Alezabi *et al. EURASIP Journal on Wireless Communications and Networking* (2020) 2020:105
https://doi.org/10.1186/s13638-020-01702-8

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks

Kamal Ali Alezabi[1*], Fazirulhisyam Hashim[2*], Shaiful J. Hashim[2], Borhanuddin M. Ali[2] and Abbas Jamalipour[3]

*Correspondence:
kamal@ucsiuniversity.edu.my;
fazirul@upm.edu.my
[1]Institute of Computer Science and Digital Innovation, UCSI University, 56000 Cheras Kuala Lumpur, Malaysia
[2]Department of Computer and Communication Systems Engineering, & Research Centre of Excellence for Wireless and Photonic Networks (WiPNET), Faculty of Engineering, Universiti Putra Malaysia, Malaysia 43400 UPM, Serdang, Selangor, Malaysia
Full list of author information is available at the end of the article

Abstract

In the next-generation heterogeneous wireless networks, designing authentication protocols that meet the demand of mobile users/applications is a challenge. This paper proposes authentication and re-authentication protocols for 4G wireless networks, in particular, LTE-Advanced (LTE-A), WLAN, and WiMAX-Advanced (WiMAX-A) interworking architecture. The proposed protocols are applicable to 5G networks. With the consideration of the existing standard authentication protocols, a new set of authentication and re-authentication protocols has been reinvented to provide fast and secure handovers (HO) in the current 4G and the next 5G networks. The proposed authentication protocols can be invoked when the users perform a vertical HO (between different networks) for the first time, whereas the re-authentication protocols can be invoked when the users perform a horizontal HO (within the same network domain). These protocols provide an efficient method to protect user identity and reduce the burden on the authentication server (AS) during the sequential handovers. The results of the analytical model show that the proposed protocols achieve better performance than standard and other protocols. The reduction of handover cost, handover delay, and energy consumption in the proposed protocols reaches up to 22%, 44%, and 17%, respectively. In addition, the verification tools show that the proposed protocols are secure, dependable, and prevent all types of authentication and secrecy attacks.

Keywords: 5G, EAP-AKA′ authentication, Fast re-authentication, AVISPA

1 Introduction

The 3GPP standards support the interworking between the advanced long-term evolution (LTE-A) networks and other wireless networks to provide better services in coverage, cost, and performance. These heterogeneous wireless networks will serve a huge number of users and applications that demand higher data rates, lower latency, and energy consumption. For the sake of providing seamless and fast handovers in the heterogeneous networks, the delay and cost caused by authentication protocols should be reduced. In addition, the authentication protocols should be secured against authentication attacks. Therefore, the authentication process has

increasingly become more important, especially in the new 5G heterogeneous networks.

The basics of current 4G Authentication and Key Agreement (AKA) protocols will be utilized in the new 5G networks; thus, the 4G authentication protocols should be improved to meet the demand of this new technology. For instance, the users in the LTE-WLAN-WiMAX interworking architecture must be authenticated by the LTE Home Subscriber Server (HSS) in the home network, which adds delay and overhead on these servers each time the user connects or moves in the interworking architecture. It also makes this server a subject of single point of failure. From the performance aspect, the delay caused by the authentication process adds overhead to the seamless and fast handover process. The effect of delay could be more severe in the case of 5G application that are delay-sensitive applications. From the security point of view, the user identity disclosure attack can be launched in the first connection, when the International Mobile Subscriber Identities (*IMSIs*) are sent by users to HSS without protection in a clear text.

In WLAN, LTE, and WiMAX networks, the fast re-authentication protocols have been proposed by standards to reduce the authentication delay and cost of full authentication protocols such as Improved Extensible Authentication Protocol-AKA′ (EAP-AKA′), Evolved Packet System-AKA (EPS-AKA), and Initial Network Entry Authentication (INEA), respectively [1] and [2]. Despite of fast re-authentication protocol's efficiency in reducing the authentication delay and cost, they still suffer from User Identity Disclosure (UID) attack, Lack of Perfect Forward Secrecy (PFS), and Man-In-The-Middle (MITM) attack. In addition, the fast re-authentication protocols are invoked regardless of the handover type (i.e., inter and intra), which inherit high delay; therefore, it is considered as insufficient solution for 5G networks.

In this paper, the standard AKA protocols that are used in LTE, WLAN, and WiMAX networks have been reinvented to present new re-authentication protocols for each network domain. The new re-authentication protocols enhance the security aspects and the performance in terms of delay, cost, and energy consumption. The proposed protocols are aimed to provide fast and secure different handover types, and these features allow the proposed protocols to effectively work in the 5G heterogeneous wireless networks.

In the case of applying the proposed protocols in the 5G networks, the names of the entities that are involved in the authentication process will be changed, for example, the functions of eNB will be handled by next-generation Evolved Node-B (ng-eNB), the functions of authentication server (AS) will be handled by Authentication Server Function (AUSF), and the function of storing long-term keys in HSS will be handled by the Unified Data Management (UDM).

The contributions of this paper can be summarized as follows:

- A new method is proposed to prevent UID attack and reduce the handover delay, cost, and the overhead on AS, which contributes significantly in reducing delay and cost during different handover types in heterogeneous networks.
- Three standard full authentication protocols, EAP-AKA′, INEA, and EPS-AKA protocols, are enhanced to provide full authentication process between the user and WLAN, WiMAX, and LTE networks, respectively, when the user connects to one of these networks for the first time.

- A set of new re-authentication protocols is proposed to be performed after the enhanced standard authentication protocols. These protocols provide fast inter and intra re-authentication processes in LTE-WiMAX-WLAN interworking architecture during inter and intra handovers, respectively. In addition, in the case of any failure occurs in the HSS server, the local servers have the ability to complete the authentication process, which results in avoiding the single point of failure.
- A new unified key hierarchy is proposed to be suitable for the module of the networks involved in this work.

The remainder of this paper is organized as follows: Section 3 presents an overview of the interworking architecture between LTE-WLAN-WiMAX networks; it also presents the standard full and fast authentication protocols. A brief of the related works is also presented in this section. Section 4 describes the proposed authentication and re-authentication protocols. Section 5 provides a security analysis of the proposed protocols while Section 6 evaluates the performance of the proposed protocols compared to the standard and other protocols. Section 7 concludes the paper.

2 Methods

In this paper, the proposed protocols and methods are presented in Section 4, where the standard AKA protocols that are used in LTE, WLAN, and WiMAX networks are enhanced to present new re-authentication protocols for each network domain. These enhancements make the proposed protocols applicable for 5G networks. To prevent the UID attack, a Kerberos-based method is proposed. A new unified key hierarchy is used to be applied in each network type in the interworking architecture. The new re-authentication protocols are locally performed during inter and intra handovers to provide secure and fast handovers. In Section 5, the security aspects of the proposed protocols are analyzed and verified using well-known verification tools. Section 6 presents the evaluation results and discussion of the proposed protocols, where a scenario of user movements and an analytical model is proposed for evaluation and comparisons of the proposed protocols with standard and other methods in terms of delay, cost, storage, and energy consumption.

3 Overview and related works

3.1 Heterogeneous wireless networks

Heterogeneity is one of the most features of the current 4G and the next 5G networks. This section presents an overview of the heterogeneous wireless networks such as LTE, WLAN, and WiMAX networks.

The security was not completely specified in the earlier versions of WLAN. It was specified in the IEEE 802.11i amendment. The key management and authentication are also included in this standard. The Remote Authentication Dial in User Service (RADIUS) protocol supports EAP-AKA authentication protocol [3].

The security of WiMAX has been specified by the IEEE 802.16 standard as a security sub-layer in the Medium Access Control layer. The INEA authentication protocol is a part of the Privacy Key Management (PKM). The PKM is a security protocol that has been adopted in the WiMAX security sub-layer to provide authorization, authentication, key exchange, and key distribution between base stations (BSs) and mobile stations (MSs) [4].

The last standard of WiMAX is the WiMAX-Advanced which has many features such as supporting mobile internet and MIMO [5].

The long-term evolution of the Universal Mobile Telephone System (UMTS) is one of the Third-Generation Partnership Projects (3GPPs) which was defined by 3GPP in November 2004. The recent projects are LTE and its enhanced version, which is the LTE-Advanced (LTE-A).

In LTE-A, a wider bandwidth is provided, and antenna technology is improved and used in both uplink and downlink directions. These technologies are called 4th Generation (4G) networks that rapidly spread over the world. This leads to more needs of higher bit rate and lesser delay to serve a large number of users.

The AKA protocol is continuously evaluated and developed by 3GPP. The development of this protocol has been started from 2G-AKA [6], 3G-AKA [7], or UMTS-AKA until 4G networks version EPS-AKA [8]. The development is ongoing to use AKA in 5G networks [9].

The future 5G networks will have extraordinary improvements in data rate, system capacity, energy consumption, and massive device connectivity. Mostly, the AKA security protocol that is used in the 4G networks will be used in the future 5G networks with some improvements.

The integration or interworking between the aforementioned different wireless networks is established via connecting those networks to the HSS server in LTE home network. The HSS server must authenticate any user connecting to the interworking architecture. Figure 1 shows a simplified LTE-WLAN-WiMAX interworking architecture where the 3GPP Authentication, Authorization, and Accounting server (3AAAS); Proxy AAA server (PAAAS); and Wireless AAA server (WAAAS) play a role of the bridge node between LTE, WiMAX, and WLAN domains. Those servers are connected via STa or Wa interfaces to perform authentication and re-authentication procedures.

A simplified domain of LTE network includes the radio part, which is identified as the evolved UMTS Terrestrial Radio Access Network (eUTRAN). This part includes one or more Evolved Node-B (eNBs). The other part is the packet core, which is identified as the Evolved Packet Core (EPC). It consists of HSS, Mobility Management Entity (MME), and Serving Gateway (S-GW). The total system is identified as the EPS. This structure makes LTE simple, scalable to be interoperable with legacy networks such as UMTS and other wireless networks. In addition, it makes LTE efficient to widely use the internet protocols and applications [10].

A WLAN domain includes the WAAAS, which may control one or several Access Points (APs), whereas WiMAX network domain includes the Access Service Network (ASN), which is the access network of WiMAX. It contains one or several BSs and ASN Gateways (ASN-GWs). The ASN is an interface between the Connectivity Service Network (CSN) and MSs or the Subscriber Stations (SSs).

3.2 Standard Full EAP-AKA′ Authentication Protocol (AKAP)

The full authentication protocol is invoked whenever the user connects to a new network domain for the first time. Unlike previous studies, this work employs the improved EAP-AKA′ protocol rather than the EAP-AKA protocol [2]. This is due to its advantages in the security aspects. In the EAP-AKA′ protocol, the Access Network Identity (*ANID*) [11] is used to derive Integrity Key (*IK*) and Ciphering Key (*CK*), to be named as IK' and CK',

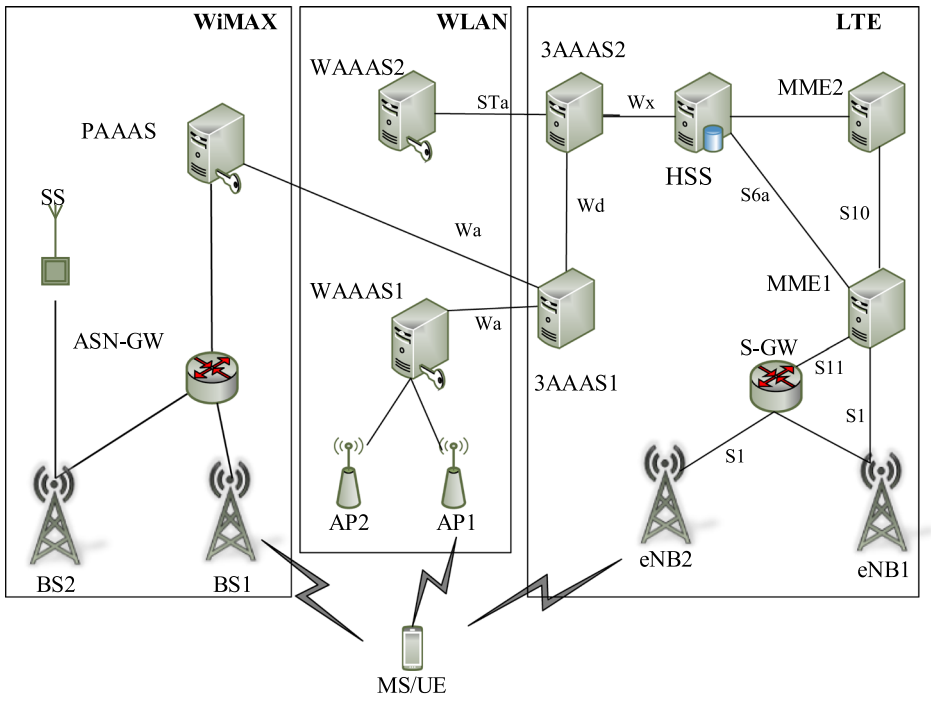

Fig. 1 LTE-WLAN-WiMAX interworking

respectively. The usage of *ANID* leads to specify the generated keys for a particular network that is provided in *ANID*; therefore, it ensures that the same *ANID* is only used by the parties involved in the authentication procedure. Moreover, it adds an additional protection against compromised node by limiting the attacker choices and allowing identifying the compromised networks. The additional keys are derived from IK' and CK' rather than from *IK* and *CK*. The manner of deriving Master Session Key (*MSK*), Extended *MSK* (*EMSK*), Transient Session Key (*TSK*), Authentication Key (K_{auth}), and Encryption Key (K_{enc}) is considerably different as compared to the manner of derivation in the EAP-AKA protocol. The EAP-AKA′ protocol uses SHA-256 (256-bit hash) [12], which is stronger and more popular than SHA-1 (160 bits hash) [13] that is used in EAP-AKA.

More details about this protocol can be found in our previous work in [14].

3.3 Standard Fast EAP-AKA′ Re-authentication Protocol (FAKAP)

The 3GPP has specified fast re-authentication to reduce authentication delay and communication overhead between the HSS and other nodes [15]. To achieve this, the full EAP-AKA′ credentials are not used in fast re-authentication, and HSS is not involved. The protocol mechanism is started by sending a user identity request message from the AP to the UE. The UE replies with a response message that contains a re-authentication ID, which was derived in the previous full EAP-AKA′. For more details about this protocol, refer to our previous work in [14].

3.4 Related works

Recent studies of authentication and re-authentication protocols in the heterogeneous networks [16, 17], and [18] are designed based on the EAP-AKA protocol [19].

However, they still suffer from UID and LNAS attacks. In literature, many studies such as [20] and [21] have been proposed to solve the limitations of EAP-AKA and improve the handover process. However, they are based on asymmetric key methods that might require additional processing capability in the UE. Moreover, other methods require modification in the architecture or adding new entities. For LTE networks, the enhanced protocol in [22] has solved the problem of UID attack, but it has been designed for non-trusted wireless networks. In addition, it has not been designed for handover process. The work in [4] can be used with minor modification to perform the authentication process with untrusted networks, since it has a tunnel phase that can protect the rest of the protocol procedure. However, it has not been designed for handover process. This work presents authentication and re-authentication protocols that overcome the aforementioned limitations. The details of the proposed protocols are in the next section. The work in [23] has proposed authentication and re-authentication protocols to reduce the delay and cost; however, handovers to LTE network have not been considered. In [24], another authentication method called EAP-CRA has been proposed for different wireless networks such as WLAN, WiMAX, and LTE networks. A single set of credentials is used with any network, which reduces the time of authentication and reduces the messages exchanged between entities. However, many channels between nodes are assumed to be secure; thus, this method could be vulnerable to many attacks when it is implemented. In addition, it needs modifying the network infrastructure, which makes it difficult to be implemented. In [25] and [26], efficient group-based authentication and re-authentication protocols for 5G networks and Wireless Mesh Networks (WMN) have been proposed. However, they are limited to LTE-WLAN interworking and WMN, respectively.

4 Proposed authentication protocols

The proposed protocols have many features that make them more secure and faster than others. These features makes them good substitute for the 4G and the next 5G generation. In the proposed protocols, the signaling between UE and the AS in the home network is reduced. This is achieved by employing the delegation concept in the re-authentication processes [27]. The AS performs a full authentication protocol with UE during the first connection. In the next authentication process, when the UE requires reconnection to the same network, the AS delegates the re-authentication and key distribution process to the local server in the serving network.

The HSS server maintains the database of users and other network entities such as APs/BSs/eNBs, GWs, and AAA servers. A part of this database is a table that contains the IDs of UEs, the corresponding keys, and the *IMSI*. This mechanism takes some concepts from the Kerberos method [28].

In the beginning of the authentication process, the UE is not required to send its *IMSI* or to perform encryption operations to protect its identity. Instead, the user sends its ID and *ANID* in a clear text. According to the received ID, the HSS retrieves the key and *IMSI*. *ANID* is used by HSS to derive the appropriate keys for the specified network. A unified key hierarchy for the LTE-WLAN-WiMAX architecture is proposed in the next section.

4.1 Unified key hierarchy

A unified key hierarchy is proposed to be applied in each network type in the interworking architecture. For instance, in WLAN networks, the *MSK* and *EMSK* are required to be sent to UE and AS; in WiMAX networks, the Pairwise Master Key (*PMK*) and Authorization Key (*AK*) are required to be sent to BS and derived in MS; in LTE networks, the K_{eNBs} key is required to be sent to eNB and derived in UE. In addition, the Master Key (*MK*) is corresponding to K_{ASME}, which is used in EPS-AKA. The K_{ASME} key is derived using *IK*, *CK* while *MK* is derived using *IK′*, *CK′*. The unified key hierarchy includes all keys that are required for each network type. Figure 2 illustrates the unified key hierarchy.

Two-level keys are proposed, one for re-authentication, which its name ends with "*r*" and the other for handover, which its name ends with "*h*." Separation between re-authentication and handover keys is useful to provide a higher level of control on different security values [23]. This concept is applied as part of the new key hierarchy that is proposed in this work with modification to be suitable for EAP-AKA′ protocol. The key hierarchy of EAP-AKA′ authentication protocol [1] is adapted to be applied on key derivation in LTE and WiMAX authentication protocols. The keys in the proposed protocols are named based on the type of network and handover. For example, in the name of key NLK_r, "*N*" denotes to WLAN network, "*L*" denotes that it is used locally, and "*r*" denotes that it is used for the re-authentication process.

The Message Authentication Code (*MAC*) messages are also named based on the network and the protocol type. For example, in the following name of *MAC* message $ANMAC_{WU}$, "*A*" denotes to intra handover, "*N*" denotes to WLAN networks, and "*WU*" meaning that the message originated in the WAAAS is intended to UE. In addition, the challenge messages are also named in the same way. For instance, in the challenge

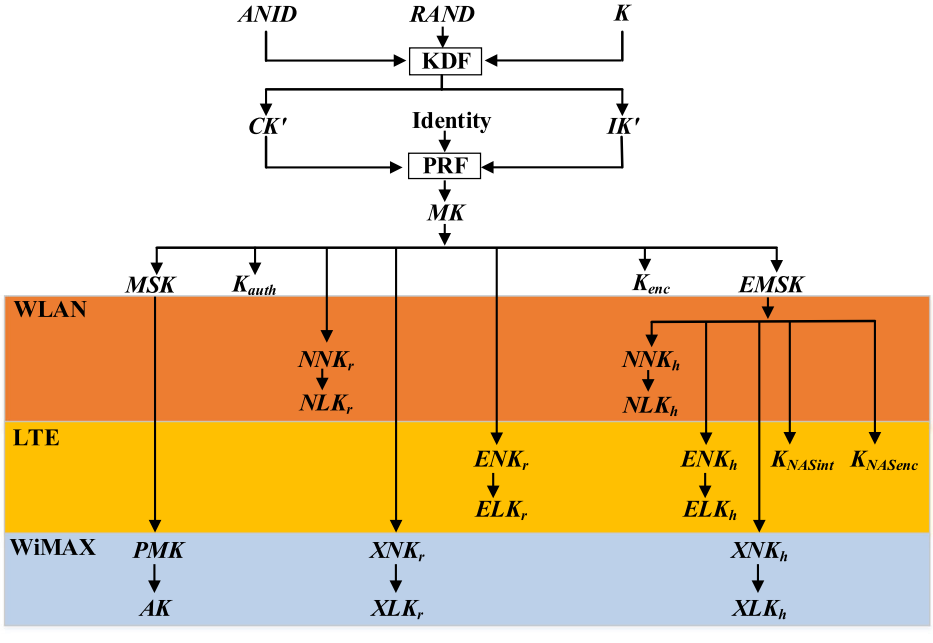

Fig. 2 The unified key hierarchy

message "*RX3PC*," "*R*" denotes to inter handover, "*X*" denotes to WiMAX networks, and "*3P*" meaning that the challenge message originated in the 3AAAS is intended to PAAAS.

Unlike the standard protocols, *EMSK* key is used to derive two-level handover keys for WLAN networks, handover WLAN Network level Key (NNK_h), and handover WLAN Local level Key (NLK_h). The same two-level keys are derived from *EMSK* in the case of WiMAX or LTE networks. The keys, *MSK*, K_{auth}, K_{enc}, K_{re}, and *EMSK* are derived from *MK* as in the standard key hierarchy. The re-authentication key K_{re} is modified to be re-authentication WLAN Network level Key NNK_r and re-authentication WLAN Local level Key NLK_r. The same two-level keys in the case of WiMAX or LTE networks. For space reasons, the keys K_{auth} and K_{enc} are named K_a and K_e, respectively, in the rest of this paper. In the following sections, the proposed set of authentication and re-authentication protocols is presented.

4.2 Protocols for handover to WLAN networks

This section presents the enhanced EAP-AKA′ protocol and the new re-authentication protocols such as the inter and intra WLAN re-authentication protocols.

4.2.1 Enhanced EAP-AKA′ Protocol (EAKAP)

The EAKAP protocol is invoked upon the following cases, if the UE connects to the WLAN for first time, the timer is expired, or if the number of re-authentications exceeds, the number of allowed re-authentication processes (n_R).

Additional keys are generated in this protocol to be used in the inter and intra WLAN re-authentication protocols. This section presents the modifications that have been applied to this protocol. These modifications aim to reduce the communication between UE and HSS and to improve the security aspects using an efficient key exchange method.

To prevent the UID attack, the IMSI is not sent by UE, instead a temporary ID, which is called user ID (UE_{ID}) is sent by the UE to the HSS. The HSS maintains a table that contains UE_{ID} for each UE, corresponding *IMSI*, the pre-shared key *K*, and an extra field to store nonces that are received from UE. In the first authentication procedure, when the HSS receives the message that contains the UE_{ID} and nonce of UE, it finds the corresponding *K* and *IMSI*. The key *K* is used to generate the Authentication Vector (*AV*). At the end of EAKAP protocol, a new re-authentication id is generated to be used in the next re-authentication process.

In addition, a new key hierarchy for the enhanced EAP-AKA′ protocol is proposed as part of the unified key hierarchy to handle the different types of HO protocols. Unlike EAP-AKA, a key for re-authentication K_{re} is derived in EAP-AKA′ from *MK* key. In the proposed key hierarchy, K_{re} is considered as a re-authentication key for network level. It is named WLAN Network level Key for re-authentication (NNK_r), and the handover keys are derived from the *EMSK* key. The details of key derivation are provided in the protocol steps. Figure 3 shows the enhanced EAP-AKA′ protocol. For space reasons, the only proposed mechanism is clarified in the following steps:

- The UE sends a user response identity message to the WAAAS. This message contains its ID UE_{ID}, *ANID*, and its nonce for the current authentication i (R_{U_i}), then, the WAAAS attaches its nonce R_{W_i} and forwards the message to HSS through the 3AAAS.

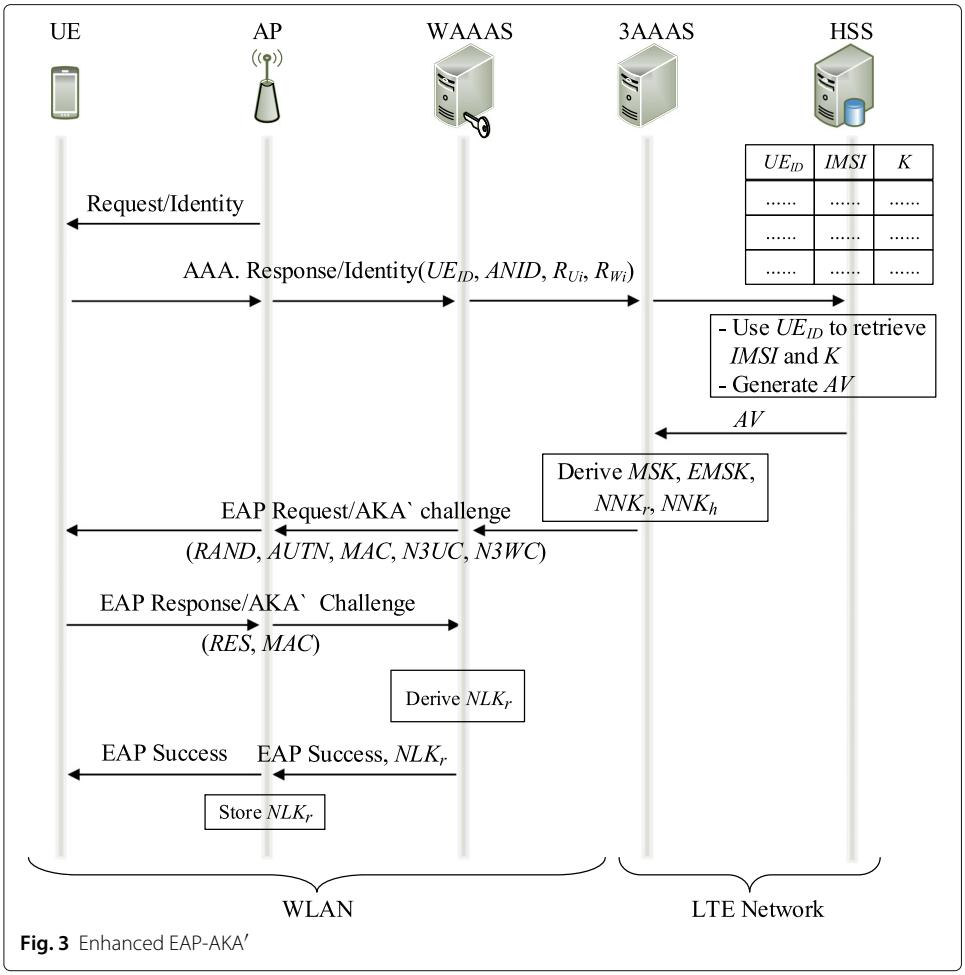

Fig. 3 Enhanced EAP-AKA′

- The HSS uses the UE_{ID} to retrieve the *IMSI* and the keys of the UE and WAAAS.
- After that, HSS generates the AV and sends it to the 3AAAS, which generates the keys K_e, K_a, K_{re}, *MSK*, and *EMSK*, then it attaches those keys in a challenge message to WAAAS (*N3WC*) using Eq. (1). The challenge message indicates that the 3AAAS delegates and provides the WAAAS with the key materials to perform the rest of the authentication process. The main part of the message contains Random number (*RAND*), Authentication Token (*AUTN*), *MAC*, and a challenge from the 3AAAS to UE (*N3UC*) as follows:

$$\begin{aligned} N3UC &= \{R_{W_i}, n_{AR}, n_R\}_{K_e} \\ N3WC &= \{K_e, K_a, NNK_r, NNK_h, MC_R, n_{AR}\}_{K_{3W}}, \end{aligned} \tag{1}$$

where MC_R is the maximum value of the counter of re-authentication process (C_R), n_{AR} is the number of allowed intra re-authentication processes, and K_e, K_a, and NNK_r are derived from *MK*. Those keys are substrings of bits [0..127], [128..383], and [384..639], respectively. The key NNK_h is derived using Eq. (2). In this paper, NNK_r and NNK_h are the network level keys for re-authentication and handover, respectively.

$$NNK_h = F(EMSK, |R_{W_i}|W_{ID}|MSM|\text{“}NNKh\text{”}, 256), \tag{2}$$

where F is a key derivation function [19], MSM is the UE address in MAC layer, "$NNKh$" is the key label, W_{ID} is the ID of WAAAS, and 256 is the key length in bits.

- The WAAAS forwards $RAND$, $AUTN$, MAC, and $N3UC$ to UE and stores $N3WC$.
- When UE receives the message, it checks MAC. If the checking process is successful, it derives the required keys. After that, the UE computes the RES and MAC and sends them in the EAP response challenge message to WAAAS.
- Upon receiving the message, WAAAS checks MAC and compares the Expected Response ($XRES$) with the RES value that has been sent from UE. If the checking process is successful, it generates NLK_r using Eq. (3), then it sends it along with the successful message to AP.

$$NLK_r = F(NNK_r, C_{AR}|AP_{ID}|MSM|\text{“}NLKr'', 512) \tag{3}$$

where C_{AR} is the counter of intra re-authentication process and AP_{ID} is the ID of AP.

- AP stores the NLK_r key and forwards the message to UE, which starts to derive the NLK_r key.
- UE and WAAAS derive a WLAN Re-authentication Identity ($NRID_i$), which is used for the next re-authentication process. $NRID_i$ is derived as follows:

$$NRID_i = SH(NNK_r, NNK_h|R_{U_i}), \tag{4}$$

where SH is a secure hash function.

4.2.2 Inter WLAN Re-authentication Protocol (RNRP)

To reduce the overhead on the HSS server, the 3AAAS performs the RNRP protocol on behalf of the HSS server using the key materials that have been sent from HSS server during the previous EAKAP protocol. The RNRP is performed when the user needs an HO to a new WLAN network domain in the interworking environment. After executing the RNRP protocol in a WLAN domain, RNRP gives permission and prepares the key materials to UE and WAAAS for future Intra handover within this domain. Figure 4 and the following steps describe this protocol.

- The UE sends the $NRID_{i-1}$ to WAAAS. $NRID_{i-1}$ has been derived using Eq. (4) in the previous EAKAP protocol.
- Upon receiving the message, WAAAS validates $NRID_{i-1}$ to check whether the UE has previously visited this domain or not. Then, it forwards $NRID_{i-1}$ along with its nonce R_{W_i} to the 3AAAS. R_{W_i} will be sent to UE, which will send it again to WAAAS in the future re-authentication process. Thus, the WAAAS can verify the UE.
- The 3AAAS computes its MAC, which is intended to UE $RNMAC_{3U}$ and a challenge ($RN3UC$) to UE as shown in Eq. (5).

$$\begin{aligned} RNMAC_{3U} &= SH(K_a, NRID_i|R_{U_{i-1}}|R_{W_i}) \\ RN3UC &= \{NRID_i, n_{AR}, R_{W_i}\}_{K_e} \end{aligned} \tag{5}$$

Note that the value $R_{U_{i-1}}$ is the nonce of UE that has been sent by UE to the 3AAAS in the previous EAKAP protocol. When UE receives this nonce, it can verify the 3AAAS. Each time the C_R exceeds n_{AR}, the full authentication EAKAP is invoked.

- After that, it prepares a delegation message, which is intended to WAAAS containing MC_R, n_{AR}, NNK_r, and NNK_h. This message will be used in the future ANRP

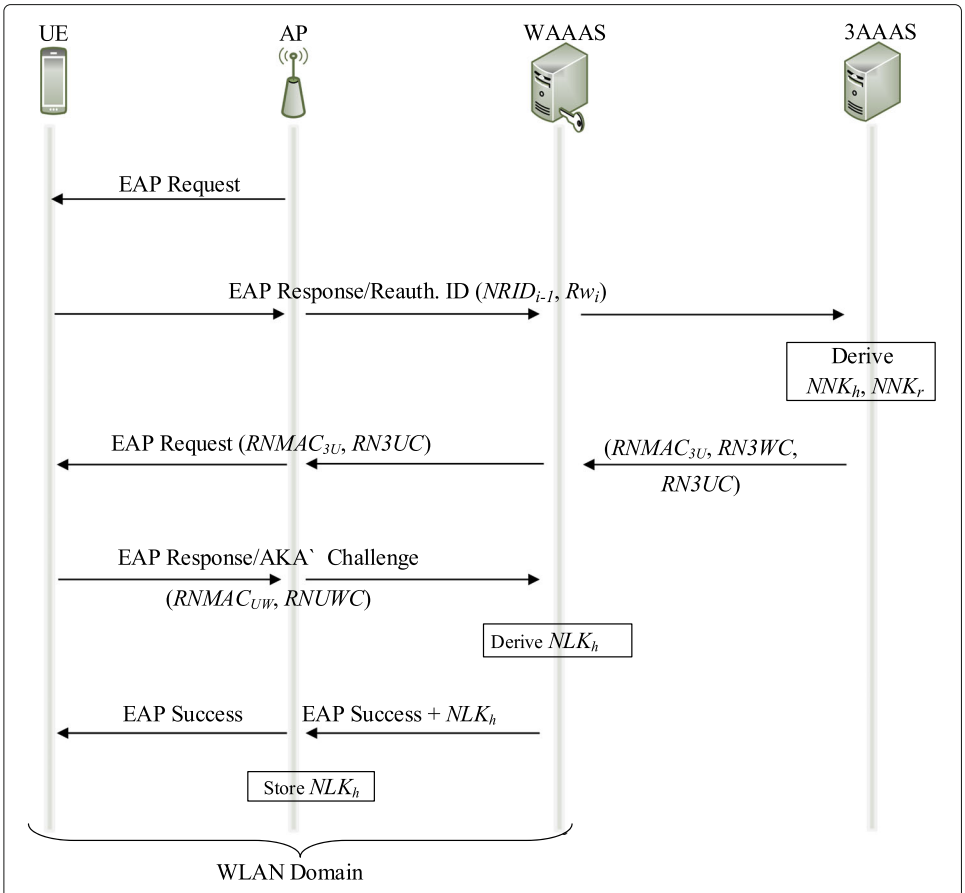

Fig. 4 Inter WLAN re-authentication protocol

protocol, and it is encrypted by the shared key between WAAAS and 3AAAS K_{3w} using Eq. (6). Then, it sends it along with $RNMAC_{3U}$ and $RN3UC$ to WAAAS.

$$RN3WC = \{K_e, K_a, NNK_r, NNK_h, MC_R, n_{AR}\}_{K_{3W}} \tag{6}$$

- The WAAAS stores $RN3WC$ and forwards $RNMAC_{3U}$ and $RN3UC$ to UE via AP.
- When UE receives $RNMAC_{3U}$, it checks the values and computes its MAC, which is named as $RNMAC_{UW}$ and a challenge to WAAAS $RNUWC$ as shown in Eq. (7).

$$\begin{aligned} RNMAC_{UW} &= SH(K_a, R_{W_{i-1}} | R_{U_i} | C_R) \\ RNUWC &= \{R_{U_i}, C_R\}_{K_e} \end{aligned} \tag{7}$$

- Then, the UE sends $RNMAC_{UW}$ along with $RNUWC$ to WAAAS.
- When WAAAS receives the message, it verifies $RNMAC_{UW}$ by checking the value of $R_{W_{i-1}}$ that has been sent from 3AAAS to UE in the previous EAKAP protocol. In case of successful verification, it derives NLK_r key using Eq. (8) and sends it in the EAP success message to AP.

$$NLK_h = F(NNK_h, C_{AR} | AP_{ID} | MSM | \text{“}NLKh\text{”}, 512) \tag{8}$$

- Finally, the AP stores the NLK_h key and forwards the message to UE, which starts to derive NLK_h that is used to protect messages between UE and AP.

4.2.3 Intra WLAN Re-authentication Protocol (ANRP)

Instead of using standard fast re-authentication protocol, the ANRP is performed when the user moves within the same WLAN domain or to another domain in the interworking environment that was previously visited. Figure 5 and the following steps describe this protocol.

- The UE sends the previous $NRID_{i-1}$ to WAAAS.
- WAAAS receives $NRID_{i-1}$, then it checks the value of counter C_{AR} to ensure that it does not exceed the n_{AR}. If the checking is successful, it generates $ANMAC_{WU}$ and a challenge $ANWUC$ as shown in Eq. (9), then it sends it along in the challenge message to UE.

$$\begin{aligned} ANMAC_{WU} &= SH(K_a, R_{W_i}|C_{AR}) \\ ANWUC &= \{C_{AR}, R_{W_i}\}_{K_e} \end{aligned} \tag{9}$$

- When UE receives the message from WAAAS, it verifies the challenge, and it matches the value of counter C_{AR} with the stored value. If it matches, it generates $ANMAC_{UW}$ and a challenge $ANUWC$ as shown Eq. (10), then it sends it along in the EAP response challenge message.

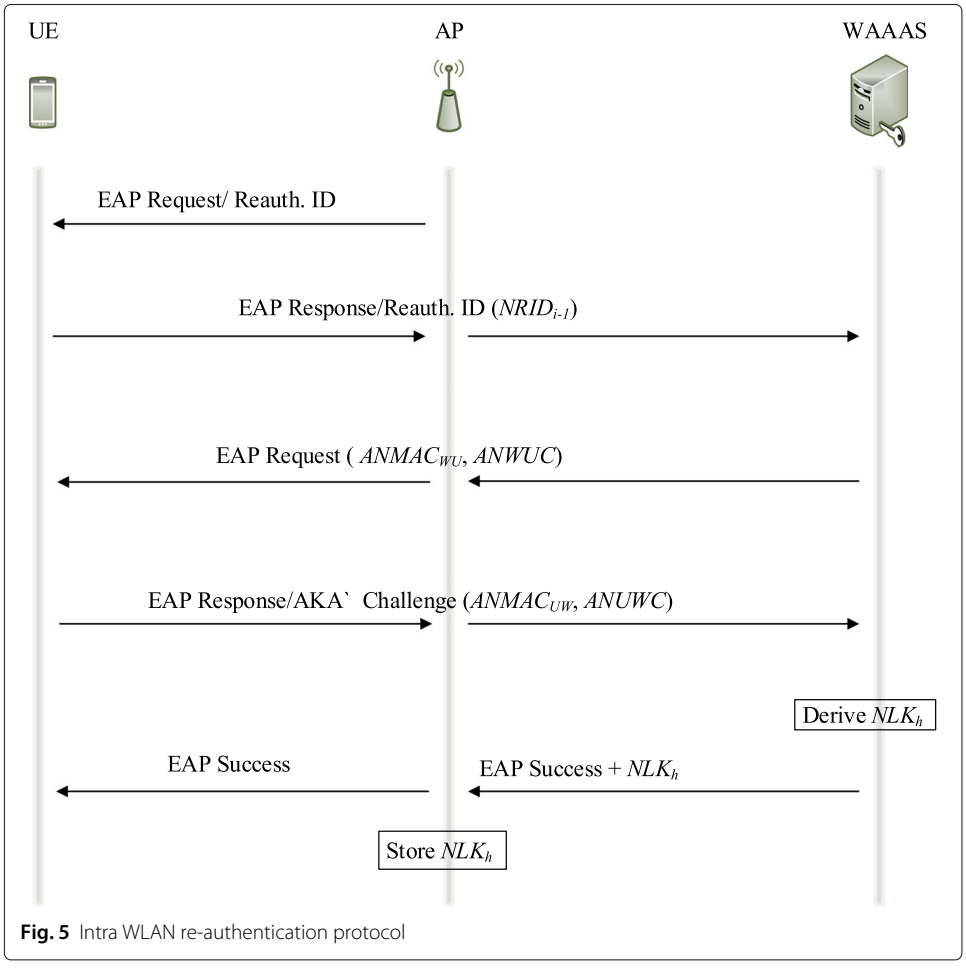

Fig. 5 Intra WLAN re-authentication protocol

$$ANMAC_{UW} = SH(K_a, R_{W_i}|C_{AR}|C_R)$$
$$ANUWC = \{C_{AR}, C_R, R_{W_i}\}_{K_e} \quad (10)$$

- The WAAAS checks whether the received C_{AR} matches the C_{AR} sent in the previous message or not. If it matches, it verifies the received *MAC*. If the verification is successful, it increments the counter C_{AR} and derives NLK_h key and sends it with EAP success message to AP.
- Upon successful authentication, the counters C_{AR} and C_R in UE are increased by 1. The UE starts deriving the NLK_h key.

4.3 Protocols for handover to WiMAX networks

The INEA protocol has been specified by WiMAX Forum in [29] and [30] to provide mutual authentication between mobile station (MS) and 3AAAS in the 3G-WiMAX interworking architecture. This section presents the enhanced INEA protocol, the inter, and intra WiMAX re-authentication protocols.

4.3.1 Enhanced INEA Protocol (EINEAP)

The EINEAP is performed if the UE connects to the WiMAX for first time. It is also performed if the timer is expired or if the number of re-authentication processes exceeds the n_R. Otherwise, the re-authentication protocols of WiMAX are invoked. The INEA protocol starts when the user receives the request identity message from ASN-GW. The rest of the protocol steps are illustrated in Fig. 6 and summarized as follows:

- The UE sends UE_{ID}, R_{U_i}, and *ANID* to ASN-GW via BS. When ASN-GW receives EAP response identity message from UE, it attaches its nonce R_{Gi} and forwards the message to HSS through PAAAS and 3AAAS.
- When the 3AAAS receives the message, it stores the nonces and forwards the other values to HSS in AV request message.
- The HSS uses the received IDs to retrieve the shared keys and *IMSI* of the user. It uses the user key K to generate the AV and sends it along with the retrieved keys to the 3AAAS.
- The 3AAAS generates the network re-authentication level key from the *MK* key. In this protocol, this key is called re-authentication WiMAX Network level Key (XNK_r). In addition, the 3AAAS generates the handover key XNK_h as illustrated in Eq. (11). It delegates the rest of the authentication to PAAAS by sending the derived keys to PAAAS in a challenge message, which is encrypted by the shared key between 3AAAS and PAAAS as shown in Eq. (12).

  $$XNK_h = F(EMSK, R_{G_i}|G_{ID}|MSM|\text{“}XNKh\text{”}, 256) \quad (11)$$

  where G_{ID} is the ID of GW.

  $$X3PC = \{K_{3G}, K_e, K_a, n_{AR}, XNK_r, XNK_h, MC_R\}_{K_{3P}} \quad (12)$$

  It also generates a challenge message to UE as shown in Eq. (13).

  $$X3UC = \{R_{G_i}, n_{AR}, n_R\}_{K_e} \quad (13)$$

- The 3AAAS sends *RAND*, *AUTN*, *MAC*, *X3UC*, and *X3PC* to the PAAAS in the request AKA challenge message. The PAAAS then forwards *RAND*, *AUTN*, *MAC*, and *X3UC* challenge to UE and stores *X3PC* challenge.

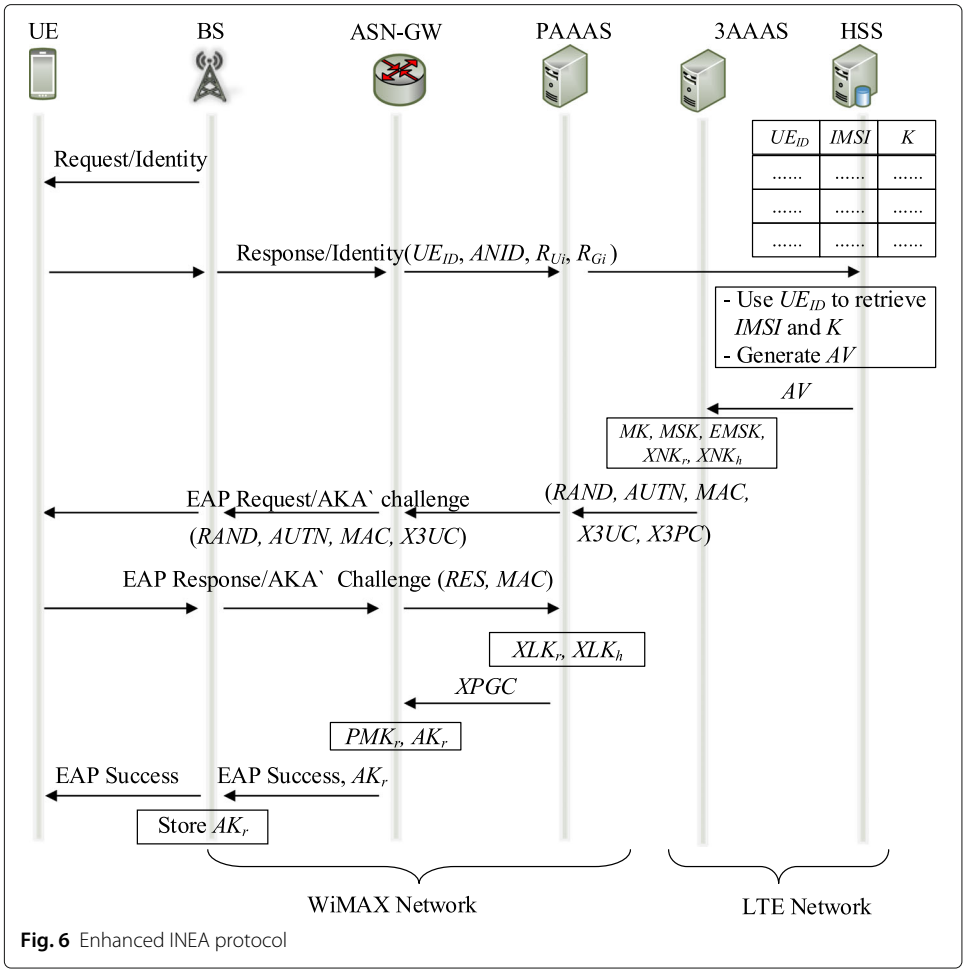

Fig. 6 Enhanced INEA protocol

- When UE receives the message, it verifies *MAC*. In the case of successful verification, it computes the *RES* and its *MAC*. Then, the UE sends those values in the response AKA challenge message to the PAAAS.
- When the PAAAS receives the message, it verifies the received values, then it generates WiMAX local re-authentication keys XLK_r and XLK_h using Eq. (14) and uses them with MC_R and n_{AR} to generate a challenge message that is intended to ASN-GW using Eq. (15). This challenge message is called *XPGC*, and it is encrypted using K_{3G} that is retrieved from *X3PC*, then it sends it to ASN-GW in the EAP success message. It sets the value of C_{AR} according to the received n_{AR} value.

$$\begin{aligned} XLK_r &= F(XNK_r, C_{AR}|BS_{ID}|MSM|\text{“}XLKr'', 512) \\ XLK_h &= F(XNK_h, C_{AR}|BS_{ID}|MSM|\text{“}XLKh'', 512) \end{aligned} \tag{14}$$

where BS_{ID} is the ID of BS.

$$XPGC = \{XLK_r, XLK_h, MC_R, n_{AR}, K_e, K_a\}_{K_{3G}} \tag{15}$$

- Then, the ASN-GW uses the received local level keys to compute PMK_r and AK_r using Eqs. (16) and (17), and it sets the counter C_{AR} according to the n_{AR} value.

$$PMK_r = TF(XLK_r, 160), \tag{16}$$

where TF is the truncate function used in [31].

$$AK_r = F(PMK_r, C_{AR}|BS_{ID}|MSM|\text{“}AKr'', 160) \tag{17}$$

- After that, the ASN-GW sends the AK_r key with the success message to BS, which forwards the message to UE and stores the AK_r key.
- The UE and ASN-GW derive a WiMAX Re-authentication Identity ($XRID_i$), which is used for the next re-authentication process as follows:

$$XRID_i = SH(XNK_r, XNK_h|R_{U_i}) \tag{18}$$

4.3.2 Inter WiMAX Re-authentication Protocol (RXRP)

The RXRP is performed when the user needs to perform an HO from WLAN or LTE domain to a BS in WiMAX domain for the first time. The RXRP protocol has the same mechanism of RNRP except that the challenges and keys generated are dedicated for WiMAX networks.

4.3.3 Intra ASN WiMAX Re-authentication Protocol (AXRP)

AXRP is performed when the user is moving from a BS to another one within the same domain or moving to a previously visited ASN-GW. The ASG-GW will authenticate the UE on behalf of the 3AAAS using the keys and values that have been received in the previous EINEAP. The AXRP protocol has the same mechanism of ANRP except that the challenges and keys generated are dedicated for WiMAX networks.

4.4 Protocols for handover to LTE networks

This section presents the enhanced EPS protocol and the inter and intra LTE re-authentication protocols.

4.4.1 Enhanced EPS Authentication Protocol (EEPSP)

In this work, the EPS-AKA protocol is enhanced to be used for trusted wireless networks. The networks involved in this work are considered as trusted networks, since WiMAX uses licensed radio spectrum and WLAN uses 802.1x—based authentication, which requires encryption and uses EAP-based authentication [32]. The EEPSP is designed to be appropriate for the subsequent types of handovers. It is invoked when the user connects to LTE for the first time. It is also invoked when the timer is expired or the number of re-authentication processes using the same key materials exceeds the n_R. The entities involved in this protocol are MME, 3AAAS, and HSS servers. As mentioned in the previous section, the unified key hierarchy is also adapted to be suitable for LTE networks. The protocol mechanism is illustrated in Fig. 7 and in the following steps:

- The UE sends UE_{ID}, R_{U_i}, and $ANID$ to HSS via MME.
- When MME receives the EAP response identity message from UE, it attaches its nonce R_{M_i} and forwards the message to HSS.
- The HSS uses UE_{ID} to retrieve $IMSI$ and the pre-shared key K. It uses K to generate the AV and sends it to the 3AAAS.
- Then, the 3AAAS generates MSK, $EMSK$, and K_{eNB}. The K_{eNB} key is derived from MK key using Eq. (20). It is considered as network level re-authentication key, and it is named LTE Network level Key for re-authentication (ENK_r) in this protocol. The 3AAAS also generates LTE Network level Key for handover (ENK_h) using Eq. (20).

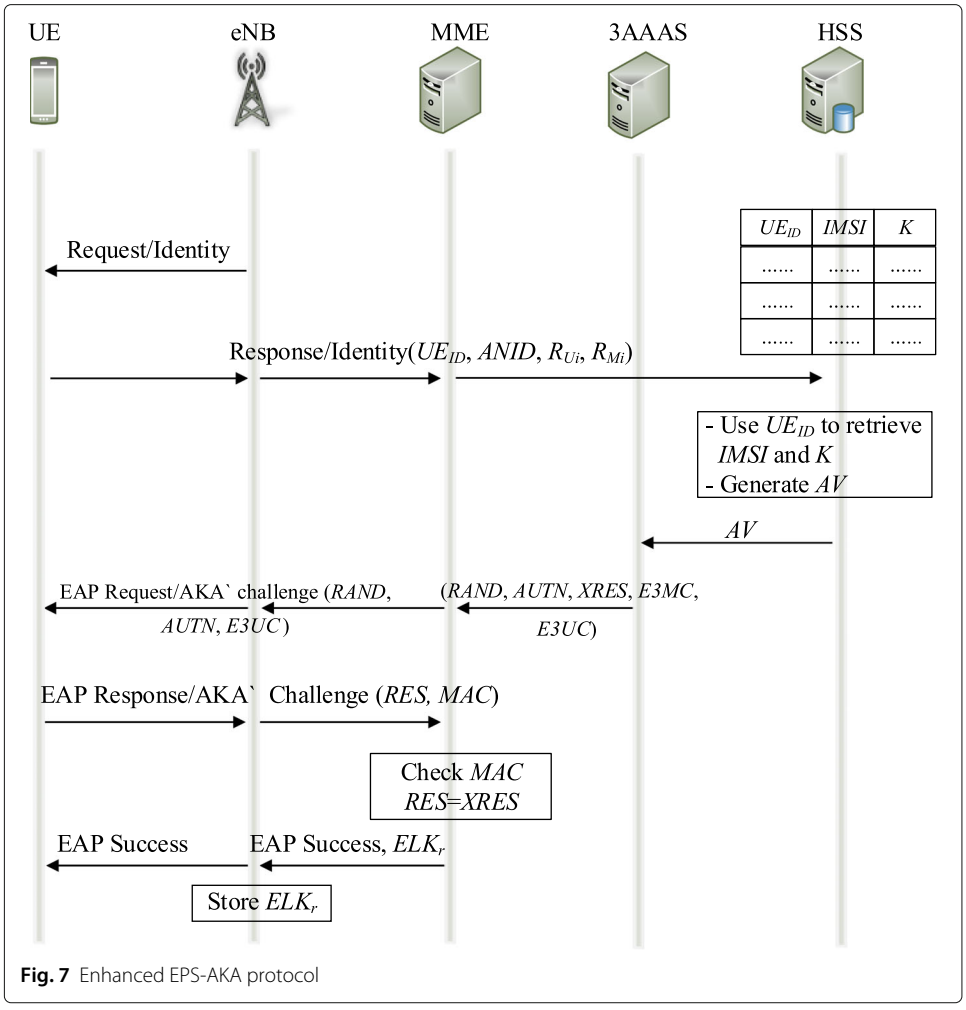

Fig. 7 Enhanced EPS-AKA protocol

- After that, the 3AAAS delegates the rest of the authentication process to MME by sending the derived keys to MME. The keys K_{NASint} and K_{NASenc} are derived from *EMSK* key [33] using Eq. (19). In this protocol, the ENK_r key and C_{AR} counter correspond to the *NH* key and *NCC* counter used in the standard protocol.

$$K_{NASint}|K_{NASenc} = PRF(EMSK), \tag{19}$$

where *PRF* is a pseudo-random function. These keys are used to protect the data in the Non-Access Stratum (NAS) layer.

$$\begin{aligned} ENK_r &= MK[\,384..639] \\ ENK_h &= F(EMSK, R_{M_i}|M_{ID}|MSM|\text{“}ENKh\text{”}, 256) \end{aligned} \tag{20}$$

In addition, the 3AAAS generates challenges to MME and UE using Eq. (21) as follows:

$$\begin{aligned} E3UC &= \{R_{M_i}|n_{AR}|n_R\}_{K_e} \\ EEMC &= \{K_{eNB}|ENK_h|MC_R|n_{AR}\}_{K_{EM}} \end{aligned} \tag{21}$$

- The 3AAAS also extracts *RAND* and *AUTN* from the received *AV* and sends them along with *E3UC* and *EEMC* to MME in the request AKA challenge message. The

MME then, forwards *RAND*, *AUTN*, *MAC*, and *E3UC* challenge to UE and stores *EEMC* challenge.

- The UE verifies *MAC*. In the case of successful verification, it computes the *RES* and its *MAC*.
- Then, the UE sends the computed values in the response AKA challenge message to MME.
- When the MME receives the message, it verifies the received *MAC* and *RES*. In case of successful verification, it generates LTE Local level keys for re-authentication and handover ELK_r using Eq. (22), then it sends ELK_r along with the successful message to eNB.

$$ELK_r = F(ENK_r, C_{AR}|eNB_{ID}|MSM|\text{“}ELKr'', 512) \tag{22}$$

- When eNB receives the message, it stores the ELK_r key and forwards the message to UE, which starts to derive the keys.
- Finally, the UE and MME derive LTE re-authentication identity ($ERID_i$), which is used for the next re-authentication process as follows:

$$ERID_i = SH(ENK_r, ENK_h|R_{U_i}) \tag{23}$$

4.4.2 Inter LTE Re-authentication Protocol (RERP)

The RERP is performed when the user moves to another MME within the same domain. It is also performed when the user performs an HO from WiMAX or WLAN networks to LTE network. The mutual authentication between the 3AAAS and UE is done without the need to communicate with HSS. In this protocol, the 3AAAS delegates the MME to perform the future re-authentication process. The RERP protocol has the same mechanism of ANRP except that the challenges and keys generated are dedicated for LTE networks.

4.4.3 Intra LTE Re-authentication Protocol (AERP)

The AERP is invoked when the user is roaming from eNB1 to eNB2 within the same LTE domain or performing an HO from other networks to a previously visited LTE domain. In AERP, the mutual authentication is done between UE and MME without the need to communicate with 3AAAS or HSS servers. MME uses the key materials that have been received when RERP was invoked. The AERP protocol has the same mechanism of ANRP except that the challenges and keys generated are dedicated for LTE networks.

5 Security analysis

5.1 Security features and robustness

In this section, the security properties of the proposed protocols are analyzed to demonstrate that the proposed protocols can satisfy the security requirements [34] and [35].

5.1.1 Mutual authentication

Full/fast EAP-AKA, INEA, and EPS-AKA authentication/re-authentication protocols achieve mutual authentication between UE and the 3AAAS server. The proposed authentication protocols provide a secure mutual authentication to prevent several attacks such as MITM, impersonation, and rogue AP/BS attacks. In the local re-authentication protocols, the 3AAAS server delegates the authentication operation to the local servers WAAA, PAAA, and MME. The local servers and UE mutually authenticate each other by checking

their *MACs* and proving that they have the correct nonces and counters. The legitimacy of local servers WAAA, PAAA, and MME is verified by checking their counters C_R and C_{AR}. The UE matches the received counters with the counters stored in its database. Successful matching indicates that the keys K_e and K_a that are used to encrypt counters and *MAC* are valid. In the same way, the local servers authenticate UE by checking the counters and *MACs*, since only the legitimate UEs can generate the keys K_e and K_a.

5.1.2 Protection of message integrity

MAC is appended with the authentication challenges/response messages that are exchanged between UE and AS in the interworking environment. It protects the integrity of those messages. In addition, it provides authentication for the sender. The sender of *MAC* attaches the previous nonce of the receiver in its *MAC*, then the receiver can authenticate the sender by checking that nonce. For example, in RERP protocol, UE receives the nonce of MME during the previous authentication process, which was called R_{M_i}. In the current authentication process, UE includes that nonce of MME, which is called $R_{M_{i-1}}$ in its *MAC* ($REMAC_{UM}$); thus, MME authenticates UE by checking this nonce.

5.1.3 Identity protection

Concealing the UE's identity helps to prevent UID attack. Most recent solutions use temporary identities to conceal the *IMSI*; however, *IMSI* is still sent in the full authentication process, which makes them vulnerable to UID attack. In the proposed protocols, the *IMSI* is not sent, instead, a temporary user identity UE_{ID} is sent in the full authentication process and re-authentication identity RID is computed and sent in the next re-authentication process. When the HSS receives UE_{ID}, it uses it as a pointer to retrieve the *IMSI* and the pre-shared key. In the full authentication and the subsequent re-authentication processes, UE and local servers must derive new ID using Eqs. (4), (18), and (23), since those IDs are only used for a single authentication process.

In the standard full authentication protocols, the 3AAAS server must generate a re-authentication ID that will be used for future fast re-authentication process. Whereas in the proposed protocols, the 3AAAS server is exonerated from computing and saving the re-authentication IDs. In addition, the re-authentication IDs are not encrypted in the proposed protocols, instead, those IDs are sent in clear text since they will not be used in the future re-authentication process.

5.1.4 Forward and backward secrecy

In the proposed protocols, the shared keys are desired to be different in each communication session to achieve one of the security requirements, which is the key freshness. After each handover process, fresh keys are computed using fresh nonces. This property also helps in limiting the number of cipher texts that can be used by some attackers. In addition, the proposed protocols provide a perfect forward and backward secrecy and prevent domino effect attacks [36]. The UE and AP/BS/eNB compute and share fresh keys K_i, which can only be used in the ith authentication process. Those keys cannot be used to decrypt messages in the previous authentication process ith-1, which provide backward secrecy. In addition, any messages exchanged in the ith+1 authentication process cannot be decrypted by those keys, which provide forward secrecy. The UE and local

servers derive network level keys *NNK*, *XNK*, and *ENK*. Those keys are computed using fresh nonces R_w, R_G, and R_M in Eq. (2), (11), and (20), respectively. This guarantees the freshness of all keys that will be computed from *NNK*, *XNK*, and *ENK* keys. In the intra re-authentication protocols, local keys *NLK*, *XLK*, and *ELK* are derived from *NNK*, *XNK*, and *ENK*, respectively. These local keys are different from the local keys in the previous intra re-authentication process. They are fresh as well since they are derived using new counter C_{AR}.

5.2 Verifying the proposed protocols

The proposed protocols are validated using one of the well known analytical tools for checking the secrecy of authentication protocols, the Automated Validation of Internet Security Protocols and Applications (AVISPA) tools [37, 38]. The AVISPA tools consider all types of attacks that target the network security protocols. It uses the High Level Protocol Specification Language (HLPSL) to allow specifying security protocols to find possible attacks. The protocol's behavior is analyzed and certain goals are checked using several back-ends. Generally, there are several back-ends defined by AVISPA, and they can be freely chosen to execute the HLPSL code after it is translated by HLPSL2IF into an Intermediate Format (IF).

In this work, each description of the proposed protocols is written using HLPLS language. Then, the On-the-fly Model-Checker (OFMC) and Constraint-Logic based Attack Searcher (CL-ATSE) back-ends are used to verify those protocols. This is mainly due to their interesting features such as supporting various security protocols, checking whether the verified protocol is able to provide strong authentication, and secrecy. The most important feature is proving the lack of security in the protocol rather than proving its security. The complete protocol description contains several parts. First, the function *role A*, which describes the behavior of the party A during the protocol session. The function *role session* is composed of each party's role. The function *role environment* describes the protocol execution under attack. Finally, the authentication requirements are defined in the part of *goals*.

All proposed authentication and re-authentication protocols are separately coded and verified by AVSPA tools. As an example, the code, simulation, goals, and results of RNRP protocol are presented in this section. The role of the UE and the goals that need to be verified are excerpted from the complete code and illustrated in Fig. 8. The goals that need to be verified are illustrated in Fig. 9. The run simulation of RNRP protocol is shown in Fig. 10. In this work, both authentication and secrecy goals are verified. The authentication goal is checked using the command *authentication_on rw1*. This indicates that when the UE sends its fresh nonce *rw1* to 3AAAS, it requires that the UE and the 3AAAS should agree on that nonce and exist in the current state. The secrecy goal is checked using the command *secrecy_of nnk1*, which indicates that the nonce nnk1 should be secreted and the intruder cannot learn such value. If the protocol is insecure or vulnerable to any authentication or secrecy attack, the result indicates that it is unsafe; otherwise, it is safe. Figure 11 shows the result of running the RNRP protocol using OFMC and ATSE tools, it shows that the protocol is safe.

```
role user_ue ( UE, WA : agent,
MSK, EMSK, Ka, Ke : symmetric_key)
RU,RW             : text,
NRID,WID,APID,CAR :text,
F1                : hash_func, %key gen. PRF
HMAC              : hash_func,
SND_UW,RCV_UW     : channel (dy))
played_by UE def=
local
MSM :text,
RNMAC3U    : hash(symmetric_key.text.text.text),
RNMACUW    : hash(symmetric_key.text.text.text),
NNKH, NNKR,
NLKH, NLKR : hash(symmetric_key.text.text),
State      : nat
const
request_id,respond_id,success : text,
nnk1 : protocol_id
init State := 1
transition
1. State  = 1 /\ RCV_UW(request_id) =|>
    State':= 5 /\ NRID' := new()
               /\ SND_UW(respond_id.NRID')
2. State  = 5 /\ RCV_UW({RW'}_Ke.RNMAC3U')
   /\ RNMAC3U' =HMAC(Ka.NRID.RU.RW') =|>
   State':= 9 /\ RU' := new()
   /\ RNMACUW' := HMAC(Ka.RU'.RW.CAR)
   /\ SND_UW({CAR}_Ke.{RU'}_Ke.RNMACUW')
   /\ request(UE,WA,rw1,RW')
   /\ witness (UE,WA,rw1,RW')
3. State  = 9  /\ RCV_UW(success) =|>
   State':= 13 /\ NNKH':= F1(MSK.RW.WID.MSM)
   /\ NLKH' := F1(NNKH.CAR.APID.NRID)
   /\ secret(NLK',nnk1,{UE,WA})
end role
```

Fig. 8 The UE rule in RNRP protocol

6 Performance evaluation results and discussion

In this section, the performance of the proposed protocols is evaluated and analyzed in terms of handover delay, key size, communication overhead, average handover cost, and energy consumption. These terms are important factors during handover process in the 4G and the next 5G networks. To do that, four different algorithms for the user

```
goal
   authentication_on rw1
   authentication_on rw2
   secrecy_of nnk1
   secrecy_of nnk2
end goal
```

Fig. 9 The goals in RNRP protocol

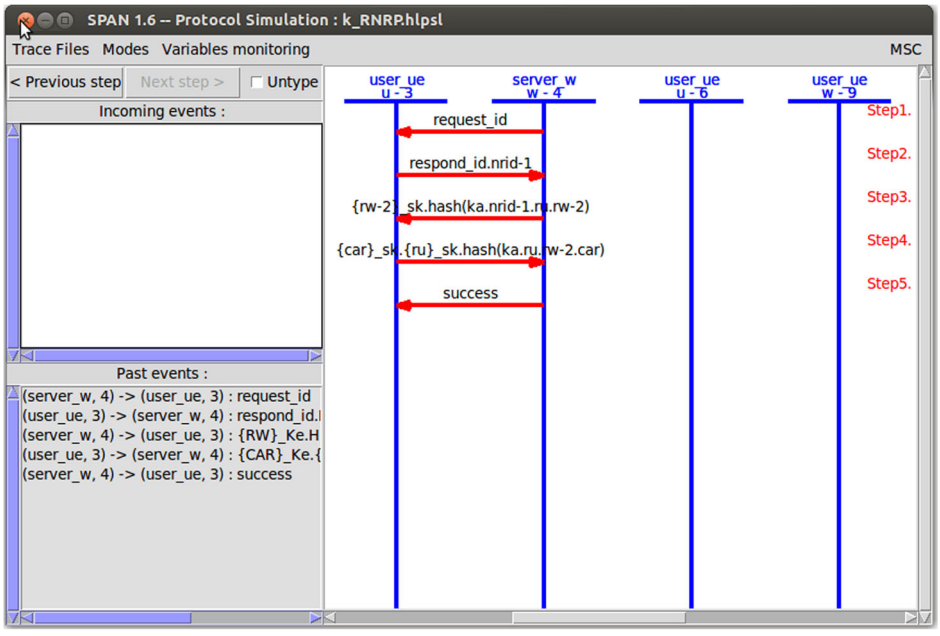

Fig. 10 The simulation of RNRP protocol

movements in the heterogeneous network environment are considered. Algorithm 1 (*A1*) represents the standard authentication protocols EAP-AKA′, INEA, and EPS-AKA [2]. Those protocols are invoked whenever the UE connects to a new network domain. Algorithm 2 (*A2*) represents the use of fast re-authentication protocols [15], which are invoked whenever the user connects to a previously visited network domain. In addition, algorithm 3 (*A3*) represents Coordinated Robust Authentication and re-authentication protocols (CRA) [24]. Whereas the proposed authentication and re-authentication protocols are invoked in algorithm 4 (*A4*) of the UE movements (handovers) model.

The UE moves in a fixed path as illustrated in Fig. 12, it initially establishes a connection to the LTE network and then moves to WLAN1 domain that controlled by WAAAS1. Next, the UE performs a vertical HO to WiMAX network. After that, the UE reconnects to the previously visited WLAN1 domain. Then, it moves to the previously visited

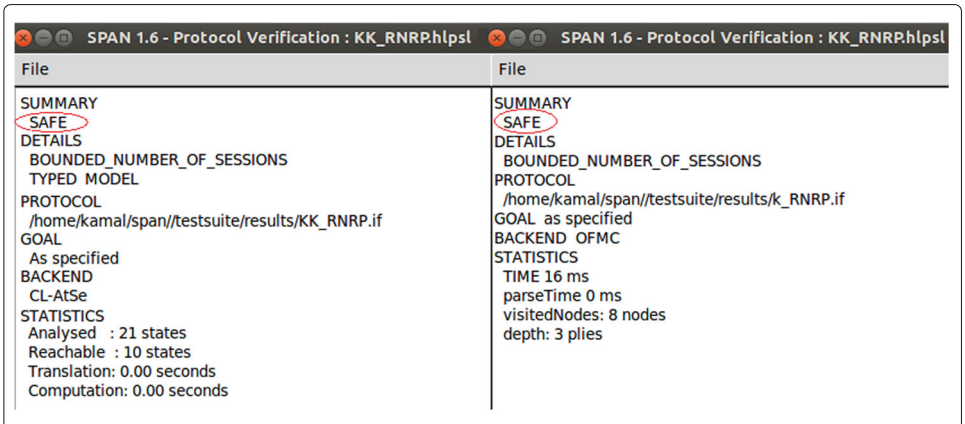

Fig. 11 Results of ATSE and OFMCE for RNRP protocol

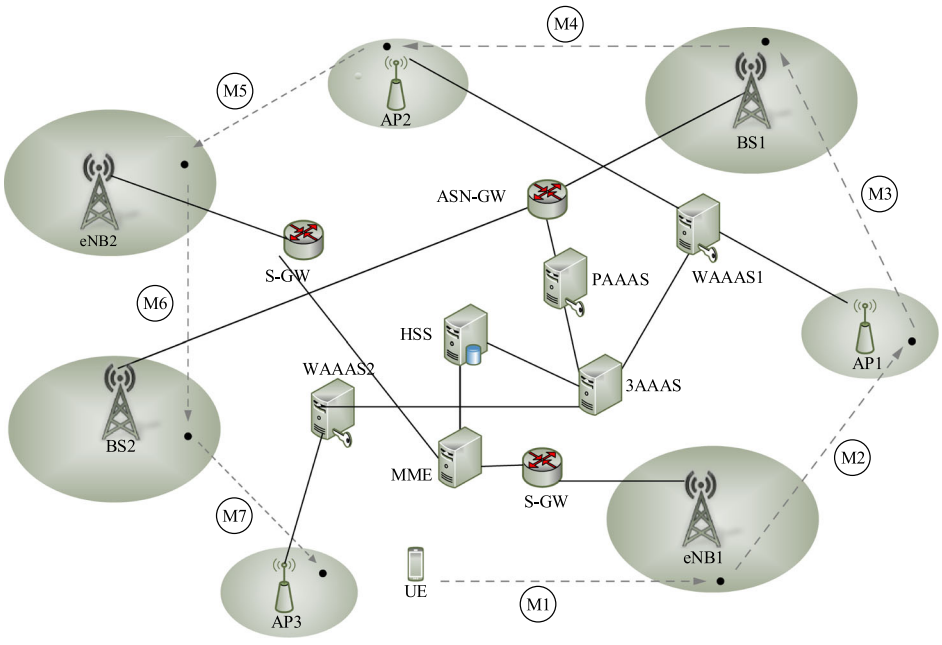

Fig. 12 User movements

LTE domain. In the next movement, the UE reconnects to the previously visited WiMAX domain. Finally, the UE moves to WLAN2 domain that controlled by WAAAS2.

In *A1*, seven standard authentication protocols are invoked to perform the authentication process during UE handovers. Four standard authentication protocols and three fast re-authentication protocols are invoked in *A2*. Four full coordinated robust authentication (FCRA) protocols and three coordinated robust re-authentication (CRR) protocols are invoked in *A3*. In *A4*, the UE establishes a connection to the LTE domain and performs either EAKAP or EEPSP authentication protocol via eNB1. When the UE moves to WLAN1, an Inter WLAN re-authentication protocol is invoked with the AP1 residing in WLAN1. Next, the UE moves to WiMAX domain and performs an Inter WiMAX re-authentication protocol. The next movement is to the previously visited WLAN1 domain, where an Intra WLAN re-authentication protocol is invoked. After that, the UE moves to the previously visited LTE domain and performs an Intra LTE re-authentication protocol. Subsequently, the UE moves to the previously visited WiMAX domain and performs an Intra WiMAX re-authentication protocol. Finally, the UE moves to WLAN2 and performs an Inter WLAN re-authentication protocol.

6.1 Handover delay

This section provides an analytical model for LTE-WLAN-WiMAX interworking to evaluate the proposed and other algorithms in terms of handover delay where the user is performing a sequential vertical and horizontal handovers between those networks. In this model, the network of Fig. 1 is modeled in Fig. 13. The variable TD_{BG} is corresponding to TD_{eG} in LTE network; TD_{PB} is corresponding to TD_{eM} and TD_{WA} in LTE and WLAN networks, respectively; TD_{PG} is corresponding to TD_{MG}; and TD_{PL} is corresponding to TD_{ML} and TD_{WL}. The random variables of WiMAX network TD_{BU}, TD_{BG}, TD_{PG}, and the corresponding variables in LTE and WLAN are exponentially distributed with mean

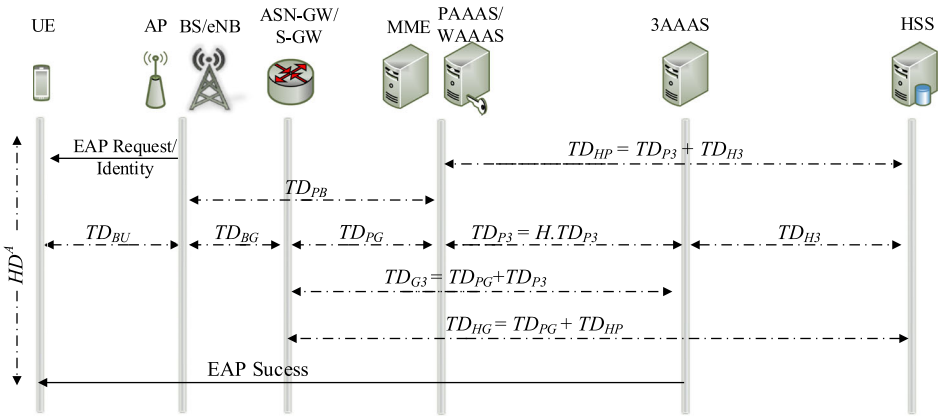

Fig. 13 Handover model

$1/TD_{BU}$, $1/TD_{BG}$, and $1/TD_{PG}$. The variable TD_{PL} and other corresponding variables are Erlang distributed $Er(H,TD_{PL})$.

The four algorithms that will be studied in this model are represented by A, where A includes $A1$, $A2$, $A3$, and $A4$ algorithms. The handover delay for each method in A is modeled using the parameter HD^A. Equation (24) illustrates the probability distribution function (PDF) for HD^A.

$$f_{HD^A}(t) = \sum_{m \in M^A} P_m . f_{HD_m^A}(t) \tag{24}$$

In this model, m is the authentication or re-authentication protocol that can be invoked in each algorithm, P_m is the ratio of invoking the method m, and M^A represents the protocols in each algorithm. For example, if A represents $A1$, then $M^A = \{AKAP, INEAP, EPSP\}$ and $M^A = \{AKAP, FAKAP, INEAP, FINEAP, EPSP, FEPSP\}$ when A represents $A2$, where $FEPSP$ and $FINEAP$ are the fast EPS and fast $INEAP$ protocols, respectively. In the case of A represents $A3$, $M^A = \{FCRA, CRR\}$, while $M^A = \{EAKAP, EINEAP, EEPSP, RNRP, ANRP, RXRP, AXRP, RERP, AERP\}$ for the proposed algorithm $A4$. According to [39], Eq. (24) can be expressed using Laplace transform in Eq. (25) as follows:

$$f^*_{HD_m^A}(s) = \sum_{m \in M^A} P_m . f^*_{HD_m^A}(s) \tag{25}$$

The HD^A contains different delay values; thus, it can be represented in a generic form using the convolution operator $\otimes$ as expressed in Eq. (26).

$$f_{HD_m^A}(t) = f_{\sum_{i \in \Phi_m^A} HD_i(t)} = \left(\otimes_{i \in \Phi_m^A} f_{HD_i} \right) \tag{26}$$

Under the condition m, the Φ_m^A is a set that represents the components of delay in algorithm A. The Laplace transform for HD^A can be written as follows:

$$f^*_{HD_m^A}(s) = f^*_{\sum_{i \in \Phi_m^A} HD_i(s)} = \left(\Pi_{i \in \Phi_m^A} f^*_{HD_i} \right) \tag{27}$$

Authentication delay is one of the delay components HD_i, and the other component is the transmission time. Equation (28) demonstrates the methods (protocols) that can be invoked during user movements in algorithms $A1$, $A2$, $A3$, and $A4$.

$$A1 = 2.EPSP+3.AKAP+2.INEAP$$
$$A2 = EPSP+FEPSP+2.AKAP + FAKAP+INEAP+FINEAP$$
$$A3 = 4.FCRA+3.CRR$$
$$A4 = EAKAP+2.RNRP+RXRP+ANRP+AERP+AXRP \quad (28)$$

When A represents $A1$, the Laplace transform of HD^{A1} can be written as follows:

$$f^*_{HD^{A1}}(s) = 2.f^*_{HD^{A1}_{EPSP}}(s) + 3.f^*_{HD^{A1}_{AKAP}}(s) + 2.f^*_{HD^{A1}_{INEAP}}(s) \quad (29)$$

The components of Eq. (29) are computed as follows:

$$f^*_{HD^{A1}_{EPSP}}(s) = (P_{FP}.(f^*_{TD_{H3}}(s))^2(f^*_{TD_{eU}}(s))^{10}.(f^*_{TD_{eM}}(s))^4 .(f^*_{TD_{M3}}(s))^{2H}.(f^*_{FP}(s))) \quad (30)$$

$$f^*_{HD^{A1}_{AKAP}}(s) = (P_{FP}.(f^*_{TD_{H3}}(s))^2(f^*_{TD_{AU}}(s))^{10}.(f^*_{TD_{WA}}(s))^4 .(f^*_{TD_{W3}}(s))^{4H}.(f^*_{FP}(s))) \quad (31)$$

$$f^*_{HD^{A1}_{INEAP}}(s) = (P_{FP}.(f^*_{TD_{H3}}(s))^2(f^*_{TD_{BU}}(s))^{10}.(f^*_{TD_{BG}}(s))^5 .(f^*_{TD_{PG}}(s))^4.(f^*_{TD_{P3}}(s))^{4H}.(f^*_{FP}(s))) \quad (32)$$

Accordingly, Eq. (29) can be written as follows:

$$\begin{aligned} f^*_{HD^{A1}}(s) = (f^*_{TD_{H3}}(s))^6(2.(P_{FP}.(f^*_{TD_{eU}}(s))^{10}.(f^*_{TD_{eM}}(s))^4 \\ .(f^*_{TD_{M3}}(s))^{2H}.(f^*_{FP}(s)))+3.(P_{FP}.(f^*_{TD_{AU}}(s))^{10} \\ .(f^*_{TD_{WA}}(s))^4.(f^*_{TD_{W3}}(s))^{4H}.(f^*_{FP}(s)))+ \\ 2.(P_{FP}.(f^*_{TD_{BU}}(s))^{10}.(f^*_{TD_{BG}}(s))^5.(f^*_{TD_{PG}}(s))^4 \\ .(f^*_{TD_{P3}}(s))^{4H}.(f^*_{FP}(s)))) \end{aligned} \quad (33)$$

According to [40], the Laplace transform notation for HD^A can be obtained from the following equation.

$$E(HD^A) = \int_0^\infty f_{HD^A}(t)dt = \int_0^\infty f_{HD^A}(t)e^{-ts}dt \Big| \quad (34)$$

Then, the mean of the density function is:

$$= -\frac{d}{ds}f^*_{HD^A}(s)\Big|_{s=0} \quad (35)$$

In the case of the standard protocols Algorithm $A1$, Eq. (35) can be written as:

$$E(HD^{A1}) = -\frac{d}{ds}f^*_{HD^{A1}}(s)\Big|_{s=0} \quad (36)$$

According to [30] and [39], Pr represents the values of P_{FP} and P_{RP}, and it varies between 0 and 1. The processing time of full authentication protocols (FP) and fast re-authentication protocols (RP) are 1240 and 600 ms, respectively. The hop count between GW and the AS is set to 4.

Figure 14 shows the performance of the proposed and other algorithms in terms of handover delay when the value of Pr increases from 0 to 1. It demonstrates that, when Pr is 0.1, the proposed and other algorithms experience convergent values of handover delay. This is because of performing full authentication protocols in the proposed and other algorithms during the first connection. When Pr increases the handover delay in $A1$, $A2$,

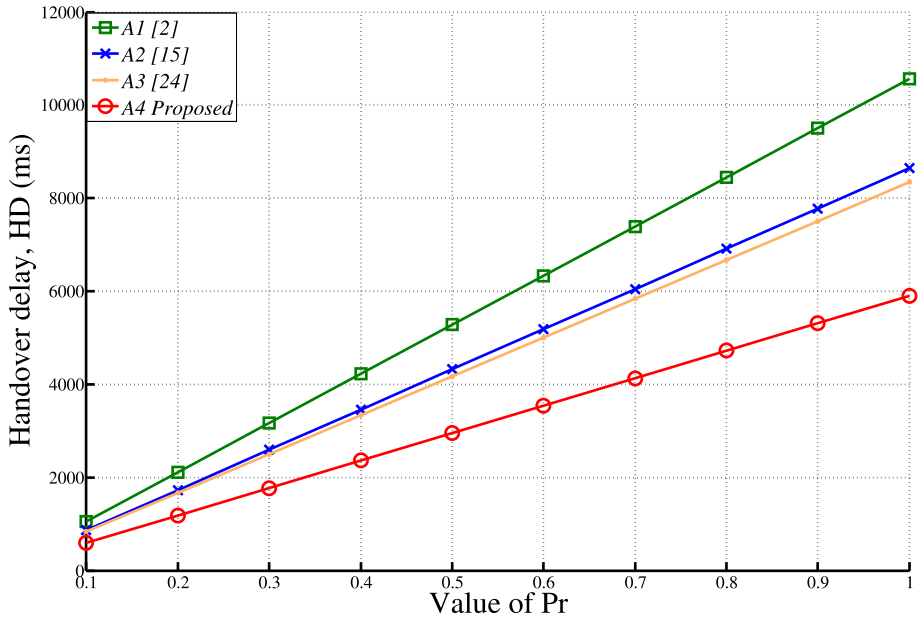

Fig. 14 Handover delay with *Pr*

A3, and *A4* algorithms is gradually increased until it reaches to 10560 ms, 8640 ms, 8340 ms, and 5900 ms, respectively.

Figure 15 shows how is the handover delay in each algorithm affected by increasing the hop count between the local servers and the 3AAAS. The value of handover delay in *A4* is slightly affected by increasing the hop count compared to other algorithms. This is due to performing the intra authentication protocols which are not affected by the number of hop count since there is no communication between the local servers and 3AAAS.

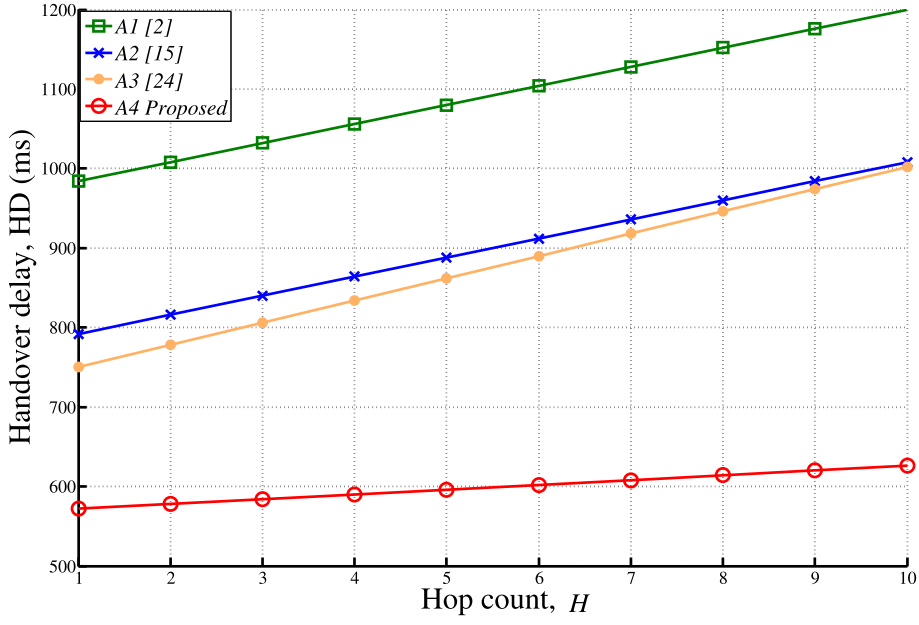

Fig. 15 Handover delay with hop count

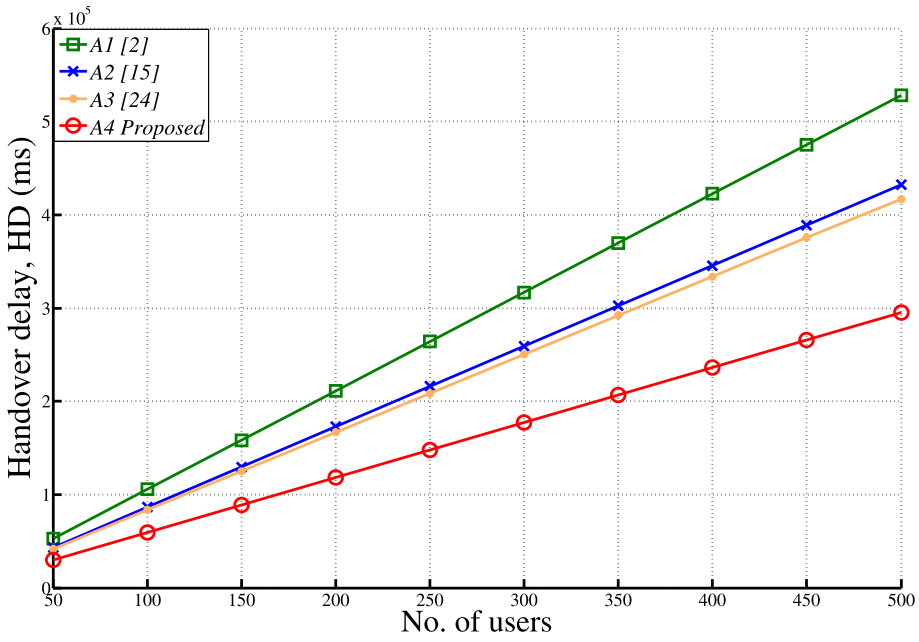

Fig. 16 Handover delay with no. of users

The local re-authentication protocols ANRP, AXRP, and AERP are not affected when the number of hop count between the WAAAS / PAAAS / MME and the 3AAAS is increased. The slight increasing in handover delay with H is due to invoking RNRP, RXRP, and RERP protocols, which requires contacting the 3AAAS. Figure 16 shows the performance of the proposed algorithm compared to the standard and other algorithms in terms of handover delay and the number of users. The handover delay increases by increasing the number of users in each algorithm. However, the proposed algorithm *A4* achieves less handover delay compared to *A1*, *A2*, and *A3* algorithms. In general, the proposed algorithm *A4* reduces the handover delay by 44%, 34%, and 29% compared to *A1*, *A2*, and *A3* algorithms, respectively.

A part of user movements is used to compare the proposed protocols with standard protocols and the WiMAX-WLAN authentication protocols of Shaidhani in [23]. In this part, authentication and re-authentication protocols are invoked during handovers from WiMAX to WLAN networks. Figure 17 shows the performance of the proposed protocols compared to standard and other protocols when the hop count increases from 1 to 11. Obviously, it is shown that the handover delay is not affected significantly by increasing the hop count number. This is due to the reduction of communication between the serving network and the AS during the handover processes in the proposed protocols. In Fig. 18, the handover delay for all protocols are almost the same when Pr is 0. This is because at this point, the re-authentication protocols are not invoked and all methods are starting with full authentication protocols; thus, the difference is starting to increase gradually until it reaches to 34%.

6.2 Key size

This section presents the key size for all keys that are generated during performing a particular protocol. The size of the exchanged and generated keys has a significant impact

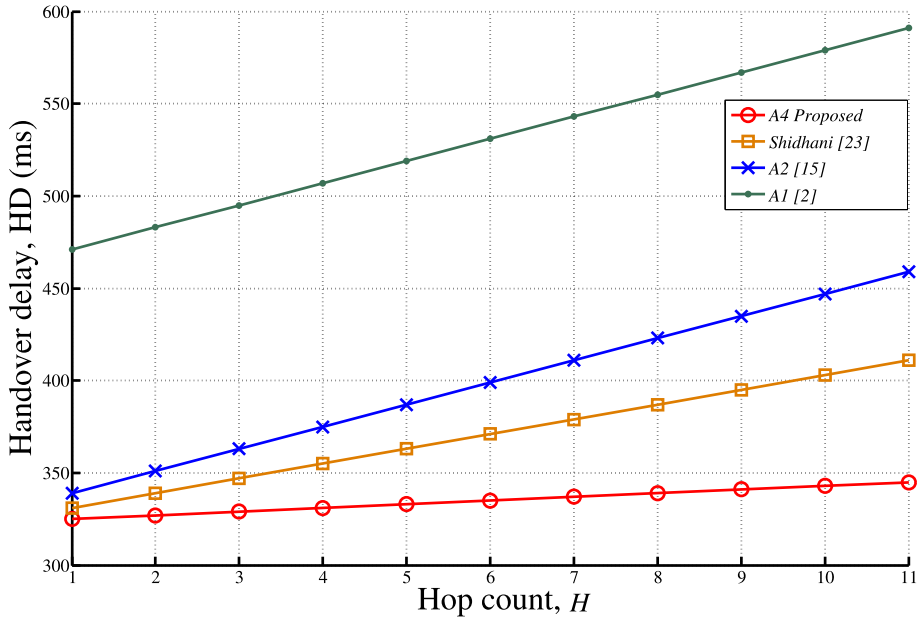

Fig. 17 Handover delay with hop count (WiMAX-WLAN)

on the storage cost because the other factors such as IDs, and nonce values used here have the same impact compared to the other methods. The sum of key size is calculated for *A1*, *A2*, *A3*, and *A4* algorithms. Figure 19 gives a clear indication that algorithm *A4* offers lesser key size compared to *A1*, *A2*, and *A3* algorithms. In the first movement M1 of the user, the modified authentication protocols are invoked and the key size is larger than the other protocols. However, it is significantly reduced during the subsequent re-authentication processes.

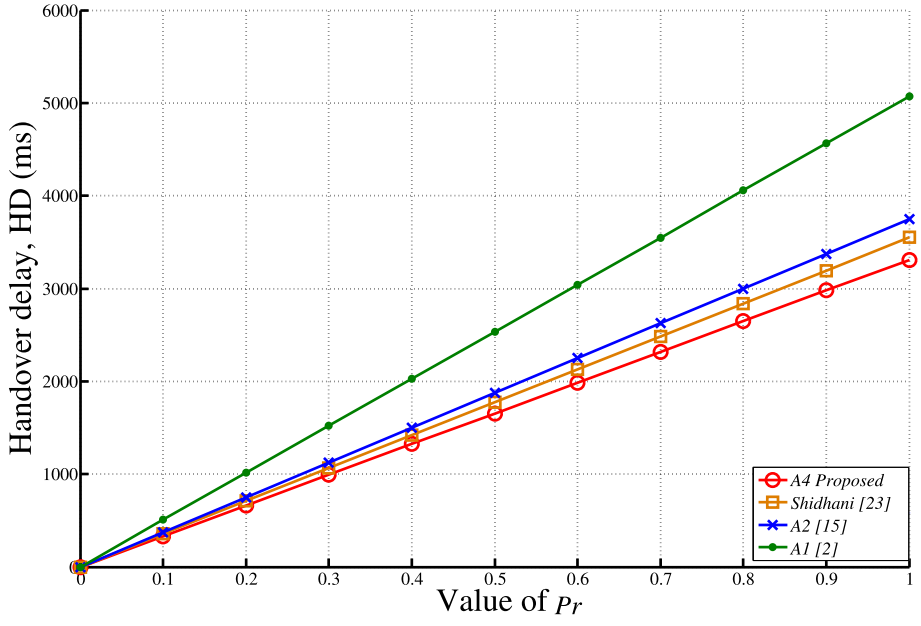

Fig. 18 Handover delay with *Pr* (WiMAX-WLAN)

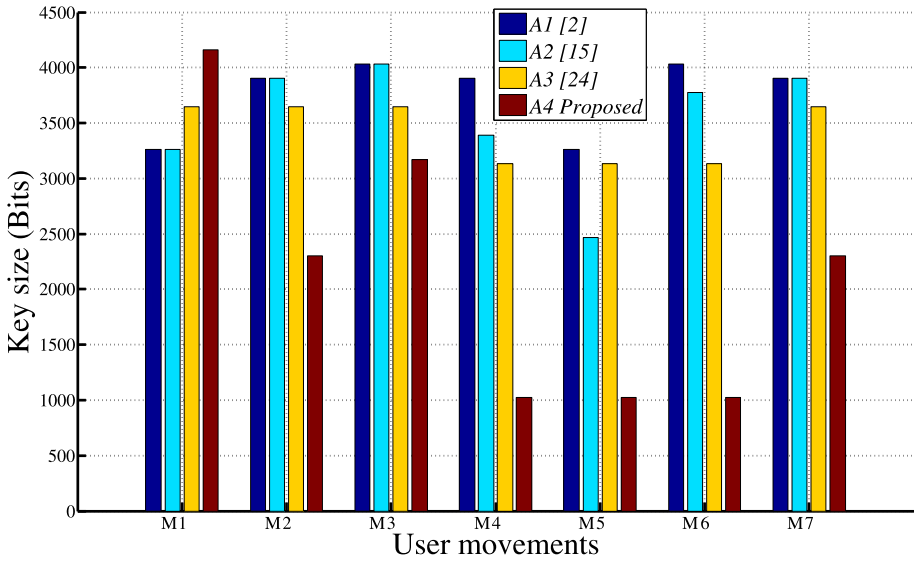

Fig. 19 The key size during user movements

During the movements M4, M5, and M6, the user moves to previously visited wireless domains; thus, no additional keys are generated in the 3GPP AAA server and intra re-authentication protocols are invoked with key size (1024 bits). Whereas in the movement M7, the value of key size jumps to (2304 bits), since the user moves to a new WLAN domain, which requires additional keys are generated in the 3AAAS server to perform an inter re-authentication protocol. In general, the storage that is required to save the generated keys during the user movements in the interworking architecture is reduced using the proposed algorithm *A4*.

6.3 Communication overhead for authentication process

The communication overhead is the time required to perform the authentication process during the HO process. In this section, we compare the communication overhead in the proposed protocols with others as illustrated in Table 1, where the TD_{UA} is the transmission delay between UE and AP/BS, TD_{AG} is the transmission delay between the AP/BS and the GW, and TD_{GP} is the transmission delay between the GW and the AAA server.

Table 1 Communication overhead

Method	Communication cost	
	Intra HO	Inter HO
A1 [2]	$10T_{UA} + 5T_{AG}$	$10T_{UA} + 5T_{AG}$
El Idrissi [46]	$10T_{UA} + 4T_{AG}$	$10T_{UA} + 5T_{AG} + 4T_{GP}$
Shen [16]	$10T_{UA} + 4T_{AG}$	$10T_{UA} + 5T_{AG} + 4T_{GP}$
Lin [17]	$20T_{UA} + 5T_{AG}$	$10T_{UA} + 5T_{AG} + 4T_{GP}$
Singh [18]	$12T_{UA} + 5T_{AG}$	$12T_{UA} + 5T_{AG}$
Proposed	$10T_{UA} + 4T_{AG}$	$10T_{UA} + 4T_{AG} + 4T_{GP}$

6.4 Average handover cost

To evaluate the performance of the proposed protocols in terms of handover cost, the hexagonal wireless network model [41] is adapted as a network model and fluid flow (FF) model [42] as mobility model. It is assumed that the sizes of each subnet are equal and take a hexagonal shape. It is also assumed that a hexagonal network model is an LTE-WLAN-WiMAX interworking domain and a cell is a subnet of one of the networks in the interworking architecture. The average handover rate (λ_j) is given by Eq. (37).

$$\lambda_j = (\nu \,.\, S(i))/(\pi \,.\, G(i)) \tag{37}$$

where j is a user group indicator and ν is the average velocity of UE in the interworking environment. The perimeter $S(i)$ of the given network domain can be computed as follows:

$$S(i) = (12i + 6).R \tag{38}$$

where i is the number of cells and R is the subnet radius. The coverage area $G(i)$ can be computed as follows:

$$G(i) = (2.6.R^2).(3i.(i + 1) + 1) \tag{39}$$

The average handover cost in time unit can be represented by,

$$AHC_m = \lambda_j \,.\, C_m, \tag{40}$$

The cost of each method C_m is expressed as follows:

$$C_m = C_{m,s} + C_{m,p}, \tag{41}$$

$C_{m,s}$ is the signaling cost and $C_{m,p}$ is the processing cost of the method m. The $AC_{m,s}$ for each algorithm can be computed as follows:

$$\begin{aligned} A1C_{m,s} &= 35C_{ws} + 50C_{wd} + 24H \\ A2C_{m,s} &= 35C_{ws} + 44C_{wd} + 22H \\ A3C_{m,s} &= 35C_{ws} + 40C_{wd} + 14H \\ A4C_{m,s} &= 35C_{ws} + 35C_{wd} + 8H \end{aligned} \tag{42}$$

where C_{ws} and C_{wd} are the transmission cost on wireless and wired links, respectively. The processing cost for each method $C_{m,p}$ is composed of the processing cost of each node $C_{n,p}$. For instance, the $C_{m,p}$ for the EPSP protocol can be written as $C_{EPSP,p} = C_{UE,p} + C_{MME,p}$, where

$$\begin{aligned} C_{UE,p} &= C_{key} + C_{enc} + C_{dec} + C_{ver} + C_{hash} \\ C_{MME,p} &= C_{key} + C_{dec} + C_{ver}, P_3 = C_{key} + C_{hash} + C_{enc} \end{aligned} \tag{43}$$

where C_{key}, C_{enc}, C_{dec}, C_{ver}, and C_{hash} are the costs of key generation, encryption, decryption, verification, and hash function, respectively. Thus, the $C_{m,p}$ for $A1$, $A2$, $A3$, and $A4$ algorithms is given as follows:

$$\begin{aligned} A1C_{m,p} =& 23C_{key} + 14C_{enc} + 14C_{dec} + 14C_{ver} + 14C_{hash} \\ A2C_{m,p} =& 20C_{key} + 14C_{enc} + 14C_{dec} + 14C_{ver} + 14C_{hash} \\ A3C_{m,p} =& 19C_{key} + 14C_{enc} + 14C_{dec} + 14C_{ver} + 14C_{hash} \\ A4C_{m,p} =& 14C_{key} + 14C_{enc} + 14C_{dec} + 14C_{ver} + 14C_{hash} \end{aligned} \tag{44}$$

The value of i is set to 10, C_{wd} is set to 20, and C_{ws} is set to 10. The other costs such as key generation cost C_{key}, encryption cost C_{enc}, decryption cost C_{dec}, verification cost C_{ver}, and hash functions cost C_{hash} are set to one unit. The results obtained from the handover cost analysis of each algorithm are shown in Fig. 20. The value of R is set to 0.1 km, and v and H vary from 2 to 5 km/h and 1 to 7 hop count, respectively. Increasing both v and H results in more average cost of handover in the standard and other algorithms compared to the proposed algorithm. This is a proof that the handover cost is effectively reduced by the proposed algorithm, which makes it suitable for such heterogeneous architecture.

Figure 21 shows the handover cost when v is set to 2 km/h, and R and H vary from 0.1 to 0.8 km and 1 to 6 hop count, respectively.

In general, when the hop count increases, the average handover cost is affected in the case of standard and other algorithms. In the case of the proposed algorithm, the handover cost is slightly affected, since the authentication process is performed by the local servers and no need to communicate with the 3AAAS (The hop count is assumed to be between the local servers and the 3AAAS). For instance, in the standard algorithm *A1*, the *AHC* increases from 1215 to 1349 when H increases from 1 to 7. Whereas in the proposed algorithm *A4*, the *AHC* increases from 1056 to 1100. The reduction of handover cost in the proposed algorithm *A4* reaches up to 22%, 18%, and 11% compared to algorithms *A1*, *A2*, and *A3*, respectively.

6.5 Energy consumption

The 4G and the 5G networks serve a huge number of users; thus, energy consumption is one of the most important issues that should be addressed. The reduction of the generated keys and the number of exchanged messages during the authentication process result in reducing energy consumption [43] and [44]. In general, the amount of energy consumed by wireless networks can be obtained by a linear equation,

$$Energy = M.N + B \tag{45}$$

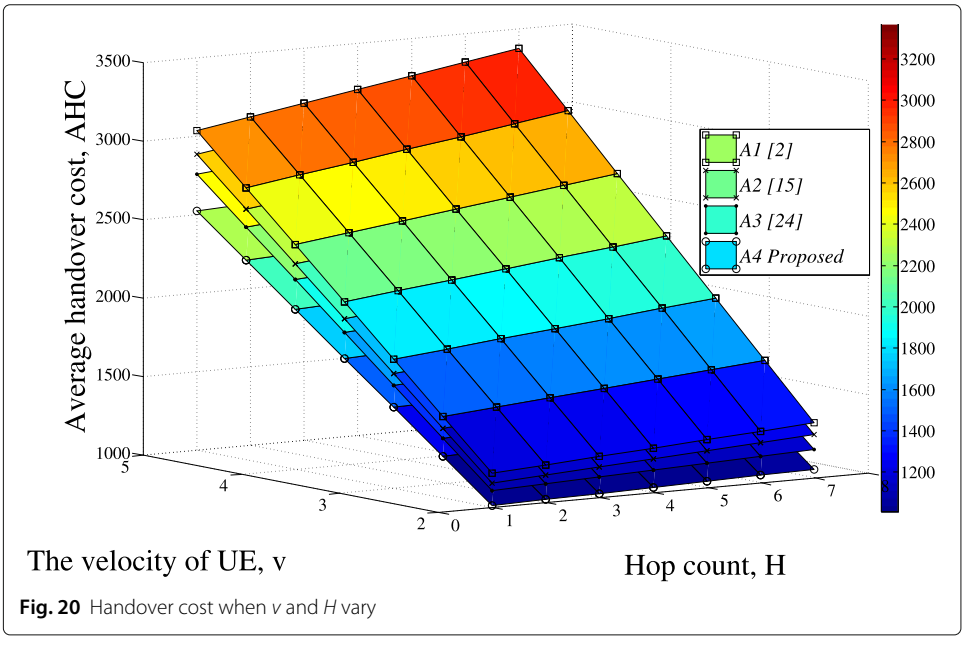

Fig. 20 Handover cost when v and H vary

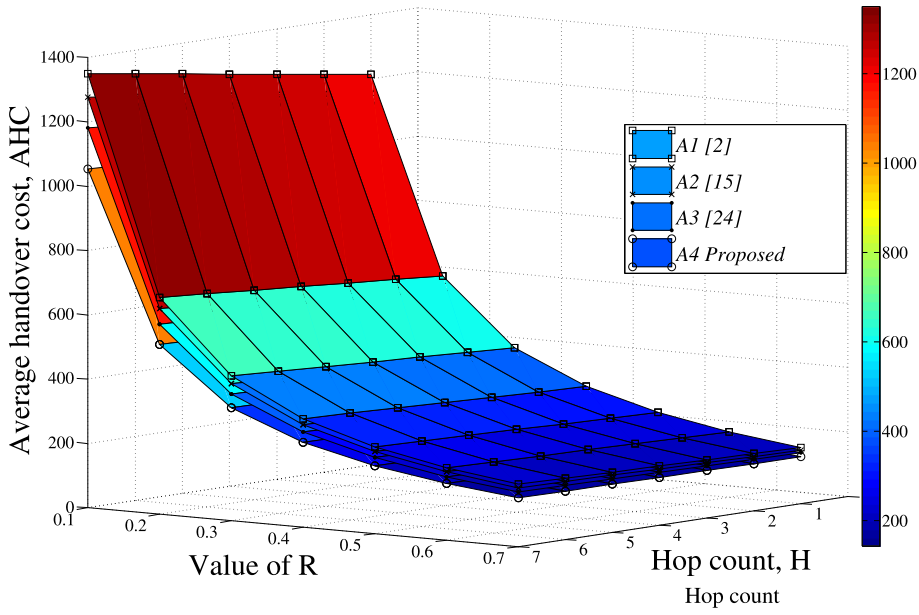

Fig. 21 Handover cost when *R* and *H* vary

where N is the total number of bytes sent or received by the UE, M is the incremental cost, and B is the fixed cost. Both the incremental and fixed cost are linear coefficients which have been computed in [45] by using experimental results for point to point model. The energy consumption can be calculated based on the number of bytes sent and received by UE as follows:

$$\begin{aligned} E_{trans} &= 0.48N + 431 \\ E_{rec} &= 0.12N + 316 \end{aligned} \tag{46}$$

The findings in [45] are utilized in this section to roughly calculate the energy consumed by the UE in each movements. Then, the calculations are applied on *A1*, *A2*, *A3*, and *A4* algorithms. Figure 22 shows that the energy consumed in *A1*, *A2*, *A3*, and *A4* algorithms is increased whenever the UE performs movement (either an inter HO or intra HO) in the LTE-WLAN-WiMAX environment. However, the energy consumption of *A4* is slightly increased in each movements compared to *A1*, *A2*, and *A3* algorithms, since the number of bytes sent and received by UE is reduced by inter and intra re-authentication protocols. The proposed algorithm *A4* achieves 17%, 13%, and 11% as a reduction in energy consumption compared to *A1*, *A2*, and *A3*, respectively.

7 Conclusion and future work

Authentication protocols provide secure communication in the wireless networks by preventing unauthorized users from using the network resources. Nevertheless, it adds delay and overhead to the communication. These problems become more pertinent in the environment of heterogeneous wireless networks such as 5G networks. For the sake of avoiding the single point of failure and providing secure and fast inter and intra handovers in the 4G and 5G networks, authentication and re-authentication protocols have been proposed in this work. The standard authentication protocols have been enhanced to be

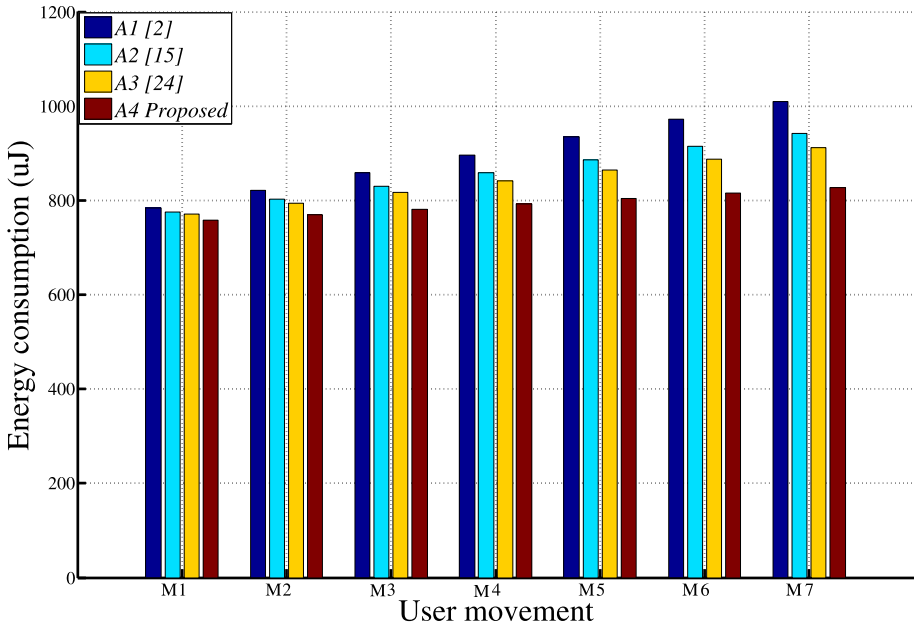

Fig. 22 Energy consumption in each user movement

more secure against authentication and secrecy attacks such as UID and MITM attacks. A new method has been proposed to protect the user identity, and this method is simple and does not add processing capability to the UE or HSS. Then, new re-authentication protocols have been proposed to locally perform fast re-authentication processes during handovers to the same domain or to a previously visited domain. The results of the analytical model show that the proposed protocols achieve better performance than the standard and other protocols in terms of handover delay, cost, and energy consumption. In addition, the verification tools show that the proposed protocols are secure and prevent all types of authentication and secrecy attacks in such environment. The future work could be conducted in the area of designing fault tolerant procedures which will improve the performance of authentication protocols. Those procedures work in case of detecting errors during the authentication process. Instead of rejecting the authentication and restart the authentication from the first step, the fault-tolerant procedure restarts the authentication process from the step where errors occurred; thus, the delay and cost of authentication and re-authentication processes will be effectively reduced. Another future work direction is to design authentication protocols for heterogeneous wireless sensors networks (WSN) which support Internet of Things (IOT) notion. The idea could be extended to design authentication and re-authentication protocols in the interworking of 5G and WSN. In WSN networks, the sink is considering as an authentication server. Each sensor node and the sink exchange the keys and perform a mutual authentication.

Abbreviations

HD^A: Handover delay of algorithm A; M^A: Protocols used in algorithm A; P_{FP}: Ratio of invoking full protocols; P_{RP}: Ratio of invoking reauth. protocols; H: Hop count between Local servers and 3AAAS; TD: Transmission delay; TD_{AU}: TD between AP and UE; TD_{BU}: TD between BS and UE; TD_{eU}: TD between eNB and UE; TD_{eG}: TD between eNB and GW; TD_{BG}: TD between BS and GW; TD_{HG}: TD between HSS and GW; TD_{PG}: TD between PAAAS and GW; TD_{WA}: TD between AP and WAAAS; TD_{eM}: TD between eNB and MME; TD_{PB}: TD between PAAAS and BS; TD_{W3}: TD between WAAAS and 3AAAS; TD_{M3}: TD between MME and 3AAAS; TD_{P3}: TD between PAAAS and 3AAAS; TD_{G3}: TD between GW and 3AAAS; TD_{H3}: TD between HSS and 3AAAS

Acknowledgements
Not applicable.

Authors' contributions
The authors have contributed jointly to the manuscript. The authors have read and approved the final manuscript.

Availability of data and materials
The first author have the source codes. Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study

Competing interests
The authors declare that they have no competing interests.

Author details
[1] Institute of Computer Science and Digital Innovation, UCSI University, 56000 Cheras Kuala Lumpur, Malaysia. [2] Department of Computer and Communication Systems Engineering, & Research Centre of Excellence for Wireless and Photonic Networks (WiPNET), Faculty of Engineering, Universiti Putra Malaysia, Malaysia 43400 UPM, Serdang, Selangor, Malaysia. [3] Faculty of Engineering and Information Technologies, University of Sydney, Sydney, Australia.

Received: 8 December 2018 Accepted: 6 April 2020
Published online: 24 May 2020

References

1. J. Arkko, V. Lehtovirta, P. Eronen, *Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'), RFC 5448*. (IETF, USA, 2009)
2. 3GPP, *3GPP system architecture evolution (SAE); Security aspects of non-3GPP accesses. TS 33.402 V13.1.0*. (3GPP, France, 2016)
3. C. Rigney, S. Willens, A. Rubens, W. Simpson, *Remote Authentication Dial In User Service, RFC 2865*. (IETF, USA, 2000)
4. K. A. Alezabi, F. Hashim, S. J. Hashim, B. M. Ali, in *IEEE Malaysia International Conference on Communications (MICC 2013)*, A new tunnelled EAP based authentication method for WIMAX networks (IEEE, Kuala Lumpur, 2013), pp. 412–417
5. P. WiMAX Forum Network Working Group, *WiMAX advanced: Deployment scenarios based on input from WiMAX operators and vendors*. (WiMAX Forum, Clackamas, 2014)
6. GSM, Digital cellular telecommunications system (phase 2+); Security aspects. (GSM 02.09 version 6.1.0 release 1997) (1997)
7. 3GPP, *3G security architecture*. (3GPP, France, 2018)
8. 3GPP, *3GPP system architecture evolution (SAE); Security architecture*. (3GPP, France, 2018)
9. 3GPP, 3GPP system architecture evolution (SAE); Security architecture and procedures for 5G system (2019)
10. E. Bou-Harb, M. Pourzandi, M. Debbabi, C. Assi, A secure, efficient, and cost-effective distributed architecture for spam mitigation on LTE 4G mobile networks. Secur. Commun. Netw. **6**(12), 1478–1489 (2013)
11. 3GPP, *Access to the evolved packet core (epc) via non-3GPP access networks; stage 3*. (3GPP, France, 2018)
12. P.UB. FIPS, 180-3. Secure hash standard. Natl. Inst. Stand. Technol. **1**, 27 (2008)
13. P. FIPS, 180-1. Secure hash standard. Natl. Inst. Stand. Technol. **17**, 45 (1995)
14. K. A. Alezabi, F. Hashim, S. J. Hashim, B. M. Ali, A. Jamalipour, On the authentication and re-authentication protocols in lte-wlan interworking architecture. Trans. Emerg. Telecommun. Technol. **28**(4), ett.3031 (2017)
15. 3GPP, *3GPP system architecture evolution (SAE); Security aspects of non-3GPP accesses (rel 14)*. (3GPP, France, 2017)
16. S.-S. Shen, S.-H. Lin, J.-H. Chiu, Fast handover pre-authentication protocol in 3GPP-WLAN heterogeneous mobile networks. Int. J. Commun. Netw. Syst. Sci. **2014**(7), 101–113 (2014)
17. S.-H. Lin, J.-H. Chiu, S.-S. Shen, The performance evaluation of fast iterative localized re-authentication for 3G/UMTS-WLAN interworking networks. J. Ambient. Intell. Humanized Comput. **4**(2), 209–221 (2013)
18. G. Singh, D. Shrimankar, A privacy-preserving authentication protocol with secure handovers for the LTE/LTE-A networks. Sādhanā. **43**(8), 128 (2018)
19. J. Arkko, H. Haverinen, *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), RFC 4187*. (USA, 2006)
20. Y. El Hajjaji El Idrissi, N. Zahid, M. Jedra, in *20th International Conference on Telecommunications (ICT 2013)*, A new fast re-authentication method for the 3G-WLAN interworking based on EAP-AKA (IEEE, 2013), pp. 1–5
21. A. H. Hassanein, A. Hafez, A. Ahmed, A. Gaafar, A. El-hamid, New authentication and key agreement protocol for LTE-WLAN interworking. Int. J. Comput. Appl. **61**(19), 20–24 (2013)
22. K. A. Alezabi, F. Hashim, S. J. Hashim, B. M. Ali, in *IEEE Region 10 Symposium 2014*, An efficient authentication and key agreement protocol for 4g (LTE) networks (IEEE, Kuala Lumpur, 2014), pp. 502–507
23. A. A. Al Shidhani, V. C. Leung, Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers. IEEE Trans. Dependable Secure Comput. **8**(5), 699–713 (2011)
24. E. Sithirasenan, K. Ramezani, S. Kumar, V. Muthukkumarasamy, EAP-CRA for WiMAX, WLAN and 4G LTE interoperability. Selected Topics in WiMAX, IntechOpen, 978–953 (2013)
25. J. Cao, M. Ma, H. Li, Y. Fu, X. Liu, EGHR: Efficient group-based handover authentication protocols for MMTC in 5G wireless networks. J. Netw. Comput. Appl. **102**, 1–16 (2018)
26. D. Wang, L. Xu, F. Wang, Q. Xu, An anonymous batch handover authentication protocol for big flow wireless mesh networks. EURASIP J. Wirel. Commun. Netw. **2018**(1), 200 (2018)
27. D. Forsberg, G. Horn, W.-D. Moeller, V. Niemi, *LTE Security, vol. 1*. (Wiley, New York, 2012)
28. J. Linn, *The Kerberos version 5 GSS-API mechanism. RFC 1964*. (IETF, USA, 1996)
29. P. WiMAX Forum Network Working Group, *WiMAX forum network architecture—stage 2 "architecture tenets, reference model and reference points 3GPP—WiMAX interworking," rel 2*. (WiMAX Forum, Clackamas, 2011)

30. R. Housley, B. Aboba, Guidance for Authentication, Authorization, and Accounting (AAA) KeyManagement. RFC4962 (2007)
31. IEEE Standard for local and metropolitan area networks, et al., Air Interface for Fixed Broadband Wireless Access Systems, Part 16, Amendment 2 and Corrigendum 1 (2005). IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1-2005
32. P. Roshan, J. Leary, *802.11 Wireless LAN Fundamentals*. (Cisco press, Indiana, 2004)
33. X. Li, J. Ma, Y. Park, L. Xu, A USIM-based uniform access authentication framework in mobile communication. EURASIP J. Wirel. Comm. Netw. **2011**, 1–12 (2011)
34. T. Clancy, M. Nakhjiri, V. Narayanan, L. Dondeti, *Handover Key Management and Re-Authentication Problem Statement. RFC 5169*. (IETF, USA, 2008)
35. T. Yang, C. Lai, R. Lu, R. Jiang, EAPSG: Efficient authentication protocol for secure group communications in maritime wideband communication networks. Peer-to-Peer Netw. Appl. **8**(2), 216–228 (2015)
36. R. Housley, B. Aboba, *Guidance for Authentication, Authorization, and Accounting (AAA) Key Management*. (IETF, 2007)
37. AVISPA, The AVISPA User Manual (2001). http://www.avispa-project.org. Accessed 19 Apr 2019
38. M. Wazid, A. K. Das, V. Odelu, N. Kumar, Susilo, Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment. IEEE Trans. Dependable Secure Comput., 1–1 (2017). https://doi.org/10.1109/TDSC.2017.2764083
39. K.-L. Huang, K.-H. Chi, J.-T. Wang, C.-C. Tseng, A fast authentication scheme for WiMAX–WLAN vertical handover. Wirel. Pers. Commun. **71**(1), 555–575 (2013)
40. L. Kleinrock, *Queueing Systems: Volume 2: Computer Applications*. (Wiley, New York, 1976)
41. J.-H. Lee, T.-M. Chung, in *International Conference on Information Security and Assurance (ISA 2008)*, A traffic analysis of authentication methods for proxy mobile ipv6 (IEEE, NW Washington, 2008), pp. 512–517
42. W. Wang, I. F. Akyildiz, in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, Intersystem location update and paging schemes for multitier wireless networks, (2000), pp. 99–109
43. D. W. Carman, P. S. Kruus, B. J. Matt, Constraints and approaches for distributed sensor network security (final). DARPA Project report, (Cryptographic Technologies Group, Trusted Information System, NAI Labs). **1**(1), 1–39 (2000)
44. L. Zhang, S. Tang, S. Zhu, An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks. J. Netw. Comput. Appl. **59**(Supplement C), 126–133 (2016)
45. L. M. Feeney, M. Nilsson, in *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 3*, Investigating the energy consumption of a wireless network interface in an ad hoc networking environment (IEEE, Anchorage, 2001), pp. 1548–1557
46. Y. E. H. El Idrissi, N. Zahid, M. Jedra, in *International Symposium on Ubiquitous Networking*, An efficient authentication protocol for 5G heterogeneous networks (Springer, Casablanca, 2017), pp. 496–508

Publisher's Note