High Security Authentication Mechanism for Mobile Networks

Ming-Huang Guo[1], Horng-Twu Liaw[1], Jui-Kheng Tang[1], and Chih-Ta Yen[2,*]

[1] Department of Computer Science and Information Engineering, Shin-Hsin University, Taipei, Taiwan
{mhguo,htliaw}@cc.shu.edu.tw, fidodido0706@hotmail.com
[2] Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan
D9709107@mail.ntust.edu.tw

Abstract. Because of the more and more services wireless communication technology can offer nowadays, the quality of wireless communication became an important key. In this research, 3G/UMTS and WLAN will be mentioned mainly. The former offers a wide-range, high-mobility, complete and safe record of accounting; the latter offers a narrow range, low mobility, high speed transmission access on the Internet. The complementary between these two techniques can not only enhance the quality of wireless communication but offer more services for customers to choose, and customers can use wireless application services regardless of any environmental limit. This research will focus on the problem of fast-handover when 3G/UMTS and WLAN is interworking, such as authentication and authorization. About the two formers, we will use W-SKE to accomplish authentication procedure, and achieve safer Mutual Full Authentication and Fast-Authentication.

Keywords: 3G/UMTS, WLAN, Mobile networks, Authentication.

1 Introduction

The mobile communication technologies have become more and more popular in recent years, and cell phone service is an important example among kinds of mobile communication. There is an idea to integrate 3G and WLAN networks to unify the advantages of the two systems as well as to minimize the disadvantages arise as a great market opportunity. They can't replace each other. When WLAN and 3G/UMTS coexist, the handoff mechanism should be created and provided. Many researches 000000000 have proposed about it actually, but it is insufficient to the security requirements. Therefore we will focus on the security of the communication sessions of 3G/UMTS and 802.11 WLAN when a handoff mechanism between them is trigged. However, some mechanisms are not secure or efficient. Hence, EAP-SIM 0 and EAP-AKA 0 have been proposed some authentication mechanism for 3G/UMTS and WLAN interworking. Both EAP-AKA and EAP-SIM provide user with anonymity

* Corresponding author.

R.-S. Chang, T.-h. Kim, and S.-L. Peng (Eds.): SUComS 2011, CCIS 223, pp. 287–296, 2011.

through pseudonyms or temporary identities called Temporary Mobile Subscriber Identities (TMSI). However, the mobile subscriber called Mobile Node (MN) of real identity is exposed to the air when authenticating MN at the first time. This might cause the real 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. Such problems incur long latency and some packet loss when mobile nodes roam into foreign environment. Salgarelli proposed W-SKE to reduce the number of message exchanged and to minimize the latency. The existing mechanisms are not so suitable for 3G/UMTS and WLAN interworking.

In this paper, we propose a secure vertical handoff policy between 3G/UMTS and 802.11 WLAN networks. To achieve this goal, our scheme is proposed to create a secure communication channel from UMTS to WLAN. Also, a security vertical handoff scheme from WLAN to 3G/UMTS is presented. On the other hand, we propose a robust authentication protocol which can perform efficient localized re-authentication procedure and provide non-repudiation service. Our scheme refers to Keyed-Hash Message Authentication Code (HMAC)0, Hash-chaining techniques0, Challenge/Response and Symmetric key Encryption which mention how to withstand the replay attack, guessing attack, impersonation attack and WEP (Wired Equivalent Privacy) weakness attack.

The summary of these articles will be presented in the following sections: The proposed our mechanism will be presented in Section 2. Moreover, the security analysis and performance of the proposed scheme will be mentioned in section 3 and section 4. Finally, we will make the conclusions and come up with some future research directions in section 5.

2 Proposed Mechanism

In this section we propose a new authentication mechanism based on challenge/response, HMAC and one-way hashed chain. Our protocols greatly improve the security and the communication performance.

2.1 Network Architecture

The network architecture as shown in Fig.1 is considered for 3G/UMTS and WLAN interworking in this study, MN denotes mobile node, H-AAA denotes home AAA server of a mobile user MN, and F-AAA denotes foreign AAA server of the WLAN that a MN wants to visit. The F-AAA and the H-AAA belong to separate providers called AAA Brokers; those should be the association between the H-AAA and the F-AAA. The AAA Brokers sets up reliable security associations and routes AAA messages to the H-AAA.

Our authentication model is based on Salgerelli's work. The authentication model directly corresponds to network architecture in previous section. Fig.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

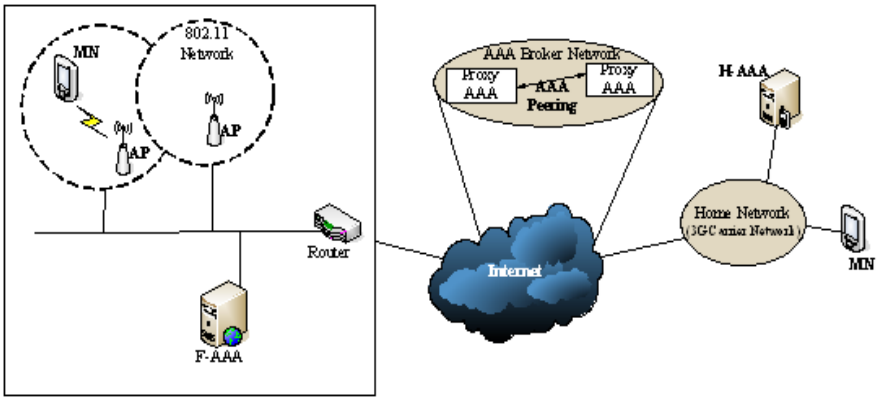

Fig. 1. The network architecture for 3G/UMTS and WLAN interworking

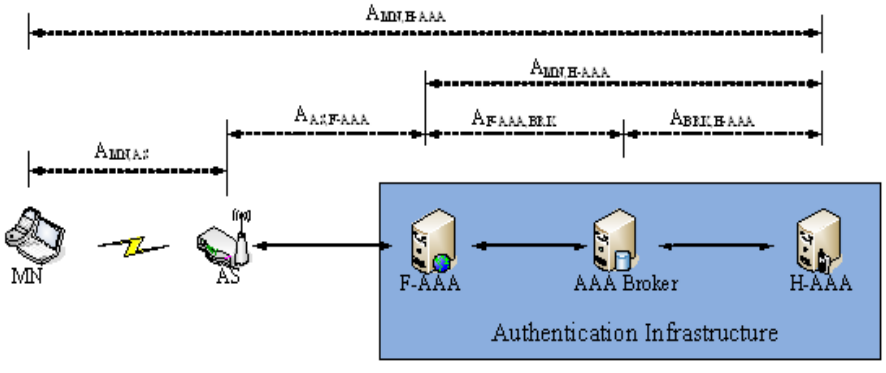

Fig. 2. The authentication model

information(e.g. IMSI, NAI), some form of cryptographic key(e.g. public keys, pre-shared symmetric key), and information on cryptographic algorithms to be used. Each AS maintains a preconfigured security association $A_{AS,F\text{-}AAA}$ with its F-AAA server, other $A_{X,Y}$ same meanings. In the 3G/WLAN interworking, 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 pair-wise relationship should be setup part of roaming agreement.

2.2 Protocols

The characteristic of our mechanism is that it doesn't need the security channel, so every node passes itself legal information of authentication to the H-AAA verity. There are four proposed protocols in our proposal: the full authentication protocol, the WLAN AS fast re-authentication protocol, the 3GPP F-AAA network fast re-authentication protocol, and the 3GPP H-AAA network fast-authentication. Table.1 shows the notations of the proposed protocols.

Table 1. The Notations of the proposed system

IMSI:	International Mobile Subscriber Identity
PID_A:	Pseudonym Identity of A
ID_A:	Real Identity of A
TID_A:	Temporary Identity of A
ASID:	Unique identity of Authentication System
k:	A Secret Key pre-shared between the H-AAA and the MN
f:	A Secret Key pre-shared between the H-AAA and the F-AAA
Ks:	A Secret Key produced between the H-AAA and the MN at authentication time
K_{AB}:	A Session key between the A and the B
RAND:	A random seed/value.
MAC_{AB}:	Message Authentication Codes Function between the A and the B
$E_k()$:	A symmetric function with key k
$PRF_k()$:	A Pseudo Random Function with key k
$f_k()$:	Produce K_S function with key k
Hash():	One way hash function
AHC_A:	Authentication Hash-Chain value of A

1. The MN sends an EAPOL start to AS after the WLAN association process.
2. The AS response an EAPOL-EAP request/identity to the MN.
3. The MN generate a random seed $RAND_M$, and computes $MAC_{HM}=HMAC_k(RAND_M,IMSI)$
4. The MN send the EAP Response/Identity message to AS, which involves ID_H, PID_M, $RAND_M$, and MAC_{HM}.
5. The AS sends the EAP Response/Identity message to F-AAA, the *ASID* append to the message.
6. F-AAA computes $MAC_{HF}=HMAC_f(RAND_F,ID_F)$, in order to make the MN easy to verity H-AAA legally.
7. The F-AAA sends the EAP Response/Identity message to H-AAA.
8. The H-AAA first checks whether the MN access profile is available. If not, the H-AAA was rejected by the MN.

   — The H-AAA uses the pre-shared key and the received $RAND_M$, $RAND_F$, ID_F, *IMSI* to verity MN and F-AAA legally.
   — If verity failed, the will be rejected. Otherwise, the H-AAA generates random seed $RAND_H$ to compute $k_s = f_k(RAND_M \oplus RAND_H)$.
   — The H-AAA generates a new temporary identity of MN, with TID_M have replace PID_M for next time of full authentication protocol.
   — The H-AAA computes the first authentication hash-chain value *xAHC* of the H-AAA and the F-AAA. In order to make the MN easy to re-authentication by the H-AAA and the F-AAA, and keep track of the MN spent based on *xAHC*. Show as follows:

$xAHC^1_H = HMAC_{Ks}(ID_H)$
$xAHC^1_F = HMAC_{Ks}(ID_F)$

- After generating the authentication hash chaining, the H-AAA computes *xAUTH* purpose to avoid falsity message.
- The H-AAA computes the authentication hash-chain value $xAHC^i_H$ and $xAHC^j_F$, in order to make the MN easy to re-authentication by the H-AAA and the F-AAA(the *i* and *j* indicates the hash time; and it can be adjusted on demand). Show as follows:
  $xAHC^i_H = Hash^i(xAHC^1_H)$
  $xAHC^j_F = Hash^i(xAHC^1_F)$
- The H-AAA computes the session key between the MN and the F-AAA, shown as follows:
  $K_{MN\text{-}F} = PRF_{Ks}(xAHC^i_H)$
- The H-AAA computes $xMAC_{FH}$ for the purpose of the F-AAA avoid falsity message from the malice attacker.
- The H-AAA keeps TID_M and *Ks*, which have replaced PID_M and *k* for next time of full authentication protocol.

9. The H-AAA sends the EAP success message to the F-AAA.
10. The F-AAA preserve $xAHC^j_F$, $K_{MN\text{-}F}$ and TID_M after receiving the EAP success message. Among $xAHC^j_F$ is the hash-chain value when MN and AS process re-authentication protocol, $K_{MN\text{-}F}$ is a session key between the MN and the F-AAA; TID_M will not be using PID_M at the time of full-authentication next-time, in order to be anonymous.

- The F-AAA proves whether $xMAC_{FH} = ?MAC_{FH}$ is equal from the H-AAA. If the F-AAA is not with the secret key pre-shared *f*, it will fail to verity.
- The F-AAA computes $xMAC_{FA}$ for the purpose that make MN avoid falsity message from the malice attacker.
- The F-AAA computes the session key between the MN and the AS as shown follows:
  $K_{MN\text{-}AS} = \boldsymbol{PRF}_{K_{MN,F}}(xAHC^j_F)$

11. After the F-AAA forwards successful authentication message to the AS.
12. The AS preserve the $K_{MN\text{-}AS}$, TID_M for the ease of transmission between the MN and the AS.
13. The AS forwards the EAP success message to the MN.
14. The MN obtains the $RAND_H$ from the H-AAA and the $RAND_M$ producted when MN requests for authentication. Then computes to the secret key K_S produce between the H-AAA and the MN of authentication time, shown as follows: $K_S = f_k(RAND_M \oplus RAND_H)$

- The MN generates a new temporary identity $TID_M = Hash(RAND_M \oplus RAND_H, IMSI)$.
- The MN computes the first authentication hash-chain value *xAHC* .
- The MN computes the authentication hash-chain value $xAHC^i_H$ and $xAHC^j_F$.
- The MN computes the session key $K_{MN\text{-}F}$.
- The MN computes the session key $K_{MN\text{-}AS}$.

- The MN verity *xAUTH* in order to avoid falsity message from the malice attacker.
- The MN computes $xMAC_{FA}$ for the purpose that make the MN avoid falsity message from the malice attacker.
- The MN keeps TID_M and *Ks* which have replace PID_M and *k* for next time of full authentication protocol.

15. In this step, the MN and the H-AAA successfully authenticate each other.

2.3 Fast Re-authentication Protocol of the F-AAA

Here we depict the detailed successful re-authentication of the F-AAA. The MN and the F-AAA share a session-key $K_{MS,F}$ which made the re-authenticate key. In the step of the *n*-th re-authentication, *j* is limited for the number of F-AAA re-authentication times, and *j-n* number of re-authentication times once left. When the MN accesses the F-AAA which belongs to the 3GPP visit network, the authentication mechanism is also based on the hash chaining technique. The MN presents its identity TID_M, and the MN computes $AHC^{j\text{-}n}{}_F$, then sends the result to the F-AAA. After this F-AAA verifies the *Hash* $(xAHC^{j\text{-}n+1}{}_F)$=?$AHC^{j\text{-}n}{}_F$; If passing, it means the F-AAA has authenticated the MN. The $AHC^{j\text{-}n}{}_F$ is stored for the next authentication and for the non-repudiation evidence. Afterwards, the F-AAA responses to a challenge $xMAC_{FA}= \boldsymbol{HMAC}_{K_{MN,F}}$ $(xAHC^{j\text{-}n}{}_F, ASID^*)$, and computes new session key $K_{MN\text{-}AS} = \boldsymbol{PRF}_{K_{MN-F}}$ $(xAHC^{j\text{-}n}{}_F)$. On the other hand, the $xMAC_{FA}$ and $K_{MN\text{-}AS}$ are sent to the WLAP AS; the AS keeps the $K_{MN\text{-}AS}$ which is used as dynamic WEP key, and forwarded the $xMAC_{FA}$ to the MN. The MN first verifies the $xMAC_{FA}$. If passing, it means the MN has authenticated the F-AAA server. Next, the MN derives the $K_{MN\text{-}AS} = \boldsymbol{PRF}_{K_{MN-F}}$ $(xAHC^{j\text{-}n}{}_F)$. Eventually, the mutual authentication has been successfully completed and the WEP key has been confidentially delivered.

2.4 Fast Re-authentication Protocol of the H-AAA

This is a roaming reference model. When the MN accesses the H-AAA which belongs to the 3GPP visit network, the authentication mechanism is also based on the hash chaining technique. The Fast Re-authentication protocol of the H-AAA is just the same as the Fast Re-authentication protocol of the F-AAA. The only difference is that the Authentication Hash-Chain Value is added to $AHC^{i\text{-}m}{}_H$, and the access control is charged by the H-AAA server. By using the $AHC^{j\text{-}n}{}_F$ and $AHC^{i\text{-}m}{}_H$ sent to the H-AAA, the re-authentication method is based on the hash chaining technique result to the mutual authentication and key agreement can be achieved.

2.5 Fast Re-authentication Protocol of the AS

This case is under the non-roaming reference model, so the authentication traffic is routed through the New AS and Old AS. The MN computes *Ticket* in order to help Old AS prove whether New AS is a legal node. The MN produces and offer the random value *RAND* to the New AS computes the New Session Key $K_{MN\text{-}AS^{**}}$ so that it can take precautions of the backward to security attack.

Because both sides have agreements of roaming, the other side shares the private session key which can decrypt message of encrypt. The New AS forwards the request message to the Old AS, then the Old AS verifies *Ticket*; if unsucceding, it will reject to serve. Otherwise, represent authentication of the New AS is legal node and produces new random key K_{RAND}. The Old AS responses to a challenge $Ticket_2$ and computes new session key $K_{MN\text{-}AS*}$, making use of private session key $K_{AS\text{-}\ OLD}$ to encrypt $K_{MN\text{-}AS*}$ and old session key $K_{MN\text{-}AS}$ to encrypt K_{RAND}. Then it produces new session $K_{MN\text{-}AS**}$ so that the New AS makes XOR operation with $K_{MN\text{-}AS*}$ and *RAND*. With that, The New AS forwarded $Ticket_2$ and encrypt K_{RAND} to the MN. The MN decrypt message obtains K_{RAND} at first, and verifies $Ticket_2$. If passing, it means the MN has authenticated the New AS. Next, the MN produces the new session $K_{MN\text{-}AS**}$. Finally, the mutual authentication has been successfully completed and the WEP key has been confidentially delivered.

3 Security Analysis

In this section, we will show our mechanism can preclude several attacks, according to Byzantine insiders, which indicates the network elements belong to independent service provider that are not trusted fully because it have a direct or indirect security association between each other. The Security Analysis as shown in Table 2.

- Prevent Guessing Attack: In full authentication protocol, the Secret Key Pre-shared *k* between the H-AAA and the MN, are for authentication purpose. Therefore, it is possible for an attacker to reveal the Secret key Pre-shared *k* from the known information. However, the *k* is impossible to derive it during a reasonable time which is at least 128bits. Utilizing one time password of $AHC^{i\text{-}m}$ and $AHC^{j\text{-}n}$ to upgrade session key in fast authentication, it is invalid to obtain session key K_{WEP}.
- Prevent Replay Attack: In full authentication protocol, it is the situation where an attacker intercepts $\{ID_H, PID_M, RAND_M, MAC_{HM}\}$ sent by the MN in step4 and uses it to masquerade as the MN to send the authentication request next time. Though $RAND_M$ is generated by the MN, the malice attacker don't knowing the Secret Key Pre-shared *k* between the H-AAA and the MN, and it can't respond the correct MAC_{HM} and *AUTH* to the H-AAA and the MN both. On the other hand, the authentication hash chaining value *AHC* of fast re-authentication will be used only once, to replay the *AHC* will not pass theauthentication.
- Prevent Impersonation Attack: The malice attacker attempts to impersonate the MN to access the WLAN. In full authentication protocol, $MAC_{HM} = HMAC_k(RAND_M, IMSI)$ is encrypted with a pre-shared secret *k*; hence without secret key *k*, it can't impersonate the MN. In fast re-authentication, the attacker cannot compute $xAHC^i{}_H = Hash^i(xAHC^1{}_H)$ or $xAHC^j{}_F = Hash^j(xAHC^1{}_F)$ to impersonate the MN, because the Pre-shared Secret Key *k* is only known by the MN-self and the AHC^1 has been securely sent to the H-AAA by the MN in full authentication. In this case, the attacker can't compute backward the authentication hash chaining value *AHC*.
- Prevent WEP weakness attack: The WEP key congenital disadvantage in the gold key IV value is not enough and easy to analyze and explain for the Brute-Force

attack in length,since the WEP key is also renewed in each full authentication of fast re-authentication protocol. Therefore, our mechanism can overcome the weakness of the original WEP.

- Prevent Forward Secrecy and Backward Secrecy to possible attacks: One session key/secret key will not lead to the compromise of the past session key/secret key and the corresponding transmission because one key follows the form of randomness, the one-way property of hashing chains and the session key pre-shared between each other. Thus, each session key/secret key is random and independently, and is fairly controlled by the MN and AAA Server or AS. It can prevent Forward/Backward secret attack then accomplishes the resistance to the known-key attack, the impersonate attack, and the replay attack.
- Legal evidence for use-bill: In the billing process, the AS and F-AAA have to submit all latest hash chain values sent by the MN after each full authentication to H-AAA. *xAHC* will record the usage of MN so that WLAN ISP and the 3G ISP will charge H-AAA for fees according to *xAHC*. Because of having one-way characteristic of hash chaining function, the ISPs is unable to compute to the $xAHC^{i\text{-}n\text{-}1}$ value so that it is also unable to cheat H-AAA with incorrect data of the usage of the evidence, then reach both sides' mutually beneficial fairness.
- Mutual Authentication: The $xAHC_H$ and $xAHC_F$ hidden in *xAUTH* is resulted from computing the AAA Server Identity. The MN will fail to authenticate if there is no legal AAA Server. According to the principle of Transitive, when the authentication between MN and H-AAA, H-AAA and F-AAA, F-AAA and AS all succeed, the one between MN and AS will success, too. The MN will prove legal node of the AS, if the mobile node computes to MAC_{FA} equals with $xMAC_{FA}$ from the H-AAA.
- Secret Key Establishment: The first secret key K_s is produced after the H-AAA and the MN accomplish full authentication. By $RAND_M$,$RAND_H$ and k compute K_s which needn't pass K_s to the MN, the MN will computes K_s by itself. The main purpose for this is to improve its security, which will replace the secret key pre-share k in the full authentication protocols next time.
- Non-repudiation: Our mechanism will complete secret key k with registering in advance. To put *RAND* and *ID* in the Message Authentication Codes Function can produce *MAC* value, then will can use *MAC*to verify the legitimacy of both sides with by its characteristic of Challenge & Response
- Message Integrity: Guarantee mainly the content in the course of transmission has not been falsified. Our mechanism check out the equality between *MAC* and *xMAC*; so does between *AUTH* and *xAUTH*, in order to confirm the integrality of the message.
- Protect Transmit Session Key: The Session Key $K_{A,B}$ is transmitted to other communication apparatus under the protection of the symmetric function, preventing $K_{A,B}$ from being stolen in the course of transmission.
- Perfect User Anonymity: H-AAA and MN will figure out TID_M, and TID_M will replace PID_M for next time of full authentication protocol. Only the issuer (MN or H-AAA) is able to produce the temporary identifier TID_M. Our scheme, different with EAP-SIM and EAP-AKA, is not transmitted for each time when the temporary identifier is not available; it adopts the dynamic way to produce TID_M. Therefore, perfect anonymity is achieved.

Table 2. The Security Analysis comparison of our mechanism and other mechanism

	EAP-AKA	W-SKE	IDKE	Our Mechanism
Prevent Guessing Attack	×	×	×	○
Prevent Replay Attack	×	○	○	○
Prevent Impersonation Attack	×	○	○	○
Prevent WEP weakness attack	○	×	○	○
Prevent Forward/Backward Secrecy attacks	×	×	×	○
Legal evidence for use-bill	×	×	×	○
Mutual Authentication	×	×	△	○
Secret Key Establishment	○	×	×	○
Non-repudiation	×	×	×	○
Message Integrity	○	○	×	○
Protect Transmit Session Key	×	×	×	○
Perfect User Anonymity	×	×	×	○

○:Achieved △:Incomplete —:No propose ×: No Achieved

Table 3. The Performance Analysis comparison of our mechanism and other mechanism

Round Trip Time	EAP-AKA		W-SKE		IDKE		Our Mechanism	
	FA	RA	FA	RA	FA	RA	FA	RA
$T_{F\text{-}AAA,H\text{-}AAA}$	2	0	1	No	No	0	1	0
$T_{F\text{-}AAA,AS}$	4	3	2	No	No	1	1	1
$T_{MS,AS}$	5	4	3	No	No	2	2	2

FA: Full Authentication **RA**: Fast Re-Authentication **RTT**: Round Trip Time

4 Performance Analysis

In this section, we will evaluate the efficiency of our mechanism in terms of authentication latency in more details. Let $T_{F\text{-}AAA,H\text{-}AAA}$ denote the one trip latency between H-AAA and F-AAA, $T_{F\text{-}AAA,AS}$ denote the one between F-AAA and AS, and $T_{MS,AS}$ denote the one between MS and AS. According to the number of authentication time, we can see that $T_{F\text{-}AAA,H\text{-}AAA} > T_{F\text{-}AAA,AS} > T_{MS,AS}$. Table.3 shows The Performance Analysis comparison among our mechanism, EAP-AKA, W-SKE and IDKE. The authentication latency of our full authentication is $2T_{F\text{-}AAA,H\text{-}AAA} + 2T_{F\text{-}AAA,AS} + 4T_{MS,AS}$, EAP-AKA is $4T_{F\text{-}AAA,H\text{-}AAA} + 8T_{F\text{-}AAA,AS} + 10T_{MS,AS}$; W-SKE is $2T_{F\text{-}AAA,H\text{-}AAA} + 4T_{F\text{-}AAA,AS} + 6T_{MS,AS}$; but IDKE doesn't point out this method. Moreover, in terms of fast re-authentication, our scheme is $2T_{F\text{-}AAA,AS} + 4T_{MS,AS}$; EAP-AKA is $6T_{F\text{-}AAA,AS} + 8T_{MS,AS}$; IDKE is $2T_{F\text{-}AAA,AS} + 4T_{MS,AS}$; while W-SKE doesn't mention it .

5 Conclusions and Future Works

In our mechanism, we discuss about the security and authentication protocol for WLAN and 3G/UMTS interworking. EAP-AKA, W-SKE and IDKE have been

examined, and shown the security weaknesses of W-SKE, the in-efficiency of EAP-AKA, and integrate localized re-authentication of IDKE. Moreover, we have figured out a new authenticated key exchange protocol. We propose a robust authentication protocol which can perform efficient localized re-authentication procedure, provide non-repudiation service, solve the problems of losing packages, shorten the authentication time delay and greatly improve the security. In our future work, we expect to do a more in-depth research focused on the handover mechanism, roaming management, packet forwarding and transmission in the future days.

References

1. 3GPP TR 22.934: Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking, Release 6 (2003)
2. 3GPP TS 22.234: 3GPP system to Wireless Local Area Network (WLAN) Interworking, System description, Release 6 (2004)
3. 3GPP TS 33.234: 3G Securtiy: Wireless Local Area Network (WLAN) interworking security, Release 7 (2006)
4. Buddhikot, M., Chandranmenon, G., Han, S., Lee, Y.W., Miller, S., Salgarelli, L.: Integration of 802.11 and Third-Generation Wireless Data Networks. In: Proceedings of the IEEE INFOCOM 2003 (2003)
5. Zhu, J., Ma, J.: A New Authentciation Scheme with Anonymity for Wireless Envioronments. IEEE Member (2004)
6. Salgrelli, L., Buddhikot, M., Garay, J., Patel, S., Miller, S.: Efficient Authentication and Key Distribution in Wireless IP Networks. Bell Laboratories, Lucent Technologies. IEEE Wireless Communication (2003)
7. Kambourakis, G., Rouskas, A., Kormentzas, G., Gritzalis, S.: Advanced SSL/TLS-Based authentication for secure WLAN-3G interworking. Communications 151 (2004)
8. Prasithsangaree, P., Krishnamuthy, P.: A new authentication mechanism for loosely coupled 3G-WLAN integrated networks. In: IEEE Vehicular Technology Conference (2004)
9. Tsen, Y.M., Yang, C.C., Su, J.H.: An efficient protocol for integrating WLAN and Cellular Networks. In: International Conference on Advanced Communication Technology (2004)
10. IETF Draft: IETF internet draft EAP-SIM authentication (2003), `http://www.ieft.org/internet-draft-haverinen-appext-eap-sim-10.txt`
11. IETF Draft: Extensible Authentication Protocol Method for 3rd Generation Authentication an Key Agreement (EAP-AKA). RFC 4187 (2006)
12. Lamport, L.: Password Authentication with Insecure Communication. Communication of ACM 24(11), 770–772 (1981)
13. Krawczyk, H., Bellare, M., Canetti, R.: Keyed-Hashing for Message Authentication. RFC 2104 (1997)