# 모바일 네트워크 보안 기술 동향

정수환
숭실대학교

## 요 약

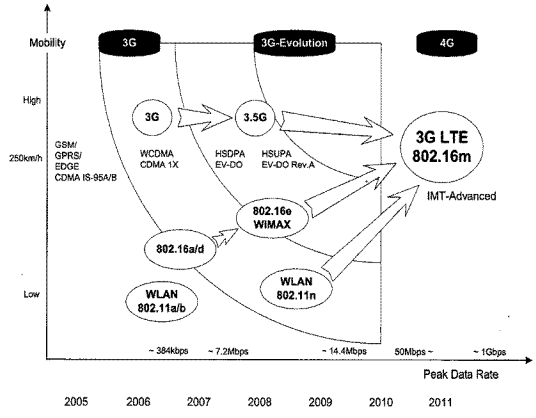
본고에서는 최근 빠르게 발전하고 있는 모바일 네트워크 보안 기술 동향에 대해서 살펴본다. 특히 모바일 네트워크의 발전으로 최근 관심이 집중되고 있는 이기종 망간 인증 연동에 대해 3GPP 진영과 IEEE 진영에서의 표준화 기술 동향을 살펴본다.

ITU-R에서는 차세대 모바일 네트워크 (4G)인 IMT-Advanced에 대한 표준화일정 및 표준 요구사항 등을 정의하여 2008년부터 본격적인 표준화 논의를 시작하였다. 이에 따라 3GPP와 IEEE에서는 ITU-R의 IMT-Advanced의 표준 요구사항을 충족하는 표준 기술로 LTE-Advanced와 802.16m에 대한 기술 논의를 ITU-R의 표준화 일정에 따라 진행하고 있으며 표준화 및 전 세계 시장 선점을 위해 치열한 경쟁을 하고 있다. 이러한 모바일 네트워크 환경의 고도화로 관심이 증가하고 있는 이기종 망간 인증연동 기술에 대한 표준화 동향을 살펴본다.

## I. 서 론

최근 몇 년간 국내외적으로 모바일 네트워크 기술은 급성장을 하고 있다. 모바일 네트워크 기술은 1세대 AMPS (Advanced Mobile Phone Service), 2세대 GSM (Global System for Mobile Communications)을 거쳐 패킷 전달에 보다 적합하도록 개발된 CDMA (Code Division Multiple Access) 기술 기반의 HSPA (High Speed Packet Access)와 1xEV-DO Rev.A (1x Evolution-Data Optimized Revision A)의 3세대와 3.5 세대인 W-CDMA (Wideband-CDMA)를 거치면서 빠르게 발전해왔다. 특히 2004년부터 IEEE (Institute of Electrical and Electronics Engineers) 중심으로 모바일 네트워크 환경에서 데이터 전송속도를 높이기 위한 표준 기술 연구가 시작되었고, 이를 통해 기존 CDMA 기술 기반이 아닌 OFDM (Orthogonal Frequency- Division Multiplexing)과 MIMO (Multiple Input, Multiple Output) 기술이 결합된 새로운 기술 적용을 위한 시도가 빠르게 확산되었다. 이러한 연구 개발 노력의 결과로 IEEE는 WiBro/WiMAX (Wireless Broadband / Worldwide Interoperability for Microwave Access)라고 불리는 802.16e 기술 표준을 완성하였다. IEEE의 WiBro/WiMAX 표준 기술의 완성은 유럽을 중심으로 연구가 진행되고 있었던 3GPP와 3GPP2에서 새로운 기술 개발을 위한 논의를 더욱 활발하게 하는 촉매가 되었으며, 이러한 결과로 LTE (Long Term Evolution)가 등장하게 되었다. 현재는 IEEE와 3GPP가 4세대 모바일 네트워크 환경인 IMT-Advanced[1] 표준화 기술 선점 및 전 세계 시장 선점을 위해 치열한 경쟁을 하고 있다. 다음 (그림 1)은 모바일 네트워크 기술의 발전 과정을 보여준다.

IMT-Advanced는 3GPP의 LTE와 IEEE의 Mobile WiMAX 기술 표준이 마무리되어 가던 2007년 말경부터 새로운 모바일 네트워크 환경 표준 기술에 대한 요구와 논의가 ITU-R (International Telecommunication Union - Radiocommunication)을 중심으로 본격화되면서 차세대 모바일 네트워크의 표준으로 등장하였다. 이러한 ITU-R의 표준화 움직임에




(그림 1) 모바일 네트워크 기술 변화 과정

따라 3GPP와 IEEE에서는 기존 LTE를 발전시킨 LTE-Advanced[2]에 대한 표준화 논의를 시작하였고, IEEE에서도 802.16m[3]에 대한 표준화 논의를 시작하였다. 3GPP와 IEEE는 2009년 10월 ITU-R 표준화 회의에서 최종 제안 제출을 완료하였고, 이를 기반으로 ITU-R에서 평가 및 합의과정을 거쳐 2011년 2월에 IMT-Advanced에 대한 표준 기술을 제정할 예정에 있다.

위에서 설명한 것과 같이 빠르게 발전하고 있는 모바일 네트워크 환경에서 이기종 망간 이동성 지원 및 인증연동에 대한 기술적 필요성과 보안 요구사항에 대한 관심이 증가하고 있다. 이에 따라 3GPP 진영과 IEEE 진영에서는 차세대 모바일 네트워크에 대한 표준화와 더불어 이기종 망간 인증연동 기술 표준화를 위한 연구를 지속적으로 수행하고 있다.

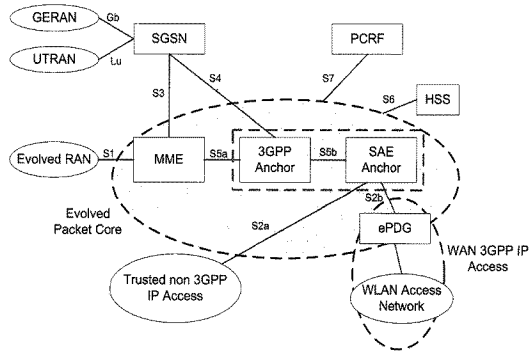
본고에서는 최근 표준화 이슈가 되고 있는 이기종 망간 인증연동 기술과 관련된 보안 기술 동향을 살펴본다.

## II. 3GPP에서의 이기종 망간 인증연동 보안 기술 동향

이번 절에서는 3GPP, WLAN, WiBro/WiMAX 등의 이기종 모바일 네트워크 환경이 혼재된 환경에서 사용자의 이동성 지원을 위해 3GPP 표준화 그룹에서 진행중인 이기종 망간 인증연동 기술 표준화 동향을 기술한다.

### 1. LTE 구조

3GPP에서는 기존에 개발된 표준기술들에 대한 성능을 최적화하고, 이기종 모바일 네트워크 간의 이동성 지원을 위한 LTE 표준화를 2004년부터 진행하였다. 현재는 차세대 모바일 네트워크인 LTE-Advanced에 대한 표준화를 진행하고 있다. 3GPP에서 표준화 진행중인 LTE에는 이기종망간 이동성지원 및 인증연동을 위해 SAE (System Architecture Evolution)[4]를 정의하고 있다. SAE는 LTE 액세스 시스템에서 높은 전송율과 낮은 레이턴시를 제공하기위해 새롭게 정의된 LTE 코어 네트워크 구조로서 All IP 네트워크를 지원한다. 특히 SAE는 2G/3G 모바일 네트워크와 WLAN, WiBro/WiMAX와 같은 이질적인 모바일 네트워크와의 이동성 및 인증연동을 지원하기 위한 표준으로 개발되고 있다. 다음 (그림 2)는 LTE에서의 SAE 논리적 구조를 보여준다.

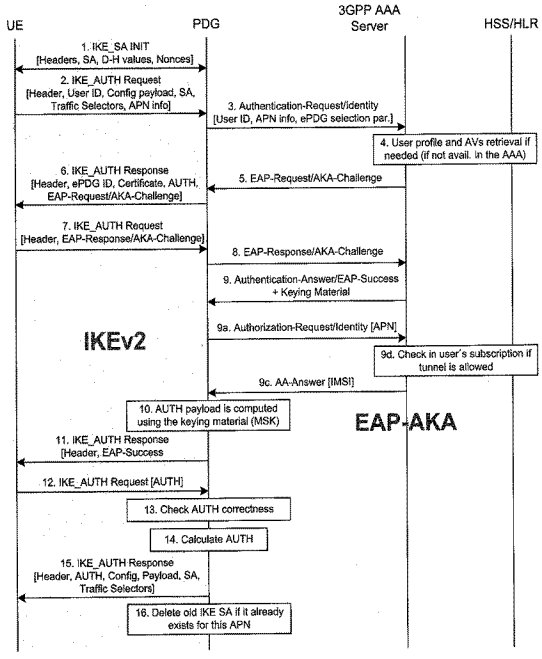



(그림 2) LTE에서의 SAE 논리적 구조

LTE는 기존 3GPP 시스템 구조와는 다르게 액세스 네트워크와 코어 네트워크 간의 Control Plane과 User Plane을 구분하여 처리하는데 MME (Mobility Management Entity)에서 Control Plane을 담당한다. 그리고 SAE 구조에서 3GPP Anchor는 2G/3G와 LTE 간의 이동성을 지원하고, SAE Anchor은 3GPP와 non-3GPP (WLAN, WiBro/WiMAX) 간의 이동성을 지원한다. ePDG (Evolved Packet Data Gateway)는 non-3GPP 모바일 네트워크에서 3GPP 서비스를 제공받을 수 있도록 지원하는 장치로 3GPP AAA 서버로부터 수신된 정보를 기반으로 네트워크 접속 권한을 non-3GPP 모바일 네트워크에 접속한 사용자 단말에 부여한다.

## 2. SAE시스템의 보안 구조

LTE의 SAE 시스템 구조에서는 기본적으로 인증연동 기술로 EAP-AKA[5]를 고려하고 있다. LTE 기반 모바일 네트워크 환경에서 AKA 인증을 수행할 수 있도록 지원하기 위해 모든 사용자 단말은 USIM 카드를 기본적으로 장착하는 것을 가정하고 있다. (그림 3)은 SAE 구조에서 non-3GPP 망을 통해 3GPP 망에 접속하는 UE에 대한 인증연동 과정을 보여준다.




(그림 3) SAE 구조에서 EAP-AKA 기반 인증 연동

위의 그림에서처럼 SAE 구조에서 non-3GPP 망에서 3GPP 망으로 접속하는 UE에 대한 네트워크 접속 인증은 EAP-AKA를 기반으로 이루어진다. UE와 PDG 간에는 기존 non-3GPP 망에서 사용되는 인증 기법을 통해 인증 메시지가 전달되고, PDG에서 3GPP-AAA 서버로 전달되는 인증 관련 메시지는 EAP-AKA를 통해 전달된다. 다음은 (그림 3)에서 보여주고 있는 WLAN에서 3GPP 망에 접속하는 UE에 대한 구간별 인증과정을 간략하게 요약하였다.

- UE와 PDG간 : UE와 PDG 간에 주고받는 메시지는 IPsec을 통해 보호된다. IPsec의 SA (Security Association) 설정은 IKEv2[6]를 이용하여 1번 과정을 통해 이루어지고, SA 과정이 성공적으로 수행된 다음 IKEv2 메시지에 사용자 인증을 위한 정보가 포함되어 PDG에게 전달된다. 이후 PDG는 3GPP-AAA 서버와의 EAP-AKA를 통해 사용자 인증을 위한 정보를 전달받고, IKEv2 기반의 EAP-AKA 인증과정을 수행한다.
- PDG와 3GPP-AAA 서버간 : PDG와 3GPP-AAA 서버간에는 EAP-AKA를 통해 UE 인증을 위한 정보들이 전달된다. UE가 IKEv2에 자신의 식별정보를 담아 전달하면 PDG는 수신한 식별정보를 3GPP-AAA 서버로 전달한다. 전달된 정보를 기반으로 3GPP-AAA 서버는 HSS/HLR로부터 AKA 인증 수행을 위한 UE의 AV 정보 등을 전달 받아 EAP-AKA 기반의 인증과정을 수행한다. PDG에서 3GPP-AAA 서버가 전달하는 EAP-AKA 메시지는 다시 IKEv2 메시지에 포함되어 UE에게로 전달되고, UE는 IKEv2 메시지에 포함된 EAP-AKA를 통해 인증과정을 수행한다.

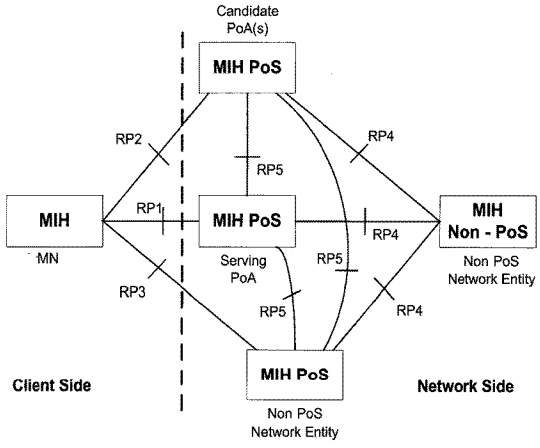
위에서 설명한 바와 같이 LTE의 SAE에서는 3GPP 망에서는 AKA 인증을 직접 수행하고, non-3GPP 망에서 PDG를 통해 기존 모바일 망에서 사용하는 인증 기술과 EAP-AKA를 통해 인증과정을 수행한다. SAE에서 정의하고 있는 PDG는 3GPP-AAA 서버의 Authenticator 역할을 수행하며, 3GPP 망과 non-3GPP 망간의 패킷 데이터 서비스 및 인증 연동을 위해 중요한 역할을 담당하고 있다. 현재 3GPP에서는 LTE의 SAE 시스템 기반의 다양한 이기종 망간 연동 및 인증 연동 시나리오를 정의하여 필요한 보안 기술 표준화를 진행하고 있다.

# III. IEEE에서의 이기종 망간 인증연동 보안 기술 동향

이번 장에서는 IEEE 표준화 그룹에서 진행중인 MIH[7] 기반의 인증연동 표준화 기술 동향에 대해서 기술한다.

## 1. MIH 통신모델

IEEE 802.21 WG은 2004년 초에 이기종 네트워크간 끊임없는 이동성 지원 기술 개발을 위한 MIH (Media Inde-



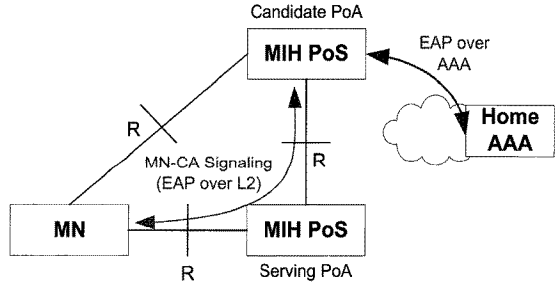

(그림 4) MIH 통신 참조모델

pendent Handover) 표준화를 시작하였다. 최근 차세대 모바일 네트워크 표준화에 대한 관심이 집중되면서 이기종 모바일 네트워크 환경에서의 인증연동에 대한 관심이 다시 고조되고 있다. 이에 IEEE에서는 이기종 망간 인증연동 기술 표준화에 MIH를 적용하기위한 논의를 계속 진행하고 있으며, 현재 표준화 논의 중인 MIH의 통신 참조모델은 위의 (그림 4)와 같다.

MIH 표준의 통신 참조모델은 크게 클라이언트 측과 네트워크 측으로 구분된다. 클라이언트 측에는 MIHF (MIH Function)가 탑재된 MIH 단말이 존재하고, 네트워크 측에는 MIH PoS (MIH Point of Service)와 MIH Non-PoS가 존재한다. MIH PoS는 MIH 단말과 MIH 프로토콜을 주고 받아 이기종 망간 이동성 서비스를 제공한다. 그리고 MIH Non-PoS는 MIH 단말에게 이동성을 직접 제공할 수 없기 때문에 MIH PoS와 연계하여 끊임 없는 이동성 서비스를 제공한다. MIH 기반 통신환경에서는 WLAN, WiBro/WiMAX, 3GPP 간에 인증연동을 제공하기 위해 하나의 AAA 도메인 환경에서의 핸드오버 시나리오와 다른 AAA 도메인간의 핸드오버 환경에서의 인증연동 시나리오를 기본적으로 정의하고 있고, EAP 기반의 Pre-Authentication 인증 모델[8]을 적용하기 위한 논의가 진행되고 있다.

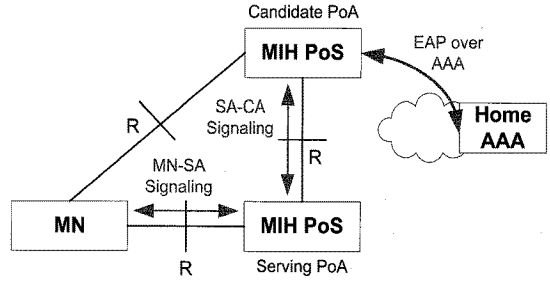
## 2. MIH 인증모델

IEEE 802.21 MIH 표준화 그룹에서는 인증연동 표준화 기술 개발을 위해 EAP 기반의 Pre-Authentication과 계층적 키 구조를 적용하기 위한 논의를 진행하고 있다. (그림 5)는 MIH에서 논의 중인 EAP 기반의 Pre-Authentication 모델 중 Direct Pre-Authentication 모델을 보여준다.




(그림 5) Direct Pre-Authentication 모델

위의 모델은 MN이 이질적인 모바일 네트워크 환경으로 핸드오버 할 때 Candidate PoS와 EAP 기반의 MN-CA (Mobile Node - Candidate Authenticator) 시그널링을 통해 직접적으로 인증관련 메시지를 전달한다. 다음 (그림 6)은 MIH의 Indirect Pre-Authentication 모델을 보여준다.




(그림 6) Indirect Pre-Authentication 모델

위의 모델 방식은 MN이 핸드오버 할 때 Candidate PoS와 주고받는 EAP 메시지가 먼저 MN-SA (Mobile Node-Serving Authenticator) 시그널링을 통해 Serving PoS로 전달되고 이후 SA-CA 간의 시그널링을 통해 EAP 메시지가 Candidate PoS로 전달된다.

IEEE에서는 앞서 설명한 것처럼 두 가지 EAP 기반의 Pre-Authentication 모델을 통해 이기종 망간 인증연동 기술 표

준화를 진행하고 있으며, 인증연동 과정에서 필요한 키 분배를 효과적으로 수행하기 위해 EAP 기반의 계층적 키 구조인 EMSK[9]를 고려하고 있다. 현재 IEEE MIH 그룹에서 논의중인 계층적 키 구조는 EAP 인증 서버 또는 지역 인증서버에서 EMSK (Extended Master Session Key)와 DSRK (Domain Specific Root Key)를 생성하고, 생성된 키를 기반으로 Re-Authentication Rook Key인 rRKs를 생성하도록 정의하고 있다. 그리고 생성된 rRKs에서 rIK (Re-Authentication Integrity Key)와 rMSK를 생성하여 이질적인 모바일 네트워크 간의 인증연동에 적용하기 위한 논의가 진행중에 있다.

MIH 표준화그룹에서는 EAP 기반의 계층적 키 구조를 적용하기 위해 MSK-KH (Media Specific Authenticator and Key Holder)와 MIA-KH (Media Independent Authenticator and Key Holder)라는 네트워크 구성요소를 추가하여 구체적인 핸드오버 인증연동 과정을 설계하고 있다. 현재 설계 중인 EAP 기반 계층적 키 구조가 적용된 핸드오버 인증 과정은 MIH Function이 탑재된 MN이 핸드오버 할 경우 핸드오버 전에 CN (Candidate Network)의 MIA-KH와 MIH 프로토콜을 통해 EAP Pre-Authentication을 수행하도록 정의하고 있다. 이때 상호 인증 및 키 공유과정이 수행되고, CN의 MIA-KH에서 생성된 계층적 키가 CN의 MSA-KH로 분배된다. 이후 새로운 모바일 네트워크로 이동하게 되면 CN의 MSA-KH와 공유된 계층적 키를 통해 상호 인증과정 및 무선구간 보호를 위한 공유키 교환 과정이 수행된다. 위와 같은 과정에 대해서 IEEE MIH 그룹에서 논의 중에 있으나 아직까지는 구체적인 동작 과정이 정의되지 않고 있다.

## IV. 결 론

본 고에서는 3GPP와 IEEE 중심으로 표준화 진행중인 차세대 모바일 네트워크 환경에서 최근 관심이 집중되고 있는 인증연동을 위한 보안 기술 동향에 대해서 살펴보았다.

인증연동 보안 기술은 빠르게 표준화 및 상용화 되고 있는 차세대 모바일 네트워크 환경에서 이질적인 모바일 네트워크를 자유롭게 이동하는 사용자에게 끊임없는 서비스를 지원하기 위해 꼭 필요한 보안 기술이다. 때문에 3GPP 표준화 그룹에서는 기존 LTE 구조에서 SAE 시스템 구조를 통해 이기종 망간 인증연동을 제공하기위한 표준화를 진행하고 있고, IEEE에서는 802.21 MIH 표준화 그룹을 통해 인증연동을 위한 표준화를 진행하고 있다. 3GPP 진영에서는 이기종 망간 인증 연동을 위해 모든 단말에서 EAP-AKA가 적용될 수 있도록 USIM 탑재를 의무화하고 있다. IEEE 802.21 MIH 표준화 그룹의 보안 파트에서는 MIH 환경에 EAP 기반의 계층적 키구조를 적용한 인증연동 보안 기술 개발을 위한 논의를 진행하고 있다. 그러나 아직까지는 분명한 인증연동 기술이 제안되지 않고 있다.

향후 고도화된 모바일 네트워크 환경을 이용하는 스마트폰, 클라우드 컴퓨팅, 스마트 그리드와 같은 융합 서비스 환경에서도 인증연동은 매우 중요한 보안 이슈가 될 것으로 예상됨에 따라 인증연동과 관련된 원천기술 확보가 필요해 보인다.

## 참 고 문 헌


[1] ITU-R, Revision 1 to Document IMT-ADV/2-E, "Submission and evaluation process and consensus building," 2009.

[2] 3GPP, RP-080997, "Proposed schedule for the submission of LTE-Advanced to ITU-R as a candidate for IMT-Advanced," AT&T et. Al, 2008.

[3] ITU-R IMT-ADV/4 (IEEE L802.16-09/010Xr5), "Submission of a candidate IMT-Advanced RIT based on IEEE 802.16 (Part 4 of 4)," 2009.

[4] 3GPP, TR 23.882 V8.0.0, "3GPP System Architecture Evolution: Report on Technical Options and Conclusions," 2008.

[5] RFC 4187, "Extensible Authentication and Key Agreement (EAP-AKA)," 2006.

[6] RFC 4945, "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX," 2007.

[7] IEEE Std 802.21-2008, "IEEE Standard for Local and

metropolitan area networks- Part 21: Media Independent Handover Services," 2009.

[8] IEEE 802.21a, "Proactive Authentication and MIH Security," 2009.

[9] RFC 5295, "Specification for the Drivation of Root Keys from an Extended Master Session Key (EMSK)," 2008.

약 력

정 수 환

1985년 서울대학교 전자공학과 학사
1987년 서울대학교 전자공학과 석사
1988년 ~ 1991년 한국통신 전임 연구원
1996년 University of Washington 박사
1996년 ~ 1997년 Stellar One S/W Engineer
1997년 ~ 현재 숭실대학교 정보통신전자공학부 부교수
2009년 ~ 현재 지식경제부 지식정보보안 PD
관심분야 : 이동 네트워크 보안, VoIP 보안, 차량 네트워크 보안, RFID/USN 보안정수환