Reliable Mobile Multicast Protocol (RMMP): A Reliable Multicast Protocol for Mobile IP Networks[1]

Chien-An Ke and Wanjiun Liao

Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan
wjliao@cc.ee.ntu.edu.tw

Abstract This paper proposes a new protocol, Reliable Mobile Multicast Protocol (RMMP), for mobile networks using Mobile IP. Unlike existing mobile multicast solutions that employ bi-directional tunneling for roaming terminals to receive multicast datagrams and which is inefficient in packet delivery, wastes system resources and results in long service latency, RMMP ensures reliable multicast service for mobiles by using remote subscription. Remote subscription, however, suffers from the out-of-synch problem when data are received from the same multicast group but from different subnets while roaming from one subnet to another, thereby causing packet losses for roaming terminals. With RMMP, the mobility agent (foreign or home agent) in Mobile IP, in addition to providing mobility management, is extended to serve as the reliable multicast agent for mobiles, and routes the difference in data sequence to other agents in the adjacent subnets via tunneling. As a result, RMMP provides reliable mobile multicast services while enjoying lower delivery cost, less service latency and better routing efficiency.

Keywords: Reliable multicast, mobile multicast, Mobile IP, reliable mobile multicast protocol, RMMP

I. INTRODUCTION

IP multicasting is a key technology for many existing and emerging applications on the Internet. It avoids transmitting packets from a sender to each recipient separately, and delivers multicast datagrams unreliably as in IP unicast. Reliable multicast enables the reliable delivery of unreliable multicast datagrams to group participants. To accommodate mobile nodes, reliable mobile multicast ensures reliable delivery of multicast services for wireless mobile terminals even while roaming.

In recent years, some efforts have been made to achieve mobile multicasting. However, the problem of reliable mobile multicast has attracted less attention [1-2]. IETF Mobile IP [3] defines two options for routing multicast datagrams to mobile nodes, namely, remote subscription and bi-directional tunneling. Existing mobile multicast approaches are based on bi-directional tunneling to accommodate the join and leave dynamics in group participation and seamless roaming for mobiles [4-5]. With bi-directional tunneled multicast, a foreign agent routes the datagrams with incorrect source addresses from visiting mobiles back to the home agents of the mobiles in the respective home networks via tunneling, thereby incurring the inefficiencies of triangular routing. With remote subscription, on the other hand, a mobile re-subscribes to the joined group on the newly visited foreign network while roaming. The remote subscription multicast, however, due to network dynamics in packet delivery, suffers from the out-of-synch problem when datagrams are received from the same multicast group but from different subnets while roaming from one subnet to another, thereby causing packet losses for roaming terminals.

[1] This work is supported by the National Science Council, Taiwan, under grant number NSC 89-2219-E-002-004, and grant number NSC 89-E-FA06-2.

0-7803-6596-8/00/$10.00

In this paper, we propose a new protocol called Reliable Mobile Multicast Protocol (RMMP), based on Mobile IP remote subscription to provide both reliable multicast datagram delivery and efficient routing mechanism but avoid the out-of-synch problem. With RMMP, the mobility agent (foreign agent or home agent), in addition to providing mobility management, is extended to assume the responsibility of reliable multicast handling for mobiles, and is easily integrated with existing reliable multicast protocols to support mobility. As a result, RMMP provides reliable mobile multicast services while enjoying both low service latency as in remote subscription and high routing efficiency as in Mobile IP routing optimization.

The rest of the paper is organized as follows. Section II presents the proposed protocol, RMMP. Finally, the paper is concluded in Section III.

II. PROTOCOL DESCRIPTION

This section describes RMMP in details. In the following, we will first present the data structure of the table maintained by each mobile agent for reliable multicast service, followed by the detailed operation of the protocol.

A. Basic Mechanism

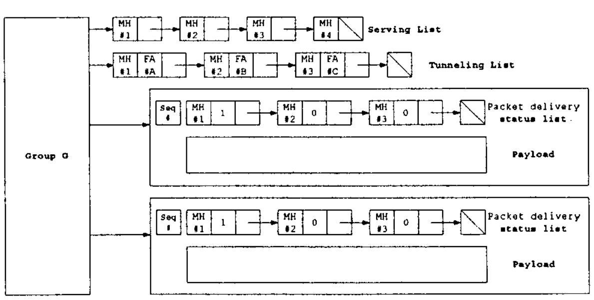

Figure 1. The data structure of the table in a mobile agent

RMMP is designed to support reliable multicast for mobile IP networks. The mobility agent, in addition to mobility management, also serves as a proxy of reliable multicast services for mobiles. On behalf of the mobiles in its affiliated subnet, the mobility agent must join the multicast group of interest, and aggregate the feedbacks collected from the mobiles to the reliable multicast agent in use. From the perspective of the reliable multicast agent, the mobility agent is a group participant periodically acknowledging data reception, and for the mobiles, the mobility agent serves as the reliable multicast agent.

The table maintained by a mobility agent to ensure reliable multicast service consists of three major components: a serving list, a tunneling list, and a packet delivery status list, on a per-group basis. Fig. 1 shows an example of the table maintained by a mobility agent. A serving list maintains the registered mobiles participating in the group, say G, in the affiliated network. A tunneling list records the mobiles previously registered with this agent but are currently roaming to adjacent networks managed by other foreign agents and requesting to recover the lost datagrams due to the out-of-synch problem. A packet delivery status list is created for each multicast packet received. It maintains the feedback status from every mobile host under the management of the respective mobility agent. Upon receipt of a multicast packet with a sequence number of *n*, the agent creates an entry in the cache as shown in Fig. 2. Every host in the serving list will be added to the packet delivery status list. For example, in Fig. 2, the serving list contains three hosts, namely MH#1, MH#2, and MH#3. 0 indicates that the corresponding host has not acknowledged the reliable reception of the packet yet. If an ACK is received, the flag is changed to 1.

The entry is removed only when all the MH's in the packet delivery status list have acknowledged.

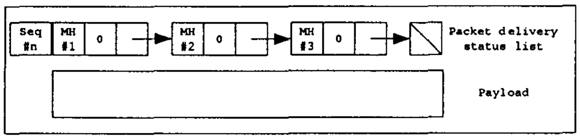

Figure 2. A packet delivery status list

B. Operation: An Overview

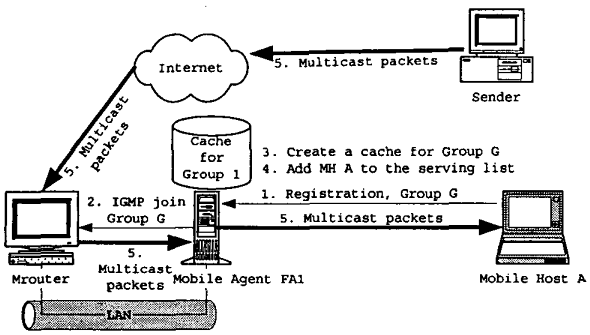

Figure 3. Join operation

When a mobile host, say *MH_A*, roams to a visited network, say subnet1, the mobile is first registered with the foreign agent *FA1*, as in Mobile IP unicast. If the mobile would like to join a multicast group, say group G, the mobile issues a join[2] message for group G to *FA1*. *FA1* then sends an IGMP-join message for the multicast group G to the immediately neighboring multicast router on behalf of the mobile if there is no other mobiles participating in group G in subnet1. Upon joining group G, *FA1* creates a cache entry, temporarily storing data received from group G. *FA1* adds *MH_A* to the serving list of multicast for group G. *MH_A* periodically acknowledges packets received in subset1 to *FA1* during its visit, and *FA1* in turn periodically acknowledges packets received by all the mobiles under its management to the reliable agent in use in the system. Upon detecting a lost packet, *FA1* retransmits the lost packet to *MH_A* for recovery purpose. The Join operation is summarized in Fig. 3.

When mobile *MH_A* roams across service boundary (say from subnet1 to subnet2), a handoff is performed so as to ensure multicast datagrams are correctly received. *MH_A* is registered with the new foreign agent *FA2*, as in Mobile IP. In addition, the mobile sends a join message for group G to *FA2*. Again, *FA2* sends an IGMP-join message for group G to the immediately neighboring multicast router on behalf of mobile *MH_A* if there is no other mobiles participating in group G in subnet2. Upon receiving a new packet in subnet2, the mobile checks if there is any offset in data packets from subnet2 to subnet1. If the packets arrived in subnet2 behind those in subnet1 due to network dynamics, the mobile sends a leave message with zero offset to the old agent *FA1*. Otherwise, the mobile treats the offset as packet losses in subnet2 and asks *FA2* to retransmit the losses for recovery. If *FA2* can recover the requested packets from its cache, the mobile sends *FA1* a leave message with zero offset; otherwise, *MH_A* sends *FA1* the leave message with an offset block, say [*a*,*b*], to be tunneled from *FA1* to *FA2*, where offset block is the difference in data sequence to be recovered between two subnets. On receipt of a leave message from a mobile host, if the leave message carries a non-zero offset block [*a*,*b*], *FA1* then removes the host from the serving list to the tunneling list; otherwise, *FA1* just deletes the mobile from the serving list. If *MH_A* is moved to the tunneling list with offset block [*a*,*b*], *FA1* tunnels data from *a* to *b* in the cache entry to *FA2*. *FA2* acknowledges the receipt of the tunneled packets to *FA1* as if *FA2* were currently in subnet1. *FA1* removes *MH_A* from the tunneling list after the retransmission. Once both the serving list and the tunneling list are empty, *FA1*

[2] which may or may not be an IGMP-Join report.

deletes the cache entry of group G and issues an IGMP-leave message to the multicast router to leave the group.

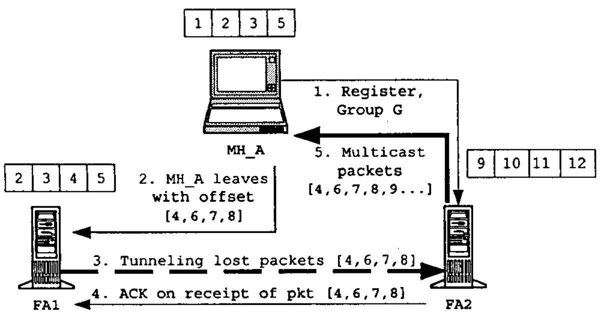

Figure 4. An example in handoff

For example, in Fig. 4, upon moving from subnet1 to subnet2 and detecting the un-repaired data packets in subnet2, i.e., *MH_A* has packets of [1, 2, 3, 5] and *FA2* caches only packets of [9,10,11,12], *MH_A* sends a leave message with a non-zero offset block of [4,6,7,8] to *FA1* to request retransmissions. *FA1* then moves *MH_A* from the serving list to the tunneling list, and encapsulates the requested packets to *FA2* via tunneling.

Note that while we have merely described roaming across two subnets, the protocol is able to handle subsequent handoffs across multiple subnets during a reliable multicast session.

III. CONCLUSION

In this paper, we have described the proposed protocol, RMMP, for reliable multicast in Mobile IP networks. Based on remote-subscription, RMMP is superior to bi-directional tunneled multicast protocols for mobiles in terms of lower delivery cost, less service latency, and better routing efficiency.

We have also conducted simulations to compare RMMP with existing reliable mobile multicast protocols. For example, Fig. 5 demonstrates that RMMP is superior to the ring approach proposed in [2] in terms of buffer requirement in each mobility agent. Due to space limitation, we did not include any other results in the paper. We will report the performance comparison of RMMP with other reliable multicast protocols for mobile networks in the future.

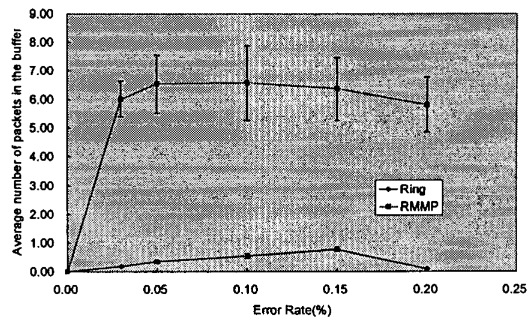

Figure 5. Performance comparison

REFERENCES

[1] K. Brown and S. Singh, "RelM: Reliable multicast for mobile networks," Technical Report, Department of Computer Science, University of South Carolina, Sept. 1995.

[2] I. Kilolaidis and J. J. Harms, "A Logical Ring Reliable Multicast Protocol for Mobile Nodes," *Proc. IEEE ICNP '99*, pp. 106-113.

[3] C. Perkins, "IP Mobility Support," *RFC 2002*, Mobile IP Working Group, Oct. 1996.

[4] T. G. Harrison et al. " Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts," *Proc. ACM MobiCom '97*, Budapest, Hungary, pp. 151-160, Sep. 1997.

[5] C. L. Williamson et al. "Performance Evaluation of the MoM Mobile Multicast Protocol," *ACM/Baltzer Mobile Networks and Applications*, v.3 no.2, pp. 189 - 201, Aug. 1998.