4세대 이동통신에 필요한 정보보호 기술

김건우, 강주성
한국전자통신연구원
wootopian@etri.re.kr

Information security for 4G mobile telecommunication

Keonwoo Kim, Jusung Kang
ETRI

요 약

3세대 이동통신은 점차 새로운 멀티미디어 서비스를 제공하는 Systems beyond IMT-2000 이라 불리우는 4세대 이동통신 시스템으로 그 영역을 넓혀가고 있다. 4G 이동통신은 3G IMT-2000의 진화, Systems beyond IMT-2000을 위한 기술적인 capabilities 향상 뿐만 아니라 이종 시스템 간의 interworking도 모두 포함하게 된다. 이러한 4세대 이동통신 환경에서 모바일 상거래 등의 다양한 응용 서비스를 활성화하기 위해서는 무엇보다도 정보보호 기술이 필수적으로 제공되어야 한다. 이를 위해, 핵심 정보보호 기반 기술인 암호화, 무결성, 인증, 익명성 보장 등을 위한 알고리즘과 프로토콜 및 인터넷 환경에서의 제반 응용 보안 기술에 관해 살펴보고자 한다.

1. 서 론

이동통신 정보보호는 이동통신 시스템에서 사용자와 네트워크 운영자 및 서비스 제공자의 권익 보호, 개인 프라이버시 등의 안전한 서비스를 제공할 수 있게 하는 전반적인 보안 기술을 일컫는다.

비동기식 IMT-2000 표준을 개발하고 있는 3GPP에서는 이미 R5 보안 기술을 거의 완료하였으며, R6 보안 작업은 현재 활발히 진행중이다. R5 이후로 진화하면서 IP 멀티미디어 서비스가 도입되고 이에 따라 기존 인터넷에서 이루어지던 많은 멀티미디어 서비스들이 이동통신 서비스로 확대되고 있으며 다양한 서비스 제공 및 VHE 실현을 목표로 하는 이동통신에서 정보보호 기술은 더욱더 중요한 기술로 대두되고 있다. 또한, 동기식 3세대 이동통신 시스템에서의 접근 제어, 키 관리, 데이터와 신원 보호 등의 정보보호 기술은 3GPP2에 의해 표준화가 진행중이다. 특히, 가입자와 네트워크의 상호 인증을 위한 강화된 가입자 인증 기술(Enhanced Subscriber Authentication), 허가되지 않은 개체에게 정보가 노출되는 것을 방지하는 액세스 구간에서의 강화된 가입자 보호 기술(Enhanced Subscriber Privacy)과 cdma2000 패킷 데이터 보호 기술, 민감한 키에 대한 키 설정 및 관리 기술 표준을 규격화하고 있다. 뿐만 아니라, seamless 이동성과 새로운 모바일 응용 서비스 제공을 가능하게 하는 All IP 기반 무선 네트워크 표준 개발이 진척됨에 따라 이에 필요한 상호 인증, 권한 부여, 기밀성, 무결성, 부인 방지 등과 같은 보안 메커니즘들을 개발하고 있다.

현재 ITU와 3GPP, 3GPP2 같은 Partnership Projects를 중심으로 전개되는 IMT-2000의 표준화는 점차 새로운 멀티미디어 서비스를 제공하는 Systems beyond IMT-2000이라 불리우는 4G 이동통신 시스템 표준화로 그 영역을 넓혀가고 있다. 4G 이동통신은 3G IMT-2000의 진화, Systems beyond IMT-2000을 위한 기술적인 성능 향상 뿐만 아니라 이종 시스템 간의 interworking도 모두 포함하게 된다. 이에 통신관련 국제 표준화 기구인 ITU는 표준화 기본골격, 요소기술 선정 등을 통한 차세대 이동통신의 표준화를 추진하고 있다. ITU-T SSG에서는 네트워크 측면에서 3G 이후에 대한 밑그림 작업을 완료하였고, ITU-R의 WP 8F에서는 무선 측면에서 4G 이동통신의 vision과 관련된 작업이 활발히 진행 중에 있다.

3GPP나 3GPP2에서는 4G 이동통신 정보보호 기술에 대한 직접적인 언급은 하고 있지 않지만, 이동통신이 3G에서 4G로 진화하는 시점에서 R5, R6은 그 중간 단계로 간주할 수 있으며, 특히 R6에서의 정보보호 기술은 4G 이동통신용 정보보호 기술의 기초를 이룰 것으로 기대된다. 따라서, 4G 이동통신 시스템이 구체적으로 정의되지 않은 현 시점에서 4G 이동통신 정보보호 기술을 정의, 개발하고 표준화하기 위해서는 enhanced IMT-2000으로 간주되는 R5와 R6 및 cdma2000 1x EV-DV에서의 정보보호 기술에 대한 연구가 필요할 것으로 보여진다. 이러한 4G 이동통신에서의 정보보호 기술은 4G용 이동통신 인증 메커니즘 기술, 4G용 암호화 및 무결성 기술, 키 분배 및 관리 메커니즘 기술, 기타 특정 서비스에 따른 보안 프로토콜 기술 등으로 분류할 수 있다.

본 논문에서는 4세대 이동통신을 위한 정보보호 기술의 필요성을 언급하고 3G, 3.5G, 4G로 이동하는 이동통신 패러다임에서 요구되는 정보보호 기술에 관하여 분석하였다.

2. 4G 이동통신 정보보호 기술의 필요성 및 비전

4G 이동통신 정보보호 기술은 정당한 사용자가 안전하고 편리을 부여할 수 있도록 하는 것이 기본 목표로 악의적인 공격자 및 응용으로부터 사용자의 개인 프라이버시 및 단말기를 보호하고 악의적인 사용자로부터 네트워크 자원을 보호하는 것을 목표로 한다. 또한, 이러한 보안 기술을 개발하는데 있어 현재 정의되지 않은 서비스 및 응용들도 프레임워크의 큰 변화 없이 제공할 수 있도록 보안 메커니즘을 개발할 것을 목표로 한다.

4G 이동통신에서는 유선망에서 이루어지던 컨텐츠들이 이동 단말을 통해 전송되고 다양한 IP 기반 서비스들이 제공됨에 따라 각 서비스에 따른 보안 프로토콜 개발과 유/무선 통합에 따른 다양한 단말 시스템 사이의 보안 메커니즘의 개발도 필요할 것으로 보인다. 이러한 4G 이동통신 시스템의 확대 및 다른 시스템들과의 연동과 다양한 IP 멀티미디어 서비스 제공으로, 정보보호 기술의 역할이 커질 것으로 예상되며 현재 이동통신 기술에서 뒤지지 않은 우리나라가 계속해서 4G 이동통신에서

도 우위를 차지하기 위해서는 국제 정보보호 기술을 반영하는 정보보호 기술의 개발 및 표준화가 필요하다.

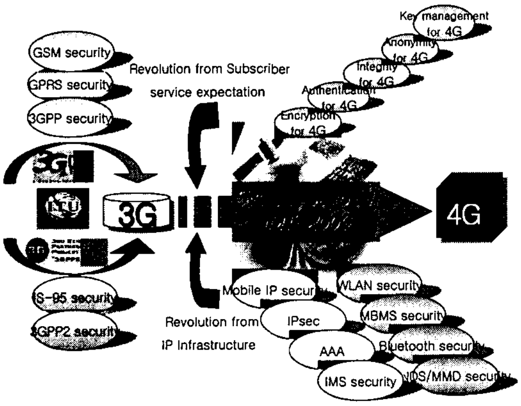

그림 1. 이동통신 정보보호 기술 진화

4G 이동통신은 ITU에서 vision을 제시하고 장기적인 로드맵을 작성하고 있는 단계로 아직까지 주파수 분배나 다른 기술적인 문제는 구체적으로 제시되고 있지 않다. 2G에서 3G IMT-2000으로의 이동통신 시스템의 진화와 마찬가지로 새로운 4G 이동통신 시스템의 도입 시기에는 IMT-2000의 진화된 시스템과 공존할 것으로 전망되고 아울러 기존의 세대별 구분과는 다른 형태로 전개되리라 예상된다. 따라서, 현재 진행중인 IMT-2000 정보보호 기술의 동향을 분석하고 이를 바탕으로 IMT-2000에서 좀 더 강화된 개념의 통신 시스템, 궁극적으로는 beyond IMT-2000인 4G 이동통신 시스템에서의 정보보호 기술에 관한 요구사항을 정립하여 관련 기술들을 개발하여야 한다. 이러한 다양한 어플리케이션의 활용이 예상되는 미래 통신 시스템에서 보다 더 안전하고 강화된 정보보호 기술이 필요한 이유는 다음과 같다.

첫째, 국내 3G 동기식/비동기식 IMT-2000 서비스 실현이 현실화됨에 따라 다양한 정보보호 서비스가 장착된 안전한 이동통신 환경 구축이 필요하고, 이에 따른 가입자 관련 정보 및 다양한 서비스 보호를 위해 암호화, 인증, 무결성 보장 등 정보보호 핵심기술의 개발이 매우 중요해졌다.

둘째, 안전한 4G 이동통신 시스템은 기술 경쟁력에 의해서만 시장확보가 가능하고 이를 위해 지속적인 기술 고도화가 요구된다.

셋째, 최근에는 3G 이동통신 시스템의 완전한 상용화가 이루어지지 않은 시점에서도 이미 선진국들은 4G 이동통신 시스템에 대한 표준규격 선점경쟁에 돌입하였으므로, 3G 시스템의 개발과 표준화에 어려움을 겪었던 우리나라는 초기 단계에서부터 4G 이동통신 정보보호기술 개발에 참가하여 핵심기술의 확보가 필요하다.

마지막으로, 4G 이동통신 시스템의 안전한 국가적 인프라 구축을 위한 표준기반의 정보보호 핵심 기술의 조기 개발과 국가 정보화 경쟁력 확보가 시급하다.

3. 4G 이동통신 정보보호 핵심기술

3.1 4G용 인증 메커니즘 기술

4G 이동통신 시스템에서 각 개체들 사이에서 상대를 정당한 개체로 인증하는 기술로써 악의적인 사용자, 응용, 시스템들의 공격을 방어하고, 정당한 사용자들의 통신을 보장하기 위해 필요한 기술로 다음과 같이 분류할 수 있다.

- 가입자와 IP 기반 서비스 제공 네트워크간의 상호 인증 기술
- 이종 네트워크 사이의 상호 인증 기술
- Application과 네트워크 사이의 상호 인증 기술
- Application과 단말기 사이의 상호 인증 기술
- WLAN interworking security : 무선 랜 서비스 제공자와 이동통신 시스템 도메인 사이의 상호 인증 기술
- Authentication framework 개발 : 글로벌 로밍을 위해 이종 네트워크간의 통신은 필수적이다. 안전한 이동통신망을 구축하기 위해 이종 네트워크 사이에서도 IPSec이 사용되는데, 현재까지는 pre-shared 키 교환 방식이 사용되고 있다. 그러나, 이에 대한 보완 및 강화가 필요하며 다양한 네트워크 도메인들의 출현을 예상할 때 공개키 방식의 키 교환을 사용하는 PKI 기반 SA 설정 및 인증 방식이 필요하다.
- 사용자 장비들 사이의 상호 인증 기술 : 4G 이동통신에서는 다양한 단말기의 통합 사용이 예상된다. 따라서, 다양한 단말 시스템들의 상호 인증을 통한 단말기 보호 및 가입자 정보보호에 사용되는 기술

3.2 4G용 암호화 및 무결성 기술

4G 이동통신 시스템의 모든 구간에서 전송되는 사용자 데이터와 개인 정보를 보호하고 시그널링 데이터를 보호하기 위한 기술로 데이터의 변조가 없음을 증명하는 무결성 기술과 정보의 기밀성을 제공하는 암호화 기술로 분류할 수 있다. 이들 기술은 시스템들 사이에서 적용되는 보안 메커니즘에서 사용될 것이며, 고속 서비스를 지향하는 4G 시스템에 적합한 고속/고비도 암호화 알고리즘, 무결성 알고리즘 기술이 필요하다.

3.3 키 분배 및 관리 메커니즘

4G 이동통신 시스템에서 인증 메커니즘, 암호화와 무결성 메커니즘 등을 제공하기 위해 필요한 기술로 키 생성, 분배, 파기 등의 키 관리 기술이 필요하다. 이 기술은 또한 국가의 법적인 장치를 필요로 하며 글로벌 PKI 기술과도 연관되어 있다. 4G 이동통신 시스템은 All IP로 진화하고, 다양한 시스템들의 상호 연동을 통한 글로벌 서비스가 될 것으로 예상되므로, 필요할 때 마다 관계가 형성되는 각 개체들 사이의 상호 인증과 키 분배 및 관리 기술은 필수적이다. 이러한 기술은 현재 정보보보 기술 동향을 고려할 때 PKI 기반의 상호 인증과 키 교환 방식으로 통합될 것으로 전망된다.

3.4 IPSec, Mobile IP, SIP Security

4G 이동통신 시스템에서 가입자와 IP 기반 서비스 제공 네트워크 사이, 이종 네트워크간, 동종 네트워크 내에서 사용되는 보안 메커니즘으로 인터넷 표준으로 사용되고 있는 기술이 IPSec이다. 이동통신 시스템에 적합하게 SA 설정 방식 등을 변형하여 사용하며, IMS 접속 구간에서는 AKA 메커니즘을 통해 SA 설정을 얻기도 한다. 따라서, IPSec과 Mobile IP 기술은 IETF 등에서 현재 연구하고 있는 표준 기술 뿐 아니라, 이를 이동통신 시스템에 적합하게 개발하는 것이 필요하다. SIP security는 VoIP 서비스 제공에 있어 세션을 안전하게 설정하는 데에 사용되는 보안 기술이다.

3.5 특정 서비스에 따른 보안 프로토콜 기술

4G 이동통신으로 진화하면서 유선 인터넷 망에서 이루어지던 많은 IP 기반 서비스들이 이동통신 서비스로 확대되고 있다. 그러나 무선 구간에서의 정보 탈취가 용이하다는 점이 이동통신에서 정보보호 기술의 필요성을 강화하고 있다. 따라서, 이동통신 환경에서 제공되는 특정 서비스에 적합하게 개발되는 정보보호 기술이 필요하며, 현재 3G에서 제기되고 있는 서비스 관련 정보보호 기술은 MBMS Security, LBS security 등이 있다.

- MBMS Security : 이동 단말을 상호 통신용으로 사용할 뿐 아니라, 서비스 가입자가 정보를 다운로드받을 때 자원의 효율적 사용을 위해 서비스 제공자는 많은 사용자들에게 동시에 정보를 방송하는 기술을 사용하게 될 것이다. 이러한 MBMS 기술은 4G 이동통신 발전에 크게 영향을 미치는 서비스 가운데 하나가 될 것으로 전망된다. 정당한 사용자의 권리를 보호하고 서비스 제공자 및 시스템 운영자의 권익을 보호하기 위해 적절한 사용자 인증과 방송되는 정보의 암호화 기술 등이 요구된다. 이는 다수의 사용자가 공동의 자원을 사용하게 되므로 고도의 보안 메커니즘 개발이 필요하며 현재까지 상용화된 보안 기술이 아니므로 좀더 깊은 연구 및 개발이 필요하다.

3.6 암호 알고리즘 안전성 분석 기술

4G 이동통신 시스템에 적용되는 암호 알고리즘은 다양한 암호학적 공격에 대한 안전성 분석이 필수적이며, 최적 기능 설계시 안전성 검증으로 신뢰할 수 있다. 그러므로 다음과 같은 기본적인 암호 알고리즘 분석 기술은 필수적이다.

- 대칭키 암호 알고리즘의 안전성 분석 기술 : 차분 및 선형 공격을 바탕으로 이들의 변형으로 볼 수 있는 고차 차분 공격, 부정 차분 공격, 불능 차분 공격, 보간 공격, 부 채널 공격 등의 대칭키 암호 안전성 분석 기술이 요구된다.
- 공개키 암호 알고리즘 안전성 분석 기술 : 공개키 암호 알고리즘의 안전성은 그 암호 알고리즘의 기반이 되는 수학적 난제(소인수 분해, 이산대수 문제 등)를 분석하는 연구와 함께 실제 적용시 발생되는 정보보호 프로토콜 관점의 안전성 분석 연구를 병행함으로써 균형있는 공개키 안전성 분석 기술이 요구된다.
- 해쉬 함수 및 MAC 알고리즘 안전성 분석 기술 : 블록 암호를 기반으로 하는 해쉬 및 MAC 함수의 안전성 분석 기술을 확보하여 4G 이동통신 시스템에서 활용될 해쉬 및 MAC 함수의 안전성 분석에 적용한다.
- 증명 가능한 안전성 분석 기술 : 유사 랜덤성(pseudo-randomness), 차분 및 선형 공격에 대한 증명 가능 안전성, 확률 공개키 암호의 안전성 등 안전성을 이론적으로 증명할 수 있는 기술을 연구 및 개발함으로써 4G 이동통신 정보보호 시스템 안전성 분석에 활용한다.

3.7 기타 보안 기술

미래 통신 시스템의 진화는 convergence를 위한 IP 기반 망의 통합과 이종 엑세스 시스템간의 연동으로 정의할 수 있다. 이를 위하여 IP 기반의 서비스에 따른 QoS 지원과 RT(Real Time)서비스의 지연문제와 함께 IP 기반핵심망 프로토콜 보호 메커니즘 및 seamless 서비스를 위한 access security에 대한 연구가 해결되어야 한다. 아울러 핸드오버와 로밍을 지원하기 위한 통합된 이동성 관리와 AAA(Authentication, Authorization, Accounting)와 같은 보안 메커니즘이 필요하다.

하지만 아직까지는 4세대 이동통신 표준화의 수준은 초기 프레임워크를 구성하고 있는 단계이며, 이후 서비스 요구 사항 정의, 기능 요구 사항 정의, 망 모델 참조 정의, 정보보호 요구사항 정의 등 단계별 정의가 이루어질 예정이다.

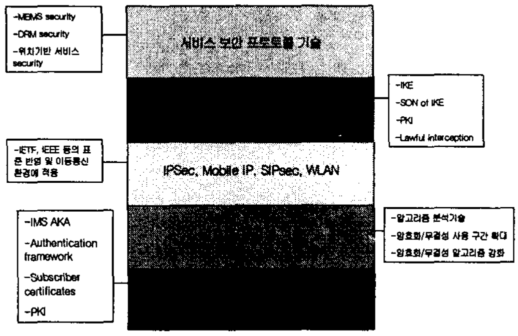

그림 2. 4G 이동통신 정보보호 요소기술

4. 결 론

4G 이동통신용 정보보호 기술은 이미 존재하는 요소기술과 새로운 개념의 보안기술을 4세대 환경을 고려하여, 이동통신 시스템에 적용하는 기술 개발이 필요하며, 3GPP/3GPP2/IETF 등의 기술개발 결과를 반영해야 한다. 인증 메커니즘 기술은 인증을 요구하는 시스템 구간별로 별도 개발하는 것이 필요하며, 키 분배 및 관리 메커니즘 기술은 현재 완료되거나 진행중인 키 관리 기술을 분석하여 4세대 이동통신 환경에 적합한 기술 개발을 추진하되 PKI 기술 등과의 연동 또한 고려해야한다.

3GPP와 3GPP2를 중심으로한 IMT-2000 시스템 표준 결과를 바탕으로, 향후 4세대 이동통신 시스템에서의 선도적 위치를 확고히 하기 위해서는 ITU-R, ITU-T, IETF, 3GPP, 3GPP2 등의 전 세계적으로 Beyond IMT-2000의 표준 및 개발 관련 단체의 주요 요소기술에 대한 동향 파악 및 이의 개발에 적극적이어야 한다. 물론 독창적인 선도기술을 개발하고 이를 국제단체를 통해 보급하는 것은 더욱 중요하고 가치있는 일이다. 그래서, 4G 이동통신 시스템에 중요한 요소기술 및 서비스들에 대한 지적재산권(IPR) 확보하여 향후의 기술개발 및 표준 전쟁에서의 교두보를 확보하고 국내기술을 국제표준으로 제정하도록 노력하여야 할 것이다.

참고문헌

[1] http://www.itu.int/ITU-R/study-groups/rsg8/rwp8f/
[2] http://www.itu.int/ITU-T/studygroups/ssg/
[3] http://www.ietf.org
[4] http://www.3gpp.org
[5] http://www.3gpp2.org
[6] http://www.4gvision.or.kr