이동통신환경에서 사용자 프라이버시 보호를 위한 익명 시스템

김구창[0] 박창설 김순석 박창윤 김성권
중앙대학교 컴퓨터공학과
{gckim[0]@alg, pcs@orchid, sskim@alg}.cse.cau.ac.kr, {cypark, skkim}@cau.ac.kr

Anonymity System for User Privacy Protection in Mobile Communication Environments

Goo-Chang Kim[0] Chang-Sul Park Soon-Seok Kim Chang-yun Park Sung-Kwon Kim
Dept. of Computer Science & Engineering, Chung-ang University

요 약

최근 이동통신 사용자수의 증가로 각 통신사업자들은 이동 네트워크가 더욱 원활하게 동작할 수 있도록 인프라를 향상시키고, 업그레이드하고, 고도화시키는데 많은 노력을 기울이고 있다. 그러나 이러한 노력들에 비해 이동통신 사업자나 혹은 서비스 제공자들로부터 사용자의 위치정보나 이동내역정보 등과 같은 개인 프라이버시를 보호하는데 필요한 노력은 아직 미비한 실정이다. 현재까지 TP(Temporary Pseudonym) [3,4]등과 같은 사용자의 프라이버시를 보호하기 위한 여러 연구들[6,7]이 이루어지고 있으나 차세대 멀티미디어 이동통신환경에 적용하기에는 몇 가지 문제점들이 있다. 따라서 본 논문에서는 이러한 문제점들을 개선한 새로운 익명 시스템을 제안하고, 아울러 제안한 시스템의 시뮬레이션을 통하여 그 성능을 검증해보고자 한다.

1. 서 론

2002년 7월 현재 국내 이동전화 가입자수는 약 3천100만 명인 것으로 잠정 집계됐으며, 이는 전체 국민의 67.4%에 해당한다[1]. 그러나 이러한 증가된 가입자수에도 불구하고 서비스를 제공하는 네트워크제공자나 혹은 부가가치 서비스제공자 등으로부터 사용자가 이동하는 현 위치라든가 사용자의 실제 신원은 여전히 보호되지 못하고 있는 실정이다.

기존 GSM 시스템[2]의 경우, 사용자의 신분에 대한 노출을 피하기 위해 실제 신원과 매칭되는 임시아이디[1]를 이용하여 제 3자들로부터 불법적인 위치추적을 방지하고 있다. 그러나 만일 내부 이용자인 네트워크제공자가 악의를 띨 경우 언제든지 사용자의 현 위치나 내역 등을 알아낼 수 있다는 문제점이 있다. 이에 반해 Kesdogan[3,4]이 제안한 일명 TP(Temporary Pseudonym)방법은 임시익명아이디(PMSI, Pseudo Mobile Subscriber Identity)를 이용하여 불법적인 제 3자뿐만 아니라 내부 이용자인 네트워크제공자들로부터 사용자의 위치와 신분 노출을 막고자 하였다. 여기서, 임시익명아이디는 사용자와 TD(Trust Device, 이하 TD라 칭한다)라는 별도의 독립된 장치를 이용하여 서로 동기화된 시간에 동시에 생성되며, 이때 TD는 외부이용자로부터의 착호 요청시 네트워크제공자에게 이 값을 알려주는 역할을 수행한다. 그러나 이 방법은 네트워크제공자가 사용자의 현 위치나 혹은 그 동안의 위치 내역 등을 알아내기 위해 주기적으로 TD에게 현재의 임시익명아이디를 요구하는 부정을 저지를 수도 있다는 문제점을 안고 있으며, 아울러 이동 발호시 통화 연결을 셋업하는 과정에 대해서는 고려하지 않고 있다. 따라서, 본 논문에서는 앞서 언급한 GSM이나 TP방법들의 문제점을 개선한 새로운 익명시스템을 제안하고 제안한 시스템의 시뮬레이션을 통하여 그 성능을 검증해보고자 한다. 제안하는 시스템의 기본 아이디어는 네트워크제공자나 그밖에 제 3자들로부터 이동 사용자의 위치정보 즉, 프라이버시를 보호하고자 사용자와 네트워크제공자들 사이에 새로운 하나의 독립된 익명서버를 두어 기존의 문제점들을 암호학적인 관점에서 해결하고자 하는데 있다. 여기서 익명서버는 기존에 제안된 TD라는 독립된 장치의 기능을 대폭 개선한 것으로, 종전 TD는 단순히 사용자의 실제 아이디를 네트워크제공자들로부터 숨기는 역할을 수행하였으나 제안하는 시스템은 이러한 역할뿐만 아니라 사용자의 현 위치 혹은 위치 내역정보 등을 파악하려는 제 3자나 혹은 네트워크제공자로부터 불법적인 시도를 막고 사용자와 네트워크제공자 사이에 인증문제라든가 통신 요금에 관한 과금, 그리고 키복구 문제에도 참여하는 등 보다 광의적인 기능을 수행한다. 또한 제안한 시스템을 실제와 유사한 환경에서 시뮬레이션하고, 그 성능을 기존의 GSM이나 TP방식들과 비교하여 검증하고자 한다.

본 논문의 2장에서는 제안하는 익명시스템에 대하여 기술하고 3장에서 본 시스템의 시뮬레이션과 그 성능을 분석한 다음, 4장을 끝으로 결론을 맺고자 한다.

2. 제안하는 익명 시스템

먼저 제안하는 익명 시스템은 [표 1]과 같이 크게 세 유형으로 나누어 볼 수 있으며, 관련한 용어 및 표기는 [표 2], [표 3]과 같다. 다음 절에서는 [표 1]의 각 유형들에 따른 프로토콜들을 기술하고자 한다.

[표 1] 제안하는 익명시스템의 세가지 유형

Type A	이동 사용자의 위치 갱신 프로토콜
Type B	이동 사용자의 발호 설정 프로토콜
Type C	이동 사용자의 착호 설정 프로토콜

1) 대개 TMSI(Temporary Mobile Subscriber Identity)라 부른다.

2) 본 연구는 한국과학재단 목적기초연구(R01-2000-000-00401-0)지원으로 수행되었음.

[표 2] 관련용어

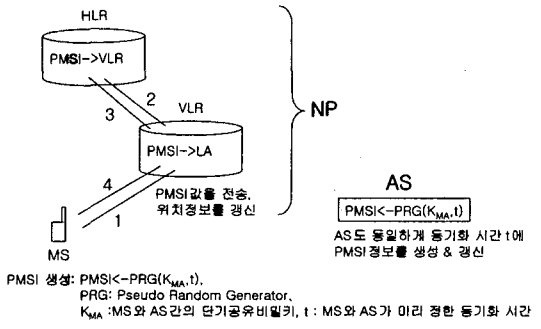
NP	Network Provider
AS	Anonymity Server
MS	Mobile Station
MSISDN	MS의 고유 ISDN Number
IAM	Initial Addressing Mode
HLR	Home Location Register
VLR	Visited Location Register
LA	Location Area

[표 3] 제안하는 프로토콜의 표기

K_{MA} : MS와 AS간의 단기공유비밀키
K_{MS}^{-1}, K_{MS} : AS가 생성한 MS의 서명키, 검증키
K_{AS}^{-1} : AS의 서명키, K_{MN} : MS와 NP간의 세션키
P_{AS} : AS의 공개키, $Cert_{AS}$: AS의 인증서
g^h : NP의 diffie-hellman 공개키, r_1, r_2 : 랜덤 정수
g : 유한군에서의 생성자, H : 일방향 해쉬함수
CNT : NP측인 GMSC로부터 AS가 실제 요청을 받은 횟수
CNT_{old} : 직전에 AS로부터 NP를 통해 전달받은 CNT
NP : NP의 아이디, S : AS가 MS에게 보내는 비밀정보
P : MS가 AS에게 착호요청에 대한 응답으로 보내는 증거
cur_t : AS가 비밀정보 S를 보낸 시간
t : MS와 AS가 미리 정한 동기화 시간

2.1 [Type A] 이동 사용자의 위치 갱신 프로토콜

본 프로토콜은 익명서버 AS와 이동 사용자 MS가 동기화 시간 t마다 주기적으로 생성한 임시익명아이디 PMSI를 MS가 네트워크제공자 NP에게 알려주는 과정을 말한다. 이때 PMSI는 외부 송신자와의 착호 설정을 위해 NP내에 있는 위치정보 저장 데이터베이스인 HLR과 VLR에 저장된다([그림 1] 참조).



[그림 1] [Type A] 이동 사용자의 위치 갱신 프로토콜

2.2 [Type B] 이동 사용자의 발호 설정 프로토콜

본 프로토콜은 이동 사용자 MS가 네트워크제공자 NP에게 특정 착신자와 통화를 요청할 경우를 의미한다. 기본 아이디어는 1)MS가 익명서버 AS로부터 인증정보를 받아 2)NP와 상호인증을 수행하고 3)NP는 인증절차가 끝난 후에 특정 착신자와 통화 연결을 설정하는 것이다.

[단계1] 초기화 단계

MS → AS: $\{PMSI,(PMSI,g^{r_1})K_{MA}\}P_{AS}$
MS ← AS: $\{Cert_{AS},g^{r_1},K_{MS}^{-1},(g^{r_1},K_{MS})K_{AS}^{-1}\}K_{MA}$

[단계2] 인증 단계

MS → NP: $g^{r_1},Cert_{AS},(g^{r_1},K_{MS})K_{AS}^{-1}$
MS ← NP: $r_2,H(K_{MN},r_2,NP)$, $K_{MN} = H(r_2,g^{hr_1})$
MS → NP: $\{(H(g^{r_1},g^h,r_2,NP))K_{MS}^{-1}\}K_{MN}$

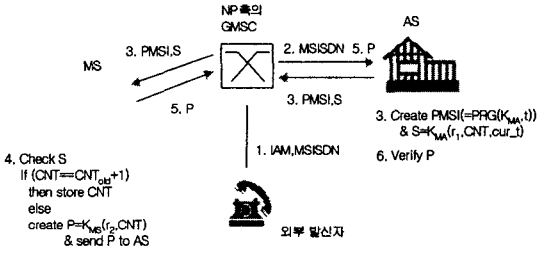
[단계3] 특정 착신자(Callee)와의 연결설정 단계

NP → Callee: {call setup message}

본 프로토콜은 차세대 이동통신 시스템 UMTS에 적용될 보안 기술을 연구하는 ASPeCT[5] 프로젝트에서 제안한 인증 및 키 설정 프로토콜을 응용한 것이다. 본 프로토콜의 안전성은 기본적으로 ASPeCT에서 언급한 요구사항들을 모두 만족하고 있으며, 관련한 상세 설명은 생략한다.

2.3 [Type C] 이동 사용자의 착호 설정 프로토콜

본 프로토콜은 외부 발신자가 이동사용자 MS와 통화를 요청하는 경우로, 네트워크제공자 NP 또는 제 3자로부터 MS의 위치정보와 실제 신원을 보호하는데 그 목적이 있다. 제안하는 프로토콜은 [그림 2]와 같다.



[그림 2] [Type C] 이동 사용자의 착호 설정 프로토콜

3. 익명시스템 시뮬레이션 및 성능평가

3.1 개발 환경 및 시스템 구성

먼저 제안하는 시스템의 시뮬레이션을 위한 개발환경은 [표 4] [표 5]와 같다.

[표 4] 하드웨어

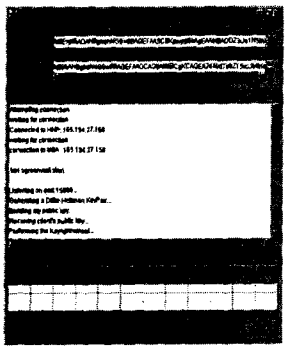
NP	Pentium III XEON 600MHz	Windows NT Server
AS	Pentium III XEON 600MHz	Windows NT Server
MS	(NoteBook) Pentium III 700MHz (256M)	Windows 2000 Professional
Callee (Caller)	Pentium III 600MHz (256M)	Windows 2000 Professional

※ 여기서 MS는 무선 랜 카드를 통하여 랜에 연결된다.

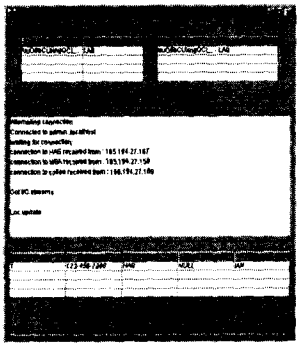
[표 5] 소프트웨어

Java	Java 2 SDK	1.3.1_03
JCE (Java Cryptography Extension)	sunJCE	1.2.1
	Bouncy Castle	jce-jdk13-114
보안 프로바이더	Bouncy Castle	bcprov-jdk13-114

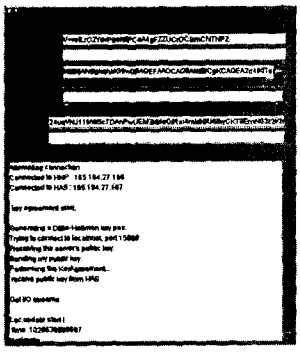
아래 [그림 3,4,5,6]은 제안하는 익명 시스템을 시뮬레이션한 화면이다. 여기서 익명서버 AS는 스스로 자신의 공개키와 개인키를 생성하며, 그밖에 요구되는 정보는 테이블내에 저장되는 것으로 가정하였다([그림 3] 참조). 또한 네트워크제공자



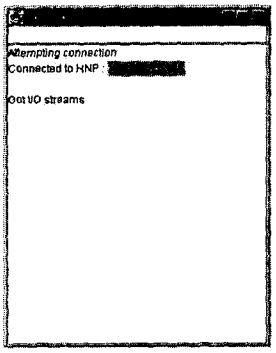
[그림 3] 익명 서버(AS)



[그림 4] 네트워크제공자(NP)



[그림 5] 이동 사용자(MS)

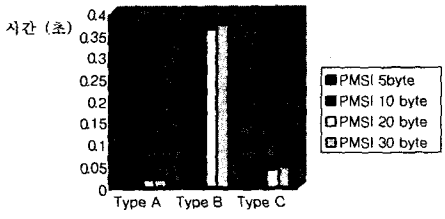


[그림 6] 착(발)신자

NP는 그 내부에 데이터베이스인 HLR과 VLR들이 존재하며, 그밖에 정보들은 역시 테이블 내에 보관하는 것으로 가정하였다([그림 4] 참조). 이동 사용자 MS는 익명 서버와의 인증에 필요한 세션키, PMSI, 그리고 AS의 공개키 등을 보관하고 있으며, 착(발)신자는 단순히 통화요청을 하고 NP로부터 통화연결 메시지를 받는 역할을 수행한다. 이때 MS와 AS는 동기화된 값으로 일정시간마다 동시에 PMSI를 생성하며, 초기설정 단계에서 AS는 자신의 공개키와 개인키를 생성하고 MS와 세션키를 공유한다.

3.2 분석

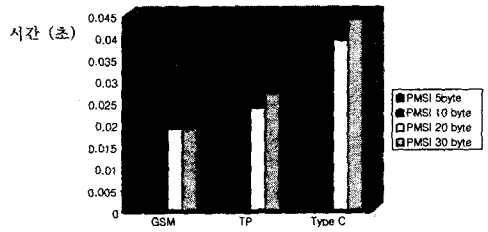
본 절에서는 앞서 언급한 시뮬레이션을 통해 수행한 결과들을 PMSI 길이와 기존 GSM 및 TP방식과의 비교로 나누어 기술한다.



[그림 7] PMSI 길이에 따른 각 프로토콜별 실행시간

위 [그림 7]은 PMSI의 길이를 각각 5, 10, 20, 30byte로 각기 다르게 변화시켰을 때 각 Type별 평균실행시간을 나타낸 것이다. 각 실행시간은 [Type A]가 0.0126초, [Type B]가 0.3445초, 그리고 [Type C]가 0.039075초이다. 이때 [Type B]는 [Type C]의 약 8.8배정도 시간이 소요된다. 그 이유는 기존 처럼 MS가 NP에 대해서만 인증하는 것이 아니라, 2.2절에서 살펴본 바와 같이 MS가 AS를 통해 NP와의 상호인증을 수행하기 때문이다.

아래 [그림 8]은 GSM, TP방법과 제안하는 시스템 [Type C]를 PMSI의 길이에 따라 비교한 것이다. 여기서 [Type C]의 경우, TP방법에 비해 약 74% 그리고 GSM 방식에 비해 약 200%의 소요시간 증가를 보이고 있으나, 보안성 측면에서 볼 때 기존 GSM방식에 비해 불법적인 네트워크제공자로부터 악의적인 시도를 막을 수 있고, TP방법에 비해 사용자의 현 위치나 내역정보 등을 알아내기 위해 주기적으로 AS에게 현 PMSI를 요구하는 네트워크제공자의 부정을 방지할 수 있다는 장점이 있다. 또한 실험결과 기존 방식들에 비해 실질적으로 소요되는 시간의 차이는 1/100초 이하로 그리 크지가 않다는 것이 확인되었다.



[그림 8] GSM, TP, 제안하는 시스템 [Type C]와의 비교

4. 결론

본 논문은 이동통신환경에서 이동 사용자의 위치정보나 내역정보 등과 같은 개인 프라이버시 정보들을 보호하고자 새로운 익명 시스템을 제안하는데 그 목적이 있다. 제안한 시스템은 기존의 GSM이나 TP방식들에 비해 보안성이 뛰어나다는 장점이 있으며, 아울러 본 시스템을 실제 시뮬레이션 해봄으로써 그 성능을 확인하였다. 향후 연구방향으로 제안한 시스템을 서비스 이용요금에 따른 과금이나 키위탁 프로토콜 등에 응용해 보고자 한다.

참 고 문 헌

[1] inews24, "허술한 이통업체 고객정보관리, 더 이상 못참겠다!," 인터넷 뉴스, 2002년 8월 (http://news.naver.com).

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

[3] D. Kesdogan, H. Federrath, A. Jericow, and A.Pfizmann, "Location Management Strategies Increasing Privacy in Mobile Communication," angenommen bei: 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] G. Horn and B. Preneel, "Authentication and Payment in Future Mobile Systems," ESORICS '98, LNCS, vol. 1485, pp. 277-293, 1998.

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

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