2012 International Conference on Information and Network Technology (ICINT 2012)
IPCSIT vol. 37 (2012) © (2012) IACSIT Press, Singapore

High Performance & Service Based HMRP in Multicasting Using HBM Technique

K. Kumaravel [1 +] and A.Marimuthu [2]

[1] Dept. of Computer Science, Dr. N.G.P. Arts and Science College, Coimbatore, India – 641 048

[2] Dept of Computer Science Govt., Arts College (Autonomous) Coimbatore, India

Abstract. According to our research we introduce a proposal for building an alternative group communication service that shifts the multicast support from core routers to end-systems. Our proposal, called Host Based Multicast (HBM), operates at application-level and provides an efficient multi-point data distribution service for one-to-many or many-to-many communications. With this approach end-hosts (running the application), dedicated servers and/or border routers automatically self-organize into an overlay distribution topology where data is disseminated. This overlay topology can be composed of both unicast connections and native multicast islands (e.g. within each site). Therefore it offers a group communication service to all hosts, even those located in a site that does not have access for any reason, to native multicast routing.HBM is a centralized solution, where everything, including group membership management and overlay topology creation, is under the control of a single Rendezvous Point (RP). This thesis focuses on three key aspects: scalability, robustness, and security. The scalability can be largely improved, with a few simple HBM protocol parameter adjustments like the frequency and size of the control messages exchanged. Robustness is another important practical issue, and we introduce packet loss reduction techniques, like the addition of redundant virtual links that avoid topology partition in case of transit node failures. Finally we investigate the use of HBM to build a fully secure but efficient group communication service between several sites using an IPSec VPN environment. We show that HBM and the IPSec VPN environment naturally fit with one-another and lead to the concept of Virtual Private Routed Network (VPRN).

Keywords: VPRN, HBM, HMRP.

1. Introduction

As the Internet grows up, new communication needs arise. First, e-mail and FTP were enough for most people. Then the WWW arrived and people wanted to see graphics, not just plaintext. Now, even static graphics are not enough; real-time video and audio are demanded. As communication needs evolve, communication paradigms originally designed to deal with e-mail and FTP need to evolve too. Multicasting is one of them. Imagine that an event needs to be transmitted to several hosts aspersed over the Internet with audio and video streams. Of course, traffic should be sent as efficiently as possible – the less bandwidth used, the better. With pre-multicast technology, two communication paradigms are available, both of which are inadequate. The first one is Unicast. TELNET, FTP, SMTP and HTTP are unicast-based protocols with one source and one destination. To send to multiple destinations, different communication paths are needed between the source and each of the destinations. Therefore, a copy of each audio and video stream needs to be sent separately to each receiver. This solution is often called multi-unicast. Clearly, this is not affordable. Even if you are quick enough in copying real-time audio and video streams, both your network and the Internet would collapse when the number of destinations increases.

[+] Corresponding author. Tel.: + 9843347837.
E-mail address: k_kumara_vel2001@yahoo.com.

The second choice is broadcast. The broadcast paradigm saves a lot of bandwidth compared to unicast. If you want to send something to all computers on your LAN, you don't need a separate copy for each. On the contrary, only one copy is sent to the wire, and all computers connected to it receive the copy. This solution is better for our problem but is still insufficient, as we probably need to broadcast to only some of our computers, not all. Even worse, it is almost certain that many hosts interested in your conference will be outside of your LAN and broadcast packets are traditionally not forwarded by routers. Thus, broadcast is good for applications and protocols that don't need to cross LAN limits (such as ARP, BOOTP,DHCP and even routed), but it is not good enough for our problem.

1.1. HBMP

By Introducing a Standard Protocol Host Based Multicast Protocol it is used to make a join and leave any multicast groups dynamically.

• IP-style semantics. A source can send multicast packets at any time, with no need to register or to schedule transmission. IP multicast is based on UDP, so packets are delivered using a best-effort policy.

• Open groups. Sources only need to know a multicast address. They do not need to know group membership, and they do not need to be a member of the multicast group to which they are sending. A group can have any number of sources.

• Dynamic groups. Multicast group members can join or leave a multicast group at will. There is no need to register, synchronize, or negotiate with a centralized group management entity.

2. Existing Techniques

As we have seen, the deployment of multicast routing in the Internet is still far behind expectations. Therefore a first motivation for an alternative group communication serviceis to bypass the lack of native IP multicast routing.

2.1. Proposed technique

AGMS (Alternative Group Communication Service). In the proposed technique one of the major disadvantages delay in spreading a packets to a group and major effects of sending duplicate packets to the end-systems. to avoid this technique One proposal of an alternative group communication service is overlay Multicast .In particular, we consider a model in which multicast related features, such as group membership, multicast routing, and packet duplication, are implemented at end systems, assuming only unicast IP services. We call the scheme either End System (i.e End Host) Multicast. The main goal is to propose an application-level multicast (HBM) that is simple, easy deployment and no need to routers that support native multicast. Our proposal HBM is a centralized approach and everything is under control by a single node, or Rendezvous point (RP). The hot topic of our proposal is studied. In this approach, it has to create not bad the overlay topology, improve the scalability, impact the robustness in front of node failures and overlay topology modification, build a secure group communication service.

In order to achieve these issues, we implemented a group communication services library (GCSL) for our proposal HBM.

3. Motivations for an Alternative Group Communication

3.1. Service (AGCS)

A Group Communication Service refers to the ability to send information to several receivers at the same time, using either a one-to-many or many-to-many model. The any-source and source specific multicast routing approaches provide such a service. Yet other solutions are possible and this chapter proposes a survey of such alternatives. Although this survey aims to give a complete overview of AGCS techniques, we do not claim to be exhaustive. Besides we only consider the routing service (i.e. as a replacement of, or complement to, IP-multicast) and ignore any upper-level service like reliability or congestion control. An AGCS can be used as a way to *bypass the multicast routing deployment problems.* Indeed, group communication traditionally requires that each node at each site has access to a native multicast routing service. If intra-domain multicast (within a LAN or a site) is widely available, this is different for inter-

domain multicast. Today many ISPs are still reluctant to provide a wide-area multicast routing service. *But other Motivations exist.* For instance an AGCS can be used to go beyond the limitations of traditional multicast routing. An AGCS can offer a bridging service between several multicast capable areas running different multicast routing protocols, for instance between IPv4 and IPv6 multicast islands. An AGCS can also be used along with PIM-SSM Since only the source *S* is allowed to send traffic to an (S, G) channel, *G* being the group addresses, no multicast back-channel is available for a receiver to provide feedback to the group.

3.2. Performance metrics

Several performance metrics have been defined to characterize AGCS performance and impacts on the network. Some of them focus on the *data path:*

Stress. Defines the stress of a physical link as the number of identical packets it carries. the optimal value, achieved with native multicast routing.

Resource usage. It defines this metric as the sum of the *delay stress* over all the links that participate in data transmissions. This metric gives an idea of network resources used by the transmission process, assuming that links with high delays are more costly.

Stretch. Its also called "Relative Delay Penalty" in the stretch metric between a source and a member is the ratio of the delay between them along the overlay distribution topology, to the delay of the direct unicast path. Another set of metrics focuses on *end-host performance:*

Losses after failures. This metric counts the average number of packet losses after an ungraceful failure of a single node.. It highlights robustness in the occurrence of unpredicted events.

Time to first packet. This defines the time required for a new member to start receiving a data flow when joining an on-going session. Finally some metrics focus on the *control part:*

Control overhead. Maintaining the AGCS topology has a cost, in terms of control information exchanged (number of messages processed and bandwidth) .The large diversity of performance metrics shows there is no single answer to the question: "what is the best solution". Some proposals can deliberately favor some of these metrics at the expense of others (e.g. the multi-unicast approach used by reflectors offers a high robustness to member failures (other than the reflector itself) at the cost of a high link stress near the reflector).

4. HBM (Host Based Multicast)

The HBM protocol automatically creates a virtual overlay topology between the various group members (sources and receivers), using point-to-point UDP tunnels between them. Everything is under the control of a single host, the *Rendezvous Point* (or RP). This RP knows the members, their features, and the communication costs between them. He is responsible of the overlay topology calculation and its setup at each member. *This proposal therefore follows a centralized approach*.

Several such messages are defined:

• *A join message* is sent by a new member to the RP, and contains: his IP address and port to send or receive date packets, his connection kind (if known), and some special member parameters.

• *A Member List (or ML) message* is sent be the RP to a new member, and contains
the current list of all members.

A Member *Update message* is sent by the RP to all the members to update the member list when a member joins or leaves a group. This message avoids the need to list all the current members, since only the delta is sent.

• *A Leave* message is sent by a group member to leave the group.

• *A Leave* message is a small message that informs the leaving member that the "leave" process is finished.

• *A Failure message* is sent by a member who detects a member failure.

• *A Metric Update (or MU) message* is sent by a member to the RP in order to update the RP's communication cost database. It contains a list of {member-metrics pair.

• *A Topology Update (or TU) message* is sent by the RP to the members in order to inform them of the new topology. Since a TU message only contains the direct neighborhood, a different message is sent to each member.

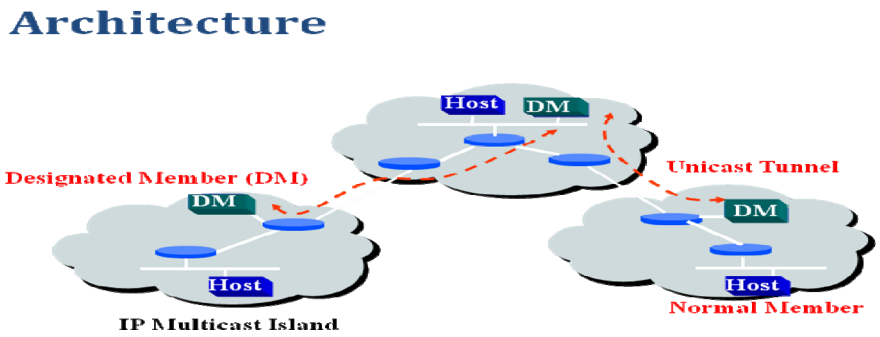

Fig. 1: Example

Table. 1: Example

	IP Multicast	Host Multicast
Host Extension	OS kernel support	A user-space daemon
Local Membership Management	IGMP	HGMP
Intra domain/island multicast routing	DVMRP, MOSPF, PIM, CBT	Using deployed IP Multicast
Inter domain/island multicast routing	MASC/BGMP, MBGP/MSDP/PIM	HMTP

Rest of the talk is focused on HMTP

4.1. HMTP

Host Multicast Tree Protocol (HMTP) is another application layer multicast protocol that uses the tree-first approach and has some similarities with the Yoid protocol.

Tree construction. In shared tree, a joining member, h, finds its parent using the following heuristic: It first discovers the root of the shared tree by querying the RP. Starting from the root, at each level of the tree h tries to find a member, x, close to itself. If the number of children is less than its degree bound, h joins as a child of x. Or else it proceeds to the next level and tries to find a potential parent among the children of x.Members in HMTP maintain information about all members on its path to the root. Periodically, each member tries to find a better (i.e. closer) parent on the tree, by re-initiating the join process from some random member on its root path. Knowing the entire root path allows members to detect loops. HMTP employs a loop detection and resolution mechanism, instead of loop avoidance. Unlike Yoid, HMTP does not explicitly create a mesh. However, each member periodically discovers and caches information about a few other members that are part of the tree. In the specific case when the RP is unavailable, the knowledge of such members is used to recover the tree from partitions. Build a bi-directional shared-tree connecting all islands the tree should be congruent to physical network topology to be efficient use member-to-member round-trip time as distance metric in current design The tree should be robust Be able to handle node failure, dynamic join/leave etc.

HMRP – joining a group. HMRP always knows the root of the tree. A new comer does a depth- first search of the tree to find a close member as its parent Clustering nearby members makes the tree congruent to physical network topology to the first order. Fig 2 .

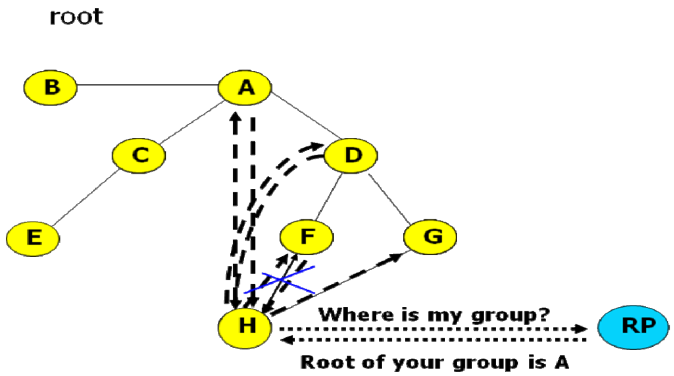

Fig. 2: Example

HMRP – tree maintenance. Each member keeps its children list and root path up to date by exchanging REFRESH and PATH messages with neighbors. Root sends REFRESH message to HMRP (fig 3).

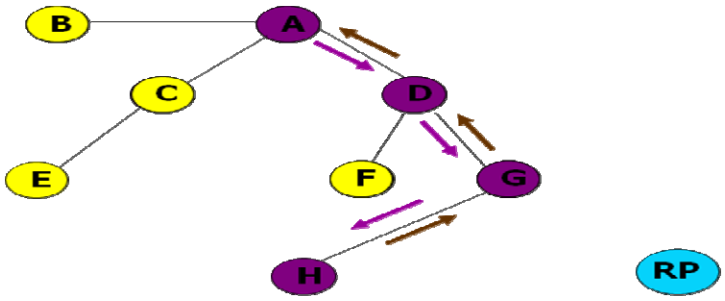

Fig. 3: Example

HMRP – member leave & partition recovery. Periodically re-run the join procedure To accommodate changes in network conditions and group membership Start from a randomly picked node in the root path. Less frequent than REFRESH and PATH messages.

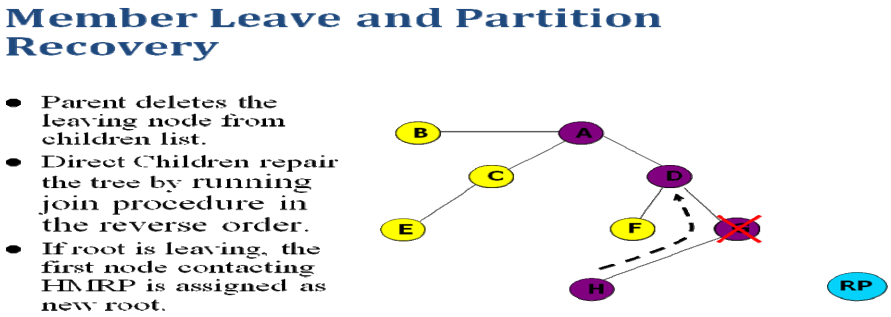

Fig. 4: Example

HMRP – loop detection & resolution. Loop is possible: Multiple conflicting joins happen at the same time. Detection One's root path contains itself Resolution: Leave the current parent and re-join the tree from the root. Loop is rare as mentioned in fig 5.

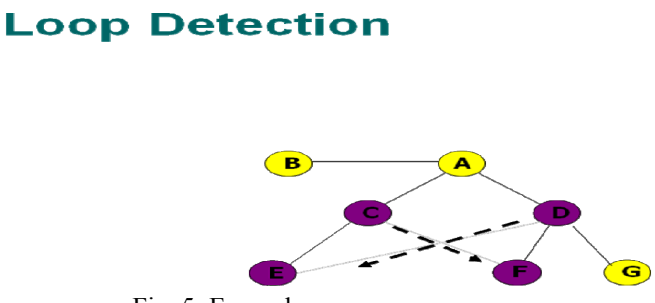

Fig. 5: Example

Forwarded data packets. Forwarded data packets contain a specific HBM header. It defines a Topology Sequence Number (TSN) which identified the current topology, and a Packet Sequence Number (PSN). The precise goal of these two fields. The data field contains the multicast data packet. In other words, HBM encapsulates the multicast data packets into HBM data packets. Since HBM is implemented as a user-level library, it simply uses unicast UDP/IP "tunnels" and TCP/IP for data packet and control messages respectively.

5. Conclusion & Further Scope

This paper focuses on the robustness of the HBM application level multicast proposal. We have identified two sources of losses: those caused by topology partition problems, usually after transit node failures, and those caused by routing instability periods, usually during the topology update process. We have introduced and compared several strategies and experiments have shown that simple yet effective solutions exist. Adding redundant virtual links to the overlay topology between a carefully chosen subset of transit nodes is an easy way to improve robustness in front of node failures, even if a full robustness is not achieved. Going further requires creating RVLs emanating from leaves, which is not possible if leaves are lightweight hosts (limited processing/networking Capabilities). A side effect of adding RVLs is a rapid failure discovery capability: the fact a node receives new packets from its RVL only denotes a failure on the normal delivery path, and an alert message should be immediately sent to the RP in order to repair the partition. This solution is far more efficient than mechanisms based on the periodic transmission.

6. References

[1] S. Banerjee, S. Lee, B. Bhattacharjee, and A. Srinivasan. Resilient Multicast using overlays. in *ACM SIGMETRICS*, June 2003.

[2] M. Castro, P. Druschel, A-M. Kermarrec and A. Rowstron. Scribe: a large-scale and decentralized application-level multicast Infrastructure. *IEEE Journal on Selected Areas in Communications(JSAC)*, 20(8), October 2002.

[3] Y-H. Chaw the, S. Rao, and H. Zhang. A case for end system Multicast. In *ACM SIGMETRICS*, June 2000.

[4] C. Diot, B. Neil Levine, B. Lyles, H. Kassem, and D. Balensiefen. Deployment issues for the ip multicast service and architecture. *IEEE Network*, January 2000.

[5] A. El-Sayed, V. Roca, and L. Mathy. A survey of proposals for an alternative group communication service. *IEEE Network*, January/February 2003.

[6] A. Essayed. *Application-Level Multicast Transmission Techniques over the Internet*, March 2004. PhD Thesis, INPG.

[7] V. Roca and A. El-Sayed. A host-based multicast (hbm) solution for group communications. In *First IEEE Int. Conf. on Networking (ICN'01)*, July 2001.

[8] W. Wang, D. Helder, S. Jamin, and L. Zhang. Overlay optimizations for end-host multicast. In *Fourth Internationa Workshop on Networked Group Communication (NGC 2002)*, October 2002.

[9] E. Zegura, K. Calvert, and S. Bhattacharjee. How to model an internetwork. In *IEEE INFOCOM'96*, March 1996.