A Generic Mechanism for Efficient Authentication in B3G Networks

Christoforos Ntantogian[1], Christos Xenakis[2], Ioannis Stavrakakis[1]

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

[2]Department of Digital Systems, University of Piraeus, Greece

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

Abstract

A user in Beyond 3rd Generation (B3G) networks in order to get access to the network services must perform a multi-pass authentication procedure, which includes two or three sequential authentications steps. These multiple authentication steps include a redundant repetition of the same or similar authentication functions, which impose an unnecessary authentication overhead. This paper proposes a security binding mechanism, which reduces the execution of the redundant authentication functions of multi-pass authentications in a simple yet effective and secure manner. To achieve this, the proposed mechanism authenticates a user in the second and third step of a multi-pass authentication, by using the user's authentication credentials of the initial step. The focal point of the security binding mechanism is its generic application in multi-pass authentications, regardless of the underlying network architecture or protocols. To prove this, we have selected to present and analyze the application of the proposed mechanism in two different B3G scenarios (i.e., 3G-WLAN and WiMAX), resulting in the improved authentication procedures. A security analysis of the improved procedures has been carried out to identify possible attacks and propose security measures to eliminate them. Moreover, a simulation model has been developed to estimate and compare the performance of the improved 3G-WLAN authentication procedure to that of the legacy 3G-WLAN authentication. Simulation results show that the improved procedure presents better performance than its legacy counterpart.

Keywords: B3G networks, B3G security, multi-pass authentication, security binding, authentication performance.

1 Introduction

Beyond 3rd Generation (B3G) networks are materialized from the gradual integration of heterogeneous wireless and wired networks to a common core network platform [1], which provides users' and networks' autonomy and supports a wide range of multimedia services in a seamless manner. A B3G network architecture generally consists of three different Network Domains (NDs) (see Fig. 1(a)): (i) ND1 that includes the different Radio Access Networks (RANs) technologies (e.g., GSM EDGE Radio Access Network (GERAN), UMTS Terrestrial Radio Access Network (UTRAN), Wireless LAN (WLAN) and Worldwide Inter-operability for Microwave Access (WiMAX)); (ii) ND2 that comprises

the core network and performs administrative tasks such as mobility management, accounting, billing, etc.; and (iii) ND3 that contains the provided network services (e.g., IP Multimedia Subsystem (IMS), Multimedia Messaging Service (MMS), Location Based Services (LBS), etc.). Although B3G networks offer great prospects in network evolution, they also present some serious operational drawbacks, driven mainly by the integration of different technologies. One of these drawbacks is related to users' authentication through the multiple network domains. More specifically, a user, in order to get access to the network services, has to perform one authentication step for each domain, called as multi-pass authentication.

In a generic form, the user multi-pass authentication includes (see Fig. 1(b)): (i) an initial authentication step that establishes a wireless connection between the user and ND1 (i.e., the RANs); (ii) a second authentication step that registers the user to ND2 (i.e., the core network); and (iii) a third authentication step that provides the user access to the network services. These steps include a redundant repetition of the same or similar authentication functions, which imposes an unnecessary overhead that is related to: (i) the computation and verification of authentication values (e.g., signatures, Hash Message Authentication Codes (HMAC), etc.); (ii) the generation of security keys; (iii) the exchange of authentication messages; and, (iv) the encryption and decryption of authentication messages. This overhead causes pointless delays in users' authentication, especially in cases that users reside far away from their home network [24]. Moreover, it increases the energy consumption and depletes the available computational resources at the level of mobile devices, which are usually characterized by low processing capabilities and limited energy power. Finally, the redundant exchange of authentication messages entails a needless consumption of the available radio resources. Thus, the multi-pass authentication has detrimental effects on the quality of service offered to end users.

The user multi-pass authentication occurs in many B3G scenarios, as explained below. For example, a WLAN user that wants to get access to IMS services (3G-WLAN scenario) should perform a multi-pass authentication that includes three authentication steps (see section 6.1.5 of [2] and section 6.1 of [5]). In the initial step, the user executes the EAP-AKA [13] or EAP-SIM [14] protocol that registers it to the WLAN domain. In the second step, it executes the Internet Key Exchange version 2 (IKEv2) protocol [15] that encapsulates EAP-AKA or EAP-SIM, which registers it to the 3G Public Land Mobile Network (PLMN) domain. Finally, in the third step, it executes IMS-AKA [5] using the Session Initiation Protocol (SIP) [19] for registration within the IMS domain. In the 3G-

WLAN scenario, the second authentication step includes a duplicated execution of EAP-AKA (or EAP-AKA), while the third step includes a redundant execution of IMS-AKA. A multi-pass authentication (i.e., two step authentication) also occurs in WiMAX (see section 7.8.2 of [8]). In the initial step of this scenario, the user executes an RSA-based authentication for its device authentication within the WiMAX Base Station (BS). In the second step, it executes an Extensible Authentication Protocol (EAP) method [11] for the user's authentication within the WiMAX core network.

Apart from the above two scenarios, which are further presented and elaborated later in this paper, a multi-pass authentication also occurs in the Unlicensed Mobile Access (UMA) networks, where a user wants to have access to the GPRS or UMTS services using the UMA technology (see section 7.5 of [3]). In this scenario, the user first performs an initial authentication step to be registered in RAN (i.e., IP access network). Then, it performs a second step with the Generic Access Network Controller (GANC) in order to use the UMA technology. Finally, it performs a third step to get access to the core network. Another scenario, where multi-pass authentication is employed, is when a WLAN user wants to get access to 3G services, e.g., MMS, LBS, etc (see section 6.1.5 of [2]). In this scenario, the user performs an initial authentication step to be registered within WLAN and then it performs a second step to be registered within the 3G PLMN domain. Finally, a multi-pass authentication also takes place in cases that a UMTS user wants to get access to IMS services (see section 6.1 of [5]). In this scenario, the user performs an initial authentication step to be registered within the UMTS network and then, it performs a second step with the IMS network to gain access to the IMS services.

To limit the execution of the redundant authentication functions of multi-pass authentications, this paper proposes a security binding mechanism. The proposed mechanism authenticates a user in the second and third step of a multi-pass authentication procedure by using the user's authentication credentials of the initial step, in a simple yet effective and secure manner. In this way, it reduces the overall authentication signaling traffic of multi-pass authentications and mitigates the associated burden. The proposed mechanism is deployed through two different forms. The focal point of this mechanism is its generic application in multi-pass authentications, regardless of the underlying network architecture or protocols. To prove this, we have selected to present and analyze the application of the proposed mechanism in two different B3G scenarios (i.e., 3G-WLAN and WiMAX), resulting in the improved authentication procedures. The analyzed 3G-WLAN scenario involves the authentication of a WLAN user who wants to have access to

the IMS services [1][4], while the WiMAX scenario involves the initial registration of a user within the WiMAX network [8]. A security analysis of the improved 3G-WLAN authentication and WiMAX authentication procedures is carried out to identify and elaborate on possible attacks that threaten the authentication procedures, the users and the underlying network. Moreover, we propose security measures that can be applied to eliminate these threats. A simulation model has been developed to assess and compare the performance of the improved 3G-WLAN authentication to that of the legacy 3G-WLAN authentication in terms of authentication delay and the rate of Authentication Vectors Request (*AVR*).

The rest of this paper is organized as follows: Section 2 provides the background, by briefly presenting the B3G network architecture, the multi-pass authentication procedure in a generic form, and the related work. Section 3 analyzes the proposed security binding mechanism. Section 4 presents the improved 3G-WLAN authentication procedure and section 5 presents the improved WiMAX authentication procedure. Section 6 and section 7 evaluate the improved procedures by performing a security analysis and a performance analysis, respectively. Finally, section 8 contains the conclusions.

2 Background

2.1 B3G network architecture

As mentioned previously, ND1 of a B3G network architecture (see Fig. 1(a)) includes the different RANs technologies such as UTRAN, GERAN, WLAN, WiMAX, etc. WLANs consist of wireless Access Points (APs), which act like Authentication, Authorization, Accounting (AAA) [22] clients that forward security related messages to the AAA server using Diameter [16]. On the other hand, WiMAX consists of BSs and a gateway called Access Service Network (ASN) gateway, which connects WiMAX with the AAA server. ND2 includes the core network elements of B3G such as the Packet Data Gateway (PDG), the AAA server, and the Home Subscriber Server (HSS)/Authentication Centre (AuC). PDG connects a WLAN with the provided network services (see Fig. 1(a)) and acts as an AAA client, which communicates with the AAA server using Diameter. The latter (i.e., AAA server) retrieves authentication information from HSS/AuC and validates authentication credentials provided by users. Finally, ND3 consists of the IMS network, which provides multimedia services to users (i.e., MMS, LBS, etc.). In IMS, services are provided by the Call Session Control Functions (CSCF) using the SIP protocol [19]. There are three types of CSCFs: (i) a Proxy-CSCF (P-CSCF) that is connected with PDG and is

responsible for controlling IMS sessions; (ii) a Serving-CSCF (S-CSCF) that communicates with HSS/AuC to receive IMS subscriber data and authentication information; and (iii) an Interrogating-CSCF (I-CSCF) that is responsible for selecting a S-CSCF for a user.

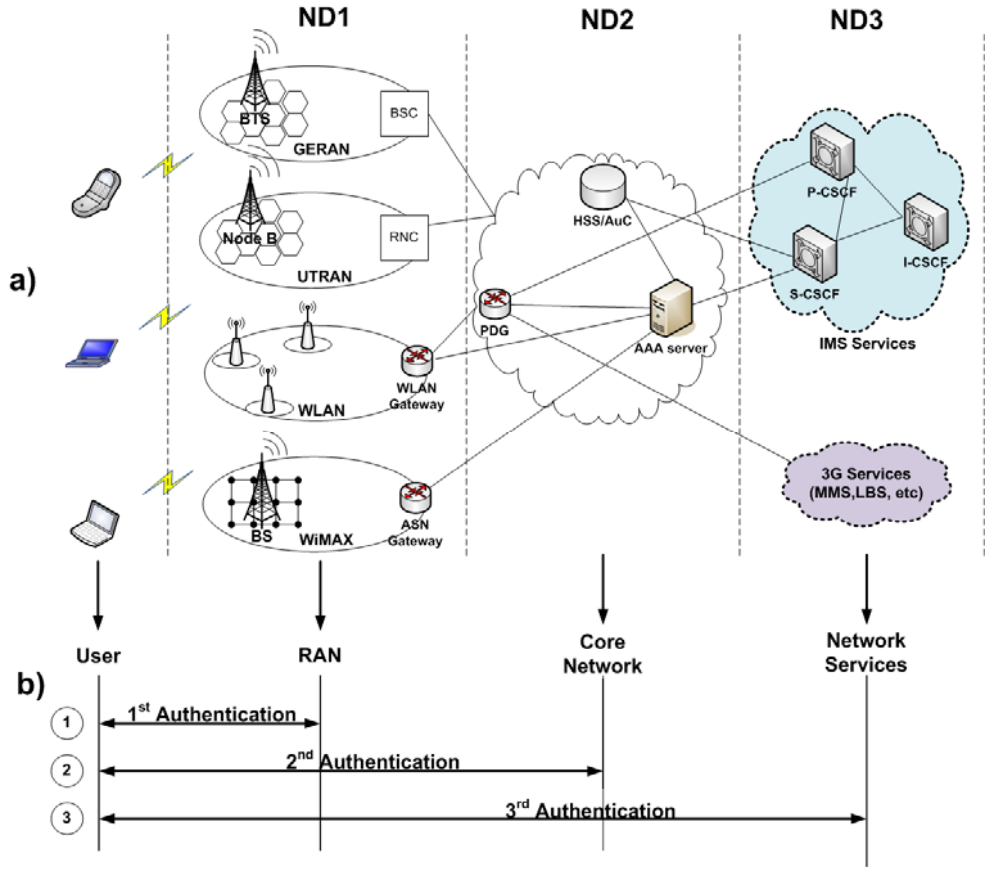

Fig. 1: (a) B3G network architecture and (b) user multi-pass authentication

2.2 User multi-pass authentication

In this section we present and analyze the user multi-pass authentication in a generic form. It is assumed that there is a trust relationship between the NDs. This assumption is based on the fact that the deployment environment and characteristics of NDs, such as wired infrastructure, fixed topology and centralized administration, promote and facilitate the establishment of robust trust relationships. In addition, trust is a crucial factor not only for security issues but also for many interworking aspects of B3G networks, such as roaming, accounting, management, mobility, etc. As mentioned above the user multi-pass authentication in a generic form includes three distinct steps. In the initial step, the user and ND1 are mutually authenticated and the former gets access to the latter. At the end of this step, the user and ND1 share a secret session key, which is used for the provision of confidentiality and integrity services to the data exchanged over the radio interface. As

shown in Fig. 2, this step starts with the user who sends its identity *(ID_1user)* to ND1. The latter, after verifying that the user is authorized to use the network recourses, responds to it by sending back the network identity *(ID_{ND1})*. Then, the user and ND1 exchange to each other authentication related information (e.g., a nonce, a timestamp, keying material, certificates, the supported cryptographic algorithms, etc.), using more than one round trip message exchanges (see Fig. 2). After these, the user generates a K_1auth key (using pseudo random functions), which is used to compute an authentication value $AUTH_{user}$ (using an HMAC function [12]) and sends the latter to ND1. On the other hand, ND1 generates the same key (i.e., K_1auth) and verifies the received $AUTH_{user}$. Similarly, ND1 computes an authentication value $AUTH_{ND1}$ using the K_1auth key and sends this value to the user for verification purposes. At the end of this negotiation, both the user and ND1 generate a secret key K_1enc, which is used to protect the data exchanged between them (see Fig. 2).

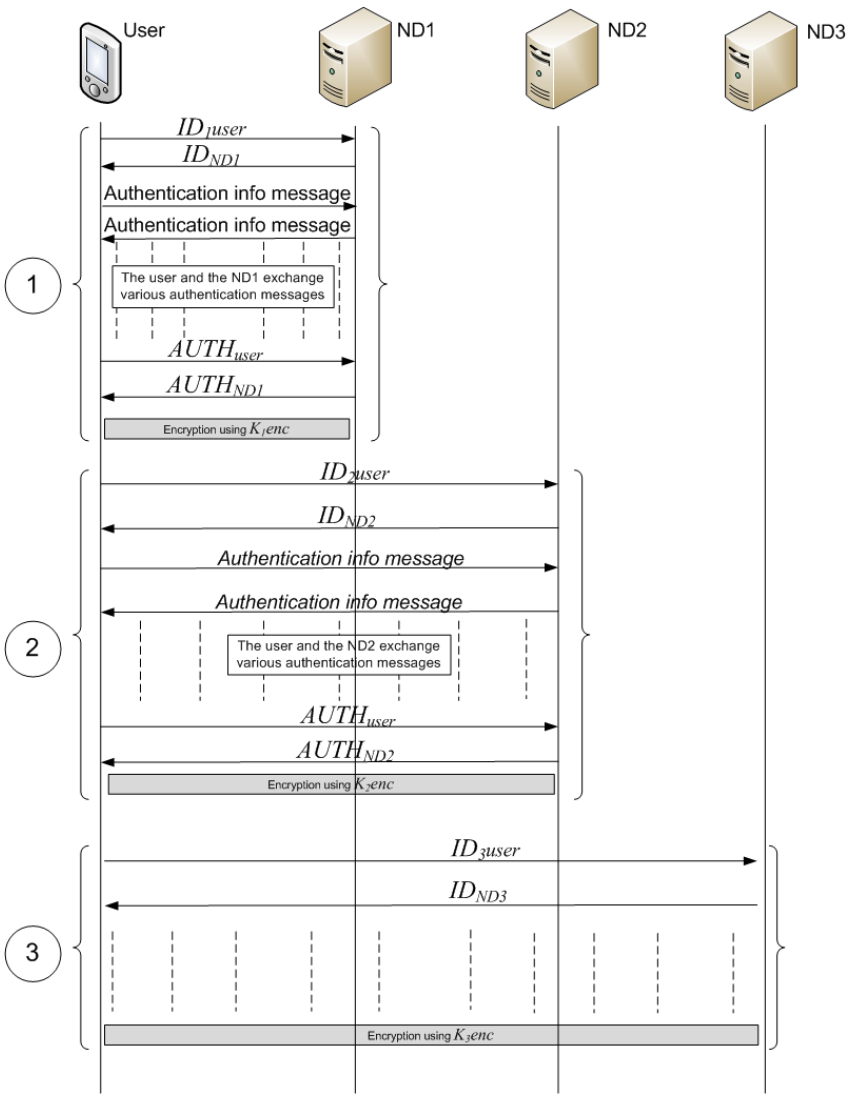

Fig. 2: Generic user multi-pass authentication

In the second authentication step, the user and ND2 are also authenticated, mutually, in a similar way with the initial step. First, the user sends its identity (ID_2user) to ND2 and the latter responds with its own (ID_{ND2}). In the sequel, both of them exchange authentication related information and generate an authentication key, K_2auth. Using this key, the user and ND2 compute $AUTH_{user}$ and $AUTH_{ND2}$ values, respectively. Then, they send to each other the computed values for verification purposes (see Fig. 2). If verifications are successful, the user and ND2 are authenticated, mutually, and both of them generate a shared secret key (K_2enc), which is used to protect the data exchanged between them (Fig. 2). Finally, in the third step, the user and ND3 are also authenticated, mutually, and the former is getting access to the provided network services. It starts with the user who sends its identity (i.e., ID_3user) to ND3, and the latter responds with its own (i.e., ID_{ND3}). The authentication procedure proceeds similarly to the previous steps, and at the end of this step both the user and ND3 share a secret key (i.e., K_3enc) that protects data exchanged between them.

2.3 Related Work

There is a rather limited literature that copes with the redundant steps and functions of the user multi-pass authentication in B3G networks and the associated overhead. A common limitation of the proposed procedures and mechanisms is that they either require extended modifications in the network infrastructure or they are vulnerable to malicious actions. In [29] the authors attempt to reduce the multiple authentication steps in the 3G-WLAN scenario, by integrating the authentication functions of the link layer (i.e., EAP-AKA) into the application layer (i.e., SIP). To achieve this they propose the incorporation of a P-CSCF entity within WLAN, eliminating in this way the execution of the EAP-AKA protocol. This reduces the authentication functions executed and the number of the related messages exchanged, but on the other hand raises some security concerns and requires enhancements in the network infrastructure. Specifically, an adversary is able to mount a Denial of Service (DoS) attack by sending endlessly spurious SIP authentication messages to WLAN, which are forwarded to the IMS network. This depletes the available resources in I-CSCF and S-CSCF, and eventually overflows the IMS network. Moreover, the proposed procedure requires the incorporation of SIP functionality in WLANs, which increases the implementation cost of them, since they have to be modified and enhanced to incorporate P-CSCFs.

Towards this direction, D. Celentano et al. [30] attempt to reduce the number of authentication steps of the legacy 3G-WLAN authentication and mitigate the associate overheads, by integrating the authentication functions of the application-layer protocols (i.e., IKEv2, SIP) into the link layer protocols (i.e., EAP-AKA). In this way, they achieve a one-pass authentication procedure that provides mutual authentication between a user and a 3G-WLAN integrated network, and at the same time establishes an IPsec tunnel between the user and PDG that protects the data exchanged. However, this procedure faces some serious weaknesses, which are highlighted below: First, it cannot establish an IPsec tunnel, since it does not negotiate the IPsec security association parameters, which are essential for the establishment and operation of an IPsec tunnel. Thus, the messages exchanged between the user and PDG are vulnerable to eavesdropping. Another security weakness is that the anonymity of users can be easily compromised. More specifically, the permanent IMS identity of a user, called IP Multimedia Private Identity (*IMPI*), is always conveyed in clear text over unprotected network channels, and thus, it can be easily disclosed. Y. B. Lin et al. [23] have proposed a mechanism that reduces the authentication steps that a user performs to get access to the IMS services, reducing also the authentication latency and the related burden in IMS networks. Finally, C. M. Huang et al. [27] have proposed a one-pass IMS authentication that reduces the authentication steps of the legacy IMS authentication. To achieve this, the proposed procedure uses timestamps and new security algorithms in order to guarantee the same security level with the legacy. On the other hand, the negative effects of this lie in the fact that its deployment requires extended modifications to the legacy IMS authentication.

In this paper, we extend and generalize the mechanism proposed by Y. B. Lin et al. [23]. In contrast to this mechanism, which is applied only to IMS networks; our mechanism is not tied to any specific network architecture or protocol. Thus, it can be applied to all of the aforementioned B3G scenarios, which employ multi-pass user authentications (i.e., legacy procedures), resulting in the corresponding improved procedures. We further enhance the work of [23] by carrying out a comprehensive performance analysis using simulations, and a security analysis to identify possible attacks and propose security measures that eliminate them. Overall, our work differs from the previous in the sense that: (a) it does not compromise the level of security provided by the legacy authentication procedures; (b) it does not require extensive modifications to the underlying network architecture; and (c) it complies with existing protocols used.

3 Security Binding Mechanism

The proposed security binding mechanism is deployed through two different forms: (i) the security identity binding and (ii) the security key binding. Both of them can be applied either in the second or third step of multi-pass authentications. The security identity binding enables ND2 or ND3 (of a B3G network architecture) to authenticate a user using the identity of the user (ID_1user) employed in the initial authentication step. The security key binding enables ND2 or ND3 to authenticate a user using the key (K_1auth) generated in the initial step. A prerequisite for the application of security identity binding is that the identity of the involved user in the first step (ID_1user) has to be different from the user's identity in the second (ID_2user) and third step (ID_3user). A prerequisite for the application of security key binding is that ND1 has to store the authentication key K_1auth, generated in the first authentication step. For the deployment of both forms of the proposed mechanism, each one of ND2 and ND3 should maintain a list. The list of ND2 will contain the pair of identities of each user employed in the initial and the second authentication step (i.e., ID_1user, ID_2user). Similarly, the list of ND3 will contain the pair of identities of each user employed in the initial and third step (i.e., ID_1user, ID_3user). Both lists (i.e., ND2 and ND3) are created during the offline registration of users (e.g., USIM/SIM purchase) within the B3G network. As they include permanent identities, there is no need for continuous updates. Therefore, they can be easily deployed and maintained without extra overhead and extensive modification to the B3G network infrastructure.

In the generic multi-pass authentication the security identity binding mechanism is deployed as follows. Initially, a user performs the first authentication step with ND1 using the identity ID_1user. In the sequel, the same user conveys its identity ID_2user or ID_3user that identifies it in ND2 and ND3, respectively, to ND1. The latter retrieves the user's identity that has been employed in the first step (ID_1user) and sends it together with ID_2user to ND2 (if the security identity binding is applied in the second step) or with ID_3user to ND3 (if it is applied in the third step). Note that the way that ND1 retrieves ID_1user depends on the specific protocols employed and thus, we analyze it in the next sections where specific cases are studied.

Upon receiving the pair of identities ((ID_1user, ID_2user) or (ID_1user, ID_3user)), ND2 or ND3 may perform the security identity binding. Using ID_2user or ID_3user as an index, ND2 or ND3, respectively, queries the list maintained locally, and retrieves the corresponding user's identity of the initial step, which is denoted as ID_1user'. In the sequel,

ND2 or ND3 checks whether ID_1user is equal to ID_1user'. If this happens, then the received ID_2user or ID_3user belongs to the requested user, which has been successfully authenticated in the initial step using ID_1user. Thus, the user is considered to be legitimate and ND2 or ND3 conveys its identity *(*ID_{ND2} or ID_{ND3}) to the user, indicating its successful authentication. By applying the security identity binding, the second or third step of the generic multi-pass authentication is executed in only one message exchange between the user and ND2 or ND3 respectively.

The application of security key binding in the generic multi-pass authentication is described below. Initially, the user performs the first authentication step with ND1 using the identity ID_1user. Recall that in this step, both the user and ND1 generate a key K_1auth for authentication purposes (see Fig. 2). In the sequel, the same user conveys its identity ID_2user to ND2 (if the security key binding is applied to the second step) or ID_3user to ND3 (if it is applied to the third step) along with the key K_1auth, generated in the first step. Upon receiving this pair *(*(ID_2user, K_1auth) *or* (ID_3user, K_1auth)*)*, ND2 or ND3 may perform the security key binding. Using the received ID_2user or ID_3user as an index, ND2 or ND3 queries the list of identities maintained locally, and retrieves the corresponding user's identity of the initial authentication step, which is denoted as ID_1user'. Then, ND2 or ND3 sends the retrieved identity (*ID_1user')* to ND1. The latter, using ID_1user' retrieves the related authentication key of the initial step, denoted as K_1auth', and conveys it to ND2 or ND3, depending on which step the security key binding is applied to. The way that ND1 retrieves the key K_1auth depends on the specific protocols employed in each scenario (see sect. 4 and 5).

Upon receiving K_1auth', ND2 or ND3 checks whether K_1auth is equal to K_1auth'. If this happens, then ID_2user or ID_3user belongs to the requested user, which has been successfully authenticated in the initial step using K_1auth. Thus, the user is considered to be legitimate and ND2 or ND3 conveys its identity *(*ID_{ND2} or ID_{ND3}) to the user, indicating its successful authentication. Similarly to the security identity binding, the application of security key identity binding in the generic multi-pass authentication results in the execution of the second or third authentication step in only one message exchange between the user and ND2 or ND3.

The proposed security binding mechanism using one of the two deployment forms (i.e., security identity or key binding) can be applied to the entire of B3G scenarios that use multi-pass authentication. To prove this fact, we have selected to analyze the application of the proposed mechanism in two different B3G scenarios (i.e., 3G-WLAN and WiMAX),

resulting in the improved authentication procedures. In the following, the improved 3G-WLAN authentication procedure (that uses both the security identity binding and the security key binding) and the improved WiMAX authentication (that uses the security key binding) are presented.

4 Improved 3G-WLAN authentication

The improved 3G-WLAN authentication includes three authentication steps, the as the legacy procedure [32]. The initial step in both procedures is the same and involves EAP-AKA or EAP-SIM. Note that in the current analysis we do not present EAP-SIM, since its functionality is similar to EAP-AKA. In the second authentication step of the improved 3G-WLAN authentication the user and the 3G PLMN domain are mutually authenticated using IKEv2. This step of the improved procedure does not include the re-execution of EAP-AKA, as in the legacy procedure, due to the application of security key binding. After being authenticated in 3G PLMN, the user proceeds to the third authentication step in which the security identity binding is applied to avoid the redundant execution of IMS-AKA.

4.1 Initial authentication step

The initial authentication step (see Fig. 3) starts when the wireless AP asks from the user its identity (*EAP Request/identity* message). The latter replies by sending to the AAA server an *EAP Response/identity* message that contains its permanent identity, called International Mobile Subscriber Identity (*IMSI*). After obtaining the user's identity, the AAA server checks whether it possesses a fresh 3G Authentication Vector (AV), stored from a previous authentication with the specific user. If not, the AAA server (using the identity of the user) performs an *AVR* procedure and gets *L* the size of fresh 3G AV from HSS/AuC. Each time that AVR is executed the requesting network receives *L* the size of fresh 3G AV [7]. A 3G AV includes a random challenge (*RAND*), the authentication token (*AUTN*), the expected response (*XRES*), the encryption key (*CK*) and the integrity key (*IK*) [6][25]. To proceed with the EAP-AKA authentication, the AAA server selects a fresh AV and uses the *CK* and *IK* keys (of the selected AV) as well as the identity of the user to compute the EAP-AKA Master Key (*MK*). This key is used as a keying material to generate the Master Session Key (*MSK*). It is important to mention that the AAA server must store the *MK* key, in order to execute the EAP-AKA fast re-authentication procedure [13]. Then, the AAA server calculates a Message Authentication Code (MAC) value, denoted as *MACserver*, which

verifies the integrity of the next EAP-AKA message (i.e., *EAP-Request/AKA-Challenge*). The AAA server sends to the user the *EAP-Request/AKA-Challenge* message, which contains the *RAND*, *AUTN* and *MACserver* payload. After receiving this message, the user executes the UMTS-AKA algorithms and verifies the *AUTN* payload. Then, it generates the *IK* and *CK* keys, calculates the *MK* key, and produces the *MSK* key. Likewise the AAA server, the user stores the generated *MK* key in order to be able to execute the fast EAP-AKA re-authentication. If the verification of the *MACserver* value is successful, the user computes its response to the challenge (noted as *SRES* payload) and sends an *EAP-Response/AKA-challenge* message to the AAA server that includes *SRES* and a *MACuser* value, which covers the whole EAP message.

Upon receiving the *EAP-Response/AKA-challenge* message, the AAA server verifies the received *MACuser* value and checks if the received user's response to the challenge (i.e., *SRES*) matches with the expected response (i.e., *XRES*) of the selected 3G AV. If all these checks are successful, the AAA server sends an *EAP-success* message along with the *MSK* key to the wireless *AP*. The latter stores the *MSK* key, and forwards the *EAP-success* message to the user. Both *AP* and the user use this key to generate the WLAN session keys, which are employed in the 802.11i security framework to provide confidentiality and integrity services [9]. After a successful EAP-AKA authentication, the user obtains a local IP address and can execute the IKEv2 protocol (i.e., next authentication step).

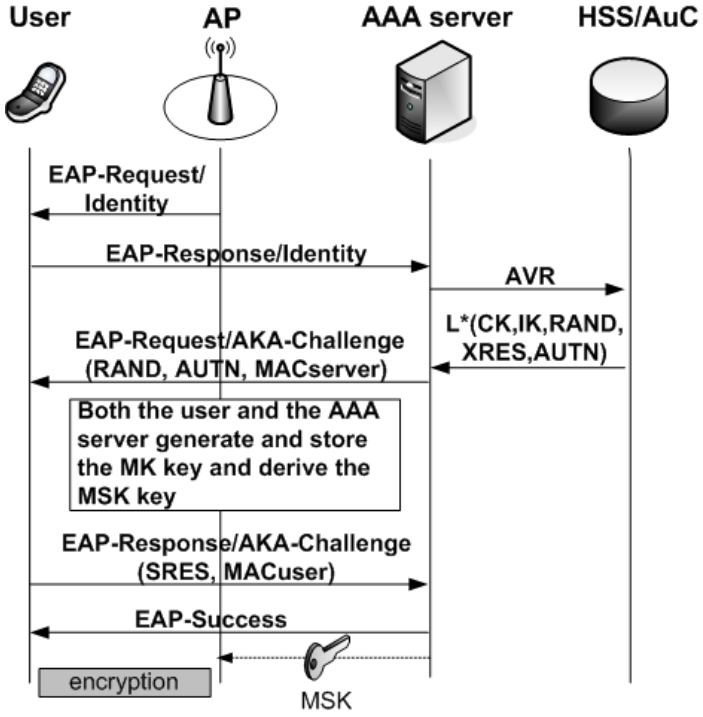

Fig. 3: Initial authentication step of the improved and legacy authentication: EAP-AKA protocol

4.2 Second authentication step-security key binding

This step starts with the user who initiates IKEv2 by sending to PDG an *IKE_SA Request* message (see Fig. 4(a) - a1), and the latter responds with an *IKE_SA Response* message. At this point both the user and PDG execute the Diffie-Hellman algorithm to establish a bidirectional IKE Security Association (IKE_SA) that provides confidentiality and integrity services to all the subsequent IKEv2 messages (see Fig. 4(a) - a2). After the establishment of IKE_SA, the user sends a message to PDG that includes its identity and various IKEv2 payloads, such as traffic selectors, supported cryptographic algorithms, etc. For the application of the proposed security key binding, the user includes in this message an *AUTHi* payload (i.e., a MAC value computed over the first IKEv2 message using the stored *MK* key), which is used for its (i.e., the user) authentication (see Eq. (1)).

$$AUTHi=HMAC_{MK}(IKE\_SA\ Request), \quad (1)$$

After receiving this information, PDG obtains the *MK* key of the user, as explained below, in order to apply the security key binding (see sect. 3). PDG forwards the user's identity (*IDi*) to the AAA server, and the latter retrieves its own copy of the *MK* key (denoted as MK_{AAA} key) and sends it to PDG via the Diameter protocol. It is worth noting that the MK_{AAA} key is conveyed securely between PDG and the AAA server, since there is a trusted relationship and a pre-established IPsec tunnel between them. [16]. Upon receiving the MK_{AAA} key, PDG applies the security key binding by computing the AUTHi′ as follows:

$$AUTHi' = HMAC_{MK_{AAA}}(IKE\_SA\ Request) \quad (2)$$

If $AUTHi=AUTHi'$, it means that $MK=MK_{AAA}$ and thus, the user is considered to be legitimate, as it possesses a valid *MK* key. Otherwise (if $AUTHi\neq AUTHi'$), the user is not valid and its registration in the 3G PLMN is discarded. In case of a successful user's authentication, PDG generates the *AUTHr* payload (i.e., by signing the *IKE_SA Response* message using its private key) and sends it to the user. Besides *AUTHr*, this message also includes the PDG's certificate, the PDG's identity *(PDG ID)*, the traffic selectors and the set of cryptographic algorithms that PDG supports. The user retrieves the public key of PDG (from the PDG's certificate) and verifies *AUTHr* to authenticate PDG. At this point, the user and PDG have been mutually authenticated using *AUTHi* and *AUTHr*, respectively. Finally, an IPsec tunnel is established between them that provides security services to the transmitted data (Fig. 4(b) – b4).

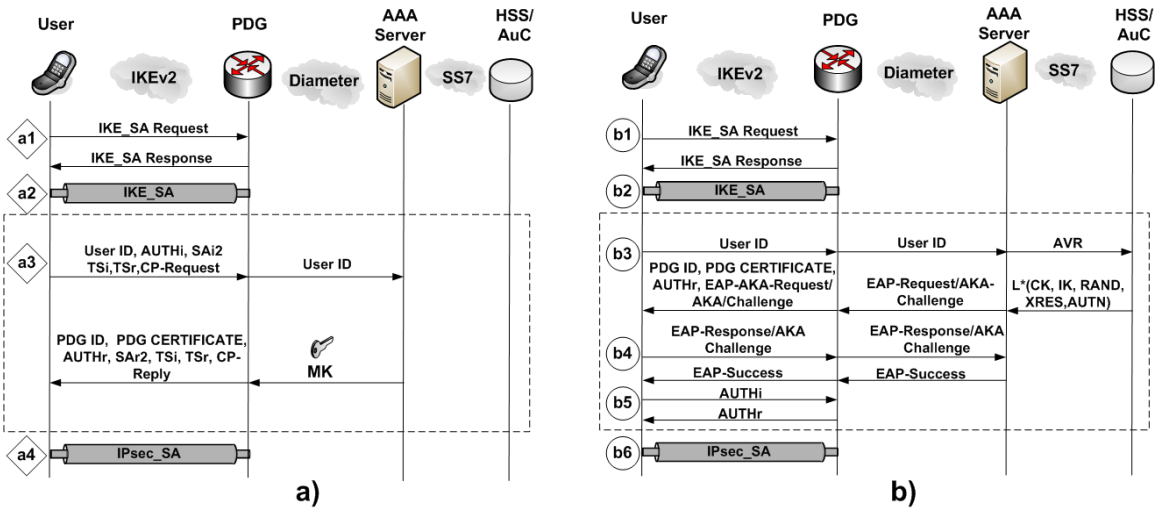

Fig. 4: Second authentication step for: (a) the improved 3G-WLAN authentication, and (b) the legacy 3G-WLAN authentication

Comparing the second step of the improved 3G-WLAN authentication (see Fig. 4(a)) with this of the legacy procedure (see Fig. 4(b)), we can pinpoint that the first includes significantly less message exchanges. More specifically, after the establishment of IKE_SA, which is exactly the same in both procedures (see Fig. 4(a) - a1, a2 and Fig. 4(b) - b1, b2 respectively), the improved 3G-WLAN authentication requires only one message exchange round between the user and PDG (Fig. 4(a) - a3) and one message exchange round between PDG and the AAA server (Fig. 4(a) - a4). On the contrary, the legacy procedure involves the execution of EAP-AKA that requires three message exchange rounds between the user and PDG (see Fig. 4(b) - b3, b6, b8), two message exchange rounds between PDG and the AAA server (see Fig. 4(b) - b4, b7) and one message exchange round between the AAA server and HSS/AuC (see Fig. 4(b) - b5).

4.3 Third authentication step-security identity binding

At the beginning of the third step, the user sends to PDG its *IMPI* identity (see Fig. 5(a) - a1), through the IPsec tunnel (established in the second step). Upon receiving the user's *IMPI*, PDG retrieves the *IMSI* identity of the user by querying the security policy database of the IPsec protocol, which maintains the user's profile [17]. Then, PDG sends the retrieved *IMSI* together with *IMPI* to S-CSCF. The latter, upon receiving the two identities, sends *IMPI* to HSS/AuC (see Fig. 5(a)). Using this information, HSS/AuC retrieves the permanent identity of the user (i.e., denoted as $IMSI_{HSS}$) and sends it to S-CSCF (see Fig. 5(a)). Finally, S-CSCF applies the security identity binding by checking whether *IMSI* = $IMSI_{HSS}$. If it is true, the user is considered to be legitimate (as it possesses a valid *IMSI* identity) and S-CSCF sends a verification message to the user to complete the latter's

registration in IMS. Otherwise (i.e., if $IMSI_{HSS} \neq IMSI$), the user is not valid and its registration to IMS is discarded.

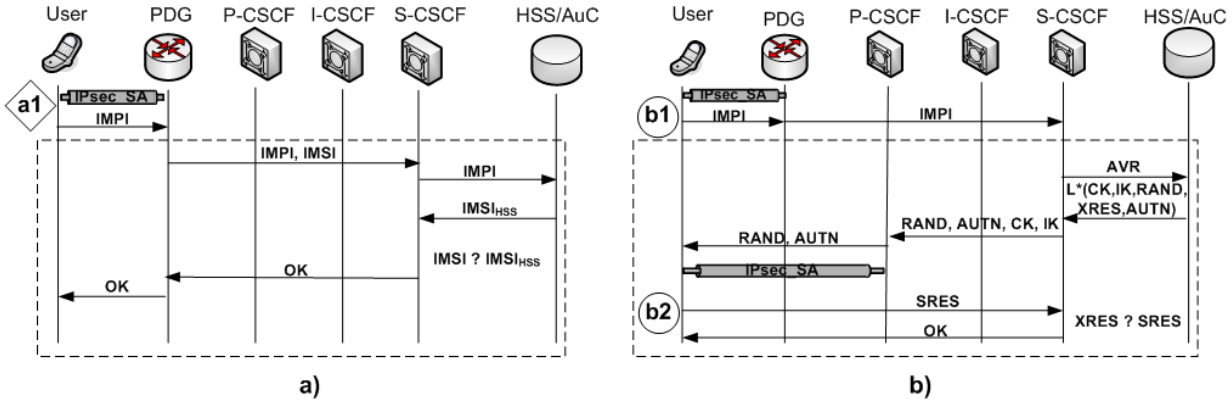

Fig. 5: Third authentication step for: (a) the improved 3G-WLAN authentication, and (b) the legacy 3G-WLAN authentication

Comparing the third step of the improved 3G-WLAN authentication (see, Fig. 5(a)) with this of the legacy procedure (see Fig. 5(b)), it can be perceived that the former (by applying the proposed security identity binding) completes this authentication step in only one message exchange round between the user and HSS/AuC. On the contrary, the legacy procedure executes the IMS-AKA authentication [5], which requires two message exchange rounds between the user and S-CSCF (see Fig. 5(b) - b1, b2) and one message exchange round between S-CSCF and HSS/AuC.

5 Improved WiMAX authentication

Similarly to the legacy WiMAX (multi-pass) authentication [8], the improved WiMAX authentication also includes two authentication steps, from which the initial step (i.e., RSA-based authentication) is the same in both procedures. In the second authentication step of the improved procedure, the security identity binding is applied to avoid the redundant execution of an EAP method. Although the WiMAX security architecture does not mandate the use of a specific EAP method, the WiMAX forum [33] advocates the use of the following methods: EAP-TLS [20], EAP-TTLS [21], EAP-AKA [13] or EAP-SIM [14]. For the studied scenario we have chosen to use EAP-TLS, since it is the most prominent and widely used security method. However, all of the above mentioned EAP methods can be used as they are seamlessly cooperating with the proposed security identity binding. For the application of security identity binding, the involved AAA server should be enhanced

with a list, which maintains for each user a pair of identities that consists of: (i) the user's device MAC address, and (ii) the user's EAP-TLS identity (*MACaddress*, $ID_{EAP\text{-}TLS}$).

5.1 Initial authentication step

The initial authentication step of the improved WiMAX authentication procedure (it is the same with the one of the legacy) includes only two messages (see Fig. 6). In the first message, the user sends to BS two different certificates: (i) *Cert(manufacturer)* that is issued by a trusted certificate authority and identifies the manufacturer of the user's device; and (ii) *Cert(device)* that is issued by the device manufacturer and identifies the user's device (i.e., it includes the MAC address of the device). Along with these certificates, the user sends to BS various security parameters such as the key size, the supported cryptographic algorithms, etc., which are required for the execution of the RSA-based authentication. After receiving this message, BS verifies *Cert(manufacturer)* using the public key of the trusted authority that has signed the certificate. If *Cert(manufacturer)* is valid, then BS obtains the public key of the manufacturer, which is included in *Cert(manufacturer)* in order to verify *Cert(device)*. In case that *Cert(device)* is valid, then the user's device is authenticated and BS generates, randomly, a *pre-PAK* key. Then, BS encrypts the *pre-PAK* key using the public key of the user's device (it is included in the *Cert(device)*) and conveys it to the user (see Fig. 6) together with its certificate *Cert(BS)* and its own set of security parameters (i.e., the key size, the supported cryptographic algorithms, etc.). After receiving this message, the user verifies *Cert(BS)* (using the public key of BS) and decrypts the *pre-PAK* key (using its private key). At this point, the user and BS have been mutually authenticated and share the *pre-PAK* key. Both of them (using the *pre-PAK* key) generate an EAP Integrity Key *(EIK)* that is used to provide origin authentication and integrity protection to the messages exchanged during the second authentication step (i.e., EAP-TLS messages) that follows. Note that at the end of the first authentication step, a WiMAX authorization Security Association (SA) [8] has been established between the authenticated user and BS, which facilitates the latter to identify the message flows of the former.

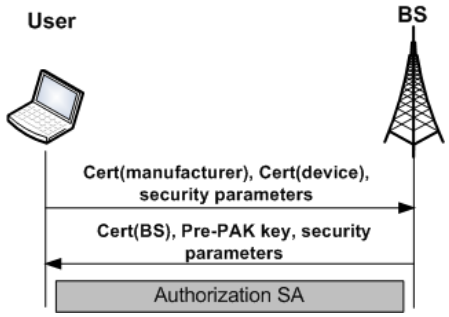

Fig. 6: Initial authentication step of both the improved and legacy authentication procedures: RSA-based authentication

5.2 Second authentication step

At the beginning of this step, the user sends an *EAPoL-Start* message to BS (see Fig. 7(a) – a1) and the latter responds by sending to the user an *EAP-Request/Identity* message. Upon receiving this message, the user sends to BS its identity $ID_{EAP\text{-}TLS}$ (see Fig. 7(a) – a2) and the latter retrieves the *MACaddress* of the user's device using the WiMAX authorization SA (it is established in the first step and identifies the message flows of the user). In the sequel, BS conveys the retrieved *MACaddress* together with $ID_{EAP\text{-}TLS}$ to the AAA server (see Fig. 7(a)). The latter (using the received $ID_{EAP\text{-}TLS}$) queries the maintained list of users' identities and retrieves the corresponding MAC address of the user (denoted as $MAC_{AAA\ server}$). Finally, the AAA server applies the security identity binding by checking whether the received *MACaddress* is equal to the retrieved $MAC_{AAA\ server}$. If yes, the user is considered to be legitimate and the AAA server sends an *EAP-Success* message to the user to complete the second authentication step. Otherwise (i.e., if $MACaddress \neq MAC_{AAA\ server}$), the user is not valid and its authentication is discarded.

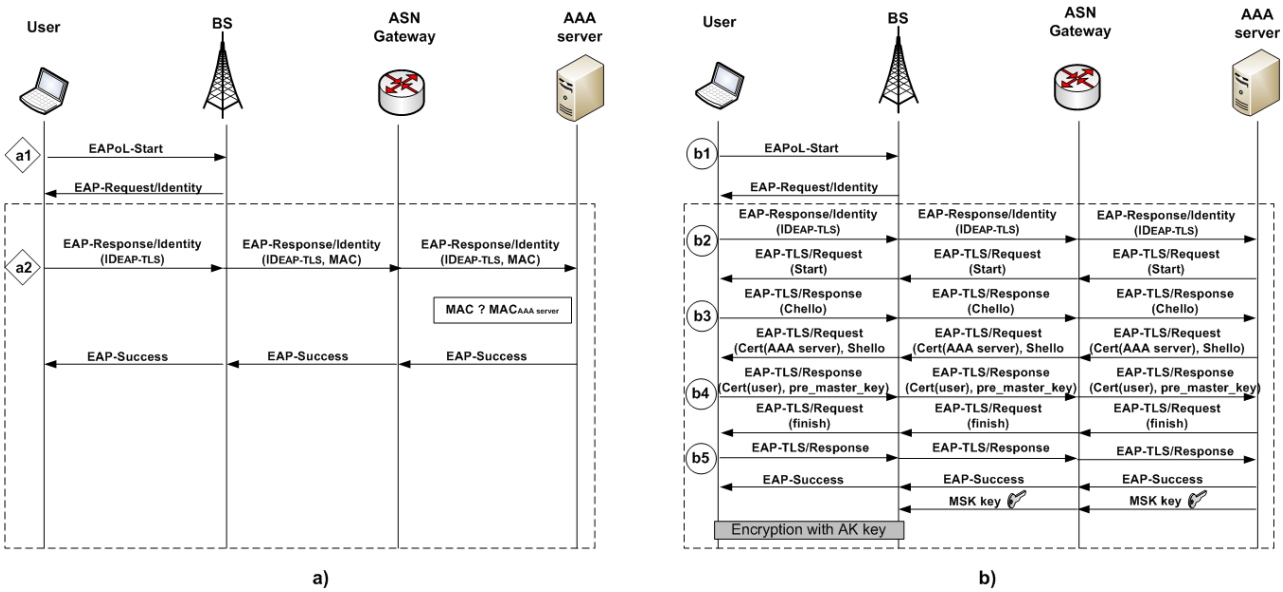

Fig. 7: Second authentication step of the: (a) improved WiMAX authentication, and (b) legacy WiMAX authentication

Comparing the second step of the improved WiMAX authentication (see Fig. 7(a)) with this of the legacy procedure (see Fig. 7(b)), it is evident that the former is faster than the latter and involves less processing and communication overhead. More specifically, the improved WiMAX authentication, in which the proposed security identity binding is applied, is completed in two message exchange rounds: one between the user and BS (see Fig. 7(a) – a1) and another between the user and the AAA server (see Fig. 7(a) - a2). On the contrary, the legacy procedure executes the entire EAP-TLS protocol, which requires one message exchange round between the user and BS (see Fig. 7(b) – b1) and four message exchange rounds between the user and the AAA server (see Fig. 7(b) - b2, b3, b4, b5). At the end of the execution of EAP-TLS, the user and the WiMAX network are mutually authenticated and the user and BS share a Master Session Key (*MSK*) (see Fig. 7(b) - b5). Both them use the *MSK* key and the *pre-PAK* key to generate an Authorization Key (*AK*), which is used to provide confidentiality and integrity services to the data exchanged between them.

6 Security Analysis

This section provides a security analysis in order to examine whether the application of both forms (i.e., security identity binding and security key binding) of the proposed security binding mechanism in the improved 3G-WLAN and WiMAX authentication procedures downgrades the provided level of security. To achieve this, we identify and elaborate on possible attacks that threaten the operation of the improved procedures, the

users and the underlying network. We examine the feasibility of these attacks and, if required, we propose security measures to defeat them.

First we elaborate on a common array of attacks, which can be performed in both proposed procedures. An adversary may attempt to obtain authentication credentials of the proposed procedures (i.e., identities and keys) by intercepting the communication links between NDs or compromising NDs. In case the adversary obtains an exchanged authentication credential, then it can impersonate a valid user, perform a replay attack or overcharge a user. However, these attacks cannot take place considering that there is a trust relationship between NDs (see section 2.2). The latter can deploy and maintain security associations (IPsec/TLS tunnels, Radius, etc.) to counteract malicious actions that target the security of them (i.e., NDs) or the communication links between them. It is important to mention that an adversary cannot compromise the wireless link between the user and ND1 to obtain authentication credentials, since it is protected using the session keys established in the first authentication step.

Another malicious action can be performed if an adversary tries to perform a DoS attack by flooding PDG or the ASN gateway in the improved 3G-WLAN or WiMAX procedure respectively to deplete the resources of the B3G core network. However, this is not possible because the wireless APs or the WiMAX BS forward messages to the core network that are originated only by authenticated users (from the first authentication step) and discard any other. On the other hand, both the proposed and legacy procedures are vulnerable to DoS attacks that target the radio interface of WLAN or WiMAX networks.

Moreover, the user device is a prime target for malicious actions, since it stores the authentication credentials of the proposed procedures, such as security keys, certificates and identities. An adversary may attempt to retrieve the stored authentication credentials from the user's device by using a malicious piece of software (such as viruses, worms, etc.). To defeat such attacks, the user's device must be protected from rogue code and the authentication credentials must be stored in an encrypted form.

Regarding the specific attacks which can be performed in the improved 3G-WLAN authentication procedure we can observe that it omits the establishment of an IPsec tunnel between a user and P-CSCF (as happens in the legacy) that protects the data exchanged (compare Fig. 5(a) to Fig. 5(b)). Thus, an adversary might eavesdrop on the messages exchanged between the user and P-CSCF (i.e., SIP messages). However, as explained below, such an attack is not feasible in the 3G-WLAN deployment scenario and extra security measures can be easily applied to counteract this weakness. The communication

channel between the user and P-CSCF consists of two separate links: one between the user and PDG, and another between PDG and P-CSCF (see Fig. 5(a)). The first link is protected by an IPsec tunnel that is established during the second authentication step of the improved procedure. On the other hand, the link between PDG and P-CSCF is unprotected and conveys SIP messages in clear text. However, an adversary cannot get access to this link and eavesdrop on the conveyed SIP messages, since this link is located within the core network of 3G-PLMN. Similarly, an adversary cannot get access to the PDG node. Therefore, we can deduce that the communication channel between the user and P-CSCF is secure.

Another security weakness of the improved 3G-WLAN authentication is related to the authentication of the IMS network to a user. More specifically, during the third authentication step (see section 4.3) the user is authenticated to the IMS network, but the latter is not authenticated to the user. On the contrary, the legacy authentication procedure provides mutual authentication between the user and IMS. An adversary may attempt to exploit the lack of mutual authentication, by impersonating an IMS network (i.e., bogus network) and deceiving the user to connect with it. Note that the adversary does not have to impersonate a user and an IMS network at the same time (i.e., man in the middle attack), since the IMS network is not authenticated to the user in the third authentication step of the proposed procedure. However, such an attack is not possible, since the IMS network is located within 3G PLMN, which has been already authenticated to the user during the second authentication step.

A more subtle attack can be performed in the improved 3G-WLAN authentication in case the adversary has obtained a valid pair of IMSI and IMPI identities and mounts a session hijacking. In this attack, the adversary initially lets the user to execute the first and second authentication step. After the successful completion of the second step, the adversary performs a jamming attack to block the radio communication of the user. At the same time relays the compromised IMPI identity to the IMS network to authenticate itself as a valid user. However, this attack is not feasible, since the adversary does not possess the security keys (established from the first authentication step) to communicate with the wireless AP. Thus, the latter discards any message originated from the adversary.

Regarding the improved WiMAX authentication procedure, we observe that this omits the generation of the *AK* key. In the legacy WiMAX authentication, the *AK* key (it is generated using the *MSK* key and the *pre-PAK* key) is used to protect the data exchanged between the user and BS (see section 5.2). In the improved procedure the user and BS

cannot generate the *AK* key, since they do not share the *MSK* key. This enables an adversary to eavesdrop on the data exchanged between the user and BS. In order to defeat such an attack, the user and BS should protect the data exchanged between them using the *pre-PAK* key, which is generated in the initial step. In this way, the improved procedure is protected from eavesdropping attacks.

Finally, the second step of the improved WiMAX authentication is one-way, meaning that only a user is authenticated to the AAA server and not the opposite. On the contrary, the legacy WiMAX authentication provides mutual authentication between the user and the AAA server. Thus, an adversary may attempt to exploit the lack of mutual authentication, by impersonating an AAA server (i.e., bogus AAA server) and deceiving the user to connect with it. However, in order to perform such an attack the adversary should have access to the B3G core network, since the AAA server is located within it. This is not feasible since the B3G core network is a protected network domain (see Fig. 1).

7 Performance Analysis

This section provides a performance analysis of the improved authentication procedures (i.e., 3G-WLAN and WiMAX) using a simulation model. Although we have studied the performance of both procedures, we have selected to present only the first one for the reasons explained below: First, the legacy 3G-WLAN authentication has been extensively studied in the related work [28], [29], [30], motivating us to elaborate on the performance improvement that we get by employing the proposed security binding mechanism. Second, the selected procedure employs three discrete authentication steps (the WiMAX authentication uses only two) and uses the two deployment forms of the proposed mechanism (i.e., security identity binding and security key binding) (the improved WiMAX authentication uses only security identity binding). Finally, both of the analyzed improved authentication procedures (i.e., 3G-WLAN and WiMAX) present similar behaviors and thus, the performance analysis for both of them would be redundant.

First, we present a simple analytic model that quantifies the performance of the improved and legacy 3G-WLAN authentication procedures. The analytical model, which is based on a previous work [32], provides insights for the cases which the improved 3G-WLAN procedure presents substantial benefits in terms of authentication cost. In this model, we consider a mobile user that establishes an IMS session and hand-offs from one access point to another during the same IMS session. We consider two handover cases: (a) intra-subnet handoff and (b) inter-subnet handoff. In the former case the user moves to a

new AP within the same IP subnet and performs the first authentication step (i.e., EAP-AKA). Since the mobile user remains at the same IP subnet, the current IP address of the user is valid to the new access point. Therefore, the established IPsec tunnel between the user and the PDG is maintained and the user avoids the execution of the second and third authentication steps (i.e., IKEv2 and IMS-AKA execution respectively). On the other hand, in case of the inter-subnet handoff the mobile user moves to a new access point within a different IP subnet. Similarly to the intra-subnet handoff, the user performs the first authentication step to register in the WLAN. In the sequel, it must obtain a new IP address, since its current IP address is not valid in the new IP subnet. This entails the execution of the second and third authentication step.

To estimate the total authentication cost C of the two procedures, first we have to estimate the average number H of handoffs performed by the mobile user. We assume that the residence time of the mobile user in the coverage area of an access point and the duration of an IMS session follows exponential distribution with mean n and μ respectively. Based on this assumption, we can derive the average number of handovers H as:

$$H = \frac{\mu}{n + \mu P_f} \tag{1}$$

where P_f is the probability that a handoff session is blocked. Using eq. (1) we derive the total authentication cost C as:

$$C = A_c + \frac{H}{b} A_c \tag{2}$$

where b is the average number of access points uniformly distributed in the WLAN coverage area and A_c is the authentication cost for each authentication procedure (i.e., improved and legacy authentication procedure). The authentication cost A_c can be determined by considering the basic and most resource consuming communication and security activities, such as message transmission and reception, calculation of authentication values and message encryption/decryption [32].

Based on eq. (2) we have derived various numerical results. We observed that for relatively small values of the user residence time, the cost improvement of the proposed authentication procedure is greater. If the value of the mean residence time is lower from the value of the mean session time (i.e., $n < \mu$), then the improvement of the proposed over the legacy authentication procedure is exponential. On the other hand, as the user residence

time increases and approaches or exceeds the session time, the improvement becomes constant, since the mobile user performs less handovers. Moreover, we drew the conclusion that in case the mean IMS session time is relatively short, then the two authentication procedures present close cost values. Increasing the mean session time, which means that the user performs more handoffs, leads to greater differences in the authentication cost values. The above analysis leads to the conclusion that the improved 3G-WLAN authentication procedure presents the best performance gain in cases the mobile user has lengthy session time with short residence time in the coverage area of an access point.

The aforementioned analytical model provides useful insights into the authentication cost of an individual user with a single established IMS session. However, it is inadequate to capture the dynamic behavior of a system model that consists of multiple mobile users that establish parallel IMS sessions. The behavior of such a system model depends on various parameters, including the users' authentication request rate, users' mobility, 3G-WLAN network dimension, bottlenecks in PDG, etc. that affect the overall network performance in a complex and integrated manner. Therefore, in this study we have performed simulations in order to derive useful statistical performance bounds of a system model composed of multiple users that establish parallel IMS sessions and interact with the various 3G-WLAN network elements (i.e., APs, PDG, AAA server, CSCFs and HSS/AuC). In particular, we evaluate and compare the performance of the improved 3G-WLAN authentication to that of the legacy 3G-WLAN authentication, in terms of authentication delay, size of 3G AV, and ratio of AVRs performed in the two authentications to fetch fresh 3G AV.

Fig. 8 presents a graphical representation of the deployed simulation model, using the NS-2 simulation platform [31]. The model consists of: (i) the users, (ii) 200 APs distributed uniformly in 10 WLANs (WLAN 1, WLAN 2, WLAN 3,…, WLAN 10), (iii) a PDG, (iv) an AAA server, (v) a S-CSCF server and (vi) a HSS/AuC. The users perform authentication requests that are aggregated to PDG through APs. The AAA server communicates with HSS/AuC to fetch (size L) fresh 3G AV (this procedure is called Authentication Vector Request (*AVR*) (see section 4.1)). Similarly, S-CSCF communicates with HSS/AuC to get (size L) fresh 3G AV. Finally, HSS/AuC generates fresh 3G AV. The aforementioned network entities have been modeled using M/M/1 queues and two types of them (i.e., the users and HSS/AuC) collect statistical information.

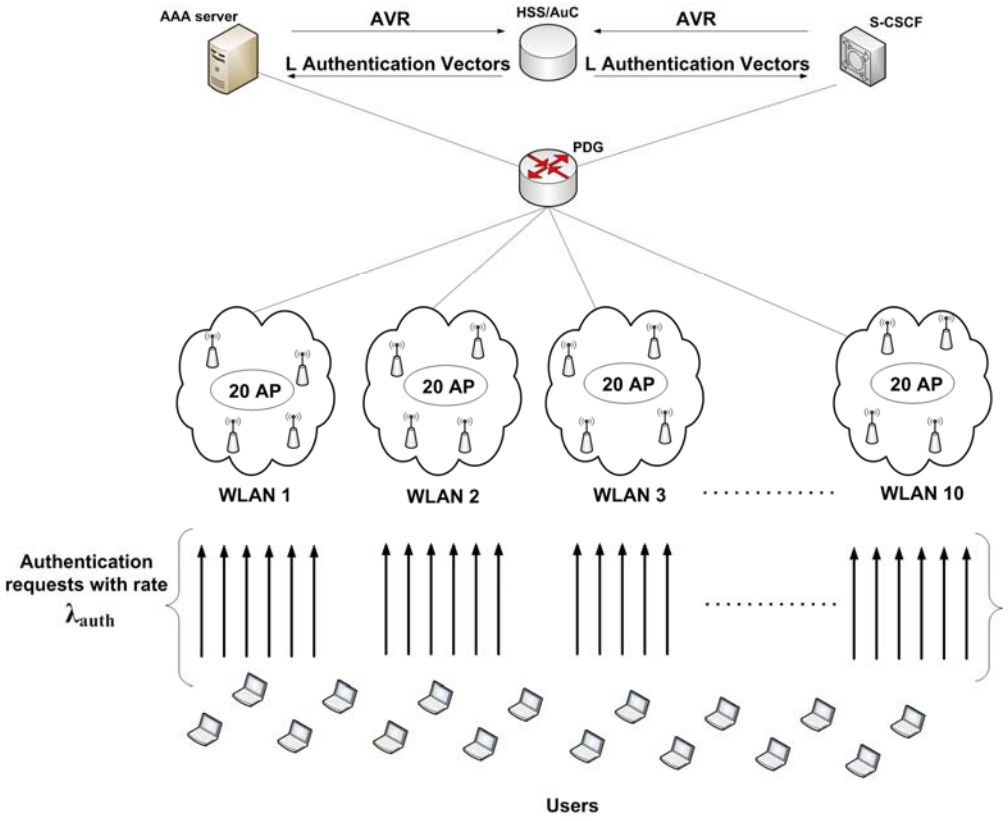

Fig. 8: Simulation model

The simulation scenario involves a WLAN deployment that covers an urban area. Real world examples of such WLAN deployments can be found in [36], [37], [38], [39]. The maximum number of users is 10000, which corresponds to the population of an urban area. The aggregated authentication requests from all the users form a Poisson process with rate λ_{auth} (see Fig. 8). The latter is used to investigate the behavior of the two procedures (i.e., improved and legacy 3G-WLAN authentications) under overloading conditions. For this reason, λ_{auth} is set initially to a very low load value (i.e., λ_{auth} = 0.5 req./sec) and it is gradually increased until the underlying network reaches its capacity limits. Another parameter of the simulation model is the size L of 3G AVs that affects significantly the overall network performance. A large value L consumes bandwidth resources in the communication link between the AAA server and HSS/AuC, since more 3G AVs are conveyed [34]. On the other hand, a small value L may increase significantly the authentication delay, since AVR procedures are more frequently performed. The 3GPP specifications do not define explicitly a specific value for L, but recommend that L=5. Therefore, in the simulation model L takes values from 1 to 20. The size of EAP-AKA, IKEv2 and SIP packets is variable and depends from the specific message being exchanged. In particular, according to the RFC specifications the size of EAP-AKA packets varies from 32 to 80 bytes [13], the size of IKEv2 varies from 82 to 338 bytes [15]

while the size of SIP packets varies from 80 to 128 bytes [19]. After a successful authentication, a user has access to VoIP services (one of the most prominent IMS services). Voice traffic has been modeled as a stream of UDP packets over IP (200 bytes length) with a constant packet inter-arrival time equal to 20ms. The bit rate of the wireless links is 54 Mbps (i.e., IEEE 802.11g [10]), and the core networks entities are connected with 100 Mbps wired links. The computational complexity and the associated processing delays of the employed encryption/decryption algorithms are taken from [26]. The duration of the carried simulations ranged between 4-16 hours, which was sufficient to provide stable results. Table 1 summarizes the simulation parameters.

Table 1: Simulation parameters

Simulation parameters	***Values***
Maximum number of users	*10000*
Aggregate authentication requests rate λ_{auth}	*Variable (initial value=0.5 req./sec)*
Size L of AV	*Variable (1,2,…,20)*
Packet size of EAP-AKA, SIP, IKEv2	*Variable (40-338 bytes)*
Data voice packet size	*200 bytes*
Data voice packet inter-arrival time	*20 ms*
Number of WLANs	*10*
Number of AP in a WLAN	*20*
Wireless link bandwidth	*54 Mbps*
Wired link bandwidth	*100 Mbps*
Simulation Time	*4-16 hours*

We have performed three sets of experiments, which are analyzed below. In the first set, the authentication delay was estimated as a function of the rate of authentication requests λ_{auth} (see Fig. 9). The size L of the 3G AV is constant and equal to 5, since it is the recommended value by the 3GPP specifications [7] (the impact of a variable L on the authentication delay is analyzed in the third experiment set). It can be deduced that for small values of the rate of authentication requests (i.e., $\lambda_{auth} < 2$), the authentication delay values are constant (see Fig. 9) for both procedures (i.e., about 0.4 seconds for the improved 3G-WLAN authentication and 1.4 seconds for the legacy). The decreased delay of the improved procedure is a direct consequence of the reduced number of authentication messages exchanged and the associated computational overhead. Moreover, it is observed that in the interval of $2 < \lambda_{auth} < 5$, the authentication delay of the legacy procedure increases exponentially, leading to excessive delay values and, eventually, to a system saturation. On the other hand, for the same values of the rate of authentication requests, the

authentication delay of the improved 3G-WLAN procedure remains constant. Only under a sufficiently high rate of authentication requests (i.e., $\lambda_{auth} > 5$), the authentication delay of the improved 3G-WLAN authentication procedure increases exponentially, indicating that the system has exceeded its maximum capacity. Therefore, it can be figured out that because of the reduced authentication delay, the improved procedure is capable of fulfilling a greater demand of authentication requests, compared to the legacy. Another benefit of the proposed procedure is that it mitigates bottlenecks in PDG. Recall that PDG is a gateway that connects RAN with the core network (see Fig. 1). Thus all the WLAN traffic is aggregated to PDG, causing bottlenecks that (i) slow down the data flow, (ii) reduce the network capacity and (iii) impede the system scalability [35]. The proposed procedure copes with bottlenecks in PDG, since it significantly reduces the total amount of authentication messages that are conveyed and processed by it. Moreover, the reduced number of messages exchanged for users' authentication in the improved procedure, optimizes the bandwidth utilization over the wireless and core network segments. This also entails a reduced computational and energy cost at the level of mobile devices, which avoid the execution of authentication functions and the associated security algorithms (i.e., encryption/decryption, computation/verification of hash values, etc.).

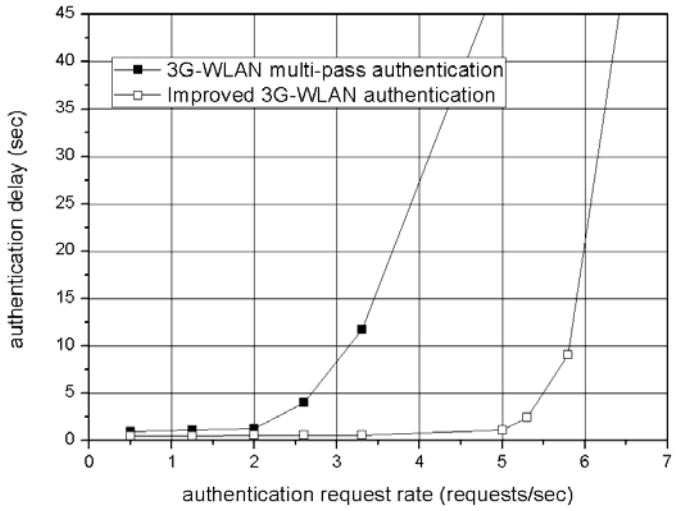

Fig. 9: Authentication delay as a function of the rate of authentication requests

The aim of the second set of experiments was to compute the ratio R_{AVR} of the *AVR* procedures in the improved 3G-WLAN authentication to those in the legacy procedure, as a function of L. In the carried experiments, the rate of authentication requests is constant (i.e., λ_{auth}=1 req./sec), since the ratio of *AVR* procedures is independent of λ_{auth}. As shown in Table 2, the ratio R_{AVR} of *AVR* procedures is constant (i.e., its value is about $R_{AVR}\approx 0.33$)

and independent of *L*. This outcome is directly linked to the fact that for each user's authentication, the legacy 3G-WLAN authentication consumes three 3G AV (one for each authentication step), while the improved consumes only one. Thus, it can be figured out that the improved 3G-WLAN authentication reduces the executions of the *AVR* procedure by 66%, compared to the legacy. It is evident that the reduced number of execution of *AVR* entails reduced authentication delays, since the AAA server and P-CSCF communicate less frequently with HSS/AuC. Moreover, the proposed procedure reduces the authentication latency of roaming users, which reside far away (in terms of number of hops) from their HSS/AuC. Recall that when an AVR procedure is performed, the AAA server or S-CSCF communicates with HSS/AuC. The latter is always located in the users' home network, since it stores the users' authentication credentials. Therefore, roaming users experience long authentication delays during an AVR procedure [24]. Thus, the proposed procedure is especially beneficial for roaming users, since it reduces the execution of AVR procedures and, consequently, the authentication latency. In addition, it mitigates the communication and processing overhead in HSS/AuC. This enables HSS/AuC to reserve resources in order to fulfill *AVR*s generated by other types of networks (e.g., UMTS, GSM, GPRS, etc.), which are also connected to the B3G network and served by the same HSS/AuC. Therefore, the improved authentication procedure optimizes the performance of the entire B3G network architecture as well as the individual networks that the latter comprises.

Table 2: Ratio R_{AVR} of the *AVR* procedures

Size of 3G AV	*Ratio* R_{AVR}
L=2	*0.32*
L=5	*0.31*
L=8	*0.31*
L=10	*0.30*
L=15	*0.29*

Finally, in the third set of experiments we have computed the authentication delay as a function of the size *L* of the 3G AVs. Observing Fig. 10, it is evident that the improved procedure achieves reduced authentication delays for all values of *L*. In case that the size *L* is relatively small, then the two authentication procedures (i.e., improved 3G-WLAN and legacy 3G-WLAN) present great differences in the delay values, meaning that the improved procedure achieves great performance improvement. Increasing the size *L*, the delay curves approximate subtly to each other, meaning reduced differences in the delay

values. Therefore, we can deduce that the improved procedure yields the best performance gain for relatively small values of *L*. Moreover, in both procedures, as *L* increases the authentication delay is reduced. This is due to the fact that as *L* increases, the execution of *AVR* is reduced, since the AAA server and P-CSCF communicate less frequently with HSS/AuC to fetch fresh 3G AV. Finally, Fig. 10 indicates that for L > 10 the authentication delay becomes almost a constant function of L. This means that for L > 10 the impact of L on the authentication latency is negligible. This outcome can be attributed to the fact that when L > 10, the AVR requests are so rare that do not affect the authentication latency.

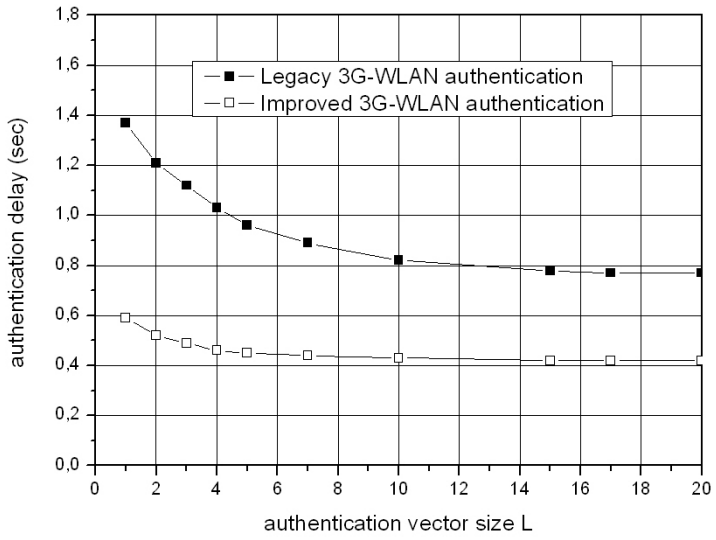

Fig. 10: Authentication delay as a function of the size *L* of the 3G Authentication Vectors

8 Conclusions

This paper has proposed a security binding mechanism, which reduces the execution of the redundant authentication functions of the legacy multi-pass authentications that are employed in B3G networks. In general, the proposed mechanism authenticates a user in the second and third step of a multi-pass authentication procedure, by using the user's authentication credentials of the initial step. The proposed mechanism is deployed through two different forms (i.e., the security identity binding and the security key binding) in order to be applied to all the B3G scenarios that that use multi-pass authentications. To prove this fact, we have selected to present and analyze the application of the proposed mechanism in two different B3G scenarios (i.e., 3G-WLAN and WiMAX), resulting in the improved authentication procedures. The improved 3G-WLAN authentication procedure uses both the security identity binding and the security key binding, while the improved WiMAX authentication uses only the security identity binding. We have performed a security

analysis to identify and elaborate on possible attacks that threaten the operation of the improved procedures, the users and the underlying network. We examined the feasibility of these attacks and, if required, we proposed security measures to defeat them. We concluded that the proposed procedures retain the same security level with the legacy procedures. In addition, we have performed simulations to estimate and compare the performance of the improved 3G-WLAN authentication to that of the legacy 3G-WLAN authentication. The simulation results indicated that the improved procedure achieves reduced authentication delays compared to the legacy procedure, as a direct consequence of the reduced number of authentication messages exchanged and the associated computational overhead. Because of the reduced authentication delays, the improved procedure is capable of fulfilling a greater demand of authentication requests, compared to the legacy. Moreover, the reduced number of messages exchanged for users' authentication, optimizes the bandwidth utilization over the wireless and core network segments. This also entails a reduced computational and energy cost at the level of mobile devices. Finally, the improved 3G-WLAN authentication reduces the executions of the *AVR* procedure (i.e., about 66%) that optimizes the performance of the entire B3G network architecture as well as the individual networks that the latter comprises.

9 References

[1] 3GPP TS 23.234 (v8.0.0), "*3GPP system to WLAN Interworking; System description*", Release 8, 2008.

[2] 3GPP TS 33.234 (v8.1.0), "*3G security; WLAN interworking security*", Release 8, 2008.

[3] 3GPP TS 43.318 (v8.3.0), "*Generic Access Network (GAN); Stage 2*", Release 8, 2008.

[4] 3GPP TS 23.228 (v8.7.0), "*IP Multimedia Subsystem; Stage 2*", Release 8, 2008.

[5] 3GPP TS 33.203 (v8.5.0), "*3G security; Access security for IP based services*", Release 8, 2008.

[6] 3GPP TS 33.102 (v.8.1.0), "*3G Security; Security architecture*", Release 8, 2008.

[7] 3GPP TS 29.002 (v. 8.8.1), "*Mobile Application Part (MAP) specification*", Release 8, 2008.

[8] IEEE 802.16e, "*Air Interface for Fixed and Mobile Broadband Wireless Access Systems",* 2005.

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

[10] IEEE Std 802.11g, *"Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4GHz Band*", 2003.

[11] B. Aboba, et. al., "*Extensible Authentication Protocol (EAP)*", RFC 3748, Jun 2004.

[12] H. Krawczyk, M. Bellare, R. Canetti, "*HMAC: Keyed-Hashing for Message Authentication",* RFC 2104, Feb 1997.

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

[14] H. Haverinen, J. Salowey, "*Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*", RFC 4186, Jan 2006.

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

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

[17] S. Kent, R. Atkinson, "*Security Architecture for Internet Protocol*", RFC 2401, Nov. 1998
[18] S. Kent, R. Atkinson, "*IP Encapsulating Security Payload (ESP)*", RFC 2406, Nov. 1998
[19] J. Rosenberg, "*SIP: Session Initiation Protocol*", RFC 3261, Jun 2002
[20] D. Simon, B. Aboba, R. Hurst, "*The EAP TLS Authentication Protocol*", RFC 5216, Mar. 2008
[21] P. Funk, S. Blake-Wilson, *"Extensible Authentication Protocol Tunneled Transport Layer Security (EAP-TTLSv0)*", RFC 5281, Aug 2008
[22] C. Laat, et. al., "*Generic AAA Architecture*", RFC 2903, Aug. 2000.
[23] 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.
[24] 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.
[25] C. Xenakis, C. Ntantogian, "*Security Architectures for B3G Mobile Networks*", Telecommunication Systems, Springer, Vol. 35, No 3-4, pp. 123-139, Aug. 2007.
[26] C. Xenakis, N. Laoutaris, L. Merakos, I. Stavrakakis, "*A Generic Characterization of the Overheads Imposed by IPsec and Associated Cryptographic Algorithms*", Computer Networks, Elsevier Science, Vol. 50, No. 17, pp. 3225-3241, Dec 2006.
[27] C.M. Huang, J.W. Li, "*One-Pass Authentication and Key Agreement Procedure in IP Multimedia Subsystem for UMTS*", IEEE 21st International Conference on Advanced Networking and Applications (AINA'07), Niagara Falls, Canada, May 2007
[28] C. Ntantogian, C. Xenakis, "*Reducing Authentication Traffic in 3G-WLAN Integrated Networks*", IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC), Athens, Greece, Sep 2007.
[29] L. Veltri, S. Salsano, G. Martiniello, "*Wireless LAN-3G Integration:Unified Mechanisms for Secure Authentication based on SIP*", IEEE, International Conference on Communications, (ICC), Istanbul, Turkey, Jun. 2006
[30] D. Celentano, A. Fresa, M. Longo, A.L. Robustelli, "*Improved Authentication for IMS Registration in 3G/WLAN Interworking*", IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, (PIMRC), Athens, Greece, Sep 2007.
[31] The Network Simulator NS-2, http://nsnam.isi.edu/nsnam/index.php/User_Information
[32] C. Ntantogian, C. Xenakis, I. Stavrakakis, "*Reducing the User Authentication Cost in Next Generation Networks*", 5th Annual Conference on Wireless On demand Network Systems and Services (WONS 2008), Garmisch-Partenkirchen, Germany, Jan 2008.
[33] WiMAX Forum Network Architecture Stages 2 and 3 - Release 1, http://www.wimaxforum.org
[34] Yi-Bing Lin, Yuan-Kai Chen, "*Reducing Authentication Signaling Traffic in Third-Generation Mobile Network*", IEEE Transactions on Wireless Communications, Vol.: 2, No 3, pp:493- 501: May 2003.
[35] Sung-Min Oh, Jae-Hyun Kim, You-Sun Hwang, Hye-Yeon Kwon, and Ae-Soon Park, "*End-to-End QoS Guaranteed Service in WLAN and 3GPP Interworking Network*", 9th Asia-Pacific Network Operations and Management Symposium (APNOMS 2006), Busan, Korea, Sept. 2006.
[36] Goggle Wifi, http://wifi.google.com/
[37] e-trikala, First Digital City in Greece, http://e-trikala.gr
[38] Panoulou, http://www.panoulu.net/ap/index.php?lang=en#hailuoto
[39] T. Ojala, T. Hakanen, T. Mäkinen and V. Rivinoja, "*Usage analysis of a large public wireless LAN,* International Conference on Wireless Networks, Communications and Mobile Computing, Maui, Jun. 2005.