이동통신 환경에서 네트워크 제공자 및 제 3자로부터 안전한 위치정보 보호기법

김 순 석† · 이 창 훈††

요 약

본 논문에서는 이동통신의 내부 이용자, 특히 네트워크 제공자들로부터의 공격에 대비하여 이동 사용자의 위치 정보를 보호하는 새로운 방법을 제안한다. 이동통신 환경에서 어떻게 사용자의 위치 정보를 보호할 것인가에 대해 이미 몇 가지 제안들이 있었다[1-5]. 이들 가운데, Kesdogan 등[2, 3]은 일명 임시 익명아이디를 이용한 새로운 방법을 제안한 바 있으며, 아울러 네트워크 제공자들의 수동적인 공격과 능동적인 공격에 대비한 보호 방법에 대해 기술한 바 있다. 그러나 이들 가운데 능동적인 공격에 대한 보호 방법은 그 기술이 명확하지가 않으며, 게다가 제안한 시스템에 도달가능 매니저[1, 6]라는 것을 부착해야하는 추가 부담이 따른다. 따라서 우리는 앞서 제안한 Kesdogan 등의 방법을 개선하고 이것의 안전성과 효율성에 대해 분석하고자 한다.

Secure Location Information Protection Scheme from the Network Provider and the third party in Mobile Communication Environments

Soon Seok Kim† · Chang Hun Lee††

ABSTRACT

In this paper, we propose a new scheme, protecting information about the location of a mobile user against attacks from inside users of the mobile communication, especially the network providers. There have already been some proposals about how to protect location information of user in mobile communication environments[1-5]. Among them, Kesdogan et al.[2, 3] proposed a new method, using so-called temporary pseudonyms and also described protection method against a passive and an active attack of network providers. However, the description of protection method against the active attack between the two is not clear. Moreover, there is an additional load that it should append a reachability manager[1, 6] to the proposed system. Therefore, we propose a new scheme improving the above method of Kesdogan et al. and analyze its security and effectiveness.

키워드 : 임시익명아이디(Temporary Pseudonym Identity), 위치불추적서비스(Location Untraceability Service), 익명성(Anonymity), 프라이버시보호(Privacy Protection), 이동통신환경(Mobile Communication Environments)

1. 서 론

이동통신 서비스를 포함하여 이동 컴퓨팅, 이동 멀티미디어 서비스 등 이동통신시스템을 통한 응용 서비스 개발과 서비스 제공이 증가함에 따라 무선통신 시스템에서 신뢰할 수 있는 보안 서비스 제공의 필요성은 더욱 강조되고 있다. 특히, 이동통신 시스템의 무선접속 구간은 송수신 데이터의 도청이 쉽고, 가용 무선 자원이 제한되어 있다는 점에서 유선 네트워크와는 다른 보안상의 취약점을 가지고 있다. 무선접속 구간에서의 이용자 신분 및 위치 정보의 노출, 불법적인 서비스의 이용, 송수신 데이터의 도청 및 변경 등은 이용자의 사생활을 침해하고 전체적인 시스템의 신뢰성을 저하시킨다. 특히, 네트워크를 관리하는 관리자(혹은 네트워크 제공자)에 의한 불법적인 데이터의 도청과 정보노출은 거의 무방비 상태이다.

이동통신 환경에서의 보안 요구사항을 분류해보면, 대개 기밀성, 무결성, 가용성으로 나뉘어 진다[1]. 특히, 이들 가운데 기밀성과 무결성에 대해 모바일 이용자의 프라이버시 측면에서 좀더 엄밀히 살펴보면 크게 다음과 같은 네 가지의 카테고리로 분류된다.

- 위치 프라이버시(location privacy)

  모바일 사용자의 현 위치나 혹은 이동한 위치들에 대한 내역 정보가 내부 이용자인 네트워크 제공자(Network Pro-

※ 본 연구는 한국과학재단 목적기초연구(R01-2000-000-00401-0)지원으로 수행되었음.
† 정 회 원 : 한라대학교 정보통신공학부 교수
†† 정 회 원 : 한경대학교 컴퓨터공학과 교수
논문접수 : 2003년 7월 31일, 심사완료 : 2003년 9월 30일

vider라 하며 이하 간단히 NP라 부른다)를 비롯하여 비인가된 자들로부터 추적이 불가능해야 한다. 그러나 이러한 위치에 대한 정보를 인가된 사용자들은 효율적으로 이용해야 한다. 대개 이러한 위치 정보는 NP 측의 데이터베이스 내에 보관된다.

- 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 증명해야 한다.

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

현 이동 통신 시스템의 경우, 가입자 즉, 모바일 사용자의 단말기 내에 들어있는 신분 정보와 현재 위치는 이동통신 네트워크 센터 즉, NP에 의해 계속 추적된다. 만일 사용자의 단말기 전원이 발신 또는 착신을 위해 켜진 상태에서는 단말기에서 방출되는 사용자의 신원 정보를 통해 사용자의 현재 위치가 NP에 의해 등록 또는 갱신되며, 아울러 이 위치 정보는 데이터베이스에 저장된다.

이러한 사용자의 현재 위치를 추적하는 것은 이동통신 서비스를 사용자에게 제공하기 위한 필수적인 기능이다. 그러나 반대로 사용자의 위치 정보는 결국 사용자의 행적을 추적하는 원인이 될 수 있기 때문에, 만일 이 정보가 내부 이용자인 NP나 그밖에 악의를 띤 제3자를 통해 외부로 노출될 경우 사용자의 프라이버시를 보호한다는 측면에서 바람직하지 않다. 이는 최악의 경우, 외부 도청자나 혹은 NP 측(혹은 NP측의 악의를 띤 어느 한 사용자)에서 이러한 사용자의 개인 정보들을 불법적으로 알아내 외부에 알리거나 혹은 상업적인 목적으로 악용하여 금전적인 이득을 취할 수 있으며, 이는 결국 사용자 자신도 모르는 사이에 자신의 개인 정보인 위치 정보가 외부로 누출되는 결과를 가져온다. 그러므로 이동 통신 환경에서 사용자에 대한 프라이버시 보호는 그 어느 요구사항 보다 선행되어야 할 과제이며, 내부 이용자나 혹은 기타 제3자에 의한 특정 사용자의 위치 추적을 불가능하게 하는 보안 서비스(이를 위치 불추적 서비스라 한다)도 선택적으로 통신 사업자가 수용하여야 한다.

1.1 연구 배경

유럽에서 현재 대표적으로 이용되고 있는 제2세대 이동통신 시스템 표준인 GSM(Global System for Mobile communications)[7]의 경우, 모바일 이용자의 송수신 호 요청에 대한 서비스를 위해 HLR(Home Location Register)과 VLR(Visited Location Register)이라는 데이터베이스를 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 측면에서 보호되어야 한다.

이러한 위치 프라이버시 보호 문제와 관련하여 현재까지 브로드캐스트(broadcast)[4], MIXes[5], 그리고 TP(Temporary Pseudonym, 이하 간단히 TP라 부른다)[2, 3] 방법 등 여러 가지 해결책들이 나와 있다. 그중 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 제3자로부터 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 NP 측에서 TD에게 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 수 없다. 또한 내부적으로 PMSI 값은 주기적으로 변화되어 앞서 말한 HLR과 VLR에 등록되기 때문에 NP측에서 PMSI를 이용한 위치 추적이 불가능하다.

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 제3자의 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[3]에서 NP의 공격 유형

을 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 요청함으로서 모바일 이용자의 위치를 지속적으로 추적하려는 시도를 말한다. Kesdogan 등[3]은 이러한 능동적인 공격과 관련하여 한가지 대안으로 도달가능 매니저(Reachability Manager)라는 추가적인 하드웨어 장비를 TD에 두어 PMSI를 NP에게 알려주는 것이 정당한 지를 검토한 후에 요청을 받아들일 것인지 아닌지를 결정하도록 언급만 하고 있다. 그러나 이 제안은 실질적인 대안이라기보다는 도달가능 매니저를 이용하여 해결할 수도 있다는 언급만 있을 뿐 구체적으로 어떠한 방식으로 공격을 막을 것인지에 대한 기술이 되어있지 않다. 즉, 도달가능 매니저가 어떻게 NP의 요청이 정당한지를 결정할 수 있는지 그 부분이 명확하지 않다. 또한 현재까지 나와있는 도달가능 매니저의 방법은 이를 고려하고 있지 않다. 따라서 본 논문에서는 도달가능 매니저와 같은 새로운 하드웨어를 추가로 설치하지 않고 위의 능동적인 공격에 대비한 실질적이고도 효율적인 방법을 제안하고자 한다.

제안하는 방법의 기본 아이디어는 다음과 같다. 외부 이용자로부터 수신 호 요청시, 외부로부터 실질적인 착호 요청이 있었는지 아니면 NP가 불법적인 요청을 시도하였는지를 확인하기 위해 NP로부터 실제로 착호 연결 요청을 받는 당사자인 모바일 이용자가 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 NP의 부정을 감지하고 이에 따른 제재를 가할 수 있다.

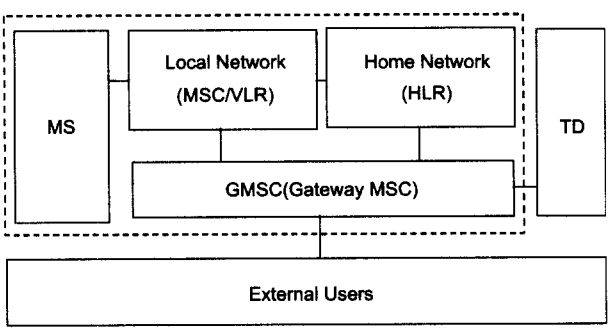
본 논문의 구성을 요약하면 아래와 같다. 먼저 2절에서 위치 프라이버시 보호와 관련하여 특히, TP 방법을 중심으로 그 내용과 문제점들을 살펴보고, 3절에서 이를 개선한 새로운 프로토콜을 제안한 후, 4절을 끝으로 결론에 대해 논하고자 한다.

2. TP 방법

TP 방법은 앞서 서론에서 언급한 바와 같이 1996년 Pfitzmann과 Kesdogan 등[2, 3]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 그밖에 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 수 없다.

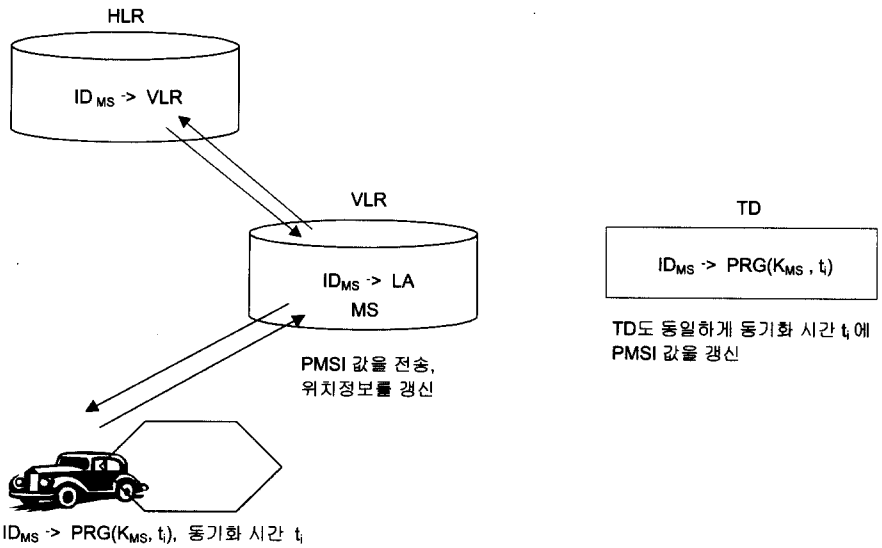
TD는 원래 처음 제안할 당시에는 HPC(Home Personal Computer)라 하여 프라이버시를 위한 민감한 데이터들(예를 들어, 이용자의 실제 아이디를 포함하여 이용자의 비밀키 등의 정보들)을 가정에 있는 PC에 저장하던 개념이었으나 이후에 TD라 하여 물리적으로 가용성이 보장되는 제 3의 안전한 장소라는 개념으로 그 명칭이 바뀌었다.

본 절에서는 앞서 언급한 GSM 네트워크[9]를 기반으로 TP 방법의 개념을 설명하고자 한다. 먼저 GSM 네트워크를 기반으로 TP 방법을 적용한 아키텍처는 (그림 1)과 같다.



(그림 1) TP 방법을 적용한 이동통신 아키텍처

GSM 네트워크는 그 영역이 계층적으로 이루어져 있는데, 그중 최상위에 몇몇 MSC(Mobile Switching Center) 영역이 있으며, 그 아래 각각 BSC(Base Station Controller)에 의해 관리되는 몇 개의 LA(Location Area)가 있다. 또한 각 LA는 최하위에 몇몇 셀(cell)들로 구성되어 있으며 이 셀 내에 모바일 이용자 즉, MS(Mobile Station)가 존재한다. 여기서 MS는 원래 모바일 이용자의 신분과 기타 개인정보 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 데이터베이스, HLR 그리고 VLR 이 세 구성요소에 의해 이루어진다. 여기서 HLR은 각 MS들에 대한 현 MSC 영역들을, 그리고 VLR은 각 MSC 영역 내에 현 LA들을 저장하고 있다. 이러한 GSM 네트워크에서 MS의 이동성에 대한 위치 관리 기법은 주로 아래 세 가지 과정으로 분류하고 있다.



(그림 2) TP 방법을 이용한 위치 갱신

- 위치 갱신(LU, Location Update) : MS가 현 LA에서 다른 LA로 이동 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 MS에 대한 위치정보가 생성된다.

- 이동 착호 설정(MT, Mobile Terminated calls setup) : 외부 이용자로부터 MS로의 호 설정으로 만약 외부 이용자가 기존의 PSTN(Public Switched Telephone Network) 네트워크로부터 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.

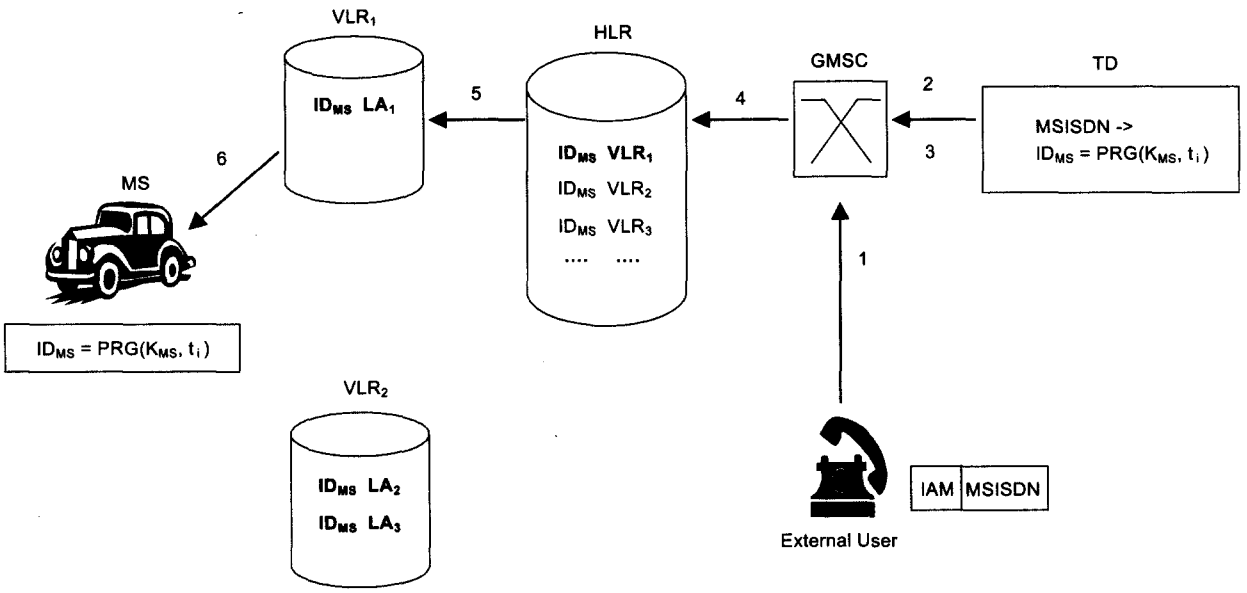
이러한 세 가지 위치관리 기법들을 MS의 위치정보에 대한 프라이버시 보호 차원에서 위 아키텍처를 기반으로 TP 방법[2, 3]에 적용하면 다음과 같다.

- 위치 갱신

TP 방법을 기반으로 한 위치 갱신 과정은 네트워크 데이터베이스(HLR과 VLR들)내에 MS의 현 위치 정보를 계속해서 갱신하는 역할을 수행하는 것으로 (그림 2)와 같다. 여기서 ID_{MS}는 MS의 PMSI로 $PRG(K_{MS}, t_i)$로 생성된다. 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 t_i에 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 (그림 3)에서 보는 바와 같이 외부 이용자가 MS에게 통화 요청시 이에 대한 호를 설정해주는 과정이다. 먼저 외부 이용자는 MS와의 통화를 위해 IAM(Initial Address Message)과 그 속에 포함된 MSISDN(Mobile Subscriber Integrated Services Digital Network Number) 번호를 GMSC에게 전달한다. 여기서 IAM 메시지는 요구되는 서비스의 종류라든가 라우팅 정보를 포함하고 있으며 MSISDN 번호는 MS의 고유 번호로 GMSC가 이것을 이용하여 MS의 위치를 파악하는데 이용한다. GMSC는 MSISDN 번호를 이용하여 TD에게 PMSI 즉, ID_{MS}를 요청한다. 이 ID_{MS}를 이용하여 GMSC는 HLR에 접근하게되고 또한, 어느 VLR에 속해 있는지를 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 이용할 경



(그림 3) TP 방법을 이용한 이동 착호 설정 과정

우, 착호가 설정되기 전까지는 제3자는 물론 이러한 호 요청을 설정해준 NP 조차도 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 추적할 수 없다.

그러나 MS는 항상 머물러있지 않고 이동한다는 특수성을 지니고 있다. 예를 들어, 시속 100KM 이상으로 달리는 차안에서 그 시간에 맞춰 ID_{MS}를 갱신하기는 힘들뿐만 아니라 전체 이용자들이 한꺼번에 갱신하려 할 경우 TD 측에서 이를 수용할만한 메모리 한계도 생각해야 한다. 따라서 동기화 시간을 지수적으로 분배한다든지 하여 부하를 줄일 필요가 있다. 실제로 Kesdogan[3]은 이러한 단점을 들어 그 공격법과 대안을 소개하고 있다. 이에 대한 내용은 다음 절에서 논하기로 한다.

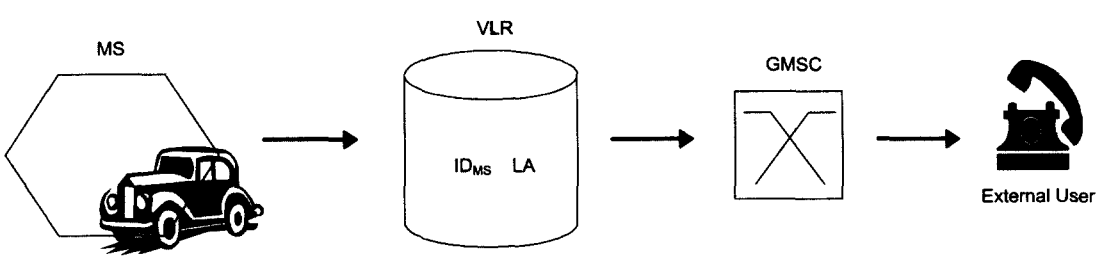
- 이동 발호 설정

이 과정은 이전의 이동 착호 설정과는 반대 과정으로 아래 (그림 4)에서 보는 바와 같이 비교적 간단하다. MS가 자신의 PMSI 즉, ID_{MS}를 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.

지금까지 설명한 TP 방법은 효율성은 있지만 TD가 만일 고장이 날 경우 이에 따른 대처 방안이 없다는 단점이다. 따라서 이 방법은 TD가 물리적으로 안전하며 언제든 이용할 수 있다는 가정이 필요하다. 본 논문에서도 이를 가정한다.

2.1 알려진 공격 유형 및 문제점

TP 방법에 대한 안전성은 임시 익명 아이디인 PMSI와 물리적으로 안전한 TD에 기반하고 있으며, 일반적으로 제3자의 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[3]에서 NP의 공격 유형을 크게 수동적인 공격(passive attack)과 능동적인 공격(active attack)으로 나누어 그 각각



(그림 4) TP 방법을 이용한 이동 발호 설정 과정

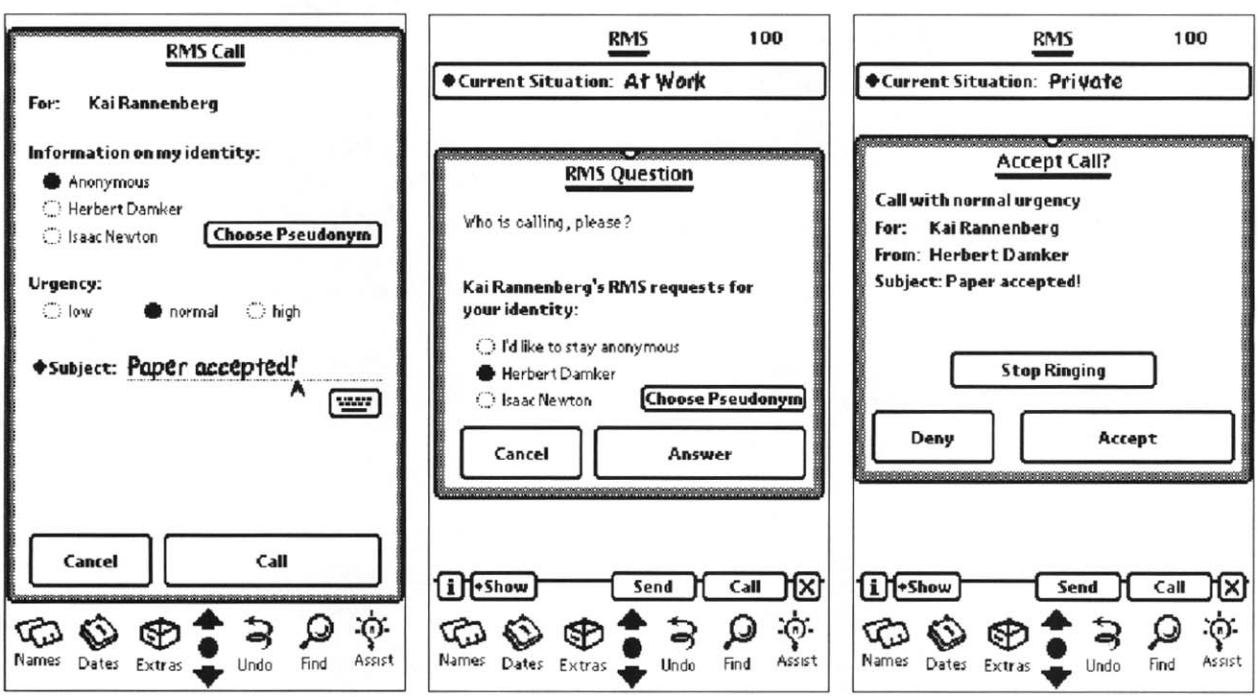
에 대한 해결 방법을 제안한 바 있다.

수동적인 공격이라 함은 이동 통신 시스템 내부에 있는 수동적인 공격자가 네트워크 상에 데이터베이스인 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 장시간 동안 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 클래스를 이용한 방법과 분산 TP를 이용한 방법을 제안한 바 있다.

이에 반해, 능동적인 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 파악한다. 물론 이 공격은 TD내에 NP로부터 모든 요청들에 대한 로그파일을 유지함으로써 그 공격에 대한 시도를 감지할 수 있다. 그러나 NP 측에서 로그파일은 TD가 위조 가능하다고 생각할 수 있기 때문에 공격을 시도했다는 정당한 증거가 되질 못한다.

Kesdogan 등은 능동적인 공격과 관련하여 한가지 대안으로 단지 도달가능 매니저를 TD에 두어 PMSI를 NP에게 알려주는 것이 정당한 지를 검토한 후에 요청을 받아들일 것인지 아닌지를 결정하도록 상세한 기술이 아닌 언급만 하고 있다. 여기서 도달가능 매니저는 유럽에서 GSM 환경을 기반으로 Reichenbach 등[6]이 제안한 방법이다. 도달가능 매니저는 개인휴대단말기인 PDA(Personal Digital Assistant)로 구현된 일종의 도우미 역할을 수행하는 장치로 원래 MS에 휴대용으로 부착하여 수행된다((그림 5) 참조). 먼저 송신자가 수신자인 MS와 통화를 위해 각종 정보(예를 들어, 송신자 개인 정보라든가 통화 주제나 목적 등의 정보)와 더불어 호 요청을 보내면 도달가능 매니저는 자신의 PDA를 통해 이에 대한 정보를 MS에게 디스플레이 한다. MS는 디스플레이된 정보를 보고 호 요청을 받아들일 것인지 아닌지를 결정하고 그 여부에 따라 도달가능 매니저가 수신 호를 설정 또는 중단하게 된다.

그러나 Kesdogan 등의 제안은 실질적인 대안이라기보다는 도달가능 매니저를 이용하여 해결할 수도 있다는 언급만 있을 뿐 구체적으로 어떠한 방식으로 공격을 막을 것인지에 대한 방법은 기술된 바가 없다. 즉, 현 도달가능 매니저를 이용할 경우 어떻게 NP의 요청이 정당한가 또는 NP가 중간에서 부정을 저질러 송신자가 보낸 개인정보를 위



(그림 5) 도달가능 매니저의 사용자 인터페이스

조할 경우 어떻게 감지하고 대처할 것인가 등등을 결정할 알고리즘이나 방법이 없으며, 또한 현재까지 나와있는 도달가능 매니저는 이러한 기능이 내재되어 있지 않다. 뿐만 아니라 이러한 공격을 막기 위해 도달가능 매니저를 이용할 경우 이에 따른 새로운 하드웨어를 추가로 설치해야 한다는 비용 부담이 따르며, 그만큼 통신 효율 면에서 오버헤드가 발생한다.

따라서 본 논문에서는 새로운 하드웨어를 추가로 설치하지 않으면서 내부 이용자인 NP로부터의 능동적인 공격에 대비한 실질적이고도 효율적인 방법을 제안한다.

3. TP 방법에 대한 새로운 제안

제시한 능동적인 공격에 대한 문제는 외부 이용자가 통화 요청을 하지도 않았는데도 불구하고 정당한 이유없이 NP가 주기적으로 TD에 PMSI를 요청하는데 있다. 이러한 NP의 공격에 대비하기 위해서는 외부 이용자로부터 실제 통화 요청이 있었는지, 또한 그 통화 요청을 NP가 받아서 MS에게 실제로 호 설정을 연결하였는지를 확인해야 한다. 즉, 이를 위해서는 MS와 TD로 하여금 실제 호가 연결되었는지를 감시하는 기능이 반드시 필요하다.

제안하는 방법은 MS의 도움을 받아 TD가 감지하는 방법으로, 호 설정이 이루어졌는지를 확인하기 위해 MS가 NP로부터 호 연결 요청을 받은 직후 그에 대한 확인으로 응답 메시지를 NP를 통해 다시 TD에게 전달하는 것이다.

이 방법은 기존의 TP 방법과 마찬가지로, 외부 이용자로부터 초기 호 요청이 왔을 때 NP측에서 MS의 고유번호인 MSISDN과 IAM을 이용하여 PMSI를 TD에 요구하고 TD는 PMSI를 부여한다. 이때 NP측의 GMSC는 PMSI 값을 자신의 테이블에 보관한 다음, TD로부터 부여받은 PMSI를 이용하여 MS에게 호 설정 신호를 보낸다. 그러면 MS는 호 설정 신호가 올바로 전달되었음을 확인하는 응답메시지(이를 ACK라 하자)를 TD에게 보냄으로써 TD는 MS가 호 설정 신호를 수신하였음을 인지하게 된다. 첫 번째 호 설정을 제외한 동일 MS의 두 번째 호요청부터 GMSC는 자신의 테이블 내에 저장된 PMSI(이를 PMSI_provided라 하자)를 이용하여 TD에게 현재의 PMSI(이를 PMSI_cur라 하자)를 요청한다. 이때 TD는 GMSC에게서 받은 PMSI_provided와 MS로부터 받은 ACK 속에 포함된 PMSI(이 값은 MS가 ACK를 보낼 당시에 생성한 값으로 TD가 이 값을 받아 자신의 테이블 내에 보관한다. 이를 PMSI_acked라 하자) 값을 비교하여 이 두 값이 같으면 PMSI_cur를 제공하게 된다.

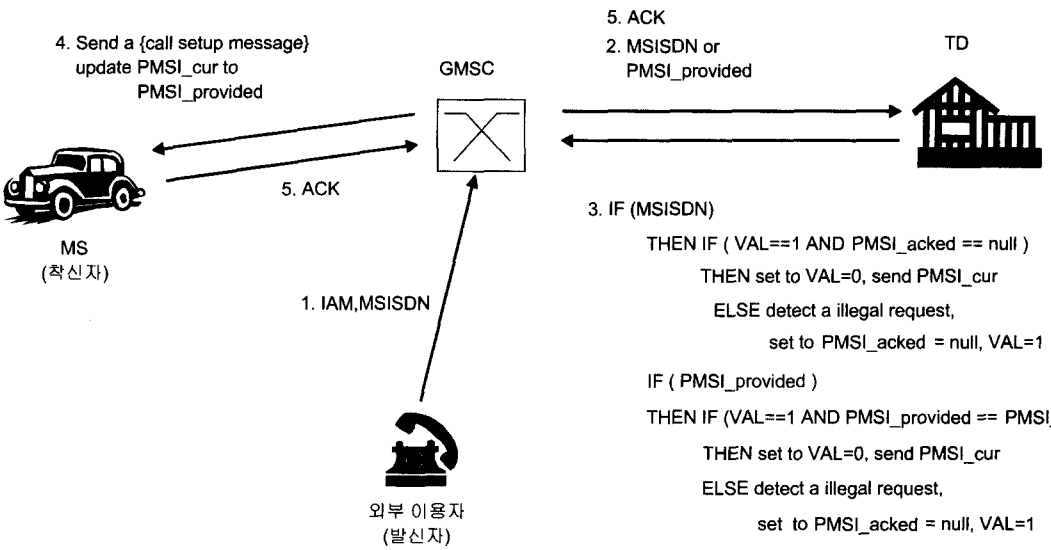
만일 이 과정에서(NP측 GMSC로부터 동일 MS로의 두 번째 호 연결 요청시) 바로 직전에 알려준 PMSI 즉, PMSI_provided를 가지고 GMSC가 요청을 하지 않았다든지, 아니면 첫 번째 요청에 대해 MS로부터 응답 메시지인 ACK가 TD로 도착하지 않았을 경우, TD는 NP가 불법적인 요청을 시도한 것으로 판단하여 곧바로 프로세스를 중지하게 된다. 왜냐하면 전자의 경우, 정해진 규칙에 어긋난 비정상적인 시도이며, 후자의 경우 정상적인 외부 이용자로부터의 호요청이 있었다면 NP는 MS로부터 ACK 메시지를 넘겨받아 TD에게 전달했을 것이다. 따라서 그 즉시 ACK 메시지가 도착하지 않았다는 것은 NP측에서 실제 외부 이용자로부터의 호요청이 아닌 불법적인 시도로 인해 TD에게 PMSI를 요청한 것으로 판단할 수 있기 때문이다. 물론 통신 장애 등을 이유로 그 즉시 ACK 메시지가 오지 않을 수 있다. 이들에 대한 해결 방법은 3.1절의 분석부분에서 다시 논의가 되겠지만 일례로, 호요청시 일정 횟수(예를 들어, 3회)를 두어 PMSI를 재차 알려주는 것을 제한하는 방법 등을 제안한다. 엄밀히 말해, 본 방법에서 이러한 불법 시도를 감지하는 시기는 NP로부터 현 PMSI에 대한 두 번째 요청시가 된다. 물론 이 방법은 첫 번째 요청시 현 PMSI 값을 무조건 알려준다는 단점이 있다. 그러나 이 값을 한번 알려준다고해서, 다시 말해 NP가 한번 정도의 현 PMSI를 안다고 해서 실제 그 MS가 누구인지를 알 수 없을뿐더러 앞으로의 위치 이동들에 대한 추적 또한 불가능하다.

제안하는 방법을 기술하기 위해 필요한 각종 표기들은 다음과 같으며, 그 외의 표기들은 이전에 정의한 것들과 동일하다.

[표 기]

- PMSI_cur : MS와의 동기화 시간에 따라 주기적으로 TD가 생성하는 현재의 PMSI 값.
- ACK : MS가 NP를 통해 외부 이용자로부터 착호 요청을 받은 데 대한 응답으로 TD에게 보내는 응답 메시지. 이 값은 r, PMSI_cur, 그리고 t를 비밀키 K[1]로 암호화한 값에 PMSI_cur를 연접한 메시지이다. 여기서 r은 임의의 정수, t는 MS가 메시지를 보낼 당시의 시간(만일, 공개키기반 구조하의 환경일 경우 이 값은 MS가 서명한 타임스탬프가 될 수도 있다).
- PMSI_acked : MS가 메시지 ACK를 보낼 당시에 생성한 PMSI_cur 값으로, 나중에 ACK를 전송받은 TD가 자신 테이블 내에 보관하며 초기값은 null이다.
- PMSI_provided : 가장 최근에 TD로부터 부여받은 PMSI 값으로 이 값은 NP 내에 있는 GMSC 테이블에 보관된다. 초기값은 null이다.
- VAL : 1비트 벡터로, 만일 MS로부터 TD가 ACK 메시지를 받은 경우는 1이 되며 그렇지 않은 경우는 0이다.

1) MS와 TD간의 단기공유비밀키(short term secret key)로 MS와 TD간에 각각 독립적으로 계산되며 정해진 주기(실제 시스템 적용시 요구되는 보안상의 레벨에 따라 짧게는 일주일에서 길게는 한달 단위)에 따라 갱신된다. MS와 TD간의 장기공유비밀키(long term secret key)를 KMT, 암호학적인 일방향 함수를 F, MS와 TD간에 미리 정한 동기화 시간(주기적으로 갱신됨)을 T라 할 때, 비밀키 K=F(KMT, T)이다.



GMSC 테이블

MSISDN	PMSI_provided	IAM
123 - 456	3124632	-

TD 테이블

MSISDN	PMSI_acked	PMSI_cur	VAL
123 - 456	3124632	1631275	0

(그림 6) 제안하는 방법

이때 이 값은 TD 테이블 내에 보관되며 초기값은 1이다.

제안하는 방법의 경우는 이전 TP 방법과는 달리 앞서 말한 PMSI_provided라든가 PMSI_acked 값 등을 보관하기 위한 장소가 요구된다. 이러한 장소의 설정을 위해 본 방법에서는 NP(특히, NP 내의 GMSC)와 TD 각자가 자신의 서버 내에 일종의 테이블을 유지하는 것으로 가정하였다. 아울러, 제안하는 방법은 아래와 같다((그림 6)참조).

[단계 1] 외부 이용자(발신자)의 통화 요청 단계

외부 이용자가 MS와의 통화를 위해 NP 내의 GMSC에게 IAM과 MSISDN 메시지를 전송한다.

[단계 2] GMSC의 현 PMSI 요청 단계

GMSC는 자신의 테이블 내에 보관된 PMSI_provided 값을 확인하여 만일 이 값이 null이라면 MSISDN을, 그렇지 않다면 PMSI_provided에 저장된 값을 TD에게 보내 현 PMSI를 요청한다.

[단계 3] NP의 불법행위 감지 후 TD가 현 PMSI를 알려주는 단계

① MSISDN을 전송받은 경우, TD는 먼저 자신 테이블 내에 VAL 값이 1이면서 동시에 PMSI_acked가 null인지를 확인하여 만일 그렇다면 VAL을 0으로 갱신한 다음 PMSI_cur를 GMSC에게 보내고, 그렇지 않다면 GMSC 측의 불법시도를 감지하고 보관중인 현 PMSI_acked를 null, VAL을 1로 재초기화한 다음, NP에게 오프라인으로 이의를 제기한다.

② GMSC로부터 PMSI_provided를 전송받은 경우, TD는 먼저 자신 테이블 내에 VAL 값이 1이면서 동시에 PMSI_provided가 PMSI_acked와 같은지를 확인하여 만일 그렇다면 VAL을 0으로 갱신한 다음 PMSI_cur를 GMSC에게 보낸다. 그렇지 않다면 GMSC 측의 불법시도를 감지하고 보관중인 현 PMSI_acked를 null, VAL을 1로 재초기화한 다음, NP에게 오프라인으로 이의를 제기한다.

[단계 4] MS와의 연결 설정 단계

GMSC는 MS에게 {call setup message}를 전달하여 외부 이용자와의 연결을 설정한 다음, TD로부터 전송받은 PMSI_cur 값을 자신 테이블 내에 PMSI_provided 값으로 갱신한다. 만일 GMSC측에서 MS로의 연결시 TD가 알려준 PMSI가 자신의 내부 데이터베이스인 HLR과 VLR에 존재하지 않을 수 있다. 왜냐하면 GMSC에서 MS로의 연결시, 이 과정에서 MS가 새로운 PMSI로 그 값을 갱신했거나 아니면 아직 갱신이 안되었을 수 있기 때문이다. 따라서 이러한 경우에는 GMSC가 TD에게 재차 현 PMSI를 요청함으로써

갱신된 PMSI를 이용하여 MS로의 연결을 시도할 수 있다. 이때 TD는 자신이 이미 알려준 바 있는 PMSI를 기준으로 동기화 시간을 검토하여 이전 혹은 그 이후에 생성한 다른 PMSI를 알려준다.

[단계 5] MS의 응답 메시지 ACK 생성과 갱신

MS는 {call setup message}를 확인한 후, 응답 메시지 ACK를 생성하여 GMSC를 통해 TD에게 전달한다. 이때 PMSI_cur 값은 현재의 PMSI이긴 하지만 보다 정확히 말해 TD가 GMSC에게 알려줄 당시의 동기화 시간에 따라 계산된 값이다. 만일 여기서 MS가 GMSC로부터 통화연결 요청을 받은 직후, PMSI를 새로이 갱신해야할 경우라면 NP 측에 갱신된 PMSI를 등록하되 ACK에 포함되는 PMSI_cur 값은 그 이전의 PMSI 값 즉, TD가 GMSC에게 알려줄 당시의 동기화 시간에 따른 값을 이용한다.

[단계 6] TD의 ACK 확인 단계

TD는 암호화된 MS로부터의 ACK 메시지를 MS와의 단기 공유비밀키인 K를 이용하여 복호화한 후 PMSI_cur 값을 자신 테이블 내에 PMSI_acked 값으로 갱신한다.

만일 [단계 3]에서 GMSC로부터의 불법시도가 감지된 이후에 외부 이용자로부터 동일 MS로의 정상적인 착호 요청이 있을 경우는 GMSC 또한 PMSI_provided 값을 null로 재초기화하여 본 프로토콜의 [단계 1]부터 새로 시작한다.

3.1 분 석

본 절에서는 제안한 방법의 안전성과 관련하여 내부 이용자인 NP 또는 기타 제3자로부터 MS의 위치를 파악하거나 추적하려는 불법 시도를 그 사례별로 어떻게 감지해 낼 수 있는지에 대해 살펴보고 그 효율성 또한 분석해 보고자 한다. 먼저 본 프로토콜의 안전성과 관련하여 아래와 같이 불법 시도가 발생할 수 있는 각종 유형들을 분류하고 감지 방법들을 제시하였다.

[Case 1] 외부 이용자로부터 실질적인 착호 요청이 없었는데도 불구하고 만일 GMSC가 MSISDN을 이용하여 TD에게 불법적으로 MS의 현 PMSI를 요청할 경우로, 이 경우는 그 직전 요청이 어떠했느냐에 따라 아래와 같이 분류된다.

- 외부 이용자로부터의 실 요청에 의해 직전에 정상적으로 PMSI를 요청한 적이 있는 상태에서 이번에 처음인 것처럼 불법 요청을 시도하는 경우
- 외부 이용자로부터의 실 요청이 없었는데 직전에 불법요청을 한번 한 상태에서 재차 처음인 것처럼 불법 요청을 시도하는 경우
- 외부 이용자로부터 실 요청이 없었는데 이번에 처음으로 불법요청을 시도하는 경우

첫 번째 경우는 프로토콜 [단계 3]의 첫 번째 과정에서 PMSI_acked 값이 null인가를 확인함으로써 쉽게 감지된다. 왜냐하면 직전에 정상적으로 PMSI를 요청한 상황이라면 TD는 이미 그때 MS로부터의 ACK 메시지를 받거나 하여 한번 알려준 적이 있는 PMSI 값 즉, PMSI_acked 값이 저장되어 있을 것이다. 따라서 이 경우는 PMSI_acked 값이 null이 아니므로 감지된다.

두 번째 경우 역시 프로토콜 [단계 3]의 첫 번째 과정에서 VAL 값이 1인가를 확인함으로써 쉽게 감지된다. 왜냐하면 직전에 불법요청을 했다는 것은 그 요청을 MS에게 전달하지 않았거나 전달했다하더라도 위조된 무의미한 {call set-up message}를 전달했을 것이다. 여기서 만일 전자의 경우라면 당연히 ACK 메시지는 TD에게 전달되지 않을 것이며, 따라서 VAL 값은 0인 상태가 된다. 만일 후자의 경우라면 혹 MS가 ACK 메시지를 보낼 수 있다. 이러한 경우는 본 프로토콜에는 기술되지 않았지만 MS측에서 정책적으로 일정 상한 횟수(예를 들어, 3회)를 정해 기록해 둠으로써 그 횟수를 초과할 경우 TD에게 알리거나 아니면 ACK 메시지를 보내지 않는 방법을 제안한다.

세 번째 경우는 이전에도 잠시 언급했지만 불행히도 당장은 감지가 불가능하다. 하지만 동일 MS로의 다음 번 착호 요청시 본 프로토콜 [단계 3]의 첫 번째(만일, 다음 번에도 처음인 것처럼 MSISDN을 이용하여 요청했다면) 또는 두 번째(다음 번에는 PMSI_provided를 이용하여 요청했다면) 과정에서 감지된다. 여기서 만일 GMSC가 재차 불법시도를 요청했다고 가정하자. 이렇게되면 그 요청이 MSISDN으로 인한 것(이 경우는 위 두 번째 경우에 해당된다)이든 아니면 PMSI_provided로 인한 것이든 상관없이 [단계 3]에서 VAL 값이 1인지를 확인함으로써 감지된다.

한편 프로토콜 진행상 그 즉시 감지를 못한다는 것은 효율성 면에서 단점일 수 있다. 그러나 다음 번 요청에 대해서는 감지가 확실하며, 아울러 한번 PMSI를 알려준 것으로 인해 실제 MS가 누구인지를 알아내거나(MS에 대한 실제 아이디를 모르기 때문에) MS에 대한 위치를 추적한다는(PMSI 값이 일정 주기마다 바뀌기 때문에) 것은 불가능하다.

[Case 2] 외부 이용자로부터 실질적인 착호 요청이 없었는데도 불구하고 만일 GMSC가 현재 테이블 내에 보관하고 있는 PMSI_provided를 이용하여 TD에게 불법적으로 MS의 현 PMSI를 요청할 경우로, 이 경우 또한 그 직전 요청이 어떠했느냐에 따라 아래와 같이 두 사례로 분류한다.

- 외부 이용자로부터의 실 요청에 의해 직전에 정상적으로 PMSI를 요청한 적이 있는 상태에서 이번에 처음으로 불법 요청을 시도하는 경우
- 외부 이용자로부터의 실 요청이 없었는데 직전에 불법 요청을 한번 한 상태에서 재차 불법 요청을 시도하는 경우

첫 번째 경우는 위 [Case 1]의 세 번째 경우와 마찬가지로 당장은 감지가 불가능하다. 하지만 동일 MS로의 다음 번 착호 요청시 본 프로토콜 [단계 3]의 두 번째 과정에서 감지된다. 우선 GMSC가 현재 테이블에 보관하고 있는 PMSI_provided 값을 이용한 것은 본 프로토콜 진행상 정당한 행위이다. 그러나 실제 외부 이용자로부터의 착호 요청이 없었기 때문에 [단계 4]에서 MS로의 호 연결이 이루어지지 않으며 또한 [단계 5]에서 ACK 메시지 또한 전송하지 않을 것이다. 따라서 VAL 값은 그대로 0으로 유지된다. 만일 다음 번에 동일 MS로의 실제 요청이 있거나 혹은 GMSC가 불법적으로 재요청할 경우는 [단계 3]의 두 번째 과정에서 VAL 값이 1인지를 비교하거나 PMSI_provided가 PMSI_acked와 같은지를 확인함으로써 감지된다. 물론 본 프로토콜의 [단계 4]에서 GMSC가 {call setup message}를 위조하여 보내고 [단계 5]에서 MS가 ACK 메시지를 생성하여 TD에게 보낸다 하더라도 앞서 언급한 상한 횟수를 두어 감지한다.

두 번째 경우는 위 [Case 1]의 두 번째 경우와 유사한 방법으로 해결할 수 있다. 즉, 프로토콜 [단계 3]의 두 번째 과정에서 VAL 값이 1인가를 확인함으로써 쉽게 감지된다. 이 과정에 대한 해결 방법은 위 [Case 1]의 두 번째 경우를 참조하기 바란다.

[Case 3] GMSC가 현 PMSI를 요청시 정당한 PMSI_provided 값이 아닌 허위의 값이나 그 이전에 한번 사용한 적이 있는 값을 이용할 경우

이 경우는 본 프로토콜 [단계 3]의 두 번째 과정에서 GMSC가 보내온 허위의 PMSI_provided 값이 TD 자신이 보관하고 있는 PMSI_acked와 같은지를 비교해봄으로써 쉽게 감지된다. 왜냐하면 PMSI_acked 값은 바로 직전 요청시 GMSC의 통화 연결에 의해 MS가 TD에게 보낸 ACK 메시지 속에 포함된 그 당시의 PMSI 값이기 때문이다.

[Case 4] GMSC가 현 PMSI를 알기 위해 실제 MS로의 연결은 하지 않는 대신 MS가 TD에게 보내는 ACK 메시지를 위조하여 마치 MS가 보낸 것처럼 위장할 경우

이 경우는 GMSC 측에서 이전에 보낸 ACK 메시지를 재사용할 수는 있지만 허위의 ACK 메시지를 TD에게 보낼 수는 없다. 왜냐하면 암호화된 ACK 메시지인 {(r,PMSI_cur,t)K}를 복호화 하거나 새로운 메시지를 생성하려면 MS와 TD 둘만이 알고있는 비밀키인 K를 알아야하는데 GMSC가 이 키를 모르고서 허위 메시지를 임의로 생성한다는 것은 불가능하다.

앞서 말한 것처럼 MS가 한번 보낸 적이 있는 ACK 메시지를 또 다시 이용(재사용)할 수 있다. 그러나 이 경우 역시 암호화된 ACK 메시지를 TD가 복호화하여 그 속에 포함된 PMSI_cur 값과 보낼 당시의 동기화 시간 t를 확인해 보면 이 메시지가 재사용 되었다는 것은 쉽게 검증된다.

[Case 5] 내부 이용자인 NP측 GMSC가 아닌 제 3자가 MS의 위치를 추적하려 할 경우

만일 제3자가 NP의 도움 없이 단독으로 MS의 위치를 추적하려할 경우 통신 링크 상에 도청을 통한 방법으로 각 개체들이 주고받는 메시지를 가로챌 수 있다. 본 프로토콜에서는 각 개체들간에 다양한 메시지들을 주고받는다. 이들 가운데 도청을 통해 알아 낼 수 있는 메시지들은 기껏해야 PMSI_provided, ACK, 그리고 MSISDN 정도이다.

첫째, PMSI_provided인 경우 MS의 현재 PMSI가 아니며, 또한 이 값을 이용하여 MS의 위치를 알아내기 위해서는 NP 내부의 데이터베이스인 HLR과 VLR에 접근 할 수 있어야 한다. 그러나 이것은 NP와의 결탁이 없고서는 불가능하다. 설사 결탁한다 하더라도 앞서 기술한 [Case 1~Case 4]에 의해 NP의 불법 시도들이 감지된다. 그리고 두 번째로 ACK 메시지를 안다하더라도 이 값은 비밀키로 암호화된 값이기 때문에 이를 복호화하여 원 메시지의 내용을 알아낸다는 것은 계산량적인 측면에서 불가능하며, 설사 시간이 걸려 이 값을 알아낸다 하더라도 PMSI 값은 주기적으로 바뀌기 때문에 사실상 추적이 힘들다. 끝으로 제3자가 MSISDN을 안다하더라도 지속적으로 현 PMSI를 알아내지 못하면 이것 역시 추적이 불가능하다.

[Case 6] 내부 이용자인 NP와 제3자가 결탁하여 MS의 위치를 추적하려 할 경우

앞서 살펴본 [Case 1~4]의 경우, 모두가 내부 이용자인 NP측 GMSC에서의 불법시도와 관련된 유형들이다. 또한 서로 결탁한다 하더라도 제 3자의 경우 NP만큼 많은 정보를 얻을 수 없다. 따라서 이 문제의 경우는 [Case 1~4]의 내용들을 참조하기 바란다.

[Case 7] NP측에서 실제 외부 이용자로부터의 요청이 없음에도 불구하고 임의로 요청이 온 것처럼 위장하여 MS가 TD에게 ACK 메시지를 보내도록 할 수 있다. 아마도 전화를 받는 수신 당사자인 MS는 무의미한 통화 또는 불완전한 통화 연결이 될 것이다. 이러한 경우 MS는 NP측의 불법 행위를 의심해 볼 수 있다. 또는 NP측에서 불법 시도를 위해 통화중이라든가 혼선, 단선, 통화연결 또는 위치 등록오류 등 통화 연결에 대한 장애를 이유로 어쩌면 주기적으로 TD에게 PMSI를 요청할 수 있다. 즉, 문제는 이러한 무의미한 통화 또는 장애의 요인이 자연적이든 의도적이든 MS나 혹은 TD가 이를 확인할 방법이 없다는데 있다. 이러한 경우들에 대비하여 근본적인 해결책은 아니지만 아래와 같은 몇 가지 대안들을 제안한다.

- 장애로 인한 NP의 요청시 TD가 PMSI를 알려주거나, 혹은 MS가 무의미한 통화 요청을 받았을 경우 ACK 메

시지를 TD에게 보내는 것을 일정기간(예를 들어, 1시간 혹은 1일)에 n(예를 들어, 3회)번으로 제한한다. 이 경우 PMSI가 변화되는 주기를 짧게 할수록 MS에게 보다 안전하다.

- 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 상태(power on 등)를 통보해올 때 다시 서비스를 이용하도록 한다.

여기서 실질적으로 고려해 볼 수 있는 방법은 첫 번째 방법이 적합하다. 나머지 두 방법은 예방차원에서 이용될 수 있다. 만일 TD와 NP가 공모를 할 경우에 기존의 TP 방법에서 소개한 분산 TP 방법[3]을 제안한 방법에 이용함으로써 해결 할 수 있다. 즉, 하나의 TD를 n개의 TD로 분할하여 PMSI를 생성하도록 함으로써 만일 n개 중 하나의 TD가 정직하다면 공모를 방지할 수 있다.

- 익명성을 제공하지 않을 경우 : M_{GM}/B_{GM}
- 익명성을 제공하는 경우 : $2(M_{GT}/B_{GT}) + (M_{GM}/B_{GM})$
- 익명성을 제공하고 MS로부터 TD로 메시지 ACK가 있는 경우 : $2(M_{GT}/B_{GT}) + (M_{GM}/B_{GM}) + (M_{MT}/B_{MT})$
  - M_{GT} : GMSC와 TD 사이에 메시지 전송량
  - B_{GT} : GMSC가 TD 사이의 채널별 할당 대역폭
  - M_{GM} : GMSC에서 MS로 호 설정에 따른 메시지 전송량
  - B_{GM} : GMSC에서 MS로 호 설정시 채널별 할당 대역폭
  - M_{MT} : MS에서 TD로의 메시지 ACK 전송량
  - B_{MT} : MS에서 TD로의 응답시 채널별 할당 대역폭

(그림 7) 호 설정을 위한 메시지 교환 부하

만일 제안한 방법을 기존 TP 방법과의 능동적인 공격에 대한 대비 차원에서 살펴본다면 제안한 방법이 보다 효율적이다. 기존 TP 방법에서 언급한 도달가능 매니저를 따로 이용하지 않고도 MS가 착호 연결을 받은 응답으로 ACK 메시지를 보냄으로써 좀더 효율적으로 NP의 능동적인 공격을 막을 수 있다. 즉, 기존 시스템의 아키텍처는 그대로 이용하되, 단지 GMSC측 테이블 내에 PMSI_provided 필드를 하나 더 두고, 단지 GMSC로부터 호 연결 메시지를 받을 때 ACK 메시지만을 추가하여 전송하기 때문에 기존에 도달가능 매니저를 추가하는 방법과는 달리 훨씬 비용부담이 적다.

한편, 위 (그림 7)에서 보는 바와 같이 기존 방법에 추가되는 시스템의 부하는 기존의 M_{GM}/B_{GM}에 비해 $2(M_{GT}/B_{GT}) + (M_{MT}/B_{MT})$가 추가되는 것으로 분석된다. 이는 사용자의 익명성 제공이라는 부가 서비스측면에서 볼 때 충분히 감내할 만한 부하이다.

끝으로, MS의 위치 프라이버시 보호 여부에 따른 기존 방법들과 제안한 방법을 비교해 보면 <표 1>과 같다. <표 1>에서 △로 표기한 것은 TP 방법에서 제 3자와 NP와의 공모시에도 이들의 수동공격을 막을 수는 있지만 능동공격을 막을 방법을 없기 때문이다. 또한 도달가능매니저를 이용할 경우 NP의 능동적인 공격에 대해 외부 발신자가 보낸 개인 정보와 통화주제 등을 NP가 중간에서 위조하거나, 혹은 외부에서 통화요청이 없는 데도 불구하고 마치 있는 것처럼 거짓으로 위장하여 발신자의 개인정보 등을 도달가능매니저를 통해 MS에게 제공할 수 있기 때문에 공격에 완벽한 대비는 하지 못한다.

〈표 1〉 MS의 신분 및 위치 프라이버시 제공 유무에 따른 기존 방법들과의 비교

		GSM [7]	TP 방법 [3]	TP 방법+도달가능 매니저 방법[6]	제안하는 방법
신분프라이버시 보호방법		TMSI 이용	PMSI, TD 이용	PMSI, TD 이용	PMSI, TD 이용
위치 프라이버시 보호 유무	제 3자	○	○	○	○
	NP의 수동 공격	×	○	○	○
	NP의 능동 공격	×	×	△	○
	제 3자와 NP와의 공모	×	△	△	○

4. 결 론

이동통신환경이 현재 제3세대로의 변환기를 맞이하고 있는 지금, 이동통신에 있어서 보안은 그 중요성이 점차 높아지고 있다. 본 논문에서는 이동통신 환경에서 NP측에 대해 MS의 위치 추적을 막고 개인 사생활을 보호하며 더 나아가 NP측의 불법 시도를 막을 수 있도록, 기존 Kesdogan의 TP 방법을 개선하였다.

본 논문에서 제안하는 방법은 기존 TP 방법에서 언급한 도달가능 매니저에 비해 새로이 하드웨어를 추가해야하는 비용 부담이 적으며, 그 방법에 대한 기술이 보다 실질적이고 구체적이다. 아울러 제안한 방법을 이용할 경우, 차세대 이동통신에 응용할 수 있을 뿐만 아니라 더 나아가 무선통신 환경이나 이동 멀티미디어 서비스 등에 응용할 수 있다. 향후 연구과제로는 제안한 방식을 실제 시뮬레이션하여 기존의 GSM 및 TP 방법들과의 성능을 비교, 이를 실제 확인하려 한다.

참 고 문 헌

[1] H. Federrath, A. Jerichow, D. Kesdogan and A. Pfitzmann, "Security in Public Mobile Communication Networks," Proc. IFIP/TC6 Personal Wireless Communications, Prague, pp. 105-116, 1995.

[2] D. Kesdogan, H. Federrath, A. Jerocow and A. Pfitzmann, "Location Management Strategies increasing Privacy in Mobile Communication Systems," Proc. The 12th IFIP International Information Security Conference SEC96, Chapman & Hall, 1996.

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

[4] D. Farber and K. C. Larson, "Network Security via Dynamic Process Renaming," Proc. The 4th Data Communications Symposion, Quebec Canada, Oct., 1975.

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

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

[7] ETSI, GSM Recommendations : GSM 01.02-12.21, Feb., 1993.

김 순 석

e-mail : sskim@halla.ac.kr

1997년 진주산업대학교 전자계산학과(공학사)

1999년 중앙대학교 컴퓨터공학과(공학석사)

2003년 중앙대학교 컴퓨터공학과(공학박사)

2003년~현재 한라대학교 정보통신공학부 전임강사

관심분야 : 정보보호, 암호응용 등

이 창 훈

e-mail : be4u@hnu.hankyong.ac.kr

1987년 광운대학교 전자계산학과 이학사

1989년 중앙대학교 전자계산학과(이학석사)

1998년 중앙대학교 컴퓨터공학과(공학박사)

1999~2002년 중앙대학교 정보통신연구소 연구전담교수

2002년~현재 한경대학교 컴퓨터공학과 조교수

관심분야 : 소프트웨어공학, 형식명세기법, 컴포넌트 기반 방법론, 품질 및 프로세스개선 등