American Journal of Applied Sciences 6 (7): 1347-1351, 2009
ISSN 1546-9239

An Approach to Improve the State Scalability of Source Specific Multicast

[1]S.A. Al-Talib, [2]B.M. Ali and [2]S. Khatun
[1]Wireless Networks and Protocols Research, Wireless Communications,
Malaysian Institute of Microelectronic Systems Berhad, Technology Park Malaysia,
57000 Kuala Lumpur, Malaysia
[2]Department of Computer and Communications Systems, University Putra Malaysia, Malaysia

Abstract: Problem statement: Source Specific Multicast (SSM) is an acceptable solution for current multicast applications; since the driving applications to date are one to many, including Internet TV, distance learning, file distribution and streaming media. **Approach:** It was useful for billing, address allocation and security. SSM still had serious state scalability problem when there were a large number of simultaneous on-going multicast groups in the network. **Results:** In this study, a scheme had been devised to improve the state scalability of source specific multicast. The scheme consisted of two stages: **Conclusion/Recommendations:** The first stage was to cluster the receivers based on their IP addresses and the second stage was to reduce the multicast state at routers. In order to prove the correctness of the proposed scheme, it had been applied to multicast trees built by other researchers. The results of the comparison approved our statement.

Key words: Source specific multicast, hash distribution tree, multicast-forwarding state

INTRODUCTION

IP multicast has existed since Stephen Deering established the model (called Any-Source Multicast (ASM)) in 1988[1]. Deering model has two important components: the service model and routing protocols. In the IP multicast service model, a group of receiver hosts can be identified by a single class D IP group address. Any host can send to the group by setting the destination address in the IP header as the group address. Receivers can dynamically join and leave the group. Such a service model provides a powerful abstraction for applications as end hosts (senders and receivers) can utilize the service without having to keep track of the membership of the group. It is the responsibility of IP multicast routing protocols to maintain the membership information and to build multicast distribution trees to deliver packets from a sender to all the receivers in a group. However, IP multicast is still far from being widely deployed in the Internet. Scalability, security, address allocation, billing are the issues that have delayed its deployment.

Recently, some alternative service models have been proposed to solve these problems. Among them, Source Specific Multicast (SSM)[2] is dedicated to single source applications. The main reason of SSM is that almost 90% of multicast applications of immediate interest, such as file transfer and streaming media, are single-source. Compared with ASM, SSM is a much simpler paradigm; besides it could solve many deployment problems in billing, address allocation and security.

Like ASM, SSM utilizes a tree delivery structure, which is constructed by means of explicit-join signaling to the source. The growing number of forwarding state entries requires more memory and entails slower forwarding process since every packet forwarding action involves an address look-up. In other words, SSM still confronts the serious state scalability problem when there are a large number of simultaneous on-going multicast groups in the network. Forwarding state reduction is the main focus for recent research efforts in order to solve the state scalability problem.

The REUNITE[3,4] and HBH[5,6] proposals follow a recursive unicast approach to solve the multicast deployment issue. The idea is to have some REUNITE/HBH-capable routers that act as branching nodes and create copies with modified unicast destination address between two hops. It is similar to XCAST[7] except that packets do not carry the list of destinations. Branching nodes thus need to keep some state for each group.

Zhang *et al*.[8] introduces the idea of recursive unicast into an existing multicast routing protocol, multicast extension to OSPF (MOSPF) to achieve

Corresponding Author: S.A. Al-Talib, Wireless Networks and Protocols Research, Wireless Communications,
MIMOS Berhad, Technology Park Malaysia, 57000 Kuala Lumpur, Malaysia

scalable multicast. To ease address allocation and sender admission control, in Holbrook *et al.*[9] designed an Explicitly Requested Single-Source (EXPRESS) multicast scheme. Express is an alternative to the IP-multicast model that uses a per-source, channel-based model. Each channel is a service identified by a tuple (S, E) where S is the sender's source address and E is the Express destination address (a class-D address). Only S may send to (S, E) because receivers subscribed to (S, E) are not subscribed to (S',E), for some other host S'. Thus, data transmitted from two sources to the same address E is only sent to receivers subscribing to both sources.

EXPRESS reduces the distribution model from M to N to 1 to N, simplifying the service.

Some proposals tried to simplify the multicast service[10]. The analysis of these works leads us to the proposition of REHASH (REcursive HASH tree) to improve IP multicast scalability by reducing multicast state at routers.

Source specific multicast: Source Specific Multicast[2] is a service model that identifies session traffic by both source and group addresses, rather than just by group address as traditional multicast does. SSM builds Shortest-Path Trees (SPTs) directly represented by (S, G) pairs. The "S" refers to the source's unicast address and the "G" refers to the specific multicast group address. The SSM (S, G) pairs are called channels to differentiate them from traditional any-source multicast (ASM) groups. Hosts will receive traffic by becoming members of this channel. "Subscribe" and "unsubscribe" in SSM channel are similar to "join" and "leave" respectively in ASM. SSM solves many of the deployment problems of ASM in the following aspects:

- SSM defines channels on a per-source basis. This eliminates the problem of global allocation of SSM destination addresses. And each source is independently responsible for resolving address collisions
- SSM requires only source-based forwarding trees. This avoids the need for complex shared tree routing infrastructure
- SSM's single source ownership of the channel gives a basis on which to charge and whom to charge: ISP charges source for net resources and source charges customers for service. However, it is much more difficult to identify an entity to bill for the network costs in ASM
- SSM gives a better solution to the access control problem. When a receiver subscribes to a (S, G) channel, it only receives data sent by the source S. By contrast, in ASM, any host can submit to a group. Hence, it is more difficult to spam an SSM channel than an ASM group[11]. In other words, there is inherent protection against unauthorized "hijacking" of a multicast tree in order to deliver a Denial of Service (DoS) attack to recipients of the multicast stream

MATERIALS AND METHODS

The motivation for this work is usually to offer an alternative to the lack of deployment of multicast service in the Internet. The proposed scheme consists of two stages: The first stage is to cluster the receivers based on their IP addresses and the second stage is to reduce the multicast state at routers which improves the multicast state scalability. Hash algorithm has been applied in the clustering stage, where a multicast distribution tree has been built based on the receiver's IP address. The tree is a single-source model that has a simple architecture. There is no third-party and scalability can be maintained by building routing tree by means of explicit-join signaling to the source, as suggested by Express. With only one source, routing can always be shortest path back to that source. Express is compatible with the current Internet, since its required functions have been well anticipated by IGMPv3[12] (for IPv4) and MLDv2[13] (for IPv6).

Edge routers can send source-specific (S, G) joins using IGMPv3 for designated Express multicast groups. Express has already been allocated a space of experimental addresses by the Internet Assigned Numbers Authority (IANA) for which joins from receivers are expected on a per-source basis[14].

The second stage of the proposed scheme is to use recursive unicast to implement multicast service. This means that multicast distribution is implemented through a REcursive HASH tree (REHASH).

Each receiver r_i sends join (S, r_i) upstream toward the source S and the route is: r_i > R>--->S. S uses hash algorithm to build clusters of receivers r_i based on their IP addresses. The cluster rooted at S (Source Specific Tree) for multicast distribution (Fig. 1). It is one of the characteristics that differentiate REHASH from other routing protocols. In this case, it become easier to deal with each cluster separately, besides it improves the scalability of the distribution tree.

To multicast a packet, the root sends a copy of the packet to each hash address (cluster) in its list, which leads to the related receivers. Similarly, when a branching node forwards such a packet, it sends a copy of the packet to each receiver in its own list. This procedure continues recursively until packets reach all leaf nodes of the tree, i.e., all receivers.

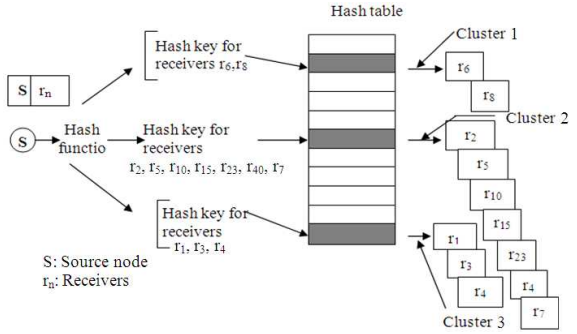

Fig. 1: Clustering of routers at the source

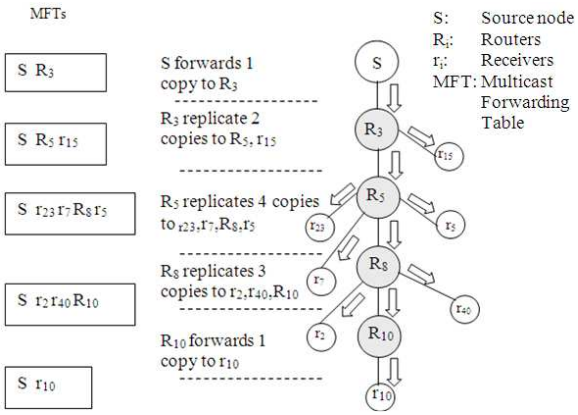

Fig. 2: Rehash multicast forwarding states at routers for cluster 2

The source sends data in unicast to the first receiver that joined the group. At a branching node R_i, entering data packets are addressed to the first receiver r_i that joined the group in the cluster below R_i. r_i is stored in a special Multicast Forwarding Table (MFT) entry. R_i creates one packet copy for each receiver in its MFT (the destination address is set to the receiver's unicast address).

Figure 1 shows how the receivers are clustered after sending their *join* messages to the source node. Implementing hash algorithm did this clustering. A detailed description of the grouping scheme for multicasting can be found in[15]. For clarity, a simple topology is shown in Fig. 1. There are 12 receivers grouped to 3 clusters. There are 2 receivers (r_6 and r_8) subscribe to cluster-1, 7 receivers (r_2, r_5, r_{10}, r_{15}, r_{23}, r_{40} and r_7) subscribe to cluster-2 and 3 receivers (r_1, r_3 and r_4) subscribe to cluster-3.

To describe the tree creation and maintenance operations, a detailed example has been used shown in Fig. 2. S is the source and the root of a group, R_3, R_5, R_8 and R_{10} are router nodes, r_2, r_5, r_{10}, r_{15}, r_{23}, r_{40} and r_7 are the receivers that constitute cluster 2 in Fig. 1.

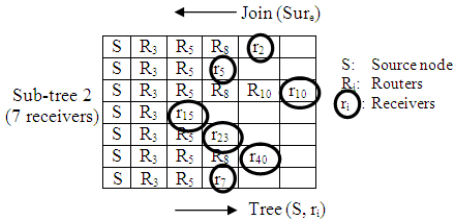

Fig. 3: Matrix representation of cluster 2 routes

To better illustrate the properties of REHASH, the following asymmetric unicast routes has been assumed for cluster 2:

$S>R_3>R_5>R_8>r_2$
$S>R_3>R_5>r_5$
$S>R_3>R_5>R_8>R_{10}>r_{10}$
$S>R_3>r_{15}$
$S>R_3>R_5>r_{23}$
$S>R_3>R_5>R_8>r_{40}$ and $S>R_3>R_5>r_7$

If a router R_i is traversed by a multicast group's delivery tree, the router will maintain an entry either in its MFT (in the case that the tree branches at the router) or in its Multicast Control Table (MCT) (in the case that the tree does not branch). Only MFT needs to be maintained on the data plane, while MCT needs to be maintained on the control plane. That is, when a data packet arrives, only MFT needs to be looked up. In contrast, MCT needs to be looked up only when control messages (join or tree) are processed. Therefore, by partitioning per group multicast state into forwarding and control state, REHASH maintained a much smaller per group forwarding table than other IP multicast protocols in a network with a large number of sparse groups.

REHASH and forwarding state prediction: In our example, packet replication in REHASH could be done based on the MFTs saved in each router.

REHASH concludes a special method for MFTs formation and forwarding state prediction. This could be performed by scanning the matrix of receivers routes shown in Fig. 3 of cluster 2 from left to right and dropping the duplicate in R_i's. The table could be summarized as shown in Fig. 4.

This dropping means deleting the forwarding states at non-branching routers, which tends to improve the state scalability. By separating the matrix in Fig. 4 vertically (by hops), the result is compatible to the real forwarding state at different routers that appears in Fig. 2. To further check the correctness of REHASH approach in predicting the multicast forwarding state

and packet replication at routers, the same steps was applied to HBH tree example in[5] and REUNITE tree example in[3].

Figure 5 shows the matrix that represents the HBH tree routes for the example in[5]. The forwarding states at MFTs in HBH tree are compatible to that given in REHASH approach. Again REHASH approach was applied to REUNITE tree introduced in[3], the results obtained support our expectations.

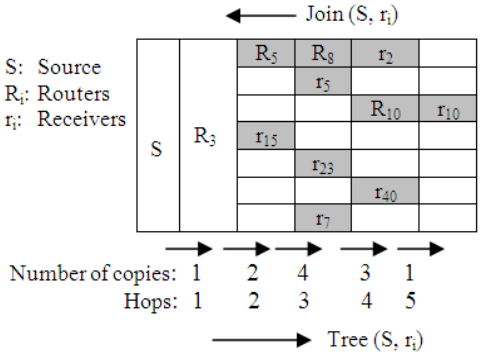

Fig. 4: Packet replication at routers to 7 receivers for cluster 2 in Fig. 1

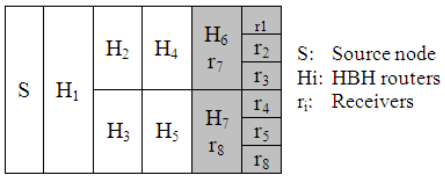

Fig. 5: Matrix representation of HBH tree route when applying REHASH approach

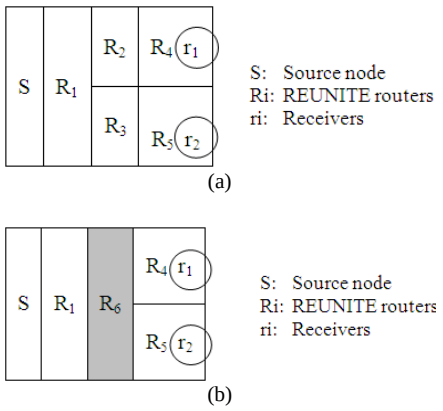

Fig. 6: Matrix representation of REUNITE tree when applying REHASH approach (a): REUNITE first route (b): REUNITE second route

Figure 6 shows the matrix representation of the forwarding states at routers by applying REHASH approach, which is compatible with the MFTs given in[3]for REUNITE tree. Further more, if we compare the two routes (a) and (b) in Fig. 6, we can conclude that the problem in REUNITE of packet duplication in one link (R1>R6) could be discovered and solved in REHASH by selecting the suitable route that is (a) in this case rather than (b).

RESULTS AND DISCUSSION

The required modules that emulates a source specific multicast hash tree has been built that can handle up to thousands of nodes. The tree can manage the receiver's arrival and departure easily besides the required updates. The average delays have been calculated for different number of nodes. Figure 7 and 8 show early results that were obtained from the simulation.

Figure 7 shows that the average time for a receiver to subscribe (hash table size = 1007) is between 0.8 and 0.9 m sec. While the average time to unsubscribe is always below 0.2 m sec.

Figure 8 shows that increasing the subscribed receivers to ten folds do not affect the average subscription or departure time.

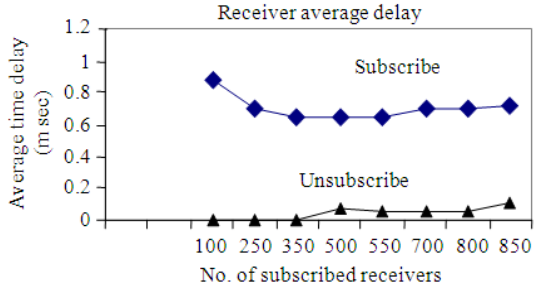

Fig.7: Results for hash tree of size 1K receivers

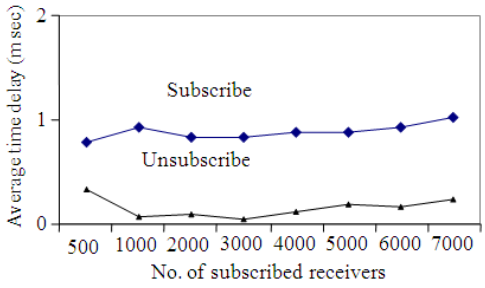

Fig. 8: Results for Hash Tree of size 10K receivers

CONCLUSION

The presented solution is a software-based and general that could be applied to both IPv4 and IPv6 networks. Another parameters such as QoS, authentication, or routing could be added for further analysis.

The key idea of the proposed scheme is to simplify address allocation and implements multicast distribution using recursive unicast hash trees. The branching nodes recursively create packet copies to implement the distribution. REHASH adopts the source-specific channel abstraction to tackle the address allocation and the sender access control problems.

Furthermore, an Express-like scheme can be used in IPv6. If the first part of the IPv6 address is placed in the first part of the 120-bit multicast address, domains can claim implicit ownership of address spaces. Using IPv6 satisfies most, if not all, of the properties for a good allocation scheme and is already supported by vendors and the IETF. Additionally, REHASH tree management provides enhanced tree stability in the presence of group dynamics.

Finally, it should be noted that many of the techniques discussed in this article could complement each other, as well as IP multicast.

REFERENCES

1. Deering, S. and D.R. Cheriton, 1990. Multicast routing in datagram internetworks and extended LANs. ACM Trans. Comput. Syst, 8: 85-110.
2. Holbrook, H. and B. Cain, 2001. Source Specific Multicast for IP. Internet Draft: Draft-Holbrook-Ssm-Arch-03.txt, Nov.2001, pp: 14.
3. Stoica, I., T.S. Eugene Ng and H. Zhang, 2000. REUNITE: A recursive unicast approach to multicast. Proceeding of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies, Mar. 26-30, IEEE XPlore Press, USA., pp: 1644-1653. DOI: 10.1109/INFCOM.2000.832563
4. Stoica, I., T.S. Eugene Ng and H. Zhang, 1999. REUNITE: A recursive unicast approach to multicast. The CMU Tech. Rep, Camegie Mellon University. http://www.cs.cmu.edu/~eugeneng/papers/00-120.pdf
5. Costa, L.H.M.K., S. Fdida and O.C.M.B. Duarte, 2001. Enabling the progressive multicast service deployment. Proceeding of the 6th IEEE Symposium on Computer Communications, July 3-5, Hammamet, Tunisia, pp: 178-183. DOI: 10.1109/ISCC.2001.935372
6. Costa, L.H.M.K., S. Fdida and O.C.M.B. Duarte, 2001. Hop by hop multicast routing protocol. RP-LIP6 Technical Report. http://www-rp.lip6.fr/site_npa/site_rp/publications.php?mots=hop+by+hop&id_publi=&cle=7&cle_externe=263&activite=&type=&hidden_valid=OK#2001
7. Boivie, R. *et al.*, 2002. Explicit multicast (Xcast) basic specification. http://tools.ietf.org/html/draft-ooms-xcast-basic-spec-03
8. Zhang, B. and H.T. Mouftah, 2005. Providing multicast through recursive unicast. IEEE Comm. Mag., 43: 1.
9. Holbrook, H.W. and D.R. Cheriton, 1999. IP multicast channels: EXPRESS support for large-scale single-source applications. ACM. SIGCOMM. Comput. Commun., 29: 65-78. http://portal.acm.org/citation.cfm?id=316194.316207
10. Diot, C., B.N. Levine, B. Liles, H. Kassem and D. Balensiefen, 2000. Deployment issues for the IP multicast service and architecture. IEEE Network, pp: 78-88.
11. Kurup, G. and Y.A. Sekercioglu, 2003. Source Specific Multicast (SSM) for MIPv6: A survey of current state of standardization and research. Proceeding of the Conference on Australian Telecommunications, Networks and Applications, Dec. 8-10, Melbourne, Australia, pp: 5.
12. Cain, B., S. Deering, I. Kouvelas and A. Thyagarajan, 2002. Internet group management protocol, Version 3. RFC 3376.
13. Deering, S., W. Fenner and B. Haberman, 1999. Multicast Listener Discovery (MLD) for IPv6. RFC 2710, pp: 22. http://www.ietf.org/rfc/rfc2710.txt, standard track
14. IANA, 1998. Internet assigned numbers authority. http://www.livinginternet.com/i/iw_mgmt_iana.htm
15. Sahar, Al-Talib, B.M. Ali, V. Prakash and M.H. Habaebi, 2003. A grouping scheme for secure multicasting in mobile IPv6. Proceeding of the IEEE 4th International Conference on Telecommunication Technology, Jan. 14-15, UiTM Shah Alam, Malaysia, pp: 106-109.