이동통신 환경에서 사용자의 위치정보를 보호하는 새로운 방법

박창설[0] 김순석 김성훈 박창윤 김성권
중앙대학교 컴퓨터공학과
pcs@orchid.cse.cau.ac.kr, sskim@alg.cse.cau.ac.kr, shkim@orchid.cau.ac.kr, cypark@cau.ac.kr, skkim@cau.ac.kr

New Scheme Protecting Location Information of User in Mobile Communication Environments

Chang-Sul Park[0] Soon-Suk Kim Sung-Hoon Kim Chang-yun Park Sung-Kwun Kim
Dept. of Computer Science & Engineering, Chung-ang University

요 약

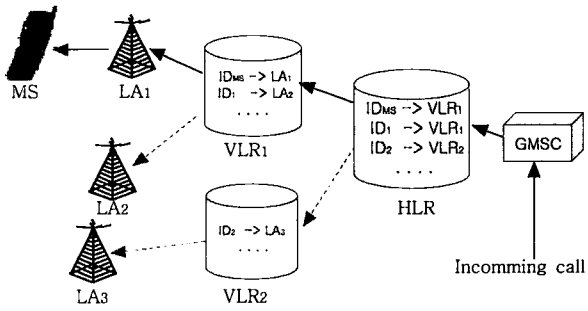
기존의 이동통신은 과거 몇 년간 이동성, 신속성, 광역성, 편리성 등으로 인하여 이용도가 크게 늘어났다. 제1세대 이동통신인 아날로그 이동전화 서비스가 시작된 이후 2세대 디지털 이동통신 기술인 CDMA 및 GSM을 거쳐 최근에 대두되고 있는 차세대 멀티미디어 이동통신인 IMT-2000 시대를 개막함으로써 이동통신에 대한 관심은 한층 증대되었으며, 또한 사용량 증가에 따라 보안문제에도 최근 많은 관심을 보이고 있다. 본 논문에서는 차세대 이동통신 환경에서 네트워크 제공자(Network Provider, 이하 줄여서 NP라 부른다)로부터 모바일 사용자의 프라이버시라 할 수 있는 위치정보를 보호하기 위한 새로운 시스템을 제안하고자 한다.

1. 서 론

이동통신은 소위 1세대라 일컫는 아날로그 방식을 거쳐 2세대 디지털 방식으로 바뀌면서 많은 발전을 거듭하였다. 이에 급격한 가입자의 증가와 제 3세대 통신이 곧 도래할 시점에서 개인의 정보보호에 관한 관심은 높아지고 있으며 이에 관한 연구는 현재 많은 전문가들에 의해 진행되고 있는 실정이다.

현재 사용되고 있는 GSM(Global System for Mobile communication) 시스템의 경우, [그림 1]에서 보는 바와 같이, HLR(Home Location Register)과 VLR(Visited Location Register)이라는 데이터 베이스를 이용하여 사용자의 아이디(ID)를 현 위치정보와 같이 매핑(Mapping)하여 보관하고 있다. 따라서 이 정보를 사용하여 외부에서 호 설정 메시지가 오면 GMSC (Gateway Mobile Switching Center)를 거쳐 HLR과 VLR에 있는 사용자의 아이디로 현재 사용자가 어느 LA(Location Area)에 위치해 있든지 MS[1]로 연결이 가능하게 된다[1].

그러나 이 아이디 정보는 모바일 사용자를 관리하는 NP측의 입장에서는 HLR과 VLR에 접근하여 특정 사용자의 위치가 어디인지 그리고 어디로 이동하는지 추적이 가능할 뿐만 아니라 사용자의 개인정보를 누출시킬 수 있음으로 인해 프라이버시가 침해될 우려가 존재한다 [2].



[그림 1] GSM subscriber identity database

현재까지 이러한 아이디 정보의 노출을 막기 위한 여러 가지 방법이 고려되어 왔으며 본 논문에서는 이 문제를 해결하기 위한 새로운 방법을 찾고자 한다.

2. 관련 연구

지금까지 모바일 사용자의 개인 신분정보라 할 수 있는 아이디 노출과 관련하여 다음과 같은 여러 해결 방법들이 연구되고 있다.

첫째, 브로드 캐스트(Broadcast)방법으로 이것은 호 설정 신호가 들어오면 사용자의 아이디를 곧바로 모바일 사용자 셀 또는 셀의 모임인 LA측으로 브로드캐스팅하는 방법이다. 이 방법은 호 설정시에 많은 부하가 걸리므로 여러 개의 그룹을 만들어 이를 브로드캐스트하는 방법을 사용한다. 그러나 이 방법 역시 부하가 많이 걸

1) Mobile Station의 약자, 일반적으로 사용자와 사용자측 단말기를 일컫는다.

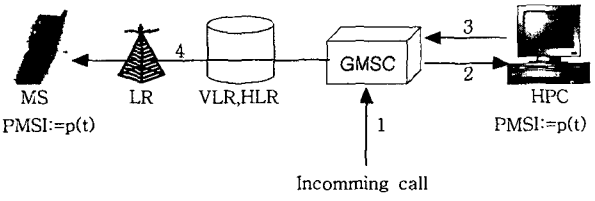
2) 본 연구는 한국과학재단 목적기초연구(R01-2000-00401)지원으로 수행되었음.

린다는 단점이 있다[3].

둘째, MIXes를 사용하는 방법이 있다. 이는 Chaum[4]에 의해 처음 제안되었고 후에 ISDN망에 적용[5]되었으며 특히 위치추적이 힘들고 변조 또한 힘들어 무선통신의 보안 형태로 연구가 진행되어 왔으며 현재는 인터넷 망에 적용시키기 위한 연구가 활발하다[6]. 그러나 MIXes는 부하가 많이 걸리고 도중에 MIX가 하나라도 오류가 발생하면 통신이 불가능하다는 단점이 있다. 최근에는 단독으로 쓰이는 것이 아니라 보안을 강화하기 위한 보조적인 수단으로서 많이 사용되고 있다.

셋째, PMSI(Pseudo Mobile Subscriber Identity)를 사용하는 방법이 연구되고 있다. 이는 호 요청 신호가 올 때 모바일 사용자의 아이디를 노출하는 것이 아니라 일정 시간 주기로 변하는 임시 아이디(Pseudonym)를 이용하여 신뢰할수 있는 장치인 TD(Trust Device)로 하여금 NP에게 이 아이디를 전달하는 방법이다.

초기에는 TD의 역할을, 모바일 사용자 자신의 집이나 회사등에 위치한 HPC(Home Personal Computer)가 수행하는 개념으로 시작했다[7]. 그러나 이는 개인의 프라이버시 보장측면에서는 우수하나 개개인이 직접적으로 관리를 해야 하며 또한 모바일 사용자가 HPC에서 멀리 떨어져 있을 때 호 설정시간이 오래 걸린다는 단점이 있다. 아래 [그림 2]는 HPC를 사용한 예를 설명하고 있다.



[그림 2] HPC의 사용

이후 HPC의 단점을 보완하고 통합적인 PMSI 관리를 위해 TD를 사용자나 NP로부터 독립된 신뢰할 수 있는 기관으로 두고 사용자들의 PMSI를 생성하고 관리하는 형태로 변형되었다. 그러나 이 경우 NP나 TD사이의 공모 가능성이 존재할 뿐만 아니라 NP측에서 PMSI를 알아내기 위해 호 설정 신호가 오지 않았음에도 지속적으로 PMSI 요청신호를 TD측으로 보낼 때 문제가 발생할 수 있다. 즉, NP가 불법적으로 PMSI값을 알기 위해 TD에게 호 설정 신호가 온 것처럼 위조하여 PMSI요청 메시지를 주기적으로 보낼 수 있다는 문제점을 가지고 있다.

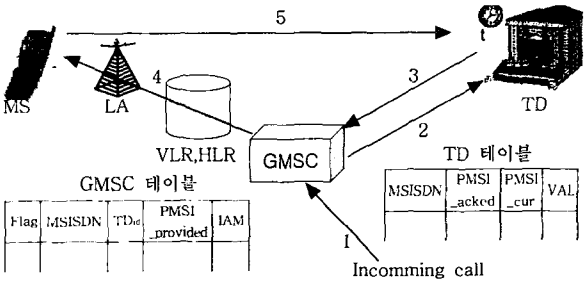
이 대안으로 나온 것이 모바일 사용자가 TD로부터 호 설정 신호와 함께 비밀 정보값을 받고 이를 토대로 모바일 사용자가 이 비밀 정보값이 실제로 TD에게서 온 적절한 값인지를 확인, 비밀정보 값이 온 횟수를 주기적으로 TD에게 응답 메시지를 보내어 확인하는 방법이다[8]. 그러나 이 방법은 TD로 하여금 확인하는 시간주기가 크거나 호 설정 신호가 빈번한 경우 불법적인 시도가 있었는지 확인하는데 시간이 오래 걸리며, 또한 MS측에서 응답신호를 보내는 시간 동안에는 NP측에서 여러번의 불법적인 시도가 가능하다는 단점이 있다.

3. 제안하는 방법

본 논문에서 제안하는 방법은 초기 호 설정 신호가 올 때 NP측에서는 MS의 아이디로 PMSI를 TD에 요구하고 TD는 PMSI를 부여한다. 이때, GMSC는 PMSI 값을 테이블에 보관한 다음 TD로부터 부여받은 PMSI를 이용하여 MS를 찾아 호 설정 신호를 보낸다. 그러면 MS는 호 설정 신호가 올바로 전달되었음을 확인하는 응답메시지를 TD로 보내게 된다.

첫 번째 호 설정을 제외한 동일 사용자의 두 번째 요청부터 GMSC는 테이블 내에 저장된 PMSI 즉, PMSI_provided 값을 이용하여 TD에게 현 PMSI인 PMSI_cur를 요청한다. 그러면 TD는 GMSC에서 전달받은 PMSI_provided와 MS로부터 응답받은 PMSI_acked 값을 비교하여 같으면 PMSI_cur를 제공하게 된다.

아래 [그림 3]은 제안하는 호 설정 메시지의 전달과정이다.



[그림 3] 제안하는 방법

[표 1] 제안하는 방법에 대한 표기

Flag : 1비트로 익명성 서비스의 제공유무를 나타내는 옵션
TD_{id} : 여러 TD를 가정할 경우 TD가 있는 주소
PMSI_provided : 가장 최근에 TD로부터 부여받은 PMSI 값
IAM : 요구되는 서비스의 종류 또는 라우팅 정보
MSISDN : GSM 네트워크에서 고유번호로 일종의 전화번호
PMSI_acked : MS에서 TD로의 응답 메시지에 포함된 MS의 현 PMSI 값
PMSI_cur : MS와의 동기화 시간에 따라 주기적으로 TD가 생성하는 현 PMSI 값
VAL : 1비트로 MS로부터 응답신호를 받은 유무를 나타내며 초기에는 값이 0이다.
$K_{vs}(r,PMSI,t)$: MS가 TD로 전달하는 응답 메시지
K_{ms} : MS와 TD간의 세션 키
r : 임의의 정수 값
PMSI : MS가 호 설정 신호를 받을 당시에 TD와 동기화된 PMSI 값
t : MS와 TD가 협의한 동기화 시간

먼저 1)외부 사용자가 MS와의 통화를 위해 호 요청을 보내면 2)NP측인 GMSC가 MS로의 연결을 위해 GMSC 테이블 내에 있는 PMSI_provided를 사용하여 PMSI_cur를 TD에게 요청한다. 3)TD는 PMSI_provided를 보고

MS로부터 응답한 PMSI_acked와 비교하여 일치하면 PMSI_cur를 제공하게 된다. 이때, TD는 MS로부터 응답 메시지가 올때까지 PMSI_cur 제공을 중단한다. 만약 GMSC에서 제공한 PMSI_provided 값이 TD 테이블에 보관하고 있는 PMSI_acked 값과 다르면 불법적인 호 요청 신호임을 인지한다. 4)GMSC는 TD로부터 PMSI_cur를 제공받은 후 GMSC 테이블 내의 PMSI_provided에 보관한 다음 호 설정 신호를 PMSI_cur 값을 이용하여 MS로 보낸다. 5)MS에서 호 설정 신호를 받게 되면 TD 측으로 호 설정 신호를 받았음을 확인하는 응답 메시지에 MS가 보관하고 있는 PMSI_cur를 첨부하여 보낸다. 끝으로 TD에서는 이를 확인하고 PMSI_acked를 테이블에 보관한다.

본 논문에서 제안하는 방법에 대한 호 설정 과정을 단계별로 나타내면 아래[표 2]와 같다.

[표 2] 호 설정 과정

```
[단계1] GMSC : check incomming call
                if PMSI_provided==NULL then send MSISDN
                    else send PMSI_provided
[단계2] TD : if receive PMSI_provided then
                if VAL==0 & PMSI_provided==PMSI_acked
                    then send PMSI_cur & VAL=1
                    else not provide PMSI_cur
             if receive MSISDN then
                if PMSI_acked==NULL
                    then send PMSI_cur & VAL=1
                    else not provide PMSI_cur
[단계3] GMSC : check PMSI_cur
                update PMSI_cur to PMSI_provided
[단계4] MS : check call-setup message
              send KMS(r,PMSI,t) to TD
[단계5] TD : check KMS(r,PMSI,t)
              update PMSI_cur to PMSI_acked & VAL=0
```

4. 분 석

만약 NP측에서 특정 사용자의 위치를 추적하기 위해 PMSI를 TD에게 두번 이상 요구한다면 GMSC 테이블 내에 있는 PMSI_provided 값이 갱신되었으므로 TD내에 있는 PMSI_acked 값과 다르게 된다. 따라서 TD는 불법적인 PMSI 요청 신호임을 감지하게 된다. 또한 PMSI_acked 값을 알고 이를 위조하여 PMSI를 요구하게 되더라도 TD측에서는 처음 한번은 PMSI를 보내게 되나 다음 요구시에는 MS로부터 응답이 올 때까지 PMSI 제공을 중단하므로 NP측의 불법적인 시도임을 감지할 수 있게 된다.

호 설정을 위한 메시지 교환에 따른 시스템 부하는 [표 3]과 같다.

본 논문에서 제안하는 방법은 NP측의 변화가 없이 기존의 이동통신 환경을 그대로 유지하면서 불법적인 호 설정 신호에 대해 감지가 가능함으로 실제 적용하는데 용이하다. 또한 GMSC에서 PMSI_provided 필드를 유지

[표 3] 호 설정을 위한 메시지 교환 부하

1. 익명성을 제공하지 않을 경우 : $M_{GM} \div B_{GM}$
2. 익명성을 제공하는 경우 : $2(M_{GT} \div B_{GT}) + (M_{GM} \div B_{GM})$
3. 익명성을 제공하고 MS로부터 TD로 응답 메시지가 있는 경우 : $2(M_{GT} \div B_{GT}) + (M_{GM} \div B_{GM}) + (M_{MT} \div B_{MT})$

GMSC와 TD사이에 메시지 전송량 : M_{GT}
GMSC가 TD사이의 채널별 할당 대역폭 : B_{GT}
GMSC에서 MS로 호 설정에 따른 메시지 전송량 : M_{GM}
GMSC에서 MS로 호 설정시의 채널별 할당 대역폭 : B_{GM}
MS에서 TD로의 응답 메시지 전송량 : M_{MT}
MS에서 TD로의 응답시의 채널별 할당 대역폭 : B_{MT}

함으로써 사전감지가 가능하고, MS로부터 호 설정 신호가 오는 즉시 TD로 응답 메시지를 보내므로 빠른 사후 감지가 가능하다는 장점이 있다.

다만 GMSC 테이블을 유지해야 한다는 부담이 있으나 단지 하나의 변수값을 추가하는 것이므로 큰 부담이라 할 수 없다. 더욱이, 호 설정 신호가 빈번할 경우 MS에서 TD로 보내는 응답 메시지에 따른 부담이 있으나 오히려 기존 연구[8]에 비해 호 설정 신호가 적은 경우에는 부담이 적다.

5. 결 론

본 논문에서는 이동통신 환경에서 이용자의 프라이버시를 보호하기 위해 모바일 이용자의 현재 위치, 그리고 행적 노출의 문제에 대한 해결책을 제시하고 아울러 NP 측에서 PMSI의 불법적인 요청시 이를 막기위한 효율적인 방법을 제시하였다.

참 고 문 헌

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

[2] H. Federrath, "Protection in Mobile Communicatio- ns", Multilateral Security in Communications, Addison-Wesley-Longman, pp.349-364, 1999.

[3] A. Pfitzmann and M. Waidner, "Networks without User Observability", Computers & Security, vol. 6, no. 2, pp. 158-166, 1987.

[4] D. Chaum, "Untraceable Electronic Mail, Return Address and Digital Peudonyms", Communications of the ACM, vol.24, no.2, pp. 65-75, 1981.

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

[6] H. Fedderrath, A. Jerichow, and A. Pfitzmann, "MIXes in Mobile Communication Systems : Location Management with Privacy", proc. Workshop on Information Hiding, 1997.

[7] D. Kesdogan, H. Federrath, A. jerichow, and A. Pfitzmann "Location Management Strategies Increasing Privacy in Mobile Communication", angenommen bei: IFIP SEC '96, 1996.

[8] 김순석, 김성권, "이동통신 환경에서 임시 익명 아이디를 이용한 위치 불추적 서비스와 지불 프로토콜에 관한 연구", 한국정보과학회 심사중, 2001년 12월.