通信情報保護學會誌
第3卷 第4號, 1993. 12

GSM시스템의 Security 특성에 관한 고찰

A Survey on the Security Features of GSM System

오현서* · 이홍섭* · 이대기*

요 약

GSM(Global System for Mobile Communications)은 범유럽적으로 추진되고 있는 디지탈 이동통신시스템으로서 ETSI(European Telecommunication Standards Institute)에 의해 표준화가 추진되고 있다. GSM시스템 규격에서는 도청 또는 불법 사용에 대비하여 암호기술을 이용한 가입자 I.D. 인증 및 보호, 그리고 무선구간에서의 정보 보호를 위해 암호화 기능을 갖도록 권고하고 있다. 본고에서는 GSM 이동통신망에서의 Security에 관련된 기능들과 암호 알고리즘 특성에 관하여 고찰하였다.

I. 개 요

무선통신 기술의 발달로 인하여 언제 어디서나 원하는 사람과 통신이 가능하게 되어가고 있다. 이러한 이동 통신망은 기존의 공중 전화망이나 데이타망과 연결되고, 점차적으로 ISDN(Integated Service Digital Network)과도 접속이 가능하도록 발전되어 가고 있다.

이동 통신망은 무선 채널을 통하여 정보가 전달되므로, 정보가 도청될 가능성이 크고, 조작될 가능성이 있으므로 안전한 정보 교환을 위해서는 통신망 차원에서의 정보보안 대책이 필요하다.

GSM은 유럽의 많은 국가들이 채택하고 있는 디지탈 방식의 이동 통신 시스템으로서 '82년부터 유럽의 ETSI에 의해 표준화되고 있는 중이며, GSM 시스템 규격에는 스펙트럼 효율, 용량, 음질, 무선정합 등과 같은 기본적인 시스템 조건과 함께 Security에 관련된 조건을 권고하고 있으며, 새로운 기능 추가 및 기존 규격의 보완, 변경 등으로 인해 지속적으로 수정이 되고 있는 중이다. 여기에서는 1988년에 발표된 Version(Phase 1)과 1993년에 발표된 Version(Phase 2)에서 제시하고 있는 GSM 시스템 규격중 Security에 관련된 이동 통신망의 구성과 망구성 설비 기능 및 구조, 그리고 암호 알고리즘 특성에 관하여 살펴보고자 한다.

II. GSM시스템의 Security 기능

Security에 관련된 기능을 살펴보면, 가입자 I.D. 인증(Subscriber Identity Authentication) 및 가입자 I.D. 보호(Subscriber Identity Confidentiality) 그리고 무선 구간에서의 데이타 기밀성(Data Confidentiality on the Radio Interface) 등 3가지로 구분된다. 가입자 I.D. 인증은 불법의 가입자가 통신망으로부터 정보를 획득하려는 것을 방지하기 위한 것이며, 가입자 I.D. 보호는 등록된 가입자

* 한국전자통신연구소

I.D. 정보 누출을 방지하고, 무선 구간에서의 데이타 보호는 무선 채널 특성상 노출되는 정보의 보호를 위한 것이다.

Security 기능은 가입자에게 제공되는 부가 서비스의 하나로서 GSM 표준에 따른 PLMN(Public Land Mobile Network)을 구축하려는 통신망 사업자에게는 반드시 필요한 것으로, 이동국과 기지국간 Point-to-Point 구간을 전제로 한다.

2.1. 가입자 I.D. 인증

통신망 관리자가 가입자에게 정확한 요금의 부과하기 위해서는, 불법의 가입자가 등록된 가입자의 I.D.를 가장하여 통화하는 것을 방지하기 위한 조치를 필요로 한다. 따라서 가입자는 매사용시 마다 자신을 증명하기 위하여, 가입자 I.D. 번호와 인증용 알고리즘 및 키가 내장된 스마트 카드를 소지하고 액세스하여야 한다.

2.2. 가입자 I.D. 보호

통신망 관리자는 언제 누가 망을 억세스하는 지를 알아야 할 뿐만 아니라, 부정한 사용자가 무선 채널의 정보를 도청하여 다른 가입자 I.D.를 알아내어 사용하는 것을 불가능하도록 하기 위해서는, 제삼자에게 등록된 가입자 I.D.가 노출되지 않도록 보호해야 한다. 그러므로 가입자의 I.D. 정보는 무선 구간에서 도청되더라도 해독이 불가능한 정보로 변환하여 전송하게 된다.

2.3. 가입자 데이타 보호

가입자 데이타는 인가되지 않은 사람이 들어서는 안되는 사업상 비밀 내용과 같은 중요한 정보일 수 있다. 이러한 정보는 음성, 데이타 또는 비음성 데이타 등으로서, 가입자 데이타를 안전하게 전송하기 위하여 무선 구간의 정보를 암호화 한다.

Ⅲ. GSM 시스템의 Security 관련 망 구성 요소

GSM 시스템의 통신망은 PLMN(Public Land Mobile Network)이라고 하며 그림 1.과 같다.

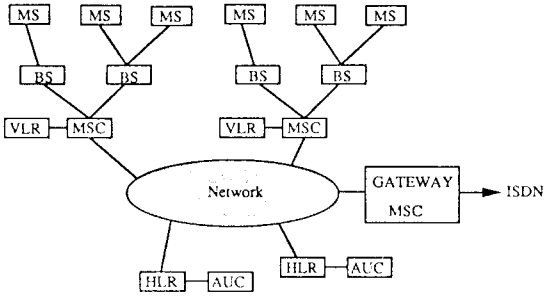


그림1. GSM시스템 통신망 구성

3.1. SIM(Subscriber Identity Module)

각 가입자는 망 등록 정보가 내장된 SIM 이라고 하는 스마트 카드를 개별적으로 소지하고 통화시 단말기에 삽입하여 사용하게 된다. SIM에는 A3라고 하는 인증 알고리즘과 A8 암호 키 생성 알고리즘 내장되어 있으며, 알고리즘을 동작을 위해 마이크로 프로세서 칩이 실장되어 있다. SIM에는 가입자 번호와 인증키 등 각 가입자에 대한 정보가 보관되어 있으며 외부에서 읽을수 없도록 설계되어 있다.

단말기 사용은 가입자 인증이 이루어진 이후에만 허용되므로 가입자는 매 사용시마다 PIN(Personal Identification No.)으로 스마트 카드에 의하여 자신을 인증하게 된다. PIN 정보는 이동국의 MMI(Man Machine Interface)를 통해 전달되며, 단말기는 PIN 정보를 스마트 카드로 보내어 Reference와 비교하도록 하며, 스마트 카드에 의한 인증이 완료된 후에야 가입자는 단말기를 억세스할 수 있게 된다.

3.2. 이동국(MS ; Mobile Station)

이동국은 단말기와 스마트 카드로 구성되며 단말기는 전화기 또는 데이타 단말기로서 암호 알고리즘이 내장되어 있다.

3.3. 기지국(BS : Base Station)

기지국은 이동국에 대응되는 설비로서, 이동국과 기지국간 교환되는 무선구간에서의 정보 보호를 위한 A5/A5X 암호 알고리즘을 실장하고 있다.

3.4. 교환기(MSC : Mobile-services Switching Center)/VLR(Visitor Location Register)

GSM시스템의 이동 서비스 교환기인 MSC에는 VLR들이 내장되어 일시적인 가입자 데이타가 저장되어 있다. VLR은 TMSI(Temporary Mobile Subscriber Identity) 번호를 발생하고 저장하며, 인증이 이루어 졌는지 여부를 판단하는 기능을 갖는다.

3.5. HLR(Home Location Register)

HLR은 등록된 가입자의 서비스 종류, 특별한 사용자 그룹에 관련된 회원권, 배정된 가입자 번호 등 영구적인 가입자 데이타의 보관을 위한 데이타 베이스이다.

3.6. 인증 센터(AUC : Authentication Center)

인증 센터에는 각각 다른 스마트 카드에서의 인증키와 동일한 각 가입자의 인증 키가 보관되어 있으며 A3 알고리즘으로 이들 인증키를 사용하여 인증 파라메터를 생성한후 HLR을 통해 MSC의 VLR로 보내는 역할을 한다. 인증 센터내에서 A8알고리즘을 발생한 암호 키는 무선 채널 정보의 암호화에 사용된다.

3.7. Gateway MSC

GSM 가입자와 기존 전화망 가입자와의 모든 종류의 통신, PLMN과 ISDN간 접속, VPLMN(Visited PLMN)에서 배회하는 가입자 호 처리 등은 Gateway MSC를 통해 이루어 진다. PLMN은 2가지로 구분되는데 가입자가 거주하며 등록한곳을 HPLMN(Home PLMN), 타지역 PLMN을 방문하여 등록하였을 때에는 VPLMN이라 한다.

Ⅳ. GSM시스템의 Security 구조

GSM시스템에서는 Security 기능 실현에 표1과 같은 특성을 갖는 3가지 암호 알고리즘을 사용하고 있다.

4.1. 인증 절차

표 1. GSM시스템의 암호 알고리즘 특성

종류	용 도	특 성	전송매체	비 고
A3	가입자 I.D. 인증 알고리즘	입력 : RAND 128 비트 키 32 비트 출력 : SRES 32 비트	무선채널	인증센터
A5/ A5X	암호 알고리즘	이력 : 암호키 64 비트 프레임 번호 0~2715647 출력 : 4.615msec마다 114 비트 주기 : 209분	무선채널	단말기, 기지국
A8	키 생성 알고리즘	입력 : A3와 동일 출력 : A5의 암호 키	스마트카드	가입자휴대

인증 절차는 그림 2와 같은 "Challenge Reponse Scheme" 방법으로 수행되며, 인가 받은 가입자가 주어진 RAND(Random Number)로 SRES(Signed Response) 생성해서 응답하게 된다. 가입자 확인은 인증 절차보다 선행되어야 한다. 인증 절차는 기지국에서 먼저 난수가 발생하여 이동국으로 전달함으로써 시작되며, 난수 RAND와 인증키 Ki는 A3 인증 알고리즘의 입력 데이타로 사용되어 SRES를 계산한다. 이와 마찬가지로 이동국에서는 수신한 난수 RAND와 인증 키 Ki를 사용하여 SRES′를 생성하고 이 결과를 기지국으로 보낸다. 기지국에서는 생성된 SRES와 SRES′를 비교하여 SRES와 SRES′ 값이 동일한 때만 입가된 가입자로 간주한다.

4.2. 인증 알고리즘 A3

인증 알고리즘은 GSM에서 표준화되어 있지 않은 관계로 통신망 관리자가 적당한 알고리즘을 선택하

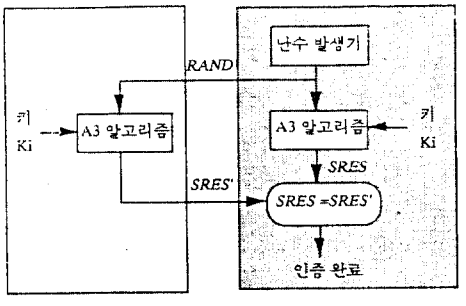


그림 2. 가입자 인증 절차

여야 한다. PLMN의 Security 레벨은 통신망 관리자의 Security 인식에 달려 있으며, 인증 알고리즘은 고비도의 단방향 함수로서 주어진 RAND와 SRES로부터 인증키를 유출하기가 불가능 하도록 설계되어야 한다. 알고리즘 A3의 입출력 조건은 RAND가 128비트이고 SRES는 32비트로 표준화되어 있다.

인증 센터는 인증 파라메터 RAND와 SRES를 발생하고 각 가입자 정보를 보관해야 하고 인증 파라메터의 발생은 가입자가 등록된 HPLMN 또는 VPLMN에서 이루어진다. 이것은 인증 파라메터가 수시로 타지역 PLMN에 전달되어야 함을 의미한다.

4.3. TSI(Temporary Subscriber Identity)

각 가입자는 등록시 부여되는 IMSI(International Mobile Subscriber Identity) 번호를 갖는데, 이 번호는 전화번호와는 동일하지 않고 통신망의 내부 Addressing을 위해 사용되며, 전화번호처럼 모든 통신망의 레지스터에서 넓게 이용할 수 없다. IMSI는 단말기로 통신망을 액세스할 때 무선채널을 통해서 전달된다.

TMSI(Temporary Mobile Service Identity)는 가입자를 식별하는데 사용하며 수시로 변경되는데, 관련되는 망관리자에 의해서 결정되고 재배치된다. TMSI는 기지국에서 이동국으로 암호화하여 전송되므로, 부정한 가입자는 무선채널 상의 신호 정보로부터 어떤 가입자가 어떤 TMSI를 갖는지 알 수 없으며, IMSI 또는 TMSI를 알았더라도 수시로 TMSI를 재할당함으로서 어떤 가입자가 망을 사용하는지 알 수 없다.

4.4. TMSI 재할당 절차

TMSI 재할당은 인증 절차의 성공적인 수행과 TMSI의 암호화를 위한 암호 키의 유용성을 가정하에 이루어진다. 기지국에서 새로운 TMSI를 암호화하여 이동국으로 전송하면 단말기에서는 새로운 TMSI를 복호화하여 스마트 카드에 저장한 후에 ACK신호를 기지국으로 보낸다. 기지국에서는 ACK 신호를 수신한 다음 과거의 TMSI 정보를 지운다.

4.5. 무선 채널상의 데이타 보호

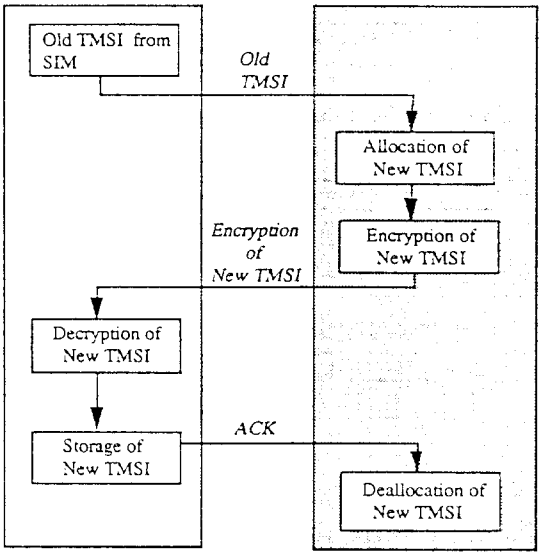


그림 3. TMSI의 재할당

데이타의 암/복호화를 위해 사용되는 암호 키 Kc 생성 과정은 그림 4와 같다. 암호키는 인증 절차가 완료된 후에 생성되며, 키 변경 주기는 인증 빈도수에 따르게 되며 통신망 관리자에 의해 결정된다. A8 알고리즘은 A3 인증 알고리즘과 동일한 입력 파라메터 RAND와 Ki를 사용하여 암호키를 생성하는데 이용된다. 암호키는 무선 채널에 노출되지 않도록, 인증 센터와 스마트 카드에 실장된 A8 알고리즘으로 생성하여 사용한다. A8 알고리즘은 GSM에서 표준화되지 않았지만 외부 파라미터가 A3 알

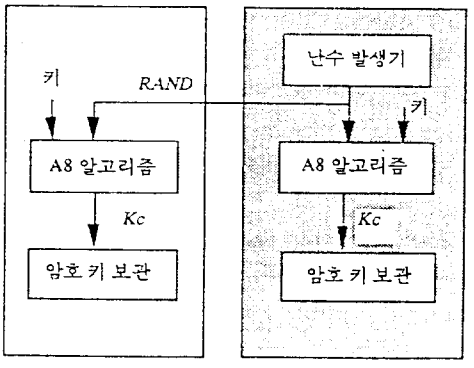


그림 4. 암호 키 분배

고리즘과 동일하므로, 단일 알고리즘으로 구성하도록 권고되고 있다.

4.6. 암호화 및 복호화

데이타의 암/복호화 과정을 살펴보면, 송신 데이타를 PN비트와 Exclusive-OR을 해서 암호화한 후에 전송하며, 수신 데이타는 다시 PN비트와 Exclusive-OR을 해서 원래의 신호를 복호화되게 된다. 암호 알고리즘은 유럽 전역 어디에서나 동일 이동국으로 통화가 가능 해야 한다는 요구조건에 따라 표준화가 이루어졌다. 암호 알고리즘 입력메터로는 A8 알고리즘으로 생성된 64비트 암호 키와 TDMA 프레임 번호가 사용되며, 이 입력 파라메터를 사용하여 A5 알고리즘에서는 4.615msec마다 114개의 PN비트 수열이 생성되며, TDMA프레임 번호는 송수신 알고리즘 동기 정보로 사용된다. TDMA 프레임 번호는 0에서 2715647사이 값을 갖게 되므로 약 209분이내에 PN 수열이 주기적으로 반복된다. 따라서 209분 이내의 일정한 시간마다 키 변경이 연속적으로 이루어져야 된다.

최근에는 ETSI에 의해 A5X 알고리즘 규격을 새롭게 제정하고 있으며 GSM 신호 방식을 강화하여 복수 암호 알고리즘을 사용할 수 있게 하였으며

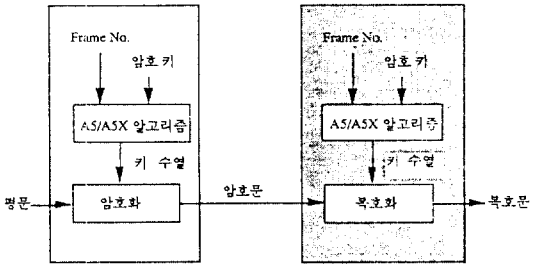


그림 5. 암호화 및 복호화 과정

1993년 하반기에 규격이 발표될 예정이다. 따라서 복잡한 통신망에서의 가입자의 이동으로 인한 사용상의 제약이 없고 모든 경우에 암호 통신이 가능하게 될 것이다.

V. 결 론

GSM시스템의 Security에 관련된 이동 통신망 구성과 Security 기능 및 구조, 그리고 암호 알고리즘의 특성을 살펴 보았다. GSM시스템에서는 Security 기능을 위해 3가지 알고리즘을 사용하고 있으며, Point-to-Point 망에서의 가입자 인증과 가입자 I.D. 보호 및 데이타 보호 방법 등을 제시하고 있다. 이러한 Security 기능은 통신망 관리자의 원하는 비도와 가입자 측면에서의 원하는 비도, 그리고 현대 통신 시스템의 기술 투자 측면에서 실현 가능한 비도간의 Trade-off관계를 갖는다.

그러므로 디지탈 이동 통신에서의 종합적인 Security 기능 실현을 위해서는 가입자 인증과 암호 기술, 스마트 카드 기술, 효율적인 키 분배 프로토콜 등의 지속적인 연구가 필요하다.

참 고 문 헌

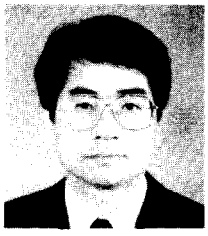
[1] Uwe Michel "The Security Feature in the GSM System", TELECOM '91, 1991.

[2] Security Related Network Functions, GSM 03.20 Recommendation, Nov., 15, 1988.

[3] Per Bjorndahl "The GSM Switching Subsystem Functions and its Signalling", The Pan-Asia Summit, March, 1993.

[4] Alain Maloberti "The GSM Radio System", The Pan-Asia Summit, March, 1993.

□ 著者紹介

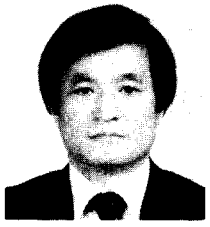


吳 鉉 瑞

1982년 숭실대학교 전자공학과 졸업(학사)
1985년 연세대학교 대학원 전자공학과 졸업(석사)
1993년 연세대학교 대학원 전자공학과 박사과정
1982년 2월~현재 한국전자통신연구소 선임연구원

李 弘 燮(正會員)

1979년 한양대학교 전자공학과(학사)
1985년 한양대학교 전자공학과(석사)
1980년~현재 한국전자통신연구소 책임연구원



李 大 基(正會員)

1966년 한양대학교 전기공학과(학사)
1987년 한양대학교 전자공학과(석사)
1980년~1992년 한국전자통신연구소 산업기술개발부장, 지상시스템연구부장
1992년~현재 한국전자통신연구소 부호기술부장
통신정보보호학회 산학이사