An Agent-Based Architecture for Securing Mobile IP

X. Yi
ICIS, School of EEE, Nanyang Technological University, Singapore 639798
exyi@ntu.edu.sg

S. Kitazawa, H.Sakazaki, E. Okamoto
JAIST, 1-1 Asahidai, Tatsunokuchi, Nomi, Ishikawa 923-1292, Japan
{shigeki, sakazaki, okamoto}@jaist.ac.jp

D.Frank Hsu
Dept.Computer and Information Science, Fordham University, NY 10023, USA
hsu@murray.fordham.edu

1. Introduction

The proliferation of powerful notebook computers and wireless communications promises to provide users with network access at any time and in any location. This continuous connectivity will allow users to be quickly notified of changing events and provide them with the resources necessary to respond to them even when in transit. Laptop computer should no longer be considered the poor cousins of workstations or even mainframe, but should be thought of instead as another choice in wide spectrum of available computer resource.

Unfortunately, present internetworking protocols such as TCP/IP, IPX, and Appletalk behave awkwardly when dealing with host migration between networks. Current versions of the Internet Protocol, or IP, make an implicit assumption that the point at which a computer attaches to the Internet is fixed and its IP address identifies the network to which it is attached. Datagrams are sent to a computer based on the location information contained in its IP address.

If a mobile computer, or mobile host, moves to a new network while keeping its IP address unchanged, its address will not reflect the new point of attachment. Consequently, existing routing protocols will be unable to route datagrams to it correctly. In this situation, the mobile host must be reconfigured with a different IP address representative of its new location. Not only is this process cumbersome for ordinary users, but it also presents the problem of informing potential correspondents of the new address. Furthermore, changing the IP address will cause already-established transport layer connections to be lost. Simply, under the current Internet Protocol, if the mobile host moves without changing its address, it will lose routing; but if it does change its address, it will lose connections.

Mobile IP [**1**] has been designed within the Internet Engineering Task Force (IETF) to server the needs of rapid growth of mobile computer users who wish to connect the Internet and maintain communications as they move from place to place. Mobile IP enables a mobile nodes to change its attachment point on the Internet which maintaining it IP address as well as its network connectivity using this IP address. The protocol permits mobile internetworking to be done on the network layer, however, it also introduces new vulnerabilities to the global Internet.

The IETF's IP Security (IPsec) Working Group is developing standards for IP-layer security mechanisms ([**2**] [**3**] [**4**] [**5**] [**6**]). The group is also developing generic key management protocols for use in the Internet. The current IPSec standards

include 3 algorithm-independent base specifications which are currently standards-track RFCs. These 3 RFCs are in the process of being revised (per usual IETF procedures) and the revisions will take into account a number of security issues.

In this paper, we propose a new solution for securing mobile IP. This solution introduces intelligent agent technology to design an architecture for securing mobile IP. The proposed agent-based architecture can provide (1) the mutual authentication among mobile user, home agent and foreign agent; (2) key distribution; (3) privacy protection for mobile user and home agent; (4) protection against replaying attack.

2. Overview of Mobile IP and Security Requirements of Mobile IP

2.1. Overview of Mobile IP. Mobile IP is an enhancement to IP which allows a computer to roam freely on the Internet while still maintaining the same IP address. IETF is currently developing a Mobile-IP standard which, at the time of this writing, is in its fifteenth revision. The Mobile-IP architecture, as proposed by the IETF, defines special entities called the Home Agent (HA) and Foreign Agent (FA) which cooperate to allow a Mobile Host (MH) to move without changing its IP address.

Each Mobile Host is associated with a unique home network as indicated by its permanent IP address. Normal IP routing always delivers packets meant for the MH to this network. When a MH is away, a specially designated computer on this network, its Home Agent, is responsible for intercepting and forwarding its packets.

The MH uses a special registration protocol to keep its HA informed about its current location. Whenever a MH moves from its home network to a foreign network, or from one foreign network to another, it chooses a Foreign Agent on the new network and uses it to forward a registration message to its HA.

After a successful registration, packets arriving for the MH on its home network are encapsulated by its HA and sent to its FA. Encapsulation refers to the process of enclosing the original datagram as data inside another datagram with a new IP header. This is similar to the post office affixing a new address label over an older label when forwarding mail for a recipient who has moved. The source and destination address fields in the outer header correspond to the HA and FA, respectively. This mechanism is also called tunneling since intermediate routers remain oblivious of the original inner IP header. In the absence of this encapsulation, intermediate routers will simply return packets back to the home network. On receiving the encapsulated datagram, the FA strips off the outer header and delivers the newly exposed datagram to the appropriate visiting MH on its local network.

As a consequence, mobile IP can be thought of as the three major cooperative subsystems. Firstly, there is a discovery mechanism defined so that the mobile computer can determine the new attachment points (new IP address) as they move from place to place within the Internet. Secondly, once the mobile computer knows the IP address as its new attachment point, it registers with the home agent which represents it at its home network. Lastly, mobile IP defines simple mechanism to deliver datagrams to the mobile host when it is away from its home network.

2.2. Security Requirements of Mobile IP. Security requirements of mobile IP should be considered from two perspectives: (1) the expectation of the foreign networks to prevent from the illegal mobile hosts while they are visited by

the mobile hosts; (2) the expectation of the mobile hosts to protect their communication when they visit the foreign networks.

The strong authentication of registration messages in both basic and route optimized Mobile IP is a crucial step to ensure correct and persistent IP connectivity for the mobile host. ¿From the economic benefit point of view, the foreign agent should authenticate the mobile host by inquiring the home agent of the mobile host during mobile IP registration of the mobile host. In addition, the home agent also should verify whether the registration request comes from its mobile host in case of providing free service to an illegal user while undertaking its network usage expense.

Once mobile IP registration of a mobile host is successful, the home agent and the foreign agent should consider the following confidentiality of traffic:

1. Confidentiality of traffic between the mobile host and its home agent.
2. Confidentiality of traffic between the mobile host and the foreign agent.
3. Confidentiality of traffic between the home agent and the foreign agent.

3. Description of the Agent-Based Architecture for Securing Mobile IP

3.1. Overview of the Proposed Architecture. The agent-based architecture intends to deal with security issues in the following situation:

A mobile host has moved from its home network to a foreign network and wants to register the foreign network. It has got access to the foreign network and have received broadcast information about a foreign agent in the foreign network. The mobile host firstly generates an intelligent agent with its registration request and then motivates it.

The intelligent agent automatically roams from the mobile host into the foreign agent. In the foreign agent, the intelligent agent submits the registration request to the foreign agent and asks for the foreign agent's information, then carries this information and further roams from the foreign agent into its home agent.

After the intelligent agent enters the home agent, submits the registration request and information of the foreign agent to the home agent and asks for the verification reply from the home agent. Based on the request, the home agent will generate another new intelligent agent. The new intelligent agent brings the verification reply and randomly selected shared secret keys among the mobile host, the home agent and the foreign agent back to the foreign agent.

The new intelligent agent submits the verification reply and shared secret key between the foreign agent and the home agent to the foreign agent and asks for registration reply and the shared secret key between the foreign agent and the mobile host from the foreign agent. Finally, the new intelligent agent brings this information back to the mobile host.

The whole architecture for securing mobile IP can be illustrated in the following figure:

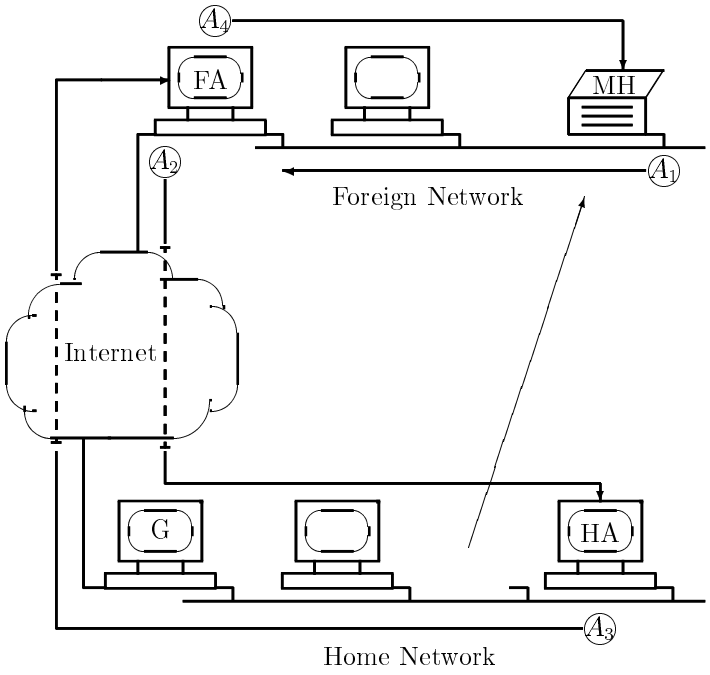

Fig.1 The agent-based architecture for securing mobile IP

In the following section, the procedures of securing mobile IP will be dealt with in detail.

3.2. Certificate and Signature Verification. We assume that the network involves a trusted certificate authority (CA) which provides participants of the network, including mobile hosts, home agents and foreign agents, with public key certificate service as follows:

1. As the Digital Signature Standard (DSS) [**7**], the certificate authority chooses three parameters (p, q, g), where p is a large prime, q is a large prime factor of $p-1$, $g = h^{(p-1)/q} \ (mod\, p)$ with h being an integer satisfying $1 < h < p-1$ and $h^{(p-1)/q} \ (mod\ p) > 1$.
2. Each participant in the network is required to generate a pair of signature public-secret keys. The pair of signature public-secret keys of the certificate authority is (y_{ca}, x_{ca}), where $y_{ca} = g^{x_{ca}}$ (mod p) and x_{ca} is a secret key chosen randomly from $GF(q)^*$. In the similar way, the pair of signature public-secret keys of a mobile host mh, denoted by (y_{mh}, x_{mh}), that of a home agent ha, denoted by (y_{ha}, x_{ha}), and that of a foreign agent fa, denoted by (y_{fa}, x_{fa}),
3. The certificate message is hashed. For example, as to a mobile host, we adopt the certificate format of X.509 [**8**] to construct C_{mh} which may contain such information as certificate serial number, validity period, the ID of mh, the public key (y_{mh}) of mh, the ID of CA, the public key (y_{ca}) of CA, etc, and then compute out the hash value $h(C_{mh})$ of C_{mh} by use of an one-way 2n-bit hash function which is based on a n-bit block cipher with 2n-bit key (such as IDEA [**9**]) and shown in the following figure:

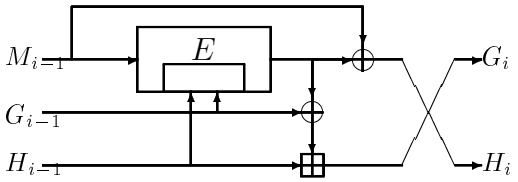

Fig.2 Computational graph for the hash round function h

In Fig.2, M_i, G_i and H_i are n-bit integers; E denotes a n-bit block cipher using 2n-bit key; $\bigoplus$ presents bitwise exclusive-or of n-bit blocks while $\boxed{+}$ indicates addition modulo 2^n of n-bit integers. The detail hash process can be seen in literature [**10**].

4. The certificate authority creates certificates for all participants. The digital signature of the certificate authority on a message C is composed of two numbers s and t which are defined as

$$s = g^r \ (mod\ p) \ (mod\ q) \tag{3.1}$$

$$t = -s \cdot x - h(C) \cdot r \ (mod\ q) \tag{3.2}$$

where r is a random number chosen from $GF(q)^*$.

Given (C^*, s^*, t^*), one can verify whether (s^*, t^*) is indeed a genuine signature of the certificate authority on C^* only by checking the following equation:

$$g^{t^*} \cdot y_{ca}^{s^*} \cdot s^{*h(C^*)} \ (mod\ p) = 1 \tag{3.3}$$

One can accept the digital signature of the certificate authority on the message C^* if the above equation holds.

3.3. Intelligent Agent Applications and its Structure. An intelligent agent can be defined as a software element (program, procedure, object, thread, etc.), owned by a user or another software element, capable of migrating, from one computer to another, to execute a set of tasks on behalf of its owner. Intelligent agents are said to be autonomous, in the sense that they can take their own decisions while away from their host. This implies that an intelligent agent is not just a piece of data being transferred between systems, but may also carry some code and state, which enables it to perform parts of its tasks in one system, migrate to another and continue its work there.

Intelligent agent technology has received growing interest from the research community and has matured significantly in the last few years [**11**] [**12**], however, the number of application using this technology is still scarce. In this paper, we try to apply the intelligent agent technology to fulfil the tasks of mobile IP registration and key distribution in a mobile IP protocol.

In the proposed architecture, the basic structure of an intelligent agent through Internet can be divided into seven distinct portions as follows:

1. Descriptor – the illustration of the intelligent agent's structure and format.
2. Certificate – the certificate of the intelligent agent's owner.
3. Code and state – the program executed in an agent execution environment to fulfil certain mission and the executed state.
4. Datagram – the information for receiver.
5. Time stamp – the time when the intelligent agent launches from the sender.
6. Signature – the signature of the intelligent agent's sender.
7. Attachment – the information attached by the foreign agent.

The structure of an intelligent agent can be illustrated in the following figure:

Fig.3 The structure of an intelligent agent

3.4. Flow of the Proposed Architecture.

3.4.1. *Foreign agent discovery.* Foreign agent advertises their availability on each link for which they provide service. The process of detecting a foreign agent is quite similar to that used by Internet nodes to detect routers running Internet Control Message Protocol (ICMP) Router Discovery (RFC 1256). The basic operation involved periodic broadcasts of advertisements by the router onto their directly attached network.

We assume that a mobile host has got access to the foreign network and has received the advertisement of a foreign agent which indicates the information of the foreign agent, such as location of the foreign agent. Now the mobile host wants to perform mobile IP registration.

3.4.2. *Intelligent agent generation.* The mobile host generates an intelligent agent on basis of the structure of intelligent agent as shown in Fig.3. In this time, the certificate portion is occupied by the mobile host's certificate issued by the certificate authority. As described in section 3.2, the certificate is composed of certificate message C_{mh} (based on the certificate format of X.509) and a pair of parameter (s_{mh}, t_{mh}) which satisfy equation (3.1) and (3.2). It should be noticed that the signature public key of the mobile host (y_{mh}) is included in the certificate message.

The code consists of two parts, the first part will be executed in the foreign agent, the second part will run in the home agent.

The datagram is filled by the registration request which at least indicates the locations of the foreign agent and the home agent.

The signature portion is put in by the signature of the mobile host on the portion $(M_{mh_{req}})$ from descriptor to time stamp of the intelligent agent. The procedure of signature is as follows (same as in the issue of certificate):

$$s_{mh_{req}} = g^r \ (mod\ p)\ (mod\ q) \tag{3.4}$$

$$t_{mh_{req}} = -s_{mh_{req}} \cdot x_{mh} - h(M_{mh_{req}}) \cdot r \cdot \ (mod\ q) \tag{3.5}$$

where r is a random number chosen from $GF(q)^*$.

Given $(M^*_{mh_{req}}, s^*_{mh_{req}}, t^*_{mh_{req}})$, one can verify whether $(s^*_{mh_{req}}, t^*_{mh_{req}})$ is indeed a genuine signature of the mobile host on $M^*_{mh_{req}}$ only by checking the following equation:

$$g^{t^*_{mh_{req}}} \cdot y_{mh}^{s^*_{mh_{req}}} \cdot {s^*_{mh_{req}}}^{h(M^*_{mh_{req}})}\ (mod\ p) = 1 \tag{3.6}$$

3.4.3. *Procedure of the Intelligent Agent Roaming Network.* The procedure of the intelligent agent roaming network can be illustrated in the following four distinct stages:

1. Mobile host $\Longrightarrow$ Foreign agent (it denotes the intelligent agent roams from the mobile host to the foreign agent)

Based on the location of the foreign agent, the intelligent agent roams from the mobile host into the foreign agent.

As soon as the intelligent agent enters the foreign agent, the foreign agent firstly performs verification procedure based on the certificate and signature of the intelligent agent by equations (3.3) and (3.6). If successful, the foreign agent supplies an agent execution environment for the intelligent agent to run.

In the environment, the intelligent agent submits the registration request to the foreign agent and asks it to provide its certificate, verification request to the home agent ($M_{fa_{req}}$) which at least involves the mobile host, the foreign agent and the current time, and its signature on ($M_{fa_{req}}$), i.e.,

$$s_{fa_{req}} = g^r \ (mod\ p)\ (mod\ q) \tag{3.7}$$

$$t_{fa_{req}} = -s_{fa_{req}} \cdot x_{fa} - h(M_{fa_{req}}) \cdot r \ (mod\ q) \tag{3.8}$$

where r is a random number chosen from $GF(q)^*$.

One can verify whether $(s^*_{fa_{req}}, t^*_{fa_{req}})$ is indeed a genuine signature of the foreign agent on $M^*_{fa_{req}}$ only by checking the following equation:

$$g^{t^*_{fa_{req}}} \cdot y_{fa}^{s^*_{fa_{req}}} \cdot {s^*_{fa_{req}}}^{h(M^*_{fa_{req}})} \ (mod\ p) = 1 \tag{3.9}$$

Then the above information from the foreign agent is attached behind the intelligent agent and brought into the home agent by the intelligent agent.

2. Foreign agent $\Longrightarrow$ Home agent

Before the home agent supplies an agent execution environment for the intelligent agent to run, it will verifies two signatures in the intelligent agent. One is signed by the mobile host. It can be checked by equation (3.6). Another is signed by the foreign agent. It can be verified by equation (3.9). If successful, the intelligent agent can reside at the agent execution environment and submits the registration request and the verification request to the home agent and asks it to form a new intelligent agent with the verification reply to the foreign agent.

According to the requirements from the intelligent agent and the structure of intelligent agent in Fig.3, the home agent generates another new intelligent agent. Now the certificate portion is replaced by the certificate of the home agent; the code is updated and specified to run at the foreign agent; the datagram is put in with the verification reply and two encapsulated secret keys which take the following forms respectively:

$$y_{fa}^{-t \cdot x_{ha}} \cdot K_1 \ (mod\ p) \tag{3.10}$$

$$y_{mh}^{-t \cdot x_{ha}} \cdot K_2 \ (mod\ p) \tag{3.11}$$

where K_1 and K_2 are 2n-bit random numbers which will act as the shared secret key of block cipher between the home agent and the foreign agent and the shared secret key of block cipher between the home agent and the mobile host respectively, t is the current time (i.e., time stamp of the new intelligent agent).

Finally, the home agent signs the portion ($M_{ha_{rep}}$) from the descriptor, to the time stamp of the new intelligent agent in the following way:

$$s_{ha_{rep}} = g^r \ (mod\ p)\ (mod\ q) \tag{3.12}$$

$$t_{ha_{rep}} = -s_{ha_{rep}} \cdot x_{ha} - h(M_{ha_{rep}}) \cdot r \ (mod\ q) \tag{3.13}$$

where r is a random number chosen from $GF(q)^*$.

One can verify whether $(s^*_{ha_{rep}}, t^*_{ha_{rep}})$ is indeed a genuine signature of the home agent on $M^*_{ha_{rep}}$ only by checking the following equation:

$$g^{t^*_{ha_{req}}} \cdot y_{ha}^{s^*_{ha_{rep}}} \cdot {s^*_{ha_{rep}}}^{h(M^*_{ha_{rep}})} \ (mod\ p) = 1 \tag{3.14}$$

3. Home agent $\Longrightarrow$ Foreign agent

   The new intelligent agent roams back to the foreign agent again. After verifying the intelligent agent by equation (3.14), the foreign agent supplies an agent execution environment for the new intelligent agent to run again. In the environment, it submits the verification reply and the encapsulated shared secret key (3.10) to the foreign agent. From (3.10), the foreign can elicit K_1 in the following way:

$$(y_{ha})^{t \cdot x_{fa}} \cdot (y_{fa}^{-t \cdot x_{ha}} \cdot K_1) \ (mod\ p) = K_1 \tag{3.15}$$

   where t is the time stamp in the intelligent agent.

   Then the new intelligent agent asks the foreign agent to provide its certificate, registration reply, the encapsulated shared secret key between the mobile host and the foreign agent, and signature on the above information (denoted as $M_{fa_{rep}}$).

   The registration reply should specify a care-of address in the foreign network to the mobile host.

   The encapsulated secret key takes the following form:

$$y_{mh}^{-t \cdot x_{fa}} \cdot K_3 \ (mod\ p) \tag{3.16}$$

   where K_3 is a 2n-bit random number which will act as the shared secret key of block cipher between the foreign agent and the mobile host, t is the time stamp of the intelligent agent.

   The signature of the foreign agent on $M_{fa_{rep}}$ is:

$$s_{fa_{rep}} = g^r \ (mod\ p)\ (mod\ q) \tag{3.17}$$

$$t_{fa_{rep}} = -s_{fa_{rep}} \cdot x_{fa} - h(M_{fa_{rep}}) \cdot r \ (mod\ q) \tag{3.18}$$

   where r is a random number chosen from $GF(q)^*$.

   One can verify whether $(s^*_{fa_{rep}}, t^*_{fa_{rep}})$ is indeed a genuine signature of the foreign agent on $M^*_{fa_{rep}}$ only by checking the following equation:

$$g^{t^*_{fa_{req}}} \cdot y_{fa}^{s^*_{fa_{rep}}} \cdot {s^*_{fa_{rep}}}^{h(M^*_{fa_{rep}})} \ (mod\ p) = 1 \tag{3.19}$$

   The new intelligent agent put all the information provided by the foreign agent in its attachment and roams back to the mobile host.

4. Foreign agent $\Longrightarrow$ Mobile host

   After receiving the new intelligent agent, the mobile host will verify the signature of the home agent on the new intelligent agent by equation (3.14) and the signature of the foreign agent on the registration reply by equation (3.19). Then it elicits the secret keys K_2, K_3 in the following way:

$$(y_{ha})^{t\cdot x_{mh}} \cdot (y_{mh}^{-t\cdot x_{ha}} \cdot K_2)\ (mod\ p) \quad = \quad K_2 \tag{3.20}$$

$$(y_{fa})^{t\cdot x_{mh}} \cdot (y_{mh}^{-t\cdot x_{fa}} \cdot K_3)\ (mod\ p) \quad = \quad K_3 \tag{3.21}$$

Finally, The secret tunnels between the home agent and the foreign agent, between the home agent and the mobile host, and between the foreign agent and the mobile host are established with the shared secret keys K_1, K_2, K_3 of block cipher respectively. It is noticed that we suggest to adopt the same block cipher to encrypt information as the underlying block cipher in Fig.2 to save storage space.

4. Security Analysis of the Architecture for Securing Mobile IP

4.1. Security of the Signature Scheme in the Architecture. We now consider that a signer signs a message by adopting the signature scheme in the proposed architecture. For example, the mobile host signs $M_{mh_{req}}$ by generating a pair $(s_{mh_{req}}, t_{mh_{req}})$ according to equation (3.4) and (3.5). Because of the participation of the mobile host's secret key in the formation of the digital signature $(s_{mh_{req}}, t_{mh_{req}})$ of the mobile host on $M_{mh_{req}}$, an attacker can not directly use the equations (3.4) and (3.5) to forge a valid signature pair $(s_{mh_{req}}, t_{mh_{req}})$.

A direct method by which an attacker may try is choosing a random number $s_{mh_{req}}$ (or $t_{mh_{req}}$) and then solving out $t_{mh_{req}}$ (or $s_{mh_{req}}$) from the equation (3.6) to forge a valid pair $(s_{mh_{req}}, t_{mh_{req}})$. However, the difficulty is at least equal to that of computing discret logarithm over finite fields.

In view of the above analysis, we conclude that:

THEOREM 4.1. *The difficulty of breaking the signature scheme in the proposed architecture is at least equivalent to the difficulty of computing discrete logarithm over finite fields.*

4.2. Security of the Key Distribution Scheme in the Architecture. We now take the key distribution between the home agent and the mobile host as an example. Except the home agent and the mobile host, the others do not know how to compute $y_{ha}^{-t\cdot x_{mh}}$ (or $y_{mh}^{-t\cdot x_{ha}}$) because at least one of the home agent's and the mobile host's signature secret keys is definitely required in the computation. Therefore, the others can not separate the shared secret key K_2 between the home agent and the mobile host from $y_{mh}^{-t\cdot x_{ha}} \cdot K_2\ (mod\ p)$ like the process in (3.20). The idea is similar to the scheme proposed by El Gamal [**13**], in which message M is sent to an entity A in the form $(g^r, M \cdot g^{r\cdot x_a})$, where r is a random number, x_a and g^{x_a} are the secret and public key of the entity A respectively. It suffices for the sender to know g^{x_a}, whereas A can recover M by computing first $g^{-r\cdot x_a}$. An eavesdropper faces the problem of computing discrete logarithms.

On basis of the above analysis, we conclude that:

THEOREM 4.2. *The difficulty of breaking the key distribution scheme in the proposed architecture is equivalent to the difficulty of breaking the El Gamal scheme.*

4.3. Protection Against Replaying Attack. The adoption of time stamp at each stage of the architecture makes the replaying attack is insignificant.

Firstly, because the existence of time stamp and signature in the structure of an intelligent agent, an eavesdropper can not use an expired intelligent agent to perform the replaying attack. In addition, the time stamp is considered in key

distribution such as (3.10). It increases the difficult of breaking the key distribution scheme and makes replaying attack vainness.

4.4. Mutual Authentication. The mobile host can authenticate its home agent in the following two ways:

1. On basis of the certificate, the verification reply, the signature of its home agent in the return intelligent agent, the mobile host can verify whether the above information has truly come from its home agent.
2. The mobile host can also authenticates its home agent by verifying whether it can elicit the true shared secret key K_2 in the process of (3.20). Actually, the mobile host can not ensure whether K_2 is true in the beginning. However, it will be verified by testing whether it can be used to recover the ciphertext to significant plaintext in the later communication between the mobile host and its home agent. If no problem, the mobile host has authenticated its home agent because only the home agent can generate the shared secret key K_2 which can only be elicited by the mobile host.

The foreign agent also can authenticate the home agent in the above same ways. As a consequence, the architecture provides double secure authentications for the mobile host and the foreign agent.

4.5. Protection of Servers against Malicious Intelligent Agents. An intelligent agent is unique in that its code is executed by a server. Thus an executing intelligent agent has automatic access to some of a server resources. With this level of access intelligent agents can mount attacks by propagating viruses, worms and Trojan horses, impersonating other users and mounting denial of service attack. The standard approach to this problem is to reject all unknown code from entry into servers. It is not a viable solution in a mobile agent environment. Both Telescript [**14**] and Safe-Tcl [**15**] offer approaches to solve the problem.

In the proposed architecture, before a server supplies an agent execution environment for a visiting intelligent agent to run its code, the server will verify the signature. Once any problem occurs when the server runs the code on an agent execution environment, the owner of the intelligent agent is probably malicious and will be accused.

4.6. Protection of Agents against Malicious Servers. In order for an intelligent agent to run, it must expose its code and data to the host environment which supplies the means for this agent to run. The host can always scan the intelligent agent for information, alter the agent state and code, even kill the agent. Thus, the intelligent agent is unprotected from the host. Fortunately, it does not affect our architecture very much from the economic benefit point of view. Both the foreign agent and the home agent are reluctant to attack an intelligent agent dedicating to mobile IP registration and key distribution.

Current consensus is that it is computationally impossible to protect mobile agents from malicious hosts. Instead of tackling the problem from a computational (difficult) point of view, current research [**16**] is looking at sociological means of enforcing good host behavior.

5. Performance Analysis of the Architecture for Securing Mobile IP

The proposed architecture has two significant performance characteristics. One is intelligent characteristic. The missions of mobile IP registration and key distribution are automatically completed by the intelligent agent. The intelligent agent automatically roams the network and executes its code in an agent execution environment supplied by a server. The manual interference is reduced to the least. The another characteristic is its mobility. The intelligent agent migrates itself to the server to fulfil its task so that the network transportation load in the architecture has been great reduced because only a few communications are needed.

6. Conclusion

Many of the most important application of intelligent agents will occur in fairly uncontrolled, heterogeneous environment. In this paper, we have proposed an agent-based architecture for securing mobile IP, which can provide (1) the mutual authentication among mobile host, home agent and foreign agent; (2) key distribution; (3) privacy protection for mobile user and home agent; (4) protection against replaying attack.

The individual properties of the proposed agent-based architecture for securing mobile IP can be concluded as follows:

1. The mission of mobile IP registration and key distribution are completed by intelligent agents;
2. A new signature scheme suitable for mobile hosts is adopted in the architecture; The difficult of breaking the signature scheme is equivalent to that of computing discrete logarithm.
3. A new key distribution is used in the architecture. The difficulty of breaking the key distribution scheme in the proposed architecture is equivalent to the difficulty of breaking the El Gamal scheme.
4. Only a block cipher is used to act as both encryption algorithm and underlying block cipher of the hash function.
5. In view of the existence of signature in each stage of intelligent agent, nonrepudiation of origin guarantees a host to falsely deny having sent a message. So any malicious action will be detected and the breeder will be captured.

Our further works will focus on optimal improvement and then implementation of the agent-based architecture for securing mobile IP. The authors will be grateful to receive any suggestion to the architecture.

Acknowledge

We would like to appreicate Dr.Tada for the helpful discussion.

References

[1] C. Perkins (ed.) *IP mobility support*, RFC2002, proposed standard. IFTF mobile IP working Group, Oct., 1996.

[2] R. Atkinson, *Security architecture for the Internet protocol*, request for comments (proposed standard) RFC 1825, IFTF mobile IP working group, August 1995.

[3] R. Atkinson, *IP authentication header*, request for comments (proposed standard) RFC 1826, IFTF mobile IP working group, August 1995.

[4] R. Atkinson, *IP encapsulation security payload (ESP)*, request for comments (proposed standard) RFC 1827, IFTF mobile IP working group, August 1995.

[5] P. Metzger and W. Simpson, *IP authentication using keyed MD5*, request for comments (proposed standard) RFC 1827, IFTF mobile IP working group, August 1995.

[6] P. Metzger, P. Karn and W. Simpson, *The ESP DES-CBC transform*, request for comments (proposed standard) RFC 1827, IFTF mobile IP working group, August 1995.

[7] *The digital signature standard*, Comm. ACM, Vol.35, No.7, pp.36-40, 1992.

[8] ISO/IEC 8696-8 (1993), Information Technology - Open System Interconnection -The Directory: *Authentication Framework*.

[9] X.J.Lai and J.L.Massey, *A proposal for a new block encryption standard*, Advances in Cryptology, Proc. of EUROCRYPT'90, Lecture Notes in Computer Science **473** (1991)389–404.

[10] X.Yi and K.Y.Lam, *Hash function based on block cipher*, IEE Electronics Letters, 33(23), 1997.

[11] D.Chess, C.Harrison and A.Kershenbaum, *Mobile agents: are they a good idea*, Technical Report, March 1995, IBM T.J.Watson Research Center, NY.

[12] D.Chess, B.Grosof, C.Harrison, D.Levine, C.Parris and G.Tsudik, *Itinerant Agents for Mobile Computing*, Technical Report, October 1995, IBM T.J.Watson Research Center, NY.

[13] T.ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithm*, IEEE Trans. Info. Theory, Vol.IT-31, No.4, pp.468-472, July 1985.

[14] J.White, Telescript Technology: *The foundation of the electronic market place*, General Magic white paper 1995.

[15] N.Borenstein, *EMail with a mind of its own: The Safe-Tcl language for enabled mail*, IFIP WG 65 Conference, Barcelona, May, 1994, North Holland, Arnsterdam, 1994.

[16] L.Rasmusson and S.Janson, *Simulated social control for secure Internet commerce*, In New Security Paradigms'96, ACM Press, September 1996.