Proc. of IASTED Parallel and Distributed Computing and Systems (PDCS'99), ACTA Press, Nov.99, Boston, USA,

Anycast Group Algorithms for Mobile Multicast Communications

Weijia Jia[1], Wanlei Zhou[2], M. A. Livani[3] and Joerg Kaiser[3]

[1]Department of Computer Science, City University of Hong Kong, 83 Tat Chee Ave, Hong Kong

[2]School of Computer Science & Mathematics, Deakin University, 662 Blackburn Rd, Melbourne, Australia

[3]Department of Computer Structures, University of Ulm, James-Franck-Ring, 89069 Ulm, Germany

(contact author: Weijia Jia at wjia@cs.cituy.edu.hk)

Fax: +852-2788-8614

ABSTRACT

Multicast has been an efficient service for applications such as video conferencing, resources discover and service location, etc. Although multicasting is well developed for static hosts, it is hard to harness in the wireless environment where resources are limited such as bandwidth and power of mobile units. This paper presents a novel and efficient multicast algorithm that aims at reducing delay and communication cost for the registration between mobile nodes and mobility agents and solicitation for foreign agent services based on Mobile IP. The protocol applies anycast group technology to support multicast transmissions for both mobile nodes and home/foreign agents. Mobile hosts use anycast tunneling to connect to an nearest available home/foreign agents where an agent is able to anycast route the multicast messages to a multicast router for efficient multicasting of messages. The performance analysis and experiments demonstrated that our algorithm can enhance the performance over existing remote subscription and bi-directional tunneling approaches regardless of the locations of mobile nodes.

1 INTRODUCTION

Multicast is an important service for mobile applications through wireless and connection to the Internet, such as email communication, query database, retrieve information, video conferencing through wired network etc. The provision of 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.

In mobile multicast communications, two issues are primary important: One is for mobile nodes and mobility agents to discover each other's presence and another is the datagram routing efficiency. Current Mobile IP [9] uses similar approach of ICMP [12] for mobility agent discovery in which an agent periodically multicast or broadcast the agent advertisement to those links to which it is connected and to the mobile nodes for offering routing services. Mobile nodes also use broadcast to connect mobility agents even a mobile node is in the home network. Mobile computing requires wireless communication, mobility and portability. The wireless link between the mobile nodes and the point of attachment has a low bandwidth, high error rate and poor connectivity. Thus, the protocols for mobile nodes should rely more on computation and communication power of static hosts. Due to dynamic group membership and location change of mobile nodes, reliable and efficient mobile multicast design and implementation are even more challenge.

This paper proposes a novel efficient mobile multicast protocol (MMP) that adapts *anycast* technology originally proposed by IPv6 [13]. It intends to reduce the time for the agent discovery as associated with existing approaches based on ICMP. MMP uses approaches of efficient anysact tunneling and anycast routing technology for group registration and multicast delivery across the environment of mobile connection to Internet. The contribution of this paper is that for those mobile agents that provide connection for mobile nodes, it can achieve efficient registration can be achieved through connection with anycast group. Thus mobile nodes may use well-known address to connect to a "nearest" mobility agent for registration. In this way the connection time can be reduced substantially.

The rest of the paper is organized as follows. Section 2 illustrates the relevant issues of mobile multicast IP, its architecture and algorithms. Section 3 presents the MMP algorithms. Section 4 describes the performance analysis and simulation results. Section 5 concludes the paper with some discussions.

2 RELATED WORK

Multicast is a communication that involves a single sender and multiple receivers. These receivers form a group that called a multicast host group. Traditional multicast research discussed reliability of message delivery in the multicast group in guaranteeing the properties such as total ordering, atomicity, dynamic group membership and fault-tolerance etc [14]. *IP multicast* [5] provides unreliable multicast deliver for wired networks. It is based on a host group formed by the hosts that communicate with each other through a given address. It is implemented by a set of routers that act as multicast routers and route all packets to the destinations. Several well-known multicast routing protocols have been developed as an extension to the existing routing protocols. Distance-Vector Multicast Routing Protocol (DVMRP) [1] is an extension to Routing Information Protocol (RIP). MOSPF [2] is a multicast extension to the Open Shortest Path First (OSPF), which is a link state protocol. Cored Based Tree (CBT) [3] is a shared tree routing algorithm as shown in Figure 1 (we will discuss the issue later). Protocol Independent Multicast (PIM) [4] is designed to be independent of the unicast routing.

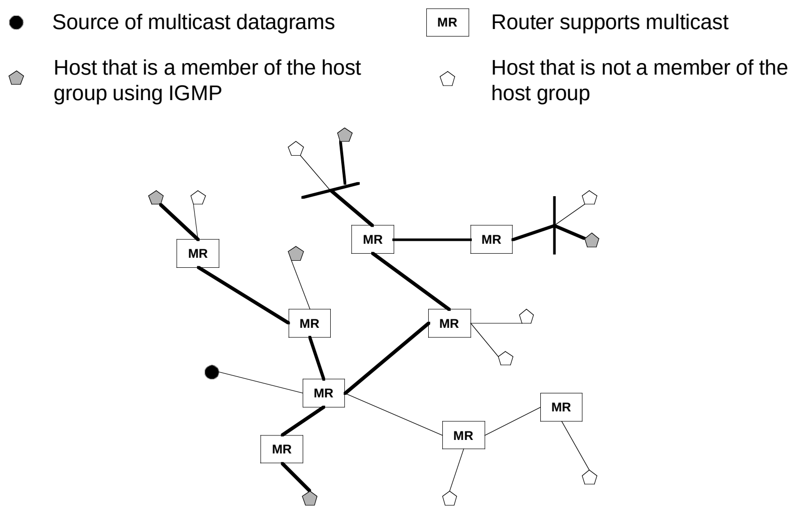


Figure 1. A Multicast Spanning Tree

In *Mobile IP* [9], in essence, it has a way of doing three relatively separate functions:

1. *Agent discovery* – Home agents and foreign agents (HA and FA) 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. A

mobility agent may transmit agent advertisements to advertise its services on a link. Mobile nodes use those advertisements to determine their current point of attachment to the Internet. A mobility agent is required to limit rate at which it sends broadcast or multicast agent advertisements with the maximal rate is once per second [16].

2. *Registration* – When a mobile node is away from home, it registers its care-of address 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 forward the registration to the home agent.
3. *Tunneling* – In Mobile IP and IP multicast, unicast tunnels are used to encapsulate and to send multicast packets over the Internet when the intermediate routers cannot handle multicast packets. In order 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 called home address.

There have been some well-known *wireless multicast systems* developed. Forwarding pointers and location independent addressing to support mobility has been discussed in [11], but the multicast service is unreliable. Host View Management Protocol (HVMP) has been developed that provides reliable multicast for mobile nodes [12]. However, it does not allow dynamic group membership. Reference [13] proposed a protocol that allows dynamic group changes and reliable multicast message delivery with different network architecture. Multicast tunneling is proposed to forward multicast packets from one foreign network to another when the mobility agent receives packets addressed to mobile nodes that are nomadic [8]. Perkins [9] defined two approaches to support mobile multicast, which are called remote subscription and bi-directional tunneling multicast. The remote subscription is inefficient for dynamic membership and location change of mobile nodes. Bi-directional tunneling multicast may cause the tunnel convergence problem with packet duplication [10] (see Figure 2).

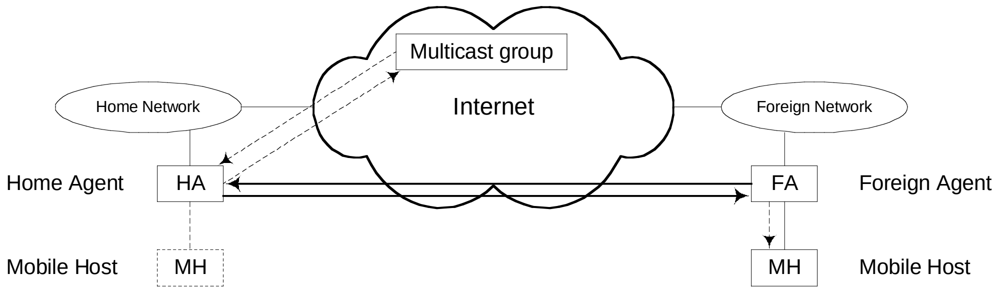


Figure 2. Bi-directional Tunneled Multicast Method

Anycast address and service has been defined for Internet Protocol version 6 (IPv6) [13]. Anycast is a communication for a single sender sends to the "nearest" member in a group of receivers, preferably only one of the servers that support the anycast address [11]. It uses 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 dose not care which server is used. Anycast can simplify the task of finding an appropriate server. For example, users can use the anycast address (i.e. ftp.download) to choose the mirrored FTP sites and to be connected to the nearest server. Besides, hosts can send a query to the DNS anycast address instead of consulting a list of DNS servers.

3 OUR PROTOCOL

This section discusses a Mobile Multicast Protocol (MMP) that provides efficient multicast services for mobile nodes by employing anycast agent group approach. The introduction of anycast technology aims at enhancing the efficiency and reducing the corresponding cost for agent discovery, registration and tunneling of multicast packets.

To form an agent group, an anycast address is configured by a group of mobility agents (both home/foreign agents) on the subnet that are designed to support a specific multicast group. When a registration request is sent to the anycast address, a home agent that receives that request can follow the same method used in IPv4 to send a registration reply to the mobile node. Approach of *anycast* group targets at two purposes: 1) Using a well-known anycast address, the home agents need not multicast/broadcast router advertisement and the mobile nodes may register directly through the well-known *anycast address* of the home/foreign anycast agent groups. This approach can reduce the time and cost for advertisement of home agents as well as for the solicitation of mobile nodes. 2) Using anycast can dynamically select the paths to the multicast router, as a result reducing the end-to-end multicast delay. The second issue has been elaborated and detailed in references [17, 18] and we omit the discussion in this paper due to lacking of space.

3.1 Assumptions and notations

Before proceeding the description of the protocol, the following assumptions are made (see Figure 3):

1. A set of hosts and mobile nodes forms a multicast group. Each individual mobile node has knowledge of the multicast group id to which it is interested in transmission and reception of multicast messages.
2. Both home agent and foreign agent (denoted as Mobility Agent-MA) are special routers that provide service for the attachment of mobile nodes.
3. There is at least one MA in each sub-net.
4. Multicast routers can configure its interface to route both multicast and anycast packets (refer to next subsection).

We introduce the following notations for the protocol design:

1. G – denote a multicast group/address and it is also taken as the group id or address such as IP class D multicast address.
2. G_A – An *anycast* address/group registered by all mobility agents that provide multicast service for group G.
3. T_A -- An *anycast* address/group registered by all routers that link the members in group G.
4. *ML(G) – Membership list* maintained by MA, it contains the ids of members in group G.
5. *VL(G)* -- *Visitor-list* maintained by MA, it is used to record the ids of foreign mobile nodes that belong to G.
6. *AL(G)* -- *Away-list* maintained by MA, it is used to record the ids of mobile nodes in G that left away from the home MA.
7. *TL(G) – Tunnel list* maintained by MA, is used to record the ids of foreign agents that tunnel to this MA and are interested in transmission/reception of multicast packets of G.

The functions applied to the lists:

1. *id(host/MA)* – return the identity of the host/node or an agent;
2. *Insert(id, L)* – insert identity *id* into the list *L*;

3. *Move(id, L_1, L_2)* – move *id* from list L_1 to L_2 where $L_1 \neq L_2$.

3.2 Design of MMP

The idea for the protocol is roughly described below. In the network, a group of routers join together to provide multicast transmission for a group of (mobile) nodes. MMP uses CBT technology [4] to build a multicast tree to connect the routers and the nodes (in case a node is a mobile node, its home agent is on the leaf of the tree). The MMP devises two anycast groups for the efficient multicast communications. The mobility agents in each subnet that provide multicast delivery for group G form the anycast group with reserved *anycast* address G_A [19]. The routers on the multicast tree form an anycast group T_A and they use a temporary anycast address for the MA to make service request or tunnel multicast packets to the member nodes throughout the lifetime of group G (see Figure 3). Therefore, in the mobile and Internet environment, the leaves of multicast tree are mobility agents and fix host whereas the mobile nodes are taken as the dynamic leaves.

MMP is divided into three major phases (below). Phase 2 and Phase 3 works interactively and they are discussed the phases in details.

1. *Initialization phase*: Multicast and anycast Group formations for routers, mobility agents and mobile nodes.
2. *Registration and membership phase:* Registration and reformation for the dynamic membership of mobile nodes.
3. *Multicast transmission phase*: Multicast packet transmissions and deliveries for the hosts and mobile nodes.

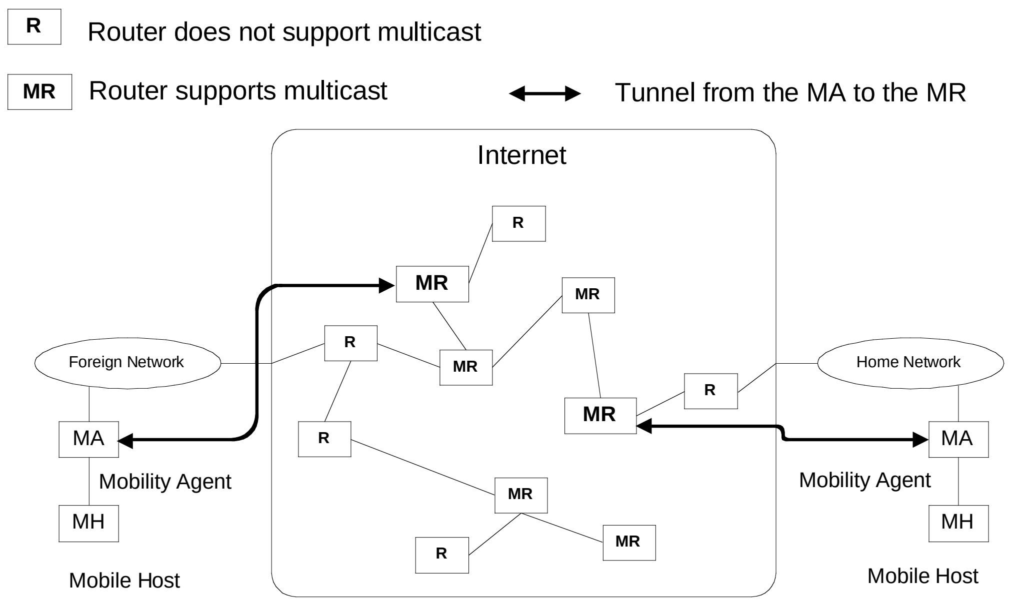


Figure 3. The illustration of MMP protocol

3.2.1 Initialization phase

This phase constitutes of four steps:

Step 1. *Membership Initialization*: An individual MA, for the services of group G, initiates $ML(G)=VL(G)=AL(G)=TL(G)=\{\}$.

Step 2. *Multicast Tree Formation*: CBT techniques are 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, Mobility Agents that provide multicast service for G join the CBT tree by linking itself to the *core* (see [4] for details). Note that all routers including MAs that are along the tree to the *core* are called on-tree routers.

Step 3. *Mobility Agent Anycast Group Configuration*: The mobility agents that offer attachment for the mobile node in *G* form an *anycast group* [17]. All the mobility agents can register any group id (address), here denoted as G_A. The agent that registered through group G_A may configure one of its interfaces to accept the registration of home or foreign mobile nodes. Address G_A can be made as a well-known address through the network under the concern of G. In our algorithm, we propose a concept called *association agents* in anycast group G_A, denoted as MA_1óMA_2 for two agents MA_1 and MA_2 where $MA_1 \in G_A$ and $MA_2 \in G_A$. If MA_1óMA_2, we define that MA_1 and MA_2 agree on the authentication and multicast packet delivery, i.e., MA_1 and MA_2 allow each other to delegate the multicast service and agree on the attachment of the mobile node that previously attached to another party. The mobility agents in the same anycast group are called in the same association.

Step 4. *On-tree Router Anycast Group Configuration*: For the group *G,* virtual anycast address T_A is assigned to and configured by all routers related to group *G* [18]. The routers are classified as *on-tree* routers and *off-tree* routers. They configure their interface for T_A in different ways:

- *On-tree Router Configuration*: For a multicast group *G*, when the CBT tree is built, all on-tree routers (including the core) on the tree 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 these nodes (hosts) outside the tree, their attaching router is not the on-tree router, may assign T_A as an interface entry and their routing table is configured with $<T_A, G>$ mappings. For any on-tree router, there is a Forwarding Information Base (FIB) used as its multicast routing table [4, 17]. An entry of the FIB has the form of <G, input-interface, output-interfaces>.
- *Off-tree Router Configuration:* Upon reception of address T_A broadcast from the *core* in CBT tree, the off-tree routers, including those foreign agents, that are interested in transmitting multicast service for *G* will register T_A on its 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 next hop failure. About details of fault-tolerant CBT routing algorithms, we refer interested readers to references [18].

3.2.2 Registration and Dynamic Membership Phase

With the proposed *anycast* group approach, a mobile node may learn the existing agents by caching the anycast address through *DHCP* or *SLP* services [16, 20]. In the *register* message of mobile node, normally the D-bit is set to enable the mobile node to receive/de-capsulate incoming multicast packet [9]. 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 free. The concept of dynamic group membership is similar to the host view and supervisor host [7]. To join a multicast group G in the home network, a mobile node must registrar through the home agent. In current Mobile IP, a mobility agent must also broadcast advertisement messages periodically (similar to ICMP advertisement messages) and the mobile node has to send solicitation message to contact with the agent when it hears no advertisement for certain period of time. In the following, we will describe how the MMP is designed to reduce the cost of advertisement using *anycast* group. The phase is divided into several sub-phases as below:

Sub-phase 1. *Mobile Node Registration*: A mobile node *Mn* can register through its home agent and join G for multicast message transmission. The registration can be accomplished through the *anycast* connection technique. Assume that a mobile node knows the anycast address of G_A for those agents that provide multicast services of G. *Mn* may uses address G_A to connect with the "nearest" MA in its home network. Because we have assumed that in each sub-net, there exists at least one MA, therefore, the solicitation procedure terminates eventually. Upon establishment of the connection between MA and *Mn*, two cases must be considered:

Case 1: The MA is an on-tree router for group *G* and executes the following steps:

1. Similar to Mobile IP [9], the MA performs the corresponding authentication and mobility binding such as care-of address assignment to *Mn* etc.
2. *Insert(id(Mn), ML(G)).*

Case 2: The MA is an off-tree router for group *G*. Similar to Case 1, the MA must first check authentication of *Mn*. Then it learns the group id G through *Mn* and initiates *ML={}, Insert(id(Mn), ML(G)).* Following sub-cases must be processed:

- *Sub-case* 1: The MA is a multicast router and uses G_A to join the CBT tree for G by sending *join-request* to T_A. In this way, it links itself to the CBT tree. Note that the *join-request* is sent to the "nearest" on-tree router in T_A [17, 18].
- *Sub-case* 2: The MA is not a multicast router. It builds an anycast tunnel to the "nearest" on-tree router so that a single "tree trunk" is grafted on the CBT tree (see [18] for detail).

Sub-phase 2. *Mobile Node-Visit a Foreign Network*: When a mobile node visits a foreign subnet, it has to send a register request with information of its home agent address, home address and care-of address to the foreign agent in another network [9]. It also informs the multicast group G it is interested in receiving/sending multicast packets. As current form of Mobile IP [9], the foreign agents seldom broadcast the advertisements for the presence of attachment service. The mobile nodes should first contact with a foreign agent (FA) for registration request, then the FA connects to the home agent for authentication of the mobile node. On successful reception of registration acknowledge message from the home agent, the FA replies to the mobile node with "acceptance" messages and adds *Mn* into its group membership list *ML* by calling *Insert(id(Mn), GL(G))*.

With the concept of *anycast group association*, the registration cost for a mobile node on the foreign network can be reduced considerably. Suppose the mobile node *Mn* originally registered in MA_1 in net 1 and now is migrating to foreign network net 2 with MA_2. Consider two cases:

Case 1: $MA_2 \in G_A$, by definition of association, since both MA_1 and MA_2 are in G_A, i.e., they are in the same authentic group. *Mn* may use address G_A to contact with MA_2 for registration. MA_2, upon checking authentication and acceptance for *Mn*, executes *Insert(id(Mn), VL(G))*. On the other hand, MA_2 calls *Move(id(Mn), ML(G), AL(G))*.

Case 2: $MA_2 \notin G_A$, MA_2 does not provide service for multicast group G. Thus, MA_2 applies bi-directional tunneling approach similar to Mobile IP. *Mn* must contact with MA_2 first. MA_2, upon reception of the registration request, contacts with MA_1 for authentic checking etc. Upon acceptance the visiting of *Mn*, MA_2 calls *Insert(id(Mn), VL(G))*. Since MA_2 is not an on-tree router, it sets a tunnel to MA_1 and receives the multicast packets and make them delivery for *Mn*. On the other hand, MA_1 calls *Insert(id(MA_2), TL(G))* to record the tunneling information.

<u>Sub-phase 3.</u> *Mobile Node Leaves*: When a mobile node leaves homes network, it should notifies its home agent MA by sending de-registration message. The later calls *Move(id(Mn), ML(G), AL(G))*. In case both *ML(G)* = {} and *TL(G)={}*, i.e., the MA does not have any mobile node attached to G nor any tunnel to members in G, then the MA uses IGMP message to notify its up-link node until *core* to trim this branch from the CBT tree [15].

3.2.3 Multicast transmission phase

If the mobile node is using a colocated care-of address, it should use this address as the source IP address of its IGMP [12] messages; otherwise, it is required to use its home address.

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 (refer to [17] for details). 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 foreign agents. Like 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.

Multicast packet reception-delivery: When a MA receives an encapsulated multicast packet *m* from a router on CBT tree, it strips-off the multicast header from the packet and makes the packet delivery to the ids in *ML(G)* and *VL(G)*. The packet is also tunneled and retransmitted to agents in *TL(G)*.

4 PERFORMANCE

This section presents the performance analysis for the MMP protocol, particularly, compares the complexity of MMP with remote subscription (RS) and bi-directional (BD) approach in terms of number of broadcast/multicast packets sent and delay introduced. We will demonstrate experiment results to show availability of the protocol by simulation results.

4.1 Analysis

To analysis the performances of the MMP protocol, we use following metrics for the comparison of MMP with methods proposed in Mobile IP [9]:

- *# of Messages (m/bcasts)* – the number of messages (including multicast and broadcast) required to complete certain operation.
- *Delay* – total delays in seconds to accomplish the operation and *Δ* is used to measure a single multicast/broadcast (minimum) transmission delay.

Operations	Protocols	# of Messages (m/bcasts)	Delay (sec)
Agent Discovery	Mobile IP MMP	1 0	1 0
Registration on HA	RS MMP	2 2	1+2Δ 2Δ
Registration on FA (HAóFA)	BD MMP	4 2	1+4Δ 2Δ

Table 1. Performance Comparisons

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

For registration of a mobile node, we differentiate the registration on the home agent (HA) from that on the foreign agent (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 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 bi-directional tunneling for a mobile node to registrar to a foreign network under the assumption that its home agent is a multicast router. The mobile node tunnels IGMP messages to its home agent and the home agent forwards 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 *deny* to FA and then FA relays the final statues to the mobile node. While in MMP, if the FA is in the same anycast group as that of HA, only two messages are required: the registration through FA is the same as through HA. For the delay analysis, the reason is similar to above argument.

4.2 Simulation Model

In the simulation, it is assumed that there are N local area networks with H mobile nodes. For simplicity, we only consider the performance simulations on the mobile nodes. Each LAN has two mobility agents (i.e. one home agent and one foreign agent).

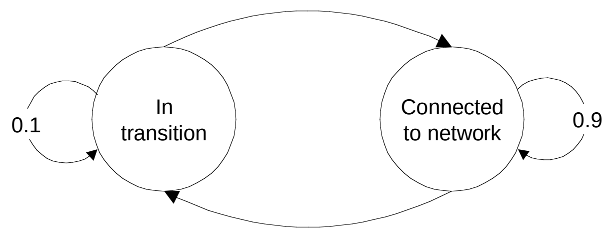


Figure 4. Host Mobility State Diagram

Figure 4 shows the state diagram of host mobility. 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 sub-nets 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 loosing the connection with a local mobility agent.

To simulate the multicast communication, we assume one multicast group and M multicast routers. It is also assumed that each multicast group has only one source for generating multicast messages in ratio of λ time-units. The simulation of delivery of each generated multicast message to the group recipients is done by scheduling from the source to a mobility agent, then to the mobile nodes.

Table 2 shows the parameters used in the simulation. The values of these parameters were chosen in an adequate way such that the simulation time and number of executions are manageable.

Parameter	**Description**	**Value**
M	Number of multicast routers	1 – 64
N	Number of wireless LANs	4 – 64
H	Number of mobile nodes per LAN	1 – 20
R	Residency mean time (second) of mobile node to stay at a network	1 – n
P	Probability of loosing the connection with a local mobility agent.	0.0 – 1.0
|G|	Multicast group size	4 – 1280
S	Number of sources per multicast group	1
λ	Multicast message generation mean time unit (us)	1 – n

Table 2. Simulation parameters

To simplify the simulation, the topology of LANs is located on a x-y coordinate system. The location of LAN is fixed for the duration of each simulation. For example, a simulation runs with N = 16 LANs has a 4-4 coordinate system as shown in Figure 5. The network topology between the LANs is not drawn for simplicity.

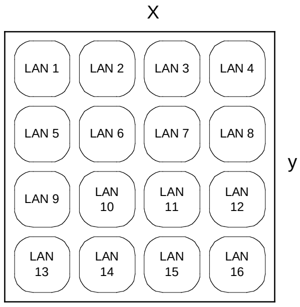
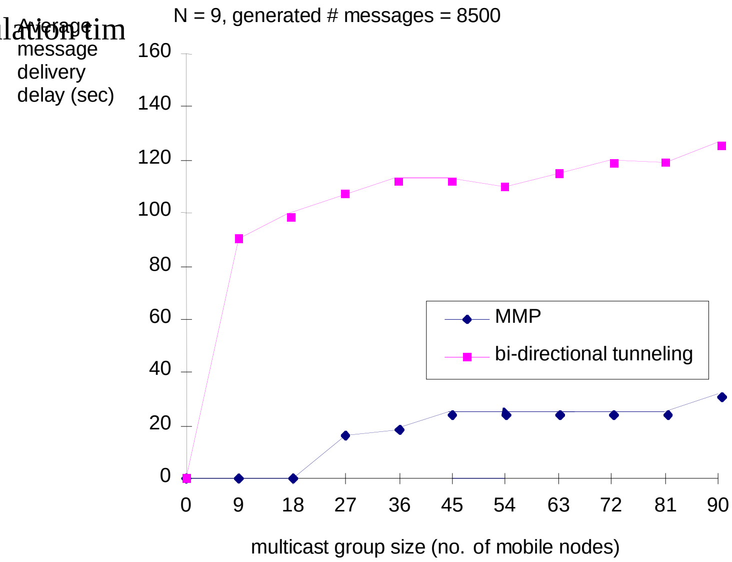


Figure 5. Network Topology of the Simulation

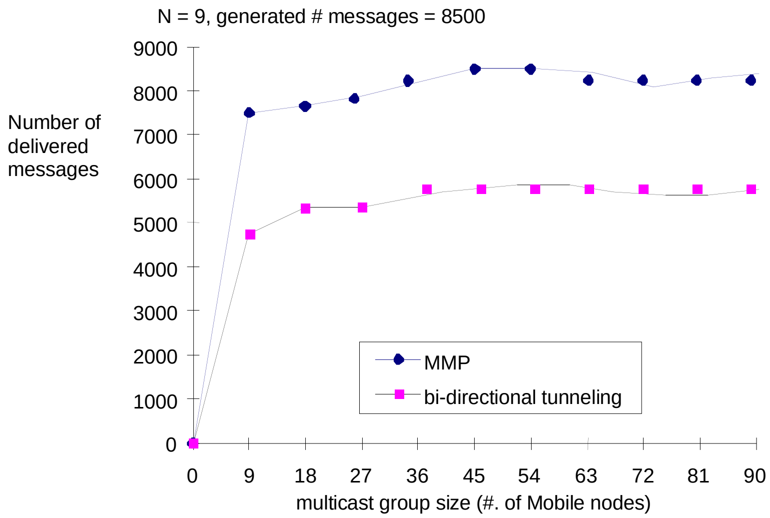
The simulation experiments were conducted using a multi-factor experimental design. The relative performance impacts of number of multicast routers, number of wireless networks, and number of mobile nodes are assessed. The warm-up period used for the simulations was 20% of the simulation time *t*, which is an input parameter. After the warm-up period, the simulator collects simulation statistics relating to mobile multicast until the end of the simulation. We execute 10 simulations for each set of workload parameters and achieve the mean value.

4.3 Simulation Results

The number of multicast packets transmitted in the inter-network is affected by the way of delivering these multicast packets to mobile nodes. In bi-directional tunneling each HA forwards all multicast packets to mobile nodes in G. When the mobile nodes are away from the home network, each MA forwards multicast packets to those MAs regardless of the mobile nodes being away from the network or not. The number of packets transmitted to each MA corresponds to the number of visitors of the network, and the number of packets delivered by each MA is proportional to the number of mobile nodes away from home. The experiment compares the effectiveness of multicast delivery of our protocol to bi-directional tunneling in terms of message delivery delay and number of delivered messages. Figure 6 presents simulation results with N = 9, |G| = 1, simulation tim)0.



(a)



(b)

Figure 6. (a) Message delivery delays. (b) Number of delivered messages.

Figure 6 (a) shows that our protocol can provide a better multicast service to mobile nodes as the message delivery delay is lower than that of bi-directional tunneling. The high delay demonstrates the transmission overhead in the tunnel from home network to foreign network of bi-directional tunneling. Figure 6(b) shows that about 90% of the generated messages were delivered to the mobile nodes by MMP and about 50% of the generated message were delivered by bi-directional tunneling protocol. For MMP, two situations may affect the delivery of multicast messages to the mobile nodes: (1) the node may be in transit and (2) the node may be attached to a network with poor link connection due to bad environments. The unsuccessful deliveries in bi-directional tunneling may be caused by inconsistent information in home network about the location of its mobile nodes.

5 CONCLUSIONS

MMP extends the Mobile IP with anycast address group technology for agent discovery, registration of mobile nodes and delivery of multicast packets. The utilization of anycast address for the mobility agent group can reduce the cost and delay when the mobile nodes make registration with mobility agents between subnets without impacting its performance. In contrast to bi-directional tunneling and remote subscriptions, MMP is more efficient in terms of delivery delay and throughput of multicast packets. The cost of the employing anycast address/group is that the multicast routers involved in the group have to manage the anycast addresses. This management may be taken as setup cost and they may not compromise the dynamic performance of MMP. In fact MMP is an initial research that intends to provide an extension for Mobile IP, especially when multicast services are desired. There are emance rooms remain for further research of using anycast group. For example, we have not addressed the issues for the multiple multicast groups for multiple agents in a subnet nor the anycast group management etc.

REFERENCES

[1] D. Waitzman, C. Partridge, S. Deering , Distance Vector Multicast Routing Protocol, RFC-1075, Nov. 1988.
[2] J. Moy, Multicast Extensions to OSPF, Network Working Group RFC 1584, March 1994.
[3] A. Ballardie, Core Based Trees (CBT version 2) Multicast Routing, Network Working Group RFC 2189, September 1997.
[4] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei, Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, Network Working Group RFC 2363, June 1998.
[5] S. Deering, Host Extensions for IP multicasting, Network Working Group RFC 1112, August 1989.
[6] D. Cheriton, VMTP: Versatile Message Transcation Protocol, RFC 1045, February 1988.
[7] K. Brown and S. Singh, RelM: Reliable Multicast for Mobile Networks, Tech. Rep. Department of Computer Science, Unversity of South Carolina Columbia, January 1996.
[8] A. Acharya, A Baker and Badrinath, IP Multicast Extensions for Mobile Internetworking, TR Department of Computer Science, Rutgers University, March 1996.
[9] C. E. Perkins, Mobile IP: Design Principles and Practices, Addison Wesley 1998.
[10] V. Chikarmane, Garey L. Williamson, Wayne L. Mackrell and Richard B. Bunt, Multicast Support for Mobile Hosts Using Mobile IP: Design Issues and Proposed Architecture, Department of Computer Science, University of Saskatchewan, Saskatoon, May 1997.
[11] C. Partridge, T. Mendez and W. Milliken, Host Anycasting Service, RFC 1546, Network Working Group, November 1993
[12] S. Deering, ICMP Router Discovery Messages, IETF RFC 1321, September 1991.
[13] S. Deering and R. Hinden, Internet Protocol Version 6 (IPv6) Specification, Network Working Group, RFC1883, December 1995.
[14] W. Jia, J. Kaiser and E. Nett, RMP: Fault-tolerant Group Communication, *IEEE Micro*, 16(15), 59-67, April 1996.
[15] W. Fenner, Internet Group Management Protocol, Version 2, Network Working Group, RFC2236, Nov. 1997
[16] R. Droms, Dynamic Host Configuration Protocol, RFC 1541, Network Working Group, November 1993.
[17] D. Xuan, W. Jia, and W. Zhao, "Routing Algorithms for Anycast Messages", *Proceedings of the 1998 International Conference on Parallel Processing* (ICPP98), August 10-14, 1998, Minneapolis, USA pp.122-130.
[18] W Jia, W Zhao, D Xuan and G Xu "An Efficient Fault-Tolerant Multicast Routing Protocol with Core-Based Tree Techniques", to appear *in IEEE Transactions on Parallel and Distributed Systems*, 1999.
[19] D. Johnson and S. Deering, Reserved Ipv6 Sunnet Anycast Address, RFC2526, March 1999.
[20] J. Veizades, C. Perkins and S. Kaplan, "Service Location Protocol" Request for Comments: 2165 June 1997.

APPENDIX: TERMINOLOGY

Home network	The network at which the mobile node seems reachable to the rest of the Internet.
Foreign network	The network to which the mobile node is attached when it is

	away from home network.
Home agent	A router on the home network that causes the mobile node to be reachable at its home network.
Foreign agent	A router on the foreign network that can assist the mobile node in receiving packets delivered to it.
Mobility agent	A node that offers support services to mobile nodes. A mobility agent can be either a home network or a foreign agent.
Mobile host/node	A host that changes its point of attachment to the Internet.
Care-of address	An IP address at the mobile node's current point of attachment to the Internet, when the mobile node is not attached to the home network.
Collocated care-of address	A care-of address assigned to one of the mobile node's network interface, instead of one being offered by a foreign agent.
Encapsulation	The process of incorporating an original IP packet inside another IP packet, making the fields within the original IP header temporally lose their effect.
Tunneling	The sample as encapsulation, but with additional connotations about changing the effects of Internet routing on the original IP packet.

The above terms and explanations are extracted from