Key Management Protocol for Roaming in Wireless Interworking System

Taenam Cho[†] , Jin-Hee Han[††] and Sung-Ik Jeon[††],

[†]Dept. of Information Security, Woosuk University, 490 HuJung-Ri, SamRye-Up, Junbuk, Korea
[††] Division of Information Security, ETRI, 161 GaJung-Dong, YuSung-Gu, Taejeon, Korea.

Summary

3GPP makes efforts to enable usage of 3GPP system functionalities such as SIP calls between mobile terminals and 3GPP systems via the WLAN and to utilize 3GPP system functionalities to complement the functionalities such as charging means, authentication, authorization, and accounting functions available in the WLAN. And an interworking framework to integrate the services of 3G, WLAN and WiBro networks is proposed by Electronics and Communications Research Institute. Since each network adopts deferent protocols for mutual authentication and key agreement between users and networks, unified authentication for the integrated system is not simple problem when a user moves from one network to another. In this paper, a secure and efficient key management protocol for roaming among different networks is proposed.

Key words:
Wireless Network, Mobile Communications, WiBro, Authentication, Key Management

1. Introduction

3G telecommunication service is mobile and fast but expensive. On the other hand, WLAN service provides high transmission speed and inexpensive service cost but has low mobility. WiBro service is designed for higher mobility than WLAN and higher transmission speed and lower cost than 3G telecommunication service [14]. The 3rd Generation Partnership Project (3GPP) makes efforts to establish wireless service system which integrates various wireless networks to provide both high data transmission speed and mobility [1], [4], [5], [10]. Integrating various networks requires many security solutions including authentication, key management and roaming/handover management [14]. To consider those security problems and minimized modification to the current system, wireless network integration model based on USIM (Universal Subscriber Identity Module) is proposed. The model supports unified user authentication and for that reason UAGS (USIM Access Gateway System) performs proxy server function to authentication center and protocol translation between authentication center and authenticators. However, there is no key management scheme for roaming in the interworking system. In this paper, we propose a key management protocol for roaming which provides unified authentication in various networks on the assumption that a single service provider runs 3 different networks. The remainder of the paper is organized as follows. Section 2 reviews the requirements of key management protocol for roaming. Section 3 presents authentication protocols and the integrated system structure on which our protocol based. Section 4 proposes a key management protocol for this integration system. Section 5 analyzes the security and efficiency of the proposed protocol and it is concluded in section 6.

2. Requirements

When a user moves from one network to another one under a same service provider, the key management protocol for roaming should meet several requirements as follows:

(R1) The amounts of computing and communication loads of authentication center, HLR/AuC, due to roaming should be minimized.
(R2) The amounts of computing of users due to roaming should be minimized.
(R3) After roaming, the visiting network can verify that the user has correct keys.
(R4) After roaming, the user and the visiting network can use the keys and authentication protocol which appropriate to the visiting network.
(R5) When a user returns to the previously visited network or visits another network, she can use authentication protocol which is appropriate to the visited network.
(R6) Even though two or more roamings are occurred without any authentication process, the security should be reserved. This is a requirement to protect replay attack.

Manuscript received August 5, 2007
Manuscript revised August 20, 2007

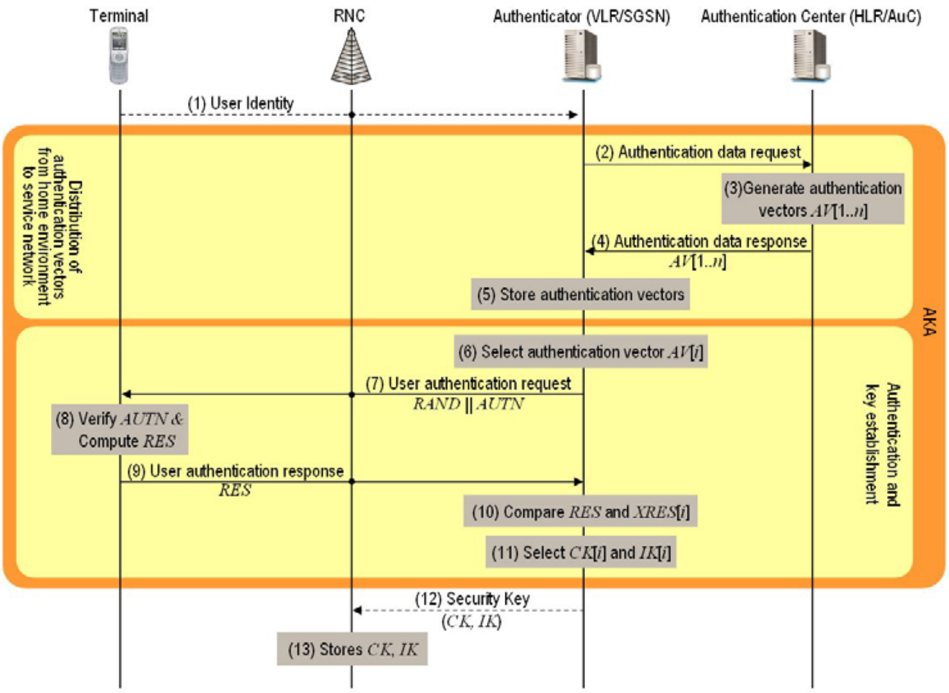
Terminal
RNC
Authenticator (VLR/SGSN)
Authentication Center (HLR/AuC)
(1) User Identity
Distribution of authentication vectors from home environment to service network
(2) Authentication data request
(3)Generate authentication vectors AV[1..n]
(4) Authentication data response AV[1..n]
(5) Store authentication vectors
AKA
(6) Select authentication vector AV[i]
(7) User authentication request RAND || AUTN
(8) Verify AUTN & Compute RES
(9) User authentication response RES
(10) Compare RES and XRES[i]
(11) Select CK[i] and IK[i]
Authentication and key establishment
(12) Security Key (CK, IK)
(13) Stores CK, IK

Fig. 1 Authentication and Key Agreement in AKa

3. Authentication Protocols and 3G-WLAN-WiBro Interworking System

In this section, we introduce the authentication protocols which are used in 3G, WLAN or WiBro and the framework

of wireless interworking system which is proposed by ETRI (Electronics and Telecommunications Research Institute).

3.1 AKA (Authentication and Key Agreement)

In this section, we'd like to introduce AKA [8], [9] protocol which is used in the 3G network for authentication. In AKA, a user and network (in 3G, HLR (Home Location Register/Authentication Center)) share a preshared key *K*. The authentication process flow using AKA is depicted in Fig. 1. Authentication process consists of three stages: User Identification stage (step 1 in Fig. 1), Authentication stage that executes AKA protocol (from step 2 to step 12 in Fig. 1) and Key Transmission stage that VLR/SGSN (Visited Location Register/Serving GPRS Support Node) sends the keys to RNC (Radio Network Controller)(from step 13 to step 14 in the Fig. 1). The detailed procedure is as follows:

(1) USIM in the user's terminal sends IMSI (International Mobile Subscriber Identity) [2], [9] as user's identity to VLR/SGSN of the service network via RNC. The user may send TMSI (Temporary Mobile Subscriber Identity) instead of IMSI to protect user's identity if this is not the first authentication.

(2) VLR/SGSN requests subscriber data corresponding to the user's identity to the authentication center, HLR/AuC.

(3) HLR/AuC generates authentication vectors (*AV*s). For one *AV*, HLR/AuC generates a random number (*RAND*) and a sequence number (*SQN*: SQuence Number) and computes *MAC* (Message Authentication Code), *XRES* (eXpedted RESponse), *CK* (Cipher Key), *IK* (Integrity Key) and *AK* (Anonymity Key) using preshared key *K* and *AMF* (Authentication Management Field). An *AV* consists of these values as depicted in Fig. 2.

(4) HLR/AuC calculates up to 5 *AV*s to reduce the communication complexity and sends them to VLR/SGSN [3], [7], [9]. Some least significant bits of *SQN* are used to *KSI* (Key Set Identifier) to identify the index of AVs [6].

(5) Upon receipt, VLR/SGSN stores the received *AV*s.

(6) VLR/SGSN selects the next unused authentication vector *AV*[*i*] from the ordered array of authentication vectors.

(7) VLR/SGSN sends to USIM the random challenge, *RAND*, and an authentication token for network

authentication, *AUTN*, from the selected authentication vector, *AV*[*i*].

(8) Upon receipt, the user calculates *CK*, *IK*, *RES* and *XMAC* (eXpected MAC) as depicted in Fig. 3 and authenticates network by checking if the *XMAC* is equal to *MAC* in *AUTN*.

(9) If they match, the user sends *RES* (RESponse) to VLR/SGSN via RNC.

(10) Upon receipt of *RES*, the VLR/SGSN compares it with the expected response, *XRES*[*i*], from the selected authentication vector *AV*[*i*].

(11) If they match, VLR/SGSN selects cipher key, *CK*, and integrity key, *IK*, from the selected authentication vector *AV*[*i*].

(12) VLR/SGN sends the keys to the RNC.

(13) Upon receipt, RNC stores the received keys.

If *MAC* is not equal to *XMAC* in step 8 or *RES* is not equal to *XRES* in step 10, authentication terminates as fail. After successful authentication, the user request *LAI* (Local Area Identifier) which represents the current location to network and stores it.

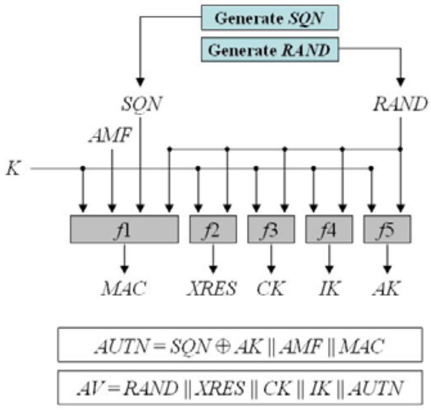
Generate SQN
Generate RAND
SQN
RAND
AMF
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN = SQN ⊕ AK || AMF || MAC
AV = RAND || XRES || CK || IK || AUTN

Fig. 2 AV Generaation at HLR/AuC

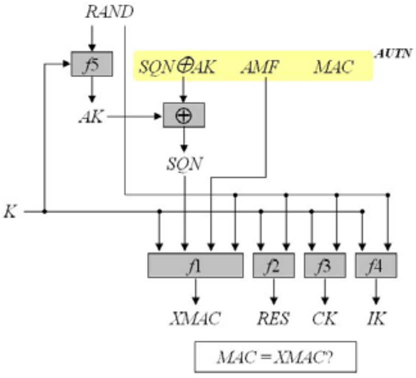

Fig. 3 AUTN Verification at USIM

3.2 EAP-AKA (Extensible Authentication Protocol-Authentication and Key Agreement)

In this section, EAP-AKA protocol [12] used in WLAN and WiBro is introduced. EAP-AKA is a EAP [11] mechanism which uses AKA as mutual authentication and key establishment protocol. EAP-AKA consists of mandatory “full authentication” protocol and optional “fast re-authentication” protocol. Fig. 4 shows the full-authentication procedure. The procedure is as follows:

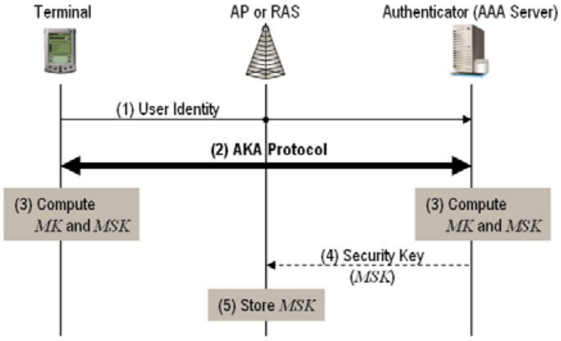

Fig. 4 Full Authentication Exchange in EAP-AKA

(1) USIM in the user's terminal sends *IMSI* [2], [9] as User Id to the authenticator, AAA (Authentication, Authorization and Accounting) server, of the service network via AP (Access Pointer) in WLAN or RAS (Radio Access Station) in WiBro. The user may send Pseudonym instead of *IMSI* to protect user's identification if this is not the first authentication.

(2) USIM and the authenticator execute AKA protocol and then, share *CK* and *IK* each other.

(3) USIM and the authenticator derive Master Key (*MK*) from the *CK*, *IK* and the identity using *SHA*1 (Secure Hash Algorithm)[17]. The Master Key is fed into a Pseudo-Random number Function (*PRF*) [16], which generates Master Session Key (*MSK*), authentication key (*Kaut*) and the encryption key (*Kencr*). Fig. 5 shows the flow of key generation.

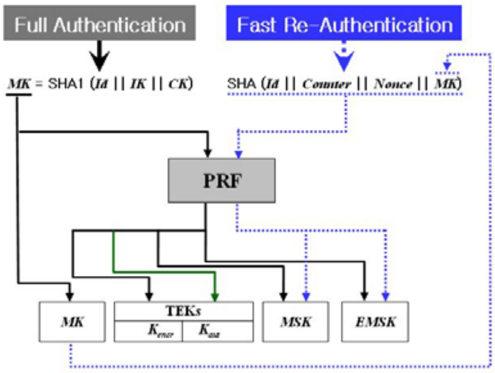

Fig. 5 Key Generation in EAP-AKA

(4) The authenticator sends the *MSK* to AP or RAS.

(5) AP or RAS stores the received *MSK*.

After successful authentication, the user request LAI which represents the location of current location to network and stores it.

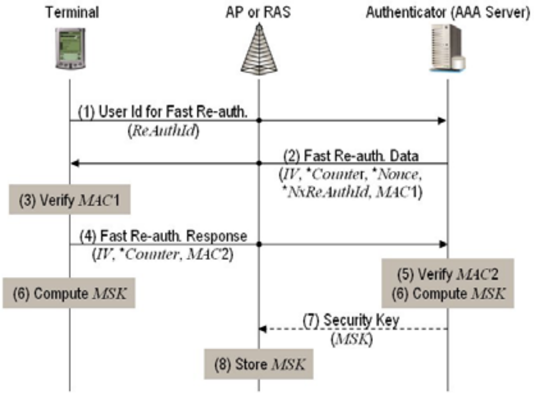

Fig. 6 Fast Re-authentication Exchange in EAP-AKA

In some environments, EAP authentication may be performed frequently. Because the EAP-AKA full authentication procedure uses the AKA algorithms, and therefore requires fresh authentication vectors from the authentication center, the full authentication procedure may result in many network operations when used very frequently. Therefore, EAP-AKA includes a more inexpensive fast re-authentication procedure that does not make use of the AKA algorithms and does not need new vectors from the authentication center. Fast re-authentication is based on the key *MK* derived on the preceding full authentication. Fig. 6 illustrates the fast re-authentication procedure. The procedure is as follows:

(1) USIM sends Identity for fast re-authentication instead of *IMSI* or psydonym to AAA server via AP or RAS to request fast re-authentication.
(2) Upon receipt, the server makes a message and sends it to the USIM via AP or RAS. The message consists of encrypted random number (*Nonce*), encrypted re-authentication counter (*Counter*), encrypted re-authentication identity (*NxReAuthId*) for the next fast re-authentication, Initialization Vector (*IV*) for encryption and the massage authentication code (*MAC*1). The encryption key is K_{encr} and message authentication key is K_{aut}. Encrypted attributes are denoted with '*' in Fig. 6.
(3) USIM authenticates the network by verifying *MAC*1.
(4) If the verification is successful, USIM makes a message and sends it to the authenticator (AAA server) via AP or RAS. The message consists of *IV*, encrypted *Counter* and message authentication code *XMAC*2.
(5) The server authenticates the user by verifying *MAC*2.
(6) If the verification is successful, the server and USIM calculate a new *MSK*. The new *MSK* is calculated using user's identity, *Counter*, *Nonce* and *MK* as in Fig. 5.
(7) The authenticator sends *MSK* to AP or RAS.
(8) AP or RAS stores the received *MSK*.

3.3 The Interworking System

Fig. 7 shows the integration model on which our protocol based. This model is proposed to minimize the modification to the current three networks models [15]. HLR/AuC is the authentication center of 3G network manages all the information needed for accounting, authentication and roaming. HLR/AuC generates Authentication Vectors (*AV*s) which are key material for authentication and security and delivers them to VLR/SGSN of 3G network and AAA server for WLAN and Wibro network. VLR/SGSN and AAA server are authenticators who perform authentication protocol with users using *AV*s delivered from HLR/AuC. Each authentication protocol is different from each service network. In 3G network, AKA [8], [9] is used, and EAP-AKA [8], [9] is used in the WLAN or WiBro. To get an integrated service from the model, a user needs to have a terminal with triple mode USIM card which supports 3G, WLAN, and Wibro. As depicted in Fig. 7, HLR/AuC uses MAP (Mobile Application Part) protocol to communicate with VLR/SGSN and AAA server uses Diameter protocol [13]. Since HLR/AuC and AAA server use different protocols, UAGS converts protocols for their communications.

4. Key Management for Interworking

The proposed key management mechanism is designed to use previously created authentication and key materials securely and efficiently when users move from one network to the other under same service provider. As users are under same service provider, HLR/AuC managing *AV*s is a common facility among three networks and one key is used between a user and the HLR/AuC. In other words, under one service provider the format of *AV* created for mutual authentication is identical. Currently when a user moves in the 3G network under one service provider, VLR/SGSN of the visited service area should transmit unused *AV* s and current keys to VLR/SGSN in the new service area [9]. However, as they use different keys from each network in a integrated system, only transmitting the current key value and the unused *AV*s can't be a solution. When moving to a new network, one can solely require to create new *AV*s to HRL/AuC and perform authentication protocol without any additional procedure. As different keys used in each network are created from same parameters, one can efficiently use the created *AV*s in the new visiting network.

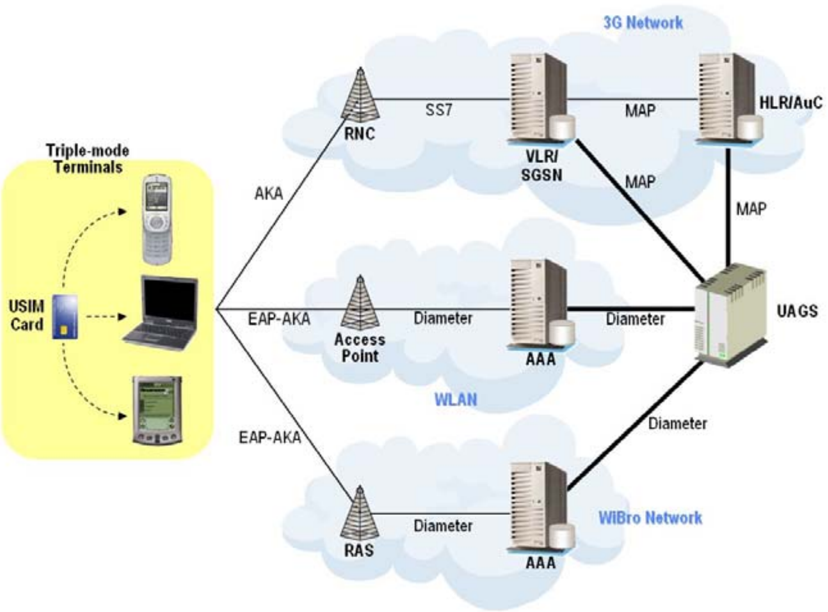

Fig. 7 The Configuration of the Interworking System

4.1 Design Overview

We designed the key management protocol for roaming being concerned about minimizing the changes of the authentication protocols AKA and EAP-AKA. Our protocol is based on some assumptions:

(1) Once an authentication protocol is started, any roaming request does not occur until the protocol succeed or failed.

(2) VLR/SGSN, AAA server and UAGS trust each other.

(3) After authentication, the USIM and authenticator (VLR/SGSN or AAA server) cache the last keys (*CK*, *IK* and/or *MSK*), *KSI* and the location information, *LAI*, until they are changed.

(4) Except the wireless link between user and RNC, AP or RAS, all other links are adequately secure.

(5) RNC, AP and RAS have capabilities to generate random numbers, to calculate message authentication codes and to verify message authentication codes.

The design ideas to satisfy the requirements in Sec. 2 are as follows:

(D1) To reduce the computation loads and communication loads of HLR/AuC, the unused *AV*s in the VLR/SGSN or the AAA server of the last visited network are sent to the VLR/SGSN or the AAA server of the visiting network.

(D2) To minimize the computation loads of user, the used keys in the last visited network or key materials to derive the used keys are sent from the authenticator of the last visited network to the authenticator of the visiting network. The three networks use *CK* and *IK* or *MSK* derived from *CK* and *IK*. Therefore, last used *CK*, *IK* and the information for the fast re-authentication in EAP-AKA should be transferred.

(D3) The network identifies the *CK* and *IK* which are stored in the USIM using *KSI*.

(D4) By exchanging a message authentication code using the shared authentication key, the user and RNC, AP or RAS verify that their partner has the correct keys.

(D5) The message for message authentication code of (D4) should include a fresh random number to protect replay attack.

(D6) UAGS has capability to pass the authentication information from the last visited network to the visiting network.

(D7) After successful roaming, the user stores the new location information in USIM for the next roaming.

(D8) UAGS maintains a database by which it can identify the VLR/SGSN or the AAA server corresponding to the location information sent from the roaming user.

(D9) The *LAI* of the VLR/SGSN or AAA server of the serving network is used as the user's location information.

Table 1 shows the design ideas to satisfy the requirements.

Table 1: Requirements and Design Ideas

Idea Req.	D1	D2	D3	D4	D5	D6	D7	D8	D9
R1	√					√	√	√	√
R2		√				√	√	√	√
R3			√	√					
R4		√				√	√	√	√
R5	√	√	√			√	√	√	√
R6				√	√				

4.2 The proposed protocol

We designed the key management protocol by extending EAP-AKA [12] and AKA [8], [9] for consistency with these authentication protocols and for easy implementation. When a user moves to another network, the key management protocol for roaming triggered by the "Roaming Request" message from the user to the new authenticator. Fig. 8 shows the proposed protocol. The procedure of our protocol is as follows:

(1) When the user moves to a different network, the USIM sends "Roaming Request" message to the new authenticator of the visiting network, VLR$_n$/SGSN$_n$ or AAA$_n$, via RNC, AP or RAS. The message contains *Id* and *LAI*$_o$. *Id* represents the user's identity and *LAI*$_o$ represents the location information of the last visited network. The *Id* may be pseudonym or *TMSI* used in the last visited network.

(2) Upon receipt, the new authenticator passes it to UAGS to authenticate the user and to receive the unused authentication vectors.

(3) UAGS recognizes the old authenticator, AAA$_o$ or VLR$_o$/SGSN$_o$, of the last visited network from *LAI*$_o$ and sends the received *Id* to the old authenticator.

(4) AAA$_o$ or VLR$_o$/SGSN$_o$ searches the *Id* from its database. If the authenticator cannot find the *Id*, the roaming fails. If the authenticator finds the *Id* then it sends information corresponding to the user to VLR$_n$/SGSN$_n$ or AAA$_n$ via UAGS. The information contains:

- *IMSI*: user's permanent identity
- *AV*s: unused *AV*s if they remain
- *CK*, *IK* and *KSI*: current *CK*, *IK* and *KSI* associated with these keys
- *IdType*: flag to identify which identity was used to calculate *MK*
- *MSK*: the last *MSK* value in EAP-AKA
- *Counter*, *NxReAuthId*: values for fast re-authentication in EAP-AKA

(5) When the visiting network is WLAN or WiBro, AAA$_n$ computes *MSK*, K_{encr} and K_{aut} using *CK*, *IK* and *Id* as in Fig. 5. If the computed *MSK* is not equal to the received *MSK*, the received *MSK* was computed by fast re-authentication. Therefore, AAA$_n$ may store the received *MSK* instead of the computed *MSK*.

(6) VLR$_n$/SGSN$_n$ or AAA$_n$ sends the new location information *LAI*$_n$ and keys to RNC, AP or RAS. When the visiting network is WLAN or WiBro, AAA$_n$ sends *KSI*, *MSK*, K_{encr} and K_{aut}. When the visiting network is 3G, VLR$_n$/SGSN$_n$ sends *KSI*, *CK* and *IK*.

(7) RNC, AP or RAS stores the received values.

(8) RNC, AP or RAS makes the "Key Confirm Request" message which contains the received *KSI*, *LAI*$_n$ and a *RN* (Random Number). And then, it attaches the message authentication code, *MAC*1, for that message. When the visiting network is WLAN or WiBro, K_{aut} may be used to calculate *MAC*1. When the visiting network is 3G, *IK* may be used to calculate *MAC*1.

(9) RNC, AP or RAS sends the message to USIM.

(10) Upon receipt, USIM checks if the received *KSI* is equal to the *KSI* stored in USIM and verifies *MAC*1. If the *KSI* is mismatched or the *MAC*1 verification failed, the roaming fails.

(11) Otherwise, USIM makes "Key Confirm Response" message which contains the received *RN* and *MAC*2. *MAC*2 is the message authentication code for *RN* using *IK* or K_{aut}.

(12) USIM sends the message to RNC, AP or RAS.

(13) Upon receipt, RNC, AP or RAS verifies *MAC*2. If the verification fails, the roaming fails.

(14) Otherwise, RNC, AP or RAS sends "Roaming Success" message to the USIM.

(15) Upon receipt, USIM stores *LAI*$_n$ as a new location information.

After successful roaming, the USIM and RNC, AP or RAS share the security keys for authentication and ciphering.

5. Analysis

The proposed protocol is designed to sends unused *AV*s to the new authenticator of the visiting network and let the user use the old keys without any additional authentication procedure. This protocol doesn't decrease the security of the authentication protocols whereas increases the efficiency by reducing the number of calculation and amount of data transfer of HLR/AuC in comparison to the re-performing the authentication protocol.

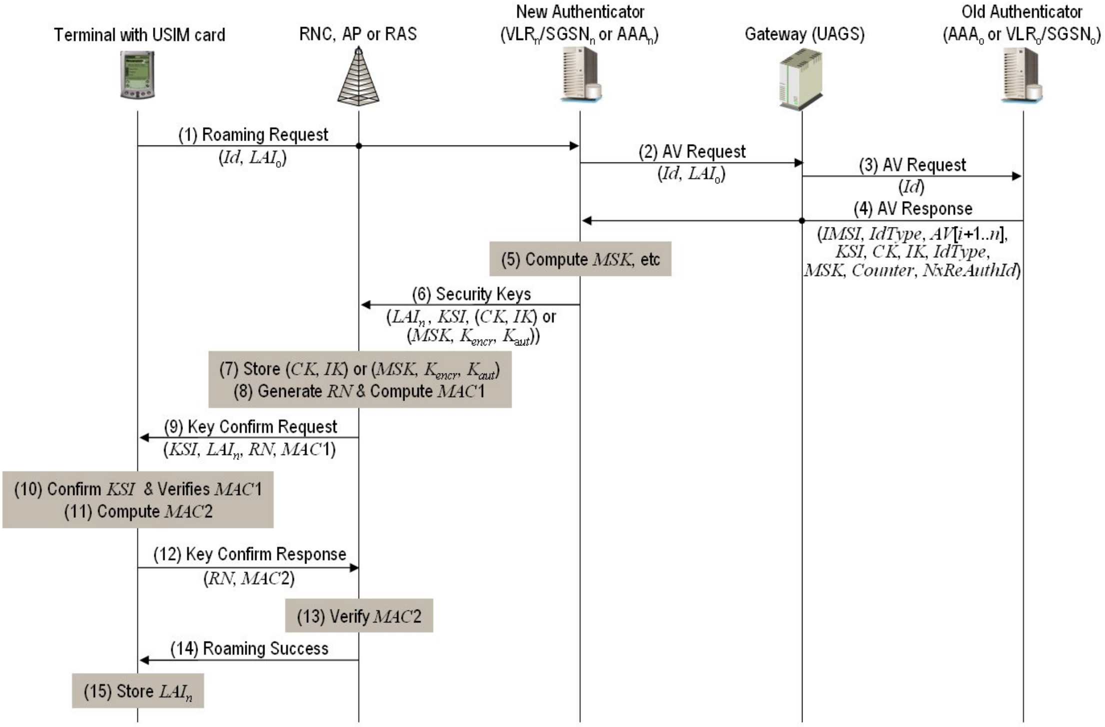
Terminal with USIM card
RNC, AP or RAS
New Authenticator ($VLR_n/SGSN_n$ or AAA_n)
Gateway (UAGS)
Old Authenticator (AAA_o or $VLR_o/SGSN_o$)
(1) Roaming Request
(Id, LAI_o)
(2) AV Request
(Id, LAI_o)
(3) AV Request
(Id)
(4) AV Response
($IMSI$, $IdType$, $AV[i+1..n]$, KSI, CK, IK, $IdType$, MSK, $Counter$, $NxReAuthId$)
(5) Compute MSK, etc
(6) Security Keys
(LAI_n, KSI, (CK, IK) or (MSK, K_{encr}, K_{aut}))
(7) Store (CK, IK) or (MSK, K_{encr}, K_{aut})
(8) Generate RN & Compute $MAC1$
(9) Key Confirm Request
(KSI, LAI_n, RN, $MAC1$)
(10) Confirm KSI & Verifies $MAC1$
(11) Compute $MAC2$
(12) Key Confirm Response
(RN, $MAC2$)
(13) Verify $MAC2$
(14) Roaming Success
(15) Store LAI_n

Fig. 8 The Proposed Key Management Protocol for Raomaing

5.1 Security Analysis

In this section, we analyze the proposed protocol based on the security requirements of EAP-AKA.

(1) Identity privacy
In the authentication protocols, AKA and EAP-AKA supports user identity privacy except when the first authentication is executed. Because the user sends permanent identity in cleartext at the first authentication and from the second authentication user identity is protected by sending one-time pseudonym or *TMSI*. The proposed protocol doesn't use permanent identity but uses pseudonym or *TMSI* because it only deals with a case that a user moves after he/she already performs authentication for one or more times. In consequence, the proposed protocol leads to the user identity privacy.

(2) Mutual authentication
The proposed protocol is a key management protocol which deals with a case when a user moves to another network after it performs mutual authentication. So, it is appropriate to analyze whether it is possible for unauthenticated user or improper authenticator to masquerade themselves as an authenticated user or a proper authenticator. As a user may possess several key sets, authenticator informs the user which key set should be used by sending the current *KSI*. And then, by sending a message each other with its authentication code calculated by *IK* or K_{aut} associated with the *KSI*, the user and the authenticator authenticate each other.

(3) Flooding AuC
As every authenticator gets *AV*s from HLR/AuC, HLR/AuC can be vulnerable to denial of service attack. As EAP-AKA standard recommends to limit traffic from/to AuC. The proposed protocol doesn't produce additional HLR/AuC calculations by sending unused *AV*s to the authenticator in the visiting area when an user moves across the networks. And it prevents authenticators from making traffic overhead to HLR/AuC by sending *AV*s via UAGS. The main feature of UAGS is converting protocols on messages between AAA servers and HLR/AuC. As the loads of UAG is less than the loads of HLR/AuC which deals with major calculation of authentication, it can lead to traffic load balancing.

(4) Replay protection
Proposed protocol assumes that there can be more than two roamings between two successive authentications. As described in "(2) mutual authentication", user and network create authentication codes on messages with the shared integrity key, *IK* or K_{aut} which are updated only when authentication protocol is performed. When the second roaming occurs without performing authentication protocol after the first one, the same *KSI* and integrity key are used. For that reason, if proposed protocol generates

identical MAC values in step 8 and 11, replay attack may be possible. To prevent that, whenever a user requests roaming, RNC, AP or RAS generates a fresh random value, *RN*, and calculates the *MAC*1 including the *RN*. The user also replies with *MAC*2 including the *RN* as well. Therefore, replay attack due to roaming is prevented.

(5) Man-in-the-middle attack
AKA and EAP-AKA, the standard of authentication and key agreement protocol require integrity protection in physically insecure networks to avoid man-in-the-middle attack and session hijacking. The proposed protocol is designed based on the assumption of AKA and EAP-AKA. Hence, as described in section 4.1, it is assumed that every communication links except for the wireless link between user and RNC, AP or RAS are adequately safe. Data transmitted via the wireless link are *KSI*, location information and the fresh *RN* which are not secret. The user and the RNC, AP or RAS tag authentication code with the key which is shared only between them. Therefore, man-in-the-middle attack in the wireless link is not possible.

5.2 Efficiency Analysis

In this section, through efficiency analysis we show that proposed protocol enhances efficiency compared to the case that performs authentication protocol when a user moves across different networks. Efficiency is analyzed by the amounts of communications and the number of calculations with aspect of HLR/AuC, UAGS and user. Also we analyze the amount of generated *AV*s that is a key feature of efficiency.

(1) HLR/AuC
The interworking system on which the proposed protocol based is a centralized model. That is, a HLR/AuC generates authentication information to support integrated authentication. As increase of amount of communications and calculations of HLR/AuC leads to the degrade of performance of the system and vulnerability to a denial of service attack. For efficiency, HLR/AuC generates up to 5 *AV*s and sends them to authenticators in one time. The authenticators use stored *AV* s without communicating with HLR/AuC for five times [3], [7], [9]. When 5 *AV*s stored in VLR/SGSN (or AAA server) from the visited network are all used up and current keys are all expired, HLR/AuC must generate new *AV* s and sends them to authenticator of the visiting network to perform an authentication protocol. In this case, the proposed protocol is not necessary. However, when unused *AV* s remain in the authenticator of visited network, our protocol is useful. In the proposed protocol, as the unused *AV* s are transferred to the authenticator of visiting network via UAGS, HLR/AuC doesn't need to communicate with authenticator of the visiting network. Therefore, in the worst case, the efficiency of the proposed protocol is same as the efficiency where the proposed protocol is not applied. In other cases, the proposed protocol enhances efficiency in terms of the amount of communications and calculations of HLR/AuC.

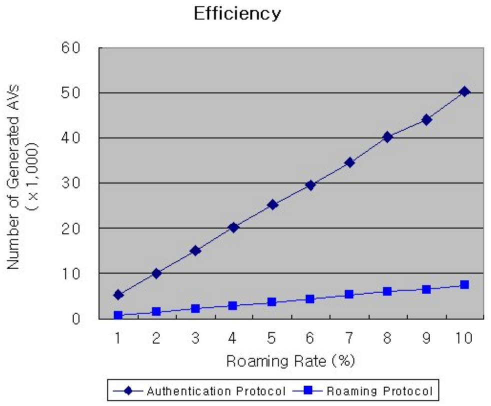

Fig. 9 The number of AVs when roaming ratio ≤ 10%

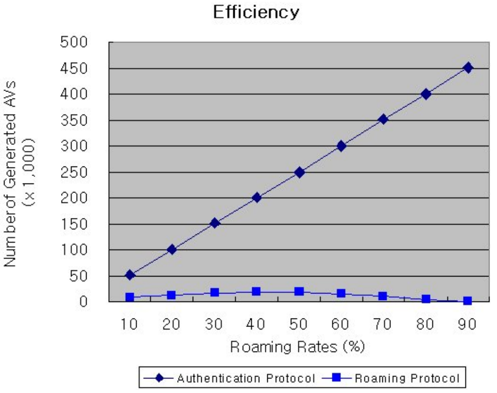

Fig. 10 The number of AVs when roaming ratio ≥ 10%

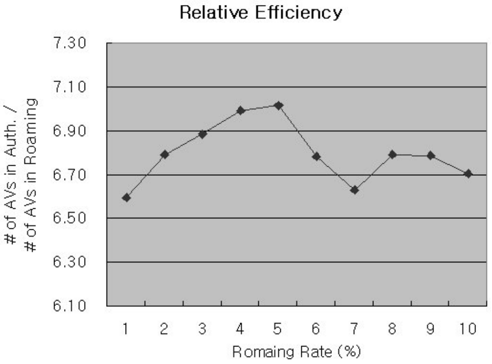

Fig. 11 The Relative efficiency when roaming ratio ≤ 10%

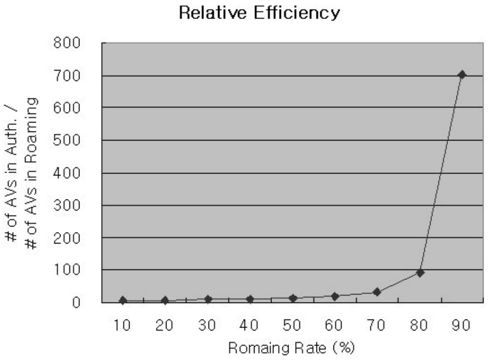

Fig. 12 The Relative efficiency when roaming ratio ≥ 10%

(2) UAGS

Consider the case that a user moves from WLAN or WiBro to 3G network. If the proposed protocol is not applied, the authenticator of the visiting network must get *AV*s from HLR/AuC directly. UAGS doesn't involve in the communication at a cost of communication and computation overhead of HLR/AuC. In other cases, even though the proposed protocol is not applied, the authenticators of the visiting network should communicate with HLR/AuC via UAGS for new *AV*s. Therefore proposed protocol doesn't create additional communication and calculation loads when UAGS involves in sending *AV*s from the visited network to the visiting network. On the other hand, it imposes communication overhead to the authenticator of the visited network to pass the unused *AV*s. However as the major function of authenticators is to reduce the load of HLR/AuC, it is reasonable.

(3) User

In the proposed protocol, a user only calculate MAC to show that he owns correct keys and verifies MAC from the authenticator to make sure the authenticator owns correct keys without newly calculating *CK* and *IK*. As calculation and verification of MAC is a necessary process in authentication protocol, the proposed protocol doesn't increase the amount of communications and reduce the amount of calculations compared to executing the authentication protocols. Moreover the proposed protocol reduces the amount of communications between RNC, AP or RAS and authenticator.

(4) Amount of Authentication Vectors

The number of generated *AV*s not only reflects the amount of computations of HLR/AuC but also is directly related to the amount of communications between user and authenticator and between HLR/AuC and authenticator. We analyze the amount of *AV* s according to the roaming ratio of user through simulation. Simulation environment and scenario are as follows: 10,000 users are randomly distributed across 3 different networks. HLR/AuC generates five *AV*s at a time. 100,000 roamings or authentications are made. When authentication protocol is executed, one of unused *AV*s is used. When roaming occurs, it is dealt in two ways: one authentication protocol is executed or the proposed protocol is executed. When an authentication protocol is executed, new *AV*s are generated even though unused *AV*s remain in the authenticator of the visited network. When the proposed protocol is executed, the unused *AV*s are sent to the authenticator of the visiting network. In this simulation, we count the number of generated *AV*s in each case. When the proposed protocol is used, it is natural that less number of *AV*s are generated because it doesn't spend any *AV*. However the efficiency varies according to the number of unused *AV*s at the time of roaming. The roaming user is chosen randomly and the visiting network is selected randomly too. Simulation is analyzed according to the ratio of (the number of roaming)/(the number of roaming + the number of authentication). Roaming ratios are set as 1%, 2%, ..., 10%, 20%, ... 90%. Fig. 9 and 10 show the number of *AV*s according to the ratio of roaming occurrence. Fig. 11 and 12 show the relative number of *AV*s generated. Fig. 9 and 10 show that the number of *AV* s is the highest when the roaming ratio is 50%. Fig. 11 and 12 show as roaming ratio increases, efficiency is enhanced. When the roaming ratio is over 70%, the efficiency increases dramatically.

6. Conclusion

3G telecommunication service provides high mobility and WLAN provides high speed and low cost. However 3G service has high cost and low speed and in case of WLAN it has poor mobility. To merge both high speed and mobility WiBro is proposed and to give coherent service for users integrated system is proposed. Each network must perform authentication protocol for security and accounting. And to integrate different networks there needs to have a way to integrate different authentication systems and protocols. In this paper, key management protocol is proposed to provide roaming and authentication when a user move across different network under the same service provider. And it has a feature of not degrading the security and reducing the communication load and the calculation load of HLR/AuC.

Acknowledgment

This work was supported by the IT R&D program of MIC/IITA. [2006-S-041-02, “Development of a common security core module for supporting secure and trusted service in the next generation mobile terminals”]

References

[1] 3GPP TR 22.934, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on 3GPP System to Wireless Local Area Network (WLAN) Interworking," 3GPP, Sep. 2003.

[2] 3GPP TS 23.003, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering Addressing and Identification," 3GPP, Jun. 2006.

[3] 3GPP TS 23.008, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Organization of subscriber data," 3GPP, Jun. 2006.

[4] 3GPP TS 23.234, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System to Wireless Local Area Network (WLAN) Interworking; System Description," 3GPP, Oct. 2006.

[5] 3GPP TS 23.934, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System to Wireless Local Area Network (WLAN) Interworking; Functional and Architectural Definition," 3GPP, Jan. 2004.

[6] 3GPP TS 24.008, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Radio Interface Layer 3 Specification; Core Network Protocols; Stage 3," 3GPP, Jun. 2006.

[7] 3GPP TS 29.002, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Application Part (MAP) Specification," Jun. 2006.

[8] 3GPP TR 31.900, "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; SIM/USIM Internal and External Interworking Aspects," 3GPP, Mar. 2006.

[9] 3GPP TS 33.102, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture," Dec. 2005.

[10] 3GPP TS 33.234, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Wireless Local Area Network(WLAN) Interworking Security," 3GPP, Jun. 2006.

[11] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, "Extensible Authentication Protocol (EAP)," IETF RFC3748, 2006. 6.

[12] J. Arkko and H. Hayerinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," IETF RFC 4187, Jan. 2006.

[13] P. Calhoun, J. Loughney, E. Guttman, G. Zorn and J. Arkko, "Diameter Base Protocol," IETF RFC3588, Sep. 2003.

[14] Jongpil Kim, Jin-Hee Han, Sung-Ik Jun, "A Study on Vulnerability and the Corresponding Strategy in Wireless Interworking System," NCS 2005, pp.13-16, 2005. 12.

[15] Jeong-Woo Lee, Sung-Ik Jun, "Design of the USIM Access Gateway System for Integrated Authentication based on the USIM," NCS 2005, pp.17-21, 2005. 12.

[16] National Institute of Standards and Technology, "\Federal Information Processing Standards (FIPS) Publication 186-2 (with change notice); Digital Signature Standard (DSS)," NIST, Jan. 2000.

[17] National Institute of Standards and Technology, "Federal Information Processing Standard (FIPS) Publication 180-1, \Secure Hash Standard," NIST Apr. 1995.

Taenam Cho received her B.S. and M.S. in Computer Science from Ewha Womans University, Seoul, Korea. She was a senior engineer of Electronics and Telecommunications Research Institute, Korea. She is now a assistant professor in Department of Information Security in Woosuk University and a visiting researcher in Electronics and Telecommunications Research Institute (ETRI). Her major interests are key management, network security, mobile communication and trusted computing groups (TCG).

Jin-Hee Han received her B.S. in Information and Telecommunications from Soong Sil University, M.S. in Information and Telecommunications from the Gwang-ju Institute of Science and Technology.

She is now a senior researcher in Division of Information Security in Electronics and Telecommunications Research Institute (ETRI). Her research interests include smart card, USIM card, cryptographic algorithms, securities for wireless networks and trusted computing groups (TCG) software stack.

Sung-Ik Jun received his B.S. ans M.S. in Department of Computer Science from Chung-Ang University.

He is now a principal research engineer and a team leader in Division of Information Security in Electronics and Telecommunications Research Institute(ETRI). His research interests include smart card, information security, wireless network security, realtime operating systems and trusted computing groups (TCG)