通信情報保護學會誌
第7卷 第1號, 1997. 3

# 차세대 이동통신 안전 체제에 관한 고찰

전 학 성*, 김 동 규**

## 요 약

차세대 이동통신 시스템인 FPLMTS(Future Public Land Mobile System)는 2,000년대에 전세계의 통신을 하나로 묶는 유무선 통합 이동통신 환경으로 자리 매김이 이루어질 것이다. 따라서 FPLMTS는 공중 전화망이나 종합 정보 통신망 과 같은 고정 통신망과의 호환성과 높은 품질의 다양한 서비스를 제공하게 된다. FPLMTS가 지니는 융통성과 가능성에 비해 통신 안전에 중요한 문제점을 지니게 된다. 본 고에서는 FPLMTS의 안전에 대하여 국제 표준을 중심으로 살펴 보고, FPLMTS가 지녀야 할 안전 체제에 대하여 살펴 본다.

## I. 서 론

우리 나라는 1996년에 CDMA(Code Division Multiple Access) 방식을 이용한 이동통신 서비스를 상용화함으로써 폭발적으로 그 수요가 증가하는 자동차 전화, 무선 호출기, 휴대용 전화 등의 이동 통신 서비스에 대처할 수 있게 되었다. 그리고 개인 통신 사업자의 선정은 이동통신 분야에 획기적인 발전을 약속하고 있다. 이러한 추세는 수년 후에 미래 공중 육상 이동통신 시스템(FPLMTS, Future Public Land Mobile System)의 사업자가 선정되면 최고조에 이를 것으로 예견된다.

차세대 이동통신 시스템, 즉 FPLMTS는 3세대 이동통신 시스템으로 대략 2000년도에 서비스가 제공될 것으로 예측되고 있다. 차세대 이동통신 시스템 는 공중 전화망 혹은 종합 정보 통신망(ISDN) 등에서 제공되는 광범위한 서비스에 대한 접근이 하나 혹은 그 이상의 무선 링크를 통하여 가능하도록 한다. 따라서 차세대 이동통신 시스템이 지원하는 이동단말의 형태는 육상과 해상 그리고 위성 등으로 확산 가능하다. 차세대 이동통신 시스템의 특징은 다음과 같다.[1]

- high degree of commonality of design worldwide
  전세계적인 설계에 대한 고도의 공통성
- compatibility of services within FPLMTS and with fixed networks
  FPLMTS 내에서 혹은 고정 통신망과의 서비스 호환성
- high quality
  높은 품질
- use of a small pocket-terminal with world wide roaming capability
  전세계적인 로밍이 가능한 소형 경량의 휴대 단말기

* 한국전자통신연구소 책임연구원
** 아주대학교 컴퓨터 공학과

FPLMTS 시스템은 FPLMTS가 실현되기 이전의 셀룰라 전화 시스템 또는 개인 통신 시스템들과 구별되기 위하여 다음의 사항들을 고려하여야 한다. [1],[2]

① 공중전화망(PSTN, Public Switched Telephone Network) 혹은 종합정보통신망(ISDN, Integrated Services Digital Network) 등과 비교될 수 있는 서비스의 질(QoS, Quality of Service)이 요구된다.
② 음성 뿐만 아니라 멀티미디어와 같은 비음성 통신 서비스가 요구된다.
③ 망의 규모 관리와 환경 요소들에 대한 적응, 새로운 개발 욕구를 만족할 수 있는 융통성 있는 시스템의 구조가 요구된다.
④ 전세계의 이동통신 망간 로밍이 가능한 이동 단말기가 요구된다.

이와 같은 고려 사항들 외에 무선 환경과 이동 환경이라는 관점에서 정보 보호와 관련된 다음의 사항들이 문제시되고 있다.

⑤ 무선 통신의 전파 특성에 의해 의도된 상대 외에 보다 많은 여러 상대들에게 정보가 전달된다.
⑥ 이동 통신이라는 본질에 의해 서비스에 대한 불법적인 접근과 서비스제공자 혹은 망 운용자의 자원들의 불법적 사용이 가능하다.
⑦ 이동 통신이라는 본질에 의해 가입자에 대한 서비스의 저하, 그리고 개인의 프라이버시 침해 등의 역기능적인 문제가 야기된다.

본 논문에서는 FPLMTS의 안전 서비스를 검토하고, 국내 FPLMTS의 안전 서비스 정책을 수립하는데 적용될 수 있는 보호 체제를 제시하고자 한다. 본 논문은 모두 5 장으로 구성된다. 먼저, FPLMTS 안전 구조에 대하여 2 장에서 정의하고, FPLMTS에서 예상되는 안전 위협 요소와 안전 목표 그리고 안전 서비스를 3 장에서 정의한다. 4 장에서는 FPLMTS의 안전 메커니즘을 정의하고, 이 메커니즘들이 FPLMTS의 안전 서비스들을 제공하는데 적합한 가를 살펴 본다. 마지막으로 5 장에서는 앞에서 검토된 내용을 참고로 하여 FPLMTS 안전 체제 구축을 위하여 고려하여야 할 사항을 중심으로 결론을 내린다.

## II. FPLMTS 안전 구조

FPLMTS 안전 구조(security architecture)에 영향을 주는 요소로 다음과 같은 사항들이 있다. [3],[4]

① FPLMTS는 여러 종류의 망 운영자와 서비스제공자 환경에서 각각의 security 정책을 가지고 운영된다.
② FPLMTS는 국내 및 국제간 로밍이 가능하도록 한다.
③ FPLMTS는 IN(Intelligent Network)과 TMN(Telecommunication Management Network) 개념을 기반으로 한 개방형 구조를 갖는다.
④ FPLMTS는 UPT(Universal Personal Telecommunication)를 지원하여야 한다.
⑤ FPLMTS는 여러 형태의 서비스들을 지원하여야 하며, 동시에 여러 서비스를 사용할 수 있어야 한다. 그리고 통신 중에 서비스 변환이 가능하여야 한다.
⑥ FPLMTS는 여러 범주의 단말기를 지원하여야 한다.
⑦ FPLMTS 사용자와 단말기는 논리적으로 서로 다른 고유의 인식 번호를 가져야 한다.

⑧ FPLMTS 사용자는 직접 접근이 가능한 개인 서비스 프로파일을 가지며, FPLMTS 사용자와 가입자는 서비스 프로파일에 대한 제한적 접근 권한을 갖는다.

이 절에서는 여러 논리적 부분 요소들로 구성된 FPLMTS 안전 운영 구조(security operational architecture)를 제시한다. 이 구조에서는 FPLMTS 서비스의 사용 및 규정 조건 등을 명시한다. 그리고 . 이 구조에서 여러 형태의 논리적 부분들로 이루어 지는 운영상의 흐름은 융통성(flexibility) 과 여러 다른 나라에서 다른 환경에 적용 가능성(possibility)을 보인다.

이 구조에서 표시되는 논리적 부분들은 각각의 역할이 부여된다. 그러나 FPLMTS가 모든 부분들을 포함하여야 한다는 것은 아니다. 즉, FPLMTS가 제공하고자 하는 서비스와 규정 조건에 따라 일부는 역할을 합칠 수 도 있다. 예로, FPLMTS 서비스제공자와 FPLMTS 망 운용자는 하나의 개체로 합칠 수 있다.

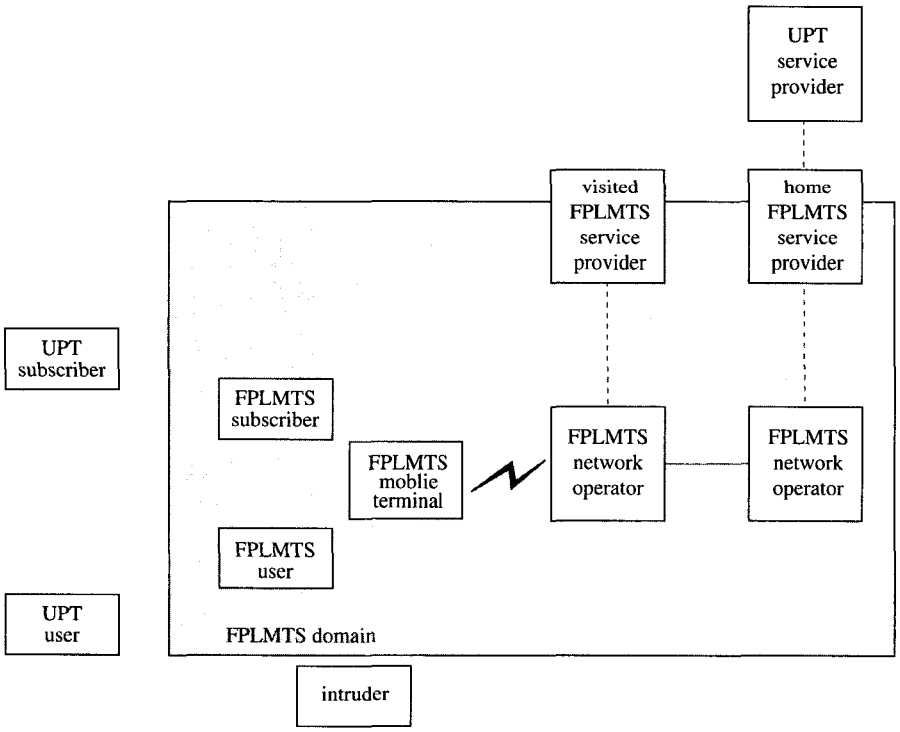



그림 1. FPLMTS 운영 구조

그림 1은 모든 논리적 부분으로 포함하는 FPLMTS 운영 구조를 나타낸다. 각 부분들의 기능은 안전성 측면에서 다음과 같이 정의한다. [4]

• FPLMTS 사용자

FPLMTS 사용자(user)는 FPLMTS 가입자와 관련 있으며, 등록 시 홈 FPLMTS 서비스제공자에 의해 할당되는 고유의 식별 번호와 고유 번호를 가지며 가입 상황

이 변하기 전에 운용상 삭제가 불가능하다. 사용자는 홈 FPLMTS 서비스제공자에 저장된 자신의 서비스 프로파일로 접근이 가능하게 되는데, 이 경우에 안전성 보장 측면에서 사용자 인증이 요구된다.

- FPLMTS 가입자

FPLMTS 가입자(subscriber)는 관련 사용자의 서비스 요금 지급에 대한 권한을 가지며, 하나 이상의 여러 사용자가 하나의 가입자와 연관된다. 가입자는 실제 서비스 운영에는 관련이 없지만, 자신의 식별 번호를 가지고 자신에 속한 사용자의 서비스 프로파일로 접근이 가능하다. 따라서 가입자에 대한 인증 기능이 요구된다.

- 홈 FPLMTS 서비스제공자

*Home FPLMTS service provider*

홈 FPLMTS 서비스제공자의 역할은 FPLMTS 네트워크의 능력에 따라 FPLMTS 사용자에게 서비스를 허용할 것인 가를 결정하는데 있다. 즉, FPLMTS 사용자 관련 정보를 가짐으로써 서비스의 제공과 서비스의 가입 여부를 판단하게 된다. 사용자 식별자들은 논리적으로 홈 FPLMTS 서비스제공자에 속하며, 홈 FPLMTS 서비스제공자는 FPLMTS 번호를 FPLMTS 사용자의 식별자 혹은 FPLMTS 이동 단말기의 식별자로 해석하는 역할을 수행한다. 여기서 유의해야 할 사항은 단말기 식별자와 사용자 식별자의 관계 그리고 식별자의 불법 사용 등에 있다. 사용자 식별자와 단말기 식별자 간의 관계는 2가지의 중요한 의미를 지니게 되는데, 첫째로 하나의 단말기에 둘 이상의 가입자가 접속을 요구하는 경우에 안정성 문제가 있고, 둘째로 단말기 식별자를 관리하는 망 운영자와 서비스제공자간에 안정성 문제를 내포하고 있다. 이러한 문제들을 해결하기 위해서는 인증과 키 분배 등의 안전성 관리 능력을 망 운영자와 서비스제공자가 갖고 있어야 한다.

- 방문 FPLMTS 서비스제공자

*Visited FPLMTS service provider*

방문 FPLMTS 서비스제공자의 역할은 사용자가 자신의 영역으로 로밍하는 경우에 홈 FPLMTS 서비스제공자와 가입자 정보 교환이 이루어져야 하며, 망 운영자로 접근 가능 여부를 결정하여야 한다.

- FPLMTS 망 운영자

*FPLMTS network operator*

FPLMTS 망 운영자는 단말기에게 망 접근과 로밍한 사용자에게 서비스 능력을 제공하는데 그 역할이 있다. 따라서 자신의 영역 안에 있는 단말기와 사용자에 관한 정보를 모두 가지고 있어야 한다. 그리고 망 운영자는 임시 루팅 번호를 부여하는 위치 정보 관리 능력을 가져야 한다. 따라서 망 운영자는 앞에서 언급한 정보들의 교환에 안정성 문제를 가지게 되며, 이를 해결하기 위하여 무선 인터페이스를 통한 망 접속 시 암호화를 적용하여야 한다.

- 침입자

침입자(intruder)는 FPLMTS 네트워크와 서비스를 불법 점유하고자 하는 부분으로 사용자 정보의 안전을 저하시키고 서비스 제공자와 망 운영자로 불법 접근을 시도하게 된다.

- UPT 사용자

UPT 사용자(user)가 FPLMTS에 연결되는 경우에는 FPLMTS의 무선 인터페이스를 통하여 UPT 서비스를 제공 받게 된다. 이 경우에도 안정성 문제가 대두되고, 이를 해결하기 위한 방법으로 사용자의 인증이 요구된다.

- UPT 가입자

UPT 가입자(subscriber)는 UPT 사용자와 동일한 이유로 인증이 요구된다.

• UPT 서비스제공자
*UPT service provider*
UPT 서비스는 FPLMTS를 기반으로 제공되므로 UPT 서비스제공자는 UPT 서비스 정보를 FPLMTS로 제공하여야 하며, 이 경우에 안정성 문제가 발생한다. 따라서 별도의 인증과 키 분배, 암호화 등의 안전성 보장 방법이 요구된다.

## III FPLMTS 안전 서비스

아날로그 이동통신 시스템에서 불법 사용에 대한 사례로 전파 스캐너를 사용하여 합법적인 가입자의 전화 번호 등을 알아낸 후, 이를 휴대전화기에 주입시켜 사용료를 내지 않고 무제한 사용할 수 있도록 하는 경우가 미국과 국내에서 빈번히 발생하였다. 디지털 이동통신 시스템에서는 저속 음성 부호화기를 사용함으로써, 통화 도청 방지를 위한 암호 기능이 기본적으로 제공되고 있어 안전성에 대한 위협 요소가 줄어 들었다. 여전히 디지털 이동통신 시스템은 가입자의 이동성과 무선 접속 등의 특성에 따른 가입자 정보의 도청(eavesdropping) 및 가로채기(interception)에 의한 불법 도용과 무선 채널상 가입자 위치 정보의 노출에 의한 프라이버시 침해 등의 문제점을 내포하고 있다.

본 절에서는 디지털 이동통신을 기반으로 하는 FPLMTS에서 예상되는 안전 위협 요소를 살펴 보고, FPLMTS의 안전 목표와 안전 서비스를 정리한다.

### 3.1 안전 위협 요소

FPLMTS의 안전 위협 요소는 다음의 3가지 범주로 구분할 수 있다.[4]

• 고의적인 위협 요소
*Intentional threats*
고의적인 위협 요소들은 악의의 침입자에 의해 발생한다.

• 우발적인 위협 요소
*Accidental threats*
우발적인 위협 요소들은 사용자에 의한 운영상의 과실이나 전송상의 과실에서 발생한다.

• 운용상의 위협 요소
*Administrative threats*
운용상의 위협 요소들은 안전성 관리의 부재와 특권의 남용에 의해 발생하는데 무선 구간의 안전성과는 직접적인 관련은 없다.

#### 3.1.1 고의적 위협 요소

고의적인 위협 요소들은 악의의 침입자에 의한 위협으로 부정적인 사용과 무결성에 대한 위협, 보안상의 위협으로 구분할 수 있다.

• 부정적인 사용
*Fraudulent use*
이동 단말기 혹은 user identity module를 도난 당한 경우와 사용자의 신임장(credential)을 도난 당한 경우에 발생하는 위협요소로 Cloning, Masquerading, Hijacking 등의 위협을 받게 된다.

• 무결성에 대한 위협
*Threats to integrity*
가입자 혹은 단말기 정보의 노출에 대한 위협요소로 합법적 사용자와 불법적 사용자의 데이터의 동시 변경(Coherent manipulation of user's data), 악의의 위치 등록(Malicious registration of location), 악의의 사용자 프로화일 변경(Malicious user 서비스 프로파일 manipulation) 등의 위협을 받게 된다.

• 기밀성, 프라이버시, 익명성에 대한 위협

*Threats to confidentiality, privacy and anonymity*
무선 구간에서 가입자 혹은 단말기 정보나 통신 내용의 노출에 대한 위협요소로 사용자 인식 정보의 노출(Exposure of user's identities), 사용자 위치 정보의 노출(Exposure of user's location), 사용자 통신의 가로채기(Eavesdropping on user's communication) 등의 위협을 받게 된다.

### 3.1.2 우발적 위협 요소

사용자에 의한 운영상의 과실이나 전송상의 과실로 발생하는 우발적인 위협요소들은 현재 연구가 진행 중에 있다.

### 3.1.3 운용상 위협 요소

안전성 관리의 부재와 특권의 남용에 의해 발생되는 운용상의 위협요소들은 데 무선 구간의 안전성과는 직접적인 관련은 없지만 FPLMTS에서는 가입자와 사용자 데이터베이스로의 침입, 타 망의 사용자 신임장의 도청, 시스템 데이터베이스나 망 제어 기능으로 불법 침입 등으로 구분된다.

- 가입자와 사용자 데이터베이스로의 침입
  *Intrusion into the subscriber/user database*
  사용자 관련 비밀 정보를 갖는 가입자와 사용자 데이터베이스는 침입자에 대하여 취약하므로 감사(audit), 유지 보수(maintenance), 대피(backup) 등이 요구된다.
- 타 망에서 사용자 신임장의 도청
  *Tapping of user's credentials in other networks*
  국내 혹은 국제간 로밍이 지원되면 사용자가 타 망에 이동 시 비밀 정보의 노출이 가능하다.
- 시스템 데이터베이스나 망 제어 기능으로 불법 침입
  *Intrusion into system database or network control functions*
  침입자가 망 제어 기능의 정보를 갖는 데이터베이스로 침입하거나 악의의 데이터 변경을 시행할 수 있으며, 악의의 컴퓨터 바이러스를 설치할 수 있다.

## 3.2 안전 목표

FPLMTS에서는 안전성 보장을 위하여 다음과 같은 목표를 지향한다.[4]

- FPLMTS 사용자에게 제공되는 서비스의 안전성은 공중 전화망이나 종합 정보 통신망과 같은 고정 망과 비교될 수 있어야 한다.
- FPLMTS 서비스제공자나 망 운용자에 부여되는 안전성은 고정 망과 비교될 수 있어야 한다.
- FPLMTS에서 제공되는 안전성은 합법성과 제약성, 사업성 측면에서 전세계적으로 공통이어야 한다.
- FPLMTS에서 제공되는 안전성은 적절한 표준화에 의하여 전 세계적으로 상호 운영이 가능하고 서로 다른 서비스제공자나 망 운용자 간 로밍이 가능하여야 한다.
- FPLMTS 무선 인터페이스의 설계는 안전성과 프라이버시를 해치지 않도록 되어야 한다.

## 3.3 안전 서비스

FPLMTS에서 제공되는 안전 서비스는 FPLMTS 서비스에 포함되거나 특정 FPLMTS 안전성 서비스 형태로 제공되어야 한다. 이러한 안전 서비스들은 일반적으로 다

음의 특성 중 하나를 지니게 된다.[4],[6]

- 방지(preventive)
- 통보(reporting)
- 제한(limiting)
- 구속(restoring)
- 제지(deterrent)

FPLMTS에서 제공되는 안전 서비스들은 기본 서비스와 선택 서비스로 구분되며, 기본 안전 서비스들은 다음과 같다.

- FPLMTS 서비스 가입 정보에 대한 접근 제어
  망에 저장된 FPLMTS 사용자나 가입자의 개인적인 정보에 대한 접근은 제어되어야 한다.
- 서비스 프로파일에 대한 접근 제어
  망에 저장된 FPLMTS 사용자나 가입자의 서비스 프로파일 정보에 대한 접근은 제어되어야 한다.
- 사용자 행위에 대한 인가(authorization)
  FPLMTS 사용자의 행위에는 여러 등급의 제한이 가해지고, 각각의 행위에 대한 권한 인가가 이루어져야 한다.
- 단말기에 대한 인가(authorization)
  FPLMTS 이동 단말기의 조작에는 여러 등급의 제한이 가해지고, 각각의 조작에 대한 권한 인가가 이루어져야 한다.
- 사용자 데이터의 기밀성(confidentiality)
  FPLMTS 무선 인터페이스상에 사용자 데이터는 노출되지 말아야 되며, 이는 음성 및 데이터에 함께 적용되어야 한다.
- 신호 정보의 기밀성(confidentiality)
  FPLMTS 무선 인터페이스상에 신호 정보는 노출되지 말아야 한다.
- 사용자 식별자의 기밀성(confidentiality)
  FPLMTS 무선 인터페이스상에 사용자 식별자는 노출되지 말아야 한다.
- 사용자 위치 정보의 기밀성(confidentiality)
  FPLMTS 무선 인터페이스상에 사용자 위치 정보는 노출되지 말아야 한다.
- 사용자 식별자의 인증(authentication)
  사용자 식별자는 FPLMTS 망 내에서 인증되어야 한다.
- 단말기 식별자의 인증(authentication)
  단말기 식별자는 FPLMTS 망 내에서 인증되어야 한다. 사용자 식별자 인증과 연관되어 효과적으로 구현되어야 한다.
- 트랜잭션 데이터의 무결성(integrity)
  사용자와 서비스제공자 간에 교환되는 데이터는 침입자에 의해 변경되지 말아야 한다.
- 사용자 위치 정보의 무결성(integrity)
  사용자와 서비스제공자 그리고 망 운영자 간에 교환되는 사용자의 위치 정보는 침입자에 의해 변경되지 말아야 한다.
- 단말기 위치 정보의 무결성(integrity)
  단말기와 서비스제공자 그리고 망 운영자 간에 교환되는 단말기의 위치 정보는 침입자에 의해 변경되지 말아야 한다.
- 사용자 식별자와 안전성 관련 정보의 안전한 분배
  FPLMTS 사용자 식별자와 안전성 관련 정보는 서비스제공자로부터 안전한 방법으로 사용자에게 분배되어야 한다. 이 이유로 스마트 카드를 사용하여 정보의 분배가 이루어 진다.
- FPLMTS 이동 단말기 식별자와 안전성 관련 정보의 안전한 분배
  FPLMTS 이동 단말기 식별자와 안전성 관련 정보는 서비스제공자로부터 안전한 방법을 사용하여 단말기로 분배되어야 한다.

FPLMTS에서 제공되는 선택 서비스들은 다음과 같다.

- 사용자와 단말기의 재인증
- FPLMTS 서비스 운영 시 사용자에게 사건 발생을 통보
- 서비스 프로파일에 대한 가입자의 접근 시 안전성 보장

### 3.4 안전 관리

FPLMTS 안전 관리(security management)[5]는 FPLMTS 사용자와 서비스 노드들을 보호하기 위하여 안전 관련 정보를 제어하고 분배하는 기능을 수행하기 위하여 가입자와 망 보호를 위한 안전 관련 사건을 보고하는 기능을 수행한다. 안전 관리는 안전 관련 정보의 생성과 교환, 처리를 위하여 특정 안전 메커니즘을 적용한다.

안전 정책(security policy)은 각각의 안전 서비스를 위한 규칙을 정의하고, 하나 이상의 망 요소들의 안전 관련 행위들로 제한되는 규칙이다. 안전 정책의 규격은 FPLMTS 망 관리 정책에 포함된다.

안전 구역(security domain) 주어진 안전 정책이 적용되는 망 요소들과 각 요소들의 행위로 규정된다. 안전 구역은 작은 구역으로 세분되며, 각 구역별로 안전 정책 및 방법이 제시된다. 그리고 전체 안전 구역은 망 전체에 대한 권한을 지닌 하나의 망 요소에 의해 제어된다.

## IV. FPLMTS 안전 메커니즘

FPLMTS는 무선 통신의 특성에 따라 권한이 없는 접근이나 전송 등을 방지하기 위하여 안전 수단(measures)을 강구한다. 안전 수단은 서비스에 대한 불법 접근을 방지하고, 서비스 제공자와 망 운영자의 자원에 대한 불법 사용을 방지한다.

FPLMTS에서는 이러한 안전 수단으로 여러 형태의 안전 메커니즘들을 검토하고 있다. 본 절에서는 FPLMTS의 안전 메커니즘을 평가하기 위한 항목들을 살펴 보고, 기존에 제안된 여러 안전 메커니즘들이 FPLMTS 안전 서비스에 적합한 지를 살펴 본다.[6]

FPLMTS에서 안전 메커니즘을 평가하기 위하여 다음과 같은 사항들이 고려된다.

- FPLMTS는 공중 전화망이나 종합 정보통신망의 안전 서비스와 비교될 수 있을 정도의 안전 서비스가 제공되어야 한다.
- 여러 형태의 비음성 통신에 대하여 고려되어야 한다.
- 무선 통신의 본질에 따라 불특정 다수에게 정보가 전달된다는 점도 고려되어야 한다.
- 무선 통신의 본질에 따라 무선 인터페이스상의 통신에 대한 프라이버시가 보장되어야 한다.
- 무선 통신의 본질에 따라 서비스에 대한 불법 접근과 서비스제공자와 망 운영자의 자원에 대한 불법 사용을 방지할 수 있는 확실한 방안이 강구되어야 한다.
- FPLMTS는 유통성이 많은 망 구조로 이루어 지지만, 이러한 환경적 요인의 제한이 없이 서비스의 개발이 가능하여야 한다.
- FPLMTS 이동 단말기는 접속 수단이 변경되거나 다른 나라로 이동하는 경우에도 망으로의 접근이 가능해야 한다.
- FPLMTS는 서로 다른 전달 수단과 이동 특성, 트래픽 밀도를 갖는 여러 환경에서 운영되어야 한다.

앞에서 언급한 평가 항목 외에 FPLMTS는 안전 메커니즘에 대하여 다음과 같은 요구 사항을 갖는다.

- 안전 메커니즘은 성능 측면에서 서비스제

공자와 망 운영자, 그리고 사용자간에 실시간 신호 전달을 최소화하여야 한다.

- 안전 메커니즘은 서비스제공자와 망 운영자 간에 사전 안전 정보의 공유가 최소화될 수 있도록 하여야 한다.
- 안전 메커니즘은 서비스제공자와 망 운영자 간에 교환되는 암호화 정보를 관리하는 수단을 가져야 한다.
- 안전 메커니즘은 사용자가 그들의 암호화 정보를 쉽게 바꾸거나 분배할 수 있도록 하여야 한다..
- 안전 메커니즘은 상호 운용성과 망간 이동, 즉 로밍을 보장하기 위하여 표준화되어야 한다.
- 안전 메커니즘은 비번한 메커니즘의 개량과 개정에 따른 버전 관리가 지원되어야 한다.
- 안전 메커니즘은 안전에 대한 위반 사항을 탐지하고 보고할 수 있는 수단과 시스템을 안전한 상태로 유지시킬 수 있는 수단을 가져야 한다.
- 안전 메커니즘은 사용자의 이동성과 단말기의 이동성을 모두 지원할 수 있어야 한다.

## 4.1 인증 메커니즘

인증 메커니즘(authentication mechanism)이 갖는 근본적인 차이는 비밀 키 즉 대칭 방식의 메커니즘이냐 또는 공개 키 즉 비대칭 방식의 메커니즘이냐 하는데 있다. 대칭형 키 메커니즘은 기존 이동 통신에 성공적으로 적용되었지만, 비대칭형 키 메커니즘은 기존 컴퓨터 통신에 적용되었지 이동 통신에는 적용되지 않고 있다. 그 이유는 인증 메커니즘의 적용으로 인한 시스템에 미치는 부하의 증가, 단말기 소형화에 따른 계산 능력의 문제점 등을 고려하였기 때문이다.

### 4.1.1 대칭 키 인증 메커니즘

대칭형 키 메커니즘에서 각각의 개체들은 비밀 키를 가지게 되고, 이 키는 소유 개체와 소유 개체가 신뢰하는 개체들간에 공유하게 된다. 따라서 이러한 키들은 안전하여야 하며, 스마트 카드 혹은 안전한 데이터베이스에 보관된다.

대칭 키 인증 메커니즘에서 인증은 인증 받고자 하는 개체가 인증하는 개체에게 대칭 키에 의한 인증 정보를 보여야만 한다. 대칭 키 인증을 위하여 각각의 개체는 한 쌍의 시도-응답(challenge-response) 정보를 만들어 서로 교환하게 되는데, 이 정보는 단방향 암호화 알고리즘과 비밀 키로 만들어 진다.

대칭 키 인증 메커니즘이 갖는 장점:

- 사용자와 망 운영자 간의 인증을 위하여 서비스제공자가 지정하는 알고리즘을 사용할 수 있다.
- 통신 중에 사용되는 세션 키의 계산이 쉽다.
- 상대적으로 빠르고 단순한 알고리즘이 적용된다.
- 인증을 위하여 적은 양의 정보가 요구된다.

대칭 키 인증 메커니즘이 갖는 단점:

- 망에서 안전한 데이터베이스가 요구된다.
- 망 운영자가 임시로 사용되는 인증 키를 받아 처리하는 경우에는 표준화된 인증 알고리즘이 사용자의 스마트 카드와 망 전체에 사용되어야 한다.
- 비밀 키의 분배가 요구되므로 인증을 위한 적합한 메커니즘을 적용하기 어렵다.
- 키와 인증 정보의 교환을 위하여 서비스제공자와 망 운영자 간의 신뢰 있는 관계가 유지되어야 한다.
- 서비스제공자와 망 운영자 간의 통신이

안전하여야 한다.

- 과금과 사용자 식별자의 안전 유지를 위한 다른 기능들의 실현이 어렵다.

### 4.1.2 비대칭 키 인증 메커니즘

비대칭형 키 메커니즘에서 인증 받고자 하는 각 개체들은 공개 키와 이에 대응하는 비밀 키를 갖는다. 비밀 키는 단지 소유자 만이 알고 있지만, 공개 키는 다른 개체들에 분배된다.

인증은 인증하는 개체에게 비밀 키에 대한 정보를 보여줌으로써 이루어 진다. 일반적으로 인증은 지정된 인증 데이터로 인증 정보를 계산하기 위하여 비밀 키를 사용하게 된다. 그리고 검증을 위하여 공개 키를 사용하게 된다.

공개 키 방식에서 공개 키의 분배 방식은 여러 가지가 있을 수 있다. 예로, 공개 키를 인증할 수 있는 개체는 필요로 하는 개체에 증명서(certificate)를 분배하기 위하여 모든 개체들에 대한 증명서를 가지는 데이터베이스를 지닌다. 이와 같은 권한을 갖는 개체를 갖지 않는 방법으로 통신의 가능성이 있는 개체들간에 미리 공개 키를 주고 받는 방법이 있다.

비대칭형 인증 메커니즘이 지니는 장점:

- 망에서 비밀 인증 키의 저장 및 전달이 필요로 하지 않는다.
- 서비스제공자와의 신호 교환이 필요하지 않다. 따라서 망 운영자와 서비스제공자 간의 트래픽이 준다.
- 임의의 한 쌍의 개체들간 인증이 쉽게 적용될 수 있다.
- 서비스제공자와 망 운영자 간의 안전한 통신이 요구되지 않는다.

비대칭형 인증 메커니즘이 지니는 단점:

- 일반적으로 인증 알고리즘은 많은 양의 계산이 요구된다.
- 사용 가능한 알고리즘의 수가 적어 매우 제한적이다.
- 유통성이 있지만 인증 알고리즘이 전 세계적으로 일치하여야 한다.
- 사용자와 망 운용자가 주고 받아야 하는 메시지의 크기가 크다.
- 증명 권한을 갖는 개체(certification authority)가 요구된다.

### 4.1.3 영 지식 인증 메커니즘

이 메커니즘은 사용자가 두개의 식별자로 공개 식별자(public identity, PI)와 이에 대응하는 비밀 식별자(secret identity, SI)를 갖아야 한다. 이 식별자들은 서비스제공자에 의해 할당되어 스마트 카드에 기록된다. 이러한 식별자를 만들기 위하여 임의의 비밀 파라미터가 요구되고 식별자 간의 관계는 이 파라미터에 의해 검증된다. 그리고 이 파라미터는 노출에 대한 방지가 전혀 필요로 하지 않는다.

개체별 식별자의 검증은 영-지식 프로토콜(zero-knowledge protocol)을 적용하게 되는데, 이 프로토콜의 검증 기능은 식별자에 대한 지식이 없이도 비밀 식별자를 알 수 있기 때문이다. 따라서 가로채기가 이루어 져도 비밀 식별자는 전혀 노출되지 않는다.

영-지식 인증 메커니즘의 장점

- 안전도의 등급을 조정할 수 있다.

영-지식 인증 메커니즘의 단점

- 인증 메커니즘이 매우 복잡하다.
- 세션 키의 일치 또는 분배가 쉽게 결합되지 않는다.
- 많은 양의 데이터를 주고 받아야 한다.

## 4.2 익명 메커니즘

### 4.2.1 대칭 키 방식의 임시 식별자 익명 메커니즘

사용자와 단말기가 이동하는 경우에 이동 지역에서 할당 받는 임시의 식별자는 지정된 시간 안에서 자유롭게 할당되고 단지 현재의 이동 영역 안에서만 유일하다. 따라서 지역 이동이 이루어지는 경우에 새로이 할당 받아야 한다.

임시 식별자(temporary identity)는 사용자나 단말기의 식별을 위하여 불안정한 링크에서 사용되며, 개체의 익명성(anonymity)을 보장한다. 임시 식별자의 배정은 안전하게 이루어져야 되므로, 특정 인증 메커니즘에서는 고정된 식별자를 사용하게 된다.

대칭 키 방식의 임시 식별자 익명 메커니즘의 장점

- 임시 식별자의 크기가 작다.

대칭 키 방식의 임시 식별자 익명 메커니즘의 단점

- 임시 식별자의 배정을 위하여 중복된 부가적인 관리 능력이 요구된다.
- 오류가 발생하게 되는 경우에는 고정 식별자를 사용하여야 한다.

### 4.2.2 비대칭 키 방식의 식별자 기밀성 유지 메커니즘

공개 키 암호 시스템을 사용하여 개체의 식별자에 대한 안전도를 높일 수 있다. 즉, 개체는 자신의 식별자를 임의 수(random number)를 덧붙여 RSA와 같은 공개 키 암호 알고리즘으로 암호화한다. 이 경우에 상대 공개 키로 식별자를 암호화하여, 침입자가 암호화된 식별자를 새로이 만들어 내는 것을 방지한다.

비대칭 방식의 식별자 익명 메커니즘의 장점

- 임시 식별자가 필요하지 않다.
- 식별자에 대한 보호가 확실하다.

비대칭 방식의 식별자 익명 메커니즘의 단점

- 암호화된 식별자가 원래의 식별자에 비해 너무 길다.

### 4.2.3 익명의 접근 방식

선불 카드와 같이 식별이 필요로 하지 않는 메커니즘을 사용하여 익명성을 유지할 수 있다.

익명의 접근 메커니즘의 장점

- 식별자의 노출에 대한 위험성이 완전하게 제거된다.

익명의 접근 메커니즘의 단점

- 이 방식이 적용된 예가 극히 드물다.

## 4.3 암호 메커니즘

암호 메커니즘(Confidentiality mechanism)으로는 흐름 비화(stream cipher) 또는 블럭 비화(block cipher)를 사용할 수 있다. 비화 기능(ciphering function)은 일반적으로 FPLMTS 이동 단말기가 가지게 된다.

- 다양한 안전 정책이 존재하므로 하나 이상의 알고리즘이 필요하다.
- 로밍을 목적으로 표준화가 요구된다.

### 4.3.1 블럭 비화 암호 메커니즘

블럭 비화기(block cipher)는 암호화 키의 제어로 고정된 크기의 데이터를 암호화하는 특징을 갖는다.

블럭 비화에 의한 암호 메커니즘의 장점

- 블럭 비화는 일반적으로 잘 정리되어 있어 적용이 쉽다.

블럭 비화에 의한 암호 메커니즘의 단점

- 오류의 발생 확률이 상대적으로 높다.
- 복호화에 따른 지연이 발생한다.

#### 4.3.2 흐름 비화 암호 메커니즘

흐름 비화기(stream cipher)는 순열 생성기(sequence generator)를 사용하는데, 순열 생성기는 키를 입력 받아 임의의 크기로 순열을 생성한다. 이러한 키 흐름은 비트 단위로 데이터에 가산된다.

흐름 비화에 의한 암호 메커니즘의 장점

- 오류의 전파가 거의 이루어지지 않는다.

### 4.4 무결성 메커니즘

#### 4.4.1 암호화 무결성 메커니즘

전달되는 데이터가 적절한 반복성을 갖는다면, 암호화를 사용한 무결성 메커니즘에서 데이터가 변경되지 않을 것이라는 충분한 확신을 갖게 된다.

암호화에 의한 무결성 메커니즘의 장점

- 별도의 암호 알고리즘이 추가될 필요가 없다.

암호화에 의한 무결성 메커니즘의 단점

- 반복 공격(replay attack)에 대하여 방어 수단이 없으므로 임의 수나 카운터 등을 추가하여야 한다.
- 비음성 정보와 같이 고도의 반복성을 지니는 데이터에 적용할 수 없다.

#### 4.4.2 대칭 키 무결성 메커니즘

일반적으로 메시지에 대한 무결성 보장은 2가지 방법을 사용한다. 첫째로 메시지 인증 코드(Message Authentication Codes, MAC)를 사용하는 방법으로 메시지 암호 기능과 비밀 키로 이루어 진다. 둘째로 조작 탐지 코드(Manipulation Detection Code, MDC)를 사용하는 방법으로 메시지의 조작을 방지하기 위한 기능 만으로 이루어 진다. 단, MDC를 만드는 기능은 널리 알려져 있으므로 최소한 MDC에 대한 암호화가 필요하다.

대칭 키를 사용한 무결성 메커니즘의 장점

- 상대적으로 매우 간단한 알고리즘을 사용한다.

대칭 키를 사용한 무결성 메커니즘의 단점

- 반복 공격(replay attack)에 대하여 방어 수단이 없으므로 임의 수나 카운터 등을 추가하여야 한다.
- 통신 상대의 비밀 키가 필요하므로 키 분배 방법이 요구된다.
- 내부자에 의한 공격에 대한 방어가 불가능하다.

#### 4.4.3 비대칭 키 무결성 메커니즘

메시지의 해쉬 값을 정보 송신자의 비밀 키로 서명하고, 이 서명을 전송 메시지에 첨부하여 송신자의 공개 키를 가진 수신자가 전송 메시지의 해쉬 값을 만들어 대조한다.

비대칭 키를 사용한 무결성 메커니즘의 장점

- 송신자의 공개 키에 의한 무결성 검사가 이루어 지므로 3자에 의한 검증이 가능하다.

비대칭 키를 사용한 무결성 메커니즘의 단점

- 알고리즘의 복잡도가 매우 높다.
- 적용 가능한 알고리즘이 매우 드물다.

### 4.5 부인 봉쇄 메커니즘

디지털 서명은 데이터의 전송 데이터와 수신 데이터에 대한 수취 거부를 확인할 수 있는 방법이다.

부인 봉쇄 메커니즘의 장점

- 여러 등급의 부인 봉쇄가 가능하다.

부인 봉쇄 메커니즘의 단점

- 위조된 서명을 탐지하기 위하여 비대칭 알고리즘이 요구된다.

### 4.6 안전 관리

#### 4.6.1 키 관리

FPLMTS 안전 서비스를 지원할 수 있는 안전 메커니즘의 선택에 따라 키 생성과 분배, 증명 등을 위한 안전 관리 기능이 요구된다.

#### 4.6.2 버전 관리

버전 관리(version management)는 안전 절차(security procedure)와 안전 메커니즘의 변경 또는 교체를 위한 메커니즘이다. 버전 관리는 기존의 FPLMTS 이동 단말기를 교체하지 않고 이루어져야 한다. 이 방법으로 착탈 가능한 스마트 카드를 사용하는 방법이 제시되고 있다.

## V. 결 론

일반적으로 디지털 이동 통신을 위한 안전 체제로는 대칭키 방식(symmetric key cryptosystem)을 채택하고 있다. 이는 안전 서비스의 제공으로 인한 시스템의 부하를 줄이고, 단말기의 계산 능력을 고려한 것으로 추정된다. 그러나 대칭 키 방식은 안전 정보를 관리하는 데이터베이스가 대규모화하고, 망 운영자와 서비스제공자 간의 안전 정보 교환에 따른 트래픽의 증가와 집중화 현상을 막을 수 없다는 단점을 지닌다. 반면에 비대칭 키 방식(asymmetric key cryptosystem)에서는 다루어야 할 데이터의 양이 많아지지만 인증 메커니즘이 단순화되어 시스템의 부하를 줄일 수 있고, 무결성 및 부인 봉쇄 등의 안전 메커니즘을 결합할 수 있어 단말기의 계산 능력이 향상되는 시점에서 적용이 가능할 것이다.[7]

앞 절에서 FPLMTS 안전 메커니즘에 대하여 살펴 보았다. 안전 메커니즘의 적용에 대하여 다시 살펴 보면, 크게 대칭 키 방식의 안전 체제와 비대칭 키 방식의 안전 체제로 구분할 수 있다. 표 1은 앞 절에서 제시된 6가지의 안전 메커니즘을 대칭 방식과 비대칭 키 방식으로 구분하여 정리하였다.

표 1에서와 같이 FPLMTS를 위한 안전 체제는 2단계로 구분하여 생각할 수 있다. FPLMTS의 1 단계에서는 기존의 셀룰라와 개인 휴대 통신에서 적용되고 있는 대칭 키 방식의 안전 체제를 유지 발전시키는 방향으로 전개될 것이다. FPLMTS 2 단계의 안전 체제는 서비스가 고도화되고, 단말기의 계산 능력이 향상될 것을 고려하여 비대칭 키 방식을 적용할 것으로 예측되고 있다.

표 1. FPLMTS 안전 메커니즘

| 종류 / 방식 | 인증 메커니즘 | 익명 메커니즘 | 암호 메커니즘 | 무결성 메커니즘 | 부인 봉쇄 메커니즘 | 안전 관리 |
|---|---|---|---|---|---|---|
| 대칭 키 방식 | 시도/응답 인증 방식 단방향 암호 알고리즘의 적용 | 임시 식별자의 배정 | 세션 키 암호 방식 인증과 별도의 세션 키 공유 | 메시지 인증 코드 혹은 조작 탐지 코드를 사용 | 적용 불가 | 인증/키 관리 데이터베이스 운영 |
| 비대칭 키 방식 | 비밀 키에 의한 인증 정보 생성과 공개 키에 의한 정보 검증 | 식별자를 공개 키로 암호화 | 세션 키 암호 방식 인증과 동시에 세션 키 공유 | 비밀 키로 서명하고, 공개 키로 대조 | 공개 키 방식의 디지털 서명을 적용 | 인증 및 키 관리 기능 분리 |

FPLMTS를 위한 안전 체제는 다음과 같은 기본 원칙에 의해 구축한다.

- 안전 서비스로는 사용자 또는 가입자와 단말기에 인증과 익명성, 암호, 무결성 등을 동일하게 적용한다.
- 서비스를 제공하기 위한 키 방식으로 1단계에서는 대칭 키 방식을, 2 단계에서는 비대칭 키 방식을 적용한다.
- 1단계에서는 사용자 혹은 가입자와 단말기의 인증을 주로 수행하며, 2 단계에서는 망 운영자와 서비스제공자의 인증도 수행한다.
- 1단계에서는 임시 식별자를 사용하여 익명성을 유지하지만, 2 단계에서는 비대칭 키 방식에 의해 암호화된 식별자를 사용하여 익명성을 유지한다.
- 1단계에서는 단말기와 망 운영자 간 암호 서비스를 주로 수행하며, 2 단계에서는 망 운영자와 서비스제공자간 암호 서비스도 수행한다.
- 1단계에서는 임의 수나 카운터 등을 적용한 대칭 방식의 무결성 메커니즘을 적용하지만, 2 단계에서는 비대칭 방식에 의한 무결성 메커니즘을 적용한다.
- 부인 봉쇄는 비대칭 방식을 적용하는 2 단계에서 제공한다.
- 1 단계에서 인증과 세션 키 관리를 위한 데이터베이스의 안전 관리가 수행된다.

현재 기본 원칙에 따라 1 단계 대칭 키 기반의 이동통신 안전 프레임워크(mobile security framework)의 실현에 대한 연구가 진행 중이며, 추후 2 단계 비대칭 키 기반의 이동통신 안전 프레임워크의 실현에 대하여 연구되어질 예정이다.

# 참 고 문 헌

[1] ITU-R Recommendation M.687, Future Public Land Mobile Telecommunication Systems(FPLMTS), 1992.

[2] ITU-R Recommendation M.816, Framework for services supported on Future Public Land Mobile Telecommunication Systems (FPLMTS), 1992.

[3] ITU-R Recommendation M.817, Future Public Land Mobile Telecommunication Systems (FPLMTS) Network architectures, 1992.

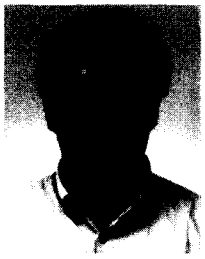
[4] ITU-R Recommendation M.1078, Security Principles for Future Public Land Mobile Telecommunication Systems (FPLMTS), 1994.

[5] ITU-R Recommendation M.1168, Framework of Future Public Land Mobile Telecommunication Systems (FPLMTS) Management, 1995.

[6] ITU-R Draft Recommendation M. FPLMTS.ESM, Evaluation of Security Mechanisms for FPLMTS, September 1995.

[7] D. Brown, "Security planning for personal communications," Proceeding the 1st ACM Conference Computer and Communications Security, pp. 107-111, ACM Press, 1993.

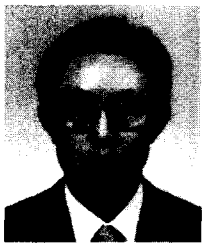
## □ 著者紹介

전 학 성

중앙대학교 공과대학 전자전자계산학과(공학사)
중앙대학원 전자계산학과(이학석사)
정보처리 계산조직응용 기술사
현재 한국전자통신연구소 이동통신연구단 책임연구원
현재 아주대학교 컴퓨터 공학과 박사과정

※ 관심분야 : 이동통신 보안, 이동 컴퓨팅 보안, CORBA 기반 지능망, JAVA



김 동 규

서울대학교 공과대학 졸업(학사)
서울대학교 자연과학대학원 졸업(석사)
미국 Kansas 주립대 대학원 졸업(Ph.D. 전산학 박사, 정보통신 전공)
미국 Kansas 주립대 전산학과 교수
1979. 3 - 현재 아주대학교 컴퓨터공학과 교수
저서 : 데이타 통신시스템, 회중당, 1986년
저서 : 컴퓨터 통신 네트워크, 상조사, 1988년
한국통신학회 상임이사, 한국통신정보보호학회 부회장

※ 주관심분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링,
정보통신 Security, 분산처리 시스템