The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)

REDUCING AUTHENTICATION TRAFFIC IN 3G-WLAN INTEGRATED NETWORKS

Christoforos Ntantogian
Department of Informatics and Telecommunications
University of Athens, Greece
ntantogian@di.uoa.gr

Christos Xenakis
Department of Technology Education and Digital Systems
University of Piraeus, Greece
xenakis@unipi.gr

ABSTRACT

The security architecture of the 3G-WLAN integrated networks specifies that a WLAN user, in order to get access to the 3G packet switched services or the public internet through the 3G PLMN, he must follow a two-pass EAP-AKA authentication procedure. This involves a double execution of EAP-AKA, which introduces a duplicated authentication overhead. This paper proposes a one-pass EAP-AKA authentication procedure for the 3G-WLAN integrated networks that reduces significantly the authentication traffic, compared to the two-pass EAP-AKA authentication, without compromising the provided level of security. The proposed procedure has minimal impact on the existing 3G-WLAN network infrastructure and functionality. A security analysis of the proposed authentication procedure is elaborated that identifies potential attacks and proposes possible countermeasures. In addition, a cost analysis is considered that compares the total number of messages required for user's authentication using the two-pass EAP-AKA and the proposed one-pass EAP-AKA authentication.

I. INTRODUCTION

The next generation of mobile/wireless systems is materialized from the integration of third generation (3G) networks with the Wireless Local Area Networks (WLAN), as specified by the 3rd Generation Partnership Project (3GPP) in 3GPP 23.234 [1]. The 3G-WLAN integrated networks promise to provide high quality services and anywhere-anytime connectivity to mobile users. Along with a variety of new perspectives, the new network model (3G-WLAN) raises new security concerns mainly, because of the complexity of the deployed architecture and the heterogeneity of the employed technologies.

To address the security concerns and promote the proliferation of the 3G-WLAN integrated networks, 3GPP has provided a specific security architecture, defined in 3GPP 33.234 [2]. This architecture aims at protecting the mobile users, the data transferred and the underlying network. One of the features of this security architecture specifies that a WLAN user, in order to get access to the 3G packet switched services or the public internet through the 3G Public Land Mobile Network (PLMN), he must follow a two-pass EAP-AKA authentication procedure. This procedure includes two discrete authentication steps. In the first authentication step, the user executes the EAP-AKA protocol [4] that registers him to the WLAN domain. In the second authentication step, the user executes the Internet Key Exchange version 2 (IKEv2) protocol [5] that encapsulates EAP-AKA, which registers him to the 3G PLMN domain. Therefore, the specified two-pass EAP-AKA authentication procedure involves a double execution of the EAP-AKA protocol, which introduces a duplicated authentication overhead. This overhead is related to: (i) the exchange of messages that cause delays in users' authentication and consume radio resources; and (ii) the computational processing at the level of mobile devices that may induce energy consumption issues. Thus, the aforementioned two-pass EAP-AKA authentication procedure has an adverse impact on aspects of quality of service offered to end-users, deteriorating the overall system performance.

This paper proposes a one-pass EAP-AKA authentication procedure for the 3G-WLAN integrated networks that reduces significantly the authentication traffic, compared to the two-pass EAP-AKA authentication, without compromising the provided level of security. The proposed procedure combines the first and the second authentication step by making a security binding between them. This binding eliminates the need for duplicated execution of EAP-AKA, reducing the overall authentication overhead. The proposed one-pass EAP-AKA authentication procedure has minimal impact on the existing 3G-WLAN network infrastructure and functionality. A security analysis of the proposed authentication procedure is elaborated that identifies potential attacks and proposes possible countermeasures. In addition, a cost analysis is considered that compares the total number of messages required for user's authentication using the two pass EAP-AKA and the proposed one-pass EAP-AKA authentication.

The rest of this paper is organized as follows. Section 2 briefly presents the 3G-WLAN network architecture and the two-pass EAP-AKA authentication procedure. Section 3 describes and analyses the proposed one-pass EAP-AKA authentication procedure. Section 4 evaluates the proposed procedure by presenting a security analysis and a cost analysis. Finally, section 5 contains the conclusions.

II. BACKGROUND

A. 3G-WLAN Interworking Architecture

As shown in Fig. 1, the 3G-WLAN interworking architecture [1] consists of three individual parts: (I) the WLAN access network, (II) the visited 3G PLMN, and (III) the home 3G PLMN. Note that Fig. 1 illustrates the architecture for a general case where the WLAN is not directly connected to the user's home 3G PLMN. The WLAN consist of the wireless Access Points (APs) that act like Authentication, Authorization, Accounting (AAA) clients, which forward security related messages to the AAA server through AAA proxies, and the WLAN-Access Gateway (WLAN-AG) that is a gateway to 3G PLMN or to the public internet. It is assumed that the WLAN is based on the IEEE 802.11 standard and the AAA protocol is Diameter [6].

On the other hand, the visited 3G PLMN includes the core network elements of the General Packet Radio Services (GPRS)/Universal Mobile Telecommunications System (UMTS), such as the Gateway GPRS Support Node (GGSN) and the Serving GPRS Support Node (SGSN), an AAA proxy that forwards AAA information to the AAA server (located in the home 3G PLMN), and the Packed Data Gateway (PDG). The latter routes user data traffic between a user and an external packet data network, which is selected based on the 3G packet switched services (such as Wireless Application Protocol (WAP), Multimedia Messaging Services (MMS), Location Based Services (LBS) etc.) requested by the user. The PDG identifies these services by means of a *WLAN-Access Point Name (W-APN)* [1], which represents a reference point to the external IP network. Finally, the home 3G PLMN includes the AAA server that provides authentication services to the WLAN, the Home Subscriber Service (HSS) and the Authentication Centre (AuC). The AAA server retrieves authentication information from the HSS/AuC and validates authentication credentials provided by users.

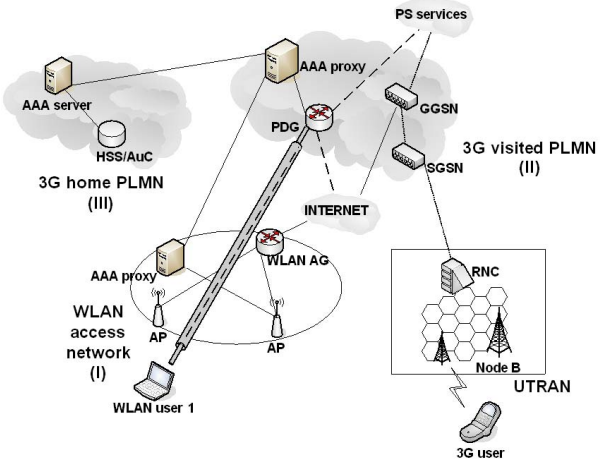

Fig. 1 3G-WLAN Interworking Architecture

B. *Two-Pass EAP-AKA Authentication*

As mentioned previously, the two-pass EAP-AKA authentication procedure [2] includes two discrete authentication steps, which are presented in Fig. 2 and analyzed below:

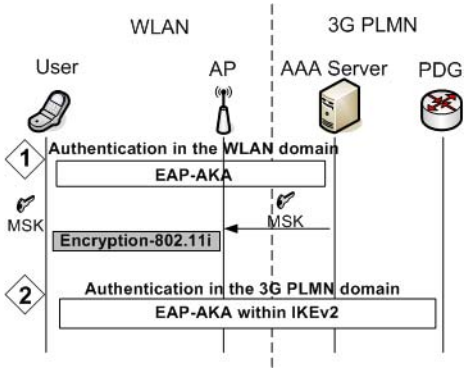

Fig. 2 Two-Pass EAP-AKA Authentication

Initial authentication. The user and the WLAN are authenticated each other using EAP-AKA [4]. This authentication step involves the user, an AAA client that is actually a wireless AP, and the AAA server that may obtain authentication information (i.e., 3G authentication vectors) from the HSS/AuC of the home 3G PLMN, where the user is subscribed. In the first two messages of the EAP-AKA negotiation (see Fig. 3), the wireless AP request for the user's identity (EAP Request/identity message) and the latter replies by sending to the AAA server an EAP Response/identity message, which contains either his permanent (i.e., International Mobile Subscriber Identity (IMSI)) or a temporary identity in the format of Network Access Identifier (NAI). After obtaining the user's identity, the AAA server checks whether it possesses a 3G authentication vector, stored from a previous authentication with the specific user. If not, the AAA server sends the user's IMSI to the HSS/AuC and obtains *n* fresh authentication vectors. Note that an authentication vector includes a random challenge (RAND), the authentication token (AUTN), the expected response (XRES), the encryption key (*CK*) and the integrity key (*IK*) [8]. The generation of authentication vectors is based on the pre-shared (between the user and the network) secret key, *K,* which is assigned to the user when the latter is subscribed to the UMTS network. In the sequel, the AAA server selects one out of the *n* obtained authentication vectors to proceed with the EAP-AKA authentication procedure and stores the remaining *n*-1 for future use. From the selected authentication vector it uses the keys *CK* and *IK* and the identity of the user to compute the Master Key (*MK*) of EAP-AKA, which is used as a keying material to generate the Master Session Key (*MSK*). As denoted in the EAP-AKA specifications [4], the AAA server has to store the *MK* key in order to execute the fast re-authentication procedure of EAP-AKA. Then, the AAA server calculates a Message Authentication Code value, denoted as MAC_{server}, which verifies the integrity of the next EAP-AKA message (i.e., EAP-Request/AKA-Challenge). The AAA server sends the EAP-Request/AKA-Challenge message to the user, which contains the RAND, AUTN and MAC_{server} payload. After receiving this information message, the user executes the UMTS-AKA algorithms and verifies the AUTN payload [8]. Then, he generates the *IK* and *CK* keys, calculates the key *MK*, and produces the *MSK* key. Likewise the AAA server, the user stores the generated *MK* key in order to execute fast re-authentication procedure of EAP-AKA. If the verification of the MAC_{server} value is successful, the user computes his response to the challenge (noted as an XRES payload) and sends an EAP-Response/AKA-challenge message to the AAA server that includes the XRES and a MAC_{user} value, which covers the whole EAP message.

Upon receiving the EAP-Response/AKA-challenge message, the AAA server verifies the received MAC_{user} value and checks if the received user's response to the challenge (XRES) matches with the response (SRES) of the selected 3G authentication vector. If all these checks are successful, the AAA server sends an EAP-success message along with the key *MSK* to the wireless AP. The latter stores the *MSK* key and forwards the EAP-success message to the user. Finalizing EAP-AKA, the following have been achieved: (i) the user and the WLAN have been authenticated to each other; (ii) the user and the AAA server have stored the *MK* key to perform the fast re-authentication procedure; and (iii) the user and the wireless AP share the key *MSK*, which is employed in the 802.11i security framework for the generation of the WLAN session keys [3]. After a successful EAP-AKA authentication, the user obtains a local IP address and can execute the IKEv2 protocol (i.e., next authentication step).

Second authentication. As shown in Fig. 4, in the second authentication step the user and the PDG execute the IKEv2 negotiation protocol [5], which encapsulates EAP-AKA for authenticating the peers (i.e., the user and the PDG). In addition, the PDG is authenticated twice using its certificate [2]. In the first two IKEv2 messages, the user and the PDG establish an IKE Security Association (IKE_SA) that provides security services to the following IKEv2 messages (see Fig. 4). Next, the user sends either his permanent or temporary identity to the PDG, and the latter forwards the identity to the AAA server. In the sequel, the AAA server obtains *n* authentication vectors from the HSS/AuC, if these are not available in the AAA server in advance. At this point, the AAA server initiates a second EAP-AKA authentication dialogue by sending to the PDG an EAP-Request/AKA-Challenge message. Upon receiving the EAP-Request/AKA-Challenge message, the PDG encapsulate it within an IKEv2 message and forwards the encapsulated message to the user. Except for the EAP-Request/AKA-Challenge payload, this message includes the PDG identity, the PDG's certificate (CERT) and the AUTHr field. The latter contains signed data used by the user to authenticate the PDG. After receiving the above fields, the user authenticates the PDG by verifying the AUTHr field (using the public key of the PDG included in the certificate field (CERT)) and the AUTN payload included in the EAP-Request/AKA-Challenge (using the UMTS-AKA algorithms). If the verifications succeed, the user sends an EAP-Response/AKA-Challenge message encapsulated again within an IKEv2 message. The EAP-AKA exchange continues, normally, until an EAP-Success message is sent from the AAA server to the PDG, which ends the EAP-AKA dialogue. In the last step of IKEv2, the user and the PDG are re-authenticated to avoid man-in-the-middle attacks [9] and establish an IPsec_SA (see Fig. 4). After the completion of IKEv2, the user obtains a global IP address, called Remote IP address, which is used for access to the 3G packet switched services or the public Internet via the 3G PLMN. In addition, the execution of IKEv2 results in the deployment of an IPsec-based Virtual Private Network (VPN) tunnel [7] between the user and the PDG that provides confidentiality and integrity to the data exchanged between them (see Fig. 1).

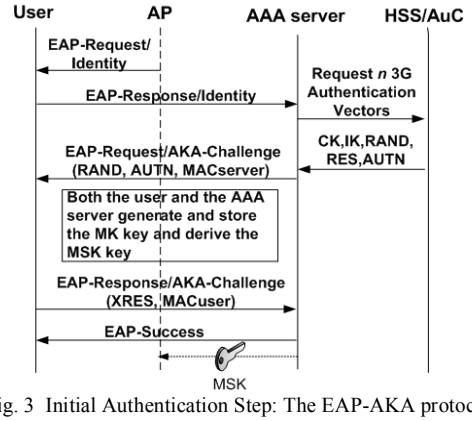

Fig. 3 Initial Authentication Step: The EAP-AKA protocol

C. *Motivation for Improving the Two-Pass EAP-AKA Authentication*

The analyzed two-pass EAP-AKA authentication procedure proposed in 3GPP 33.234 [2] involves a double execution of EAP-AKA. The first is carried out to register the user in the WLAN domain, while the second registers him in the 3G PLMN. Therefore, the two-pass EAP-AKA authentication procedure is not efficient, since it introduces a duplicated authentication overhead. This overhead is related to the exchange of messages that cause delays in users' authentication and consume radio resources, as well as to the computational processing at the level of mobile devices, which may induce energy consumption issues. It has to be noted that the mobile devices usually are characterized by low computational capabilities and limited energy power.

Trying to reduce this duplicated authentication overhead, the 3GPP standard (3GPP 23.234 [1]) specifies that in case that the PDG trusts the WLAN network, the first execution of EAP-AKA for registration in the WLAN domain can be omitted. Although this policy speeds up the authentication procedure, it may raise new security risks and threats. More specifically, if the first authentication step is omitted, an adversary could merely obtain a local IP address from the WLAN. Using this IP address, the adversary my either perform flooding attacks to the PDG exploiting the IKEv2 protocol or mount bandwidth attacks to the wireless interface of the WLAN. Although IKEv2 employs cookies to protect the network from flooding attacks, this mechanism can not provide an adequate level of protection [5]. Therefore, since the above Denial of Service (DoS) attacks (i.e., flooding and bandwidth attacks) may reduce significantly the quality of service offered by the network, the aforementioned policy must be carefully considered before applied.

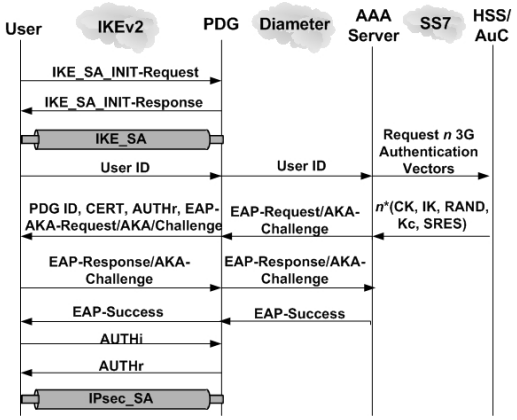

Fig. 4 EAP-AKA within IKEv2 (two-pass EAP-AKA authentication)

III. ONE-PASS EAP-AKA AUTHENTICATION

A. *Outline*

To address the duplicated authentication overhead of the two-pass EAP-AKA authentication procedure, this paper proposes a one-pass EAP-AKA authentication for the 3G-WLAN integrated networks. The proposed procedure reduces the authentication traffic, compared to the two-pass EAP-AKA authentication, without compromising the provided level of security.

Similarly to the two-pass EAP-AKA authentication, the proposed one-pass EAP-AKA authentication procedure includes two authentication steps. In the first step, the user and the WLAN are authenticated each other performing EAP-AKA. In addition, in this step the user and the AAA server generate and store the *MK* key, which is used in the next step. In the second step, the user is authenticated to the 3G PLMN domain by executing pure IKEv2 that omits the encapsulation of EAP-

AKA. In this step the authentication of the negotiating end-points (i.e., the user and the PDG) is based on the *MK* key, which is generated in the previous step from the execution of EAP-AKA. Thus, the proposed one-pass EAP-AKA authentication combines the first and the second authentication step by making a security binding between them. This binding eliminates the requirement for duplicated execution of EAP-AKA, reducing the overall authentication overhead.

The proposed one-pass EAP-AKA authentication procedure has minimal impact on the existing 3G-WLAN network infrastructure and functionality. The only requirement is that the PDG must be capable of retrieving the *MK* key, generated in the initial EAP-AKA authentication, from the AAA server. As mentioned previously, the AAA server stores the *MK* key and maintains a list which associates the user's identities (i.e., IMSI and temporary identity) with the *MK* key. Thus, the PDG can retrieve the *MK* key from the AAA server using the Diameter protocol. It is worth noting that there is a trusted relationship between the PDG and the AAA server, since there is a pre-established IPsec tunnel between them that protects the exchange of Diameter messages [6]. In addition, this tunnel protects the conveyance of the *MK* key during the proposed one-pass EAP-AKA authentication execution.

B. Authentication Procedure

Since the initial authentication step of the proposed one-pass EAP-AKA authentication is the same with the one of the two-pass, we do not elaborate it further. Thus, we assume the followings: i) a user has performed a successful initial authentication in the WLAN domain using EAP-AKA; ii) both the user and the AAA server have stored the *MK* key generated during EAP-AKA; and iii) the user and the wireless AP apply encryption to the data conveyed over the radio interface using the WLAN session keys (see sect. 2.2).

During the second authentication step of the proposed procedure, the user and the PDG are authenticated using the IKEv2 protocol. In addition, they establish a VPN tunnel that protects the data conveyed between them. The IKEv2 is executed in two phases (i.e., phase 1 and phase 2). In phase 1 the user and the PDG establish a bidirectional IKE_SA that protects all the subsequent IKEv2 messages. To initiate this phase, the user sends to the PDG the SAi1 (message 1-Fig. 5), which denotes the set of cryptographic algorithms for the IKE_SA that he supports, the KEi that is the Diffie-Hellman value, and a Ni value that represents the nonce. The nonce is used as input to the cryptographic functions employed by IKEv2 to ensure liveliness of the keying material and protect against replay attacks. The PDG answers with a message (message 2-Fig. 5) that contains its choice from the set of cryptographic algorithms for the IKE_SA (SAr1), its value to complete the Diffie-Hellman exchange (KEr) and its nonce (Nr). At this point, both the user and the PDG share a bidirectional IKE_SA that provides confidentiality and integrity services to the following IKEv2 messages.

After the establishment of the IKE_SA, the second phase of IKEv2 authenticates the peers and establishes an IPsec_SA. To achieve this both the user and the PDG calculate the AUTHi and the AUTHr payloads, respectively, using the *MK* key generated during the execution of EAP-AKA in the initial authentication step. Then, they send to each other the AUTHi and AUTHr payloads for verification achieving the security binding between the initial authentication step (i.e., the execution of EAP-AKA in the WLAN domain) and the second authentication step (i.e., the execution of IKEv2 in the 3G PLMN domain).

More specifically, in the second phase of IKEv2, the user sends to the PDG a message that includes his identity, the SAi2 payload that contains the chosen cryptographic suit for the IPsec_SA that the user supports, the traffic selectors (TSi and TSr) that allow the peers to identify the packet flows that require processing by IPsec, and the Configuration Payload Request (CP-Request) that is used to obtain a Remote IP address from the PDG and get access to the 3G-PLMN. The user also includes in this message the AUTHi payload, which is a MAC over the first IKEv2 message (i.e., message 1-Fig. 5) using the stored *MK* key.

After receiving this information, the PDG forwards to the AAA server the user identity (IDi) including a parameter, which indicates that the authentication is being performed for access to the 3G PLMN [2]. This will facilitate the AAA server to distinguish between authentications for WLAN access or for 3G PLMN access. Based on the user's identity, the AAA server retrieves the appropriate *MK* key and sends it to the PDG via the Diameter protocol (message 4 -Fig. 5). Recall that the *MK key* is conveyed in a secure manner, since there is a pre-established IPsec tunnel between the PDG and the AAA server.

Upon receiving the *MK* key, the PDG verifies the AUTHi payload in order to authenticate the user. In the sequel, it generates the AUTHr payload by computing a MAC over the second IKEv2 message (i.e., message 2 in Fig. 5) using the obtained *MK* key and sends it to the user. Except for the AUTHr payload, this message also includes the PDG's identity (i.e., W-APN) that identifies the provided 3G services, the traffic selector payloads (TSi and TSr), the SAr2 payload that contains the chosen cryptographic suit for the IPsec_SA that the PDG supports, and the assigned user's Remote IP address that is included in the Configuration Payload Reply (CP-REPLY) payload. Finally, the user verifies the AUTHr payload using the *MK* key and authenticates the PDG. At this point the authentication in the 3G PLMN is completed and an IPsec_SA is established between the user and the PDG that provides security services (see Fig. 5).

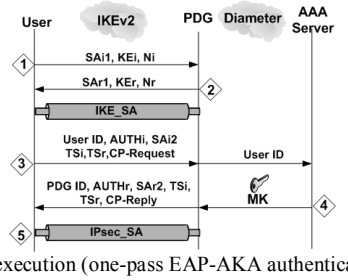

Fig. 5 IKEv2 execution (one-pass EAP-AKA authentication)

IV. EVALUATION OF THE PROPOSED ONE-PASS EAP-AKA AUTHENTICATION

A. Security Analysis

The security provided by the proposed one-pass EAP-AKA authentication procedure is based on the privacy of the *MK* key, which is generated during the initial authentication step in the WLAN domain. If this key is revealed, then an adversary can exploit it either to authenticate itself as a valid user to the 3G

PLMN or to eavesdrop on the legitimate user's data traffic. The ways in which the adversary could reveal the *MK* key are the following: (i) by retrieving the *MK* key from the WLAN session keys; (ii) by compromising the security of the entities that store the *MK* key (i.e., the user's device and the AAA server); and (iii) by performing an impersonation/spoofing attack in order to retrieve the *MK* key from the AAA server.

In the first type of attack, the adversary may get physical access to the wireless AP and obtain the WLAN session keys. Then, from the WLAN session keys he will try to retrieve the *MK* key. However, this type of attack can not be realized, since it requires the inversion of the one way hash functions used for the generation of the WLAN session keys [3]. Moreover, since the generation of the *MK* key is not based on a password [4], the adversary cannot retrieve it by performing a dictionary attack.

The second type of attack targets the user's device and the AAA server. More specifically, the adversary may attempt to retrieve the stored *MK* key either from the user's device by using a malicious piece of software (such as viruses, worms, etc.) or from the AAA server by invading the security of the 3G-WLAN core network. To defeat such attacks, the user's device must be protected from rogue code and the *MK* key must be stored in an encrypted form. Moreover, the AAA server must be secured by using firewalls, which protect it from unauthorized penetration and external attacks.

In the third type of attack, the adversary performs an impersonation/spoofing attack, which is executed as follows: First, the adversary, impersonating a valid PDG, communicates with the user and obtains his identity. Then, impersonating a valid AAA client, he sends the obtained user's identity to the AAA server and retrieves the user's *MK* key. Thus, the adversary can be authenticated to the user and establish a VPN tunnel between them. However, an essential prerequisite to render this attack successful is that the adversary must be capable of invading the security of the 3G-WLAN core network, since the communication link between the PDG and the AAA server is protected using a pre-established IPsec tunnel (see sect. 3.1).

B. Cost Analysis

Observing Fig. 4 and Fig. 5, it is evident that the proposed one-pass EAP-AKA authentication reduces the total number of messages exchanged, compared to the two-pass EAP-AKA. More specifically, for the registration of a user in the 3G PLMN the two-pass EAP-AKA authentication involves: (i) the exchange of eight IKEv2 messages between the user and the PDG; (ii) the exchange of four Diameter messages between the PDG and the AAA server; and (iii) the exchange of two message between the AAA server and the HSS/AuC for the retrieval of 3G authentication vectors. Thus, the two-pass EAP-AKA authentication procedure requires a total number of fourteen messages for user's registration in the 3G PLMN.

On the other hand, for the same procedure the proposed one-pass EAP-AKA involves the exchange of four IKEv2 messages between the user and the PDG, and two Diameter messages between the PDG and the AAA server. The AAA server does not exchange any credentials with the HSS/AuC, since the second authentication step of the proposed procedure avoids the retrieval of 3G authentication vectors. Thus, the one-pass EAP-AKA authentication procedure requires only a total of six messages for user's registration in the 3G PLMN.

Table 1. The number of messages exchanged for user's registration in the 3G PLMN using the two-pass and one-pass EAP-AKA authentication

Communication link	*Two-pass EAP-AKA*	*One-Pass EAP-AKA*
User-PDG	8	4
PDG-AAA server	4	2
AAA server-HSS/AuC	2	-
Total	**14**	**6**

The reduced authentication overhead entails a reduced computational processing and energy cost at the level of mobile devices as well as a reduced consumption of the radio resources. More specifically, the mobile devices avoid the computational processing and the energy consumption induced by the duplicated execution of EAP-AKA, the associated UMTS security algorithms, and the execution of public key algorithms. In addition, the reduced number of messages exchanged optimizes the usage of the radio resources improving the efficiency of user authentication in 3G-WLAN. Apart from reducing the authentication overhead, the one-pass EAP-AKA authentication consumes less 3G authentication vectors, compared to the two-pass EAP-AKA. Finally, the proposed procedure avoids the deployment of a public key infrastructure, since it does not employ certificates for the PDG authentication.

V. CONCLUSIONS

This paper has proposed a one-pass EAP-AKA authentication procedure for the 3G-WLAN integrated networks. The proposed procedure reduces the authentication traffic, compared to the two-pass EAP-AKA, without compromising the provided level of security. It combines the first and the second authentication step by making a security binding between them, eliminating the need for duplicated execution of EAP-AKA. As a future work we intend to estimate numerically the message delivery cost of the one-pass EAP-AKA and compare it with the one of the two-pass. Finally, we are going to provide a formal proof of the correctness of the proposed procedure.

REFERENCES

[1] *3GPP TS 23.234 (v7.3.0), "3GPP System to WLAN Interworking; System description", Release 7, Sep. 2006.*

[2] *3GPP TS 33.234 (v7.2.0), "3G security; WLAN interworking security; System description", Release 7, Sep. 2006.*

[3] *IEEE Std 802.11i, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements", 2004.*

[4] *J. Arkko, H. Haverinen, "EAP-AKA Authentication", RFC 4187, Jan. 2006.*

[5] *C. Kaufman, "The Internet Key Exchange (IKEv2) Protocol", RFC 4306, Dec. 2005.*

[6] *P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, "Diameter Base Protocol", RFC 3588, Sep. 2003.*

[7] *S. Kent, R. Atkinson, "Security Architecture for Internet Protocol", RFC 2401, Nov. 1998.*

[8] *C. Xenakis, L. Merakos, "Security in third Generation Mobile Networks", Computer Communications, Elsevier Science, Vol.27, No. 7, pp 638-650, May 2004.*

[9] *N. Asokan, V. Niemi, K. Nyberg. "Man-in-the-Middle in Tunneled Authentication Protocols". Lecture Notes in Computer Science, Vol. 3364, pp. 28-41, Springer 2005.*

ACKNOWLEDGMENT

Work supported by the project CASCADAS (IST-027807) funded by the FET Program of the European Commission.