공개키 기반의 GPRS 인증 프로토콜과 Key 관리에 관한 연구

김 성용, 송 윤경, 최 현, 박 동선
전북대학교 멀티미디어 연구실

Public Key based GPRS Authentication Protocol and Key management

Sung Yong Kim, Yoon Kyung Song, Hyun Choi, Dong Sun Park
Multimedia Lab., Chonbuk National University

Abstract

GPRS(General Packet Radio Service) 서비스는 circuit 기반의 GSM(Global System for Mobile Communication)의 기본 망구조를 이용하여 packet 서비스를 지원하도록 변형시킨 모델이다. 기본적으로 GPRS는 GSM의 많은 부분을 계승하여 서비스를 지원하고 있기 때문에 GSM이 가지고 있던 문제점을 그대로 이어받게 되었는데, 본 논문에서는 사용자 인증 프로시져등에서 문제시 될 수 있는 부분들에 대해 살펴보고, 이를 보완 할 수 있는 방법으로 공개키의 암호화 모드와 인증 모드를 사용한 인증 프로시져와 시스템 구조를 소개하고자 한다. 또한 공개키 구조의 인증을 사용함으로써 필요로 하게 되는 키 관리에 대한 방법을 제시하고 앞으로 해결해 나가야 될 문제에 대해 언급을 하고자 한다.

I. 서론

2.5세대 통신 규격인 GPRS(General Packet Radio Service)는 이미 상용 서비스하고 있는 GSM(Global System for Mobile Communication)의 하부 구조를 사용하여 별도의 장비 추가 없이 기지국 단에서의 펌웨어 업그레이드를 통한 GPRS 서비스를 지원하도록 하였고 이러한 Packet 서비스를 지원하기 위한 두개의 새로운 네트웍 노드인 SGSN과 GGSN 두개를 추가하였다. 그러나 대부분의 GSM 네트웍 구조를 가져다 사용 하였기 때문에 많은 부분 GSM의 것을 가져오게 되었고, 보안의 취약점도 그대로 가져오게 되었다. 2세대 통신 규격인 GSM 이후의 이동 통신 규격이 기존의 다른 아날로그 등과 같은 통신 방식과 두드러진 차이를 보이는 부분중 하나가 바로 사용자 인증과 정보의 암호화인데, GSM에서는 이러한 사용자 인증을 challenge 방식으로 수행한다. 이러한 구조는 네트웍이 외부의 공격으로부터 안전하다는 가정에서는 별다른 문제가 없었다. 그러나 Network Entity 사이의 연결이 IP망으로 바뀌기 시작하고 기지국 자체를 흉내낼 수 있게 됨으로써 단말기가 접속하는 네트웍에 대한 신뢰성이 떨어지고 그에 비례하여 사용자 정보의 보호가 크게 증가 하게 되었다. 이러한 문제는 비단 GSM뿐만 아니라 GPRS 역시 그대로 가지고 있는 부분이며, 이러한 문제를 해결하기 위해 공개키를 사용한 방법[1]과 추가적인 메시지와 비밀키를 사용하여 인증을 시도하는 방법[2]등이 시도 되었지만, 각각 사용자 인증을 위한 IMSI값과 RAND값만을 보호하고 나머지 시퀀스는 동일 하게 사용하고 있다는 점과 추가되는 메시지에 의해 복잡하다는 단점이 있다.

본 논문에서 사용자 인증 프로토콜로 사용한 모델은 [3]에서 제안하였던 방법으로써, 본 논문에서는 이에대한 자세한 설명은 생략 하도록 하고 대략적인 적용 방법에 대해서 설명을 한후, 이러한 모델을 사용할 때 필요시 되는 키 관리 프로시져에 대해 자세히 살펴 보도

록 하겠다. 이후 2장에서는 GSM/GPRS에서의 사용자 인증 단계와 관련 프로토콜에 대해 살펴보고, 3장에서 GPRS에서 사용자 정보를 보호하기 위해 적용한 공개키 기반의 사용자 인증 프로토콜 방법에 대해 간략히 살펴볼 것이다. 또한 공개키를 사용할 때 필요한 키 배포, 관리에 대한 시스템 구성과 메커니즘에 대해서도 언급하고 4장에서는 이에 대한 결론을 내고자 한다.

II. 관련 프로토콜

2.1. GSM/GPRS

GSM에서의 사용자 인증을 위한 프로시져의 흐름은 그림 1과 같이 최초 인증 요청은 단말기로부터 TMSI(Temporary Mobile Subscriber Identity)를 가지고 시작이 되어 GSM 네트웍의 사용자 정보를 가지고 있는 HLR(Home Location Register)로 사용자 데이터를 요구하고, challenge값을 받아 단말기로 응답을 하게 되면, 단말기는 받은 challenge값을 가지고 response를 만들어 네트웍에 보내어 인증을 수행하는 challenge-response 형식의 프로시져를 따르고 있다[4].

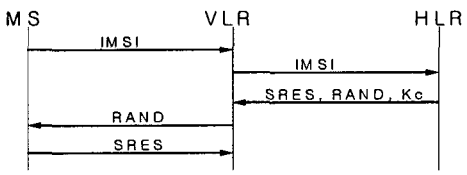

그림 1. GSM에서의 사용자 인증 흐름도

GPRS의 경우는 보통 TLLI(Temporary Logical Link Identity)라 불리는 임시 구분자를 가지고 그림 2에서 볼 수 있듯이 SGSN에서 인증 요구를 시작하는 프로시져를 보이고 있다.

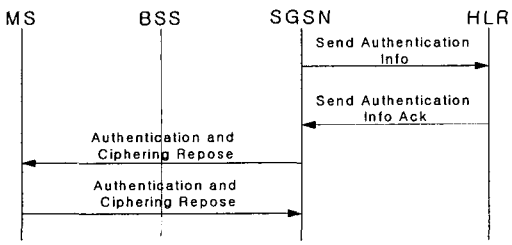

그림 2. GPRS에서의 사용자 인증 흐름도

이 두 경우 모두 네트웍이 단말기의 임시 구분자에 대해 사용자를 확인할 수 있는 대칭되는 값이 없을 경우, IMSI(International Mobile Subscriber Identity)라 불리는 사용자 식별 고유 번호가 네트웍으로 전송이 되어 단말기의 사용자를 인증할 수 있도록 되어 있다. 그림 3은 GPRS에 대해 TLLI값이 확인되지 않을 경우를 보이고 있다. 이는 신뢰를 받는 네트웍에서는 문제가 되지 않지만, 기지국과 같은 네트웍 레벨을 제 3자가 흉내내게 되면 잠재적 공격 지점으로 작용하게 되며, 보안의 필요성이 부각되는 지점으로 남게된다.

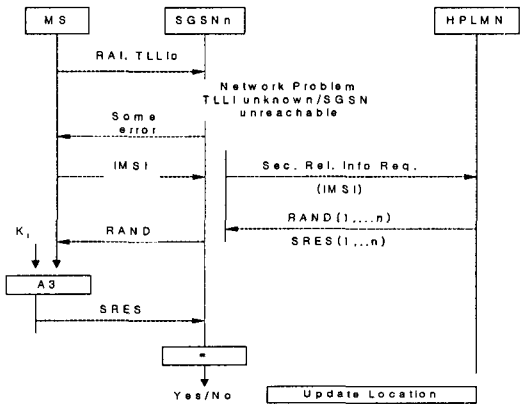

그림 3. TLLI 대응이 실패할 경우 사용자 인증 절차

2.2 공개키 기반의 사용자 인증 프로토콜

기존의 GSM/GPRS 인증 모델에서 가장 큰 문제가 되는 점은 앞에서 언급했듯이 IMSI값이 비보호 상태로 신뢰받지 못하는 네트웍을 통과할 수 있다는 점이다. 이를 보호하기 위해 비대칭키를 사용하는 공개키의 전자 서명 기능과 메시지 암호화 기능을 사용하였다. 그림 4는 이에 대한 전체적 메시지 흐름을 나타내고 있다.

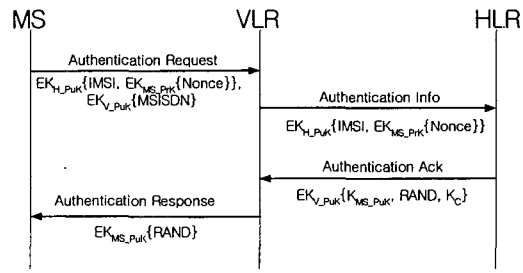

그림 4. 공개키를 사용한 인증 프로토콜 흐름

공개키를 사용한 인증 프로토콜에 대한 자세한 사항은 [3]을 참조해보면 알 수 있다.

III. 제안 모델

3.1 공개키 기반의 사용자 인증 모델

기존의 GSM/GPRS 인증 모델에서 가장 큰 문제가 되는 점은 앞에서 언급했듯이 IMSI값이 비보호 상태로 신뢰받지 못하는 네트웍을 통과할 수 있다는 점이다. 앞서 그림 3에서 보였듯이 GPRS 역시 TLLI값이 확인되지 못할 경우 IMSI값이 그대로 넘어가는 GSM의 인증 방법을 사용하기 때문에, 이를 보호하기 위해 공개키 기반의 사용자 인증을 접목시켰다. 이 제안된 방법은 비대칭키를 사용하는 공개키의 전자 서명 기능과 메시지 암호화 기능을 사용하는 방법으로 사용자의 데이터를 보호함과 동시에 불확실한 네트웍 노드들에 대해 기본적으로 신뢰할 수 없다는 가정 하에 인증을 해나갈 수 있다는 장점을 가지고 있다. 그림 3에서 볼 수 있듯이 TLLI값이 네트웍에서 확인이 불가할 경우 GSM과 동일한 인증 프로시져를 그대로 가져다 쓰고 있기 때문에 GPRS의 경우 역시 적용시킬 수 있게 된다. GPRS에서의 사용자 데이터를 보호하기 위해 사용한 공개키를 사용한 인증 프로토콜에 대한 자세한 사항은 [3]을 참조해보면 알 수 있으므로 자세한 설명은 본 논문에서 제외하였다.

3.2 Key 관리에 대한 제안

위와 같이 공개키를 사용하게 되면, 사용자의 요구나 네트웍의 요구에 의해 암호화에 사용이 되는 키를 갱신시키는 과정이 필요하게 된다. 일단 네트웍은 허가받지 않는 제 3자에 의해서도 구성이 될 수 있다는 잠재적 위험 요소를 가만하게 되면, Key관리를 하기 위한 프로시져로 사용자 인증과 암호화등의 과정이 선행되게 되고, 그 후 키의 교환등이 있어야 한다.

Key관리 모델을 만들기 위해 기본적으로 사용이 되는 모델은 Kerberos의 Ticket을 얻어오는 과정과 흡사하게 구성이 되어 있다. 즉, 단말기가 네트웍의 AuC단까지 키를 보내기 위해서는 현재 구성되어 있는 네트웍에 접근할 수 있는 1차 접근 권한을 기지국이 주기적으로 뿌려주는 broadcast 정보에서 얻어와 이를 가지고 2차적으로 네트웍의 구성요소들과 키 교환을 시도하게 된다. 전체적인 키 교환 모델의 메시지 흐름은 그림 5와 같다.

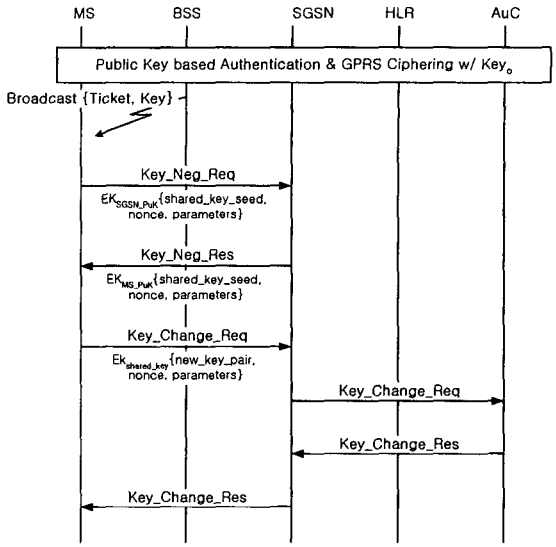

그림 5. 공개키 관리 모델

그림 5에서 볼 수 있듯이 전체적인 프로시져는 GPRS의 사용자 인증과 암호화가 시작된 다음에 일어나게 된다. 실제 이 단계를 거치게 되면 dedicated channel이 형성이 되기 때문에 컨트롤 채널의 길이 제한에 따른 부담이 없어지게 된다. Ticket과 Key는 BSS(Base Station System)에서 주기적으로 전송되는 System Information에 담겨있는 메시지이다. Ticket은 BSS와 SGSN과의 신뢰성을 증가하기 위해 포함이 되는데, 값 자체를 인증값으로 사용할 수도 있지만, 암호화 되는 메시지의 입력 변수로도 사용이 될 수 있다. 일단 정상적으로 SGSN으로 접근이 가능하게 되면, 다음의 두가지 프로시져가 일어나게 된다.

1. 새로운 비대칭키 쌍을 보호하기 위한 Shared key의 협상
2. Shared key를 이용하여 보호되는 비대칭 key pair의 교환

1의 단계에서는 Diffie-Hellman의 키 교환 모델을 이용한 것으로써, 기존의 비대칭 키를 통해 shared_key의 seed값을 서로 넘겨받게 된다. 이 seed값을 기준으로 양단이 동일한 shared_key 생성 알고리즘을 통해 동일한 key를 서로 가지게 되고, 이후 전송되는 메시지에 대해 제 3자의 해독이 불가능하도록 할 수 있게 된다.

1의 단계에서의 대칭키 교환이 정상적으로 끝나게 되면 2단계에서의 새로운 키 갱신을 수행하게 된다. 이

단계는 단말기에서 SGSN으로 1차적인 키 전송을 하게 되고, 이를 HLR로 전송하여 AuC(Athentication Center)에 저장되어 있는 단말기의 정보를 갱신하게 된다.

VI. 결론

본 논문에서는 GPRS에서도 역시 문제를 가지고 있는 사용자 인증의 문제점에 대해서 알아보았고, 이를 해결하기 위한 방법으로 공개키 기반의 사용자 인증 프로토콜의 이용에 대해 알아보았다. 또한 이러한 공개키를 사용함으로써 기존에 사용하던 키 쌍을 갱신해야 될 때 필요로 하는 메시지들에 대해 제안을 하였다.

GPRS에서의 사용자 인증은 SGSN에서 시작이 되고 임시로 사용하는 데이터 역시 TLLI를 사용하는 점이 GSM과 다르지만, 일단 네트웍쪽의 문제로 인하여 TLLI와 IMSI를 대응시키지 못할 경우 GSM의 TMSI 대응 실패시 사용하는 프로시져와 동일한 프로시져를 가져다 쓰기 때문에 공개키 기반의 GSM인증 프로토콜을 그대로 사용할 수 있게 된다. 이 방법은 네트웍이 기본적으로 신뢰할 수 없는것에 기반을 두고 만들어졌기 때문에 차후 All-IP망이 들어가면서 생길 수 있는 유사 기지국과 같은 문제에 대해 해결책을 제시해줄 수 있다.

또한 키 교환을 사용하기 위해 제안된 메시지들은 SGSN과 1차적으로 새로운 키 쌍을 만들기 위해 사용할 대칭키의 *seed*값들을 교환하고, 사전에 정의 되어 있는 키 생성 알고리즘을 통해 새롭게 적용될 비대칭 키 쌍을 보호하도록 하였다. 이때 대칭키를 만들기 위해 사용이 되는 알고리즘은 기존의 GPRS에서 사용이 되는 알고리즘을 그대로 사용할 수도 있고 각 메시지 전송시 넘겨지는 nonce값고 다른 parameter값들과의 HASH function에 의해 만들어진 값에 의해 수행이 될 수도 있다.

비대칭 키는 대칭키에 비해 연산 부하가 크기 때문에 메시지의 길이가 길어질수록 제한된 성능을 가지고 있는 이동 단말기 환경에 접목하기 힘들어지게 된다. 제안한 알고리즘은 전체적으로 단말기에 많은 성능을 요구하고 있기 때문에 메시지의 길이를 최대한 줄이는 방법이 일차적인 부하를 줄일 수 있는 방법이지만, 현재 단말기 자체의 성능 역시 계속 발전하고 있고, PDA등에 GPRS 모듈을 얹어 사용하는 경우는 이러한 기능을 GPRS 모듈에서 하지않고 PDA쪽으로 돌려 구현할 수 있기 때문에 차후 큰 문제가 되진 않는다.

차후 제안된 모델을 실제 GPRS에 접목시킬 때 발생할 수 있는 각 노드단에서의 부하와 기존에 이미 사용이 되고 있는 GPRS 네트웍 망에 하위 호환이 될 수 있도록 검증하는 단계가 이루어져야 할 것이다.

참고 문헌

[1] Grecas, C.F.; Maniatis, S.I.; Venieris, I.S., Towards the introduction of the asymmetric cryptography in GSM, GPRS, and UMTS networks, Computers and Communications, 2001. Proceedings. Sixth IEEE Symposium, pp 15-21, 2001

[2] El-Fishway, N.; Nofal, M.; Tadros, A., An Effective Approach for Authentication of Mobile Users, Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th , Volume: 2 , pp 598-601, 2002

[3] 김성용, 송광석, 박동선, 공개키를 이용한 GSM 인증 프로토콜의 연구, 2002 대한전자공학회 추계 학술대회, pp 745-748

[4] GSM 03.20 Security related Network Functions, v8.1.0(2001-07)

[5] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[6] Hakan Granbohm and Joakim Wiklund, GPRS-General Packet Radio Service, Ericsson Review No. 2, 1999

[7] NetScreen Technologies Inc., GPRS Security Threats and Solutions, March 2002

[8] Charles Brookson, GPRS Security, December 2001