3G 與 WLAN 整合式網路下具完整匿名性的認證協定

An efficient authentication protocol with perfect anonymity for 3G/WLAN interworking

詹進科 [1,*]　　簡宏宇 [2]　　鄧鴻毅 [2]
Jinn-Ke Jan　　Hung-Yu Chien　　Hung-Yi Teng

[1] 國立中興大學資訊科學研究所
Department of Computer Science
National Chung Hsing University
Taichung, Taiwan, Republic of China

[2] 朝陽科技大學資訊管理系
Department of Information management
Chaoyang University of Technology
Taichung, Taiwan, Republic of China

摘　　要

本論文提出了在第三代行動通訊與無線區域網路整合式網路下具完整匿名性的認證協定。首先，提出一整合第三代行動通訊與無線區域網路的網路架構、認證模型與認證協定應具備的要素。再介紹錯誤更正碼與單向雜湊鍊，可以提供驗證時使用者身份不會被曝露，及提升認證程序整體效能。基於以上方法，我們提出了一個具完整匿名性及效率性的認證協定，可以提供使用者身份在整個認證過程中完整的保護，因為即使使用者第一次進行驗證時身份也無法被任何人探知，並且行動通訊業者可以不需要花費多餘成本去維護使用者金鑰的資料庫。相較於目前已提出的方法，EAP-AKA 與 W-SKE，本方法整體大幅降低了通訊與運算成本。最後，藉由實驗的結果，可以證明我們所提出的方法是較有效率的。

關鍵詞：第三代行動通訊、無線區域網路、整合式網路、認證、匿名性、錯誤更正碼

Abstract

An efficient authentication protocol is crucial to the success of 3G/WLAN interworking. This paper, based on error correction codes, one-way hashing and symmetric cryptography, proposes a new authentication scheme for integrated 3G/WLAN networks. The new scheme provides perfect anonymity because it does not expose mobile users' identifiers on the air even they are authenticated for the first time. Additionally, it greatly improves the communication performance.

Keyword：3G、WLAN、Interworking、Authentication、Anonymity、EAP-AKA、W-SKE、Error correction codes

* 通訊作者

1. Introduction

Although the third generation cellular network (3G) can provide higher data capacity (up to 2Mb/s) than 2G cellular network to support new services (videophone or video streaming) for mobile subscribers, it suffers from the limited data rate and expensive deployment. In contrast, wireless local area networks (WLAN) [7][8] are adopted widely by service providers in small areas or hotspots, because of their cost-effectiveness, ease of deployment and high data rates (802.11g up to 54 Mb/s) in an unlicensed frequency band. However, WLAN can not cost-efficiently provide the wide coverage 3G does. In order to provide ubiquitous wireless communications at high data rate and large varieties of services in the hotspots and campus-wide areas, 3G service providers regard WLAN as a technology to compliment their 3G system. Therefore, integrating both WLAN and 3G network is seen as an ideal choice for 3G service providers.

Third Generation Partnership Project (3GPP)[1] looks into the feasibility of integrating 3G and WLAN and discusses six common inter-working scenarios in an incremental set of services and operational features. Currently, scenarios 2 and 3, where an IP connectivity is activated via WLAN for 3G subscribers, are more attractive and attainable, because they allow 3G users to access high-data-rate IP services of WLAN, and the WLAN does not need to confirm to the complicated 3G access/core network interfaces. In such mixed infrastructure environments, the mobile subscribers should be authenticated by an authentication, authorization, and accounting (AAA) server before they can actually access whatever services allowed. In general, the following elements should be involved in the authentication process: mobile subscriber (MS), authentication system (AS) of visited WLAN (for example, AP in 802.11), foreign AAA server of visited WLAN (F-AAA) and home AAA server of mobile subscriber (H-AAA).

There are several main concerns in the authentications– the protection of user's identity, the efficiency of the protocol, and the generation of secure authenticated key. User identity privacy (anonymity) is used to avoid exposing any information about permanent subscriber identification. Exposing once permanent identification would compromise the subscriber's location on the radio interface, and allow different communications of the same subscriber on the radio interface to be linked. The efficiency of the protocol is to minimize the authentication latency that a roaming user experiences. So, an authentication protocols should minimize the message sizes and the number of exchanges between foreign domain and home domain. Additionally, the low computational power of mobile stations should be considered, which means an authentication protocol requiring heavy computation on the mobile stations is not applicable.

Regarding potential authentication protocols, EAP-AKA and EAP-SIM [2][3][6] have been proposed (by 3GPP) as the authentication protocols for 3G/WLAN interworking. Both EAP-AKA and EAP-SIM provide user anonymity through temporary identities, or pseudonyms, which are equivalent to but separate from the Temporary Mobile Subscriber Identities (TMSI). However, the real identity of mobile subscribers is exposed to the air when authenticating mobile subscribers at the first time. This might cause the identity of the user to be exposed and traced at some time periods. Moreover, EAP-AKA and EAP-SIM do not minimize the number of exchanges between the foreign domain and home domain. It, therefore, incurs long latency when mobile users roam into foreign environments. Salgarelli et al. [11] noticed the long latency of both EAP-SIM and EAP-AKA, and proposed W-SKE to reduce the number of messages exchanged and to minimize the latency. However, there are several weaknesses inherent in W-SKE: (1) W-SKE cannot prevent a F-AAA from overcharging H-AAA if the F-AAA is dishonest; (2) protection of subscriber's identity is not considered; (3) the authentication latency is not optimized.

Park [9] has proposed an authentication protocol with anonymity and untraceability, which is based on the secret-key certificate and the algebraic structure of error-correcting codes. The concept of the secret-key certificate, originally due to [5], provides a means for the authentication server to get rid of maintaining a secure database of subscribers' secrets. Park's scheme further encodes the secret-key certificate, by using the transformation of error correction codes and by adding artificial error vector, such that user anonymity and untraceability are achieved. However, the protocol is one-way authentication only, and is not designed for the integrated 3G/WLAN environment.

In this paper, we propose a new authentication protocol to improve the performance in several respects: (1) user's identity is never exposed even the user is authenticated for the first time; (2) AAA servers do not need to keep secret databases for subscriber's secret keys; (3) the authentication latency is greatly improved. Combining the technique based on secret-key certificate, the algebraic of the error correcting code and temporary identity, our protocol can protect user's anonymity through the whole process. The rest of the paper is organized as follows. Section 2 introduces our model and the requirements. Section 3 proposes our protocol, which is followed by the security analysis and the performance analysis in Section 4. Finally, Section 5 states our conclusions.

2. Requirements and Authentication model

2.1 Network architecture

The network architecture as shown in Figure 1 is considered for 3G/WLAN interworking in this paper. In the architecture, MS denotes mobile user, H-AAA denotes home AAA server of a mobile user MS, and F-AAA denotes foreign AAA server of the WLAN that a mobile user MS want to visit. If the F-AAA and the H-AAA belong to separate providers, the association between the F-AAA and the AAA proxies (brokers) as well as those between the AAA proxies and H-AAA should be set up. The AAA broker sets up appropriate security associations and routes AAA messages to appropriate H-AAAs. Hence, the path between the F-AAA of the visited WLAN and the H-AAA in the home network may pass several hops of intermediate AAA relays that are part of the broker network.

2.2 The authentication model

Our authentication model is based on Salgarelli's work [11]. The authentication model directly corresponds to the network architecture introduced in previous section. Figure 2 illustrates the various network entities involved in the authentication procedure. In order to authenticate and/or protect data in transit between X and Y, a security association $A_{X,Y}$ should be set up and can be defined as the combination of the nodes' identity information (e.g., NAIs), some form of cryptographic keys (e.g., public keys, pre-shared symmetric keys), and information on cryptographic algorithms to be used.

In the model, several security associations are identified and set up for providing communication privacy. Each MS shares a security association $A_{MS,H\text{-}AAA}$ with its H-AAA server. In the authentication phase, the MS communicates with an authentication system (AS) that is part of a network element like an AP in an 802.11 network. We assume that each AS has a unique identity (ASID) that is meaningful to the MS. For example, the ASID of an AP could be represented by its Extended Service Set ID (ESSID) in an 802.11 network (e.g., taichung.tw.hotspot.com). The ESSID is used in networks to identify the name of each LAN.

Each AS maintains a preconfigured security association $A_{AS,F\text{-}AAA}$ with its F-AAA server. We also assume that a security association $A_{F\text{-}AAA,H\text{-}AAA}$ exists between F-AAA and H-AAA, which allows them to authenticate and/or encrypt each other's message. In the 3G/WLAN interworking network, F-AAA and H-AAA may belong to separate service providers, and then an association has to be set up via an AAA broker or explicit pair-wise relationship should be setup as part of roaming agreement. For simplicity, we assume that a pre-configured security association exists between any pair of adjacent nodes on the network path between the AS and H-AAA. One of the objectives of the authentication model is to setup temporary per-session association and cryptographic keys between MS and AS, $A_{MS,AS}$. These keys are used to encrypt and authenticate data exchanged between MS and AS.

2.3 Protocol requirements

The requirements that an authentication protocol for 3G/WLAN interworking should satisfy include the following points. (1) Network efficiency: The protocol has to minimize the number of exchanges between the F-AAA and H-AAA. (2) User anonymity: Prevent the MS's real identity from being exposed to the wireless environment. (3) Mutual Authentication: both H-AAA and MS can authenticate each other. So do MS and F-AAA. (4) Secure session key exchange: in each session, the session key should be fresh, random, and distinct. (5) Forward secrecy: Even if an attacker happens to derive the cryptography key of one

session, the future sessions will be not compromised. (6) Fraud protection: The system should prevent unauthorized users from obtaining services from visited network, and prevent F-AAA from overcharging H-AAA.

3. A New Authentication Protocol

In this section, we propose a new authentication protocol with user anonymity and untraceability for 3G/WLAN interworking. The protocol aims to satisfy all requirements discussed earlier. Especially, home/foreign domain does not need to keep a secure database for maintaining registered users' secret keys, and therefore the overhead on H-AAA/F-AAA is reduced. The protocol consists of three phases: subscription phase, full authentication phase, and fast re-authentication phase. In the subscription phase, H-AAA issues MS an encoded secret-key certificate that contains the MS's real identity, a hashed value, and the master key shared between MS and its H-AAA.

When the MS roams to a new foreign domain or when the encoded secret-key certificate issued by F-AAA becomes expired, the full authentication phase is performed. The full authentication phase involves MS, AS, F-AAA and H-AAA. Once a full authentication has been executed, the MS also receives another encoded secret-key certificate issued by F-AAA. The secret-key certificate issued by F-AAA contains the MS's temporal identity, a hashed value, and the master key shared between MS and F-AAA. After one successful execution of full authentication, MS can perform several times of fast re-authentications, by using an un-expired the secret-key certificate. The lifespan of each secret-key certificate should be defined in the roaming agreement. The fast re-authentication phase only involves MS, AS and F-AAA.

3.1 Preliminaries

Error correction codes and anonymity

Now we briefly introduce the concept of error correction codes as follows. A linear error correction code of length N, dimension K, and minimum distance D is denoted by (N, K, D), and the codes can be defined by its generator matrix G. G denotes the K-by-N generator matrix. A binary K-tuple m can be encoded to an N-bit codeword by computing $c = (c_1c_2\cdots c_{N-1}c_N) = m \cdot G$. If an error vector e is added to the codeword c, then the final transmission vector is $r = c + e$. Assume that the Hamming weight of the error vector e is less than or equal to $t = \lfloor (D-1)/2 \rfloor$, then r can be decoded into c based on the syndrome vector $s = r \cdot H^T$, where H denotes an (N-K)-by N party-check matrix such that $G \bullet H^T = 0$.

Park [9] utilized the added error vector to convey additional information. The concept is to transform the additional information into an error vector with hamming weight t such that both the error vector e and the codeword c can be recovered by the receiver who has the parity-check matrix H. Since there are N bits in a codeword, there are distinct error vectors with weight t. Let z_i denotes the additional information, and $|z_i|$ denotes its bit length. So, for $|z_i| < \left\lfloor \log_2 \binom{N}{t} \right\rfloor$, the information can be transformed into an error vector e with Hamming weight t, by using the order-preserving mapping induced by the lexicographic order of the vectors and the natural order of the integers [4][10]. Algorithm 1 and 2 are used to transform the information into the error vector and the error vector back into the information respectively. Let the codeword carry the user's related information and let the added error vector carry the random-generated authentication information for each session, Park's scheme can achieve anonymity and un-linkability through the authentication processes.

Algorithm 1

$$
\begin{aligned}
&\text{for } j = 1,2,\ldots,N \{ \\
&\quad \text{if } z_i \geq \binom{N-j}{t} \text{ then } \{ e_j^{(i)} \leftarrow 1; \\
&\qquad\qquad z_i \leftarrow \left(z_i - \binom{N-j}{t}\right); t \leftarrow (t-1); \} \\
&\quad \text{else } e_j^{(i)} \leftarrow 0; \\
&\}
\end{aligned}
$$

Algorithm 2

$$
\begin{aligned}
&\text{for } j = 1,2,\ldots,N \{ \\
&\quad \text{if } z_i \geq \binom{N-j}{t} \text{ then } \{ e_j^{(i)} \leftarrow 1; \\
&\qquad\qquad z_i \leftarrow \left(z_i - \binom{N-j}{t}\right); t \leftarrow (t-1); \} \\
&\quad \text{else } e_j^{(i)} \leftarrow 0; \\
&\}
\end{aligned}
$$

Unbalanced one-way binary tree

In our scheme, we will use the unbalanced one-way binary tree (UOBT) [12] to accelerate the authentication process. Now we introduce UOBT. Let $P_{0,0}$ denotes one randomly chosen integer. Now we compute $P_{i,0} = h_1^i(P_{0,0})$ for $i = 1 \sim n$, and $P_{i,j} = h_2^j(P_{i,0})$ for $j = 1 \sim m$. That is, $P_{2,0} = h_1^2(P_{0,0}) = h_1(h_1(P_{0,0}))$ and $P_{2,2} = h_2^2(P_{2,0}) = h_2(h_2(P_{2,0}))$. Then, a UOBT with initial seed $P_{0,0}$ can be depicted in Figure 3, where the chain $(P_{0,0}, P_{1,0}, ..., P_{n,0})$ is called the main chain, and the chains $(P_{i,0}, P_{i,1}, ..., P_{i,m})$ for $i \in [0, n-1]$ are called the sub-chains in this paper. The main chain will be used to authenticate a mobile user to its H-AAA in the full authentication phase, where the value $P_{i,0}$ for $i = 0 \sim n-1$ is used as the authentication token in (*n-i*)th full authentication. While each sub-chain $(P_{i,0}, P_{i,1}, ..., P_{i,m})$ could be used to authenticate a mobile user to a F-AAA in the fast re-authentications and the value $P_{i,j}$ will be used as the (*m-j*)th fast re-authentication token in the F-AAA, if the F-AAA involves in the full authentication using $P_{i,0}$. *n* specifies the maximum numbers of allowed full authentications for each H-AAA issued certificate, and *m* specifies the maximum numbers of allowed fast re-authentications for each F-AAA issued certificate. *n* and m should be pre-defined in the agreement.

3.2 The detailed protocol

Now we are ready to present our protocol in details. Initially, each AAA server (H-AAA and F-AAA) sets up its own secret parameters- the generator matrix *G*, the party-check matrix *H*, and the server secret key. The matrices of H-AAA are denoted as G_{H-AAA} and $H_{H\text{-}AAA}$, and those of F-AAA are denoted as G_{F-AAA} and H_{F-AAA}. The secret key of H-AAA is denoted as K_{H-AAA}, and that of F-AAA is denoted as K_{F-AAA}. Each mobile user (MS) has a device that enables the encryption algorithm and the order-preserving mapping algorithms. Now we describe the three phases of our protocol - subscription phase, full authentication phase, and fast re-authentication phase- as follows.

Table 1. Notations

Notation	Meaning
h_1, h_2	One-way hashing functions
K_A	The secret key of A
$K_{A,B}$	The shared key between A and B
m_A	The secret-key certificate generated by A
G_A	The generator matrix of A
H_A	The parity check matrix of A
c_A	The encoded secret-key certificate generated by A
$E_K()$	A symmetric-key encryption using the key K
$PRF_K()$	A pseudo-random function with the key *K*
r	The transmission vector
UID	The real identity of the subscriber
TID	The temporal identity of the subscriber
SID	The session identity of the subscriber
ASID	The unique identity of the AS
$AUTH_A$	The message authentication code computed by A

The subscription phase

To subscribe the service, MS first chooses an integer $P_{0,0}$, computes $P_{n,0}$, and sends its real identity (*UID*) and the value $P_{n,0}$ to its H-AAA through a secure channel. H-AAA randomly generates a shared key $K_{MS,H-AAA}$ for the MS, computes a secret-key certificate $m_{H\text{-}AAA} = E_{K_{H\text{-}AAA}}(UID||P_{n,0}||K_{MS,\text{-}H\text{-}AAA}||valid\_time)$, where *valid_time* denotes the valid time period of this certificate, and $E_{K_{H-AAA}}()$ denote the encryption using the key K_{H-AAA}. H-AAA encodes the certificate as a codeword c_{H-AAA}

$= m_{H-AAA} \cdot G_{H-AAA}$, and sends MS the values ($K_{MS,H-AAA}$, c_{H-AAA}) through a secure channel. Please notice that H-AAA does not need to keep the secret database for storing the values $K_{MS,H-AAA}$.

The full authentication phase

Figure 4 depicts the successful execution of *i*-th full authentication, and the steps are described as follows.

1. MS send a START message: MS initiates the protocol by sending a START message, when it listens to *ASID*s broadcasts by the AS or explicitly probes for the presence of the AS.
2. AS inquires MN ID.
3. MS prepares the transmission vector *r*: MS computes the *i*-th authentication token of the main chain, $P_{n-i,0}$, and then transform the value $[i \| P_{n-i,0}]$ into an error vector *e* with length *N* and hamming weight *t* = $\lfloor (D-1)/2 \rfloor$, using the mapping algorithm 1. It adds the error vector *e* to the encoded certificate c_{H-AAA} to get the transmission vector $r = c_{H-AAA} + e$.
4. MS sends the transmission vector *SID*, *r* to AS. *SID* denotes the session identifier.
5. AS relays MS response and its identity *ASID* to F-AAA.
6. F-AAA forwards MS's response and *ASID* to the appropriate H-AAA using pre-established secure channel.
7. H-AAA processing: H-AAA performs the following steps:
   - H-AAA uses the parity matrix HH-AAA and the reverse mapping algorithm 2 to derive the value $[i \| P_{n-i,0}]$ as well as the encrypted certificate m_{H-AAA}. It then decrypts the certificate to get the data ($UID, P_{n,0}$, $K_{MS,-H-AAA}$, $valid\_time$).
   - H-AAA checks whether MS' s real identity *UID* and the valid time *valid_time* are still valid. If so, it further checks whether (1) *i* is larger than the counter value stored in its database, and (2) $h_1^i(P_{n-i,0})$ equals $P_{n,0}$. If all the verifications succeed, H-AAA accepts this request and updates the stored counter as *i*.
   - From *ASID*, H-AAA notices that the MS is visiting the foreign domain, and may ask for services from the domain for a period of time. In order to allow the F-AAA to perform fast re-authentications of the MS on behalf of itself, H-AAA uses $P_{n-i,0}$ as a seed to generate the sub-chain ($P_{n-i,0}, P_{n-i,1}, ..., P_{n-i,m}$).
   - H-AAA computes its response $AUTH_{H-AAA}$, the session key $K_{MS,AS}$ between MS and AS, and the temporary master key $K_{MS,\text{-F-}AAA}$ between MS and F-AAA as follows:

$$AUTH_{H-AAA} = MAC_{K_{MS,H-AAA}}(P_{n-i,0} || UID || SID || ASID) \quad (1)$$

$$K_{MS,AS} = PRF_{K_{MS,H-AAA}}(AUTH_{H-AAA}) \quad (2)$$

$$K_{MS,F-AAA} = PRF_{K_{MS,H-AAA}}(P_{n-i,m} || AUTH_{H-AAA}) \quad (3)$$

8. H-AAA sends an AAA message which includes *TID*, $P_{n-i,m}$, $K_{MS,\text{-F-}AAA}$, $AUTH_{H-AAA}$ and $K_{MS,AS}$ to F-AAA, where *TID* is the temporary identifier for MS.
9. F-AAA sends $AUTH_{H-AAA}$, $K_{\text{F-AAA}}$, *TID* and c_{F-AAA} to AS: F-AAA uses its secret key $K_{\text{F-AAA}}$ to generate a secret-key certificate $m_{F-AAA} = E_{K_{F-AAA}}(TID || P_{n-i,m} || K_{MS,F-AAA} || valid\_time)$, and then decodes it into a codeword of length by computing $c_{F-AAA} = m_{F-AAA} \cdot G_{F-AAA}$. Finally, it sends an AAA message includes $AUTH_{H-AAA}$, $K_{MS,AS}$, *TID* and the encoded secret-key certificate, c_{F-AAA}, to AS.
10. AS processing of F-AAA message: AS extracts from the AAA message and forwards $AUTH_{H-AAA}$, $K_{MS,\text{AS}}(TID)$ and c_{F-AAA} to the MS.
11. MS processing of AS's message: MS verifies $AUTH_{H-AAA}$ as per Eq. 1, which should successfully prove the authentication of H-AAA's to MS. Using $AUTH_{H-AAA}$, MS can locally generate the session key $K_{MS,AS}$ and the temporary master key $K_{MS,F-AAA}$ as Equation 2 and Equation 3. Finally, it uses the key $K_{MS,AS}$ to decrypt $K_{MS,\text{AS}}(TID)$ and get *TID*. It finally stores the encoded cer-

tificate $c_{F\text{-}AAA}$ and the counter j=0 that will enable MS to perform fast re-authentications in F-AAA's domain for up to m times fast re-authentications.

Please notice that, before using up the main chain, the MS should subscribe for the next secret key certificate by submitting related data, and the H-AAA should generate the new certificate for the MS. This process can be done through a successful full authentication.

The fast re-authentication phase

After one successful execution of full authentication, MS has obtained one encoded certificate issued by F-AAA, and has shared one master key $K_{MS,\text{-F-}AAA}$ with F-AAA. Please notice that F-AAA does not need to keep the secret key $K_{MS,\text{-F-}AAA}$, since F-AAA can derive the secret key when MS returns the encoded certificate. MS can request up to m times of fast re-authentications from F-AAA during the valid period of the certificate. The successful execution of the j-th fast re-authentication is depicted in Figure 5, and the steps are described as follows.

The step 1 and 2 are same as those of the full authentication procedure.

3. MS prepares the transmission vector r: MS computes the j-th authentication token of the sub chain, $P_{n-i,m-j}$, and then transform the value $[j \| P_{n-i,m-j}]$ into an error vector e with length N and hamming weight $t = \lfloor (D-1)/2 \rfloor$, using the mapping algorithm 1. It adds the error vector e to the encoded certificate $c_{F\text{-}AAA}$ to get the transmission vector $r = c_{F\text{-}AAA} + e$.
4. MS sends *SID* and r to AS.
5. AS relays the MS response and *ASID* to F-AAA.
6. F-AAA's processing:
   - F-AAA uses the parity matrix $H_{F\text{-}AAA}$ and the reverse mapping algorithm 2 to derive the value $[j \| P_{n\text{-}i,m-j}]$ as well as the encrypted certificate $m_{F\text{-}AAA}$. It then decrypts the certificate to get the data $(TID, P_{n\text{-}i,m}, K_{MS,F\text{-}AAA}, valid\_time)$.
   - F-AAA checks whether MS's identity TID and the valid time *valid_time* are still valid. If so, it further checks whether (1) j is larger than the counter value stored in its database, and (2) $h_2^{\,j}(P_{n\text{-}i,m-j})$ equals $P_{n\text{-}i,m}$.
   - If all the verifications succeed, F-AAA updates its local counter, and generates the session key $K_{MS,AS}$ and the authentication code $AUTH_{F\text{-}AAA}$ as follows.

$$AUTH_{\text{F-AAA}} = MAC_{K_{MS,F\text{-}AAA}}(P_{n-i,m-j} \| TID \| SID \| ASID) \quad (4)$$

$$K_{MS,AS} = PRF_{K_{MS,F\text{-}AAA}}(AUTH_{F\text{-}AAA}) \quad (5)$$

7. F-AAA sends an AAA message which includes $AUTH_{F\text{-}AAA}$ and $K_{MS,AS}$ to the AS.
8. AS processing of F-AAA message: AS extracts $K_{MS,AS}$ from the AAA message and forwards $AUTH_{F\text{-}AAA}$ to the MS.
9. MS processing of AS message: MS verifies $AUTH_{F\text{-}AAA}$ as per Eq. 4, which proves the authentication of F-AAA's to MS. Then, it generates $K_{MS,AS}$ locally using Eq. 5. The fast re-authentication is done.

4. Security and Performance Analysis

4.1 Security analysis

In this section, we analyze the security properties of the proposed protocol.

Perfect user Anonymity — The secret-key certificates issued by H-AAA and by F-AAA respectively are used to identify the mobile user, and no other identification information is transmitted. Only the issuer (H-AAA or F-AAA) is able to decrypt the corresponding certificate and retrieve the identifier (or temporary identifier). Unlike EAP-SIM and EAP-AKA where the user identifier (NAI based on IMSI) is transmitted for each time when the temporary identifier is not available, our scheme never exposes any user's identification. Therefore, perfect anonymity is achieved.

Mutual Authentication — In the i-th execution of full authentication, H-AAA can authenticate MS by verifying the chain value $[i \| P_{n-i,0}]$ encoded in the transmission vector r, and MS can authenticate H-AAA by verifying $AUTH_{H\text{-}AAA}$. Likewise, in the j-th fast re-authentication, F-AAA can authenticate MS by verifying the encoded value $[j \| P_{n\text{-}i,m-j}]$, and MS can verify F-AAA by the authenticator $AUTH_{F\text{-}AAA}$. So, mutual authentication is achieved.

Secure session key establishment — The freshness and randomness of the session keys (generated according to Eq. 2 and Eq. 5) follows from

the freshness of $AUTH_{H\text{-}AAA}$, $AUTH_{\text{F-AAA}}$ and the properties of pseudo-random functions. The security of the session keys are based on the privacy of the master keys $K_{MS,H\text{-}AAA}$ or $K_{MS,F\text{-}AAA}$. Therefore, those session keys are secure.

Forward Secrecy — Since each session key is distinct, random and independent, disclosure of one session key will not compromise other session keys.

4.2 Performance analysis

We now evaluate the efficiency of our scheme in terms of authentication latency in more details. Let $T_{F-AAA,H-AAA}$ denotes the one trip latency between H-AAA and F-AAA, $T_{F-AAA,AP}$ denotes that between F-AAA and AP, and $T_{MS,AP}$ denotes that between MS and AP. The authentication latency of our full authentication is $2T_{F-AAA,H-AAA} + 2T_{F-AAA,AP} + 2T_{MS,AP}$, that of our fast reauthentication is $2\ T_{F-AAA,AP} + 2\ T_{MS,AP}$, that of W-SKE scheme is $2T_{F-AAA,H-AAA} + 4T_{F-AAA,AP} + 6T_{MS,AP}$, and that of EAP-AKA is $4\ T_{F-AAA,H-AAA} + 4\ T_{F-AAA,AP} + 6\ T_{MS,AP}$. Under the figures that $T_{F-AAA,H-AAA}$ = 130 ms, $T_{F-AAA,AP}$ = 25ms and $T_{MS,AP}$ = 2 ms, EAP-AKA takes 632 ms, W-SKE takes 372 ms, our full authentication takes 314 ms, and our fast re-authentication takes 54 ms. Assume the average number of executed fast re-authentications per full authentication is 15, our scheme averagely takes 70 ms. For such cases, our scheme takes only 19% time of W-SKE, and takes only 11% time of EAP-AKA.

Figure 6 shows the authentication latencies of various schemes, under the figures that $T_{F-AAA,H-AAA}$ = 130 ms, $T_{F-AAA,AP}$ = 25ms and $T_{MS,AP}$ = 2 ms. “15:1” denotes that there are average 15 fast re-authentications per full authentication in our scheme, and “30:1” denotes that there are averagely 30 fast re-authentications per full authentication. From the figure, we can see that our scheme greatly improves the authentication latency.

6. Conclusions

In this paper, based on error correction codes, one-way hashing and symmetric cryptography, we propose an efficient authentication protocol with perfect user anonymity and untraceability for integrated 3G/WLAN networks. Compared to its counterparts, the new scheme own several practical merits: (1) it provides perfect anonymity, (2) it eliminates the overhead of maintaining the secret key database of registered users, and (3) it greatly improves the communication performance. Under practical figures, it takes only 19% authentication latency of W-SKE, and takes only 11% that of EAP-AKA.

References

[1] 3GPP TR 22.934, “Feasibility study on 3GPP system to wireless local area network (WLAN) interworking (Release 6),” v. 6.2.0, Sep. 2003.

[2] 3GPP TS 33.234, “3G Security; Wireless Local Area Network (WLAN) Interworking Security,” v. 6.3.0, Release 6, Dec 2004.

[3] Arkko, J. and H. Haverinen, “Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement (EAP-AKA),” Internet Draft (Work in progress), draft-arkko-pppext-eap-aka-12, April 2004.

[4] Cover, T.M., “Enumerative source encoding,” IEEE Transactions on Information Theory, Volume: 19, Issue: 1, Jan. 1973, Pages: 73–77.

[5] Davis, D., R. Swick, “Network Security via private-key certificate,” Operating System Review, Volume: 24, Issue: 4, October 1990, Pages: 64–67.

[6] Haverinen, H. and J. Salowey, “Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM),” Internet Draft (Work in progress), draft-haverinen-pppext-eap-sim-14, October 2004.

[7] IEEE 802.11, “Wireless LAN medium Access Control (MAC) and Physical Layer (PHY) Specifications”, 1999.

[8] IEEE 802.1x, “Port-Based Network Control”, 2001.

[9] Park, Chang-Seop, “Authentication protocol providing user anonymity and untraceability in wireless mobile communication systems,” Computer Networks, Volume: 44, Issue: 2, February 2004, Pages: 267–273.

[10] Park, Chang-Seop, “Improving code rate of McEliece public-key cryptosystem,” Elec-

tronics Letters, Volume: 25, Issue: 21, October 1989, Pages: 1466–1467.

[11] Salgarelli, L., M. Buddhikot, J. Garay, S. Patel, S. Miller, "Efficient authentication and key distribution in wireless IP networks," IEEE Wireless Communications, Volume: 10, Issue: 6 , Dec. 2003, Pages:52 – 61.

[12] Yen, S., L. Ho, and C. Huang, "Internet Micropayment Based on Unbalanced One-way Binary Tree," Proc. CwpTEC '99, Hong Kong, July 1999, Pages: 155–162.

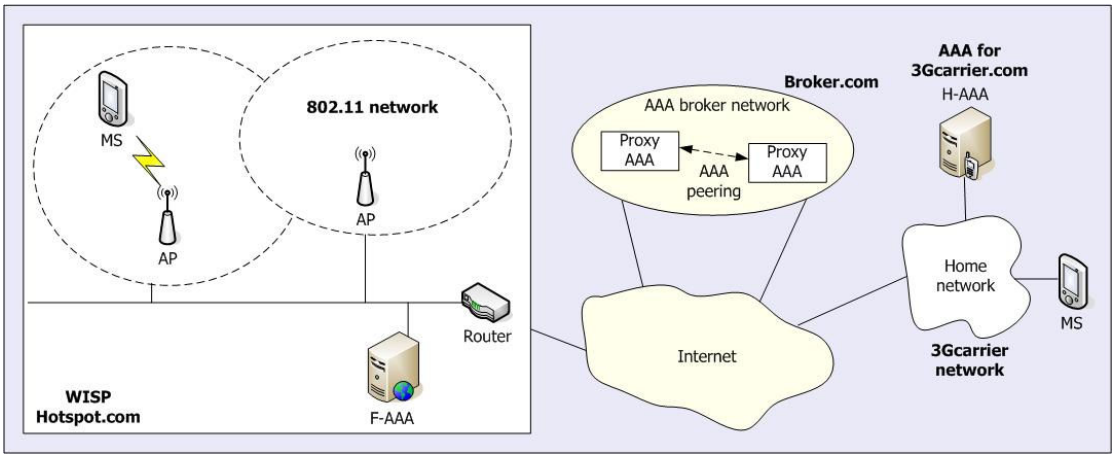

Fig. 1. A network architecture for 3G/WLAN interworking

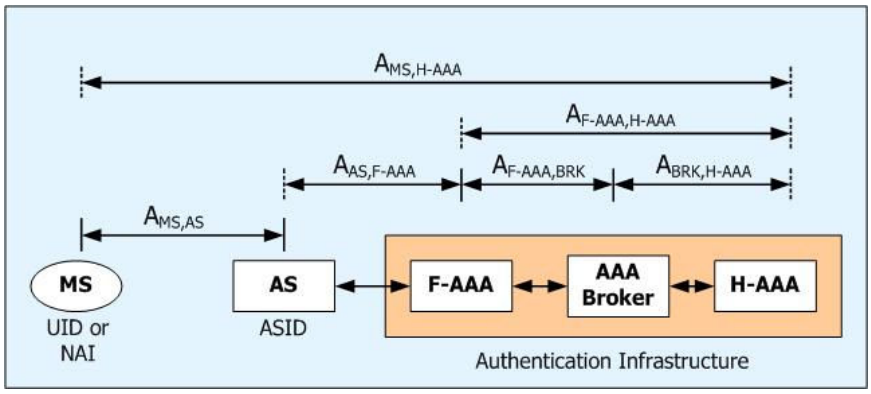

Fig. 2. The authentication model

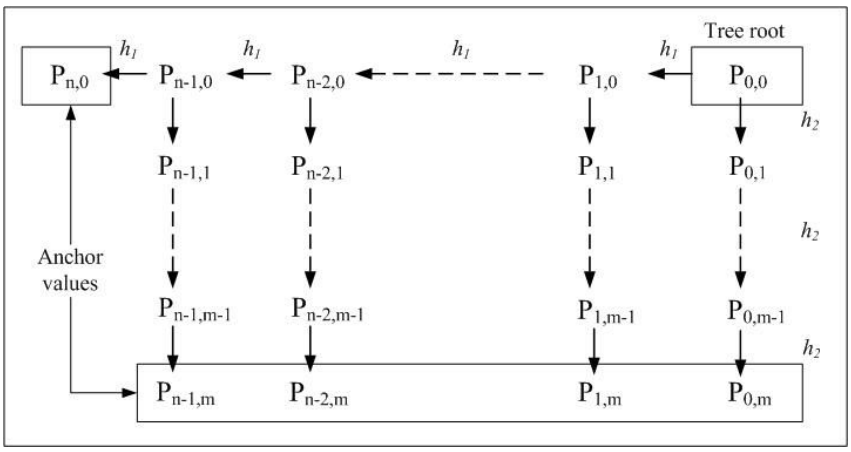

Fig. 3. The unbalanced one-way binary tree scheme

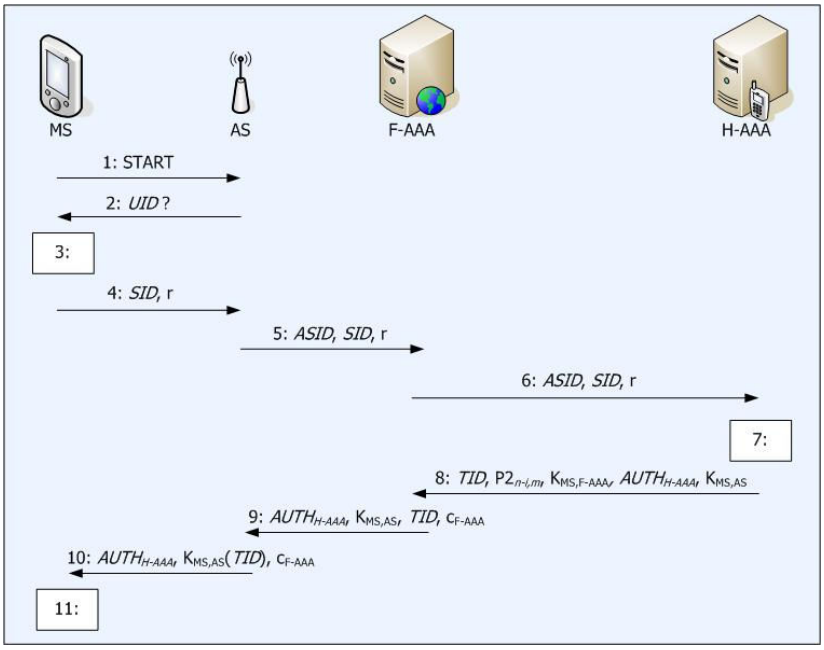

Fig. 4. A full authentication with *i-th* session

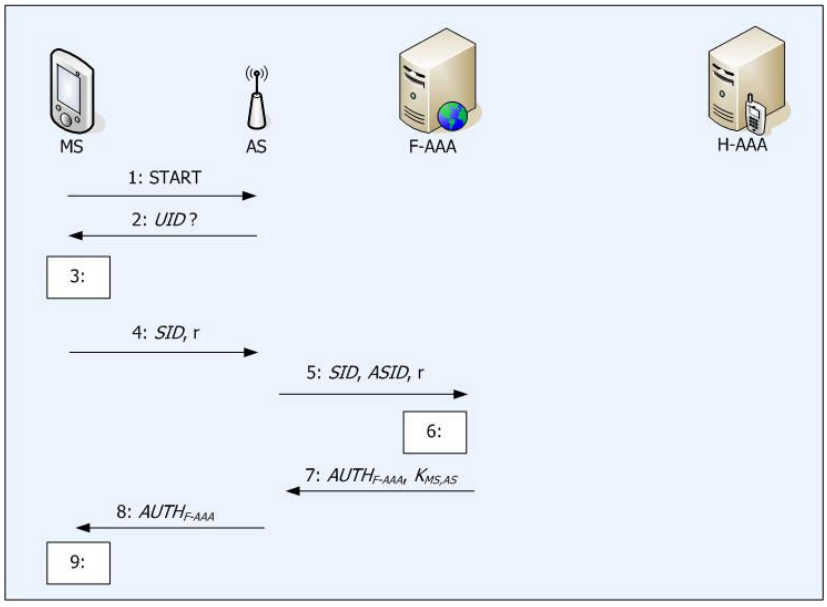

Fig. 5. A fast reauthentication with *j-th* session

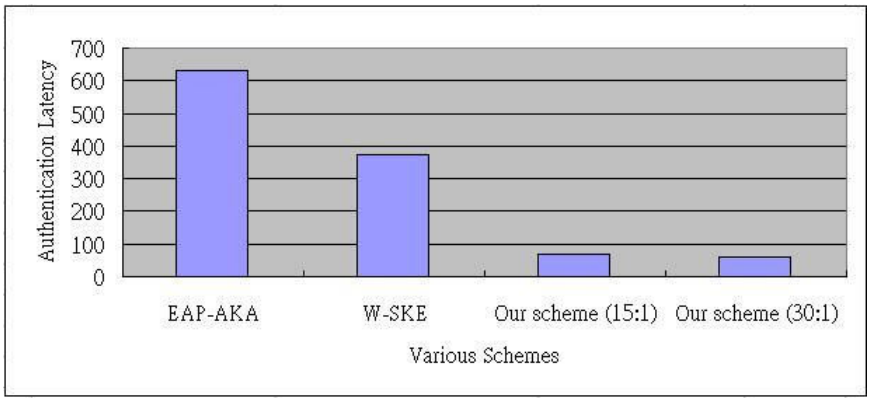

Fig. 6. Authentication latency for various schemes