control message may be generated from the administrator manually or automatically which will check the available (S,G) states in different routers and terminate the (S,G) states that are 1 or 2 days older considering those as junk. Various parameters of this message will be configurable. Using this mechanism any kind of unnecessary (S,G) states can be removed.

3.2.7 Corporate Multicast Confidentiality

The proposed protocol will use Time to live (TTL) on multicast routers interfaces to limit the forwarding of multicast packets. This can be used to set up multicast boundaries to prevent unwanted multicast traffic from entering or leaving the corporate network and thus it enhances multicast confidentiality and security.

TTL Threshold Check

1) Whenever a packet comes to the router through any interface, the TTL value is decremented by one.

If <= Zero, it will be dropped.

2) Whenever a multicast packet is to be forwarded out an interface with a non-zero TTL Threshold; then its TTL is checked with the TTL Threshold. If the TTL of the packet is < the specified threshold, it will not be forwarded.

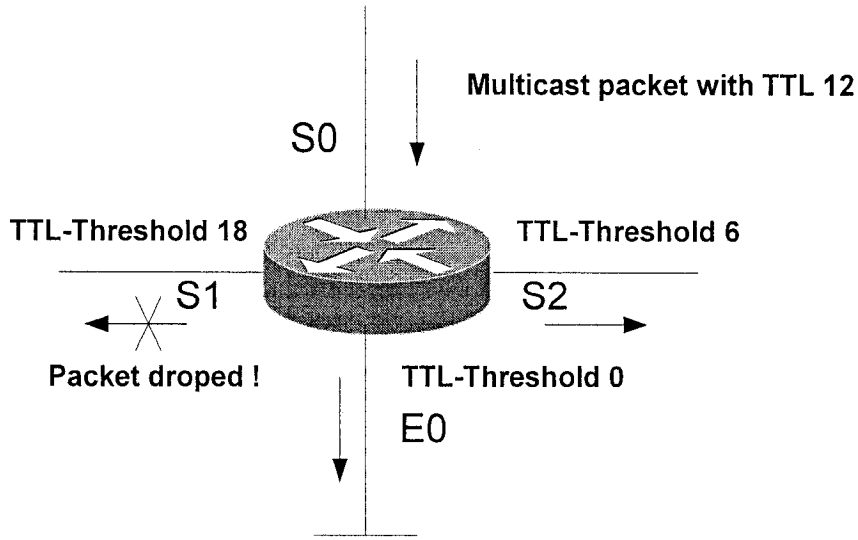


Figure 3.1: TTL threshold [4]

In the Figure 3.1, the interfaces have the following TTL -Thresholds:

S1 = 18

S2= 6

E0= 0

A multicast packet has been received on interface S0 with a TTL of 12. The TTL is decremented to 11 by the router. The outgoing interface list for the Group has interfaces S1, S2 and E0.

The TTL-Threshold check is performed on each outgoing interface as follows:

S1: TTL (11) < TTL -Threshold (18). So the packet is dropped.

S2: TTL (11) > TTL -Threshold (6). So the packet will be forwarded.

E0: TTL (11) > TTL -Threshold (0). So the packet will be forwarded.

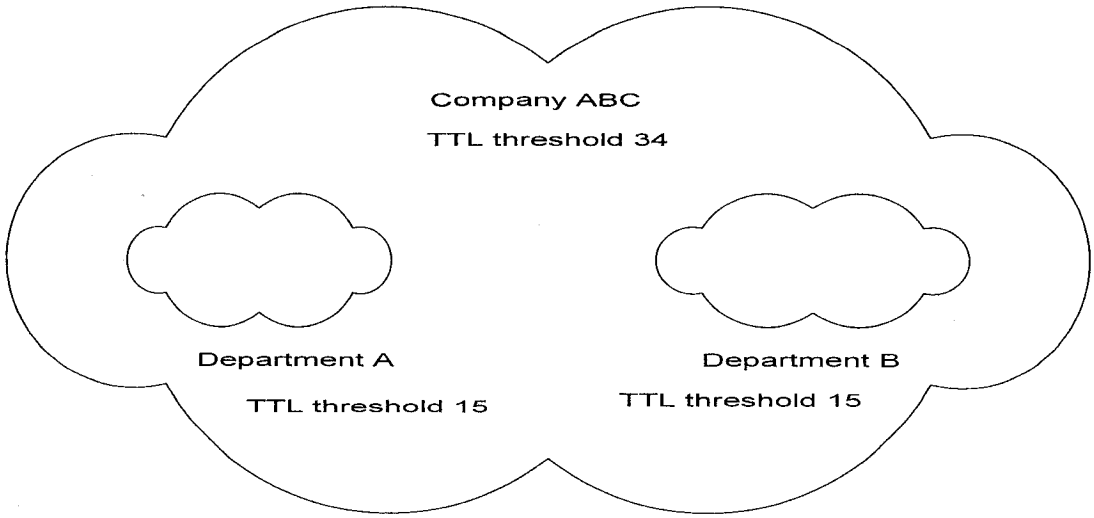


Figure 3.2: Corporate multicast confidentiality [4]

In the Figure 3.2, departments A and B can prevent their own departmental multicast traffic from leaving their network by using packets of TTL 14.

Company ABC can secure its private multicast traffic from leaving its own network to internet or other networks by using a TTL of 33. [4]

3.2.8 Packet Header

Each packet includes multicast source and group address. The packet header contains the control information. Packet header format is shown in Figure 3.3.

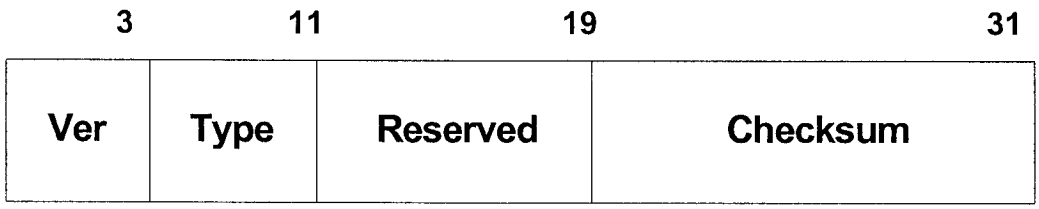


Figure 3.3: Multicast packet header format

Ver:
Version = 1
Type:
0 = Hello
1= Register (PIM-SM only)
2= Register stop (PIM-SM only)
3 =Join/Prune
5 = Assert
6 = Graft
7 =Multicast session end
8 = Graft-Acknowledge
9 = Prune Acknowledge
10=Multicast session end acknowledge

3.3 Simulation Description of the Proposed Protocol

3.3.1 Input Traffic Load and Loss Model:

The source input traffic of multicast session is a Bernoulli process that follows the uniform distribution between (0,1). A uniformly distributed random function generates random number output for every iteration. If the random number is less than the given traffic load of the source then the function return a value of 1 and thus indicates that the source has generated a packet at that iteration; otherwise no packet is generated in that iteration. As an example if the traffic load of a source is .8 and the generated random number at certain iteration is .65, then the source will generate a packet at this iteration.

Buffer overflow and bad link state at intermediate routers can generate packet loss. In the simulation we consider both the effects. The packet loss due to buffer overflow is considered as a dependent (i.e. program output) and the link loss is assumed to be independent (i.e. program input). The packet loss due to bad link is dependent on the uniform distribution between (0,1) and the loss rate of the link. Before a packet passes a

link, we call a uniform distribution function between (0,1) to generate a uniformly distributed random number. If the random number is less than the given input loss rate of the link then loss happens on this link for the iteration and the packet is discarded; otherwise the packet will not be lost on the link at this iteration.

3.3.2 Assumptions of the Simulation

In this simulation, we assume the following points :

- All data packets have equal size.
- Packet losses on links are independent and follow uniform distribution .
- Best effort packet forwarding has been implemented.
- Acknowledge is considered only for control messages like- Graft, Prune and multicast session end.

3.3.3 Confidence Interval

Confidence interval was considered for our simulation to maintain the integrity of the simulation. We ran all points of the simulations for a large number of times. Such that the error between the average of sample results obtained and the theoretical average which correspond to infinite number of runs will not exceed 5% with a level of confidence 95%.

3.3.4 Performance Criterions

We changed the packet generation probability (ρ) and packet loss rate (*l*) and observed the results regarding- End to end delay, Buffer overflow and Delay jitter properties of PIM-DM, PIM-DM V2 (With state refresh) and the proposed protocol. These criterions are described below.

3.3.4.1 Average and Variance of Forwarding Buffer Overflow

In every router, each queue length has a maximum limit because every output port has a finite buffer size. If the packet arrival rate and queue up rate exceeds the rate at which packets are transmitted out of the buffer then the queue size grows to its limit and packets will be lost. This is called Buffer overflow.

In the simulation, we set counters within the routers to count their corresponding buffer overflows.

The average of the forwarding buffer overflow is calculated by dividing the sum of these overflows by the total iterations and by the sum of the number of the output ports of all routers. We used the following formulas to calculate the average forwarding buffer overflow (AFBO) and variance of buffer overflow (VFBO).

$$AFBO = \frac{\sum_{i=1}^{N}\sum_{j=1}^{R}\sum_{k=1}^{p(j)} overflow(i,j,k)}{N * \sum_{j=1}^{R} p(j)} \qquad (4.1)$$

$$VFBO = \frac{\sum_{i=1}^{N}\sum_{j=1}^{R}\sum_{k=1}^{p(j)}[overflow(i,j,k) - AFBO]^2}{[N * \sum_{j=1}^{R} p(j)] - 1} \quad (4.2)$$

Where Overflow (i,j,k) =1, if the buffer at output port k of router j at iteration i overflows. Otherwise, 0. P(j) is the total number of output ports of router j, N is the number of iteration, and R is the number of routers.

3.3.4.2 Average and variance of the End to End delay

In this simulation we considered the End to end delay as the total time required for a successful delivery of a packet from the source to the final destination. It includes different queuing, processing and propagation delays. The average and variance of end to end delay can be calculated as follows.

Method 1: Average end to end delay over all receivers

$$AEED = \frac{\sum_{i=1}^{R}\left[\frac{\sum_{i=1}^{Pac(i)} TL_{ij} - TF_{ij}}{Pac(i)}\right]}{R} \quad (4.3)$$

$$VEED = \frac{\sum_{i=1}^{R} \left[\frac{\sum_{i=1}^{Pac(i)} TL_{ij} - TF_{ij}}{Pac(i)} - AED \right]^2}{R-1} \quad (4.4)$$

Here AEED is the average end to end delay, VEED is the variance of end to end delay. R is the total number of receivers of all sessions, $Pac(i)$ is the number of packets received by the receiver i in the whole simulation time, TL_{ij} is the end iteration of packet j of receiver i and TF_{ij} is the starting iteration of packet j of receiver i.

Method 2: Average end to end delay over all sessions

$$AEED = \frac{\sum_{i=1}^{S} \left[\frac{\sum_{j=1}^{Rec(i)} \sum_{k=1}^{Pac(i)} TL_{ijk} - TF_{ijk}}{\sum_{j=1}^{Rec(i)} Pac(j)} \right]}{S} \quad (4.5)$$

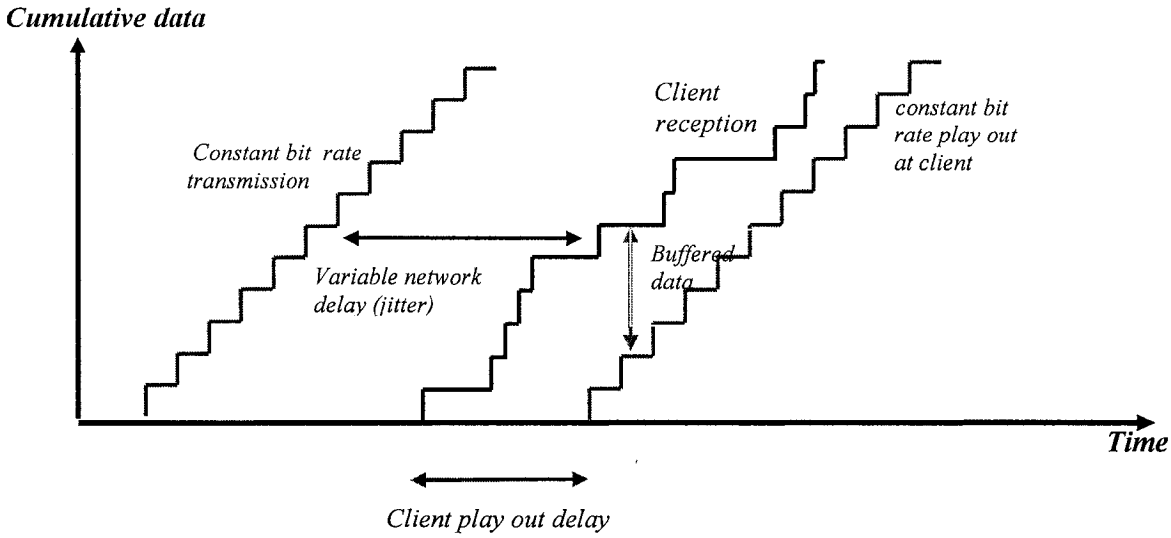
$$VEED = \frac{\sum_{i=1}^{S} \left[\frac{\sum_{j=1}^{Rec(i)} \sum_{k=1}^{Pac(i)} TL_{ijk} - TF_{ijk}}{\sum_{j=1}^{Rec(i)} Pac(j)} - AEED \right]^2}{S-1} \quad (4.6)$$

Where AEED is the average end to end delay, VEED is the variance of end to end delay, S is the total number of sessions, Rec(i) is the number of receivers of session i, Pac(j) is

the number of packets of receiver j, TL_{ijk} is the end iteration of packet k of receiver j of session i, and TF_{ikj} is the starting iteration of packet k of receiver j of session i.

3.3.4.3 Average and Variance of Delay Jitter

Jitter is the variation in delay over time. This is very important criteria especially for real time communication like VoIP. If the delay of transmissions varies too widely in a VoIP call, the call quality is greatly degraded. Figure 3.4 describes delay jitter and its effects.



Consider the end-to-end delays of two consecutive packets. The difference can be more or less than 25 milliseconds and thus creating delay jitter. Too much jitter can impair the conversation or transmission qualities.

Figure 3.4: Delay jitter and its effect [35]

We calculated the average and variance of delay jitter exactly in the same way as we calculated average and variance of buffer overflow in the section 3.3.4.1.

3.3.5 Simulation Network Model

In the figure 3.5, the simulation network is shown where we have an infrastructure integrated LAN-WLAN with both fixed and mobile users. We have 5 wireless routers (AP) and 5 general routers. Different kinds of messages have also been shown. The network of the figure is also an example of typical small scale deployment suitable for the proposed PIM-DM.

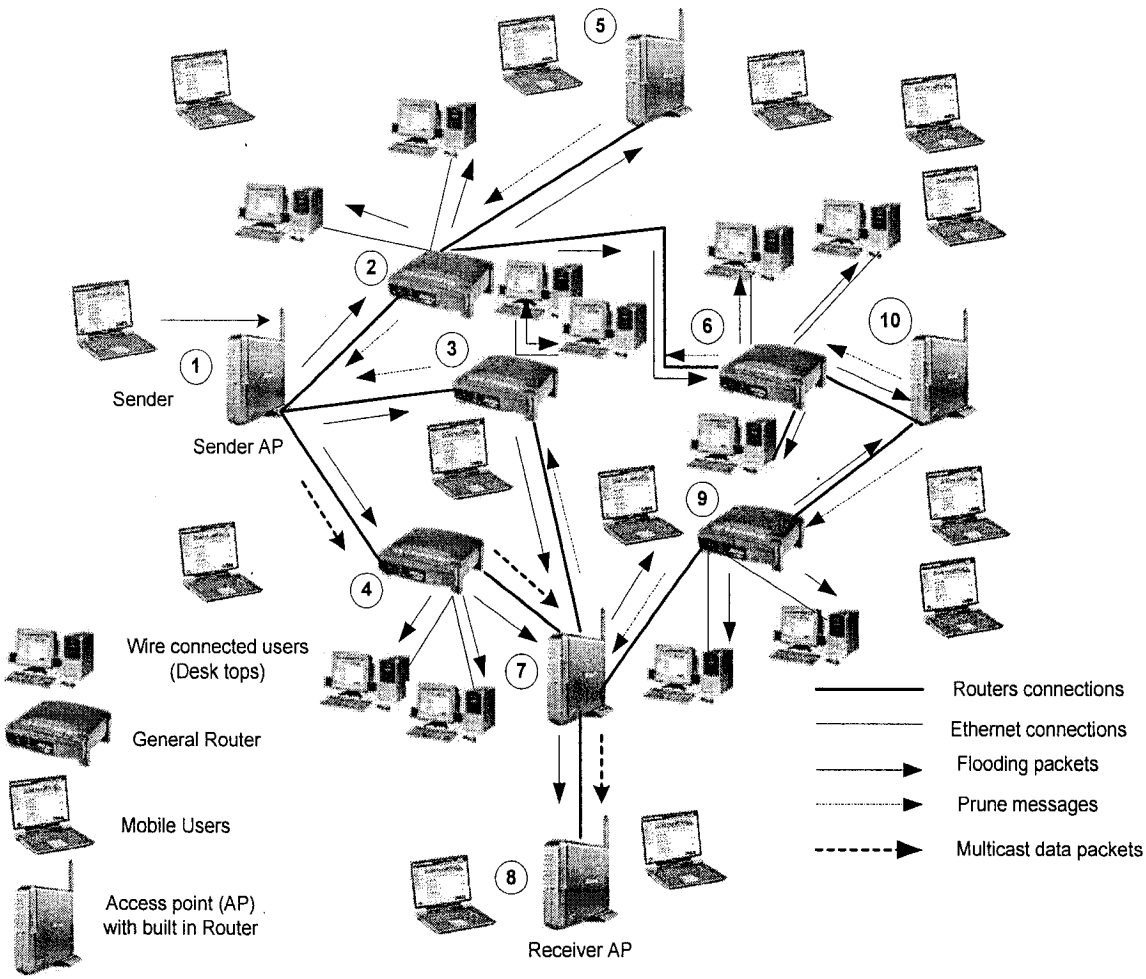


Figure 3.5: Simulation network model

3.3.5.1 Multicast Tree Structure of the Simulation Network Model

In the figure below the tree structure of the simulation network model has been shown. However, the dotted connections between point 3, 7 and 9, 10 create loops in the network. These loops can generate duplicate packets for routers 7 and 9. This problem is overcome by the RPF check mechanism mentioned in the section 3.2.4.

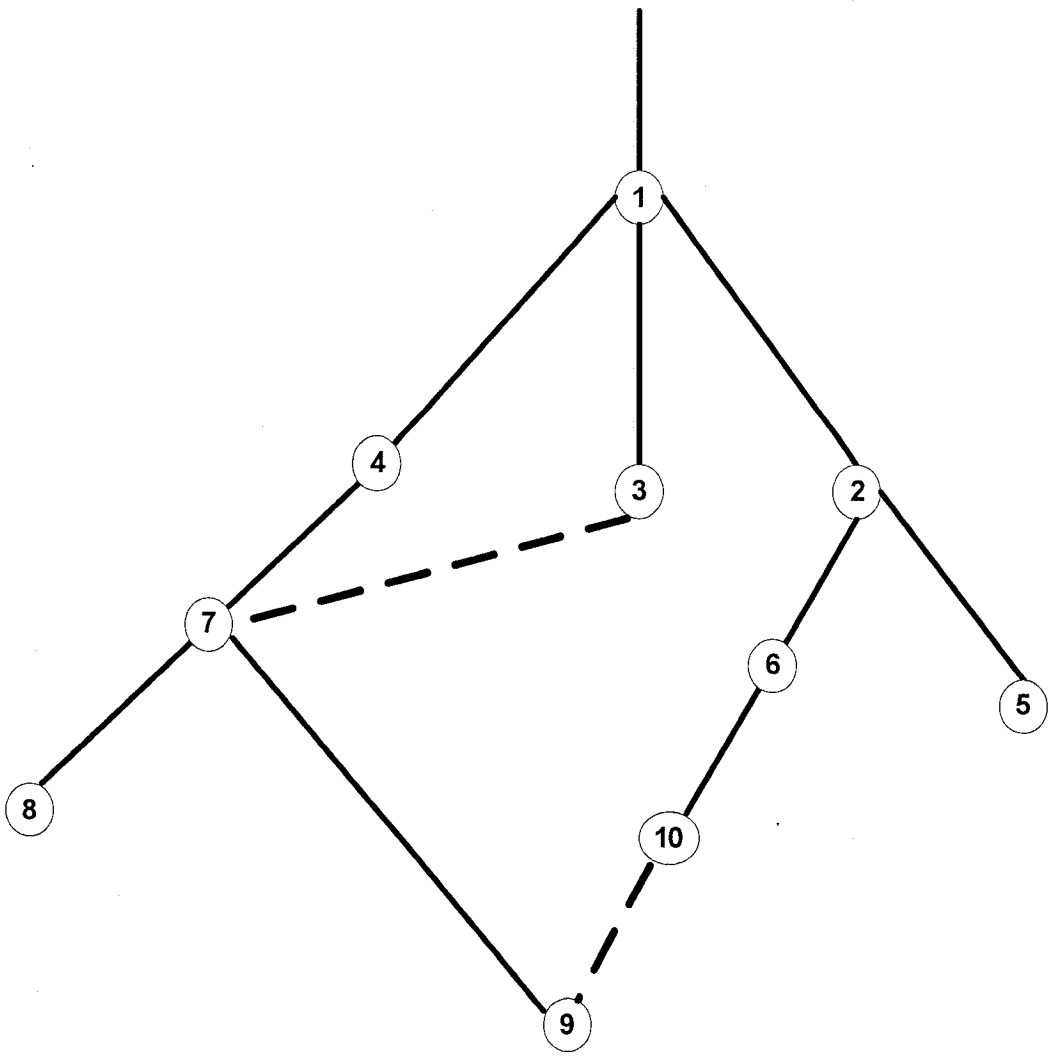


Fig 3.6: Multicast tree diagram of the network model

3.3.6 Input Parameters

In this simulation we considered some network parameters as fixed parameters. However there are some paramenters which were varied to evaluate the performance under different conditions.

3.3.6.1 Constant Parameters

- **Sessions :** We took 5 sessions.
- **Nodes:** Number of multicast routers is10.
- **Sources:** Number of sources is 1.
- **Maximum iterations:** Maximum running time of this simulation is 7000 iterations.

3.3.6.2 Variable Input Parameters

- **Input traffic load**

Input traffic load of each session indicates the number and the frequency of data packets which will be generated.

- **Loss rate**

Loss rate denotes the random loss probability of packet at each link.

3.3.6.3 Output Parameters

The output parameters are number of buffer overflow, end to end delay and number of delay jitter.

3.3.7 Simulation Environment

The simulation program was built in Microsoft Visual studio.net environment. An add-in utility - Softwire V 4.3 was used in parallel with the Basic language codes. This tool gives an easy way to interconnect processes and to maintain inter-process communications. As we considered every multicast router as a different process in the simulation program.

3.3.8 Flowcharts of Processes

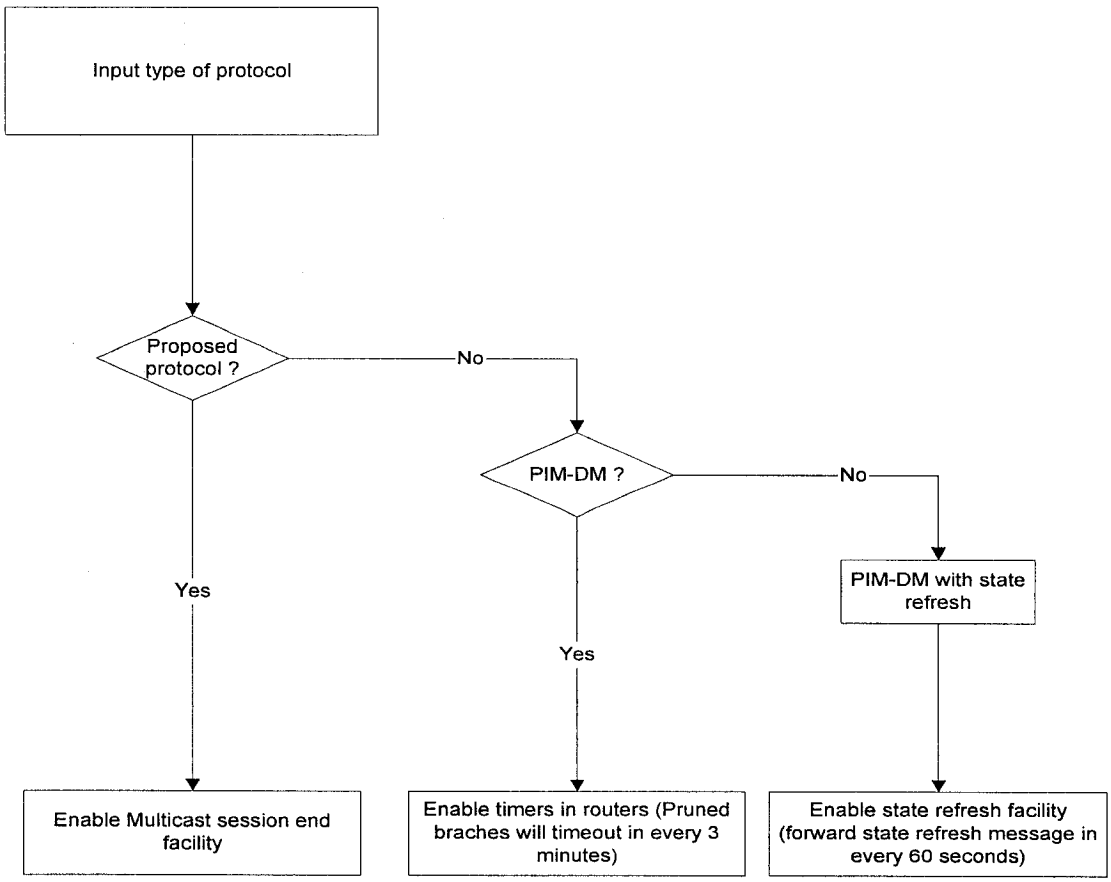


Figure 3.7: Protocol selection

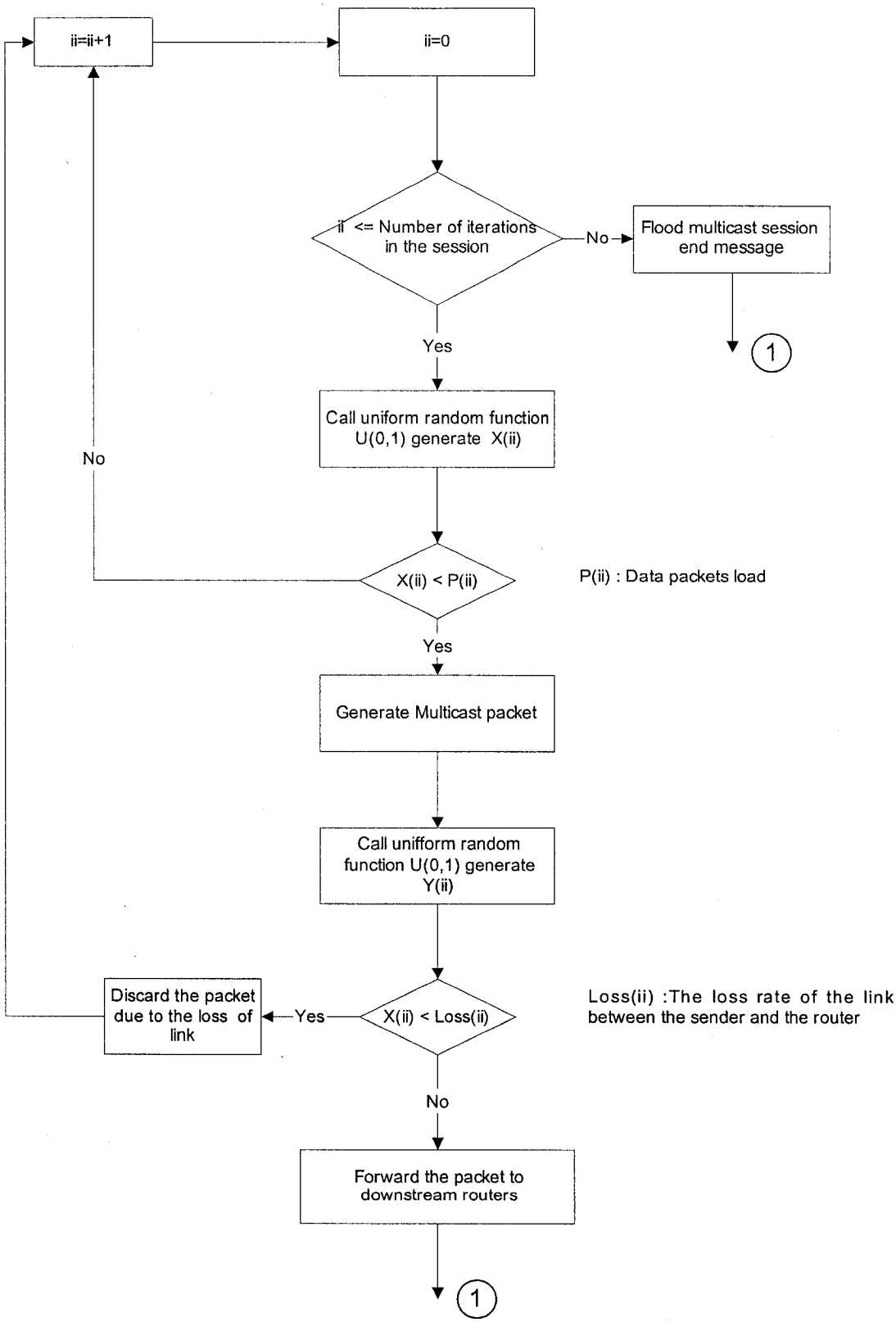


Figure 3.8: Sender process

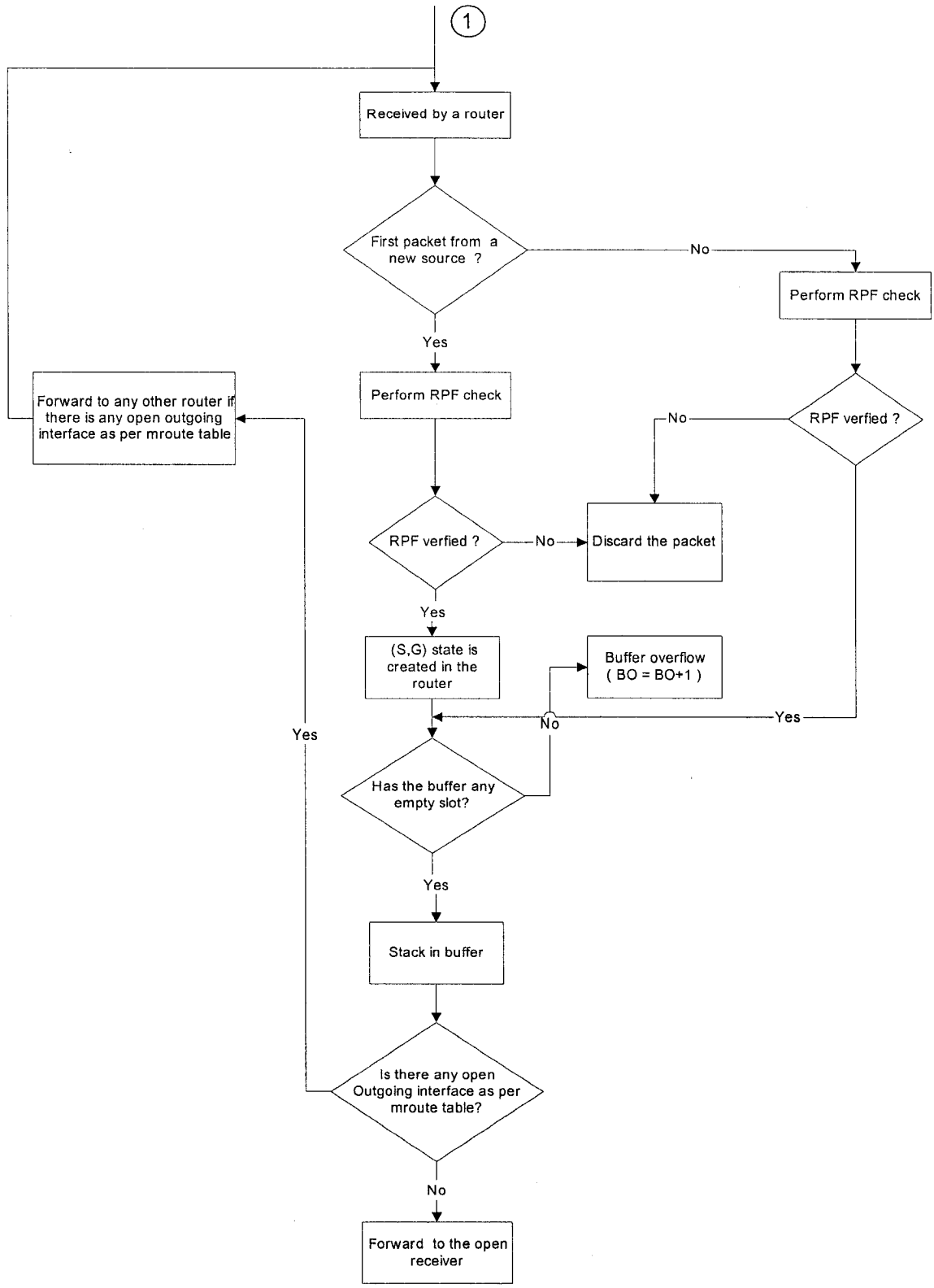


Figure 3.9: Forwarding and receiving process

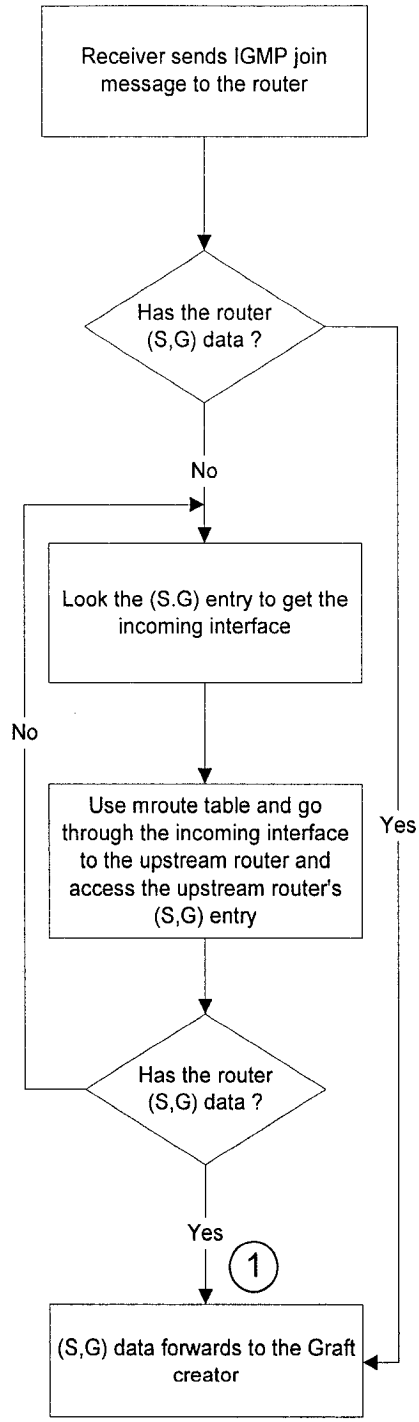


Fig 3.10: Graft process

3.3.8.1 Protocol Selection Process

Figure 3.7 describes the protocol selection process. In the protocol selection part, the program takes input from the user on what protocol to be used for the simulation on the network model. In the simulation we will compare PIM-DM, PIM-DM with state refresh and the newly proposed protocol.

If the input is proposed protocol then the program will enable multicast session end mechanism.

If the input is PIM-DM then timers will be enabled in the routers and thus pruned branches will be timed out in every 3 minutes.

If the input is PIM-DM with state refresh then PIM-DM mechanism will be there, in addition state refresh message will be enabled which will be forwarded in every 60 seconds.

3.3.8.2 Sender Process

Figure 3.8 describes the sender process. In sender part the primary looping starts. After every iteration the loop checks for the maximum number of input iterations. If the iteration number reaches the maximum number of iterations, the loop terminates by creating multicast session end message. Otherwise it calls a uniform random number generator to get a uniformly distributed random number between (0,1). If the generated random number is smaller than the given traffic load then no packet will be generated otherwise a multicast packet will be generated.

As the packet forwards, again the program will call uniform random number generator to get a uniformly distributed random number between (0,1). If the generated number is

smaller than a given loss rate then the packet will be forwarded through that link otherwise the packet will be discarded.

3.3.8.3 Forwarding and Receiving Process

Figure 3.9 describes the protocol selection process. As soon as the packet is received by a router, it checks if the packet is from a new source. If yes, then RPF check is performed and if it the packet pass the RPF check then (S,G) state table entry is created. And the packet is forwarded to the buffer. If the packet is not RPF verified then the packet will be discarded.

If the packet is not from a new source then also RPF check will be performed. If the packet fails the RPF check then it will be discarded. Otherwise it will be forwarded to the buffer without creating any new state table entry.

If the buffer has any empty slot to take the multicast packet then it will be stacked in the buffer. Otherwise, buffer overflow will occur.

Finally, the multicast packets will be forwarded through the outgoing interfaces as per corresponding OIL list (outgoing interface list).

3.3.8.4 Graft Process

Figure 3.10 describes the Graft process. Receiver will send IGMP join message to the router. If the router has the desired (S,G) data then (S,G) data will be forwarded to the Graft creator.

Otherwise, it will look the (S,G) entry to get the incoming interface. Then it will use the particular incoming interface to reach the upstream router, in search of the desired data.

Similar procedure will go on until the Graft message gets the desired data.

3.3.9 Analysis of Simulation Results

In this part, results of the simulation have been shown in graphical format. Where the proposed protocol has been compared with PIM-DM and PIM-DM with state refresh. However, Figure 3.11 to 3.14 are obtained directly from the protocol definitions without any simulation.

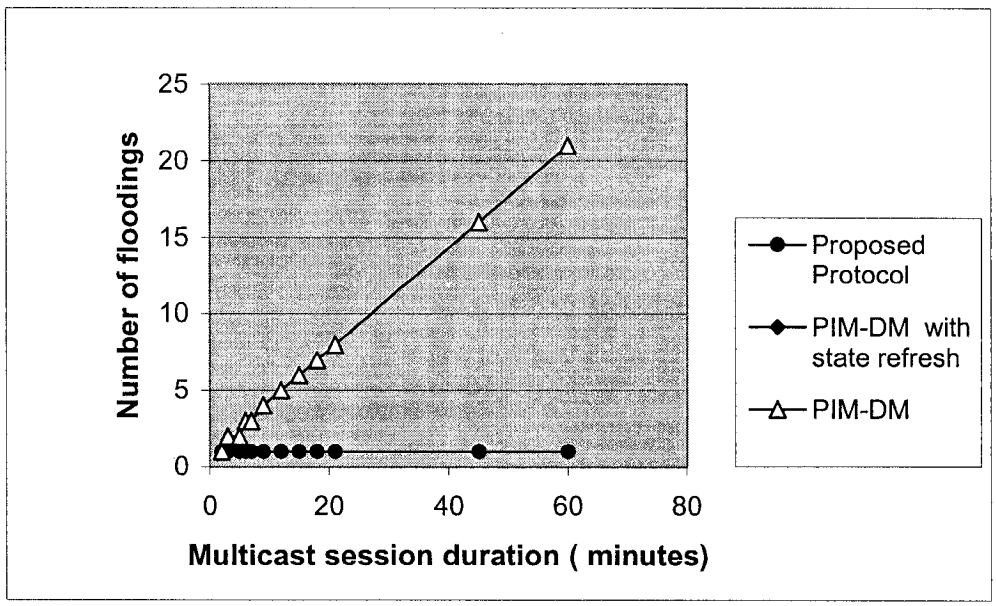


Figure 3.11: Number of massive floodings Vs Multicast session duration

Regarding Figure 3.11 - Pruned states in PIM dense mode times out approximately in every 3 minutes and the entire network is re flooded with multicast packets. So, with the increase of session duration, number of massive floodings increases in PIM-DM.

But both PIM-DM with state refresh and PIM-DM with multicast session end need 1 massive flood irrespective of session duration. They overlapped each other in Figure 3.11.

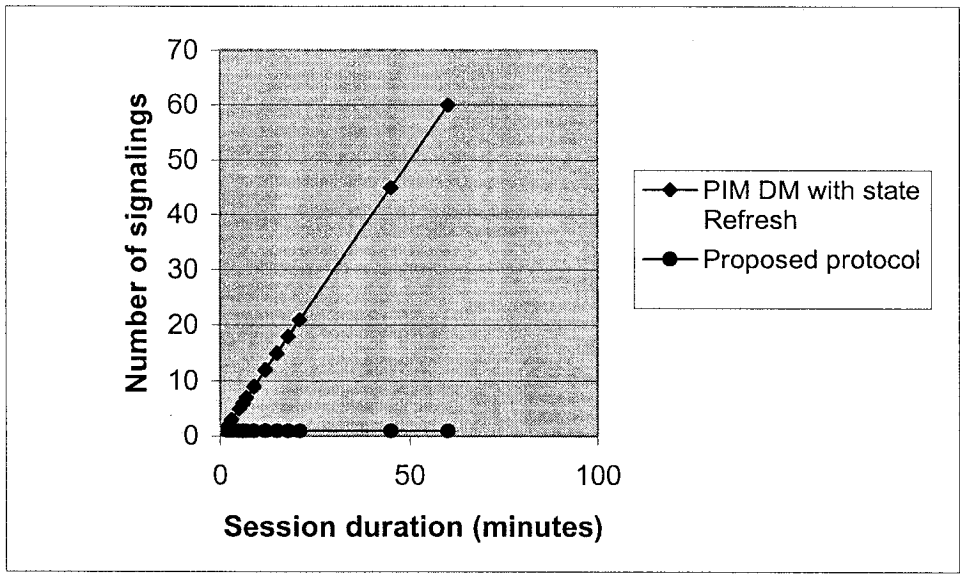


Figure 3.12: Number of signaling Vs Session duration

In Figure 3.12, we see that with the increase of session duration, the number of signaling increases for PIM-DM with state refresh. But PIM-DM with multicast session end needs 1 signaling, irrespective of session duration. And thus saving band-width.

Regarding Figure 3.13 - Proposed protocol cleans up the (S,G) states immediately with the multicast session end message but PIM-DM is controlled by timers and waits for 3 minutes before deleting the (S,G) states. And thus the proposed protocol is memory efficient compared to PIM-DM.

Regarding Figure 3.14 - the Proposed protocol is timer free, while PIM-DM is timer oriented and with the increase of (S,G) states in the router, the number of timers increases in the router. This causes extra processor load.

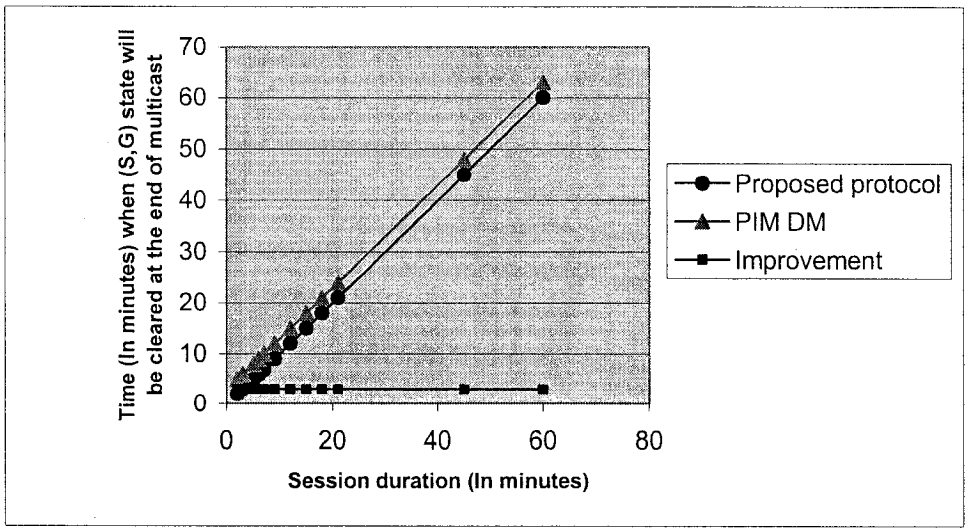


Figure 3.13: The time when (S, G) state will be cleared at the end of multicast session Vs Session duration.

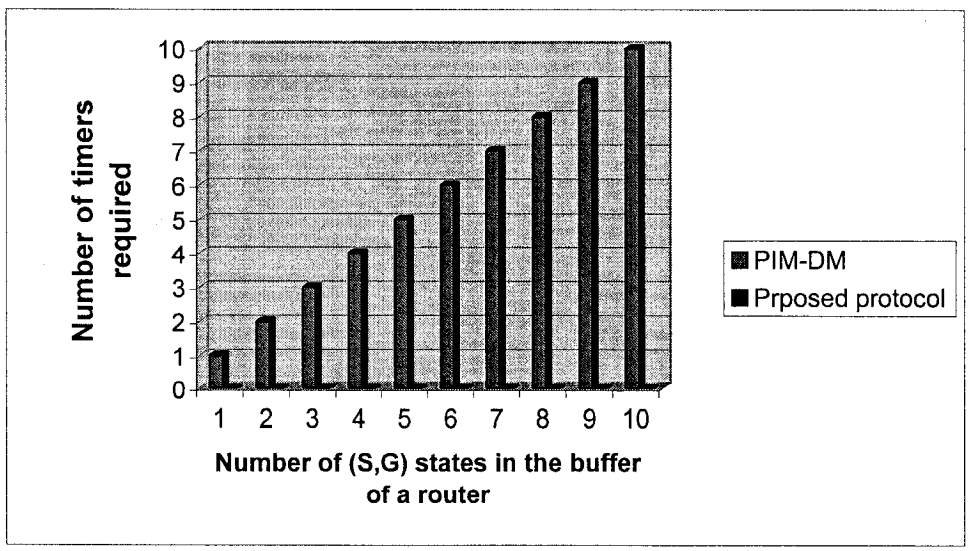


Figure 3.14: Number of (S,G) states in the buffer of a router Vs number of timers Required

3.3.9.1 Buffer Overflow

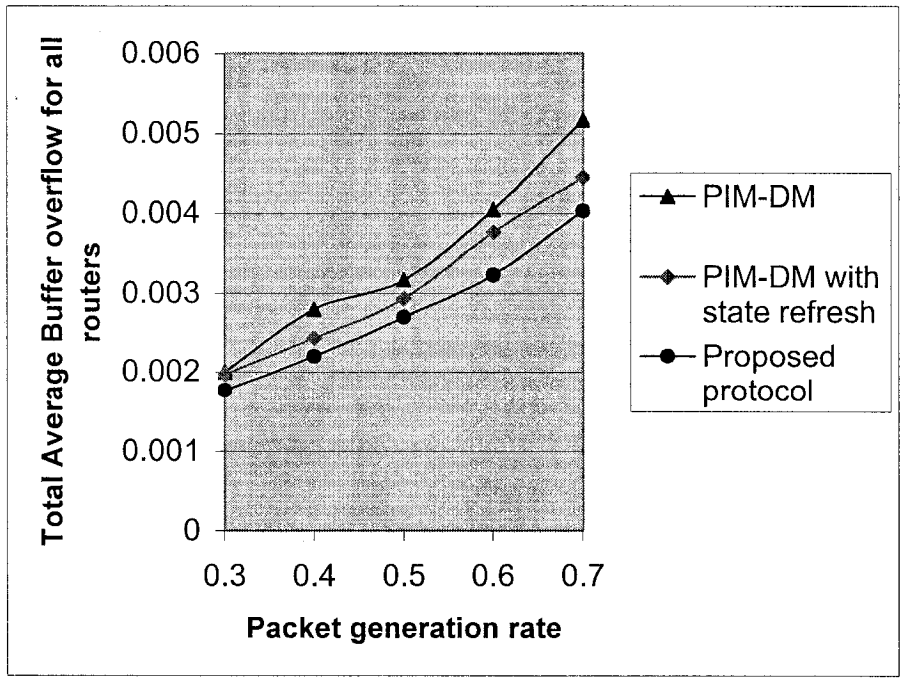


Figure 3.15: Total average Buffer overflow for all routers Vs Packet generation rate

In Figure 3.15, we see that with the increase of packet generation rate, total average buffer overflow increases for all those protocols. The concept of packet generation rate and buffer overflow for this simulation has been described in the section 3.3.1. Unit of buffer overflow is the number of buffer overflows. However, the proposed protocol always exhibits less buffer overflow than those of PIM-DM and PIM-DM with state refresh. Due to the periodic flooding, PIM-DM faces more buffer overflow.

In Figure 3.16, we see that the total average buffer overflow variance for all routers is always less for our proposed protocol. It is because of its non periodic nature. Periodic flooding increases the number of packets in the network and thus variance goes higher.

In Figure 3.17, we see that for any router, the average buffer overflow is higher for PIM-DM, relatively less for the PIM-DM with state refresh and least for the proposed protocol. This is because of the periodic flooding effect.

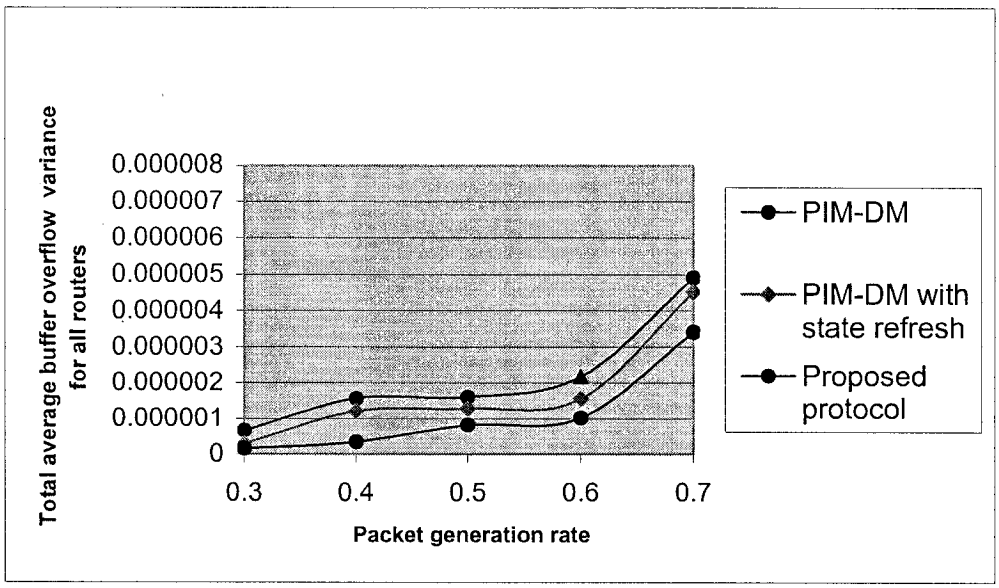


Figure 3.16: Total average buffer overflow variance for all routers Vs Packet generation rate

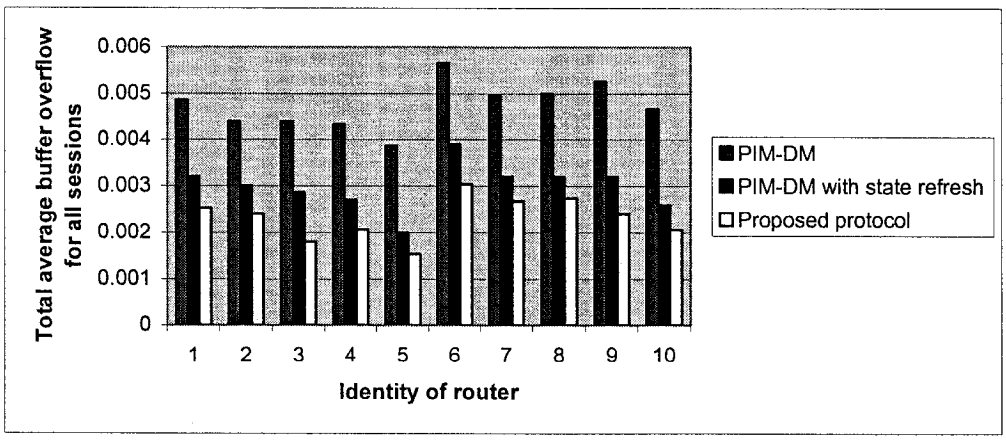


Figure 3.17: Total average buffer overflow for all sessions Vs Identity of router

3.3.9.2 End to End delay

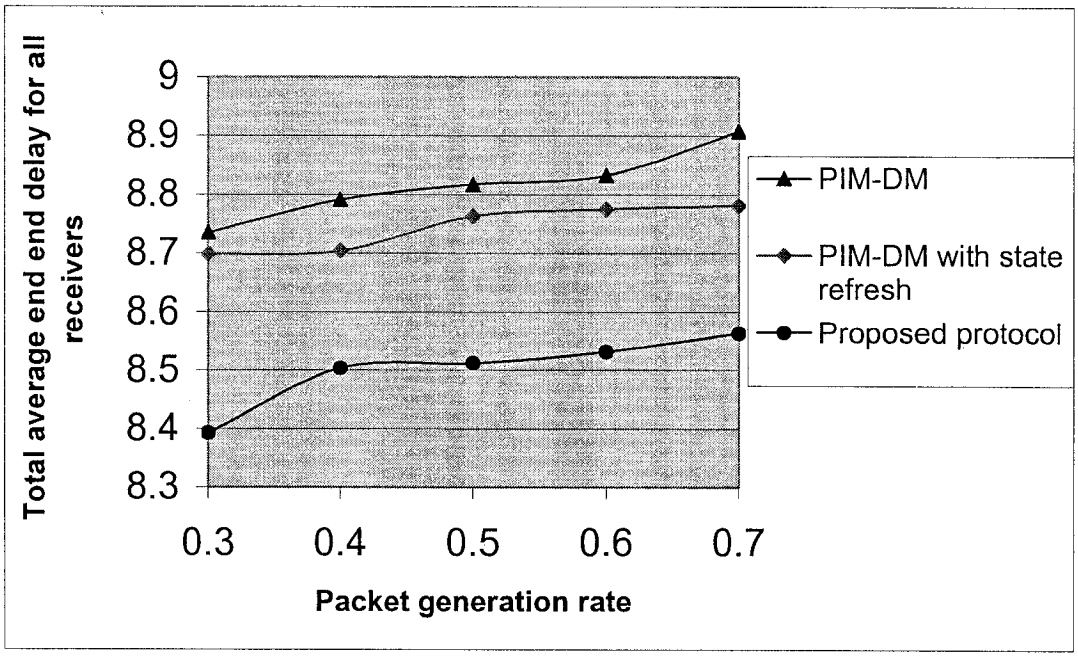


Figure 3.18: Total average end to end delay for all routers Vs Packet generation rate

In Figure 3.18 and 3.19, the packet generation rate has been varied. We see that multicast packets face less average and variance of the end to end delay with the proposed protocol. Because of the absence of periodic flooding in the proposed protocol, buffers have less queuing and fewer overflows so the average end to end delay decreases.

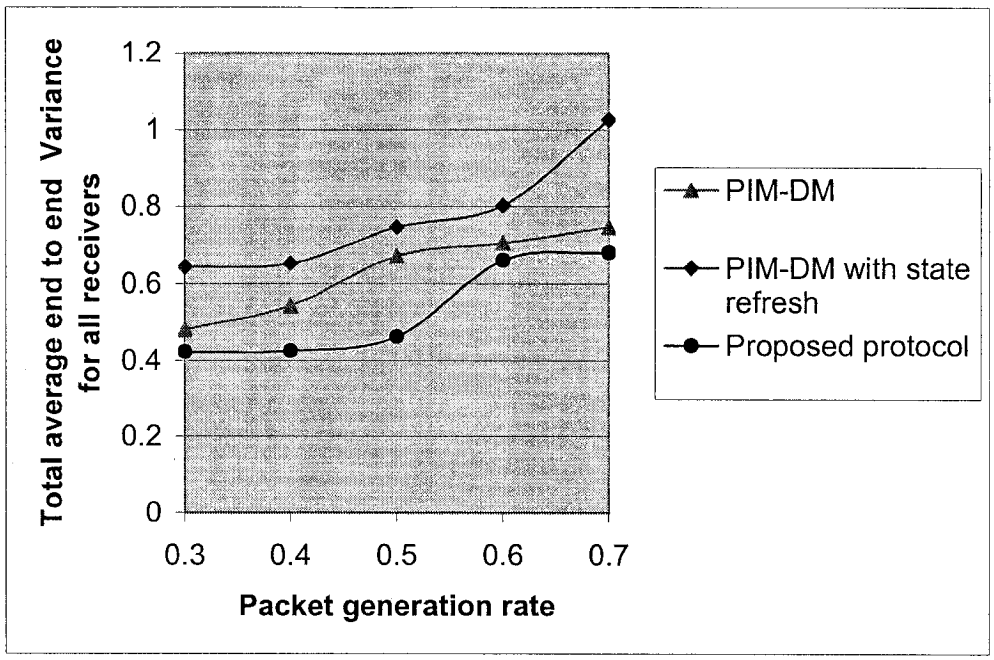


Figure 3.19: Total average end to end variance for all routers Vs Packet generation rate

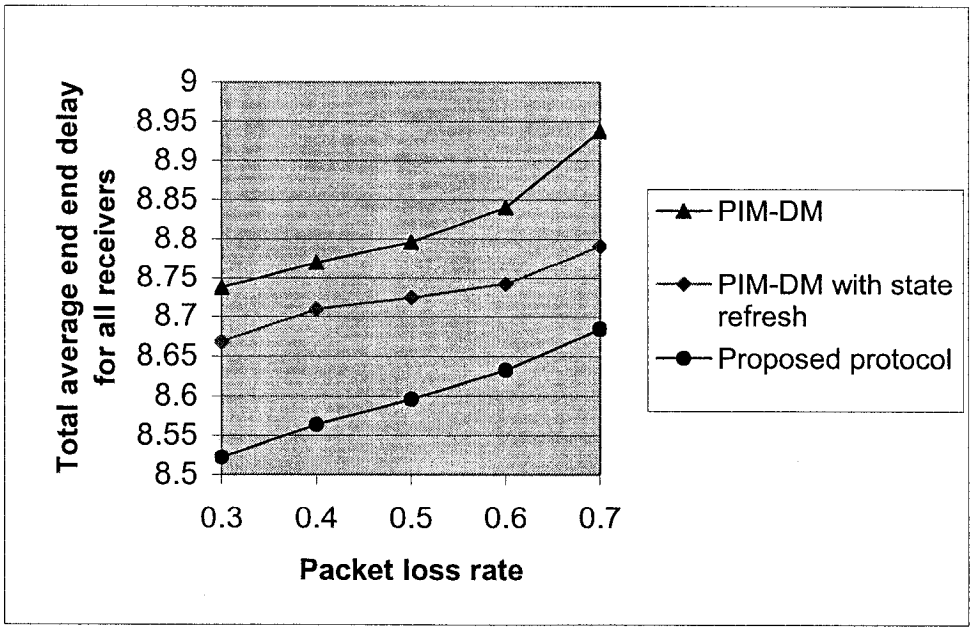


Figure 3.20: Total average end to end delay for all routers Vs Packet loss rate

Similarly, in Figure 3.20 and 3.21 we see that, with the increase of packet loss rate the proposed protocol faces less average and variance of end to end delay. This is also because of its flooding free and non periodic nature. Finally in Figure 3.21 we see that, for different receivers, the average end to end delay is less for the proposed protocol.

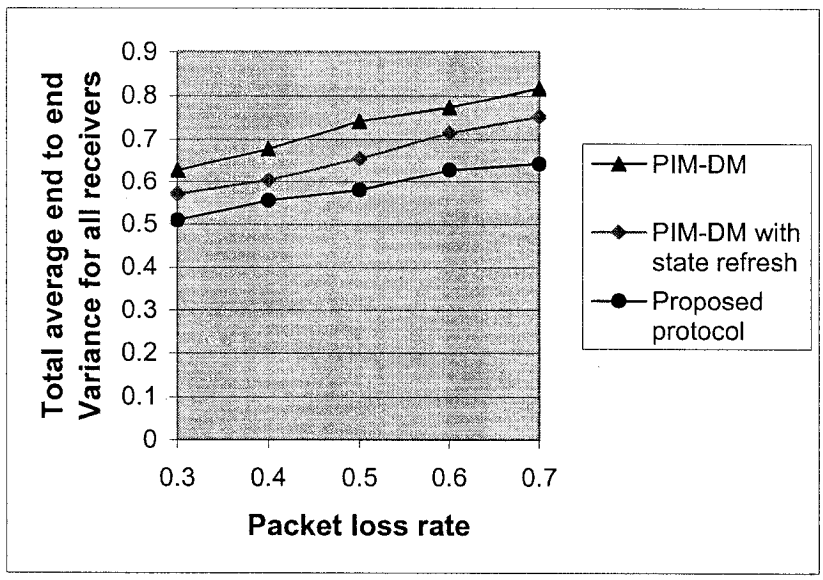


Figure 3.21: Total average end to end variance for all routers Vs packet loss rate

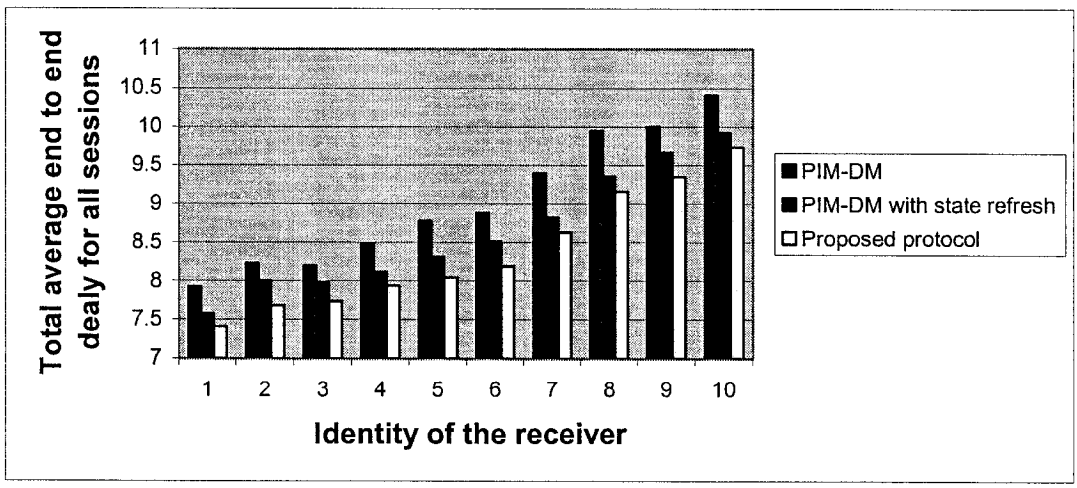


Figure 3.22 Total average end to end delays for all sessions Vs Identity of the router

3.3.9.3 Delay Jitter

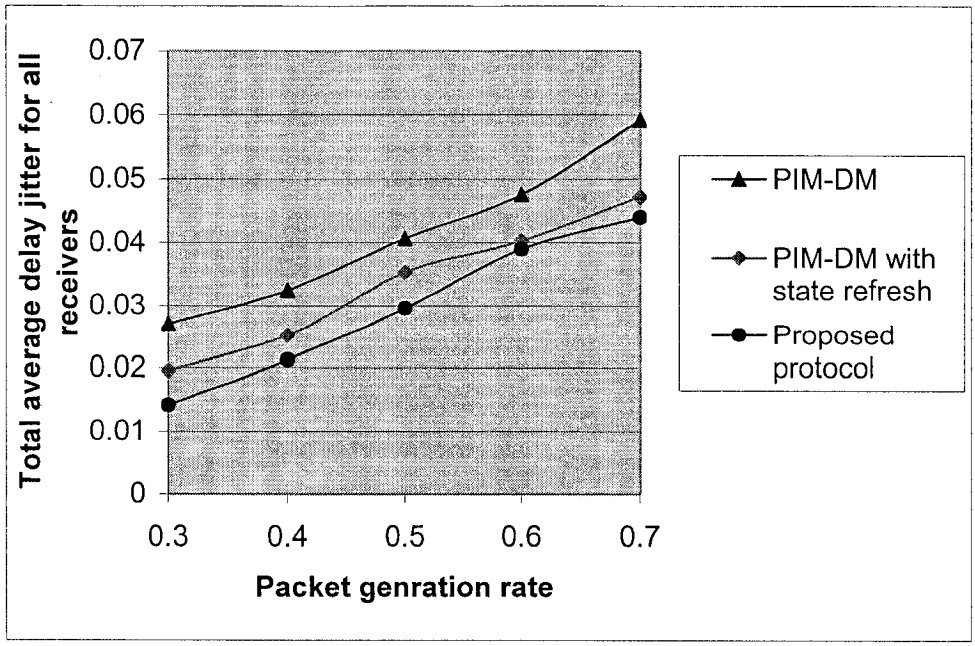


Figure 3.23: Total average delay jitter for all routers Vs Packet generation rate

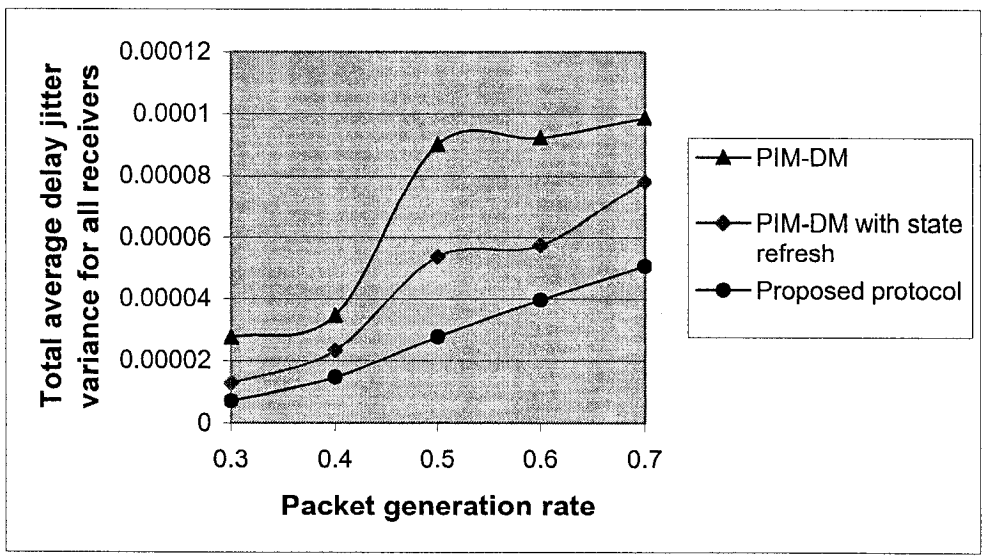


Figure 3.24: Total average delay jitter variance for all routers Vs Packet generation rate

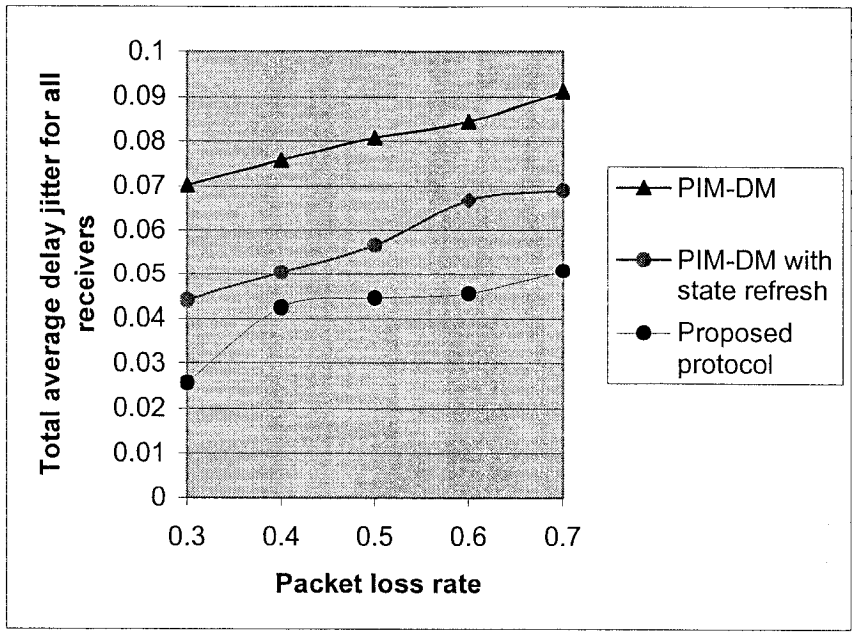


Figure 3.25: Total average delay jitter for all routers Vs Packet loss rate

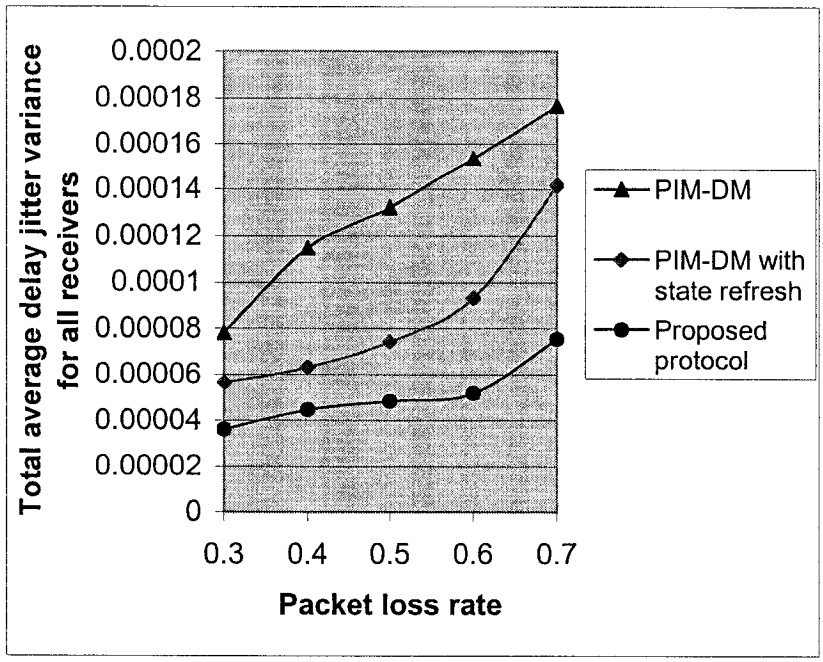


Figure 3.26: Total average delay jitter variance for all routers Vs Packet loss rate

In Figure 3.23 and 3.24 we varied the packet generation rate. We see that multicast packets face less average and variance of delay jitter with the proposed protocol. This is Because of the absence of periodic flooding effect in the proposed protocol, buffers have less queuing length and fewer overflows and this creates less jitter.

Similarly in Figure 3.25 and 3.26 we varied the packet loss rate and found the proposed protocol better for the above mentioned reasons.

Chapter 4

Proposed Multicast Protocol's Mobility Support Mechanism for Integrated LAN-WLAN

In this chapter we focus on the proposed protocol's mobility support mechanism. The proposed protocol ensures simple mechanism for reaching all possible receivers and eliminating distribution to uninterested receivers. It also ensures saving of bandwidth, first and smooth handover with the use of fewer control signals. We overcame the problem of bandwidth consuming inefficient periodic flooding by making it non periodic in true sense.

The handovers of mobile users among AP's are maintained by micromobility protocol. Micromobility protocols are still under intensive research and none of them has been implemented yet. Most popular micro mobility protocols are Hierarchical Mobile IP (Mobile IP Regional Registration), Cellular IP and HAWAII. This thesis does not work

on micro mobility protocols. It assumes that the basic handover is done by any micro mobility protocol and gives description of the post handover multicast mechanism. By the way, the Triangular routing problem is already solved in Hierarchical Mobile IP by the use of Route optimization.

4.1 Problem Definition

General multicast protocols considered for Infra-structured LAN-WLAN faces some major problems. DVMRP could lead to the dropping of multicast packets when users move and MOSPF faces the problem of inefficient routing of multicast packets. PIM allows mobile users to join the group at any node and provide efficient routing [36]. But PIM-SM (sparse mode) and The Core-Based Tree (CBT), both may need excessive control signals while mobile users move and handovers occur. PIM–SM is widely used for Wired LAN but for WLAN it could suffer from too many control signals, as it is a complicated algorithm. And WLAN APs have very small coverage area (100 - 250 meter, depending on types and locations of the APs) and thus due to movement of users, lots of handovers occur. Specially when there is a huge number of users, handovers due to their mobility generate many control signals for a single Rendezvous Point (RP). A single RP can not handle all these efficiently, because for every handover, PIM-SM will have to make the shared tree first and then move to the source tree. These processes take some time. These may cause inefficient and slow handovers and subsequently lots of drops. It may happen that a speedy mobile user has crossed the coverage area of the new AP before the handover process has been completed. Again when the RP is down it will affect the whole multicasting system.

Again, we faced some problems when we considered PIM- DM for multicast over integrated LAN-WLAN with mobile users. Major potential problems are:

1. The periodic flood and prune nature of PIM dense mode is a problem for WLAN. As it is bandwidth hungry. PIM-DM uses the push model and the traffic is initially flooded to all PIM neighbors. Branches that don't need data are pruned, and multicast forwarding states are created. But this pruned states timeout in every 3 minutes and thus creates a new flood in every 3 minutes. This creates extra unwanted traffic for the uninterested branches of networks and the mobile receivers.

2. If we stop the periodic flooding process, that has some side effects, (S,G) state (Source tree) in multicast routers will expire. And without (S,G) state a handovered mobile user can not join in the existing multicast session through the new AP.

3. PIM-DM does not provide specifications for mobile user's handover policies as it was defined for wired LAN.

4. When the multicasting sender moves then tunneling of multicasting data packets may be required and that is not specified by PIM-DM.

4.2 Handover Processes

User movement will change the multicast tree topology. In order to maintain old topology and thus smooth handover, we assume that handover is done by Hierarchical Mobile IP (Mobile IP Regional Registration) micro mobility protocol . In addition, we have to include some mechanism to continue with the ongoing multicast process.

When sender/receiver moves from it's HA (Home agent) to FA (Foreign agent) or one FA to another FA it will send an IGMP leave message to its agent before leaving. This will prune that agent if that agent does not have any multicast group receiver. So, when there is a leave, each time an IGMP query is generated by the previous agent to make sure whether it still has any more receivers or not. If it does not have any then the agent will send prune message to its upstream router to prune.

4.2.1 Source Movement

After the general handover process is completed. Source needs to use tunneling method. Sender encapsulates the multicast packet as a general unicast packet and sends it to FA with the destination address of HA. FA sends this unicast packet to HA. HA de-capsulates the packet and send the multicast packet to MR (Multicast router) and Finally MR multicasts the packet.

4.2.2 Receiver Movement

After the general handover process is completed, receiver will generate IGMP V2 join for group specific join and or IGMP V3 for source specific join. If the corresponding

router has the desired multicast traffic then it will transmit the traffic immediately to the receiver. Otherwise it will create a Graft message to manage the multicast traffic for the receiver. However, in our flowchart and simulation on the basis of "Graft required or not" and the "number of nodes graft needs to visit", we classified the handovers as first, moderate or slow handovers. This is not a fixed number. It is just an assumption on the basis of number of hops Graft needs to visit. It will vary on the performance of the micro mobility protocol. Because, if the Graft needs to visit many hops then it will cause more signaling delay and thus will cause slow handover. If it visits less number of hops then it will cause less signaling delay and thus create moderate handover. If graft is not required to manage desired multicast data then the signaling delay due to Graft mechanism will be absent and thus it will cause fast handover.

4.3 Flowcharts of the Simulation Model

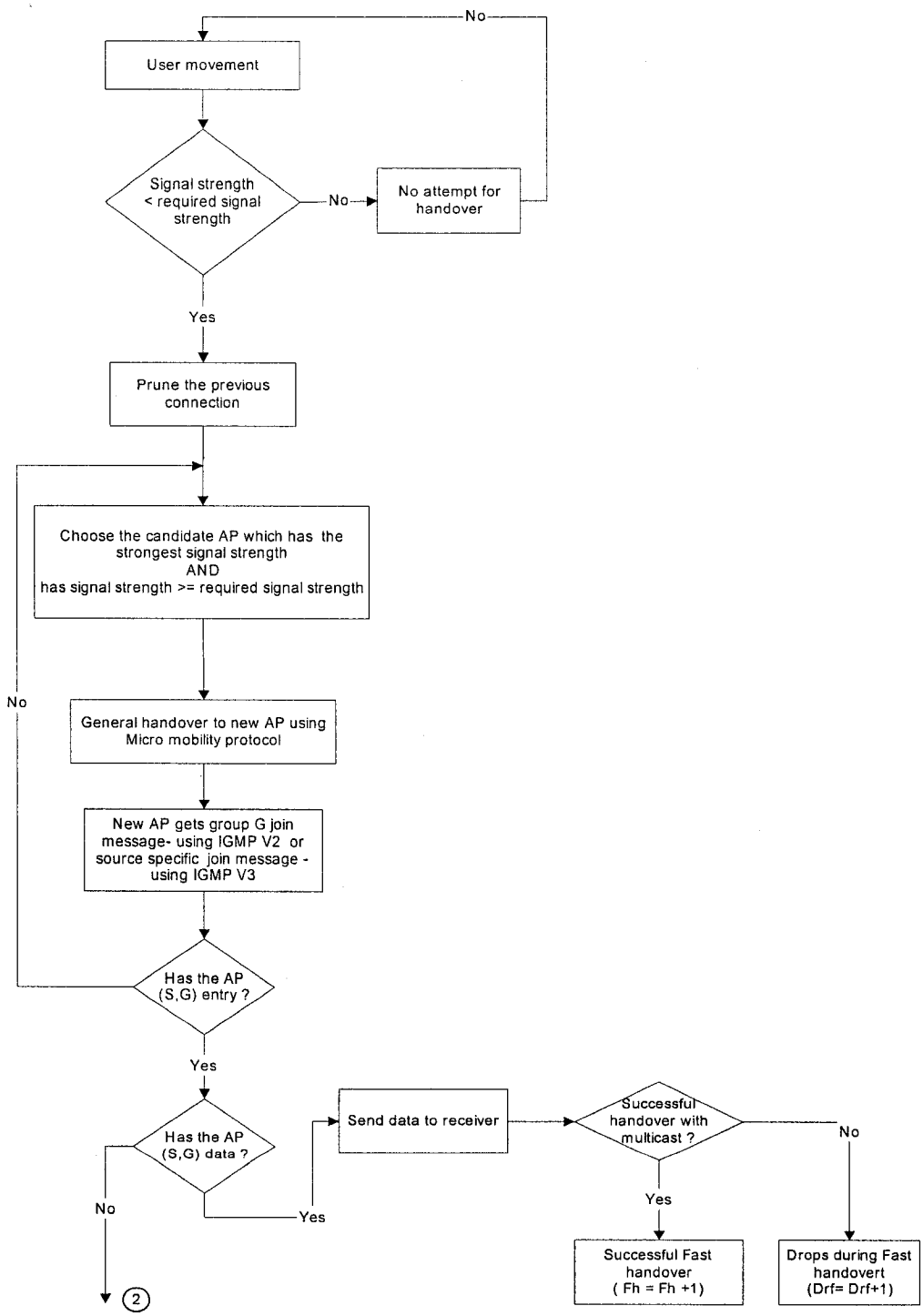


Figure 4.1: Handover with multicast (Without Graft)

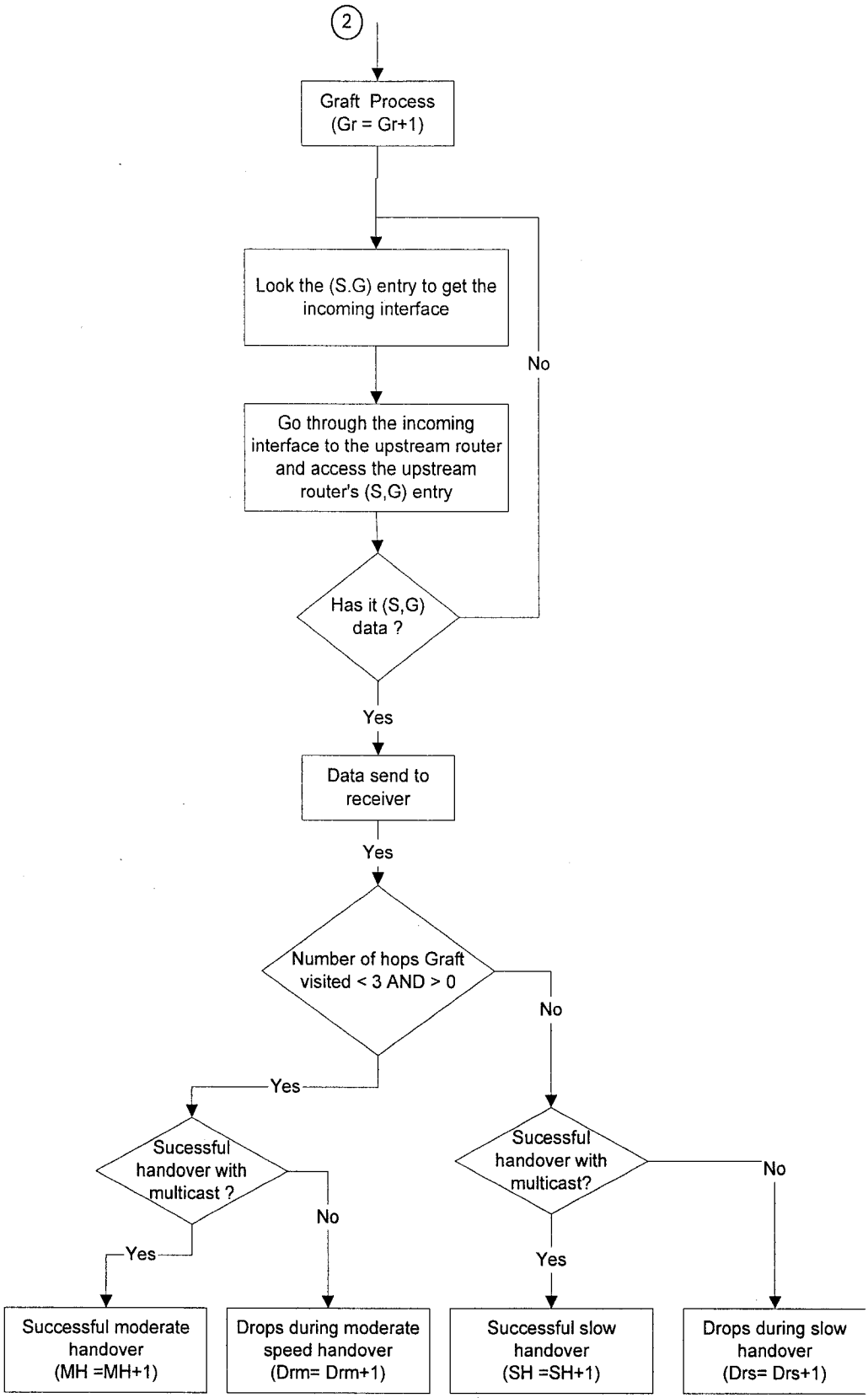


Figure 4.2: Handover with multicast (With graft)

4.3.1 Handover with Multicast (Without Graft)

Figure 4.1 describes the handover with multicast without any Graft. After certain iteration (movement), the mobile station will check the signal strength. If the measured signal strength is smaller than the required signal strength then the mobile user prunes the previous connection and chooses a candidate AP which has the strongest signal strength. Moreover, this signal strength must satisfy the given allowed signal strength. Then the handover is done using micro mobility protocol.

The router with the new AP will get the IGMP join message from the receiver. If the router does not have the desired (S,G) entry then the receiver will try for another AP.

If the router has the (S,G) data, then it will send the data directly to the receiver through the AP. Handovers without any Graft will create fast handover, as there is no signaling delay due to Graft message creation and the passing of the Graft message through the hops. Drops will be counted for unsuccessful attempts.

If the router does not have the (S,G) data then it needs to create a Graft.

4.3.2 Handover with Multicast (With Graft)

Figure 4.2 describes handover with multicast (with Graft). If the number of the hops graft message needs to visit is smaller than 3 and greater than 0, then it creates a moderate speedy handover. And if the number is greater than 2 then it will create a slow handover. Because, if the Graft message travels a large number of hops then the signaling delay increases. This is not a fixed number. This is an assumption.

4.4 Performance Analysis

We analyzed the performance of the proposed scheme with number crunching computer simulations.

4.4.1 Network Parameters

Number of LANs: 1

Number of users per node: 0-20

Total number of hosts: Up to 100

Mobile host mobility probability: .4

Number of multicast sessions: 5 for each phase.

Number of multicast sources: 1

Number of multicast groups: 1

Number of users per group: Up to 100

Speed of mobile users: 0-5 meter/second

In this phase we changed the multicast group size and session duration and observed the effects on number of handover attempts, number of grafts required and number of different kinds of handovers. For the first phase various session durations are - Session1 - 1200 unit, Session2 -1800 unit, Session3 -2400 unit, Session4 -3000 unit, Session5 - 3600 unit

For every session, we took 5 different group sizes- Group size of 20,40,60,80 and 100 receivers. Please note that here by the word "handover" we recognize handover with multicast process.

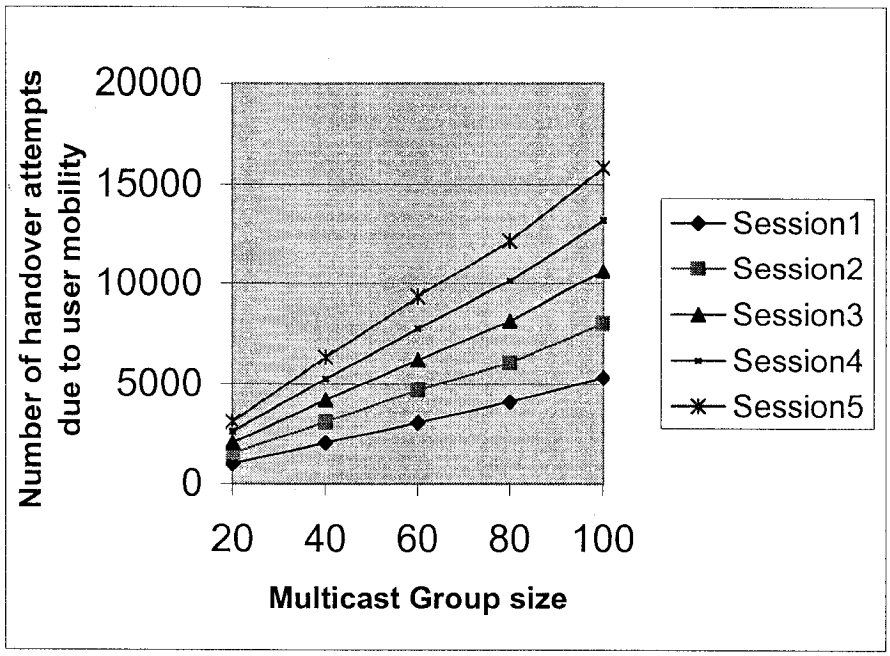


Figure 4.3: Group size Vs Number of handover attempts

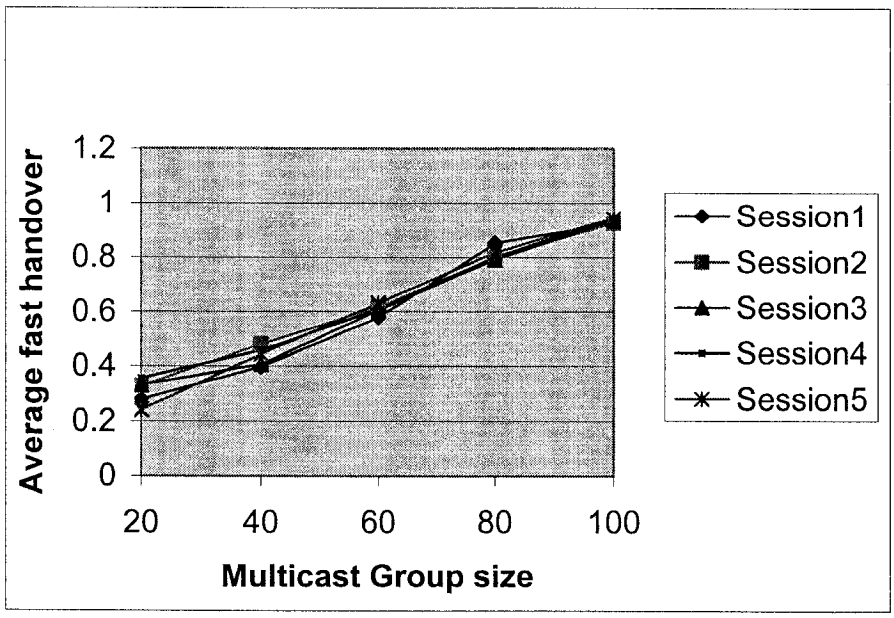


Figure 4.4: Multicast Group size Vs average fast handovers

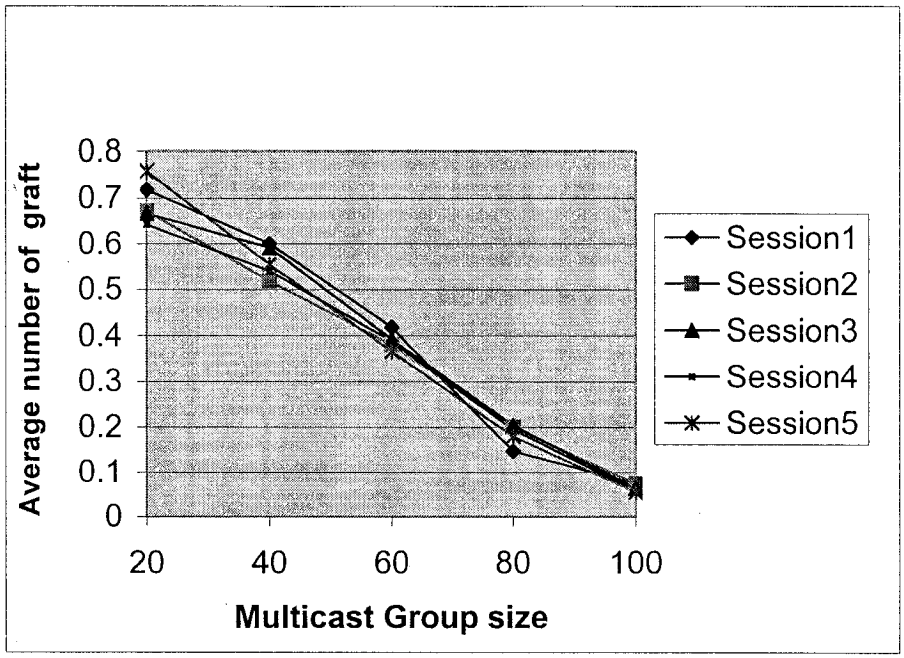


Figure 4.5: Multicast Group size Vs average Grafts

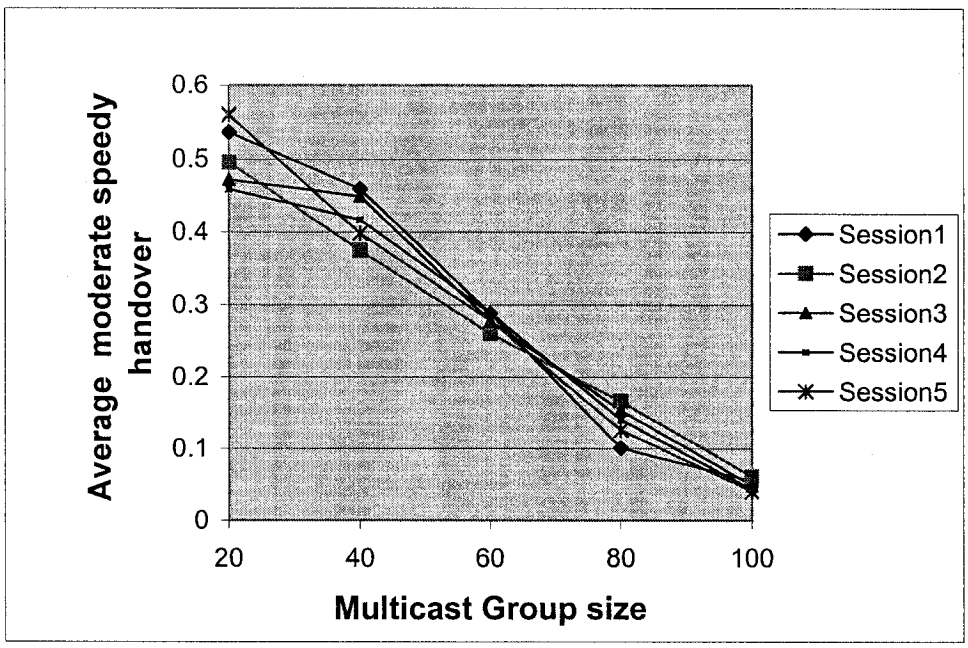


Figure 4.6: Multicast Group size Vs average moderate speedy handovers

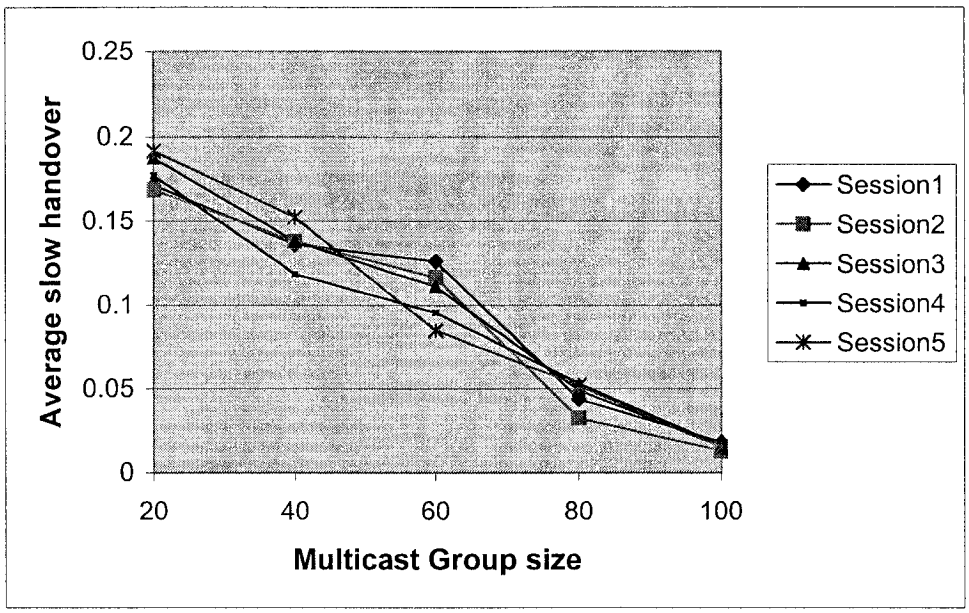


Figure 4.7: Multicast Group size Vs average slow handovers

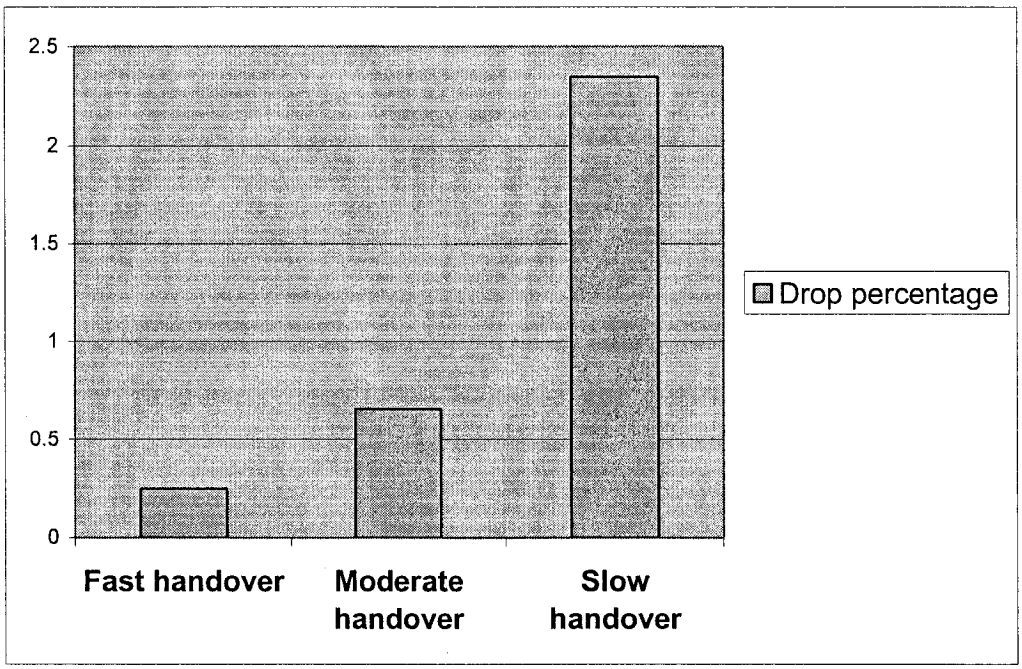


Figure 4.8: Drop percentage in different types of handovers

In Figure 4.3, we see that with the increase of the group size, the number of handover attempts increases due to user mobility. Generally it is very normal that when the number of the users increases, number of handover attempts will also increase due to their mobility.

In Figure 4.4, with the increase of group size fast handovers increase and in Figure 4.5 - with the increase of the group size graft request is decreased.

Actually most interesting findings of this simulation are shown in Figures 4.4 and 4.5, where we see that, with the increase of group size, number of graft decreases. This is because, when a small number of users become subscriber of a multicast session, then it is more likely that they are not uniformly distributed through out the network. But when a large number of users subscribe to a multicast session the possibility of their uniform distribution through out the network is more evident. In this case, almost all the routers have more possibility to have a user who is attending the multicast session. And for that, when a new user joins multicast group or when a current multicast receiver is handovered to a new AP, the router does not need a graft for (S,G) traffic, because the router already has the (S,G) traffic. This results in fast handovers. As there is no signaling delay due to Graft message creation and the passing of the Graft message through the hops.

And even when it does not has the (S,G) traffic, it does not need a graft that requires many hops to search for finding the desired (S,G) data. As almost all the routers already have the (S,G) traffic. So, it will more probably find the (S,G) traffic from a nearer router rather than to search for many hops for the desired (S,G) traffic . This results in moderate speedy handovers. Because, if the Graft message travels a large number of hops then the signaling delay increases and that causes extra delay. So, we assumed that if the number

of hops needed to be visited by the Graft message is greater than 0 but less than 3 then it will cause a moderate handover. If greater than 2 , then it will cause a slow handover. So, in our proposed protocol when the number of receivers is more, then most of the handovers are fast and smooth. And average drops during fast handovers are less than that of moderate and slow handovers.

In Figure 4.6, we see that with the increase of group size, moderate handover decreases and in Figure 4.7, with the increase of group size, slow handover decreases. As with the increase of the group size almost all the APs will have at least one receiver and therefore the newly handover receiver will get the desired traffic without creation of graft message and thus causing fast handover rather than slow or moderate speedy handover.

In Figure 4.8, we see that first handover faces least number of drops and moderate handover faces relatively more drops and slow handover faces more drops. If the Graft message travels a large number of hops then the signaling delay increases and that causes extra delay and if this delay is very high then it leads to a drop. That's why slow handover faces more drops mainly due to signaling delay. However, in the First handovers most of the drops are regarding signaling errors and not due to the signaling delay. Similarly in the moderate handovers, drops are mainly due to signaling errors but signaling delay also has some contributions.

Chapter 5

Conclusions and Future Works

5.1 Contributions and Conclusions

The thesis outlines an overview of a periodic flooding free and non periodic natured PIM-DM for corporate level multicast over LAN and integrated LAN-WLAN. In the proposed protocol, PIM-DM has been made non periodic in true sense. And control signaling mechanism has been simplified and optimized by introducing some new techniques. Simulation results support the advantages and applicability of the proposed protocol. The proposed protocol will be very efficient for corporate level closed network multicasting. This is the contribution of the thesis.

In the first part of the thesis, we introduced some new control signals and acknowledge messages. Newly introduced multicast session end message makes the PIM-DM free from periodic massive floodings without the need of any state refresh message. Moreover, the advantages of the multicast session end messages are over the state refresh message have been described. It was shown that multicast session end messages are more efficient in terms of number of control signaling, timers and processor load and memory

utilization. Moreover, it makes the PIM-DM non periodic in true sense. It also shows efficiency, when the number of (S,G) states increases in the multicast routers.

In the second part of the thesis, reliability issues of the proposed protocol have been described. Acknowledging messages for Prune, graft and multicast session end message were introduced. These acknowledging messages increase the reliability of the proposed multicast protocol. Solution of the first hop router failure and its corresponding infinite lifetime (S,G) state problem has also been described and solved. Using this mechanism any kind of unnecessary (S,G) states can be removed. In this part, the corporate multicast confidentiality mechanism has also been described with the use of TTL threshold.

In the third part of the thesis, mobility support mechanism of the proposed protocol has been described. It has been described, why the proposed protocol is better suited for mobility support than the other general multicast protocols? Both the sender and the receiver movements and their corresponding mobility support mechanisms for multicast have also been described. The proposed protocol ensures fast and seamless mobility of the mobile users while they are attending multicast sessions.

Simulations have been done to test our proposed protocol for different performance criterions. Simulations results in different parts of the thesis, support advantages and applicability of the proposed protocol for corporate level multicast over LAN and integrated LAN-WLAN.

5.2 Suggestions and Future Works

The research and development work done on PIM-DM in this thesis is only part of study in this research direction. There remain many aspects that can be further studied and investigated.

Firstly, further reliable signaling of the multicast session end message can be studied to make the proposed protocol suitable for more rough networks, where packet losses are high.

Secondly, different bugs may exist in the proposed protocol for different conditions, which may be further studied.

Thirdly, further works can be done on the proposed protocol's tolerability mechanism on various network disasters.

Fourthly, we considered only the most important performance criterions for simulations. However, some more performance criterions can be considered in future simulations.

Fifthly, the simulators designed for this thesis are based on some important assumptions. More efforts and time can be given to design a better simulator that can generate more realistic results.

Finally, the proposed protocol can be employed in real time or semi real time networks and can be tested for different performance criterions and bugs.

References

[1] S.E. Deering, "Host extensions for IP multicast", **RFC 1112, August 1989.

[2] Jeffrey Mogul, "Broadcasting Internet datagrams", RFC 0922 or STD 0005, October 1984.

[3] C. Partridge, T. Mendez, W. Milliken, "Host Anycasting Service", RFC 1546, November 1993.

[4] Fundamentals of IP Multicast, Module 1, Tutorial document of Cisco systems, 2001

[5] W. Fenner, "Internet Group Management Protocol, Version 2", RFC 2236, November 1997

[6] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, "Internet Group Management Protocol, Version 3" RFC 33376, October 2002.

[7] Peter J. Welcher, "The Protocols of IP Multicast", September 2001, http://www.netcraftsmen.net/welcher/papers/multicast01.html

[8] Z. Albanna, K. Almeroth, D. Meyer, M. Schipper, "IANA Guidelines for IPv4 Multicast Address Assignments", RFC 3171, BCP 0051, August 2001.

[9] Qingfeng XU, "Router Buffering and Caching techniques for Multi-session reliable multicast", M.A.Sc thesis in the dept of ECE of Concordia University, April 2003

[10] Andrew Adams, Jonathan Nicholas, William Siadak, "Protocol independent multicast dense mode-Protocol specification (revised)", Internet draft of IETF, September 2003.

**RFC means Request for comments. The official specification documents of the Internet Protocol suite that are defined by the Internet Engineering Task Force (IETF) and the Internet Engineering Steering Group (IESG) are recorded and published as *standards track* RFCs. As a result, the RFC publication process plays an important role in the Internet standards process. RFCs must first be published as Internet Drafts.

[11] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei "Protocol Independent Multicast-Sparse Mode (PIM-SM) – Protocol Specification :" RFC 2362 , June 1998.

[12] D. Waitzman, C. Partridge, S.E. Deering, "Distance Vector Multicast Routing Protocol", RFC 1075, November1988.

[13] J.Moy, "Multicast extensions to OSPF", Network Working Group, RFC 1584, Mar.1994.

[14] A. ballardie, "Core-based trees (CBT version2) multicast routing", Network Working group, RFC 2189, Sept. 1997.

[15] T. Maufer, C.Semeria, 3Com Corporation, "Introduction to IP Multicast Routing", draft-ietf-mboned-intro-multicast-01.txt, March 1997.

[16] Peter J. Welcher, PIM Dense Mode, tutorial web pp., 10/1/2001, (www.netcraftsmen.net/welcher/papers/multicast02.html)

[17] Peter J. Welcher, PIM Sparse Mode, tutorial webpp., 11/2/2001, (www.netcraftsmen.net/welcher/papers/multicast03.html)

[18] C.L. Hedrick, "Routing Information Protocol", RFC 1058, June 1988.

[19] Mohammad Banikazemi, "IP Multicasting: Concepts, Algorithms, and Protocols", survey paper, http://www.cse.ohio-state.edu/~jain/cis788-97/ftp/ip_multicast/index.htm, August 1997.

[20] Mike Rodbell, "Standards & Protocols Sparse Mode Multicast", http://www.commsdesign.com/main/9810/9810standards.htm CBT

[21] Hiperlan/2 Global Forum (web pp.). URL: http://www.hiperlan2.com/web/

[22] HomeRF Wireless LAN (web pp.). URL: http://www.homerf.org

[23] Crow, Brian P., Indra Kim Widjaja, Geun Jeong, and Prescott T. Sakai., "IEEE-802.11 Wireless local Area Networks" IEEE Communications Magazine, September 1997, vol. 35, No.9: pp.s 116-126.

[24] Alberto Leon-Garcia, Indra Widjaja, "Communication Networks: Fundamental concepts and key architecture", Mcgraw-Hill, 2002

[25] Perkins, C.E., "Ad Hoc Networks", Addison-Wesley, Reading, MA, 2001.

[26] Jim Geier, "Wireless LANs: Implementing interoperable networks", Macmillan Technical Publishing, First Edition, 2001

[27] William Stallings, "Wireless Communications and Networks", Prantice Hall, New York, 2003

[28] A. T. Campbell and J. Gomez,"IP Micro-Mobility Protocols,"ACM SIGMOBILE, Mobile Comp. and Commun. Rev., vol. 4, no. 4, Oct. 2001, pp. 45–54.

[29] C. Perkins, Ed., "IP Mobility Support," Internet RFC 2002, Oct. 1996.

[30] Andrew t. campbell, Javier gomez, Sanghyo kim, and Chieh-yih wan, Zoltan r. turanyi and Andras g. valko "Comparison of IP micromobility protocols", IEEE Wireless Communications, Feburary 2002.

[31] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IP Regional Registration," Internet draft, draft-ietfmobileip-reg-tunnel-03, July 2000.

[32] A. Valkó, "Cellular IP: A New Approach to Internet Host Mobility," ACM SIGCOMM Comp. Commun. Rev., vol. 29, no. 1, Jan. 1999, pp. 50–65.

[33] R. Ramjee et al., "HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-area Wireless Networks," Proc. IEEE Int'l. Conf. Network Protocols, 1999.

[34] PIM Dense Mode ,Module3, 2001 Cisco systems

[35] "Delay jitter",www.csd.uwo.ca/courses/CS457a/notes/cs457_2.ppt, pp. 5

[36] Upakar Varshney, "Multicast over WLAN"(Communication of the ACM December 2002/Vol. 45. No. 12, pp. 31-37)