

Reliable Multicast with Host Mobility¹

Wanjiun Liao, Chien-An Ke, and Jiunn-Ru Lai

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

Abstract This paper studies the issue of reliable multicast with host mobility using Mobile IP. Mobile IP suggests two approaches for mobile multicasting, namely, remote subscription (MIP-RS) and bi-directional tunneled multicast (MIP-BT). However, both approaches suffer from problems when used as the basic mechanism to provide reliable multicast service for mobiles. MIP-RS enjoys efficient delivery, but suffers from serious packet losses during roaming due to using the naïve join-and-leave policy. MIP-BT is free from packet losses due to roaming; however, it suffers from the triangular routing problem, resulting in inefficient routing and wastage of system resources. We propose a new protocol called Reliable Mobile Multicast Protocol (RMMP) to provide reliable multicast services for mobile IP networks. Our approach imposes no restriction on the particular mechanisms for reliable multicast in the wired part of the network, and is easily integrated with any existing reliable multicast protocols used for stationary hosts. Being derived from MIP-RS and with the assistance of mobility agents, RMMP routes the missing datagrams due to the out-of-synch problem in adjacent subnets via tunneling to ensure optimal delivery efficiency and to ensure no packet losses from roaming. We also conducted a simulation study to evaluate the performance of RMMP. The results demonstrate that RMMP has high delivery efficiency, low buffer requirement, and high robustness, as compared to other approaches.

Keywords: Mobile reliable multicast, Mobile IP, RMMP

I. INTRODUCTION

IP multicasting is an important technology for many existing and emerging multimedia applications on the Internet. A multicast data packet, which contains a class D group address in the destination address field of the IP header, is delivered to destination group members with the same unreliable and best effort service as in unicast IP data transmission. Reliable multicast protocols ensure the end-to-end reliability of the reception of unreliable multicast datagrams for group participants, assuming the existence of multicast delivery trees provided by the underlying multicast routing protocols. A reliable multicast protocol on the Internet must employ mechanisms to cope with occasional packet losses, errors, duplication, and out-of-order delivery of datagrams. The recovery mechanisms may rely on feedback, either using positive acknowledgment (ACK) or negative acknowledgment (NACK), from the receivers to data sources to indicate correct data reception or to request retransmissions.

The challenges of reliable multicast stem from the requirement of efficiency and scalability while ensuring reliability for the protocols.

Mobile reliable multicast adds the dimension of host mobility within the scope of reliable multicast. A given multicast group may have both stationary and mobile hosts. Multicast datagrams are still delivered with the best-effort and unreliable service for group members, both in wired and wireless links, and reliable receptions are ensured by mobile reliable multicast protocols. More importantly, once a mobile has joined a multicast group, no losses or duplication in multicast datagrams would be caused by roaming, allowing the mobile to enjoy the service quality of reliable multicast as if it were a stationary host, receiving data streams continuously and reliably even while roaming.

In recent years, the study of reliable multicast for stationary hosts has been an active research field [1-4]. However, the problem of providing reliable multicast service for mobile hosts (or a mixture of stationary and mobile hosts) has attracted less attention. [5][6][7] have investigated the problem of mobile reliable multicast. In [5], the authors focused on the power and memory limitations of mobiles, and proposed to collect feedback by the base stations and then forward to the data sources. In [6], the authors proposed a three-tiered scheme that employs supervisory hosts to collect feedback which is sent to the data sources. Both [5] and [6] require the involvement of data sources and impose restrictions on the particular mechanisms used for reliable multicasting within the fixed part of the network. In [7], the authors proposed a logical ring scheme for mobile reliable multicast. The maintenance of the rings in the logical ring scheme is, however, very complicated, especially when mobile recipients dynamically join and leave the groups of interest. Besides, the protocol relies on token rotation to ensure global reliability for roaming users, causing high service latency, high buffer requirement, and low throughput for mobile receivers.

While existing work [5-7] has investigated the problem of reliable multicast for mobile hosts using different mobile technologies, this paper, attempts to study reliable multicast

¹ This work is supported in part by the National Science Council, Taiwan, under Grant Number NSC 89-2219-E-002-004 and Grant Number NSC 89-E-FA06-2.

for mobiles based on IETF Mobile IP [8], the dominant standard for IP mobility. Mobile IP supports seamless roaming for mobile terminals mainly within the scope of unicast delivery, through the cooperative support of the home agent (HA) and the foreign agents (FA) via tunneling and mobility binding. Mobile IP defines two approaches for multicasting, namely, remote subscription (MIP-RS) and bi-directional tunneled multicast (MIP-BT). However, both approaches suffer from problems when used as the basic mechanism to provide reliable multicast service for mobiles.

Remote subscription (MIP-RS) requires a mobile to re-subscribe to the joined group on the newly visited foreign network while roaming. While having the advantages of simple implementation and efficient delivery, MIP-RS suffers from serious packet losses due to using naïve join-and-leave mechanism for mobiles to participate in the groups of interest. As a result, it causes long join and graft latencies to participate in the interested group are incurred when there is no other group members in the newly visited network. In addition, due to network dynamics in packet delivery, even if there are other participants in the joined group in the newly visited network, MIP-RS still has the “out-of-synch” problem, described as follows. Hosts belonging to the same multicast group are supposed to receive the same datagrams in different subnets. However, due to differential transmission delays, as shown in Fig. 1, hosts in subnet1 may be receiving the datagram with sequence number 4, while those in subnet2 are receiving the datagram with sequence number 9. A mobile host roaming from subnet1 to subnet2 at this time will be missing datagrams 5, 6, 7, and 8. With the bi-directional tunneled multicast (MIT-BT), a mobile must subscribe to the groups of interest through the home agent. When the mobile is away from home, the multicast datagrams are first routed to the home agent, from where the datagrams are encapsulated in a unicast packet destined to the mobile via tunneling. Thus, MIP-BT allows no packet losses from roaming but suffers from the inefficient delivery of triangle routing and low scalability to accommodate the large number of mobile terminals.

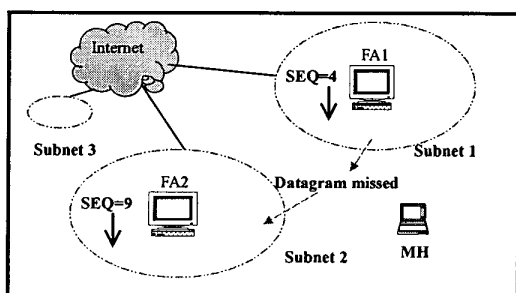


Figure 1. The out-of-synch problem in MIP-RS

In this paper, we propose a new reliable multicast protocol called Reliable Mobile Multicast Protocol (RMMP) for mobiles using Mobile IP. The performance issues of reliable multicast with host mobility using Mobile IP are studied through simulation. We compare the performance of RMMP with MIP-RS, MIP-BT, and the logical ring scheme in [7] in terms of packet losses, delivery efficiency, and buffer requirement, respectively. The results consistently

demonstrate that RMMP enjoys high routing efficiency as in MIP-RS, high robustness while roaming as in MIP-BT, and low buffer requirement as compared to the ring approach.

The rest of the paper is organized as follows. The RMMP operations are described in Section II. The performance comparisons of RMMP with MIP-RS, MIP-BT, and the logical ring approach are presented in Section III. Finally the concluding remarks are included in Section IV.

II. PROTOCOL DESCRIPTION

A. The mechanism of RMMP

RMMP is designed to support reliable multicast for mobile hosts using Mobile IP. It is derived from MIP-RS and thus enjoys the advantages of high delivery efficiency as in MIP-RS and high robustness while roaming as in MIP-BT. To ensure reliable multicast for mobiles using Mobile IP, a mobility agent (foreign or home agent) in Mobile IP, in addition to mobility management, is extended to assist reliable multicast for mobile hosts. On behalf of the mobiles in its affiliated subnet, the mobility agent must join the multicast group of interest, and aggregate the feedback 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 from the mobiles, the mobility agent serves as the reliable multicast agent. As a result, the integration of stationary and mobile recipients in a multicast group is transparent to the data sources. More importantly, this approach imposes no restriction on the particular mechanisms for reliable multicast in the wired part of the network, and is easily integrated with any existing reliable multicast protocols used for stationary hosts. Being derived from MIP-RS, RMMP allows roaming users to enjoy reliable multicast services, without suffering from the triangular delivery in MIP-BT based approaches.

The table maintained by an RMMP mobility agent consists of three major components: a serving list, a tunneling list, and a packet delivery status list (cache), on a per-group. The cache of a group, say, G, temporarily stores the multicast datagrams destined for group G in the affiliated network. The serving list maintains the registered mobiles participating in group G in the network. The tunneling list records the mobile hosts 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. The mobility agent encapsulates the datagrams requested by the mobiles in the tunneling list from the cache in unicast packets to the corresponding foreign agents in the adjacent networks, where the tunneled packets are de-capsulated, stored in the corresponding cache entries of group G and forwarded to the affiliated networks.

B. Operation overview of RMMP

When a mobile host (MH) 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 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* to the serving list of multicast for group *G*. *MH* periodically acknowledges packets received in subnet1 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* for recovery.

When the mobile is roaming across a service boundary (say from subnet1 to subnet2), a handoff is performed so as to ensure multicast datagrams are correctly received by *MH*. The mobile is registered with the new foreign agent *FA2*, as in Mobile IP unicast. 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 the mobile *MH* if there are no other mobiles participating in group *G* in subnet2. Upon joining group *G*, *FA2* creates a cache entry, temporarily storing data received from group *G*. *FA2* adds *MH* to its serving list of group *G*. Upon receiving a new packet in subnet2, the mobile checks if there is any offset in datagram sequence number from subnet2 to subnet1. If the packets received in subnet2 are behind (in terms of received sequence number) subnet1 due to network dynamics (see (1) in Fig. 2 for example), the mobile ignores the duplications and 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* sends *FA1* a leave message with an offset block, say $[a,b]$, to be tunneled from *FA1* to *FA2*, where the offset block is the difference in data sequence to be recovered between two adjacent subnets. On receipt of a tunneled packet from *FA1*, if the encapsulated packet is detected as a multicast datagram of group *G*, *FA2* will first store the multicast datagram in the cache entry of group *G* and then forward the datagram to its affiliated subnet. In this way, RMMP can solve the out-of-synch problem encountered by roaming hosts and supports cascading handoff scenarios in which the mobile moves to another subnet, say subnet3, while receiving the data for the offset block from *FA1*.

On receipt of a leave message for group *G* from a mobile host, if the leave message carries a non-zero offset block $[a,b]$, *FA1* removes the host from the serving list to the tunneling list in the entry of group *G*; otherwise, *FA1* just deletes the mobile from the serving list. If *MH* is moved to the tunneling list with offset block $[a,b]$, *FA1* tunnels data from *a* to *b*² in the cache to *FA2*. *FA1* removes *MH* from the tunneling list after the transmission has finished. Once both the serving list and the

tunneling list are empty, *FA1* deletes the cache of group *G* and issues an IGMP-leave message to the multicast router for leaving the group.

Fig. 2 shows an example of a cascading handoff scenario for a mobile that receives multicast datagrams from a joined group, say, *G*, while roaming.

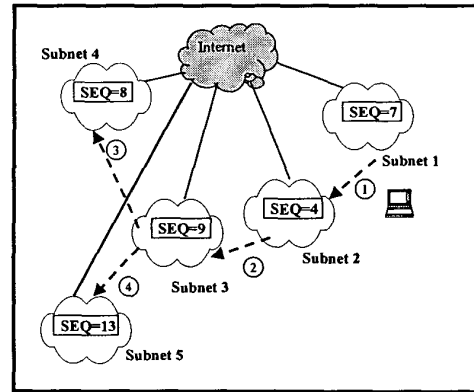


Figure 2. An example of cascading handoff

- (1) When the mobile moves from subnet1 to subnet2 (indicated by (1)), since the datagram being received in subnet2 (the one with sequence number 4, denoted as SEQ=4) is behind that in subnet1 (SEQ=7), the mobile just sends a leave message with zero offset to *FA1* after re-joining the group in subnet2.
- (2) When the mobile moves from subnet2 to subnet3 (indicated by (2)), the datagrams being received in subnet3 are ahead of those in subnet2. To recover the packet losses due to this move, the mobile sends the old foreign agent *FA2* a leave message with an offset block of $[4, 8]$, along with the address of the new agent *FA3*. On receiving the leave message, *FA2* moves the mobile from the serving list to the tunneling list, associating the mobile with the offset block $[4,8]$. *FA2* then encapsulates the datagrams 4, 5, 6, 7 and 8, when received, in unicast packets tunneled to *FA3*. Upon receipt of the encapsulated datagrams, *FA3* first saves the datagrams in the cache for group *G* and then forwards them to subnet3. In this way, the cache for group *G* in *FA3* will have datagrams starting from SEQ=4, instead of SEQ=9.
- (3) When the mobile moves from subnet3 to subnet4 (indicated by (3)) while recovering the data offset between subnet2 and subnet3 (i.e., the mobile is in the tunneling list of *FA2*), say receiving up to SEQ=5, if *FA4* can not recover the losses (i.e., datagrams 6 and 7), the mobile sends a leave message with an offset block $[6, 7]$ to the old foreign agent *FA3* to request for recovery. Similarly, if the mobile moves to subnet5 (indicated by (4)) instead of to subnet4, the mobile sends a leave message with an offset block $[6,12]$ to *FA3* to request for recovery.

² As soon as the leave message is received, some packets up to *b* may not have been stored in the cache due to not having been received in this subnet. *FA1* will keep tunneling upon receipt of datagrams within the offset block.

III. PERFORMANCE EVALUATION

This section describes the performance evaluation for RMMP. We will focus only on the problem of packet loss due to roaming and compare the performance of RMMP with MIP-RS, MIP-BT, and the logical ring approach in terms of packet losses, delivery efficiency and buffer requirement, respectively.

A. Simulation setup

This section describes the simulation setup for our experiments to compare RMMP with MIP-RS, MIP-BT, and the logical ring approach. We consider a network topology of a 10-by-10 mesh with each node connected to four neighboring nodes, and each node consists of a mobility agent associated with a multicast router and is connected to a subnet. To observe the packet losses and delivery efficiency of the four approaches, we assume that packet transmission is reliable and thus all the losses are due to roaming. Besides, we also assume all the group participants to be mobile and simulate one multicast group with one data source only, varying the group size and the mean sojourn time that a mobile stays in each subnet. The multicast delivery tree is rooted at a node randomly selected from the 10x10 mesh and grows on-demand. We randomly determine a set of N mobiles, which are initially located at N randomly selected coordinates in the mesh and are roaming across the network during the simulation. A branch is added to the multicast tree from the node the mobile is visiting in the shortest path to the root when a mobile terminal moves to a subnet where no other mobile is participating in the group. Similarly, a branch of the multicast delivery tree is deleted when no other mobiles are both in the subnet and are from the downstream interfaces. The source generates datagrams with a uniformly distributed inter-arrival time with a mean of 6 minutes.

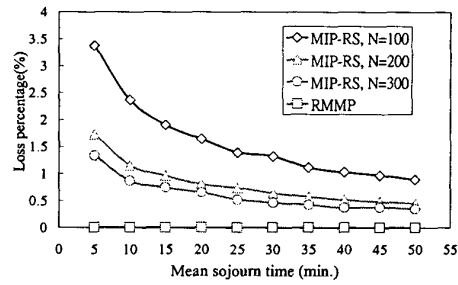
In our simulation, the mobility pattern of a mobile is described as (D, T) , where D is the direction to move, and T , the mean sojourn time to stay in the newly visited network. A mobile can move to one of the four directions of east, west, south, and north. Initially, a mobile may roam to any direction with an equal probability of $1/4$. The next move is then determined with the probability of $4/7$ for the on-going direction and that of $1/7$ for the others. T is exponentially distributed, with a mean varying from 5 to 50 minutes.

B. Simulation results

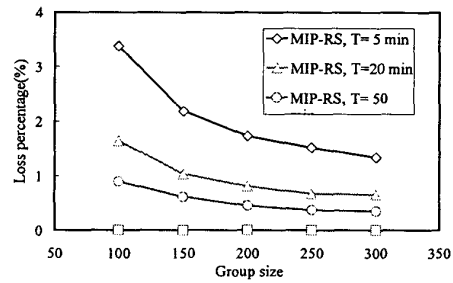
1) Packet loss

The first experiment was conducted to study the degree of packet losses from roaming for both MIP-RS and RMMP, upon varying the mean sojourn time and group size. The three curves of MIP-RS in Fig. 3 (a) for the loss percentage, defined as the number of the datagrams lost due to roaming to the total number of datagrams sent by the source, have different group size (N). The three curves in Fig. 3 (b) are with different sojourn time (T). Fig. 3 shows that RMMP is robust and has no packet losses due to roaming in all cases considered. MIP-RS, on the other hand, suffers from the out-of-synch problem and

serious packet losses, especially when the mean sojourn time is short (in Fig. 3 (a)) and group size is small (in Fig. 3 (b)).



(a) Loss percentage versus mean sojourn time for different group sizes

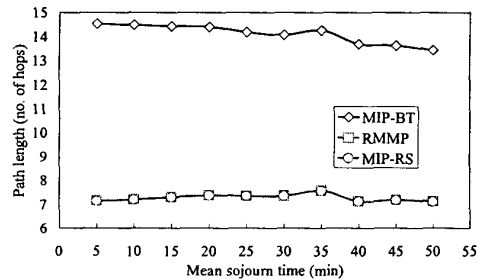


(b) Loss percentage versus group size for different sojourn times

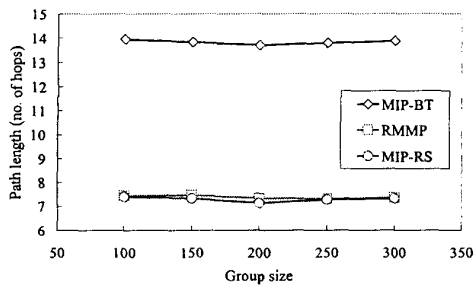
Figure 3. Packet losses

2) Delivery efficiency

This experiment was conducted to investigate the delivery efficiency of the three approaches in terms of the average number of hops each multicast datagram travels from the source to the mobiles. Fig. 4 shows that RMMP has the same efficient delivery as MIP-RS. Suffering from the triangular routing problem, the number of hops traveled by multicast datagrams when using MIP-BT is almost twice as much as that of using MIP-RS or RMMP.



(a) Loss percentage versus mean sojourn time for different group sizes



(b) Loss percentage versus group size for different sojourn times

Figure 4. Delivery efficiency

3) Buffer requirement

In [4], the authors have shown that tree-based reliable multicast protocols perform much better than ring-based protocols in terms of efficiency and scalability. For the sake of performance, it should be more desirable to have reliable mobile multicast protocols that allow local recovery and are organized hierarchically as in RMMP, as compared to global ring-based approaches as in [7]. This experiment was conducted to compare the buffer requirement of RMMP with that of the logical ring approach, both of which promises to provide reliable multicast service for mobile users. Fig. 5 shows that, for both approaches, the average buffer size increases as the error rate increases. Besides, as compared to RMMP, the ring approach requires much larger average buffer size due to its token rotating mechanism.

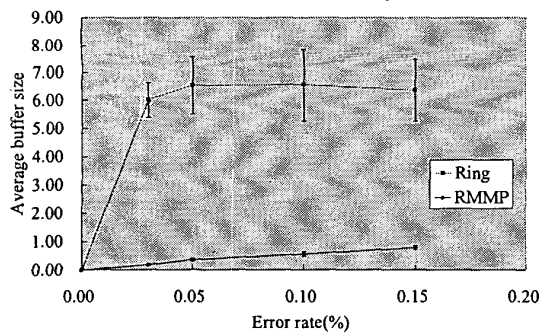


Figure 5. Buffer requirement

V. CONCLUSION

In this paper, we have proposed a new reliable multicast protocol for mobiles called Reliable Mobile Multicast Protocol (RMMP) with the characteristics of optimal delivery efficiency, robustness, scalability, simplicity, and flexibility. With RMMP, the mobility agent in Mobile IP, in addition to mobility management, is extended to assist reliable

multicasting for mobiles. On behalf of the mobiles in its affiliated subnet, the mobility agent must join the multicast group of interest, and aggregate the feedback 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 from the mobiles, the mobility agent serves as the reliable multicast agent. RMMP imposes no restriction on the particular mechanisms for reliable multicast in the wired part of the network, and is easily integrated with any existing reliable multicast protocols used for stationary hosts.

MIP-RS suffers from packet losses during roaming due to using the naïve join-and-leave policy, causing poor service quality of multicasting for mobiles as compared to stationary hosts. MIP-BT allows no packet losses from roaming, because multicast datagrams are first routed to the home agent in the home network, from where the packets are tunneled to mobiles in the visited foreign networks. Being derived from MIP-RS and with the assistance of mobility agents, RMMP routes the missing datagrams due to the out-of-synch problem in adjacent subnets via tunneling to ensure optimal delivery efficiency and no packet losses from roaming. We also conducted a simulation to evaluate the performance of RMMP, in comparison to MIP-RS, MIP-BT, and the logical ring approach. The results demonstrate that RMMP has high efficient delivery, low buffer requirement, and high robustness, as compared to other approaches.

REFERENCES

- [1] S. Floyd et al., "A Reliable Multicast Framework for Light-weight Sessions and Application Level Framing," *IEEE/ACM Transaction on Networking*, Dec. 1997, Vol.5, No. 6, pp. 784-803.
- [2] Jo-Mei Chang and N. F. Maxemchuk, "Reliable Broadcast Protocols," *ACM Transactions on Computer Systems*, Vol. 1, No. 3, pp. 151-173, Aug. 1984.
- [3] S. Paul et al., "Reliable Multicast Transport Protocol (RMTP)," *IEEE Journal on Selected Areas in Communications*, Vol. 15, No. 3, pp. 407-421, 1997.
- [4] B. N. Levine and J. J. Garcia-Luna-Aceves, "A Comparison of Known Classes of Reliable Multicast Transport Protocols," *Proc. IEEE ICNP '96*.
- [5] A. Acharya and B. Badrinath, "A Framework for Delivering Multicast Messages in Networks with Mobile Hosts," *ACM MONET*, Vol. 3, No. 4, pp. 365-379, 1998.
- [6] K. Brown and S. Singh, "RelM: Reliable multicast for mobile networks," Technical Report, Department of Computer Science, University of South Carolina, Sept. 1995.
- [7] Ioanis Kilolaidis and J. J. Harms, "A Logical Ring Reliable Multicast Protocol for Mobile Nodes," *Proc. IEEE ICNP '99*, pp. 106-113.
- [8] C. Perkins, "IP Mobility Support," *RFC 2002*, Mobile IP Working Group, Oct. 1996.