2003년도 대한전자공학회 하계종합학술대회 논문집 제26권 제1호

새로운 GSM의 인증프로토콜 제안

최 현 , 송 윤 경 , 박 동 선
전북대학교 정보통신공학과
전화 : 063-270-2465 / 핸드폰 : 011-9644-0860

Proposal of new GSM Authentication protocol

Hyun Choi, Yun-kyung Song, Dong-Sun Park
Dept. of Info. & Comm., Chonbuk National University
E-mail : hyun66@korea.com

Abstract

Mobile communication network because information through radio channel is passed, information may be *eavesdropped and need information security* countermeasure in communication network dimension for safe information exchange because there is possibility that is manufactured. This paper used Public Key Cryptography for protection and authentication connected with user authentication. Use public key and private key that is asymmetry *encryption key to quote that is used at encryption*, decryption of Public key. Encrypt IMSI and authentication message that is transmitted MS, VLR and HLR interval to public key, wish to embody transmitted authentication protocol safety.

1. 서론

GSM(Global System for Mobile Communications)은 범유럽적으로 추진되고 있는 디지털 이동통신시스템으로서 ETSI에 의해서 표준화가 추진되고 있다. 모든 GSM가입자들은 MS의 SIM카드 안에 HLR과 공유하는 비밀키(Ki)를 저장하고 있다. 가입자는 홈이 아닌 방문 지역에 위치하였을 경우 이동통신서비스를 받기 위해서는 인증프로토콜을 거쳐야 한다. 사용되는 인증 프로토콜방식은 먼저 사용자의 정보가 담겨있는 IMSI을 VLR에 전송하게 되고 VLR은 받은 IMSI을 HLR에 전송하게 된다. HLR은 MS을 인증하기 위하여 도전/응답메시지를 VLR에게 전송한다. 이때 IMSI은 무선구간에서 아무런 보호를 받지 못하고 평문상태로 방문지역으로 보내지게 된다. 또한 홈 지역과 방문 지역사이의 네트워크가 안전하고 가정을 하였기 때문에 방문지역에서 홈지역으로 가입자의 IMSI와 위치정보를 아무런 보호 없이 평문상태로 보내지게 되어 가입자의 정보를 유출시킬 수 있다.

본 논문에서는 사용자인증에 관련된 보호와 인증을 위해서 공개키를 사용하였다. MS에서 HLR로 전송되는 IMSI은 HLR의 공개키로 암호화하게 되고 VLR과 HLR사이에서 전송되는 인증메시지를 VLR과 HLR의 공개키와 비밀키를 사용하여 암호화해서 안전하게 전송되는 프로토콜을 구현해보고자 한다.

본 논문의 구성은 2장에서 GSM에 대한 배경과 구조를 알아보고, 3장에서는 공개키알고리즘에 대해서 살펴보고, 4장에서는 새로이 제안한 GSM인증프로토콜의 방법과 메시지흐름을 살펴보고, 끝으로 5장에서 결론을 맺는다.

2. GSM소개

2.1 GSM 시스템 구조

그림 1은 GSM PLMN의 전체 구조와 핵심적인 요소들을 보여주고 있다. MS(Mobile Station)는 GSM의

이동단말을 나타낸다. 한 셀은 하나의 BTS(Base Transceiver Station)가 관리할 수 있는 라디오 영역으로 구별된다. 다수의 BTS 는 하나의 BSC(Base Station Controller)에 의해 제어된다. BTS와 BSC를 묶어 BSS(Base Station Subsystem)라 부른다. 각 셀에 포함된 MS들로부터 모아진 트래픽은 MSC(Mobile Switching Center)를 통해 네트워크로 라우팅 된다. MSC는 하나의 서비스 영역을 관리하고, 이 관리 영역은 다시 LA(Location Area)로 불리는 영역들로 구성된다. LA는 다수의 셀 그룹으로 구성되고, 이들 그룹마다 하나의 BSC가 할당된다.

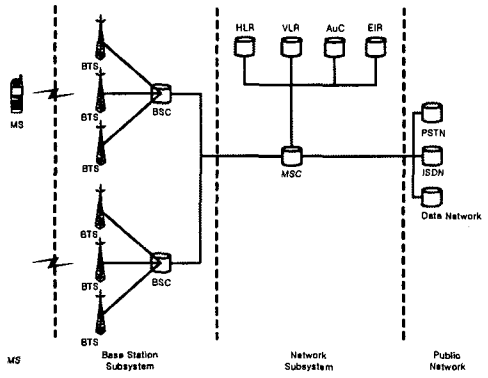

그림 1. GSM 시스템 구조

호 제어와 네트워크관리를 위해 다수의 데이터베이스가 사용된다. HLR(Home Location Register), VLR(Visited Location Register), AuC(Authentication Center), EIR(Equipment Identity Register) 등이 이러한 데이터베이스이다.

HLR은 모든 네트워크 서비스 가입자들에 대한 영구적인 데이터와 임시적인 데이터를 저장한다. 사용자에게 전화가 걸려오면, 현재 사용자의 위치를 알아내기 위해 제일 먼저 HLR 데이터베이스 내용이 참조된다. VLR은 다수의 LA 내부에 위치하는 사용자들에 대한 정보를 관리하는 책임을 가지고 있다. 여기에는 좀 더 빠른 서비스 제공을 위해 HLR로부터 얻어온 정보들도 포함된다. 하지만 VLR이 자체적으로 할당하고 관리하는 정보들도 있으며, MS에게 부여되는 임시 ID (TMSI)가 그러한 예이다. AuC는 인증과 암호화를 위해 필요한 키값과 같은 보안과 인증에 관련된 정보를 저장한다.

GSM은 사용자와 단말을 명시적으로 구분해 별도로 취급한다. 전화 번호, 가입자 ID, 단말 ID이외에도 다수의 ID 가 정의되어 있다. 이들 ID는 가입자 이동성 관리(mobility management)와 기타 네트워크 구성 요소를 지정하기 위해 필요하다.

IMEI(International Mobile Equipment Identity)는 국제적으로 단말을 구분하기 위해 사용된다. IMEI는 장비 제조업자에 의해 할당되며, 네트워크 운영자에 의해 EIR에 그 정보가 저장된다.

각 가입자는 IMSI(International Mobile Subscriber Identity)에 의해 국제적으로 구별되고, 이 정보는 SIM(Subscriber Identity Module)카드에 저장된다. MS은 합법적인 IMSI를 내장한 SIM카드가 합법적인 IMEI를 가진 단말에 삽입되었을 때만 정상적으로 이용이 가능하다.

VLR 은 자신의 관리 영역 내의 이동 단말들을 관리하기 위해 임시적으로 ID 를 부여하는데 이를 TMSI(Temporary Mobile Subscriber Identity)라고 한다. 이 TMSI는 VLR 이 관리하는 LA 안에서만 유효하며 HLR 에게 전달되지 않는다.

2.2 GSM 인증 알고리즘

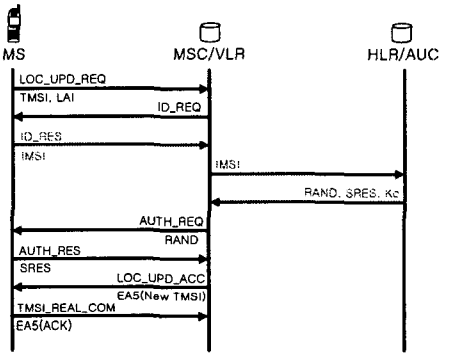

그림 2. 현재의 GSM 인증 알고리즘

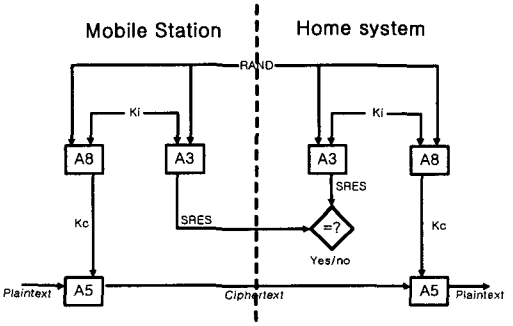

그림 3. 현재의 GSM 인증구조

GSM에서의 인증 절차는 그림 2, 3과 같이 challenge/response방법으로 수행되며, 인가 받은 가입자가 주어진 RAND(Random Number)로 SERS(Signed Response) 생성해서 응답하게 된다. 가입자확인은 인증절차보다 선행되어야 한다. 인증절차는 네트워크에서 먼저 난수(RAND)가 발생하여 MS로 전달함으로 써 시작되면. 난수(RAND)와 인증키(Ki)는 A3인증알고리즘의 입력 데이터로 사용되어 SRES를 계산한다. 이와 마찬가지로 MS에서 수신한 난수(RAND)와 인증키(Ki)를 사용

하여 SRES를 생성하고 이 결과를 네트워크로 보낸다. 네트워크에서는 생성된 SRES와 MS에서 생성된 SRES를 비교하여 값이 동일한 때만 승인된 가입자로 간주한다.

3. 공개키 암호화 알고리즘

공개키 암호시스템에서는 암호화 할 때 사용하는 키와 복호화할 때 사용하는 키가 다른데 전자를 공개키(public key)라 하고 후자를 비밀키(private key)라 한다. 공개키 암호시스템은 공개키와 비밀키를 각각 다르게 생성하여 공개키는 공개하고 비밀키는 안전하게 유지하면 되므로 키의 안전한 분배는 필요없게 된다.

사용자 A가 수신자 B의 공개키로 메시지를 암호화하여 B에게 보내면 B는 자신의 비밀키로 사용자 A가 보내온 메시지를 복호화하여 내용을 파악할 수 있다. 만일 사용자 B가 B 자신의 비밀키로 메시지를 암호화하여 사용자 A에게 보낸다고 하면 사용자 A는 B의 공개키를 이용하여 암호화된 메시지를 복호화할 수 있는데 이것은 아주 재미있는 일이다.

공개키 암호 알고리즘으로는 1978년 개발된 소인수 분해의 난해성을 기반으로하는 RSA(Rivest-Shamir-Adleman)와 미국표준기술연구소가 미국국가안전보장국과 공동으로 이산대수의 문제를 기반으로 개발한 DSA(Digital Signature Algorithm)등이 있다.

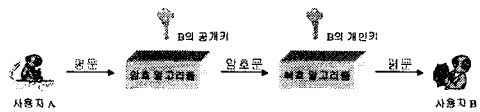

그림 4. 공개키 암호화 방식

4. 새로운 GSM의 인증프로토콜

본 절에서 공개키를 사용하여 GSM의 사용자 인증을 위한 프로토콜 모델과 전반적인 메시지흐름을 소개하였다.

다음은 본 논문에서 사용한 표기법을 나타낸다.

구분	설명
H_{id}	HLR의 ID
K_{Hu}	HLR의 공개키
K_{Hr}	HLR의 비밀키
K_{Vu}	VLR의 공개키
K_{Vr}	VLR의 비밀키
RC5	RC5의 암호화키
EK_x(message)	암호화 키 K_x를 사용해서 message를 암호화함.

표 1. 구현과정의 표기법

제안된 프로토콜의 구체적인 동작은 다음과 같다. 본 논문에서 제안한 프로토콜상의 메시지는 메시지 필드 값들은 전체적인 인증 절차만을 설명하기 위해 간략화 시킨 형태로써, 필요에 의해 다른 정보들도 같이 실어 전송할수 있다.

초기가정한값으로는 SIM카드에 Ki, IMSI, TMSI, HLR의 공개키가 저장되어 있다. MS는 새로운 LA에 들어왔다.

전체적인 메시지흐름은 그림5와 같다.

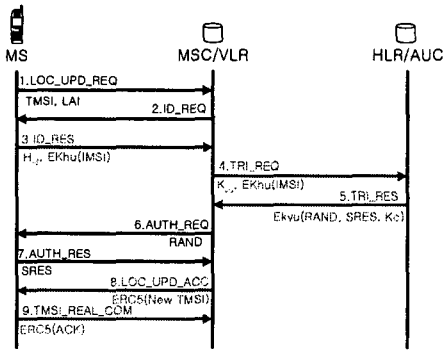

그림 5. 새로운 GSM의 인증프로토콜

다음은 메시지 흐름에 대한 설명이다.

1. MS측에서 네트워크 측에 접근하기 위해서 MS의 SIM카드에 저장되어있는 TMSI와 LAI을 VLR에 전송한다.

2. VLR에서는 MS에서 보내온 TMSI와 LAI을 확인한다. TMSI으로 MS을 확인할수 있으면 이전에 등록된 MS의 IMSI(K_{Hu}으로 암호화됨)을 HLR로 전송하면 되지만 VLR에서 알 수 없는 TMSI이라면 MS에게 IMSI을 요구하는 메시지를 MS에게 보내게 된다. 본 논문에서는 VLR에서 MS의 TMSI을 알수없는 값으로 가정하고 MS에게 MS의 IMSI을 요구하게 된다.

3. MS는 VLR에서 MS의 IMSI을 요구하는 메시지를 받으면, HLR의 공개키(K_{Hu})로 IMSI을 암호화하여 HLR의 ID(H_{id})와 함께 VLR에게 전송하게 된다.

4. VLR은 MS로부터 받은 H_{id}(HLR의 ID)을 가지고 MS가 등록되어있는 HLR을 찾을수 있다. VLR은 자신의 공개키와 함께 MS의 IMSI을 HLR에게 전송한다. 이때 VLR은 HLR의 비밀키를 알지못하므로 IMSI을 복호화하지 못하므로 HLR의 공개키로 암호화된 IMSI을 그대로 HLR에게 전달하게 된다. VLR에서 MS의 IMSI을 알지 못하게 하는 이유는 MS가 방문한 지역이 보안적으로 안전하지 못할 경우가 있을 경우를 대비한 것이다.

5. HLR은 VLR으로부터 받은 IMSI을 자신의 비밀키로 복호화하여 IMSI을 얻을 수 있다. HLR, AuC에서는 IMSI, Ki, RAND으로 A3, A8 알고리즘을 돌려서 SRES와 Kc을 만들어 낸다. 만들어진 RAND, SRES, Kc들은 VLR의 공개키로 암호화되어 VLR로 전달되게 된다. VLR과 HLR사이에 공개키알고리즘을 사용하는 이유는 MS가 방문하는 지역과 홈지역사이의 네트워크가 안전하지 못할경우를 대비한 것이다.

6. VLR은 HLR에서 보내진 RAND, SRES, Kc 들은 자신의 비밀키로 복호화하여 RAND, SRES, Kc 들은 얻을수 있다. SRES와 Kc은 자신이 저장하고 RAND은 MS을 인증하기 위해서 MS에게 보내어진다.

7. MS에서는 VLR에서 보내어진 RAND과 SIM카드에 저장되어 있는 Ki으로 A3, A8알고리즘을 돌려서 SRES, Kc 을 산출해낸다. Kc은 SIM카드에 저장하고 SRES은 자신을 인증하기 위해서 VLR로 전송한다.

8. VLR은 MS에게 받은 SRES과 HLR에서 받은 SRES을 서로 비교하여 MS을 인증하게 된다. MS을 인증하게 되면 VLR은 MS에가 새로운 TMSI을 할당한다.

9. MS는 새로 받은 TMSI을 저장하고 VLR에게 ACK 신호를 보낸다.

기존의 제안 방법들은 MS의 고유 ID를 제공하기 위해서 IMSI를 직접보내거나, IMSI의 직접적인 전송을 막기 위해 별도로 MS를 구별할 수 있는 ID를 만들어 네트워크에 전송, 별도의 데이터베이스에서 정보를 찾아내서 인증을 시도하는 과정을 거치고 있다. 이러한 방법은 각각의 네트워크에 IMSI가 유출 될 수 있다는 문제점과 별도의 데이터베이스추가가 고려되어야 되고 데이터베이스의 관리가 문제된다는 단점을 가지고 있다. 본 논문에서는 IMSI를 MS가 등록되어 있는 HLR의 공개기로 보호하고 있어, 신뢰할 수 없는 네트워크에서 VLR은 MS를 인식하여 HLR을 찾는 방법이 별도로 필요하게 되었는데, 본 논문에서는 HLR을 찾아내기 위한 수단으로 H_{id}을 사용하도록 하였다. H_{id}은 IMSI에서 MCC(Mobile Country Code)와 MNC(Mobile Network Code)을 조합해서 만들 수 있다. 그러므로 별도의 ID를 만들 필요가 없이 기존의 값을 사용하면 된다. 이때 IMSI에서 MSIN(Mobile Subscriber Identification Number)은 사용자의 고유번호이기 때문에 공개돼서는 안 된다.

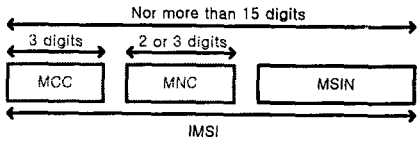

그림 6. IMSI필드값

5. 결론

본 논문에서는 IMSI를 MS가 등록되어 있는 HLR의 공개기로 암호화하여 신뢰할 수 없는 네트워크에서 MS의 IMSI을 보호하고 VLR과 HLR사이에서도 공개키암호화방식을 사용해서 VLR과 HLR사이의 신뢰할 수 없는 네트워크에서 데이터를 보호할 수 있다. VLR에서 MS를 인식하기 위해서 HLR을 찾는 방법으로 H_{id}(HLR의 ID)을 사용하도록 하였다. H_{id}은 IMSI에서 MCC와 MNC을 조합해서 만들 수 있다. 그러므로 별도의 아이디를 만들 필요가 없이 기존의 값을 사용하면 된다.

암호화방법으로 사용한 공개키 방식은 비밀키 방식에 비해 부하가 많이 걸릴 수 있지만 이 경우 실제로 암호화되는 메시지의 길이가 상대적으로 짧고 MS의 성능 자체가 발전하고 있고 MS에서는 단순히 HLR의 공개키로 암호화만 하는 방식을 사용하여 많은 부하가 걸리지는 않는다.

본 논문은 기존의 인증프로토콜보다는 빠르고 안전한 인증프로토콜이라고 볼 수 있다.

참고문헌

[1] GSM 02.09 "Digital cellular telecommunications system (Phase 2+); Security aspects"

[2] GSM 03.03 "Digital cellular telecommunications system (Phase 2+); Numbering, Addressing and Identification"

[3] GSM 03.20 "Digital cellular telecommunications system (Phase 2+); Security related network functions"

[4] GSM 04.08 "Digital cellular telecommunications system (Phase 2+); Mobile radio interface; Layer 3 specification"

[5] CCITT Recommendation E.212: "Identification plan for land mobile stations"