Research Journal of Applied Sciences, Engineering and Technology 7(2): 329-342, 2014
DOI:10.19026/rjaset.7.259
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: April 12, 2013 Accepted: April 22, 2013 Published: January 10, 2014

Research Article

A New Authentication Method for Vertical and Horizontal Handover in 3G-WLAN Interworking Architecture

Younes El Hajjaji El Idrissi, Noureddine Zahid and Mohamed Jedra
Faculty of Science, Laboratory of Conception and System, University Mohammed V-Agdal, Avenue Ibn Batouta, B.P. 1014, Rabat, Morocco

Abstract: The interworking of the 3G and the WLAN technique provides a perfect connectivity solution in terms of data rate, service cost and area coverage. However the Vertical Handover (VH) from the 3G to WLAN and the Horizontal Handover (HH) between WLAN domains present an additional security challenge. The V/H handover must be fast and secure without impacting the security in both networks. Several authentication methods have been proposed to secure the VH and HH. The Extensible Authentication Protocol Key Agreement (EAP-AKA) is the authentication protocol adopted by the 3rd Generation Partnership Project (3GPP) to authenticate User Equipment by the 3G Home Networks. The EAP-AKA protocol suffers from several weaknesses, such as user identity display and high authentication delay. In this study we propose a new simplify authentication method and key agreement for vertical and horizontal handovers based on the existed method EAP-AKA. Performances analysis of the proposed method show superior results in comparison to the existing EAP-AKA method in terms of bandwidth consumption, signaling cost and authentication delay. The security property of the new method is verified by using the formal security analyzer Automated Validation of Internet Security Protocols and Applications (AVISPA) which has a high talent in finding potential attacks automatically in security protocols.

Keywords: 3G-WLAN, authentication, EAP-AKA, ECC, horizontal and vertical handover

INTRODUCTION

The user authentication and accounting are the most important features in the network management (Rigney and Willens, 2000). All other services depend on it and no provider service can be used without a legal user authentication. The 3G mobile communication system is developed by the 3GPP for secure and high bandwidth communication. The architecture of 3G network defines a new mechanism to interwork the 3G with the WLAN networks (3GPP, 2008). The 3G network can use the WLAN technology as an access network and benefits of the low cost implementation and the high bandwidth connectivity. One of the big challenges for this interworking is to keep the high security level for different services. In 3G-WLAN architecture, the User Equipment (UE) connected to WLAN is authenticated firstly by the 3G home network (3GHN). This is due to the presence of the user information only in the 3G authentications servers (3GPP, 2004). The UE must be authenticated by the Home Subscriber Server (HSS), Home Location Registry (HLR) and Home Authentication Authorization and Accounting (HAAA). The 3G-WLAN architecture defines two types of handovers, vertical and horizontal handover. A vertical handover is a handover between heterogeneous networks, such as, the handover between 3G and WLAN Access Point (AP). A horizontal handover is a handover between 2 points in the same network technology (Shi *et al*., 2004).

The 3GPP architecture recommends using EAP-AKA to secure the 3G-WLAN inter-working and to authenticate UE attached to a WLAN (Arkko and Haverinen, 2006). The EAP-AKA method suffers from several weaknesses such as, UE identity disclosing, SQN synchronization and high authentication delay. In addition the EAP-AKA doesn't offer an implicit authentication mechanism to manage the UE horizontal handover between WLAN domains. The WLAN must always authenticate the UE on behalf of the 3GHN (Matsunaga *et al*., 2003). These have a negative impact on the handover delay, constraint the user mobility and decrease the Quality of Service (QOS).

In this study we propose a new authentication method to simplify the UE mobility in 3G-WLAN architecture. Our authentication method reduces the authentication steps, doesn't require any change to the existed 3G-WLAN architecture, match with the 3GPP recommendation and doesn't require any public infrastructure. The proposed protocol requires one round of full authentication between the local WAAA server and the 3GHN authentication server. Also we propose a

Corresponding Author: Younes El Hajjaji El Idrissi, Faculty of Science, Laboratory of Conception and System, University Mohammed V-Agdal, Avenue Ibn Batouta, B.P. 1014, Rabat, Morocco

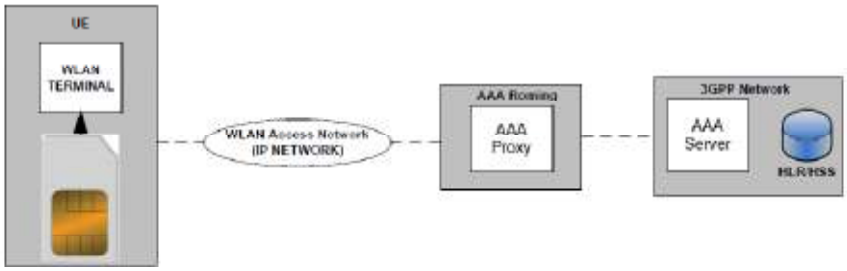


Fig. 1: Architecture of inter-working WLAN-3GPP

new key framework which permits to authenticate the UE locally by the WAAA during the horizontal handover. In addition this method reduces the authentication delay and the number of authentication keys, achieves mutual authentication and protects the user identity.

EAP-AKA AUTHENTICATION METHOD

Generally the UE makes a general scan in a specific frequency and searches a beacon packet with SSID. When a beacon is detected, the service SSID checker is started and compares the received SSID with the saved one. In positive check, both parties perform the authentication and the association procedures. It is likely that the WLAN reuse the 3GPP USIM authentication method. The Fig. 1 shows the 3G-WLAN interworking architecture.

Extensible Authentication Protocol (EAP) is an authentication protocol defined by the IETF (Internet Engineering Task Force) (Aboba *et al*., 2004). The success of the EAP is the distinction between the EAP protocol and the used EAP methods. The principal function of the EAP protocol is the protection of the confidential data (login, password, certificate, etc.) used in the authentication operation. The EAP method takes in charge the authentication process and the generation of the session keys. The protocol EAP is not attached to a particular EAP authentication method. This flexibility gives an important advantage to the EAP protocol face to the other authentication protocol, because in case of security fail, we change only the authentication method without changing all the protocol.

EAP-AKA is the authentication technique adopted by the 3GPP for the 3G-WLAN architecture. It is based on challenge-response mechanisms and a pre-shared secret key K between the UE and the HSS. The EAP-AKA provides a mutual authentication, generation of cipher and integrity keys (Arkko and Haverinen, 2006). It can be divided in two types of authentication. EAP-AKA full authentication is invoked the first time user equipment is attached to a wireless network. EAP-AKA fast re-authentication mechanism is executed in 3G-WLAN handover or when a UE is attached to a new AP. The UE re-authentication is done by the HAAA based on the previously received AV from the HLR/HSS and on the number of re-authentications allowed time.

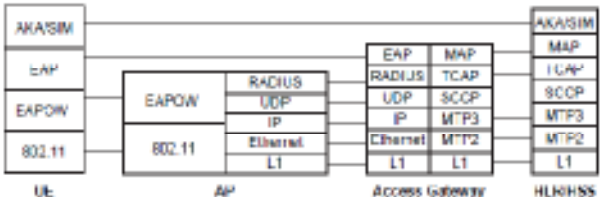


Fig. 2: 3G-WLAN authentication protocol architecture

All the authentication operation is handled by the UE and the 3GHN. The WLAN uses 802.11 and RADIUS protocols to forward the authentication packets between the UE and the authentication server HAAA in 3GHN. Integrating 3G and WLAN networks requires authentication of UE to the 3G service when it enters a WLAN for the purpose of registration, accounting and generation keys (3GPP, 2006). The authentication protocols architecture is shown in Fig. 2.

The authentication procedure shown in Fig. 3 is based on the deployment of EAP with 802.11. The authentication process starts after UE association with an AP. In the first step, The UE sends an EAPOL (EAP over LAN) message to start the initiation of 802.1X authentication. In steps 2 the AP requests the UE identity and in step 3 the identity of the UE (IMSI stored in the USIM card) is obtained with EAP response messages from the UE. After receiving the UE identity the WAAA initiates a RADIUS dialog with 3GHN authentication server HAAA and forwards the Access-request message that contains the identity reported by the UE (step 4). The HAAA uses the received UE identity to obtain the address of the HLR/HSS that contains subscription information. In steps 5, the HAAA retrieves a number of authentication vectors from the HLR/HSS. The AV is generated by using a total of 10 functions to perform the entire necessary feature (3GPP, 2005). Each AV is composed by a Random Number (RAND), an Expected Response (XRES), a Cipher Key (CK), an Integrity Key (IK) and an Authentication Token (AUTN). The AUTN token is composed by a sequential number SQN, Authentication Management Field (AMF) and an integrity check value MAC. Each AV is valid only for one authentication operation. In steps 6 and 7 the HAAA challenges the UE through the WAAA by sending an authentication request to the UE with the RAND number and the AUTN token. By using the pre-shared key K, the received SQN, RAND and the authentication algorithm

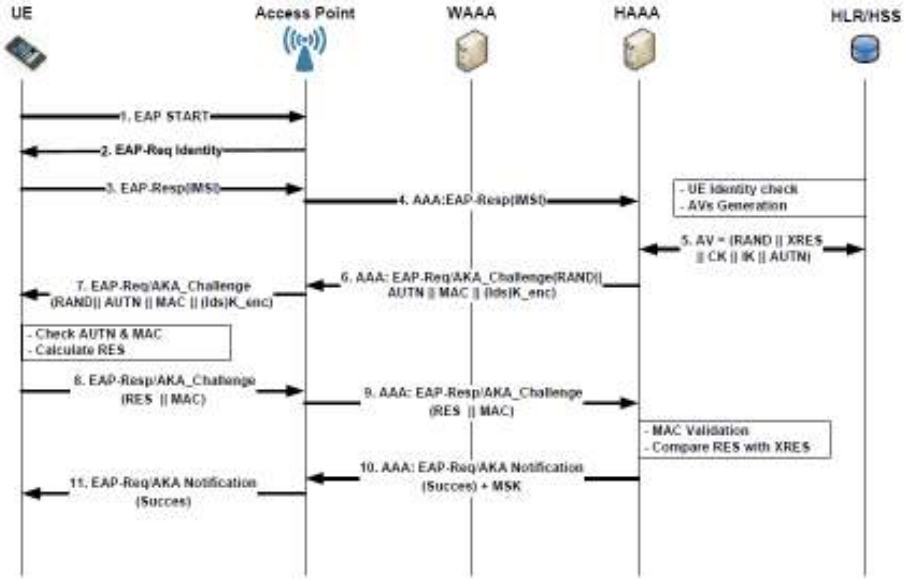


Fig. 3: EAP- AKA authentication protocol

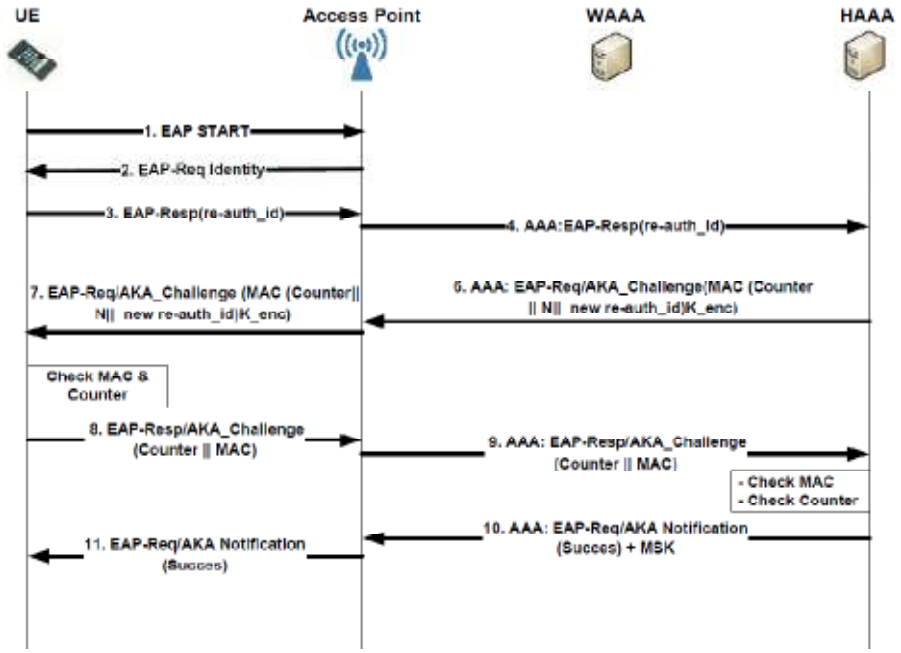


Fig. 4: EAP- AKA Re-authentication protocol

implemented in the USIM card, the UE checks the received AUTN and MAC. If they are accepted the UE calculates a response RES (RES = f2(K, RAND)) and sends RES to HAAA in steps 8 and 9. The HAAA checks the RES with the expected one XRES (already received from the HLR/HSS). In success authentication a RADIUS Access-Accept request is generated in step 11. Otherwise a RADIUS Access Reject is generated. The UE and HAAA generate a Master Session Key (MSK) and a Transient Session Key (TSK) to be used to secure communication between the UE an associated Access Point (AP) (IEEE, 2004).

EAP-AKA supports a fast re-authentication mechanism invoked in the case of 3G-WLAN HH (Arkko and Haverinen, 2006). The UE re-authentication is done by the HAAA based on the previous received AV from the HLR/HSS and on the number of re-authentication allowed by the service provider. The Fig. 4 presents the EAP-AKA re-authentication schema.

Some types of attacks benefit of the full/fast EAP-AKA authentication drawbacks, such as UE identity disclosing, SQN synchronization and high re-authentication delays. These weaknesses are due to the necessity of transmitting the UE identity in clear text to

the HAAAA and to multiple exchanged messages between the UE and 3GHN. To cover the user identity issue, the 3GPP proposed to use two temporary identities. Pseudonym ID used in full re-authentication and re-authentication ID used in fast re-authentication process (3GPP, 2006). This solution needs to handle 3 identities by UE which include an additional management's complicity and authentication delay. The fast re-authentication raises less operation numbers than the full EAP authentication. The experimentation done in Kwon *et al*. (2006) shows that the fast re-authentication can reduce the full authentication delay by 46%. However the EAP-AKA fast re-authentication method still suffers from some additional delays. This is due essentially to the fact that the HAAA is constantly busy by answering authentication requests from other UE. All these weaknesses impact the application running in the UE and have a negative impact on the Quality of Service (QOS).

The IEEE recommends using the EAP-TLS as an authentication method for UE handover in WLAN architecture. Unlike IEEE, the 3GPP recommends using the EAP-AKA in horizontal handover for 3G-WLAN architecture. A Number of solutions are proposed to bypass this divergence. Long and all (Long *et al*., 2004) propose to use a public key cryptography to authenticate the UE by the home network in interworking architecture similar to 3G-WLAN. Lee *et al*. (2005) propose to modify the 3G-WLAN interworking architecture to perform a location aware handover. This proposal protocol predicts the UE movement and performs a fast authentication during the handover. Lim *et al*. (2009) propose to modify the role of the AP by playing some UMTS base station functionalities. This solution needs to change the 3G-WLAN interworking architecture. The proposed solution in Kambourakis *et al*. (2004) proposes to change the EAP-AKA method to reduce the re-authentication delay. This protocol can modify the 3G-WLAN architecture. Another authentication method EAP-SKE is proposed in Salgarelli *et al*. (2003). This method is based on a pre-shared key between the UE and wireless and needs one round of exchanged message between the WAAA and the HAAA, but doesn't solve the UE identity problem. Others solutions are propose to reduce the HH delays inside the WLAN architecture. For example, the proposed protocol in Hur *et al*. (2007) proposes to predict the target AP by using the neighbor graphs performs a key distribution and using the EAP-TLS as authentication method. The authentication protocol in Pack and Choi (2002) proposes to predict the UE mobility and pre-authenticates the UE by the target AP before the HH. All these authentication protocols need to change the 3G-WLAN architecture, increase the authentication delay and introduce unnecessary distribution of authentication keys. In the next section we propose a new authentication method which reduces the authentication delay and provides a secure vertical and horizontal handover.

PROPOSED AUTHENTICATION METHOD

A seamless handover is needed to enable the integration of heterogeneous networks technologies into common system architecture. In this section, we present a new authentication method to secure the vertical handoff from 3G to WLAN network and the horizontal handover inside the WLAN or between WLAN domains. The proposed approach eliminates the need of communication between the target WLAN network and 3GHN to verify the UE identity during V/H handover process. Our method is based on the preparation of authentication keys by using the Elliptic Curve Cryptosystem (ECC). And involves a sequence of messages exchanged at the beginning between the UE, the target network (TWLAN) and the 3GHN. The proposed method offers a mutual authentication mechanism and guaranty the confidentiality of data by using a hybrid cipher cryptosystem.

The ECC security is based on the hardness of Elliptic Curve Discrete Logarithm Problem (ECDLP). The ECC offers a better performance compared with other public-key cryptosystems, it can attain the same security level with a smaller key size. The elliptic curve equation is defined as the form of Ep (a, b): $y^2 = x^3 + ax + b \pmod q$ with the order n over Fq, where a, b ε Fq, q> 3 and $4a^3 + 27b^2 \neq 0 \bmod p$; (Hankerson *et al*., 2004). Given an integer x ε F^*_q and a point P ε Eq (a, b), the point multiplication x*P over E_q (a, b) can be defined as x*P = P+P+P+…..+P (x time). As mentioned the security of ECC is based on the ECDLP defined in the following definition: "Given two points P and Q over Ep (a, b), the elliptic curve discrete logarithm problem (ECDLP) is to find an integer I ε F^*_q such that Q = I * P The integer I is called the discrete logarithm of Q to the base P, denoted I = logP Q (Hankerson *et al*., 2004). The most naive attack to solving the ECDLP is exhaustive search which can be circumvented by selecting elliptic curve parameters with n sufficiently large to represent an infeasible amount of computation (n≥280). Until today the ECC resist to all known attacks (Li *et al*., 2008).

We assume the following directives in the proposed method:

- A secure channel between the HAAA server and the HSS.
- A secure channel between the WAAA servers and the HAAA server.
- A secure channel between the WAAA servers.
- A WAAA is responsible for a multiple Aps with secure channel between the WAAA and APs.
- The UE can identify the identity of AAA server and AP.
- Each operator service selects a finite field F_q over a large odd prime $q>2^{160}$ and defines an elliptic curve equation E_q (a, b) : $y^2 = x^3 + ax + b \pmod q$ with

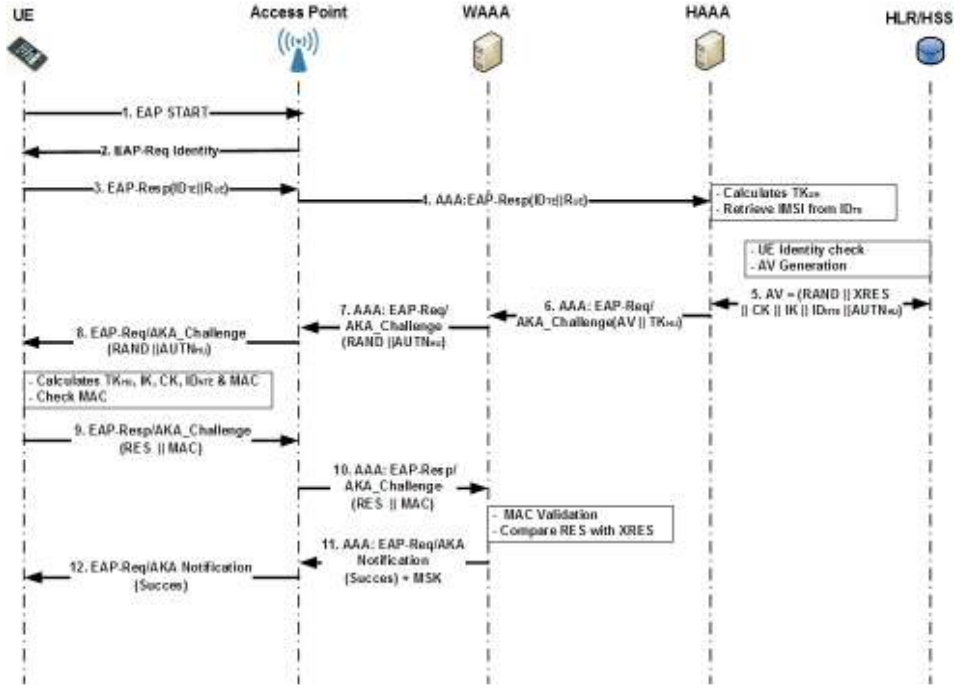


Fig. 5: Modified EAP- AKA authentication protocol

the order n over F_q, where a, b εF_q, q > 3 and $4a^3 + 27b^2 \neq 0$ mod q. And selects a public point Q with the order n over E_q (a, b).

- Each authentication server HAAA has a known public encryption key $U_H = d_H * Q$ (with d_H indicates the private key and ‘‘*” denotes the point multiplication over E_q(a, b)).
- Each authentication server WAAA has a pre-shared key with the HLR server, composed of (of (U_w, d_w) ($U_w = d_w * Q$).
- Each UE has a pre-shared secret key with the HLR server, composed of (U_E, d_E) ($U_E = d_E * Q$).

To hide the UE identity (IMSI) during the first UE authentication, the UE generates a temporary identity. The HSS will generate the next local user ID to be used in the next UE authentication. Also the HSS determines the life cycle of the main local authentication key.

Modified EAP-AKA full authentication method: Our protocol consists of seven steps shown in Fig. 5.

Step 1: After UE detection, the AP sends an EAP request identity to the UE.

Step 2: To protect the user identity (IMSI), the UE generates a temporary ID_{TE} that can be computed in this way:

- UE randomly selects an integer $r_{UE} \varepsilon Z^*_q$ and computes $R_{UE} = r_{UE} * U_E$, $R_{UE}' = r_{UE} * U_H$
- The encryption key is $TK_{UH} = d_E * R_{UE}'$ and the temporary user ID is $ID_{TE} = E_{TKUH}$ (IMSI, TK_{UH})
- The UE sends to the AP an EAP response message composed by ($ID_{TE} \| R_{UE}$)

Step 3: The AP forwards the EAP response message to the WAAA, which forwards it to the HAAA. Upon reception of this message, the HAAA first calculates the local decryption key TK_{UH} by: $TK_{UH} = d_H * R_{UE}$ and retrieves the user IMSI by decryption of the received ID_{TE} (D_{TKUH} (ID_{TE}) = IMSI). Then the HAAA contacts the HSS server to obtain the authentication vector which is built in this way.

The HSS generates a random number RAND, randomly selects an integer $r_H \varepsilon Z^*_q$, computes $R_H = r_H * U_H$, $R_H' = r_H * U_E$and creates the encryption key $TK_{HU} = d_H * R_H'$. The TK_{HU} is used with the help of AKA functions (f0-9) to generate the authentication vector AV composed by:

- The EAP authentication key CK = f3(TK_{HU}, RAND) and IK= f4(TK_{HU} , RAND)
- The next authentication ID, $ID_{NTE} = f_{TKUH}$ (IMSI, TK_{HU}), the expected response XRES= f2 (TK_{HU}, RAND), the MAC_{HU} = f1(IK,RAND, ID_{NTE}) and the authentication token $AUTN_{HU} = R_H \| RAND \| MAC_{HU}$.

The HSS sends the AV and the TK_{HU} to the HAAA which forwards it to the WAAA.

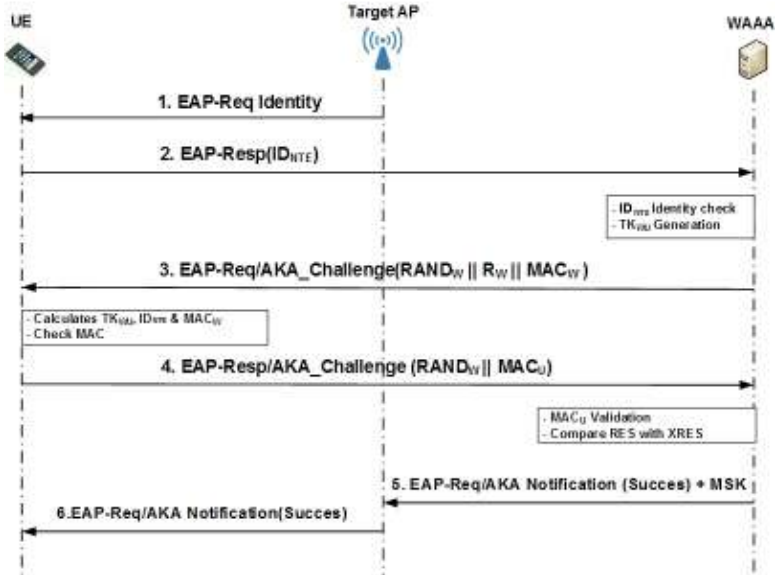


Fig. 6: Intra 3G-WLAN authentication protocol

Step 4: After receiving the AV from the HAAA, the WAAA sends an EAP request message composed by the RAND and AUTN to the UE.

Step 5: Upon receiving the EAP request message, the UE computes the authentication key $TK_{HU} = d_E * R_H$, CK and IK, next authentication ID, a local MAC_{HU} and verifies it with the received one. The authentication procedure is stopped in the case of negative verification. Otherwise, the UE produces a response (RES) and a message integrity check MAC = f1(RES || IK) that are sent back to the WAAA as an EAP response message.

Step 6: The WAAA receives the EAP response message and verifies the received RESP with the expected one XRESP. In positive check, the WAAA derives the session key MSK from the TKHU and sends an EAP success message to the UE. In addition the WAAA sends the MSK to the AP.

Step 7: After receiving the EAP success message, the UE and the AP generates a TSK key (Transient Session Key) by using the 4-way handshake protocol.

Horizontal handover: Since the 3GPP don't specify a particular protocol for HH in 3G-WLAN interworking architecture. In the next section we propose a new authentication protocol for inter and intra Horizontal Handover based on our modified EAP-AKA. The Intra-HH is executed when the currently associated AP and the target AP are in the same WLAN domain. The inter-HH is achieved when the currently associated AP and the target AP are in different WLAN domains. The proposed method authenticates the UE locally without HAAA intervention which improves the authentication performance.

Intra-horizontal handover: UE roams to a Target AP (TAP) when receiving poor signal-strength from the currently associated AP in the same WLAN domain. The WAAA locally authenticates the UE on behalf of HAAA by using the previous received key TKHU. The Fig. 6 describes the proposed intra-HH authentication protocol:

Step 1: After UE detection, the TAP sends an EAP request identity to the UE.

Step 2: The UE sends to the WAAA the previous received temporary identity ID_{NTE}.

Step 3: Upon receiving the UE identity ID_{NTE}. The WAAA checks the received ID_{NTE}. The WAAA classifies the request as an intra-HH if it has the same ID as the ID_{NTE} postfix. The WAAA then validates the key lifetime of TK_{HU}, generates a random number $RAND_W$, randomly selects an integer $r_W \varepsilon Z^*_q$ and computes $R_W = r_W * R_W' = r_W * TK_{HU}$, the authentication key $TK_{WU} = U_W * R_W'$. Also the WAAA computes the next UE local ID $ID_{NTE} = (ID_{WLAN} \| fTK_{UH}(ID_{NTE}, ID_{WLAN}, TK_{WU}))$, the message integrity token check $MAC_W = f1(RAND_W \| ID_{NTE} \| TK_{WU})$ and sends to the UE an EAP request message with $RAND_W$, R_W, MAC_W through the TAP.

Step 4: After receiving the EAP request message, the UE computes the authentication key $TK_{WU} = d_E * R_W$, next authentication ID, a local MAC_{WU} and verifies it with the received one.

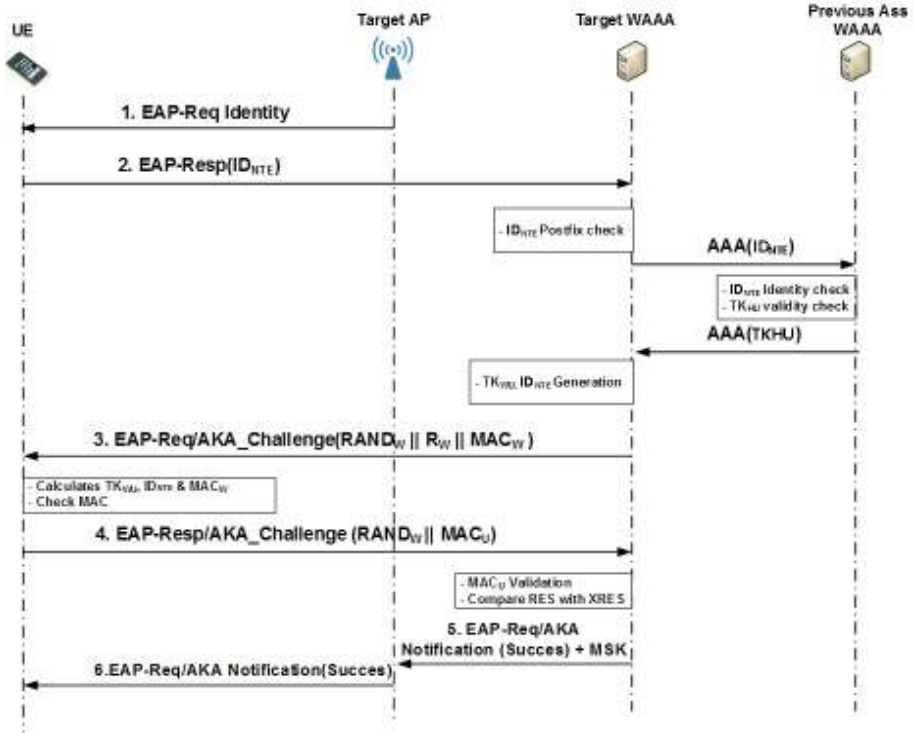


Fig. 7: Inter 3G-WLAN authentication protocol

The authentication procedure is stopped in the case of negative check, otherwise the UE replies with an EAP response message with the $RAND_W$ and a message integrity check $MAC_U = PRF (RAND_W || TK_{WU})$.

Step 5: The WAAA receives the EAP response message from the UE and verifies if the received $RAND_W$ is identical with the generated one. In positive check The WAAA derives the session key MSK from the TK_{WU} ($MSK = SHA1 (TK_{WU}, ID_{NTE} || ID_{TAP} || ID_{WAAA})$) and sends an EAP success message to the UE and sends the MSK to the AP.

Step 6: After receiving the EAP success message, the UE and the TAP generates a TSK key (Transient Session Key) by using the 4-way handshake protocol.

Inter-horizontal handover: The inter-HH is the same as the intra-HH with the difference that the target AP exists in another WAAA domain. As shown in Fig. 7 the authentication procedure is completed without the need of the authentication vector from the HAAA. The protocol proceeds as follows:

Step 1: After UE detection, the TAP sends an EAP request identity to the UE.

Step 2: The UE sends to the target WAAA his temporary identity ID_{NTE}.

Step 3: The TWAAA checks the received ID_{NTE} and classifies the request as an inter-HH if the ID_{NTE} postfix not matches with his ID. Then the TWAAA sends an authentication request with the ID_{NTE} to the previous UE authentication server PWAAA. The PWAAA validates the user ID_{NTE} and checks the lifetime of TK_{HU}. The PWAAA sends the TK_{HU} to the TWAAA if it's not expired; else it forwards the authentication request with the permanent ID and TWAAA ID to the HAAA. Then the authentication method continues in the same way as intra-HH in step 4, 5 and 6.

SECURITY ANALYSIS

To avoid the domino effect problem (Housley and Aboba, 2006), unnecessary distribution of key must be avoided. For this all generated keys must be used in a specific context. The UE secret key is hold only by the UE and the 3 GHN. The UE and the WAAA can share the authentication key with the help of the HAAA and without knowing the secret key of each other. The Fig. 8 shows the key hierarchy of the proposed authentication method. The TK_{HU} key is specific for the WLAN authentication. It's generated only by the UE and the HSS, because only the UE and the HSS have access to the UE key (d_E, U_E). The TK_{WU} key is generated by the UE and the WAAA to be used as

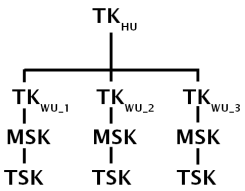


Fig. 8: Modified EAP-AKA key hierarchy

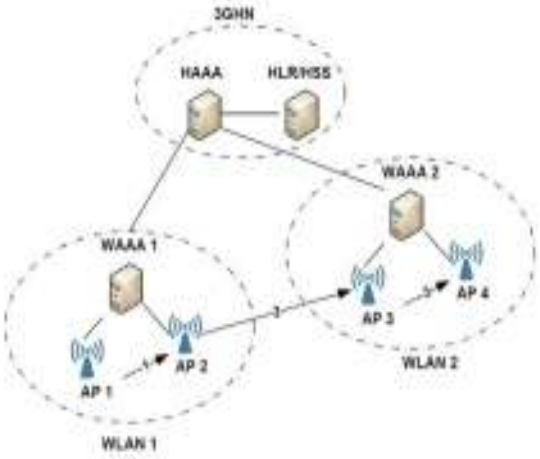


Fig. 9: User equipment mobility

authentication key and to derive a new session key for each AP. A new key TK_{WU} is generated for each re-authentication operation. Also our method simplifies the authentication mechanism in UE, because the same authentication mechanism is used for the vertical and horizontal handover. To avoid the replay attacks, all keys are used one time. The TK_{HU} is newest because the $r_H$is randomly generated in each full EAP-AKA authentication. The same thing for the fresh key TK_{WU} generated from the TK_{HU} and r_w.

The proposed protocol satisfies all network security requirements defined by the 3GPP. In particular UE identity protection, secure key management and mutual authentication. In this section we will analyse the security of our proposed protocol:

- **Protection of the UE identity:** To avoid disclosing user identity, the IMSI is protected by encryption in the first UE connection. Onetime local ID_{NTE} is used instead of the permanent ID. The UE must obtain a new local ID_{NTE} from the WAAA on every authentication. Therefore, our protocol provides a strong user identity protection against identity related attacks.
- **Mutual authentication:** Our method proposes a strong mutual authentication mechanism between the UE and the WAAA. The HAAA delegates the UE authentication to the WAAA. The UE and the WAAA authenticate each other by proving the possession of the correct TK_{HU}. The UE authenticates the authentication server WAAA by verifying the calculated MAC_w with the received one. The WAAA authenticates the user by checking the $RAND_W$ with the generated one.
- **Man in the middle attack protection (Hwang *et al*., 2008):** The user identity is protected by using a onetime generation key. The attacker cannot retrieve or modify the user identity, only the UE and the WAAA server can retrieve it. In addition all encryption key is randomly generated for each request and response packets and no key is transformed in clear. Finally all messages are protected by a message integrity code MAC. Therefore our protocol can resist to the man in middle attack.
- **Protection to the replay attack:** Our protocol is robust to the replay attack because the $RAND_W$ and r_W are generated randomly for each new re-authentication and are used one time.

PERFORMANCE ANALYSIS

This section compares the performance of our method with the existed EAP-AKA standard method. The performance comparison is based on the bandwidth consumption and authentication delay for UE movement between 3G, WLAN1 and WLAN2. As descripted in Fig. 9, firstly, the UE is connected to the AP1 in WLAN1. After this, the UE moves to the AP2 in the same WLAN1 domain by executing an intra-HH. Then he performs an inter-HH to the AP3 in WLAN2 and moves after to AP4 by an intra-HH. To cover the UE movements two authentication scenarios are proposed:

Scenario 1: This scenario uses the existed authentication protocol adopted by the 3G-WLAN architecture. The UE performs EAP-AKA authentication in all authentication stages.

Scenario 2: In this scenario, we propose to use our modified EAP-AKA, intra-HH and inter-HH authentication methods.

Bandwidth consumption: The UE is authenticated by the HAAA in the EAP-AKA. However in our proposed method, the user authentication is delegated to the local WAAA authentication server. This can reduces the bandwidth consumption between the HAAA and the WAAA by 50% compared to the full EAP-AKA. Also our protocol doesn't require any SQN synchronization between the UE and the 3GHN, which can reduce the bandwidth consumption.

Authentication signaling cost: In this section we evaluate the signalling cost of both authentication scenarios. The signalling cost can be defined as the total

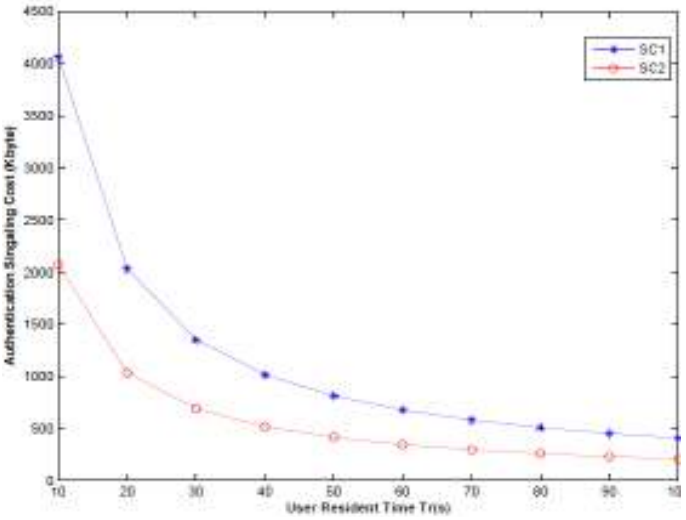


Fig. 10: Authentication signaling cost for SC1 and SC2

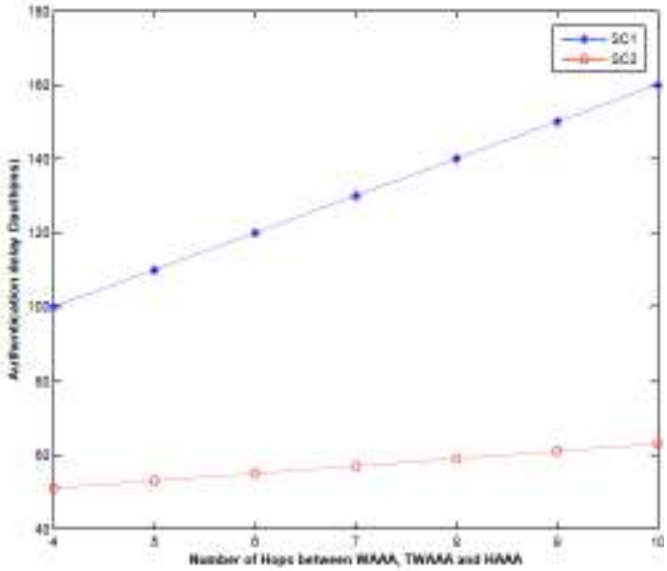


Fig. 11: Authentication delay in SC1 and SC2

authentication signalling message traffic during a communication session (Choi *et al*., 2007). Practically two network nodes are separated by a set of H hops. We assume that the number of hops between the UE and the AP is HUE-AP = 1, HAP-WAAA = 1 is the number of hops between AP and WAAA, 4 is the number of hops between WAAA1 and WAAA2 HWAAA-HAAA= 4, HWAAA-HAAA= 4 is the number of hops between WAAA and HAAA and HHAAA-HLR= 1 is the number of hops between HAAA and HLR. Therefore, the number of exchanged message in standard EAP-AKA NEAP-AKA = 26, Nmodif(EAP-AKA) = 18, Nintra-HH = 9 and Ninter-HH = 17. The authentication signalling cost for both scenarios is:

$$C_{(SC1)} = (4\times N_{EAP\text{-}AKA})\times R\times Nr \quad (1)$$

$$C_{(SC2)} = (N_{modif(EAP\text{-}AKA)} + 2\times N_{intra\text{-}HH} + N_{inter\text{-}HH}) \times R\times Nr \quad (2)$$

The Average message size 'R' is set to 200 bytes. Nr = Ts/Tr is the average number of UE movements during a session. The average session time "Ts" is set to 2000s. Tr is the average WLAN resident time, it varies between 10 and 100s. The Fig. 10 shows the authentication signalling cost for both authentication scenarios. As we can see a higher resident time implies a low signalling cost. And the scenario 2 reduce the authentication signalling cost by 50, 96% relative to the scenario 1. Improved performance results can be reached when increasing the life cycle of authentication key Tk_{HU}.

Authentication delay: The total authentication delay (D_{auth}) can be defined as the delay taken by an authentication protocol to complete the authentication process. In this section we compare the D_{auth} of both authentication scenarios. The D_{auth} can be divided in three components, the delay of the EAP messages transmission (D_{trans}), the EAP message treatment delay (D_{tre}) (Data base access, key and tag generation, computation, encryption/decryption,…) and the propagation delay (D_{prop}) (Prasithsangaree and Krishnamurthy, 2004). According to Prasithsangaree and Krishnamurthy (2004) the transmission delay in WLANs at 11 Mbps is insignificant compared to the D_{tre} and $D_{prop.}$ And we assume that both methods use symmetric key encryption with similar key sizes and perform moderately the same operations. Therefore, the transmission delay can be ignored.

The total authentication delay D_{auth} depends basically on the propagation delay D_{prop}. The propagation delay can be divided in four set. $D_{prop\ (UE-AP)}$ is the propagation delay between the UE and the access point, $D_{prop(AP-WAAA)}$ is the propagation delay between the access point and the WAAA, the propagation delay between the WAAA and HAAA ($D_{prop(WAAA-HAAA)}$), the propagation delay between two WAAAs ($D_{prop\ (WAAA-TWAAA)}$) and the $D_{prop(HAAA-HLR)}$ the propagation delay between the HAAA and the data base HLR.

The total authentication delay for the EAP-AKA standard can be expressed as:

$$D_{auth(EAP-AKA)} = (5\ D_{prop(UE-AP)} + 4\ D_{prop(AP-WAAA)} + 4\ D_{prop(WAAA-HAAA)})$$

$$D_{auth(modif\ EAP-AKA)} = (5\ D_{prop(UE-AP)} + 4\ D_{prop(AP-WAAA)} + 2\ D_{prop(WAAA-HAAA)})$$

$$D_{auth(intra-HH)} = (5\ D_{prop(UE-AP)} + 4\ D_{prop(AP-WAAA)})$$

$$D_{auth(inter-HH)} = (5\ D_{prop(UE-AP)} + 4\ D_{prop(AP-WAAA)} + 2\ D_{prop(TWAAA-WAAA)})$$

The total authentication delay for the proposed SC1 and SC2 can be expressed as:

$$D_{auth(SC2)} = 5\ D_{prop(EAP-AKA)}$$

$$D_{auth(SC2)} = D_{prop(EAP-AKA)} + 2\ x\ D_{auth(intra-HH)} + D_{auth(inter-HH)}$$

We assume that we have the same propagation delay between the WAAA, TWAAA and the HAAA ($D_{prop(TWAAA-WAAA)} = D_{prop(WAAA-HAAA)} = H \times Dprop_{(Wired)}$ with $Dprop_{(Wired)}$ is the wired propagation delay and H is the number of hops separating two nods). From (Prasithsangaree and Krishnamurthy, 2004) we note that the $D_{prop(UE-AP)}$ is set to 2 ms and $D_{prop(Wired)} = D_{prop(AP-WAAA)}$ are set to 0.5 ms. The Fig. 11 shows the authentication delay of both scenarios by varying the number of hops between WAAA, TWAAA and HAAA. Our authentication protocol reduces the authentication delay in scenario 2 compared to scenario 1 which uses only the standard protocol EAP-AKA. The authentication delay can be reduced by 30% in SC2 compared to SC1.

The network security should not be impacted by the performance improvement of the authentication method. In this section we evaluate the security proprieties of the proposed authentication protocol. The security evaluation checks that our method achieves the required security goals including user identity protection, mutual authentication, protection of transmitted message and secure key management. To verify this, our protocol is evaluated by using the formal security verification platform AVISPA (Armando *et al*., 2005).

SECURITY EVALUATION

AVISPA is an automatic push-button formal validation tool for internet security protocols. It has been developed in a project funded by the European Commission under the Information Society Technologies IST programme.

AVISPA is based on sending and receiving messages and performing decryption and digital signature verification actions. AVISPA takes as input a High Level Protocol Specification Language (HLPSL) for describing security protocols and specifying their intended security properties. HLPSL is an explicit and intuitive language to model a protocol; its semantics is based on Lamport's Temporal Logic of Actions (TLA). The HLPSL is based on roles; each protocol is divided into a set of Basic Roles representing the actions of one single agent in a run of the protocol and Composition Roles which represent the entire protocol and instantiate the Basic Roles. Each role is modelled as a 'state'. Each state has variables which are responsible for the state transitions, retrieves its initial information by parameters and communicates synchronously with other roles by channel. The security goal is the most important feature of this tool. It allows the model checkers to find the possible attacks (Fig. 12).

In general, authentication goals are modelled by these words: witness, request, wrequest and secret. Once the protocol is modelled in HLPSL, AVISPA translates them into a lower-level language Intermediate Format (IF) by a translator called hlpsl2if. IF is executed directly by the back-ends tools (OFMC, CL-AtSe, SATMC and TA4SP) to verify if the security goals are satisfied or violated.

The AVISPA tools and HLPSL language are a very popular formal verification pack. However, the differences between the specification language and the notation User and Server, particularly the definitions role by role and not message by message, make this pack difficult to use. For this reason, a new tool "Security Protocol Animator" (SPAN) was created to facilitate the specification phase by allowing the animation of the language HLPSL (Glouche and Genet, 2006).

```
role server ( P,S        : agent,
              F1         : hash_func,
              HMAC       : hash_func,
              IDS        : text,
              TKhu       : symmetric_key,
              Q          : public_key,
              Multi      : hash_func,
              SND,RCV    : channel (dy))
played_by S def=
  local
    AT_RAND, RAND2,Rw                    : text,
    Rwu,R1wu,TKwu,IDnte,AT_MAC1, AT_MAC2: message,
    Dw                                   : symmetric_key,
    State                                : nat

  const
    request_id, user_id,success : text,
    at_rand,at_rand2            : protocol_id
  init
    State := 0
  transition
  1.    State   = 0     /\ RCV(start)    =|>
        State' := 3     /\ SND(request_id)
  2.    State   = 3     /\ RCV(IDS.user_id) =|>
        State' := 5     /\ Rw'       := new()
                        /\ Rwu'      := Multi(Rw'.Multi(Dw.Q))
                        /\ R1wu'     := Multi(Rwu'.TKhu)
                        /\ TKwu'     := Multi(R1wu'.Dw)
                        /\ AT_RAND'  := new()
                        /\ IDnte'    := (IDS.F1(user_id.TKwu'))
                        /\ AT_MAC1'  := HMAC(AT_RAND'.IDnte'.TKwu')
                        /\ SND(Rwu'.AT_RAND'.AT_MAC1')
                        /\ witness(S,P,at_rand,AT_RAND')
  3.    State   = 5     /\ RCV(AT_RAND.AT_MAC2')
                        /\ AT_MAC2' = HMAC(AT_RAND'.TKwu) =|>
        State' := 7     /\ SND(success)
                        /\ request(S,P,at_rand2,AT_RAND)
end role
```

```
role peer ( P,S              : agent,
            F1               : hash_func,
            HMAC             : hash_func,
            IDS              : text,
            TKhu             : symmetric_key,
            Q                : public_key,
            Multi            : hash_func,
            SND,RCV          : channel (dy))
played_by P def=
  local
      AT_RAND, RAND2,Rw  : text,
      Dw                 : symmetric_key,
      TKwu,AT_MAC2,IDnte : message,
      State              : nat
  const
      request_id, user_id, success: text,
      sec_Tk, at_rand, at_rand2   : protocol_id
  init
    State := 0
  transition
  1.    State   = 0     /\ RCV(request_id)  =|>
        State' := 2     /\ SND(IDS.user_id)
  2.    State   = 2     /\
  RCV(Multi(Rw'.Multi(Dw'.Q)).AT_RAND'.HMAC(AT_RAND'.(IDS.F1(user_id.TKwu')).TKwu'))
                        /\ TKwu' = Multi(Multi(Multi(Rw'.Multi(Dw'.Q)).TKhu) .Dw') =|>
        State' := 4     /\ AT_MAC2' := HMAC(AT_RAND'.TKwu')
                        /\ SND(AT_RAND'.AT_MAC2')
                        /\ request(P,S,at_rand,AT_RAND')
                        /\ witness(P,S,at_rand2,AT_RAND')
                        /\ secret(TKwu',sec_Tk,{S,P})
  3.    State   = 4     /\ RCV(success) =|>
        State' := 6
end role
```

Fig. 12: Intra 3G-WLAN UE and WAAA roles specification in HLPSL

```
role twaaaa (
            P,PWAAA,TWAAA    : agent,
            F1,F2,P3,F4,F5   : hash_func,
            HMAC             : hash_func,
            IDTWAAA          : text,
            IDPWAAA          : text,
            Q                : public_key,
            Multi            : hash_func,
            SND_TWAAA,RCV_TWAAA,SND_PWAAA,RCV_PWAAA      : channel (d
played_by TWAAA def=
  local
    AT_RAND, RAND2,Rw                        : text,
    TKhu, Dw                                 : symmetric_key,
    Rwu,R1wu,TKwu,AT_MAC1, AT_MAC2,IDnte     : message,
    State                                    : nat
  const
    request_id,user_id, success      : text,
    at_rand,sec_Tkh, at_rand2        : protocol_id
  init
    State := 0
  transition
  1.    State   = 0     /\ RCV_TWAAA(start)      =|>
        State' := 1     /\ SND_TWAAA(request_id)
  2.    State   = 1     /\ RCV_TWAAA(IDPWAAA.user_id) =|>
        State' := 3     /\ SND_PWAAA(IDPWAAA.user_id)
  3.    State   = 3     /\ RCV_PWAAA(Multi(TKhu')) =|>
        State' := 5     /\ Rw'       := new()
                        /\ Rwu'      := Multi(Rw'.Multi(Dw.Q))
                        /\ R1wu'     := Multi(Rwu'.TKhu')
                        /\ TKwu'     := Multi(R1wu'.Dw)
                        /\ AT_RAND'  := new()
                        /\ IDnte'    := (IDTWAAA.F1(user_id.TKwu'))
                        /\ AT_MAC1'  := HMAC(AT_RAND'.IDnte'.TKwu')
                        /\ SND_TWAAA(Rwu'.AT_RAND'.AT_MAC1')
                        /\ witness(TWAAA,P,at_rand,AT_RAND')
                        /\ secret(TKhu,sec_Tkh,{TWAAA,PWAAA,P})
  3.    State   = 5     /\ RCV_TWAAA(AT_RAND.AT_MAC2')
                        /\ AT_MAC2' = HMAC(AT_RAND'.TKwu) =|>
        State' := 7     /\ SND_TWAAA(success)
                        /\ request(TWAAA,P,at_rand2,AT_RAND)
end role
```

Fig. 13: Inter 3G-WLAN TWAAA role specification in HLPSL

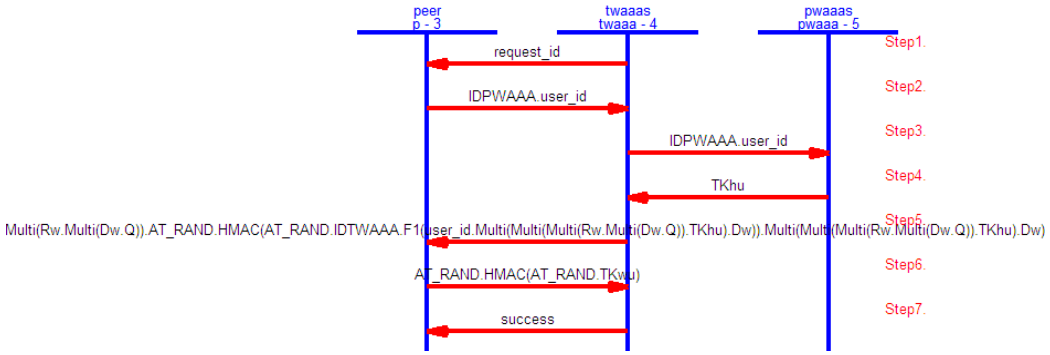
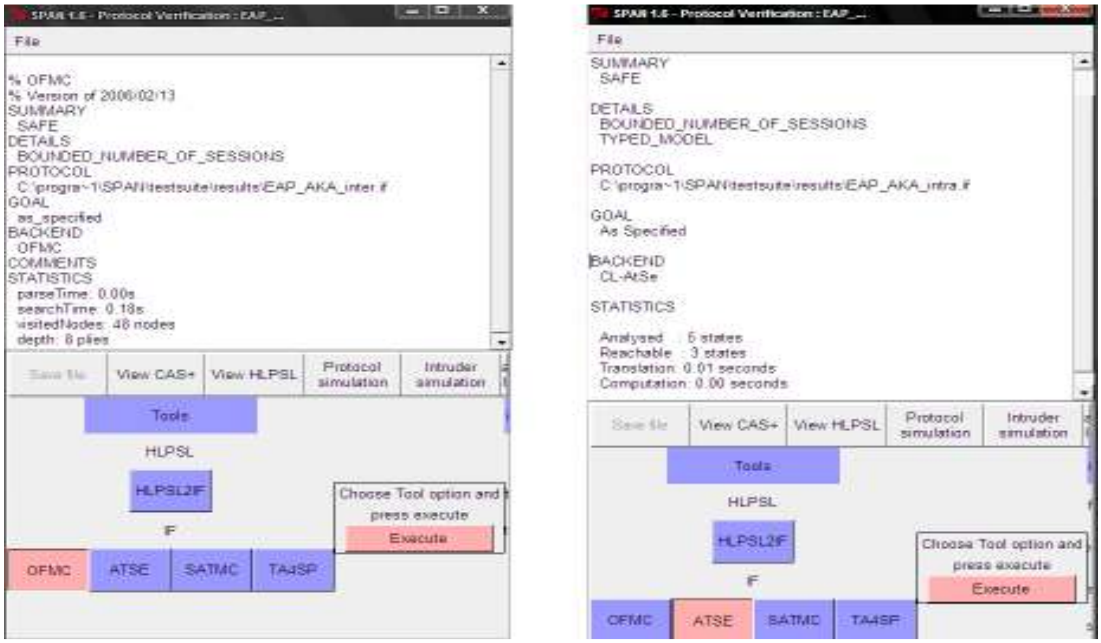


Fig. 14: Inter 3G-WLAN protocol handover simulation by SPAN



(a) (b)

Fig. 15: (a) Inter 3G-WLAN check returned message by OFMC message-(b) Intra 3G-WLAN check returned message by CLATSE message

Our protocol is defined in Peer (UE) and Server (WAAA) model and is expressed in the formal language HLPSL used in AVISPA. The Fig. 12 illustrates the UE and WAAA roles in intra 3G-WLAN handover. We use the request and witness goal specification to check the mutual authentication between UE and WAAA. The assertion witness(S,P,at_rand,AT_RAND') means that the WAAA should be authenticated by the UE by agreeing on the value AT_RAND. While the assertion request (P,S,at_rand,AT_RAND') indicates that the UE authenticates the WAAA and agrees on the value AT_RAND. The Fig. 13 shows HLPSL role specification of the TWAAA in inter 3G-WLAN handover. The statement secret (TKhu, sec_Tkh,{TWAAA,PWAAA,P}) validates the confidentiality of the key TKhu between the PWAAA, TWAAA and UE. The Fig. 14 shows the inter 3G-WLAN protocol simulation by SPAN, which prove that our specification is corrected written and interpreted by AVISPA.

The mutual authentication and secrecy of keys of our protocols was checked by using OFMC and CLATSE. All tests are passed and no attacks or vulnerabilities were found, which confirm the secure key management and mutual authentication service of the proposed protocols. The Fig. 15a and b show the messages returned by OFMC and CLATSE verification tools. Our protocols achieves mutual authentication, assures the confidentiality of shared keys Tk_{HU} and TK_{wu} between UE and WAAAs and is safe to use by both verification check tools.

CONCLUSION

Due to the limited area coverage of WLAN network, the vertical and horizontal handover of UE in 3G-WLAN interworking architecture is a necessary. The handover process must not impact the running user application and decrease the QOS of 3GHN service. For that, a seamless handover is absolutely required. The authentication delay has an impact on handover delay and simplified authentication schema can reduce handover delay and increase handover performance. In this study we have proposed a modified EAP-AKA authentication method to reduce the authentication delay during vertical handover and intra/inter horizontal handover in 3G-WLAN architecture. The proposed protocol shows superior performance results in comparison to the existing EAP-AKA method in terms of bandwidth consumption, signalling cost and authentication delay. The security proprieties of our method are verified by using AVISA, which proved that our method its resistance to known authentication attacks.

REFERENCES

Aboba, B., L. Blunk, J. Vollbrecht, J. Carlson and H. Levkowetz, 2004. Extensible Authentication Protocol. RFC 3748.

Arkko, J. and H. Haverinen, 2006. Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). IETF, RFC 4187.

Armando, A., D. Basin, J. Cuellar, M. Rusinowitch and L. Viganò, 2005. The AVISPA tool for the automated validation of internet security protocols and applications. CAV 2005, LNCS 3576, pp: 281-285.

Choi, H.H., O. Song and D.H. Cho, 2007. Seamless handoff scheme based on pre-registration and pre-authentication for UMTS-WLAN interworking. Wirel. Pers. Commun., 41(3): 345-364.

Glouche, Y. and T. Genet, 2006. SPAN: A Security Protocol Animator for AVISPA-User Manual. IRISA/Rennes university's 1. Retrieved from: http ://www.irisa.fr/lande/genet/span.

Hankerson, D., A. Menezes and S. Vanstone, 2004. Guide to Elliptic Curve Cryptography. Springer-Verlag, New York, USA.

Housley, R. and B. Aboba, 2006. Guidance for AAA Key Management. IETF Internet Draft (draft-housley-aaa-key-mgmt-06). (work in Progress), November, 2006.

Hur, J., C. Park and H. Yoon, 2007. An efficient pre-authentication scheme for IEEE 802.11-based vehicular networks. Lect. Notes Comput. Sc., 4752: 121-136.

Hwang, H., G. Jung, K. Sohn and S. Park, 2008. A study on man in the middle vulnerability in wireless network using 802.1X and EAP. Proceeding of the International Conference on Information Science and Security. Seoul, Korea, pp: 164-170.

Kambourakis, G., A. Rouskas and S. Gritzalis, 2004. Advanced SSL/TLS based authentication for secure WLAN-3G interworking. IEEE Proc. Commun., 151(5): 501-506.

Kwon, H., K.Y. Cheon, K.H. Roh and A. Park, 2006. USIM based authentication test-bed for UMTS-WLAN handover. Proceedings of IEEE Infocom, Barcelona, Spain.

Lee, M., G. Kim and S. Park, 2005. Seamless and secure mobility management with Location-Aware Service (LAS) broker for future mobile interworking networks. J. Commun. Netw., 7(2): 207-221.

Li, F., X. Xin and Y. Hu, 2008. Identity-based broadcast signcryption. Comput. Standard Interf., 30: 89-94.

Lim, C., D.Y. Kim, O. Song and C.H. Choi, 2009. SHARE: Seamless handover architecture for 3G-WLAN roaming environment. J. Wirel. Netw., 15(3): 353-363.

Long, M., C.H. Wu and J.D. Irwin, 2004. Localised authentication for inter-network roaming across wireless LANs. IEEE Proc. Commun., 151(5): 496-500.

Matsunaga,Y., A.S. Merino, T. Suzuki and R.H. Katz, 2003. Secure authentication system for public WLAN roaming. Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH). ACM Press, San Diego, CA, USA, pp: 113-121.

Pack, S. and Y. Choi, 2002. Pre-authenticated fast handoff in a public wireless LAN based on IEEE 802.1x model. Proceedings of IFIP TC6 Personal Wireless Communications, 234: 175-182.

Prasithsangaree, P. and P. Krishnamurthy, 2004. A new authentication mechanism for loosely coupled 3G-WLAN integrated networks. Proceeding of the IEEE 59th Vehicular Technology Conference. Spring, 5: 2998-3003.

Rigney, C. and S. Willens, 2000. Remote Authentication Dial in User Service (RADIUS). IETF RFC 2865. Retrieved from: tools.ietf.org/html/rfc2865.

Salgarelli, L., M. Buddhikot, J. Garay, S. Patel and S. Miller, 2003. Efficient authentication and key distribution in wireless IP networks. IEEE Wirel. Commun. Mag., 10(6): 52-61.

Shi, M., X. Shen and J.W. Mark, 2004. IEEE802.11 roaming and authentication in wireless LAN/cellular mobile networks. IEEE Wirel. Commun., 11(4): 66-75.

3GPP, 2004. System to Wireless Local Area Network (WLAN) Interworking, System Description. Rel. 6, 3GPP TS 23.234, v6.3.0.

3GPP, 2005. Security Architecture (Release 7). 3GPP Technical Specifications, 3G Security TS 33.102 v7.0.0, 3GPP, Valbonne, France.

3GPP, 2006. 3G security WLAN Interworking Security (Release 7). 3GPP Technical Specifications TS 33.234 v7.0.0, 3GPP, Valbonne, France.

3GPP, 2008. 3G Security: Security Architecture (Release 8). TS 33.102 v8.0.0, June 2008.