이동통신 환경에서 사용자 프라이버시 보호를 위한 새로운 이동 착호프로토콜

김 순 석*

New Mobile Terminated Protocol for User Privacy Protection in Mobile Communication Environments

Soon-seok Kim*

본 연구는 한국과학재단 특정기초연구(R01-2005-000-10568-0) 지원으로 수행되었음.

요 약

이동통신 환경과 관련하여 프라이버시 측면에서 모바일 이용자들의 현 위치와 행적 노출에 대한 문제를 해결하기 위해 Kesdogan과 Pfitzmann[1,2,3]은 TP(Temporary Pseudonym)라는 임시 익명 아이디를 이용한 방법들을 제안하였으며, 그 후 우리는 [4]에서 네트워크 제공자 측의 능동적인 공격들로부터 모바일 이용자들을 보호할 수 있는 보다 개선된 방법을 제안한 바 있다. 그러나 우리가 기존에 제안한 프로토콜은 이동 사용자가 홈도메인 내에 위치할 경우만을 가정한 것이다. 본 논문에서는 이를 보다 확장하여 이동 사용자가 홈도메인 내에서 원격지에 있는 방문 도메인으로 이동할 경우에 사용자의 프라이버시를 보호할 수 있는 새로운 이동 착호 프로토콜을 제안하고 그것의 안전성에 대해 분석하고자 한다.

ABSTRACT

In related to mobile communication environment, Kesdogan and Pfitzmann[1,2,3] proposed solutions using temporary pseudonym identification, called TP(Temporary Pseudonym) to solve the problems concerning current locations of mobile users and exposure of their movements in the privacy aspect. After that, We proposed more improved method protecting mobile users from active attacks of network providers in [4]. But it is the case that mobile users are located in only home domain. As a more extended method, we propose new mobile terminated protocol protecting user privacy in case of moving from the home domain to the remote domain and analyze its security.

키워드

temporary pseudonym identity, location untraceability service, anonymity, privacy protection

Ⅰ. 서 론

이동 통신 환경에서 사용자의 프라이버시를 보호한다고 함은 대개 시스템 내부의 모바일 사용자에 대한 개인정보를 보호한다는 것을 의미한다. 여기서 사용자의 개인정보는 사용자 자신의 신원 즉, 아이디와 모바일 사용자

* 한라대학교 컴퓨터공학과

접수일자 : 2006. 6. 20

의 현 위치 정보 및 이동 내역, 그리고 사용자가 주고받는 메시지 등의 정보를 말한다. 이와 관련하여 Askwith 등[5]은 프라이버시에 따른 종류를 위치, 신분, 컨텐츠 이 세 가지로 나누어 정의한 바 있다. 본 논문에서는 이러한 프라이버시의 종류들 가운데 특히, 모바일 사용자의 현재 위치와 행적의 노출 즉, 위치 프라이버시에 대한 문제와 신분 프라이버시 보호에 대한 문제를 중점적으로 다루고자 한다.

위치 프라이버시 보호 문제와 관련하여 현재까지 브로드캐스트(broadcast)[6], MIXes[7,8], 그리고 TP(Temporary Pseudonym, 이하 간단히 TP라 부른다)[1,2,3] 방법 등 여러 가지 해결책들이 제안된 바 있다. 그중 TP방법은 1996년 Pfitzmann과 Kesdogan 등[2]이 제안한 개념으로, 기본 아이디어는 모바일 이용자의 실제 아이디 대신 PMSI (Pseudo Mobile Subscriber Identity)라는 임시 익명 아이디를 이용하여 통신함으로써 이용자의 신분에 대한 프라이버시를 보호한 것이다. 또한 네트워크 제공자를 비롯한 제 3자로부터 실제 아이디에 대한 노출을 피하기 위해 각 가정이나 그밖에 안전한 장소의 컴퓨터(이를 Trusted Device라하며 이하 간단히 TD라 부른다)내에 실제 아이디와 이에 대응되는 PMSI를 저장해 둠으로써 이용자에 대한 위치 프라이버시를 추가로 제공하는 메커니즘이다. 즉, 외부 이용자로부터 수신 호 요청시 네트워크 제공자 측에서 TD에게 이용자에 해당하는 PMSI를 요청함으로서 이 PMSI를 이용하여 네트워크 제공자가 이용자와 통화연결을 시켜주는 방법이다. 따라서 네트워크 제공자의 경우 모바일 이용자에 대한 PMSI는 알지만 실제 아이디가 무엇인지를 모르기 때문에 이용자의 신분을 알 수가 없다. 또한 내부적으로 PMSI값은 주기적으로 변화되어 앞서 말한 HLR과 VLR에 등록되기 때문에 네트워크 제공자 측에서 PMSI를 이용한 위치 추적이 어렵다.

이에 반해 GSM의 경우 IMSI(International Mobile Subscriber Identity)라 불리우는 실제 아이디 대신 사용자에 대한 익명성을 위해 TMSI(Temporary Mobile Subscriber Identity)라 불리우는 임시 아이디를 이용하고 있다. 그러나 이 TMSI 또한 내부 이용자인 네트워크 제공자측에서는 실제 모바일 이용자가 누구인지를 알고있기 때문에 이용자의 네트워크 제공자에 대한 위치 프라이버시는 여전히 제공되질 않는다.

TP 방법에 대한 안전성은 임시 익명 아이디인 PMSI와 물리적으로 안전한 TD에 기반하고 있으며, 일반적으로 제 3자의 공격에 대해서는 안전하다고 알려진 바 있다. 그러나 네트워크 제공자가 만일 사용자의 현 위치를 추적하기 위해 악의를 가지고 공격을 시도할 경우 몇 가지 문제점이 발생한다. Kesdogan 등은 이 문제점에 대해 논문 [3]에서 네트워크 제공자의 공격 유형을 크게 수동적인 공격(passive attack)과 능동적인 공격(active attack)으로 나누어 그 각각에 대한 해결 방법을 제안한 바 있다.

이 가운데 능동적인 공격은 수동적인 공격에 비해 좀 더 적극적인 공격으로 공격자인 네트워크 제공자가 이용자의 위치 정보를 알기 위해 TD에 주기적으로 PMSI를 요청함으로서 모바일 이용자의 위치를 지속적으로 추적하려는 시도를 말한다. Kesdogan 등[3]은 이러한 능동적인 공격과 관련하여 한가지 대안으로 RM(Reachability Manager)이라는 추가적인 하드웨어 장비를 TD에 두어 PMSI를 네트워크 제공자에게 알려주는 것이 정당한 지를 검토한 후에 요청을 받아들일 것인지 아닌지를 결정하도록 언급하고 있다. 그러나 이 제안은 실질적인 대안이라기보다는 RM을 이용하여 해결할 수도 있다는 언급만 있을 뿐 구체적으로 어떠한 방식으로 공격을 막을 것인지에 대한 기술이 되어있지 않다. 즉, RM이 어떻게 네트워크 제공자의 요청이 정당한지를 결정할 수 있는지 그 부분이 명확하지 않다.

이러한 능동적인 공격에 대한 문제점을 해결하기위해 우리는 논문 [4]에서 다음과 같은 방법을 제안한 바 있다. 즉, 외부 이용자로부터 수신 호 요청시, 외부로부터 실질적인 착호 요청이 있었는지 아니면 네트워크 제공자가 불법적인 요청을 시도하였는지를 확인하기 위해 네트워크 제공자로부터 실제로 착호 연결 요청을 받는 당사자인 사용자가 이를 확인하는 응답 메시지를 TD에게 전달하는 것이다. 이때 만일 TD가 사용자로부터 응답 메시지를 받았으면 올바른 착호 요청이므로 그 이후에도 계속 PMSI를 알려준다. 그러나 그렇지 않을 경우엔 역시 네트워크 제공자의 부정을 감지하고 이에 따른 제재를 가할 수 있다.

한편 제시한 위 방법은 이동 사용자가 홈 도메인 내에서만 머물고 있을 경우를 가정한 것이다. 여기서 홈 도메인이라 함은 현재 사용자가 가입되어 있는 홈 네트워크 제공자에 의해 공통으로 관리, 제어되는 지역과 그 지역 내에 있는 모든 개체들을 의미한다.

그러나 사용자들은 항상 자신의 홈 도메인 내에서만 머무르는 것이 아니라 때에 따라서는 서울에서 타 지역에

있는 북경으로 이동 할 수도 있다. 여기서 타 지역을 방문 도메인이라 부른다.

현재 이동 통신을 이용하고 있는 사용자들은 자신의 현 위치라든가 기타 개인 정보들이 이동 통신 사업자인 홈 도메인 측이나 방문 도메인 측에 의해 노출되어 있다는 사실을 알면서도 그 중요성을 크게 인식하지 못하고 있다. 그것은 이들 도메인 측에서 사용자와 관련한 개인 정보들을 절대 외부로 유출시키지 않으리라고 믿고 있기 때문일 것이다. 그러나 사실은 이들 도메인 측에서는 그렇지 않을 지라도, 만일 그들 가운데 어느 한 내부 이용자가 악의를 품거나 혹은 그가 외부 도청자나 기타 제3자와 공모할 경우, 사용자 자신도 모르는 사이에 자신의 개인 정보가 유출되어 직, 간접적으로 사용자에게 어떤 불이익이 생길 수 있다는 심각한 문제가 있다. 그러므로 이들 문제에 대한 대비가 반드시 필요하다.

따라서 본 논문에서는 지난번 발표한 논문 [4]를 보다 확장하여 사용자가 방문 도메인으로 이동할 경우 외부 도청자는 물론이고 홈 도메인과 방문 도메인의 내부 이용자들에 대해서도 사용자 개인의 프라이버시를 보호할 수 있는 새로운 방법을 제안코자 한다. 물론 제안하는 방법은 앞서 제시한 능동적인 공격뿐만 아니라 사용자의 위치 및 신분에 대한 익명성을 제공할 것이다.

Ⅱ. 제안하는 프로토콜

- 이동 사용자가 홈 도메인에서 방문 도메인으로 위치를 이동하였을 경우

MS가 홈 도메인을 떠나 방문 도메인에 도착시 제일 먼저 하는 일은 자신의 위치 즉, MS의 PMSI 정보를 방문 도메인 내에 있는 네트워크 제공자에게 등록하는 것과 리모트 익명서버[1]에게 자신의 존재를 알리는 것이다. 여기서 네트워크 제공자에게 등록하는 과정은 종전 홈 도메인에서의 등록과정과 동일하다(Kesdogan의 논문 [3]참조). 그러나 리모트 익명서버의 경우는 MS에 대한 정보(예를 들어, MS의 PMSI라든가 키정보 등)를 알지 못하기 때문에 홈 익명서버를 통해 MS에 대한 인증을 수행한 뒤, 비로소

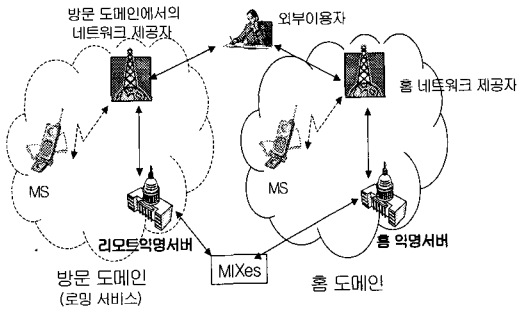

그림 1. 홈도메인에서 방문도메인으로의 이동 착호 프로토콜 모델

Fig. 1. Mobile terminated protocol model from home domain to remote domain

이 정보들을 갖게 된다. 이러한 등록과정을 거친 이후에 MS는 홈 익명서버가 아닌 리모트 익명서버와 정해진 시간 간격으로 PMSI 정보를 생성하게 된다. 이때 [그림 1]에서 보는 바와 같이, 리모트 익명서버와 홈 익명서버가 서로간에 메시지를 주고받는 과정에서 중간 노드인 MIXes[8,9]를 거쳐가게 된다.

[표기]

- *MS, HAS, HNP* : 각각 MS, HAS, HNP의 아이디.
- *RAS* : 방문 도메인 내에 존재하는 리모트 익명서버의 아이디.
- *RAS´* : MS가 직전 즉, 현 도메인 이전에 머물렀던 RAS의 아이디.
- *RNP* : 방문 도메인 내에 존재하는 네트워크 제공자의 아이디.
- K_{MH} : MS와 HAS간의 장기 공유 비밀키(long term secret key).
- *TS* : 각 개체가 서명한 타임스탬프(timestamp), 주로 메시지를 보낼 당시의 시간 정보를 서명한 값이다.
- K_{MH}´ : MS와 HAS간의 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 한 달 단위로 갱신될 수 있다.
- K_{MR} : MS와 RAS간의 세션키.

1) 기존 Kesdogan 등이 제안한 논문 [3]에서는 TD(Trust Device)라 표기하였으나, 본 논문에서는 리모트 도메인 내에 있는 익명서버로 표기함. 그 이유는 기존의 TD와 기본적인 기능은 동일하나 사용자의 능동적인 공격에 대비한 보다 확장된 기능을 갖는 독립적인 서버로 가정하여 RAS(Remote Anonymity Server)로 부르기로 함.

- K_{MN} : MS와 HNP간의 세션키.
- K_{MP} : MS와 RNP간의 세션키.
- g : 유한군(finite group)에서의 생성자.
- h, g^h : 세션키 생성을 위한 HNP의 diffie-hellman 개인키(private key)와 공개키(public key) 쌍.
- 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_{HAS}^{-1}, K_{RAS}^{-1} : HAS와 RAS의 서명키.
- U_{HAS}, P_{HAS} : HAS의 개인키와 공개키쌍
- U_{RAS}, P_{RAS} : RAS의 개인키와 공개키쌍.
- $Cert_{HAS}$, $Cert_{RAS}$: 무선 공개키기반구조(PKI, Public Key Infrastructure)에서 HAS와 RAS의 상위 인증기관(CA, Certificate Authority)이 각각 서명한 인증서(certificate), 이때 편의상 HAS와 RAS의 상위 인증기관은 동일한 것으로 가정한다.
- t : MS와 HAS가 임시익명아이디인 PMSI를 생성하기 위해 사전에 합의한 동기화 시간으로 이 값은 초 단위로 계산한다.
- cur_t : MS가 메시지를 보낼 당시의 시간으로, 만일 공개키기반구조 하의 환경일 경우 이 값은 MS가 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 생성 시 마다 다른 값을 갖는다.
- *PRG code* : 의사난수발생기인 PRG(Pseudo Random Generator) 알고리즘의 종류를 나타내는 고유번호.
- $\{m\}K$: 메시지 m을 키 K로 암호화.
- *PMSI_cur* : MS와의 동기화 시간에 따라 주기적으로 HAS가 생성하는 현재의 *PMSI* 값.
- *ACK* : MS가 HNP를 통해 외부 이용자로부터 착호 요청을 받은 데 대한 응답으로 HAS에게 보내는 메시지 (=*PMSI_cur*,(*r*,*PMSI_cur*,*cur_t*) K_{MH} ′).
- *PMSI_acked* : MS가 메시지 *ACK*를 보낼 당시에 생성한 *PMSI_cur* 값으로, 나중에 *ACK*를 전송받은 HAS가 자신 테이블 내에 보관하며 초기값은 null이다.
- *PMSI_provided* : 가장 최근에 HAS로부터 부여받은 *PMSI* 값으로 이 값은 HNP 내에 있는 *GMSC* 테이블에 보관된다. 초기값은 null이다.
- *VAL* : 1비트 벡터로, 만일 MS로부터 HAS가 *ACK* 메시지를 받은 경우는 1이 되며 그렇지 않은 경우는 0이다. 이때 이 값은 HAS 테이블 내에 보관되며 초기값은 1이다.

2.1. 사용자가 방문 도메인으로 이동하였을 경우의 위치 갱신 프로토콜

제안하는 위치갱신 프로토콜은 다음과 같다. 여기서 최초에 MS가 리모트 네트워크 제공자인 RNP에게 자신의 PMSI를 등록하는 과정은 종전 MS가 홈 도메인에 위치할 경우의 위치 갱신 프로토콜(Kesdogan의 논문 [3] 참조)과 동일하므로 여기서는 생략하고, 그 이후의 과정만을 다룬다.

[단계 1] MS가 RAS에게 인증을 요청

MS는 먼저 임의의 정수 r1과 r2를 생성, g^{r1}과 (r2,PMSI)KMH를 각각 계산한 다음 HAS의 아이디, RAS와의 세션키 생성에 필요한 정보 g^{r1}, PMSI, HAS가 MS를 인증하기 위한 정보 (r2,PMSI)KMH를 RAS의 공개키 PRAS로 암호화하여 RNP를 통해 RAS에게 전송한다.

[단계 2] RAS가 HAS에게 MS에 대한 인증을 요청

RAS는 받은 메시지를 자신의 개인키 URAS로 복호화하여 MS가 보낸 g^{r1}, PMSI, (r2,PMSI,cur_t)KMH와 더불어 상위 인증기관이 서명한 자신의 인증서 CertRAS를 HAS의 공개키 PHAS로 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}, $(r_2,K_{MS}^{-1})K_{MH}$, $(H(TS, r_2, K_{MS}^{-1}, g^{r1}, PMSI, HAS, RAS))K_{HAS}^{-1}$}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 TS를 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 PMSI와 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 PMSI를 등록한 이후부터 진행된다. 아울러 본 프로토콜에서 기술된 PMSI는 전 단계를 거치는 동안 현 PMSI에 대한 상호 동기화를 위해 PMSI를 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 방문 도메인에서 또 다른 방문 도메인으로 이동할 경우, 종전 HAS가 하던 MS의 인증을 현 방문 도메인의 RAS가 대신하여 수행하면서 계속 동일한 과정을 반복하게 된다.

2.1.1. 위치갱신 프로토콜 분석

■ **MS의 RAS에 대한 인증과 키 확인** : 제안하는 프로토콜 [단계 1]에서 MS가 보낸 g^{r_1}에 대해 [단계 4]에서 HAS가 임의의 정수 r_3과 더불어 세션키 K_{MR}을 계산하여 해쉬한 인증 정보 $H(K_{MR}, r_3, RAS)$를 줌으로써 MS 측에서는 RAS가 올바른 RAS임을 인증하고 세션키 K_{MR}의 진위 여부를 확인할 수 있다. 왜냐하면 일단 메시지 $\{K_{MR}, r_3, RAS\}$를 해쉬해서 보냈다는 것은 해쉬된 메시지 K_{MR}, r_3, 그리고 RAS에 대한 무결성과 그 속에 들어있는 세션키 K_{MR}을 보호하려는 데 그 목적이 있다. 또한, 세션키를 계산하는 식 $K_{MR}=H(r_3, g^{r_1 b})$에서 RAS가 K_{MR}을 계산하기 위해서는 해쉬함수 H와 r_3을 안다하더라도 $g^{r_1 b}$을 알아야 하며, 또한 $g^{r_1 b}$을 알기 위해서는 MS에게서 전달받은 g^{r_1}을 안다하더라도 RAS만이 알고있는 자신의 개인키인 b를 모르면 세션키 K_{MR}을 계산해 낼 수 없기 때문이다.

■ **RAS의 MS에 대한 인증과 키 확인** : 우선 제안한 프로토콜 [단계 5]에서 MS가 메시지 $H(TS, PMSI, g^{r_1}, g^b, r_3, RAS)K_{MS}^{-1}$을 세션키 K_{MR}로 암호화해서 RAS에게 보냈다는 것은 RAS 측에서 이 메시지를 복호화 함으로써 MS 또한 세션키 K_{MR}을 알고 있는 것으로 쉽게 확인이 가능하다. 또한 MS가 이 과정에서 세션키 K_{MR}을 계산하여 해쉬한 메시지 $H(TS, PMSI, g^{r_1}, g^b, r_3, RAS)$를 서명하여 RAS에게 전송함으로써 RAS는 MS가 올바른 MS임을 인증할 수 있다. 왜냐하면 세션키를 계산하는 식 $K_{MR}=H(r_3, g^{r_1 b})$에서 MS가 K_{MR}을 계산하기 위해서는 해쉬함수 H와 RAS로부터 전달받은 r_3을 안다하더라도 $g^{r_1 b}$을 알아야 하며, 또한 $g^{r_1 b}$을 알기 위해서는 RAS의 diffie-hellman 공개키인 g^b을 안다하더라도 MS만이 알고있는 자신의 비밀 값인 r_1을 모르면 세션키 K_{MR}을 계산해 낼 수 없기 때문이다. 여기서 설령 제 3자가 해쉬함수 H, HNP의 공개키 g^b, r_3, 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.

■ **HAS의 RAS에 대한 인증** : 제안하는 프로토콜 [단계 2]에서 RAS가 자신의 상위인증기관이 서명하고 발급한 인증서 $Cert_{RAS}$를 HAS에게 보냄으로써 HAS는 RAS의 신원을 믿을 수 있다. 왜냐하면 인증서 $Cert_{RAS}$속에는 인증서의 고유번호, 인증서가 발급되는 사용자의 신원, 사용자에 대한 공개키 정보, 그리고 이들 정보들을 상위인증기관이 해쉬하고 서명한 값들이 들어 있다. 만일 이 값을 NP를 비롯한 기타 제 3자가 위조하려한다면 상위인증기관만이 유일하게 알고있는 서명키를 가지고 있어야 한다. 따라서 제 3자가 이 값을 위조하기란 불가능하다. 또한 본 프로토콜에서는 기본적으로 MIXes를 가정하고 있기 때문에 HAS와 RAS(혹은 RAS들)간에 주고받는 메시지들에 대해 NP를 비롯한 제 3자 입장에서는 이 메시지가 어디에서 어디로 가는지 즉, 메시지의 송수신자가 누구인지를 식별할 수가 없으며, 또한 수신자의 공개키로 메시지가 암호화되기 때문에 그 내용을 확인할 수도 없다. 그러나 간혹 MIXes를 이용할 경우 프라이버시 보호 서비스

를 받고자하는 MS의 수가 적어 MIXes를 거쳐가더라도 자칫 그 위치가 노출 될 수도 있다. 극단적인 경우 여러 명이 아닌 한 명의 MS에 대해 HAS에서 RAS로 하나의 메시지를 보내고자 한다면 MIXes를 통과하더라도 MIXes를 통해 전달되는 사용자가 누구일 거라는 것은 금방 알 수 있다. 따라서 이러한 단점을 극복하기 위해 HAS(또는 RAS)측에서 보내고자하는 원 메시지와 함께 일종의 의미 없는 더미(dummy) 메시지를 덧붙여 전송함으로써 [그림 2]와 같이 해결 할 수 있다.

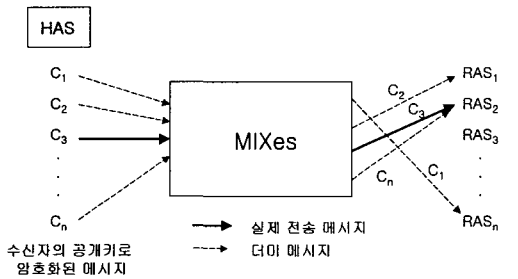

그림 2. 개선된 MIXes 방법
Fig. 2. The improved MIXes method

■ **RAS의 HAS에 대한 인증** : 이전과 마찬가지로 제안하는 프로토콜 [단계 3]에서 HAS가 자신의 상위인증기관이 서명하고 발급한 인증서 $Cert_{HAS}$를 RAS에게 보냄으로써 RAS는 HAS의 신원을 믿을 수 있으며, 또한 이 과정에서 메시지들이 MIXes를 통해 전송됨으로써 NP를 비롯한 제 3자들로부터 HAS와 RAS의 신원에 대한 익명성을 제공할 수 있다.

■ **HAS의 MS에 대한 인증** : 제안하는 프로토콜 [단계 1]에서 MS가 RAS를 통해 HAS에게 보낸 값 *PMSI*(이를 *PMSI* ′이라 하자) 즉, $(r_2, PMSI, cur_t)K_{MH}$를 통해 HAS측에서의 인증이 가능하다. 즉, MS와 HAS 둘만이 알고있는 장기 공유비밀키인 K_{MH}를 이용하여 HAS가 메시지 $(r_2, PMSI, cur_t)K_{MH}$를 복호화 한 다음 그 속에 포함된 *cur_t*를 통해 *PMSI*와 *PMSI* ′이 같은지를 비교해봄으로써 HAS는 유일한 MS가 보낸 것임을 확인할 수 있다. 또한 제 3자가 동일한 *PMSI*를 재사용 할지라도 매번 생성시 마다 r_2 값이 바뀌기 때문에 이 경우를 쉽게 확인할 수 있다. 뿐만 아니라, 기본적으로 이 값들은 다른 값들과 더불어 HAS 또는 RAS의 공개키로 암호화되어 전송되기 때문에 이 메시지가 무슨 메시지인지를 제 3자가 알 수 없다.

■ **MS의 HAS에 대한 인증** : 제안하는 프로토콜 [단계 3]에서 *TS*, $(r_2, K_{MS}^{-1})K_{MH}$와 더불어 HAS가 서명한 메시지 $(H(TS, r_2, K_{MS}^{-1}, g^{r_1}, PMSI, HAS, RAS))K_{HAS}^{-1}$을 HAS의 공개검증키를 이용하여 확인함으로써, MS는 이 값을 전달한 RAS와 더불어 HAS가 보낸 것임을 인증할 수 있다.

■ **키 신규성과 이전 키들을 이용한 재사용 공격** : 이전키를 이용한 재사용 공격이라 함은 MS를 포함한 기타 제 3자가 이전에 이용한 세션키 KMR을 사용하여 마치 자신이 정당한 MS인 것처럼 RAS와 상호인증을 수행하려 할 경우를 말한다. 따라서, 본 프로토콜에서는 세션키 KMR(=H(r3,$g^{r_1 b}$))의 계산에 참여하는 r3을 본 프로토콜 [단계 4]에서 RAS가 생성하여 MS에게 전달함으로써 이러한 상황에 대비하고 있다. 또한 MS와 RAS가 세션키 계산시 각각 r1과 r3을 생성하여 계산함으로써 매 세션 즉, 매번 이러한 인증과정을 수행할 때마다 새로운 키를 생성하고 있다.

■ **부인방지(non-repudiation)** : 이 요구사항은 만일 인증과정에서 MS가 RAS로부터 전달받은 메시지를 받지 않았다고 하거나 혹은 그 반대로 RAS가 MS로부터 전달받은 메시지를 받지 않았다고 부인할 경우에 대한 대비를 말한다. 만일 여기서 MS가 RAS로부터 전달받은 메시지에 대해 부인한다면 RAS는 [단계 5]에서 전달받은 MS의 서명 정보 $(H(TS, PMSI, g^{r_1}, g^{b}, r_3, RAS))K_{MS}^{-1}$을 그 증거로 제시할 수 있다. 반대로 RAS가 MS로부터 전달받은 메시지에 대해 부인한다면 MS는 [단계 4]에서 RAS가 임의의 정수 r_3과 더불어 세션키 K_{MR}을 계산하여 해쉬한 인증 정보 $H(K_{MR}, r_3, RAS)$와 RAS의 요청에 의해 HAS가 MS에 대해 확인하여 서명한 메시지 $(H(TS, r_2, K_{MS}^{-1}, g^{r_1}, PMSI, HAS, RAS))K_{HAS}^{-1}$을 증거로 제시함으로써 분쟁을 해결할 수 있다.

■ **NP 혹은 제 3자로부터 MS의 신분 프라이버시** : 본 프로토콜에서 MS, RAS, 그리고 HAS들간에 주고받는 PMSI 정보는 모두 수신자의 공개키로 암호화되거나 해쉬되어 있다. NP 혹은 제 3자가 PMSI를 알기 위해서는 HAS라든지 혹은 HAS와 결탁해야 한다. 그러나 본 연구는 기본적으로 HAS(혹은 RAS)가 신뢰할 수 있는 제 3의 기관이라 가정하고 있다.

■ **MS에 대한 위치 프라이버시** : 본 프로토콜의 위치

갱신과정은 기본적으로 홈 도메인에서의 위치 갱신 과정인 MS가 홈 도메인 내에 위치할 경우의 위치 갱신 프로토콜에 따르고 있다. 또한 MS가 RNP에 자신의 PMSI를 등록하기 전까지는 RAS(또는 HAS)를 제외한 어느 누구도 MS가 누구이며 어디에 위치해 있는가를 모르며, 설령 RNP에 자신의 PMSI를 등록했다하더라도 RNP 측에서는 PMSI 만을 가지고서는 HNP가 누구인지를 알 수 없다. 이것은 도청을 통한 제 3자 또한 마찬가지이다. 그밖에 MS가 자신의 PMSI를 RAS에 등록하는 과정에서 HAS와의 메시지 전송이 이루어지지만 이 역시 MIXes를 거쳐가지 때문에 추적이 어렵다.

2.2 사용자가 방문 도메인으로 이동하였을 경우의 이동 착호프로토콜

제안하는 프로토콜은 MS가 홈 도메인에서 방문 도메인으로 이동한 경우에 외부 이용자로부터의 착호 요청에 대한 설정 프로토콜로 이전 논문 [4]의 MS가 홈 도메인 내에 위치할 경우의 이동 착호 프로토콜을 확장한 것이다. 따라서 기존에 이용되던 GMSC와 HAS 측에서의 테이블은 본 프로토콜에서도 그대로 유지되며, 아울러 RNP와 RAS 측에서도 동일하게 유지된다. 다만 RNP와 RAS측에서는 착호 요청시 *PMSI_provided*라든지 *PMSI_acked*와 같은 값들이 이용되지 않기 때문에 테이블을 유지하고는 있으나, 본 프로토콜의 경우엔 이용되지 않는다. 그러나 RAS 측에 홈을 둔 MS의 경우는 MS가 홈 도메인 내에 위치할 경우의 이동 착호 프로토콜이 적용되므로 테이블 내에 있는 정보들이 그대로 유지된다.

한편 기존 논문 [4]에서 *ACK* 메시지를 둔 이유는 HNP 측에서의 불법 시도를 막기 위해 MS가 외부 이용자로부터 실제 요청이 있었는지를 확인하는 데 있었다. 그러나 본 프로토콜은 외부 이용자로부터의 착호 요청 시 HNP에게 PMSI를 알려주는 것이 아닌 RNP에게 알려 MS에게 착호를 연결하는 것이 기본 아이디어이다.

제안하는 프로토콜은 다음과 같다([그림 3]참조).

[단계 1] 외부 이용자(발신자)의 통화 요청 단계

외부 이용자가 MS와의 통화를 위해 HNP 내의 GMSC에게 *IAM*과 *MSISDN* 메시지[2]를 전송한다.

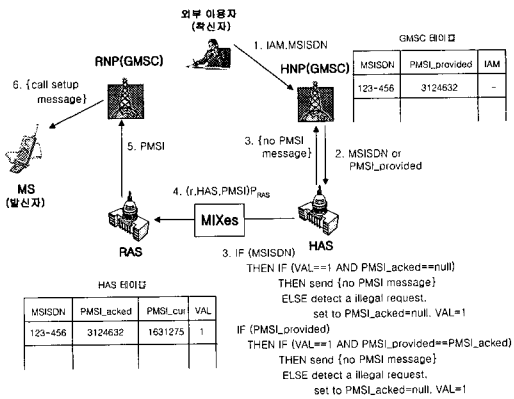

그림 3. 제안하는 이동 착호 프로토콜
Fig. 3. The proposed mobile terminated protocol

[단계 2] GMSC의 현 PMSI 요청 단계

GMSC는 자신의 테이블 내에 보관된 *PMSI_provided* 값을 확인하여 만일 이 값이 null이라면 *MSISDN*을, 그렇지 않다면 *PMSI_provided*에 저장된 값을 HAS에게 보내 현 PMSI를 요청한다.

[단계 3] HNP의 불법행위 감지 후, HAS가 {*no PMSI message*}를 보내는 단계

(1) *MSISDN*을 전송받은 경우, HAS는 먼저 자신 테이블 내에 *VAL* 값이 1이면서 동시에 *PMSI_acked*가 null인지를 확인하여 만일 그렇다면 {*no PMSI message*}를 GMSC에게 보내 MS가 현 도메인 내에 없음을 알리고, 그렇지 않다면 GMSC 측의 불법시도를 감지하고 보관중인 현 *PMSI_acked*를 null, *VAL*을 1로 재초기화한 다음, HNP에게 오프라인으로 이의를 제기한다.

(2) GMSC로부터 *PMSI_provided*를 전송받은 경우, HAS는 먼저 자신 테이블 내에 *VAL* 값이 1이면서 동시에 *PMSI_provided*가 *PMSI_acked*와 같은지를 확인하여 만일 그렇다면 {*no PMSI message*}를 GMSC에게 보낸다. 그렇지 않다면 GMSC 측의 불법시도를 감지하고 보관중인 현 *PMSI_acked*를 null, *VAL*을 1로 재초기화한 다음, HNP에게 오프라인으로 의의를 제기한다.

[단계 4] RAS로의 PMSI 전송 단계

HAS는 임의의 정수 *r*을 생성한 다음, *r*과 함께 자신의

2) 여기서 IAM(Initial Address Mobile) 메시지는 요구되는 서비스의 종류라든가 라우팅 정보를 포함하고 있으며, MSISDN(Mobile Subscriber Integrated Service Digital Network Number)은 MS의 고유 번호로 GMSC가 이것을 이용하여 MS의 위치를 파악하는데 이용한다.

아이디 *HAS*, 그리고 MS의 현 *PMSI*를 연접하여 RAS의 공개키 P_{RAS}로 암호화한 다음 RAS에게 전달한다.

[단계 5] RNP 측 GMSC로의 PMSI 전송 단계

RAS는 먼저 자신의 비밀키 U_{RAS}를 이용, 암호화된 메시지를 복호화하여 임의의 정수 *r*과 *HAS*를 제거한 다음, 전달받은 PMSI를 RNP(GMSC)에게 전달한다.[3)]

[단계 6] MS와의 연결 설정 단계

RNP(GMSC)는 {*call setup message*}를 MS에게 전달하여 발신자와의 연결을 설정한다.[4)]

만일 MS가 방문 도메인에 위치하다가 또 다시 홈 도메인으로 이동한 경우는 MS가 홈 도메인 내에 위치할 경우의 이동 착호 프로토콜이 그대로 적용된다. 즉, 응답 메시지 *ACK*가 다시 이용되며 HNP와 HAS 내에 유지하고 있는 테이블 정보들이 갱신된다.

2.2.1 이동 착호프로토콜 분석

제안한 프로토콜은 방문 도메인에서의 새로운 이동 착호 설정 프로토콜로 기존에 다른 연구들에서 제안된 바가 없는 부분이다. 따라서 본 절에서는 효율성보다는 안전성을 위주로 프로토콜을 분석하고자 한다.

제안한 프로토콜 [단계 2]와 [단계 3]의 경우는 기존 MS가 홈 도메인 내에 위치할 경우의 이동 착호 프로토콜에서 HNP 측의 GMSC로부터 보내온 *MSISDN*이나 혹은 *PMSI_provided* 값들에 대해 HAS가 이를 확인하여 현 PMSI 값인 *PMSI_cur*를 GMSC에게 알려주던 것을 *PMSI_cur* 대신 {*no PMSI message*}를 보낸다는 것 외에는 종전과 동일하다. 여기서 기존 방법과 동일하게 HAS가 이 값들을 확인하는 이유는 기존 프로토콜과의 호환성 문제도 있지만 HNP 측에서 발생할 수 있는 불법 시도를 사전에 감지하기 위함이다. 또한 MS가 현 방문 도메인에 위치하기 직전에 만일 홈 도메인에 위치하고 있었다면 홈 도메인에서의 마지막 호 요청시 MS가 보낸 *ACK* 메시지 또한 확인할 필요가 있기 때문이다.

안전성에 대한 기본적인 사항들은 종전 홈 도메인 내에서의 착호 프로토콜과 동일하므로 논문 [4]를 참조하기 바란다. 그 외에 여기서는 HNP 측에서 일어날 수 있는 각종 공격들에 대해 그 유형별로 살펴보고자 한다.

[Case 1] HAS가 PMSI를 HNP에게 알려주지 않지만 그래도 PMSI를 요청하여 이후 HAS로부터 전송되는 트래픽을 관찰함으로써 어느 곳으로 가는지를 감시하는 공격을 가할 수 있다.

본 프로토콜에서는 [그림 3]에서 보는 바와 같이 기본적으로 HAS 측에서 RAS로 메시지가 전송될 때 MIXes를 거쳐가도록 되어 있으므로 HNP를 비롯한 제 3자는 HAS 측에서 전송되는 메시지가 어느 곳으로 가는지를 알 수 없다. 그러나 이러한 불법적인 PMSI 요청의 경우, 본 프로토콜에서는 MS에게 연결되어 MS가 이를 확인하기 전까지는 정상적으로 연결이 이루어진다는 단점이 있다. 또한 MS가 확인한다 해도 통화가 되지 않고 곧바로 끊길 수가 있기 때문에 실질적으로 알아내기가 힘들다. 종전 MS가 홈 도메인 내에 위치할 경우의 이동 착호 프로토콜에서도 유사한 경우가 있었지만 이러한 경우는 그 대안으로 다음 방법을 생각해 볼 수 있다. 즉, MS 측에서 이러한 경우가 있을 때 그 횟수를 파악하여 일정 횟수(예를 들어, 주당 3회)를 초과할 경우 HAS에게 알려 HNP에게 이의를 제기하는 것이다.

[Case 2] 다른 경우로 MS가 홈 도메인에 있다가 방문 도메인으로 이동하기 직전에 HNP가 알고있던 PMSI가 있다고 하자. 이때 HNP는 이 PMSI가 현재 어느 방문 도메인에 있는지를 알아보려는 시도를 할 수 있다.

이 경우는 이전에 MS가 방문 도메인으로 이동하였을 경우의 위치 갱신 프로토콜에서도 언급한 바와 같이 MS가 방문 도메인으로 이동한 후 자신의 PMSI를 RNP에게 등록할 때는 이전의 PMSI를 그대로 등록하지 않고 갱신된 PMSI를 등록하기 때문에 HNP 측에서 이를 관찰하더라도 알 수가 없다.

그 외에도 아래와 같은 유형들을 생각해 볼 수 있다.

[Case 3] HNP를 제외한 제 3자가 위치를 추적하고자 할 경우.

이 경우는 [그림 3]에서 보는 바와 같이 기껏해야 PMSI 정도이다. 그러나 제 3자가 PMSI를 안다하더라도 PMSI가 사용자의 실제 아이디는 아니며, 또 일정 주기마다 매

3) 이 과정에서 RAS가 HAS로부터 전달 받은 PMSI를 확인한 결과 자신의 테이블 내에 해당되는 PMSI가 존재하지 않을 수도 있다. 이 경우 역시 RAS측에서 갱신된 PMSI와 더불어 이전의 PMSI를 같이 보관함으로써 이러한 문제를 해결할 수 있다.

4) 이 경우 또한 이전과 마찬가지로 GMSC측에서 MS로의 연결시 RAS가 알려준 PMSI가 HLR과 VLR에 존재하지 않을 수도 있기 때문에 GMSC가 HAS에게 재차 현 PMSI를 요청함으로써 갱신된 혹은 이전의 PMSI를 이용하여 MS로의 연결을 시도할 수 있다.

번 바뀌기 때문에 위치를 추적한다는 것을 불가능하다. 아울러 제 3자가 알아낼 수 있는 정보는 내부 이용자인 HNP에 비하면 그리 많지가 않으며 설령 HNP와 결탁한다 하더라도 현재 HNP가 시도할 수 있는 그 이상의 불법시도가 일어날 가능성은 없다.

[Case 4] RNP측에서 불법시도 여부.

RNP 측에서는 기본적으로 RAS에게 PMSI를 요청하는 것이 아니라, 그 반대로 RAS로부터의 요청에 호 연결 서비스를 제공한다. 물론 때에 따라서는 통화중이라든가 혼선, 단선 등 통화 연결에 대한 장애를 이유로 어쩌면 주기적으로 HAS에게 PMSI를 요청할 수 있다.

Ⅲ. 결 론

본 논문에서는 종전 우리가 발표한 논문 [4]를 보다 확장하여 사용자가 방문 도메인으로 이동할 경우 외부 도청자는 물론이고 홈 도메인과 방문 도메인의 내부 이용자들에 대해서도 사용자 개인의 프라이버시를 보호할 수 있는 새로운 방법을 제안하고 그 안전성에 대해 분석하였다. 물론 제안하는 방법은 앞서 Kesdogan 등이 제시한 능동적인 공격뿐만 아니라 사용자의 위치 및 신분에 대한 익명 서비스를 기본적으로 제공하고 있다.

참고문헌

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

[2] D. Kesdogan, H. Federrath, A. Jericow, and A. Pfizmann, "Location Management Strategies increasing Privacy in Mobile Communication Systems," 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," MMM-ACNS '2005, LNCS vol. 3685, pp. 436-441, 2005.

[5] B. Askwith, M. Merabti, Q. Shi, and K. Whiteley, "Achieving User Privacy in Mobile Networks," 13th Annual Computer Security Applications Conference, 1997.

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

[7] D. J. Farber and K. C. Larson, "Network Security Via Dynamic Process Renaming," Proc. of Fourth Data Communications Symposium, pp. 8-18, 1975.

[8] A. Pfitzmann, B. Pfitzmann, and M. Waidner, "ISDN-MIXes Untraceable Communication with Very Small Bandwidth Overhead," 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.

[10] V. Benjumea, J. Lopez, J. A. Montenegro, and J. M. Troya, "A First Approach to Provide Anonymity in Attribute Certificates," Proc. of the PKC2004: 7th International Workshop on Theory and Practice in Public Key Cryptography, LNCS vol. 2047, pp. 12-28, 2004.

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 전임강사
※ 관심분야 : 정보보호, 암호응용, 생체보안