Authentication Optimization for Vertical Handover in Heterogeneous Wireless Networks

Ikram Smaoui[1], Faouzi Zarai[1], Mohammad S. Obaidat[2] and Lotfi Kamoun[1]
[1]*LETI Laboratory, University of Sfax, Sfax, Tunisia*
[2]*Computer Science and Software Engineering Department, Monmouth University, NJ 07764, West Long Branch, U.S.A.*

Keywords: Authentication, Seamless Handover, Security, EAP-AKA Protocol, Heterogeneous Networks.

Abstract: In this paper, we present a scheme for reducing vertical handover delay in heterogeneous wireless networks by optimizing the network access authentication procedure as it is a heavy burden due to its latencies and overhead. Indeed, optimizing the authentication procedure while at the same time providing the same or best level of security represents a key factor in the design of the next generation of heterogeneous wireless networks. In this context, the aim of our work in this paper is to provide a security framework accounting for heterogeneity in wireless access networks without degrading the security level currently provided by each wireless system. We also demonstrate using simulation analysis the handover performance improvement provided by our proposed security frame work.

1 INTRODUCTION

The Next Generation of Heterogeneous Wireless Networks (NGHWNs) is migrating towards the interworking of diverse access systems such as (3GPP Long Term Evolution/Service Architecture Evolution (LTE/SAE), Universal Mobile Telecommunications System (UMTS), Wireless Local Area Network (WLAN) and Worldwide Interoperability for Microwave Access (WiMax)) (Smaoui, 2007). In fact, interworking these access networks requires seamless mobility management with optimized network authentication and keying material establishment and distribution to guarantee uninterrupted services continuity especially in case of mobile terminals' handover across the integrated heterogeneous networks owned by a single operator or by different operators having roaming agreement between them. In fact, each access system has its specific network access authentication procedure and its key management mechanism. Therefore, when a Mobile Terminal (MT) handovers to a new network, the MT has to do network specific authentication procedure and establishes the keys to secure its communication. Thus, the number of messages exchanged for network access authentication during vertical handover imposes a heavy burden on both the MT as well as the network side, which increases the vertical handover latency (Rajavelsamy, 2007).

The NGHWNs are expected to support seamless mobility between all integrated heterogeneous wireless networks. On the other hand, security is also an important concern in handover operation. Indeed, while moving from one network to another network, MT should be authenticated. Thus, as authentication procedure incurs high latency; executing pre-authentication is becoming essential, especially for non-delay tolerant connections. Consequently, security becomes a crucial issue when this authentication is between heterogeneous networks. In this context, the NGHWNs tend to provide an authentication framework independent of the wireless network technology and a mobility management that does not degrade security.

In this paper, we propose a security framework accounting for heterogeneity in wireless access networks without degrading the security level currently provided by each individual wireless system. The main idea of our proposed optimized authentication scheme is to securely transfer the temporary identity and its correspondent handover key already generated by the Hybrid Interworking Unit (HIU) (Smaoui, 2010) to the mobile terminal that will be used in the target network, during handover preparation phase. By means of obtaining temporary identity and handover key in the handover

Smaoui I., Zarai F., S. Obaidat M. and Kamoun L..
Authentication Optimization for Vertical Handover in Heterogeneous Wireless Networks.
DOI: 10.5220/0004011602490254
In *Proceedings of the International Conference on Signal Processing and Multimedia Applications and Wireless Information Networks and Systems* (WINSYS-2012), pages 249-254
ISBN: 978-989-8565-25-9
Copyright © 2012 SCITEPRESS (Science and Technology Publications, Lda.)

preparation phase, the authentication process in the target network can be reduced considerably.

The rest of this paper is organized as follows. Section 2 represents overview of the EAP-AKA (Extensible Authentication Protocol Method for Authentication and Key Agreement), protocol that allows the authentication of a MT in heterogeneous wireless environment. In section 3, we describe the proposed security authentication procedure. Section 4 represents the performances evaluation of the proposed scheme and we conclude the paper in section 5.

2 EAP-AKA PROTOCOL

The EAP-AKA protocol is an authentication mechanism used in a 3G-WLAN interworking to authenticate user equipment that attempts to access Non-3GPP network such as the WLAN. Indeed, the EAP-AKA is a Universal Subscriber Identity Module (USIM) based mechanism for authentication and session key distribution that allows usage of AKA over the EAP protocol (Arkko, 2006). This authentication mechanism is used in case of 3GPP and non-3GPP networks interworking such as the 3GPP-LTE and WLAN interworking.

As in the UMTS-AKA (3GPP, 2006), the USIM and the network have agreed on a pre-shared secret key. The authentication vector (AV) components for EAP-AKA are transmitted on *AKA-Challenge Message* of EAP Request and EAP Response Packets. In EAP-AKA, the User Equipment (UE) executes a mutual authentication with an EAP server located at the network side. On successful mutual authentication, both derive Ciphering Key (CK) and Integrity Key (IK) which will be used to derive the EAP Master Key (MK), from which both derive the EAP Master Session Key (MSK). The MSK is transferred to the Authenticator (e.g., Access Point (AP)) in order to protect further communications.

In fact, we distinguish two EAP-AKA procedures, a full and a fast re-authentication mechanisms. The full authentication is considered as an initial authentication procedure to generate new keys in an USIM card and the network. On the other hand, the fast re-authentication reuses the keys already generated from the previous authentication process to save processing time in the UE and the AAA server and to save power consumption in the UE. Indeed, The AAA server aggregates the use of a fast re-authentication with the UE by sending a *re-authentication identity* in any authentication process. When a re-authentication procedure is initiated by the network, the UE replies with the *re-authentication identity* received in the previous successful authentication. Moreover, the use of the fast re-authentication procedure depends on the operator's policies.

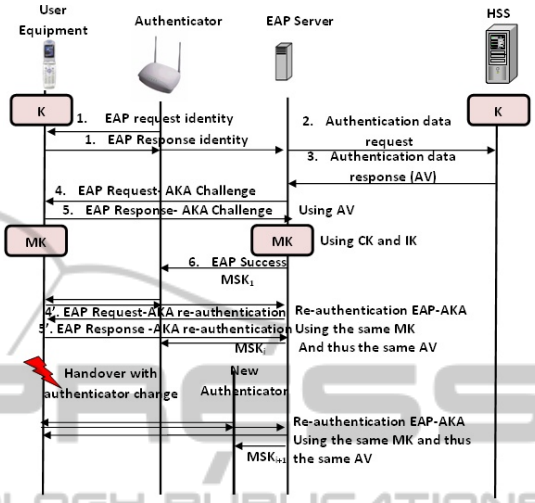

Figure 1: EAP-AKA authentication procedure.

However, the EAP-AKA protocol represents several vulnerabilities which can cause man-in-the-middle attacks or bandwidth consumption (Mun, 2009). In fact, on the first connection between the UE and the EAP server, the IMSI is sent in plaintext. Therefore, an attacker may intercept the International Mobile Subscriber Identity (IMSI) and can modify or misuse it.

Furthermore, although the UE and the EAP server can be successfully authenticated each other, the EAP server sends EAP Success message with MSK to the AP and the UE without authentication. Consequently, an attacker who impersonates the AP can receive EAP Success message with MSK, modify the received message and then send it to the UE or to another UE. Moreover, the EAP server requests again the user identity before the challenge/response procedure because immediate nodes can modify user identity. For this reason, EAP-AKA has additional bandwidth consumption.

3 PROPOSED AUTHENTICATION OPTIMIZATION MECHANISM

In our proposed solution, the hybrid interworking unit generates temporary identities (temp IDs) with their respective authentication keys (temp K) for

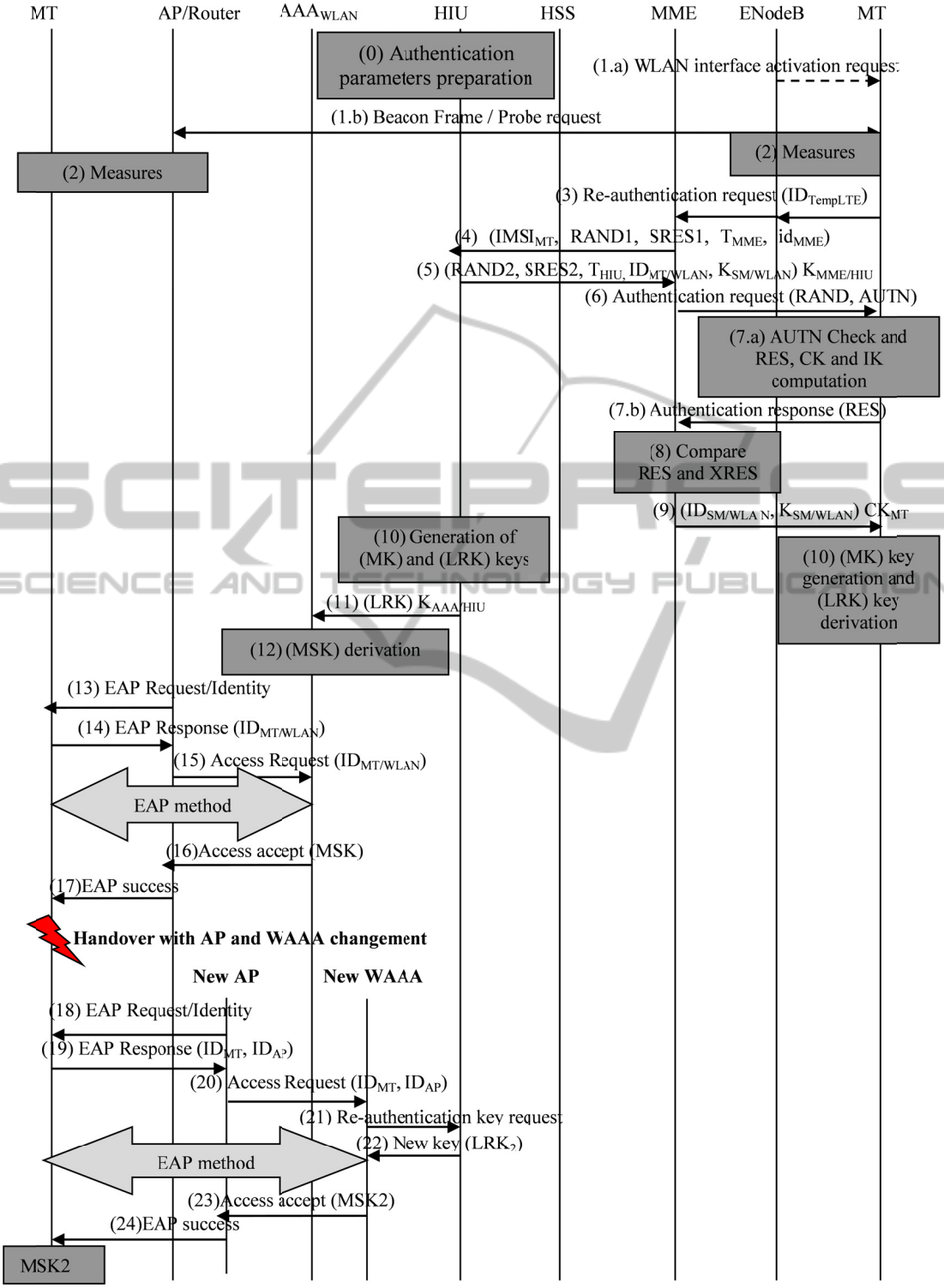

Figure 2: Proposed authentication protocol.

mobile stations that prepare to handover to the WLAN system. The MT can do a fast re-authentication with the visited network during handover in order to reduce the authentication delay and consequently reducing the handover delay.

Thus, in our proposed authentication procedure, we assume the following:

- Secure tunnels are established between the Mobility Management Entity (MME) and the Home Subscriber Server (HSS) server on one hand and between the HSS and the HIU on the other hand to secure the transfer of the users' authentication parameters.
- The hybrid interworking unit shares a key ($K_{MME/HIU}$) with the MME that will be dynamically refreshed by the HSS. The same, the HIU shares also a key ($K_{AAA/HIU}$) with the Authentication, Authorization and Accouting AAA server of the WLAN network (AAA_{WLAN}).
- The HIU may choose any authentication vector (pair of tempID and temp K) to authenticate the MT (i.e. there is not a specific authentication vector for a specific MT).
- An efficient authentication process in our case (i.e. handover from LTE system to WLAN system) should enclose three types of mutual authentication: First, a mutual authentication between the MT and the home network (LTE network). Second, a mutual authentication between the LTE network and the WLAN network. Finally, a mutual authentication between the MT and the visited network (WLAN network).

Figure 2 explains our proposed authentication procedure for handover from LTE system to WLAN system.

The messages sequences are presented below:

1. MT initiates the measurement process periodically or after a new discovered pre-handover trigger such as MT velocity variation, LTE performance degradation, or a new discovered network, etc.

2. Based on these measurements (MT velocity, network load…), if the WLAN system is pre-selected as the best available network in the MT coverage area, the MT decides to execute a pre-handover process to the WLAN network.

3. The MT initiates a pre-authentication procedure with the MME of its home network by sending a pre-authentication request containing the MT temporary identity in the LTE system ($ID_{MTTemp\ LTE}$). As the MT has already execute successfully the initial authentication process with the MME since its first attachment to the LTE network, the MME at this step uses one unused authentication vector already retrieved from the HSS since the initial authentication to do the mutual authentication with the MT.

4. At this step, the MME initiates a mutual authentication with the HIU to secure the communication between them. So, the MME sends to the HIU a message that contains the permanent identity of the MT ($IMSI_{MT}$), a random number (*Rand1*), its signature (SRES1), a Timestamp (T_{MME}) and the MME identity (id_{MME}). All encrypted with their shared key $K_{MME/HIU}$.

5. As a response, the HIU sends a second random number *Rand2,* its signature (*SRES2*), a Timestamp (T_{HIU}) and the MT's identity and key in the WLAN. The message is encrypted by the shared key $K_{MME/HIU}$. In fact, the $ID_{MT/WLAN}$ is a function of the MT permanent identity ($IMSI_{MT}$) and the temporary identity (temp ID) generated by the HIU in one authentication vector. The same, the $K_{MT/WLAN}$ is a function of the MT permanent identity ($IMSI_{MT}$) and the temporary key (temp K) in this same selected authentication vector.

6. In case of successful authentication, the MME sends to the MT an authentication request that contains the values of RAND and AUTN.

7. The MT at its turn authenticates the MME by checking the AUTN, generates the CK and IK keys and calculates the RES.

8. The MME compares the obtained RES with the XRES retrieved from the authentication vector and if the MT is successfully authenticated, the MME sends its authentication parameters ($ID_{MT/WLAN}$, $K_{MT/WLAN}$) encrypted with MT's CK,

9. At this step, the MT and the HIU compute the Master Key (*MK*) and the Local Re-authentication key (LRK). The (MK) key is obtained by the application of a pseudo random function (*prf*) on the $ID_{MT/WLAN}$ and the $K_{MT/WLAN}$ according to equation (1) while the (LRK) is derived by using a key derivation function on the MK and the AAA_{WLAN} identity.

$$MK = prf\left(ID_{MT/WLAN} \middle| K_{MT/WLAN}\right) \quad (1)$$

$$LRK = KDF(MK|ID_{AAAWLAN}) \quad (2)$$

10. The HIU sends the LRK to the AAA_{WLAN} encrypted with their shared key $K_{AAA/HIU}$,

11. The $K_{AAA/HIU}$ at this step derives the Master Session Key MSK from the LRK.

12. The last part of this authentication procedure concerns the one established between the MT, the AP and the AAA_{WLAN} to secure the communication between these equipment. Therefore, firstly, the AP requires the identity of the MT through an EAP request. The MT at its turn responds by an EAP response that contains its $ID_{MT/WLAN}$. The AP relays this response to the AAA_{WLAN} through an access request. At this step, an EAP method is executed and

in case of successful authentication, the AAA_{WLAN} authorizes the access to the WLAN system and sends the MSK key to the AP. This key is also generated by the MT by applying the same function.

13. In case of MT's horizontal handover to a new AP that belongs to a new AAA_{WLAN}, this later can demand a new LRK from the HIU to re-authenticate the MT which reduces considerably the authentication latency.

4 PERFORMANCES EVALUATION

In this section, we analyze our protocol and then compare its performance with the EAP-AKA protocol through simulation analysis.

4.1 Security Analysis

Our protocol has several security properties improvement as summarized below:

- Our proposed authentication mechanism protects the user identity (*IMSI*) by using the MT's temporary identity ($ID_{MTTemp\ LTE}$) in the mutual authentication between the MT and the MME on one hand and then by generating a temporary identity for the MT to use it on handover on the other hand.
- All messages between the authentication entities are encrypted by correspondent keys in order to ensure messages confidentiality.
- Our protocol can prevent replay attack by using Timestamps in exchanged messages and verifying random numbers (steps 4 and 5).
- Our proposed protocol provides several mutual authentication procedures such as between the MT and the MME, the MME and the HIU and between the AAA_{WLAN} and the AP. These procedures prevent man-in-the-middle attacks, which make communications more secure.

4.2 Performances Analysis

To evaluate our proposed authentication protocol, we used the simulator developed by us (Daly, 2011) that implements the WLAN and the LTE systems, the mobility, the propagation and the traffic models. We consider a WLAN network covering 300*300m containing 9 access points and a variable number of WLAN terminals (the total number is fixed to 200) and also some LTE terminals switching to the WLAN network. The simulated network is shown in Figure 3.

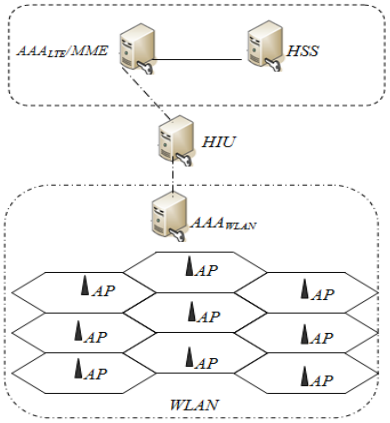

Figure 3: Simulated network.

We evaluate the simulation results based on the following performance evaluation metrics:

- Handover latency which represents the time elapsed between the point of attachment change request and the association with the new one.
- Blocking rate represents the number of blocked handover connections for the total number of handover requests.

Thus, Figure 4 shows the influence of our proposed protocol and of the EAP-AKA protocol on handover latency. Indeed, we notice that handover latency increases when the number of terminals increases in the WLAN system. This can be explained by the fact that the increase of handover requests introduces additional delays during handover procedure generally due to layer treatments and the query waiting time in different network nodes. However, by comparing the two curves, we notice that our proposed protocol offers the reduced latency since it uses the pre-authentication mechanism which reduces the authentication latency and consequently the handover latency.

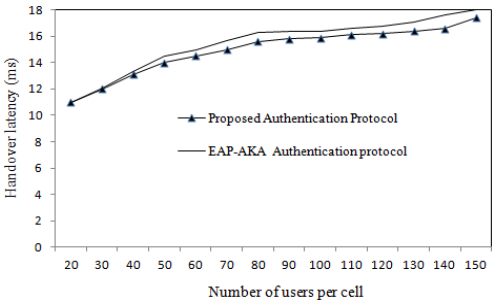

Figure 4: Handover latency.

Figure 5 shows the influence of our proposed protocol and of the EAP-AKA protocol on the handover blocking rate. Thus, we see that our

protocol offers a reduced blocking rate. This result can be explained by the elimination of blocked connections caused by authentication latency.

In fact, the obtained simulation results associated to the security policy reinforcement in the authentication procedure constitute satisfactory results for the user experience as well as the network performance.

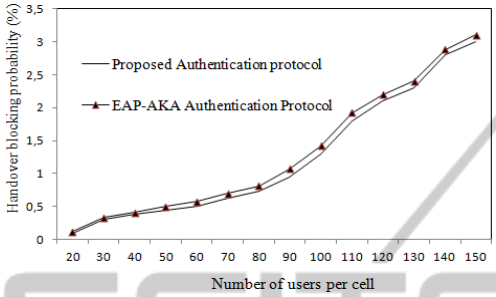

Figure 5: Handover blocking probability.

5 CONCLUSIONS

In this paper, we have study the EAP-AKA protocol that allows user authentication in 3G-WLAN interworking and we have identified its vulnerabilities. Then, we have proposed our authentication mechanism in case of 3GPP-LTE and WLAN interworking. The performance results have shown that our proposed protocol outperforms the EAP-AKA protocol in terms of offered security level and handover performance which satisfy the user requirements and the network capacity. Our future works in this topic will include the evaluation of the implementation overheads of our proposed protocol compared with the EAP-AKA protocol.

REFERENCES

Smaoui, I., Zarai, F., Kamoun, L., 2007. “Vertical handoff management for next generation heterogeneous networks”, *5th International Conference on Information and Communications Technology (ICICT 2007),* pp. 19-25.

Rajavelsamy, R., Jeedigunta, V., Osok Song, 2007. “A Novel Method for Authentication Optimization during Handover in Heterogeneous Wireless Networks”, *2nd International Conference on Communication Systems Software and Middleware*, *COMSWARE 2007,* pp.1-5.

Smaoui, I. Zarai, F., Banat, M., Kamoun, L., 2010. “Heterogeneous Wireless Networks: Configuration and Vertical Handoff Management”, *Wireless Personal Communications,* Vol. 54, No. 3, pp. 417-445.

Arkko, J., Haverinen, H., 2006. “Extensible Authentication Protocol method for 3rd Generation Authentication and Key Agreement (EAPAKA)”, *RFC 4187*.

3GPP TS 33.102, 2006. “Technical Specification group services and system aspects, 3G security; Security Architecture”, release 7.

Mun, H., Han, K., Kim, K., 2009. "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA", *IEEE Wireless Telecommunications Symposium*, WTS 2009, pp. 1-8.

Daly, I., Zarai, I., Kamoun, L., 2011.“Design and implementation of a simulation environment for the evaluation of authentication protocols in IEEE 802.11s networks”, *3rd International ICST Conference on Mobile Lightweight Wireless ystems*, Bilbao Espagne.

SCITEPRESS
SCIENCE AND TECHNOLOGY PUBLICATIONS