International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:1, No:5, 2007

Improving Location Management in Mobile IPv4 Networks

Haidar Safa, Hassan Artail, Ahmad Mehio, Hicham Zahr, and Ziad Matragi

***Abstract*—**The Mobile IP Standard has been developed to support mobility over the Internet. This standard contains several drawbacks as in the cases where packets are routed via sub-optimal paths and significant amount of signaling messages is generated due to the home registration procedure which keeps the network aware of the current location of the mobile nodes. Recently, a dynamic hierarchical mobility management strategy for mobile IP networks (DHMIP) has been proposed to reduce home registrations costs. However, this strategy induces a packet delivery delay and increases the risk of packet loss. In this paper, we propose an enhanced version of the dynamic hierarchical strategy that reduces the packet delivery delay and minimizes the risk of packet loss. Preliminary results obtained from simulations are promising. They show that the enhanced version outperforms the original dynamic hierarchical mobility management strategy version.

***Keywords*—** Location management, Mobile IP (MIP), Home Agent, Foreign Agent.

I. Introduction

The next-generation telecommunications network (NGN) is anticipated to integrate the Internet and the third generation wireless communication. In today's Internet, the Internet Protocol (IP) routes packets from source to destination according to the network prefix derived from the destination IP address by masking off some of the low order bits. Thus an IP address typically carries with it information that specifies the IP node's point of attachment to the Internet. As a mobile node roams in the Internet, it needs to change its point of attachment to the Internet and consequently its IP address. Changing between points of attachment will cause any existing transport layer connection to be disrupted and lost. In addition, if a node changes its points of attachment to a foreign network, packets intended to it will be lost because they will be routed to the wrong network. The main objective of IP mobility support is to enable a mobile host to change its point of attachment to the Internet while still maintaining connectivity at the transport layer.

IP mobility was initially defined in [1] then revised in [2] and [3]. In this paper we focus on mobile IPv4 since we believe that this protocol will continue to dominate in the next years. In order to understand the architecture of Mobile IP, one must understand the terminology. Mobile IPv4 defines some functional components such as mobile node, home agent, foreign agent, and correspondent node. A *Mobile Node* (MN) is a host that changes its point of attachment from one network or subnet to another. A *Home Agent* (HA) is a router on an MN's home network that maintains current location information for the MN and tunnels datagrams for delivery to the MN when it moves away from its home network. A *Foreign Agent* (FA) is a router on a MN's visited network that provides routing services to the MN while registered with the HA. A *Correspondent Node* (CN) is a peer with which an MN communicates. It may be either mobile or stationary. Figure 1 depicts a mobile IP architecture.

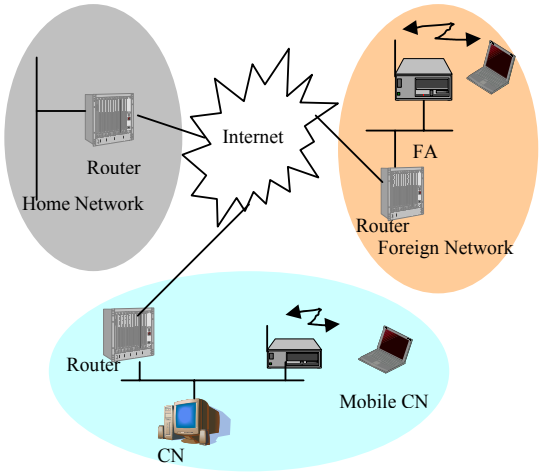

Fig. 1 Example of Mobile Network

According to [1], [2] and [3], an MN is always identified by its home address, which is a permanent address in its home network. While visiting a foreign network, the MN obtains from an FA a temporary address known as *care-of address* (CoA). Whenever an MN obtains a care-of address from the FA, it must notify its HA of the new address. This is called a home registration process and is completed by the MN's HA sending a registration reply message to the MN. Packets addressed to the MN's home address from a CN are intercepted by the MN's home agent, knowing that the MN is currently not in its home network. The HA tunnels (IP packets

Manuscript received March 31, 2005.
Dr. Haidar Safa, Ahmad Mehio, Hicham Zahr, and Ziad Matragi are with the Computer Science department at the American University of Beirut (e-mail: {hs33, amm25, haz04, zmm06}@aub.edu.lb).
Dr. Hassan Artail is with the Electrical and Computer Engineering Department at the American University of Beirut (e-mail: ha27@aub.edu.lb).
P.O.Box: 11-0236, Riad El-Solh, Beirut 1107 2020, Lebanon.

are placed within the payload part of new IP packets) the packets to the MN's foreign agent. The FA de-tunnels and delivers the packets to the MN. For packets sent by an MN, the FA may serve as default router. MN sends packets to the CN using its own home address as source address and the CN's address as destination address. This mechanism is known as *triangle routing.*

Although this mobility management scheme is simple and scalable, it has some deficiencies. First, the triangle routing constitutes a problem since packets that are designated to an MN are routed via sub-optimal paths (to the home network then to the foreign network). Second, MN needs to update its HA about every movement, even when it is far away from its home network. This makes the update/registration operation expensive and sometimes even impossible when the user movements are too frequent [4], [6] and [8].

The Route Optimization protocol was proposed to solve the triangle routing problem [5]. It is based on caching the care-of address of the MN at the CN. When packets are sent from a CN to an MN, they can be directly tunneled without the help of the HA to the care-of address indicated in the binding cache. The problem with this approach is the need to maintain the cache updated. Indeed, route optimization is achieved by sending additional control messages such as binding update and binding warning messages from the HA to the CN.

In [6], a hierarchical mobility mechanism (HMIP) approach was proposed to reduce signaling cost and communication overhead of the registration procedure by performing local registrations. Indeed, it consists of dividing the network into many regions. A region may contain several foreign agents managed by a single *Gateway Foreign Agent* (GFA). When an MN changes FA within the same region, it does not need to register with its HA. Instead, it performs local regional registration to the GFA to update its FA's care-of address. When an MN moves from one region to another one, it performs a home registration with its HA. This mechanism is sensitive to the failure of GFAs, because of the centralized system architecture. The failure of a GFA will prevent packets routed to all the users in the regional network from reaching its destinations. In addition, the number of FAs beneath a GFA within a regional network is very critical for the performance of the system. A small number of FAs will lead to excessive location updates to the home network. A large number of FAs will degrade the overall performance since it will generate a high traffic load on GFAs, thus resulting in high packet delivery cost.

A novel dynamic hierarchical mobility management strategy (DHMIP) was proposed recently in [7] as a solution to MIP's drawbacks. In this solution, when an MN moves from one foreign network to another, it obtains a new CoA from the new FA and informs its previous FA about its new address, thus forming a chain of FAs as shown in Figure 2. All packets destined to the MN are first sent to the HA which tunnels them to the MN's CoA, which is the first FA in the chain. The packets will then be tunneled along the chain until they reach the MN's current FA. To avoid long packet delivery delays, the chain's length (number of FAs) is restricted by a threshold which depends on the call-to-mobility ratio. Once the threshold is reached or exceeded, the MN performs a home registration and a new FA hierarchy is started.

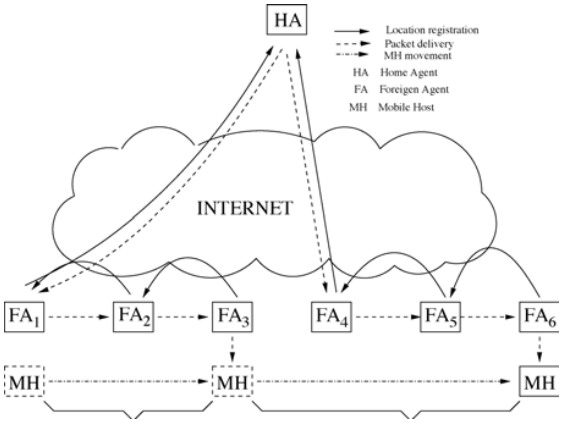

Fig. 2 Dynamic hierarchical management scheme.

DHMIP does not represent an optimal solution for the mobility management problem. The main goal of DHMIP is to reduce the registration cost and the signaling delays to the home agent. However, DHMIP suffers from an excessive tunneling since the packets sent from a CN to an MN are first delivered to the HA and then tunneled along the FAs' chain to the current FA of the MN. Similarly, packets sent from an MN to a CN are tunneled through the FA hierarchy to the HA then to the CN. This long delivery route induces a packet delay and increases the risk of packet loss. We believe that an efficient location management strategy should reduce the home registration costs as well as packet delivery cost.

In this paper, we propose an enhanced version of the dynamic hierarchical strategy that reduces the packet delivery delay and minimizes the risk of packet loss. It is organized as follows. Section II describes our enhanced version of DHMIP. Section III presents the simulation environment and evaluates the proposed enhancement. Conclusion and future work are drawn in Section IV.

II. Enhanced Version of DHMIP

As mentioned earlier, forwarding the packets, in DHMIP, through multiple foreign agents will cause some service delays and may lead to packet loss even when the length of the FAs' chain is bound to a threshold. Our enhanced version of DHMIP makes use of the route optimization protocol proposed in [5] in order to reduce the packet delivery cost and eliminate the excessive tunneling. It considers two scenarios: 1) the packets are originated by a CN and destined to the MN and 2) the packets are originated by the MN and destined to a CN.

In the first scenario, the first packet sent by a CN to the MN arrives at the HA. The HA tunnels it through the FA hierarchy

to the MN and informs the CN about the MN's registered CoA (which is the first FA in the FAs' chain). All following packets will be sent directly to the MN's registered CoA thus shortening the packet delivery route as shown in Figure 3. Consequently, the delay in packet delivery is reduced and the risk of packet loss is minimized since packets are traveling through a shorter path.

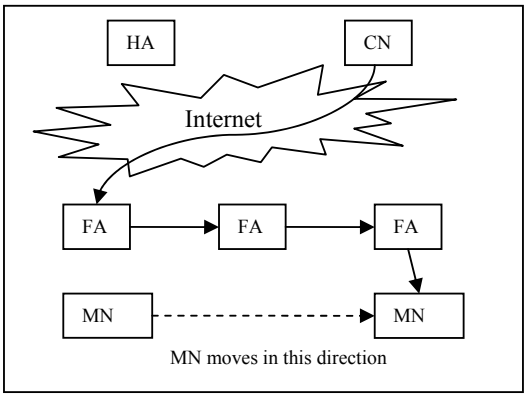

Fig. 3 Packets originated by a CN and destined to a MN are directly sent to the first FA in the FAs' chain.

When the MN moves to a new FA and the threshold is reached, the chain of FAs will be broken and a new chain is started as shown in Figure 4. In this case the MN will obtain a new CoA from the new FA (step 1 in Figure 4). Then, the MN informs its HA about its new CoA (new head of the chain) and informs also the previous FA (the tail FA in old FAs' chain) about this new CoA (step 2 in the Figure 4). The CN is not yet aware of MN's CoA change, so it keeps on sending packets to the FA which is the old chain head. This FA queues those packets and forwards them via the old chain to MN's new CoA (the head of the new chain) (step 3 in Figure 4) . The tail FA in the old chain warns the CN about the fact that the MN is not any more in its range (step 4 in Figure 4). The CN will then update its binding table by requesting the MN's new CoA from the MN's HA. Another alternative would allow the tail FA of the old chain to send the MN's new CoA in the warning message. When the CN gets the MN's new CoA, the new packets will be transmitted directly to this address (step 5 in Figure 4). Then the old path between the CN and the MN will be deleted (step 6 in Figure 4).

In the second scenario, the packets are originated by the MN and destined to the CN. Instead of tunneling the packets through the FAs' chain, the enhanced DHMIP approach consists of sending packets directly from the MN to the CN via the MN's current FA without following the FAs' chain as shown in Figure 5. Indeed, when the MN leaves its HA for a foreign agent, it registers its CoA at the HA. When the CN communicates with the MN, it expects the MN to reply using its CoA as source IP address. Also, when the MN communicates with a CN, it uses its CoA as source IP address and the CN can reply directly to MN's CoA.

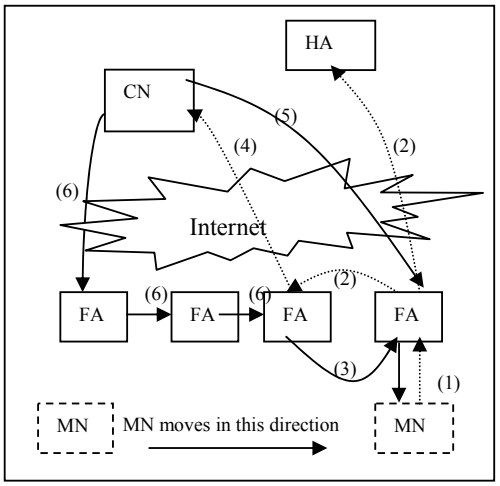

Fig. 4 When the threshold is reached a new chain is created and the old one is deleted.

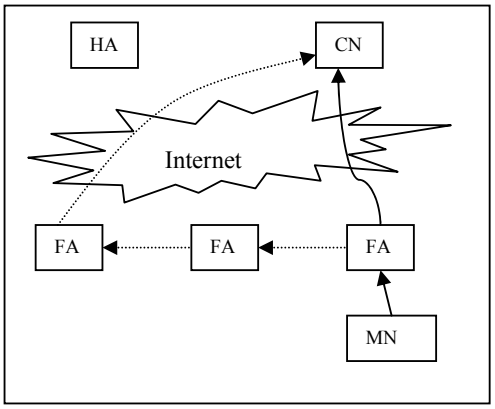

Fig. 5 MN sends packets destined to CH directly using its current FA. Packets are no more tunneled

As previously mentioned, while communicating with the CN, if the MN moves to a new FA and the FAs' chain threshold is reached, the old chain will be dropped and a new chain will be created. In this case, the MN notifies the CN about its new CoA and continues sending packets to the CN using its new CoA as source IP address.

The enhanced DHMIP approach has many advantages over DHMIP. To begin with, packet delivery delay is significantly minimized. Using DHMIP, packets sent from an MN to a CN are also tunneled through the FA hierarchy back to the HA and finally to the CN. Whereas, in the enhanced DHMIP, packets sent by the MN are directly forwarded by the FA, in which it currently resides, to the CN via the internet. Also here, the packet delivery delay is minimized. In both scenarios (CN to MN and MN to CN), the risk of packet loss is dramatically reduced since messages are traveling through shorter routes.

III. Simulations

To evaluate the performance of the enhanced DHMIP approach compared with the DHMIP approach and to get some preliminary results, the network simulator NS-2 is used [9]. We configured our simulation environment to use hierarchical addressing (19 domains) and UDP packets of size 500 bytes. We considered a network that includes 2 wired nodes, W(0) and W(1), that act as CNs, 1 mobile node (MN), and 17 base stations divided into 1 Home Agent (HA) and 16 Foreign Agents (FA1 to FA16) that route packets to and from the mobile node. The Simulation lasted for 450 seconds.

The first simulation scenario simulated the DHMIP approach. The simulation started a time 0. At this time the MN is located near the HA. At time 0.1, the node W(0) starts sending UDP packets to the MN. At time 20, the MN starts moving toward the first FA, FA_1. When the MN reaches FA_1 it performs a home registration with the HA. When the MN reaches the FA, FA_n, it informs its previous FA, FA_{n-1}, about its new CoA. Then the MN holds its position for 20 seconds to receive UDP packets from FA_n before continuing moving toward FA_{n+1}.

The second simulation scenario simulated the enhanced DHMIP approach. This scenario is similar to the previous one except that when the MN reaches FA_1 and registers its CoA at its HA, the HA informs the node W(0) about the MN's new CoA requesting it to send packets directly to FA_1.

Table I shows the packet delivery cost under both approaches given different number of FAs forming a chain. When considering a chain made of four FAs, then it takes 1870 ms for a packet to reach the MN under DHMIP compared to 1260 ms under the enhanced DHMIP. Figure 6 shows that our approach outperforms the DHMIP model in terms of packet delivery cost.

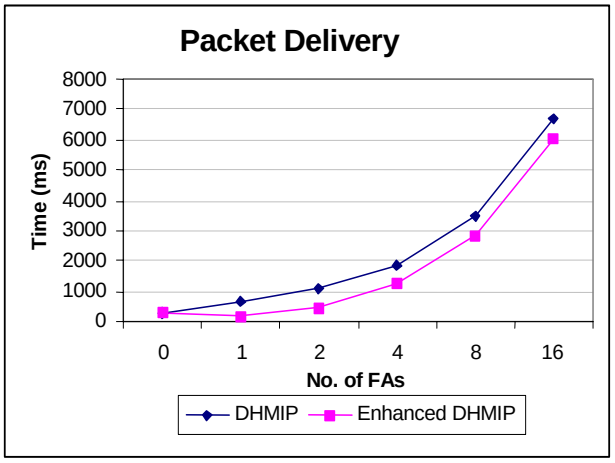

Fig. 5 Packet delivery cost in both approaches

TABLE I
PACKET DELIVERY TIME UNDER BOTH APPROACHES DHMIP & OUR EXTENDED APPROACH

Delivery Time	Number of Foreign Agents					
	0	1	2	4	8	16
DHMIP	251	663	1069	1870	3471	6670
Enhanced DHMIP	251	160	460	1260	2816	6060

IV. Conclusion and Future Work

In this paper, we have proposed an enhanced version of the DHMIP mobility approach that was proposed in [7]. The enhanced version takes advantage of the route optimization protocol that was proposed in [5] so as to improve the packet delivery cost in DHMIP. Using our approach, the packets sent from CN to MN follow a shorter route since they are no more tunneled by the HA into the FA hierarchy. In addition, packets sent by the MN to a CN no more follow the FA chain. Instead they are directly forwarded by the currently visited FA to CN.

Despite the use of a threshold, the enhanced DHMIP approach still suffers from the possibility of the failure of an intermediate FA. In fact, the system's packet delivery is highly dependent on the FA hierarchy. So if one of the FAs fails, the whole process of packet delivery will stop and communication with the outside world is discontinued. To solve this problem, there is need to integrate a fault tolerance strategy within the presented approach. In addition, the use of MN's CoA as source IP address might introduce security breaches since it is an explicit use of IP spoofing. Nevertheless, we can solve this problem by introducing an authentication mechanism to the system where only authenticated messages are accepted by the parties involved in a communication session.

References

[1] C. Perkins, "IP Mobility Support," RFC 2002, 1996
[2] C. Perkins, " IP mobility Support for IPv4," internet draft, draft-ietf, mobileip-rfc2002-bis-08.txt, Sept. 2001
[3] D. Johnson and C. Perkins, "Mobility Support in IPv6," internet draft, draft-ietf-mobileip-ipv6-15.txt july 2001
[4] H. Chaskar, " requirements of a QoS solution for mobile IP," Internet draft, draft-ietf-mobileip-qos-requirements-01.txt (August 2001), work in progress.
[5] C. Perkins and D. Johnson, "Route Optimization in Mobile IP," internet draft, draft-ietf-mobileip-optim-09.txt Feb 2000
[6] E. Gustafsson, A. Jonsson, and C.Perkins, "Mobile IP Regional Registration," Internet draft, draft-ietf-mobileip-reg-tunnel-05.txt, sept. 2001, work in progress.
[7] W. Ma and Y. Fang, "Dynamic Hierarchical Mobility Management Strategy for Mobile IP Networks", IEEE Journal on Selected Areas in Communications, Vol. 22, No. 4, pp. 664-676, May 2004.
[8] R. Caceres and V.. Padmanabhan, "Fast and scalable wireless handoffs in support of Mobile Internet Audio," Mobile Network and Applications 3, pp. 351-363, 1998
[9] NS-2 simulator. http://www.insi.edu/nsnam/ns/ [April 2002]