ISSN:0975-9646

A Comprehensive Study of Multicast based Routing Protocols in Wired Networks(LAN)

Alok Sahu[#1], Dr. Bharat Mishra[*2]

[#]*Faculty of Physical Science and Environment, M.G.C.G.V Chitrakoot, Satna M.P.*

[*]*Associate Professor, Faculty of Physical Science and Environment, M.G.C.G.V Chitrakoot, Satna M.P.*

Abstract: As network grows in size and complexity, network management has become an increasingly challenging task in multicast routing. "Routing is acts moving information across an interconnected LAN from Source to a destination". Probability that a LAN groups consists of a large number of nodes and likelihood of an interest in connection to other groups with similar interest, the management of the routes between different routing protocols could be quit complex. Routing of data in a LAN is a challenging task due to the changing topology of such a network. In this paper we analyze different Multicast Routing Protocols and their strategies on the basis of type and sub type and implemented model. Multicast routing is a group oriented communication whose objective is to support the propagation of data from a sender to all the receivers of a multicast group while trying to use the available bandwidth efficiently, it also reduces the communication cost and saves the network resources. We proposed, multicast routing protocols in wired networks that was proposed in recent years has been covered and made a comprehensive study on existing multicast routing protocols.

Keywords: Multicast routing protocols, Source based Tree, Core Based Tree, and Border Gateway Multicast Protocol

1. INTRODUCTION

Network management is the continuous process of monitoring a network to detect and diagnose problems, and of configuring protocols and mechanism in different types of computer network flows. A multicast is designed to enable the delivery of datagram's to a set of hosts that have been configured as members of a multicast group in various scattered sub-networks. Multicasting is not connection oriented. A multicast datagram is delivered to destination group members with the same "best-effort" reliability as a standard unicast datagram. This means that a multicast datagram is not guaranteed to reach all members of the group, or arrive in the same order relative to the transmission of other packets. Wired Network is a common type of wired configuration which uses physical cables to transfer data between different devices and computer systems. Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology [2]. In recent times with the prosperity of peer-to-peer (P2P) networking, researchers have proposed alternative solutions to bypass the limitations. The solution is overlay multicast, also called end system multicast or application level multicast, which shifts multicast support from core routers to end systems Conversely security issues in overlay multicast have received relatively little attention so far. Previous work on overlay network security either investigates the impact of selfish cheating nodes on the performance of overlay multicast trees, or investigates schemes that improve the fault tolerance or denial of service (DoS) resilience of overlay networks by introducing path redundancy.[1]

2. ISSUES IN DESIGNING A MULTICAST ROUTING PROTOCOL

Limited bandwidth availability, an error-prone shared broadcast channel, the LAN of nodes with limited energy resources, the hidden terminal problem, and limited security make the design of a multicast routing protocol for ad hoc networks a challenging one. There are several issues involved:

Robustness: Due to the mobility of the nodes, link failures are quite common in LAN. Thus, data packets sent by the source may be dropped, which results in a low packet delivery ratio. Hence, a multicast routing protocol should be robust enough to sustain the networks of the nodes and achieve a high packet delivery ratio.

Efficiency: In a LAN network environment, where the bandwidth is scarce, the efficiency of the multicast protocol is very important. Multicast efficiency is defined as the ratio of the total number of data packets received by the receivers to the total number of (data and control) packets transmitted in the network.

Control overhead: In order to keep track of the members in a multicast group, the exchange of control packets is required. This consumes a considerable amount of bandwidth. Since bandwidth is limited in ad hoc networks, the design of a multicast protocol should ensure that the total number of control packets transmitted for maintaining the multicast group is kept to a minimum.

Quality of service: One of the important applications of LAN Networks applications. Hence, provisioning quality of service (QoS) is an issue in ad hoc multicast routing protocols. The main parameters which are taken into consideration for providing the required QoS are throughput, delay and reliability.

Dependency on the unicast routing protocol: If a multicast routing protocol needs the support of a particular routing protocol, then it is difficult for the multicast protocol to work in heterogeneous networks. Hence, it is desirable if the multicast routing protocol is independent of any specific unicast routing protocol.

Resource management: A multicast routing protocol should use minimum power by reducing the number of packet transmissions. To reduce memory usage, it should use minimum state information.

3. MULTICAST ROUTING PROTOCOLS

Multicast routing protocols for wire networks can be broadly classified into two types: application-independent/generic multicast protocols and application-dependent multicast protocols. While application-independent multicast protocols are used for conventional multicasting, application-dependent multicast protocols are meant only for specific applications for which they are designed. Application-independent multicast protocols can be classified along different dimensions as shown in figure (1).

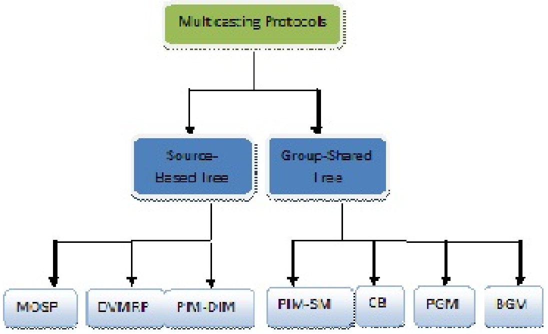

Figure1: Testimony of Multicasting Protocols

3.1`Source Based Tree: In this each router needs to have one shortest path tree for each group. It constructs a separate tree for each source, using the least cost paths between the source and the members. The shortest path tree for a group defines the next hop for each network that has loyal members for that group as shown in figure(2,3).

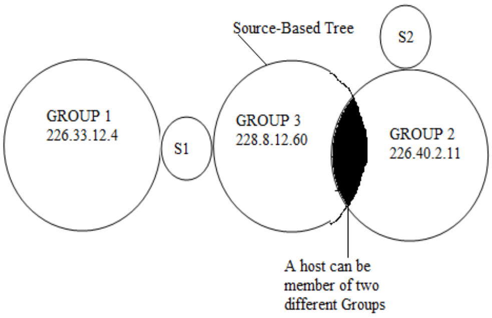

Figure 2: Source-Based Tree Hosts in Groups

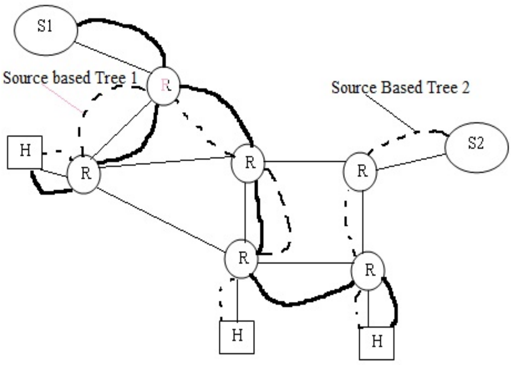

Figure 3: Data Relay on Source-Based Tree protocols

3.2.Group shared tree: In the group shared tree approach, instead of each route having m shortest path trees, only one designated router, called the centre core, a rendezvous router, takes the responsibility of distributing multicast traffic. The core has multicast shortest path trees in its routing table. The rest of the routers in the domain have none. If a router receives a multicast packet, it encapsulates the packet in a unicast packet and sends it to the core router. The core router removes the multicast packet from its capsule, and consults its routing table to route the packet as shown in figure (4) with Rendezvous Routers.

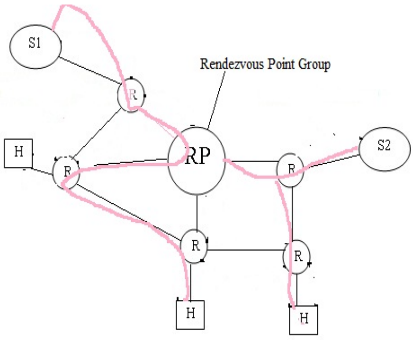

Figure 4: Data Relay on Source-Based Tree protocols with Rendezvous Routers.

4. DIFFERENT MULTICAST ROUTING PROTOCOLS

4.1 Distance Vector Multicast Routing Protocol (DVMRP):-The distance vector multicast routing protocol is an implementation of multicast distance vector routing. DVMRP builds a multicast tree for each source and destination host group. It implements the Reverse Path Multicasting (RPM) algorithm. It is a source based routing protocol, based on RIP, but the router never actually makes a routing table but it uses unicast routing protocol for this purpose. When a router receives a multicast packet it forwards it. DVMRP uses a Broadcast & Prune mechanism. That is, a broadcast tree is build from a source by exchanging routing information. Then this broadcast tree is changed to multicast tree by using pruning technique. More specifically, initially multicast datagram's are delivered to all nodes on the tree. Those leaves that do not have any group members send prune messages to the upstream router, noting the absence of a group. The upstream router maintains a prune state for this group for the given sender. A prune state is aged out after a given configurable interval, allowing multicasts to resume. Pruned branches are restored to a multicast tree by sending graft messages towards the upstream router. Graft messages start at the leaf node and travel up the tree, first sending the message to its neighbor upstream router. It works on broadcasting, pruning and grafting process.

4.2 Protocol Independent Multicast-Dense Mode (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 or link state protocol.

It is envisioned that PIMDM will be deployed in resource rich environments, such as a campus LAN where group membership is relatively dense and bandwidth is readily available. PIM DM protocol works in two phases:

In the first phase, the whole network is flooded with multicast data and this is done by propagation of packet on all interfaces except on upstream interface. This phase is highly inefficient because it leads to excessive network resource usage because of its network flooding technique.

In the second phase, called a prune phase, cuts out unnecessary branches by means of a Prune massage. A network device, after reception of a Prune packet, terminates further forwarding of multicast traffic on this interface and the interface is set to be in prune state.

There is one important message that is periodically exchanged between PIM DM routers are Hello packets. It helps routers learn about the presence of PIM DM capable neighbor routers in the network[10];

4.3 Multicast open shortest path first (MOSPF)

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 (link state advertisements). This LSA makes it possible to identify the location of each group member. In this way, we can include in the tree only the hosts 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. In addition, the tree can be saved in cache memory for future use by the same source/group pair. MOSPF is data driven protocol; the first time an MOSPF router sees a data-gram with a given source and group address, the router constructs the Dijkstra shortest path tree. MOSPF routers maintain a current image of the network topology through the unicast OSPF link state routing protocol. [8]

4.4 Core Based Tree (CBT)

The Latest addition to the existing set of multicast forwarding algorithm is Core Based Tree. It constructs a single delivery tree that is shared by all members of group. The CBT algorithm is quit similar to the spanning tree algorithm expect it allows a different core-based tree for each group. Multicast traffic for each group is sent and received over the same delivery tree, regardless of the source.

A core-based tree may involve a single router of set of routers, which acts as the core of a multicast delivery tree. Figure-5 illustrates how multicast traffic is forwarded across a CBT "backbone" to all members of group. Note that the CBT backbone contain both core and non-core routers.

Each station that wishes to receive traffic that has been addressed to a multicast group is required to send a "join" message forwarded the "core tree" of the particular multicast group. A potential group member only needs to know the address of one of the group's core router in order to transmit a unicast join group. The join request is processed by all intermediate routers that identify the interface on which the join has received as belonging to the group's delivery tree. The intermediate routers continue to forward the join message towards the core and marking local interfaces until the request reaches a core router as shown in figure(5).

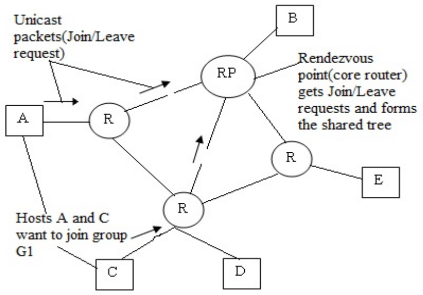
Unicast packets(Join/Leave request)
B
RP
Rendezvous point(core router) gets Join/Leave requests and forms the shared tree
A
R
R
E
R
Hosts A and C want to join group G1
C
D

Figure 5: Packets Relay on CBT with Rendezvous Routers.

4.5 Protocol Independent Multicast Sparse Mode (PIM-SM)

PIM-SM is a group shared tree routing protocol that has a rendezvous point (RP) as the source of the tree and operation is like CBT. In addition, it creates a backup set of RPs for each region to cover RP failures. PIM-SM creates and maintains unidirectional multicast trees based on explicit Join/Prune protocol messages. It is designed to support sparse groups. PIM-SM creates a shared, RP routed distribution tree that reaches all group members and it authorizes the receivers to switch from a RP (Rendezvous Point) routed tree (RPT) to a shortest path tree (SPT). It works in following phases:

The phase one of the protocol formulates a distribution tree for multicast. The receiver designates one local router as a Designated Router (DR) for its contained subnet. All the DR's sent JOIN messages [in form of (Sn, G)here S- Source Based Tree and n -constant number] towards the RP for Multicast transmissions. When many receivers join the group, their join messages converge at the Performing a distribution tree. This is called as RP tree (RPT) and is a shared tree as it is shared by all the sources sending to the group. The Multicast sender sent the multicast data to the group through the DR. The DR Unicast encapsulates the data and sends them to the RP. [10]This process is called Registering. The encapsulated packets are called PIM Register Packets. RP encapsulated the data and forwards them to the intended shared tree and replicates wherever the RP Tree branches, and eventually reaching all the receivers for that multicast group [5].

The second phase of PIM-SM operation is the Register STOP operation. Encapsulation and encapsulation process at the router may be expensive. Hence when the RP receives a register encapsulated data packet from source S on group G, it will normally initiate an (S, G) source specific Join towards S and RP will switch to native forwarding. Eventually the messages reach the subnet S and the packets flow towards the RP. While RP is in the process of joining source specific packets, data

Packets continue to encapsulate to RP. Thus RP receives packets forwarded natively from S as well as encapsulated packets. RP now begins to discard the encapsulated copy of the packets and sends a Register STOP message to DR of the source S.

The third phase of protocol is the formation of Shortest Path Tree (SPT). The phase results in optimization of the forwarding paths. This is done to achieve low latency and efficient bandwidth utilization. The route through RP may not always be appreciable. It may cause significant delays by detouring of paths. DR may initiate a transfer from shared tree to source specific SPT by using an (S, G) join message. Data packets then flow from S to the receiving nodes following the (S, G) entry. The receiver thus receives two copies of data, one following RPT and other from SPT. When traffic starts arriving from SPT, it sends a PRUNE message towards the RP known as (S, G, rpt) prune. It maintains state indicating that the traffic from S for G should not be propagated in that direction. Thus the shortest path tree is formed[12].

4.6 Pragmatic General Multicast (PGM): PGM is a reliable multicast transport protocol implemented on the sources and on the receivers for applications that require ordered, duplicate free, multicast data delivery from multiple sources to multiple receivers. It guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions or can detect unrecoverable data packet loss.PGM provides a reliable sequence of packets to multiple recipients simultaneously, making it suitable for applications like multi-receiver file transfer. [15, 16]

The source maintains a transmit window of outgoing data packets and will resend individual packets when it receives a negative acknowledgment (NAK). The network elements assist in suppressing an implosion of NAKs (when a data packet is dropped) and in efficient forwarding of the resent data only to the networks that need it. PGM allows a receiver to detect missing information in all cases and to request replacement information if the receiver application requires it. PGM has only a few data packets that are defined:

1. ODATA: original content data
2. NAK: selective negative acknowledgment
3. NCF: NAK confirmation
4. RDATA: retransmission (repair)
5. SPM: source path message

4.7 Border Gateway Multicast Protocol (BGMP)

Border Gateway Multicast Protocol (BGMP) is a protocol used for inter domain multicast routing, this is run by the border routers of a domain, and has inter domain bidirectional shared trees, constructed by using BGP group routes. Previously it is known as GUM. BGMP builds trees of domains that are similar to CBT trees of routers they are inter domain bidirectional shared trees rooted at a single domain built by sending explicit join messages towards a root domain. In each domain, any multicast routing protocols can be used for intra domain routing and they are called MIGPs. However BGMP can also build source specific branches, which are similar in concept to source specific trees in PIMSM. In BGMP, since each domain needs to have a range of multicast addresses to be used by groups rooted in the domain, a hierarchical multicast address allocation scheme is required. This is an important mechanism to support applications such as multimedia teleconferencing, distance learning, data replication and network games[20].

5. Summary Of Source-Based Tree And Group Based Tree Protocols

TABLE.1 Different Multicast Protocol in wired LAN Network

Multicast Protocols	Multicast Topology	Initialization	Independent of Routing Protocol	Dependency on Specific Routing Protocol	Maintenance Approach
MOSF	Source-Based Tree	Source	Yes	No	Hard-State
DVMRP	Source-Based Tree	Source	Yes	No	Soft-State
PIM-DM	Source-Based Tree	Receiver	No	No	Hard-State
PIM-SM	Group-Based Tree	Source	No	No	Hard-State
CBT	Group-Based Tree	Source/ Receiver	Yes	No	Soft-State
PGM	Group-Based Tree	Receiver	Yes	Yes	Hard-State
BGMP	Group-Based Tree	Source/ Receiver	Yes	No	Soft-State

6. Result

On this paper we have selected seven multicast routing protocols out of twelve because these protocols are the back bone of multicasting Routing (LAN). It helps in characterizing and identifying the qualitative behavior of multicasting protocols. Provisioning quality of service(Qos) implies providing guarantees such as deterministic end-to-end delay, availability of fixed amount of bandwidth, buffers, and computational resources to the Multicasting Routing Protocols.

7. Conclusion

In this paper, we have reviewed Shared Tree and Per Source Tree solutions for wired multicast. From the study, it can be concluded that number of multicast routing protocols are able for wired network and all these protocols has low bandwidth requirements.

The quality of service and reliability guaranteed by the proposed network is worth mentioning for the superior uses of multimedia and other emerging applications of the era especially by PGM. For each protocol, we have summarized the properties, and reveal the characteristics and tradeoffs, describe the operation, and list the strengths and weaknesses. There are other multicast routing protocols that aim at providing reliability, QoS guarantees, and security.

ACKNOWLEDGMENT

This research paper is made possible through the help and support from everyone, including: parents, teachers, friends and in essence, all sentient beings. Especially, please allow me to dedicate my acknowledgment of gratitude towards the following significant advisors and contributes.

First and foremost, I would like to thank Dr. Bharat Mishra (Asso. Proff.) for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization and theme of paper. Finally, I sincerely thanks to my parents, family and friends, who provide the advice and financial support.

BIBILIOGRAFY AND REFERENCES

[1]. **BIRYUKOV, A., SHAMIR, A., and WAGNER, D.:** ‘‘Real Time Cryptanalysis of A5/1 on a PC,’’ *Proc. Seventh Int’l Workshop on Fast Software Encryption,* Berlin: Springer- Verlag LNCS 1978, pp. 1–8, 2000.

[2]. **BLAZE, M., and BELLOVIN, S.:** ‘‘Tapping on My Network Door,’’ *Commun. of the ACM,* vol. 43, p. 136, Oct. 2000.

[3]. **BOGGS, D., MOGUL, J., and KENT, C.:** ‘‘Measured Capacity of an Ethernet: Myths and Reality,’’ *Proc. SIGCOMM ’88 Conf.,* ACM, pp. 222–234, 1988.

[4]. **BRAY, T., PAOLI, J., SPERBERG-MCQUEEN, C., MALER, E., YERGEAU, F., and COWAN, J.:** ‘‘Extensible Markup Language (XML) 1.1 (Second Edition),’’ W3C Recommendation, Sept. 2006.

[5]. **BURLEIGH, S., HOOKE, A., TORGERSON, L., FALL, K., CERF, V., DURST, B., SCOTT, K., and WEISS, H.:** ‘‘Delay-Tolerant Networking: An Approach to Interplanetary Internet,’’ *IEEE Commun. Magazine*, vol. 41, pp. 128–136, June 2003.

[6]. **CAPETANAKIS, J.I.:** ‘‘Tree Algorithms for Packet Broadcast Channels,’’ *IEEE Trans. on Information Theory,* vol. IT–5, pp. 505–515, Sept. 1979.

[7]. **CERF, V., and KAHN, R.:** ‘‘A Protocol for Packet Network Interconnection,’’ *IEEE Trans. on Commun.*, vol. COM–2, pp. 637–648, May 1974.

[8]. **CHASE, J.S., GALLATIN, A.J., and YOCUM, K.G.:** ‘‘End System Optimizations for High- Speed TCP,’’ *IEEE Commun. Magazine*, vol. 39, pp. 68–75, Apr. 2001

[9]. **CHEN, S., and NAHRSTEDT, K.:** ‘‘An Overview of QoS Routing for Next-Generation Networks,’’ *IEEE Network Magazine*, vol. 12, pp. 64–69, Nov./Dec. 1998.

[10]. **CHIU, D., and JAIN, R.:** ‘‘Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks,’’ *Comput. Netw. ISDN Syst.*, vol. 17, pp. 1–4, June 1989.

[11]. **CISCO:** ‘‘Cisco Visual Networking Index: Forecast and Methodology, 2009–2014,’’ Cisco Systems Inc., June 2010.

[12]. **DALAL, Y., and METCLFE, R.:** ‘‘Reverse Path Forwarding of Broadcast Packets,’’ *Commun. of the ACM*, vol. 21, pp. 1040–1048, Dec. 1978.

[13]. **DEERING, S.E.:** ‘‘SIP: Simple Internet Protocol,’’ *IEEE Network Magazine*, vol. 7, pp. 16–28, May/June 1993.

[14]. **DEERING, S., and CHERITON, D.:** ‘‘Multicast Routing in Datagram Networks and Extended LANs,’’ *ACM Trans. on Computer Systems*, vol. 8, pp. 85–110, May 1990.

[15]. **DEMERS, A., KESHAV, S., and SHENKER, S.:** ‘‘Analysis and Simulation of a Fair Queueing Algorithm,’’ *Internetwork: Research and Experience*, vol. 1, pp. 3–26, Sept. 1990.

[16]. **DENNING, D.E., and SACCO, G.M.:** ‘‘Timestamps in Key Distribution Protocols,’’ *Commun. of the ACM*, vol. 24, pp. 533–536, Aug. 1981.

[17]. **FLOYD, S., and JACOBSON, V.:** ‘‘Random Early Detection for Congestion Avoidance,’’ *IEEE/ACM Trans. on Networking*, vol. 1, pp. 397–413, Aug. 1993.

[18]. **FLUHRER, S., MANTIN, I., and SHAMIR, A.:** ‘‘Weakness in the Key Scheduling Algorithm of RC4,’’ *Proc. Eighth Ann. Workshop on Selected Areas in Cryptography*, Berlin: Springer-Verlag LNCS 2259, pp. 1–24, 2001.

[19]. **HAMMING, R.W.:** ‘‘Error Detecting and Error Correcting Codes,’’ *Bell System Tech. J.*, vol. 29, pp. 147–160, Apr. 1950.

[**20**]. **HARTE, L., KELLOGG, S., DREHER, R., and SCHAFFNIT, T.:** *The Comprehensive Guide to Wireless Technology,* Fuquay-Varina, NC: APDG Publishing, 2000.