2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

# IMT-2000에서 사용자 식별을 위한 인증 프로토콜 설계 및 평가

정운영, 정선화, 김성주, 이준호, 박석천
경원대학교 컴퓨터공학과
e-mail:scpark@mail.kyungwon.ac.kr

# Design and Evaluation of Authentication Protocol for User Identification in IMT-2000

Woon-Young Jung, Sun-Hwa Jung, Sung-Ju Kim,
Jun-Ho Lee, Seok-Cheon Park
Dept. of Computer Engineering, 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 무선망의 특성상 전송로가 노출되어 허가 받지 않은 사용자에 의한 불법적인 절취사용과 공유된 전송매체를 통한 전파의 도청 등의 문제점을 가지고 있다. 이러한 문제를 해결하기 위해 본 논문에서는 IMT-2000에서 사용자 식별을 위한 쌍방향 인증 프로토콜을 설계하고 그 성능을 평가하였다.

## 1. 서론

우리 나라의 이동통신은 제 1세대와 제 2세대를 거치면서 많은 발전을 이루어 왔다. 그러나 1세대 시스템과 2세대 시스템은 기본적으로 음성위주의 서비스를 염두에 두고 개발하였기 때문에 이동 멀티미디어 서비스와 같은 고속 무선통신 서비스 수요자의 욕구를 충족시키기에는 어려움이 있었다.

이에 따라 유선통신 시장에서 확고히 자리잡은 인터넷 서비스와 멀티미디어 고속 데이터 정보를 무선으로 공급받고자 하는 사용자의 욕구를 충족시키기 위하여 1, 2세대의 시스템보다 더욱 발전된 개념의 이동통신 시스템인 IMT-2000이 등장하게 되었다. 제 3세대 이동통신 시스템인 IMT-2000은 기존 유선망의 서비스를 포함하면서 유선망서비스 이상의 품질을 보장한다는 목표를 가지고 있다.

그러나 무선망은 전송로가 노출되어 있어서 정당하지 않은 사용자에 의한 불법적인 정보사용과 공유된 전송매체를 통해 전파가 도청되기 쉬운 문제점을 가진다.

따라서 본 논문에서는 위에서 언급한 문제점을 해결하기 위해 IMT-2000에서 사용하는 가입자의 식별자를 이용한 쌍방향 인증 프로토콜을 설계하고 성능을 평가하였다.

## 2. IMT-2000과 보안 요소

### 2.1 IMT-2000에서의 보안 요소

IMT-2000에서 보안을 제공하기 위한 구조를 그림 1에 나타내었다.

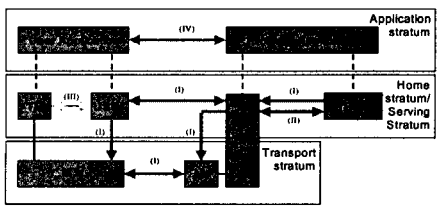


그림 1. 다섯 가지 보안 요소

위 그림에서는 다섯 가지의 보안에 관련된 부분을

정의하였으며, 각각의 그룹은 다음과 같다.

- Network Access Security (I)
- Network Domain Security (II)
- User Domain Security (III)
- Application Domain Security (IV)
- Visibility and Configuration of Security (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. 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. 가입자 식별자 보호 기능 및 인증 기능은 다음과 같이 정의된다.

(1) 가입자 식별자 보호 기능

이 기능은 무선 선로상에서 교환되는 신호를 수신함으로써 가입자가 사용하고 있는 무선 선로상에 주어진 재원을 확인하려는 침입자로부터의 공격을 방지해주기 위한 기능이다.

(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.

3.2 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 MSC (Mobile-services Switching Center)에 속하는 기존 위치 지역과 새로운 위치 지역이 있을 때 수행하는 갱신 절차이다.

(2) MSC 내에 동일한 VLR내에서 위치 정보 갱신

이 절차는 기존 위치 정보와 새로운 위치 정보가 같은 VLR (Visitor Location Register)내에 있으면서 여러 MSC에 의존해 있는 경우 취하는 절차이다.

(3) 서로 다른 VLR사이에서 위치 갱신

이 절차는 기존 위치와 새 위치가 서로 다른 VLR에 의존할 때 TMSI (Temporary Mobile Subscriber Identity)와 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 TMSIo(old) 와 IMSI (International Mobile Subscriber Identity)사이의 관계를 잃어버린 경우 MS의 식별자가 필요하다.

3.3 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.

3.3.1 기존의 인증 방식

기존의 사용자 인증 방식은 AuC (Authentication

Center)에서 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. 요청메시지를 받은 AuC는 MS에게 인증 과정을 수행하도록 메시지를 인증값 계산을 위하여 랜덤값과 같이 보낸다. MS는 랜덤값을 전송 받을 후에 cdma에서 적용하는 인증 계산을 일컫는 단어인 CAVE를 실행한다. MS는 다시 인증 센터인 AuC에 계산값을 전송하고 AuC 역시 CAVE를 실행하고 인증값을 생성 후 전송 받은 값과 비교한다. 그 후 AuC는 MS에 인증 여부를 통보 후 값이 같으면 서비스 제공에 관한 기능을 수행하는 MSC에게 서비스를 제공할 것을 지시하고 값이 다르면 인증 거부를 행함으로써 전체적인 인증 과정을 끝마친다.

3.3.2 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 MS가 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 방식에 비해 제안한 방식이 전체 홉수를 줄임으로써 효율성을 높였다.

표 1. 인증 절차에 사용되는 메시지 정의

| 메 시 지 | 내 용 |
|---|---|
| 비밀공유데이터 | 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 |

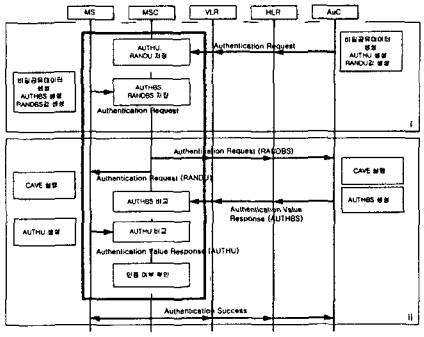


그림 2. 제안한 인증 프로토콜의 전체 절차

제안한 프로토콜의 전체 절차는 그림 2에 나타내었으며, 동작 순서를 살펴보면 다음과 같다.

VLR은 MS를 감지한 후, AuC에게 MS에 대한 인증을 수행할 것을 지시한다. Authentication Request 메시지를 받은 AuC는 비밀 공유데이터와 AUTHU, RANDU을 생성하고, 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. 인증 프로토콜 검증 및 평가

4.1 인증 프로토콜 검증

본 논문에서 설계한 인증 프로토콜의 검증을 위해 통신프로토콜의 설계와 검증에 많이 사용되는 프레디키트/액션 페트리네트를 이용해서 MS와 AuC간의 메시지를 교환하는 동작 절차를 페트리네트로 모델링하고 이를 통해 얻어낸 인증 프로토콜 모델의 도달성 트리를 도출해서 그림 3에 나타내었다.

그림 3에서 알 수 있듯이 제안한 인증 프로토콜의 도달성 트리는 데드락없이 어느 상태에서든지 초기 상태로 갈 수 있음을 보여주고, 각 장소에 토큰이 둘 이상이 있는 경우가 발생하지 않으므로 제한성을 지닌다고 할 수 있다.

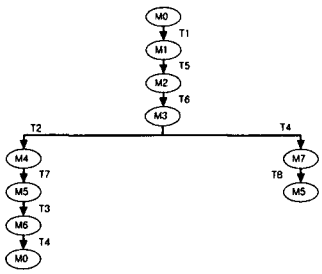


그림 3 제안한 인증 프로토콜의 도달성트리

이러한 페트리네트 모델을 이용한 검증은 본 논문에서 설계된 연동프로토콜이 에러 없이 동작함을 증명해주며, 프로토콜의 상태천이가 설계된 절차에 의해 적절히 동작함을 증명한다.

4.2 인증 프로토콜의 성능 평가

본 논문에서 제안한 프로토콜의 성능 평가를 위해 SLAM II를 사용하여 MS와 MSC, VLR간의 무선링크를 통한 전송구간과 VLR과 HLR, AuC간의 유선링크를 통한 전송구간의 전송속도 차이와 처리시간을 따로 계산을 하여 효율성을 검증하였고 핸드오프 간격에 따른 처리율의 분석 결과는 그림 4에 나타내었다. 이 결과는 기존 방식의 경우보다 제안한 방식이 잦은 핸드오프시에도 우수한 성능을 확인할 수 있었다.

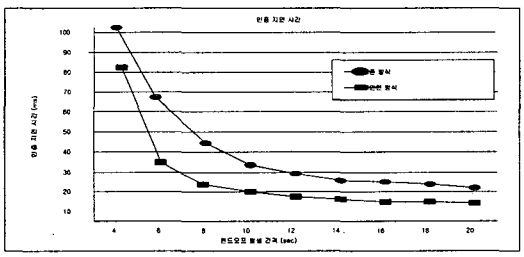

그림 4. MS 측면에서의 전송 지연 시간

그림 5에서는 인증 발생 회수에 따른 인증 처리율을 나타내었다. 이것은 제안한 인증 프로토콜이 기존 방식에 비해 처리속도가 짧아 더 많은 인증 절차를 처리 할 수 있음을 나타낸다.

따라서 본 논문에서 제안한 인증 프로토콜은 MS 측면과 AuC측면 전체에서 기존 방식보다 높은 효율의 성능을 가짐을 알 수 있다.

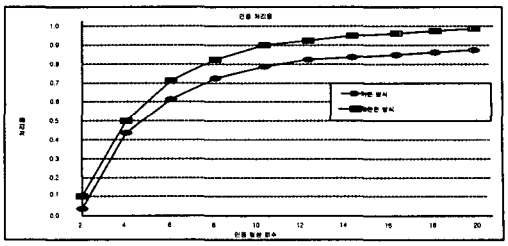

그림 5. AuC 측면에서의 처리율

## 5. 결론

이동통신의 급속한 발전과 함께 기존의 1, 2세대 이동통신의 장점과 멀티미디어 서비스를 제공할 수 있는 IMT-2000 시스템이 등장하였다. 하지만 무선망은 그 특성상 정당하지 않은 사용자의 절취사용과 전파의 도청 등의 문제점을 가진다.

본 논문에서는 위에서 언급한 문제점을 해결하기 위해서 IMT-2000에서 사용자 식별을 위한 인증 프로토콜을 설계 및 평가하였다. 또한 제안한 프로토콜을 모델링하여 동작 절차가 설계에 위배하는 가에 대한 검증과 함께 기존 방식과 비교하여 효율성을 평가하기 위하여 MS와 AuC 측면 모두를 고려하여 성능 평가를 수행하였으며, 모든 경우에서 성능이 향상되었음을 확인하였다.

본 논문에서 설계한 IMT-2000에서 사용자 식별을 위한 인증 프로토콜에 관한 결과는 향후 상용화될 IMT-2000 환경에서 강력한 인증 기능을 제공하기 위한 기반 기술로 활용될 수 있을 것으로 사료된다.

## 참고문헌

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

[2] Jong Eberspcher, Hans-Jang Vogel "GSM Switching, Services and Protocols," 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