A Mobile Multicast Protocol with Error Control for IP Networks†

Chunhung Richard Lin and *Chang-Jai Chung*

Department of Computer Science and Engineering, National Sun Yat-Sen University, Kaohsiung 804, TAIWAN
Email: lin@cse.nsysu.edu.tw

Abstract – We propose a new protocol to achieve fault recovery of multicast applications in IP internetwork with mobile participants. Our protocol uses the basic unicast routing capability of IETF Mobile IP as the foundation to leverage existing static hosts reliable IP multicast models to provide reliable multicast services for mobile hosts as well. We believe that the resulting scheme is simple, scalable, transparent, and independent of the underlying multicast routing facility. A key feature of our protocol is the use of *multicast forwarding agent (MFA)* to address the scalability and reliability issues in the reliable mobile multicast applications. Our simulation results show the distinct performance advantages of our protocol using MFAs over two other approaches proposed for the mobile multicast service, namely Mobile Multicast Protocol (MoM) and bi-directional tunneling, particularly as the number of mobile group members and home agents increases.

1. INTRODUCTION

The exponential growth of the MBONE and other multicast-capable networks has led to the widespread deployment of multicast applications such as video-conferencing, news distribution. Many of these applications require data delivery guarantees from the multicast source to multiple receivers. Thus, we require reliable multicast services that work on top of the network multicast protocol to provide delivery guarantees. Conventional control schemes (e.g., TCP), used primarily in point-to-point applications, do not scale to meet the demands of large-scale multicast. In schemes like TCP, the receiver sends an acknowledgment (ACK) to the sender after receiving each uniquely numbered message. The sender is responsible for deciding which receivers have lost the message (based on missing ACK). Such a scheme would lead to *ACK implosion* with a large number of receivers, and also burden the sender with the problem of loss and retransmissions.

Providing reliable multicast support for mobile hosts in an IP internetwork complicates the problem for several reasons. First, the IETF Mobile IP protocol concentrates on unicast delivery to mobile hosts; additional mechanism must be added to those proposed to efficiently support multicast delivery. Second, the addition of mobility to the host group model implies that multicast routing algorithm must deal with dynamic member location. Third, many of the algorithms used in multicast routing protocols, such as DVMRP, MOSPF, CBT, and PIM [9], implicitly assume static hosts when setting up a multicast delivery tree. Reconstructing the delivery tree every time a multicast source moves is not always a good solution.

† This work was supported in part by Ministry of Education, Taiwan, under Contract 89-H-FA07-1-4 "Learning Technology".

We present a new approach to mobile multicast with reliable services. We call our protocol *RMoM*, for Reliable Mobile Multicast. The main idea in RMoM is to use the home agent functionality of IETF Mobile IP to support delivery of multicast datagrams to mobile hosts, while maintaining the reliability and scalability of our approach through the use of a *multicast forwarding agent* (MFA) optimization per multicast group for each foreign networks, and the use of dynamic unicast tunnels to each foreign networks.

The remainder of this paper is organized as follows. Section 2 discusses the design of reliable mobile multicast protocol, RMoM, identifying several issues raised by mobile and reliable multicast support. These are the issues that RMoM is intended to address and solve. Section 3 presents and discusses the simulation results of our reliable mobile multicast protocol. Finally, Section 4 presents the conclusions from our work.

2. DESIGN OF RMoM

Our protocol addresses the problem of reliable multicasting to mobile hosts in an IP internetwork. Adapting a static host reliable multicast mechanism to support mobile hosts as well is the main challenge. The addition of reliability to the mobile hosts implies that our protocol must deal not only with dynamic member location, but also with data loss in the network. We believe that a deployed, proven reliable multicast mechanism that already exists for static hosts on the Internet is potentially of great utility if it can be leveraged to provide the same services for mobile hosts as well. In order to support both reliability and mobility services efficiently, our protocol would use the approach proposed by Mobile IP and some existing reliable multicast protocols on the Internet to solve the related issues.

2.1. Overview of Mobile Multicast Support of RMoM

In Mobile IP, every home agent (HA) always knows the location of the mobile hosts (MHs) it serves. Therefore, it is logically feasible for a multicast HA to forward multicast datagrams by unicasting to each MH through the Mobile IP tunnel via foreign agent (FA). Like bi-directional tunneling [2], in our protocol (*RMoM*), the HA must join the multicast group when its mobile hosts subscribed to such a multicast group. That is, if the HA has some mobile hosts that need the multicast datagrams of some multicast group, the HA must join the multicast group. As shown in Figure 1(a), the HA_1, HA_2, HA_3, and HA_4 can receive multicast datagrams via the IP multicast distribution tree (it is assumed that a multicast router is co-resident with the HA) because they have mobile hosts subscribing to these multicast datagrams. In this figure, the multicast source is at the root of the multicast tree, and the HAs are members of the multicast group. In RMoM, the FA need

0-7803-6451-1/00/$10.00 © 2000 IEEE

not join the multicast group on behalf of mobile hosts that are visiting its networks, and mobile hosts that are members of a multicast group are not subject to join and graft delays every time they move. The join and graft latencies may not be much more than any handoff latencies needed by our protocol in some cases.

Since the FA need not join the multicast group, there must be some HA that takes responsibility for forwarding multicast datagrams to the FA. In the DMSP solution in MoM [2], FA selected this HA from the set of HAs of its visiting MHs to avoid the *tunnel convergence problem* [2]. That is, this solution focuses on avoiding the unnecessary duplication of multicast packets on the foreign network in the event that the HA has multiple MHs present there. However, by using this selection approach, the mobile host handoff will make the selection re-performed. In addition, the tunnel length is not easy to be further shortened because the number of the possible candidates is quite limited. While tunnel length do not constitute a violation of the IP multicast service assumptions, they would constitute an additional load on the Internet. Thus, the tunnel length is an important issue in the bi-directional tunneling method. In RMoM, we will pay more attention to this issue. If a HA in our protocol has to forward multicast datagrams to a FA, it is working as a *multicast forwarding agent, MFA*, of that FA. Since each MFA maybe serves several FAs that wish to receive multicast datagrams addressed to the multicast address for each multicast group, it forwards a copy into each corresponding Mobile IP tunnels, as shown in Figure 1(b). The MFA need not forward a separate copy for each mobile host individually, but only one copy for each foreign network at which the mobile hosts reside. Then the LAN-level multicast is used by FA at each foreign network to complete the delivery.

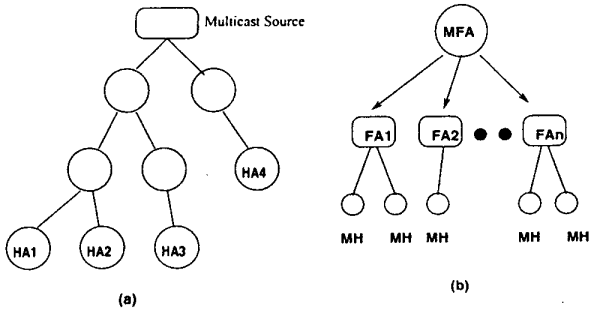

Figure 1: Multicast Distribution Tree of RMoM

Currently only two schemes were proposed for the MFA selection. They are bi-directional tunneling and Mobile Multicast protocol (MoM) [2]. In bi-directional tunneling, all multicast packages are forwarded individually to each MH by its HA, regardless of at which foreign networks the MH resides. This scheme is simple but will result in the tunnel convergence problem, and the duplicate datagram will constitute an additional load on possibly low-bandwidth links.

Let $h(M)$ denote the home agent of mobile host M; $f(M)$ could represent the foreign agent of M. In order to avoid the tunnel convergence problem, MoM protocol performs a selection at each FA to appoint one HA from the set of $\{h(MH_i) \mid \text{where } f(MH_i) = \text{FA}\}$ as the DMSP. The DMSP forwards only one multicast packet into the tunnel even if it serves multiple MHs at the foreign network. This scheme provides *at-most-once* delivery of multicast datagrams, which is identical to the semantics of IP multicast. Several different DMSP selection policies were studied in MoM. Two main performance issues were considered while performing DMSP selection: DMSP handoffs and route optimality. These two issues indeed also affect the system performance in our reliable mobile multicast protocol. From the study in MoM, the Closest-to-FA DMSP selection policy has the better average performance than the other policies.

2.2. MFA Selection Algorithms of RMoM

In order to provide shorter routing path to increase the performance of multicasting, we propose three new MFA selection algorithms and will compare their performances with the above two algorithms. The main idea of our selection algorithms is different from the one of MoM. The same issues are also considered here, i.e., MFA handoffs and route-optimality.

1. MFA handoffs: MFA handoff for a FA means the change of the MFA of the FA. This change may result from the mobile host handoff. Observe that the MFA handoffs will not only cause an increase of the number of control message transmissions, but also cause data loss in the handoff duration. Therefore, the number of MFA handoffs must be minimized as possible as we can. In MoM, each MFA of the FA is selected from the HA list of visiting MHs. Obviously, the number of MFA handoffs will be directly affected by the mobile host location change (i.e., mobile host arrival and departure). To minimize the amount of MFA handoff, the algorithms must be independent of the visiting MHs. Thus, each FA only performs the MFA selection once when the first mobile subscriber enters into its network. In addition, the selection algorithm must consider more candidates rather than only the HA list of the visiting MH to make a relatively *good* choices. Then the final choice could be better than the algorithm of MoM.

2. Route-optimality: The second issue related to MFA selection is the optimality of the routes that multicast packets take to their destinations. That is, how long is the routing path to get a multicast packet to a group recipient via the MFA, compared to routing the packet directly (i.e., remote subscription) [2] or via the home agent (i.e., bi-directional tunneling). Of course, the routing path should be as short as possible.

Next, we will describe our three new MFA selection algorithms using in our RMoM.

A. Modified MoM: This selection policy is modified from the forwarder selection algorithm of MoM. In MoM, each forwarder is selected by FA from the HA list of visiting MHs. On the way to the FA from the forwarder, there may exist a HA that belongs to the same multicast group. Thus the tunnel length could be improved if this HA is selected as the MFA of the FA. How does the FA know the existence of the HA? In our protocol, the FA issues a Search_for_MFA message to the HA of the handoff MH. On the way to the HA, if there exists a HA belonging to the same multicast group and receiving this message, it will reply to the FA and no longer forward this message. This HA then becomes a candidate of MFA for the FA. If it is a *better* choice than the current MFA, the FA appoints this HA as its MFA. Observe that this algorithm is focusing on reducing the tunnel length. It is not

necessary to get a shorter end-to-end delivery path from the source to the mobile hosts.

B. The First HA to Sender: Unlike the above algorithm, this algorithm is designed to provide the shortest end-to-end routing path from the multicast source (or sender) to the FA. When the first mobile host of a multicast group enters a new network, the FA of the network issues a Search_for_MFA message to the multicast source. On the way to the multicast source, there may exist a HA which belongs to the same multicast group and receives this request. The HA replies this request and drop the Search_for_MFA message. FA then appoints this HA as its MFA for this multicast group and no longer performs this algorithm again even though there are some other mobile subscribers of the same multicast group moving in later. That is, this selection algorithm is "static" because MFA can not be changed once it is appointed. Obviously, there is no MFA handoff. Comparing to this algorithm, the Modified MoM is "dynamic" because the MFA is dynamically changed according to the mobile subscribers arrival and departure. It is notable that in worst case there may not be any home agent on the path from the FA to the sender. In this case, the sender would become the MFA. Namely, the sender unicasts all multicast datagrams to the FA. So it is inefficient and violates the IP multicast service assumptions. If the amount of home agents is small, this situation may occur easily.

C. The Closest HA: When the first MH of a multicast group enters a foreign network, the FA broadcasts a Search_for_MFA message to search for a *good* MFA using an expanding ring search. During the search, the FA repeatedly broadcasts a Search_for_MFA request by increasing the TTL (time-to-live) value to limit the scope. When one or more HAs respond this message, the FA selects the closest HA as its MFA.

Like First-HA-to-Sender, Closest-HA is also static. They can adapt to rapid mobile subscribers location change. There is no MFA handoff occurring. The Closest-HA algorithm relies on an approximate method (expanding ring search using the TTL field) to discover HAs, send replies and then appoint the MFA. Thus, it suffers from the exposure problems. That is, non-HA hosts may receive this requests within the radius. The use of expanding ring search for MFA selection can lead to other forms of suboptimality, as well. For example, the MFA chosen by a FA can be downstream, with respect to the source of the FA. This can increase end-to-end delivery latency compared to an optimal choice of MFA.

2.3. Data Backup Schemes of RMoM

RMoM has to tackle the data loss due to unreliability of network links and mobility of mobile subscribers. In order to recover the data loss, we could buffer the entire multicast datagrams at the multicast source and all HAs during the multicast session. This allows FAs to request for retransmission for any lost data from its corresponding MFA. In some existing reliable IP multicast protocol, such as LSM, SRM, and RMTP, the data backup nodes are selected from the set of multicast receivers. In RMoM, however, we do not select the backup nodes from the receivers because they are mobile hosts. The backup node moving will make it difficult for a node to find a backup node for loss recovery. Besides, if we backup multicast datagrams at mobile receivers, the retransmission request messages and recovery messages must pass through the wireless links. Since the quality and bandwidth of wireless links is not as good as wired links, the recovery latency may be increased. So in RMoM, we simply backup the transmitted multicast datagrams in HAs and the multicast source because they are static during the session. We believe that the data backup nodes should not be dynamically changed during a multicast session since a change of backup nodes would cause serious overheads, for example, the backup data exchange from the old backup node to the new backup node.

2.4. Loss Recovery Schemes of RMoM

RMoM is designed to provide error control service for mobile multicast on IP networks. Reliability means that multicast datagrams must be successfully delivered to the mobile subscribers without any error. RMoM achieves the reliability by dividing the end-to-end reliable problem into three parts, and then guarantees the reliability in each part.

1. From the multicast source to the HAs: Since the multicast source and HAs are static, the reliability between the multicast source and HAs can be achieved by using any existing reliable multicast protocol designed for Internet. A reliable IP multicast protocol designed for static hosts (e.g., RMTP, LSM, SRM, TMTP, LBRRM) could guarantee us against all data loss in the multicast distribution tree, and each HA could successfully receive the multicast datagrams from the source eventually.

2. From MFA to the FA: MFA must forward the multicast packets to the FAs which it is serving by using Mobile IP unicast tunneling (RFC 2003 [8]). We use the NACK-based scheme to support reliability between each pair of MFA and FA. Each FA issues a data request to its MFA when it detects any data loss. Each FA has to monitor the status of the mobile hosts it serves. In RMoM, when many mobile receivers within a network lose a common packet, only their FA issues one request to its MFA for loss recovery. This can significantly eliminate the request implosion from the FA to its MFA. After receiving the request data packet, the FA uses LAN-level multicast to complete the loss recovery.

3. From FA to the mobile receivers: LAN-level multicast is used by FA at each foreign network to complete the delivery of multicast datagrams. The reliability problem is tackled by LLC (Logic Link Control) layer protocol.

Another reason that may cause data loss is the mobile host handoffs. The solution in our protocol is very simple. Each FA could request for the missing data from its MFA in which all transmitted multicast datagrams are kept during the multicast session. When entering a new foreign network, a MH has to report its status information to the FA. The status information contains the current status of the received data so far. According to this information, then the FA may request for the missing data packets from its MFA if necessary.

Here, let us closely examine if our proposed protocol could solve the following four new important issues which are absent from unicast error control: request implosion, duplicate replies, recovery latency, and recovery isolation. Because we backup the transmitted datagrams

in the source and HAs, the work of processing requests and sending retransmissions is shared among FAs, source and MFAs, not just the source only. This significantly increases the scalability. In addition, the problems of request implosion, duplicate reply, and recovery isolation are also solved since we use unicast tunnels between the MFA and FAs. It can provide *at-most-once* delivery of requests and replies. The repair of a fault in a foreign network stays only on the tunnel.Thus, There is no exposure problem. The problem of recovery latency could also be improved through different MFA selection algorithms.

3. PERFORMANCE EVALUATION

In our simulation, the network topology is randomly constructed at each time. Each node in the topology represents a LAN. Each LAN has a multicast router. Each multicast router in a LAN also acts as a base station, and it is co-resident with the HA. The home agents and foreign agents are static hosts. Our topologies are based on 10×10 mesh networks. We use Prim's algorithm to further determine the connectivity among multicast routers as was to be described in [3]. The distance between two nearby base stations is 100 meters and the power range of a wireless link is 75 meters.

In order to control the upper bound of the number of backup nodes in our simulation, we first randomly select some nodes from the network topology as the candidates of the HAs. The number of the candidates is the value of the upper bound which is an input parameter. Then we randomly deploy the mobile hosts among these candidates. A real HA must have at least one mobile host. For simplicity, we assume there is only one multicast group in our simulation. The amount of the mobile participants may be from 20 to 250. Because wireless and wired channels have quite different bandwidth inherently, two system time ticks are needed. We let the ratio of wireless time tick to wired time tick be 10. Here, we also define a wireless time tick to be the length of time to transmit a data packet through a wireless link. The mobile hosts in our simulation move uniformly in any direction at each time tick.

The purpose of the first experiment is to compare the average routing length from the source to FA. The upper bound of the number of HAs is 20. We get the simulation results by running 5000 different network topologies. The results are shown in Figure 2. As is to be expected, remote-subscription and First-HA-to-sender has the shortest routing path (both curves are overlapping). Closest-HA has better performance than MoM, Modified MoM, and bi-directional because more candidates are available to be selected as the MFA. In addition, the Modified MoM outperforms MoM since it can always find a closer MFA than MoM. The bi-directional tunneling method has the worst performance because of no choice for the MFA. It is notable that when the number of mobile receivers increases, the performance of MoM is improved. This is because with more HAs available to choose from, better choices can be made (according to the law of large numbers).

In the next experiment, we compare the average tunnel length from MFA to FA. The upper bound of the number of HAs is 20. We get the simulation results from 5000 different network topologies. These results are illustrated in Figure 3. We can observe that First-HA-to-Sender has the longest tunnel length. This is because when the

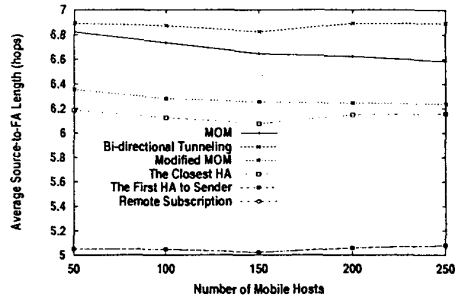

Figure 2: Comparison of source to FA route length

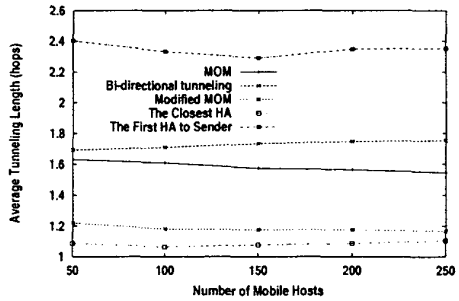

Figure 3: Comparison of tunnel route length

number of HAs is smaller, there will be few chance to choose a *good* HA as the MFA. Therefore, the average tunnel length will be longer than others. Besides, Closest-HA has the best performance because all HAs are the candidates of MFA. We can get the best one.

Figure 4 shows the average number of MFA handoff. The upper bound of the number of HAs is 30. We get the simulation results from 100 different network topologies and run 1000 time ticks for each network topology. The mobility of mobile hosts of this experiment is 1 meter/sec. Observe that First-HA-to-Sender and the Closest-HA have the least number of handoffs (both curves are overlapping) since they only need to perform the MFA selection once. The MFA handoff of both MoM and Modified MoM is sensitive to the mobile host handoff.

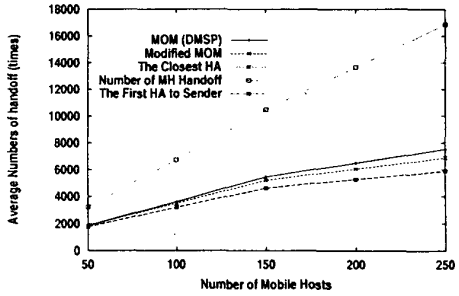

Figure 4: Comparison of MFA handoff

Like the last experiment, we compares the average tunnel length by varying the number of HAs. The result is shown in Figure 5.

Basically, this result is similar to Figure 3. It is notable that the performance of First-HA-to-Sender is improved obviously when there are more HAs in the network. When the number of HAs is more than 30, First-HA-to-Sender even outperforms bi-directional and MoM. This means that there is more chance to appear a good HA on the way from FA to the sender if there are more HAs. In addition, we can find that First-HA-to-Sender, Closest-HA, and Modified MoM are all easier to be affected by the number of HAs. More HAs can have better performance for these three methods.

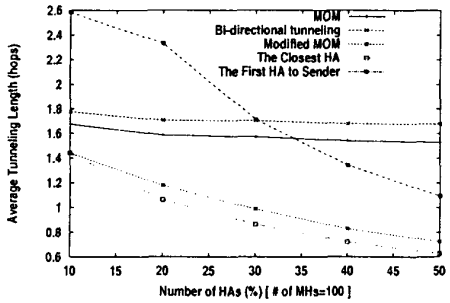

Figure 5: Comparison of tunnel length

Figure 6 shows the comparison of tunneling load of a MFA. That is, how many FAs for a MFA need to be served at most. The results of this experiment show that First-HA-to-Sender has the worst performance since all MFA are near the multicast sender. The tunneling load concentrates only on a small list of MFAs. Besides, when the number of HAs increases, the tunneling load is decreased since more HAs will share the responsibility of tunneling.

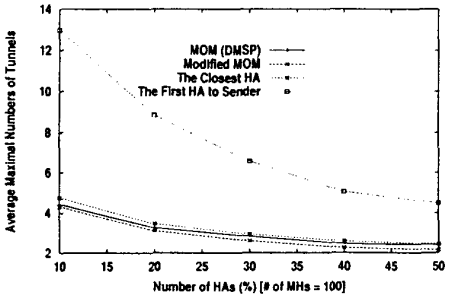

Figure 6: Comparison of tunneling load

Finally, we compare the average end-to-end delay. The results are illustrated in Figure 7. In this experiment, we consider different background traffic loads to measure the end-to-end delay. In heavy load, the system is easier to be congestion to result in data loss. Thus more retransmissions occur and the end-to-end delay is increased. Here, we simply assume that the transmission latency are only affected by the queueing delay. As is to be expected, First-HA-to-Sender has the worst performance since it has the most unbalanced tunneling load and longest tunnel length than other method on average.

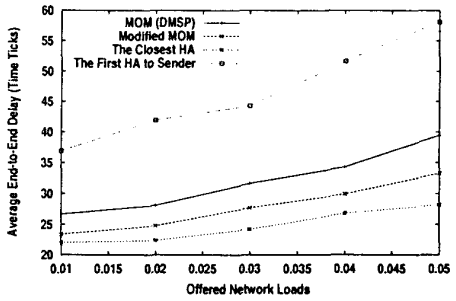

Figure 7: Comparison of average end-to-end delay

4. CONCLUSIONS

We present a new protocol, RMoM, for reliable IP multicast support for mobile hosts. RMoM extends the IP multicast by including Mobile IP tunneling concept for reliable delivery of multicast datagrams to mobile hosts. There are three new options for MFA selection that intend to reduce the routing path and MFA handoff to improve the overall system performance. The proposed mobile multicast architecture is suitable for developing reliable services. It has several features to make it practical for mobile hosts on IP internetworks as well.

We believe that such an approach offers important advantages. First, it requires minimal modification to IP multicast and Mobile IP. Second, it is designed to support reliable services for mobile hosts. Furthermore, it has scalability and performance advantages over other approaches for mobile multicast, such as bi-directional tunneling, mobile multicast protocol (MoM), and remote subscription. Compared to remote subscription model, RMoM offers great generality, less tree maintenance cost and great functionality, but must sacrifice on longer routing path for multicast datagrams.

REFERENCES

[1] S. Floyd, V. Jacobson, C.-G. Liu, S. McCanne, and L. Zhang, "A Reliable Multicast Framework for Light Weight Sessions and Application Framing,", *IEEE/ACM Transactions on Networking*, November 1996.

[2] T.G. Harrison, C.L. Williamson, W.L. Mackrell, and R.B. Bunt, "Mobile Multicast (MoM) Protocol: Multicast Support for Mobile Hosts", *Proceedings of ACM/IEEE MOBICOM '97*, September 1997.

[3] C.R. Lin, and K.-M. Wang, "Mobile Multicast Support in IP Networks", *Proceedings of IEEE INFOCOM 2000*. pp. 1664-1672.

[4] J.C.-H. Lin, S. Paul, K.K. Sabnani, and Bhattacharyya, "Reliable Multicast Transport Protocol (RMTP)", *IEEE Journal on Selected Areas in Communications*, April 1997, pp. 407-421.

[5] S. Pingali, D. Towsley, and J. Kurose, "A Comparison of Sender-Initiated and Receiver-Initiated Reliable Multicast Protocols", *IEEE Journal on Selected Areas in Communications*, April 1991.

[6] B. Rajagopalan, "Reliability and scaling issues in multicast communication", *Proceedings of ACM SIGCOMM '92*, Sept. 1992, pp. 188-198.

[7] C. Perkins (editor), *IP Mobility Support*, RFC 2002, IBM, October, 1996.

[8] C. Perkins (editor), *IP Encapsulation within IP*, RFC 2003, IBM, October, 1996.

[9] W. Stallings, *High-speed Networks: TCP/IP and ATM Design Principles*, Prentice-Hall, 1998.