EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH **Open Access**

A fast iterative localized re-authentication protocol for UMTS-WLAN heterogeneous mobile communication networks

Shen-Ho Lin[1*], Jung-Hui Chiu[1] and Sung-Shiou Shen[2]

Abstract

UMTS-WLAN heterogeneous mobile networks allow a single mobile user with different radio technologies to access different mobile networks, but how to secure such interworking networks and provide a seamless service is a new challenge. Even if EAP-AKA protocol provides authentication services in UMTS-WLAN interworking networks, a fast re-authentication of EAP-AKA protocol still cannot overcome high re-authentication delays and delay-sensitive applications. Because a mobile user is authenticated by a remote RADIUS or a HLR/HSS both resided in 3G-UMTS home networks whatever a full authentication or a fast re-authentication is occurred. It causes that huge re-authentication session loads and cryptographic operation loads concentrated on the RADIUS and the HLR/HSS. In addition, such an inefficient authentication/re-authentication protocol also causes long authentication/re-authentication latency. Therefore, this article proposes a novel protocol named fast iterative localized re-authentication (FIL re-authentication) to replace the fast re-authentication of EAP-AKA protocol. The proposed protocol not only has minor modifications to attain the same security level as EAP-AKA, but it uses both localized re-authentication process and iterative process within the AP to handle the fast re-authentication locally and iteratively for speeding up the re-authentication. Additionally, the IEEE 802.11 WLAN simulation mode based on Network Simulator 2 is used for proving a valid implementation and for analyzing the performance of the proposed protocol. It shows superior results in comparison to the existing EAP-AKA protocol.

Keywords: authentication, 3G/UMTS-WLAN, EAP-AKA, HLR/HSS, RADIUS, access point

1. Introduction

Currently, the demands for broadband wireless access to IP services between different wireless and mobile communication networks are increased rapidly. IP backbone constituted a core network for heterogeneous mobile communication networks become the major goal in the next generation wireless and mobile communication networks. The heterogeneous mobile communication network aims to provide seamless services for the mobile user (MS) roaming across different mobile communication networks. In various types of heterogeneous mobile networks, 3G/UMTS-WLAN is one of main representatives today. The general architecture of 3G/UMTS-WLAN heterogeneous mobile networks is depicted in Figure 1 [1-6]. As a result of different radio access technologies, 3G/UMTS wireless cellular systems provide high mobility with wide area coverage, but with a low data transmission rate. On the other hand, WLAN mobile communication systems offer high data rates with low mobility over smaller areas.

Because the heterogeneous mobile communication network requires a high reliability for access authentication, mobility managements, seamless handovers and quality of service guarantee, access authentication especially. Thus, the integration and interoperability issues of different authentication protocols become new challenges [2-13]. In 3G/UMTS-WLAN heterogeneous mobile networks, 3GPP adopts the EAP-AKA protocol proposed by Internet engineering task force (IETF) to provide security and authentication services [14]. It provides a 'challenge-response' mutual authentication based on AKA-based security mechanism between the Home

* Correspondence: marcular@gmail.com
[1]Department of Electrical Engineering, Chang Gung University, No. 259, Wunhua 1st Rd., Gueishan Township, Taoyuan County 333, Taiwan, ROC
Full list of author information is available at the end of the article

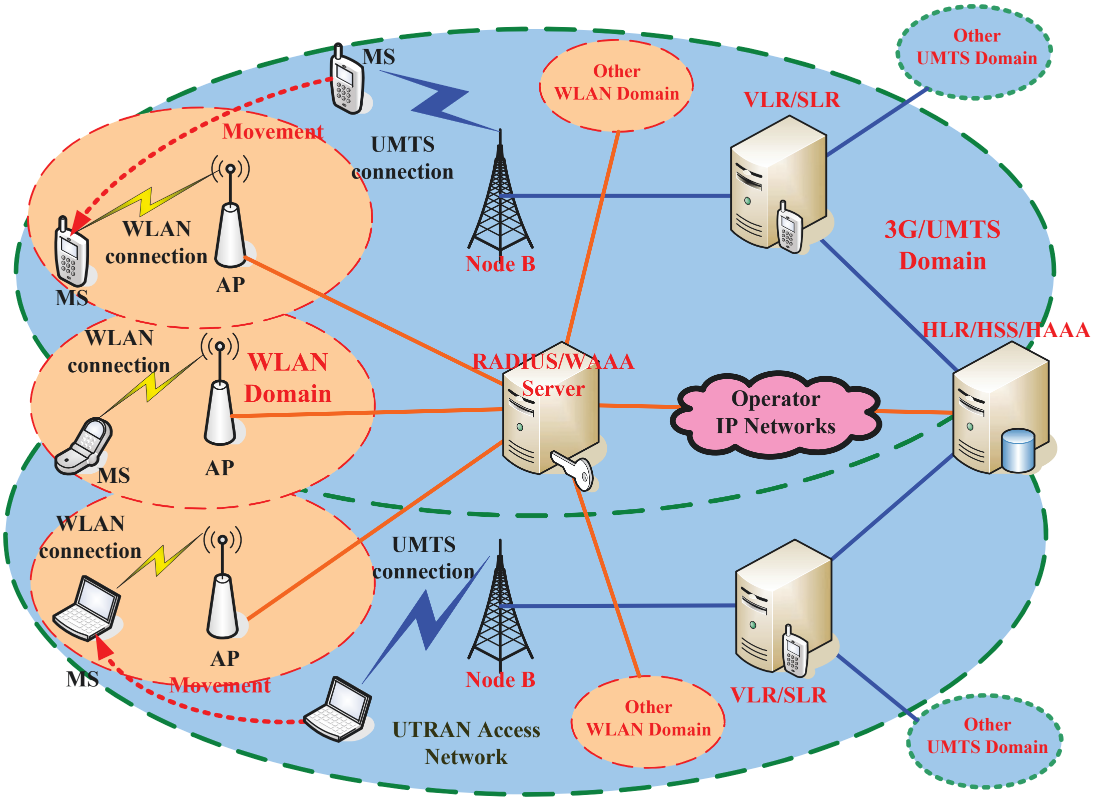

Figure 1 3G/UMTS-WLAN Heterogeneous Mobile Networks.

Location Registry/Home Subscriber Server (HLR/HSS) located in the 3G/UMTS Home Network (3GHN) [1-3,13,14] and the WLAN MS. In addition, when mutual authentication operation is completed, the HLR/HSS delivers related authentication vectors (AVs) to the RADIUS or authentication, authorization and accounting (AAA). Subsequently, an end-to-end secure session between the the RADIUS and the UE can be established to secure wireless links.

In general, EAP-AKA protocol invokes periodically and frequently in 3G/UMTS-WLAN heterogeneous mobile networks, while connection requests are launched, while temporary connection services interrupt, or as a result of intra-domain handovers and inter-domain handovers. Once any condition is occurred, EAP-AKA full authentication must be set up between the HLR/HSS and the MS to secure wireless links. It causes multiple rounds of message transactions traveling between the 3G/UMTS domain and the WLAN domain. As long as a number of full authentication sessions are increased, a vast amount of messages are traveling between the 3G/UMTS domain and the WLAN domain; meanwhile, a huge amount of process loads are taken place in the HAAA and in the HLR/HSS. Such drawback greatly influences authentication efficiency. Furthermore, EAP-AKA adopts the fast re-authentication to support user re-authentication requests for providing better authentication efficiency than the full authentication. Fast re-authentication is handled by the HAAA/RADIUS server in the 3GHN when the MS require re-authenticating. Although such procedures can reduce unnecessary authentication-related transactions between the HLR/HSS and the HAAA/RADIUS server in the 3GHN, some drawbacks existed and need to be overcome as follows: (1) a huge amount of re-authentication sessions are concentrated on the HAAA/RADIUS server, (2) a huge amount of processing loads are concentrated on the HAAA/RADIUS server, and (3) both re-authentication session loads and processing loads in the HAAA/RADIUS server are increased due to a number of re-authentication request increases. Thus, authentication efficiency improvement comparing with the full authentication is limited [12,14].

In recent years, many articles proposed to solve authentication and re-authentication latency problems in 3G/UMTS-WLAN heterogeneous mobile communication networks. Pack et al. [15,16] and Mukherjee et al. [17] proposed predicting user's next move for pre-authenticating UE with potential target AP (TAP). Pre-authentication process makes roaming a smoother operation because authentication or re-authentication can take place in advance before it is needed to support an association, rather than waiting for authentication exchanges. Those schemes cannot predict where the MH (mobile host) moves in the future, thus the pre-authentication may be restricted to intra-domain operators, results in unnecessary authentication procedures and increases signaling overheads in the WLAN domain as a number of users increase. In addition, pro-active key distribution mechanisms using neighbor graphs to predict potential TAP are proposed by Arbaugh et al. [18], Mishra et al. [19], Kassab et al. [20], and Hur et al. [21]. Those schemes require additional authentication server to pre-distribute pairwise master keys (PMK) during a fast re-authentication session. In particular, the increase in unnecessary keys pre-distribution process becomes the primary drawback as a number of users increase. Other drawbacks are similar to references [15-17]. Other related schemes in references [22-26] are used to minimize re-authentication delays without retrieving AVs from the HLR/HSS and establish re-authentication sessions in the WLAN domain. However, those solutions must require major modifications the original EAP-AKA, or 3G/UMTS-WLAN interworking architectures or adopts other EAP-based authentication protocols instead of EAP-AKA protocol.

To reform existent drawbacks of the fast re-authentication and to enhance re-authentication efficiency, this article proposes a novel re-authentication protocol named fast iterative localized re-authentication (FIL re-authentication) to replace the fast re-authentication in EAP-AKA. The localized re-authentication implementing in 2G/GSM-WLAN heterogeneous mobile communication networks was first proposed by Lin et al [27-30]. Based on the similar interworking considerations and architectures to the 2G/GSM-WLAN heterogeneous communication networks, this article not only extends the localized re-authentication concept to 3G/UMTS-WLAN heterogeneous mobile communication networks, but it adds authentication vectors distributor (AVD) in the RADIUS server and local authentication agent (LAA) in access points (APs) for handling both the localized re-authentication process and the iterative process. The AVD is designed to deliver AV resources to related APs. The LAA is used to handle the localized re-authentication process and the iterative process. The objective of proposed authentication protocol in this paper is to expedite authenticating mobile users by completing re-authentications locally and iteratively without contacting the HAAA/RADIUS in 3GHN. Furthermore, it also provides the same level of security and performance by applying minor modifications to the existing standard security protocols and architectures in 3G/UMTS-WLAN heterogeneous mobile networks. Some advantages of proposed authentication protocol are summarizes as follows: (1) both re-authentication session loads and computing process loads concentrated on the RADIUS server are distributed to related APs, (2) unnecessary Avs message transactions between the 3GHN domain and the WLAN domain are omitted, (3) fast re-authentication sessions are executed locally and iteratively between involved APs and involved MSs, and (4) finally, the increased trend in authentication latency is lightened when a number of re-authentication requests increase.

Besides, this article also provides a proof of implementation based on Network Simulator 2 (NS-2) [31] with the IEEE 802.11 WLAN mode, and the performance evaluation in terms of authentication session time, bandwidth cost, and authentication delay show superior results in comparison to existing EAP-AKA protocol. In following sections, the standard EAP-AKA protocol is introduced. Section 3 describes the architecture and the procedure of FIL re-authentication protocol. In Section 4, the numerical analysis and performance evaluation are present. Finally, the conclusion is given in Section 5.

2. Standard EAP-AKA protocol

EAP-AKA protocol adopted by 3GPP for the 3G/UMTS-WLAN heterogeneous mobile networks could be reorganized and shown in Figure 2[14]. The authentication may be a full authentication or a fast re-authentication depended on communication status and the capability of the 3G/UMTS network and the MS. In general, the fast re-authentication session must be occurred after a completed full authentication session. During the full authentication session, four network entities are involved in operating security-related functions included authentication (identity authentication and HMAC authentication), AV generation, key generation, SQN-synchronization and encryption. On the other hand, the fast re-authentication session does not need to retrieve new AVs from the HLR/HSS, thus only the HLR/HSS is not participated in operating five security-related functions, authentication (identity authentication and HMAC authentication), AV and key generation, counter-synchronization and encryption. As comparing two authentications shown in Figure 2, it is obviously that the fast re-authentication session has less message roundtrips and reduces approximate 46% authentication delays than the full authentication [12,14]. Because the proposed FIL re-authentication protocol in this article is modified to the fast re-authentication in EAP-AKA protocol, only security-related function aspects of the fast re-authentication are explored in the following, and the other detailed aspects of the full authentication can be referred to EAP-AKA protocol, RFC 4187 [14].

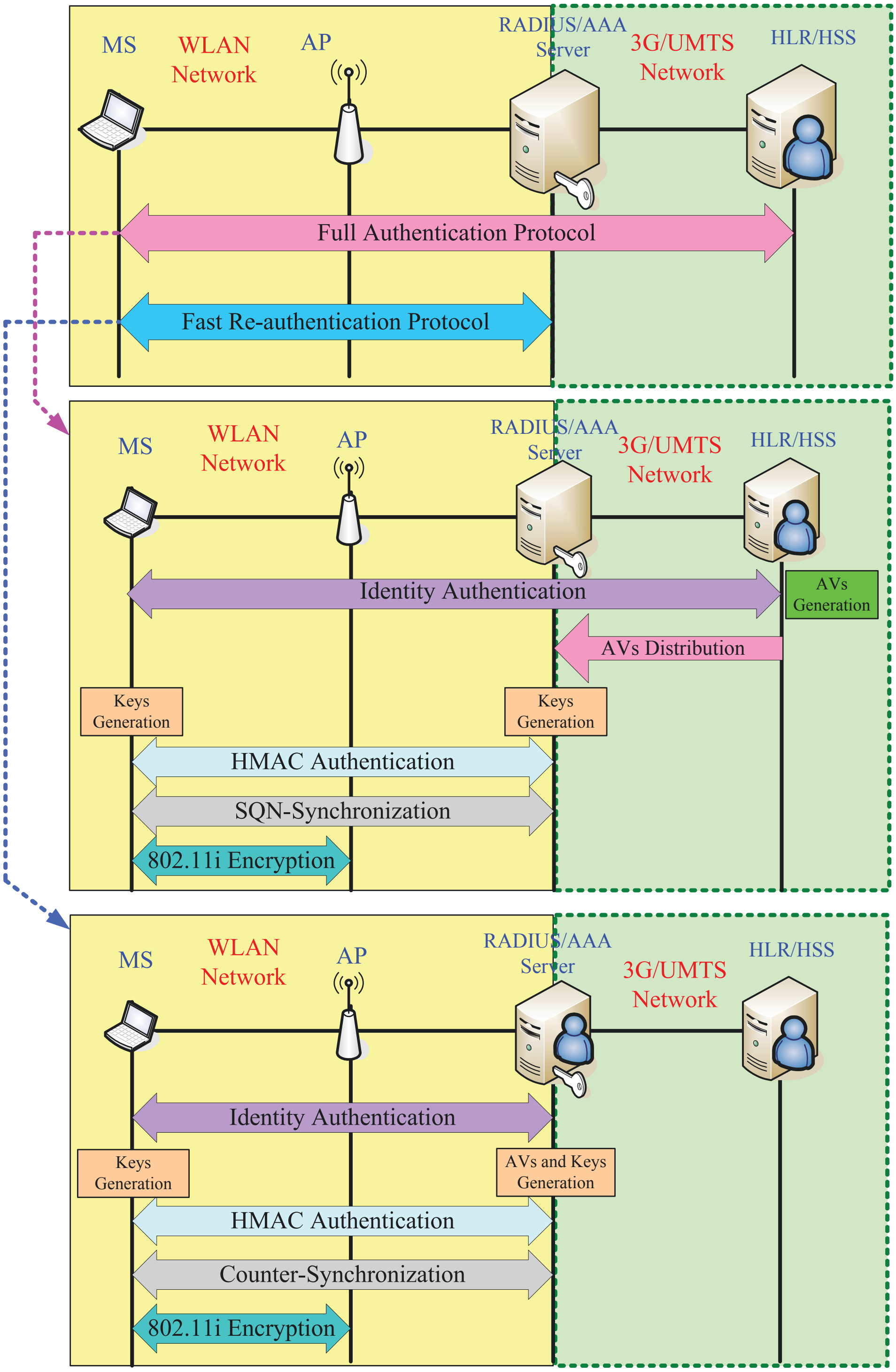

Figure 2 Standard EAP-AKA protocol.

2.1. Identity authentication

Invoking an authentication at the beginning of a communication session is inevitable. When completing a full authentication, some authentication-related attributes, such as master key (MK), K_encr, K_auth, and temporary fast re-authentication identity have already been stored in the RADIUS server and in the MS, respectively. As requesting a re-connection again, the MS must provide its temporary fast re-authentication identity used to support the privacy of subscriber permanent identity to the RADIUS server. Then the RADIUS server can recognize the identity as a legal UE by using the network access identifier (NAI) mechanism [14].

2.2. AVs and keys generation

As receiving the legal fast re-authentication identity, AVs and keys generation procedures must be activated in the RADIUS server for generating new AVs included new fast re-authentication identity, Nonce_S, and Counter_S attributes. The new fast re-authentication identity is used for the next fast re-authentication session and also used to support the privacy of identity. The Nonce_S is a random attribute for protecting replay attacks. The Counter_S is a sequence attribute for limiting the number of successive re-authentication exchanges and for protecting the RADIUS server and the MS from replays. Next, when the RADIUS server has available AVs, key generation procedures are launched immediately. First, old fast re-authentication identity, Nonce_S, Counter_S, and MK are used as seeds to generate new MK (XKEY) key calculated as XKEY = SHA-1 (fast re-authentication identity || Counter_S || Nonce_S || MK) where '||' denotes a concatenation operation. Then the XKEY is fed into the PRF function to generate new key sets (K_auth and K_encr). The overall attributes generated in this operation must be saved back to the RADIUS server database. In addition, some attributes contained the fast re-authentication identity, the Nonce_S and the Counter_S are protected by the AES algorithm and forwarded to the intended MS via the involved AP. As the MS receives available attributes, then the same attributes (XKEY, K_auth, K_encr, fast re-authentication identity) are acquired by using AVs and Keys generation procedures as well in the RADIUS server [14].

2.3. HMAC authentication

When completing the AV and Key generation operation, the RADIUS server and the MS apply the HMAC-SHA1-128 function to generate two message authentication codes, AT_MAC and AT_RES attributes, respectively. Furthermore, both message authentication codes are exchanged each other between the RADIUS server and the MS for providing the support of mutual HMAC authentication operations. In other words, the RADIUS server provides the AT_MAC attribute to the UE for a legal authorization. On the other hand, the MS also provides the AT_RES attribute to the RADIUS server for proofing legal access [14].

2.4. Counter-synchronization

In EAP-AKA protocol, SQN-synchronization and counter-synchronization are involved in the full authentication and in the fast re-authentication, respectively. In SQN-synchronization, the primary attribute, sequence number (SQN), is used to protect the HLR/HSS and the MS from replays and to limit the number of the full authentication sessions by mutual checking the value of SQN attribute separately stored in the HLR/HSS and in the MS. On the other hand, the dominant attribute in the counter-synchronization is the counter attribute. It is also used to generate desired key sets, to protect the RADIUS server and the MS from replays and to limit the number of successive re-authentication sessions by mutual checking the value of counter attribute separately stored in the RADIUS server and in the UE [14].

2.5. 802.11i encryption

This function is not specified in EAP-AKA protocol. However, for supporting the link layer security of the WLAN network, two encryption schemes are adopted in EAP-AKA. One is the traditional wired equivalent privacy (WEP) specified by IEEE 802.11 standards. However, some known weaknesses and vulnerabilities are suffered in the WEP today. As considering with higher level of security, the Wi-Fi protected access (WPA) specified by IEEE 802.11i is adopted by the EAP-AKA protocol. When the RADIUS has successfully authenticated the UE through the EAP-AKA mutual authentication protocol, they will share related keys, such as MK, MSK, TEK, and EMSK. The MSK is designated as pairwise mater key (PMK) and delivered to the APs. Then the AP and MS using a four-way handshake and a two-way handshake generate a pairwise transient key (PTK) and a group transient key (GTK) to support IEEE 802.11i encryption operation, respectively. Furthermore, IEEE 802.11i encryption operations include RC4 based encryption temporal key integrity protocol (TKIP) algorithm for integrity protection and advanced encryption standard (AES) algorithm counter mode CBC-MAC protocol (CCMP) for the confidentiality.

3. Proposed FIL re-authentication protocol

Invoking a full authentication or a fast re-authentication at the beginning of a communication session in EAP-AKA protocol depends on the capabilities of the authentication server and the MS and is inevitable. In addition, the authentication service indeed is occurred periodically and frequently. Thus, minimizing authentication delay can greatly improve interworking performance and provide the support of seamless service in 3G/UMTS-WLAN heterogeneous mobile communication networks. Although fast re-authentication can enhance 46% authentication efficiency than the full authentication by neglecting unnecessary authentication-related transactions between the HLR/HSS and the RADIUS [12,14], periodical fast re-authentication sessions are still handled by the RADIUS resided in the 3GHN when the MS requires a re-authentication. It is inefficient for stationary and mobile users to communicate with remote authentication server in the 3GHN whenever re-authentication is required. Meanwhile, a huge amount of re-authentication message transactions between the 3G domain and the WLAN might result in high authentication delays and might introduce unnecessary signaling and processing overhead. Such delays directly affect real-time applications and delay-sensitive applications running in 3G/UMTS-WLAN heterogeneous mobile communication networks. In addition, the impact of authentication delays is increased with a number of fast re-authentication session increases.

For improving re-authentication delays in 3G/UMTS-WLAN heterogeneous mobile communication networks, this paper proposed FIL re-authentication protocol that is based on the EAP-AKA fast re-authentication and also extends the concepts of FIL re-authentication in GSM-WLAN heterogeneous mobile communication networks [27-30] to 3G/UMTS-WLAN heterogeneous mobile communication networks. Furthermore, the AVD function in the RADIUS is responsible for the execution of MS full authentication and for delivering authentication-related messages to the LAA in the AP. The LAA take over the RADIUS to enable the MS re-authentication locally and iteratively. FIL re-authentication protocol model is depicted in Figure 3. In the figure, two major processes in the proposed model are localized re-authentication process and iterative process. In the full authentication, the AVD function is designated to distribute AV resources from the remote HLR/HSS to intended APs. When the MS requests a re-authentication access, the LAA can rederive new AVs and key sets according to received AV resources stored in the database of AP. Subsequently, the AP has sufficient AVs for handling re-authentication sessions with the intended MS locally. Such authentication operations between the AP and the MS are called as localized re-authentication process. The aim of localized re-authentication process is to decentralize re-authentication session loads and processing loads in the RADIUS server to APs. In addition, the iterative process is designed to enable the execution of localized re-authentication process iteratively and for completing re-authentications locally without contacting the RADIUS. It also contains iterative localized re-authentication and iterative AVs generation. The localized re-authentication process and iterative process are discussed in detail as follows.

3.1. FIL re-authentication protocol architecture

Figure 2 clearly shows that RADIUS server, AP and MS are participating in the fast re-authentication session. However, as comparing with Figure 4, the difference is that the fast re-authentication is replaced by the FIL re-authentication protocol performed between the AP and the MS. In Figure 4, ① represents the localized re-authentication process. ② and ③ represent iterative localized re-authentication and iterative AVs generation, respectively.

3.1.1. Localized re-authentication process

In order to explain how FIL re-authentication protocol works, the localized re-authentication process must be introduced first. The design objective of localized re-authentication process is to expedite authenticating mobile users by completing re-authentications locally without contacting the RADIUS. Note that the first round of FIL re-authentication must be activated after a successful full authentication session, and some AVs included temporal fast re-authentication identity (Fast_ID), MK, K_auth, and K_encr have been delivering to the AP's database via the AVD function during a full authentication. Fast_ID and MK attributes are used in subsequent first round iterative AVs generation of the iterative process that is introduced in the following iterative process sub-section. K_auth and K_encr keys not only are use to preserve integrity and confidentiality of EAP messages during the full authentication session, but those are responsible for preserving integrity and confidentiality of EAP messages during this round localized re-authentication process, which is also called the initial round of iterative process.

After a successful full authentication, when the MS provides its temporal Fast_ID to request a re-authentication access, the FIL re-authentication protocol is launched to trigger the localized re-authentication process so-called the initial round of the iterative process. The localized re-authentication process included some security-related functions shown in Figure 4 is executed between the AP and the MS. Upon receiving the temporal Fast_ID, the LAA first runs the identity authentication to check whether the identity is legal or not. If positive, then both the LAA and the UE runs the initial round iterative AVs generation for re-deriving new AVs, which are also stored back to its database, respectively. The iterative AVs generation details in the iterative process sub-section. By using the iterative AVs generation, the AP and the MS can acquire available AVs and key sets, which are used to enable the execution of the following security-related functions. Next, other security-related functions can be performed between the AP and the UE as well as the fast re-authentication. As the final 802.11i encryption function has been completed, it represents that this round localized re-authentication process has been finished. When the MS requests a re-authentication access to the same AP again, the FIL re-authentication protocol will be launched again to trigger

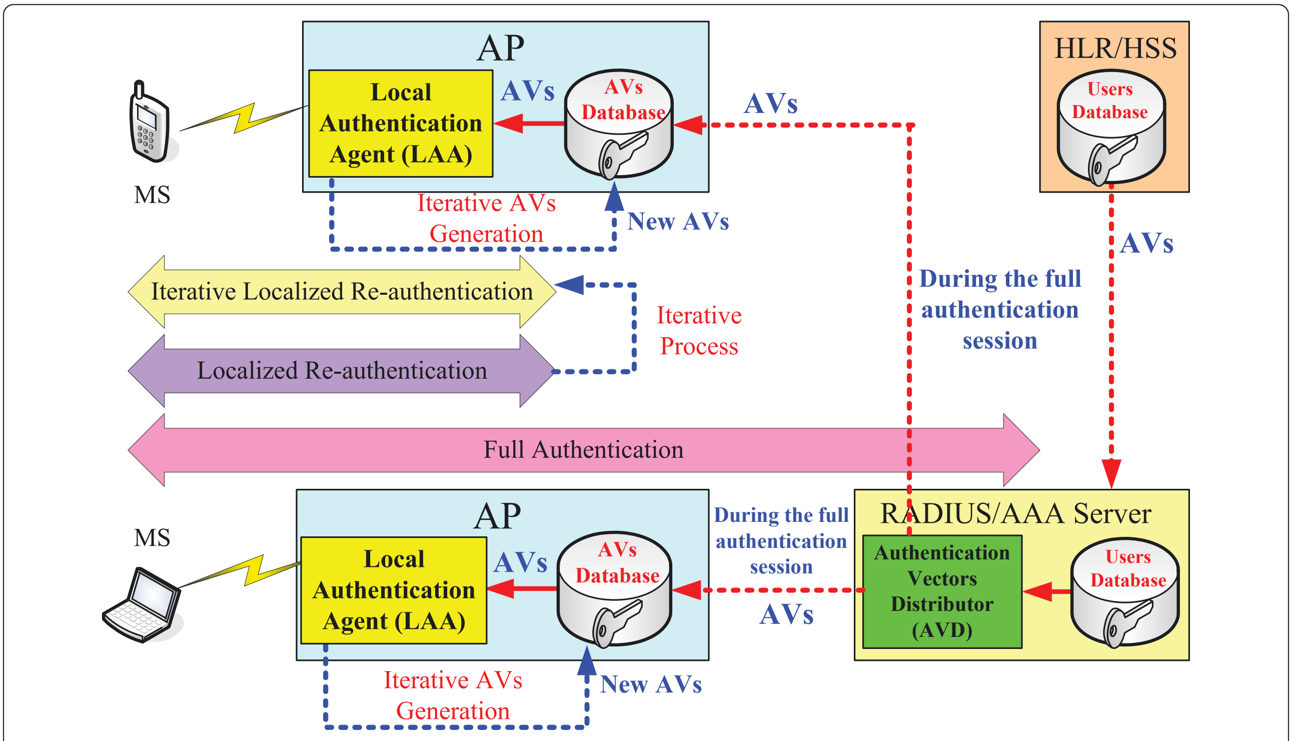
AP
Local Authentication Agent (LAA)
AVs
AVs Database
AVs
HLR/HSS
Users Database
MS
Iterative AVs Generation
New AVs
AVs
Iterative Localized Re-authentication
Iterative Process
During the full authentication session
Localized Re-authentication
Full Authentication
MS
AP
Local Authentication Agent (LAA)
AVs
AVs Database
During the full authentication session
AVs
RADIUS/AAA Server
Authentication Vectors Distributor (AVD)
Users Database
Iterative AVs Generation
New AVs

Figure 3 FIL re-authentication protocol model.

new round iterative process introduced in detail as follows. According to the above mentioned, the database of the AP not only needs to store pre-loaded AV resources that are from the AVD function during an ongoing full authentication, but it stores new AVs that are re-derived by itself during an ongoing localized re-authentication process.

3.1.2. Iterative process

In order to continue executing the localized re-authentication process between the AP and UEs without contacting the RADIUS, the iterative process is proposed to achieve this objective. In FIL re-authentication protocol illustrated in Figure 4, the iterative process represents two aspects. One is iterative localized re-authentication (②) and other is iterative AVs generation (③). Meanwhile, the iterative AVs generation is one of functions included in the iterative localized re-authentication.

3.1.2.1. Iterative localized re-authentication The previous section clearly shows one round localized re-authentication, which also represents initial round of iterative process. When the MS responses the Fast_ID(i - 1) to request a re-authentication access again where the index 'i' denotes the i-th iterative process, FIL re-authentication is invoked again for activating new round iterative process, which is so-called first round iterative process. Here, Fast_ID(i - 1) was generated by the AP during the previous iterative process. But in the first round iterative process, Fast_ID(i - 1) was from the RADIUS during the full authentication. Upon receiving the identity, the LAA runs the identity authentication function to check the identity and agrees running iterative localized re-authentication with the MS. As completing the identity authentication of this round iterative localized re-authentication, iterative AVs generation function of this round iterative localized re-authentication is subsequently invoked for deriving new AVs. The iterative AVs generation operation is shown in Figure 5 and details in the following section. The AP and the MS can acquire available AVs and key sets by using such iterative operations. Furthermore, those new derived AVs are used for enabling the execution of the subsequent security-related functions of this round iterative localized re-authentication between the AP and the MS. When the operations of other security-related functions perform as well as the localized re-authentication process and have succeeded. It represents that both this round iterative localized re-authentication and iterative AVs generation have been finished. When the MS requires a re-authentication access again, a new round iterative process is triggered for invoking a new round iterative localized re-authentication included a new round iterative AVs generation again. Accordingly, if any error has been occurred during any round iterative localized re-authentication, the iterative process is terminated immediately. Meanwhile, while the MS requests a re-connection again, the full authentication will be

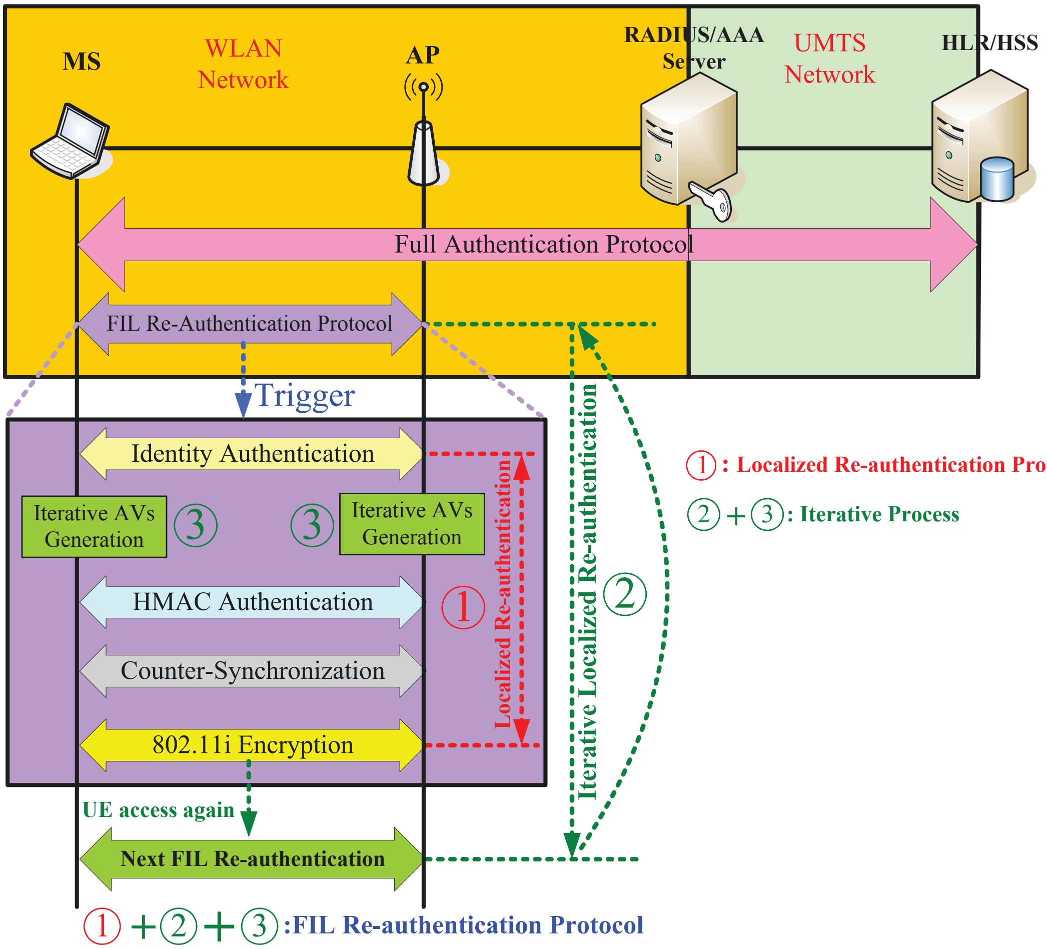
MS
WLAN Network
AP
RADIUS/AAA Server
UMTS Network
HLR/HSS
Full Authentication Protocol
FIL Re-Authentication Protocol
Trigger
Identity Authentication
Iterative AVs Generation
3
3
Iterative AVs Generation
HMAC Authentication
1
Counter-Synchronization
802.11i Encryption
Localized Re-authentication
Iterative Localized Re-authentication
2
1 : Localized Re-authentication Process
2 + 3 : Iterative Process
UE access again
Next FIL Re-authentication
1 + 2 + 3 :FIL Re-authentication Protocol

Figure 4 FIL re-authentication protocol architecture.

activated, rather than FIL re-authentication protocol. Otherwise, the iterative process is keeping on going.

3.1.2.2. Iterative AVs generation The iterative AVs generation establishes a secure AVs and key sets generation operation that results in generating fresh AVs and keys to secure the communications between the AP and the MS. Moreover, iterative localized re-authentication is completed efficiently with minimum communications between the MS and the AP. As the MS responses the Fast_ID(i - 1) to requests a re-authentication access again and demonstrates the temporal identity is valid, FIL re-authentication protocol is trigger to invoke the new round iterative process. Then the new round iterative AVs generation shown in Figure 5 is also invoked in the LAA. In Figure 5, the LAA first acquires Fast_ID (i - 1) and MK(i - 1) attributes from the its database and generates new Counter_A(i) and Nonce_A(i) attributes where the index 'i' denotes the number of iterative process. Second, for the user identity privacy in the next round iterative process, the AP also generates new temporal Fast_ID, denoted as Fast_ID(i). Then new mater key denoted as MK(i) is derived as MK(i) = SHA - 1 (Fast_ID(i - 1) || Counter_A(i) || Nonce_A(i) || MK(i - 1)). Other new key sets included K_auth(i) and K_encr (i) are also acquired by using the PRF according to MK (i) key. Finally, new key sets (MK(i), K_auth(i) and K_encr(i)), Fast_ID(i), Counter_A(i), and Nonce_A(i) attributes need to store back to the AP's database for supporting the execution of following security-related functions of this round iterative localized re-authentication and the next round iterative process. When completing above operation, it represents that one round iterative AVs generation operation has been accomplished. Subsequently, other security-related functions can be executed between the AP and the MS in order during this round iterative localized re-authentication. In the final 802.11i encryption function, new re-derived key sets results in generating fresh PTK and GTK by using a four-way handshake and a two-way handshake to support IEEE 802.11i encryption operation. As the 802.11i encryption function has been completed, it represents that this round localized re-authentication

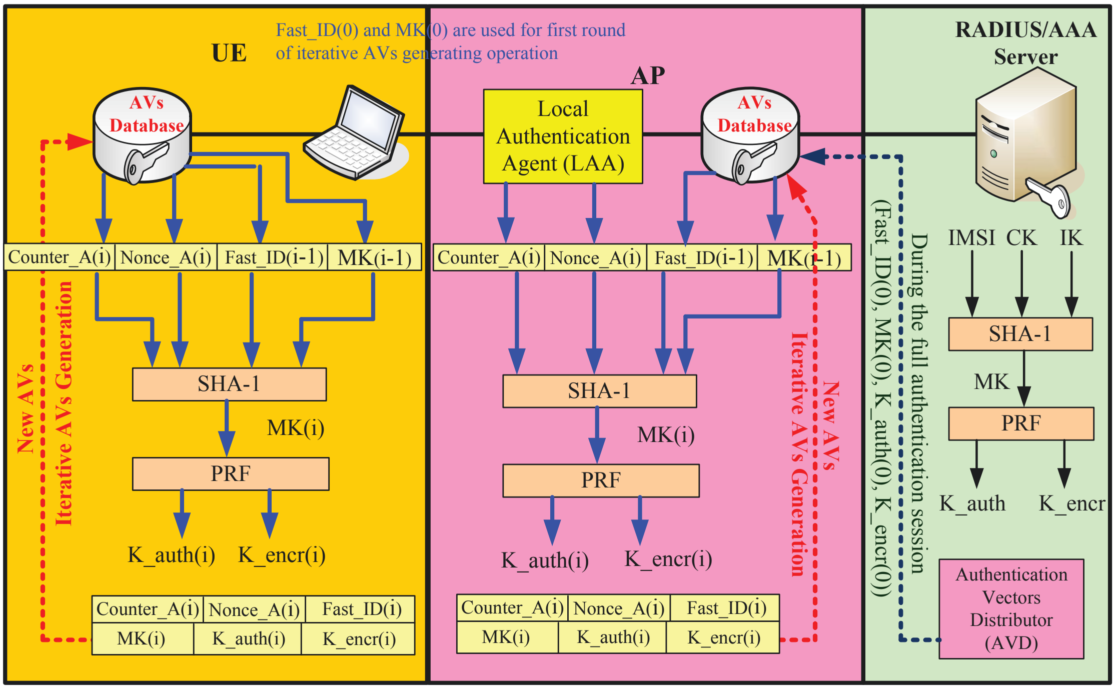

Figure 5 Iterative AVs generation operation.

has been finished. When the next round iterative process is invoked, the next round iterative AVs generation is also invoked.

3.2. FIL re-authentication protocol procedure

In this section, the sequence procedures of FIL re-authentication protocol are presented in detail. Since FIL re-authentication protocol is proposed to replace the fast re-authentication in EAP-AKA, it must be invoked after a successful full authentication session while the MS requires a re-authentication with the related APs again. The sequences are illustrated in Figure 6 and detail as follows.

3.2.1. STEP ⓪: initial state

Upon completing a full authentication, available AVs included temporal Fast_ID(i - 1), MK(i - 1), K_auth(i - 1), and K_encr(i - 1) have been stored in the AP and in the MS, respectively. It is so-called the initial state of the FIL re-authentication protocol. In the first round FIL re-authentication case, the related AVs are denoted as Fast_ID(0), MK(0), K_auth(0) and K_encr(0), respectively. Here, those AVs are generated by the RADIUS during an ongoing full authentication session.

3.2.2. STEP ①: identity authentication

When the MS sends an EAPOL-start message to request a FIL re-connection access, the AP immediately sends EAP request/identity message to the MS for running the identity authentication. Then the UE must response the Fast_ID(i - 1) to demonstrate the temporal identity is valid. Upon receiving the temporal identity, the AP first runs the identity authentication to check whether the received identity is valid. If the identity check is positive, the AP agrees on using the first round iterative localized re-authentication and also invokes the first round iterative AVs generation function.

3.2.3. STEP ②: iterative AVs generation (AP)

The symbol (AP) represents that the function operation is handled by the AP. In this function, the LAA first generates Counter_A(i) and Nonce_A(i) attributes. Then two attributes with MK(i - 1) and Fast_ID(i - 1) are used as the seeds to generate fresh key sets (MK(i), K_encr(i), K_auth(i)) by the iterative AVs generation operation shown in the Figure 5. Secondly, in order to implement the later HMAC authentication function, two message authentication code attributes (AT_MAC(i) and AT_XRES(i)) must be calculated, respectively. The AT_MAC(i) attribute is calculated as AT_MAC(i) = HMAC-SHA1-128 (K_auth(i - 1) || Nonce_A(i) || EAP message). The AT_XRES(i) attribute is calculated as AT_XRES(i) = HMAC-SHA1-128 (K_auth(i) || Nonce_A(i) || EAP message). Furthermore, for supporting the user identity privacy, the new temporal Fast_ID(i) must be generated randomly and is also used in the identity authentication and iterative AVs generation of the next round iterative localized re-authentication. Meanwhile, the temporal Fast_ID(i) is protected by an AES algorithm with K_auth(i) key and the encrypted attribute is denoted as *AT_Encr_Data(i). In addition,

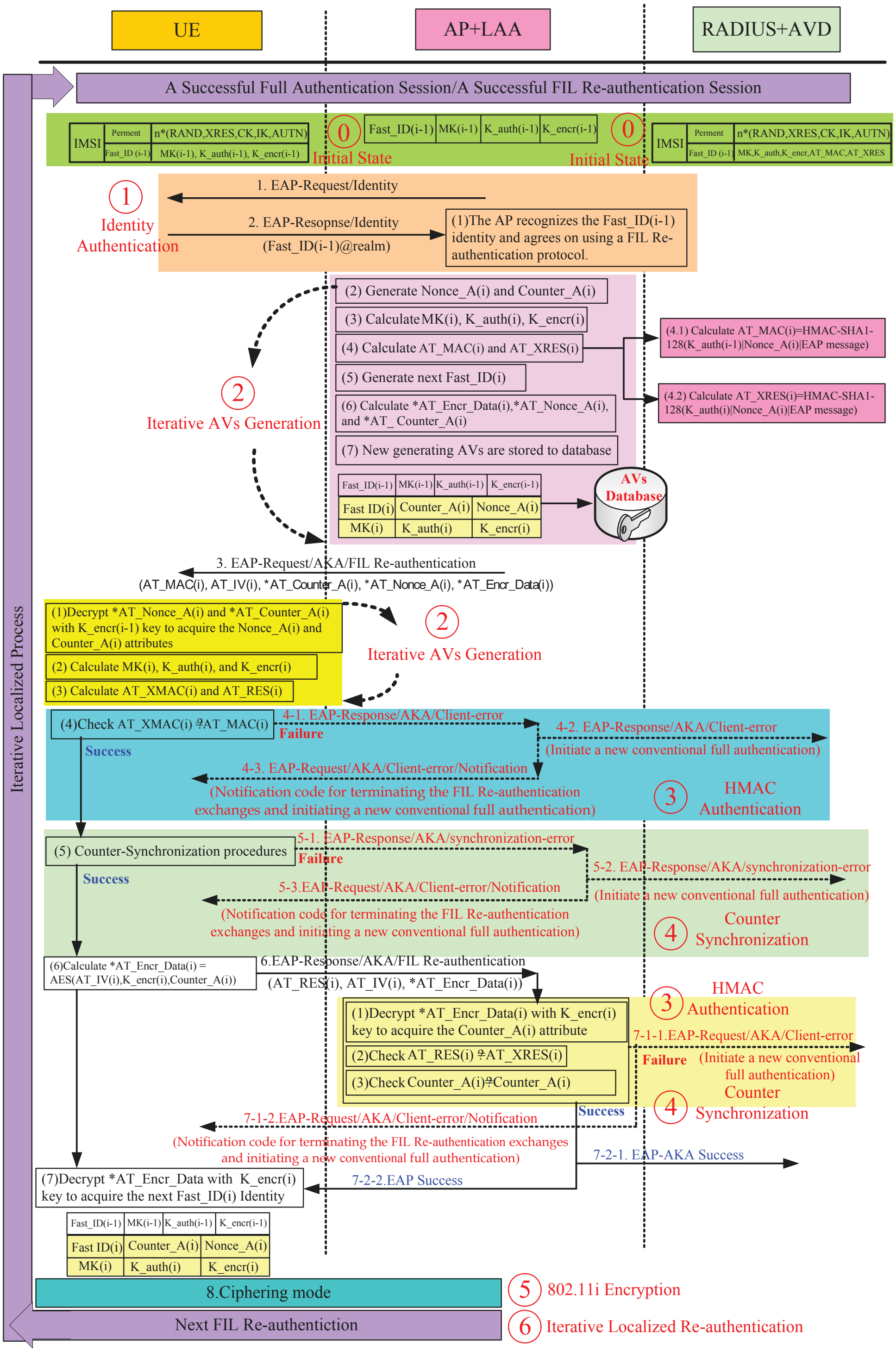
UE
AP+LAA
RADIUS+AVD
A Successful Full Authentication Session/A Successful FIL Re-authentication Session
IMSI
Perment
n*(RAND,XRES,CK,IK,AUTN)
Fast_ID (i-1)
MK(i-1), K_auth(i-1), K_encr(i-1)
0
Initial State
Fast_ID(i-1)
MK(i-1)
K_auth(i-1)
K_encr(i-1)
0
Initial State
IMSI
Perment
n*(RAND,XRES,CK,IK,AUTN)
Fast_ID (i-1)
MK,K_auth,K_encr,AT_MAC,AT_XRES
1
Identity Authentication
1. EAP-Request/Identity
2. EAP-Resopnse/Identity
(Fast_ID(i-1)@realm)
(1)The AP recognizes the Fast_ID(i-1) identity and agrees on using a FIL Re-authentication protocol.
(2) Generate Nonce_A(i) and Counter_A(i)
(3) Calculate MK(i), K_auth(i), K_encr(i)
(4) Calculate AT_MAC(i) and AT_XRES(i)
(5) Generate next Fast_ID(i)
(6) Calculate *AT_Encr_Data(i),*AT_Nonce_A(i), and *AT_ Counter_A(i)
(7) New generating AVs are stored to database
(4.1) Calculate AT_MAC(i)=HMAC-SHA1-128(K_auth(i-1)|Nonce_A(i)|EAP message)
(4.2) Calculate AT_XRES(i)=HMAC-SHA1-128(K_auth(i)|Nonce_A(i)|EAP message)
2
Iterative AVs Generation
Fast_ID(i-1)
MK(i-1)
K_auth(i-1)
K_encr(i-1)
Fast ID(i)
Counter_A(i)
Nonce_A(i)
MK(i)
K_auth(i)
K_encr(i)
AVs Database
3. EAP-Request/AKA/FIL Re-authentication
(AT_MAC(i), AT_IV(i), *AT_Counter_A(i), *AT_Nonce_A(i), *AT_Encr_Data(i))
(1)Decrypt *AT_Nonce_A(i) and *AT_Counter_A(i) with K_encr(i-1) key to acquire the Nonce_A(i) and Counter_A(i) attributes
(2) Calculate MK(i), K_auth(i), and K_encr(i)
(3) Calculate AT_XMAC(i) and AT_RES(i)
2
Iterative AVs Generation
(4)Check AT_XMAC(i) ≟AT_MAC(i)
4-1. EAP-Response/AKA/Client-error
Failure
4-2. EAP-Response/AKA/Client-error
(Initiate a new conventional full authentication)
Success
4-3. EAP-Request/AKA/Client-error/Notification
(Notification code for terminating the FIL Re-authentication exchanges and initiating a new conventional full authentication)
3
HMAC Authentication
(5) Counter-Synchronization procedures
5-1. EAP-Response/AKA/synchronization-error
Failure
5-2. EAP-Response/AKA/synchronization-error
(Initiate a new conventional full authentication)
Success
5-3.EAP-Request/AKA/Client-error/Notification
(Notification code for terminating the FIL Re-authentication exchanges and initiating a new conventional full authentication)
4
Counter Synchronization
(6)Calculate *AT_Encr_Data(i) = AES(AT_IV(i),K_encr(i),Counter_A(i))
6.EAP-Response/AKA/FIL Re-authentication
(AT_RES(i), AT_IV(i), *AT_Encr_Data(i))
3
HMAC Authentication
(1)Decrypt *AT_Encr_Data(i) with K_encr(i) key to acquire the Counter_A(i) attribute
(2)Check AT_RES(i) ≟AT_XRES(i)
(3)Check Counter_A(i)≟Counter_A(i)
7-1-1.EAP-Request/AKA/Client-error
Failure
(Initiate a new conventional full authentication)
4
Counter Synchronization
Success
7-1-2.EAP-Request/AKA/Client-error/Notification
(Notification code for terminating the FIL Re-authentication exchanges and initiating a new conventional full authentication)
7-2-1. EAP-AKA Success
(7)Decrypt *AT_Encr_Data with K_encr(i) key to acquire the next Fast_ID(i) Identity
7-2-2.EAP Success
Fast_ID(i-1)
MK(i-1)
K_auth(i-1)
K_encr(i-1)
Fast ID(i)
Counter_A(i)
Nonce_A(i)
MK(i)
K_auth(i)
K_encr(i)
8.Ciphering mode
5
802.11i Encryption
Next FIL Re-authentiction
6
Iterative Localized Re-authentication
Iterative Localized Process

Figure 6 The sequence of FIL re-authentication protocol.

Nonce_A(*i*) and Counter_A(*i*) must be encrypted by using an AES algorithm with K_auth(*i* - 1) key to prevent from masquerading and compromising. Those encrypted attributes are denoted as *AT_Nonce_A(*i*) and *AT_Counter_A(*i*), respectively. Once completing the preceding security-related parameters generation, new AVs need to stored back to its database. Then the AP immediately sends the EAP-request/AKA/FIL re-authentication message including AT_MAC(*i*), AT_IV(*i*), *AT_Counter_A(*i*), *AT_Nonce_A(*i*), and *AT_Encr_Data(*i*) to the MS.

3.2.4. STEP ②: iterative AVs generation (UE)

Upon receiving the EAP-request message, the MS first decrypts *AT_Counter_A(*i*) and *AT_Nonce_A(*i*) with K_auth(*i* - 1) key to acquire Nonce_A(*i*) and Counter_A (*i*) attributes. Then the MS performs the iterative AVs generation operations as well as in the AP to re-derive fresh key sets (MK(*i*), K_encr(*i*), K_auth(*i*)) and message authentication codes (AT_XMAC(*i*) and AT_RES(*i*)).

3.2.5. STEP ③-④: HMAC authentication and counter-synchronization (UE)

When completing iterative AVs generation and message authentication code operations, then the MS runs the HMAC authentication function to verify the calculated AT_XMAC(*i*) with the received AT_MAC(*i*) to confirm whether the AP is legal. If invalid, the MS responses an EAP-response/AKA/client-error message to the AP for terminating FIL re-authentication exchanges and for asking a new full authentication. Otherwise, the counter-synchronization function has continued performing. In the counter-synchronization function, the MS checks the value of the received Counter_A(*i*) to make sure that the number of the FIL re-authentication has not exceeded the assigned limit. The detailed counter synchronization procedures in the FIL re-authentication are as well as the fast re-authentication in the EAP-AKA [14]. In addition, in order to prevent the Counter_A(*i*) attribute from masquerading and compromising, it must be encrypted by an AES algorithm with K_encr(*i*) key and the encrypted attribute is denoted as *AT_Encr_Data(*i*). If both HMAC authentication and counter-synchronization checks are valid, the UE replies the EAP-response message included *AT_Encr_Data(*i*), AT_IV(*i*), and AT_RES(*i*) to the AP.

3.2.6. STEP ③-④: HMAC authentication and counter-synchronization (AP)

As receiving the EAP-response message from the MS, the AP first decrypts the *AT_Encr_Data(*i*) with K_encr (*i*) key to acquire the Counter_A(*i*) attribute. Then it, respectively, runs the HMAC authentication function and counter-synchronization function to verify the received AT_RES(*i*) and Counter_A(*i*) with the AT_XRES(*i*) and Counter_A(*i*) that are stored in its database. If both checks are positive, the AP sends an EAP success message to the MS. Otherwise, the AP immediately announces an authentication failure message to the RADIUS serve for requesting a new full authentication. Meanwhile, it also sends a client-error notification to the MS for terminating the FIL re-authentication exchanges and for initiating a new full authentication.

3.2.7. STEP ⑤: 802.11i encryption

Upon receiving the EAP success message from the AP, the MS can decrypt the received *AT_Encr_Data(*i*) with K_auth(*i*) key to acquire new temporal Fast_ID(*i*). Then Fast_ID(*i*) and new derived AVs are stored back to the its database. Next, the AP and the MS get into the ciphering mode. When the final encryption function is completed, it represents one round iterative localized re-authentication has been finished.

3.2.8. STEP ⑥: iterative localized re-authentication

The steps from ① to ⑤ are represented one round iterative localized re-authentication. While the MS requests a FIL re-connection again, the FIL re-authentication protocol will be activated again for triggering the next round iterative localized re-authentication.

The preceding procedures clearly show that the FIL re-authentication enables the execution of the re-authentication session between the AP and the MS locally and iteratively. It expedites authenticating mobile users by using the localized re-authentication process and the iterative process. The localized re-authentication process is designated to the support of the local re-authentication, which results in distributing re-authentication session loads and processing loads. The iterative process is designated to enable the execution of localized re-authentication process iterative, which contributes to complete re-authentications iteratively without contact the RADIUS. Based on those advantages, the re-authentication efficiency can be obviously improved as comparing the FIL re-authentication with the standard fast re-authentication and the standard full authentication, respectively. For validating the re-authentication efficiency in the FIL re-authentication, the numerical analysis and performance evaluations about the authentication session time, bandwidth cost, and authentication delays are given in the following section.

4. Numerical analysis and performance evaluation

In this section, the performance of the FIL re-authentication protocol are evaluated and are compared with the standard full authentication and the standard fast re-authentication in EAP-AKA protocol in terms of authentication session time, bandwidth cost, and authentication delay. In actual, it is difficult to measure authentication performance accurately since the real system performance depends on a variety of factors, such as security tunnel, bandwidth limitation, device computing capability, network topology, and entity location. Thus, for providing a proof implementation, some factors in our simulation model are neglected and are assumed in Table 1. In addition, the simulation model is based on the NS-2 with extensions for the IEEE 802.11 model [31] and is written in C++ and Otcl languages.

Table 1 Simulation parameter

Simulation parameter	Value
MAC protocol	802.11
Simulation area	4 (km^2)
Number of HLR/HSS	1
Number of RADIUS server	1
Number of local APs (*N*)	100
Number of UEs (*n*)	100-1000
Service radius of RADIUS service (r_r)	1 (km)
Service radius of single AP (r_a)	0.1 (km)
Local AP placement	Grid
UEs placement	Uniform
Average speed of UE (*V*)	10 (km/h)
Direction of UE movement	[0, 2*π*]
Simulation time (*T*)	1800 (s)

4.1. Authentication session time

In the initial state of the simulation model, 100 APs and a number of MSs from 100 to 1000 are placed together onto a rectangular grid (4 km^2). The location of MSs is evenly distributed in the different AP's coverage. Moreover, all MSs simultaneously move with fixed velocity (*V*), the MS may moves $2r_a$ distance to crossover different AP service area in the worst case. Based on such assumptions, the authentication request rate in the RADIUS server denoted as $R_{\text{AR\_RADIUS}}$ can be derived as follows:

$$R_{\text{AR\_RADIUS}} = \frac{n^* \text{ user authentication request}}{T} = \frac{\frac{n * V * T}{2r_a}}{T} = \frac{n * \sqrt{N} * V}{2r_r}. \quad (1)$$

In addition, there are only one HLR/HSS and one RADIUS server resided in the proposed simulation model. Thus, the authentication request rate in the HLR/HSS $R_{\text{AR\_HLR/HSS}}$ is approximated to the $R_{\text{AR\_RADIUS}}$. Also, the authentication request rate of the single AP is expressed as follows:

$$R_{\text{AR\_AP}} = \frac{n^* \text{user authentication request}}{N * T} = \frac{\frac{n * V * T}{2r_a}}{N * T} = \frac{n * V}{2r_r * \sqrt{N}}. \quad (2)$$

Based on preceding derived formulas and simulation model assumptions, the actual simulation results in authentication request rate in different network entity are summarized in Table 2. It clearly shows that the increase trend in the authentication request rate is proportional to the MS increases. In addition, since most authentication requests are concentrated in RADIUS and HLR/HSS, the authentication request rate in the RADIUS or HLR/HSS is much large than in the single AP. In fact, the simulation results indeed show that centralized authentication requests not only made a great impact on the authentication session loads and processing loads in the RADIUS and HLR/HSS, but these loads affect authentication efficiency running on the 3G/UMTS-WLAN interworking networks.

Table 2 Authentication request rate in different network entity

Network entity:	HLR/HSS ($R_{\text{AR\_HLR/HSS}}$)	RADIUS server ($R_{\text{AR\_RADIUS}}$)	Single AP ($R_{\text{AR\_AP}}$)
Number of UEs			
100	2.218	2.226	0.0247
300	4.207	4.213	0.0438
500	8.019	8.093	0.0818
700	10.442	10.876	0.1131
900	13.175	13.202	0.1397
1000	14.227	14.436	0.1483

Next, in order to verify the impacts on the authentication session time, the authentication request rate in Table 2 must be taken into account in the authentication session time simulation. The simulation results about the authentication session time in different authentication protocols are illustrated in Figure 7. In the figure, the average authentication session time in the conventional full authentication and in the conventional fast re-authentication is 96.457 and 50.145 (ms), respectively. As a result of the reduction in authentication-related message transactions between the HLR/HSS and the RADIUS, since the fast re-authentication can lower about 48.1% authentication session time comparing to the conventional full authentication. On the other hand, the authentication session time in the FIL re-authentication protocol is 15.575 (ms). As comparing the FIL re-authentication protocol with two conventional authentication protocols, the reduction of authentication session time in the full authentication and in the fast re-authentication reaches up to 83.9 and 69%, respectively. Therefore, it clearly shows that the FIL re-authentication indeed improves authentication performance and provides better authentication efficiency than two conventional authentication protocols.

4.2. Bandwidth cost

To validate the best performance in bandwidth consumption of the FIL re-authentication, first all transaction message size between different network entity sections in one round authentication session are calculated and summarized in Table 3. Next, as referring to previous simulation model, the simulation results in bandwidth cost are illustrated in Figure 8.

Figure 8a illustrates the curves of bandwidth cost between the AP and the UE in different authentications. The curve of the fast re-authentication is approximately equal to the curve in the FIL re-authentication; moreover, as a result of extra counter and nonce attribute transactions in the HMAC authentication and counter

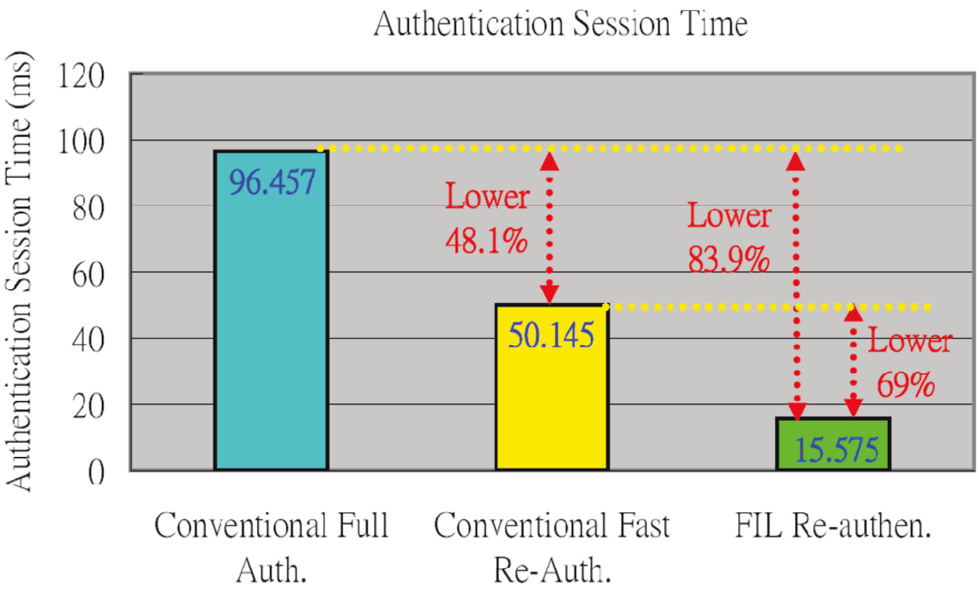

Figure 7 Authentication session time.

synchronization functions, thus both curves of bandwidth cost are increased approximately 14% than in the full authentication.

In Figure 8b, the curves of conventional full authentication and conventional fast re-authentication will change as mobile users increase. It is a significant increasing trend as a result of centralized authentication sessions result in a huge pile of messages traveling between the RADIUS server and APs. In addition, the localized re-authentication process and iterative process in the FIL re-authentication protocol are designated to decentralize re-authentication sessions from the RADIUS server to APs and to omit unnecessary authentication-related transactions between the RADIUS and the AP. Thus, the bandwidth cost between the RADIUS and the AP in the FIL re-authentication lowers approximately 94 and 89% than in the full authentication and in the fast re-authentication, respectively. This impact also reflects on the curve raised smooth comparing with two conventional authentication protocol curves.

In Figure 8c, the increased trend of the curve implies that authentication-related tansactions between the HLR/HSS and the RADIUS are only occurred in the full authentication. The increased trend is proportional to the UE increases. Such unnecessary authentication-related transactions can be neglected by using the fast re-authentication and the FIL re-authentication. Thus, the overall bandwidth cost in different authentication protocols can be depicted in Figure 8d. The figure clearly shows that the FIL re-authentication approximately lowers 53 and 48% bandwidth cost than that in the full authentication and in the fast re-authentication, respectively. To bandwidth consumption point of view, FIL re-authentication indeed has the best bandwidth consumption performance than other authentication protocols.

4.3. Authentication delay

To the authentication performance point of view, authentication delay is a major critical factor. It is also constituted of three delay elements, such as processing delay (D_{Proc}), transmission delay (D_{T}), and propagation delay (D_{Prop}). Thus, the D_{Auth} can be expressed as follows:

$$D_{\mathrm{Auth}} = D_{\mathrm{proc}} + D_{\mathrm{T}} + D_{\mathrm{prop}} \tag{3}$$

The processing delay is the delay experience by each node while processing cryptographic operations and key generation accounts for most of the processing delay. It

Table 3 Total message size between different network entity

Authentication type	Between UE-AP	Between AP-RADIUS	Between RADIUS-HLR/HSS	Total
Full authentication	245 Bytes	240 Bytes	124 Bytes	609 Bytes
Fast re-authentication	285 Bytes	280 Bytes	0 Bytes	565 Bytes
FIL re-authentication	285 Bytes	4 Bytes	0 Bytes	289 Bytes

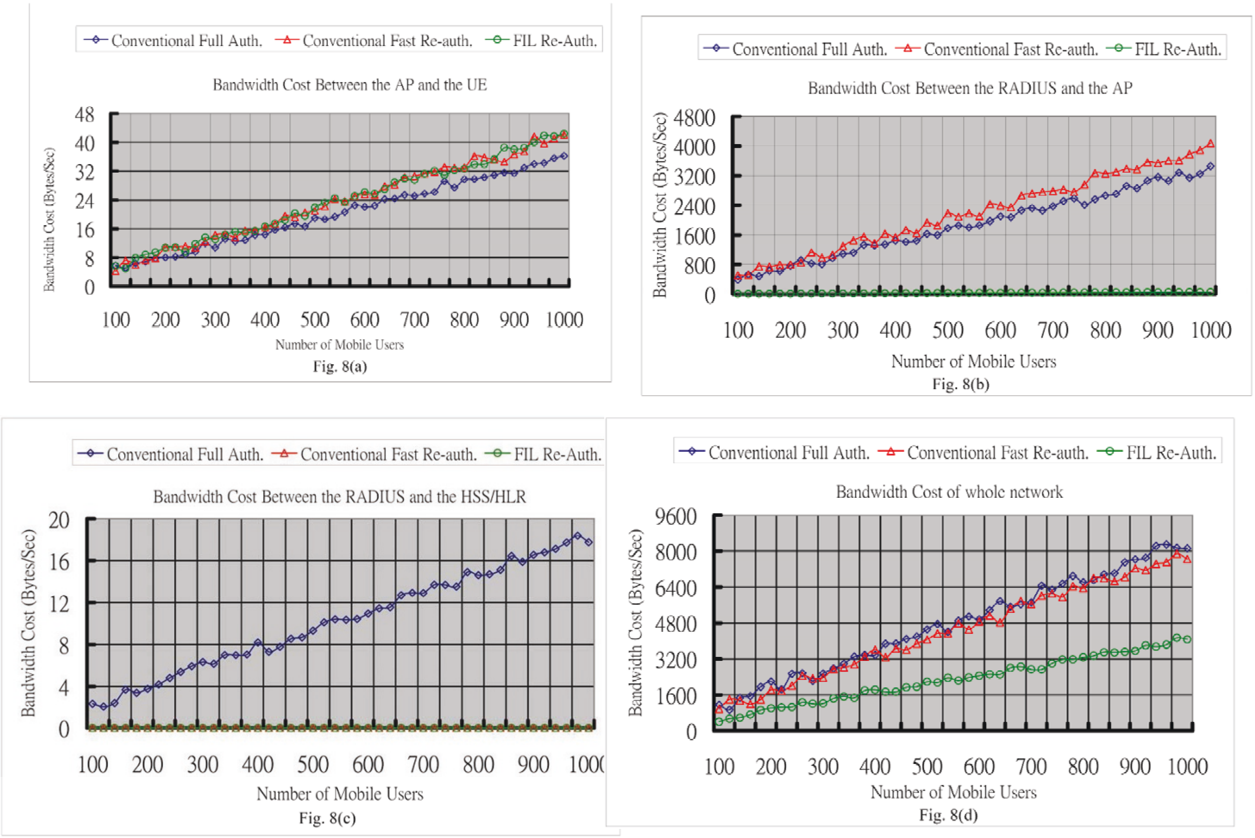

Figure 8 Bandwidth cost between different network entity. (a) Bandwidth cost between the AP and the UE. **(b)** Bandwidth cost between the RADIUS and the AP. **(c)** Bandwidth cost between the RADIUS and the HLR/HSS. **(d)** Total bandwidth cost.

mainly depends on the processing capability held by each node. To simplify the simulation model, the factor of processing capability among different network entities is neglected, and each processing operation is unified a basic value, 0.01 (ms). Thus, it can be easy comprehended that the processing delay of different authentications is depended on the number of processing operations of each network entity.

The transmission delay is the delay experience while transmitting an EAP message. It usually varies with some factors, such as transmission bandwidth and transmission protocols. Some researches discussed that it is insignificant compared the processing delay with the propagation delay [11,12,25,27-30]. Based on such assumptions, the transmission delay is not taken into account in the simulation model without affecting estimating the authentication delay in different authentication protocols.

The propagation delay is one-direction propagation delay between different network entity sections. The propagation delay of EAP-AKA protocol is constituted of three propagation sections in the simulation model. One is the propagation delay between the UE and the AP, another is between the AP and the RADIUS and the other is between the RADIUS and the HLR/HSS. For simplifying the estimation model, the value of one-direction propagation delay is designated as an identical value. Thus, it can be easy expressed that the propagation delay of different authentication protocols is depended on the number of propagation sections in different authentication protocols. Such assumption does not affect overall authentication efficiency comparisons in our simulation model [11,12,25,27-30].

Based on the above assumptions, the authentication delay in different authentication protocols is expressed in Table 4. According to the authentication delay expression in Table 4 FIL re-authentication has the lowest propagation delays than other conventional authentication protocols. However, both the FIL re-

Table 4 Authentication delay expression

Authentication type	Authentication delay (D_{Auth})
Full authentication protocol	12 * D_{Prop} + 16 * D_{Proc}
Fast re-authentication protocol	9 * D_{Prop} + 21 * D_{Proc}
FIL re-authentication protocol	6 * D_{Prop} + 21 * D_{Proc}

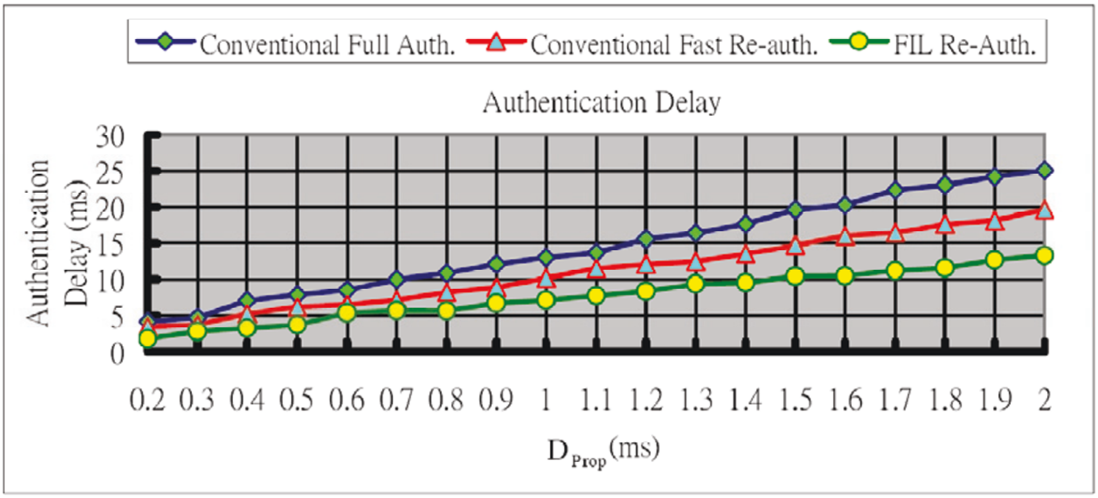

Figure 9 Authentication delay.

authentication and the fast re-authentication have the higher processing delays than the conventional full authentication. Next, the processing delay is set to a unified value, 0.01 (ms). The propagation delay is designated a value, which is varies from 0.2 to 2 (ms) and the sampling interval is set to 0.1 (ms). Then the simulation results about authentication delay in different authentication protocols are depicted in Figure 9. In the figure, the FIL re-authentication significantly lowers 47 and 30% authentication delay time than in the full authentication and in the fast re-authentication, respectively. Furthermore, the impact of the authentication delay is proportional to the propagation delays, which is depended on the number of authentication message transactions. Alternatively, the simulation results also give one proof that FIL re-authentication has the best authentication performance than other authentication protocols.

5. Conclusion

In EAP-AKA protocol, the fast re-authentication has the better authentication performance than the full authentication. However, the re-authentication efficiency of the fast re-authentication is still limited since the execution of re-authentication is handled by the authentication server resided in 3GHN. In this article, FIL re-authentication protocol is proposed to replace the fast re-authentication in EAP-AKA protocol. It can be summarized some advantages as follows: (1) it provides the same level of security and performance by applying minor modifications to the existing standard security protocols and architectures in 3G/UMTS-WLAN heterogeneous mobile networks, (2) it is to expedite authenticating mobile users by completing re-authentications locally without contacting the HAAA/RADIUS in 3GHN, and (3) localized re-authentication sessions are executed between the AP and the MS iteratively without contacting the RADIUS server in the WLAN domain. In addition, the simulation results show that FIL re-authentication has the best performance comparing to other conventional authentication protocols in terms of authentication session time, bandwidth cost, and authentication delay.

List of abbreviations

AAA: authentication: authorization and accounting; AES: advanced encryption standard; APs: access points; Avs: authentication vectors; AVD: authentication vectors distributor; CCMP: counter mode CBC-MAC protocol; IETF: Internet engineering task force; FIL re-authentication: fast iterative localized re-authentication; HLR/HSS: Home Location Registry/Home Subscriber Server; GTK: group transient key; 3GHN: 3G/UMTS Home Network; LAA: local authentication agent; MH: mobile host; MK: master key; MS: mobile user; NAI: network access identifier; PMK: pairwise master keys; PTK: pairwise transient key; TAP: target AP; TKIP: temporal key integrity protocol; WEP: wired equivalent privacy; WPA: Wi-Fi protected access.

Author details

[1]Department of Electrical Engineering, Chang Gung University, No. 259, Wunhua 1st Rd., Gueishan Township, Taoyuan County 333, Taiwan, ROC
[2]Department of Electronic Engineering, De Lin Institute of Technology, No. 1, Lane 380, Qingyun Rd., Tucheng City, Taipei County 236, Taiwan, ROC

Competing interests

The authors declare that they have no competing interests.

Received: 13 December 2010 Accepted: 10 October 2011
Published: 10 October 2011

References

1. 3GPP TS 23.101 V4.0.0. General UMTS Architecture (April 2001)
2. 3GPP TS 23.234, Rel.6, v6.3.0, 3GPP System to Wireless Local Area Network (WLAN) Interworking; System Description (December 2004)
3. K Ahmavaara, H Haverinen, R Pichna, Interworking architecture between 3GPP and WLAN systems. IEEE Commun Mag. **41**(11), 74–81 (2003). doi:10.1109/MCOM.2003.1244926

4. VK Varma, S Ramesh, KD Wong, M Barton, G Hayward, JA Friedhoffer, Telecodia Technol., Red Bank, Mobility management in integrated UMTS/WLAN networks, in *Proceedings of IEEE ICC 2003*, **2**, 1048–1053 (2003)
5. GM Koien, T Haslestad, Security aspects of 3G-WLAN interworking. IEEE Commun Mag. **41**, 82–88 (2003)
6. HH Choi, O Song, DH Cho, A seamless handoff scheme for UMTS-WLAN interworking, in *Proceedings of IEEE Globalcom 2004*, **3**, 1559–1564 (2004)
7. M Kim, H Ju, Y Kim, J Park, Design and implementation of mobile trusted module for trusted mobile computing. IEEE Trans Consum Electron. **56**(1), 134–140 (2010)
8. J McNair, F Zhu, Vertical handoffs in fourth-generation multi-network environments. IEEE Wireless Commun. **11**, 8–15 (2004)
9. M Shi, X Shen, J Mark, IEEE802.11 Roaming and authentication in Wireless LAN/Cellular Mobile Networks. IEEE Wireless Communications. **11**(4), 66–75 (2004). doi:10.1109/MWC.2004.1325893
10. P TalebiFard, T Wong, VCM Leung, Access and service convergence over the mobile internet–a survey. Comput Netw. **54**(5), 545–557 (2010)
11. A Tsakountakis, G Kambourakis, S Gritzalis, A generic accounting scheme for next generation networks. Comput Netw. **53**(14), 2408–2426 (2009). doi:10.1016/j.comnet.2009.04.009
12. H Kwon, K-Y Cheon, K-H Roh, A Park, USIM based authentication test-bed for UMTS-WLAN handover, in *Proceedings of IEEE INFOCOM* (April 2006)
13. 3rd Generation Partnership Project, 3G security; WLAN interworking security (Release 7), 3GPP Technical Specifications TS 33.234 v7.0.0, 3GPP, Valbonne, France (March 2006)
14. IETF, RFC 4187, J Arkko, H Haverinen, Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA). (2006)
15. S Pack, Y Choi, Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1x model, in *IFIP TC6 Personal Wireless Communications* (October 2002)
16. S Pack, Y Choi, Fast handoff scheme based on mobility prediction in public wireless LAN systems. IEE Proc Commun. **151**(5), 489–495 (2004). doi:10.1049/ip-com:20040834
17. A Mukherjee, T Joshi, DP Agrawal, Minimizing re-authentication overheads in infrastructure IEEE 802.11 WLAN networks, in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC '05)*, **4**, 2344–2349 (March 2005)
18. W Arbaugh, A Mishra, M Shin, Context caching using neighbor graphs for fast hand-offs in a wireless network, in *IEEE INFOCOM* (March 2004)
19. A Mishra, M Shin, NL Petroni Jr, TC Clancy, WA Arbaugh, Proactive key distribution using neighbor graphs. IEEE Wireless Commun. **11**(1), 26–36 (2004). doi:10.1109/MWC.2004.1269714
20. M Kassab, A Belghith, J-M Bonnin, S Sassi, Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks, in *Proceedings of the 1st ACM International Workshop on Wireless Multimedia Networking and Performance Modeling (WMuNeP '05)*, pp. 46–53 (October 2005)
21. J Hur, C Park, H Yoon, An efficient pre-authentication scheme for IEEE 802.11-based vehicular networks. Adv Inf Comput Security **4752**, 121–136 (2007). doi:10.1007/978-3-540-75651-4_9
22. P Prasithsangaree, P Krishnamurthy, A new authentication mechanism for loosely coupled 3G-WLAN integrated networks, in *IEEE 59th Vehicular Technology Conference* **5**, 2998–3003 (2004)
23. G Kambourakis, A Rouskas, S Gritzalis, Advanced SSL/TLS based authentication for secure WLAN-3G interworking. IEE Commun Proc. **151**, 501–506 (2004). doi:10.1049/ip-com:20040835
24. M Lee, G Kim, S Park, Seamless and secure mobility management with location-aware service (LAS) broker for future mobile interworking networks. J Commun Netw. **7**(2), 207–221 (2005)
25. AA Shidhani, V Leung, Local fast re-authentication for 3G-WLAN interworking architecture. Security Commun Netw. **1**(4), 309–323 (2008). doi:10.1002/sec.30
26. AA Shidhani, VCM Leung, Pre-authentication schemes for UMTS-WLAN interworking. EURASIP J Wireless Commun Netw 2009. Article ID 806563 (2009)
27. SH Lin, JH Chiu, SS Shen, Authentication schemes based on the EAP-SIM mechanism in GSM-WLAN heterogeneous mobile networks, in *Proceedings of NCM 5th International Joint Conference on INC, IMS and IDC*, pp. 2089–2094 (August 2009)
28. SH Lin, JH Chiu, SS Shen, Performance evaluation of the fast authentication schemes in GSM-WLAN heterogeneous networks. J Netw. **5**(8), 956–963 (2010)
29. S-H Lin, J-H Chiu, G-R Lee, A fast iterative localized re-authentication protocol for heterogeneous mobile networks. IEEE Trans Consum Electron. **56**(4), 2267–2276 (2010)
30. SH Lin, JH Chiu, SS Shen, The iterative distributed re-authentication scheme based on EAP-AKA in 3G/UMTS-WLAN heterogeneous mobile networks, in *International Conference on Broadband, Wireless Computing, Communication and Applications 2010 (BWCCA 2010)*, pp. 429–434 (2010)
31. S Macanne, S Floyd, http://www-mash.cs.berkeley.edu/ns. Network Simulator

doi:10.1186/1687-1499-2011-124
Cite this article as: Lin *et al.*: **A fast iterative localized re-authentication protocol for UMTS-WLAN heterogeneous mobile communication networks.** *EURASIP Journal on Wireless Communications and Networking* 2011 **2011**:124.