Int. J. Communications, Network and System Sciences, 2014, 7, 101-113
Published Online April 2014 in SciRes. http://www.scirp.org/journal/ijcns
http://dx.doi.org/10.4236/ijcns.2014.74012

Scientific Research

Fast Handover Pre-Authentication Protocol in 3GPP-WLAN Heterogeneous Mobile Networks

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

[1]Department of Electrical Engineering, De Lin Institute of Technology, New Taipei City, Taiwan
[2]Department of Electrical Engineering, Chang Gung University, Taoyuan County, Taiwan
Email: shen@dlit.edu.tw, marcular@gmail.com, jhchiu@mail.cgu.edu.tw

Received 8 February 2014; revised 8 March 2014; accepted 20 March 2014

Open Access

Abstract

The demand of ubiquitous communications drives the development of advanced mobile technologies. Meanwhile, recent increases in mobile data usage and the emergence of new IP service applications constitute the motivation to integrate 3GPP cellular mobile systems with broadband WLANs. Since 3GPP and WLAN systems complement each other in terms of infrastructure and network coverage and bandwidth, 3GPP-WLAN Heterogeneous Mobile Networks based on the 3GPP-based Home Network (3GHN) are proposed for meeting the growing demands in high-speed data access on any mobile devices. However, heterogeneous radio access technologies and architectures lead to many interworking issues, such as network transparency, security mechanism, seamless handover, and quality of service. Among of them, security and handover are the major motives to ensure the confidentiality, reliability and continuity of services in 3GPP-WLAN Heterogeneous Mobile Networks. This paper proposes fast handover pre-authentication protocol to reduce the handover authentication latency and authentication signaling overhead during the whole handover session. The proposed protocol supports Intra-Domain Handover Pre-Authentication (Intra-HO Pre-Auth) and Inter-Domain Handover Pre-Authentication (Inter-HO Pre-Auth) for pre-authenticating the Mobile User (MS) prior to performing an Inter-domain Handover (Inter-domain HO)/Intra-domain Handover (Intra-domain HO) process. Meanwhile, the reduction in retrieving new Authentication Vector sand key sets from the Home Location Register/Home Subscriber Service/Authentication Center in 3GHN achieves for minimized redundant authentication signaling transactions between 3GPP domains and WLAN domains. In addition, this paper provides simulation results which show that the proposed Intra-HO Pre-Auth achieves 49% handover authentication performance improvement compared to EAP-AKA, and the proposed Inter-HO Pre-Auth achieves 26% handover authentication performance improvement as well.

How to cite this paper: Shen, S.-S., Lin, S.-H. and Chiu, J.-H. (2014) Fast Handover Pre-Authentication Protocol in 3GPP-WLAN Heterogeneous Mobile Networks. *Int. J. Communications, Network and System Sciences*, **7**, 101-113.
http://dx.doi.org/10.4236/ijcns.2014.74012

Keywords

3GPP-WLAN, Handover, Authentication, EAP-AKA, HLR/HSS/AuC

1. Introduction

Over recent years, the evolution in wireless communications and mobile communications satisfies the growing demand for broadband wireless access to IP services at anytime, anywhere and on any mobile devices. But, it is not easy to achieve for single system. Thereby, the integration of current communication systems, including 3GPP systems, WLANs and other future technologies, becomes an economic and practical solution. It is also called as heterogeneous mobile network, which takes advantages of integrated and combined capabilities in different communications. 3GPP-WLAN Heterogeneous Mobile Network, illustrated in **Figure 1**, was proposed by 3GPP to support the requirement of high-speed data services with wide coverage areas for 3GPP/WLAN multimode terminals [1]-[3]. Security and seamless handover are import aspects of service confidentiality, reliability and continuity in 3GPP-WLAN Heterogeneous Mobile Network [4]-[6]. Meanwhile, 3GPP also recommended Extensible Authentication Protocol-Authentication and Key Agreement protocol (EAP-AKA) supporting security services [7] [8].

In **Figure 1**, Home Authentication, Authorization, and Accounting (HAAA)/WLAN Authentication, Authorization, and Accounting (WAAA) are used as the bridge node between 3GPP domain and WLAN domain. From the perspective of WLAN, EAP is adopted to support security services between HAAA/WAAA and MS [9]. On the other hand, 3GPP-AKAprovidessecurity services to ensure 3GPP domain resources accessed by authorized MS. The combined protocol, EAP-AKA, mandates any MS within 3GPP-WLAN Heterogeneous Mo-

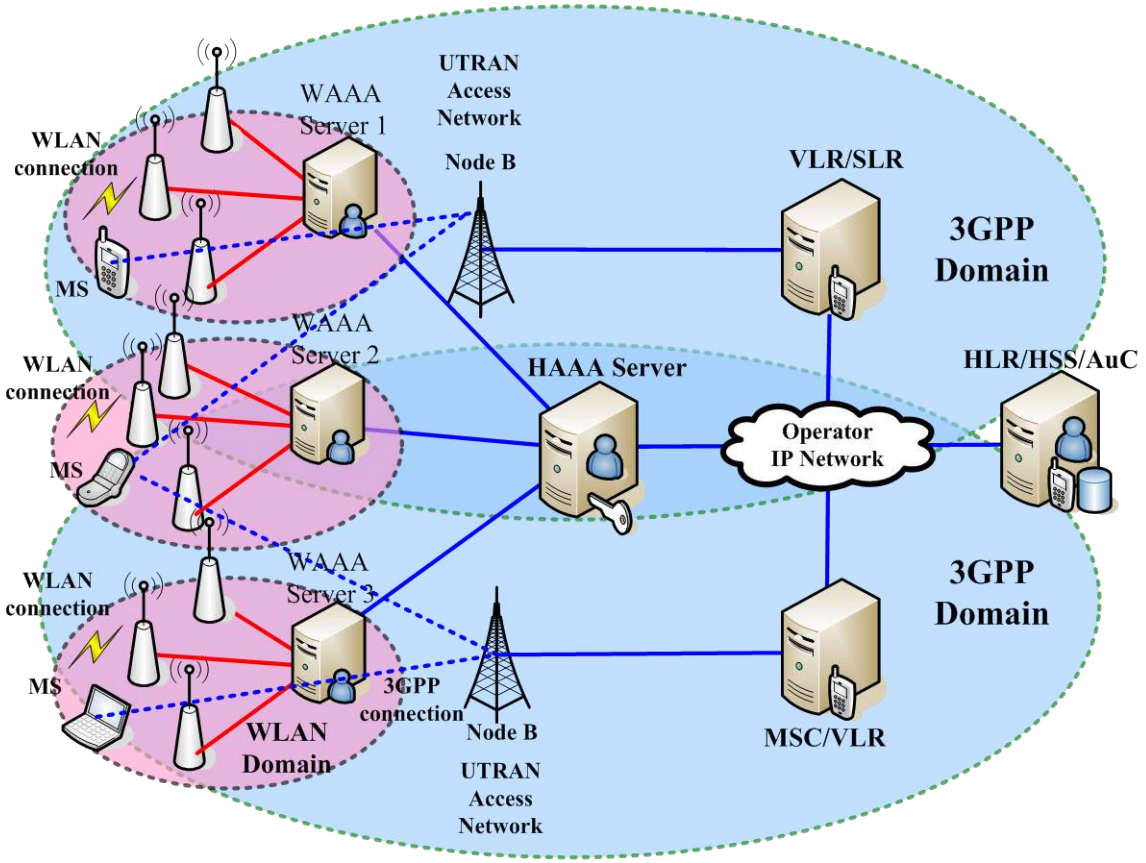

Figure 1. 3GPP-WLAN heterogeneous mobile network.

bile Network to perform authentication process with the HLR/HSS/AuC. However, HLR/HSS/AuC might be far away or separated by several network domains from the MS. Such a long journey authentication round trip may result in enormous authentication message transactions between 3GPP networks and WLAN networks. In addition, authentication process is inevitable prior to any connection services and occurred frequently when temporary connection services interrupt or as a result of handovers. Thereby, repetitive invocation of long journey authentication round trips which are owing to frequent connections and handover requirements might result in high authentication delays and introduce unnecessary signaling and processing overhead. Even though EAP-AKA provided a re-authentication trying to solve inefficiency authentication bottleneck, authentication performance improves a bit due to the elimination of authentication signaling transactions between HLR/HSS/AuC and HAAA. The enormous re-authentication processing overhead and message transactions still exist between 3GPP networks and WLAN networks. Handover authentication in 3GPP-WLAN interworking networks is an essential phase to ensure connection continuity when handover process is invoked. But, 3GPP does not designate any handover authentication protocol for supporting handover process. In other words, the inefficient full (re-) authenticational ways invokes to implement handover authentication services no matter what kind of handover is occurred. Consequently, the strategy of designating EAP-AKA as handover authentication protocol seems unfavorable for minimizing handover latency and for ensuring continuity services in 3GPP-WLAN Heterogeneous Mobile Network.

The contribution of this paper is to propose a fast handover authentication protocol, including Inter-HOPre-Auth and Intra-HO Pre-Auth, which reduces handover authentication delays during Inter-domain HO and Intra-domain HO. Actually, the tactics of proposed protocol is extended the concept of Fast Iterative Localized Re-authentication (FIL Re-authentication) implementing in GSM-WLAN Heterogeneous Mobile Networks proposed by S. H. Lin *et al.* in 2010 [10] [11] and based on FIL Re-authentication protocol for UMTS-WLAN Heterogeneous Mobile Networks also proposed by S. H. Lin *et al.* in 2011 as well [12] [13]. When the MS roams across different APs located within the same WLAN domain, WAAA server is appointed to replace HAAA/HLR/HSS/AuC for authenticating the MS via Intra-HO Pre-Auth prior to performing Intra-domain HO process. On the other hand, HAAA server authenticates the MS roaming across different WLAN domains before performing Inter-domain HO process through Inter-HO Pre-Auth. By using similar iteration strategy [13] allows the repeated execution of Inter-HO Pre-Auth/Intra-HO Pre-Auth to reduce the probability of long journey full (re-) authentication occurrence when the MS continues requesting Inter-domain HO/Intra-domain HO. The advantage of integrating with FIL Re-authentication is to provide fast and flexible authentication mechanisms to support stationary user authentication and roaming user authentication.

Fast Handover Pre-Authentication Protocol achieves secure key management distribution, fresh key re-generation, and minimum handover authentication latency in 3GPP-WLAN Heterogeneous Mobile Network. This paper also provides a proof implementation based on NS-2 with 802.11 WLAN model; moreover, the simulation results show the superior performance in handover authentication delay than that in EAP-AKA. The rest of this paper is organized as follows. In Section 2, the related works are introduced. Section 3 gives detailed descriptions of the proposed protocol. In Section 4, the performance evaluation is present. Finally, some conclusion is given in Section 5.

2. Related Works

3GPP recommends invoking EAP-AKA to authenticate users accessing 3GPP-WLAN Heterogeneous Mobile Network. It relies on pre-shared secrets held by the MS and HLR/HSS/AuC. Authentication process may be a full authentication or re-authentication depended on communication status and the capability of the 3GPP HN and MS. In general, re-authentication must be invoked after a successful full authentication session. In full authentication, the HAAA and the MS exchange multiple EAP request/response messages to verify the user identity; meanwhile, HAAA communicates with HLR/HSS/AuC to obtain essential security keys and credential information known as Authentication Vectors (AVs) for the needs of operating security-related functions including Identity Authentication, HMAC Authentication, AV Generation, Key Generation, SQN-synchronization and Encryption. After Identity authentication process, HAAA invokes SHA-1 and Pseudo-Random Function (PRF) to derive essential key sets likes Master Key (MK), Master Session Key (MSK), Extended MSK (EMSK), and Transient EAP Keys (TEKs) [8]. As successfully completed HMAC authentication and SQN-synchronization process, HAAA immediately delivers MSK to WAAA and Access Point (AP). Then WAAA and MS derive new

session keys like Pair wise Transient Key (PTK) and Group Transient Key (GTK) by using four-way handshake and two-way handshake. Those derived keys are used to support IEEE 802.11i encryption operation [14].

EAP-AKA also provides re-authentication for supporting repeated authentications. The advantage of re-authentication is the reduction in redundant resource usage because HAAA does not need new key sets retrieved from HLR/HSS/AuC. In a word, HAAA inherits MK from full authentication to derive new key sets (MSK, EMSK, TEKs) for supporting subsequent security-related functions. Because the process of key derivation in re-authentication is similar to full authentication, only HLR/HSS/AuC is not participated in re-authentication process.

Indeed, handover delay is an important metric in evaluating the guarantee of the continuity services in 3GPP-WLAN Heterogeneous Mobile Networks. Unfortunately, 3GPP did not designate any handover authentication protocols. Thereby, handover authentication delay largely contributes to the overall handover delay because long journey full (re-)authentication process must be invoked. In recent years, many researches focus on minimizing handover authentication delay in an autonomous WLAN. S. Pack *et al.* [15] and A. Mukherjee *et al.* [16] proposed predicting user's next move for pre-authenticating the MS with potential Target AP (TAP). However, those solutions result in unnecessary authentication procedure, which brings up signaling overhead increases in autonomous WLANs. J. Hur *et al.* [17] and Lee M. *et al.* [18] proposed new movement predictions to predict user mobility and pre-authenticate the MS with the TAP before the handover. However, those solutions need additional authentication servers and are also restricted to intra-WLAN domain handovers. Pro-active key distribution solutions proposed by W. Arbaugh *et al.* [19], A. Mishra *et al.* [20], and M. Kassab *et al.* [21] still require additional authentication servers to pre-distribute pair wise master keys during a re-authentication session. The increase in unnecessary key pre-distribution process is the primary drawback when the number of users increases. The abovementioned solutions are only favorable for an autonomous WLAN domain to reduce the handover authentication latency rather than for 3GPP-WLAN Heterogeneous Mobile Networks as a result of the network interoperability.

Although IEEE proposed many handover protocols like IEEE 802.11i, IEEE 802.11fand IEEE 802.11rto solve handover authentication latency, those solutions still only meet for autonomous WLANs rather than for 3GPP-WLAN Heterogeneous Mobile Networks. In addition, some researches [18] [22] [23] adopt other authentication protocols or introduce major modifications to 3GPP-WLAN interworking architecture for enhancing handover authentication performance. But those solutions result in raising the system integration complexity and reducing the network transparency. Based on the above constraints, this paper proposes fast handover authentication protocol for supporting roaming user handover authentications. Besides, the proposal greatly aids in minimizing the handover latency and guarantees the service continuity in 3GPP-WLAN Heterogeneous Mobile Networks.

3. Fast Handover Pre-Authentication Protocol

Inter-HO Pre-Auth is invoked when the MS roams across different WLANs and acquires an Inter-domain HO in 3GPP-WLAN Heterogeneous Mobile Networks. Then, HAAA server authenticates the MS before performing Inter-domain HO process. On the other hand, WAAA authenticates the MS via Intra-HO Pre-Auth before the Intra-domain HO process when the MS roams across different APs within the same WLAN domain. There are some key features of proposed protocol: 1) Without any modifications for 3GPP-WLAN Heterogeneous Mobile Network architecture to ensure network interoperability, 2) Based on EAP-AKA to maintain the same level security strength and performance, and 3) Integrated with FIL Re-authentication protocol proposed in [12] [13] to provide stationary authentication and handover authentication for a single user.

3.1. Assumption

To realize the proposed protocol, some assumptions for authenticating a user in 3GPP-WLAN Heterogeneous Mobile Networks must be elaborated. Firstly, HAAA has a Long Term Security Association and roaming agreements with different WAAA servers resided in different WLAN domains. Secondly, multiple APs are controlled by a WAAA to form a WLAN domain; meanwhile, strong trust authentication associations and security tunnels are pre-agreed. Third, both HAAA and WAAA can provide a new temporary user identity respectively used in Inter-domain HO/Intra-domain HO. Fourth, HAAA and WAAA respectively share $\text{Counter}_{\text{HAAA}}$ and $\text{Counter}_{\text{WAAA}}$ counter value with the MS to limit the number of successive handover au-

thentication sessions, maintain key fresh, and prevent replay attacks. An attached subscript of attribute indicates that the attribute generated by specific entity.

3.2. Proposed Key Schedule

The efficient key schedule is proposed to guarantee protocol realized and secured. Thus, simple modifications of key schedule in EAP-AKA and proposed key schedules in Inter-HO/Intra-HO Pre-Auth are required to be addressed in detail. In EAP-AKA full authentication, HAAA must derive key sets (MK_{HAAA}, $EMSK_{HAAA}$, MSK_{HAAA}, $TEKs_{HAAA}$). In proposed key schedule, these keys are divided into two categories according to specific functions. First category includes MK_{HAAA} and $EMSK_{HAAA}$ keys, which are used as the key seeds to derive additional handover keys for supporting keys update when Inter-HO Pre-Auth invoked. Second category includes MSK_{HAAA} and $TEKs_{HAAA}$, which are pre-loaded to WAAA and used as the key seeds to derive new key sets (MK_{WAAA}, $EMSK_{WAAA}$, MSK_{WAAA}, $TEKs_{WAAA}$) via the proposed key derivation shown in **Figure 2**. These keys are also classified two categories. MK_{WAAA} and $EMSK_{WAAA}$ are the key seed used to derive new handover keys for supporting keys update when Intra-HO Pre-Auth is triggered. On the other hand, the usage of MSK_{WAAA} and $TEKs_{WAAA}$ are similar to EAP-AKA full authentication.

The feature of Inter-HO Pre-Auth needs the support of HAAA for authenticating the MS roaming across different WLAN domains, and without retrieving new AVs from the HLR/HSS/AuC. It re-uses keys pre-derived in proposed key schedule in **Figure 2**, which results in minimizing the dependence on HLR/HSS/AuC and reducing authentication signaling transactions between HLR/HSS/AuC and HAAA. Due to the strategy of inherited keys re-using in HAAA, proposed key derivation shown in **Figure 3** is invoked to re-generate key sets (MKHAAA(k), EMSKHAAA(k), MSKHAAA(k), TEKs HAAA(k)) when an Inter-HO Pre-Auth is invoked. In the figure, MKHAAA(k-1) and EMSKHAAA(k-1) was pre-derived in proposed key schedule of full authentication or the previous round Inter-HO Pre-Auth. The temporary identity, TMSI(k), is generated by HAAA. The counter attribute is used to limit the number of successive Inter-HO Pre-Auth sessions, and the nonce attribute is used to prevent replay attacks during Inter-HO Pre-Auth exchanges. The index "k" represents the number of successive Inter-HO Pre-Auth sessions. These deriving keys are also divided into following groups according to different functions: 1) One group included MKHAAA(k) and EMSKHAAA(k) is designated to be key seeds

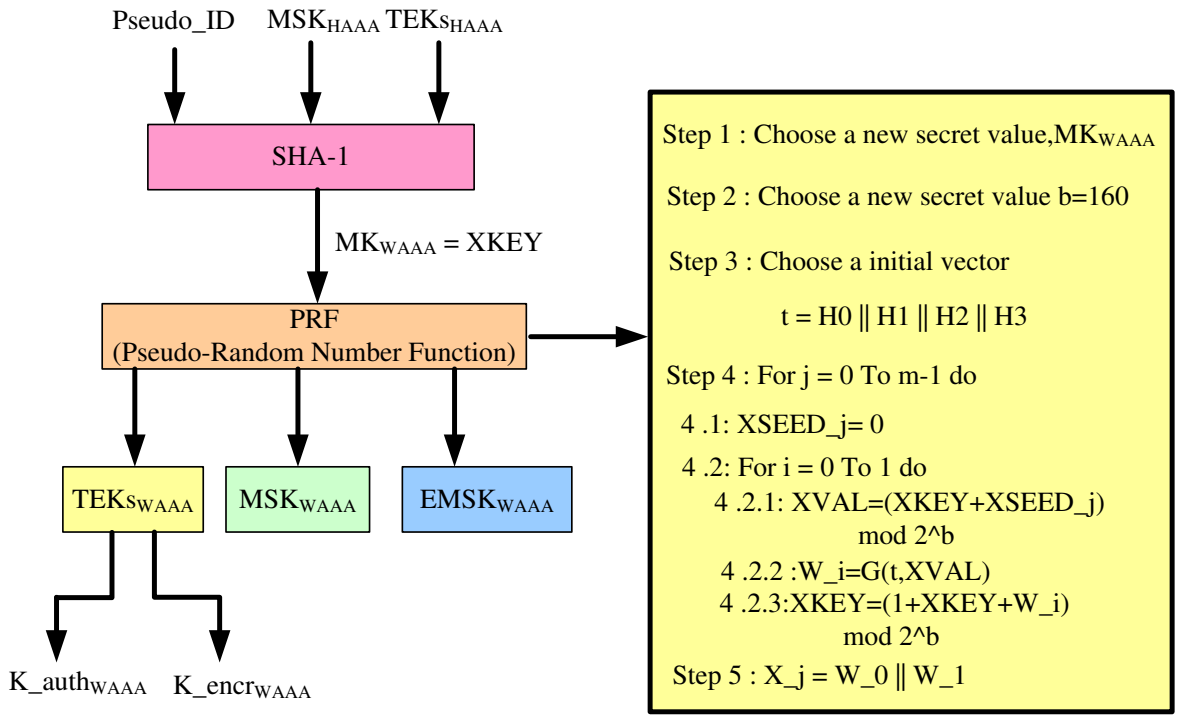

Figure 2. Propose key derivation of WAAA in full authentication.

using for the next round Inter-HO Pre-Auth, 2) another group contained MSKHAAA(k) and TEKs HAAA(k) is used for securing traffic exchanges during current Inter-HO Pre-Auth session between HAAA and MS, and 3) MSKHAAA(k) and TEKs HAAA(k) were pre-delivered to Target WAAA (TWAAA) for updating key sets using in the next round Intra-HO Pre-Auth or in the FIL Re-authentication within Target WLAN domain

Intra-HO Pre-Auth enables local WAAA to authenticate the MS roaming across different APs resided within the same WLAN domain. The feature of Intra-HO Pre-Auth is to re-use keys inherited from proposed key schedule in full authentication or in Inter-HO Pre-Auth, which minimizes the dependency on the 3GPP HN during an Intra-domain HO process. When the MS acquires an Intra-HO Pre-Auth, the proposed key derivation shown in **Figure 4** is invoked to re-derive key sets ($MK_{WAAA(j)}$, $EMSK_{WAAA(j)}$, $MSK_{WAAA(j)}$, $TEKs_{WAAA(j)}$). $MK_{WAAA(j-1)}$ and $EMSK_{WAAA(j-1)}$ are pre-derived in the proposed key schedule of the full authentication or the previous round Inter-HO/Intra-HO Pre-Auth. In the figure, temporary identity, Pseudo_ID(j), is generated by the WAAA. The

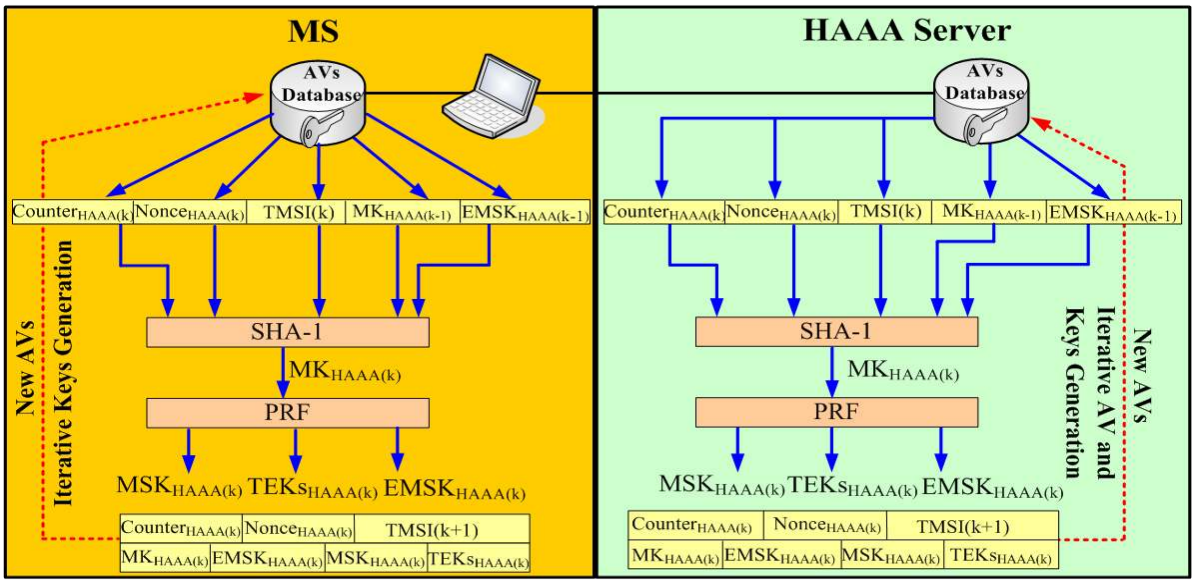

Figure 3. Propose Key Derivation of HAAA in Inter-HO Pre-Auth.

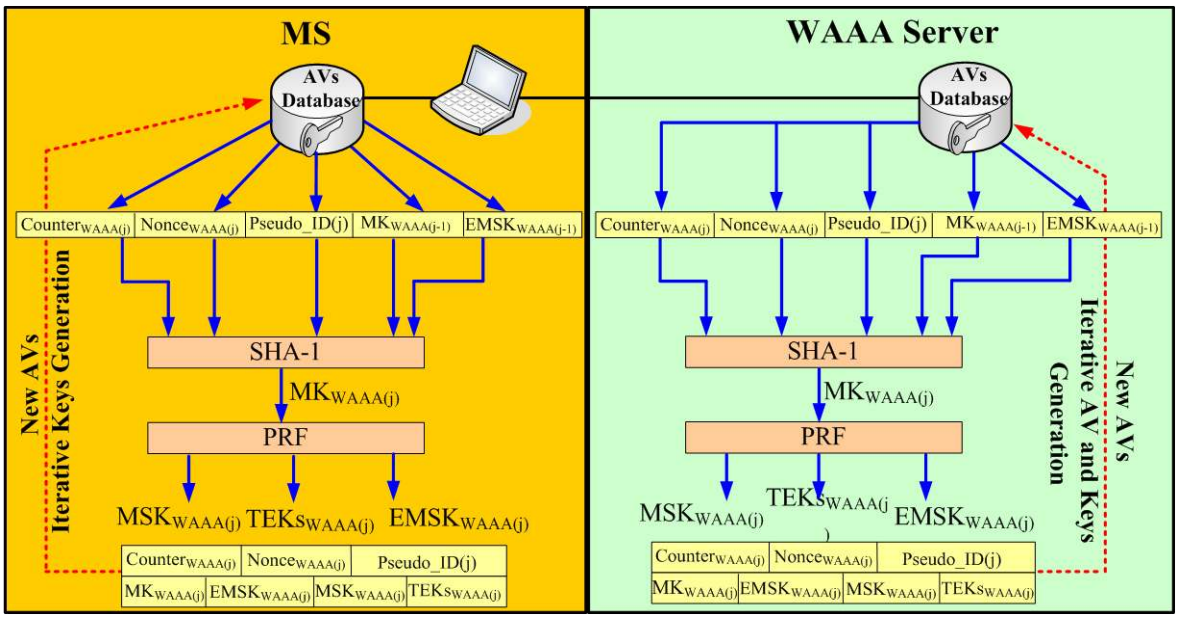

Figure 4. Propose key derivation of WAAA in Intra-HO Pre-Auth.

counter attribute is to limit the number of successive Intra-HO Pre-Auth sessions, and the nonce attribute is used to prevent replay attacks during current Intra-HO Pre-Auth exchanges. The index "j" represents the number of successive Intra-HO Pre-Auth sessions. Also, those keys are also divided into following categories: 1) $MK_{WAAA(j)}$ and $EMSK_{WAAA(j)}$ are used as root keys to re-new key sets, which will be used in the next round Intra-HO Pre-Auth, 2) $MSK_{WAAA(j)}$ and $TEKs_{WAAA(j)}$ are used to secure the traffic exchanges between WAAA and MS during current Intra-HO Pre-Auth session, and 3) $MSK_{WAAA(j)}$ and $TEKs_{WAAA(j)}$ are also delivered to Target AP (TAP) for deriving fresh PTK and GTK for enabling the later 802.11i encryption or FIL Re-authentication between Target AP (TAP) and MS. After completely understanding the proposed key schedule, then Inter-HO/Intra-HO Pre-Auth procedure are proceeded to discuss in detail as follows.

3.3. Proposed Intra-HO Pre-Auth Procedure

When a MS roams across different TAPs located within the same WLAN domain, the procedure of Intra-HO Pre-Auth between WAAA and MS shown in **Figure 5** is invoked and proceeds as follows:

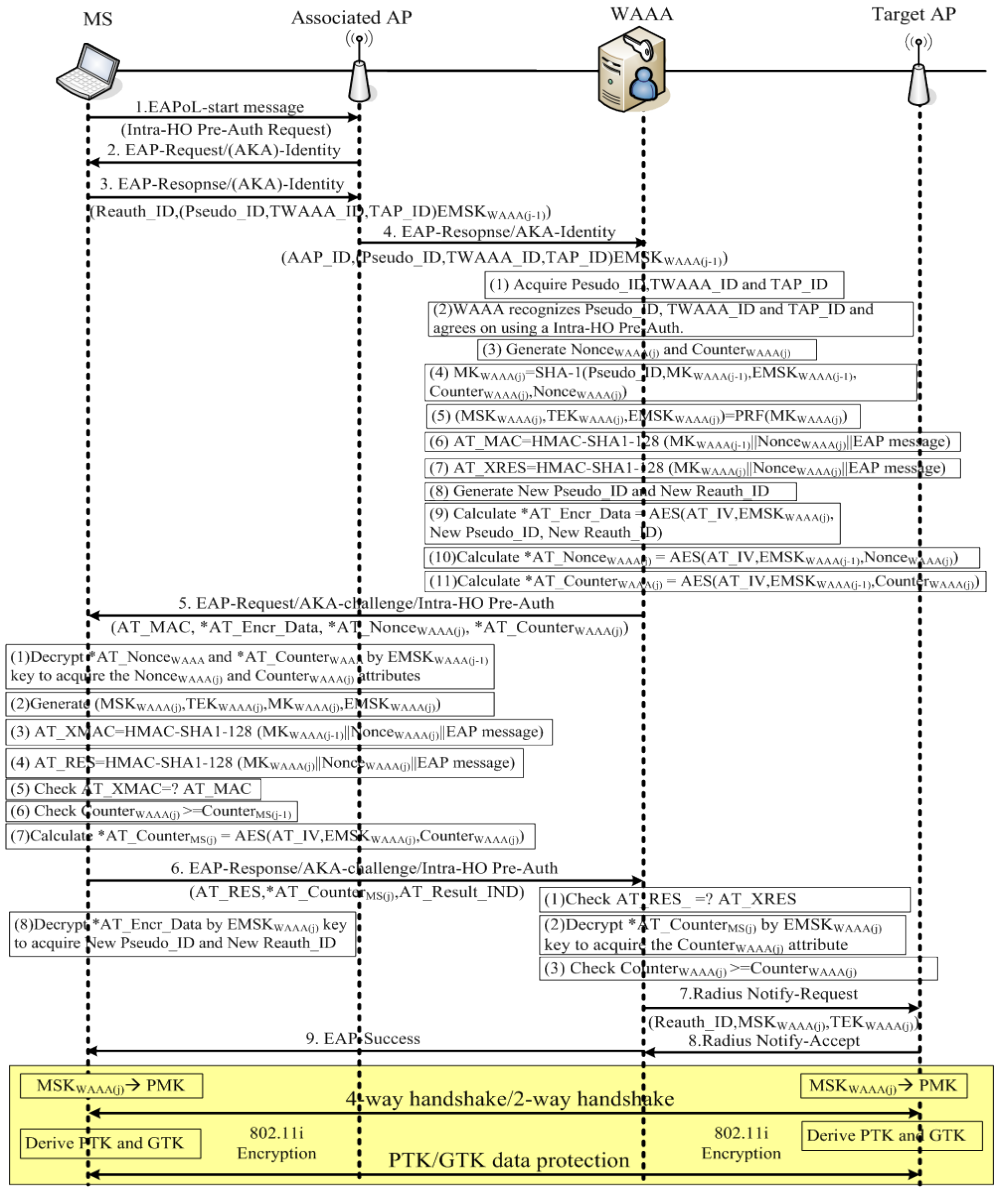

Figure 5. The detailed flow of proposed intra-ho pre-auth.

- **STEP 1-3:**

When MS receives current AP's advertisement poor-signal and recognizes the need for Intra-domain HO process, MS first supplies Reauth_ID and other encrypted attributes (Pseudo_ID, TWAAA_ID, TAP_ID) to require an Intra-HO Pre-Auth association with Associated AP (AAP). Reauth_ID is similar to the temporal Fast_ID in FIL Re-authentication proved the legal certification to AAP. The encrypted attributes are protected by $EMSK_{WAAA(j-1)}$, which was pre-shared between WAAA and MS in proposed key schedule of full authentication or the previous round Inter-HO Pre-Auth/Intra-HO Pre-Auth.

- **STEP 4-5:**

AAP initially checks if the received Reauth_ID identity is valid and agrees on using Intra-HO Pre-Auth. If the identity check is positive, then AAP immediately forwards the request included encrypted attributes (Pseudo_ID, TWAAA_ID, TAP_ID) with AAP_ID to WAAA. If the received AAP_ID is valid, WAAA acquires Pseudo_ID, TWAAA_ID and TAP_ID by $EMSK_{WAAA(j-1)}$and checks if Pseudo_ID is legal. Subsequently, $Nonce_{WAAA(j)}$ and $Counter_{WAAA(j)}$ are generated by the WAAA. Next, the proposed Intra-HO Pre-Auth key derivation is proceeding to derive related key sets. Besides, message authentication codes (AT_MAC and AT_XRES) are also generated by HMAC-SHA1-128. Then, WAAA and MS exchange message authentication codes to verify each other. For user identity privacy in the next round Intra-HO Pre-Auth or the later FIL Re-authentication, new Reauth_ID and Intra-HO Pre-Auth identity (Pseudo_ID) are generated by WAAA. Two identities are also encrypted by $EMSK_{WAAA(j)}$ to securely push to MS. Besides, $Counter_{WAAA(j)}$ and $Nonce_{WAAA(j)}$ are secured by $EMSK_{WAAA(j-1)}$. Those are denoted as $*AT\_Counter_{WAAA(j)}$ and $*AT\_Nonce_{WAAA(j)}$, respectively. Then, WAAA sends EAP-Request/AKA-challenge/Intra-HO Pre-Auth message to MS, which includes AT_MAC, *AT_Encr_Data, $*AT\_Nonce_{WAAA(j)}$ and $*AT\_Counter_{WAAA(j)}$.

- **STEP 6:**

MS acquires clear counter and nonce through $EMSK_{WAAA(j-1)}$, which was pre-derived in the proposed key schedule of the full authentication or the previous round Intra-HO Pre-Auth. Subsequently, the related key sets ($MK_{WAAA(j)}$, $EMSK_{WAAA(j)}$, $MSK_{WAAA(j)}$, $TEKs_{WAAA(j)}$) are pre-derived by using proposed key derivation in full authentication or in Intra-HO Pre-Auth, Meanwhile, AT_XMAC and AT_RES are calculated as well as WAAA server. MS runs HMAC authentication to verify if the received AT_MAC is valid. In addition, MS also checks $Counter_{MS(j-1)} \leq Counter_{WAAA(j)}$. The counter attribute is pre-agreed upon between WAAA and MS. When accomplishing one round Intra-HO Pre-Auth, the counter value is continuously increased by one in both sides. If HMAC validation and counter synchronization are successful, MS sends an EAP-Response/AKA-challenge/Intra-HO Pre-Auth to WAAA, which includes AT_RES and $*AT\_Counter_{MS(j)}$.

- **STEP 7-9:**

WAAA matches received AT_RES with AT_XRES maintained in it-self and acquires clear $Counter_{WAAA(j)}$ by $EMSK_{WAAA(j)}$. In addition, WAAA also verifies if the received counter attribute is identical to $Counter_{WAAA(j)}$ maintained in it-self. If both validations are successful, $Counter_{WAAA(j)}$ is increased by one and stored back to its database. Then, WAAA sends a Radius Notify-Request to TAP, which includes the Reauth_ID, $MSK_{WAAA(j)}$ and $TEKs_{WAAA(j)}$. TAP also responds a Radius Notify-Accept message to WAAA for confirming the handover operation. Subsequently, WAAA pushes EAP-Success message to MS to inform Intra-HO Pre-Auth is successful. Finally, TAP and MS immediately seed $MSK_{WAAA(j)}$ into the four-way handshake protocol and the two-way handshake protocol to derive fresh PTK and GTK for enabling the subsequent 802.11i encryption.

After a successful Intra-HO Pre-Auth, if MS acquires an authentication with the current TAP again, FIL Re-authentication referred to [13] is immediately invoked for supporting stationary user re-authentication. On the other hand, if the MS roams to other TAP within the same WLAN domain, Intra-HO Pre-Auth will be invoked again. The combination of Intra-HO Pre-Auth and FIL Re-authentication indeed provides supporting non-roaming and roaming authentication services for a single user moving within the same WLAN domain and enhances re-authentication and Intra-domain HO authentication efficiency.

3.4. Proposed Inter-HO Pre-Auth Procedure

Inter-HO Pre-Auth is invoked between HAAA and MS when MS roams across different WLAN domains. The detailed procedures of Inter-HO Pre-Auth depicted in **Figure 6** are presented in the following steps:

- **STEP 1-3:**

When the roaming MS receives AAP's advertisement poor-signal and recognizes the need for Inter-domain HO process, MS replies Reauth_ID, Pseudo_ID and other encrypted attributes (TMSI, TWAAA_ID, TAP_ID)

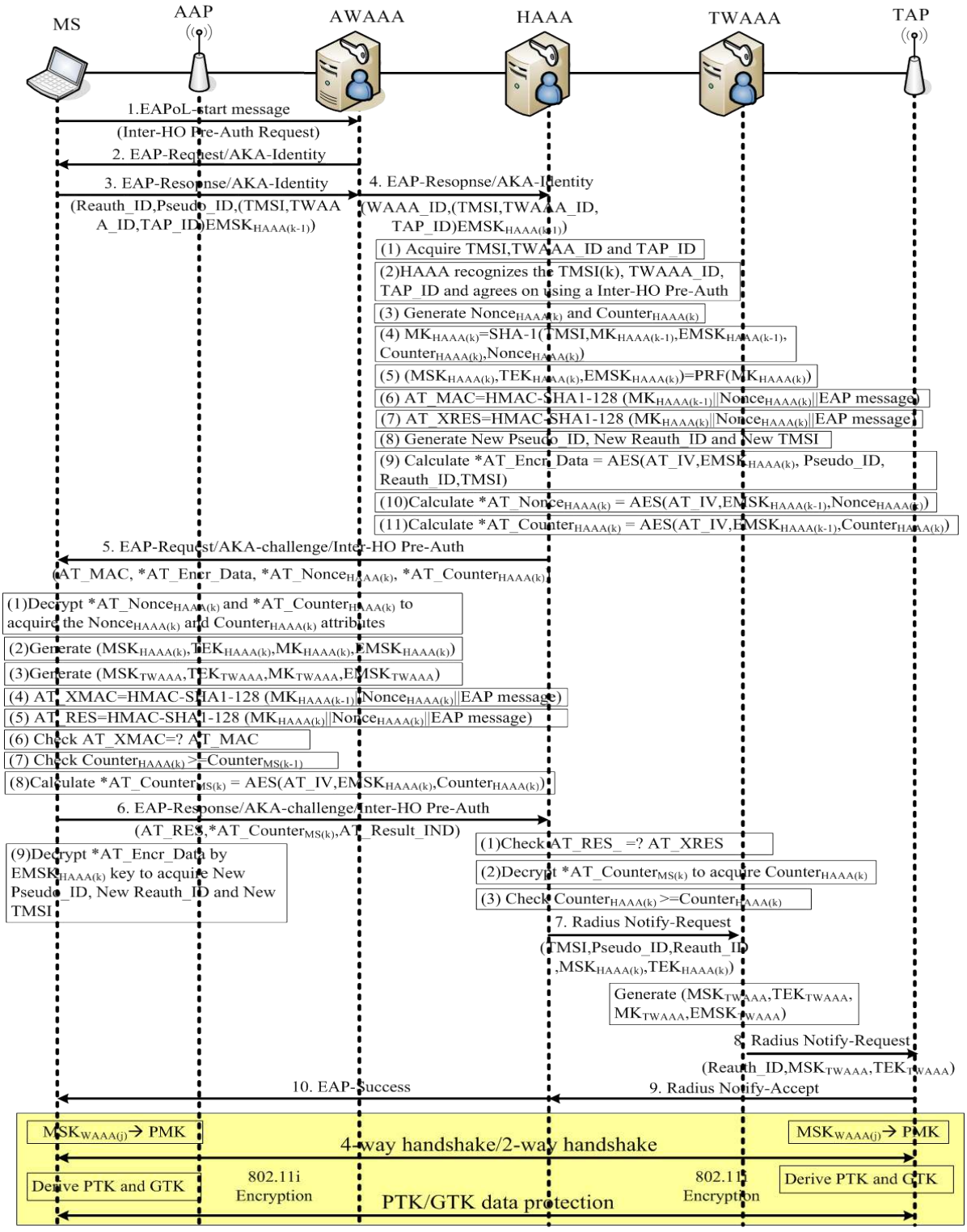

Figure 6. The detailed flow of proposed inter-ho pre-auth.

to AAP. Those encrypted attributes are protected by EMSK$_{HAAA(k-1)}$ key, which was pre-shared between HAAA and MS.

- **STEP4-5:**

Receiving the EAP-Response/AKA-Identity, AAP and Associated WAAA (AWAAA) match received Reauth_ID and Pseudo_ID, respectively. If both checks are positive, AWAAA immediately delivers Inter-HO Pre-Auth request to HAAA. HAAA immediately checks if the received TMSI is legal and recognizes that the MS is requesting an Inter-HO Pre-Auth. Then $Counter_{HAAA(k)}$ and $Nonce_{HAAA(k)}$ are generated first in HAAA. In addition, the proposed key derivation in **Figure 3** proceeds to derive related key sets ($MK_{HAAA(k)}$, $EMSK_{HAAA(k)}$, $MSK_{HAAA(k)}$, $TEKs_{HAAA(k)}$). AT_MAC and AT_XRES are calculated for subsequent HMAC authentication. Besides, new TMSI, Pseudo_ID and Reauth_ID are generated for using in the next round authentications like Inter-HO/Intra-HO Pre-Auth or FIL Re-authentication and are also encrypted with $EMSK_{HAAA(k)}$. Counter and nonce are secured by $EMSK_{HAAA(k-1)}$. Then, Inter-HO Pre-Auth challenge message included AT_MAC, *AT_Encr_Data, $*AT\_Nonce_{HAAA(k)}$ and $*AT\_Counter_{HAAA(k)}$ is forwarded to MS.

- **STEP6:**

Upon receiving the challenge message, MS first acquires clear counter and nonce by $EMSK_{HAAA(k-1)}$. Secondly,the related key sets ($MK_{WAAA(j)}$, $EMSK_{WAAA(j)}$, $MSK_{WAAA(j)}$, $TEKs_{WAAA(j)}$) and (MK_{TWAAA}, $EMSK_{TWAAA}$, MSK_{TWAAA}, $TEKs_{TWAAA}$) are derived by using Inter-HO Pre-Auth key derivation and Intra-HO Pre-Auth key derivation. MSK_{TWAAA} and $TEKs_{TWAAA}$ are used askey seeds to derive additional keys for the next round FIL Re-authentication. In addition, MSK_{TWAAA} is also designated as key seed to derive fresh PTK and GTK for subsequent 802.11i encryption between TAP and MS. Then, AT_MAC and AT_RES attributes are also generated for HMAC authentication with HAAA. If AT_MAC validation and counter synchronization check are positive, MS sends an EAP-Response/AKA-challenge/Inter-HO Pre-Auth message included AT_RES and $*AT\_Counter_{MS(k)}$ to HAAA.

- **STEP7-9:**

On receipt of the response message, HAAA verifies received AT_RES and $AT\_Counter_{MS(k)}$. If both verifications return positive, HAAA sends a Radius Notify-Request included TMSI, Pseudo_ID, Reauth_ID, $MSK_{HAAA(k)}$ and $TEKs_{HAAA(k)}$ to TWAAA. TMSI is used in the next round Inter-HO Pre-Auth. Pseudo_ID and Reauth_ID are used in the subsequent Intra-HO Pre-Auth and FIL Re-authentication, respectively. Then, TWAAA derives new key sets (MK_{TWAAA}, $EMSK_{TWAAA}$, MSK_{TWAAA}, $TEKs_{TWAAA}$) by Intra-HO Pre-Auth key derivation, and forwards Notify-Request to TAP. Finally, TAP responds the Radius Notify-Accept message to confirm the handover operation, and HAAA delivers EAP-Success message to MS for notifying Inter-HO Pre-Auth is successful. Then, TAP and MS seeds MSK_{TWAAA} into the four-way handshake protocol and two-way handshake protocol to derive new PTK and GTK for 802.11i encryption between them.

When MS roams to other WLAN domains and acquires a handover authentication again, Inter-HO Pre-Auth will be repeated again; moreover, all related key sets in Inter-HO/Intra-HO Pre-Auth and FIL Re-authentication are also together with updates.

4. Performance Evaluation

In this section, the handover authentication efficiency of Inter-HO Pre-Auth/Intra-HO Pre-Auth protocol is compared against that of standard EAP-AKA protocol. In reality, it is difficult to measure handover 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, etc. Thus, this paper only provides a proof-of-concept implementation and validation in the proposed protocol. Besides, the related parameters in this simulation model, based on the NS-2 with extensions for IEEE 802.11 model and written in C++ and OTcl language, are shown in **Table 1**. In the perspective of authentication performance, authentication delay is the major critical factor. In general, the authentication delay is calculated starting from reception of the EAP identity request message to reception of the last EAP-Success message. Thereby the expression of authentication delay (D_{Auth}) in simulation model canbe expressed as $\mathbf{D_{Auth} = D_{Proc} + D_T + D_{Prop}}$.

Where it encompasses processing delay (DProc), transmission delay (DT) and propagation delay (DProp). The definition of those elements may refer to [10] [13]. According to the trajectory of MS movement model in **Figure 7**, MS initially at location ❶ must acquire a full authentication via the AP1 resided in WLAN1 domain, and then a re-authentication is invoked with the AP1. Next, the MS continuously performs two round Intra-domain HO when moving from location ❷ to location ❹ within the WLAN1. When the MS moves from location ❹ to location ❺, an Inter-domain HO is occurred. From location ❺ to location ❼, the MS must perform two round Intra-domain HO within WLAN2 domain. Finally, an Inter-domain HO is invoked when the MS roams

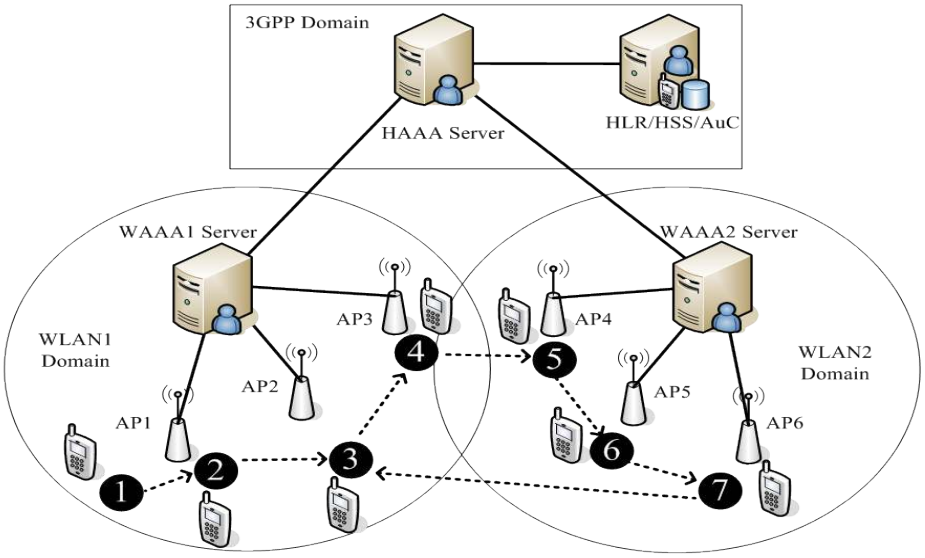

Figure 7. The trajectory of MS movement model.

Table 1. Assumption parameters.

Simulation Parameter			
Assumption Item	Assumption Value	Assumption Item	Assumption Value
MAC Protocol	802.11 g	Service radius of WAAA	1 (Km)
Simulation Area	4 (Km^2)	Service radius of single AP	0.1 (Km)
Number of HLR/HSS/Auc	1	Local AP Placement	Grid
Number of HAAA Server	1	MS Placement	Uniform
Number of WAAA Server	5	Average speed of MS	10 (Km/hr)
Number of Local AP	100	Direction of MS movement	[0, 2π]
Number of MS	100 - 1000	Simulation Time	1800 (Sec)

from location ⑦ to location ③. Since EAP-AKA does not specific any handover authentication mechanism, the MS must perform a long journey full authentication whenever an Inter-domain HO or an Intra-domain HO is needed.

As referring to the assumptions of authentication delay in [10] [13], standard full authentication delay and re-authentication delay can be expressed as $23*D_{Prop} + 16*D_{Proc}$ and $14*D_{Prop} + 14*D_{Proc}$. On the other hand, the authentication delay in FIL Re-authentication, Intra-HO Pre-Auth and Inter-HO Pre-Auth can be expressed as $6*D_{Prop} + 20*D_{Proc}$, $11*D_{Prop} + 23*D_{Proc}$ and $17*D_{Prop} + 23*D_{Proc}$, respectively. When the MS moves from location ① to location ②, the authentication delay in EAP-AKA protocol includes full authentication delay and re-authentication delay, and in proposed protocol encompasses full authentication delay and FIL Re-authentication delay. From location ② to location ④, two rounds Intra-domain HO process are occurred in which respectively results $2*(23*D_{Prop} + 16*D_{Proc})$ and $2*(11*D_{Prop} + 23*D_{Proc})$ handover authentication delay in EAP-AKA and in Intra-HO Pre-Auth. Intra-domain HO delay performance simulation illustrated in **Figure 8** shows the reduction in Intra-HO Pre-Auth reaches up to 49% and 23% compared to standard full authentication and re-authentication, respectively.

From location ④ to location ⑤, Inter-domain HO delay in EAP-AKA is distinctly equal to full authentication delay since a long journey full authentication must be invoked. Thus, the performance of Inter-domain HO delay is illustrated in **Figure 8**, and the delay reduction in Inter-HO Pre-Auth protocol reaches up to 26% compared to EAP-AKA full authentication protocol. Although the reduction in Inter-HO Pre-Auth protocol is nearly equiva-

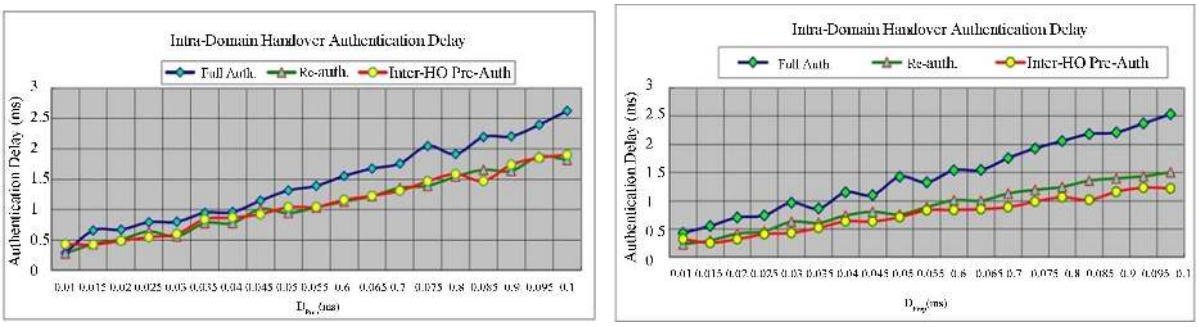

Figure 8. Intra-domain handover authentication delay comparison.

lent to standard re-authentication protocol, it might be an unrealistic comparison since standard re-authentication is not designated to handle the Inter-domain HO authentication.

5. Conclusion

Intra-HO Pre-Auth enables that the roaming user executes an authentication with the WAAA prior to performing Intra-domain HO procedure. It inherits key resources from the previous round proposed key schedule in standard full authentication or in Inter-HO/Intra-HO Pre-Auth, and thereby it supports the Intra-domain HO authentication without interacting with the HLR/HSS/AuC/HAAA. Similarly, Inter-HO Pre-Auth allows an authentication execution between the HAAA server and MS before performing Inter-domain HO procedure. It also re-uses key resources derived from the previous round proposed key schedule in standard full authentication or in Inter-HO Pre-Auth, which results in minimizing the redundant authentication signaling transactions between the HAAA and HLR/HSS/AuC. Indeed, the performance clearly shows that handover authentication delay reductions in Intra-HO Pre-Auth and in Inter-HO Pre-Auth reaches up to 49% and 26% compared to EAP-AKA. Besides, similar iteration strategy of FIL Ra-authentication is adopted by the proposed handover protocol to enable the repetitive execution in Inter-HO/Intra-HO Pre-Auth, which enhances the overall handover efficiency when the Inter-domain HO/Intra-domain HO process is invoked continuously and frequently. Finally, the integration of proposed handover authentication and FIL Re-authentication enable a single MS executing non-roaming authentication and roaming authentication.

References

[1] 3GPP TS 23.234, Rel. 6, v6.3.0 (2004) 3GPP System to Wireless Local Area Network (WLAN) Interworking; System Description.

[2] Ahmavaara, K., *et al.* (2003) Interworking Architecture between 3GPP and WLAN Systems. *IEEE Communication Magazine*, **41**, 74-81.

[3] Mingozzi, E., Stea, G. and Callejo-Rodríguez, M.A., *et al.* (2009) EuQoS: End-to-End Quality of Service over Heterogeneous Networks. *Computer Communications*, **32**, 1355-1370. http://dx.doi.org/10.1016/j.comcom.2008.12.013

[4] Koien, G.M. and Haslestad, T. (2003) Security aspects of 3G-WLAN interworking. *IEEE Communication Magazine*, **41**, 82-88. http://dx.doi.org/10.1109/MCOM.2003.1244927

[5] Choi, H.H., Song, O. and Cho, D.H. (2004) A Seamless Handoff Scheme for UMTS-WLAN Interworking. *Proceedings of IEEE Globalcom*, **3**, 559-1564.

[6] Cao, J., Li, H., Ma, M., *et al.* (2012) A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks. *Journal Computer Networks*: *The International Journal of Computer and Telecommunications Networking*, **56**, 2119-2131.

[7] 3rd Generation Partnership Project (2006) 3G security; WLAN Interworking Security (Release 7). 3GPP Technical Specifications TS 33.234 v7.0.0, 3GPP, Valbonne.

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

[9] Aboba, B., *et al.* (2003) RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP). RFC 3576.

[10] Lin, S.-H., Chiu, J.-H. and Lee, G.-R. (2010) A Fast Iterative Localized Re-authentication Protocol for Heterogeneous

Mobile Networks. *IEEE Transaction on Consumer Electronic*, **56**, 2267-2276. http://dx.doi.org/10.1109/TCE.2010.5681099

[11] Lin, S.H., Chiu, J.H. and Shen, S.S. (2010) Performance Evaluation of the Fast Authentication Schemes in GSM-WLAN Heterogeneous Networks. *Journal of Networks*, **5**, 956-963. http://dx.doi.org/10.4304/jnw.5.8.956-963

[12] Lin, S.-H., Chiu, J.-H. and Shen, S.-S. (2011) The Performance Evaluation of Fast Iterative Localized Re-Authentication for 3G/UMTS-WLAN Interworking Networks. *Journal of Ambient Intelligence and Humanized Computing*, **4**, 209-221.

[13] Lin, S.-H., Chiu, J.-H. and Shen, S.-S. (2011) A Fast Iterative Localized Re-authentication Protocol for UMTS-WLAN Heterogeneous Mobile Communication Networks. *EURASIP Journal on Wireless Communications and Networking*, **2011**, 124.

[14] IEEE (2004) Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE Std 802.11.

[15] Pack, S. and Choi, Y. (2004) Fast Handoff Scheme based on Mobility Prediction in Public Wireless LAN Systems. *IEEE Proceedings Communications*, **151**, 489-495. http://dx.doi.org/10.1049/ip-com:20040834

[16] Mukherjee, A., Joshi, T. and Agrawal, D.P. (2005) Minimizing Re-Authentication Overheads in Infrastructure IEEE 802.11 WLAN Networks. *Proceedings of IEEE Wireless Communications and Networking Conference* (WCNC'05), **4**, 2344-2349.

[17] Hur, J., Park, C. and Yoon, H. (2007) An Efficient Pre-Authentication Scheme for IEEE 802.11-Based Vehicular Networks. *Advances in Information and Computer Security*, **4752**, 121-136. http://dx.doi.org/10.1007/978-3-540-75651-4_9

[18] Lee, M., Kim, G. and Park, S. (2005) Seamless and Secure Mobility Management with Location-Aware Service (LAS) Broker for Future Mobile Interworking Networks. *Journal of Communications and Networks*, **7**, 207-221. http://dx.doi.org/10.1109/JCN.2005.6387867

[19] Arbaugh, W., Mishra, A. and Shin, M. (2004) Context Caching Using Neighbor Graphs for Fast Handoffs in a Wireless Network. *IEEE INFOCOM*. 23*rd Annual Joint Conference of the IEEE Computer and Communications Societies*, **1**, 11.

[20] Mishra, A., Shin, M., Petroni Jr., N.L., Clancy, T.C. and Arbaugh, W.A. (2004) Proactive Key Distribution Using Neighbor Graphs. *IEEE Wireless Communications*, **11**, 26-36. http://dx.doi.org/10.1109/MWC.2004.1269714

[21] Kassab, M., Belghith, A., Bonnin, J.M. and Sassi, S. (2005) Fast Pre-Authentication Based on Proactive Key Distribution for 802.11 Infrastructure Networks. *Proceedings of the* 1*st ACM International Workshop on Wireless Multimedia Networking and Performance Modeling* (WMuNeP'05), Montreal, 13 October 2005, 46-53.

[22] Al Shidhani, A. and Leung, V.C.M. (2009) Pre-Authentication Schemes for UMTS-WLAN Interworking. *EURASIP Journal on Wireless Communications and Networking*, **2009**, Article ID: 806563.

[23] Abiona, O., Oluwaranti, A., Oluwatope, A., Bello, S., Onime, C., Sanni, M. and Kehinde, L. (2013) Wireless Network Security: The Mobile Agent Approach. *International Journal of Communications*, *Network and System Sciences*, **6**, 443-450. http://dx.doi.org/10.4236/ijcns.2013.610046