An Efficient Multicast Service Switching Protocol in Mobile IP

Jiannong Cao, *Member, IEEE*, Srinivasan Mullai, David Leung, and Hui Cheng

Abstract— **Mobile IP proposes two approaches for supporting mobile multicasting, namely remote subscription (RS) and bi-directional tunneling (BT). In RS the datagrams are delivered in a shortest route but requires the deployment of a multicast router in every visited network where the Mobile Host (MH) may roam. In BT the multicast delivery tree will not be updated when members change locations. However, it suffers from non-optimal delivery path and inefficient usage of network resources because the home agent must replicate and deliver tunneled multicast datagrams to all its MHs in a unicast way. Several multicast routing protocols have been proposed to solve the aforementioned problems such as non-optimal delivery path and frequent reconstruction of a multicast tree. In this paper, we propose a new multicast service switching protocol that not only solves the multicast tree reconstruction and non-optimal delivery path but also improve the existing multicast extension of the Mobile IP to provide transparent service to multicast connections that have been established, without disruption or loss of connection due to MHs moving to another network. Another advantage of our protocol is that the home agent does not need to be a multicast router and does not need to participate in the multicast so as to reduce the control overhead of the network. We evaluated and compared the performance of our approach with the existing protocols by simulation under various environments and we observed a better performance over the existing proposals.**

Index Terms— **Mobile IP, mobile multicast, multicast service switching.**

I. Introduction

MOBILE IP [1] is defined by the IETF and has roots in a few previously developed protocols for IP mobility [2]. It has three functional entities: MH (Mobile Host), HA (Home Agent) and FA (Foreign Agent). All IP packets for the MH are first routed to its home network by regular IP routing. Then they are tunneled by the HA to the FA (care-of address: CoA), which will in turn forward them to the destination MH.

A MH can join a multicast group in two ways. First, a MH may join the multicast group through a (local) multicast router on the visited foreign network. However, if the MH moves to another foreign network, the MH will be unable to report the change of multicast group membership to the previous network. Thus the multicast routing protocol will finally prune the multicast router (assuming that there are no other members for the multicast group in the foreign network) from the multicast tree. Second, a MH can join the multicast group through its HA. But this is based on the assumption that the HA is a multicast router. If it is not, the MH cannot get multicast service from its HA.

Several problems have been encountered when providing multicast service to the MH in an IP network. First, the addition of mobility implies that multicast routing protocols must deal not only with dynamic group membership, but also with dynamic locations of MH. Many of the multicast routing protocols such as DVMRP [3], MOSPF [4] and PIM [5], implicitly assume static hosts when constructing a multicast delivery tree. Second, when the MH enters a network, where no other group member is located, the MH may experience a long delay in receiving multicast datagrams. Third, the multicast datagrams from a stationary source may not reach some networks subject to the TTL value used with the multicast datagram. Thus, the same MH may receive datagrams from the source in some networks but not in others [6].

This paper proposes an efficient multicast service switching protocol to improve the existing Mobile IP protocol, enhancing the mobility support for IP multicasting. The protocol is compatible with the existing Mobile IP protocol. It is designed to address the following issues. First, it can provide transparent multicast service for MHs. Once the multicast connection has been established, there will be no any disruption or loss of connection caused by MH movement between networks. Second, it can utilize the network resources fully. Since the MH can travel from one network to another, the protocol is smart enough to use network resources available in the local network. Third, the protocol tries to establish the connections consisting of the shortest paths.

The remainder of this paper is organized as follows. Section 2 gives a brief background and related works on multicasting in Mobile IP. Section 3 presents the detailed description of our new multicast service switching protocol. Section 4 presents performance evaluations and discussion results. Finally we conclude the paper in section 5.

II. Background and Related Work

A. BT and RS

Mobile IP proposes two approaches for supporting Mobile

The Authors are with the Department of Computing, Hong Kong Polytechnic University, Hong Kong, China (e-mail: csjcao@comp.polyu.edu.hk).

0-7803-9305-8/05/$20.00 ©2005 IEEE

multicasting: RS (Remote Subscription) and BT (Bidirectional Tunneling).

In RS, when a MH moves to a foreign network, it has to subscribe to a multicast group in order to receive the multicast datagram. If the network visited by the MH has no multicast router, the MH has to move to another network with a multicast router to get the service. The advantages of this method include an optimal routing and elimination of duplicate datagrams. The disadvantages are: first, that when the MH is highly mobile the cost of reconstructing multicast tree may be expensive, second, that the disruption in multicast data delivery occurs due to the extra delay incurred from the multicast tree reconstruction, and third, that source mobility is not handled.

In BT, the MH sends and receives multicast datagrams through its HA using the Mobile IP tunnels. Although this approach efficiently handles source mobility and recipient mobility, it has a number of disadvantages. First, it conceals host mobility from all other members of the group. As a result of this concealment, the multicast delivery tree will not be updated when members change locations. Second, Bi-directional tunneling causes the HA to waste network resources because HA must replicate and deliver tunneled multicast datagram to all its MHs in a unicast way, regardless of which foreign networks they reside on. This also limits the scalability. Third, the routing path used by BT for multicast delivery can be far from optimal.

B. *Mobile Multicast Protocols*

In BT, each HA creates a separate tunnel to the FA so that multicast packets can be forwarded to their MHs. If these MHs belong to the same group, all of the tunnels from different HAs to the FA would carry the same multicast packets and result in packet duplication. This is called as "tunnel convergence problem". Harrison et al. [7] proposed the protocol MoM to solve the tunnel convergence problem in BT. The method is to select only one HA among the given set of HAs called DMSP (Designated Multicast Service Provider).

But MoM protocol still has some problems. It will result in packet loss if the MH belonging to the currently serving DMSP moves out. When a mobile host handoff occurs, its HA can learn about the new FA of the MH immediately using Mobile IP protocol, but the previous FA can not know the handoff until the timeout. So, before the new DMSP is selected, none will serve the MHs in the previous network. During this period, multicast packets to the MH will be lost. For MoM, if the number of mobile group members is small (i.e. in sparse mode), the DMSP handoff will occur frequently. This has the adverse effect of increasing the network traffic. In MoM, a MH can receive the datagrams from the DMSP and also from the multicast router in the foreign network in turn that results in duplicating multicast datagrams. Packets that are sent and received by MHs must always traverse the home network that also makes routing non-optimal.

RBMoM [8] overcomes the disadvantages of MoM based on the concept of Multicast Home Agent (MHA) and service range. RBMoM selects a router called Multicast Home Agent, which is responsible for tunneling multicast datagrams to the FA to which the MH is currently registered. MHA should be one of the multicast group members. Each MH can have only one MHA. Moreover, MHA is changed dynamically according to the location of the MH whereas the HA of a MH never changes. The MHA can only serve a MH which is within its service range. If the MH is out of the service range of MHA, then MHA handoff will take place and another MHA will serve the MH. The main drawback of this protocol is that if the service range of MHA is larger, the tree update will be much slower and multicast datagrams will be forwarded through a longer tunnel which results in high cost of tunneling and MHA maintenance. During DMSP handoff, there also will be a disruption in multicast service.

MMROP [9] provides recipient mobility based on RS. The disadvantage of this scheme is that if there is no multicast router in the visited network then disruption in multicast service occurs. The MMA [10] introduces the multicast agent (MA) and multicast forwarder (MF) to reduces data delivery path length and decreases the amount of duplicate copies of multicast datagrams. MMG [11] introduces the concept of mobile multicast gateway and integrates it with the hierarchical mobile IP to manage mobile multicasting. The main drawback of this approach is that it depends on the MMG entity, which constitutes the single point of failure.

III. Multicast Service Switching Protocol

Our protocol intends to solve the problems of non-optimal delivery path, inefficient usage of network resources and frequent multicast tree reconstruction. It provides transparent multicast service by compressing the datagram delivery path and avoiding service disruption. To fully utilize network resources and reduce inefficient multicast routing, three mechanisms are designed. First, after moving to another foreign network, the MH still needs to respond to IGMP [12] host membership query in previous foreign network. Second, maintain the connection between the MH and its previous foreign network. Third, enable multicast service switching among networks to support MH mobility.

A. *Overview of the Protocol*

When a MH moves to a foreign network, it can join the multicast group through the HA in the home network. But in this way, extra load caused by data encapsulation and IP tunneling has to be imposed to the HA to redirect the datagrams to the MH. This will overload the HA which results in poor network performance for the home network. Also this protocol is not supported if the HA does not support multicasting. But if the MH can request multicast service to a multicast router located in the current foreign network, the extra workload imposed to HA can be eliminated because datagrams are delivered directly from the FA to the MH. Thus the local network resources in the foreign network can be used efficiently. Also it is better to use more local resources than

remote network resources.

Generally a MH always re-subscribes to the multicast group when entering a foreign network, denoted as FN1, if FN1 has multicast router. Later if it moves to another foreign network FN2 without multicast router, the multicast services are then disrupted. This is because the MH does not respond to the IGMP host membership query message of the multicast router in FN1. Due to the lack of host membership report, the multicast router in FN1 will think that there are no members for this multicast group. Hence the multicast protocol will finally prune the multicast router from the multicast tree. But if the multicast router in FN1 continues supporting the multicast service until the MH finds an available multicast router in another foreign network, transparent services can be achieved.

In our protocol, such continuous and transparent multicast services will be provided to improve the existing Mobile IP multicast extension. We denote the multicast router in FN1 as FA1. Also, nine messages are created in our protocol, which are listed as follows.

1. MRM –Mobile host Requests Multicast
   Sender: MH, Receiver: FA;
   Action: MH requests continuous multicast service to the visited network. It contains MH's home address, care-of address and list of multicast addresses.
2. FAM – Foreign Agent Acknowledges
   Sender: FA, Receiver: MH;
   Action: FA notifies MH for support of continuous multicast services. It contains care-of address and list of multicast addresses.
3. MLN – Mobile host Leaves the current Network
   Sender: FA, Receiver: MH;
   Action: FA detects if the MH has left the current network. Once a MH has left, FA deletes the content of the MH's care-of address field or CoA field and sets E field to 1. Trigger mechanisms to response to IGMP message and buffer the datagrams destined to MH.
4. MNL – Mobile host New Location
   Sender: MH, Receiver: FA;
   Action: MH notifies FA about its new location and reset E bit to 0. It contains MH's home address and new care-of address.
5. MJM – Mobile host Join new Multicast
   Sender: MH, Receiver: FA;
   Action: MH notifies FA about joining new multicast group. It contains MH's home address and new multicast address.
6. MMC – Mobile host Multicast Connection
   Sender: MH, Receiver: FA;
   Action: MH sends this message to FA for continues multicast support. It serves as a heart beat of MH. It contains list of multicast addresses.
7. MCC – Mobile host Close Connection
   Sender: MH, Receiver: FA;
   Action: MH sends this message to FA to close the support of a specific multicast connection.
   It contains list of target multicast addresses.
8. MSQ – Multicast Switching Query
   Sender: MH, Receiver: FA;
   Action: MH requests for switching multicast service to the current FA.
9. MSR – Multicast Switching Reply
   Sender: FA, Receiver: MH;
   Action: FA agrees to switch the multicast service.

When the MH leaves FN1, extra fields are added to the routing table maintained by FA1. These fields record the MHs' home address, care-of address, E bit, L bit and timestamp. An additional field for MH's new care-of address is also added. The 'E' bit indicates if the MH has left the current foreign network. The 'L' bit indicates if the MH has returned its new care-of address. The 'L' bit must be set if the MH is using a new care-of address, which will also be recorded. Then the FA1 should tunnel the datagram to the new care-of address. The E bit is set when the MH notifies FA1 that it will leave FN1. When the MH moves back to the FN1, the E bit will be reset and both the connection mechanism and IGMP proxy service provided by FA1 will be stopped. The timestamp field is renewed once an MMC message is received. It serves as a resource cleanup flag for unexpected disconnection. If the timestamp is not updated for a certain period, the records about the MH will be deleted and the resources held for the MH will be released. These fields keep track of the connection between the FA1 and the MH when the MH moves out of FN1 and still uses the multicast services provided by FA1. With the MH's new location information, FA1 can then tunnel all the multicast messages to the MH.

B. Maintain Connection between MN and FN1

In our protocol, the MH registers its multicast service request by sending an MRM message to FA1 when it enters FN1. If FN1 can provide multicast service, FA1 will acknowledge a FAM message to the MH. Once the MH receives the FAM message, the MH will periodically send an MMC message to FA1 to indicate that it is still using the multicast service. This MMC message serves to tell FA1 that the MH is still alive. Periodically, FA1 will send a MLN message to check whether the MH has moved to another foreign network.

Periodically, FA1 will send an MLN message to check whether the MH has moved to another foreign network. Once FA1 detects that the MH is away from the current network FN1, it will de-register the care-of address of the MH and set the E bit to 1. The E bit triggers the FA1 to buffer the packets sent to MH until it receives MNL message from the MH. During this procedure, FA1 can report, on behalf of the MH, about its multicast status to the multicast router in FN1. Thus, the IGMP protocol will not prune the multicast router in FN1 from the multicast tree. When the MH reaches another foreign network FN2 without multicast router, it sends a MMC message to FA1 for continuous multicast services registration. This enables FA1 to be aware that the MH is continuously using the multicast services even it has left FN1. The MH also sends a MNL message containing its new care-of address to

FA1.

The connection mechanism between the MH and FN1 will be triggered so that FA1 can tunnel the IGMP host membership query to the MH. In the connection mechanism, FA1 will be responsible for maintaining a record of the MH including home address, co- located address or CoA, new care-of address, the location information and the timestamp. With this information, FA1 can tunnel the multicast message to the new care-of address. If the MH wants to join a new multicast group, it will send an MJM message to FA1, which participates the multicast session on behalf of the MH.

When the MH wants to leave the multicast group or establish the multicast connection with another multicast router, a MCC message will be sent to the FA1. FA1 will terminate the service and release all the resources. The situation here is similar to joining the multicast group through the home network but the only difference is that the service is now provided by FA1 instead of HA.

C. *Enable Multicast Service Switching*

In order to use the network resources efficiently, when the MH moves from FN1 to FN2, it should send a MSQ request to FA2 (the current FA in FN2) for switching multicast services from the multicast router in FN1 to the multicast router in FN2. FA2 will reply a MSR message to the MH if it agrees to establish a multicast connection for the MH. The MSR message from FA2 contains the average stay duration for every visited MH in FN2. Meanwhile, the MH should maintain two timers: the threshold timer and the delay timer. The threshold timer prevents instant multicast switching setup due to the roving of MH between the boundaries of the two networks. After the threshold timer expires, the MH will compare the value of its delay timer and the reported average stay duration. If the average stay duration is greater than the delay time, the MH will join the multicast group in FN2 and a MRM message will be sent back to FA2 for multicast service request. Otherwise, the MH will start the switching process after the delay timer expires. Once the switching is finished, the MH will send a MCC message back to FA1 to terminate the previous multicast service.

For efficient use of network resources, the MH should always try to switch service providers to the current local network if possible.

Even though the MH has moved to FN2, FN1 should not release the care-of address of the MH until the MH terminates the multicast service in FN1. The reason is that the MH may use this care-of address as a source IP address to send multicast messages to the multicast group. The MH should also maintain information about the IP address of the "multicast service provider" in foreign network. This information enables the MH to identify sources for the tunneling datagram. In case security is needed, public and private key algorithms may be used for identification of the trusted host.

IV. Performance Evaluations

The performance of our protocol has been evaluated using a discrete-event simulator and compared with that of Bi-directional Tunneling and MoM with various numbers of MHs. The simulation parameters used in the study are given in Table 1.

Each HA must maintain an away list to keep track of which of its own MHs are away and similarly each FA maintains a visitor list to keep track of the MHs that are currently in its domain. When a MH arrives at a foreign network, it informs the FA about its wish to join the multicast group. Once the FA receives the join request, it will check whether it is currently serving the multicast group. If so the MH switches its multicast service to the current FA. Otherwise in order to avoid the disruption in multicast service, a temporary bidirectional tunnel will be created between the current FA and the previous multicast agent with whom the MH previously got the multicast service.

The following analysis as in [13] illustrates the advantage of our approach over BT. Let M be the number of multicast routers in the networks (M<N), G be the number of multicast groups, c be the average number of MHs at each foreign network, R be the number of redundant DMSPs forwarding multicast packets to the MHs. The number of multicast messages in the network for BT will be O(c*N*M*G). In our approach the number of multicast packets will be O((N-M)*G).

Table 2 contains the comparison information on important factors for using home agent, improved foreign agent, or the improved foreign agent with switch mechanism as a multicast service provider. In the same sequence, they correspond to three protocols: BT, MoM, Our protocol.

The MHs can be either in the home network or in the visited network. In our approach at first the MHs begin their simulation at their home network and are allowed to move to the foreign network. We vary the number of MHs from 1 to 29 at each domain. The mobility rate of the MH, network load

TABLE I
SIMULATION PARAMETERS

Parameters	Description	Values
N	number of LANs	400
S	sources per multicast group	1
MH	number of MHs	1-29
MR	mobility rate of the MHs	0.1-0.5
ST	service time	1 unit
JD	join delay	1 unit
Time	total simulation time	100 units

TABLE II
COMPARISON OF TRANSPARENT MULTICAST SERVICE BY DIFFERENT AGENTS

	HA (BT)	MoM	FA Switching
redundant packet delivery	Yes	Yes	No
multicast reconfiguration	No	No	Yes
delivery overhead	Heavy	Medium	Low
resource usage efficiency	Low	Medium	High
transmission mode	Unicast	Unicast	Multicast
multicast optimization	Low	Low	High

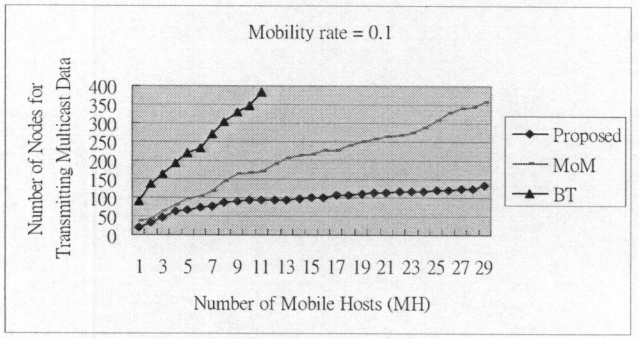

Fig. 1. Comparison of network load (MR =0.1).

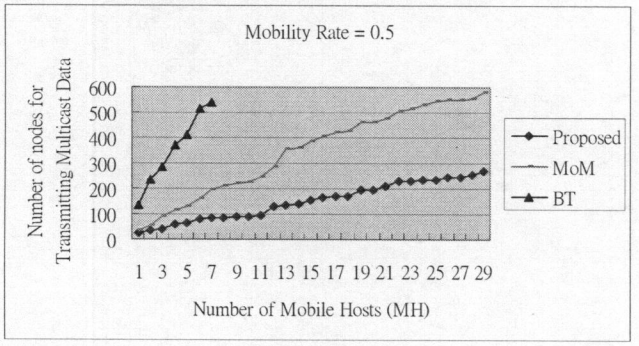

Fig. 2. Comparison of network load (MR =0.5).

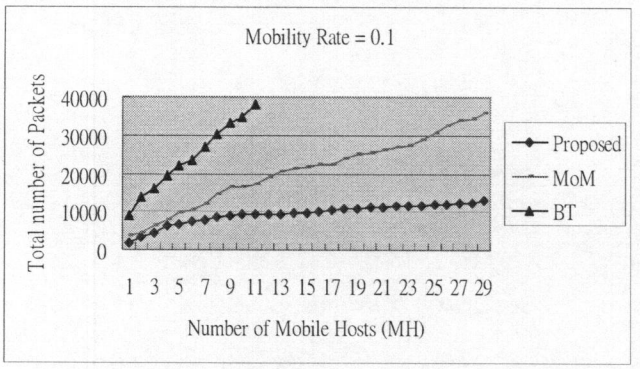

Fig. 3. Comparison of multicast traffic load (MR =0.1).

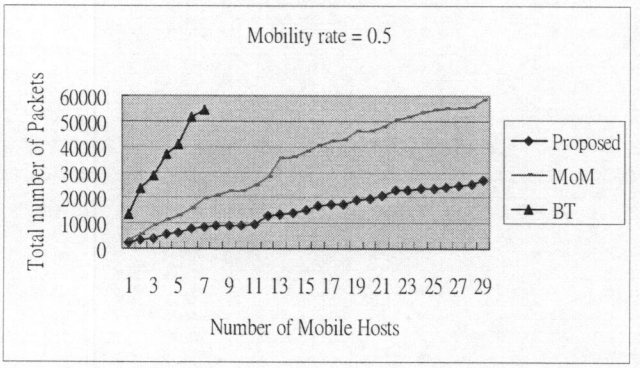

Fig. 4. Comparison of multicast traffic load (MR =0.5).

and handoff rate are the important factors considered in our simulation experiment. The total network load is represented as the number of transmitted packets to the MHs, which can be considered as the traffic occurred by tunneling the

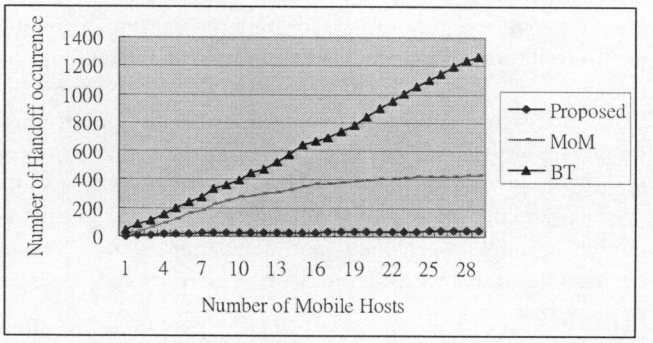

Fig. 5. Comparison of handoff rate with tree join operation (MR =0.7).

datagrams from the forwarding agent (either HA or FA). The network load increases with the increase of mobility rate because the speed of the MH may increase the frequency of the handoff that results in both high tree reconstruction overhead and network congestion. Fig. 1 and 2 show the number of nodes (hosts involved in tunneling) involved in forwarding multicast packets to the MHs. Fig. 3 and 4 compare the network load with that of BT and MoM with various mobility rate (0.1 and 0.5). It can be seen that an improved performance in the network load is achieved by our protocol.

As is evident from the figure, our protocol achieves low network load when compared to BT and MOM at different mobility rate. The reason is that our protocol gets the multicast service from the local network and needs no tunneling. When the MH joins the multicast group with the improved FA in the current network, local resources are used instead of the remote resources from the home network. The efficiency of resource usage can also be increased since more multicast rather than unicast transmissions can be used. It also reduces unnecessary data encapsulation. Although there is some overhead on the protocol for using the improved FA as a multicast service provider, the availability of the service can be guaranteed and the transparent multicast service can be provided. Multicast routing can also be optimized since the FA is closer to the actual physical location of the MH. Switching to the current FA as a multicast provider from the previous can further optimize the network resource usage.

Frequent handoffs may cause extra network load and degrade the performance of the protocol. Fig. 5 compares the multicast service switching handoff rate with that of MoM and Bi-directional Tunneling handoff.

V. Conclusion

This paper addresses the limitations of the existing multicast extensions to Mobile IP protocol and proposes an efficient multicast service switching protocol. The design of the protocol is based on three major criteria: compatibility with the existing Mobile IP protocol, provision of transparent multicast service to the MH, full and efficient utilization of network resources. Using our multicast service switching protocol, the MH receives the multicast datagrams directly from the multicast router in the current network or accepts

tunneled multicast services from the previous FA. The procedure of accepting tunneled multicast services is similar to BT but the difference is that in BT the datagrams are tunneled in a unicast way where as in our protocol the datagrams are delivered in a multicast way. With these improvements, the protocol can provide transparent service to the MH and utilize the network resources fully and efficiently. We compare the performance of our protocol with the existing mobile multicast protocols by simulation under various environments and we observe a better performance over the existing protocols.

ACKNOWLEDGMENT

The work is supported by the University Grant Council of Hong Kong under the CERG Grant B-Q672 (PolyU 5170/03E).

REFERENCES

[1] C. Perkins, "IP Mobility Support for IPv4," RFC 3220, January 2002.
[2] D. Johnson, "Scalable and Robust Internetwork Routing for Mobile Hosts," Proc. of the 14th International Conference on Distributed Computing Systems, Amsterdam, Netherlands, June 1994.
[3] D. Waitzman, C. Partridge, S. Deering, "Distance Vector Multicast Routing Protocol," RFC 1075, November 1998.
[4] J. Moy, "Multicast Routing Extensions for OSPF," Communications of the ACM, Vol. 37, No. 8, pp. 61-66, August 1994.
[5] S. Deering, D. Estrin, D. Farinacci, V. Jacobson, C. G. Liu and L. M. Wei, "The PIM Architecture for Wide-Area Multicast Routing," IEEE/ACM Transactions on Networking, Vol. 4, No. 2, April 1996.
[6] A. Acharya, A. Bakre and B. Badrinath, "IP multicast extensions for mobile Internetworking," Proc. INFOCOM 1996, SanFrancisco, CA, March 1996.
[7] T. G. Harrison, C. L. Williamson, W. L. Mackrell and R. B. Bunt, "Mobile multicast (MoM) protocol: multicast support for mobile hosts," Proc. of the 3rd annual ACM/IEEE international conference on mobile computing and networking (MobiCom), Budapest, Hungary, September 1997.
[8] R. Lin and K. M. Wang, "Mobile multicast support in IP networks," Proc. INFOCOM 2000, Israel, March 2000.
[9] J. R. Lai and W. J. Liao, "Mobile multicast with routing optimization for recipient Mobility," IEEE Transactions on Consumer Electronics, Vol. 47, No. 1, pp. 199 –206, Feb 2001.
[10] Y. J. Suh, H. S. Shin and D. H. Kwon, "An efficient multicast routing protocol in wireless mobile Networks," Wireless Networks, Vol. 7, No. 5, pp. 443-453, September 2001.
[11] M. H. Ye, L. Y. Yang, L. Yu and H. M. Zhang, "The implementation of multicast in Mobile IP," Proc. IEEE Wireless Communications and Networking Conference, New Orleans, Louisiana, March 2003.
[12] W. C. Fenner, "Internet Group Management Protocol, Version 2," RFC 2236, November 1997.
[13] V. Chikarmane, C. L. Williamson, R. B. Hunt, and W. L. Mackrell, "Performance evaluation of the MoM mobile multicast protocol," Mobile Networks and Applications, Vol. 3, No. 2, pp. 189–201, 1998.