UMTS-WLAN간 핸드오버를 위한 USIM 기반의 인증 테스트베드에 관한 연구

A Study on USIM-based Authentication Testbed for UMTS-WLAN Handover

노광현*, 권혜연**

Kwang-Hyun Ro*, Hye-Yeon Kwon**

요 약

3GPP에서는 넓은 서비스 영역과 높은 이동성의 장점을 가지는 3G 이동통신과 높은 데이터 전송률의 장점을 가지는 WLAN간 인터워킹 시스템에 대한 표준화 및 기술 개발이 진행되고 있다. 3GPP와 WLAN 이종망간의 서비스 연속성을 지원하기 위해서는 seamless handover를 지원해야하며 이를 위해서는 핸드오버시 발생하는 지연을 최소화해야 한다. 본 논문에서는 핸드오버 과정에서 발생하는 지연 시간의 많은 부분을 차지하는 인증 메커니즘을 실제 USIM 기반의 인증 테스트베드에 구현하여 분석하였다. EAP-AKA 완전 인증 방법과 빠른 재인증 방법에 대해 단말과 AAA 서버에서 발생하는 지연 시간을 구체적으로 분석하였고, 실험 결과 빠른 재인증 방법이 인증에 소요되는 시간을 48.6% 단축시킬 수 있는 것으로 측정되었다.

Abstract

In view of mutual complementary feature of wide coverage and high data rate, the interworking between 3G cellular network and WLAN is a global trend of wireless communications. This paper introduces the analytic result of an authentication mechanism for 3GPP-WLAN seamless mobility under the USIM-based authentication test-bed. In a handover process between heterogeneous networks, authentication is the main factor of handover delay. So authentication processing time should be firstly reduced. This paper describes an USIM-based EAP-AKA test-bed implemented for handover in UMTS and WLAN interworking systems. Experimental result has shown that the fast re-authentication mechanism during handover has reduced the handover delay by about 48.6%.

Keywords : UMTS-WLAN interwokring, seamless handover, UMTS-WLAN authentication, EAP-AKA, Full authentication, Fast re-authentication

I. 서 론

최근 이동통신분야에서는 넓은 서비스 영역과 높은 이동성의 장점을 가지는 3G 이동통신과 높은 데이터 전송률의 장점을 가지는 WLAN간의 연동을 통한 상호 장점을 활용하기 위한 기술 연구 및 표준화 작업이 진행 중이다. 특히, WCDMA 방식의 이동통신시스템의 진화 버전인 3GE (3G Evolution) 시스템에서도 WLAN과의 연동을 좀더 강화하는 방향으로 표준화 규격을 완성해 가고 있다.

3G 이동통신망과 WLAN이 중첩된 네트워크 구조에서 3G와 WLAN간 끊김없는 이동성(seamless mobility)을 지원하기 위해서 해결해야할 여러 가지 문제 중 사용자의 서비스 측면에서 가장 중요한 것은 버티컬 핸드오버(vertical handover)시 발생하는 지연을 최소화하는 것이다. 일반적으로 이종망간 핸드오버시 발생하는 지연은 주로 인증(authentication) 절차에서 발생한다. 따라서, 3G와 WLAN간 핸드오버시 인증 처리 시간을 줄이기 위한 방안으로 빠른 재인증(fast re-authentication) 메커니즘이 제안된 바 있다[1,2].

본 논문에서는 3GE 시스템에 대한 표준 규격 및 시스템 개발 연구의 일환으로 진행된 내용 중 3GE와 WLAN의 인터워킹 시스템의 서브시스템으로 개발된 USIM 기반의 EAP-AKA 인증 테스트베드를 설명하고, 이 테스트베드에 EAP-AKA 완전 인증(full authentication) 절차와 빠른 재인증 절차를 모두 구현하여 버티컬 핸드오버시 발생하는

* 한성대학교 산업시스템공학과 ** ETRI 이동통신연구본부
접 수 일 자 : 2008. 2. 21 수 정 완 료 : 2008. 7. 23
게재확정일자 : 2009. 1. 28
※ 본 연구는 2007년도 한성대학교 교내연구비 지원 과제임.

지연 시간을 비교, 분석한 결과를 설명한다. 3GE와 WLAN 간의 인터워킹 시스템의 기능 중 인증 관련 부분은 기존의 UMTS와 WLAN간의 사용자 인증 및 권한 검증 절차를 기본적으로 승계하는 것으로 가정하여, 3GPP Release 6 기반으로 본 연구를 수행하였다.

논문은 다음과 같이 구성된다. Ⅱ장에서는 Mobile IPv6 기반의 UMTS-WLAN 연동망 구조와 USIM에 대해 소개하고, Ⅲ장에서는 UMTS와 WLAN의 인증 메커니즘에 대해 설명한다. Ⅳ장에서는 USIM 기반의 EAP-AKA 테스트베드를 구체적으로 설명하고, Ⅴ장에서는 테스트베드에 완전 인증 절차와 빠른 재인증 절차를 적용한 결과를 분석한다. 마지막으로 Ⅵ장에서는 결론 및 향후 연구 방향을 제시한다.

Ⅱ. UMTS-WLAN 연동망 구조 및 USIM

2.1 UMTS-WLAN 연동망 구조

3GPP 진영에서는 기존의 3G망과 WLAN간의 연동을 위한 기술 표준화를 작업해 왔으며, loosely coupled 기반의 망구조를 정의하였다. 이러한 3GPP의 활동은 3G망에서 제공되는 서비스와 기능을 WLAN 환경으로 확장하기 위한 것이 목적이다. 따라서, 3G망과 WLAN간의 연동에서는 기본적으로 WLAN 접속망이 3G망의 확장이라는 가정하에서 고려되어야 한다.

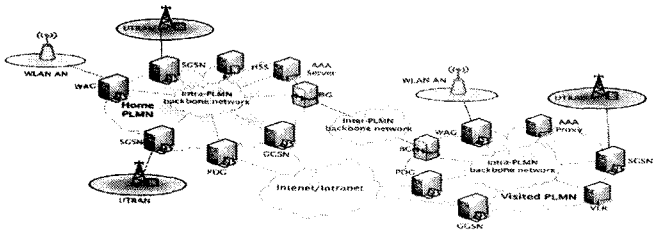

그림 1. UMTS-WLAN 연동망 구조

Fig. 1. UMTS-WLAN interworking network architecture

그림 1은 3GPP 표준화 문서에서 정의하고 있는 3GPP와 WLAN 연동망이다[3]. 이 시스템에서 WLAN AN은 WLAN AP를 하나 이상 포함하는 WLAN 접속망이며, 3GPP AAA Proxy는 방문망(visited network)에서 프락시와 필터링 기능을 수행한다. AAA 서버는 가입자의 홈망(home network)에 위치한 HSS (Home Subscriber Server)에서 인증 관련 정보와 가입자 프로파일을 받아온다. HSS는 AuC(Authentication Canter)와 HLR (Home Location Register) 기능을 수행하고, WAG(WLAN Access Gateway)는 WLAN AN과 UE간에 전달되는 데이터의 게이트웨어 역할을 수행한다. 3GPP PS 기반 서비스는 사용자 홈망이나 방문망에 있는 PDG(Packet Data Gateway)를 경유하여 제공된다.

UMTS에서 SGSN(Serving GPRS Support Node)은 packet core network에 접속하기 위한 게이트웨이 역할을 하고, GGSN (Gateway GPRS Support Node)은 PS 기반 서비스나 외부 IP망에 접속하기 위한 게이트웨이 역할을 하며, PDG도 GGSN과 동일한 기능을 수행한다. 또한, 인증을 위한 Auc와 HLR/VLR이 있다.

WLAN UE(User Equipment)는 USIM(User Subscriber Identity Module)을 포함하며, UMTS와 WLAN과의 통신을 위한 제어 및 데이터 프로토콜을 내장한 듀얼 모드 단말이다.

2.2 USIM

일반적으로 3G 가입자 관리와 사용자 인증/서비스 권한을 위한 사용자 프로파일, 인증 파라메터, 알고리즘 등은 SIM(Subscriber Identity Module, 2.5세대 이전)과 USIM (Universal Subscriber Identity Module, 3세대 이후)이라는 칩카드에 담겨져 MT(Mobile Terminal)에 탑재된다. 향후에는 USIM과 금융권 EMV(Europay Master Visa)카드를 하나로 결합하는 범용 표준 원칩카드인 UICC(Universal IC Card)가 표준화되어 기본 모듈로 탑재될 것이다.

이러한 SIM 또는 USIM에서 기본적으로 관리하는 기능과 데이터를 요약하면 표 1과 같다[4].

표 1. SIM/USIM 데이터 요약

Table. 1. Data summary of SIM/USIM

파일 분류	파일 내용
환경변수 파일	카드 ID 및 발급자 정보, 사용언어, 고유 ID, 암호화 관련키, 위치정보, 접속제어 클래스, 사용이 금지된 PLMN, 데이터 서비스 변수값 셀 방송용 변수값
서비스 파일	긴급용 전화번호, 전화번호(AND, FDN, SDN), 단문메시지 변수값, 기능 및 환경변수값, 서비스망 정보, 애플리케이션 구분자, 애플리케이션 디렉토리, 서비스 테이블
보안인증 관련 파일	가입자 인증키, PIN / Unblock Pin, PIN 활성화 상태 표시자, PIN 오류 카운터 데이터 Integrity 키
기타	착발신 호 정보, 통화시간 및 요금정보

Ⅲ. UMTS와 WLAN에서의 인증 메커니즘

3.1 USIM을 이용한 AKA 인증

AKA(Authentication and Key Agreement)는 2G에서 사용하였던 단향 인증방법을 보완한 상호인증방법으로서 3G 이동통신망의 표준 인증방법으로 하나의 UE에서 서로 다른 망인 3G망과 WLAN망의 연동을 위해 유선 혹은 무선상에서 다양하고 안전한 사용자 인증을 제공하는 EAP (Extensible Authentication Protocol) 인증 프로토콜과 연동하여야 한다[5,6,7].

3G망의 보안정책을 그대로 유지한 상태로 WLAN에서 3G의 인증방법인 AKA를 그대로 적용하여 EAP-AKA를 WLAN UE와 인증서버(AAA)간에 적용한다.

3G 환경에서 UE가 USIM을 통해서 AKA 인증처리를 수행하는 기본적인 개념은 그림 2와 같다.

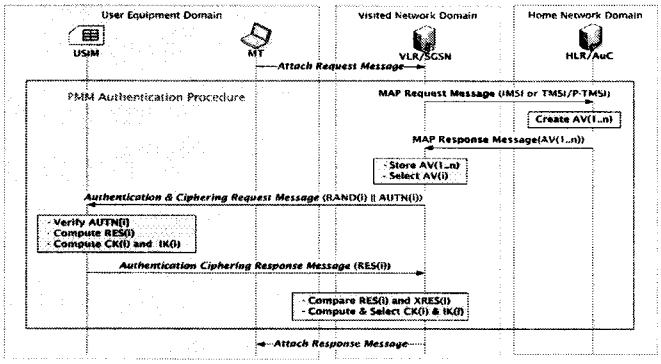

그림 2. UMTS-AKA 인증 절차
Fig. 2. UMTS-AKA authentication procedure

사용자와 3G망은 사용자의 HE내 USIM과 AuC 사이의 공유 비밀키를 통하여 상호 인증을 수행한다. USIM과 HE는 네트워크 인증을 지원하기 위하여 각각 카운터 SQNMS, SQNHE를 가지고 있다. SQNHE는 각각의 사용자에게 제공되는 연속 번호이고, SQNMS는 USIM이 인정하는 최상위 연속 번호이다. 이 방법은 현재 GSM 보안 구조와의 최대 호환성과 GSM에서 UMTS로의 이전을 용이하게 하는 방식으로 Challenge/response 프로토콜과 ISO/IEC 9798-4의 네트워크 인증을 위한 연속 번호 기반 단일 패스(sequence number-based one-pass)프로토콜이 결합된 키 정립 프로토콜로 구성된다.

HE/AuC가 VLR/SGSN으로부터 요청을 받으면, HE/AuC는 n 인증벡터를 VLR/SGSN로 보낸다. 인증 벡터는 연속 번호로 임의 수 RAND, 예상 응답 XRES, 비밀키 CK, 무결성 키 IK, 인증 토큰 AUTN으로 구성된다. 각 인증 벡터는 VLR/SGSN과 USIM 사이의 단일 인증 및 키 일치 수행에 적합하다. VLR/SGSN이 인증 및 키 일치 초기화할 때 배열된 어레이에서 다음 인증 벡터를 선택하고, RAND와 AUTN 값을 사용자에게 전달한다. 인증 벡터는 선입선출 방식이다. USIM은 AUTN 인정 여부를 확인하고 인정되는 경우, RES값을 VLR/SGSN로 보내며 CK, IK를 계산한다. VLR/SGSN은 전달 받은 RES을 XRES과 비교하고 일치하는 경우, VLR/SGSN는 인증과키 일치가 성공적으로 수행되었다고 판단하는 근거가 되며 이에 따라서 인증 프로세스가 완료된다.

3.2 EAP-AKA 메커니즘

3G와 WLAN의 인터워킹 시스템에서 WLAN UE와 인증서버간에 EAP-AKA 인증 메커니즘을 적용한다. 버티컬 핸드오버시 발생하는 인증 시간을 줄이기 위하여 제안된 빠른 재인증 절차와 기존의 완전 인증 절차를 그림 3에 간략히 나타내었다. 완전 재인증 메커니즘은 초기 인증 절차에서 USIM 카드와 망에서 새로운 키를 생성하는 반면 빠른 재인증 메커니즘은 이전 인증 과정에서 생성된 키를 재사용한다. 따라서, 빠른 재인증 메커니즘은 WLAN UE와 AAA 서버간 인증 시간을 줄임과 동시에 UE의 파워 소모도 줄일수 있는 장점이 있다. 이러한 빠른 재인증 메커니즘의 사용 여부는 통신망 사업자의 정책에 따라 달라질 수 있다.

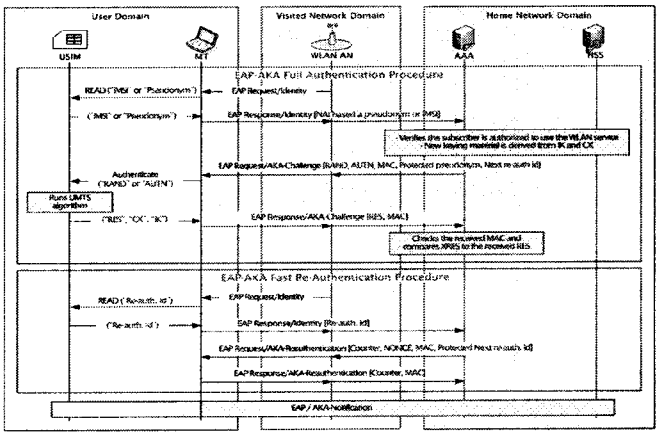

그림 3. EAP-AKA 인증 절차
Fig. 3. EAP-AKA authentication procedure

Ⅳ. USIM 기반의 인증 테스트베드

4.1 인증 테스트베드 구성

UMTS와 WLAN간의 핸드오버시 USIM 기반으로 인증 작업을 수행하기 위한 테스트베드를 그림 4와 같이 구성하였다. 사용자에 해당하는 UE(User Equipment)는 노트북에 802.1x 무선랜 장치를 탑재하고, USIM 카드 에뮬레이션 기능을 위한 CF 혹은 SD 메모리를 부착하여 클라이언트 시스템으로 동작을 하도록 하였다. UE는 AP(Access Point)를 통해서 RADIUS(Remote Authentication Dial In User Service) 시스템과 EAP-AKA 기반의 사용자 인증을 통한 네트워크 접근을 태스트하게 된다.

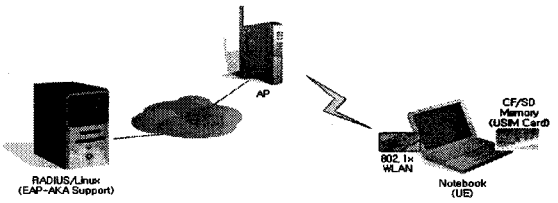

그림 4. 인증 테스트베드 구성
Fig. Authentication testbed configuration

실제 구현된 모습은 그림 5와 같다. 왼쪽 컴퓨터는 RADISU 서버 기능을 수행하고, 오른쪽 노트북은 USIM 에뮬레이터 기능과 WLAN 접속 기능이 있는 UE에 해당하며, 가운데에 WLAN AP가 위치해 있다.

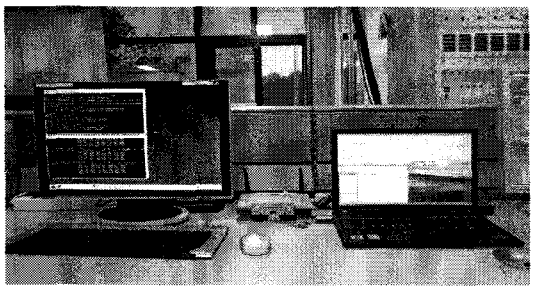

그림 5. 인증 테스트베드 구현 모습
Fig. 5. Implementation of authentication testbed

인증 테스트베드에 사용된 시험 장비의 하드웨어/소프트웨어 사양은 표 2와 같다. 단, IPv6환경에 대해서는 IPv6 지원 AP와 EAP-AKA 지원 RADIUS 서버를 구성하기가 용이하지 않은 관계로 IPv4망에서 시험하였다.

표 2. 인증 테스트베드 사양
Table. 2. Specification of authentication testbed

구성 요소	사양
UE (Client)	HW: IBM Notebook - Intel Pentium-IV OS: Windows XP sp2 802.11b/g WLAN card USB 메모리스틱 or CF type 메모리 IPv4
AP	Cisco aironet 1200 Series
RADIUS Server	HW: IBM Notebook - Intel Pentium-IV OS: 한컴 리눅스 freeRadius 1.0.4

인증 테스트베드에서 사용된 UE인 노트북에서 실제 USIM을 대신하여 USB 또는 PCMCIA 메모리를 사용한 USIM 에뮬레이터 장치를 사용하였다. USIM 에뮬레이터 장치는 다음과 같은 특징을 가지고 구현되었다.

- 3GPP TS21.111에 기반한 USIM 기능
- 3GPP 가입자 정보 및 3GPP TS 33.102에 기반한 사용자 인증 데이터 관리 기능
- 3GPP TS33.234 기반 EAP-AKA 인증 알고리즘 구동
- USIM과 3GPP 무선 모듈간, USIM과 무선랜 모듈간 인터페이스를 위한 사용자 인터페이스 및 USIM 제어 기능

USIM 에뮬레이터의 시험에서 기능에 대한 확인 및 성능 측정은 각 운영체제에서 제공되는 패킷 분석 Tool을 사용하였다. 단말에는 EAP 패킷을 필터링하여 측정 가능한 Ethereal이라는 패킷 모니터링 툴을 사용하고, AAA 서버에는 Linux에서 제공되는 snooping 툴인 tcpdump라는 툴을 사용하며, tcpdump로 port 1645에 대한 패킷을 측정할 수 있다.

4.2 인증 테스트베드 구동

USIM Emulator를 구동시키고 USIM 정보가 들어있는 USB 메모리를 노트북 컴퓨터에 꽂으면 메모리가 검색된다. 인증을 위해 USB 메모리를 액세스하기 위해서는 PIN number를 입력해야 한다. 이에 대한 절차는 그림 6과 같고, 그림 7은 인증 절차가 완료되는 과정을 나타낸다.

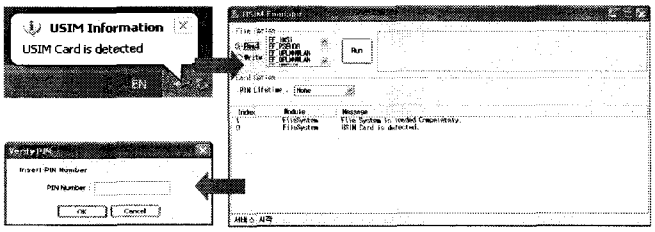

그림 6. USIM 에뮬레이터와 PIN 입력창
Fig. 6. USIM Emulator and PIN input windows

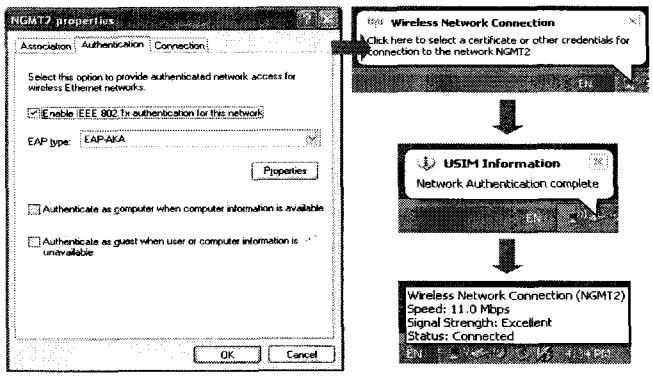

그림 7. 인증 완료 화면
Fig. 7. Authentication completed

4.3 시험 방법

구현된 인증 테스트베드의 성능을 측정하기 위해 버티컬 핸드오버시 수행되는 완전 인증 절차와 빠른 재인증 절차를 주요 성능 파라미터로 설정하여 시험을 수행하였다.

AAA 서버의 인증 절차와 관련하여 완전 인증 절차와 빠른 재인증 절차를 통한 인증 시간을 비교하였다. 총 인증시간은 AAA 서버에 인증 절차 중 최초 메시지(EAP-Response/Identity)를 받고 성공 응답(EAP-Success)을 전송하는 시간으로 정의하였다.

3G 단말에서도 완전 인증과 빠른 재인증 절차를 통한 인증 시간을 비교하였다. 총 인증시간은 성능 외적 요인(완전 인증시 EAP Request/Identity를 받고 사용자가 PIN 넘버를 넣는 시간 등)을 제외할 수 있도록 EAP-Response/Identity 전송으로부터 EAP Success를 받는 시간으로 정의하였다.

그림 8은 UMTS에서 WLAN으로 핸드오버 수행시 필요한 절차를 간략히 보이고 있다. 핸드오버 지연은 케넥션

설정과 인증 절차에 의해 발생한다.

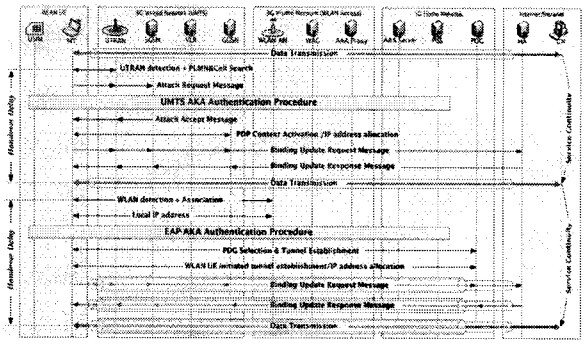

그림 8. UMTS에서 WLAN으로의 핸드오버 절차
Fig. 8. UMTS to WLAN handover procedure

시험 환경은 그림 5에 나타나 있는 시스템 환경에서 다음의 순서에 의해서 시험을 위한 환경을 구축하고, 시험을 진행하였다.

① USIM Card(CF/SD Memory) 상에 필요한 파일 생성
② USIM Emulator 설치
③ USIM Interface Module 및 RAS 기반의 EAP-AKA 모듈 설치 및 셋팅
④ RADIUS 시스템 구성 및 설정
⑤ RADIUS 시스템에 테스트 사용자 및 사용자에 대한 Test Value 값 적용

위와 같은 모든 설정이 완료되면 시험을 위한 기본적인 환경 구축이 완료된다. 단, 상기의 항목 중 Test Value 값에 대한 적용 사항은 다음과 같다.

- K 값 : 465b5ce8 b199b49f aa5f0a2e e238a6bc
- OP 값 : cdc202d5 123e20f6 2b6d676a c72cb318
- SQN 값 : ff9bb4d0 b607
- AMF 값 : b9b9
- RAND 값 : 23553cbe 9637a89d 218ae64d ae47bf35

시험 항목은 이미 언급한 바와 같이 USIM 에뮬레이터 성능 시험과 RADIUS 인증 서버 성능 시험으로 구성된다. USIM 에뮬레이터 구현 항목에 대해서는 EAP-AKA full Authentication 기능과 re-Authentication 기능 시험을 수행하고, RADIUS의 EAP-AKA 구현 항목에 대해서는 EAP-AKA Authentication 기능 시험과 re-Authentication 기능 시험으로 나뉜다.

V. 시험 결과

시험 결과는 총 10회의 시험 결과를 평균으로 내어 측정하였다. 테스트베드를 통해 10회를 반복하여 얻어진 EAP-AKA 완전 인증 및 빠른 재인증에 소요되는 시간에 대한 다양한 시험 결과는 표 3, 4와 같다. AAA 서버와 단말에 두 가지 인증 방법 적용하여 핸드오버시 발생한 지연 시간을 측정한 결과이다. 단말의 경우에는 암호화 시간을 추가로 측정하였다.

표 3. 시험 결과
Table. 3. Experimental results

	AAA서버		단말			
	FULL	FAST	FULL		FAST	
	총시간	총시간	암호화 처리	총시간	암호화 처리	총시간
1	1.213	0.716	0.920	1.217	0.334	0.720
2	0.922	0.810	0.779	0.926	0.331	0.814
3	1.101	0.646	0.809	1.104	0.343	0.650
4	1.179	0.670	0.978	1.184	0.229	0.674
5	1.155	0.564	0.866	1.160	0.296	0.568
6	1.113	0.498	0.837	1.119	0.405	0.502
7	1.839	0.629	1.168	1.843	0.331	0.634
8	1.142	0.591	0.834	1.146	0.291	0.594
9	0.915	0.400	0.831	0.919	0.333	0.404
10	1.815	0.488	1.159	1.819	0.408	0.493
평균	1.239	0.601	0.918	1.244	0.330	0.605

표 4. RTT와 암호화 시간 비교
Table. 4. Comparison of RTT and cypering time

	RTT		암호화 시간 비율		단축 비율
	FULL	FAST	FULL	FAST	
1	0.004	0.004	75.6%	46.4%	40.8%
2	0.004	0.004	84.1%	40.7%	12.1%
3	0.003	0.004	73.3%	52.8%	41.1%
4	0.005	0.004	82.6%	34.0%	43.1%
5	0.005	0.004	74.7%	52.1%	51.0%
6	0.006	0.004	74.8%	80.7%	55.1%
7	0.004	0.005	63.4%	52.2%	65.6%
8	0.004	0.003	72.8%	49.0%	48.2%
9	0.004	0.004	90.4%	82.4%	56.0%
10	0.004	0.005	63.7%	82.8%	72.9%
평균	0.004	0.004	75.5%	57.3%	48.6%

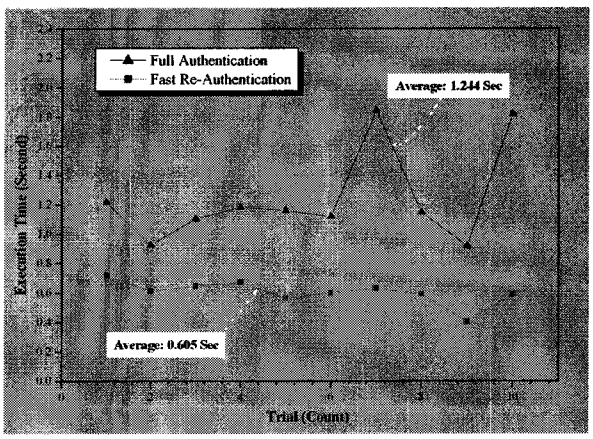

그림 9. 평균 인증 소요 시간
Fig. 9. Average authentication processing time

측정결과는 최초 UE가 WLAN AP와의 association이 끝나고 EAP Request/Identity를 수신한 다음 그에 대한 응답을 보낸 후 AAA 서버와의 인증 절차가 이루어 진 후 EAP success를 수신할 때까지 걸린 시간을 나타낸다.

UE와 AAA 서버간의 완전인증에 소요되는 시간은 그림 9에서 보듯이 은 평균 1.244 Sec이며 빠른 재인증에 소요되는 시간은 평균 0.605 Sec가 된다. 따라서, UMTS와 WLAN간 서비스 연속성 관점에서 완전 인증으로 인해 발생하는 지연 시간이 비교적 크게 발생함을 알 수 있으며, 빠른 재인증을 사용함으로써 인증에 소요되는 시간을 48.6% 단축시킬 것으로 측정되었다. 이는 곧 서비스 연속성을 보장하기 위해 요구되는 핸드오버 지연을 줄일 수 있다. 단말에서의 전체 인증 시간 중 USIM 카드에서 암호화 알고리즘을 처리하는 시간이 완전 인증과 빠른 재인증시에 각각 전체 시간의 75%, 57.3%를 차지하였다. 위의 암호화 알고리즘 처리 시간은 실제 USIM 에뮬레이터가 PCMCIA 인터페이스의 CF 메모리 카드를 액세스하고 암호화 알고리즘을 처리하는 시간을 포함하고 있으므로 실제 UE내에 칩으로 설계되어 설치될 경우 시간이 훨씬 단축될 것으로 예상된다. 평균 RTT(Round Trip Time)은 0.004초로 전체 인증 시간에 큰 영향 미치지 않았다.

VI. 결 론

3GPP 진영에서의 UMTS-WLAN간 연동에 대한 표준화 작업은 마무리가 되고 있다. 하지만 이들 이종망간 끊김 없는 이동성이 제공되기 위해서는 해결해야할 기술적인 문제들이 남아 있으며, 3GPP에 추구하고 있는 AIPN(All IP Network), LTE-Advanced 성공을 위해 앞으로 꾸준하게 진행되어야 할 기술 분야이다.

본 논문에서는 UMTS와 WLAN간의 핸드오버 지연을 줄이기 위해서 인증 절차가 실제 핸드오버 지연 시간에서 차지하는 비중을 살펴보고, 인증 처리 시간을 줄이는 것이 효율적임을 보이기 위하여 완전 인증 절차와 빠른 재인증 절차를 EAP-AKA 테스트베드에 구축하여 비교하였다. 본 테스트베드는 향후 UMTS-WLAN 인터워킹 시스템에서의 핸드오버 기능 구현시 좋은 참고 자료가 될 것이다.

참고 문헌

[1] H. Kwon, K. Ro, A. Park and J. Ryou, "Mobility Management for UMTS-WLAN Seamless Handover; Within the Framework of Subscriber Authentication," *ISATED Communication, Network, and Information Security (CNIS)*, Nov. 2005.

[2] H. Kwon, K. Jung, A. Parkand J. Ryou, "Consideration of UMTS-WLAN Seamless Handover," *Proceedings of the Seventh IEEE International Symposium on Multimedia Technologies over Wireless Networks*, pp.649-656, Dec. 2005.

[3] 3GPP TSG SA, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6)," *3GPP TS 23.234*, pp.25-32, March 2005.

[4] 3GPP TSG Terminals, "USIM and IC card requirements (Release 6)," *3GPP TS 21.111*, pp.10-12, June 2004.

[5] 3GPP TSG SA, "3G Security; Security Architecture (Release 6)," *3GPP TS 33.102*, pp.16-39, December 2005.

[6] 3GPP TSG SA, "3G security; Wireless Local Area Network (WLAN) interworking security," *3GPP TS 33.234*, pp.22-59, December 2005.

[7] J. Arkko & H. Haverinen, EAP AKA Authentication, Internet Draft draft-arkko-pppext-eap-aka-13, Oct. 2004.

노 광 현(Kwang-Hyun Ro)
1995년 고려대학교 산업공학과 (공학사)
1997년 고려대학교 산업공학과 (공학석사)
2001년 고려대학교 산업공학과 (공학박사)
2001년 ~ 2002년 Ecole des Mines de Paris, Robotic Center (Post-Doc)
2003년 ~ 2006년 한국전자통신연구원 연구원
2006년 ~ 2007년 한국항공우주연구원 선임연구원
2007년 ~ 현재 한성대학교 산업시스템공학과 조교수
관심분야: Mobile telecommunication, IP mobility, Embedded systems

권 혜 연(Hyeyeon Kwon)
1990년 충남대학교 계산통계학과 (이학사)
2000년 충남대학교 컴퓨터공학과 (이학석사)
2006년 충남대학교 컴퓨터공학과 (이학박사)
1990년 ~ 현재 한국전자통신연구원 이동통신연구본부 책임연구원
관심분야: Mobile telecommunication, Communication protocol, Mobile ad-hoc networks, IP mobility