Workshop on Computer Networks

Domain Mobility Management for Wireless Network with Public Key Cryptsystem*

Chou-Chen Yang† Min-Shiang Hwang‡
Jian-Wei Li† Ting-Yi Chang †

Department of Information and Communication Engineering†
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Tel: (886)-4-23323000 ext 4226
Fax: (886)-4-23742375
Email: ccyang@cyut.edu.tw

Department of Information Management‡
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw

July 10, 2002

Abstract

Mobile IP presents an efficient solution to the mobility problem on the Internet. However, if an MH handoffs so frequestly that it needs to register with a distant HA for each handoff which causes high overhead, besides the handoff may be delayed and packet loss aggravated. Hence we propose the *Group Foreign Agent* management scheme in the foreign domain to alleviate these problems, and all the FAs have the authentication information of the MHs which are sent in advance by other neighboring FAs so that they have the ability to *authenticate* MHs independently, not through anyone.
Keywords: Mobile IP, secret key, public key,registration,authenticate

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2626-E-324-001.
†Responsible for correspondence: Prof. Chou-Chen Yang.

Domain Mobility Management for Wireless Network with Public Key Cyptsystem

Abstract

Mobile IP presents an efficient solution to the mobility problem on the Internet. However, if an MH handoffs so frequestly that it needs to register with a distant HA for each handoff which causes high overhead, besides the handoff may be delayed and packet loss aggravated. Hence we propose the *Group Foreign Agent* management scheme in the foreign domain to alleviate these problems, and all the FAs have the authentication information of the MHs which are sent in advance by other neighboring FAs so that they have the ability to *authenticate* MHs independently, not through anyone.

Keywords: Mobile IP, secret key, public key,registration,authenticate

1 Introduction

Within the Internet, an MH belonging one administrative domain (the home domain) may often roam into a foreign domain, expecting to seamlessly access network services and resources from any where at any time. Unfortunately, an MH continuously changing its point of attachment to the network creates a serious problem for a *TCP/IP* based Internet; for example, a packet addressed to an MH will be routed to the MH's home network, not to its current location. To solve this problem, a working group within the Internet Engineering Task Force (IETF) is under construction to develop the $MobileIP$ standard [6, 7, 8, 9], and the *Mobile IP* protocol presents a network layer solution to offering seamless roaming to mobile computers on the Internet.

Mobile IP uses a two level addressing architecture where an MH is associated with two addresses: one is a constant address called the home IP address, and the other is a temporary address called the *care-of address* which reflects this MH's point of attachment at the particular time. Whenever an MH is away from its home network in a visited domain, firstly it must obtain a *care-of address* from a *Foreign Agent (FA)* in the visited domain and register its current *care-of address* at its *Home Agent (HA)*. In other words, the MH is required to register with its HA, which may be far away when it changes its point of attachment to other FAs. Hence, the HA *registration* causes a huge traffic load between the visited network and home network in the wide-area mobility case, and large handoff latencies in the local-area mobility case. One solution to these problems is the *Hierarchical Foreign Agent* management scheme [10].

In the*Hierarchical Foreign Agent* management scheme, the MH must store a list of multiple *care-of addresses* which are the IP addresses of all the ancestors of the visited FA as well as the visited FA ifself, and they are situated from the current FA up to the root in the tree of regional FAs, and it must find the *target FA* which is an intersection of the old and new lists of multiple *care-of addresses* if it changes its point of attachment. And when a datagram from the MH's HA arrives at the top of the hierarchy, the datagram will be tunneled from the top FA of the hierarchy downward to the FA which is the MH's current point of attachment, and then the last tunnel FA will deliver the datagram to the MH.

In this paper, we shall propose a *Group Foreign Agent* management scheme to reduce the traffic between the visited network and the home network and to reduce the handoff delay when an MH moves from one FA to another within the same visited domain where all the FAs have authentication information of the MH sent to them in advance from other neighboring FAs so that they have the ability to *authenticate* MHs independently, not through anyone.

The rest of this paper is organized as follows. Session 2 presents an overview of the *Regional Registration protocol* [4] and the *Hierarchical Foreign Agent* management scheme [10]. Session 3 presents the *Group Foreign Agent* management scheme and its detailed operations. Session 4 presents the security analysis of our mobility management scheme. Finally, this paper is to be concluded in Session 5 with some perspectives for the future.

2 Overview

2.1 Regional Registration protocol

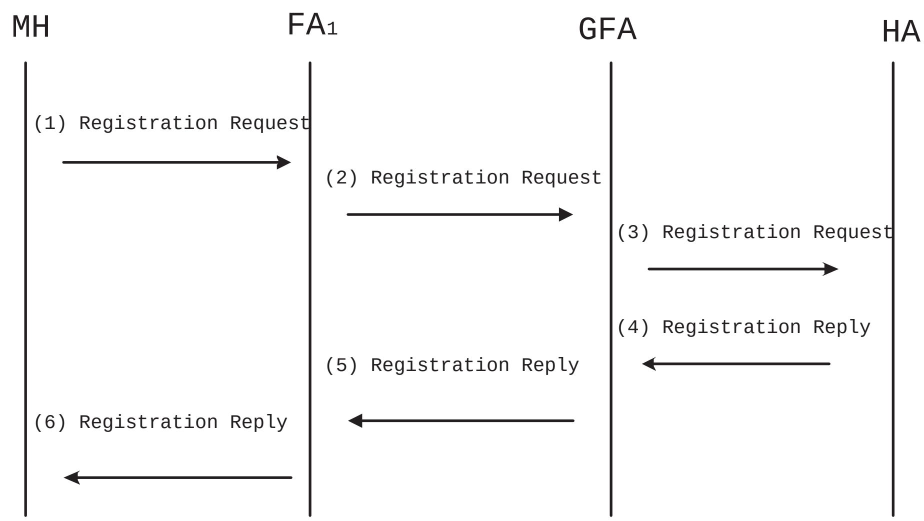

Figure 1: Registration at the GFA and the HA

When an MH first arrives at a visited domain which supports *regional registrations* [4], it registers with its HA an GFA's IP address as its *care-of address*. The GFA keeps a visitor list of all the MHs currently registered with it. Since the HA records the GFA's IP address as the MH's *care-of address*, it will not change the record when the MH changes its point of attachment within the same visited domain. Thus, the HA does not need to be notified of any further MH movements within the same visited domain. Figure 1 illustrates the signaling message flow for *registration* with the home network. After the *registration* at the HA, the HA records the GFA's IP address as the MH's *care-of address*. If the MH micro-moves from FA_1 to the FA_2 within the same visited domain, the signaling message flow for *regional registration* with the GFA only arrives at the GFA . Even though the MH's local *care-of address* changes, the HA still keeps the record of the GFA's IP address as the MH's *care-of address*.

However, as for the FAs, they must be dependent on the GFA to *authenticate* MHs, so the GFA must *authenticate* all the MHs whether all MHs firstly arrive at the visited domain or not. Therefore, it load is quite heavy.

2.2 Hierarchical Foreign Agent Management Scheme

If an MH handoffs so frequestly that it needs to register with a distant HA, then each handoff will cause higher overhead and further aggravate packet loss. The *Hierarchical Foreign Agent* [10] management scheme is proposed to solve such a problem of MH's frequent handoff . The proposal is specified to use a *Regional Registration* Request and *Registration* Reply, which is no longer always required to be transacted with the HA. The FAs are arranged hierarchically in the regional topology, and the MH is then allowed to move from one FA to another within the same visited domain without approval by or rebinding at its HA (As Figure 2 shows).

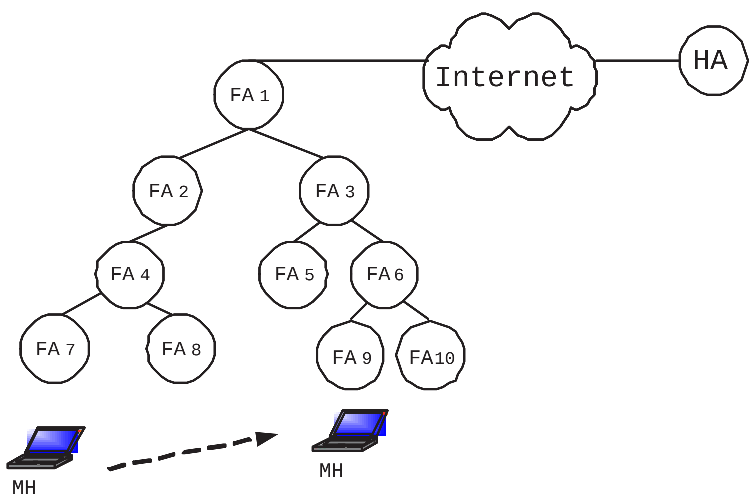

Figure 2: The *Hierarchical Foreign Agent* architecure

Registration and Datagram deliver

As Figure 2 shows, the MH first arrives at FA_7, and it accepts an Agent Advertisement of FA_7 containing a list of multiple *care-of addresses* which are the IP addresses of all FA_7's ancestors as well as its own, and they are arranged from the current FA up to the root of the tree of the regional FAs, $< FA_7, FA_4, FA_2, FA_1 >$. The MH keeps the list of multiple *care-of addresses* and registers orderly from FA_7 through FA_4, FA_2 and FA_1 to its HA. The HA records the FA_1's IP address as the MH's *care-of address*, and a datagram will be delivered to the MH along the path $< FA_1, FA_2, FA_4, FA_7 >$. If the MH moves to FA_8, it compares the previous list and the new list $< FA_8, FA_4, FA_2, FA_1 >$ to find out the *target FA* which is an intersection of the previous list and the new one, namely FA_4. It performs *regional registration* withFA_4.

Assume a datagram is sent from a corresponding node. The HA will tunnel it to the root of the FA hierarchy. When the FA_1 receives the datagram, it will tunnel it to the node of next level, FA_2. Simlarily, FA_2 will tunnel the datagram to FA_4, and FA_4 will tunnel it to FA_8. Lastly, FA_8 will deliver the datagram to the MH.

In this scheme, when an MH first arrives at a domain or micro-moves to some other FA in the same visited domain, it must send a $registration$ request through several FAs to the *target FA*. To do so, the $registration$ may be delay, and the FAs in the hierarchical lineage will maintain its binding cache, which binds the MH to the *care-of addresses* of the FAs at the next level. MHs must not only store the current list of multiple *care-of addresses*, but also compare it with a new one to find a target FA.

When a datagram from the MH's HA arrives at the top of the hierarchy, it will be decapsulated and reencapsulated with a new tunnel FA at each level of the hierarchy. These two operations occur at each level of the hierarchy until the datagram reaches the last tunnel FA, which is either the MH itself or an

FA that can deliver the decapsulated datagram to the MH with no further special *Mobile IP* handling. So these operations will increase the overhead of delivering datagram. Besides, the FAs may cause datagram loss.

3 Group Foreign Agent Management Scheme

3.1 Architecture

Neither the *regional registration* nor *Hierarchical Foreign Agent* is optimal in terms of this datagram sent to an MH , and there is still something else an MH needs to store and process when it is in a visited domain; therefore we propose a group FA architecture as Figure 3 shows. In our new architecture, a visited domain has one or more groups. A group has a *Master Foreign Agent (MFA)* which must have a publicly routable address. Beneath the MFA, there is at least one FA. We assume that there exists established security association between the MFA and each FA beneath the MFA as well as between an FA and any of the neighbors of the FA.

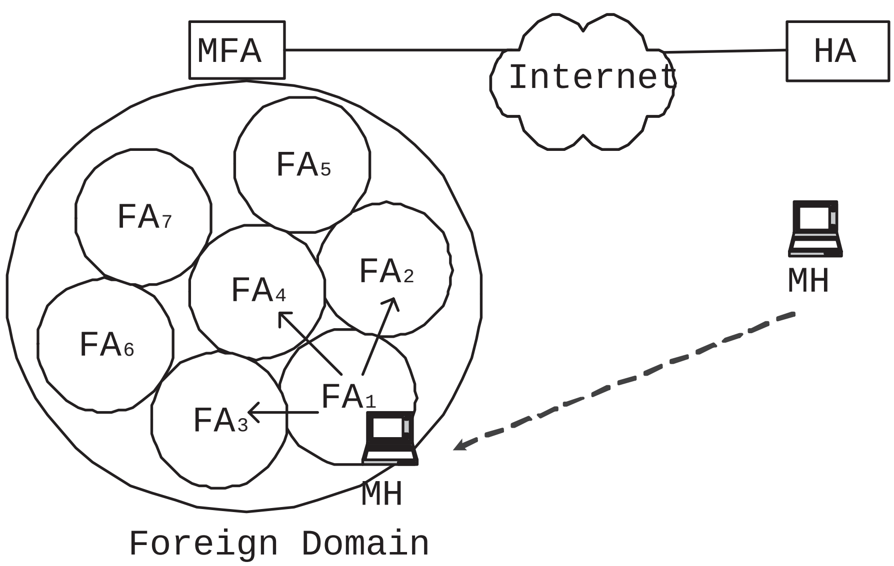

Figure 3: *Group Foreign Agent* architecure

3.2 Registration

When an MH is roaming in a visited domain, it will perform two operations: one is Home Registration which is performed when the MH first arrives at the visited domain, and the other is Micro-Move Re-registration which is performed when the MH micro-moves from one FA to another within the same visited domain.

Home Registration

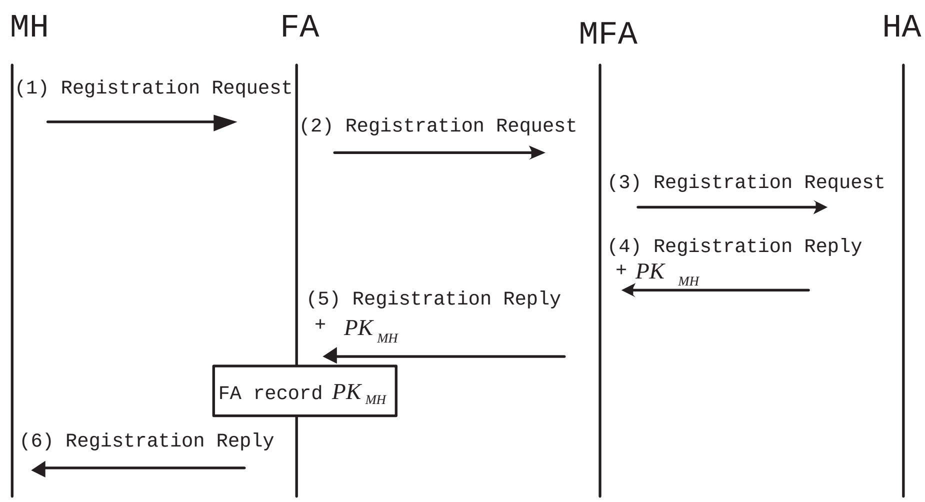

Figure 4: Registration at the MFA and the Home Agent

The first message (1) in Figure 4 is a *registration* request sent by the MH to a visited FA. The FA relays the *registration* request (2) to the MFA. After receiving the *registration* request (3), the MFA sends the *home registration* request to the MH's HA.

Then, the HA will *authenticate* the MH with the *home registration* request. After authenticating, the HA records the MFA's IP address as the MH's *care-of address*. Then the HA sends the *registration* reply (4), which includes the MH's *public key* (PK_{MH}) [3, 12, 13, 14], to the MFA. After receiving the *registration* reply, the MFA adds the MH to its binding cache, (5) and the sends reply to the FA.

After receiving the reply, the FA sends the MH's authenticated message, including the PK_{MH} and the pair of MH's IP address and MAC address, to other neighboring FAs. This MH's authenticated message can help those FAs independently *authenticate* the MH. Finally, the FA sends the *registration* reply to the MH (6).

Micro-Move Re-registration

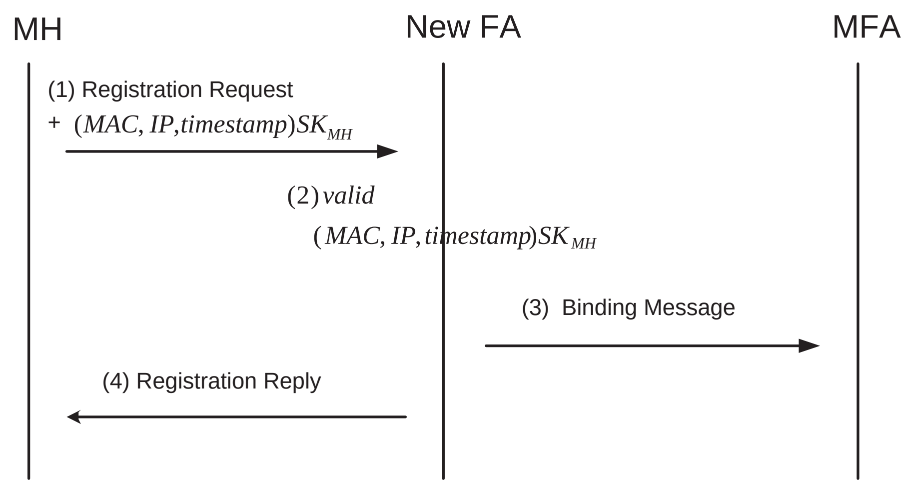

Figure 5: Micro-Move Re-registration at the FAs

As Figure 5 shows, when the MH micro-moves to another FA within the same visited domain, (1) it sends a $re-registration$ request to the new FA. The $re-registration$ request includes its *signature* as its *credential*, which includes its IP address, MAC address and *timestamp* encrypted by its *secret Key* (SK_{MH}) [3, 12, 13, 14]. The new FA can *authenticate* the MH by verifying the MH' *credential* without doing home registration again.

3.3 Authentication

When an FA receives a re-registration request, it needs to perform the four operations as follows:

1. As Figure 5 shows, (2) it must verify the *credential* in the $re-registration$ request. Firstly, the *credential* is decrypted by the PK_{MH}, and then the

FA compares the pair of the MH's MAC address and IP address in the *credential* to the pair in the MH's authenticated message sent by the previous FA.

2. If the *credential* is validated, (3) the new FA sends a *binding* message to the MFA to inform it that the MH has arrived [2, 11]. After receiving the message, the MFA modifies its binding cache with the FA's IP address as the MH's *care-of address*.

3. Meanwhile, (4) the new FA sends a $re-registration$ reply to the MH and starts to provide its service.

4. Then the new FA sends the authenticated message of the MH to its neighboring FAs according to its routing table (See Fig 3).

3.4 Merits

In comparison with the *regional registration* and the *Hierarchical Foreign Agent* management scheme, our new architecture has the following advantages:

1. The *registration* in our proposal only takes two levels of FAs, so only the MFA needs to maintain its binding cache when the MH moves to another FA within the same visited domain. In addition, the MH does not need to store any additional information, and thus its registration will not be delayed.

2. Assume the Hierarchical Foreign Agent architecture has n levels of FAs. When a datagram is sent to an MH, the maximum number of FAs which need to do two operations, namely decapsulation and reencapsulation is $n-1$. In our proposal, there are two levels of FAs, which means the maximum number of FAs which need to do two operations is one, and that leads to lower overhead due to transmitting datagrams than the Hierarchical Foreign Agent.

3. In the Hierarchical Foreign Agent architecture, a datagram may be sent through many FAs to an MH. As the number of FAs is big, the probability of FA failure and thus of datagram loss will increase. In our proposal, the maximum number of FAs a datagram is sent through is two, so probability of the datagram loss is lower.

4. When the MH micro-moves to another FA within the same visited domain, the new FA has the ability to independently *authenticate* the MH, not through the MFA. Hence the MFA will not need to authenticate MHs when MHs micro-move within the same visited domain. In other words, the FAs share the MFA's responsibility for authentication.

4 Security Analysis

Unforgeability

Our mobility management scheme employs the $public - key$ cryptosystem to achieve the MH's authentication. Like RSA [1, 12], our scheme achieves its security by offering difficulty of factorizing a composite positive integer that is the product of two large primes. To obtain the *secret key* d from the *public key* (e, N) is as difficult as to break RSA. So no attacker can use any other's *secret key* d to forge the *signature* S . Even if an attacker can produce a pair of his *public key* (e_A, N_A) and *secret key* d_A, she/he still cannot forge the *signature*.

Reply attacks

To fight reply attacks, each time MH is away to other FAs, it must add a *timestamp* to its *signature* for the micro-move re-registration request.

5 Conclusions and Future Work

In this article, we have proposed the *Group Foreign Agent* Management Scheme with *Public-Key* Cryptosystem. Our scheme can indeed reduce much traffic between the visited network and the home network, and the handoff delay is also avoided when an MH moves from one FA to another within the same visited domain. In addition, the FAs can *authenticate* MHs independently so that the heavy load on the MFA can be relieved. We will observe how the proposed scheme works by using a network simulator such as ns2 [5] in the future and compare our approach to other exiting approaches.

References

[1] Chin-Chen Chang and Min-Shiang Hwang, "Parallel computation of the generating keys for RSA cryptosystems," *IEE Electronics Letters*, vol. 32, no. 15, pp. 1365–1366, 1996.

[2] Stephen E. Deering, "ICMP router discovery message," *RFC 1256, Requset for Comments*, September 1991.

[3] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

[4] E. Gustafsson, A. Jonsson, and C. Perkins, "Mobile IP regional registration," *Internet Draft, draft-ietf-mobileip-reg-tunnel-04.txt, Mar 2001, Work in Progress*, 2001.

[5] ns2 network simulator. Available at http://www.isi.edu/nsnam/ns/.

[6] C. Perkins, "Application Statement for IP Mobility Support," *RFC 2005, Requset for Comments*, October 1996.

[7] C. Perkins, "IP Encapsulation within IP," *RFC 2003, Requset for Comments*, October 1996.

[8] C. Perkins, "IP Mobility Support," *RFC 2002, Requset for Comments*, October 1996.

[9] C. Perkins, “Minimal Encapsulation within IP,” *RFC 2004, Requset for Comments*, October 1996.

[10] C. Perkins, “Mobile-IP Local Registration with Hierarchical Foreign Agents,” *Internet Draft*, February 1996.

[11] J. B. Postel, “Inernet Control Message Protocol,” *RFC 792, Requset for Comments*, September 1981.

[12] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems,” *Communications of the ACM*, vol. 21, pp. 120–126, Feb. 1978.

[13] Bruce Schneier, *Applied Cryptography, 2nd Edition.* New York: John Wiley & Sons, 1996.

[14] John Zao, Stephen Kent, Joshua Gahmb, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, and Isidro Castineyra, “A public-key based secure mobile ip,” *Wireless Networks 5 (1999) 373-390*, 1999.