

USIM based Authentication Test-bed For UMTS-WLAN Handover

25 April, 2006

Hyeyeon Kwon, Kyung-yul Cheon, Kwang-hyun Roh, Aesoon Park
Electronics and Telecommunications Research Institute
161, Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
hykwon@etri.re.kr, kycheon@etri.re.kr, khrho@etri.re.kr, aspark@etri.re.kr

Contents

1. Abstract

2. Introduction

3. Background

1. UMTS-WLAN Interworking Architecture
2. Authentication Mechanism in UMTS
3. Authentication Mechanism in WLAN Access System

4. Authentication Test-bed

1. Analysis of Handover Delay
2. USIM based Authentication Test-bed
3. Results & Analysis

5. Conclusion and future work

1. Conclusion
2. Future Work
3. Reference

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.
- In this paper, we analyze an authentication mechanism for 3GPP-WLAN seamless mobility by USIM-based authentication test-bed.
- In handover 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**. For considering the fast re-authentication mechanism during handover, we show the **analytic results of EAP-AKA processing in our test-bed**.

Introduction

- Recently, due to the mutual complementary feature of wide coverage and high data rate, the interworking between 3G mobile networks and Wireless LAN (WLAN) is a global trend of wireless communications.
- For the seamless mobility between 3G and WLAN, low handover delay has to be achieved. Main factor of handover delay between these heterogeneous networks is authentication.
- For the purpose of reducing authentication processing time in 3G-WLAN handover, the application of fast re-authentication mechanism during handover is considered [1][2].
- This paper describes the USIM based EAP-AKA Test-bed implemented for handover in UMTS and WLAN interworking systems and shows the analytic results by measuring and comparing the delay of fast re-authentication and full authentication of EAP-AKA in our test-bed

Authentication Mechanism in UMTS (1/2)

■ UMTS AKA [4]

- ◆ Mutual authentication and all key agreement mechanism based on symmetric keys in USIM module of UE in UMTS.
- ◆ USIM and network have a common secret key beforehand.

◆ Authentication entities

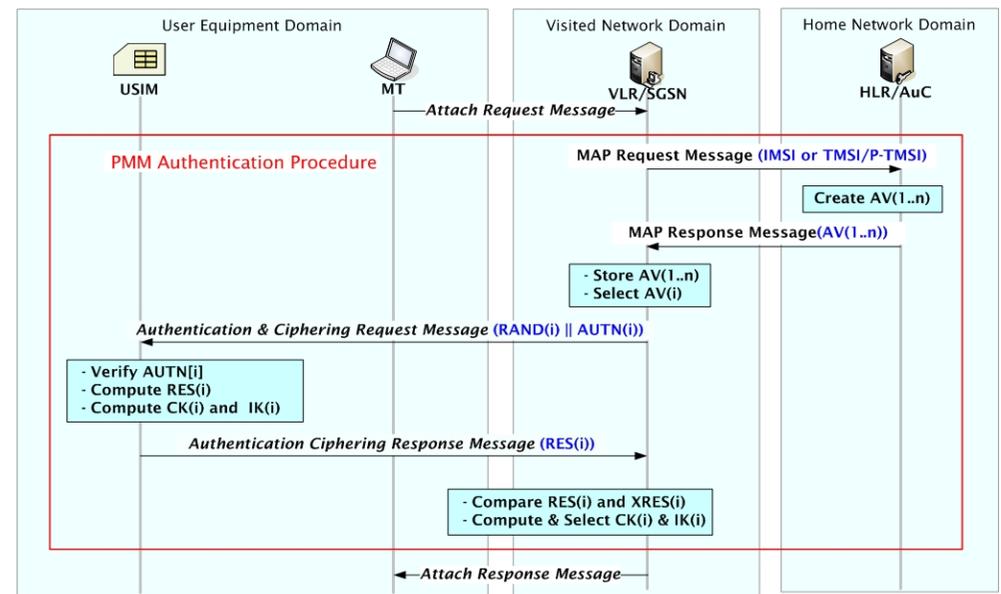
- AuC, VLR and USIM

◆ Authentication vector (AV)

- *RAND* : A random number
- *XRES* : An expected response
- *CK* : A cipher key
- *IK* : An integrity key
- *AUTN* : An authentication token

- ◆ Each AV is only valid for one AKA between the VLR and the USIM

- ◆ Each AV is ordered by the sequence number *SQN*.



Authentication Mechanism in WLAN Access System (1/2)

■ EAP-AKA [5][6]

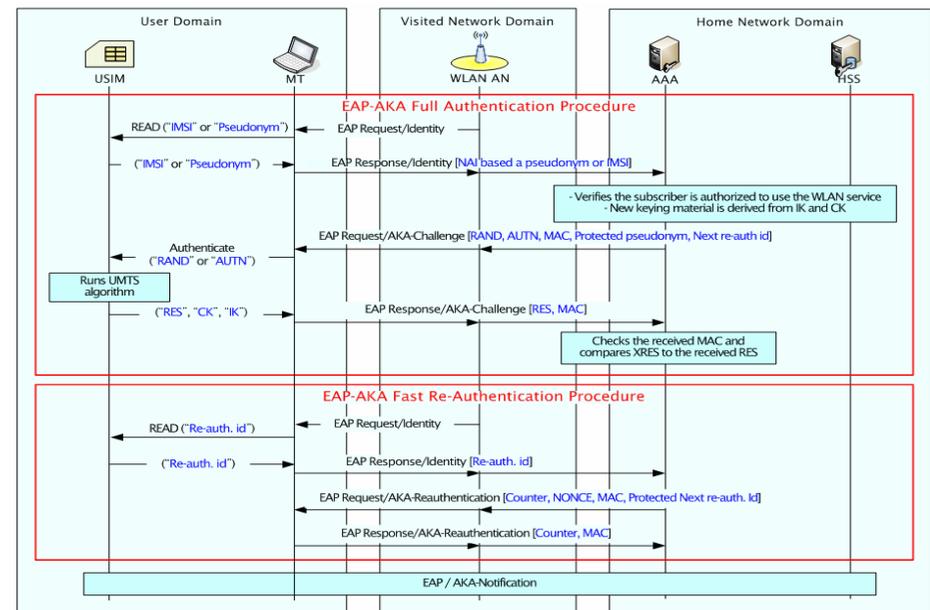
- ◆ An EAP [7] mechanism for authentication and session key distribution using the AKA mechanism used in the 3G mobile networks such as UMTS and cdma2000.
- ◆ EAP contains a negotiation sequence where the authenticator requests information about which authentication method would be used.
- ◆ EAP server is located on a backend authentication server using an AAA protocol, i.e. 3GPP AAA server.

◆ Full authentication

- An initial authentication procedure where new keys are generated in the USIM card and the network.

◆ Fast re-authentication

- Reuse the keys generated from the previous authentication process.
- Save processing time in the WLAN UE and the AAA server
- Save power consumption in the UE.
- The use of fast re-authentication depends on the operator's policies.

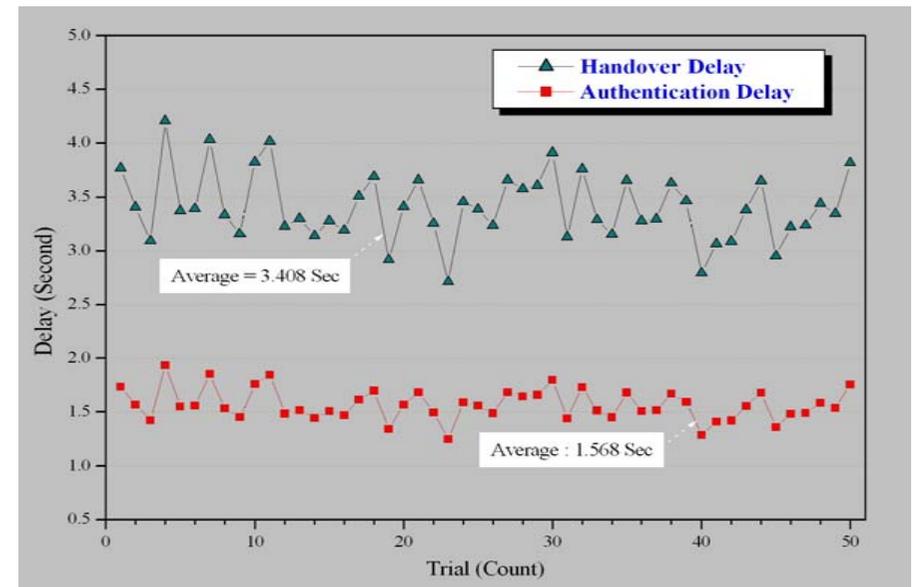


Analysis of Handover Delay

- Handover delay is caused by connection establishment to each network and authentication procedure while handover is performed.
- For measuring the handover delay from UMTS to WLAN, the simulation performing the handover procedure was conducted 50 times under network simulator.

■ Simulation Results

- ◆ Average handover delay from UMTS to WLAN: 3.408sec.
- ◆ Average authentication processing time: 1.568sec
 - ⦿ 46% of overall handover delay
- ◆ Less authentication processing time,
Less handover delay
- ◆ One of the good solutions
➔ **Fast re-authentication.**



USIM based Authentication Test-bed (1/2)

■ Goal of USIM-based EAP-AKA test-bed

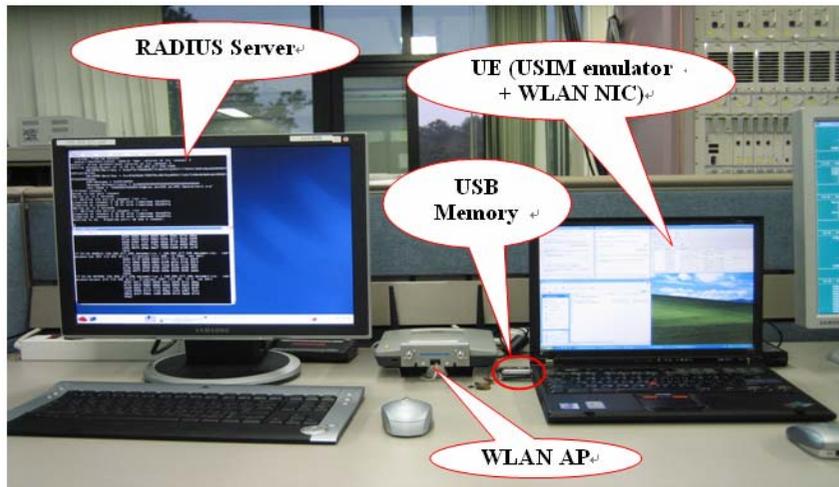
- ◆ Measure and compare the processing time of full authentication and fast re-authentication in our test-bed
- ◆ Analyze the efficiency of fast re-authentication.

■ USIM emulator

- ◆ USB (or PCMCIA) memory and emulator program in a notebook computer
 - USIM functions specified in 3GPP TS 21.111[8]
 - 3GPP subscriber information and functions of managing subscriber authentication data specified in 3GPP TS 33.102[4]
 - Execution of EAP AKA authentication algorithm specified in 3GPP TS 33.234[8]
 - User interfaces between USIM and 3GPP wireless module/WLAN module, and USIM control function
- ◆ USB memory was used instead of an IC card as USIM
 - It seems that Read/Write delay of USB memory caused much more delay compared with IC card type USIM.
 - Therefore, the delay can be more reduced by using an IC card type USIM.

USIM based Authentication Test-bed (2/2)

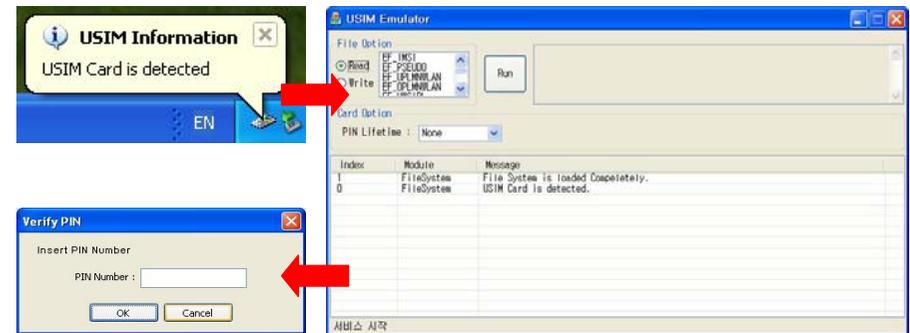
Configuration of authentication Test-bed



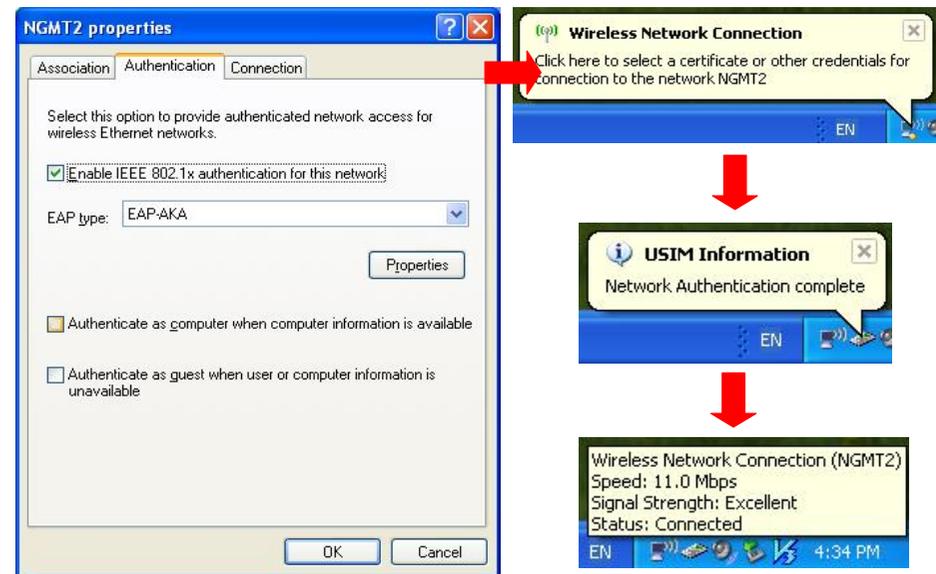
Environment of Test-bed

	Client	AP	AAA Server
OS	Windows XP	Cisco AP 1200	Linux
Language	C/C++	None	C/C++
Protocol	EAP-AKA	RADIUS/EAP	RADIUS/EAP/AKA
Remarks	WLAN Mini PCI Adapter	Cisco Aironet 1200	Open RADIUS

PIN Input for USIM Access



EAP-AKA Operation

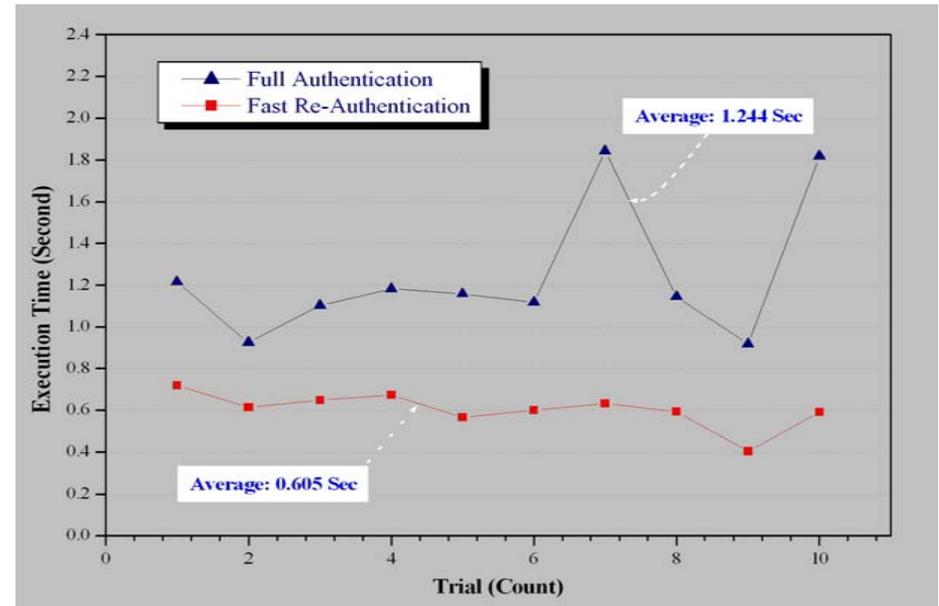


Results & Analysis

Experimental Results by Test-bed execution

- ◆ 10 times trial of authentication processing in test-bed
 - ⦿ Including UE's association with WLAN AP, reception and response of EAP Request/ Identity, authentication with AAA server and reception of EAP success message.
- ◆ Average RTT between UE and AAA server : 0.0004 sec
- ◆ Average full authentication processing time : 1.244 sec
- ◆ Average fast re-authentication processing time : 0.605 sec.
 - ⦿ 48.6% saving time by fast re-authentication

Handover delay can be enough minimized by using of the fast re-authentication mechanism during handover !!!



Conclusion and Future Works

■ This paper

- ◆ analyzed how much authentication costs processing time of overall handover delay
- ◆ Analyzed how much the fast re-authentication can reduce the authentication latency.
- ◆ Showed that handover latency during UMTS-WLAN handover can be considerably reduced by minimizing authentication processing time

■ Future Works

- ◆ EAP-AKA test-bed will be applied to our UMTS-WLAN handover system under development.

■ References

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. Park and J. Ryou, "Consideration of UMTS-WLAN seamless handover," IEEE Multimedia Technologies over Wireless Networks (WMOw), Dec. 2005.
3. 3GPP; TSG SA, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6)," 3GPP TS 23.234, March 2005.
4. 3GPP; TSG SA, "3G Security; Security Architecture (Release 6)," 3GPP TS 33.102, March 2005.
5. 3GPP; TSG SA, "3G security; Wireless Local Area Network (WLAN) interworking security," 3GPP TS 33.234, March 2005.
6. J. Arkko and H. Haverinen, EAP AKA Authentication, *Internet Draft draft-arkko-pppext-eap-aka-13*, Oct. 2004.
7. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz, Extensible Authentication Protocol (EAP), *RFC3748*, June 2004.
8. 3GPP; TSG Terminals; "USIM and IC card requirements (Release 6)," 3GPP TS 21.111, June 2004.