3G LTE 및 SAE 네트워크에서 키 관리 방법에 관한 연구†

*정영준 **윤승환 ***이옥연 ****임종인

고려대학교 정보경영공학전문대학원, *** 국민대학교 자연과학대학 수학과

*yz0415@naver.com

The Study on The Key Management Mechanism on 3G LTE and SAE

*Jung, Young-Jun **Yun, Seung-Hwan ***Yi, Okyeon ****Lim, Joing-In

Graduate School of Information Management & Security,

*** Department of Mathematics, Kookmin University

요약

차세대 이동 통신 서비스 4G는 이동 중 100Mbps, 정지 중 1Gbps급 전송 속도를 제공하는 미래 무선 통신 기술이다. 이것은 현재 상용서비스가 이뤄지고 있는 3G HSDPA(High Speed Packet Access)의 전송속도 14Mbps에 비해 10~100배까지 빠른 속도로 무선 인터넷이 가능함으로 유선으로 인터넷을 사용할 필요가 없어진다. 현재 4G 기술로 진화하기 위한 중간 단계로써 ITU-R, 3GPP, 3GPP2, IEEE 등 세계 각국의 표준 및 기술 단체에서 새로운 무선 이동 통신 기술을 제안하고 있다. 이 중에서 2G의 GSM과 3G의 비동기식 기술 WCDMA의 진화 기술인 3GPP LTE(Long Term Evolution) 및 SAE(System Architecture Evolution)가 유력한 4G 이동 통신 기술 후보로 평가 받고 있다.

본 논문에서는 4G 기술로 주목 받고 있는 3GPP LTE 및 SAE 네트워크에서 3G 시스템 보다 진화된 서비스를 제공하기 위한 목적으로 논의되고 있는 일반적인 요구사항과 이를 만족시키기 위한 기술에 대하여 알아본다. 또한 LTE 표준화와 병행하여 네트워크의 구조를 결정하는 SAE의 구성요소와 프로토콜 구조를 소개하고 LTE 및 SAE 네트워크의 보안위협과 안전한 통신을 위한 키 관리 방법에 대하여 논의한다.

1. 서론

국제전기통신연합은 차세대 이동 통신 서비스 4G를 현재 상용서비스가 이뤄지고 있는 HSDPA의 전송속도에 비해 10~100배 까지 빠른 속도로 무선 인터넷이 가능한 무선 통신 기술로 정의하고 공식 명칭은 'IMT-Advanced'라고 칭하였다. 따라서 모든 서비스가 고속의 인터넷 기반으로 이뤄져 무선으로 음성과 영상, 데이터를 한꺼번에 처리할 수 있는 TPS(Triple Play Service)가 가능해진다.

현재는 4G 기술로 진화하기 위한 중간 단계로써 세계 각국의 표준 및 기술 단체에서 새로운 무선 이동 통신 기술을 제안하고 있으며, 이 중 3GPP LTE가 유력한 4G 이동 통신 기술 후보로 평가받고 있다.[1]

이러한 3GPP LTE 표준은 급속히 발전되는 통신 서비스를 효율적으로 제공하기 위해서 3GPP R6보다 고품질의 다양한 새로운 이동 통신 기술의 필요성을 인식하고 낮은 전송 지연, 높은 전송률, 시스템 용량과 커버리즈를 개선하여 작성되고 있다. 이들 연구는 상호 운용성을 제공하기 위한 기술적 솔루션을 최소로 하면서 다양한 액세스 네트워크 사이에서 이동성을 제공하는 것을 목적으로 하고 있다.

SAE는 LTE 표준화와 병행하여 LTE에서 정의하는 목표 실현을 위해 네트워크 구조를 결정하고 이종 네트워크 간 핸드오버를 지원하기 위한 기술을 연구한다.

본 논문에서는 3GPP LTE 및 SAE 네트워크에서 논의되고 있는 일반적인 요구사항과 이를 만족시키기 위한 기술에 대하여 알아본다. 또한 LTE 표준화와 병행하여 네트워크의 구조를 결정하는 SAE의 구성요소와 프로토콜 구조를 소개하고 LTE 및 SAE 네트워크의 보안위협과 안전한 통신을 위한 키 관리 방법에 대하여 논의한다.

2. LTE 및 SAE의 개요

가. Long Term Evolution(LTE)

3G시스템에서 최대 및 평균 data rate을 높이고 IMT-2000의 진화된 서비스를 목적으로 low latency를 제공하기 위하여 Long Term Evolution(LTE) 표준화가 진행되고 있다.[2]

구체적인 목표는 WCDMA(Wideband Code Division Multiple Access) 대역폭의 4배인 20MHz 대역폭을 기준으로 downlink에서는 100Mbps를 uplink에서는 50Mbps를 목표로 하고 있으며, delay 측면에서는 단말에서 IP의 edge router까지 사용자 패킷이 도달하는데 걸리는 시간이 5ms보다 작을 것을 요구한다.

이와 같은 요구 조건을 만족하기 위해서 LTE에서는 새로운 다중 접속 기술과 다중 안테나 기술인 MIMO(Multi Input Multi Output)등의 발전된 물리계층 기술과 네트워크 기술들의 도입을 위해서 기술들을 제안하고 논의를 진행 중에 있다.[5]

† "본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음"
(IITA-2008-(C1090-0801-0025))

나. System Architecture Evolution(SAE)

LTE 표준화와 병행하여 네트워크 구조를 결정하고 이기종 망간의 핸드오버를 지원하기 위한 기술이 SAE라는 이름으로 3GPP TSG-SA WG2를 중심으로 표준화가 진행 중이다.[2]

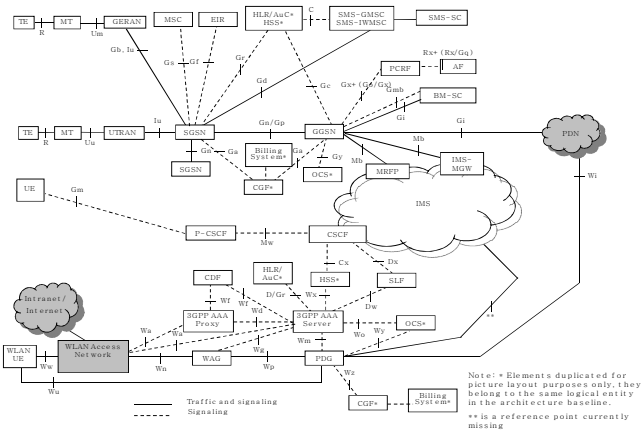
구체적으로 SAE는 3GPP 시스템을 IP를 기반으로 한 다양한 Radio Access Technology를 지원하는 시스템으로 발전시키기 위한 작업을 통칭한다. SAE는 패킷 최적화 시스템, 높은 데이터 전송률, 낮은 지연 시간의 지원을 시스템 목표로 하고 있다. 또한 이 기종 망간의 핸드오버 기술에 대한 표준을 확정하여 연구하고 있다. 현재 새로운 RAN(Radio Access Network) 구조의 모델로 기존 WCDMA 시스템에서의 기지국 기능과 기지국 제어기 기능을 담당하는 eNB (Enhanc -ed Node B)와 WCDMA 시스템에서의 SGSN (Serving GPRS Supp -ort Node) 기능과 GGSN(Gateway GPRS Support Node) 기능을 담당하는 Access Gateway로 구성된 2-Tier 모델이 결정되었다. 이기종 망간의 핸드오버는 Mobile IP를 기반으로 하여 연구 중에 있다.

3. SAE 구조

가. Architecture Baseline

[그림 1]은 진화된 시스템을 위한 상위 수준의 아키텍처이다. 진화된 핵심망은 크게 MME/UPE(Mobility Management Entity, User Plane Entity)와 3GPP 앵커(Anchor), SAE 앵커로 구성된다. 3GPP 앵커와 SAE 앵커를 묶어 IASA(Inter Access System Anchor)라고 한다. MME/UPE는 S1 인터페이스를 이용하여 LTE RAN과 직접 연결되는 기능상의 객체로 LTE 게이트웨이 역할을 하게 된다. 3GPP 앵커는 기존 2G/3G 접근 시스템과 LTE 접근 시스템 사이의 이동성 지원을 위한 앵커 역할을 한다. 또한 SAE 앵커는 3GPP 접근 시스템(2G/3G/LTE)과 Non-3GPP 접근 시스템(WLAN, WiMAX 등) 사이의 이동성 지원을 위해 앵커 역할을 하는 기능상의 객체이다.[4]

기존 2G/3G GPRS 망과 진화된 핵심 망 사이의 연동을 위해 S3 및 S4 인터페이스가 정의되어 있다. 이 인터페이스들은 GTP(GPRS Tunneling Protocol)을 사용하기로 결정되었다. Non-3GPP 접근 시스템과 3GPP 시스템과의 연동 및 이동성 지원을 위해서는 S2 인터페이스가 정의되었다.[5,6]

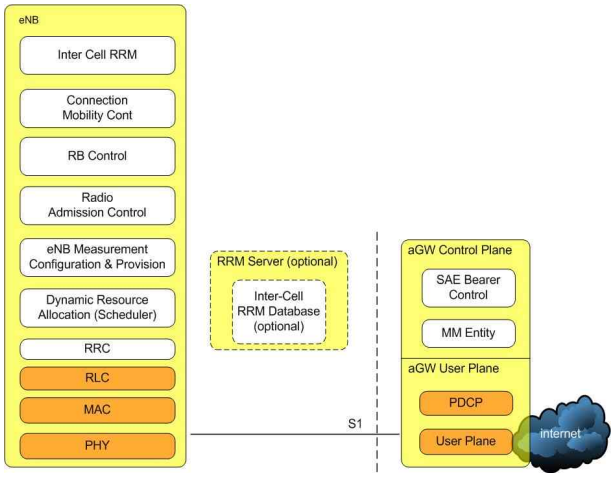


[그림 1] 3GPP를 위한 논리적인 기본 아키텍처

나. E-UTRAN의 Protocol Architecture

E-UTRAN(Evolved Universal Terrestrial Radio Access Net -work)은 UE(User Equipment)에게 E-UTRAN의 사용자 평면(RLC /MAC/ PHY)과 제어 평면(RRC) 프로토콜의 종단점을 제공하는 eNB와 UE의 세션 및 이동성 관리 기능의 종단점을 제공하는 aGW로 구성되며, 이들은 S1 인터페이스를 통해 연결된다.[3] [그림 2]는 E-UTRAN의 전체 프로토콜 아키텍처를 보여준다. E-UTRAN 아키텍처에서 eNB는 aGW 선택, RRC 활성화 시에 aWG로의 라우팅, 페이징 메시지의 전송 및 스케줄링 등의 기능을 수행한다. aGW는 페이징 시작, 사용자 평면 데이터 암호화, NAS(Non Access Stratum) 시그널링의 기밀성과 무결성 보호 등의 기능을 수행한다.

사용자 평면 프로토콜 스택에서 eNB에 위치한 RLC와 MAC 계층은 스케줄링 등의 기능을 수행하며, aGW에 위치한 보안 계층은 암호화를 수행한다.



[그림 2] E-UTRAN 아키텍처

4. SAE Security

가. 이동성 관리 위협

이동성 관리는 다른 접속 네트워크 사이의 UE 핸드오버를 위해 사용되는 구조와 프로토콜을 모두 포함하며, 다음과 같은 위협이 존재한다.

- 프라이버시
- 제어 평면 데이터로의 비 허가된 접근 및 수정
- 네트워크 서비스에 대한 교란과 악용 및 비 허가된 접근

위와 같은 위협을 줄이기 위해서는 인증, 전자서명, 모니터링, 로깅 및 Hash와 같은 다양한 Detection 메커니즘과 종단간에 안전한 암호키를 기반으로 한 트래픽 암호화가 필요하다.

나. 사용자 평면 보안

사용자 평면의 무결성 보호를 위해 다음과 같은 내용에 대해 고려해야 한다.

- IP 패킷의 소형화
- 화상대화 및 스트리밍 서비스
- 분실 패킷에 대한 신뢰성 만족
- 시간과 비용을 고려한 무결성 보호 적용
- 상·하위 계층 사이에서의 보안 메커니즘 중복 문제
- 무결성 보호를 위한 사용자 평면 패킷으로의 MAC 추가

위와 같은 문제점들을 해결하기 위해 무결성 보호를 위해 추가되거나 TCP와 VoIP 트래픽에 발생되는 오버헤드가 고려되어야 하며, 화상대화 및 스트리밍 서비스의 경우 무결성 체크로 인한 품질 저하 현상을 사용자가 인식할 수 없을 정도로 서비스를 제공하여야 한다. 또한 PDCP 패킷은 무결성 체크 실패에 대해 해당 패킷을 버리기 때문에 결과적으로 많은 양의 소형 TCP 패킷이 사용된다. 따라서 작은 패킷들에 대해 무결성 보호는 오버헤드가 발생되며, 처리율 관점에서 무결성 보호를 하는 것과 단독으로 암호화만 하는 것을 결정하여야 한다.

5. SAE Key

가. SAE Key 개요

UMTS(Universal Mobile Telecommunications System) AKA (Authentication Key Agreement)과정을 통하여 한 쌍의 암호키 CK와 무결성키 IK를 공유한다. 그러나 LTE/SAE는 하나 이상의 보안 결합이 있다. UE와 네트워크는 NAS를 지원하기 위하여 UTRAN과 무선 인터페이스 상에서 정보를 전송하기 위한 함수와 프로토콜인 AS (Access Stratum), CN과 UE 사이에서 작동하는 기능적인 계층으로서 트래픽과 시그널링 메시지를 지원하는 NAS 및 사용자 데이터 보호를 위한 키를 생성한다. 이 생성된 키는 네트워크 측면에서 각 대응되는 객체에 전달된다.[4]

네트워크 객체에 대응되는 UP(User Plane), AS, NAS 보안을 위한 키의 생성과 전달에는 다음과 같은 두 가지 방식이 있다.

- UE와 HSS에서 다수의 키 생성 함수가 수행된다. UE와 HSS는 키 생성 함수를 사용한다. HSS는 생성된 키를 인증 벡터로 캡슐화 하여 MME로 키를 전달한다. MME는 보안 작동 수행 과정에서 대응되는 객체에 이 키를 전달하고 받은 객체는 보안을 위하여 각 키를 이용한다.
- UE와 HSS는 마스터키로서 CK와 IK를 생성한다. MME는 HSS로부터 마스터키를 전달 받는다. MME와 UE는 마스터키를 기반으로 키를 생성한다. MME는 보안 작동을 수행할 대응되는 네트워크 객체에 생성한 키를 전달한다.

나. SAE 키 생성과정

SAE의 키 생성 과정은 크게 4 가지 과정으로 구분되며, [표 1]은 각 과정에 대한 설명을 나타내고 있다.

과정	설명
Initial Access	UE와 MME 사이에 초기 접속 과정을 통하여 기본적인 네트워크와 관련된 정보를 교환하는 과정
Authentication Request	네트워크 서비스를 이용받기 위하여 사용자의 인증 정보를 전달하는 인증 요청 과정
Fetch Authentication Data	전달 받은 인증 정보를 이용하여 HLR과 인증을 수행하고 보안을 위해 이용될 키 정보 및 부가의 정보를 전달받는 과정
Authentication Response	인증 요청에 대한 대응으로서 인증이 성공적으로 이루어졌음을 알리고 동시에 네트워크와 UE가 공유해야할 키에 대한 관련 정보를 전달하는 과정

[표 1] SAE 키 생성과정

SAE의 키 생성 과정은 UMTS의 키 생성 과정과 유사하게 진행된다. 하지만 UE를 통해 받은 인증에 필요한 정보 및 요청 메시지를 전달하는 기능 및 실제 통신에 사용될 세션키를 생성하는 기능이 MME를 통하여 이루어진다는 점에서 차이를 가진다. 성공적인 인증 과정 이후에 MME와 UE는 AKA 과정 동안 공유한 CK, IK, RAND에 기반으로 하여 키 생성을 위하여 KDF를 이용한다. 키 생성 함수로서 세 종류의 KDF를 3GPP 표준 문서에서 제안하고 있다.

6. SAE 키 관리

가. Inter-RAT 내에서의 핸드오버 과정에서의 키 분배

핸드오버 과정 중에도 암호화 모드가 유지되는 것이 필요하다. Inter-RAT 핸드오버의 키 변환과 키 전달 과정은 크게 두 가지로 나눌 수 있다.

LTE 이전의 시스템으로 핸드오버는 3G 시스템과 2G 시스템으로 나누어진다. LTE에서 3G의 경우 MME는 일방향 함수를 이용해 CK, IK로 변환 후, 3G SGSN으로 전달한다. LTE에서 2G의 경우 MME는 일방향 함수를 이용해 Ks로 변환 후, 2G SGSN으로 전달한다. LTE 이전 시스템에서 LTE로 핸드오버 하는 경우는 MME가 CK, IK를 받은 후, KDF를 이용하여 SAE_keys를 생성한다.

나. LTE/UMTS 연동을 위한 키 관리

키는 보안과 관련하여 알고리즘과 더불어 핵심적인 요소이다. LTE는 기존의 시스템과의 연동 과정에서 안전한 보안 서비스를 제공하기 위하여 LTE와 UMTS의 연동 과정에서 키 관리가 필요하다.

LTE와 UMTS의 연동 과정에서 키 관리를 위해 LTE의 MME는 합법적인 시스템을 통하여 역방향 키(UMTS에서 이용가능한 키) 생성을 수행하고, SGSN은 LTE에 대해 역방향 키 생성을 수행한다. 또한 MME는 UTRAN에 필요한 키 변환을 위하여 강력한 키 변환 함수를 수행한다.

다. LTE/SAE의 키 식별자

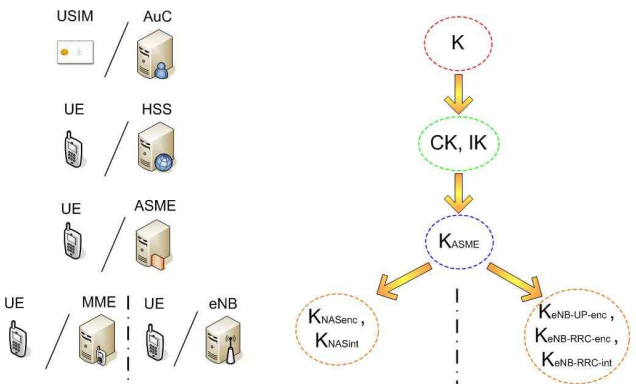
키 식별자는 UMTS 네트워크 내의 AKA 과정의 값들을 식별하여, CK, IK를 별도의 인증 과정 없이 식별을 통해 이전에 사용되었던 값들의 재사용을 위하여 이용한다.

UMTS는 AKA 과정의 실행을 통하여 생성된 결과로서 발생된 인증 정보 및 보안 서비스와 연관된 정보를 사용자와 서빙 네트워크 사이에 보안 컨텍스트로서 생성을 하고 저장을 한다. 여기서 보안 컨텍스트는 적어도 CK, IK, 키 식별자 KSI를 포함하고 있다. KSI의 경우 키를 식별하는 것으로써 UMTS가 단일의 CK, IK를 가지고 있어서 하나의 KSI 값을 사용하였지만, LTE/SAE의 경우에는 KSI_{ASME}, KSI_{NAS}, KSI_{RRC}, KSI_{UP}의 다수의 KSI 값을 가지고 있다. 각각의 다른 키 쌍에 의하여 보호되는 데이터의 양이 다르기 때문에 키 쌍의 갱신되는 과정은 각 키($K_{eNB-UP-enc}$, $K_{eNB-RRC-enc}$, $K_{eNB-RRC-int}$, K_{NAS_enc}, K_{NAS_int})에 대해서 분리된 과정으로 이루어진다.[4]

라. LTE/SAE의 키 계층 구조

LTE/SAE에서는 ASME라는 키 관리를 위한 추가의 객체를 정의하고 있다. ASME는 HSS로부터 접근 네트워크의 최상위의 키를 받는 객체로서, 키 관리를 위하여 SAE 코어 네트워크에서 정의한 객체이다. 보통 ASME의 역할은 MME에 의해 수행된다고 가정한다.[4]

[그림 3]과 같이 SAE/LTE에서는 UMTS의 키 구조에서 사용되었던 K라는 USIM과 AuC가 공유하고 있는 식별자와 AKA 과정을 통하여 생성되는 CK, IK 이외의 추가의 키가 정의된다. CK, IK 및 K의



[그림 3] LTE/SAE 키 계층구조

값들은 네트워크의 객체에 분배하는 대신에 K_{ASME}를 ASME에 전송하여 필요한 키들을 생성한다.

LTE 또는 Non-3GPP SAE 접근 네트워크에서 AKA가 작동할 경우, CK, IK는 HSS이외의 객체에 노출되지 않는다. 또한 UTRAN 네트워크에서 AKA가 작동할 경우, CK, IK는 HSS에서 VLR, SGSN, AAA 서버의 각 객체에 맞게 변환된다. 그리고 한 네트워크에서 AKA로 인해 만들어진 CK, IK는 다른 객체, 네트워크의 키 설립 과정에서 이용될 수 없다. [표 2]는 각 키들에 관한 역할을 나타내고 있다.

키	설명
K	USIM과 AuC 사이에 저장된 항구적으로 사용되는 키
CK, IK	AKA 과정을 통하여 USIM과 AuC에서 생성된 키 쌍
K_{ASME}	AKA 과정 동안 CK, IK로부터 UE와 HSS로부터 발생되는 키
K_{eNB}	K_{ASME}로부터 UE와 MME에 의해 생성된 키로서 RRC와 UP 트래픽을 위한 생성하였다. MME로부터 요청하는 eNB의 식별자에 의존하여 생성된다.
K_{NAS_int}	K_{ASME}부터 UE와 MME에 의해 생성된 키로서 특정 무결성 알고리즘에 대해 NAS 트래픽을 보호하기 위해 사용된다.
K_{NAS_enc}	K_{ASME}부터 UE와 MME에 의해 생성된 키, 특정 암호화 알고리즘에 대해 NAS 트래픽을 보호하기 위해 사용된다.
$K_{eNB\_UP\_enc}$	K_{eNB}로부터 UE와 eNB에 의해 생성된 키로서 특정 암호화 알고리즘에 대해 UP 트래픽을 보호하기 위해 사용된다.
$K_{eNB\_RRC\_int}$	K_{eNB}로부터 UE와 eNB에 의해 생성된 키로서 특정 무결성 알고리즘에 대해 RRC 트래픽을 보호하기 위해 사용된다.
$K_{eNB\_RRC\_enc}$	K_{eNB}로부터 UE와 eNB에 의해 생성된 키로서 특정 암호화 알고리즘에 대해 RRC 트래픽을 보호하기 위해 사용된다.

[표 2] LTE/SAE의 각 키들의 역할

마. 키 구조의 타당성 분석

다른 컨텍스트의 키 설립하는 과정에서 공격자에 의하여 키가 이용될 수 없게 하기 위해서 설립된 키에 컨텍스트 정보를 결합한다.[4] UMTS의 키 구조와 마찬가지로 USIM과 AuC에 저장된 키 K가 최상위의 사용자와 관련된 키로서 안전하게 보관되어 키를 발생시킴으로써 안전한 서비스가 가능하다. UMTS에서 이용되었던 CK, IK는 SAE 네트워크에서 이용할 경우 다음 사항을 준수해야 한다.

- LTE/SAE의 접근 네트워크에서 AKA 작동할 경우, CK, IK는 HSS에서만 이용되고 다른 객체에 전달되지 않는다.
- UTRAN 접근 네트워크의 AKA 작동할 경우, CK, IK는 HSS에서 VLR, SGSN, AAA 서버로 전달된다.
- 한 시스템에서 AKA를 통해 만들어진 CK, IK는 다른 시스템의 키 설립 과정에서 이용 불가해야 한다.

LTE는 다른 트래픽에 대하여 다른 다수의 키를 사용하여 위협을 경감시킨다. 동시에 LTE 키를 특정 암호 알고리즘에만 사용하게 하여 보다 강한 암호학적 특징을 제공하고 이전의 암호 알고리즘 취약점의 위협을 경감시킨다. 또한 RRC와 UP는 eNB에 의존적이어서 핸드오버 과정에서 다른 객체에서 키 정보를 이용하는 것이 불가능하다.

라. 응용 서비스를 위한 객체 정의

LTE 및 SAE 네트워크에서는 네트워크 및 모바일 환경에서 응용계층과 연동을 위한 보안 메커니즘이 존재하지 않은 실정이다. 따라서 응용 계층과 연동을 위한 보안 메커니즘을 제공하기 위해서는 SAE 상에 존재하는 객체들을 인증과 키 분배에 따라서 역할을 정의해야 한다.

4G 환경에서 각 SP(Service Provider)는 기존의 3G 환경과는 다르게 다른 영역에 존재한다. 이러한 환경의 모바일 상에서 서비스를 제공하기 위해서는 SAE 게이트웨이(MME/UPE)가 SP와 사용자 사이에서 상호 인증과 키 생성 및 분배를 주관하는 주체가 되어야 한다.

MME는 HSS와의 통신 채널을 통해 UE와 네트워크의 상호 인증을 수행하며, UE와 MME 사이의 통신 채널을 보호하기 위한 암호화 키와 무결성 키를 생성한다. 이 키들은 HSS와 UE만이 CK, IK를 보유하고 있는 LTE/SAE 네트워크에서 가장 최상위의 세션키라 할 수 있다. 또한 각 eNB와 UE 사이에서 상호 인증을 지원하고 안전한 통신을 위한 키를 생성 할 수 있도록 한다.

또한 MME/UPE는 SAE 게이트웨이의 역할을 한다. SAE 게이트웨이는 IASA와 함께 LTE/SAE 네트워크가 아닌 이기종 네트워크와의 연계를 가능하게 한다. 따라서 MME를 통해 다른 네트워크에 존재하는 SP로 접근이 가능하며, 신뢰할 수 없는 SP로부터 안전하게 서비스를 제공받을 수 있다.

7. 결론

현재 멀티미디어 방송 다중송출 서비스(MBMS)및 OMA-BCAST 등 다양한 모바일 TV 기술이 주목 받고 있으며, 모바일 환경에서 대용량의 영상을 고속으로 주고받을 수 있는 기술들이 연구되고 있다. 이러한 연구들은 Beyond 3G 또는 4G라는 이름으로 진행 중이며, 그 중에서도 3GPP LTE가 유력한 4G 이동 통신 기술 후보로 평가받고 있다.

3GPP LTE는 대용량 HD급 방송콘텐츠를 고속으로 주고받을 수 있으며, 사용자가 무리 없이 시청할 수 있다. 현재 상용화된 3G 이동통신 기술과 비교해 동일 주파수 대역폭에서 6~8배 이상의 속도로 영상을 내려 받을 수 있다. 이뿐만 아니라, 사용자가 언제 어디서나 인터넷 서비스와 동영상서비스, IP기반 전화서비스와 파일의 전송을 자유롭게 할 수 있다.

하지만 4G 환경을 이끌어 나가기 위한 LTE 및 SAE 네트워크에서는 네트워크 및 모바일 환경에서 응용계층과 연동을 위한 보안 메커니즘이 존재하지 않은 실정이다. 3G 환경에서는 네트워크 및 모바일 환경에서 응용계층과 연동을 위한 GBA와 같은 인증 및 키 공유 메커니즘이 존재하고 이것을 통하여 다양한 서비스가 제공되고 있다. 따라서 이러한 모바일 환경에서의 인증 및 키 공유 메커니즘의 연구를 위해서는 LTE 및 SAE 네트워크에서 정의한 각 키의 역할과 키를 생성하고 관리하는 과정에 대한 연구가 필요하다.

본 논문에서는 3GPP LTE 및 SAE 네트워크에서 3G 시스템 보다 진화된 서비스를 제공하기 위한 목적으로 논의되고 있는 일반적인 요구사항과 이를 만족시키기 위한 기술에 대하여 알아보았다. 또한 LTE 표준화와 병행하여 네트워크의 구조를 결정하는 SAE의 구성요소, 프로토콜 구조와 LTE 및 SAE 네트워크에서 보안위협과 안전한 통신을 위한 키 관리 방법에 대하여 논의하였다. 향후과제로 LTE 및 SAE 네트워크에서 제공되고 있는 키를 바탕으로 한 모바일 환경에서 인증 및 키 공유 메커니즘에 관한 연구가 필요하다.

[참고문헌]

[1] 이현우, “3G LTE and SAE”, 한국통신학회지 (정보통신) 제23권 제6호, 29~38쪽

[2] 이현우, 최성호, “3G LTE 및 IMT-Advanced 서비스”, TTA 저널 통권 104호, 2006. 4., pp.107-114.

[3] 3GPP TS 36.300, E-TURAN Overall Description

[4] 3GPP TR 33.821, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE)”

[5] Hammes Ekstrom, “Technical Solutions for the 3G Long-Term Evolution,” IEEE Commun. Mag., March. 2006, pp.30-45.

[6] Erik Dahlman, “The long-term evolution of 3G,” Ericsson Review N0.2, 2005, pp.119-120.