Practical Solution for Location Privacy in Mobile IPv6

SuGil Choi, Kwangjo Kim, and ByeongGon Kim

International Research center for Information Security (IRIS)
Information and Communications University (ICU)
58-4 Hwaam-dong, Yusong-gu, Daejeon, 305-732, South Korea
{sooguri, kkj, virus}@icu.ac.kr

Abstract. Mobile IP (MIP) enables the Mobile Node (MN) to move around without loosing their transport-layer connectivity by using resources in the foreign domain network. MIP is expected to be the core infrastructure of future mobile communication, but certain level of security services must be provided before the wide deployment of MIP. Security services, such as authentication and access control, have been considered since the birth of MIP, but little attention has been given to location privacy services despite of their increased significance in wireless network. MIPv6 uses IPSec to provide data confidentiality and authentication between Home Agent (HA) and the Mobile Node (MN). However, no practical solution was suggested for location information protection in MIP. During the past years a variety of theoretical concepts for location privacy have been proposed, but most of them are not applicable to MIP communication. So, in this paper, we identify required level of location privacy, and propose new protocol for providing the identified level of location privacy.

1 Introduction

Mobile IP is a protocol for passing IP datagrams between the MN and its Corresponding Node (CN) as the MN changes its attachment point on the Internet. MIP is currently a hot research area and expected to be the core part of future mobile communication. However, there are several issues that must be addressed before the wide deployment of MIP. One of the important tasks is to provide secure MIP communication.

Throughout the development of MIP, the following security services have been considered useful for protecting a mobile Internet:

- Data integrity, origin authentication and anti-replay protection of MIP registration and location update message
- Access control of the MN when they use resources on the foreign networks
- Location privacy and anonymity of the MN

Among these services, the first two are essential to secure MIP communications and have been main research area in MIP security. On the other hand, location privacy and anonymity have been largely ignored. But, these two services have a great significance especially in wireless network which is more vulnerable to eavesdropping attack than wired network. The disclosure of the MN's location or identity can be a serious violation of the MN's privacy.

In MIP communication, location privacy and anonymity are not independent security services because location privacy service can be provided on top of anonymity service. As long as the identity of the MN is kept secret, the disclosure of the MN's location is not a violation of the MN's privacy as nobody knows who is in the place. Therefore, we don't need to worry about location privacy while anaonymity is provided. To help understanding, before proceeding any further, we need to clarify the scope of anonymity and location privacy that we strive to achieve in a MIP communication.

- anonymity: no entity other than the MN should know any information regarding the user's identity, unless the MN decides to disclose such information.
- location privacy: any entity which is authorized to know the MN's real identity will not be able to know the exact physical location of the MN, unless the MN decides to reveal such information or another person physically sees the MN at that location.

As we can see in the definition, anonymity is prerequisite to location privacy.

During the past years a variety of theoretical concepts for location privacy and anonymity, such as Mix-network [9], Onion Routing [12], and Anonymizer [8], have been proposed. These can be classified into *Cascading Overlay Network based system* and *Centralized Trusted Entity based system. Cascading Overlay Network based system* can hide the location of communicating entities from strong attackers, but it is not suitable for real time communication. *Centralized Trusted Entity based system* is strong against only weak attacker, but it is more efficient and practical. We will explain those systems in Section 2.2 and the definition of strong attacker and weak attacker will be given in Section 4.1.

Our approach employs the concept of centralized trusted entity and we would call the entity *Information Translating Proxy* (ITP). ITP makes the location information and identification information invisible to other communication participants and attackers by translating those information, unless the MN decides to disclose such information. This is similar to the function of Anonymizer, but our approach has several distinct characteristics such as:

- It operates on the network layer, so it uses only network layer information to process received information and forward it to final destination. It is compatible with IPv6 specifications.
- The operation of ITP doesn't require storing any session state information, so it doesn't need to worry about state information safeguarding as in Anonymizer.
- It authenticates every incoming request.

Our proposed scheme is focused on providing location privacy on network control messages, not content data. Also, it will provide revocable privacy rather than perfect privacy because, in case of serious crime, the location history and identity must be revealed.

Organization. The organization of this paper is as follows: In Section 2, we explain Mobile IP and location privacy providing systems. Section 3 classifies different requirements of location privacy in MIP communication. Considered factors for designing protocol are described in section 4, and our proposed protocol is presented in section 5. In Section 6, we conclude by mentioning a few directions about the following research.

2 Background

2.1 Mobile IP

Internet Protocol routes packets to their destination according to IP addresses which are associated with a fixed network. So, when the packet's destination is a mobile node, this means that each new point of access made by the node is associated with a new network number, hence, new IP address must be set to maintain connections as the MN moves from place to place. This makes transparent mobility impossible.

In MIPv4, MNs use two IP addresses: home address and care-of address (CoA). The home address is static and used to identify TCP connections. The CoA changes at each new point of attachment. MIP requires the existence of a network node known as the home agent (HA) and foreign agent (FA). Whenever the MN moves, it registers its new CoA with its HA and the HA redirects all the packets destined for the MN to the MN's CoA. In MIPv4, FA broadcasts agent advertisement at regular intervals and the MN gets network configuration information from the FA advertisement.

MIPv6 shares many features with MIPv4 but there are several major differences. First of all, MIPv6 uses IPv6 address structure [4]. Another difference is the support for "Route Optimization" as a built-in fundamental part of the MIPv6 protocol. The Route optimization allows direct routing from any CN to any MN without needing to pass through the MN's home network and be forwarded by its HA, and thus eliminates the problem of "triangle routing" present in MIPv4. And, there is no need to deploy special routers as FA.

2.2 Location Privacy Providing Systems

Mix-network In [9], Chaum introduced the idea of mix-network. It is a set of servers that serially decrypt or encrypt lists of incoming messages and outputs them in a random order in such a way that attacker cannot correlate which output message belongs to which input message, without the aid of the mix nodes, when several messages are passed simultaneously. However, the goal of real time communication can't be achieved because it requires several public key encryption and decryption, and intentional time delay to defeat correlation attack.

Onion Routing When using Onion Routing [12], a user sends encrypted data to a network of so-called Onion Routers. A trusted proxy chooses a series of these network nodes and opens a connection by sending a multiply encrypted data structure called an "onion" to the first of them. Each node removes one layer of encryption, which reveals parameters such as session keys, and forwards the encrypted remainder of the onion to the next network node. Once the connection is set up, an application specific proxy forwards HTTP data through the Onion Routing network to a responder proxy which establishes a connection with the web server the user wishes to use. The user's proxy multiply encrypts outgoing packets with the session keys it sent out in the setup phase; each node decrypts and forwards the packets, and encrypts and forwards packets that contain the server's response. In spite of the similar design to mix-network, Onion Routing cannot achieve the traffic analysis protection of an ideal mix-network due to the low-latency requirements.

Crowds Crowds [11] consists of a number of network nodes that are run by the users of the system. Web requests are randomly chained through a number of them before being forwarded to the web server hosting the requested data. The server will see a connection coming from one of the Crowds users, but cannot tell which of them is the original sender. In addition, Crowds uses encryption, so that some protection is provided against attackers who intercept a user's network connection. However, this encryption does not protect against an attacker who cooperates with one of the nodes that the user has selected, since the encryption key is shared between all nodes participating in a connection. Crowds is also vulnerable to passive traffic analysis: since the encrypted messages are forwarded without modification, traffic analysis is trivial if the attacker can observe all network connections. An eavesdropper intercepting only the encrypted messages between the user and the first node in the chain as well as the cleartext messages between the final node and the web server can associate the encrypted data with the plaintext using the data length and the transmission time.

Anonymizer Anonymizer [8] is essentially a server with a web proxy that filters out identifying headers and source addresses from web browsers' requests (instead of seeing the users true identity, a web server sees only the identity of the Anonymizer server). This solution offers rather weak security (no log safeguarding and a single point of vulnerability).

We classify the first three into *Cascading Overlay Network based system* and Anonymizer into *Centralized Trusted Entity based system.*

3 Classification of Location Privacy Requirements

Location privacy can be defined according to two different dimensional parameters: information related to the identification of the user and entities which are able to have access to these pieces of information. The required level of location privacy depends on various factors like the effect on performance incurred by providing this service, assumed attackers' capabilities and so on. To help choose the adequate level of location privacy necessary for a given environment, it is necessary to develop a classification scheme to represent the various possible levels of location privacy requirements.

A specific location privacy requirement is represented in terms of two dimensional matrix. If a particular class of entities knows a particular piece of information, the corresponding table entry is marked 1. Otherwise, it is marked 0.

In the case of Mobile IP communication, the different classes of entities which might know private information are: the home network provider (H), the foreign network provider (F), the corresponding node (C) and attacker (A).

The reason why we use the term private information, instead of location information, is that hiding location information alone can not guarantee location privacy and perfect protection of location information from all entities mentioned above is impossible because foreign network provider can always know the location of the MN. To provide location privacy against foreign network provider, the MN's identification information should not be disclosed. Without knowledge of the MN's real identity, it is not a violation of the MN's privacy to know the MN's physical location. In other words, as long as anonymity is provided, we don't need to try to protect location information. Therefore, we can define location privacy requirements on top of anonymity requirements and we will see possible levels of anonymity requirements first.

3.1 Possible Levels of Anonymity Requirements

The real identity of the MN may be discovered by the disclosure of identity itself or analyzing the traffic between the foreign and the home network. In other words, when the MN accesses the foreign network, if the identity of his home network is not protected, the information about the MN's real identity may be inferred. The home network address in address field of packet header or Network Access Identifier (NAI) [3] can reveal the identity of home network. NAI is formed like (username"@" realm). Example of valid NAI is fred@wisa.com. NAI is a standardized method for identifying users and enhances the interoperability of roaming and tunnelling services. So, we expect NAI will be used widely and assume identity is represented using NAI. Here is one example that the MN's real identity is inferred from the HN identity. If the MN visiting the foreign network in Japan wants to authenticate to his HN cwd.go.kr and an attacker happens to know that the only user from cwd.go.kr currently in Japan is president, the attacker can know that the the user of the MN is president. We call the MN identity Mi and the HN identity Hi.

We saw that Mi can be inferred from Hi. But, it is also true that, in most cases, Hi gives just rough idea about Mi. So, revealing Hi while keeping Mi secret is not so serious as disclosing Mi itself. But, hiding Hi while disclosing Mi is meaningless because NAI contains the HN identity. Hence, there are only two kinds of the MN identity protection. One is weak identity protection, hiding Mi while revealing Hi, so others can know to which home network this MN belongs, but not exact the MN identity. The other is strong identity protection or *complete anonymity*, hiding both Mi and Hi.

The possible levels of anonymity requirements can be a combination of four different classes of entities and two kinds of the MN's identity protection mechanism. (Anonymity Level: AL)

Table 1. AL4

	H	**F**	**C**	**A**
Mi	1	0	0	0
Hi	1	1	1	1

AL1: hiding Mi from only attacker
AL2: hiding Mi from the FN and attacker
AL3: hiding Mi from the CN and attacker
AL4: hiding Mi from the CN, the FN, and attacker

Table 2. AL8

	H	**F**	**C**	**A**
Mi	1	0	0	0
Hi	1	0	0	0

AL5: AL4 + hiding Hi from attacker
AL6: AL4 + hiding Hi from the FN and attacker
AL7: AL4 + hiding Hi from the CN and attacker
AL8: AL4 + hiding Hi from the CN, the FN, and attacker

AL8 is the minimum set of requirement for *complete anonymity* against all entities except the HN. We assume that the HN should know the MN's real identity for authentication.

3.2 Possible Levels of Location Privacy Requirements

Various levels of anonymity requirements was identified in 3.1. We can provide location privacy just by hiding location information against entities which know the MN's identity because, without knowledge of the MN's real identity, it is not a violation of the MN's privacy to know the MN's physical location. So, there can be eight different location privacy requirements. We show two location

Table 3. LPL6

	H	**F**	**C**	**A**
Mi	1	0	0	0
Hi	1	0	1	0
Li	0	1	0	1

Table 4. LPL8

	H	**F**	**C**	**A**
Mi	1	0	0	0
Hi	1	0	0	0
Li	0	1	1	1

privacy requirements built on top of AL6 and AL8. We call location information Li. (Location Privacy Level: LPL)

When any one of 8 LPLs is provided, no entities other than the MN can know the location information of the MN. However, LPL8 is the most desired level of location privacy requirement because it provides *complete anonymity* at the same time.

4 Practical Considerations

4.1 Threat Model

Potential entities that might try to collect location history of the MN can be classified into two groups: legitimate entities and illegitimate entities.

The HN, the FN, and the CN are legitimate entities. It is assumed that the maintainer of the FN and the CN are not necessarily trustworthy. Likewise, Home Network operator and thus home agent need not be trusted. These legitimate entities can collect location information from incoming messages without much effort and can use it against user's privacy. We assume these entities are passive in gathering location information, which means they don't take any other actions to get the information but extracting it from incoming messages.

Attackers are illegitimate entities. They can be roughly classified into strong attacker and weak attacker. Strong attacker is the one who is able to perform eavesdropping at arbitrary locations in the network and may trace messages while they traverse the network and thus link the sender of a message to its recipient. Eavesdropping at arbitrary locations in the network requires the capability of compromising arbitrary routers, which is very difficult if proper security measure is in place. We define weak attacker as the one who doesn't have the ability of compromising existing system, but just use leaking information. One example of leaking information is the message transmitted over wireless network. Everyone with simple device can eavesdrop the communication. When we build security measure against strong attacker, location privacy can be guaranteed almost perfect, but strong security comes with high cost and low performance. So, in this paper, we develop protocol assuming weak attacker for practicality and wide deployment. We expect there will be other systems that provide location privacy against strong attacker.

- legitimate entities (HN, FN, CN): passive collection of location information from incoming messages
- illegitimate entities (attackers): no ability of compromising existing systems, just can eavesdrop messages transmitted over wireless network

4.2 Selection of Protocol Components

Return Routability (RR) Protocol. The RR procedure enables the CN to obtain some reasonable assurance that the MN is in fact addressable at its claimed care-of address (CoA) as well as its home address. Only with this assurance is the CN able to accept Binding Update from the MN which instructs the CN to direct that MN's data traffic to its claimed CoA. This is done by testing whether packets addressed to the two claimed addresses are routed to the MN. The MN can pass the test only if it is able to supply proof that it received certain data which the CN sends to those addresses. The below figure shows the message flow for the RR procedure. Due to space constraints, we do not go into the details of RR protocol. The reader is referred to the document [2] for more information.

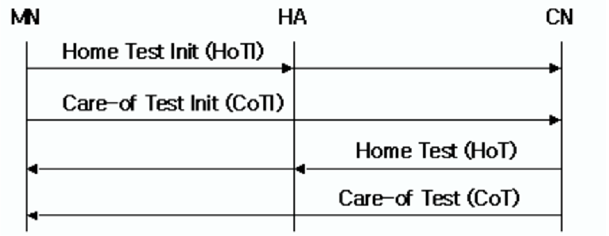

Fig. 1. RR Protocol

This protocol does not protect against attackers who are on the path between the HN and the CN. However, in our threat model, attackers don't have the ability of compromising existing systems, so attackers can't eavesdrop communication between the HN and the CN. RR protocol is not vulnerable in our threat model and it doesn't assume security associations or existence of authentication infrastructure between the MN and the CN. Therefore, RR protocol is just right fit in our model.

Information Translating Proxy. We classified location privacy providing systems into *Cascading Overlay Network based system* and *Centralized Trusted Entity based system. Cascading Overlay Network based system* assumes strong attackers, but can hardly provide real time service. *Centralized Trusted Entity based system* assumes relatively weak attackers, but provides practical solution. As we assumed weak attackers and passive collection of location information from incoming messages by legitimate entities, in our threat model, *Centralized Trusted Entity based system* can give enough level of security. We would call the system *Information Translating Proxy* (ITP).

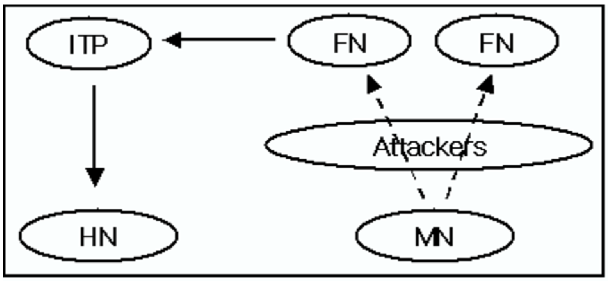

Fig. 2. Scenario based on ITP and weak attacker

5 Our Proposed Protocol

This section presents the way our proposed protocol provides location privacy in Home Binding Procedure and shows how location privacy can be revoked in case of serious crime. This protocol aims at providing LPL8 defined in section 3. We will use the following notations to describe the protocol.

Table 5. Notation

Symbol	**Description**
K_{AB}	Shared key between A and B
h()	One-way hash function
A | B	Concatenation of A and B
$prf(k, M)$	keyed pseudo random function. It accepts a secret key k and a message M, and generates a pseudo random output
$\{M\}_K$	Encryption of message M using key K

5.1 System Setup

Every message that needs special treatment for location privacy goes through ITP. ITP processes incoming messages and forwards it to the final destination. Hence, ITP needs association mechanism which enables bidirectional communication through ITP. In Anonymizer, system keeps track of source IP addresses and source port numbers of each request from users, and destination IP addresses and source port numbers of forwarded requests to the final destination. With those mapping information, Anonymizer can deliver received data to users in correct way.

As an association mechanism in ITP, we developed new mechanism. It operates on the network layer, so it uses only network layer information to associate incoming and outgoing traffic, not other layer element like port number. The operation of ITP doesn't require storing any session state information, so we don't need to worry about state information safeguarding as in Anonymizer and it becomes easy to manage the system.

New Association Mechanism. This requires secret key sharing between ITP and the MN. Each MN creates ephemeral pseudonym (64 bit) randomly and ITP generates secret key between ITP and the MN

K_{IM} = h(K_I | MN's pseudonym) (K_I is the secret key of ITP)

Initial Key Creation: When MN joins home network for the first time, it gets K_{IM}. MN shows that he belongs to the home network with the help of home network and delivers pseudonym and certificate to ITP. ITP authenticates the MN and his home network, and creates K_{IM} as shown above. K_{IM} is encrypted with the MN's public key, so nobody can know the key during delivery. This procedure is done just after the MN joins home network, so we can assume that the MN's communication doesn't need to go through ITP because the MN is in home network and, thus, the time delay for initial key setup doesn't cause a problem.

Key Update: When MN moves to different foreign network, it updates key K_{IM}.

- The MN creates new ephemeral pseudonym (64 bit)
- The MN creates care-of address (CoA) = { FN subnet prefix (64 bit) | pseudonym (64 bit)}
- Duplication check of CoA
- The MN sends Key Update Message to ITP
  Key Update Message = {previous pseudonym, nonce, $\{homeaddress, newCoA\}_{K_{IM}}$, MAC}
  MAC = $prf(K_{IM}, previouspseudonym|nonce|\{homeaddress, newCoA\}_{K_{IM}})$
- ITP verifies the Key Update Message, generates new K_{IM}, and sends Acknowledgement containing new K_{IM} encrypted with previous K_{IM}.

Key update procedure includes normal MIP procedure. When MNs arrive at new foreign network, they create new CoA and check duplication of CoA. The process of Duplicate Address Detection is explained in the following paragraph. But, proposed key update procedure employs different way of CoA creation. The FN subnet prefix is obtained by listening to local router advertisement. It is common practice to derive the remaining 64 bit *Interface Id* from the interface's MAC (EUI-64 global identifier) address [4]. However, in this protocol, the *Interface Id* is a randomly generated ephemeral pseudonym. This pseudonym is 64 bit long and random collisions occur after 2^{32} pseudonyms have been generated. But, this is not a problem because it is not likely that 2^{32} addresses are used at the same time in a subnetwork and, if collisions occur, the collisions can be avoided through Duplicate Address Detection. The "u" and "g" bits of an IPv6 *Interface Id* have the semantics defined for EUI-64 global identifiers in which the "u" bit is set to one to indicate global scope, and it is set to zero to indicate local scope. "g" bit is the individual/group bit and is set to zero to indicate unicast address. (The "u" and "g" bits are the seventh bit and eighth bit of the first byte of *Interface Id* respectively) Therefore, in our way of CoA creation, "u" and "g" bits are always set to zero because its uniqueness is checked locally through Duplicate Address Detection [5]. In other words, the seventh and eighth bits of pseudonym must be zero. But, it should not be mistaken for locally routable address. For a set of addresses formed from the same subnet prefix, it is sufficient to check that the link local address generated from the subnet prefix is unique on the link to be a globally routable address. In this sense, the CoA generated in new way is globally routable address with locally unique *Interface Id*.

There is one thing that we have to be very careful in checking address duplication. For address duplication check, the MN sends a Neighbor Solicitation Message containing the tentative address as the target. If another node is already using that address, it will return a Neighbor Advertisement saying so. When globally routable address with locally unique *Interface Id* is used, this Duplicate Address Detection works fine in IPv6 communication. But, it can cause a problem in MIPv6 communication. When the MN sends a Neighbor Solicitation Message containing new CoA, if a node using the home address same as the CoA is visiting foreign network, the node can't respond to the Neighbor Solicitation Message though the CoA is same as his home address. If the MN uses the CoA, he can't receive any data from outside because HA will intercept every packet destined for the CoA and redirect it to outside. This problem happens because a network can be home network to a node and foreign network to visiting node at the same time. To solve this problem, HA must have the functionality to respond to the Neighbor Solicitation Message if there is a node using the requested CoA as the home address while the node is away from home network.

In Key Update Message, home address and new CoA are encrypted with K_{IM} to prevent correlation of pseudonyms of the MN. As only previous pseudonym appears in plaintext, others can not correlate the previous pseudonym to new pseudonym or new CoA. New pseudonym is contained in new CoA, so ITP can extract new pseudonym from new CoA. But, care must be taken not to use new CoA as the source address of the packet containing Key Update Message. Otherwise, attacker can correlate previous pseudonym to new CoA and, thus, new pseudonym. Temporary CoA must be used just for sending and receiving Key Update Message and Acknowledgement. ITP can generate key K_{IM} to decrypt the encrypted part of Key Update Message from previous pseudonym and its secret key as shown above.

In the verification of Key Update Message, it is not sufficient to check that the MN knows the K_{IM} corresponding to the claimed previous pseudonym. Let's suppose that the MN is not allowed to get service from home network any more due to some reason. If the current status of the MN in home network is not checked, the MN can send valid Key Update Message forever. Therefore, the current status of the MN in home network should be checked and ITP should keep the list of valid home address. But, we recommend the checking should be done after sending Acknowledgement to avoid time delay for that check. If the home address of the MN is known to be invalid in home network, the home address should be deleted from the list of valid home address and any Key Update Message containing a home address which is not in the list must be silently dropped.

However, there is still a problem. It is that we can't detect false Key Update Message, if valid home address of other nodes is used. In order to detect this, ITP has to keep home address-pseudonym binding information such as {*valid home address*, h(*valid home address* | *the most recent pseudonym bound to the home address*)}. When the MN uses other nods's home address, ITP can detect this attempt because {*other node's home address*, h(*other node's home address* | *his pseudonym*)} would not appear in the *home address-pseudonym binding list.* Therefore, ITP should keep *home address-pseudonym binding list* rather than the list of valid home address.

When ITP verifies Key Update Message using *home address-pseudonym binding list*, Key Update process can go wrong if the Acknowledgement gets lost.

- ITP keeps {*home address*, h(*home address* | *pseudonym #1*)}
- The MN sends Key Update Message = {pseudonym #1, nonce, $\{homeaddress, newCoA\}_{K_{IM}}$, MAC}, the *Interface Id* of new CoA is pseudonym #2
- ITP updates the list, {*home address*, h(*home address* | *pseudonym #2*)}
- Acknowledgement gets lost
- The MN sends Key Update Message again as above
- Verification of Key Update Message fails because {*home address*, h(*home address* | *pseudonym #1*)} is not valid any more

Therefore, ITP must keep both {*home address*, h(*home address* | *pseudonym #1*)} and {*home address*, h(*home address* | *pseudonym #2*)} until it receives Binding Update Message from new CoA. After that, ITP deletes {*home address*, h(*home address* | *pseudonym #1*)} from the list.

5.2 Location Privacy in Home Binding Procedure

Binding Update message must go through ITP to remove or translate information related to the MN identity or current location. We show how the Binding

Update Message and Acknowledgement will look like.

<Binding Update Message>

IPv6 outer header (source = CoA, destination = ITP)
IPv6 inner header (source = ITP, destination = $\{HAaddress\}_{K_{IM}}$)
Destination options header
  Home address option ($\{homeaddress\}_{K_{IM}}$)
ESP header
Mobility header
  Binding Update
    Alternate care-of address option ($\{CoA\}_{K_{IM}}$)

<Binding Acknowledgement>

IPv6 outer header (source = HA address, destination = ITP)
IPv6 inner header (source = ITP, destination = $\{CoA\}_{K_{IM}}$)
Routing header (type2)
  home address
ESP header
Mobility header
  Binding Acknowledgement

Foreign network and attackers can't know the home agent address and home address because they are encrypted with K_{IM}. These are decrypted at ITP, outer header is removed, and remaining part is forwarded to HA. Home network can't know the location of the MN because CoA is encrypted. $\{CoA\}_{K_{IM}}$ in Alternate care-of address option is copied to destination address field of inner header of Biding Acknowledgement. ITP removes outer header of Binding Acknowledgement, decrypts $\{CoA\}_{K_{IM}}$ at inner header, encrypts home address at Routing header with K_{IM}, and forwards it to the MN's CoA.

Now, we are going to see how ITP can generate K_{IM} without any prior information. The source address of Binding Update Message is CoA of which pseudonym is *Interface Id*. ITP can know the MN's pseudonym, so it can generate K_{IM} = h(K_I | MN's pseudonym). The way to know the MN's pseudonym from Binding Acknowledgement is different. CoA should not appear at the header of Binding Acknowledgement, otherwise, home network can know the current location of the MN. So, ITP should find it out from other parts of header. We manipulate ITP address to carry pseudonym

ITP address = { ITP subnet prefix (64 bit) | MN's pseudonym (64 bit)}
We have mainly two benefits from forming ITP address as above:

- ITP subnet prefix is normally much more persistent than a ITP address, so the MN doesn't need to recognize reconfiguration of ITP address and doesn't need to try to find out new ITP address.

- ITP can extract the MN's pseudonym from ITP address and generate K_{IM}

When we use that form of ITP address, messages can be delivered to the network where ITPs reside by referring to just subnet prefix. But, the routers on the network should have the functionality to forward the messages to arbitrary ITPs because exact ITP address is not given.

5.3 Revocation of Location History

This protocol provides revocable location privacy rather than perfect location privacy. In case of serious crime, the location history must be revealed. The location privacy can be revoked this way:

- ITP stores (MN's pseudonym, $\{CoA\}_{K_{IM}}$, time in millisecond)
- The HN stores (home address, $\{CoA\}_{K_{IM}}$, time in millisecond)
- When there is quite enough reason to revoke location privacy, the HN asks ITP to decrypt the encrypted CoA.
- ITP looks up pseudonym by comparing $\{CoA\}_{K_{IM}}$ and time. If the time gap between the times recorded at ITP and the HN is within predefined value, the pseudonym is selected.
- ITP generates key using the pseudonym and decrypts the encrypted CoA

To minimize the time gap between the times recorded at ITP and the HN, it is required that ITP record the time when it receives Binding Update Message rather than Key Update Message. As the location history of the MN can be revealed only when the information at ITP and the HN was combined, keeping the information separately doesn't cause a problem. The clocks at ITP and HNs should be synchronized.

5.4 Discussion

In our protocol, the MN and ITP are not required to perform any public key cryptographic operations while the MN moves around foreign network, and traffic goes through just a single ITP. Only some parts of a packet are encrypted and decrypted, not multiple encryption and decryption of whole packet. Therefore this protocol can be very efficient.

We showed how location privacy can be provided in the Binding Update Procedure. We omitted how it can be provided in Route Optimization because of space constraints, though it would be better if it is seif-contained.

6 Conclusions

We realized an issue that has had little attention in MIP. That is location privacy which has increased significance in wireless network. We employed Centralized Trusted Entity based approach as the way of providing location privacy and it is quite efficient compared to Cascading Overlay Networks based approach. We identified adequate level of location privacy requirements and selected protocol components based on defined threat model.

Our protocol takes the initiative in providing practical solution for location privacy in MIP communication. Previous approach [13] is impractical because it performs multiple public key cryptographic operations and is based on Cascading Overlay Networks. However, this is the first proposal, so it might need to be improved. There are some open issues that need to be considered in the future work's agenda :

- consideration of employing payment schemes for the use of foreign network resource
- providing location privacy in Internet Key Exchange of IPSec
- ITP's secret key update
- ITP's survivability improvement

Acknowledgements
The authors are deeply grateful to the anonymous reviewers for their valuable suggestions and comments on the first version of this paper.

References

1. C. Perkins, "IP Mobility Support", IETF RFC 2002, October 1996
2. D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", IETF Internet-Draft, draft-ietf-mobileip-ipv6-21.txt, February 26, 2003
3. B. Aboba and M. Beadles, "The Network Access Identifier", IETF RFC 2486, January 1999
4. R. Hinden and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", IETF RFC 3513, April 2003
5. T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", IETF RFC 2461, December 1998
6. G. OShea and M. Roe, "Child-proof Authentication for MIPv6 (CAM)", Computer Communication Review, ACM SIGCOMM, volume 31, number 2, April 2001
7. D. Samfat, R. Molva, and N. Asokan, "Untraceability in Mobile Networks", Proceedings of the First Annual International Conference on Mobile Computing and Networking, ACM MOBICOM, November 13-15, 1995, pp. 26-36
8. Anonymizer.com, http://www.anonymizer.com
9. D. Chaum, "Untraceable electronic mail, return address, and digital pseudonyms", Communications of the ACM, Vol.24, No. 2, 1981, pp. 84-88
10. D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash", Crypto, LNCS 0403, 1988, pp. 319-327
11. M. Reiter and A. Rubin, "Crowds: anonymity for web trasactions", ACM Transactions on Information System Security, Vol. 1, No. 1, November 1998, pp. 66-92
12. M. Reed, P. Syverson, and D. Goldschag, "Anonymous connections and Onion Routing", IEEE J. Selected Areas in Commun, Vol. 16, No. 4, May 1998, pp.482-494
13. T. Lopatik, C. Eckert, and U. Baumgarten, "MMIP-Mixed Mobile Internet Protocol", Communications and Multimedia Security (CMS), 1997