# 이동통신 환경에서 프라이버시를 고려한 지불 방법†

김순석*, 신제용*, 김성권*

*중앙대학교, 컴퓨터공학과

# Payment Scheme Considering Privacy in Mobile Communication Environments

Soon-Seok Kim*, Je-Yong Shin*, Sung-Kwon Kim*

*Department of Computer Science & Engineering Chung-Ang Univ.

## 요 약

본 논문에서는 차세대 이동통신 환경에서 모바일 이용자가 자신의 단말기를 이용, 부가가치 서비스 제공자(VASP, Value Added Service Provider)에게 접근하여 서비스를 받을 경우에 대한 과금 문제를 다루고자 한다. 또한 이 과정에서 발생할 수 있는 모바일 이용자와 부가가치 서비스 제공자사이에 인증문제, 상호간에 분쟁이 발생했을 경우에 대한 해결, 모바일 사용자의 위치 정보에 대한 프라이버시 보호 그리고 모바일 사용자의 신분에 대한 익명성 보장문제 등을 암호학적인 프리미티브들을 이용하여 아울러 해결하고자 한다.

## I. 서론

현재까지 많은 연구자들이 이동통신 환경하에서의 보안 요구사항들에 대해 논의해오고 있다. 그 중 [1]에 따르면 크게 1)기밀성(confidentiality), 2)무결성(integrity), 그리고 3)가용성(availability) 이 세 가지로 구분하고 있으며, 특히 기밀성은 다시 내용(content), 위치(location) 그리고 수신자[1] (addressee)에 대한 프라이버시로 세분하고 있다. 내용에 대한 프라이버시는 송수신자간에 주고받는 메시지는 비인가된 자들로부터 안전하게 보호되어야 한다는 것으로 주로 암호학적인 프리미티브들을 이용하여 메시지를 암호화함으로서 해결할 수 있다. 수신자에 대한 프라이버시는 주로 메시지를 수신받는 수신자인 모바일 이용자에 대한 신분이 비인가된 사용자들로부터 노출되지 않아야 한다는 것으로, 흔히 이용자에 대한 익명성을 말한다. 현재 이 부분에 대한 연구는 모바일 이용자의 실제 아이디가 아닌 임시 아이디나 별명(alias) 등을 이용하여 암호화하여 전송함으로써 해결하고 있다. 위치에 대한 프라이버시는 모바일 이용자의 현 위치나 혹은 이동한 위치들에 대한 내역 정보가 비인가된 자들로부터 추적이 불가능해야 한다는 것이다. 그러나 이러한 위치에 대한 정보는 인가된 사용자들로부터는 효율적인 방법으로 이용되어야 한다. 현재 MIXes[2,3], TD(Trusted Device)[4,5], 그리고 브로드캐스트 등의 방법을 이용하고 해결하고 있다. 이를 위해 본 논문에서는 TD를 이용하여 위치 프라이버시에 대한 문제를 해결하고자 한다. 왜냐하면 이 방법은 타 방법들에 비해 암호화 효율이 좋고 현 네트워크 아키텍처를 그대로 이용할 수 있다는 장점이 있다.

본 논문에서는 차세대 이동통신 환경에서 모바일 이용자가 자신의 단말기를 이용, 부가가치 서비스 제공자(이하 VASP라 한다)에게 접근하여 서비스를 받을 경우에 대한 과금 문제를 다루고자 한다. 또한 이 과정에서 발생할 수 있는 모바일 이용자와 부가가치 서비스 제공자사이에 인증문제, 상호간에 분쟁이 발생했을 경우에 대한 해결, 모바일 사용자의 위치에 대한 프라이버시 보호 그리고 모바일 사용자의 신분에 대한 익명성 보장문제 등을 아울러 해결하고자 한다.

본 논문의 2장에서는 이 문제와 관련한 기존 논문들의 장단점을 다루고 3장에서 새로운 과금 프로토콜을 제안한 뒤 4장을 끝으로 결론을 맺고

† 본 연구는 한국과학재단 목적기초연구 R01-2000-00401 지원으로 수행되었음.

1) 주로 모바일 사용자를 말한다.

자 한다.

## II. 관련연구

본 논문에서는 위치 프라이버시의 보장을 위해 여러 방법들 가운데 TD를 이용한 방법을 제안한다. 이 방법은 원래 Pfitzmann[2]이 제안한 방법으로 모바일 이용자의 위치정보를 집이나 특정 건물 등의 안전한 장소인 HPC(Home Personal Computer)내에 보관함으로써 이용자의 위치 프라이버시를 보장한 개념이다. 이후 Kesdodan[4,5]이 HPC 대신 TD라 하여 물리적인 HPC의 붕괴를 방지하고 아울러 모바일 이용자의 익명성을 보장하기 위해 임시 익명 아이디[2](temporary pseudonym)라는 개념을 제안하여 기존 방법을 더욱 개선시켰다.

MIXes 방법을 간단히 설명하면 여러 송(수)신자들로부터의 메시지들을 MIX를 통해 수집하여 일정한 암호화 과정을 거친 뒤 그 내용을 변형하여 수(송)신자들에게 전달하는 방식이다. 이 방법의 경우 MIX측에서 주어진 메시지에 대해 512비트의 추가적인 암호화가 필요하며 기존 이동 통신 환경에 MIX를 추가적으로 설치해야하기 때문에 구조적인 변화가 요구된다. 브로드캐스트 방법의 경우도 송신자로부터의 수신호 요청을 모바일 이용자가 위치한 LA(Location Area)에 브로드캐스트하는 것으로 모바일 이용자가 이 신호를 받아들임으로 인한 추가적인 네트워크 부담이 따른다. 이에 반해 TD를 이용한 방법은 기존 모바일 환경의 구조적인 변화없이 별도로 TD만 설치하면 되고 메시지에 대한 추가적인 암호화도 요구되지 않으므로 매우 효율적이다.

Buttyan이 제안한 논문 [6]에서는 모바일 이용자의 익명성을 보장하기 위해 CCA(Customer Care Agency)라는 제 3의 기관을 두고 있는 것이 특징이다. 이 기관을 이용하여 모바일 이용자에게 티켓을 발부하면 이용자는 이 티켓을 VASP에게 제시함으로써 부가가치 서비스를 받고 CCA가 대신 VASP에게 과금한다. 그 후 오프라인으로 모바일 이용자에게 과금한 금액만큼 청구를 하는 방식이다. 또한 위치 프라이버시에 대한 보호를 위해 MIXes 방법을 이용하고 있다. 그러나 이 방법은 기본적으로 MIXes를 이용하며 사용자 익명성 보장을 위해 추가적으로 CCA를 둠으로 비효율적이다.

차세대 이동통신 시스템인 UMTS에 적용될 보안기술을 연구 개발하는 ASPeCT 프로젝트[7]에서는 공개키 기반의 신뢰성 있는 제 3자인 TTP(Trusted Third Party)를 두어 모바일 이용자들에게 부가가치 서비스를 제공하는 방식을 제안하였다. 그러나 이 방법은 TTP를 추가적으로 설치해야하는 부담이 있으며 사용자에 대한 익명성과 위치에 대한 프라이버시가 제공되지 않는 단점이 있다. 그 외에 여러 논문들에서 이와 관련한 방법들을 제안하였으나 이들 역시 익명성이라든가 위치에 대한 프라이버시가 제공되지 않는다.

## III. 제안하는 과금 방법

본 논문에서 제안하는 기본 모델은 아래 [그림 1]에서 보는 바와 같이 익명 서비스와 위치에 대한 프라이버시를 제공하는 TD와 모바일 이용자인 User 그리고 부가가치 서비스를 제공하는 VASP로 나뉜다. 먼저 1)User가 TD에게 서비스를 제공받기 위해 일회용 티켓을 요청하면 TD가 이 요청을 확인하고 티켓을 발부한다. 2)그 후 User가 서비스 요청을 위해 VASP에게 TD로부터 받은 티켓을 제시하고 VASP는 이를 확인한다. 확인이 끝나면 3)이 티켓을 이용하여 VASP로부터 서비스를 제공받는다. 서비스 제공이 끝나면 4)VASP는 일정시간이 지난 후(예를 들어, 당일 자정) 그 동안의 과금 정보를 TD에게 제시하고 TD가 이를 확인, 해당 금액을 VASP에게 지불한 다음 User에게 또한 이 금액을 청구한다.

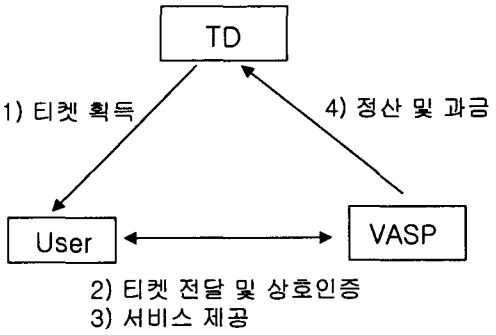


그림 1: 기본 모델

제안하는 방법에서는 모바일 이용자의 비밀키와 공개키쌍 그리고 모바일 이용자와 TD간의 공

2) PMSI(Pseudo Mobile Subscriber Identity)라 하며 모바일 이용자의 실제 아이디가 아닌 임시 아이디를 말한다. 예를 들어, 유사난수발생 함수를 PRG, 모바일 이용자와 TD사이의 공통키를 k, 그리고 현 시각을 t라 할 때, PMSI=PRG(k, t)이며, 이때 t는 모바일 이용자와 TD간에 미리 약속된 시간 간격으로 동기화가 일어난다.

통키에 대한 정보는 모바일 이용자가 사전에 TD에 등록할 당시에 합의된 것으로 가정하며 아울러 TD와 VASP의 공개키에 대한 정보는 공개키 디렉토리 서비스나 브로드캐스트 등의 방법을 이용하여 알고 있다고 가정한다.

**[표기]**

- User : U, VASP: SP
- $PMSI_U$ : U의 id로 임시 익명 아이디
- t : U가 TD에게 티켓 요청을 보낼 당시의 동기화 시간
- $TD_{id}$ : TD의 아이디, $SP_{id}$ : SP의 아이디
- T : 티켓, $T_{id}$ : 티켓의 아이디
- TS : 타임스탬프(timestamp)
- H : 충돌회피 일방향 해쉬함수
- $tck_n$ : tick[3] 정보로 $tck_0$(H의 seed)를 이용, n번째 hash한 값
- $tck_v$ : U가 SP에게 보낸 최종 tick 정보
- tck_cnt : SP가 U로부터 tick을 모두 받은 갯수
- $K_{U\_TD}$ : U와 TD사이의 공통키
- $K_{U\_SP}$ : U와 SP사이의 공통키(세션키)
- amt_tck : tick당 금액
- data_tck : tick당 전송되는 데이터 량으로 바이트 수
- $P_U$, $S_U$ : U의 공개키와 비밀키쌍
- $g^{\alpha}$ : Diffie-Hellman 키교환 파라미터로 U의 공개키
- $\alpha$ : Diffie-Hellman 키교환 파라미터로 U의 비밀키
- $r_1$, $r_2$ : random number
- $SIG_A(m)$ : A의 메시지 m에 대한 서명
- $m_k$ : SP가 제공하는 서비스를 담은 메시지 m을 data_tck만큼의 블록으로 분할했을 때 k번째 메시지, 이때 $k \in \{1,2, ..., n\}$
- || : 접속(concatenation)

## 1. 제안하는 과금 프로토콜

**[단계1] 티켓 획득**

U가 TD에게 T를 요청하면 TD가 T를 생성하여 U에게 준다.

U->TD: $K_{U\_TD}(PMSI_U||t||r_1)$

TD->U: $K_{U\_TD}(r_1||T||tck_0||S_U)$,

$T=(T_{id}||TS||g^{\alpha}||P_U||tck_n||TD_{id}||SIG_{TD}(T_{id}||TS||g^{\alpha}||P_U||tck_n))$

U는 TD로부터 받은 티켓을 보관한다.

**[단계 2] 티켓 전달 및 상호인증**

아래 두 번째 메시지를 통해 U가 SP를 인증하게 되고 세 번째 메시지를 통해 SP가 U를 인증한 후 이 정보를 SP가 분쟁을 대비하여 보관한다.

U->SP: T

SP->U: $r_2||data\_tck||amt\_tck||H(K_{U\_SP}^{4})||r_2||SP_{id})$

U->SP:
$SIG_U(T_{id}||TS||K_{U\_SP}||r_2||SP_{id}||data\_tck||amt\_tck)$

**[단계 3] 서비스 제공**

SP가 U에게 첫 번째 메시지 블록을 전송하면 U는 이에 해당하는 tick 정보 $tck_{n-1}$ 값을 SP에게 전달한다. 이런 식으로 하여 주어진 메시지 블록이 k번째가 될 때까지 반복한다.

SP->U: $K_{U\_SP}(m_k)$

U->SP: $tck_{n-k}$

**[단계 4] 정산 및 과금**

SP가 지금까지 U로부터 받은 모든 정보를 자신의 서명정보와 더불어 TD에게 전달한다. TD는 이 정보들을 검토하여 해당 금액(amt_tck*tck_cnt)만큼 지불하고 U에게 이 금액을 청구한다.

SP->TD:
$T_{id}||SP_{id}||TS||data\_tck||amt\_tck||tck_v||tck\_cnt||$
$SIG_U(T_{id}||TS||K_{U\_SP}||r_2||SP_{id}||data\_tck||amt\_tck)||$
$SIG_{SP}(T_{id}||TS||data\_tck||amt\_tck||tck_v||tck\_cnt)$

위 정보들을 전달받은 TD는 U의 서명을 확인하고 $T_{id}$와 TS를 이용하여 티켓이 유효한지를 검사한다. 검사 결과 만일 이상이 없으면 data_tck와 amt_tck에 따라 지불 프로토콜을 수행한다. 그러나 이상이 있는 경우, U와 SP 각각이 가지고 있는 서명과 증거들을 이용하여 분쟁을 해결한다. 그 후 TD는 SP로부터 받은 위의 정보들을 증거로 보관하고 SP에게 지불한 금액을 U에게 청구한다.

---

3) Pederson[8]이 제안한 일명 Micropayment 방식으로 일방향 해쉬함수를 H, seed를 s라 할때, $H^1=H(s)$, $H^2=H(H^1)$, ..., $H^n=H(H^{n-1})$이다. 이때 $H^1$, $H^2$, ..., $H^n$ 각각을 tick이라 하며 티켓의 총액을 w라 할 때 일종의 w/n 값이다.

4) 세션키 $K_{U_SP}$는 다음과 같이 계산될 수 있다. 식 $y=g(\text{mod } p)$에서 만일 SP의 비밀키를 $\beta$, 공개키를 $g^{\beta}$라 한다면, Diffie-Hellman 키분배 방법에 의해 이 둘간의 세션키, $K_{U_SP}=g^{\alpha\beta}(\text{mod } p)$가 된다.

## 2. 프로토콜 분석

• **상호인증**: SP가 U에게 보낸 해쉬정보와 U가 SP에게 보낸 서명정보를 이용하여 상호인증이 가능하다.

• **부인방지**: 만일 U가 SP로부터 받은 메시지에 대해 부인한다면 SP가 U의 서명정보와 $tck_v$를 증거로 제시하고 그 반대의 경우는 TD가 SP로부터 최종단계에서 받은 서명정보를 증거로 제시함으로서 상호간의 분쟁을 해결할 수 있다.

• **티켓의 이중사용(double spending)**: U가 동일한 티켓을 다른 SP들에게 이용하려 할 경우, 티켓 내에 저장된 $T_{id}$와 TS를 TD가 확인함으로써 방지할 수 있다.

• **모바일 사용자에 대한 익명성**: TD의 방법에 근거하여, U의 실제 아이디가 아닌 임시 익명 아이디로 $PMSI_U$를 이용함으로 익명성이 제공된다.

• **모바일 사용자의 위치에 대한 프라이버시 보호**: 만일 SP나 NP(Network Provider) 혹은 외부의 제 3자가 U의 현 위치를 알고자 한다거나 위치를 추적하기 위해서는 GSM 환경을 예를 들어 VLR(Visite Location Register)이나 혹은 HLR(Home Location Register)내에 있는 U의 아이디를 알아내야 한다. 이 경우 U의 아이디를 알아내는 것은 어렵지 않다. 그러나 저장된 이 아이디는 U의 실제 아이디가 아닌 임시 익명 아이디이므로 사용자가 누구인지를 알 길이 없다. 또한 외부에서 수신 호 요청이 들어오더라도 U가 아닌 TD가 이 요청에 대해 응답을 하므로 위치에 대한 추적이 불가능하다. 보다 자세한 내용은 [5,6]을 참고하기 바라며 여기서는 생략하기로 한다.

• **만일 서비스 제공 단계에서 이미 정해놓은 tick을 모두 사용했을 경우**: 다음과 같은 재초기화 프로토콜을 추가로 수행함으로서 해결이 가능하다.

**[단계 3] 서비스 제공**

U가 기존에 TD가 생성한 것과는 다른 $tck_n'$와 $tck_0'$를 생성하여 아래 메시지를 SP에게 전송한 다음 기존 프로토콜을 계속 진행한다. 이때 기존의 $m_k$는 $m_k'$가 되고 $tck_{n-k}$는 $tck_{n-k}'$가 된다.

U->SP : $tck_n' \| T_{id} \| TS \| SIG_U(tck_n' \| T_{id} \| TS)$

**[단계 4] 정산 및 과금**

기존에 SP가 TD에게 보내는 메시지에 아래 메시지가 추가된다.

SP->TD: $TS \| tck_v' \| tck\_cnt' \| SIG_U(T_{id} \| TS \| tck_v' \| tck\_cnt')$

# IV. 결론

본 논문에서는 차세대 이동통신 환경에서 적용될 수 있는 부가가치 서비스를 위한 과금 프로토콜을 제안하였다. 제안한 방법은 아울러 기존 논문들에 비해 모바일 사용자에 대한 익명성과 현 위치 및 행적에 관한 노출을 피할 수 있다는 특징을 가지고 있다.

# 참고문헌


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

[2] H. Federrath, A. Jerichow, D. Kesdogan, and A. Pfitzmann, "Security in Public Mobile Communication Networks," Proc. of the IFIP TC6 International Workshop on Personal Wireless Communications, pp105-116, 1995.

[3] 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.

[4] 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.

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

[6] L. Buttyán and J. Hubaux, "Accountable and Anonymous Access to Services in Mobile Communication Systems," IEEE Symposium on Reliable Distributed Systems, pp. 384-389, 1999.

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

[8] T. P. Pederson, "Electronic Payments of Small Accounts," Security Protocols, LNCS, vol. 1361, pp. 59-68, 1997.