USIM based Authentication Test-bed For UMTS-WLAN Handover

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

Abstracts – 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.

Index – UMTS-WLAN interworking, UMTS-WLAN handover, UMTS-WLAN authentication, UMTS-WLAN security

I. 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

The rests of this paper are organized as follows: we show the UMTS-WLAN overlay network architecture with Mobile IPv6 and authentication mechanisms for UMTS and WLAN in section 2. In section 3, we describe the USIM based EAP-AKA Test-bed and show the performance evaluation with analysis. Finally, we conclude the paper with remarks and future works.

II. Background

1. UMTS-WLAN Interworking Architecture

In 3GPP, a feasibility study and the most skeleton for 3GPP-WLAN interworking was complete [3] and the loosely coupled based architectures has been defined [4]. The main objective of 3GPP activity is to extend 3GPP services and functionality to the WLAN access environment. So it is based on an assumption that WLAN access network is mainly operated as an extension to 3GPP access network [1].

Fig.1 shows the UMTS (Universal Mobile Telecommunications System) and WLAN (Wireless LAN) Interwoking architecture following the 3GPP specification [5]. In this system, WLAN AN is a WLAN access network having more than one WLAN AP (Access Point). The 3GPP AAA Proxy performs a proxying and filtering function in the visited network. And the 3GPP AAA Server retrieves authentication information and subscriber profile from the HSS (Home Subscriber Server) in 3GPP subscriber's home network. HSS has the functionality of AuC (Authentication Center) and HLR (Home Location Register). The WAG (WLAN Access Gateway) is a gateway for the data to/from the WLAN AN and the UE (User Equipment). 3GPP PS (Packet Service) based services may be accessed via a PDG (Packet Data Gateway) in the user's home network or in the selected visited network.

In UMTS [6], SGSN (Serving GPRS Support Node) is a gateway for accessing the packet core network and GGSN (Gateway GPRS Support Node) is a gateway for accessing the 3GPP PS based services or external IP based network, the PDG has the same functionality as that of the GGSN. Also, there are AuC for authentication and HLR/VLR (Visitor Location Register).

WLAN UE is a dual-mode mobile terminal with USIM (User Subscriber Identity Module), which has UMTS module and WLAN module with signaling and data protocols for each system.

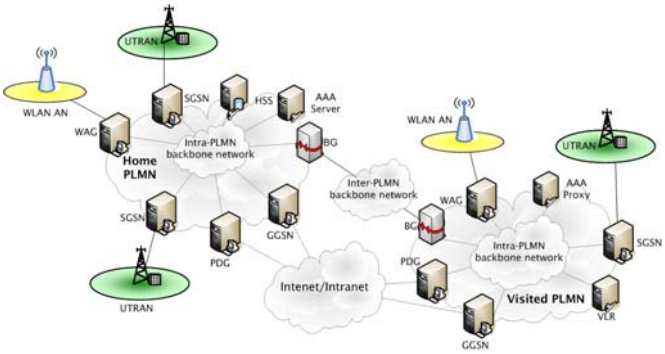

Fig. 1. UMTS-WLAN Interworking Architecture

2. Authentication Mechanism in UMTS

In UMTS, UMTS AKA [7] performs the mutual authentication and all key agreement based on symmetric keys in USIM module of UE. USIM and network have a common secret key beforehand. The authentication entities, such as AuC, VLR and USIM, commonly have an ordered array of *n* authentication vector (AV) with following components (Quintet): a random number *RAND*, an expected response *XRES*, a cipher key *CK*, an integrity key *IK* and an authentication token *AUTN*. Each AV is only valid for one AKA between the VLR and the USIM and is ordered by the sequence number *SQN*. Fig. 2 shows a UMTS AKA signaling in PMM (Packet Mobility Management) attach procedures. As shown in figure, the authentication parameters are delivered by *Authentication & Ciphering Message*.

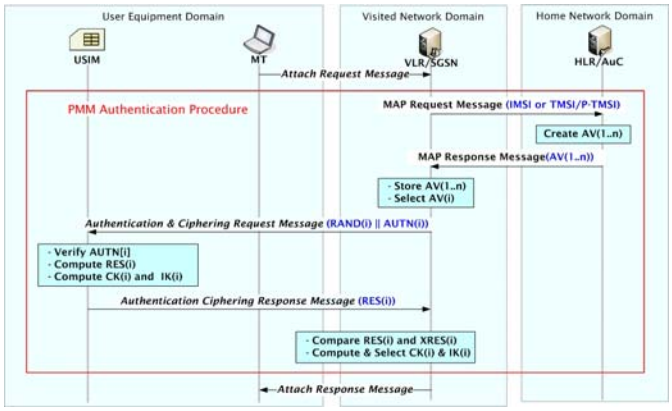

Fig. 2. UMTS-AKA procedure

3. Authentication Mechanism in WLAN Access System

In WLAN access system, EAP-AKA [8][9] is an EAP [10] mechanism for authentication and session key distribution using the AKA mechanism used in the 3G mobile networks such as UMTS and cdma2000. The EAP contains a negotiation sequence where the authenticator requests information about which authentication method would be used. The EAP server is located on a backend authentication server using an AAA protocol, i.e. 3GPP AAA server.

Fig. 3 shows the EAP-AKA authentication procedures.

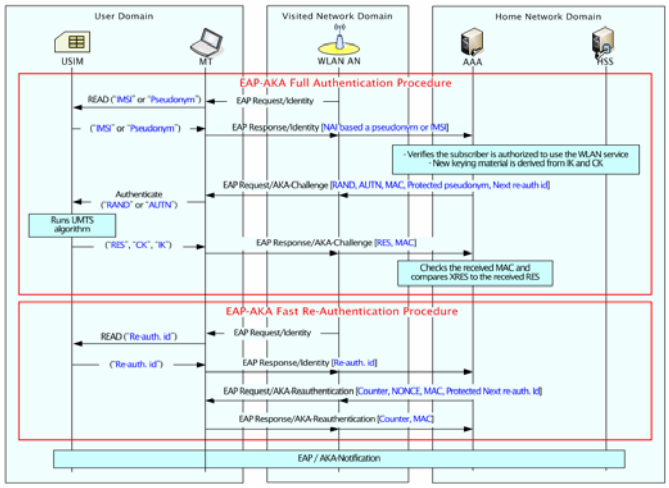

Fig. 3. EAP-AKA authentication Procedure

There are two authentication procedures for EAP-AKA, full authentication and fast re-authentication. The full authentication is an initial authentication procedure where new keys are generated in the USIM card and the network. However, fast re-authentication reuses the keys generated from the previous authentication process. The advantages of fast re-authentication are not only to save processing time in the WLAN UE and the AAA server, but also to save power consumption in the UE. The use of fast re-authentication depends on the operator's policies.

III. Authentication Test-bed

1. 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.

Fig. 4 shows the simulation result. The average handover delay from UMTS to WLAN was 3.408sec. The average authentication processing time was 1.568sec and it costs 46% of overall handover delay. Therefore, it is necessary to minimize the authentication processing time for reducing the handover delay. One of the good solutions is to use fast re-authentication.

As mentioned above, UMTS AKA and EAP-AKA are almost identical except that a low level packet transmission protocol for sending AKA is PMM protocol in case of UMTS and EAP protocol in case of WLAN, and UMTS AKA doesn't have a fast re-authentication function of EAP-AKA [9]. So, UMTS AKA has to add the fast re-authentication mechanism.

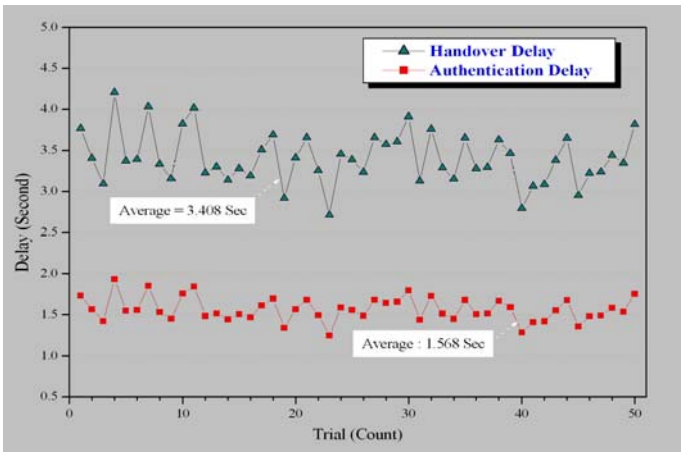

Fig. 4. Handover delay from UMTS to WLAN

2. USIM based Authentication Test-bed

This section shows the USIM-based EAP-AKA test-bed implemented for the handover in UMTS and WLAN interworking systems. And we measure and compare the processing time of full authentication and fast re-authentication in our test-bed and analyze the efficiency of fast re-authentication.

USIM is implemented with USB (or PCMCIA) memory and emulator program in a notebook computer. We call this USIM emulator. The USIM emulator has following characteristics.

- USIM functions specified in 3GPP TS 21.111[11]
- 3GPP subscriber information and functions of managing subscriber authentication data specified in 3GPP TS 33.102[7]
- 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

The configuration of an authentication test-bed for executing EAP-AKA is shown in Fig. 5. Also, table 1 describes the test-bed environment.

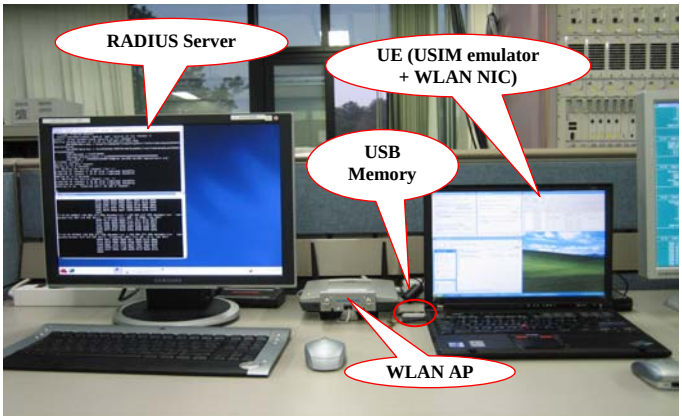

Fig. 5. Configuration of authentication test-bed

Table 1. EAP-AKA Test-bed Environment

	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

As soon as USB memory including USIM information is plugged into the terminal, the memory is automatically detected. It is necessary to input PIN number for the memory access for authentication. Fig. 6 and fig. 7 show the operation of the test-bed.

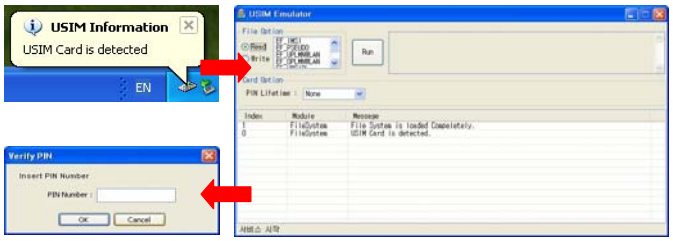

Fig. 6. USIM emulator and PIN input windows

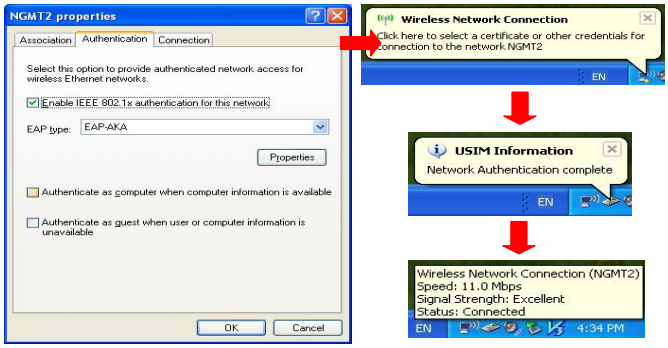

Fig. 7. Authentication operation window

3. Results & Analysis

For measuring the processing time for EAP-AKA full authentication and fast re-authentication, the experiment on authentication processing was performed 10 times under the test-bed and the experimental results are shown in fig. 8.

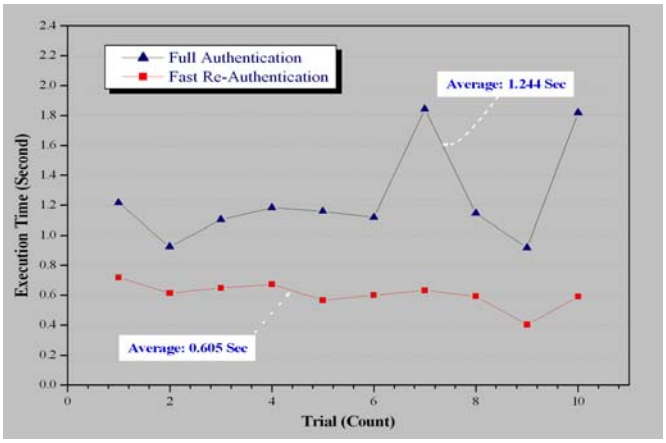

Fig. 8. Average authentication processing time

The execution time in the above figure includes the processing time of the following procedures; 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 is 0.0004 sec and average full authentication processing time is 1.244 sec and average fast re-authentication processing time is 0.605 sec. Therefore, the fast re-authentication may be able to reduce 48.6% of full authentication processing time. It means that the handover delay can be enough minimized by using of the fast re-authentication mechanism during handover.

Meanwhile, in our test-bed, 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.

IV. Conclusion and Future Works

Interworking of UMTS and WLAN comes to the final step in 3GPP but the seamless mobility needs further consideration and has many technical challenges. This is an on-going evolutional step in AIPN (All IP Network) of 3GPP WG SA#1, SAE of 3GPP WG SA#2, LTE (Long-Term evolution) of 3GPP WG RAN for B3G mobile communications.

This paper analyzed how much authentication costs processing time of overall handover delay and how much the fast re-authentication can reduces the authentication latency. To achieve the authentication mechanism for UMTS-WLAN handover and verify that handover delay can be considerably reduced by minimizing authentication processing time, USIM-based EAP-AKA test-bed was implemented and the experimental results were analyzed. The 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, "Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking; (Release 6)," *3GPP TS 22.934*, Sept, 2003

[4] ETSI, "Requirements and Architectures for Interwoking between HIPERLAN/3 and 3rd Generation Cellular Systems," *Tech. rep. ETSI 101 957*, Aug 2001.

[5] 3GPP; TSG SA, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6)," *3GPP TS 23.234*, March 2005.

[6] 3GPP; TSG SA, "General Packet Radio Service (GPRS); Service description; Stage 2 (Release 6)," *3GPP TS 23.060*, March 2005.

[7] 3GPP; TSG SA, "3G Security; Security Architecture (Release 6)," *3GPP TS 33.102*, March 2005.

[8] 3GPP; TSG SA, "3G security; Wireless Local Area Network (WLAN) interworking security," *3GPP TS 33.234*, March 2005.

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

[10] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, Extensible Authentication Protocol (EAP), *RFC3748*, June 2004.

[11] 3GPP; TSG Terminals; "USIM and IC card requirements (Release 6)," *3GPP TS 21.111*, June 2004