Authentication and Payment Protocol Preserving Location Privacy in Mobile IP

SuGil Choi and Kwangjo Kim
International Research Center for Information Security (IRIS)
Information and Communications University (ICU), Korea
E-mail : {sooguri, kkj}@icu.ac.kr

Abstract— **Mobile IP enables a mobile node (MN) to move around without losing their transport-layer connectivity by using resources in a foreign domain network. Mobile IP (MIP) is expected to be the core infrastructure of future mobile communication, but two services must be provided before the wide deployment of MIP. One is to provide secure communication and the other is to make payment. 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 and anonymity services despite of their increased significance in wireless network. Incontestable payment protocol must be also developed, considering the usage of foreign domain network resources by the MN. As mix-network provides basic concept of location privacy protection, this paper proposes an authentication and payment protocol hiding location information, based on mix-network.**

I. Introduction

Mobile IP is a protocol for passing IP datagrams between a 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. The two most important tasks are to provide secure MIP communication and to build incontestable payment protocol.

Throughout the development of Mobile IP, the following security services have been considered useful:

- Data integrity, origin authentication and anti-replay protection of MIP registration and location update message
- Access control of the MN when he uses resource on a visiting network
- 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, i.e. preventing the tracing of mobile user's point of attachment to the network, and identity concealment have gotten little attention. 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 and identity allows unauthorized entities to track down its moving history, which can be a serious violation of privacy.

Fulfilling those security requirements mentioned above is not the only condition for the successful deployment of MIP. Considering the usage of foreign network resources by a MN, it can be easily expected that a foreign network will require the MN to pay for network use. Hence, it is another issue to develop an incontestable payment protocol. The payment protocol must make sure that it doesn't reveal location history of a MN as normal payments reveal the payer (HA) and payee (FA). Otherwise, the HA can know the foreign networks that the MN visited.

While providing location privacy and anonymity, proposed protocol must support revocable privacy rather than perfect privacy. In case of serious crime on communication or dispute on payment, the location history and identity must be revealed.

Among several ideas of providing location privacy, mix-network was first introduced by Chaum in 1981 [1]. So far, some proposals to improve mix-network have been made by Jakobsson [7] and Abe [6], and there have been some applications based on mix-network, such as Onion Routing [5] and Freedom network [4]. Among them, our protocol is based on Chaum's mix-network because others are designed after mix-network, which means this protocol might be applied to others without major changes.

While mix-network can hide the location of communicating entities, the iterated encryption of message with difference public keys can cause serious performance degradation. Therefore, our proposed protocol focuses on how to reduce computational overhead in the MN, still achieving the goal of authentication and payment preserving location privacy.

The organization of this paper is as follows: In Section 2, we explain Mobile IP and mix-network briefly. Section 3 clarifies concerned entities and shows communication flow between the entities. Our proposed protocol and design principles are presented in section 4 and its evaluation is given in section 5. In Section 6, we conclude by mentioning a few directions about the following research.

II. Background

A. 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 MIP, a MN uses 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, a HA and a FA broadcast agent advertisement at regular intervals and a MN gets network configuration information from the advertisement.

B. Mix Network

In general terms, it is a set of servers that serially decrypt and permute lists of incoming encrypted messages. Here, the messages are either encrypted using all the individual public keys of the servers, or using one public-key, where the corresponding secret key is shared by the mix servers.

The protocol implements privacy as long as at least one of the active mix-servers does not reveal what random permutation it applied, and the encryption protocol is probabilistic, so that it is not possible to compute the same encrypted messages that constituted the input given the decrypted messages that constitute the output.

In this paper, we use two terms, mix-encryption and mix-decryption. Mix-encryption represents the serial encryption with the public keys of a set of servers and mix-decryption is the reverse operation of mix-encryption.

III. Problem descriptions

In this section, we define the entities that consist of our model and assumptions on each entity. We also show communication flow to help understanding our proposed protocol which will be described in the next section.

A. Entities and Assumptions

There are seven related entities:

- *Mobile Node* (*MN*) : A MN moves around and requests network use to a FA. It is assumed that a MN has low computational power and wireless communication is more expensive than wired communication. A MN has security association with a HA and identify itself to the HA using Network Access Identifier (NAI). The MN takes the responsibility of authenticating the FA.
- *Home Agent* (*HA*) : A HA represents home network. The HA authenticates the payment request from a MN and performs payment through transaction center. In our model, a HA is a real payer and has an account with banks. A HA has a certificate issued by legal CA. We assume that the HA has no other bad intention towards a MN, except that it tries to collect the moving history of the MN from incoming messages.
- *Foreign Agent* (*FA*) : A FA represents foreign network and provides network resource to a MN. A FA is a payee and has an account with banks (but not necessarily the same banks as that of HA). A FA doesn't have any predefined security associations with a MN. A FA allows a MN to use its network resource only after receiving valid payment signature from transaction center. We assume that the FA has no other bad intention towards a MN, except that it tries to collect the identity information of the MN from incoming messages.
- *Mix-Server* : Several mix-servers compose mix-network and they have public/private key pairs. We assume that mix-servers are controlled by a conglomerate of government organizations and do not cooperate to reveal connection information. We also assume that mix-servers know the public-key of HAs.
- *Transaction Center* (*TC*) : TC processes transfers between accounts of HA and FA. TC includes mix-servers, which are controlled by a conglomerate of banks, to make payment anonymous. We call these mix-servers *TC-mix-servers* to distinguish from the above-mentioned mix-servers. TC-mix-encryption represents the serial encryption with the public keys of a set of *TC-mix-servers*.
- *Certification Authority* (*CA*) : CA issues certificates on all other participants' public keys, and may be controlled by banks or government organizations.
- *Attacker* : Attacker 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.

B. Communication Flow

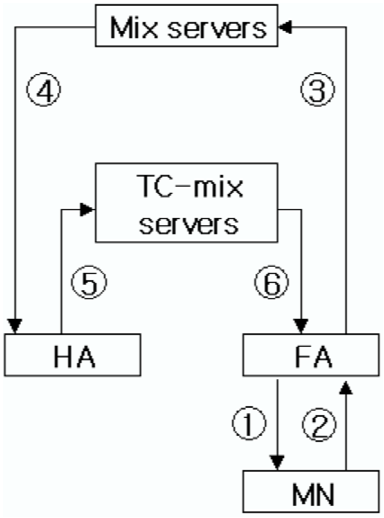

Fig. 1. Communication Flow

After applying design principles, the communication flow will be looking a bit different

IV. Proposed Protocol

This section presents a secure authentication and payment protocol preserving location privacy of a MN. The location privacy is derived solely from the use of mix-network.

We will use the following notations to describe the protocol throughout this section.

TABLE I
NOTATION

Symbol	Description
K_{AB}	Shared key between A and B
PK_A	Public key of A
SK_A	Private key of A
$Cert_A$	Certificate of A
h()	One-way hash function
$prf(k, M)$	keyed hash 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*
$\{M\}_{SK_A}$	Signature of message *M* with a secret key *SK* of A
$(M_1, \ldots, M_r)$	Concatenation of messages $M_1, \ldots, M_r$
ME{M}	Mix-encryption of message *M* with mix-servers' public keys
TCME{M}	Mix-encryption of message *M* with TC-mix-servers' public keys
A $\rightarrow$ B : $[M_1, \ldots, M_r]$	A sends $M_1, M_2, \ldots, M_r$ to B

A. Principles for the design of protocol

We considered the following design priciples:

- Shifting as much computational effort as possible from a MN to the other entities which reside in the wired network, because it is assumed that the MN will be represented by a mobile device which has limited computational power.
- Pre-computing values to reduce processing time if there are some values eligible for that. However, we have to be very careful not to have unexpected vulnerabilities, such as exchanging right value for false one, by including pre-computed value in the protocol.
- Forming messages as short as possible. One way to arrive at shorter messages is the use of a streamlined certificate format which provides certificates much shorter than X.509 certificates. Another way to arrive at shorter messages is to transmit hashed value rather than original value.
- Reducing the time taken until a FA grants a MN to use network resource . In order to achieve this goal, a FA must be convinced, before its account is actually credited, that it will receive money at a later point.
- Reducing the number of transactions between payer's account and transaction center. This is a way of speeding up payment processing. In order to achieve this goal, it is important to decide which one between a HA and a MN is going to pay directly to a FA. A HA represents several MNs, so it might be economical for the HA to pay to the FA and, at a later time, the MN pays to the HA.

B. Protocol Description

Here, we present the protocol that fulfills the goals and takes those design principles into account.

Setup

A FA, a HA, mix-servers, and TC-mix-servers create public/private key pairs. CA issues certificates on these participants' public keys. The public keys of HAs, mix-servers and TC-mix-servers are broadcast beforehand. A FA selects some TC-mix-servers and TC-mix-encrypts its account number (*FAaccnb*). A FA prepares mix-encrypted *FAaccnb* (TCME{*FAaccnb*}) and hashed value of it (h(TCME{*FAaccnb*})).

A MN selects one mix-server, say its ID is *msL*, and encrypts the concatenated value of HA address (*HAaddr*) and fixed-length random value (*flrv*) with the public key of *msL*. A MN encrypts the concatenated value of its NAI and (*flrv*) with the Shared key between a MN and a HA. The MN keeps the value *encHAaddr* = $\{HAaddr, flrv\}_{PK_{msL}}$ and *encNAI* = $\{NAI, flrv\}_{K_{MNHA}}$.

Operation

1) *FA* $\rightarrow$ *MN* : [h(TCME{*FAaccnb*}), *TimeStamp*, $\{h(TCME\{FAaccnb\}), TimeStamp\}_{SK_{FA}}, Cert_{FA}$]

2) *MN Operation* :
- MN verifies the certificate and signature.
- MN creates a *serial number* and temporary ID (*TID*).
- MN creates keyed-MAC value to authenticate itself and payment order to HA. The keyed-MAC value is MAC_1 = *prf*(K_{MNHA}, (*MN's encNAI, TID*, h(TCME{*FAaccnb*}), *serial number, encHAaddr, nonce*)).

3) *MN* $\rightarrow$ *FA* : [*MN's encNAI, TID*, *serial number, encHAaddr, nonce, msL,* MAC_1]

4) *FA Operation* :
- FA stores the TID to match with the response from TC which says the result of payment order processing.
- FA creates untraceable return address (*uraddr*) that enables TC or HA to respond [1].
- FA forms a *payment order*. A *payment order* = (TCME{*FAaccnb*}, *serial number*).
- FA prepares messages M_1 = {*MN's encNAI*, *TID*, *payment order*, *nonce*, MAC_1, *uraddr*, *encHAaddr*}
- FA mix-encrypts M_1 with the public keys of selected mix-servers. But the last mix-server must be *msL* which has the private key to decrypt *encHAaddr*.

5) *FA* $\rightarrow$ *Mix-servers* : [ME{M_1}]

6) *Mix-server Operation* :
- Mix-servers serially decrypt and permute lists of incoming encrypted messages. The output of former mix-server is fed into next mix-server as input.
- Each participating mix-servers store the input for revocation.
- The output from last mix-server is M_1.
- Last mix-server decrypts *encHAaddr* and removes the

fixed-length random value. Now, last mix-server knows the address of HA.
- Last mix-server encrypts M_1 with the public-key of a HA.

7) *Mix-server* $\rightarrow$ *HA* : [$\{M1\}_{PK_{HA}}$]

8) *HA Operation* :
- Encrypted TCME{*FAaccnb*} and *encNAI* are decrypted.
- HA verifies MAC_1 with the shared secret with the claimed NAI.
- If the verification is successful, HA adds its account number (*HAaccnb*) and *timestamp* to *payment order*. So, the *payment order* = (*HAaccnb*, TCME{*FAaccnb*}, *timestamp, serial number*).
- HA signs the *payment order* and stores the message from MN as evidence.

9) *HA* $\rightarrow$ *TC* : [*payment order, MN's TID, uraddr*, $\{paymentorder, TID, uraddr\}_{SK_{HA}}$, $Cert_{HA}$].

10) *TC Operation* :
- TC checks the timestamp in *payment order* and verifires the certificate and signature. If the verification is successful, TC stores the received request as evidence. The account number of a HA is added to an internal list and each account is debited in a given internal. We assume the denomination to be credited is pre-determined.
- TC adds TCME{*FAaccnb*} to an internal list to be performed later.
- TC forms reply message *REP* = {*TID*, h(*TCME*{*FAaccnb*}), *serial number* } and signs it with its private key.

11) *TC* $\rightarrow$ *FA* : [*REP*, $\{REP, timeStamp\}_{SK_{TC}}$, $Cert_{TC}$] These messages go through mix-servers, guided by untraceable return address (*uraddr*) [1].

12) *FA action* :
- FA verifies the signature on *REP* and checks that the *REP* from TC is for valid *TID*, its account number, and a serial number not yet received.
- If the verification is successful, FA stores the message from TC and allows MN to use its network resource. This idea comes from Jakobsson's Mix-based Electronic Payments [8].

13) In a given interval, TC decrypts all the TC-mix-encrypted FA account numbers TCME{*FAaccnb*}s. The result is a list of account numbers. The banks corresponding to the accounts credit these accounts accordingly.

V. Discussion

As long as there is no dishonest quorum of mix-servers, location privacy of a MN, HA anonymity, and FA anonymity are guaranteed. But, if a HA is corrupted, the impersonation safety can't be guaranteed. A HA can create valid payment order, because the payment request from a MN is protected by shared secret with the HA. But we don't consider this attack, as we assumed that a HA has no other bad intention towards a MN, except that it tries to collect the moving history of the MN from incoming messages.

The following two types of tracing can be performed:

1) mix-encrypted message $\rightarrow$ plaintext message:
The trace is performed simply by decrypting the encrypted message, arriving at the plaintext message.
2) plaintext message $\rightarrow$ mix-encrypted message:
The given plaintext message is encrypted with the public key of last mix-sever and the result is compared with the stored inputs. When a match is found, we can know which mix-server can apply next encryption. By iterating this procedure, we can arrive at the mix-encrypted message.

A MN performs one signature verification and one keyed-MAC creation operation. Much of the computation is performed by other entities. Otherwise, a MN has to perform several public-key encryptions for mix-encryption.

A FA prepares mix-encrypted account number (TCME{*FAaccnb*}) and hashed value (h(TCME{*FAaccnb*})) before communication starts. A MN prepares encrypted HA address (*encHAaddr*). With these pre-computations, the time taken for public-key encryptions can be saved. But, we have to be very careful when using these pre-computed values, as following attacks are possible. TCME{*FAaccnb*} must be encrypted at the last mix-server. Otherwise, an attacker can find TCME{*FAaccnb*} in the message between the last mix-server and the HA. An attacker can compute hashed value (h(TCME{*FAaccnb*})) from the found TCME{*FAaccnb*}, and can know approximate location of MNs that belong to the HA, by searching h(TCME{*FAaccnb*}) in FA advertisements. Fixed-length random value (*flrv*) must be concatenated to HA address before it is encrypted. Otherwise, an attacker can make the table which stores pairs of {known HA addresses, HA addresses encrypted with known mix-servers' public-keys (*encHAaddrs*)}. An attacker can find MNs that belong to the HA, by searching matching *encHAaddr* in the communications between FAs and MNs. By encrypting with *flrv*, this attack can be prevented.

h(TCME{*FAaccnb*}) is used to form messages instead of TCME{*FAaccnb*}. This approach can shorten the messages. Fourth and fifth principles are fully incorporated into our protocol. In our protocol, NAI is encrypted and *encNAI* looks different on each movement by including *flrv*. Therefore, attackers can't know the identity of a MN and encNAI correlation attack can be defeated.

As a FA mix-encrypts M_1, it can be thought that the FA can correlate input and output at each mix-server. But, as last

mix-server encrypts M_1 with the public-key of a HA, a FA can't find the final destination of the M_1.

However, this protocol requires stronger computational power and trust at the mix-server which was selected as the last mix-server. The mix-server has to perform one more decryption and encryption than other mix-servers. We have to assume that the private key of this mix-server is kept more securely than that of other mix-servers.

In this protocol, inputs are decrypted at a given interval, so the goal of real time communication can't be achieved. If mix-servers decrypt input immediately, the processing speed can be improved, but traffic correlation attack can be mounted. In order to defeat traffic correlation attack while enhancing efficiency, original mix-network needs to be amended. Mix-servers are grouped into several groups of g members and every message forwarded to a member of a group is also sent to each of the remaining entities in the group. If there are no messages pending for a group member, a decoy message is generated instead. Therefore, after a message has passed the first grouping mix server, an attacker correlating incoming and outgoing traffic would have to verify g potential recipients; after the second mix-server g^2. [9]

There is one preceding research [9] that employs mix-network to hide location information in MIP. But the protocol imposes too much computational overhead onto MN, because MN has to mix-encrypt request messages. Our protocol shifted much of the expensive computation to other participants. The protocol [9] and other applications based on mix-network, such as Onion Routing [5] or Freedom network [4], do not consider payment. We incorporated incontestable payment into the protocol, still keeping MN's identity and location secret. Therefore, we propose the first authentication and payment protocol which preserves location privacy in Mobile IP.

VI. Conclusion

We realized two issues that have been given little attention in MIP. One is location privacy and the other is payment. We used mix-network as the way of providing location privacy and incorporated incontestable payment into the protocol. Our protocol design was guided by six principles to make it more efficient and secure.

Our protocol takes the initiative in designing authentication and payment protocol which doesn't reveal a MN's identity and location. 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 :

- lowering required amount of operation and trust for each mix-server
- consideration of employing other payment protocols besides an account-based payment protocol [8]

References

[1] D. Chaum, "Untraceable electronic mail, return address, and digital pseudonyms", Communications of the ACM, Vol.24, No. 2, 1981, pp. 84-88

[2] D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash", Crypto, LNCS 0403, 1988, pp. 319-327

[3] C. Perkins, "IP Mobility Support", IETF RFC 2002, October 1996

[4] Freedom.net, http://www.freedom.net

[5] 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

[6] M. Abe, "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-centers", Eurocrypt, LNCS 1403, 1998

[7] M. Jakobsson, "A Practical Mix", Eurocrypt, LNCS 1403, 1998

[8] M. Jakobsson, "Mix-Based Electronic Payments", Selected Areas in Cryptography, LNCS 1556, 1998

[9] T. Lopatik, C. Eckert, and U. Baumgarten, "MMIP-Mixed Mobile Internet Protocol", Communications and Multimedia Security (CMS), 1997

[10] G. Horn and B. Preneel, "Authentication and Payment in the Future Mobile Systems", European Symposium on Research in Computer Security, LNCS 1485, 1998

[11] A. Escudero, "Anonymous and Untraceable Communications: Location Privacy in Mobile Internetworking", Licentiate Thesis, 2001

[12] Ian Avrum Goldberg, "A Pseudonymous Communications Infrastructure for the Internet", University of California at Berkely Thesis, 2000