IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SCHEME FOR RELIABLE MULTICASTING APPROACH BASED ON ROUTER

Dr.R. SARAVANA MOORTHY
Associate Professor (SF)
Department of Computer science.
Kongunadu college of Arts and Science, Coimbatore, Tamil Nādu.

ABSTRACT

IP Multicast is a natural extension of the unicast model. Multicast is a powerful service because it allows a single source to reach a virtually unlimited number of receivers in a very efficient and scalable manner. This work is implemented based on the concept of light weight multicast services (LMS). It is an extension to IP multicast that provides scalable and reliable multicast transport services. LMS extends IP multicast with a set of simple and lightweight services that enhance router forwarding for reliable multi casting. LMS cleanly separates the transport and forwarding component of error control by keeping the former at the end points thus avoiding layer violations, and pushes the latter to the routers where it can be implemented more efficiently. In the existing system implementation of single source sending data to destination is considered. In this work implementation of multiple sources sending data to many destinations is considered in this paper remedies to the loss of retransmitted packets are provided.

Key words: **Multicast, LMS, IP, Packets.**

1) INTRODUCTION

Proposed solutions are either inflexible, or incur high control overhead. In the proposed, Lightweight Multicast Services (LMS), it enhances the IP Multicast model with simple forwarding services to facilitate scalable and efficient (compared to pure end-to-end) as reliable multicast. In LMS, routers tag and steer control packets to pre selected end points and perform fine-grain multicast to guide responses to a subset of the group without transport-level processing. In the network systems the multicast systems are one of the main systems of building the success of the net workings.

IP Multicast systems are adopted as simple, open, best-effort delivery models with many-to many semantics. Despite several years of effort, a general, scalable and reliable end-to-end transport protocol analogous to TCP has proven elusive. The Internet architecture lays the simplicity and elegance of IP and its design principles. Internet architects realized early on that by foregoing the wire-like robustness of traditional communications networks (such as the telephone network) and pushing the intelligence to the edges, a network can be built on a much simpler and forwarding components, which allows the former to remain at the end-points while the latter is pushed to the routers, where it can be implanted very efficiently.

The division is clean, resulting in significant gain in performance and scalability while reducing application complexity. LMS reaches beyond reliable multicast to applications such as scalable collect, any-cast, and in general, any application that can benefit from a hierarchy congruent with the underlying topology.

This paper is implemented based on Lightweight Multicast Services (LMS), an extension to IP Multicast, on top of which a general and scalable reliable multicast transport service can be constructed. LMS extends IP Multicast with a set of simple and lightweight services that enhance router forwarding to enable highly scalable, *network-assisted* solutions to reliable multicast. LMS cleanly separates the transport and forwarding components of error control, keeps the former at the endpoints thus avoiding layer violations, and pushes the latter to the routers where it can be implemented most efficiently.

Unicast error control mechanisms are not suitable for large-scale multicast due to the many-to-many nature of IP Multicast. Losses in multicast typically affect part of the multicast tree and attempting to recover localized loss leads to the following problems.

• **Implosion** occurs when the loss of a packet triggers redundant messages (requests and/or retransmissions). In large multicast groups, such messages may swamp the group and the network.

• **Exposure** occurs when recovery-related messages reach receivers that have not experienced loss. Exposure wastes both network and end-system resources.

• **Recovery latency**, defined as the latency experienced by a member from the instant a loss is detected until a reply is received, impacts buffering requirements and application utility.

• **Adaptability**: frequent changes in-group membership and network conditions impact the efficiency of error recovery (in terms of loss of service, redundant messages, additional processing, and/or latency), particularly when tenuous assumptions are made about receiver population and/or topology.

Briefly, LMS works as follows: as receivers join a multicast tree, the routers in a hierarchy with each router dynamically selecting a parent organize them. Upon detecting loss, all requests from children are steered toward the parent, while the request from the parent is forwarded upstream, ensuring that only one request escapes each subtree. Before funneling requests to the parent, a router inserts the address of both the incoming and outgoing interfaces in passing requests. We call such a router the *turning point* of the request, which identifies the root of the subtree that originated the request. The process ensures that a request will find a receiver that has the requested data, or reach the sender. In either case, a retransmission is unicast to the turning point router, which in turn multicasts it to the affected subtree.

Implosion and exposure are addressed by constructing a hierarchy, which localizes recovery between parents and children. The hierarchy adapts quickly to both group membership and routing changes since routers ensure that it always tracks the multicast routing tree. Recovery latency is minimized because with LMS the endpoints closest to the loss are involved and recovery messages are sent immediately. Finally, the router-maintained hierarchy eliminates all topology-related state from the receivers, such as timers, hop counts, parent/child relations, etc., and most associated signaling overhead.

2) LIGHTWEIGHT MULTICAST SERVICES

LMS is a small set of forwarding services which enhance IP multicast to allow routers to automatically build an application- driven hierarchy and exchange packets between the different levels of the hierarchy. In this section, we first discuss why a hierarchy enables very efficient multicast error recovery. Then, we describe why this is difficult under the current multicast model. Finally, we show how LMS addresses this problem.

In Fig. 1, we observe a subset of receivers that have just experienced loss after a packet was dropped on link. Assuming a nearby receiver has the data and is willing to retransmit, we call this receiver a *replier* and the one sending a request a *requestor*. Recovery is initiated by the requestor sending a NACK directly to the replier, followed by a multicast by the replier at link. Recovery latency is minimized if the requestor and the replier are closest to the loss. We refer to this recovery process as *near-best*2 because it eliminates implosion and exposure and minimizes recovery latency.

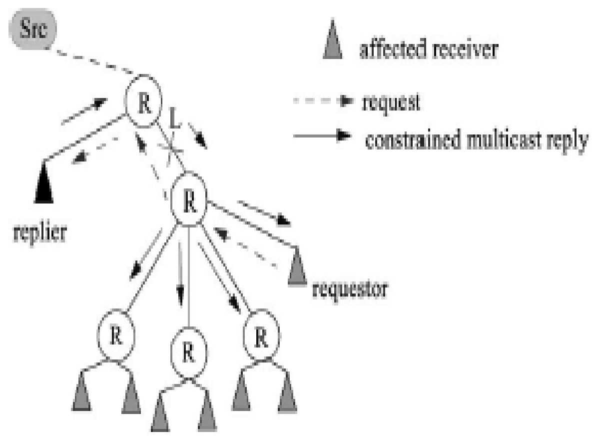

Fig. 1. Idealized recovery scenario.

A router-based hierarchical solution, that is, one where routers temporarily buffer data and send retransmissions in response to NACKs, is architecturally incompatible with IP because it requires transport level processing at routers; yet it is attractive because it is conceptually simple and elegant. LMS reconciles this incompatibility by making the following key observation: a router-based solution is desirable not because it harnesses the router's processing power, but because it exploits the router's *location.*

3) MODULES

a) Selection of a Replier
b) Steering messages to replier
c) Request Handling at the Routers
d) Directed Multicast

a) **Selection of a replier**:

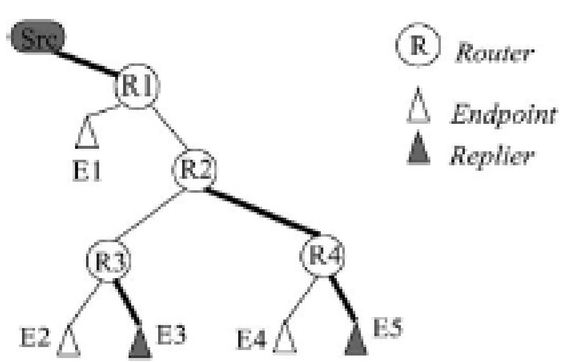

Fig.2. Possible replier allocation in LMS

Each router selects a single replier *for each source* in a multicast group. To simplify the description we assume that receivers are attached directly to routers. Each router selects a replier as follows.

• If the router has two or more downstream links it selects one as the replier link

• If the router has only one downstream link, then that becomes the replier link by default.

As an optimization, if the source is directly attached to the router the source becomes the replier. Fig. 2 shows a possible router-replier allocation. The links leading to a replier are in bold. It is important to note that similar to data forwarding, a router only needs to know the *next hop* to the replier, not the actual replier address. For example, router R2 selects R4 as the next hop knowing that it leads to *some* replier. This has some important advantages.

• Replier changes are localized. For example, if R4 decides to switch to replier E4 (because E5 either left the group or crashed), R2 does not need to change its replier information.

• Receivers do not have to be notified when selected as repliers. A receiver knows it has been selected if it receives a request. A receiver, however, is not guaranteed to remain a replier for future requests.

• The replier state at the router is small, consisting of an identifier for the replier link.

Next, we address the replier selection criteria when a router has more than one potential replier link.

b) Steering messages to replier

When loss is detected, requestors multicast a request that contains a new (to be defined) IP option. Requests are handled hop-by-hop by LMS routers. Initially, routers steer requests toward the source until a replier path is found and then toward the replier. Hop-by-hop forwarding requires routers to intercept each request, which is accomplished via the IP Router Alert option included in every request.

c) Request Handling at the Routers

Router allows only one request to escape upstream. A request may arrive at a router from one of three possible directions.

From a non replier link:

When a request arrives from non-replier link the router becomes the turning point then it turns requests around and forwards them out of the replier link. Before forwarding the request it is empty, then router adds information to the packet as:

- An identifier interfaces the request arrived on
- The address of the replier interface

From the replier link:

When a request arrives from the replier link the router forwards it to the upstream link. The packet is not modified.

From the upstream link:

When a request arrives from the upstream link, the router forwards it to replier link. The pocket is not modified.

d) Directed Multicast

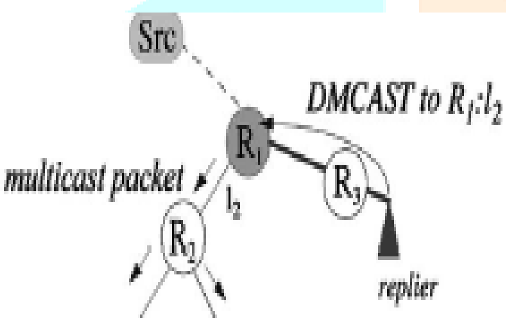

Fig.3.Directed Multicast

A replier retransmits the data using a new service called Directed Multicast (DMCAST). This is the final service provided by LMS and its purpose is to enable fine-grain multicast to eliminate exposure.

The operation of a DMCAST is summarized in Fig. 3. To perform a DMCAST, a replier first creates a multicast packet containing the requested data. The source address is set to the original source and the destination address to the group. An IP option is added to the packet, containing the turning point information, which is obtained from the request. The replier then encapsulates the multicast packet in a unicast packet and sends it to the turning point router, whose address is again obtained from the request. When the turning point router receives the packet, it decapsulates the multicast packet, strips the IP option, and multicasts it on the specified interface. From there, the packet travels as if it had originated from the source.

CONCLUSION

In this work, I have presented LMS, a set of forwarding services that enhance the IP multicast service model to allow the implementation of highly scalable, reliable multicast applications. I have shown that LMS is simple to implement and its overhead at the routers is comparable to normal multicast. LMS can also be used in other allocations, such as any cast and scalable collect service. A novel contribution of this work is the decomposition of transport and forwarding functionality of multicast error control, such that each can be located where it is most beneficial. This separation is very clean that it does not violate any layering principles.

5) REFERENCES

(1). T. Speakman, J. Gemmell, D. Farinacci, S.lin, D. Leshchiner, M. Luby,
T. Montogomery, L. Vicisano, "PGMReliable Transport protocol specification," IETF, RFC 3208,dec.2001.

(2). W. Fenner and S. Casner, " A traceroute facility for the IP Multicast," IETF, Internet Draft, draft-traceroute-ipm-00.txt, Dec.2003.

(3). C. Diot, B. Levine, B. Lyle, H. Kassem and D. Balensiefen, "deployment issues for the IP multicast service and architecture", IEEE Network, vol.14, pp. 78-88,Jan. /Feb. 2000.

(4). B. Whetten, L. Vicisano, R. Kermode, M. Handley, S. Floyd, and M.Luby, "Reliable Multicast transport buildings blocks for one- to-many bulkdata transfer," IETF, RFC 3048, Jan 2001.

(5). C. Papadopoulos, " Error control for continuous media and large scale multicast applications," Ph.D. thesis, Dept. Comput. Sci., Washington Univ., St. Louis, MO, Aug. 1999.

BIOGRAPHIES

Dr.R.Saravana moorthy
Associate Professor (SF)
Department of Computer science.
Kongunadu college of Arts and ScienceCoimbatore.Tamilnadu.