Enhanced Authentication for WLAN-EPS Interworking Systems

R. Bassoli, H. Marques, J. Rodriguez, C. Gruet and R. Tafazolli

This letter proposes novel authentication procedures [1] for WLAN-EPS interworking systems for 3GPP TS 33.402 (Release 12 - September 2014) standard. The novel solutions mainly exploit public-key fully homomorphic encryption (FHE) schemes and one-way functions. That not only mitigates potential security threats, but significantly reduces the authentication load of the standard, especially in case of 3GPP-IP access.

Introduction: In 2014, 3GPP published its standard [2] to provide secure solutions for WLAN-EPS (evolved packet systems) interworking: the main scope of this standard is to allow 3GPP user equipments (UEs) to securely authenticate when they want to access to the internet via non-3GPP access points (APs): in this case, they are named WLAN UEs.

The 3GPP standard defines two possible ways for WLAN UEs to access to the internet via WLAN APs: Direct IP access (Fig. 1(a)) and 3GPP-IP access (Fig. 1(b)). The first scheme is used when WLAN APs belong to 3GPP operator's network (*trusted*), while the second scheme is used when WLAN APs do not belong to 3GPP operator's network (*untrusted*).

Direct IP access procedure (Fig. 2(a)) starts with the EAP-AKA and, if the EAP-AKA authentication of WLAN UE fails, the server begins the EAP-AKA′ procedure [3, 4]. Especially, the EAP-AKA′ avoids the issue of 'lying authenticators'. The communication between WLAN AP and AAA server encapsulates messages in the DIAMETER protocol [3]. If the WLAN UE does not support EAP-AKA′ an error occurs, and the server leaves the procedure. The AAA server starts the EAP-AKA′ challenge, which permits the mutual authentication of the three entities involved. Moreover, this challenge includes the derivation of the keys that will be used in the rest of the communication.

3GPP-IP access procedure (Fig. 2(b)) uses EAP-AKA over IKEv2 since WLAN AP is untrusted [3, 4]. The authentication procedure starts with the negotiation of cryptographic algorithms between the UE and the ePDG, and with Diffie-Hellman exchange. Next, the EAP-AKA challenge is performed. The WLAN UE and the AAA server authenticate each others at the end of both EAP-AKA and IKEv2 procedures. If IP mobility is required, there are optional messages inside the EAP-AKA protocol, which can allow the selection of an IP mobility scheme. The keys that are generated at the end of the challenge permit to derive the keys for the communication and the set-up of the IPsec tunnel (Fig. 2(b)).

Problems and motivation: The two authentication procedures described above present some issues [3, 4]. An analysis of the Direct IP access scheme firstly reveals that an attacker can passively eavesdrop user identity at the beginning of the EAP-AKA protocol, and can track user position. Proposed solutions to that consist in IMSI (International Mobile Subscriber Identity) protection via public key encryption and one-way functions. These solutions increase security, that is paid by higher authentication load of the protocol. In Direct IP access, other possible attacks are the passive eavesdropping of user credentials to access services, and the known-plaintext attack: in particular, the latter happens because EAP implementations rely on clear-text authentication using RADIUS. Moreover, the attacker may use samples of both plaintext and its encrypted version to reveal further secret information. Finally, a man-in-the-middle attack is also possible: as IMSI is plaintext at the first connection, an attacker can see it and modify it.

The study of 3GPP-IP access scheme also reveals some weaknesses. From security point of view, a roaming problem can raise: the IMSI is visible to ePDG, which in roaming situations may be in the visited public land mobile network. This problem is significant if the home network operator does not trust the ePDG of the visited network operator. However, the main issue of this procedure is the high authentication load: this is due to two authentication protocols, EAP-AKA and IKEv2.

Proposed Direct IP Access Scheme: Fig. 3 depicts the proposed authentication method for Direct IP access scenarios. The additions in the encrypted domain are considered at the bit level (XORs), and are possible because of the deployment of FHE schemes [5]. WLAN UE owns the secret key K, its IMSI and the public key pk_{AAA}. The WLAN AP owns a $WLAN\ ID$, encrypted with public key pk_{AAA}. The AAA server knows all these parameters and the secret key sk_{AAA} to decrypt the messages previously encrypted with pk_{AAA}. $\mathrm{E}[\bullet]_{pk}$ and $\mathrm{D}[\bullet]_{sk}$ respectively identifies the encryption and decryption.

The procedure starts with the establishment of the wireless link between the WLAN UE and the WLAN AP. Next, the WLAN AP sends a message, containing its encrypted $WLAN\ ID$, to the AAA server to start the authentication (Fig. 3).

[Step (I)]. The AAA server gets $WLAN\ ID = \mathrm{D}\left[\mathrm{E}[WLAN\ ID]_{pk_{AAA}}\right]_{sk_{AAA}}$ and generates a random number ($RAND$) to perform

$$\mathrm{E}[WLAN\ ID \oplus RAND]_{pk_{AAA}} = X. \tag{1}$$

[Step (II)]. Thanks to the FHE schemes [5], from (1), the WLAN AP calculates

$$X \oplus \mathrm{E}[WLAN\ ID]_{pk_{AAA}} = \mathrm{E}[RAND]_{pk_{AAA}}. \tag{2}$$

This calculation helps the AAA server to verify the identity of the WLAN AP at Step (IV) (it avoids the 'lying authenticator' problem).

[Step (III)]. The WLAN UE encrypts its IMSI with pk_{AAA} and calculates

$$\mathrm{E}[RAND]_{pk_{AAA}} \oplus \mathrm{E}[IMSI]_{pk_{AAA}} = Z. \tag{3}$$

Moreover, it calculates message authentication code (MAC) by using the cryptographic hash function $\mathrm{H}_k(\bullet)$ in combination with the secret key K:

$$MAC_{UE} = \mathrm{H}_K(Z). \tag{4}$$

[Step (IV)]. The AAA server calculates

$$Z \oplus \mathrm{E}[RAND]_{pk_{AAA}} = \mathrm{E}[IMSI]_{pk_{AAA}} \tag{5}$$

$$IMSI = \mathrm{D}\left[\mathrm{E}[IMSI]_{pk_{AAA}}\right]_{sk_{AAA}} \tag{6}$$

hence, it authenticates the WLAN UE. In parallel, the identity of the WLAN UE is also checked by comparing $MAC_{AAA} = \mathrm{H}_K(Z)$ with the received MAC_{UE}. If the two values are equal, the WLAN UE is fully authenticated. So, the authentication procedure ends.

[Step (V)]. Now the AAA server generates the two main keys CK and IK for the communication. The keys are generated with the operator number OP as

$$CK||IK = \mathrm{H}_K(\mathrm{E}[OP]_{pk_{AAA}}, RAND) \tag{7}$$

[Step (VI)]. The WLAN UE performs $OP_{H\_AAA} = \mathrm{H}_K(\mathrm{E}[OP]_{pk_{AAA}})$ to verify the integrity of $\mathrm{E}[OP]_{pk_{AAA}}$. If successful, it calculates (7).

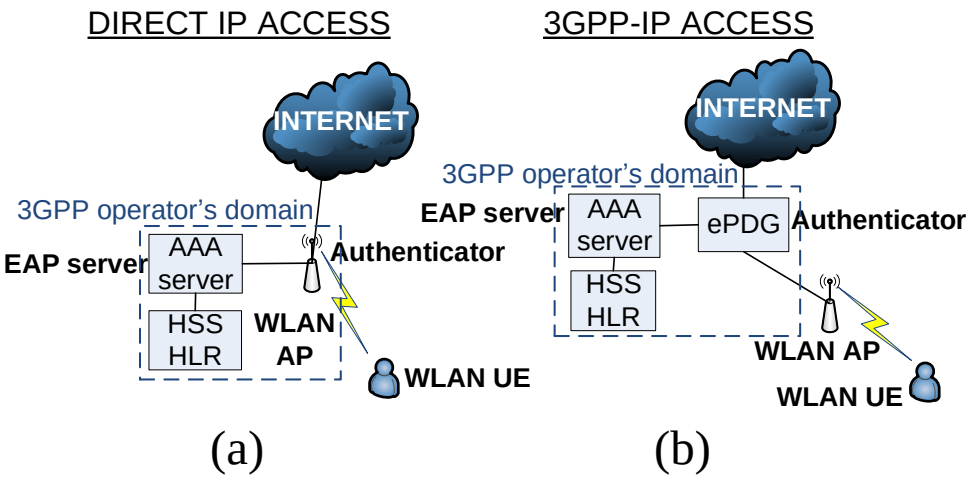

Fig. 1 (a) *Direct IP access scenario* (b) *3GPP-IP access scenario*

The scenarios include HSS-HLR (Home Subscriber Server - Home Location Register), which contain users' subscription data. They are usually placed in the AAA (authentication, authorization and accounting) server. Next, the ePDG (Evolved Packet Data Gateway) is the authenticator in 3GPP-IP access

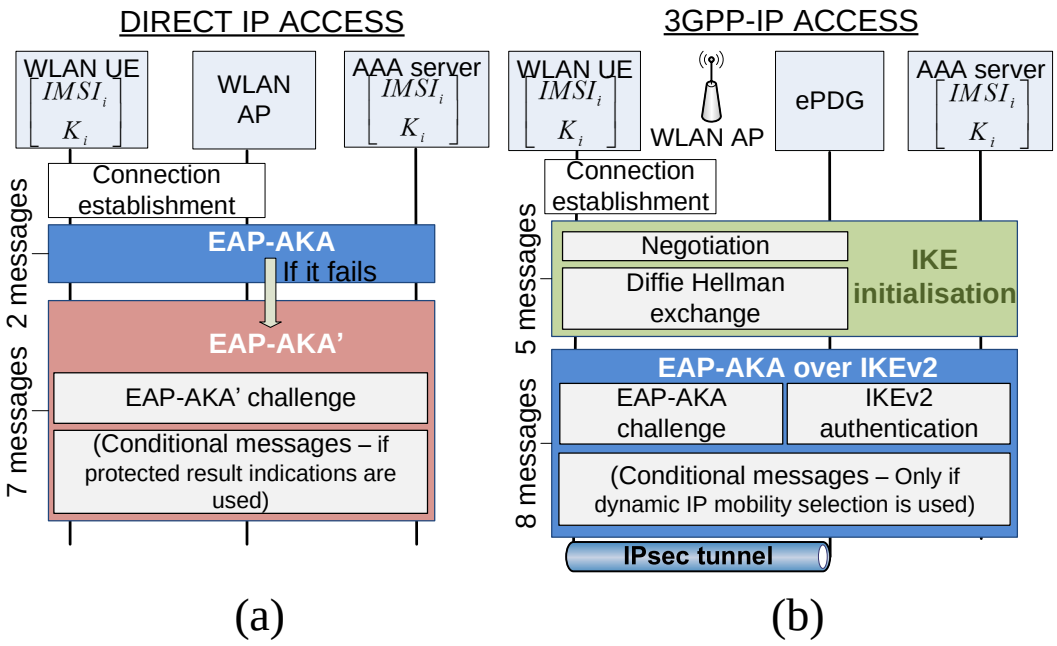

Fig. 2 (a) *Direct IP access procedure* (b) *3GPP-IP access procedure*

Direct IP access supports either EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement) or EAP-AKA′. 3GPP-IP access uses EAP-AKA over IKEv2 (Internet Key Exchange) protocol. Confidentiality (CK) and integrity (IK) keys are generated at the end of the protocols. All the other keys are derived from those ones. The number of messages show the authentication load on the wireless link

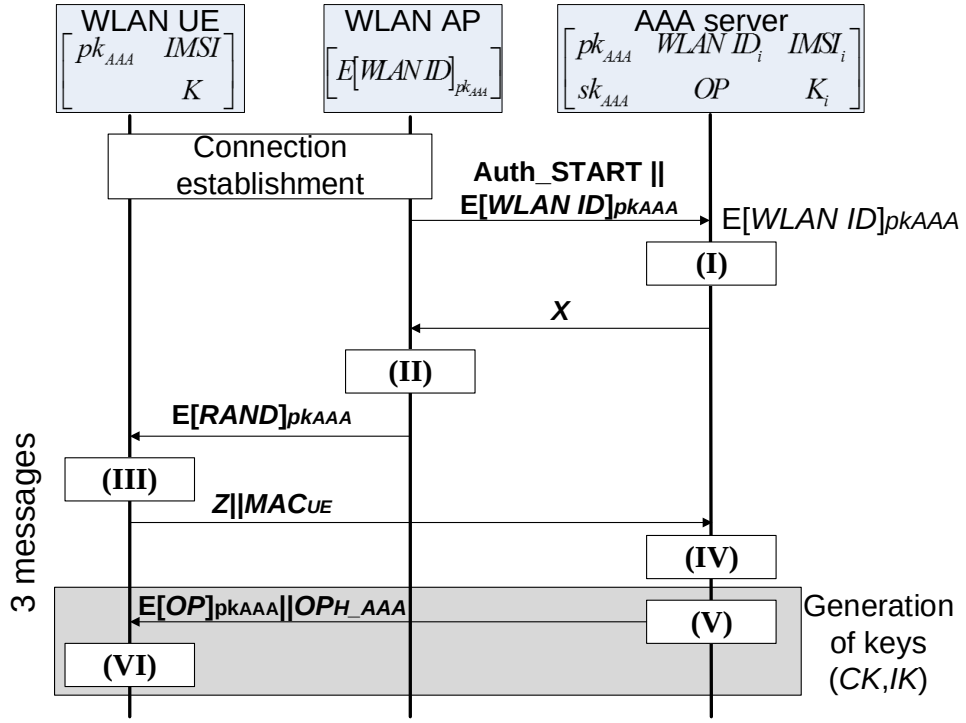

Fig. 3 *New Direct IP access procedure*

$WLAN\ ID$ uniquely identifies a WLAN AP. The operator number (OP) identifies a network operator and is kept secure by encryption. $A||B$ is the concatenation of A and B. The number of messages show the authentication load on the wireless link

Proposed 3GPP-IP Access Scheme: Fig. 4 shows the novel authentication procedure for 3GPP-IP access scenarios. The structure is similar to the one explained in the previous section: this time the role of authenticator is performed by the ePDG instead of by the WLAN AP.

The procedure begins with the establishment of the wireless link between the WLAN UE and the WLAN AP. Next, the WLAN AP sends an authentication start message to the ePDG, that appends its ID, and forwards this to the AAA server. Hence, the server knows the identity of the ePDG and authenticates it. The authentication of the ePDG is important when the UE is in roaming and the home operator does not trust in it.

[Step (I)]. The ePDG calculates

$$\mathrm{E}[ePDG\,ID \oplus RAND]_{pk_{AAA}} = X \tag{8}$$

[Step (II)]. The WLAN UE obtains $RAND$ and performs

$$X \oplus \mathrm{E}[IMSI]_{pk_{AAA}} = Y \tag{9}$$

$$MAC_{UE} = \mathrm{H}_K(Y). \tag{10}$$

$RAND$ is also used in the generation of CK and IK.

[Step (III)]. The AAA server checks if $MAC_{UE} = MAC_{AAA} = \mathrm{H}_K(Y)$. If successful, it authenticates the WLAN UE from (9), with the following operations:

$$Y \oplus \mathrm{E}[ePDG\,ID \oplus RAND]_{pk_{AAA}} = \mathrm{E}[IMSI]_{pk_{AAA}} \tag{11}$$

$$IMSI = \mathrm{D}\left[\mathrm{E}[IMSI]_{pk_{AAA}}\right]_{sk_{AAA}}. \tag{12}$$

(9) and (11) are operations in the encrypted domain by applying FHE schemes.

Finally, the mechanism generates CK and IK as previously in (7). Nevertheless, this time the further step is the set-up of an IPsec tunnel between the WLAN UE and the ePDG. The keys to generate the IPsec tunnel are derived from CK and IK at both the WLAN UE and the AAA server, as the 3GPP standard describes. Then, the AAA server sends them to the ePDG for secure channel set-up.

Conclusion: The proposed novel procedures provide efficient authentication for both Direct IP access and 3GPP-IP access. These procedures remain compatible with the 3GPP standard [2] while mitigating the security threats previously underlined. In parallel, they significantly reduce the authentication load of the standard, especially in case of 3GPP-IP access. In fact, the proposed authentication mechanisms use three messages on the wireless link instead of nine (Direct IP access) and thirteen (3GPP-IP access).

The improvements are mainly possible due to the use of public-key FHE schemes and hash functions. The performed operations in the encrypted domain are only XORs, so to keep complexity low. Moreover, decryption is only performed at the AAA server, which does not have computational constraints and limited battery life as the UE. MAC size can be chosen according to the needs (i.e optimising the overhead).

New approach to generate CK and IK has also been presented. This approach ensures the protection of OP, since it is computed off the UE, and is kept confidential by public encryption. New 3GPP-recommended parameters for authentication are introduced: first, $WLAN\ ID$ is a value that uniquely identifies each AP belonging to the operator (in Direct IP scenarios). This identity for the AP compares directly to the IMSI address for the UE: it is not disclosed to the UE, and is protected against attacks by encryption. In fact, at the AP, the encrypted version is stored in order not to be cracked. Furthermore, $ePDG\,ID$ represents the unique identifier of an ePDG (in 3GPP-IP scenarios). In fact, the way of using this in the invention opens up new opportunities for solving the roaming problems of the 3GPP standard.

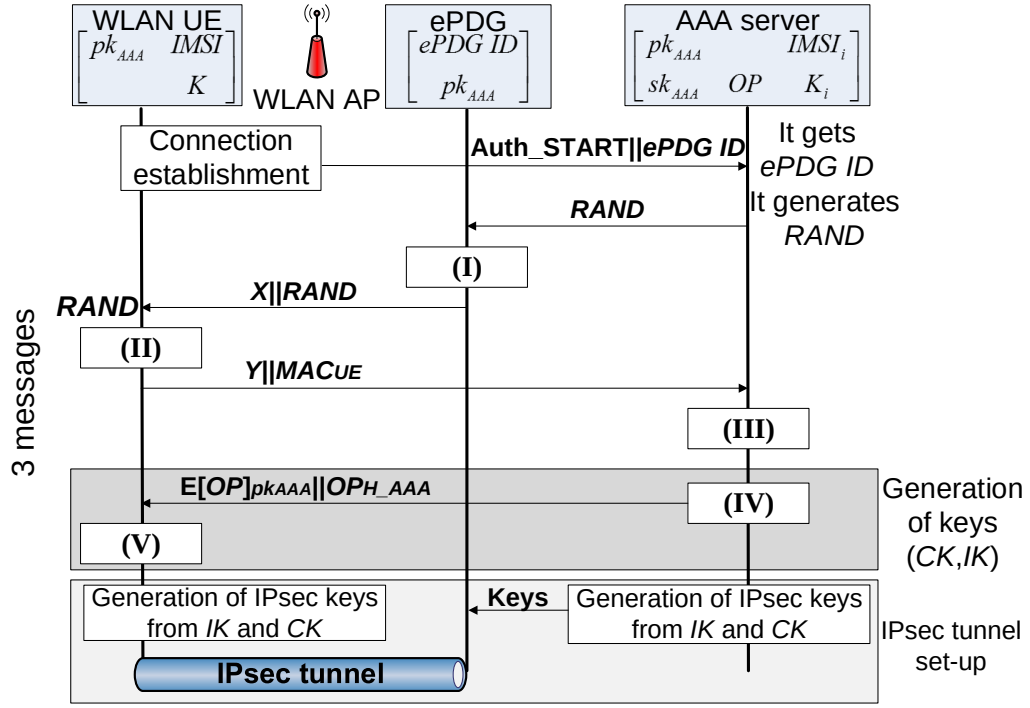

Fig. 4. New 3GPP-IP access procedure $ePDG\ ID$ uniquely identifies an ePDG. The number of messages show the authentication load on the wireless link

Acknowledgment: This work has been supported by the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement 264759 (GREENET).

R. Bassoli and H. Marques (*Instituto de Telecomunicações, Aveiro, Portugal, and Institute for Communication Systems, University of Surrey, UK*)
J. Rodriguez (*Instituto de Telecomunicações, Aveiro, Portugal*)
C. Gruet (*Airbus Defence and Space, Elancourt, France*)
R. Tafazolli (*Institute for Communication Systems, University of Surrey, UK*)

E-mail: bassoli@av.it.pt

References

1 R. Bassoli, H. Marques, J. Rodriguez, C. Gruet: 'A Novel Authentication Procedure for WLAN-EPS Interworking Systems', Portuguese Patent Application 20141000082396, 2014
2 3GPP: '3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses', 2014
3 D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi: 'LTE Security', (John Wiley and Sons, Ltd., 2010)
4 M. Olsson, S. Sultana, S. Rommer, L. Frid, and C. Mulligan: 'SAE and the evolved packet core', (Academic Press, 2009)
5 C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, and R. Sirdey: 'Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain', IEEE Signal Processing Magazine, 2013, **30**, (2), pp. 108-117