Mobile Terminated Protocol to Remote Domain Considering User Location Untraceability Service

Soon-Seok Kim, *Member, KIMICS*

Abstract—In previous papers [1] and [2], we proposed two improved methods protecting mobile users from active attacks[3,4] of network providers in mobile communication environment. But they were the case that mobile users were located in only home domain. In [5], we proposed protocol extending the method of [1] in case of roaming from the home domain to the remote domain. The purpose of this paper is to propose new mobile terminated protocol extending the method of [2] and analyze its security.

Index Terms—Location Privacy, Mobile Communication, Protocol, Anonymity, Domain.

I. INTRODUCTION

The purpose of this research is to develop new system for the protection of privacy on mobile users' identity and location in next generation mobile communication environment. In particular, this paper intends to put focus on the call configuration of mobile user in an integrated system when the user moves from home domain(for instance, Seoul of Korea) to another domain in a remote place(for instance, Rome of Italy). Here, the subject of privacy protection is the mobile user, the entity to be protected from a third party that attempts illegal wiretapping in mobile communication environment, mobile communication business(ie, network provider), and the association of these two entities. According to the researches so far, in the case of GSM[6] system, the existing European standard, when user moves to another domain, in reality the user privacy is protected from wiretapping attempts by outside 3rd party, but not from those by the network provider, someone inside the system, and the situation is pretty much the same with IMT-2000, a next generation mobile communication system.

On the other hand, regarding this research, Kesdogan[3,4], et al. once proposed method that all satisfies the restrictions suggested by the 3rd party and network provider previously mentioned in this paper. However, the suggested issue has the assumption that the user is located within home domain, and at the same time, we have already presented in the papers [1] and [2] the problems and the solutions Kesdogan et al suggested.

Therefore, this paper intends to propose a new mobile terminated protocol that covers up to the scope when the mobile user moves to remote domain located in an another place based on the already presented paper [2]. We hope that the protocol extending the method of [1] is refer to the previous paper [5].

II. BASIC SYSTEM ARCHITECTURE

The basic architecture of the system proposed in this paper is as the Figure 1 below, and the anonymity server proposed here has the assumption that it remains within the domain either when the mobile user is located within home domain or when the user roams to remote domain, marking the former HAS(Home Domain Anonymity Server) and the latter RAS(Remote Domain Anonymity Server). However, the communication can be done also directly through wireless network by connecting to the laptop computer on the user's side - not passing through network provider. In this case, though bypassing the network provider brings some advantages on security, it causes inconvenience to the user, while various communications occurring on the network provider or the connectivity, etc from outside users to the network provider are the same as the existing GSM system. On the other hand, this serves also as a strong point. For the proposed system is provided as an additional system while still using the existing GSM environment - not modifying the architecture, the mechanism applies to the actual system easily.

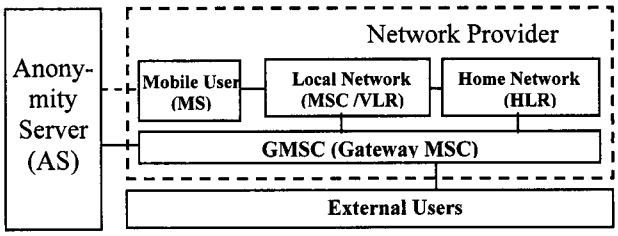

Fig. 1 Basic Architecture of the Proposed System

III. BASIC HYPOTHESIS

This protocol refers to the configuration protocol for the call request from outside user in case the mobile user moves from home domain to remote domain, and at the

Manuscript received June 9, 2007.

Soon-Seok Kim is with the Department of Computer Engineering, Halla University, Wonju, Kangwon, 220-712, Korea (Tel: +82-33-760-1289, Fax: +82-33-760-1314, Email: sskim@halla.ac.kr)

same time requires several assumptions as below prior to the description of this protocol.

First, no one knows the current location of the mobile user except HAS and RAS. Therefore, in case outside user wants to talk with the user, even though the user is currently located in remote domain, this communication request is assumed that the communication business on the home domain side, ie, network provider takes the request and connects to the user.

Second, this protocol, basically, is an expansion of mobile terminated protocol where the user is located in home domain as we proposed in the paper [2]. Therefore, this protocol applies when the user moves from home domain to remote domain.

Third, it is assumed that in principle the network provider(hereinafter "HNP") within home domain and the network provider(hereinafter "RNP") in remote domain provide call connection service for normal call requests from outside user. However, it is possible that HNP or RNP may attempt to find out PMSI(Pseudo Mobile Subscribed Identity)[3,4], the current ID of MS illegally in order to spot or track the user location regardless of such call connection service.

On the other hand, in case mobile user moves from home domain to remote domain, as mentioned in the above first assumption, the gateway mobile switching center(referred to as "GMSC") on HNP side receives the call request by outside user. In this course, if HAS informs on PMSI and the user's temporary anonymous ID, and lets HNP connect the call to the user via RNP, HNP may easily learn at least the domain to which the user moved and the RNP by which the user is currently controlled. This is an exposure of privacy on the user's location, which undermines the satisfaction for high level privacy protection service. Therefore, to keep up with this level of privacy protection, the connection between HNP and RNP need be cut off.

IV. PROTOCOL PROPOSITION

The underlying idea of the proposed mobile terminated protocol is as follows(refer to Figure 2). When call is requested by external user, the GMSC on HNP will receive this request and inquire the HAS of the current PMSI. At this time, HAS does not inform GMSC on the current PMSI of the user but instead receives the information the outside user sent on request, *IAM* and *MSISDN*[6] and send this request to RAS along with the current PMSI so that RAS may let the GMSC on RNP side configure connection to MS. In other words, 1) when an external user requests a call to the GMSC of HNP side to talk with MS, 2) the GMSC takes this request and then requests HAS the current PMSI of MS. At this time, since HAS is aware that MS is not present within the current domain by executing the location update protocol[5] when MS moved to the remote domain beforehand, 3) HAS notifies the GMSC the fact that the user that sent {*no PMSI message*} is not within the current domain. After that, 4) HAS sends RAS the current PMSI along with its own ID, and the RAS that received this message again sends the GMSC of RNP side the PMSI. Lastly, 6) the GMSC of RNP side, using this message, configures the call connection to MS. At this time, since MS already registered its own current PMSI at RNP by executing location update protocol[5] when MS moved to remote domain beforehand, call connection is already made ready.

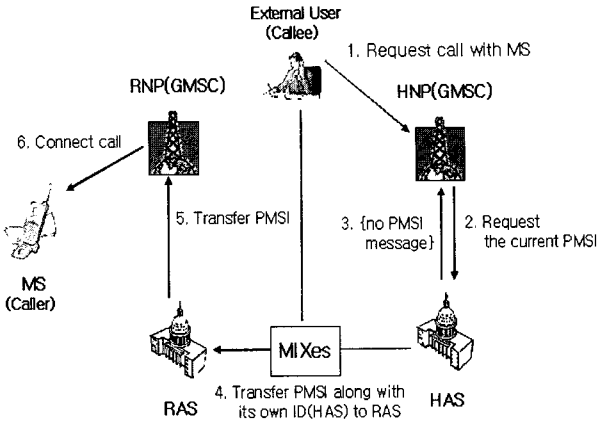

Fig. 2 Basic Scenario of the Proposed Protocol

The following protocol is as follows(refer to [Figure 3]).

[Step 1] The stage an External User Requests a Call

The sender, the external user transfers the GMSC within HNP *IAM* and *MSISDN* message to talk with MS.

[Step 2] The Stage the GMSC Requests the Current PMSI

(1) HNP(GMSC) requests current PMSI by sending HAS *MSISDN* to find out the PMSI by *MSISDN*.

(2) HAS confirms that MS is located within the remote domain, and sends HNP(GMSC) the corresponding message {*no PMSI message*} for it.

(3) After generating an arbitrary integer, r, HAS connects its own ID *HAS* and the current *PMSI* of MS, encode them by the public key P_{RAS} of RAS, and transfers to RAS.

(4) First off by using its own secret key U_{RAS}, RAS deciphers the encoded message, and after removing the arbitrary integer r and *HAS*, transfers to RNP(GMSC) the received *PMSI*.[1]

[Step 3] The Stage to Configure Connection with MS

RNP(GMSC) configures connection with the sender by transferring MS {*call setup message*}.[2]

If MS moved to another home domain after staying in the remote domain, the mobile terminated protocol[2]

[1] In some cases, the PMSI that RAS received from HAS in this process may not exist within its own database table. This is the case where the applicable PMSI value was already renewed to a new value on the RAS side while the message transferred via MIXes or the value was not renewed at all. Therefore, the issue on RAS side may be solved by storing the previous PMSI along with the renewed PMSI.

[2] In some case, when connecting from GMSC to MS, the PMSI that RAS informed of may not exist in HLR which is its own internal database and in VLR. That is because MS renewed to a new PMSI or no renewal is done yet while connecting GMSC to MS. Therefore, in such case, GMSC may attempt to connect to MS by requesting HAS the current PMSI again and then using the renewed PMSI. At this time, RAS informs of other PMSI generated before or after that by reviewing the synchronizing time based on the PMSI it already informed of.

where MS is located within home domain is directly applied. In other words, the secret information S is used again.

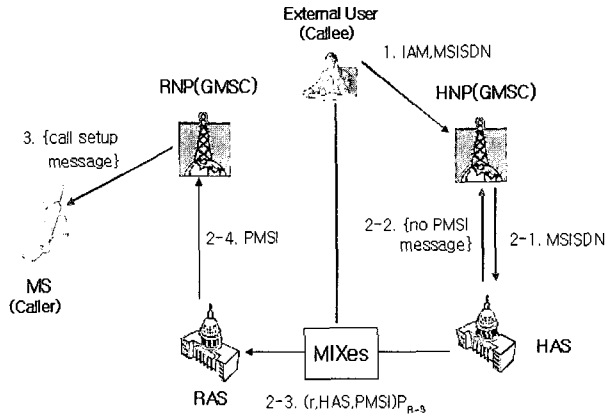

Fig. 3 The Proposed Mobile Terminated Protocol

A. Analysis of the Proposed Protocol

The proposed protocol, a mobile terminated protocol in a remote domain, is an area that has never been proposed about by other researchers. Moreover, in the cases of GSM or IMT-2000 which are currently in use, such global roaming service is not available. Therefore, this section intends to analyze protocol with emphasis on safety rather than efficiency.

This protocol fundamentally is an expanded version of mobile terminated protocol when MS is located within home domain. However, unlike the existing ones, it does not generate the secret information S. The past secret information S intended to let MS confirm whether there is any actual request by outside user by generating HAS when PMSI is requested by HNP and then sending the HAS to MS. If no request is placed in this process, it may be determined that HNP illegally attempted for the PMSI. However, this protocol basically adopts the policy not to release PMSI to HNP by sending *{no PMSI message}* as in the above [Step 2]. In other words, it means it is not necessary to generate secret information S and check it out because HNP is not to be informed of PMSI.

Now then, let's have a look through various attacks that may occur on HNP side by the types.

[Case 1] Though HAS does not inform HNP of PMSI, it may attack to monitor by requesting PMSI and observing the traffic from HAS later on to see which way the traffic flows to.

In this protocol, since message fundamentally passes through MIXes when it is transferred from HAS to RAS as seen in the above Figure 3, any third party like HNP do not know which way the message being transferred from HAS is headed for. For details on MIXes, see paper [7,8]. However, it has a shortcoming that in case of such illegal PMSI request, the connection remains normal until connection to MS is established and MS confirms it. In addition, since the call may be immediately terminated even if MS confirms it, it is hard to find out in practice. There was similar case in the protocol of the previous paper [2], and in such case, the following method can be considered as alternative. In detail, when such case occurs on MS side, count the number of such cases, and if the number exceeds certain frequency(for instance, three times per week), raise objection to HNP by informing to HAS.

[Case 2] In another case, let's suppose that there is a PMSI HNP knew just before MS stayed in home domain and moved to remote domain. At this time, HNP may attempt to find out which remote domain PMSI is currently staying.

In this case, just as mentioned in the location update protocol proposed in the previous paper [2], because MS does not register the previous PMSI as it is but register the renewed PMSI when registering its own PMSI to RNP after moving to remote domain, HNP may not recognize the PMSI value though HNP observes.

Additionally, the types below may also be considered.

[Case 3] When a third party except HNP intends to track the location

This case is merely about PMSI as seen in the above Figure 3. However, even though a third party is aware of PMSI, the PMSI is not the actual user ID, and it changes every time in each regular period, so location tracking is impossible. Besides, the amount of information a third party can find out is not much compared to the HNP, an internal user, and if ever, the possibility of illegal attempt beyond what HNP can attempt right now is negligible.

[Case 4] Possibility of illegal attempt from RNP

Basically RNP does not request RAS of PMSI, but instead the connection service is provided by the RAS's request. Such service was assumed to be basically provided as mentioned at the start of Chapter 3. Of course, PMSI can be requested to HAS periodically due to call connection failure such as busy line, confusion, line termination, etc. For solutions on such issues, see the protocol safety analysis part that we previously proposed in paper [2].

V. CONCLUSIONS

The objective of this paper is to propose new mobile terminated protocol that provide users with high level of privacy service while the mobile user moves from home domain to remote domain in an another place. This protocol is an expanded version of protocol that we proposed in paper [2], expanding domain to another domain. Although, this protocol is only a part of an integrated system, the protocol may be seen as valuable outcome in that it provides privacy protection service for high level mobile user that the existing GSM or IMT-2000 system could not provide with.

ACKNOWLEDGMENT

This work was supported by grant No. R01-2005-000-10568-0 from the Basic Research Program of the Korea Science & Engineering Foundation.

REFERENCES

[1] S. S. Kim, S. S. Yeo, H. J. Park, and S. K. Kim, "A New Scheme for the Location Information Protection in Mobile Communication Environments," Proc. of the MMM-ACNS 2005: 3th International Workshop on Mathmatical Methods, Models, and Architectures for Computer Network Security, LNCS, Vol. 3685, pp. 436-441, 2005.

[2] S. S. Kim and S. K. Kim, "A Study on Location Untraceability Service and Payment Protocol Using Temporary Pseudonym in Mobile Communication Environments," Journal of Korea Information Science Society(KISS):System & Theory, Vol. 30, No. 2, pp 78-92, 2003.

[3] D. Kesdogan, H. Federrath, A. Jericow, and A. Pfizmann, "Location Management Strategies increasing Privacy in Mobile Communication Systems," Proc. of the 12th IFIP International Conference on Informatin Security(IFIP/SEC'96), 1996.

[4] D. Kesdogan, P. Reichl, and K. Junghärtchen, "Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks," ESOROCS '98, LNCS vol. 1485, pp. 295-312, 1998.

[5] S. S. Kim, "New Mobile Terminated Protocol for User Privacy Protection in Mobile Communication Environments," Journal of the Korean Institute of Maritime Information & Communication Sciences(KIMICS), Vol. 10, No. 12, pp 2193-2201, 2006.

[6] ETSI, "GSM Recommendations: GSM 01.02-12.21," Feb. 1993, Release 1992.

[7] A. Pfitzmann, B. Pfitzmann, and M. Waidner, "ISDN-MIXes Untraceable Communication with Very Small Bandwidth Overhead," Proc. of the 7th IFIP International Conference on Informatin Security(IFIP/SEC'91), 1991.

[8] H. Federrath, A. Jericow, and A. Pfitzmann, "MIXes in Mobile Communication Systems: Location Management with Privacy," Proc. of the Workshop on Information Hiding, 1997.

Soon Seok Kim

Member KIMICS Received B. S. degree in Computer Engineering, Chinju National University, Korea, in 1997. M. S. and Ph. D. Degree in Computer Engineering, Chung-Ang University, Korea, 1999 and 2003. Since 2003, he has been Assistant Professor, Department of Computer Engineering, Halla University, Wonju, Korea. The areas of interest are information security, cryptography application, biometric authentication.