IMT-2000에서 사용자 식별을 위한 인증 프로토콜 설계

서동운, 남기모, 박재균, 강성용, 김정훈, 박석천
경원대학교 전자계산학과

Design of Authentication Protocol for User Identification in IMT-2000

Dong-Woon Seo, Ki-Mo Nam, Jae-Kyun Park, Sung-Yong Kang, Jung-Hoon Kim, Seok-Cheon Park
Dept. of Computer Science, Kyungwon University

요 약

IMT-2000은 유선통신 시장에서 확고히 자리잡은 인터넷 서비스와 멀티미디어 고속 데이터 정보를 무선으로 공급하고자 하는 사용자의 요구를 충족시키기 위해 등장하였다. 그러나 이러한 서비스는 무선망을 통하여 제공되기 때문에 그 특성상 전송로가 노출되어 있어 허가받지 않은 사용자에 의한 불법적인 절취사용과 악의를 가진 제3자가 공유된 전송매체를 통해 전파를 도청하기 쉽다는 문제점을 가지고 있다. 따라서 이동 무선 환경에서의 보안과 인증 문제는 필수적인 사항이라고 할 수 있다. 이를 위해 본 논문에서는 기존의 인증 방식을 분석하고 사용자의 식별을 위한 쌍방향 인증 프로토콜을 설계하고 그 효율성을 분석하였다.

1. 서론

우리 나라의 이동통신은 제 1세대와 2세대를 거치면서 비약적인 발전을 거듭하였으며, 많은 가입자를 확보해 나가고 있다. 그러나 1세대 시스템과 2세대 시스템은 기본적으로 음성위주의 서비스를 염두에 두고 개발하였기 때문에 이동 멀티미디어 서비스와 같은 고속 무선통신 서비스 수요자의 요구를 충족시키기에는 어려움이 있다. 또한 이동전화 서비스 사업자의 입장에서 미래의 수익은 음성위주의 서비스가 아닌 데이터와 이동 멀티미디어 서비스와 같이 고도화된 서비스를 통하여 얻을 수 있을 것이다. 이에 따라 유선통신 시장에서 확고히 자리잡은 인터넷 서비스와 멀티미디어 고속 데이터 정보를 무선으로 공급받고자 하는 사용자의 요구를 충족시키기 위하여 1, 2세대의 시스템보다 더욱 발전된 개념의 이동통신 시스템인 IMT-2000이 등장하게 되었다[1][2]. 제 3세대 이동통신 시스템인 IMT-2000의 특징은 현재 유선망에서 제공하고 있는 서비스의 대부분을 무선망에서도 사용할 수 있게 하면서 유선망에서의 품질을 보장한다는 목표를 가지고 있다. 그렇지만 무선망은 전송로가 노출되어 있어서 정당하지 않은 사용자에 의한 불법적인 절취사용과 악의를 가진 제3자가 공유된 전송매체를 통해 전파를 도청하기 쉽다는 문제점을 가지고 있다[3].

따라서 본 논문에서는 위에서 언급한 문제의 해결과 함께 기존의 방식에서 단방향 인증을 제공하는 것과는 달리 보다 강력한 인증을 제공하기 위해서 IMT-2000에서 사용하는 가입자의 식별자를 이용한 쌍방향 인증 프로토콜을 설계하였다.

2. IMT-2000과 보안 구성도

본 절에서는 인증을 위한 IMT-2000과 그에 따른 보안 요소에 대하여 알아본다.

2.1 IMT-2000의 망 구성도

IMT-2000에서 제공되는 서비스 중 사용자들이 가장 많이 사용할 것으로 예상되는 서비스는 정보 전송등 패킷 위주의 서비스가 될 것으로 예상하고 있다.

따라서, 패킷 데이터를 처리하기 위해 IMT-2000은 그림 1과 같은 네트워크 아키텍처와 인터페이스를 제공하고 있다[4].

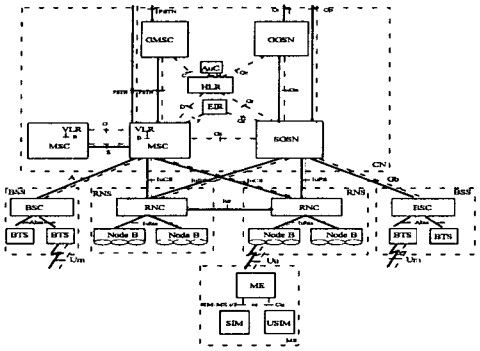

그림 1. IMT-2000의 네트워크 아키텍처와 인터페이스

위의 그림 1에서 인증을 위해 필요한 기능 개체로 AuC (Authentication Center), MSC (Mobile-services Switching Center), HLR (Home Location Register), VLR (Visitor Location Register), MS (Mobile Station)가 포함된다[1].

MS에는 사용자의 식별을 위한 식별자를 가지고 있는데, 인증을 위해서 IMSI, TMSI 등의 식별자를 사용한다.

IMSI (International Mobile Subscriber Identity)는 망 운영자가 서비스를 위해 사용자를 등록할 때, 각각의 사용자에게 요청하는 유일한 식별자로써, 이 값은 SIM (subscriber Identity Module)에 저장되어 있다. TMSI (Temporary Mobile Subscriber Identity)는 가입자의 현재 위치를 항상 갱신시키기 위해서 VLR에 응답으로 보내주는 값이다. TMSI는 거의 모든 경우 IMSI를 대신하는 값으로 사용된다. 이것은 IMSI의 값이 노출되면 가입자에 대한 많은 정보가 유출된다는 것을 의미하는데, 이러한 경우를 방지하기 위해서 IMSI의 대안으로 TMSI를 사용하는 것이다. 다시 말하면 무선 구간에서 현위치의 도청 방지를 위해서 TMSI가 사용이 되고, 호시도와 위치등록시마다 TMSI를 변경함으로써 망내에 보안관리를 제공한다.

2.2 IMT-2000에서의 보안 요소

앞에서 언급한 내용을 바탕으로 IMT-2000에서 보안을 제공하기 위한 구조를 그림 2에 나타내었다[4].

아래의 그림 2에서는 다섯 가지의 보안에 관련된 부분을 정의하였으며, 각각의 그룹은 다음과 같다.

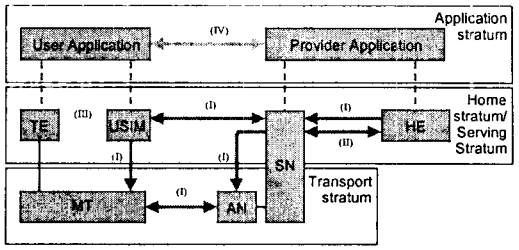

그림 2. 다섯 가지 보안 구성도

- 네트워크 액세스 보안 (I)
- 네트워크 도메인 보안 (II)
- 사용자 도메인 보안 (III)
- 어플리케이션 도메인 보안 (IV)
- 보안의 가시성과 구성 (V)

본 논문에서의 사용자 인증은 무선 환경에서 식별자를 이용한 인증 기능을 제공하기 때문에 무선 링크에서의 보안에 관련된 서비스를 제공하는 네트워크 액세스 보안에 대해 사용자 인증 프로토콜을 설계한다.

3. IMT-2000에서 사용자 식별을 위한 인증 프로토콜 설계

3.1 IMT-2000 가입자 인증 프로토콜의 요구사항

가입자 인증을 위해서는 가입자 식별자 보호 기능과 가입자 식별자 인증 기능이 동시에 수반되어야 한다. 이러한 기능은 암호 프로토콜과 함께 동시에 수반되어야 하고, 이들 프로토콜은 시스템 라이프사이클에 따라 변경된다. 이런 변경은 시스템간 교환되는 메시지의 형식을 바꾸는 것은 아니고 시스템의 대체/전환으로 이루어진다.

3.2 가입자 식별자 보호 기능 및 인증 기능 정의

본 절에서는 인증을 위해 가입자 식별자에 대한 식별자 보호 기능과 인증 기능에 대해 설명한다.

(1) 가입자 식별자 보호 기능

이 기능은 무선 선로상에서 교환하는 신호를 수신하므로써 가입자가 사용하고 있는 무선 선로상에 주어진 재원을 확인하려는 침입자로부터의 공격을 방지해주기 위

한 기능이다. 사용자 데이터와 신호에 대한 보호 기능과 사용자 위치 추적에 대한 보호 기능이 해당한다.

(2) 가입자 식별자 인증 기능

본 기능의 요구사항은 물리적인 액세스만으로는 사용자 식별을 할 수 없기 때문에 강한 인증을 필요로 하고 있고, 무선 시스템은 쉽게 도청이 되는 점을 줄이기 위해서 신뢰성을 제공하여야 한다. 또한 가입자가 넓은 지역으로 이동하기 때문에 로밍 상태에서도 보안관리가 이루어져야 한다.

3.3 가입자 식별자 보호 기능의 설계

본 논문에서는 사용자 식별을 위한 인증 기능을 제공하기 위해서 가입자 식별자의 보호 기능이 어느 범위까지 수행할 것인가를 결정하고 그에 따른 여섯 가지 경우에 대한 기능을 설계하였다.

(1) 동일한 MSC 지역내에서의 위치 갱신

이 절차는 동일한 MSC에 속하는 기존 위치 지역과 새로운 위치 지역이 있을 때 수행하는 갱신 절차이다. 여기서는 위치 갱신을 위해서 앞서 언급한 TMSI를 할당해 주기 위한 절차로써, MS가 MSC에게 위치 갱신을 위해 이전에 받은 TMSIo(old)를 전송하게 되면, 새로운 암호화 절차에 따라 관리를 수행하게 된다. 그 후에 MSC는 새로운 TMSIn(new)를 할당받게 되고, 역시 암호화 절차를 거쳐 MS에게 전송하게 된다.

(2) MSC내에 동일한 VLR에서 위치 정보 갱신

이 절차는 기존 위치 정보와 새로운 위치 정보가 같은 VLR내에 있으면서 여러 MSC에 의존해 있는 경우에 취하는 절차이다.

(3) 서로 다른 VLR사이에서 위치 갱신

이 절차는 기존 위치와 새 위치가 서로 다른 VLR에 의존할 때 TMSI와 LAI (Location Area Identification)를 사용하는 정상적인 위치 갱신 부분이다.

(4) 새로운 TMSI의 재할당

이 절차는 어떤 시점에 네트워크에 의해 주도될 수 있으며 선택적인 파라메터 설정 방법을 통해 이루어진다. 또한, 새로운 TMSI의 할당과 이에 따라 지금까지 가지고 있었던 TMSI의 해제절차로써, 할당과 해제시 암호화를 필요로 한다.

(5) 로컬내에서 통보되지 않은 TMSI

이 절차는 하나의 VLR내에서 데이터 손실시 혹은 MS가 알려지지 않은 TMSI를 사용할 때 새로운 TMSI를 할당하기 위한 절차이다.

(6) 정보 손실시 VLR사이에서 위치 갱신

이 절차는 MS를 관장하는 VLR이 데이터 손실로 어려움을 겪고 있을 때 일어나는 절차로 TMSIo와 IMSI 사이의 관계를 잃어버린 경우에는 MS의 식별자가 필요하다.

3.4 사용자 식별을 위한 인증 프로토콜 설계

사용자 식별을 위한 인증은 앞서 언급한 가입자 식별자 보호 기능에서의 인증 절차를 기반으로 하여 사용자 인증 프로토콜을 설계한다.

본 논문에서 설계한 인증 프로토콜은 기존 방식에 비해 보다 강력한 인증 기능을 제공하며 MSC에 저장·비교 기능을 첨부하여 효율성을 높였다.

3.4.1 기존의 인증 방식

기존의 사용자 인증 방식은, AuC에서 MS로 단방향 인증을 수행하는 절차를 가지고 있으며, 최소한의 인증 기능만을 제공하고 있기 때문에 보안 측면에서 상당히 취약점을 가지고 있다.

다음은 기존 인증 방식에 대한 절차를 나타냈다.

처음 VLR은 AuC에 MS의 인증을 위해 비밀공유데이터와 랜덤값을 생성할 것을 요청한다. 또한 MS는 서비스를 받기 위해 비밀공유데이터를 생성한다. 요청 메시지를 받은 AuC는 MS에게 인증 과정을 수행하도록 메시지를, 인증값 계산을 위하여 랜덤값과 같이 보낸다. MS는 랜덤값을 전송 받은 후에 cdma에서 적용하는 인증 계산을 일컫는 단어인 CAVE를 실행한다. MS는 다시 인증센터인 AuC에 계산값을 전송하고 AuC 역시 CAVE를 실행하고 인증값을 생성 후 전송 받은 값과 비교한다. 그 후 AuC는 MS에 인증 여부를 통보 후 값이 같으면 서비스를 제공에 관한 기능을 수행하는 MSC에게 서비스를 제공할 것을 지시하고 값이 다르면 인증 거부를 행함으로써 전체적인 인증 과정을 끝마친다.

3.4.2 제안한 인증 프로토콜 설계

본 논문에서 설계한 인증 프로토콜은 MS에서 AuC로, AuC에서 MS로의 인증이 가능하도록 하기 위하여, 두 가지 인증 방식을 통합한 쌍방향 인증 프로토콜을 설계하였다.

설계한 프로토콜은 기존 방식이 단일 인증 방식을 수행한 반면에, AuC와 MS간 쌍방향 인증 프로토콜을 제안하였다. 이것은 MSC에 하드웨어나 소프트웨어를 모듈화시켜 간단한 기능을 쉽게 탑재할 수 있다는 장점을 살린 것이며, MSC 자체에 값을 저장하고, 비교하는 기능을 추가시켜 단일 인증 방식을 가진 기존 방식과 비교해 볼 때, 제안한 방식이 기존 방식에 비해 전체 홉수를 줄임으로써 효율성을 높였다. 또한 인증 자체를 놓고 비교해 보았을 경우에도 쌍방향 인증을 수행하기 때문에 보다 강력한 인증을 제공하고 있다.

다음 그림 3에 설계한 인증 프로토콜의 절차를 나타내었으며, 제안한 프로토콜에 사용된 메시지는 표 1과 같이 정의하였다.

표 1. 인증 절차에 사용되는 메시지 정의

메 시 지	내 용
비밀공유 데이터	이동국의 유효성을 검증하기 위한 값
AUTHBS	RANDBS와 비밀공유데이터를 사용하여 계산한 AuC를 인증하기 위한 MS의 응답 값
AUTHU	RANDU와 비밀공유데이터를 사용하여 계산한 MS를 인증하기 위한 AuC의 응답 값
RANDBS	AuC의 인증을 위해 사용되는 랜덤 변수
RANDU	특정 MS의 인증을 위해 사용되는 랜덤 변수

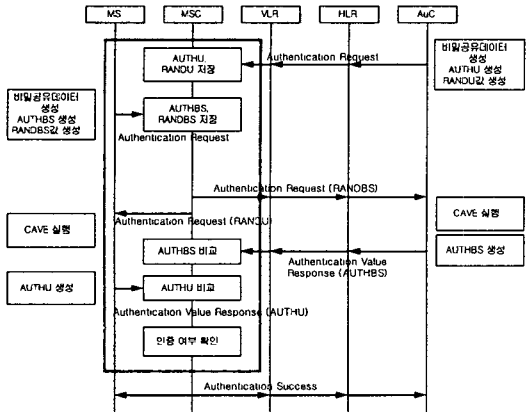

그림 3. 제안한 인증 프로토콜의 전체 절차

제안한 프로토콜의 동작 순서를 살펴보면 다음과 같다.

VLR은 MS를 감지한 후, AuC에게 MS에 대한 인증을 수행할 것을 지시한다. Authentication Request 메시지를 받은 AuC는 비밀공유데이터와 AUTHU, RANDU을 생성한 후, MSC에게 AUTHU와 RANDU 값을 전송하고, MSC는 이를 저장한다. AuC와 마찬가지로 MS도 비밀공유데이터, AUTHBS와 RANDBS를 생성하고, MSC에 전송한다. MSC는 상호간 인증을 위하여 AuC와 MS에게 서로를 인증하는데 사용될 값인 랜덤값(RANDBS, RANDU)을 전송한다. AuC와 MS는 각각의 값을 전송 받은 후, CAVE를 실행하여 인증값을 계산한다. 계산된 인증값을 MSC에 전송한다. 인증값을 전송 받은 MSC는 값을 서로 비교하여 인증 여부를 판단한다.

4. 결론 및 향후 연구 방향

이동통신의 급속한 발전과 함께 유선시장에서 확고히 자리잡은 인터넷 서비스와 멀티미디어 고속 데이터 정보를 무선으로 공급받고자 하는 사용자의 요구를 충족시키기 위해서 1, 2세대 이동통신의 장점과 멀티미디어 서비스를 제공할 수 있는 IMT-2000 시스템이 등장하게 되었다. 하지만, 무선망은 그 특성상 전송로가 노출되어 있어서 정당하지 않은 사용자에 의한 불법적인 절취사용과 악의를 가진 제3자가 공유된 전송매체를 통해 전파를 도청하기 쉽다는 문제점을 가진다.

사용자 식별을 위한 인증 기능을 제공하기 위해, 가입자 식별자의 보호 기능을 분석하여 여섯 가지 보호 기능을 설계하고 기존의 사용자 인증 방식의 단방향 인증을 수행하는 인증의 취약점을 보완한 쌍방향 사용자 인증 프로토콜을 제안하였다. 본 논문에서 설계한 쌍방향 사용자 인증 프로토콜은 기존의 인증 방식보다 강력한 인증 기능을 제공하며 MSC에 저장·비교 기능을 첨부하여 그 효율성을 높였다.

향본 논문의 제안 방안은 전자상거래, 전자결재 등의 분야에 활용이 가능할 것으로 사료되며, 향후 설계한 프로토콜의 구현 및 효율성 검증에 대한 연구가 수행될 것이다.

[참고문헌]

[1] Tero Ojanpera, Ramjee Prasad, *"Wideband CDMA for Third Generation Mobile Communications,"* Artech House, 1998

[2] Jorg Eberspacher, Hans-Jorg Vogel *"GSM Switching, Services and Protocols,"* Wiley, 1999

[3] Max Progler, and et.al., "Air Interface Access Schemes for Broadband Mobile Systems," IEEE Communication Magazine, September 1999

[4] 3GPP, 3G TS 23.002 version 3.2.0, "Technical Specification Group Services and System Aspects : Network Architecture," January 2000