Efficient algorithm for mobile multicast using anycast group

W.Jia, W.Zhou and J.Kaiser

Abstract: The authors present a novel and efficient multicast algorithm that aims to reduce delay and communication cost for the registration between mobile nodes and mobility agents and solicitation for foreign agent services based on the mobile IP. The protocol applies anycast group technology to support multicast transmissions for both mobile nodes and home/foreign agents. Mobile hosts use anycast tunnelling to connect to the nearest available home/foreign agent where an agent is able to forward the multicast messages by selecting an anycast route to a multicast router so as to reduce the end-to-end delay. The performance analysis and experiments demonstrated that the proposed algorithm is able to enhance the performance over existing remote subscription and bidirectional tunnelling approaches regardless of the locations of mobile nodes/hosts.

1 Introduction

Mobile computing requires wireless communication, mobility and portability. Mobile multicast [1] is an important service for mobile applications through wireless and connection to the Internet, such as email communication, query database, retrieving information, video conferencing through wired networks etc. The provision of a multicast service to mobile nodes is a complex task especially in the wireless environment. The physical constraints of mobile communications typically include low bandwidth of link layer connection, high error rates, and temporary disconnection. IP multicast [2] provides unreliable multicast delivery for wired networks. In mobile multicast communications, two issues are of primary importance: one is for mobile nodes and mobility agents to discover each other's presence, and another is the datagram routing efficiency. Traditional multicast research discussed reliability of message delivery in the multicast group in guaranteeing properties such as total ordering, atomicity, dynamic group membership and fault-tolerance etc. [3].

Some well known wireless multicast systems have been developed. Forwarding pointers and location-independent addressing to support mobility has been discussed [4], but the multicast service is unreliable. A host view management protocol (HVMP) has been developed that provides reliable multicast for mobile nodes [5]. However, it does not allow dynamic group membership. Brown and Singh [6] have proposed a protocol that allows dynamic group changes and reliable multicast message delivery with different network architectures. Multicast tunnelling is proposed for forwarding multicast packets from one foreign network to another when the mobility agent receives packets addressed to mobile nodes that are nomadic [7].

1.1 Problems with mobile IP

Mobile IP [1] defined three approaches to support mobile connection and multicast: first, agent discovery, where home agents (HAs) and foreign agents (FAs) may advertise their availability on each link for which they provide service. A newly arrived mobile node can send a solicitation on the link to learn if any prospective agents are present. Secondly, remote subscription, when a mobile node is away from home, it registers its care-of address (an IP address at the mobile node's current point of attachment to the Internet when it is not attached to the home network [1]) with its home agent. Depending on its method of attachment, the mobile node will register either directly with its home agent or through a foreign agent, which will forward the registration to the home agent. Thirdly, bidirectional tunnelling multicast, in this case unicast tunnels are used to encapsulate and to send multicast packets over the Internet when the intermediate routers cannot handle multicast packets. For multicast datagrams to be delivered to the mobile node when it is away from home, the home agent has to tunnel the datagrams to the care-of address. A mobile node is addressed on its home network that is known as its 'home address'. Agent discovery may require more advertisements and solicitation messages. Remote subscription is inefficient for dynamic membership and location change of mobile nodes. Bidirectional tunnelling multicast may cause the tunnel convergence problem with packet duplication [5] (Fig. 1).

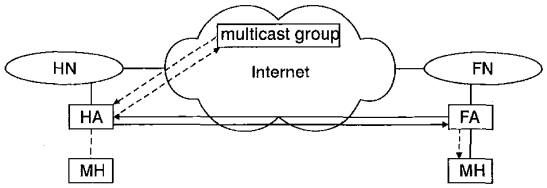

Fig. 1 *Bidirectional tunnelled multicast method*
FA – foreign agent; FN – foreign network; HA – home agent; HN – home network; MH – mobile host

IEE Proceedings online no. 20010211

DOI: 10.1049/ip-com:20010211

Paper first received 9th August 1999 and in revised form 24th July 2000

W. Jia is with the Department of Computer Science, City University of Hong Kong, 83 Tat Chee Avenue, Hong Kong

W. Zhou is with the School of Computer Science and Mathematics, Deakin University, 662 Blackburn Road, Melbourne, Australia

J. Kaiser is with the Department of Computer Structures, University of Ulm, James-Franck-Ring, 89069 Ulm, Germany

1.2 Motivation of the research

The anycast address and service have been defined for Internet protocol version 6 (IPv6) [7]. It is a communication for a single sender sending to the 'nearest' member in a group of receivers, preferably only one of the servers that supports the anycast address [8]. It uses a unicast address and the router can register the anycast address for its interface. Anycast is useful when a host requests a service from a server in a group but does not care which server is used. Anycast can simplify the task of finding an appropriate server. For example, users can use the anycast address to choose the mirrored FTP sites and to connect to the nearest (available) server.

To improve the efficiency in terms of mobile IP on multicast communication, particularly in terms of the three issues mentioned above, we propose a novel efficient mobile multicast protocol (MMP), taking advantage of anycast routing technology. The MMP has two aims: first, mobility agents (MAs, both HAs and FAs) anycast group to facilitate flexible connections for mobile nodes. Using a well known anycast address, the HAs need not multicast/broadcast router advertisement and the mobile nodes may register directly through the well known anycast address of the anycast agent groups so as to reduce the connection cost for the mobile nodes. Secondly, an anycast address is configured by a group of multicast routers on the subnet that are designed to support a specific multicast group. Using anycast can dynamically select the paths to the multicast router to reduce the end-to-end multicast delay. The second issue has been considered in [9, 10] and we omit the discussion in this paper due to lack of space.

2 Our mobile multicast protocol (MMP)

Before describing the protocol, the following assumptions are made (see Fig. 2 for example of MMP topology):

- A set of hosts and mobile nodes forms a multicast group G. Each individual mobile node has knowledge of the multicast group id to which it wishes to transmit and accept multicast messages.
- HA and FA are special routers that provide service for the attachment of mobile nodes.
- There is at least one MA in each subnet.

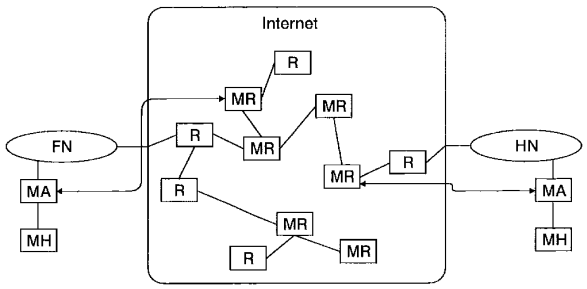

Fig. 2 *MMP topology and mobile connections*
MA – mobility agent
MH – mobile host
FN – foreign network
HN – home network
R – router does not support multicast
MR – router supports multicast
↔ tunnel from MA to MR

A multicast router can configure its interface to route both multicast and anycast packets [9]. Each MA maintains four lists for the dynamic memberships of mobile nodes in multicast group G: the membership list, $ML(G)$, contains the IDs of members in group G; the visitor list, $VL(G)$, records the IDs of foreign mobile nodes that belong to G that visit this MA; the away list, $AL(G)$, records the IDs of mobile nodes in G that departed (or were disconnected) from this MA; finally, the tunnelling list, $TL(G)$, records the IDs of foreign agents that are interested in transmission/reception of multicast packets for G. The MMP is designed in three major phases that work interactively:

(i) Initialisation phase: configurations of multicast and anycast group for routers, mobility agents and mobile nodes;

(ii) Registration and membership phase: registrations and reformation for the dynamic membership of mobile nodes;

(iii) Multicast transmission phase: multicast packet transmissions and deliveries for the group of members including station hosts and mobile nodes.

2.1 Phase 1: Initialisation

(i) Membership initialisation for a given group of G: an individual MA sets $ML(G) = VL(G) = AL(G) = TL(G) = \{\}$.

(ii) Multicast tree formation: The core-based tree (CBT) technique is used to build a multicast propagation tree for the routers (called a CBT tree). One router is selected as the core (or root) of the tree. To establish such a tree, MAs that provide multicast service for G must join the CBT tree by linking themselves to the core [10, 11]. All routers including MAs in the tree are called ontree routers.

(iii) Mobility agent anycast group configuration: the mobility agents that offer attachment for mobile nodes in G form an anycast group [9]. All the mobility agents that provide connections for G can register through well known group reserved anycast address G_A [8] and configure one of its interfaces to accept the registration for home/foreign mobile nodes. Our protocol defines that the agents in the same anycast group G_A will share the same authentication for mobile node registrations, i.e. $MA_1 \in G_A$ and $MA_2 \in G_A$ imply that both MA_1 and MA_2 agree to delegate connection authentication and multicast packet delivery to each other for the mobile nodes that were previously attached to another party.

(iv) Ontree router anycast group configuration: for the group G, virtual anycast address T_A is assigned to and configured by all routers in the CBT tree for group G [9]. The router configurations are classified as ontree and offtree:

- Ontree router configuration: For a multicast group G, when the CBT tree is built, all ontree routers (including the core) are selected to join an anycast group with anycast address T_A which is advertised to the network (broadcast by the core). T_A may be considered as some 'temporary' anycast address as long as the CBT tree exists. For any ontree router, there is a forwarding information base (FIB) used as its multicast routing table [9, 11]. An entry in the FIB has the form <G, input-interface, output-interfaces>.
- Offtree router configuration: Upon reception of address T_A broadcast from the core in the CBT tree, the offtree routers, including those foreign agents, that are interested in transmitting multicast packets to G will assign T_A as an interface entry by configuring with <T_A, G> mappings in the routing table. The anycast routing table enables the router to dynamically select a 'better' path to reach the CBT tree among multiple paths even in the presence of link or hop failure. For details of fault-tolerant CBT routing algorithms, we refer interested readers to [10].

2.2 Phase 2: Dynamic member registration and connection

With the proposed anycast group, a mobile node may learn existing agents by caching the anycast address through *DHCP* or *SLP* services [12, 13]. In the register message of mobile node, normally the D-bit is set to enable the mobile node to receive/decapsulate incoming multicast packet [1]. MMP allows membership changes to be made to a multicast group G. A mobile node is allowed to join or leave a multicast group at will. The concept of dynamic group membership is similar to the host view and supervisor host [14]. To join a multicast group G in the home network, a mobile node must register through the home agent. In the current mobile IP, a mobility agent must also broadcast advertisement messages periodically (similar to ICMP advertisement messages [15]) and the mobile node has to send a solicitation message to contact the agent when it hears no advertisement for a certain period of time. This phase is designed to reduce the cost of advertisement using an anycast group by the following steps:

Step 1. Mobile node home registration: A mobile node *Mn* must register through its home agent and join G for multicast message transmission. The registration can be accomplished through anycast connection by using G_A to connect to the 'nearest' MA in its home network. On establishment of the connection between MA and *Mn*, two cases must be considered:

Case 1: The MA is an ontree router of G: Similar to the mobile IP [1], the MA performs the corresponding authentication and mobility binding such as care-of address (CA) assignment to *Mn* (denoted as $CA(Mn)$) and calls $Insert(CA(Mn)), ML(G))$ to insert CA of *Mn* into membership list $ML(G)$.

Case 2: The MA is an offtree router. Similar to case 1, the MA must first check authentication of *Mn*, then calls $Insert(CA(Mn), ML(G))$. The following subcases must be considered:

- *Subcase 1*: The MA is a multicast router and uses G_A to join CBT tree for G by sending *join-request* to the 'nearest' ontree router in T_A [9, 10].
- *Subcase 2*: The MA is not a multicast router. It builds an anycast tunnel to the 'nearest' ontree router so that a single 'tree trunk' is grafted on the CBT tree [10].

Step 2. Mobile node visits a foreign network: A mobile node *Mn* originally registered in $MA_1 \in G_A$ in subnet 1 and moves to foreign network subnet 2 to connect with MA_2. Two cases must be considered:

Case 1: $MA_2 \in G_A$, since both MA_1 and MA_2 are in G_A, they are in the same authentication group. *Mn* may use address G_A to make contact with MA_2 for registration. On checking authentication and acceptance for *Mn*, MA_2 executes $Insert(CA(Mn), VL(G))$. On the other hand, MA_1 calls $Move(CA(Mn), ML(G), AL(G))$ to move CA of *Mn* from the membership list $ML(G)$ to the away list $AL(G)$.

Case 2: $MA_2 \notin G_A$, MA_2 does not provide service for multicast group G. Thus, MA_2 applies a bidirectional tunnelling approach similar to the mobile IP [1]. Upon acceptance of the visit of *Mn*, MA_2 calls $Insert(CA(Mn), VL(G))$. Since MA_2 is not an ontree router, it sets a tunnel to MA_1 and the later calls $Insert(id(MA_2), TL(G))$ to record the tunnelling information for MA_2.

Step 3. Mobile node leaves: When a mobile node leaves its home network, it should notify its home agent MA by sending a deregistration message. The latter calls $Move(CA(Mn), ML(G), AL(G))$. If $ML(G) = VL(G) = TL(G) = \{\}$, i.e. the MA has neither a mobile node attached to G nor any tunnel for visitor members in G, then the MA uses an IGMP message to notify its up-link node until 'core' to trim this branch from the CBT tree [16].

Step 4. *Foreign mobile node/agent leaves*: An MA may set up a specific timeout for the foreign mobile nodes in list $VL(G)$. When the timer expires, the MA just deletes the node ID from its $VL(G)$. A similar approach can be applied for the management of list $TL(G)$.

2.3 Phase 3: Multicast transmission phase

(i) *Multicast transmission*: A mobile node may generate a multicast message m intending to send to G. Message m is thus transmitted to home agent MA. When MA receives m, it first encapsulates m with a multicast header and then imbeds m within an anycast address T_A into an anycast packet m_A. The packet is then routed to the address T_A using dynamic anycast routing algorithms [9]. When a router in T_A receives the anycast packet, it strips off the anycast header of m_A into m and propagates it across group G. For a visited mobile node *Mn*, if it wants to send the multicast packet, the packets can be forwarded through the FAs. As in the mobile IP, a co-located care-of address on the foreign network is required and used as the source address for multicast packets to group G.

(ii) *Multicast packet reception-delivery*: When an MA receives an encapsulated multicast packet m from a router on the CBT tree, it strips the multicast header from the packet and makes the packet delivery to the IDs in $ML(G)$ and $VL(G)$. The packet is also tunnelled and retransmitted to the agents in $TL(G)$ when $TL(G)$ is not empty.

Note that if the mobile node is using a co-located care-of address, it should use this address as the source IP address of its IGMP [16] (membership) messages; otherwise, it is required to use its home address for multicast transmissions.

3 Performance

This Section presents the performance analysis for the MMP protocol and demonstrates experimental results to show the availability of the protocol by simulation results, in particular, it compares the complexity of MMP with remote subscription (RS) and bidirectional (BD) approaches in terms of number of broadcast/multicast packets and end-to-end delay of multicast.

Table 1: Performance comparisons

Operations	Protocols	Number of messages (m/bcasts)	Delay (s)
Agent discovery	Mobile IP	1	1
	MMP	0	0
Registration on HA	RS	2	1+2Δ
	MMP	2	2Δ
Registration on FA	BD	4	1+4Δ
	MMP	2	2Δ

3.1 Analysis

To analyse the performances of the MMP protocol, we use the following metrics for the comparison of MMP with methods proposed in mobile IP [1]:

- *number of messages (m/bcasts)*, this is the number of messages (including multicast and broadcast) required for the corresponding operation.

• *delay*, this is the total delays in seconds to accomplish the operation and Δ is used to measure a single multicast/broadcast (minimum) transmission delay.

According to the mobile IP, the agent discovery requires the MA to send a broadcast for agent advertisement. Mobile nodes use these advertisements to determine their current point of attachment to the Internet. The advertisement is sent at a maximum rate of once every second (hence the delay). Therefore, for a mobile node, it has to wait for the advertisement and then it discovers the presence of MA. With MMP, in the presence of anycast address G_A, mobile nodes are aware of the presence of MA. Thus no agent advertisement is required.

For registration of a mobile node, we differentiate the registration on the HA from that on the FA. If the registration is on the HA, in terms of message number, MMP is the same as the protocols based on mobile IP. But the delay is shorter as MMP does not wait for the advertisements of HA. Only the transmission delay of two messages is taken into account.

Mobile IP makes use of bidirectional tunnelling for a mobile node to register to a foreign network under the assumption that its HA is a multicast router. The mobile node tunnels IGMP messages to its HA and the HA forwards the multicast datagram down the tunnel to the mobile nodes. It is known that four messages are required: one is the request from a mobile node to FA, then FA relays the request to HA. HA, in turn, sends back a message of acceptance or denial to FA and then FA relays the final status to the mobile node. While in MMP, if the FA is in the same anycast group as that of the HA, only two messages are required: the registration through FA is the same as through HA. For the delay analysis, the reasoning is similar to the above argument.

3.2 Simulation model

In the simulation, we consider 16 local area networks (LANs) with a maximum of 90 mobile nodes. Each LAN has two mobility agents (i.e. one HA and one FA). All mobile nodes are allowed to roam in the network at random. The residency time for each mobile node to stay at a network (home or foreign) is drawn from an exponential distribution with a mean of r time units. The travel time for going between subnets is exponentially distributed with a mean of $(r/0.9) * 0.1$ time units. Thus, mobile nodes spend 10% of their time in transition, and 90% of their time connected to a LAN. In addition, each mobile node has a probability p of losing the connection with a local mobility agent.

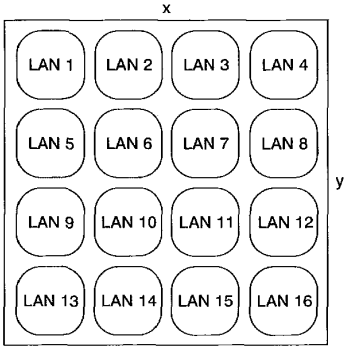

Fig. 3 *Network topology of simulation*

We assume that each multicast group has only one source for generating multicast messages in ratio of λ time units. The delivery of each multicast message to the group recipients is done by scheduling from the source to a mobility agent, and then to the mobile nodes. To simplify the simulation, the topology of LANs is located on an x–y coordinate as shown in Fig. 3. The network topology between the LANs is not drawn for simplicity.

The simulation experiments were conducted using a multi-factor experimental design. The warm-up period used for the simulations was 20% of the simulation time t, which is an input parameter. After the warm-up period, the simulator collects simulation statistics relating to the mobile multicast until the end of the simulation. We execute ten simulations for each set of workload parameters and obtain the mean value.

3.3 Simulation results

The experiment compares the effectiveness of multicast delivery of MMP with bidirectional tunnelling in terms of message delivery delay and number of delivered messages. The simulation considers one multicast group with up to 90 (mobile) nodes across nine LANs, and 8500 multicast messages are generated within 2500s.

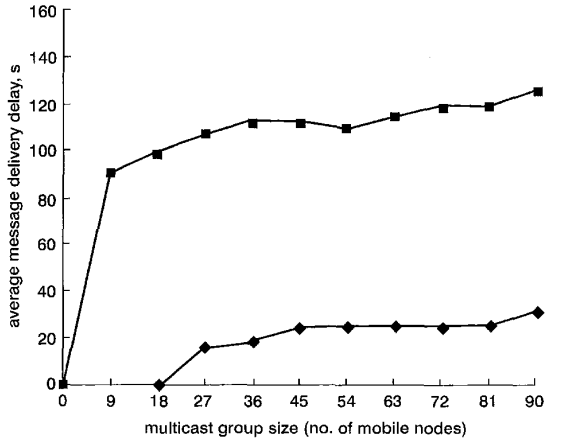

Fig. 4 *Message delivery delays*
$N = 9$, 8500 messages generated
—◆— MMP
—■— bidirectional tunnelling

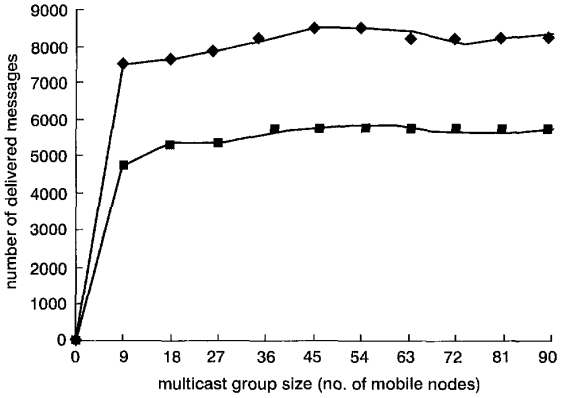

Fig. 5 *Number of delivered messages*
$N = 9$, 8500 messages generated
—◆— MMP
—■— bidirectional tunnelling

Fig. 4 shows that our protocol can provide a better multicast service to mobile nodes as the message delivery delay is lower than that of bidirectional tunnelling. The high delay demonstrates the transmission overhead in the tunnel from home network to foreign network of bidirectional tunnelling. Fig. 5 shows that about 90% of the generated

messages were delivered to the mobile nodes by MMP and about 50% of the generated messages were delivered by the bidirectional tunnelling protocol. For MMP, two situations may affect the delivery of multicast messages to the mobile nodes: first, the node may be in transit state; and secondly, the node may be attached to a network with poor link connection due to the noise environments. The unsuccessful deliveries in bidirectional tunnelling may be caused by inconsistent information in home network about the location of its mobile nodes.

4 Conclusions

MMP extends the mobile IP with anycast address group technology for agent discovery, registration of mobile nodes and delivery of multicast packets. The utilisation of an anycast address for the mobility agent group can reduce the cost and delay when the mobile nodes register with mobility agents between subnets without impacting its performance. In contrast to bidirectional tunnelling and remote subscriptions, MMP is more efficient in terms of delivery delay and throughput of multicast packets. The cost of employing the anycast address/group is that the multicast routers involved in the group have to manage the anycast addresses. This management may be taken as a set-up cost and will not compromise the (run time) dynamic performance of MMP. In this sense, MMP will extend the performance of mobile IP, especially when multicast services are desired.

5 Acknowledgments

This work was partially sponsored by the City University of Hong Kong under grants 7001060, and UGC (University Grant Council) Hong Kong under grants 9040352 CityU 1059/98E and 9040511 CityU 1076/00E. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of the UGC Hong Kong or the City University of Hong Kong.

6 References

1 PERKINS, C.E.: 'Mobile IP: design principles and practices' (Addison Wesley, 1998)
2 DEERING, S.: 'Host extensions for IP multicasting'. IETF Network Working Group Request for comment 1112, 1989
3 JIA, W., KAISER, J., and NETT, E.: 'RMP: Fault-tolerant group communication', *IEEE Micro*, 1996, **16**, (15), pp. 59–67
4 PARTRIDGE, C., MENDEZ, T., and MILLIKEN, W.: 'Host anycasting service'. IETF Network Working Group, Request for comment 1546, 1993
5 CHIKARMANE, V., WILLIAMSON, G.L., MACKRELL, W.L., and BUNT, R.B.: 'Multicast support for mobile hosts using mobile IP: design issues and proposed architecture'. Department of Computer Science, University of Saskatchewan, Saskatoon, 1997
6 BROWN, K., and SINGH, S.: 'RelM: Reliable multicast for mobile networks'. Technical Report, Department of Computer Science, University of South Carolina, Columbia, 1996
7 DEERING, S., and HINDEN, R.: 'Internet Protocol version 6 (IPv6) specification'. IETF Network Working Group, Request for comment 1883, 1995
8 JOHNSON, D., and DEERING, S.: 'Reserved IPv6 Sunnet anycast address'. IETF Network Working Group, Request for comment 2526, 1999
9 JIA, W., XUAN, D., and ZHAO, W.: 'Integrated routing algorithms for anycast messages', *IEEE Commun. Mag.*, 2000, **38**, (1), pp. 48–53
10 JIA, W., ZHAO, W., XUAN, D., and XU, G.: 'An efficient fault-tolerant multicast routing protocol with core-based tree techniques', *IEEE Trans. Parallel Distrib. Syst.*, 1999, **10**, (10), pp. 984–999
11 BALLARDIE, A.: 'Core based trees (CBT version 2) multicast routing'. IETF Network Working Group Request for comment 2189, 1997
12 DROMS, R.: 'Dynamic host configuration protocol'. IETF Network Working Group, Request for comment 1541, 1993
13 VEIZADES, J., PERKINS, C., and KAPLAN, S.: 'Service location protocol'. IETF Network Working Group, Request for comment 2165, 1997
14 ACHARYA, A., and BAKER, A.: 'Badrinath IP multicast extensions for mobile internetworking'. Department of Computer Science, Rutgers University, 1996
15 DEERING, S.: 'ICMP router discovery messages'. IETF Request for comment 1321, 1991
16 FENNER, W.: 'Internet group management protocol, version 2'. IETF Network Working Group, Request for comment 2236, 1997