IMT-2000 네트워크에서의 인증/보안을 위한 관리 객체 모델링

이주열*, 김성조*, 박철희**, 이승복**
* 중앙대학교 컴퓨터공학과
** 한국통신 무선통신연구소

Managed Object Modelling for Authentication and Security Management on IMT-2000 Network

Joo-Yeol Lee*, Sung-jo Kim*, Chul-Hye Park**, Soong-Bok Lee**
* Department of Computer Science & Engineering, Chung-Ang University
** Wireless Communication Research Lab, Korea Telecom

요 약

3세대 이동통신인 IMT-2000에서는 기존의 GSM과 CDMA 이동통신과 구별되는 인증 및 보안 관리가 필요하다. IMT-2000은 유무선 통합망인 동시에 기존의 망과의 연동이 가능해야 한다. 또한, 다양한 서비스 제공을 위해 IN과의 연동이 불가피하고, 글로벌 로밍 지원을 위해 보다 향상된 보안 관리가 필요하다. 본 연구에서는 IMT-2000에서의 인증/보안 네트워크 요소를 정립하고, 기능 모델을 통해 사용자 인증과 ID 보안에 대한 시나리오를 정의한 다음, 그 시나리오를 통해서 망 관리 대상 객체와 관리 정보를 도출한다.

1. 서론

3세대 이동통신인 IMT-2000에서는 기존의 GSM과 CDMA 이동통신과 구별되는 인증 및 보안 관리가 필요하다. IMT-2000 망은 유, 무선 통합 망인 동시에 전세계 어디에서나 사용될 수 있는 글로벌 로밍을 지원하고, 기존의 망과의 연동(Backward Compatibility)이 이루어져야 한다. 또한 멀티미디어 서비스를 지원해야 하므로 여러 가지 문제가 발생할 수 있다. 서비스 프로파일의 증가에 따라 가입자 정보가 다양해짐으로써 보안 관리의 문제가 보다 중요해졌으며, 글로벌 로밍을 지원하기 위한 이기종간의 보안 문제와 개인 이동성과 사용자별 과금을 지원할 수 있는 스마트카드(UIM)에 대한 향상된 보안 관리가 필요하다.

본 논문에서는 IMT-2000 망에 대한 ITU의 최근 회의자료를 토대로 IMT-2000 특유의 보안 관련 요구 사항과 관리 기능을 정의하고, 관련 시나리오를 분석해서 망 관리 정보를 도출하였다. 2장에서는 기존의 이동통신분야에서 다양하게 적용되고 있는 GSM의 보안 관리 기능 및 객체들을 분석하고, 3장에서는 이동통신분야에서 다양하게 적용되고 있는 GSM의 보안 관리를 통해서 정의된 관리 객체를 살펴본다. 4장에서는 IMT-2000의 보안 관리 요구 사항과 기능을 정의하고, 5장에서는 IMT-2000에서의 인증/보안 관리 망 자원을 선정하며 6장에서는 사용자 인증 시나리오를 분석하였다. 7장에서는 정의된 시나리오를 토대로 망 관리 대상 객체를 선정하고 나아가, TMN의 관리 기능 블록을 모델링한다.

2. 관련연구: GSM의 망 관리 객체 연구

GSM의 망 관리 모델에서 인증/보안 형태는 크게 두가지로 나뉜다. 그것은 ID의 관리이고, 다른 하나는 데이터의 관리이다. 이것은 이동통신의 특성인 공중인터페이스의 노출 위험을 최소화시키기 위함이다. ID의 관리는 불법 침입에 대한 사용자의 보호이고, 데이터의 보호는 도청 등의 프라이버시와 관련된 혹은 정확한 정보의 전송의 의미가 있다. 즉 ID의 인증과 비밀성 보장을 요구하고, 또한 데이터의 비밀성을 보장해야 한다

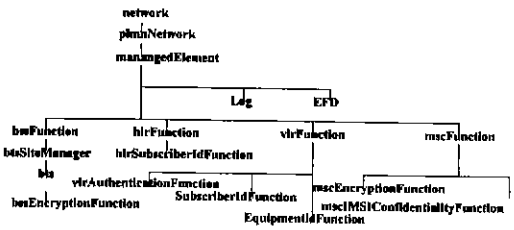
GSM에서는 사용자의 ID관리를 위해서 IMSI(International Mobile Subscriber Identification)라는 가입자별로 정해진 글로벌 ID를 TMSI(Temporal Mobile Subscriber Identification)라는 임시 대체 ID로써 기밀성을 제공한다. ID의 인증은 MS(Mobile Station)와 AUC(Authentication Center)에 각각 저장되어 있는 비밀키와 AUC에서 발생시킨 임의의 값(RAND)을 공중 인터페이스에 전달해서 결과값의 비교함로써 이루어진다 인증 후에 HLR로부터 현재 방문중인 네트워크로 사용자 프로파일이 전송된다.

따라서 GSM에서는 다음과 같은 관리 기능이 요구된다

- ▶ IMSI의 기밀성 관리 기능: VLR에 등록이 되면 MSC가 TMSI 발생
- ▶ IMSI의 인증 관리 기능: 접근 요구나 위치 갱신시 MAP(Mobile Application Part) 프로시져 발생
- ▶ 데이터 보안 관리 기능. 암호화 및 알고리즘 관리, 키 관리
- ▶ 이동 장비의 보안 관리 기능: IMEI(International Mobile Equipment Identification)이 정의된 것들은 EIR(Equipment

Identification Register)에 등록되는 과정을 겪는다.

위의 기능을 지원해줄 수 있는 보안 관리 객체의 포함 트리는 (그림 1)과 같이 정의된다.[6]



(그림 1) GSM 보안 관리 객체 포함 트리

3. IMT-2000 인증/보안 요구사항 및 관리 기능 정의

IMT-2000은 2세대 이동통신과 구별이 되는 다음과 같은 관리 요구사항을 필요로 한다.

- ▶ 공개키의 사용: GSM에서는 비밀키만 사용했으나 IS-95 계열 CDMA 이동통신부터 키의 분배에 대한 노출의 위험을 감소시킬 수 있는 공개키의 사용이 필요하다. 또한 CN과 CN사이에 공개키를 관리하는 데이터베이스가 사용될 수 있다.
- ▶ 상호 인증(Mutual Authentication): ITU X.509에 나타난 강한 인증 방법인 양방향(2-way) 인증 방식이 요구된다. UIM-MT, MT-RAN, RAN-CN 사이의 인터페이스에 적용된다.
- ▶ 글로벌 로밍(Global roaming): IMT-2000 패밀리 개념으로 이기종간의 사용자 인증 및 등급의 연동이 가능한 보안 관리가 요구된다.
- ▶ 사용자 모듈(User Identification Module) 보안: 다양해진 서비스 파라메터와 개인별 과금에 요구되는 향상된 보안 관리기 요구된다.

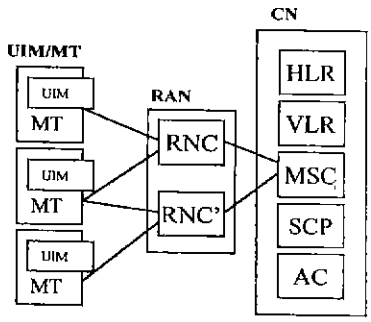
위와 같은 요구사항을 만족하는 다음과 같은 관리 기능이 정의된다.

- ▶ 키 암호화 관리 기능: 사용자 인증과 관련된 무선 채널 암호화와 복호화를 위한 기능.
- ▶ 인증 데이터 관리: 인증 정보와 인증 데이터에 대한 관리와 제어 기능이다. 공개키 저장 데이터베이스 관리 포함한다.
- ▶ 인증 처리(사용자 인증): 인증 과정을 초기화하고 제어하며, 결과를 처리하는 기능이다.
- ▶ 네트워크 fraud/abuse 제어 기능: 가입하지 않은 사용자의 불법 사용 제어를 막기 위해 필요한 정보를 제공하는 기능이다. 그 정보는 일반적인 수/송신 전화번호 정보의 모니터링, 지리적인 위치, 가입자 ID, 네트워크 요소의 주소 정보, 부가 서비스의 사용 이벤트 로그 등이다.
- ▶ ID 관리 기능: IMUI와 TMUI를 관리하는 기능이다. TMUI는 IMUI를 대신해서 사용된다. 다음과 같은 기능들을 포함한다.
  - ① IMUI를 이용해서 네트워크에 접근할 경우에 MT에 TMUI를 할당.
  - ② TMUI를 사용 중 유효시간 초과일 경우에 MT에 TMUI를 갱신.
  - ③ 이미 TMUI가 할당된 사용자가 이동시 방문한 네트워크에서 TMUI가 확인되지 않을 때, 홈네트워크에게 IMUI 요구.
- ▶ 글로벌 로밍 지원 기능: 이질적인 네트워크 사이에서의 사용자 인증 및 보안 기능이다.
- ▶ 서비스 프로파일 기밀성 보장 기능: 다양한 서비스 프로파일에 대한 파라메터 암호화 등을 제공해주는 기능이다.

4. IMT-2000 인증/보안 관리 망 관리 요소 선정 및 관리 시나리오 분석

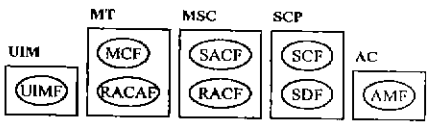
4.1 망 관리 요소 선정

IMT-2000의 기본 구조는 GSM에서 진화되었기 때문에 인증/보안 과정은 기본적으로 GSM과 비슷하다. 2장의 관련연구에서와 같이, GSM의 ID 인증에 관여 하는 네트워크 요소인 AUC, HLR, VLR, MSC 등은 IMT-2000에서도 적용되며 다양한 서비스 제어를 위해 IN과의 연동 모델을 따랐다. 따라서, 접근 허가를 제어할 수 있는 SCP(Service Control Point)가 추가되었다. 아래 그림은 IMT-2000의 인증/보안 관리에 관여하는 네트워크 요소들을 나타낸 것이다.



(그림 2) IMT-2000 보안 관련 네트워크 요소

각 네트워크 요소는 망 기능과 관리를 지원할 수 있는 기능 개체(Functional Entity)가 존재한다. IMT-2000의 기능 개체는 망의 물리적인 기능 구현뿐만 아니라 관리를 위한 논리적인 역할도 담당한다. 그 중에서 몇 가지의 네트워크 요소가 갖는 기능 개체를 살펴보면 (그림 3)과 같다.



(그림 3) 기능 개체의 예

4.2 시나리오 분석

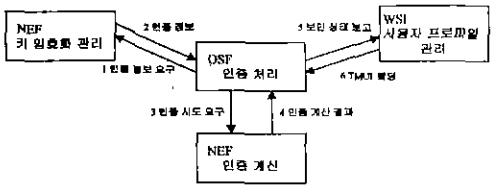
사용자 인증은 단말기가 처음 전원을 켰을 때나 새로운 지역으로 위치 갱신을 시도할 때 발생한다. 따라서 인증/보안 관리를 위한 관리 정보를 도출하고, 관리 객체를 정의하기 위해서는 사용자 인증에 관련된 시나리오를 분석을 통해 관리 정보와 필요한 행위 등

을 파악해야 한다.

기본적으로, MT가 호를 연결하려고 시도하면, 단말 접근(Terminal Access)에 대한 허가와 호 연결(Call Connection), 베어러 설정 등이 일어난다. 각각의 단계가 성공적으로 일어나면, 사용자 인증이 일어나게 된다. 위와 같은 시나리오를 통해서 IMT-2000은 홈 네트워크로부터 인증에 필요한 정보(공개키 등)를 받고, 그것을 통해서 단말기에 인증 계산을 실시한다. 인증 계산 결과를 다시 전송하여 승인 시 서비스 사용을 가능하게 한다.

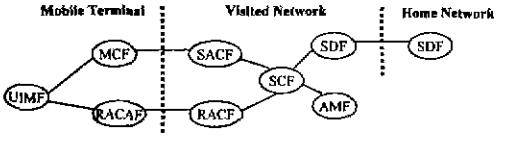
인증이 끝나면 VLR은 새로운 ID임을 감지하고, MSC를 통해서 HLR로 부터 IMUI를 확인하고, MT에 TMUI를 할당한다. 이러한 작업은 사용자 ID 검증 후에 ID 기일성 보장을 해 주는 것이다.

이 시나리오를 TMN M.3010에 정의된 기능 블록으로 표현하면 (그림 4)와 같다.



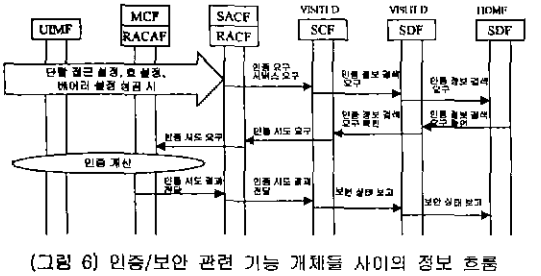
(그림 4) TMN 기능 블록을 이용한 사용자 인증 시나리오

위와 같은 시나리오에 따라 4.1절에서 나타난 기능 개체들의 관계성을 나타내면 아래 (그림 5)와 같다[5].



(그림 5) 사용자 인증 관련 기능 개체의 관계

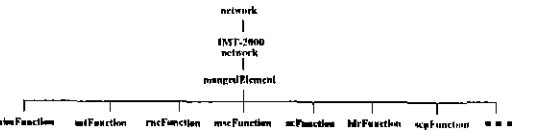
또한, 각 기능 개체들 사이에 전달되는 정보 흐름을 나타내면 (그림 6)와 같다[5].



(그림 6) 인증/보안 관련 기능 개체들 사이의 정보 흐름

5. 인증/보안 관리 객체 모델링

하나의 네트워크 자원에 구성된 기능 개체들의 논리적 집합은 망 관리 객체로서 정의될 수 있다. 또한, 시나리오에서의 정보 흐름도 망 관리 객체들 사이의 관리 정보로서 정의될 수 있다. 따라서, 앞절에서 기술된 시나리오를 바탕으로 인증/보안 관리 관련된 관리 객체들을 포함 트리로 나타내면 (그림 7)과 같다. 궁극적으로 (그림 7)은 (그림 1)의 형태로 상세히 정의되어야 한다. 현재는 (그림 7)의 포함 트리의 확장이 이루어지고 있으며, 앞으로 이를 바탕으로 관리 객체의 정의가 이루어질 것이다.



(그림 7) 사용자 인증 관련 관리 객체 포함 트리

6. 결론 및 향후 연구 과제

지금까지 IMT-2000 인증/보안 관련 요구사항을 분석하여 관리 기능을 정의했다. 그리고, 관련 망 관리 네트워크 요소를 선정하고, 사용자 인증 시나리오를 분석하여 이와 관련된 기능 개체들의 관계를 정의했다. 이 정보의 흐름을 관리 객체의 관리 정보로 파악하여 보안 관리와 관계된 IMT-2000 특정 관리 객체를 정의하고 이를 TMN의 기능 블록 모델에 확장시켜 관리 정보의 흐름 및 각 관계를 명시했다.

향후 연구 과제로써는 사용자 인증 관련 관리 객체를 보다 명확히 정의하고, 사용자 인증 분야뿐만 아니라 사용자 프로파일의 인증과 암호화 관련 네트워크 관리 등 그 밖의 관리 기능을 지원해 줄 수 있는 분야에 대한 연구이다. 또한 글로벌 로밍을 위한 UIM과 관련된 이기종간의 보안 관리에 대한 모델링과 이를 확장해서 IMT-2000의 전체적인 인증/보안 분야에 대한 망 관리 모델을 정립하는 것이다. 나아가 TMN과의 인터페이스 확장을 통해 유, 무선 통합망으로써의 전체적인 보안 관리 객체 모델을 정의할 예정이다.

참고 문헌

[1] ITU-T, M.3010, Principles for Telecommunication management network, 1996.

[2] ITU-T, M.3400, TMN management functions, 1997.

[3] ITU-T, Q.1711, Version 12.2 of Draft new recommandation Q.1711, Network Functional Model for IMT-2000, 1998.

[4] ITU-T Q FIN, Framework For IMT-2000 Network,1998

[5] ITU-T, Q.FIF attachment 1(part1), Section 7.1of Q FIF(version10 0)-IF Diagrams for Registration, Authentication, and Privacy related services

[6] ETSI, GSM 12.00, Objectives and structure of Network Management, 1995

[7] ETSI, GSM 12.03, Security management, 1994.

[8] ITU-T, Baseline Document of Q.23/11 on IMT-2000 standardization, 1998.

[9] ITU-R, M.1078, Security Principles for FPLMTS, 1994

[10] ITU-T X.509 Framework of Security management, 1993.

[11] J.H Lee, Certifying Authority Based FPLMTS Authentication, IEEE ICCS/ISPACS '96, 1996.