# SHORTEST PATH COMPUTATION IN MULTICAST NETWORK WITH MULTICAST CAPABLE AND INCAPABLE DELAY ASSOCIATED NODES

A dissertation report

Submitted in partial fulfillment of the requirements for the

Degree of

**Master of Technology**

**In**

**Electronics and Communication Engineering**

Submitted By

**Sonal Yadav(11000954)**

**Under the supervision of**

Mr. Sharath Naik

Assistant Professor

Department of Electronics & Communication Engineering

Transforming Education Transforming India

**Lovely Professional University Jalandhar-Delhi G.T Road (NH-1), Phagwara, Punjab, 144411, India**

**2015**

# CERTIFICATE

This is to certify that the realization of the dissertation titled "Shortest path computation in multicast network with multicast capable and multicast incapable delay associated nodes" that is being submitted by **Sonal Yadav** is in partial fulfillment of the requirements for the award of Master Of Technology Degree and is a record of bonafide work done under my guidance. The contents of this report, in full or in parts, have neither been taken from any other source nor have been submitted to any other institute or university for award of any degree or diploma and the same is certified.

**Mr. Sharath Naik**

**Assistant Professor**

Lovely Professional University

Phagwara, Punjab

# CANDIDATE DECLARATION

I declare that the work presented in this report entitled "Shortest path computation in multicast network with multicast capable and multicast incapable delay associated nodes", submitted to the department of Electronics and Communication, Lovely Professional University, Phagwara, Punjab for the award of Master of Technology degree in Electronics and Communication Engineering is my original work. The contents of the report do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution. This is an authentic record of our own work carried out during the period January-2015 to April-2015 under the supervision of Mr. Sharath Naik.

**Date:**

**Name of student**:

# ACKNOWLEDGMENT

The real spirit of achieving is through the way of excellence of austere discipline, without which I would never have succeeded in finishing it without the co-operation, encouragement and help provided to me by various personalities. With this deep felt consent and pleasure, I would like to express my heartfelt gratitude to all those who helped me in preparation of this training report.

It gives me immense pleasure in expressing my deepest and sincerest gratitude towards my mentor Mr. Sharath Naik, for his considerate help, inspiring guidance throughout this work.

# ABSTRACT

The new technologies for networking based system are evolving significantly. We are going at a very fast speed towards creating a network that can fulfill all the requirements of the users . Demand of each user is unique and different from other user. However sometimes we need to send similar packets to different group of user simultaneously. In such cases unicast will result in waste in time while if we make use of broadcast that will result in waste of bandwidth. For such cases we need to make use of multicast. Within a multicast network we can make use of multicast capable and multicast incapable nodes. For maximum bandwidth usage we need to calculate the shortest path for data transfer.

The objective of this research is to increase the success rate of finding the minimum cost path as we increase the number of destinations for any given source along with multicast incapable nodes. I will try to consider delay associated with each node and then will try to find the final minimum cost path with the help of algorithm proposed in order to increase the success rate for transmission of the packets from the considered transmitted to corresponding multiple receivers and correspondingly will compare the success rate obtained to the one obtained in the base paper.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# CHAPTER 1

# INTRODUCTION

## 1.1 Introduction to Different Networking Protocols

### Unicast Message

When using unicast method, one device will send the packets to exactly one destination device. If some device needs to send a message to multiple devices, it will have to send multiple unicast messages, each packet addressed to a specific device. So, the sender has to send a separate message to each destination device, and to do that it has to know the exact IP address of each destination device. In uni-casting, each packet is destined for only one destination [10].

In the example I have taken one source device, and multiple receivers which belong to different groups of users (marked with different colours). As we can see in the diagram, unicast packets will be transferred to specific users by using the unique and particular IP address of the device, as the receiver address in the packet.

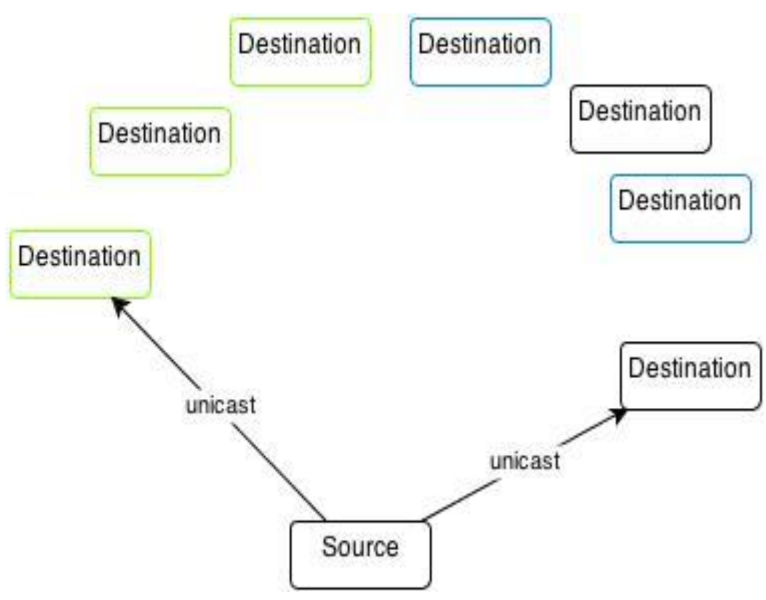


**Figure 1: Unicast Message**

## Broadcast Message

The second way of sending the packets is called the broadcasting. In broadcast, a packet is sent to all the users on specific network. The destination address in the packet is the special broadcast address. If the message has a broadcast address attached to it, all users that receive that particular message will receive it. So, all the users on the same network will receive the same message. Another thing to be noticed that routers don't forward broadcast packets. The router will receive the broadcast traffic, but it will not send through the router.

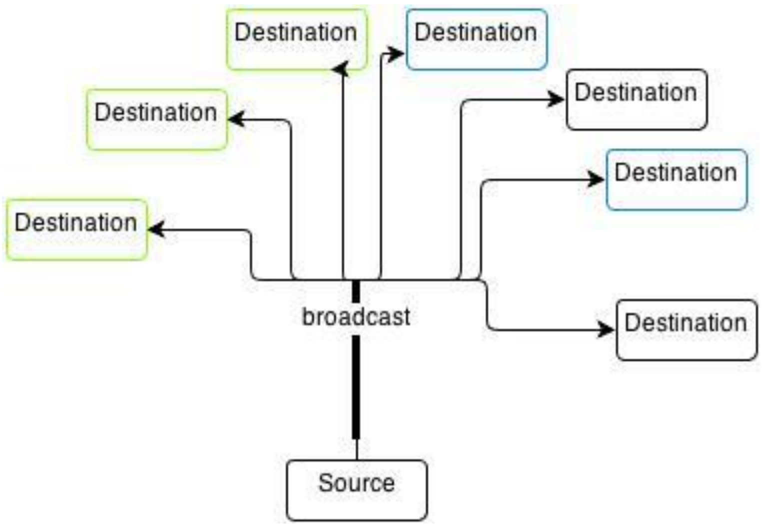


**Figure 2: Broadcast Message**

## Multicast Message

Multicasting detects logical groups of users. A single message can then be sent to the group.

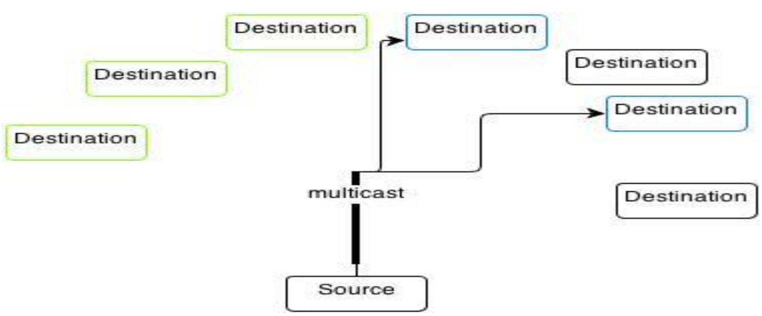


**Figure 3: Multicast Message**

Multicasting makes use of the Internet Group Management Protocol (IGMP) to detect groups and group members within the network. Routers will also use IGMP to send messages to subnets that have group members. The router actually doesn't keep track of which hosts are members of which group, only that the subnet contains at least one member for each group. If we have multiple routers, they will communicate and exchange information about multicast groups that they have.

Each host on the network can belong to multiple multicast groups. Hosts can join or leave groups at any time. Multicast groups are identified by special IP addresses between the range of 224.0.0.0 and 239.255.255.255. Each group is assigned its own address. Addresses within the 224.0.0.0 range are reserved for local subnet communications.

## 1.2 Network Assisted Unicast

### 1.2.1 Intra-Domain and Inter-Domain Routing

Today, an internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems. An autonomous system (AS**)** is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is referred to as intra-domain routing. Routing between autonomous systems is referred to as inter-domain routing. Each autonomous system can choose one or more intra-domain routing protocols to handle routing inside the autonomous system. However, only one inter-domain routing protocol handles routing between autonomous systems.

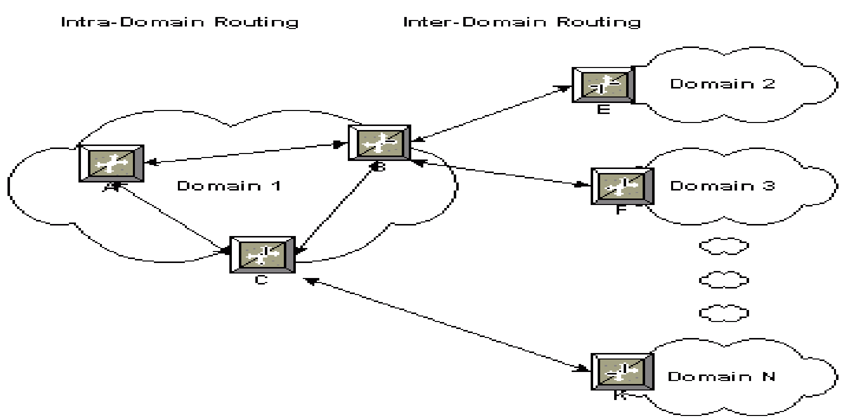


**Figure 4: Intra and Inter Domain Routing**

Several intra-domain and inter-domain routing protocols are in use. Routing Information Protocol (RIP) is the implementation of the distance vector protocol. Open Shortest Path First (OSPF) is the implementation of the link state protocol. Border Gateway Protocol (BGP) is the implementation of the path vector protocol. BGP is an exterior routing protocol.

### 1.2.2 Static and Dynamic Routing

A routing table can be either static or dynamic. A *static table* is one with manual entries. A *dynamic table*, on the other hand, is one that is updated automatically when there is a change somewhere in the internet. Today, an internet needs dynamic routing tables. The tables need to be updated as soon as there is a change in the internet. For instance, they need to be updated when a link is down, and they need to be updated whenever a better route has been found.

### 1.2.3 Network Assisted Unicast Protocols

#### 1.2.3.1 Distance Vector Routing (RIP)

Distance vector routing**,** sees an Autonomous System, with all routers and networks, as a *graph*, a set of nodes and lines (edges) connecting the nodes. A router can normally be represented by a node and a network by a link connecting two nodes, although other representations are also possible. The concept of distance vector routing can easily be understood with the help of routing information protocol which makes use of DVR in order to calculate minimum distance.

In distance vector routing, each node constructs a one-dimensional array containing the "distances"(costs) to all other nodes and distributes that vector to its immediate neighbours.

1. The starting assumption for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbours.

2. A link that is down is assigned an infinite cost.

For example consider the network given below:

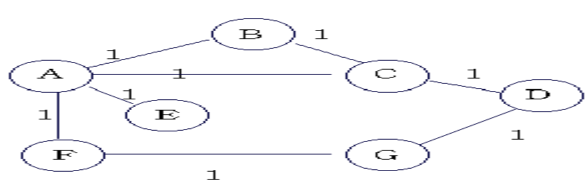


**Figure 5: Network 1**

**Table1. Initial distances stored at each node (global view).**

| Information at node | D(A) | D(B) | D(C) | D(D) | D(E) | D(F) | D(G) |
|---|---|---|---|---|---|---|---|
| **A** | 0 | 1 | 1 | - | 1 | 1 | - |
| **B** | 1 | 0 | 1 | - | - | - | - |
| **C** | 1 | 1 | 0 | 1 | - | - | - |
| **D** | - | - | 1 | 0 | - | - | 1 |
| **E** | 1 | - | - | - | 0 | - | - |
| **F** | 1 | - | - | - | - | 0 | 1 |
| **G** | - | - | - | 1 | - | 1 | 0 |

We can represent each node's knowledge about the distances to all other nodes as a table like the one given in Table 1. Note that each node only knows the information in one row of the table.

1. Every node sends a message to its directly connected neighbours containing its personal list of distance. (for example, **A** sends its information to its neighbours **B,C,E**, and **F**. )
2. If any of the recipients of the information from **A** find that **A** is advertising a path shorter than the one they currently know about, they update their list to give the new path length and note that they should send packets for that destination through **A**. ( node **B** learns from **A** that node **E** can be reached at a cost of 1; **B** also knows it can reach **A** at a cost of 1, so it adds these to get the cost of reaching **E** by means of **A**. **B** records that it can reach **E** at a cost of 2 by going through **A**.) [11]
3. After every node has exchanged a few updates with its directly connected neighbours, all nodes will know the least-cost path to all the other nodes.
4. In addition to updating their list of distances when they receive updates, the nodes need to keep track of which node told them about the path that they used to calculate the cost, so that they can create their forwarding table. (for example, **B** knows that it was **A** who said " I can reach **E** in one hop" and so **B** puts an entry in its table that says " To reach **E**, use the link to **A**.)

**Table 2. Final distances stored at each node (global view).**

| Information at node | D(A) | D(B) | D(C) | D(D) | D(E) | D(F) | D(G) |
|---|---|---|---|---|---|---|---|
| **A** | 0 | 1 | 1 | 2 | 1 | 1 | 2 |
| **B** | 1 | 0 | 1 | 2 | 2 | 2 | 3 |
| **C** | 1 | 1 | 0 | 1 | 2 | 2 | 2 |
| **D** | - | 2 | 1 | 0 | 3 | 2 | 1 |
| **E** | 1 | 2 | 2 | 3 | 0 | 2 | 3 |
| **F** | 1 | 2 | 2 | 2 | 2 | 0 | 1 |
| **G** | - | 3 | 2 | 1 | 3 | 1 | 0 |

In practice, each node's forwarding table consists of a set of triples of the form: (Destination, Cost, Next Hop)

For example, Table 3 shows the complete routing table maintained at node B for the network in Figure1.

**Table 3. Routing table maintained at node B.**

| Destination | Cost | Next Hop |
|---|---|---|
| **A** | 1 | A |
| **C** | 1 | C |
| **D** | 2 | C |
| **E** | 2 | A |
| **F** | 2 | A |
| **G** | 3 | A |

Routing table is maintained for each node in a similar fashion and after creation of all the routing tables, minimum distance is calculated for the required packet. Thus, distance Vector routing protocols base their decisions on the best path to a given destination based on the distance.

Distance is usually measured in hops, though the distance metric could be delay, packets lost, or something similar. If the distance metric is hop, then each time a packet goes through a router, a hop is considered to have traversed. The route with the least number of hops to a given network is concluded to be the best route towards that network. The vector shows the direction to that specific network. Distance vector protocols send their entire routing table to directly connected neighbours. Examples of distance vector protocols include RIP – Routing Information Protocol and IGRP – Interior Gateway Routing Protoco [10]l**.**

### 1.2.3.2 Link State Routing

In link state routing, if each node in the domain has the entire topology of the domain— the list of nodes and links, how they are connected including the type, cost (metric), and the condition of the links (up or down)—the node can use the Dijkstra algorithm to build a routing table.

**Building Routing Tables**

In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.

**1.** Creation of the states of the links by each node, called the link state packet or LSP.

**2.** Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.

**3.** Formation of a shortest path tree for each node.

**4.** Calculation of a routing table based on the shortest path tree.

**1. Creation of Link State Packet (LSP)**

A link state packet (LSP) can carry a large amount of information. For the moment, however, we assume that it carries a minimum amount of data: the node identity, the list of links, a sequence number, and age. The first two, node identity and the list of links, are needed to make the topology. The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones. The fourth, age, prevents old LSPs from remaining in the domain for a long time. LSPs are generated on two occasions:

**(a) When there is a change in the topology of the domain.** Triggering of LSP dissemination is the main way of quickly informing any node in the domain to update its topology.

**(b) On a periodic basis.** The period in this case is much longer compared to distance vector routing. As a matter of fact, there is no actual need for this type of LSP dissemination. It is done to ensure that old information is removed from the domain. The timer set for periodic dissemination is normally in the range of 60 minutes or 2 hours based on the implementation. A longer period ensures that flooding does not create too much traffic on the network.

**2. Flooding of LSPs**

After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbours. The process is called flooding and based on the following:

(a) The creating node sends a copy of the LSP out of each interface.

(b) A node that receives an LSP compares it with the copy it may already have. If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP. If it is newer, the node does the following:

i. It discards the old LSP and keeps the new one.

ii**.** It sends a copy of it out of each interface except the one from which the packet arrived. This guarantees that flooding stops somewhere in the domain (where a node has only one interface).

**3. Formation of Shortest Path Tree: Dijkstra Algorithm**

After receiving all LSPs, each node will have a copy of the whole topology. However, the topology is not sufficient to find the shortest path to every other node; a shortest path tree is needed [12].

A tree is a graph of nodes and links; one node is called the root. All other nodes can be reached from the root through only one single route. A shortest path tree is a tree in which the path between the root and every other node is the shortest. What we need for each node is a shortest path tree with that node as the root. The Dijkstra algorithm is used to create a shortest path tree from a given graph. The algorithm uses the following steps:

**(a) Initialization:** Select the node as the root of the tree and add it to the path. Set the shortest distances for all the root’s neighbours to the cost between the root and those neighbours. Set the shortest distance of the root to zero.

**(b) Iteration:** Repeat the following two steps until all nodes are added to the path:

**i. Adding the next node to the path:** Search the nodes not in the path. Select the one with minimum shortest distance and add it to the path.

**ii. Updating:** Update the shortest distance for all remaining nodes using the shortest distance of the node just moved to the path in step 2.

$$Dj = \text{minimum} (Dj, Di + cij) \text{ for all remaining nodes}$$

Following figure shows the formation of the shortest path tree for the graph of seven nodes. All the nodes in the graph have the same topology, but each node creates a different shortest path tree with itself as the root of the tree. We show the tree created by node A. We need to go through an initialization step and six iterations to find the shortest tree. In the initialization step, node A selects itself as the root. It then assigns shortest path distances to each node on the topology. The nodes that are not neighbours of A receive a shortest path distance value of infinity [13].

In each iteration, the next node with minimum distance is selected and added to the path. Then all shortest distances are updated with respect to the last node selected. For example, in the first iteration, node B is selected and added to the path and the shortest distances are updated with respect to node B (The shortest distances for C and E are changed, but for the others remain the same). After six iterations, the shortest path tree is found for node A. Note that in iteration 4, the shortest path to G is found via C, but in iteration 5, a new shortest route is discovered (via G); the previous path is erased and the new one is added.

## 4. Calculation of Routing Table from Shortest Path Tree

Each node uses the shortest path tree found in the previous discussion to construct its routing table. The routing table shows the cost of reaching each node from the root. This table shows the routing table for node A using the shortest path tree found in Figure

**Table 4. Routing table for node A**

| Destination | Cost | Next Router |
|---|---|---|
| A | 0 | - |
| B | 2 | - |
| C | 7 | B |
| D | 3 | - |
| E | 6 | B |

| | | |
|---|---|---|
| F | 8 | B |
| G | 9 | B |

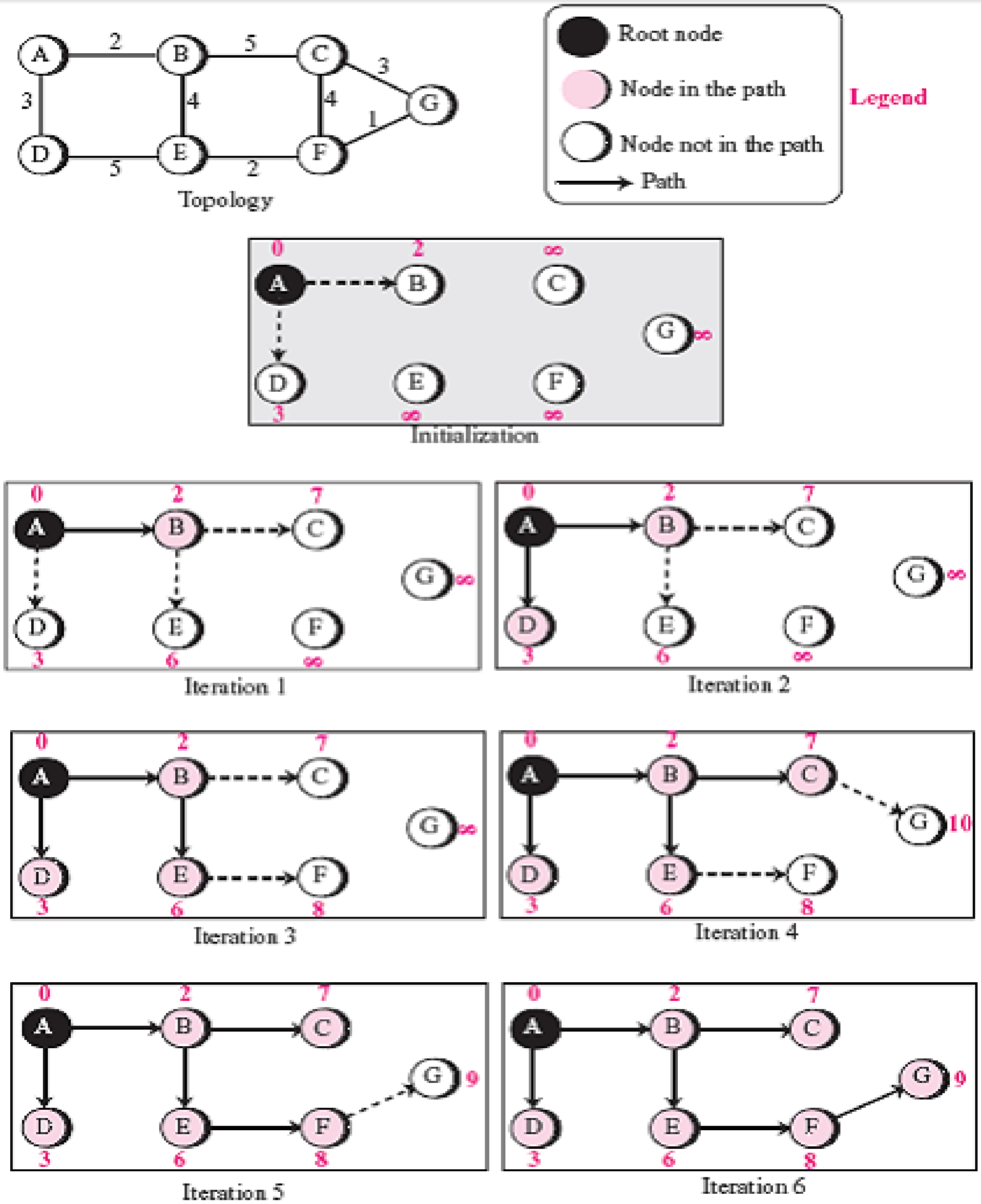


**Figure 7: Dijkastra algorithm**

### 1.2.3.3 Path Vector Routing

Distance vector and link state routing are both interior routing protocols. They can be used inside an autonomous system as intra-domain or intra-AS (as sometimes are called), but not between autonomous systems. Both of these routing protocols become intractable when the domain of operation becomes large. Distance vector routing is subject to instability if there is more than a few hops in the domain of operation. Link state routing needs a huge amount of resources to calculate routing tables. It also creates heavy traffic because of flooding. There is a need for a third routing protocol which we call path vector routing [14].

Path vector routing is exterior routing protocol proved to be useful for inter-domain or inter-AS routing as it is sometimes called. In distance vector routing, a router has a list of networks that can be reached in the same AS with the corresponding cost (number of hops). In path vector routing, a router has a list of networks that can be reached with the path (list of ASs to pass) to reach each one. In other words, the domain of operation of the distance vector routing is a single AS; the domain of operation of the path vector routing is the whole Internet. The distance vector routing tells us the distance to each network; the path vector routing tells us the path.

## 1.3 Introduction to Multicast Network

Multicasting uses the Internet Group Management Protocol (IGMP) to identify groups and group members. Routers will also use IGMP to send messages to subnets that have group members. The router actually doesn't keep track of which hosts are members of which group, only that the subnet contains at least one member for each group. If we have multiple routers, they will communicate and exchange information about multicast groups that they have. Each host on the network can belong to multiple multicast groups. Hosts can join or leave groups at any time. Multicast groups are identified by special IP addresses between the range of 224.0.0.0 and 239.255.255.255. Each group is assigned its own address. Addresses within the 224.0.0.0 range are reserved for local subnet communications.

When we use a switch to connect hosts, multicast messages are actually forwarded to all hosts on the hub or the switch. As you should know, devices actually use MAC addresses to communicate on the local network segment. When the device on the local segment needs to send a multicast message, it will use a frame with a special MAC address. Special multicast addresses in the MAC address begin with 01-00-5E. The remaining portion of the MAC address is a modified format of the multicast IP address. When the switch receives the frame with the multicast MAC address, it will forward the frame out all ports to all connected devices. In this case, even devices that are not members of the original IP multicast group will see the frame. However, devices that don't belong to the IP multicast group will not process the frame since they will check the destination IP address. If we want to avoid this problem in which devices which don't belong to the original IP multicast group still receive packets, we have to implement switches that are capable of IGMP snooping. IGMP snooping feature enables switches to check which device belongs to which multicast group. In that case, when a message arrives at the switch addressed to a specific group using the special frame address, the switch will forward that frame to the individual group members. It will not forward the frame to the devices that are not a member of the group. Only the switch with IGMP snooping can do that. So, the switch controls forwarding the frames to specific group members. The router keeps track of which subnets have group members [15].

## 1.4 What is Multicasting?

In computer networking, **multicast** (one-to-many or many-to-many distribution) is group communication where information is addressed to a group of destination computers simultaneously. Multicast should not be confused with physical layer point-to-multipoint communication. Group communication may either be application layer multicast or network assisted multicast, where the latter makes it possible for the source to efficiently send to the group in a single transmission. Copies are automatically created in other network elements, such as routers, switches and cellular network base stations, but only to network segments that currently contain members of the group. Network assisted multicast may be implemented at the Internet layer using IP multicast, which is often employed in Internet Protocol (IP) applications of streaming media, such as Internet television scheduled content (but not media-on-demand) and multipoint videoconferencing, but also for ghost distribution of backup disk images to multiple computers simultaneously. In IP multicast the implementation of the multicast concept occurs at the IP routing level, where routers create optimal distribution paths for data grams sent to a multicast destination address [10].

## 1.5 Need of multicasting

Multicast is the most cost effective method to broadcast data or images from any one point to a multitude of required receivers. Broadband (Unicast) is expensive to create because it requires a one to one broadcast receiver relationship like a telephone connection. It would be impossible using current broadband Unicast technology to create an Internet television broadcast to multiple desktops in a targeted office. The bandwidth (data space) consumed by such a transmission would saturate the office building's connection to the Internet. Most businesses have broadband Internet access, even so they are limited by the size of their service. Traditional Internet transmissions are expensive because they utilize "one-to-one" technology. This means that each end-user receives a single and distinct signal directly from a remote sending station. Each signal transmission takes up an identical amount of bandwidth (data space allowed). Therefore, depending upon the number of requested viewers, each discreet event broadcasted could take up an enormous amount of bandwidth. Unlike traditional Internet transmissions (also called Unicast), Multicasting is akin to television or radio, where ONE signal is transmitted, and any number of potential users can access them (as easily as turning a dial) without any additional usage of valuable bandwidth. In fact, with Multicasting the more end-users who participate in the transmission the greater the efficiency in both cost, speed, and ease of dissemination of information, be it direct, real-time, photographs of the factory floor as seen from a camera, or transmissions of important strategic meetings for those unable to attend [13].

## 1.6 Network Assisted Multicast

### 1.6.1 Multicast Addresses

A multicast address is a logical identifier for a group of hosts in a computer network, that are available to process data-grams or frames intended to be multicast for a designated network service. Multicast addressing can be used in the Link Layer (Layer 2 in the OSI model), such as Ethernet multicast, and at the Internet Layer (Layer 3 for OSI) for Internet Protocol Version 4 (IPv4) or Version 6 (IPv6) multicast.

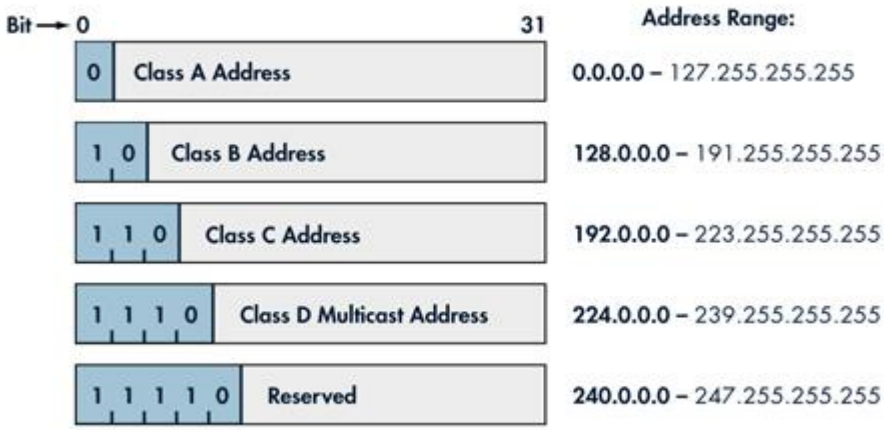


**Figure 8: Addresses Ranges**

**Table 5: Address Ranges in Multicast Range**

| Multicast Address Range | Usage |
|---|---|
| 224.0.0.0 to 239.255.255.255 | This range represents the entire IPv4 multicast address space. It is reserved for multicast applications. |
| 224.0.0.0 to 224.0.0.255 | This range is part of the permanent groups. Addresses from this range are assigned by IANA for network protocols on a local segment. Routers do not forward packets with destination addresses used from this range. |
| 224.0.1.0 to 224.0.1.255 | This range is also part of the permanent groups. Addresses from this range are assigned by IANA for the network protocols that are forwarded in the entire network. Routers forward packets with destination addresses used from this range. |
| 232.0.0.0 to 232.255.255.255 | This range is used for SSM applications. |
| 233.0.0.0 to 233.255.255.255 | This range is called the GLOP addressing. It is used for automatically allocating 256 multicast addresses to any enterprise that owns a registered ASN. |
| 239.0.0.0 to 239.255.255.255 | This range is used for private multicast domains. These addresses are called administratively scoped addresses. |
| Remaining ranges of addresses in the multicast address space | Addresses from these ranges are called transient groups. Any enterprise can allocate a multicast address from the transient groups for a global multicast application and should release it when the application is no longer in use. |

## 1.6.2 IGMP

IGMP is used by IP hosts to register their dynamic multicast group membership. It is also used by connected routers to discover these group members.

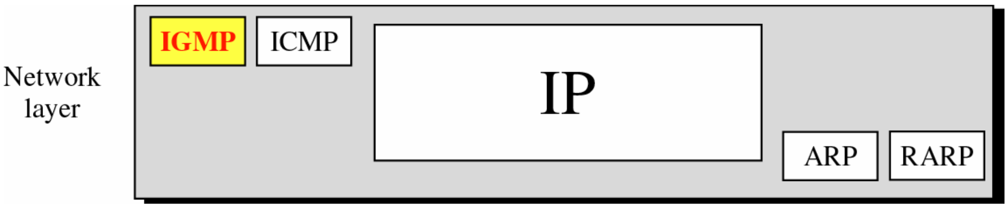


**Figure 8: IGMP**

IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications. IGMP is used on IPv4 networks. Multicast management on IPv6 networks is handled by Multicast Listener Discovery (MLD) which uses ICMPv6 messaging in contrast to IGMP's bare IP encapsulation.

**Architecture :**A network designed to deliver a multicast service using IGMP might use this basic architecture:

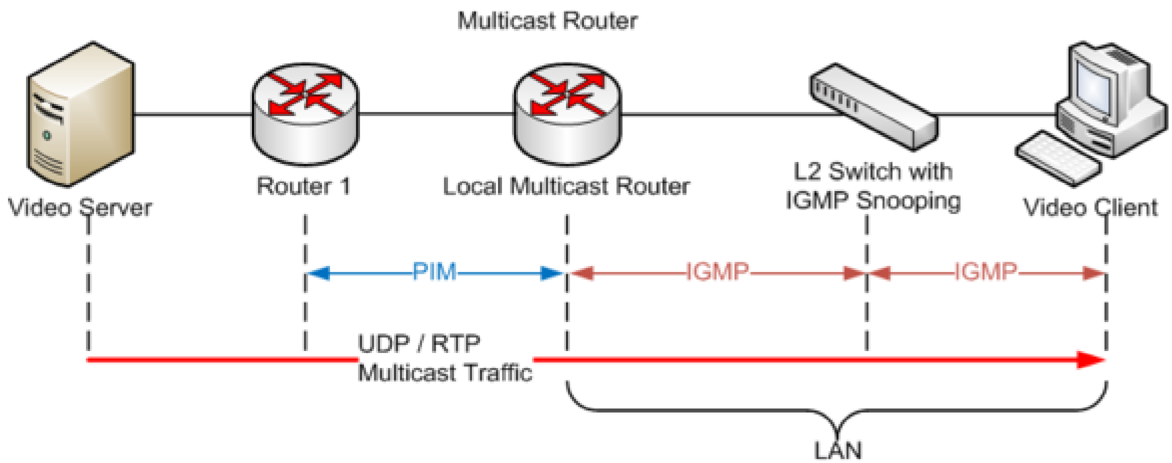


**Figure 9: Architecture used**

IGMP operates between the client computer and a local multicast router. Switches featuring IGMP snooping derive useful information by observing these IGMP transactions. Protocol Independent Multicast (PIM) is then used between the local and remote multicast routers, to direct multicast traffic from the multicast server to many multicast clients. IGMP operates on the network layer, just the same as other network management protocols like ICMP. The IGMP protocol is implemented on a particular host and within a router. A host requests membership to a group through its local router while a router listens for these requests and periodically sends out subscription queries. IGMP is vulnerable to some attacks, and firewalls commonly allow the user to disable it if not needed.

**Standards**

There are three versions of IGMP, as defined by Request for Comments (RFC) documents of the Internet Engineering Task Force (IETF). IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236 and IGMPv3 was initially defined by RFC 3376 and has been updated by RFC 4604 which defines both IGMPv3 and MLDv2. IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves over IGMPv2 mainly by supporting source-specific multicast [10]

**Packet Structure**

IGMP messages are carried in bare IP packets with IP protocol number 2.There is no transport layer used with IGMP messaging, similar to the Internet Control Message Protocol. There are several types of IGMP messages: Membership Queries (general and group-specific), Membership Reports, and Leave Group messages. Membership Queries are sent by multicast routers to determine which multicast addresses are of interest to systems attached to its network. Routers periodically send General Queries to refresh the group membership state for all systems on its network. Group-Specific Queries are used for determining the reception state for a particular multicast address. Group-and-Source-Specific Queries allow the router to determine if any systems desire reception of messages sent to a multicast group from a source address specified in a list of unicast addresses [11].

## 1.6.3 Multicast Routing Protocols

### 1.6.3.1 Source Based Tree

#### 1.6.3.1.1 MOSPF

MOSPF Multicast Open Shortest Path First (MOSPF) protocol is an extension of the OSPF protocol that uses multicast link state routing to create source-based trees. The protocol requires a new link state update packet to associate the unicast address of a host with the group address or addresses the host is sponsoring. This packet is called the group-membership LSA. In this way, we can include in the tree only the hosts (using their unicast addresses) that belong to a particular group. In other words, we make a tree that contains all the hosts belonging to a group, but we use the unicast address of the host in the calculation. For efficiency, the router calculates the shortest path trees on demand (when it receives the first multicast packet). In addition, the tree can be saved in cache memory for future use by the same source/group pair. MOSPF is a data-driven protocol; the first time an MOSPF router sees a datagram with a given source and group address, the router constructs the Dijkstra shortest path tree.

#### 1.6.3.1.2 DVMRP

In this section, we briefly discuss multicast distance vector routing and its implementation in the Internet, DVMRP. Multicast Distance Vector Routing Unicast distance vector routing is very simple; extending it to support multicast routing is complicated. Multicast routing does not allow a router to send its routing table to its neighbours. The idea is to create a table from scratch by using the information from the unicast distance vector tables.

Multicast distance vector routing uses source-based trees, but the router never actually makes a routing table. When a router receives a multicast packet, it forwards the packet as though it is consulting a routing table. We can say that the shortest path tree is evanescent. After its use (after a packet is forwarded) the table is destroyed. To accomplish this, the multicast distance vector algorithm uses a process based on four decision-making strategies. Each strategy is built on its predecessor. We explain them one by one and see how each strategy can improve the shortcomings of the previous one [13].

**Flooding**: Flooding is the first strategy that comes to mind. A router receives a packet and, without even looking at the destination group address, sends it out from every interlace except the one from which it was received. Flooding accomplishes the first goal of multicasting: every network with active members receives the packet. However, so will networks without active members. This is a broadcast, not a multicast. There is another problem: it creates loops. A packet that has left the router may come back again from another interlace or the same interlace and be forwarded again. Some flooding protocols keep a copy of the packet for a while and discard any duplicates to avoid loops. The next strategy, reverse path forwarding, corrects this defect [15].

**Reverse Path Forwarding (RPF)**: RPF is a modified flooding strategy. To prevent loops, only one copy is forwarded; the other copies are dropped. In RPF, a router forwards only the copy that has travelled the shortest path from the source to the router. To find this copy, RPF uses the unicast routing table. The router receives a packet and extracts the source address (a unicast address). It consults its unicast routing table as though it wants to send a packet to the source address. The routing table tells the router the next hop [9].

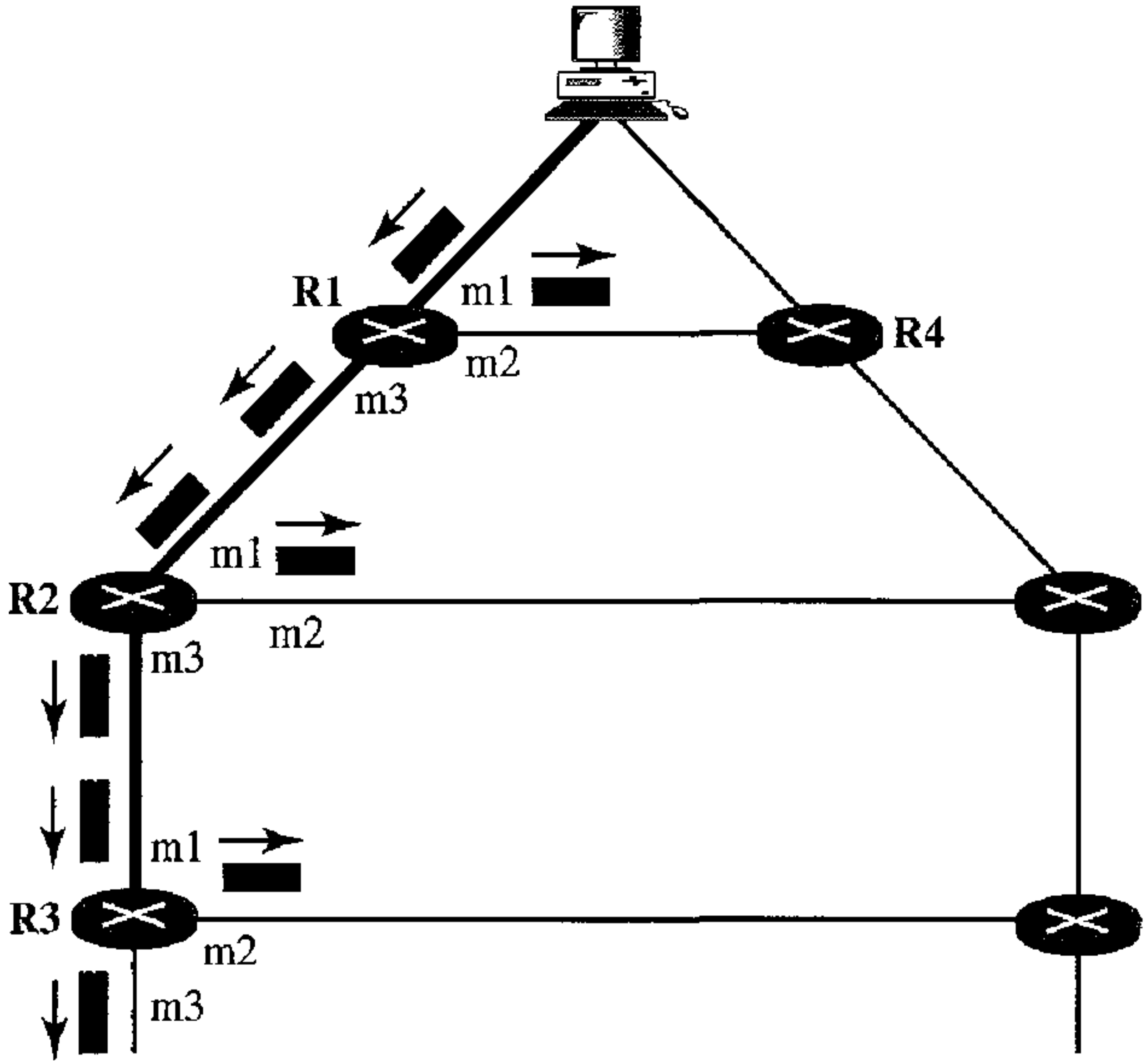


**Figure 10: RPF**

If the multicast packet has just come from the hop defined in the table, the packet has travelled the shortest path from the source to the router because the shortest path is reciprocal in unicast distance vector routing protocols. If the path from A to B is the shortest, then it is also the shortest from B to A. The router forwards the packet if it has travelled from the shortest path; it discards it otherwise. This strategy prevents loops because there is always one shortest path from the source to the router. If a packet leaves the router and comes back again, it has not travelled the shortest path. To make the point clear, let us look at Figure. Figure given shows part of a domain and a source. The shortest path tree as calculated by routers RI, R2, and R3 is shown by a thick line. When RI receives a packet from the source through the interface rnl, it consults its routing table and finds that the shortest path from RI to the source is through interface mI. The packet is forwarded. However, if a copy of the packet has arrived through interface m2, it is discarded because m2 does not define the shortest path from RI to the source. The story is the same with R2 and R3. You may wonder what happens if a copy of a packet that arrives at the ml interface of R3, travels through R6, R5, R2, and then enters R3 through interface ml. This interface is the correct interface for R3. Is the copy of the packet forwarded? The answer is that this scenario never happens because when the packet goes from R5 to R2, it will be discarded by R2 and never reaches R3. The upstream routers toward the source always discard a packet that has not gone through the shortest path, thus preventing confusion for the downstream routers [13].

**Reverse Path Broadcasting** (RPB): RPF guarantees that each network receives a copy of the multicast packet without formation of loops. However, RPF does not guarantee that each network receives only one copy; a network may receive two or more copies. The reason is that RPF is not based on the destination address (a group address); forwarding is based on the source address. To visualize the problem, let us look at Figure.Net3 in this figure receives two copies of the packet even though each router just sends out one copy from each interface. There is duplication because a tree has not been made; instead of a tree we have a graph. Net3 has two parents: routers R2 andR4. To eliminate duplication, we must define only one parent router for each network. We must have this restriction: A network can receive a multicast packet from a particularsource only through a designated parent router [15].

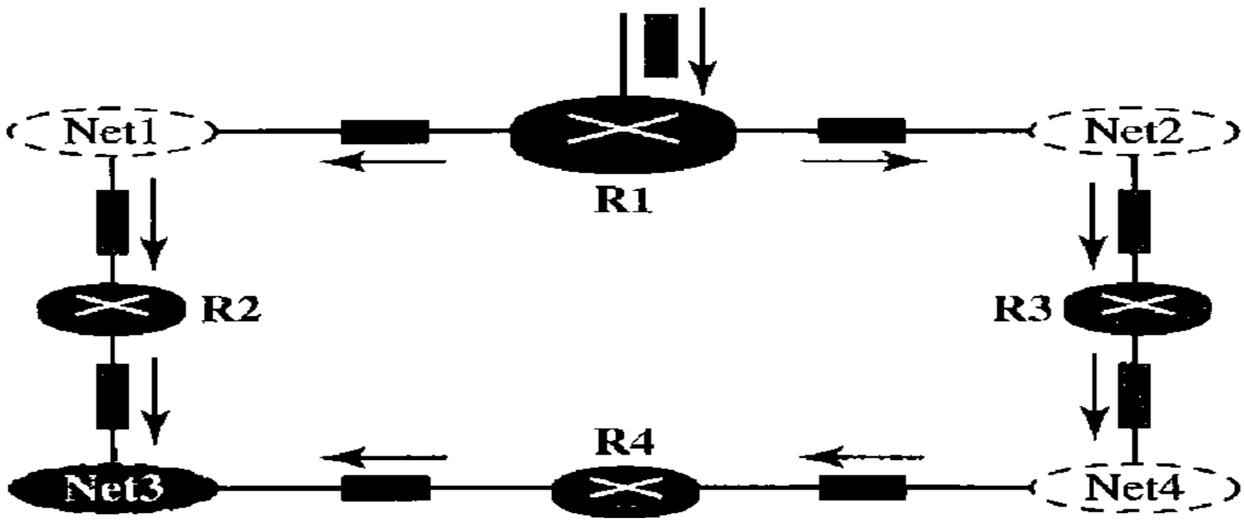


**Figure 11: RPB**

**Reverse Path Multicasting (RPM)**: As you may have noticed, RPB does not multicast the packet, it broadcasts it. This is not efficient. To increase efficiency, the multicast packet must reach only those networks that have active members for that particular group. This is called reverse path multicasting (RPM). To convert broadcasting to multicasting, the protocol uses two procedures, pruning and grafting.

### 1.6.3.1.3 PIM-DM

PIM-DM is a source-based tree routing protocol that uses RPF and pruning and grafting strategies for multicasting. Its operation is like that of DVMRP; however, unlike DVMRP, it does not depend on a specific unicasting protocol. It assumes that the autonomous system is using a unicast protocol and each router has a table that can find the outgoing interface that has an optimal path to a destination. This unicast protocol can be a distance vector protocol (RIP) or link state protocol (OSPF).

## 1.6.3.2 Group Based Tree

### 1.6.3.2.1 PIM-SM

PIM-SM is used when there is a slight possibility that each router is involved in multicasting (sparse mode). In this environment, the use of a protocol that broadcasts the packet is not justified; a protocol such as CBT that uses a group-shared tree is more appropriate. PIM-SM is used in a sparse multicast environment such as a WAN. PIM-SM is a group-shared tree routing protocol that has a rendezvous point (RP) as the source of the tree. Its operation is like CBT; however, it is simpler because it does not require acknowledgment from ajoin message. In addition, it creates a backup set of RPs for each region to cover RP failures. One of the characteristics of PIM-SM is that it can switch from a group-shared tree strategy to a source-based tree strategy when necessary. This can happen if there is a dense area of activity far from the RP. That area can be more efficiently handled with a source-based tree strategy instead of a group-shared tree strategy. PIM-SM is similar to CRT but uses a simpler procedure [13]

### 1.6.3.2.2 CBT

The Core-Based Tree (CBT) is a group-shared tree, center-based protocol using one tree per group. One of the routers in the tree is called the core. A packet is sent from the source to members of the group following this procedure:

1. The source, which may or may not be part of the tree, encapsulates the multicast packet inside a unicast packet with the unicast destination address of the core and sends it to the core. This part of delivery is done using a unicast address; the only recipient is the core router.

2. The core encapsulates the unicast packet and forwards it to all interested interfaces.

3. Each router that receives the multicast packet, in turn, forwards it to all interested interfaces.

# CHAPTER 2
# LITERATURE REVIEW

## Takashima.E [1]

In this paper, the author proposed a new method to construct a semi-optimal QoS-aware multicast tree on MANET using distributed computation of the tree based on genetic algorithm (GA). This tree is sub-optimal for a given objective (e.g., communication stability and power consumption), and satisfies given QoS constraints for bandwidth and delay. In order to increase scalability, our proposed method first divides the whole MANET to multiple clusters, and computes a tree for each cluster and a tree connecting all clusters. Each tree is computed by GA in some nodes selected in the corresponding cluster. Through experiments using network simulator, we confirmed that our method outperforms existing on-demand multicast routing protocol in some useful objectives.

## Gopalan, N.P[2]

Modern group communication based applications require multiple parameters to be considered for routing in a Cellular network. Traditional algorithms fail in the situations where these parameters frequently change due to the dynamism prevailing in the network. A new technique for topology discovery in these types of networks using ant colony optimization (ACO) has been proposed based on the restricted flooding principle. To provide a better quality of service in routing with multiple constraints, a genetic algorithm based routing has been proposed to find optimal routes within a shorter span of time than the traditional deterministic routing algorithms. Moreover, with the exponential growth in the number of mobile users, to enable a large number of users to participate in a group communication, a parallel genetic algorithm (GA) is proposed in this paper. Our simulation results show that the topology discovery using ant colony optimization is faster. The Call service rate using parallel genetic algorithm is more than that of sequential genetic algorithm and the Call blocking rate of parallel genetic algorithm is less than that of sequential genetic algorithm, for large number of routers in the network.

## Limin Tang[3]

Multicast transmission offers a bandwidth efficient solution for delivering media content to multiple destinations over the Internet. However, in many existing networks, some (if not all) nodes do notsupport multicast, i.e., they cannot create multiple outgoing flows with one incoming data flow. In this paper, the authors propose an algorithm for multicast tree computation in networks with multicast incapable nodes. Paths that originate at the source and traversing all destinations are computed first; if such paths cannot be found, destinations are partitioned into subsets and traverse paths are computed over each subset, which is executed recursively until feasible trees can be built based on traverse paths found or no further partition is possible. Two procedures for traverse path computation are presented and their respective advantages are discussed, in terms of both complexity and solution optimality. The algorithm is also shown to be very effective in finding multicast trees even if only a few multicast capable nodes exist in the network

## Xin Li[4]

Wireless sensor network is a revolution of information collection and perception field, which has been draw much more application gradually. However, The WSN with characteristic of self-organization, multi-hop, dynamic topology and limited energy resources, which make the network to prolong it's lifetime become extremely difficult. This paper analyzed variety multicast protocols in existence and the current achievements in the research based on a comprehensive studying of a mess of multicastrouting protocols. This document provided the appropriate application environment for types of multicast protocols and the specific improvements. It has an active significance for WSN to increase it's performance in the near future.

## Hee Sook Shin[5]

Providing multicast service to mobile hosts is difficult due to frequent changes of mobile host location and group membership. To overcome the difficulty, several multicast protocols for mobile hosts have been proposed. Although the protocols solve several problems inherent in multicast routing proposals for static hosts, they still have problems such as non-optimal delivery path, datagram duplication, etc. In this paper, we summarize these problems of multicast routing protocols and propose an efficient multicast protocol using a multicast agent in wireless mobile networks, where a mobile host receives a tunneled multicast datagram from a multicast agent located in a network close to it or directly from the multicast router in the current network. While receiving a tunneled multicast datagram from a remote multicast agent, the local multicast agent starts multicast join process, which makes the multicast delivery route optimal. The proposed protocol reduces data delivery path length and decreases not only the amount of duplicate copies of multicast datagram but also multicast traffic load. We examined and compared the performance of the proposed protocol and existing protocols by simulation under various environments and we got an improved performance over the existing proposals.

## Wan-Seon Lim[6]

The legacy multicasting over IEEE 802.11-based WLANs has two well-known problems-poor reliability and low-rate transmission. In the literature, various WLAN multicast protocols have been proposed in order to overcome these problems. Existing multicast protocols, however, are not so efficient when they are used combining with the frame aggregation scheme of IEEE 802.11n. In this paper, we propose a novel MAC-level multicast protocol for IEEE 802.11n, named Reliable and Efficient Multicast Protocol (REMP). To enhance the reliability and efficiency of multicast services in IEEE 802.11n WLANs, REMP enables selective retransmissions for erroneous multicast frames and efficient adjustments of the modulation and coding scheme (MCS). In addition, we propose an extension of REMP, named scalable REMP (S-REMP), for efficient delivery of scalable video over IEEE 802.11n WLANs. In S-REMP, different MCSs are assigned to different layers of scalable video to guarantee the minimal video quality to all users while providing a higher video quality to users exhibiting better channel conditions. Our simulation results show that REMP outperforms existing multicast protocols for normal multicast traffic and S-REMP offers improved performance for scalable video streaming.

## Shi[7]

The authors study the impact of congestion on the stability of a multicast (one-to-many) tree in the context of a cumulative layered multicast system. A stability factor is defined to evaluate and quantify this impact. To obtain the general expression of the stability factor, they develop a simple statistical model. They show that, even in the case of lower link-marking probability, a tree will become more stable when the dependency degree between different links increases. To the best of the authors' knowledge, this is the first work to quantify a multicast tree's stability with layered multicast congestion control. The modeling techniques they use are generic, and can be applied not only to analyze the stability of trees in layered multicast systems, but also to design general algorithms for both layered multicast and single-rate multicast congestion control.

### Ki-ll Kim[8]

The ASM (any source multicast) have been proposed to forward IP multicast datagram. However, there remain unsolved deployment issues such as network management and address allocation of multicast sessions. To overcome the above issues, largely new three multicast mechanisms-SGM (Small Group Multicast), ALM (Application Level Multicast) and SSM (Source Specific Multicast)-have been proposed. While the SGM and ALM can support multicast service without constructing the multicast routing tree, SSM constructs the multicast routing tree rooted in the source. SGM is proposed to support a very large number of small multicast groups. However, since SGM needs an additional packet header to service multicast, modification of the legacy routers is inevitable. ALM provides multicast by means of a combination of unicast in WAN and multicast in LAN. Since the standard is not fixed, this mechanism has limited implementation conditions. SSM identifies the multicast session not by G but by (S, G) pair. This mechanism solves the multicast address allocation problem, which is the biggest issue in the ASM. However, all routers along the delivery path must maintain the state (S, G) in order to transmit multicast data. Though the three new mechanisms can solve the many of the problems, one feature of ASM, the scalability problem is not be removed at all. We propose a fast deployment mechanism, which is based on SSM as well as the use the Internet hierarchical architecture. This mechanism may help multicast deployment without any modification of the IP layer while the advantage of SSM is kept. A key feature of the new mechanism is the use of a different multicast service for macro level multicast and micro level multicast.

# CHAPTER 3
# OBJECTIVE AND SCOPE OF THE STUDY

## 3.1 Objective

The objective of this research is to increase the success rate of finding the minimum cost path as we increase the number of destinations for any given source along with multicast incapable nodes. I will try to consider delay associated with each node and then will try to find the final minimum cost path with the help of algorithm proposed in order to increase the success rate for transmission of the packets from the considered transmitted to corresponding multiple receivers and correspondingly will compare the success rate obtained to the one obtained in the base paper.

## 3.2 Scope of the Study

Multicasting provides a very wide range of area to study about. There are different types of protocols that are used on daily basis for multicasting in real life situations. A complete range of (224.0.0.0 -239.255.255.255) address is reserved for multicasting purpose in the address ranges defined. The range defined above has its own categories within which different functions are performed in accordance with the specifications.

Multicast is repeatedly used in real life situations for different purposes. Multicasting is used whenever the user needs to send the message to a specified number of unique users. The basic examples of real life situations wherein we make use of multicast can be given are emailing some content over the internet, different subscriptions done by different users ,conference calls , conference chatting , distance learning etc. in all these situations its not really possible to broadcast the message or uni-multicast it because in such a case it will result in unnecessary use of the bandwidth available. So multicast is the ultimate option that remains.

Different types of algorithms and protocols are used when we deal with multicast. Different types of trees are used for same purpose. These trees can further be source based tree or group based tree. MOSPF, DVMPRP, PIM-DM ,PIM-SM are the most common examples of multicast protocols. All these protocols basically make a routing table at each router and further functions in order to obtain the shortest path. Thus multicast is really a very wide area with a lot of components within to study about.

# CHAPTER 4

# RESEARCH METHODOLOGY

## 4.1 Methodology

The basic algorithm used for computing the shortest path with varied number of sources and destinations with five iterations for each case can prominently be given as below.

The objective of this algorithm is to find multicast trees for a given multicast request in a given network. It is assumed that source of the multicast request can transmit to as many children as needed when computing multicast trees for the request.

### 4.1.1 Algorithm Proposed

The following notations are used:

s=Source
d=Destination
v=Set of vertices
V=All vertices within given network
N=Total number of neighbours for a given source
D=Distance between any two given nodes
$D_n$ = Minimum cost path
$D_g$ = Distance between source and neighbouring nodes
Q=Queue
$S_{new}$ =New source
$D_{new}$ =New destination

```
// initialization
dist[s]←0                    //(distance to  source vertex is zero)
repeat(s,d)
for all
{
v∈ V–{s}
do
for (j=1 to N)
{
if ( j is a neighbour of s and j ≠ s)
D_j = d_sj
```

If( j is not a neighbour of s )
D= $\infty$
}
} //Iterations

Mindistance (Q,dist)
for(j=1 to N)
{
if $D_n$ < all $D_g$
dist= $D_n$
}
Return dist

S←0 // (S, the set of visited vertices is initially empty)
Q←V // (Q, the queue initially contains all vertices)

while
Q≠0 // (while the queue is not empty)
Do u ← mindistance(Q,dist) // (select the element of Q with the min. distance)
Repeat
{
path=path $\cup$ n //(where $D_n$ is minimum cost path)
}
For (k=1 to M) // M=No. of remaining nodes
{
$D_k = \min(D_k , D_k + C_{jk})$
}(until all nodes included in the path,M=0)

put
$s_{new} = d_{new-1}$
repeat( $s_{new}, d_{new-1}$ ) //till all the destinations are covered
end

### 4.1.2 Delay and Cost Effective Bandwidth Introduction:

Along with the algorithm proposed above I have also tried to introduce appropriate delay and bandwidth with each given node in order to increase the success rate of finding minimum cost path for a given source and the random provided destinations in the given multicast network.

# CHAPTER 5

# RESULTS AND DISCUSSIONS

In my base paper ,the authors have proposed an algorithm to calculate success rate for finding the minimum cost path with increase in number of destinations while multicasting from a given source to various destinations neither having introduction to delay mechanism nor the proper bandwidth considerations. Different types of algorithms were proposed regarding the same mechanism used according to requirements of user.

## 5.1 Shortest path calculation using the constraints proposed in considered paper :

Different networks were considered for the purpose of calculating success rate

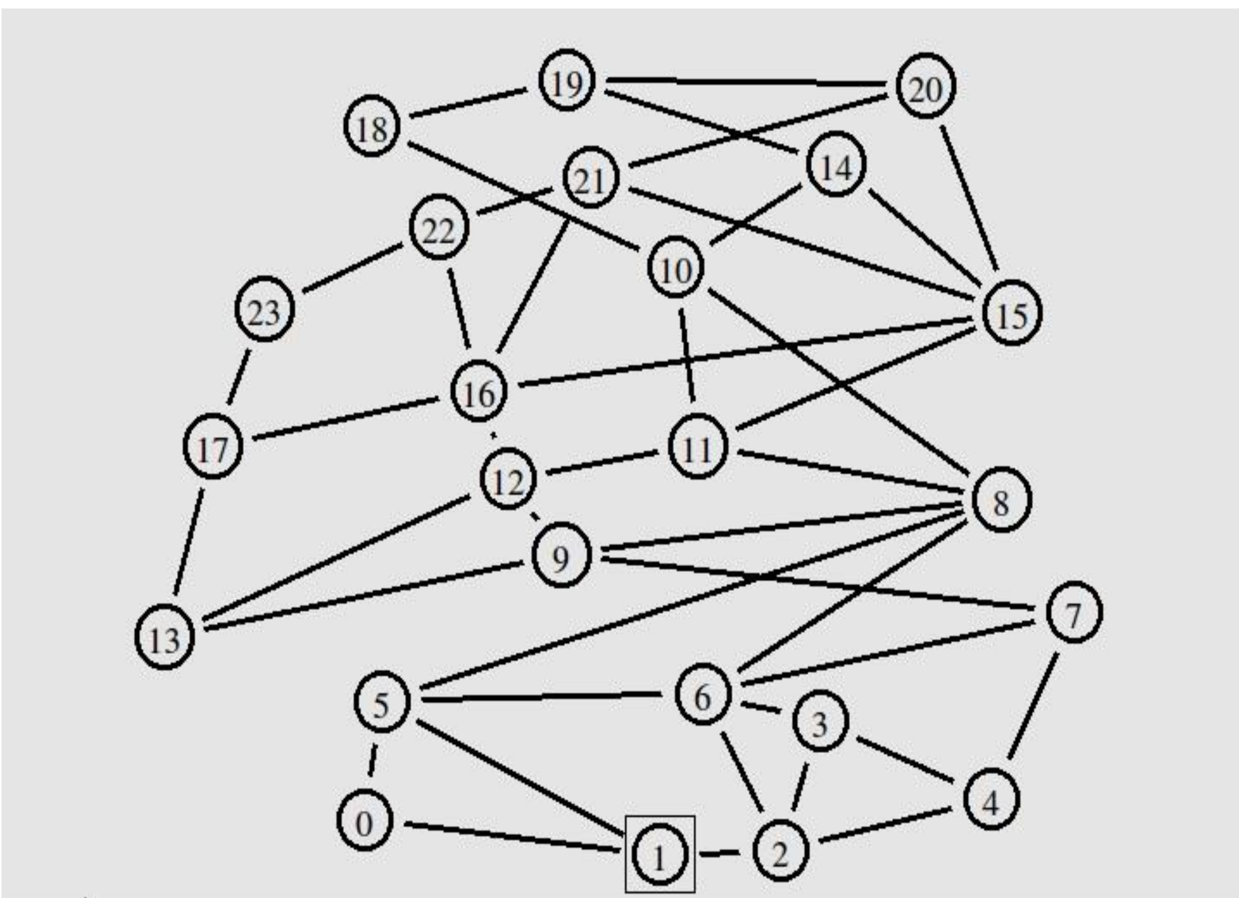


**Figure 12: Network 1**

Given network 1 is the first network that was considered in order to calculate the success rate.

In the network considered above 21 nodes are taken within which some nodes are multicast incapable nodes while others are multicast capable nodes .consideration of multicast incapable nodes helps to deal with real life situation because all the nodes or the router in real life situation are not multicast capable.

The graph obtained for success rate of the network above can be given as:

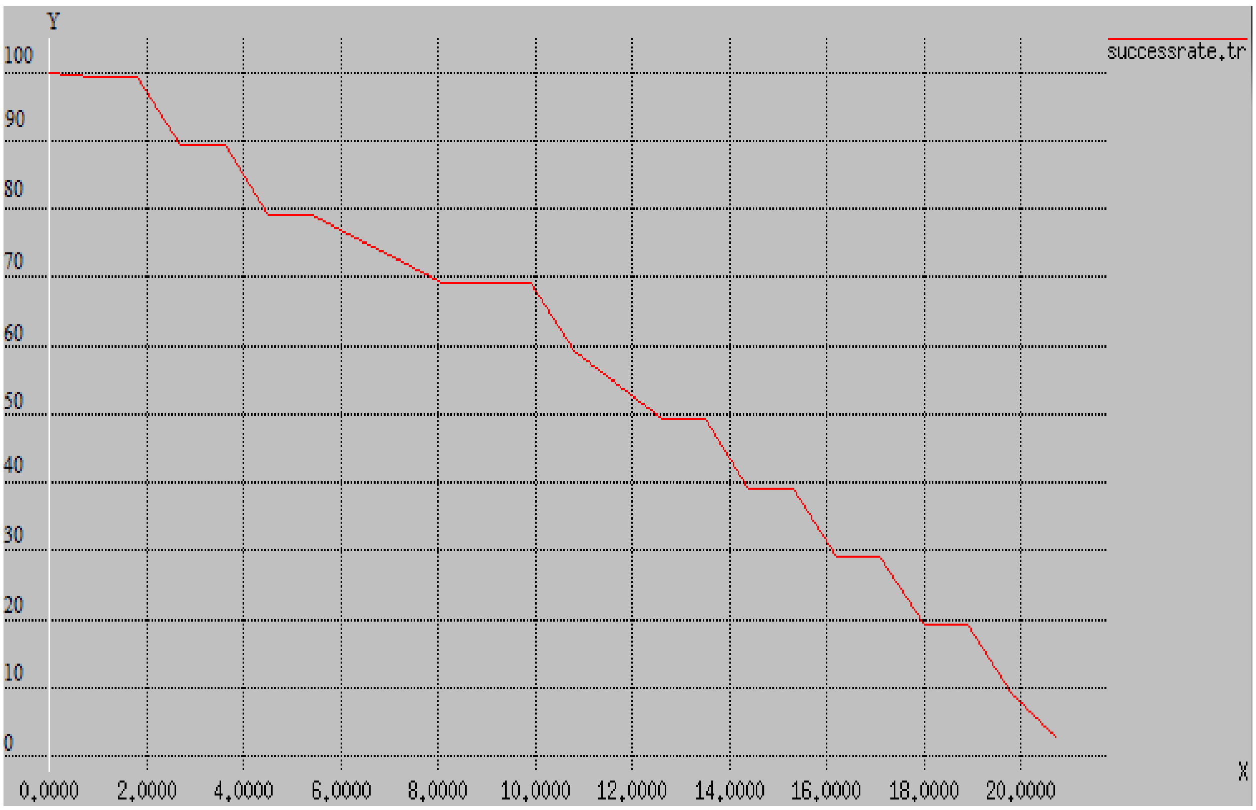


**Figure 13 : Success rate for network 1**

where

y-axis -> percentage success rate of finding minimum cost path.

x-axis-> No. of destinations for a particular source

From the graph above it can be concluded that success rate for finding the minimum cost path decreases with increase in number of destinations for any given source. This concept will get crystal clear with the help of data analysis of the graphic values in tabular form as given on the next page.

If we analyze the result in tabular form then it can be given as on the next page.

**Table 6: Tabular analysis for success rate of network 1**

| Number of destinations | Success rate |
|---|---|
| 2 | 100 |
| 4 | 85 |
| 6 | 76 |
| 8 | 70 |
| 10 | 70 |
| 12 | 54 |
| 14 | 45 |
| 16 | 30 |
| 18 | 20 |
| 20 | 9 |

The tabular analysis strengthens the concept discussed above.

Correspondingly, the average number of trees found per request can be given by the graph below:

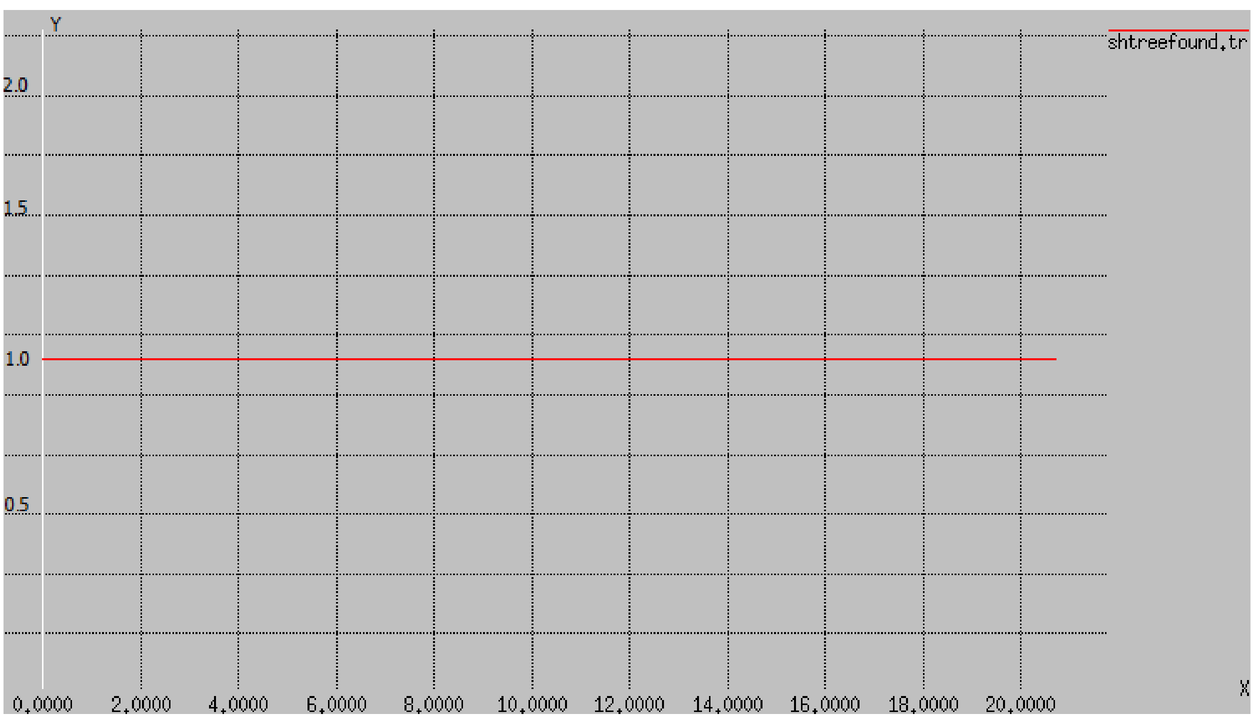


**Figure 14. Average number of trees found for network 1**

Where

y-axis-> Average no. of trees found per request.

x-axis-> No. of destinations for any given source

The second network that was considered can be given as:

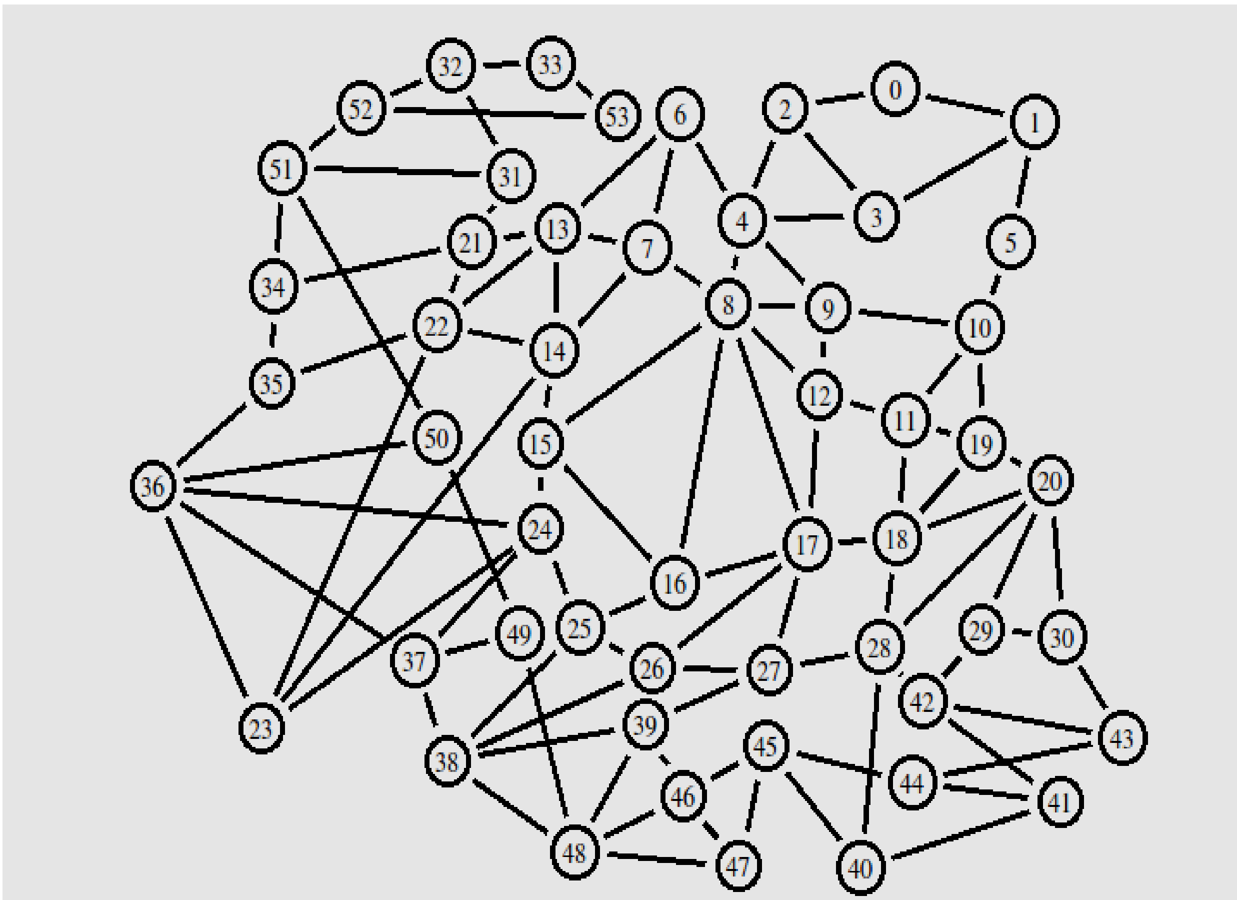


**Figure 15. Network 2**

Given network 2 is the second network that was considered in order to calculate the success rate. In the network considered above 53 nodes are taken within which some nodes are multicast incapable nodes while others are multicast capable nodes .consideration of multicast incapable nodes helps to deal with real life situation because all the nodes or the router in real life situation are not multicast capable.

Now we need to analyze the success rate in the network considered above for finding the minimum cost path with increase in number of destination

The graph obtained for the network 2 can be given as below

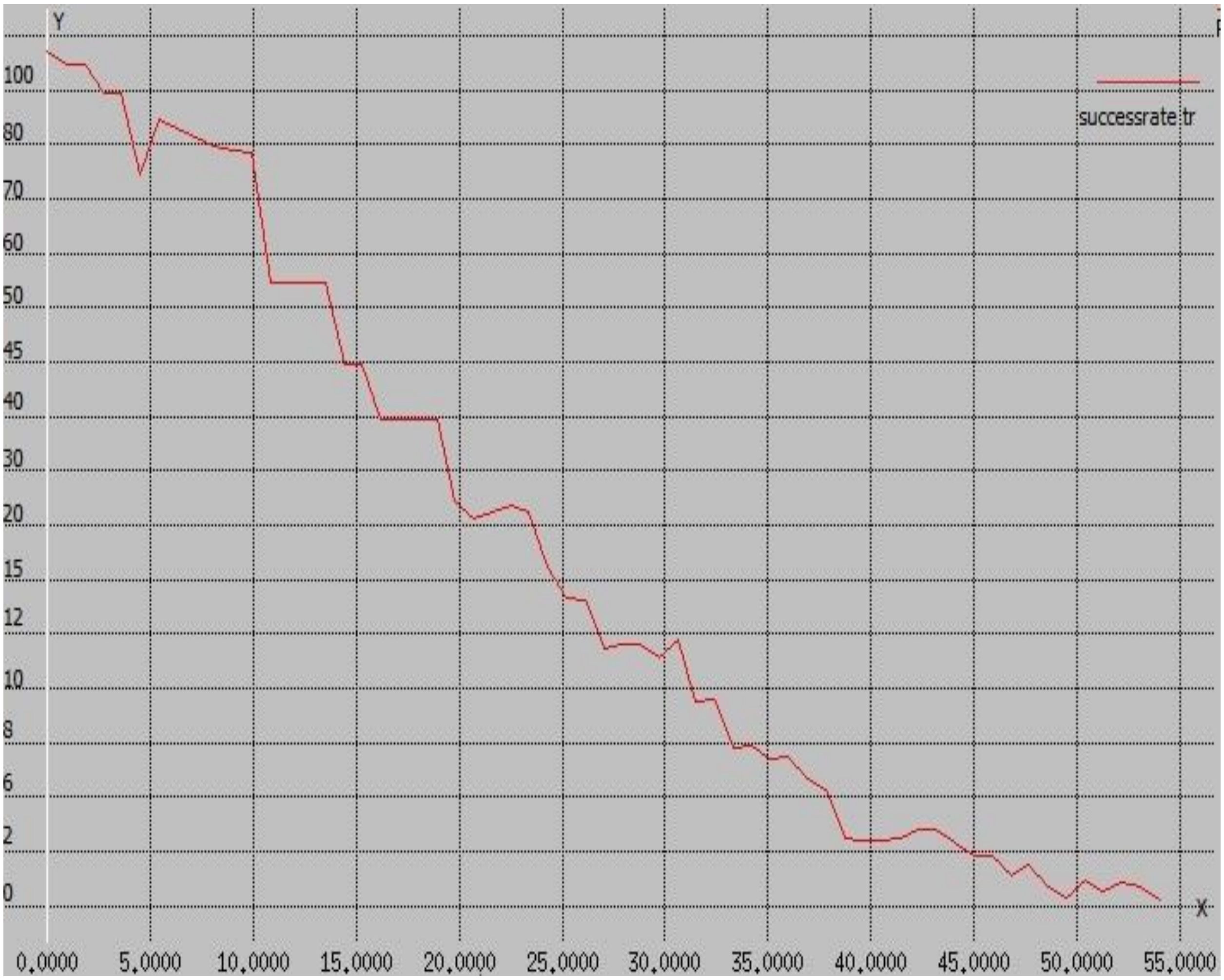


**Figure 16. Success rate for network 2**

Where:

y-axis -> percentage success rate of finding minimum cost path.

x-axis-> No. of destinations for a particular source

From the graph above it can be concluded that success rate for finding the minimum cost path decreases with increase in number of destinations for any given source. This concept will get crystal clear with the help of data analysis of the graphic values in tabular form as given below.

The tabular analysis of graph above can be given as:

**Table 7. Tabular analysis for success rate of network 2**

| No. of destinations | Success rate |
|---|---|
| 5 | 81 |
| 10 | 76 |
| 15 | 45 |
| 20 | 22 |
| 25 | 14 |
| 30 | 12 |
| 35 | 7 |
| 40 | 4 |
| 45 | 2 |
| 50 | 2 |

The tabular analysis strengthens the concept of decrease in number of shortest path found with increase in number of destinations.

Correspondingly, the average number of trees found per request can be given by the graph below:

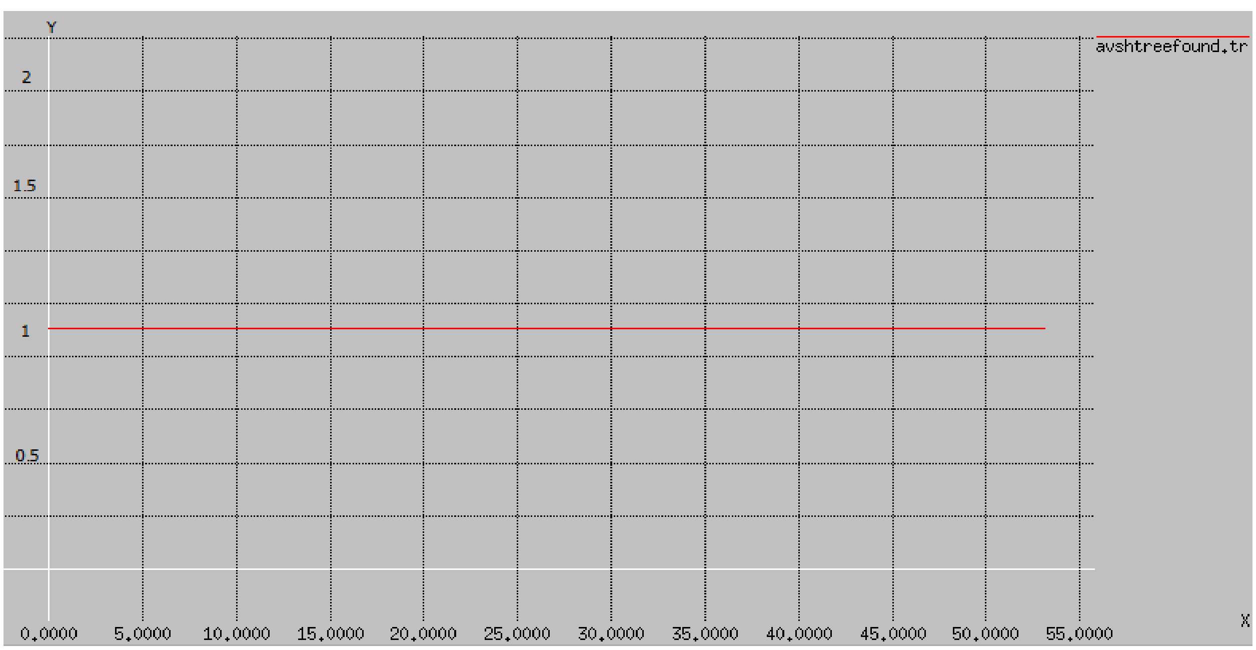


**Figure 17. Average number of trees found for network 2**

## 5.2 Shortest Path Calculation using the Algorithm Proposed

For my research work I have considered the network given below. I have considered 80 nodes within the network. Some of these nodes are multicast capable nodes while other one's are multicast incapable nodes. Consideration of both types of nodes within the network helps to make it more tangible to real life situations. Along with all these considerations I have introduced delay and appropriate bandwidth with each node in order to increase the success rate of finding minimum cost path from source to destination while numbers of destination for each source is continuously increased in order to study the phenomenon properly.

Network considered can be given as:

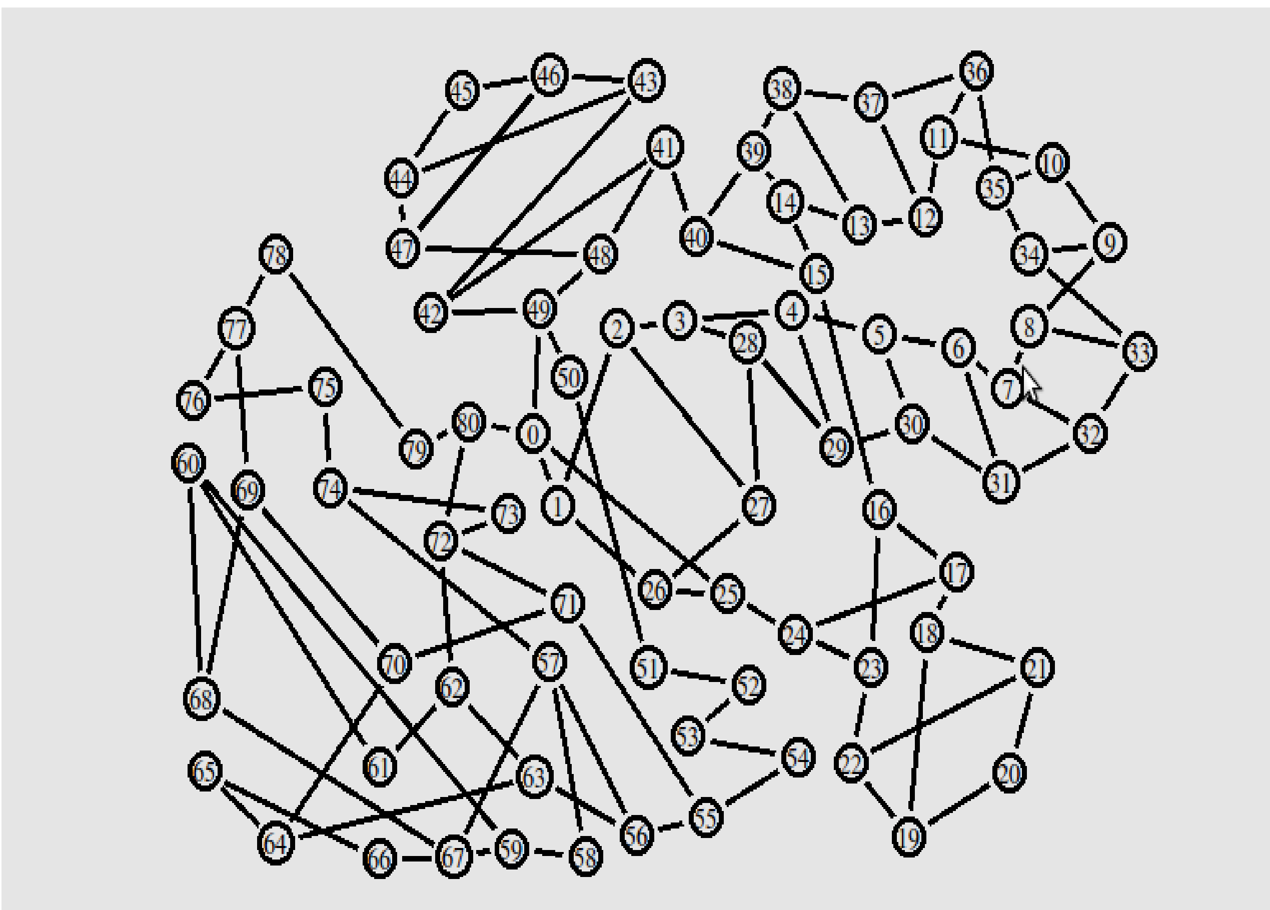


**Figure 18. Network 3**

Now, the graph obtained for success rate of packet transmission with minimum path calculation can be given as given on the next page. Along with the graph I have considered the tabular analysis as well in order to make result more easier to understand and to make it more esy to compare the values obtained from different graphs.

In the graph below variable deined can be given as:

y-axis -> percentage success rate of finding minimum cost path.

x-axis-> No. of destinations for a particular source

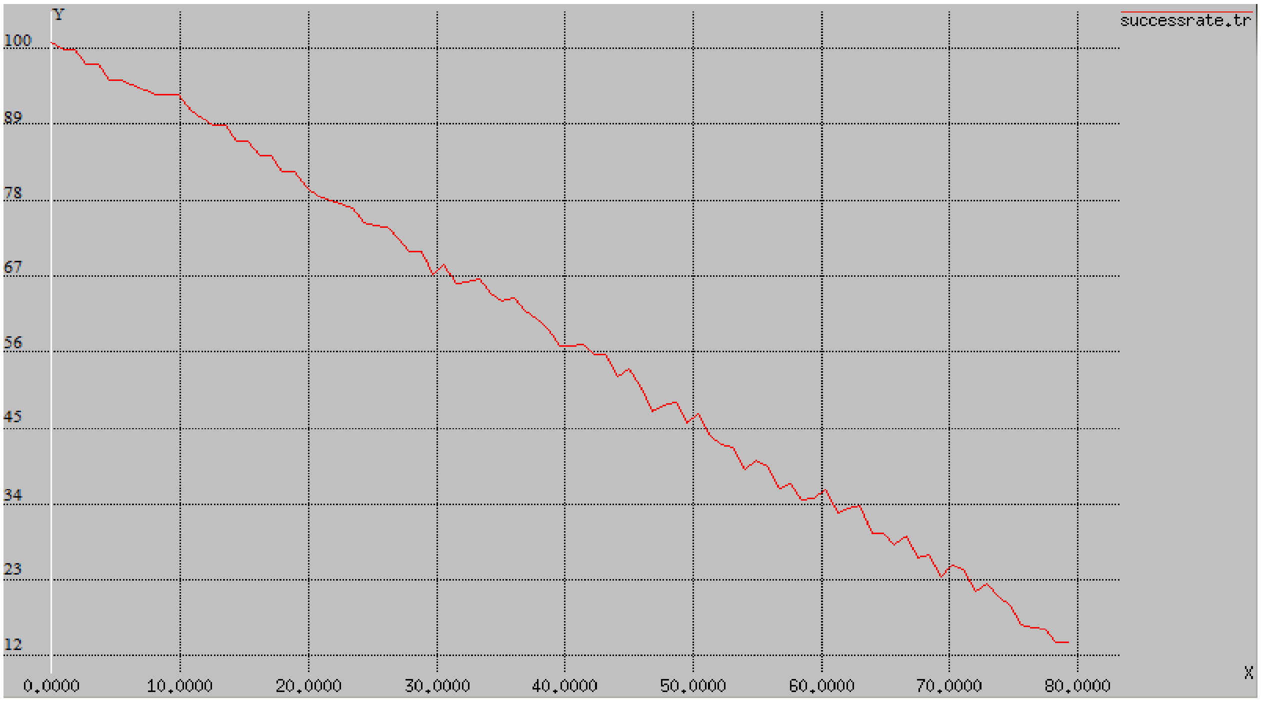


**Figure 19.Success rate for network 3**

The tabular analysis of the graph can be given as

**Table 8. Tabular analysis for success rate of network 3**

| No. of destinations | Success rate |
|---|---|
| 10 | 93 |
| 20 | 80 |
| 30 | 69 |
| 40 | 57 |
| 50 | 46 |
| 60 | 36 |
| 70 | 25 |
| 80 | 13 |

The graph for average number of minimum trees found per request can be given as:

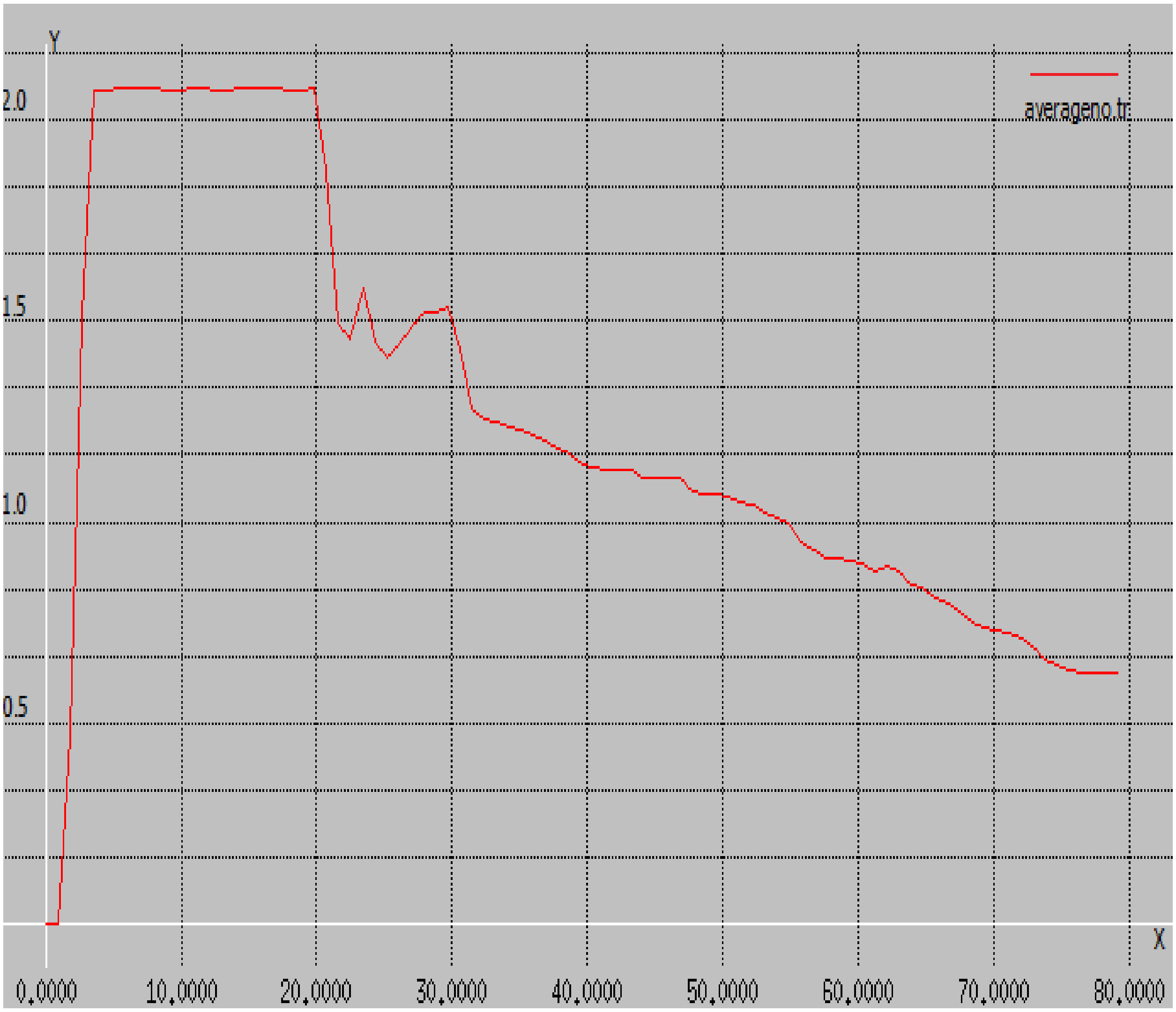


**Figure 20. Average number of trees found for network 3**

From the analysis done above it is pretty much clear that if we make use of the algorithm proposed the success rate of finding minimum cost path in a network with both multicast capable nodes and multicast incapable nodes can be increased significantly.

The tabular representation makes the improvement crystal clear which is basically because of delay association with each node along with proper bandwidth consideration within the algorithm proposed to calculate the shortest path.

## 5.3 Comparative Analysis and Improvement Obtained

Improvement using the proposed algorithm over the one proposed in base paper

**Table 9. Comparative analysis**

| No. of destinations | Network 1 | Network 2 | Network 3 |
|---|---|---|---|
| 10 | 70 | 76 | 93 |
| 20 | 8 | 20 | 80 |
| 30 | - | 12 | 69 |
| 40 | - | 4 | 57 |
| 50 | - | 2 | 46 |
| 60 | - | - | 36 |
| 70 | - | - | 25 |
| 80 | - | - | 13 |

# CHAPTER 6
# CONCLUSION AND FUTURE SCOPE

## 6.1 Conclusion

After studying every aspect of the thesis proposed it becomes pretty clear that if we make use of the proposed algorithm in any network having multicast capable and multicast incapable nodes in accordance with real life situations along with delay associated nodes and appropriate bandwidth then it becomes possible to increase the success rate up to a considerable value.

In my base paper ,the authors had proposed an algorithm to calculate success rate for finding the minimum cost path with increase in number of destinations while multicasting from a given source to various destinations neither having introduction to delay mechanism nor the proper bandwidth considerations. Different types of algorithms were proposed regarding the same mechanism used according to requirements of user.

There were scopes of improvement basically and by making those improvements the proposed thesis tries to improve the success rate for finding the minimum cost path.

## 6.2 Future Scope

The result obtained can further be improved if we make use of application layer multicast instead of network layer multicast. Application layer multicast is not that much popular now a days but that is where the future lies. Following are the advantages if we make use of application layer multicast instead of network layer multicast:

- **Quality of the data delivery path**

  The quality of the tree delivery path increases if we make use of application layer multicast instead of network layer multicast

- **Robustness of the overlay**

  Since end-hosts are reportedly less stable than the routers in between, it is important for application-layer multicast protocols to remove the effects of the receiver failures. The robustness of the application-layer multicast protocols can be measured by the value of the disruption in message delivery when different nodes fail, and the time it takes for the protocol to restore the delivery to the other users.

- **Control Overhead**

  For efficient use of the network resources, the control overhead at the users should be low. This is an important aspect to study the scalability of the scheme to large user groups. Application layer overlay networks which are built on top of the physical network, behave like an independent virtual network consist up of only logical links between the nodes.

# REFERENCES

[1] Takashima, E.," A Method for Distributed Computation of Semi-Optimal Multicast Tree in MANET**",** Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE

[2] Gopalan.N.P," Group Communication in Mobile Networks using Optimization Techniques", Ad Hoc and Ubiquitous Computing, 2006. ISAUHC '06. International Symposium on

[3] Limin Tang," Multicast tree computation in networks with multicast incapable nodes" High Performance Switching and Routing (HPSR), 2011 IEEE 12th International Conference on

[4] Xin Li," Research on Multicast Routing Protocol in Wireless Sensor Network" Control, Automation and Systems Engineering (CASE), 2011 International Conference on

[5] Hee Sook Shin," Multicast routing protocol by multicast agent in mobile networks", Parallel Processing, 2000. Proceedings. 2000 International Conference on

[6] Wan-Seon Lim," Design of Efficient Multicast Protocol for IEEE 802.11n WLANs and Cross-Layer Optimization for Scalable Video Streaming", mobile computing,IEEE transaction.

[7] Shi," Impact of congestion on the stability of a multicast tree in cumulative layered multicast",communications,IEE proceedings

[8] Ki-ll Kim," Internet multicast provisioning issues for hierarchical architecture" Networks, 2001. Proceedings. Ninth IEEE International Conference on

[9] Behrouz.A. Forouzan,"Data communications and networking"

[10] "Cisco Visual Networking Index: Forecast and Methodology, 2009- 014," "http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white paper c11-481360 ns827 Networking Solutions White Paper.html", Cisco Inc., 2010.

[11] L. Tang, W. Huang, M. Razo, A. Sivasankaran, P. Monti, M. Tacca, and A. Fumagalli, "Computing Alternate Multicast Trees with Maximum Latency Guarantee," 11th International Conference on High Performance Switching and Routing, 2010.

[12] J. Jannotti, D. K. Gifford, K. L. Johnson, M. F. Kaashoek, and J. W. O'Toole, Jr., "Overcast: Reliable Multicasting with an Overlay Network," in Proceedings of the 4th conference on Symposium on Operating System Design & Implementation - Volume 4, 2000.

[13] "Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)," "http://tools.ietf.org/html/rfc4875", IETF, 2007.

[14] X. Zhang, J. Y. Wei, and C. Qiao, "Constrained Multicast Routing in WDM Networks with Sparse Light Splitting," Journal of Lightwave Technology, 2000.

[15] G. Gutin, A. Yeo, and A. Zverovich, "Traveling Salesman Should not be Greedy: Domination Analysis of Greedy-Type Heuristics for the TSP," Discrete Applied Mathematics, 2002.