이동통신 환경에서 프라이버시 보호를 위한 새로운 이동발호 프로토콜

김 순 석*

New Mobile Originated Protocol for Privacy Protection in Mobile Communication Environments

Soon-seok Kim*

요 약

본 논문은 차세대 이동통신 환경에서 이동 사용자에 대한 위치와 신분 프라이버시를 만족하기 위해 개발 중인 새로운 통합시스템의 일부로, 종전 유럽의 GSM[1] 시스템에서 제공되지 못한 고수준의 프라이버시를 만족하는 새로운 이동발호프로토콜을 제안하고 분석한 것이다. 아울러 제안하는 프로토콜은 이동 사용자가 홈 도메인에서만 머무르는 것이 아니라 원격지 도메인으로 이동하는 경우를 포함한다.

ABSTRACT

We have studied to protect location and identity privacy of mobile users in mobile communication environments. In this paper, we propose and analyze new mobile originated protocols as a part of our new integrated system for high level privacy protection service which is not provided in the traditional GSM[1] system of europe. Also our protocols support a roaming service into the remote domain as well as the home domain.

키워드

Mobile Communication, Privacy, Anonymity, Protocol

Ⅰ. 서 론

본 연구의 목적은 차세대 이동통신환경에서 이동 사용자에 대한 신분과 위치에 대한 프라이버시를 보호하기위한 새로운 시스템을 개발하는데 있다. 특히, 본 논문은 이러한 통합 시스템 가운데 이동 사용자의 발호 설정에 대한 부분을 중점적으로 다루고자 한다. 여기서 프라이버시의 보호 대상은 이동 사용자이며 그 범위는 이동환경에서 불법적인 도청을 시도하려는 제3자, 이동통신 사업자(즉, 네트워크 제공자), 그리고 이들 두 객체간의 결탁으로 한정한다.

현재까지 연구된 바에 따르면, 기존의 유럽 표준인 GSM[1] 시스템의 경우 외부 제 3자로부터의 도청시도에 대해서는 이를 보호하고 있으나 시스템의 내부 이용자인 네트워크 제공자로부터 이동 사용자의 프라이버시는 보호되고 있지 못한 실정이며, 이러한 사항은 차세대 이동통신 시스템인 IMT-2000 또한 동일하다.

본 연구와 관련하여 Kesdogan[2,3]등은 앞서 제기한

* 한라대학교 컴퓨터공학과

접수일자 : 2007. 7. 26

제 3자와 네트워크 제공자로부터 이동 사용자의 신분과 위치 프라이버시를 만족하는 새로운 방법을 제안한 바 있다. 그러나 이 방법은 이동 사용자의 착호 설정과 관련한 제안이며 특히, 네트워크 제공자나 제 3자로부터의 능동적인 공격에 대해서는 이미 취약점을 드러낸 바가 있다. 본 저자는 이미 논문 [4,5]에서 이러한 취약점을 개선한 새로운 논문을 제안한 바 있다.

따라서 본 논문에서는 기존 Kesdogan[2,3]등이 제안한 임시익명아이디를 이용한 방법을 개선하고 이미 본 저자가 제안한 바 있는 논문 [4,5]의 방법을 보다 확장한 새로운 이동 발호 프로토콜을 제안하고자 한다. 또한 제안하는 방법은 이동 사용자에 대한 프라이버시 보호는 물론이고, IMT-2000시스템에서 제공하고 있는 사용자와 네트워크 제공자와의 상호인증 서비스를 지원하고 있다.

본 논문에서 제안하는 이동 발호 설정 프로토콜의 범위는 첫째, 이동사용자가 홈 도메인 내에 위치해 있는 경우와 둘째, 이동사용자가 홈 도메인 내에 위치해 있다가 타 도메인인 원격지(예를 들어, 서울에서 중국 북경으로의 위치 이동 등) 도메인으로 위치를 이동할 경우 모두를 다루고 있다.

끝으로 제안하는 방법은 기존에 본 저자가 발표한 이동 착호 설정 및 위치 갱신 프로토콜 논문들[4,5]과 통합하여 차세대 이동통신 환경에 적합한 새로운 시스템으로 완성될 수 있다.

본 논문의 구성은 다음과 같다. 먼저 2장에서 이동 사용자가 홈 도메인 내에 위치할 경우의 위치 갱신과 새로운 이동 발호 프로토콜을 제안하고 분석한 후, 3장에서 이동 사용자가 홈 도메인 내에 위치해 있다가 타 도메인으로 위치를 이동할 경우에 대한 프로토콜을 제안한 다음, 4장을 끝으로 결론을 맺고자 한다.

Ⅱ. 새로운 이동발호 프로토콜 제안
- 이동 사용자가 홈 도메인 내에 위치할 경우

먼저 제안하는 프로토콜들에서 사용되는 각종 표기들은 다음과 같다.

[표기]

- *MS* : 단말기 내에 SIM(Subscriber Identity Module)과 ME(Mobile Equipment)가 부착된 모바일 사용자의 아이디.
- *HAS* : 홈 도메인 익명 서버의 아이디.
- *HNP* : 홈 네트워크 제공자의 아이디.
- K_{MH} : *MS*와 *HAS*간의 장기 공유 비밀키(long term secret key).
- *TS* : 각 개체가 서명한 타임스탬프(timestamp), 주로 메시지를 보낼 당시의 시간 정보를 서명한 값이다.
- K_{MH}' : *MS*와 *HAS*간의 단기 공유 비밀키(short term secret key), f를 암호학적인 일방향(one-way) 함수라 할 때, $K_{MH}'=f(K_{MH},TS)$이며 이 값은 실제 시스템 적용시 요구되는 보안성의 레벨에 따라 짧게는 일주일에서 길게는 한달 단위로 갱신될 수 있다.
- K_{MN} : *MS*와 *HNP*간의 세션키(session key).
- g : 유한군(finite group)에서의 생성자.
- h, g^h : 세션키 생성을 위한 *HNP*의 diffie-hellman 개인키(private key)와 공개키(public key) 쌍.
- K_{MS}^{-1}, K_{MS} : *HAS*가 임시로 생성한 *MS*의 서명키와 검증키.
- K_{HAS}^{-1} : *HAS*의 서명키.
- U_{HAS}, P_{HAS} : *HAS*의 개인키와 공개키쌍
- $Cert_{HAS}$: 무선 공개키기반구조(PKI, Public Key Infrastructure)에서 *HAS*의 상위 인증기관(CA, Certificate Authority)이 각각 서명한 인증서(certificate), 이때 편의상 *HAS*의 상위 인증기관은 동일한 것으로 가정한다.
- t : *MS*와 *HAS*가 임시익명아이디인 *PMSI** 를 생성하기 위해 사전에 합의한 동기화 시간으로 이 값은 초 단위

* Pfitzmann과 Kesdogan 등[2]이 제안한 것으로, 모바일 사용자의 실제 아이디 대신 PMSI(Pseudo Mobile Subscriber Identity)라는 임시 익명 아이디를 이용하여 통신함으로써 사용자의 신분에 대한 프라이버시를 보호하고자 한 개념이다. 즉, 네트워크 제공자를 비롯한 제 3자로부터 실제 아이디에 대한 노출을 피하기 위해 각 가정이나 그밖에 안전한 장소의 컴퓨터 내에 실제 아이디와 이에 대응되는 PMSI를 저장해 둠으로써 사용자에 대한 위치 프라이버시를 추가로 제공하는 메커니즘이다. 따라서 네트워크 제공자의 경우 모바일 사용자에 대한 PMSI는 알지만 실제 아이디가 무엇인지를 모르기 때문에 사용자의 신분을 알 수가 없다. 또한 PMSI 값은 주기적으로 변화되어 HLR과 VLR에 등록되기 때문에 네트워크 제공자 측에서 PMSI를 이용한 위치 추적이 어렵다. 이에 반해 GSM의 경우 사용자에 대한 익명성을 위해 TMSI(Temporary Mobile Subscriber Identity)라는 임시 아이디를 이용하고 있다. 그러나 이 TMSI 또한 내부 이용자인 네트워크 제공자 측에서는 실제 모바일 사용자가 누구인지를 알고 있기 때문에 네트워크 제공자에 대한 위치 프라이버시는 여전히 제공되질 않는다.

로 계산한다.

- *cur_t* : *MS*가 메시지를 보낼 당시의 시간으로, 만일 공개키기반구조 하의 환경일 경우 이 값은 *MS*가 서명한 타임스탬프가 될 수도 있다.
- *H* : 암호학적인 충돌회피 일방향 해쉬함수 (cryptographic collision-free one-way hash function).
- r, r_1, r_2, r_3 : 각 개체가 생성하는 임의의 정수로 생성시마다 다른 값을 갖는다.
- *PRG code* : 암호학적 의사난수발생기인 *PRG*(Pseudo Random Generator) 알고리즘의 종류를 나타내는 고유번호.
- $\{m\}K$: 메시지 m을 키 K로 암호화.

2.1 이동 사용자가 홈 도메인 내에 위치할 경우의 위치 갱신 프로토콜

본 프로토콜은 모바일 사용자인 MS가 홈 도메인 내에 위치해 있을 경우에 자신의 위치 즉, *PMSI* 정보를 홈 네트워크 제공자인 HNP 측의 위치 관련 데이터베이스인 HLR(Home Location Register)과 VLR(Visited Location Register)들에 등록하고 또 매 동기화 시간 t_i마다 갱신하는 과정을 말한다([그림 1] 참조).

[그림 1]에서 *PMSI* 생성은 MS와 홈 익명서버인 HAS가 서로 동기화된 시간 t_i에 각기 독립적으로 계산되며, 또 주기적으로 갱신된다. 여기서 말하는 시간은 그 단위가 초가 되며, 주기는 실제 시스템 적용 시 보안성의 정도에 따라 달라질 수 있는데, 예를 들어 1분, 10분, 30분, 1시간 등이 가능하다. 이때 주기는 그 길이가 짧으면 짧을수록 보안 비도는 높아지지만, 반면에 MS와 HAS측에서 그 만큼 많은 오버헤드가 발생할 수 있다. 따라서 이 주기에 대한 결정은 실제 적용하는 시스템의 성능에 따라 필요한 값을 선택해야 한다. 또한 이 *PMSI* 값은 실제 MS가 HNP 측에 등록하는 값이기도 하다.

여기서 *PMSI*는 $PRG(K_{MH}', t_i)$로 계산되며, 이 값은 MS와 HAS간의 단기 공유 비밀키인 K_{MH}'과 동기화 시간 t_i를 초기값으로 하여 의사난수발생기인 *PRG*로 계산한 값이다. 이때 중요한 점은 MS와 HAS간에 시간을 맞춰 동시에 *PMSI*가 갱신되어야 한다는 것이다. 대개 MS 측의 이동 단말기 내에 설정되는 시간 값은 GSM 시스템의 경우, 각 베이스 트랜시버 스테이션으로부터 방출하는 표준 시간 정보를 송신 받아 이 값을 현재 시간으로 사용하고 있으며, IMT-2000의 경우는 GPS(Global Positioning System)에서 방출하는 표준 시각을 스캔하여 이 값을 현재 시간으로 이용하고 있어, 이 과정에서 약간의 전송 지연이 발생할 수 있다. 물론 본 시스템에서 생성하는 *PMSI* 정보는 서로 간에 정해진 동기화 시간에 그 값이 생성되므로 HAS와 MS가 서로 동일한 결과 값을 갖지만, 이러한 지연으로 인해 발생하는 시간에 약간의 차이를 보일 수 있다는 것이다. 때로는 이러한 시간 차이가 MS의 위치 갱신이나 등록에는 문제가 없지만, 외부 이용자로부터 MS에 대한 착호 설정시, MS와 HAS간에 서로 다른 *PMSI* 정보로 인해 오류를 범할 수도 있다. 예를 들어, 지연으로 인해 MS측에서 *PMSI*에 대한 갱신 및 위치 등록이 HAS가 갱신한 *PMSI*보다 느린 경우와 그 반대 경우가 있을 수 있다. 이러한 문제에 대해 본 논문에서는 해결 방안으로 호 설정을 위해 HNP가 HAS에게 현 *PMSI*를 요청 시 자신이 알고 있는 값을 알려준 후에, 만일 잘못될 경우 갱신된 값을 재차 알려주는 방법을 이용하였다. 만일 MS측의 갱신이 느린 경우라면 이전의 *PMSI*를 재차 알려주고 그렇지 않은 경우라면 갱신된 *PMSI*를 재차 알려줌으로써 호 설정동안 동일한 *PMSI*값이 이용될 수 있도록 한 것이다. 보다 자세한 설명은 이전에 제안한 이동 착호 프로토콜에 관한 논문들[4,5]을 참조하기 바란다.

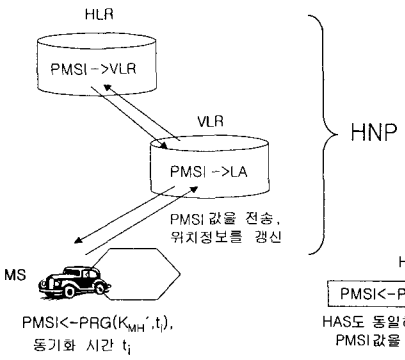

그림 1. 홈 도메인에서의 위치 갱신 프로토콜
Fig. 1 Location Update Protocol in Home Domain

2.2 이동 사용자가 홈 도메인 내에 위치할 경우의 이동 발호 프로토콜

본 프로토콜은 이동 사용자가 외부 이용자와의 통화를 위해 네트워크 제공자에게 통화를 요청하고 이를 네트워크 제공자가 외부 이용자에게 연결하는 과정을 말

한다. 이 경우 네트워크 제공자는 사용자가 요청한 통화에 대한 서비스를 제공함으로써 과금을 하게 되며, 이 과정에서 현 사용자가 합법적인 사용자인지를 확인하는 상호 인증을 거친다. 만일 이 인증과정이 원활하게 진행될 경우, 마지막으로 네트워크 제공자는 사용자와 외부 이용자와의 통화를 연결한다. 여기서 중요한 점은 사용자가 외부 이용자와의 통화 요청 시, 사용자와 네트워크 제공자 사이의 인증 과정에서 익명서버는 네트워크 제공자를 비롯한 기타 제3자들에게 사용자의 신분을 노출시키지 않으면서 원활한 상호인증을 위해 필요한 정보들을 사용자에게 제공해야 한다.

사용자가 외부 이용자인 수신자와의 통화를 위해서는 우선 네트워크 제공자와의 인증 및 이에 수반된 세션키를 설정하는 과정이 필요하다. 그 이후에 주고받는 통화 내용들은 설정된 이 세션키를 이용하여 암호화가 이루어진다. 이때 사용자의 신분을 노출시키지 않으면서 네트워크 제공자와 인증을 해야 하기 때문에, 사용자의 신분에 대한 증명을 사용자 측 익명 서버가 대신해 주는 것이 본 방법의 기본 아이디어이다.

제안하는 프로토콜은 다음과 같다([그림 2] 참조).

[단계 1] 초기화 단계

(1) 사용자는 먼저 임의의 정수 r_1을 생성한 다음, 메시지 $\{PMSI, (PMSI, cur_t, g^{r_1})K_{MH}'\}$을 익명서버의 공개키 P_{HAS}로 암호화하여 익명서버에게 보낸다.

(2) 메시지를 전달받은 익명서버는 먼저 자신의 개인키 U_{HAS}와 사용자와의 단기 공유 비밀키 K_{MH}'을 이용하여 암호문들을 복호화한 다음, 전달받은 $PMSI$와 자신이 복호화한 $PMSI$가 같은지를 확인한다. 이때 사용자가 메시지를 보낼 당시의 $PMSI$와 자신이 메시지를 받은 직후에 $PMSI$가 다를 수 있기 때문에 보낼 당시의 시간 cur_t를 아울러 확인한다. 이후 메시지 $\{g^{r_1}, Cert_{HAS}, K_{MS}^{-1}, (g^{r_1}, K_{MS})K_{HAS}^{-1}\}$을 키 K_{MH}'으로 암호화한 다음, 사용자에게 전송한다.

[단계 2] 인증 단계

(1) 먼저 사용자는 네트워크 제공자와의 인증을 위해 익명서버로부터 전달받은 g^{r_1}, 익명서버의 인증서 $Cert_{HAS}$, 그리고 $(g^{r_1}, K_{MS})K_{HAS}^{-1}$을 네트워크 제공자에게 보낸다.

(2) 이 메시지를 전달받은 네트워크 제공자는 먼저 익명서버의 인증서 $Cert_{HAS}$로부터 익명서버의 서명 검증키를 얻어 $(g^{r_1}, K_{MS})K_{HAS}^{-1}$을 복호화 함으로써 익명서버가 사용자에 대해 서명한 것임을 확인하고, 사용자와의 세션키 생성에 필요한 임의의 정수 r_2와 세션키 확인에 필요한 인증 정보 $H(K_{MN}, r_2, HNP)$를 사용자에게 전달한다. 이때 생성되는 세션키는 $K_{MN}=H(r_2, g^{hr_1})$이다.

(3) 사용자는 먼저 네트워크 제공자로부터 전달받은 r_2와 g^h를 이용하여 K_{MN}을 계산한 다음, 네트워크 제공자와 동일하게 $H'(K_{MN}, r_2, HNP)$를 생성하여 네트워크 제공자가 보낸 $H(K_{MN}, r_2, HNP)$와 같은지를 비교함으로써 네트워크 제공자에 대한 인증 정보를 확인한다. 그 후 메시지 $H(g^{r_1}, g^h, r_2, HNP)$를 자신의 서명키 K_{MS}^{-1}으로 서

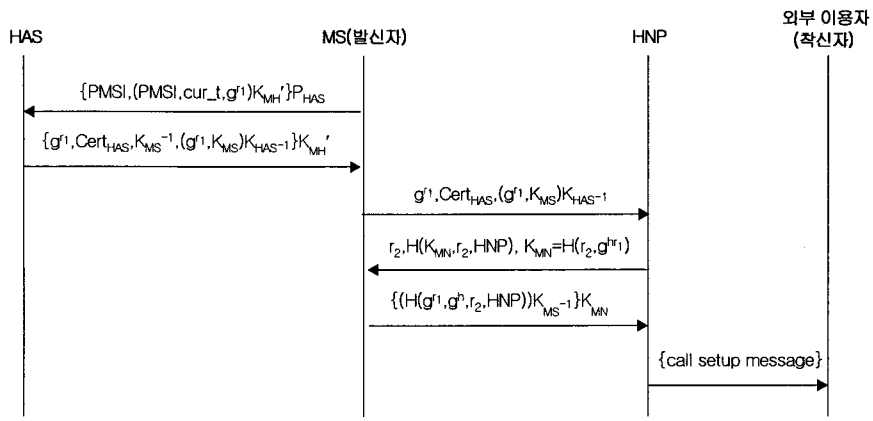

그림 2. 홈 도메인에서의 이동 발호 프로토콜
Fig. 2 Mobile Originated Protocol in Home Domain

명하고 이를 다시 세션키 K_{MN}으로 암호화한 다음, 이 메시지를 증거로서 네트워크 제공자에게 전달한다.

[단계 3] 수신자와의 콜 셋업 단계

(1) 네트워크 제공자는 착신자인 외부 이용자에게 {call setup message}를 보냄으로써 수신자와의 통화 연결을 설정한다.

이후에 주고받는 통화 내용들은 이 과정에서 상호간에 설정한 세션키 K_{MN}으로 암호화가 이루어진다.

2.3 프로토콜 분석

제안한 프로토콜에 대한 분석은 ASPeCT 프로젝트에서 기술하고 있는 이동통신에서의 인증부분에 관한 보안 요구사항들[6,7]과 아울러 본 연구의 주목적인 사용자에 대한 프라이버시를 만족하는지를 기준으로 살펴보고자 한다.

■ MS의 HNP에 대한 인증과 키 확인 : 제안하는 프로토콜 [단계 2]의 첫 번째 토큰에서 MS가 보낸 g^{r_1}에 대해 두 번째 토큰에서 HNP가 임의의 정수 r_2와 더불어 세션키 K_{MN}을 계산하여 해쉬한 인증 정보 $H(K_{MN}, r_2, HNP)$를 줌으로써 MS 측에서는 HNP가 올바른 HNP임을 인증하고 세션키 K_{MN}의 진위 여부를 확인할 수 있다. 왜냐하면 일단 메시지 $\{K_{MN}, r_2, HNP\}$를 해쉬해서 보냈다는 것은 해쉬된 메시지 K_{MN}, r_2, 그리고 HNP에 대한 무결성과 그 속에 들어있는 세션키 K_{MN}을 보호하려는 데 그 목적이 있다. 또한, 세션키를 계산하는 식 $K_{MN}=H(r_2, g^{hr_1})$에서 HNP가 K_{MN}을 계산하기 위해서는 해쉬함수 H와 r_2를 안다하더라도 g^{hr_1}을 알아야 하며, 또한 g^{hr_1}을 알기 위해서는 MS에게서 전달받은 g^{r_1}을 안다하더라도 HNP만이 알고있는 자신의 개인키인 h를 모르면 세션키 K_{MN}을 계산해 낼 수 없기 때문이다.

■ HNP의 MS에 대한 인증과 키 확인 : 우선 제안한 프로토콜 [단계 2]의 세 번째 토큰에서 MS가 메시지 $H(g^{r_1}, g^h, r_2, HNP)K_{MS}^{-1}$을 세션키 K_{MN}으로 암호화해서 HNP에게 보냈다는 것은 HNP 측에서 이 메시지를 복호화 함으로써 MS 또한 세션키 K_{MN}을 알고 있는 것으로 쉽게 확인이 가능하다. 또한 MS가 이 과정에서 세션키 K_{MN}을 계산하여 해쉬한 메시지 $H(g^{r_1}, g^h, r_2, HNP)$를 서명하여 HNP에게 전송함으로써 HNP는 MS가 올바른 MS임을 인증할 수 있다. 왜냐하면 세션키를 계산하는 식 $K_{MN}=H(r_2, g^{hr_1})$에서 MS가 K_{MN}을 계산하기 위해서는 해쉬함수 H와 HNP로부터 전달받은 r_2를 안다하더라도 g^{hr_1}을 알아야 하며, 또한 g^{hr_1}을 알기 위해서는 HNP의 diffie-hellman 공개키인 g^h을 안다하더라도 MS만이 알고있는 자신의 비밀 값인 r_1을 모르면 세션키 K_{MN}을 계산해 낼 수 없기 때문이다. 여기서 설령 제 3자가 해쉬함수 H, HNP의 공개키 g^h, r_2, 그리고 g^{r_1} 등을 안다하더라도 이들로부터 MS만이 유일하게 알고 있는 r_1이 어떤 값인지를 안다는 것은 계산적으로 불가능하다. 왜냐하면 이 문제는 암호학에서 말하는 이산대수 문제의 어려움에 기반하고 있기 때문이다.

■ 키 신규성(refreshness)과 이전의 키(old key)들을 이용한 재사용(replay) 공격 : 여기서 이전키를 이용한 재사용 공격이라 함은 MS를 포함한 기타 제 3자가 이전에 이용한 세션키 K_{MN}을 사용하여 마치 자신이 정당한 MS인 것처럼 HNP와 상호인증을 수행하려 할 경우를 말한다. 따라서, 본 프로토콜에서는 세션키 $K_{MN}(=H(r_2, g^{hr_1}))$의 계산에 참여하는 r_2를 본 프로토콜 [단계 2]의 두 번째 토큰에서 HNP가 생성하여 MS에게 전달함으로써 이러한 상황에 대비하고 있다. 또한 MS와 HNP가 세션키 계산시 각각 r_1과 r_2를 생성하여 계산함으로써 매 세션 즉, 매번 이러한 인증과정을 수행할 때마다 새로운 키를 생성하고 있다.

■ 부인방지(non-repudiation) : 이 요구사항은 만일 인증과정에서 MS가 HNP로부터 전달받은 메시지를 받지 않았다고 하거나 혹은 그 반대로 HNP가 MS로부터 전달받은 메시지를 받지 않았다고 부인할 경우에 대한 대비를 말한다. 그러나 실제 환경에서 대개 후자의 경우는 발생할 확률이 적다. 왜냐하면 이동통신 서비스를 제공하고자 하는 HNP 측에서 MS에 대한 서비스 요청을 거절할 리가 없기 때문이다. ASPeCT 프로젝트에서 제시한 요구사항 또한 후자가 아닌 전자 쪽에서의 부인방지를 논하고 있다.

만일 여기서 MS가 HNP로부터 전달받은 메시지에 대해 부인한다면 HNP는 [단계 1]의 첫 번째 토큰에서 전달받은 HAS의 인증서인 CertHAS와 [단계 2]의 세 번째 토큰에서 전달받은 MS의 서명 정보 $H(g^{r_1}, g^h, r_2, HNP)K_{MS}^{-1}$을 그 증거로 제시할 수 있다. 혹 드물지만 그 반대의 경우로 HNP가 MS로부터 전달받은 메시지에 대

해 부인한다면 MS는 [단계 2]의 두 번째 토큰에서 HNP가 임의의 정수 r_2와 더불어 세션키 K_{MN}을 계산하여 해쉬한 인증 정보 $H(K_{MN}, r_2, HNP)$를 그 증거로 제시할 수 있다. 하지만 이것만으로는 근본적인 해결은 되지 않을 것이다. 왜냐하면 그 이전에 r_2라든지 HNP 값에 대해 HNP 측에서 부인할 수가 있기 때문이다. 따라서 보다 확실한 방법은 MS 측에서 HNP로부터 해쉬한 인증 정보 $H(K_{MN}, r_2, HNP)$에 대한 서명을 받아두는 것이다. 이 방법은 본 프로토콜 제안에서는 언급되지 않은 부분이다. 그러나 때에 따라서는 이러한 부분은 본 프로토콜에 추가할 수 있다. 이를 실제 환경에 적용하고 않고는 보안 정책에 따라 유동적일 수 있다.

■ MS의 신분에 대한 프라이버시 : 제안한 프로토콜 [단계 1]의 두 번째 토큰에서 HAS로부터 전달받은 HAS의 g^{r_1}, 인증서 $Cert_{HAS}$, 그리고 $(g^{r_1}, K_{MS})K_{HAS}^{-1}$을 MS는 [단계 2]의 첫 번째 토큰에서 HNP에게 보내고 있다. 그 이유는 MS의 신분이라 할 수 있는 PMSI 정보를 HNP에게 노출시키지 않으면서 HNP로부터 MS에 대한 인증을 받기 위함이다. 즉, HAS의 공개키라든지 상위기관의 서명정보 등을 포함한 기타 개인 정보들이 담긴 HAS의 인증서 $Cert_{HAS}$와 더불어, MS와의 세션키 $K_{MN}(=H(r_2, g^{hr_1}))$의 생성에 필요한 g^{r_1}과 [단계 2]의 세 번째 토큰에서 MS가 보내온 서명 정보 $H(g^{r_1}, g^h, r_2, HNP)K_{MS}^{-1}$에 대한 검증키 K_{MS}를 HAS가 직접 서명한 메시지 $(g^{r_1}, K_{MS})K_{HAS}^{-1}$을 HNP에게 전달함으로써 MS가 아닌 HAS의 인증서와 서명을 통해 HNP가 MS를 인증하는 것이다.

■ MS의 위치에 대한 프라이버시 : MS에 대한 이동발호 설정은 기본적으로 HNP의 내부 데이터베이스인 VLR을 통해 감지되어 GMSC에 의해 외부 이용자와 연결이 된다. 또한 이 과정에서 VLR은 자신의 지역 영역들 가운데 하나인 특정 위치 영역에 등록된 MS의 PMSI 정보를 이용하여 감지하게 된다. 그러나 이 PMSI 정보는 MS의 실제 아이디가 아니며, 아울러 현 PMSI가 그 상태 그대로 계속 머물러 있지 않고 계속하여 일정 동기화 시간마다 바뀌어 VLR에 또다시 등록된다. 따라서 이 PMSI 정보만을 가지고 HNP라든지 혹은 HNP와 공모한 제 3자가 MS에 대한 위치를 파악하기란 불가능하다.

Ⅲ. 새로운 이동발호 프로토콜 제안 - 이동 사용자가 홈 도메인 내에서 타 도메인으로 위치를 이동할 경우

본 장에서는 이동 사용자가 홈 도메인에서 타 도메인으로 그 위치를 이동한 경우에 대한 이동발호 프로토콜에 대해 기술하고자 한다. 먼저 이 경우에 대한 구성 요소와 기본 모델은 [그림 3]과 같다.

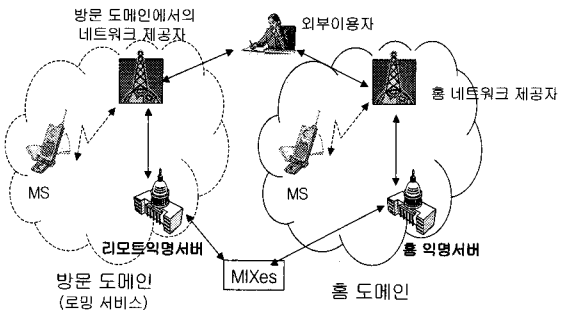

그림 3. 기본 모델: 타도메인의 경우
Fig. 3 Basic Model: Case of Remote Domain

이동 사용자인 MS가 만일 홈 도메인을 떠나 타 도메인에 도착 시 제일 먼저 하는 일은 자신의 위치 즉, MS의 PMSI 정보를 타 도메인 내에 있는 네트워크 제공자에게 등록하는 것과 리모트 익명서버에게 자신의 존재를 알리는 것이다. 여기서 네트워크 제공자에게 등록하는 과정은 종전 홈 도메인에서의 등록과정과 동일하다. 그러나 리모트 익명서버의 경우는 MS에 대한 정보(예를 들어, MS의 *PMSI*라든가 비밀키 정보 등)를 알지 못하기 때문에 홈 익명서버를 통해 MS에 대한 인증을 수행한 뒤, 비로소 정보들을 갖게 된다. 이러한 등록과정을 거친 이후에 MS는 홈 익명서버가 아닌 리모트 익명서버와 정해진 시간 간격으로 PMSI 정보를 생성하게 된다. 이때 [그림 3]에서 보는 바와 같이, 리모트 익명서버와 홈 익명서버가 서로간에 메시지를 주고받는 과정에서 중간 노드인 MIXes[8,9]를 거쳐가게 된다.

그 이후에 MS로부터 외부 이용자로의 발호 설정과정은 종전 홈 도메인에서와 마찬가지로 리모트 익명 서버의 도움으로 MS와 타 도메인측 네트워크 제공자와의 상호인증 및 키 설정에 필요한 정보들을 제공받는다. 또한 이동 착호시에도 홈 도메인에서의 방법과 마찬가지로

외부 이용자로부터 MS로의 경로 설정을 위해 필요한 MS의 임시익명 아이디인 PMSI 정보와 기타 부가정보들을 리모트 익명 서버가 네트워크 제공자에게 제공한다. 본 프로토콜 기술을 위해 추가된 각종 표기들은 다음과 같다.

[표기]

- RAS : 타 도메인 내에 있는 익명서버의 아이디, RAS' : MS가 직전 즉, 현 도메인 이전에 머물렀던 RAS의 아이디, RNP : 타 도메인 내에 있는 네트워크 제공자의 아이디.
- K_{MR} : MS와 RAS간의 세션키(session key), K_{MN} : MS와 HNP간의 세션키, K_{MP} : MS와 RNP간의 세션키.
- n, g^n : 세션키 생성을 위한 RNP의 diffie-hellman 개인키와 공개키쌍.
- b, g^b : 세션키 생성을 위한 RAS의 diffie-hellman 개인키와 공개키쌍.
- K_{MS}^{-1}, K_{MS} : HAS(또는 RAS)가 임시로 생성한 MS의 서명키와 검증키.
- K_{RAS}^{-1} : RAS의 서명키.
- U_{RAS}, P_{RAS} : RAS의 개인키와 공개키쌍.
- $Cert_{RAS}$: 무선 공개키기반구조(PKI, Public Key Infrastructure)에서 RAS의 상위 인증기관(CA, Certificate Authority)이 각각 서명한 인증서(certificate), 이때 편의상 HAS와 RAS의 상위 인증기관은 동일한 것으로 가정한다.

3.1 MS가 타 도메인으로 이동하였을 경우의 위치 갱신 프로토콜

본 프로토콜은 이동 사용자인 MS가 홈 도메인에 머물러 있다가 다른 타 도메인으로 이동했을 경우에 위치 갱신 프로토콜을 말한다. 본 프로토콜은 기본적으로는 MS가 홈 도메인 내에 위치할 경우의 위치 갱신 프로토콜의 확장이지만 이전과 달리 아래와 같은 사항들을 고려해야한다.

MS가 타 도메인에 진입 시 MS는 먼저 자신의 현 PMSI를 리모트 네트워크 제공자인 RNP에게 등록한 다음, 리모트 익명서버인 RAS에게 등록해야 한다. 그 이유는 MS의 단말기를 이용하여 곧바로 RAS에게 메시지를 전달할 방법이 없기 때문이다. 여기서 MS가 RNP에게 자신의 현 *PMSI*를 등록하는 과정은 MS가 홈 도메인에서 HNP에게 등록한 과정과 동일한 방식으로 동기화 시간 t_j마다 갱신된다. 이때 *PMSI*는 종전 홈 도메인에서 이용하던 *PMSI*가 아닌 갱신된 새로운 *PMSI*를 등록한다. 왜냐하면 HNP가 알고있는 *PMSI*와 MS가 RNP에게 등록한 *PMSI*가 같은 경우는 HNP 측으로부터 MS의 위치가 노출될 가능성이 있기 때문이다. 이 경우 *PMSI*가 갱신되는 동기화 시간 t는 그 주기가 짧을수록 자주 갱신이 일어나며 또한 보안상 유리하다. 그러나 MS가 RAS에게 등록하는 과정은 앞서 홈 도메인에서의 방법과 다르다. 즉, MS가 홈 도메인에 있을 경우는 이미 HAS와 필요한 정보들(예를 들어, 자신의 현 *PMSI*와 비밀키 등)을 합의한 상태에서 프로토콜이 시작된다. 하지만 MS가 타 도메인에 있을 경우에 RAS는 MS에 대한 정보를 전혀 가지고 있지 않기 때문에 등록시 MS는 자신의 HAS를 통해 RAS와의 상호 인증이 이루어져야 하며 동시에 RAS와의 *PMSI* 생성에 필요한 정보들(예를 들어, K_{MH}', *PRG code*, t 등)을 공유해야 한다. 이때 HAS과 RAS간의 메시지 교환은 앞서 설명한 MIXes를 통해 이루어진다. 그 이유는 내부 이용자나 기타 제 3자들로부터 이 과정에서 주고받는 메시지에 대한 비밀성과 송수신자에 대한 익명성을 부여하기 위함이다. 따라서 MS는 먼저 자신의 홈 익명서버인 HAS의 아이디와 자신의 임시익명아이디인 *PMSI*를 RNP를 통해 RAS에게 알림으로써 자신을 인증해줄 것을 요청하고 RAS는 HAS와의 정보 교환을 통해 MS와 상호 인증을 수행한다. 이 과정에서 HAS는 RAS에게 *PMSI* 생성과 관련한 정보들을 아울러 알려주게 되며 상호 인증을 수행한 결과로 MS와 RAS간의 상호 세션키에 대한 교환이 이루어진다.

제안하는 프로토콜은 아래와 같다([그림 4] 참조). 여기서 최초에 MS가 리모트 네트워크 제공자인 RNP에게 자신의 *PMSI*를 등록하는 과정은 종전 MS가 홈 도메인에 위치할 경우의 위치 갱신 프로토콜과 동일하므로 여기서는 생략하고, 그 이후의 과정만을 다룬다.

[단계 1] MS가 RAS에게 인증을 요청

MS는 먼저 임의의 정수 r_1과 r_2를 생성, g^{r_1}과 $(r_2,PMSI)K_{MH}$를 각각 계산한 다음 HAS의 아이디, RAS와의 세션키 생성에 필요한 정보 g^{r_1}, *PMSI*, HAS가 MS를 인증하기 위한 정보 $(r_2,PMSI)K_{MH}$를 RAS의 공개키 P_{RAS}로 암호화하여 RNP를 통해 RAS에게 전송한다.

[단계 2] RAS가 HAS에게 MS에 대한 인증을 요청

RAS는 받은 메시지를 자신의 개인키 U_{RAS}로 복호화하여 MS가 보낸 g^{r_1}, *PMSI*, $(r_2,PMSI,cur_t)K_{MH}$와 더불어 상위 인증기관이 서명한 자신의 인증서 $Cert_{RAS}$를 HAS의 공개키 P_{HAS}로 암호화하여 HAS에 전송한다.

[단계 3] HAS의 MS에 대한 인증과 PMSI 생성을 위한 정보를 RAS에게 제공

HAS는 전달받은 메시지를 자신의 개인키 U_{HAS}로 복호화하여 *PMSI*와 $(r_2,PMSI,cur_t)K_{MH}$를 이용, MS를 식별 및 인증한다. 또한 $Cert_{RAS}$를 이용하여 MS의 현 RAS가 누구인지를 확인한다. 만일 RAS가 기존에 머물렀던 도메인에서의 *RAS'*이 아닌 경우라면 MS에게 메시지 {*TS*, *PMSI*, *PRG code*, *t*, K_{MH}', $Cert_{HAS}$, K_{MS}, $(r_2,K_{MS}^{-1})K_{MH}$, $(H(TS, r_2, K_{MS}^{-1}, g^{r_1}, PMSI, HAS, RAS))K_{HAS}^{-1}$}을 RAS의 공개키 P_{RAS}로 암호화하여 RAS에게 전송하고, 아울러 *RAS'*에게 MS가 현재 다른 도메인으로 이동했음을 알리는 메시지 {outer domain message}를 보낸다.

[단계 4] RAS의 인증 및 세션키 합의

RAS는 임의의 정수 r_2, r_3, 그리고 타임스탬프 *TS*를 생성한 다음 *PMSI*, r_3, 해쉬값 $H(K_{MR}, r_3, RAS)$, 그리고 메시지 $\{(r_2, K_{MS}^{-1})K_{MH}, (H(TS, r_2, K_{MS}^{-1}, g^{r_1}, PMSI, HAS, RAS))K_{HAS}^{-1}\}$을 MS와 RAS 간의 세션키 K_{MR}로 암호화하여 RNP를 통해 MS에게 전송한다. 이때 $K_{MR}=H(r_3, g^{r_1 b})$이다.

[단계5] MS의 인증 및 서명

MS는 *PMSI*와 더불어 해쉬값 $H(TS, PMSI, g^{r_1}, g^{b}, r_3, RAS)$를 자신의 서명키 K_{MS}^{-1}을 이용하여 서명한 다음, 이를 MS와 RAS 간의 세션키 K_{MR}로 암호화하여 RNP를 통해 RAS에게 전송한다.

본 프로토콜은 MS가 자신의 현 *PMSI*를 등록한 이후부터 진행된다. 아울러 본 프로토콜에서 기술된 *PMSI*는 전 단계를 거치는 동안 현 *PMSI*에 대한 상호 동기화를 위해 *PMSI*를 갱신하지 않고 그대로 유지한다. 즉, 본 프로토콜이 안전하게 진행된 이후에 MS와 RAS는 외부 이용자와의 착발호 설정을 위해 홈 도메인에서와 마찬가지로 *PMSI* 정보에 대한 갱신이 일어난다. 다시 말해, 위 [단계 5] 이후, RAS는 [단계 3]에서 HAS로부터 전달받은 *PRG code*, *t*, 그리고 K_{MH}'을 이용하여 해당 MS에 대한 $PMSI(=PRG(K_{MH}',t))$를 동기화 주기마다 갱신한다. 또한 만일 여기서 MS가 현 타 도메인에서 또 다른 타 도메인으로 이동할 경우, 종전 HAS가 하던 MS의 인증을 현 타 도메인의 RAS가 대신하여 수행하면서 계속 동일한 과정을 반복하게 된다.

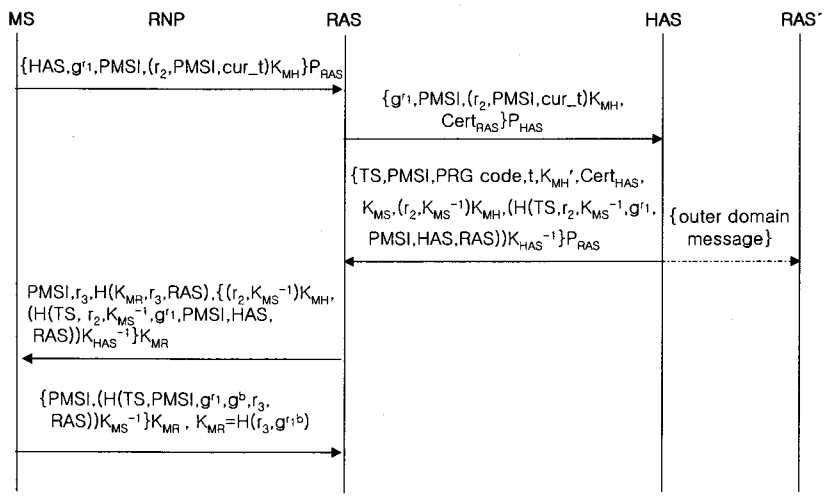

그림 4. 타 도메인에서의 위치 갱신 프로토콜
Fig. 4 Location Update Protocol in Remote Domain

3.2 이동 사용자가 타 도메인으로 이동하였을 경우의 이동 발호 프로토콜

본 프로토콜은 앞서 3.1절을 통해 MS가 리모트 네트워크 제공자인 RNP와 위치 등록을 한 상태이며 리모트 익명서버인 RAS와도 인증과 PMSI 생성에 관한 동기화가 이루어진 상태에서 진행된다. 여기서 타 도메인에서 MS에 대한 이동 발호 과정은 MS가 RAS에게 인증 정보를 요청하고 이를 이용하여 RNP와 상호인증을 수행한 다음, RNP를 통해 외부 이용자와 통화를 연결하는 것이다. 이 과정은 HAS 대신 RAS, HNP 대신 RNP가 이용된다는 것을 제외하면 위 2장에서 기술한 MS가 홈 도메인 내에 위치할 경우의 이동 발호 프로토콜과 동일하다. 아울러 프로토콜 분석 부분은 위 2.3절을 참조하기 바란다.

제안하는 프로토콜은 다음과 같다.

[프로토콜]

[단계 1] 초기화 단계

(1) MS는 먼저 임의의 정수 r_1을 생성한 다음, 메시지 $\{PMSI, (PMSI, cur_t, g^{r_1})K_{MH}'\}$을 RAS의 공개키 P_{RAS}로 암호화하여 RAS에게 보낸다.

(2) 메시지를 전달받은 RAS는 먼저 자신의 개인키 U_{RAS}와 MS와의 단기 공유 비밀키 K_{MH}'을 이용하여 암호문들을 복호화한 다음, 전달받은 $PMSI$와 자신이 복호화한 $PMSI$가 같은지를 확인한다. 이때 MS가 메시지를 보낼 당시의 $PMSI$와 자신이 메시지를 받은 직후에 $PMSI$가 다를 수 있기 때문에 보낼 당시의 시간 cur_t를 아울러 확인한다. 이후 메시지 $\{g^{r_1}, Cert_{RAS}, K_{MS}^{-1}, (g^{r_1}, K_{MS})K_{RAS}^{-1}\}$을 키 K_{MH}'으로 암호화한 다음 MS에게 전송한다.

[단계 2] 인증 단계

(1) 먼저 MS는 RNP와의 인증을 위해 RAS로부터 전달받은 g^{r_1}, RAS의 인증서 $Cert_{RAS}$, 그리고 $(g^{r_1}, K_{MS})K_{RAS}^{-1}$을 RNP에게 보낸다.

(2) 이 메시지를 전달받은 RNP는 먼저 RAS의 인증서 $Cert_{RAS}$로부터 RAS의 서명 검증키를 얻어 $(g^{r_1}, K_{MS})K_{RAS}^{-1}$을 복호화 함으로써 RAS가 MS에 대해 서명한 것임을 확인하고, MS와의 세션키 생성에 필요한 임의의 정수 r_2와 세션키 확인에 필요한 인증 정보 $H(K_{MP}, r_2, RNP)$를 MS에게 전달한다. 이때 생성되는 세션키는 $K_{MP}=H(r_2, g^{nr_1})$이다.

(3) MS는 먼저 RNP로부터 전달받은 r_2와 RNP의 공개키 g^n를 이용하여 K_{MP}를 계산한 다음, RNP와 동일하게 $H'(K_{MP}, r_2, RNP)$를 생성하여 RNP가 보낸 $H(K_{MP}, r_2, RNP)$와 같은지를 비교함으로써 RNP에 대한 인증 정보를 확인한다. 그 후 메시지 $H(g^{r_1}, g^n, r_2, RNP)$를 자신의 서명키 K_{MS}^{-1}으로 서명하고 이를 다시 세션키 K_{MP}로 암호화한 다음, 이 메시지를 증거로서 RNP에게 전달한다.

[단계 3] 수신자와의 콜 셋업 단계

(1) RNP는 착신자인 외부 이용자에게 {call setup message}를 보냄으로써 수신자와의 통화 연결을 설정한다.

이후에 주고받는 통화 내용들은 이 과정에서 상호간에 설정한 세션키 K_{MP}로 암호화가 이루어진다.

Ⅳ. 결 론

지금까지 차세대 이동통신환경에서 적용할 수 있는 새로운 위치 갱신 프로토콜과 이동 발호 프로토콜을 제안하였다. 제안한 프로토콜들은 이동 사용자가 홈 도메인 내에 위치할 경우와 타 도메인으로 위치를 이동할 경우의 프로토콜들로 기존 GSM이나 IMT-2000시스템에서 적용되지 못한 보다 고수준의 이동 사용자를 위한 프라이버시 보호 서비스를 제공한다는 점에서 매우 가치있는 성과라 할 수 있다.

참고문헌

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

[2] 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.

[3] 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.

[4] 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.

[5] 김순석, "이동통신 환경에서 사용자 프라이버시 보호를 위한 새로운 이동 착호프로토콜," *한국해양정보통신학회논문지*, 제 10권 12호, pp 2193-2201, 2006.

[6] ACTS AC095, "ASPeCT Deliverable D02, Initial Report on Security Requirements, AC095/ATEA/W21/DS/P/02/B," Feb. 1997, Available on-line as http://www.esat.kuleuven.ac.be/cosic/aspect/

[7] G. Horn and B. Preneel, "Authentication and Payment in Future Mobile Systems," *ESORICS '98*, LNCS, vol. 1485, pp. 277-293, 1998.

[8] 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.

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

저자소개

김 순 석(Soon-Seok Kim)

1997년 2월 진주산업대학교 컴퓨터공학과(공학사)
1999년 2월 중앙대학교 컴퓨터공학과(공학석사)
2003년 2월 중앙대학교 컴퓨터공학과(공학박사)
2003년 3월 ~ 현재 한라대학교 컴퓨터공학과 조교수
※ 관심분야 : 정보보호, 암호응용, 생체보안