One-pass EAP-AKA Authentication in 3G-WLAN Integrated Networks

Christoforos Ntantogian[1], Christos Xenakis[2]

[1]Department of Informatics and Telecommunications, University of Athens, Greece

[2]Department of Technology Education and Digital Systems, University of Piraeus, Greece

E-mail: ntantogian@di.uoa.gr, xenakis@unipi.gr

Abstract

The incorporation of Wireless Local Area Networks (WLANs) within the third generation (3G) networks materializes the next generation of mobile/wireless systems, named 3G-WLANs integrated networks. This paper proposes an improved authentication procedure for the 3G-WLANs integrated networks that enables a WLAN user to get access to the 3G packet switched services or to the public Internet through the 3G public land mobile network. The proposed procedure reduces significantly the authentication overhead compared to the legacy one, without compromising the provided security services. A security analysis of the proposed authentication procedure is elaborated that ensures the correctness of the authentication procedure, the provision of advanced security services and the elimination of possible attacks that may threaten the proposed authentication procedure. In addition, an energy cost analysis is carried out that compares the energy consumption induced by the legacy and the proposed authentication procedures. Finally, a communication cost analysis is provided that estimates the cost improvement of the proposed over the legacy authentication procedure.

Keywords: 3G-WLANs, EAP-AKA, authentication, security.

1 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 must follow a two-pass EAP-AKA authentication procedure in order to get access to the 3G packet switched services or the public internet through the 3G Public Land Mobile Network (PLMN). This procedure includes two discrete authentications. In the first authentication, the user executes the EAP-AKA protocol [7] that registers it to the WLAN domain. In the second authentication, the user executes the Internet Key Exchange version 2 (IKEv2) protocol [8] that encapsulates EAP-AKA, which registers it 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 [26]. This overhead is related to: (i) the exchange of messages that cause delays in users' authentication (i.e., especially in cases that the users are located away from their home network) and consumes radio resources; and (ii) the computational processing at the level of mobile devices that 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. 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 overhead, compared to the two-pass EAP-AKA authentication, without compromising the provided level of security. The proposed procedure combines the initial and the second authentications by making a security binding between them. This binding eliminates the need for duplicated execution of EAP-AKA resulting in less exchange of messages and authentication computations. Apart from reducing the authentication overhead, the proposed procedure consumes less 3G authentication vectors, compared to the two-pass EAP-AKA. The one-pass EAP-AKA authentication procedure has minimal impact on the functionality of the existing EAP-AKA and IKEv2 protocols and does not require any changes to the 3G-WLAN network infrastructure. A security analysis of the proposed authentication procedure is elaborated that ensures the correctness of the authentication procedure, the provision of advanced security services and the elimination of possible attacks that may threaten the proposed one-pass EAP authentication procedure. In addition, an energy cost analysis is carried out that compares the energy consumption induced by the two authentication procedures. Finally, a communication cost analysis is provided that estimates the cost improvement of the one-pass EAP-AKA over the legacy two-pass EAP-AKA authentication.

The rest of this paper is organized as follows. Section 2 briefly presents the related work, the 3G-WLAN interworking architecture and the specified 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 elaborating a security analysis, an energy cost analysis and a communication cost analysis. Finally, section 5 contains the conclusions.

2 Background

2.1 Related Work

Recent studies have focused on the security and performance of existing authentication procedures in mobile/wireless networks and how these can be improved. Specifically, W. Liang et al. [23] analyze the effects of the challenge-response authentication method in mobile/wireless networks. They classify the provided levels of security in terms of information secrecy, data integrity and resource availability. In addition, they analyze the effects of users' authentication on various Quality of Service (QoS) parameters such as authentication cost, time delay and call dropping probability, considering different levels of security.

Y. Zhang et al. [15] have proposed an improvement for the UMTS-Authentication and Key Agreement (AKA) procedure that addresses the potential of long delays induced by the retrieval of 3G authentication vectors. This occurs either in cases that the involved Serving GPRS Support Node (SGSN) and the Home Location Register/Authentication Centrer (HLR/AuC) are located far away the one from the other, or in cases that these two entities belong to different operators. Y. B. Lin et al. [14] have noticed that the fixed size of the generated 3G authentication vectors may impose authentication delays or bandwidth consumption during users' authentication in UMTS. Thus, they have proposed a mechanism that selects dynamically the size of the 3G authentication vectors using the

user's residence time in a cell and traffic patterns in order to optimize network resources and the efficiency of the authentication procedure.

Towards this direction, A. Saraireh et al. [24] have proposed a new authentication protocol that improves the performance of the UMTS-AKA procedure by minimizing the authentication time delay, call setup time and signaling message exchange between the user and the HLR/AuC. Moreover, C.C. Chang [25] has proposed an enhanced authentication and key agreement protocol for the Global System for Mobile communication (GSM) / General Packet Radio Services (GPRS). This protocol reduces the storage overhead in the Visited Location Register (VLR) and the bandwidth consumption induced between the VLR and the HLR during the GSM/GRPS authentication and key agreement procedure.

In the 3G-WLAN integrated networks a roaming user may experience long authentication delays in cases that it is attached to a foreign network, which is located far away (in terms of number of hops) from its home Authentication Authorization Accounting (AAA) server. To minimize the authentication delay and the associated computational overheads, several recent studies [18-21] have attempted to perform local authentication for the roaming user within the foreign network, which reduces the number of messages that the user exchanges with its home AAA server. Finally, Y. B. Lin et al. [13] have tried to reduce the authentication steps that a user performs to get access to the IP Multimedia Subsystem (IMS) services (i.e., one to get access to the GPRS and another to the IMS network). To achieve this, they have proposed a one-pass authentication procedure that reduces the total number of messages exchanged. However,

the proposed procedure does not include the IMS key agreement negotiation, downgrading the supported level of security.

In this paper, we pinpoint and address another significant challenge, which is neglected in the 3GPP specifications as well as in the previous studies. Specifically, we alleviate the authentication burden of the two-pass EAP-AKA authentication in the 3G-WLAN integrated networks. A common limitation of the existing literature is that they attempt to ameliorate the authentication overhead, either by undermining the provided security level, or by modifying extensively the underlying network architecture (e.g., including new entities) or the functionality of the authentication protocols. Driven by this observation, our approach differs from the previous studies in the sense that the proposed procedure reduces the authentication overhead without compromising the provided level of security. At the same time it does not require any modifications to the 3G-WLAN network infrastructure and has minimal impact on the functionality of the existing authentication protocols.

2.2 3G-WLAN Interworking Architecture

As shown in Fig. 1, the 3G-WLAN interworking architecture [1] consists of three individual parts: (I) the WLAN, (II) the visited 3G PLMN and (III) the home 3G PLMN. Note that Fig. 1 illustrates the architecture for the cases where the WLAN is not directly connected to the user's home 3G PLMN. The WLAN consists of the wireless Access Points (APs) that act like AAA clients, the AAA proxies that forward security related messages and the WLAN-Access Gateway (WLAN-AG) that is a gateway to 3G PLMN. It is assumed that the WLAN is based on the IEEE 802.11 standard [5] and the AAA protocol is Diameter [9].

On the other hand, the visited 3G PLMN includes the core network elements of the GPRS/UMTS such as the Gateway GPRS Support Node (GGSN) and the SGSN, an AAA proxy that forwards AAA information to the home AAA server (always 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 (PS) services requested by the user (i.e., Wireless Application Protocol, Multimedia Messaging Services, Location Based Services, etc.). 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, and the Home Subscriber Service (HSS)/Authentication Centre (AuC). The AAA server retrieves authentication information from the HSS/AuC and validates authentication credentials provided by users.

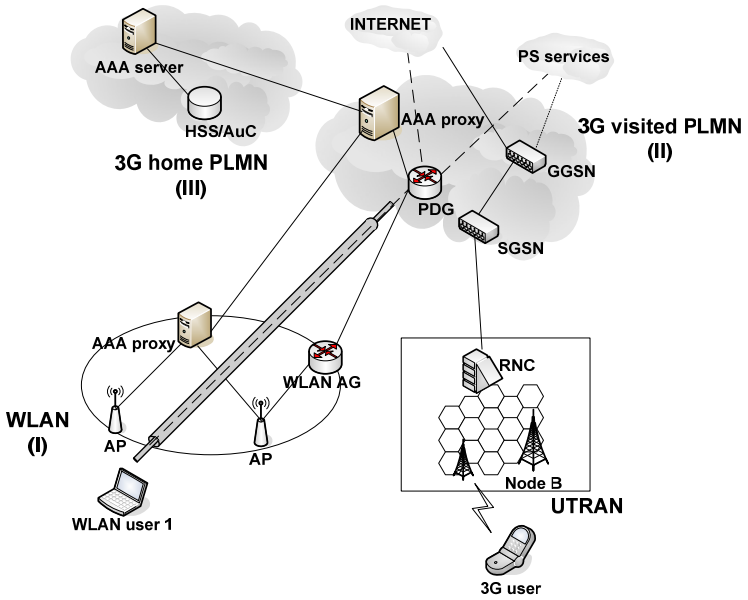


Fig. 1 3G-WLAN Network Architecture

2.3 Two-pass EAP-AKA Authentication

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

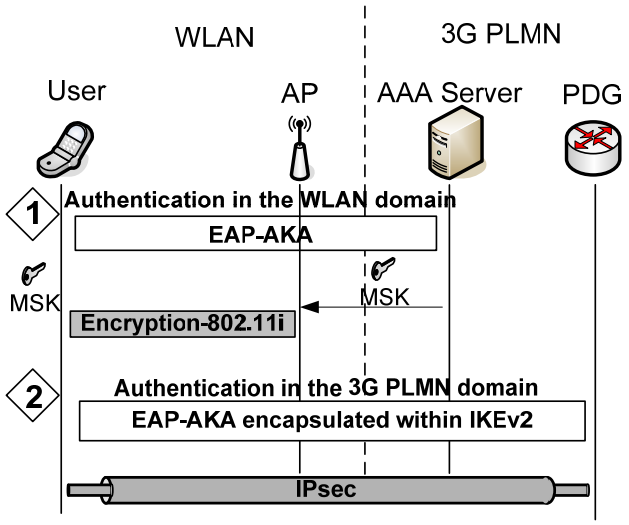


Fig. 2 Two-Pass EAP-AKA Authentication

Initial authentication for registration in the WLAN domain. The user and the WLAN are authenticated to each other using EAP-AKA [7] (see Fig. 4). This authentication involves the user, an AAA client that is actually a wireless AP, and the AAA server that obtains authentication information (i.e., 3G authentication vectors) from the HSS/AuC of the 3G PLMN, where the user is subscribed. After executing EAP-AKA, the user and the AAA server share an EAP-AKA *Master Key* (*MK*) key, which is used for the execution of EAP-AKA fast re-authentication and the generation of security keys [7]. The user and the AAA server use the MK to calculate the Master Session Key (MSK), and the second forwards it to the wireless AP. The AP and the user use this key to generate the WLAN session keys which are employed in the 802.11i security framework to provide security services [4].

Second authentication for registration in the 3G PLMN domain. In this authentication (see Fig. 3) the user and the PDG execute the IKEv2 protocol [8], which encapsulates EAP-AKA for authenticating the user and the 3G PLMN. At the beginning of IKEv2, the user and the PDG establish a bidirectional IKE Security Association (IKE_SA) that protects all the subsequent IKEv2 messages (see Fig. 3 - step a2). After the establishment of the IKE_SA, the user and the AAA server execute EAP-AKA encapsulated in IKEv2 messages for mutual authentication (see Fig. 3 - steps a3 to a7). Note that the PDG forwards the EAP-AKA messages to the AAA server using the Diameter protocol [9]. In addition, the PDG is authenticated to the user using its certificate [2]. At the end of IKEv2 the user obtains from the PDG 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. Moreover, an IPsec-based Virtual Private Network (VPN) tunnel [11] is deployed between the user and the PDG, which uses the Encapsulating Security Payload (ESP) [12] protocol that provides confidentiality and integrity to the data exchanged between them (see Fig. 3 - step a9).

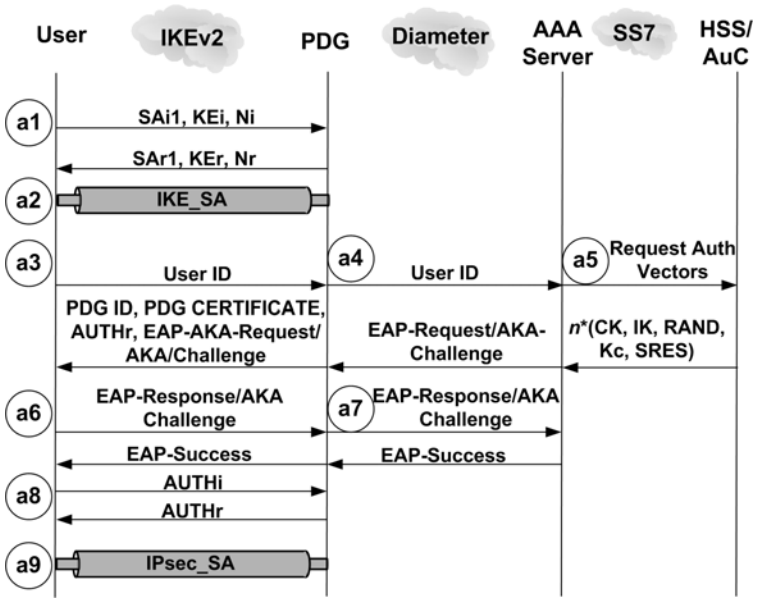


Fig. 3 Second Authentication for two-pass EAP-AKA authentication: EAP-AKA within IKEv2

Trying to avoid the double execution of EAP-AKA [26], 3GPP 23.234 [1] specifies that in cases 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. Specifically, if the first authentication is omitted, an adversary could merely obtain a local IP address from the WLAN. Using this IP address, the adversary may 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 cannot provide an adequate level of protection [8]. Therefore, since the above Denial of Service (DoS) attacks (i.e., flooding and bandwidth attacks) may reduce significantly the QoS offered by the network, the aforementioned policy must be carefully considered before applied.

3 One-pass EAP-AKA Authentication

3.1 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 and the related computations, compared to the two-pass EAP-AKA authentication, without compromising the provided level of security. Similarly to the two-pass EAP-AKA authentication, the one-pass EAP-AKA authentication procedure includes two authentications. In the initial authentication the user and the WLAN are authenticated to each other performing EAP-AKA. In addition, the user and the AAA server generate and store the *MK* key, which is used in the second authentication. An important notice here is that the initial authentication of the proposed one-pass EAP-AKA is exactly the same with the one of the two-pass EAP-AKA. In the second authentication of the proposed procedure, the user is authenticated to the 3G PLMN domain by executing pure IKEv2 that omits the encapsulation of EAP-AKA and the associated overhead. On the contrary, the second authentication of the legacy two-pass EAP-AKA re-executes EAP-AKA encapsulated within IKEv2 messages and utilizes the certificate of the PDG to achieve mutual authentication between the user and the PDG.

3.2 Authentication procedure

3.2.1 Initial authentication

As mentioned previously, the initial authentication of the proposed one-pass EAP-AKA (i.e., EAP-AKA authentication between the user and the AAA server) is the same with the one of the two-pass (see Fig. 4) and starts when the wireless AP requests the user's identity (EAP Request/identity message). The latter replies by sending to the AAA server

an EAP Response/identity message, which contain either the user's permanent (i.e., 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 fresh 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 (SRES), the encryption key (*CK*) and the integrity key (*IK*) [16]. The generation of authentication vectors is based on the pre-shared (between the user and the 3G network) secret key, *K,* which is assigned to the user when it 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* as well as the identity of the user to compute the EAP-AKA *MK* (see eq.1). This key is used as a keying material to generate the Master Session Key (*MSK*).

$$MK=prf^{1}(Identity \mid IK \mid CK) \quad (1)$$

As mentioned in the specifications of EAP-AKA [7], the AAA server stores the *MK* key in order to execute the EAP-AKA fast re-authentication and maintains a list that associates the user's identities (i.e., International Mobile Subscriber Identity (IMSI) and temporary identity) with the relative *MK* key. After generating and storing the MK key, the AAA server calculates a Message Authentication Code (MAC) value, denoted as MAC_{server}, which verifies the integrity of the next EAP-AKA message (i.e., EAP-

[1] prf represents a pseudo-random function. Pseudo-random functions are characterized by the pseudo randomness of their output, namely, each bit in the output of the function is unpredictable. In practice, a prf is implemented using block ciphers or one-way hash functions.

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 [16]. Then, it 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 be able to execute a fast EAP-AKA re-authentication. If the verification of the MAC_{server} value is successful, the user computes its 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 expected 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 followings 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 in order to be able to perform fast re-authentications; 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 [4]. After a successful EAP-AKA authentication, the user obtains a local IP address and can execute the IKEv2 protocol (i.e., second authentication).

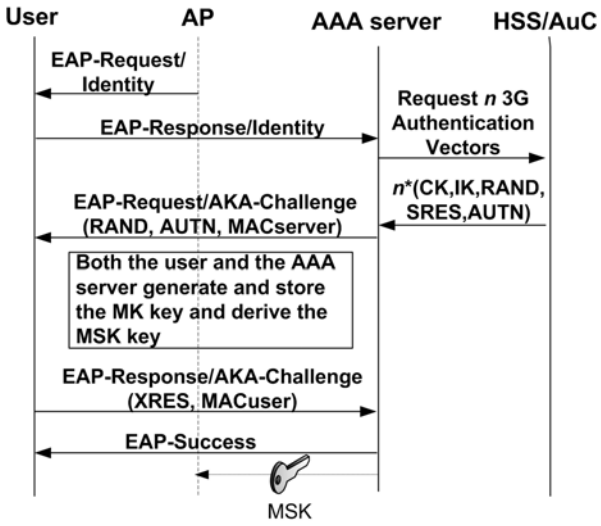


Fig. 4 Initial Authentication for the two-pass and one-pass EAP-AKA authentication: The EAP-AKA protocol

3.2.2 Second authentication

In the second authentication of the proposed procedure, the user and the 3G PLMN are authenticated using IKEv2, without executing EAP-AKA. In addition, the user and the PDG establish a VPN tunnel that protects the data conveyed between them.

To initiate IKEv2 the user sends to the PDG the SAi1 (Fig. 5(b) - step b1), which denotes the set of cryptographic algorithms for the IKE_SA that it 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 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 (Fig. 5 (b) - step b2).

After the establishment of the IKE_SA, the user sends to the PDG a message that includes its identity, the SAi2 payload that contains the chosen cryptographic suit for the

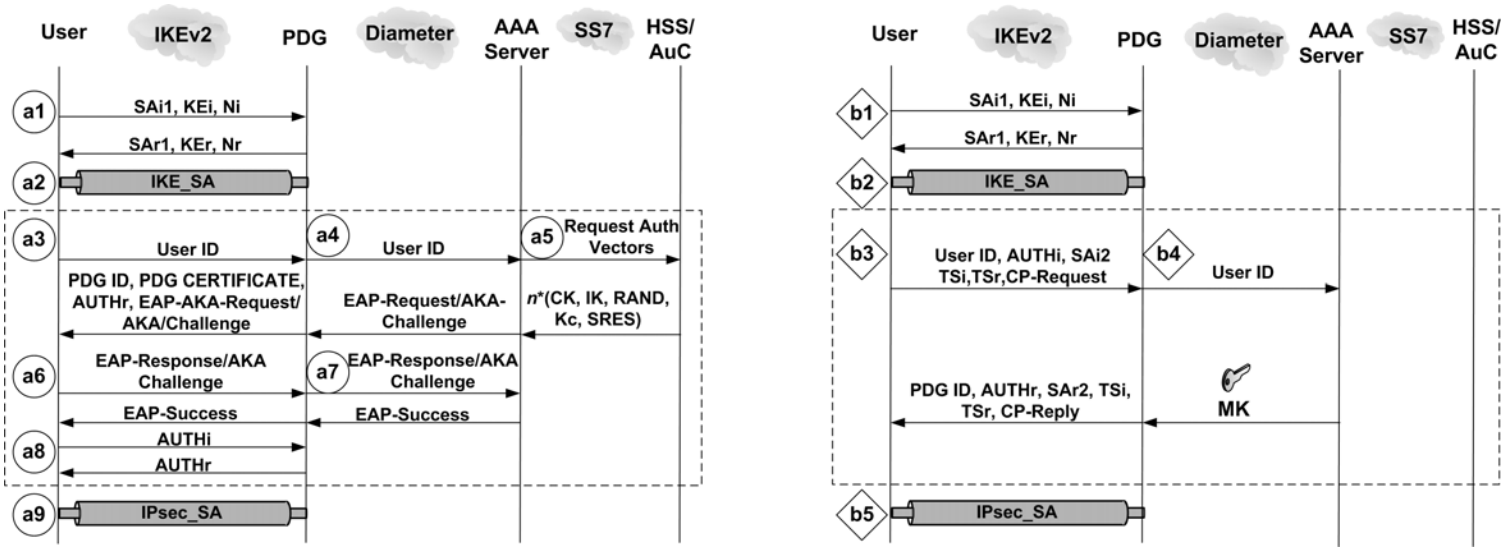
IPsec_SA that the user supports, the traffic selectors (TSi and TSr) that allow the peers to identify the packet flows that require processing by IPsec, and the Configuration Payload Request (CP-Request) that facilitates the user to obtain a Remote IP address from the PDG and get access to the 3G-PLMN. In addition, the user includes in this message the AUTHi payload, which is a MAC value computed over the first IKEv2 message using the stored *MK* key and it is used for the user's authentication. Recall that the user generates and stores the *MK* key during the execution of EAP-AKA in the initial authentication (see section 3.2.1). After receiving this information, the PDG forwards to the AAA server the user identity (IDi) (Fig. 5 (b) - step b4) 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. It is worth noting that the MK key is conveyed in a secure manner, since there is a trusted relationship between the PDG and the AAA server and a pre-established IPsec tunnel between them that protects the exchange of Diameter messages [9].

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 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 selectors (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. In order to complete the second authentication, the user verifies the AUTHr payload using the *MK* key and authenticates the PDG. At this point, the user and the PDG have been authenticated mutually using the AUTHi and AUTHr payloads respectively, which were computed using the *MK* key generated in the initial authentication. In this way, a security binding between the initial authentication and the second authentication has been achieved, eliminating the need for a duplicated execution of EAP-AKA within IKEv2. Finally, an IPsec tunnel is established between the user and the PDG that provides security services to the transmitted data (Fig. 5 (b) - step b5).

Comparing Fig 5 (a) (i.e., two-pass EAP-AKA) and Fig. 5 (b) (i.e., one-pass EAP-AKA) it can be perceived which authentication messages have been eliminated in the proposed one-pass EAP-AKA, optimizing the authentication procedure. It is evident that the IKEv2 message exchange for the establishment of the IKE_SA is exactly the same in the two-pass and one-pass EAP-AKA authentication (see Fig. 5 (a) - steps a1, a2 & Fig. 5 (b) - steps b1, b2 respectively). After the establishment of the IKE_SA, the user and the AAA server are mutually authenticated. To achieve this in the two-pass EAP-AKA, the user initiates the execution of EAP-AKA that requires three message exchange rounds (see Fig. 5 (a) - steps a3, a6, a8) between the user and the PDG, two message exchange rounds (see Fig. 5 (a) - steps a4, a7) between the PDG and the AAA server and one message exchange round (see Fig. 5 (a) - steps a5) between the AAA server and the HSS/AuC. On the other hand, the same in the one-pass EAP-AKA requires only one message exchange round (Fig. 5 (b) - step b3) between the user and the PDP, and one

between the PDG and the AAA server (Fig. 5 (b) - step b4). Finally, the proposed procedure avoids the communication between the AAA server and the HSS/AuC.



(a) two-pass EAP-AKA authentication

(b) one-pass EAP-AKA authentication

Fig. 5 Second Authentication for (a) two-pass EAP-AKA and (b) one-pass EAP-AKA (the message exchanges in the dashed boxes are the ones being optimized)

4 Evaluation of the One-Pass EAP-AKA Authentication

4.1 Security Analysis

Based on the previous analysis, we can deduce that the proposed one-pass EAP-AKA authentication procedure fulfills the security requirements of the 3G-WLANs integrated networks. This can be justified since the one-pass EAP-AKA authentication ensures three basic security features: (i) the correctness of the authentication procedure, (ii) the provision of advanced security services, and (iii) the elimination of possible attacks that may threaten the proposed authentication procedure.

Correctness of the authentication procedure: This feature evaluates the employed authentication mechanism. In the proposed one pass EAP-AKA authentication, a user,

identified by its IMSI, is authenticated only if it posses the same MK key with the one that is stored in the network for it. The MK key for each user is generated during the initial EAP-AKA negotiation of the proposed procedure, by applying a one-way function on the user's identity and the keys CK and IK (see eq.1). Both CK and IK directly derive from the pre-shared key K that is assigned to the user when it is subscribed to the 3G home network. Moreover, the AAA server is capable of associating the user's IMSI and the MK key with the pre-shared key K. Similarly, a legal user in UMTS is authenticated if it shares with the HSS/AuC the same key K. Therefore, it is evident that the proposed one-pass EAP-AKA correctly authenticates the user. In addition, it provides mutual authentication between the user and the WLAN, as well as between the user and the 3G PLMN.

Provision of advanced security services: Except for authentication, the proposed procedure establishes an IPsec-based VPN between the user and the PDG. IPsec employs the ESP protocol that provides confidentiality and integrity services to the transmitted data. Moreover, IPsec operates in tunnel mode (i.e., encapsulates and protects the entire IP packet including the IP header) and thus it protects the originally exchanged IP packets from traffic analysis. The proposed authentication procedure retains the security feature of IKEv2 for cipher suite negotiation among a plethora of supported security algorithms. In addition, the user can execute the IKEv2 protocol with the perfect forward secrecy feature enabled, which guarantees that a potential attacker cannot calculate fresh session keys from a disclosed key. Finally, the employment of IKEv2 also provides anonymity, since the user's identity (i.e., IMSI) as well as the identities of the requested services (i.e., W-APN) are conveyed securely using the IKE_SA (see Fig. 5 (b) – step b2).

Possible attacks: 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 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 by: (i) retrieving the *MK* key from the WLAN session keys; (ii) compromising the security of the entities that store the *MK* key (i.e., the user's device and the AAA server); and (iii) mounting a man in the middle attack in order to retrieve the *MK* key from the AAA server. Apart from the disclosure of the MK key, another type of attack that may threaten the proposed one-pass EAP-AKA authentication is related to DoS.

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 it tries to retrieve the *MK* key. However, this cannot be realized, since it requires the inversion of the one-way hash functions used for the generation of the WLAN session keys [4]. Moreover, since the generation of the *MK* key is not based on a password [7], the adversary cannot retrieve it by performing a dictionary attack.

The second type of attack targets the user's device and the AAA server. 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 a man in the middle attack, which is executed as follows: First, the adversary, impersonating a valid PDG, communicates with the user and obtains its identity. Then, impersonating a valid AAA client, it 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 itself and the user. 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).

Finally, attempting to perform a DoS attack an adversary may try to flood the PDG, which is located in the 3G PLMN, and deplete the resources of the core network. However, this is not possible because the proposed procedure incorporates the IEEE 802.1X port based authentication framework [6], which instructs the wireless APs to forward messages that are sent only by authenticated users and discard any other messages. On the other hand, both procedures (i.e., two-pass & one-pass) are vulnerable to DoS attacks that target the wireless APs.

4.2 Energy Cost Analysis

This section provides an energy cost analysis that compares the energy consumption induced by the legacy (i.e., two-pass EAP-AKA) and the proposed (i.e., one-pass EAP-AKA) authentication procedure. Note that in this analysis we do not consider the initial authentication, since it is identical in the two authentication procedures.

Table 1: Energy cost parameters

Symbol	Description
E_M	The energy cost of transmitting or receiving an IKEv2 message
E_{MAC}	The energy cost of providing or verifying a MAC using a pre-shared key
$E_{certificate}$	The energy cost of providing or verifying a certificate using a public key algorithm
$E_{KEY\text{-}UMTS}$	The energy cost of keys calculation using the UMTS-AKA algorithms
$E_{KEY\text{-}DH}$	The energy cost of keys calculation using the Diffie-Hellman algorithm
E_{ENC}	The energy cost of IKEv2 message encryption or decryption

The energy cost can be estimated considering the energy consuming communication and security activities. These activities concern: (i) the IKEv2 message transmission and reception, (ii) the calculation of an authentication value using a pre-shared key for providing or verifying a MAC, (iii) the calculation of an authentication value using PKI for providing or verifying a certificate, (iv) the calculation of keys using the UMTS-AKA algorithms, (v) the calculation of keys using the Diffie-Hellman algorithm, and (vi) the encryption or decryption of an IKEv2 message. The notation of the energy cost of each one of the above activities is presented in Table 1.

The legacy two-pass EAP-AKA authentication procedure involves the mobile user's device in the following energy consuming activities: (i) the verification of the PDG's certificate using a public key algorithm (see sect 2.3) , (ii) the generation of the AUTHi and XRES payloads and the verification of the AUTHr and AUTH payloads, (iii) the exchange of eight IKEv2 messages with the PDG; (iv) the encryption - decryption of six IKEv2 messages (IKE_SA) (see Fig. 3); (v) the execution of the Diffie-Hellman algorithm that generates keys for the IPsec SA, and (vi) the execution of the UMTS-AKA algorithms that generate the EAP-AKA session keys. Thus, the total energy consumption

induced by the legacy two-pass EAP-AKA authentication procedure to the involved mobile user's device is computed as:

$$E_{two\text{-}pass} = E_{MAC\text{-}PKI} + 4 \times E_{MAC} + 8 \times E_{M} + 6 \times E_{ENC} + E_{KEY\text{-}DH} + E_{KEY\text{-}UMTS} \quad (2)$$

On the other hand, the proposed one-pass EAP-AKA authentication procedure involves the mobile user's device in the following resource consuming activities: (i) the generation of AUTHi and the verification of AUTHr, (ii) the exchange of four messages with the PDG, (iii) the encryption - decryption of two IKEv2 messages (IKE_SA) (see Fig. 5 (b)); and (iv) the execution of the Diffie-Hellman algorithm that generates the IPsec session keys. Thus, the total energy cost is:

$$E_{one\text{-}pass} = 2 \times E_{MAC} + 4 \times E_{M} + 2 \times E_{ENC} + E_{KEY\text{-}DH} \quad (3)$$

From eq. (2) and (3), it can be perceived that the proposed authentication procedure reduces the computational processing and consequently the energy consumption at the level of mobile user device, compared to the two-pass EAP-AKA authentication. This is because the one-pass EAP-AKA does not involve a double execution of EAP-AKA, which duplicates resource consuming activities such as the calculation of authentication values, the exchange of IKEv2 messages and the encryption – decryption of them. The user's device avoids the computation of an authentication value using a public key algorithm, which consumes significant amount of energy [18], since the proposed procedure does not employ certificates for the authentication of the PDG. Moreover, the one-pass EAP-AKA avoids the execution of the UMTS-AKA algorithms that generate keys. Apart from reducing the computational processing and the energy consumption at the level of mobile devices, the proposed procedure optimizes the usage of radio resources improving the efficiency of user authentication in 3G-WLAN. In addition, it

consumes less 3G authentication vectors, compared to the two-pass EAP-AKA, and avoids the deployment of a PKI.

4.3 Communication Cost Analysis

This section provides an analysis of the communication cost that each one of the studied authentication procedures (i.e., one-pass and two-pass EAP-AKA) imposes to the underlying network infrastructure. Note that in this analysis we do not consider the initial authentication (i.e., the execution of EAP-AKA for registration in the WLAN domain), since it is exactly the same in both procedures. Recall from section 2.2 that we study the cases in which the user is away from its home 3G PLMN (roaming user) and it wants to access the PS services of the visited 3G PLMN. We assume that the delivery cost of a message between the user and the AAA server is one unit, and between the user and the PDG is a units. It is expected that $a<1$ since the AAA server is always located in the home network of the user, while the PDG typically resides in a visited network (see Fig. 1). Therefore, the number of hops for a message exchanged between the user and the PDG is less than the number of hops for a message exchanged between the user and the AAA server. We also assume that the delivery cost of a message exchanged between the AAA server and the HSS/AuC is x units. Since both the AAA server and the HSS/AuC are located in the user's home network, while the user resides in a visiting network (see Fig. 1), it is expected that $x<1$.

As shown in Fig. 5 (b), the proposed one-pass EAP-AKA authentication for the user's registration in the 3G domain, involves the exchange of two messages between the user and the PDG, and two messages between the PDG and the AAA server. Recall that the AAA server does not communicate with the HSS/AuC, since the one-pass EAP-AKA

does not execute EAP-AKA in the second authentication. Thus, the expected communication cost is:

$$C_1 = 2a + 2 \quad (4)$$

To estimate the communication cost for the user's registration in the 3G domain using the legacy two-pass EAP-AKA authentication, we consider two distinct cases. In the first case, the AAA server has to obtain fresh 3G authentication vectors from the HSS/AuC. In the second case, the AAA server has already a fresh 3G authentication vector (i.e., from a previous authentication of the user), and thus it does not communicate with the HSS/AuC. In the first case the legacy two-pass EAP-AKA authentication involves: (i) the exchange of four messages between the user and the PDG; (ii) the exchange of four messages between the user and the AAA server; and (iii) the exchange of two messages between the AAA server and the HSS/AuC for obtaining fresh 3G authentication vectors (see Fig. 3). Thus, the communication cost in this case is:

$$C_{2,1} = 4a + 2x + 4 \quad (5)$$

In the second case, where the AAA server does not communicate with the HSS/AuC, the communication cost is:

$$C_{2,2} = 4a + 4 \quad (6)$$

Note that one out of n authentications using the legacy two-pass EAP-AKA requires that the AAA server will obtain $2n$ authentication vectors from the HSS/AuC. Therefore, from eq. (5) and (6) we can deduce that the total communication cost for the legacy two-pass EAP-AKA authentication is:

$$C_2 = \frac{1}{n} C_{2,1} + \frac{n-1}{n} C_{2,2} \Rightarrow$$

$$C_2 = \left(\frac{1}{n}\right)(4a + 2x + 4) + \left(\frac{n-1}{n}\right)(4a + 4) = \frac{[n(4a+4) + 2x]}{n} \qquad (7)$$

From eq. (4) and (7) we can figure out that the improvement I of the communication cost of the proposed one-pass over the legacy two-pass EAP-AKA authentication is:

$$I = \frac{C_2 - C_1}{C_2} = \frac{4an + 4n + 2x - 2an - 2n}{4an + 4n + 2x} = \frac{2n + 2x + 2an}{4an + 4n + 2x} = \frac{n + x + an}{2an + 2n + x}$$

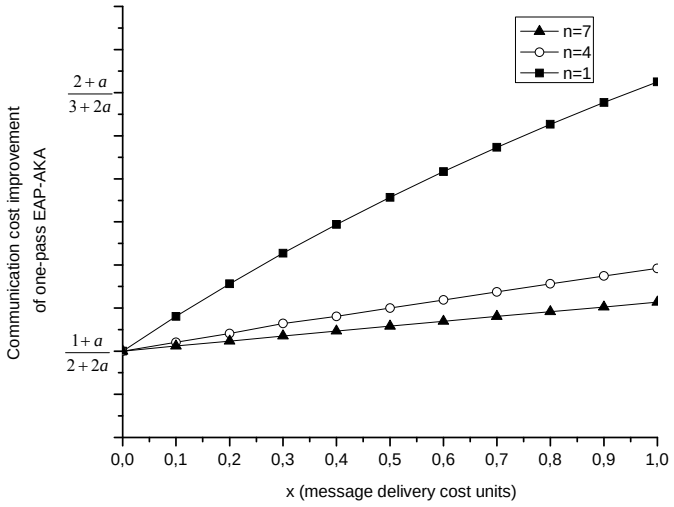


Fig. 6 Communication cost improvement I of the one-pass EAP-AKA over the two-pass EAP authentication

In Fig. 6 we plot the communication cost improvement *I* of the proposed procedure over the legacy two-pass EAP-AKA authentication as a function of the size *n* of authentication vectors and the value *x* that represents the message delivery cost between the AAA server and the HSS/AuC. We can deduce that the proposed procedure can save from $\frac{1+a}{2+2a}$ (n=1, x=0) up to $\frac{2+a}{3+2a}$ (n=1, x=1) delivery cost units. We observe that as the size *n* of 3G authentication vectors reduces, the communication cost improvement of the proposed procedure increases. This occurs because in the legacy two-pass EAP-AKA the AAA server has to communicate more frequently with the HSS/AuC to obtain fresh

3G authentication vectors. In addition, we notice that as the message delivery cost x increases, the communication cost improvement of the proposed procedure also increases. This is due the fact that the proposed one-pass EAP-AKA avoids the cost of obtaining 3G authentication vectors, since it does not require the additional message exchange between the AAA server and the HSS/AuC.

5 Conclusions

This paper has proposed a one-pass EAP-AKA authentication procedure for the 3G-WLAN integrated networks that reduces significantly the authentication overhead, compared to the two-pass EAP-AKA authentication, without compromising the provided level of security. The proposed authentication procedure combines the first and the second authentications by making a security binding between them. This binding eliminates the need for duplicated execution of EAP-AKA resulting in less exchange of messages and authentication computations. In this way the one-pass EAP-AKA improves the communication cost as well as the energy consumption compared to the legacy two-pass EAP-AKA authentication procedure. At the same time, it consumes less 3G authentication vectors and avoids the deployment of a PKI. A key advantage of the proposed procedure is that it does not require any modifications to the 3G-WLAN network infrastructure and it has minimal impact on the functionality of the existing EAP-AKA and IKEv2 protocols. Finally, the provided security analysis ensures the correctness of the one-pass EAP-AKA procedure, the provision of advanced security services and the elimination of possible attacks that may threaten the proposed authentication procedure.

Acknowledgement

Work supported in part by the project CASCADAS (IST-027807) funded by the FET Program of the European Commission and the 03ED910 research project, implemented within the framework of the Reinforcement Program of Human Research Manpower (PENED) and co-financed by National and Community Funds (75% from E.U.-European Social Fund and 25% from the Greek Ministry of Development-General Secretariat of Research and Technology).

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] ETSI TS 33.902, "*Formal Analysis of 3G Authentication Protocol*", 2002.

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

[5] IEEE Std 802.11, "*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*", 1999.

[6] IEEE Std 802.11X, "*Port Based Network Access Control*", 2004.

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

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

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

[10] C. Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence, "*Generic AAA Architecture*", RFC 2903, Aug. 2000.

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

[12] S. Kent, R. Atkinson, "*IP Encapsulating Security Payload (ESP)*", RFC 2406, Nov. 1998.

[13] Y.B. Lin, M.F. Chang, M.T. Hsu, L.Y. Wu, "*One-pass GPRS and IMS Authentication Procedure for UMTS*", IEEE Journal on Selected Areas in Communications, Vol. 23, No. 6, pp 1233-1239, Jun. 2005.

[14] Y.B. Lin, Y.K. Chen, *"Reducing Authentication Signalling Traffic in Third-Generation Mobile Network",* IEEE Transactions on Wireless Communications", Vol.2, No. 3, pp 493-501, May 2003.

[15] Y. Zhang, M. Fujise, "*An Improvement for Authentication Protocol in Third Generation Wireless Networks*", IEEE Transactions on Wireless Communications", Vol.5, No. 9, pp 2348-2352, Sep.2006.

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

[17] 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.

[18] N.R. Potlapally, S. Ravi, A. Raghunathan, N. K. Jha, "*Analyzing the Energy Consumption of Security Protocols*", International Symposium on Low Power Electronics and Design (ISLPED), Seoul, Korea, Aug. 2003.

[19] C.C. Yang, Y.W. Yang, W.T. Liu, "*A Robust Authentication Protocol with Non-Repudiation Service for Integrating WLAN and 3G Network*", Wireless Personal Communications, Springer, Vol. 39, No 2, pp 229-251, Oct 2006.

[20] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, S. Miller, "*Efficient Authentication and Key Distribution in Wireless IP Networks*", IEEE Wireless Communications, Vol 10, No 6, pp 52–61, Dec 2003.

[21] P. Prasithsangaree, P. Krishnamurthy, "*A new authentication mechanism for loosely coupled 3G-WLAN integrated networks*" in IEEE 59th Vehicular Technology Conference, (VTC), Vol. 5, pp. 2998–3003, May 2004.

[22] W. Liang, W. Wang, "*A Local Authentication Control Scheme Based on AAA Architecture in Wireless Networks*", in IEEE 60th Vehicular Technology Conference (VTC), Vol. 7, pp. 5276-5280, Sep. 2004.

[23] W. Liang, W. Wang, "*On Performance Analysis of Challenge/Response Based Authentication in Wireless Networks*", Computer Networks, Elsevier Science, Vol. 48, No. 2, pp. 267-288, Jun 2005.

[24] J.A. Saraireh, S. Yousef, "*A New Authentication Protocol for UMTS Mobile Networks*", EURASIP Journal on Wireless Communications and Networking, 2006.

[25] C.C. Chang, J.S. Lee, Y.F. Chang, "*Efficient Authentication Protocols of GSM*", Computer Communication, Elsevier Science, Vol. 28, No 8, pp. 921-928, Feb. 2005.

[26] C. Xenakis, C. Ntantogian, "*Security Architectures for B3G Mobile Networks*", Telecommunication Systems, Springer, Vol.35, pp: 123-139, Aug. 2007.