이동통신 환경에서 임시 익명 아이디를 이용한 위치 불추적 서비스와 지불 프로토콜에 관한 연구

(A Study on Location Untraceability Service and Payment Protocol using Temporary Pseudonym in Mobile Communication Environments)

김 순 석 † 김 성 권 ††
(Soon Seok Kim) (Sung Kwon Kim)

요 약 지금까지 많은 연구자들이 이동통신 환경과 관련하여 프라이버시 측면에서 모바일 이용자들의 현 위치와 행적의 노출에 대한 문제를 다루어 왔다[1,2,3,4,5,6,7,8]. 그 중에서도 Kesdogan과 Pfitzmann[3,6]은 이 문제를 해결하기 위해 TP(Temporary Pseudonym)라는 임시 익명 아이디를 이용한 효율적인 방법을 제안하였다. 그 후 Kesdogan 등은 [8]에서 이 방법을 더욱 개선하여 네트워크 제공자 측의 각종 공격 유형들과 이들로부터 모바일 이용자들을 보호할 수 있는 방법을 제안한 바 있다. 그러나 그들이 제안한 공격 유형들 가운데 특히, 네트워크 제공자의 능동적인 공격에 대비한 방법은, 새로운 또 하나의 장비(이를 Reachability Manager라 부른다)를 시스템에 부착하는 방법으로, 실질적이라기 보다는 대안에 가까우며 그 방법에 대한 기술이 구체적이지가 않다. 게다가 이것은 또 다른 비용과 부담을 요구한다. 따라서 본 논문에서는 이러한 추가적인 장비가 없이 기존의 환경에서 네트워크 제공자의 능동적인 공격에 대비하는 실질적인 방법을 제안한다. 제안한 방법의 기본 아이디어는 모바일 이용자, 그리고 이용자와 네트워크 제공자가 신뢰하는 제 3자(이를 Trust Device라 부른다) 이 둘만이 알고 있는 비밀 정보를 네트워크 제공자를 통해 교환함으로써 내부 이용자인 네트워크 제공자 측의 부정을 방지하는데 있다. 아울러 제안한 방법을 응용한 새로운 지불 프로토콜을 소개하고자 한다.

국문키워드 : 임시익명아이디, 위치불추적서비스, 익명성

Abstract In related to mobile communication environment, many researchers have studied problems concerning current locations of mobile users and exposure of their movements in the privacy aspect so far[1,2,3,4,5,7,8,9]. Among them, Kesdogan and Pfitzmann[3,6] proposed effective solutions using temporary pseudonym identification, called TP(Temporary Pseudonym) to solve them. After that, Kesdogan et al. proposed an improved method protecting mobile users from some types of attacks of network providers in [8]. However, among their methods, in particular the method, attaching the other new device (so-called Reachability Manager) to system against active attack of network providers, is alterative rather than practical and is not clear. Moreover, it requires the other cost and overhead. Therefore we propose a practical method against active attack of network providers without attaching new device in original environments. The basic idea of proposed method is to protect a fraud act of network provider as a inside user by exchanging a secret information, which only users and network providers know, via network provider between mobile users and the trusted third party (so-called Trust Device). Moreover, we introduce a new payment protocol which applied our method.

key word : temporary pseudonym identity, location untraceability service, anonymity

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

† 비 회 원 : 중앙대학교 컴퓨터공학과
sskim@alg.cse.cau.ac.kr
†† 종신회원 : 중앙대학교 컴퓨터공학과 교수
skkim@cau.ac.kr

논문접수 : 2001년 12월 31일
심사완료 : 2002년 12월 18일

1. 서 론

IMT-2000(International Mobile Telecommunication -2000), 일명 FPLMTS(Future Public Land Mobile Telecommunications System)와 같은 제 3세대 무선 이동통신 시스템뿐만 아니라, 여기에 기존의 무선 인터넷 서비스를 통합 지원하게 될 제 4세대로 불리는 무선 멀티미디어 서비스 등은 'any service, anywhere, any time'이란 말처럼 가입자가 언제든지 타 지역으로 이동할 수 있는 이동성(mobility)과 통신 네트워크에 무선으로 접속한다는 특수성을 지니고 있다. 현재 이러한 3세대 이동통신 시스템의 등장과 더불어 기존의 디지털 셀룰러 폰이나 PCS(Personal Communication Service)에서 고려되지 않은 여러 문제점들과 보안 이슈들이 나타나고 있다[1,2].

이동통신 환경에서의 보안 요구사항은 크게 기밀성(confidentiality), 무결성(integrity), 그리고 가용성(availability), 이 세 가지로 나뉘어 볼 수 있다[1]. 그 중 기밀성은 다시 컨텐트(content), location(위치), 그리고 수신자(addressee)에 대한 프라이버시 보장으로 분류되며 무결성은 컨텐트, 수신자, 그리고 이용(usage)에 대한 무결성 보장으로 나눌 수 있다. 여기서 가용성은 메시지를 주고 받고자 하는 양측사이에는 언제나 통신이 가능해야 한다는 것이다. 특히, 이들 가운데 기밀성과 무결성에 대해 모바일 이용자의 프라이버시 측면에서 좀더 엄밀히 살펴보면 크게 다음과 같은 네 가지의 카테고리로 분류해 볼 수 있다.

- **위치 프라이버시(location privacy)**
  모바일 이용자의 현 위치나 혹은 이동한 위치들에 대한 내역 정보가 내부 이용자인 네트워크 제공자(Network provider라 하며 이하 간단히 NP라 부른다)를 비롯하여 비인가된 자들로부터 추적이 불가능해야 한다. 그러나 이러한 위치에 대한 정보를 인가된 이용자들은 효율적으로 이용할 수 있어야 한다.
- **신분에 대한 프라이버시(identification privacy)**
  모바일 이용자에 대한 신분이 비인가된 사용자들에게 노출되지 않아야 한다는 것으로, 흔히 이용자에 대한 익명성(anonymity)을 말한다.
- **컨텐트 프라이버시(content privacy)**
  메시지의 내용이 비인가된 이용자들로부터 보호되어야 한다.
- **인증(authentication)**
  메시지를 주고받으려는 양측이 스스로 자신의 신분이 올바름을 상대방에게 증명할 수 있어야 한다.

현재까지 이러한 각종 요구사항들에 대한 대응책들이 Pfitzmann과 Federrath[2,3,4,5,6]를 비롯한 몇몇 연구자들에 의해 연구되고 있다[1,7,8]. 본 논문에서는 이러한 여러 보안 요구사항들 가운데 특히, 모바일 이용자의 현재 위치와 행적의 노출 즉, 위치 프라이버시 보호에 대한 문제를 다루고자 한다.

유럽에서 현재 대표적으로 이용되고 있는 제 2세대 이동통신 시스템 표준인 GSM(Global System for Mobile communications)[9]의 경우, 모바일 이용자의 송수신호(call) 요청에 대한 서비스를 위해 HLR(Home Location Register)과 VLR(Visited Location Register)이라는 데이타베이스를 이용하여 일정 시간 간격으로 이용자의 아이디와 현 위치에 대한 정보를 저장하고 있다. 따라서 이 정보를 이용할 경우 NP측에서는 언제든지 이용자에 대한 위치를 추적할 수 있을 뿐만 아니라 이용자의 행적에 대한 프로파일을 생성할 수 있으며 자칫 범죄에도 악용될 수 있는 가능성이 있다. 이는 특히 이용자의 프라이버시 보장측면에서 보호되어야 한다. 기존의 GSM 네트워크에 대한 부연 설명은 2장에서 다루기로 한다.

모바일 이용자에 대한 위치 프라이버시 보호 문제와 관련하여 현재까지 브로드캐스트(broadcast)[7], MIXes [3,5], 그리고 TP(Temporary Pseudonym, 이하 간단히 TP라 부른다)[3,6,8] 방법 등 여러 가지 해결책들이 나와 있다. 이들 중 각 방법들과 관련하여 서로간에 장단점들이 있지만 보다 상세한 설명한 2장에서 다루기로 하고 본 논문에서는 TP 방법에 대해 좀더 논의해보고자 한다.

TP방법은 1996년 Pfitzmann과 Kesdogan 등[3,6]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 보호하는데 있다. 또한 NP를 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 NP측에서 TD에게 이용자에 해당하는 PMSI를 요청함으로서 이 PMSI를 이용하여 NP가 이용자와 통화연결을 시켜주는 방법이다. 따라서 NP의 경우 모바일 이용자에 대한 PMSI는 알지만 실제 아이디

가 무엇인지를 모르기 때문에 이용자의 신분을 알 수가 없다. 또한 내부적으로 PMSI값은 주기적으로 변화되어 앞서 말한 HLR과 VLR에 등록되기 때문에 NP측에서 PMSI를 이용한 위치 추적이 어렵다.

이에 반해 GSM의 경우 IMSI(Iternational 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 NP측에서는 실제 모바일 이용자가 누구인지를 알고있기 때문에 이용자의 NP에 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 NP가 만일 사용자의 현 위치를 추적하기 위해 악의를 가지고 공격을 시도할 경우 몇 가지 문제점이 발생한다. Kesdogan 등은 이 문제점에 대해 그의 논문 [8]에서 NP의 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 좀더 적극적인 공격으로 공격자인 NP가 이용자의 위치 정보를 알기 위해 TD에 주기적으로 PMSI를 요청하려는 시도를 말한다.

Kesdogan 등[8]은 이러한 능동적인 공격과 관련하여 한가지 대안으로 Reachability Manager라는 추가적인 하드웨어 장비를 TD에 두어 PMSI를 NP에게 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 NP의 요청이 정당한지를 결정할 수 있는지 그 부분이 명확하지 않다. 또한 현재까지 나와있는 RM의 방법은 이를 고려하고 있지 않다. 따라서 본 논문에서는 RM과 같은 새로운 하드웨어를 추가로 설치한다든가 혹은 기존의 이동 통신 아키텍처에 수정을 가하지 않으면서 위의 능동적인 공격에 대비한 실질적이고도 효율적인 방법을 제안하고자 한다. 아울러 제안한 방법을 응용한 새로운 지불 프로토콜을 소개하고자 한다.

본 논문의 구성을 요약하면 아래와 같다. 먼저 2장에서 GSM 네트워크와 기존의 위치 프라이버시 보호와 관련한 방법들, 그리고 그들의 문제점들을 각각 살펴보고, 3장에서 이들 방법들 가운데 특히, TP 방법의 문제점을 개선한 새로운 프로토콜을 제안한 후, 4장에서 제안한 방법을 응용하여 모바일 이용자가 부가가치서비스 제공자, 일명 VASP(Value Added Service Provider)로부터 제공되는 컨텐츠에 대해 유료 서비스를 받고자 할 경우 그 활용방안에 대해 소개한 다음, 5장을 끝으로 결론에 대해 논하고자 한다.

2. 관련 연구

유럽의 제2세대 모바일 폰으로 이동통신 표준인 GSM 네트워크[9]는 아래 그림 1과 같이 그 영역이 계층적으로 이루어져 있는데, 그중 최상위에 몇몇 MSC (Mobile Switching Center) 영역이 있으며, 그 아래 각각 BSC(Base Station Controller)에 의해 관리되는 몇개의 LA(Location Area)가 있다. 또한 각 LA는 최하위

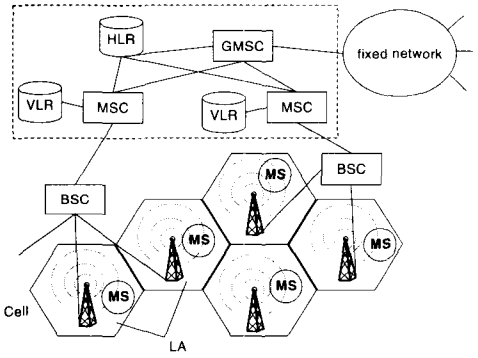

그림 1 GSM 네트워크

에 몇몇 셀(cell)들로 구성되어 있으며 이 셀 내에 모바일 이용자 즉, MS(Mobile Station)가 존재한다. 여기서 MS는 원래 모바일 이용자의 신분과 기타 개인 정보 등이 담긴 모듈과 이동 단말기 즉, 모바일 폰을 포함하여 일컫는 말인데 본 논문에서는 간단히 모바일 이용자를 대신해서 사용하기로 한다. 또한 각 셀 내에 각각의 MS들은 BTS(Base Transceiver Station)에 의해 BSC와 주어진 주파수 스펙트럼 내에 라디오파를 송수신하고 있다. 이러한 계층 구조에서 모바일 사용자에 대한 위치 관리는 크게 중앙 데이타베이스, HLR 그리고 VLR 이 세 구성요소에 의해 이루어진다. 여기서 HLR은 각 모바일 이용자들에 대한 현 MSC 영역들을, 그리고 VLR은 각 MSC 영역 내에 현 LA들을 저장하고 있다.

이러한 GSM 네트워크에서 모바일 이용자 즉, MS의 이동성에 대한 위치 관리 기법은 주로 아래 세 가지 과

정으로 분류하고 있다.

- **위치 갱신**(LU, Location Update) : MS가 현 LA에서 다른 LA로 로밍 할 때마다 위치정보를 HLR과 해당 VLR들에 갱신하는 과정으로 만약 두 LA가 같은 MSC의 제어 하에 있을 경우는 지역적으로 해당 VLR만을 갱신한다. 그러나 다른 제어 하에 있을 경우는 이전 VLR 내에 저장된 위치정보는 삭제되고 새로 이동한 MSC 내에 있는 VLR에 새로이 이용자에 대한 위치정보가 생성된다.
- **이동 착호 설정**(MT, Mobile Terminated calls setup) : 외부 이용자로부터 MS로의 호 설정으로 만약 외부 이용자가 기존의 PSTN(Public Switched Tele phone Network)망으로부터 GSM 네트워크로 통화를 요청할 경우에 이 요청은 GSM 측의 GMSC(Gateway MSC)에 의해 받아들여진다. 이때 GMSC는 현 MS가 위치한 MSC로 통화 요청을 연결하기위해 HLR과 해당 VLR에 위치정보(예를 들어, 현 MS가 어느 LA에 있는지 대한 정보)를 요청한 다음 그곳 MSC로 요청을 넘긴다. 그러면 MSC는 이 요청을 받아 해당 MS 그리고 BTS와의 통화 연결을 설정한다.
- **이동 발호 설정**(MO, Mobile Originated calls setup) : MS로부터 외부 이용자로의 호 연결 설정으로 MS가 BTS와 BSC를 통해 외부 이용자로의 통화를 요청하면 해당 MSC내에 있는 VLR을 통해 MS로의 라우팅 정보가 GMSC로 전달되고 이 정보를 받은 GMSC가 해당되는 외부 이용자로의 통화 연결을 설정한다.

2.1 위치 불추적 서비스와 관련한 기존 연구들

위치 불추적 서비스와 관련하여 현재까지 제안되고 있는 해결책들은 크게 브로드캐스트, MIXes, 그리고 TP 방법으로 분류해 볼 수 있다. 본 장에서는 이들 각각에 대해 살펴보고 아울러 이들 가운데 TP 방법과 관련하여 그 공격법과 문제점들에 대해 살펴보고자 한다.

2.1.1 브로드캐스트 방법

이 방법은 위치 프라이버시를 제공하는 가장 간단한 방법으로, 외부 송신자가 전달한 메시지를 수신자가 위치하고 있는 LA내에 있는 임의의 모든 MS들에게 브로드캐스트하는 것을 말한다[7]. 이 경우 만일 MS가 메시지를 전달받는 수신자일 경우 악의를 띤 제 3자는 실제 메시지가 어느 MS로 전달되는 지를 알 수가 없다. 따라서 제 3자로부터 MS에 대한 위치 프라이버시는 보장된다. 그러나 만일 MS가 메시지를 송신하는 송신자가 될 경우 (이 경우는 브로드캐스트가 일어나지 않는다) 악의를 띤 제 3자는 도청이라든가 그밖에 NP와의 결탁 등을 통해 MS의 현 위치와 행적이 노출될 수 있다. 이때 NP는 MS의 송수신 여부를 떠나 언제든지 마음만 먹으면 MS의 위치를 파악할 수 있다. 또한 이 방법은 간단하기는 하지만 NP측에서 전송에 따른 부담이 많아 현실적으로 적용하기는 힘들다.

2.1.2 MIXes

MIXes의 개념은 1981년 Chaum[10]에 의해 처음으로 소개되었다. Chaum의 개념은 원래 추적 불가능한 E-Mail 송수신을 위해 개발되었지만 곧바로 응용되지 못하다가 1991년 Pfitzmann[3]에 의해 ISDN망에 적용되었고 그 후 1997년 역시 Pfitzmann[5]에 의해 이동통신망에 적용될 수 있도록 변형되었다.

MIXes의 기본 아이디어는 다음과 같다. 메시지를 주고받는 송신자와 수신자 사이에 일종의 라우터 역할을 수행하는 일련의 MIX들(이를 MIX 체인이라 부른다)을 두고 각 MIX들을 통해 메시지를 암호화하여 통신 패스를 인코딩(encoding)함으로써 악의를 띤 제 3자로부터 송수신자 사이에 위치 프라이버시를 제공하는 메커니즘이다. 이때 각 MIX들은 암호화를 위하여 공개키와 비밀키의 쌍을 갖고 있는데, 예를 들어 MIX 체인에 속한 t+1개의 각 MIX들을 M_1, M_2, .., M_{t+1}, 이들의 공개키들을 각각 $K_{M_1}, K_{M_2}, \ldots, K_{M_{t+1}}$, b를 메시지 레이블(label), m을 메시지, 그리고 s를 메시지 수신자의 아이디라 하자. 이때 송신자는 메시지 m을 아래와 같이 암호화하여 M1에게 전달한다.

$$K_{M_1}(K_{M_2}(K_{M_3}(..K_{M_{t+1}}(b,m,s)..,M_4),M_3),M_2)$$

위의 메시지를 전달받은 M_1은 자신의 비밀키를 이용하여 위 메시지를 복호화 한 다음 나머지 메시지 $K_{M_2}(K_{M_3}(..K_{M_{t+1}}(b,m,s)..,M_4),M_3)$를 이웃한 다음 MIX인 M_2에게 전달한다. 이런 방법으로 최종 MIX인 M_{t+1}은 메시지 b, m, s를 얻게 되고 이 메시지를 수신자에게 전달하는 방법이다.

이때 불법적인 제 3자로부터의 공격을 막기 위해 전 과정에 걸쳐 메시지에 랜덤 데이타를 패딩(padding)하거나, 그밖에 입력 메시지와 출력메시지 간의 관련성을 가지고 메시지를 추적하는 공격에 대비하여 여러 송신자들로부터 메시지들의 순서를 재배치(reordering)한다. 또한 t개의 MIX들이 공격자와 공모한다하더라도 최소한 남아있는 한 MIX가 정직하다면 여전히 전송되는 메시지를 추적할 수 없다. 이 과정에 대한 자세한 설명은 [3,5]를 참조하기 바란다.

그러나 이 방법은 다음과 같은 단점들을 내포하고 있

다. 첫째, 메시지를 보내고자하는 송신자에게 많은 부하가 따른다. 즉, 송신자는 각 MIX 서버들의 공개키를 알고 있어야 하며 각 MIX의 수만큼 공개키 연산을 수행해야 한다. 일반적으로 이 연산에 필요한 입력의 길이는 512비트 이상으로 알려져 있다[8]. 둘째, 만일 각 MIX들 가운데 한 MIX가 고장이 났을 경우 메시지 전송은 일단 중단될 수밖에 없다. 왜냐하면 각 MIX들의 비밀키는 오직 자신만이 알고있기 때문이다. 셋째, 이 방법을 현 이동통신 환경에 적용할 경우 네트워크의 구조적인 면에서 많은 부담이 따른다. 넷째, 드문 경우지만 MIX 체인 내에 있는 모든 MIX 들이 결탁할 경우 더 이상의 위치 프라이버시는 기대할 수 없으며 끝으로, 이 방법은 악의를 띤 제 3자로부터의 위치 프라이버시는 보장되나 여전히 네트워크 내부에 있는 NP가 악의를 띠는 경우 MS의 위치는 언제든 파악될 수가 있다. 왜냐하면 MIX들을 통해 송수신이 일어나지만 최종 MS로(부터)의 연결은 내부 이용자인 NP에 의해 이루어지기 때문이다. 따라서, 이 방법을 현 이동 통신 환경에 응용하기 위해서는 많은 수정이 필요하다.

2.1.3 TP 방법

TP 방법은 앞서 서론에서 언급한 바와 같이 1996년 Pfitzmann과 Kesdogan 등[3,6]이 제안한 개념으로, 기본 아이디어는 모바일 이용자의 실제 아이디가 아닌 PMSI를 이용하여 통신함으로써 이용자의 신분에 대한 프라이버시를 보호하고 NP를 비롯한 제 3자로부터 실제 아이디에 대한 노출을 피하기 위해 각 가정이나 그 밖에 안전한 장소의 컴퓨터 즉, TD내에 실제 아이디와 이에 대응되는 PMSI를 저장해 둠으로써 이용자에 대한 위치 프라이버시를 추가로 제공하는 메커니즘이다. 즉, 외부 이용자로부터 수신 호 요청시 NP측에서 TD에게 모바일 이용자에 해당하는 PMSI를 요청함으로서 이 PMSI를 이용하여 NP가 이용자와 통화연결을 시켜주는 방법이다. 따라서 NP의 경우 모바일 이용자에 대한 PMSI는 알지만 실제 아이디가 무엇인지를 모르기 때문에 이용자의 신분을 알 수가 없다.

TD는 원래 처음 제안할 당시에는 HPC(Home Personal Computer)라 하여 프라이버시를 위한 민감한 데이타들(예를 들어, 이용자의 실제 아이디를 포함하여 이용자의 비밀키 등의 정보들)을 가정에 있는 PC에 저장하던 개념이었으나 이후에 TD라 하여 물리적으로 가용성이 보장되는 제 3의 안전한 장소라는 개념으로 그 명칭이 바뀌었다.

본 절에서는 앞서 언급한 GSM 네트워크를 기반으로 그 개념을 설명하고자 한다. 먼저 GSM 네트워크를 기반으로 TP 방법을 적용한 아키텍처는 그림 2와 같다.

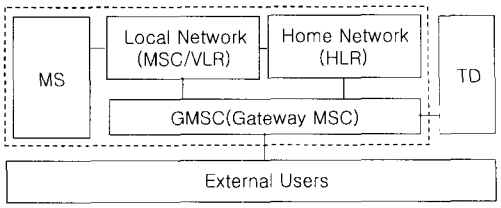

그림 2 TP 방법을 적용한 이동통신 아키텍처

위 아키텍처를 기반으로 앞서 언급한 세 가지 위치관리 기법을 TP 방법에 적용하면 아래와 같이 설명될 수 있다.

■ **위치 갱신**

TP 방법을 기반으로 한 위치 갱신 과정은 네트워크 데이타베이스(HLR과 VLR들)내에 MS의 현 위치 정보를 계속해서 갱신하는 역할을 수행하는 것으로 그림 3과 같이 나타낼 수 있다.

여기서 ID_{MS}는 이전에 설명한 MS의 PMSI로 PRG(K_{MS},t_i)로 생성됨을 알 수 있다. 이때 PRG는 유사 난수 발생기(Pseudo Random Generator), K_{MS}는 TD와 MS가 사전에 협의하여 공유하고 있는 비밀키, 그리고 t_i는 현재 시간으로 이 값 역시 양측이 사전에 협의한 일정 주기에 따라 동기화가 일어난다. 즉, 일정 시간 간격마다 미리 정해진 시간 ti에 따라 MS와 TD가 동시에 ID_{MS}를 생성하게 되며 MS가 이전 LA에서 새로운 LA로 진입시 이 값을 각각 VLR과 HLR에 등록한다.

■ **이동 착호 설정**

이 과정은 아래 그림 4에서 보는 바와 같이 외부 이용자가 MS에게 통화 요청시 이에 대한 호를 설정해주는 과정이다. 먼저 외부 이용자는 MS와의 통화를 위해 IAM(*Initial Address Mobile*)과 *MSISDN*(*Mobile Subscriber Integrated Service Digital Network Number*) 메시지를 GMSC에게 전달한다. 여기서 *IAM* 메시지는 요구되는 서비스의 종류라든가 라우팅 정보를 포함하고 있으며 *MSISDN*은 MS의 고유 번호로 GMSC가 이것을 이용하여 MS의 위치를 파악하는데 이용한다. GMSC는 *MSISDN*을 이용하여 TD에게 PMSI 즉, ID_{MS}를 요청한다. 이 ID_{MS}를 이용하여 GMSC는 HLR에 접근하게되고 또한, 어느 VLR에 속해있는지를 알아내어 외부 이용자의 착호 요청을 해당 VLR이 있는 MSC로 전송한다. 이때 MSC는 자신에 속한 VLR을 이용, MS의 LA 정보를 얻어 그곳으로 요청을 보내게 되고 이를 MS가 수신하는 과정이다. 따라서 이 방법을

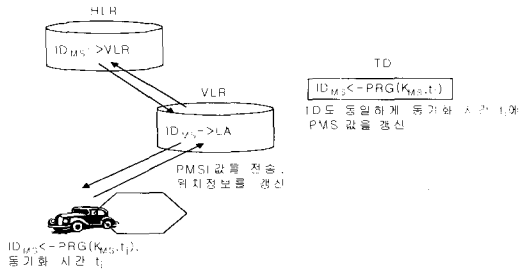

그림 3 TP방법을 이용한 위치 갱신

이용할 경우, 착호가 설정되기 전까지는 제 3자는 물론 이러한 호요청을 설정해준 NP조차도 MS가 누구이며 어느 위치에 있는지를 모른다. 심지어 착호가 설정된 직후에라도 MS의 현 위치는 알 수 있지만 그가 정확히 누구인지는 모른다. 뿐만 아니라, PMSI 값이 일정 주기마다 갱신되어 HLR과 VLR에 등록되기 때문에 착호가 설정된 직후의 PMSI를 안다하더라도 향후에 그 위치를 계속해서 추적하기가 어렵다.

그러나 MS는 항상 머물러있지 않고 이동한다는 특수성을 지니고 있다. 예를 들어, 시속 100KM 이상으로 달리는 차안에서 그 시간에 맞춰 ID_{MS}를 갱신하기는 힘들 뿐만 아니라 전체 이용자들이 한꺼번에 갱신하려 할 경우 TD측에서 이를 수용할만한 메모리 한계도 생각해야 한다. 따라서 동기화 시간을 지수적으로 분배한다든지 하여 부하를 줄일 필요가 있다. 실제로 Kesdogan[8]은 이러한 단점을 들어 그 공격법과 대안을 소개하고 있다. 이에 대한 내용은 다음절에서 논하기로 한다.

■ **이동 발호 설정**

이 과정은 이전의 이동 착호 설정과는 반대 과정으로 아래 그림 5에서 보는 바와 같이 비교적 간단하다. MS가 자신의 PMSI 즉, IDMS를 이용하여 발호 요청을 보내면 이를 MSC가 받아 VLR을 이용하여 GMSC에게 전달하게 되고 이를 GMSC가 외부 이용자에게 보냄으로써 발호를 설정하는 과정이다. 이 과정은 기존 GSM 네트워크에서 사용하던 TMSI 대신 PMSI를 사용한다는 것 외에는 기본적으로 GSM 방식과 동일하다.

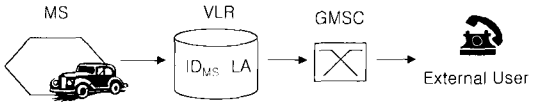

그림 5 TP 방법을 이용한 이동 발호 설정 과정

지금까지 설명한 TP 방법은 앞서 설명한 방법들에 비해 계산적인 측면에서 효율적이기 때문에 이동통신에 응용하기에 적합하다. 왜냐하면 브로드캐스트 방법의 경우 송신자로부터의 메시지를 모든 LA 내에 있는 MS들에게 전달해야하며, MIXes의 경우 또한 각 MIX 서버 측에서 송수신 메시지에 대해 추가적인 공개키 암호화 연산을 수행해야 하는 추가적인 부담이 따르기 때문이다. 그러나 TP 방법은 효율성은 있지만 TD가 만일 고장이 날 경우 이에 따른 대처 방안이 없다. 따라서 이 방법은 TD가 물리적으로 안전하며 언제든 이용할 수 있다는 가정이 필요하다. 본 논문에서도 이를 가정한다.

2.2 TP 방법에 대한 알려진 공격 유형들

TP 방법에 대한 안전성은 임시 익명 아이디인 PMSI와 물리적으로 안전한 TD에 기반하고 있으며, 일반적으로 제 3자의 공격에 대해서는 안전하다고 알려진 바 있다. 그러나 NP가 만일 악의를 가지고 공격을 시도할 경우 몇 가지 문제점이 발생한다. Kesdogan 등은 이 문제점에 대해 그의 논문 [8]에서 NP의 공격 유형을 아래와 같이 크게 수동적인 공격(passive attack)과 능동적인 공격(active attack)으로 나누어 그 각각에 대한 해결 방법을 제안한 바 있다.

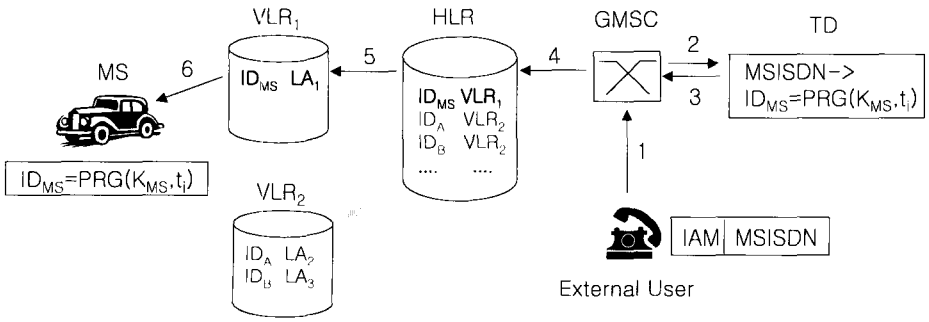

그림 4 TP 방법을 이용한 이동 착호 설정 과정

2.2.1 수동적인 공격

이동 통신 시스템 내부에 있는 수동적인 공격자가 네트워크 상에 데이타베이스인 HLR과 VLR을 지속적으로 관찰함으로써 MS에 대한 위치 정보를 얻으려는 시도를 말한다. 예를 들어, 외부 이용자가 MS에게 착호 요청을 할 경우 호 요청은 TD를 통해 MS의 PMSI가 드러나게 되고 이를 MS에게 연결하는 과정에서 현 위치도 드러나게 된다. 즉, MS의 PMSI와 위치가 링크된다. 이때부터 공격자는 HLR과 VLR을 지속적으로 관찰함으로써 해당 MS의 PMSI가 새로이 갱신되는 동기화 시간을 파악하고 위치 이동에 대한 추적을 시작한다. 따라서 만일 공격자가 장 시간동안 특정 MS의 위치 정보를 관찰할 경우 MS가 실제 누구인지는 몰라도 그동안 어느 곳을 다녔는지에 대한 행적 프로파일(이를 movement profile이라 부른다)을 만들 수 있다. 또한 만일 NP가 TD와 공모를 한다면 실제 누구인지도 드러나게 된다. 이러한 공격에 대비하여 Kesdogan은 다음과 같은 대안들을 제시하고 있다.

■ **클래스를 이용한 PMSI 변화**

대개 MS는 외부 이용자로부터 송수신을 위해 자신의 PMSI를 TD와의 동기화 시간에 맞춰 주기적으로 갱신하여 VLR에 등록한다.(그림 3 참조) 여기서 제안된 방법은 내부 공격자로부터 HLR과 VLR의 지속적인 관찰을 막기 위해 여러 명의 MS가 하나의 클래스를 형성하여 동시에 PMSI를 갱신함으로써 매번 PMSI가 변화되는 동기화 시간을 무의미하게 만드는 것이다. 이때 각 MS들 스스로가 자신이 속할 클래스를 선택하며 그 클래스에 속한 모든 멤버들은 되도록 여러 LA에 걸쳐 골고루 분포되도록 조정한다. 그리고 동기화 시간은 각 클래스마다 예를 들어, 20초, 1분, 20분 주기 등으로 정할 수 있다. 따라서 이 경우 각 클래스에 속한 MS들의 PMSI가 동시에 바뀌므로 NP측에서는 어느 MS가 자신이 알고자 하는 해당 MS인가를 식별하기가 어렵다.

■ **분산 TP 방법**

이 방법은 앞서 말한 NP와 TD간의 공모를 막기 위한 것으로 기본 아이디어는 TD를 n개로 분할하여 NP로부터 PMSI 요청시 단일 TD가 아닌 n개의 TD가 협력하여 PMSI를 제공하는 방법이다. 그림 6은 예를 들어, 4개의 TD로 분할한 것으로서 GMSC로부터 PMSI 요청에 대해 각 TD의 PMSI를 XOR한 결과를 실제 PMSI로 제공하고 있다. 즉 $PMSI = pmsi_1 \oplus pmsi_2 \oplus pmsi_3 \oplus pmsi_4$이며 ⊕는 XOR연산이다. 이 방법은 n개의 TD 가운데 적어도 한 개의 TD가 정직하다면 NP와의 공모를 막을 수 있다. 그러나 이 경우 MS 또한 각 TD에 대한 부분 $pmsi$ 값들을 생성할 수 있어야 하며 이를 위해 MS는 각 TD들과의 비밀키를 하나씩 가지고 있어야 한다. 따라서 이 방법을 적용할 경우 TD와 NP간의 공모는 막을 수 있지만 PMSI 값을 생성하는데 있어 MS측에 약간의 부담이 따른다는 단점이 있다.

2.2.2 능동적인 공격

이 공격은 수동적인 공격에 비해 좀더 적극적인 공격으로 공격자인 NP가 MS의 위치 정보를 알기 위해 TD에 주기적으로 PMSI를 요청하려는 시도를 말한다. 이 경우 TD는 주기적으로 PMSI를 알려주게 되고 앞서 말한 HLR과 VLR을 주기적으로 관찰함으로써 좀더 손쉽게 MS의 위치정보와 행적을 파악할 수 있다. 이 공격은 이전의 수동적인 공격에 비해 훨씬 적극적인 공격으로, 물론 TD내에 NP로부터 모든 요청들에 대한 로그파일을 유지함으로써 그 공격에 대한 시도를 감지할 수 있다. 그러나 NP측에서 로그파일은 TD가 위조 가능하다고 생각할 수 있기 때문에 공격을 시도했다는 정당한 증거가 되질 못한다.

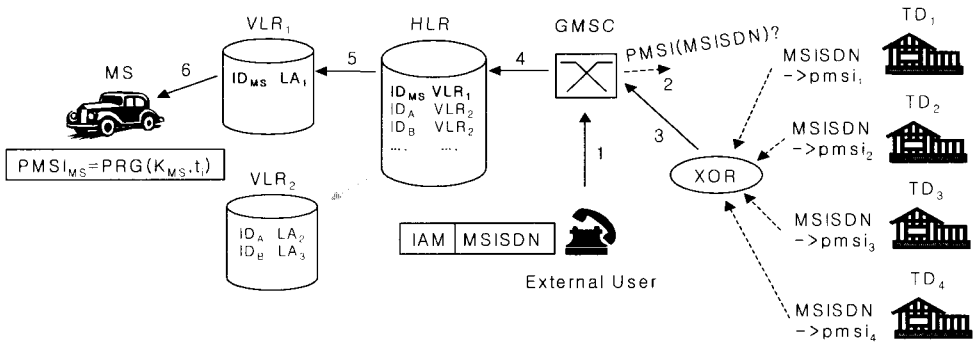

그림 6 분산 TP 방법을 이용한 이동 착호 과정

2.3 능동적인 공격에 대한 문제점

Kesdogan 등[8]은 위 2.2.2에서 언급한 능동적인 공격과 관련하여 한가지 대안으로 단지 Reachability Manager(이하 간단히 RM이라 부른다)를 TD에 두어 PMSI를 NP에게 알려주는 것이 정당한 지를 검토한 후에 요청을 받아들일 것인지 아닌지를 결정하도록 언급하고 있다. 여기서 RM은 유럽에서 GSM 환경을 기반으로 Reichenbach 등[11]이 제안한 방법이다. RM은 개인휴대단말기인 PDA(Personal Digital Assistant)로 구현된 일종의 도우미역할을 수행하는 장치로 원래 MS에 휴대용으로 부착하여 수행된다. 먼저 송신자가 수신자인 MS와 통화를 위해 각종 정보(예를 들어, 송신자 개인 정보라든가 통화 주제나 목적 등의 정보)와 더불어 호 요청을 보내면 RM은 자신의 PDA를 통해 이에 대한 정보를 MS에게 디스플레이 한다. MS는 디스플레이된 정보를 보고 호 요청을 받아들일 것인지 아닌지를 결정하고 그 여부에 따라 RM이 수신 호를 설정 또는 중단하게 된다.

그러나 Kesdogan 등의 제안은 실질적인 대안이라기보다는 RM을 이용하여 해결할 수도 있다는 언급만 있을 뿐 구체적으로 어떠한 방식으로 공격을 막을 것인지에 대한 해결책은 제시된 바가 없다. 즉, RM이 어떻게 NP의 요청이 정당한지를 결정할 수 있는지 그 부분이 명확하지 않다. 또한 현재까지 나와있는 RM은 이러한 기능이 내재되어 있지 않다. 뿐만 아니라 이러한 공격을 막기 위해 RM을 이용할 경우 이에 따른 새로운 하드웨어를 추가로 설치해야 한다는 비용 부담이 따르며, 그만큼 통신 효율 면에서 적잖은 오버헤드가 발생한다. 따라서 본 논문에서는 새로운 하드웨어를 추가로 설치한다든가 혹은 기존의 이동 통신 아키텍처에 수정을 가하지 않으면서 내부 이용자인 NP로부터의 능동적인 공격에 대비한 실질적이고도 효율적인 방법을 제안한다.

3. TP 방법에 대한 새로운 제안

앞서 Kesdogan이 제시한 능동적인 공격에 대한 문제는 외부 이용자가 통화 요청을 하지도 않았는데도 불구하고 정당한 이유없이 NP가 주기적으로 TD에 PMSI를 요청하는데 있다. 따라서 이에 대한 해결책으로 외부 이용자로부터 호 요청이 올 때만 NP에게 PMSI를 알려주는 방법을 생각해 볼 수 있다. 본 논문에서는 이 방법과 관련하여 Kesdogan이 언급한 RM을 이용하지 않으면서 NP로부터 능동적인 공격에 대처할 수 있는 새로운 프로토콜을 제안하고자 한다.

제안하는 프로토콜의 기본 아이디어는 악의를 띤 NP로부터 주기적인 요청을 피하기 위해 MS와 TD만이 알 수 있는 비밀 정보 S를 서로간에 교환하여 실제 요청이 있었는지를 확인하는데 있다. 이때 S는 NP가 TD에게 PMSI를 요청한 횟수로 NP가 이 값을 위변조 할 수 없도록 암호화하여 MS에게 전달한다.

또한 제안하는 프로토콜에 대한 기본 시나리오는 다음과 같이 요약될 수 있다(그림 7 참조). 먼저 1)외부 이용자가 MS와의 통화를 위해 호 요청을 보내면 2)NP측인 GMSC가 MS로 연결하기 위해 TD에게 PMSI를 요청한다. 3)TD는 PMSI와 S를 생성하여 GMSC를 통해 MS에게 보낸다. 4)MS는 S를 확인하고 이상이 없으면 증거로 보관한다. 5) 일정 시간 reg_t가 지나 MS는 보관하고 있는 증거를 생성하여 TD에게 보내고 6)TD는 이 증거를 검토하여 NP로부터 불법적인 시도가 있었는지를 확인한다. 이때 변수 reg_t는 MS가 TD와 협의하여 평소 통화량이나 단말기 용량 등에 따라 조정하거나 혹은 일주일 혹은 한달 단위의 주기가 될 수 있다.

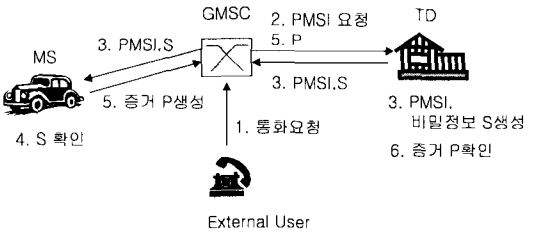

그림 7 제안하는 프로토콜의 기본 시나리오

3.1 프로토콜 제안

본 프로토콜 제안에서 TD는 가용성이 보장되는 신뢰성 있는 제 3의 기관이라고 가정한다. 먼저 제안하는 프로토콜에 대한 표기는 다음과 같다.

[표 기]

- CNT : NP측인 GMSC로부터 TD가 실제 요청을 받은 횟수. 이때 초기값은 0이며 요청이 있을 때마다 1씩 증가한다.
- cur_t : TD가 메시지를 보낼 당시의 시간. 만일 PKI(Public Key Infrastructure) 기반의 환경일 경우, 이 값은 TD가 서명한 타임스탬프(timestamp)가 될 수도 있다.
- K_{MS} : MS와 TD가 서로 공유하고 있는 비밀키. 이 값은 MS가 사전에 TD에 등록할 당시 서로 합의한 것으로 가정한다.
- $K_{MS}(m)$: 메시지 m을 키 K_{MS}로 비밀키 암호화.

이때 사용되는 암호 알고리즘은 DES나 Triple-DES, AES 등 선택적으로 사용 가능하다.

- r_1, r_2, r_3 : 각각 TD와 MS가 생성하는 임의의 정수로 매번 보낼 때마다 다르다.
- S : TD가 MS에게 보내는 비밀 정보($=K_{MS}(r_1, CNT, cur\_t)$).
- P : MS가 TD로부터 받은 값 S를 확인하여 TD에게 보내는 증거($=K_{MS}(r, CNT)$).
- *reg_t* : TD와 MS가 사전에 합의한 일정 주기(예를 들어, 일주일 또는 한달).

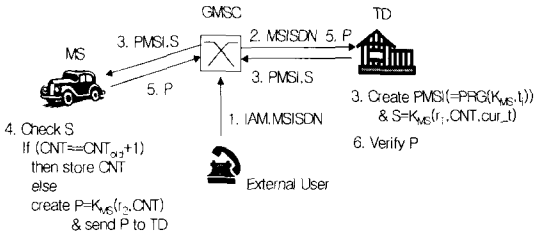

그림 8 제안하는 프로토콜

아울러 제안하는 방법에 대한 각 단계별 프로토콜은 다음과 같다(그림 8 참조).

[단계 1] 외부 이용자의 통화 요청

외부 이용자가 MS와의 통화를 위해 NP측의 GMSC에게 IAM과 MSISDN 메시지를 전송한다.

[단계 2] GMSC의 PMSI 요청

*GMSC*는 *MSISDN*에 따른 익명 아이디인 *PMSI*를 알기 위해 TD에게 *MSISDN*을 보내 현재의 PMSI를 요청한다.

[단계 3] PMSI와 비밀 정보 S 전달

TD는 MS와의 동기화 시간에 따라 미리 계산해둔 *PMSI*와 함께 비밀 정보 $S(=K_{MS}(r_1, CNT, cur_t))$를 계산하여 GMSC에게 전달한다. 그 후 GMSC는 방금 전 TD에게서 알아낸 *PMSI*를 이용하여 MS로의 연결을 설정하며, 이때 S 또한 MS에게 전달한다.

[단계 4] 비밀 정보 S에 대한 확인

MS는 비밀 정보 S를 K_{MS}로 복호화하여 올바른 자신의 메시지인지를 확인한다. 이때 직전에 전달받은 CNT를 CNT_{old}라 할때, $CNT=CNT_{old}+1$이 성립하는지를 확인하여 만일 만족한다면 현 CNT를 자신의 터미널에 보관하고, 그렇지 않으면 NP가 TD에 불법적인 요청을 시도한 경우이므로 증거로 $P(=K_{MS}(r_2, CNT))$를 생성하여 TD에 전달하고 [단계 6]으로 이동한다.

[단계 5] MS의 증거 생성

MS는 일정 주기 *reg_t*가 지난 직후 현재 보관하고 있는 가장 최근의 CNT를 임의의 정수 r3과 더불어 암호화하여 증거 $P(=K_{MS}(r_3, CNT))$를 생성한 다음 TD에 전달하여 확인을 요청한다. 만약 외부로부터 통화 요청이 한번도 없었을 경우는 CNT를 0으로 설정한다.

[단계 6] TD의 증거 검증

증거 P를 받은 TD는 메시지를 복호화하여 r_2(혹은 r_3)를 제거한 후 전달받은 CNT'이 자신이 마지막으로 보낸 CNT와 동일한지를 확인한다. 만일 이 두 값이 같다면 NP로부터 불법 시도가 없었다는 것을 알 수 있고, 그렇지 않다면(아마도 $CNT'<CNT$ 일 것이다) NP가 악의를 띤 시도를 하였다는 것을 감지하고 MS로부터 받은 P를 증거로 NP에게 제시한다.

본 프로토콜은 MS를 기준으로 한 방법이다. 따라서, 동일 MS로의 재연결 요청에 대해서는 주어진 *reg_t* 동안 기존에 저장된 CNT 값이 1씩 계속해서 누적될 것이며 다른 MS로의 새로운 요청에 대해서는 처음부터 본 프로토콜이 반복 적용된다.

3.2 프로토콜 분석

정리 1 만약 악의를 띤 NP가 특정 MS의 현 위치나 혹은 위치에 대한 추적을 하기 위해 특정 MS에 대한 PMSI를 주기적으로 알아내려는 능동공격을 시도할 경우 감지가 가능하다.

증명 : 본 프로토콜에서 능동공격을 시도할 경우 NP는 임의의 혹은 과거에 이용된 적이 있는 MSISDN을 이용하여 [단계 1]을 뺀 [단계 2]부터 프로토콜을 진행할 수 있다. 그러나, [단계 3]에서 TD로부터 현 PMSI를 알아낸 NP(혹은 NP내의 GMSC)는 외부 이용자로부터 실 요청이 없었기 때문에 MS로의 연결을 설정하지 않을 것이다. 이때 만약 이전의 CNT 즉, CNT_{old}가 5였다면 [단계 3]에서 TD는 현 CNT를 6으로 하여 비밀정보 S를 생성할 것이다. 물론 여기까진 별 문제가 없이 진행된다. 그러나, 여기서 만약 외부 이용자가 실제로 통화를 요청하거나 혹은 현 시점이 일정 주기 *reg_t*가 지난 직후가 될 경우 상황은 달라진다. 먼저 실제 외부 이용자가 통화를 요청할 경우 [단계 3]에서 TD는 현 CNT를 7(이전의 6에서 1을 더한)로 하여 S를 생성하고, 이 값을 [단계 4]에서 MS가 확인하게 된다. 이때 현 CNT는 7이고 MS가 현재 보관하고 있는 CNT_{old}는 5이다. 따라서, 주어진 식 $CNT=CNT_{old}+1$이 만족되지 않음으로 인해 NP의 불법시도가 MS에 의해 감지된다. 또한 실제 외부 이용자로부터 통화 요청이 없

거나 혹은 외부로부터의 모든 요청을 실제 MS에게 연결하지 않은 경우라 하더라도 [단계 5]에서 말한 일정 주기 *reg_t*가 지난 직후가 될 경우 MS가 보관하고 있던 최근의 *CNT*(이 경우 *CNT* 값은 0 또는 NP가 마지막으로 MS에게 전달한 값이다)를 암호화하여 증거 *P*로 TD에게 전달하기 때문에 TD가 이를 확인함으로써 NP의 불법시도를 감지할 수 있다. ■

정리 2 MS와 TD간의 비밀정보나 혹은 증거 *P* 교환시, NP는 전송 중에 이 값을 위변조 할 수 없다.

증명: 제안한 프로토콜의 안전성은 기본적으로 비밀키 암호 알고리즘의 안전성에 기반하며 전송되는 통신 채널은 안전하다는 것을 가정한다. 비밀 정보 $S(=K_{MS}(r_3,CNT,cur_t))$의 경우 NP가 이 내용을 위변조하기 위해서는 MS와 TD 둘만이 알고있는 비밀키인 KMS를 알아야 한다. 즉, 이 키 값을 모르고서 S를 알 수 없는 값 S'으로 위변조 했다면 이 값을 전송받는 MS나 TD가 S'을 복호할 경우 이는 알수 없는 무의미한 값일 것이다. 이는 증거 P(=KMS(r3,CNT))의 경우 또한 마찬가지이다. 따라서 NP가 설령 위변조하더라도 이 값은 MS나 TD에 의해 감지되므로 NP는 이 값을 위변조 할 수 없다. ■

한편 NP는 불법 시도를 위해 통화중이라든가 혼선, 단선 등 통화 연결에 대한 장애를 이유로 어쩌면 주기적으로 TD에게 PMSI를 요청할 수 있다. 문제는 이러한 장애의 요인이 자연적이든 의도적이든 MS나 혹은 TD가 이를 확인할 방법이 없다는데 있다. 이 경우 근본적인 해결책은 아니지만 아래와 같은 몇 가지 대안들을 생각해 볼 수 있다.

- 장애로 인한 NP의 요청시 TD가 PMSI를 알려주는 것을 일정기간(예를 들어, 1시간 혹은 1일)에 n(예를 들어, 3회)번으로 제한한다. 이 경우 PMSI가 변화되는 주기를 짧게 할수록 MS에게 보다 안전할 것이다.
- 장애로 인한 NP의 요청시 TD가 PMSI를 알려주는 일을 즉시 중단하고 추후 장애가 복구될 때 서비스를 재개한다. 물론 이 사실에 대한 내용은 TD가 MS에게 수시로 알려야 한다. 대개 MS에게 위치 프라이버시를 제공하는 일은 일반적인 서비스와 달리 특수한 경우에 해당된다. 만일 MS가 동의한다면 이 방법이 제일 안전하다.
- MS가 수신거부, 전원 오프 등 수신할 수 없는 상황 발생시 사전에 이를 TD와 NP에게 알린다. 이 경우 TD는 예를 들어, 상태 필드를 두어 이 사실을 기록하고 추후 MS가 수신가능 상태를 통보해올 때 다시 서비스를 이용하도록 할 수 있다.

여기서 실질적으로 고려해 볼 수 있는 방법은 첫 번째 방법이 적합하다. 나머지 두 방법은 예방차원에서 고려할 수 있을 것이다.

그밖에 불법시도를 위해 TD와 NP가 공모를 할 경우에 앞서 2.2.1절에서 언급한 분산 TP 방법을 제안한 방법에 이용함으로써 해결 할 수 있다. 즉, 하나의 TD를 *n*개의 TD로 분할하여 PMSI를 생성하도록 함으로써 만일 *n*개중 하나의 TD가 정직하다면 공모를 방지할 수 있다. 아울러 NP의 수동적인 공격에 대해서는 위 2.2.1절에서 Kesdogan 등[8]이 제시한 클래스를 이용한 PMSI 변화방법을 본 프로토콜에 동일하게 적용함으로써 해결할 수 있다.

그러나, 본 프로토콜은 기본적으로 하나의 NP로부터 연결되는 이동착호 과정을 기술하고 있다. 만일 MS가 한 NP가 미칠 수 있는 영역(이를 홈도메인이라 하자)에 머물지 않고 만일 다른 곳으로 이동할 경우 타 NP가 미칠 수 있는 영역(이를 타도메인이라 하자)에서의 착호 과정도 고려되어야 할 것이다. 예를 들어, MS가 원 거주지인 미국에 있다가 영국으로 갈 경우에 대한 프라이버시 서비스도 제공할 수 있어야 한다는 의미이다. 이 경우 본 프로토콜 적용시 발생할 수 있는 문제점은 완벽한 MS에 대한 위치 프라이버시가 보장되지 않는다는 점이다. 왜냐하면 적어도 타 NP측(원 NP와 공모할 경우)에서는 MS가 원래 살고있는 곳이 미국이며 언제 미국에서 영국으로 왔으며 영국을 떠난 시점은 언제이다라는 정도의 정보를 얻을 수 있다는 것이다. 따라서 향후 연구 과제로 이러한 문제점에 대한 개선방안을 생각해 보고자 한다. 또한 본 프로토콜을 실제 이동통신 환경에 적용할 경우 오히려 그 역기능으로 MS 측에서 이를 범죄에 악용될 수 있다는 문제점이 있다. 즉, 지나치게 프라이버시를 강조하다보면 MS측에서 불법적인 통화나 컨텐츠 등을 주고받을 수 있는 가능성이 있다. 따라서 본 프로토콜을 실제 환경에 적용하기에 앞서 MS의 불법 행위를 감지시 암호화된 메시지 내용을 복구하는 키 위탁 기술이나 혹은 위법행위시 MS에 대한 신원을 밝혀내는 신원위탁 방법에 대한 선행연구가 필요하다.

아래 [표 1]은 기존 방법들과 본 프로토콜과의 비교를 나타낸 것이다. [표 1]에서 박스 안의 각 표기는 프라이버시 제공 유무를 나타낸다. 특히, NP의 능동적인 공격에 대한 보호에서 TP 방법을 △로 표기한 이유는 앞서 설명한 대로 제안하는 프로토콜에 비해 [8]에서 제안한 방법에 대한 기술이 언급만 되어 있을 뿐 구체적이지가 않으며, 좀더 검증이 필요하기 때문이다. 아울

러 효율성 면에서 볼 때 제안하는 프로토콜은 [8]에서처럼 새로운 하드웨어를 추가하는 비용부담이 없고 기존의 GSM 시스템에 본 프로토콜을 그대로 적용할 수 있기 때문이다.

정리 3 본 프로토콜로 인해 발생되는 부하는 기존의 [8]에서 RM을 추가하는 방법에 비해 훨씬 효율적이다.

증명 : 제안한 프로토콜의 특징은 Kesdogan이 언급한 RM을 따로 이용하지 않고도 TD와 MS 둘만이 아는 비밀 정보인 S를 교환함으로써 좀더 효율적으로 NP의 능동적인 공격을 예방할 수 있다는 것이다. 즉, 현 시스템의 아키텍처를 변화시키지 않으면서 비밀정보 S를 기존 프로토콜에 덧붙여 전송함으로 기존에 RM을 추가하는 방법과는 달리 훨씬 비용부담이 적다. 또한 MS가 실제 저장하고 있는 정보량은 일정 시간 reg_t 동안 TD가 보내온 모든 값들이 아니라 가장 최신의 정보로 갱신된 단지 CNT이다. 계산적인 면에 있어서도 외부 이용자의 통화 요청에 대해 S와 P 생성 및 확인시 MS와 TD가 각각 한번의 대칭키 암호연산만 수행하면 된다. 따라서, 본 프로토콜로 인해 발생되는 부하는 기존의 [8]에서 RM을 추가하는 방법에 비해 전체 시스템에 큰 영향을 미치지 않는다. ■

4. 제안한 방법을 기반으로 한 지불 프로토콜

본 논문에서는 앞서 제안한 개선된 TP 방법을 기반으로 이를 지불 프로토콜에 응용해 보고자 한다. TP 방법의 특징은 MS의 신분이나 위치에 대한 프라이버시를 제공한다는 데 있다. 따라서 제안한 방법을 지불 프로토콜에 응용할 경우 기본적으로 이러한 서비스를 제공한다고 볼 수 있다. 본 논문에서 제안하는 지불 프로토콜은 MS가 NP를 통해 부가가치서비스 제공자(VASP, Value Added Service Provider)에게 특정 서비스(예를 들어, 게임이나 각종 유료 컨텐츠 등)를 제공받고자 할 경우에 서비스를 제공받은 데이타의 양만큼 금액을 지불하는 방법을 말한다. 아울러 이 과정에서 발생할 수 있는 MS와 부가가치서비스 제공자(이하 VASP라 한다)사이에 인증문제라든가 상호간에 분쟁이 발생했을 경우에 대한 해결문제 등을 해결하고자 한다.

TP 방법을 이용하여 지불할 경우 가장 좋은 방법은 이미 요금이 지불된 카드, 일명 Prepaid Phone Card[12]를 이용하는 것을 생각해 볼 수 있다. 그러나 현재 서비스되고 있는 Prepaid Phone Card 시스템을 TD기반의 TP 방법에 적용하기 위해서는 현 이동 통신 시스템 아키텍처에 많은 변화가 필요하다. 따라서, 본 논문에서는 앞서 그림 2에서 살펴본 아키텍처를 기반으로 지불 프로토콜을 설계하고자 한다. 예를 들어, 이동 단말기 내에 일종의 스위치 모드 기능을 두어 프라이버시를 보장하는 경우와 아닌 경우에 따라 선택적으로 서비스를 수행하도록 할 때, 전자에 대한 경우로 제안하는 지불 방법을 응용해 볼 수 있다.

제안하는 방법과 관련하여 Buttyan이 제안한 논문 [13]에서는 MS의 익명성을 보장하기 위해 CCA(Customer Care Agency)라는 제 3의 기관을 두고 있는 것이 특징이다. 이 기관을 이용하여 MS에게 일종의 티켓을 발부하면 MS는 이 티켓을 VASP에게 제시함으로써 부가가치 서비스를 받고 CCA가 대신 VASP에게 지불한다. 그 후 오프라인으로 MS에게 과금한 금액만큼 청구를 하는 방식이다. 그러나 이 방법은 기본적으로 위치 프라이버시에 대한 보호를 위해 MIXes 방법을 기반으

표 1 MS의 위치 프라이버시 제공 유무에 따른 기존 프로토콜과의 비교

		브로드캐스트 방법	MIXes 방법	TP 방법	제안하는 프로토콜
제 3자로부터 MS에 대한 위치 프라이버시	MS가 송신자일 경우	×	○	○	○
	MS가 수신자일 경우	○	○	○	○
NP로부터 MS에 대한 위치 프라이버시	NP에 대한 MS의 위치 프라이버시	×	×	△	○
	NP로부터의 수동적인 공격에 대한 위치 프라이버시	-	-	○	○
	NP로부터의 능동적인 공격에 대한 위치 프라이버시	-	-	△	○
MS가 홈도메인에서 타도메인으로 이동시에 대한 위치 프라이버시		×	×	×	×

로 하며, MS의 신분에 대한 프라이버시를 위해 추가적으로 CCA를 둔 것으로 TP 방법과 비교해 볼 때 효율성이 떨어진다.

차세대 이동통신 시스템인 UMTS에 적용될 보안기술을 연구 개발하는 ASPeCT 프로젝트[14]에서는 공개키 기반의 신뢰성 있는 제 3자인 TTP(Trusted Third Party)를 두어 MS에게 부가가치 서비스를 제공하는 방식을 제안하였다. 그러나 이 방법은 TTP를 추가적으로 설치해야하는 부담이 있으며 MS의 신분과 위치에 대한 프라이버시가 제공되지 않는 단점이 있다. 그 외에 여러 논문들[15,16]에서 이와 관련한 방법들을 제안하였으나 이들 역시 신분이라든가 위치에 대한 프라이버시가 제공되지 않는다. 본 논문에서는 앞서 언급한 논문들의 기법들을 참고로 하여 이를 TD기반에 맞게 변형하였다.

4.1 지불 프로토콜 제안

본 논문에서 제안하는 기본 모델은 앞서 언급한 [13,14]와 같은 티켓 기반으로 신분 및 위치에 대한 프라이버시를 제공하는 TD, MS, 그리고 VASP로 나뉜다(그림 9 참조). 이때 NP는 각각이 제공하는 메시지들을 상호 연결하는 환경을 제공하는 역할을 수행하므로 편의상 그림 9에서는 생략하였다. 제안하는 지불 프로토콜의 기본 시나리오는 다음과 같다. 먼저 1)MS가 TD에게 서비스를 제공받기 위해 일회용 티켓을 요청하면 TD가 이 요청을 확인하고 티켓을 발부한다. 2)그 후 MS가 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 MS에게 이 금액을 청구한다.

제안하는 프로토콜에서 MS의 비밀키와 공개키쌍 그리고 MS와 TD간의 비밀키에 대한 정보는 MS가 사전에 TD에 등록할 당시에 합의된 것으로 가정하며 아울러 TD와 VASP의 공개키에 대한 정보는 공개키 디렉토리 서비스나 브로드캐스트 등의 방법을 이용하여 알고 있다고 가정한다. 제안하는 프로토콜에서 사용되는 각종 표기들은 다음과 같다.

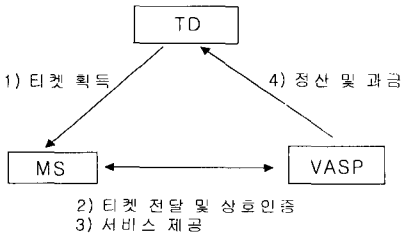

그림 9 제안하는 지불 프로토콜의 환경

[표기]

- A : MS의 실제 아이디, $PMSI$: A의 임시 익명 아이디.
- B : VASP의 아이디.
- TD : TD의 아이디. $Cert_{TD}$: TD가 발행한 공개키 인증서(certificate).
- T : 티켓, T_{id} : 티켓의 아이디.
- TS : 타임스탬프(timestamp).
- H : 충돌회피 일방향 해쉬함수.
- tck_n : $tick$ 정보로 tck_0(H의 seed)를 n번 해쉬한 값, 여기서 $tick$이란 Pederson[17]이 제안한, 일명 *Micropayment* 방식으로 일방향 해쉬함수를 H, $seed$를 s라 할 때, $H^1=H(s)$, $H^2=H(H^1)$, ..., $H^n=H(H^{n-1})$이다. 이때 H^1, H^2, ..., H^n 각각을 $tick$이라 하며 티켓의 총액을 w라 할 때 일종의 w/n 값이다.
- tck_v : A가 B에게 보낸 최종 $tick$ 정보.
- tck_cnt : B가 A로부터 $tick$을 모두 받은 갯수.
- amt_tck : $tick$당 금액.
- $data\_tck$: $tick$당 전송되는 데이타량으로 바이트 수.
- K_{AT} : A와 TD사이의 공유 비밀키.
- K_{AB} : A와 B사이의 세션키.
- K_A^{-1}, K_A : TD가 생성한 A의 서명키와 검증키.
- K_{TD}^{-1} : TD의 서명키.
- K_B^{-1} : B의 서명키.
- $K(m)$: 메시지 m을 키 K로 암호화.
- g : 위수 q를 갖는 유한군에서의 생성자.
- α, g^{α} : Diffie-Hellman 키교환 파라미터로 A의 개인키와 공개키.
- β, g^{β} : Diffie-Hellman 키교환 파라미터로 B의 개인키와 공개키.
- m_k : B가 제공하는 서비스를 담은 메시지 m을 $data_tck$만큼의 블록으로 분할했을 때 k번째 메시지, 이때 $k \in \{1,2, ..., n-1\}$.
- t : A가 TD에게 티켓 요청을 보낼 당시의 동기화 시간.
- r_1, r_2 : 임의의 정수.

본 논문에서 제안하는 지불 프로토콜은 아래와 같다.

[단계1] 티켓 획득

A가 TD에게 티켓 T를 요청하면 TD가 T를 생성하여 A에게 주고, 이때 A는 TD로부터 전달받은 티켓을

보관한다.

$A \rightarrow TD$: $K_{AT}(PMSI, t, r_1)$

$TD \rightarrow A$: $K_{AT}(r_1, T, tck_0, K_A^{-1})$

$T = (T_{id}, TS, g^a, tck_n, Cert_{TD}, K_{TD}^{-1}(T_{id}, TS, g^a, K_A, tck_n))$

[단계 2] 티켓 전달 및 상호인증

아래 세 개의 메시지를 교환한다. 그 중 두 번째 메시지를 통해 A가 B를 인증하게되고, 세 번째 메시지를 통해 B가 A를 인증한 후 이 정보를 B가 분쟁에 대비하여 보관한다. 이때 세션키 $K_{AB}=H(g^{a\beta}, r_2)$이다.

$A \rightarrow B$: T

$B \rightarrow A$: $r_2, data\_tck, amt\_tck, H(K_{AB}, r_2, B)$

$A \rightarrow B$: $K_{AB}\{K_A^{-1}(T_{id}, K_{AB}, r_2, B, data\_tck, amt\_tck)\}$

[단계 3] 서비스 제공

B가 A에게 첫 번째 메시지 블록 m_1을 전송하면 A는 이에 해당하는 $tick$ 정보 tck_{n-1}값을 B에게 전달한다. 이 값을 전송 받은 B는 A에게 두 번째 메시지 블록인 m_2를 전송하게 되고 A는 이에 해당하는 $tick$ 정보 tck_{n-2} 값을 B에게 전달한다. 만일 A가 B로부터 원하는 서비스 메시지가 k블록의 길이를 갖는다고 가정하면, 이런 식으로 하여 주어진 메시지 블록이 k번째가 될 때까지 반복하여 A는 k개의 메시지 블록을 얻게되고 B 또한 k개의 $tick$ 정보를 얻게된다. 결국 B가 A에게 보내는 각 메시지 블록에 대해 A가 이에 대한 증거로 $tick$ 정보들을 B에게 보내주는 것이다.

$B \rightarrow A$: $K_{t\_SP}(m_k)$

$A \rightarrow B$: tck_{n-k}

[단계 4] 정산 및 지불

B가 지금까지 A로부터 받은 모든 정보를 자신의 서명정보와 더불어 TD에게 전달한다. TD는 이 정보들을 검토하여 이상이 없을 경우 해당 금액($amt\_tck*tck\_cnt$)만큼 지불하고 A에게 이 금액을 청구한다. 즉, 아래 정보들을 전달받은 TD는 A의 서명을 확인하고 T_{id}와 TS를 이용하여 티켓이 유효한지를 검사한다. 검사 결과 만일 이상이 없으면 $data_tck$와 amt_tck에 따라 지불 프로토콜을 수행한다. 그러나 이상이 있는 경우, A와 B 각각이 가지고 있는 서명과 증거들을 이용하여 분쟁을 해결한다. 그 후 TD는 B로부터 받은 아래 정보들을 증거로 보관하고 B에게 지불한 금액을 A에게 청구한다.

$B \rightarrow TD$: $T_{id}, B, TS, data\_tck, amt\_tck, tck_v, tck\_cnt,$
$K_A^{-1}(T_{id}, K_{AB}, r_2, B, data\_tck, amt\_tck),$
$K_B^{-1}(T_{id}, B, TS, data\_tck, amt\_tck, tck_v, tck\_cnt)$

4.2 프로토콜 분석

제안한 지불 프로토콜의 안전성에 대한 분석은 아래와 같다.

[개체인증과 키 인증] A는 B가 [단계 2]의 두 번째 메시지에서 보낸 해쉬정보 $H(K_{AB}, r_2, B)$내에 키 정보인 K_{AB}와 B를 검증함으로써 인증이 가능하며 반대로 B는 세 번째 메시지에서 A가 보낸 서명 정보인 $KAB\{K_A^{-1}(T_{id}, K_{AB}, r_2, B, data_tck, amt_tck)\}$내에 키 정보인 K_{AB}와 자신이 보낸 r_2의 존재를 각각 검증함으로써 상호간에 함축적인 키 인증과 개체인증이 가능하다.

[키 교환과 키 신규성(refreshness)] A와 B간의 세션키 $KAB(=H(g^{a\beta}, r_2))$ 생성은 A와 B 공동의 참여하에 이루어지며, 또한 랜덤 정수인 r_2를 이용함으로써 매 세션마다 새로운 키가 생성된다.

[부인방지] 만일 A가 B로부터 받은 메시지에 대해 부인한다면 B는 A의 서명정보와 더불어 최종 $tick$ 정보인 tck_v를 증거로 제시하고 그 반대의 경우는 TD가 B로부터 최종단계에서 받은 서명정보를 증거로 제시함으로서 상호간의 분쟁을 해결할 수 있다.

[티켓의 이중사용(double spending) 방지] A가 동일한 티켓을 다른 B들에게 이용하려 할 경우, 티켓 내에 저장된 유일한 식별 아이디인 T_{id}와 타임스탬프 TS를 TD가 최종 검증단계에 확인함으로써 티켓의 이중사용을 방지할 수 있다.

[MS의 신분에 대한 프라이버시] TP 방법에 근거하여, A의 실제 아이디가 아닌 임시 익명아이디 $PMSI$를 이용함으로써 프라이버시가 제공된다(본문의 1, 2장 참조).

[MS의 위치에 대한 프라이버시] 본 논문의 2, 3장을 참조하시오.

또한 아래와 같은 외부 침입자로부터의 공격 유형들에 대한 방지가 가능하다.

만일 외부 침입자가 티켓을 임의로 위변조 하려 할 경우, 본 프로토콜에서는 티켓 발생시 기본적으로 TD의 서명을 생성하여 이를 A와의 공통키로 암호화하여 전송하기 때문에 위변조가 불가능하다. 그리고 TD와 B가 공모하여 A를 속이고 지불 금액을 과장되게 조작할 수 있다. 그러나 본 논문의 2.2.1절에서 언급한 분산 TP방법을 제안한 프로토콜에 적용할 경우 여러 TD들 가운데 적어도 하나의 TD가 정직하다는 가정 하에 공모를 막을 수 있다.

그밖에 만일 서비스 제공 단계에서 이미 정해놓은 $tick$을 모두 사용했을 경우 [단계 3,4]에 다음과 같은 과정을 추가로 수행함으로써 해결이 가능하다.

[단계 3] 서비스 제공

A가 기존에 TD가 생성한 것과는 다른 tck_n'과 tck_0'을 생성하여 아래 메시지를 B에게 전송한 다음 기존 프로토콜을 계속 진행한다. 이때 기존의 m_k는 m_k'이 되고

tck_{n-k}는 tck_{n-k}'이 된다.

$A->B$: $tck_n', T_{id}, TS, K_A^{-1}(tck_n', T_{id}, TS)$

[단계 4] 정산 및 지불

기존에 B가 TD에게 보내는 메시지에 아래 메시지가 추가된다.

$B->TD$: $TS, tck_0', tck\_cnt', K_A^{-1}(T_{id}, TS, tck_0', tck\_cnt')$

제안한 프로토콜은 공개키 연산을 이용하여 MS와 VASP 상호간에 인증 문제를 해결하고 있는데 이 또한, 다가오는 제 3세대 이동 통신환경에서는 보다 넓은 대역폭을 지원할 것을 기본 요구사항으로 하고 있기 때문에 충분히 적용이 가능할 것이라 예상된다.

5. 결 론

본 논문에서는 이동통신 환경에서 모바일 이용자의 현 위치와 행적 노출 즉, 위치 프라이버시의 문제에 대한 새로운 해결책을 제안하고 이를 응용한 지불 프로토콜을 설계하였다.

임시 익명 아이디를 이용한 TP 방법은 지금까지 알려진 브로드캐스트나 MIXes 등의 방법들에 비해 효율성이 뛰어나다. 그러나 이 방법은 앞서 살펴본 바와 같이 네트워크 제공자측의 능동적인 공격에 대처할만한 뚜렷한 방법이 제시되지 못하였다. 본 논문에서는 MS와 TD사이에 비밀 정보를 주고받음으로써 이러한 능동적인 공격에 대처할 수 있는 새로운 방법을 제안하였다. 기존에 제안된 Kesdogan의 방법[8]은 RM이라는 새로운 모듈을 따로 설치함으로 인해 비용이라든가 효율성에 문제가 있었다. 그러나 제안한 프로토콜은 RM을 추가로 설치하지 않고도 문제를 해결할 수 있어 보다 효율적이다.

참 고 문 헌

[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, pp. 105-116, 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] A. Pfitzmann and M. Waidner, "Networks without User Observability," Computers & Security, vol. 6, no. 2, pp. 158-166, 1987.

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

[6] 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.

[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] D. Kesdogan, P. Reichl, and K. Junghärtchen, "Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks," ESORICS '98, LNCS vol. 1485, pp. 295-312, 1998.

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

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

[11] M. Reichenbach, H. Damker, H. Federrath, and K. Rannenberg, "Individual Management of Personal Reachability in Mobile Communication," Proc. of the IFIP TC11 SEC 97, 13th International Information Security Conference, pp. 14-16, 1997.

[12] Y. B. Lin, C. H. R. Rao, and M. F. Chang, "Mobile Prepaid Phone Services," IEEE Personal Communications Magazine, vol 7, no. 3, pp. 6 14, 2000.

[13] 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.

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

[15] B. Patel and J. Crowcroft, "Ticket Based Service Access for the Mobile User," Mobicom '97, pp. 223-233, 1997.

[16] J. Zhou and K. Y. Lam, "Undeniable Billing in Mobile Communication," Mobicom '98, pp. 284-290, 1998.

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

김 순 석
1997년 2월 진주대학교 컴퓨터공학과 학사. 1999년 2월 중앙대학교 컴퓨터공학과 석사. 1999년 3월 ~ 현재 중앙대학교 대학원 컴퓨터 공학과 박사과정. 관심분야는 암호 프로토콜, 이동통신 보안, 정보보호

김 성 권
1981년 2월 서울대학교 계산통계학과 학사. 1983년 2월 한국과학기술원 전산학과 석사. 1990년 8월 University of Washington 전산학 박사. 1991년 3월 ~ 1996년 2월 경성대학교 전산통계학과 조교수. 1996년 3월 ~ 현재 중앙대학교 컴퓨터공학과 부교수. 관심분야는 계산기하학, 암호 응용 및 정보보호, 생물정보학