Arab J Sci Eng (2014) 39:8837–8850
DOI 10.1007/s13369-014-1445-4

RESEARCH ARTICLE - COMPUTER ENGINEERING AND COMPUTER SCIENCE

A New Handover Authentication Method for WiMAX Architecture

Younes El Hajjaji El Idrissi · Noureddine Zahid · Mohamed Jedra

Received: 4 December 2013 / Accepted: 30 September 2014 / Published online: 15 November 2014

Abstract The Initial Network Entry Authentication (INEA) process is the first security entry between client and WiMAX network. WiMAX architecture provides a significant flexibility to respect wireless security requirements. The INEA framework is based on the Extensible Authentication Protocol (EAP) for user authentication and key management. However, EAP authentication method introduces high authentication delay and signaling cost when the user moves between stations. These impact negatively the handover process and decrease the Quality of Service of WiMAX networks. In this paper, we analyze the existing INEA authentication process and we propose a new authentication method and key agreement for handovers process. To prove the new method validity, the verification is performed by using the formal security analyzer Automated Validation of Internet Security Protocols and Applications which is a performed tool to find automatically potential attacks in security protocols. Furthermore, the proposed protocol is compared with other handover protocols. The comparison shows that proposed protocol outperforms the other protocols.

Keywords WiMAX · Handover · Authentication · INEA · EAP-AKA · AVISPA

الخلاصة

إن عملية المصادقة الأولية لدخول الشبكة هي دخول أمني أول بين العميل وشبكة واي ماكس. ويقدم أسلوب بناء واي ماكس مرونة كبيرة لاحترام متطلبات الأمن اللاسلكية. ويستند إطار عملية المصادقة الأولية لدخول الشبكة إلى بروتوكول المصادقة المتوسع للمصادقة على المستخدم وإدارة المفتاح. ومع ذلك، فإن طريقة مصادقة بروتوكول المصادقة المتوسع تقدم تأخير مصادقة، وتكلفة دلالة مرتفعين عندما ينتقل المستخدم بين المحطات. وهذان الأمران يؤثران بشكل سلبي في عملية التسليم ويقللان من جودة الخدمة من شبكات واي ماكس. ونحن ـ في هذه الورقة العلمية – سوف نحلّل المصادقة الأولية لدخول الشبكة القائمة ونقترح طريقة مصادقة جديدة واتفاق مفتاح لعملية عمليات التسليم. وقد تم ـلإثبات صحة الطريقة الجديدة ـ تنفيذ التحقق باستخدام التحقق الآلي لمحلل أمني رسمي من بروتوكولات وتطبيقات أمن الإنترنت التي هي أداة تجرى لمعرفة الهجمات المحتملة تلقائيا في البروتوكولات الأمنية. وتمت ـعلاوة على ذلك ـمقارنة البروتوكول المقترح ببروتوكولات تسليم أخرى. وتظهر المقارنة أن البروتوكول المقترح يتفوق على البروتوكولات الأخرى.

1 Introduction

Mobile Worldwide Interoperability for Microwave Access (WiMAX) defined by IEEE 802.16e is considered as an emerging mobile broadband technology supporting Broadband Wireless Access (BWA) [1]. It is the latest wireless broadband technology designed to provide user equipment with new wireless services, such as Voice over Internet Protocol (VoIP), multimedia streaming and video conference. WiMAX presents a cheap technology to expand service coverage to remote areas and supports broadband wireless Internet access. The current Mobile WiMAX can support a data rate up to 100 Mbit/s for mobile and 1 Gbit/s in fixed speed [2]. However, the area coverage of WiMAX in public space is still limited.

Network security service is the most important feature in public network. All other services depend on it, and no higher level service can be used without robust security

Y. El Hajjaji El Idrissi (✉) · N. Zahid · M. Jedra
Laboratory of Conception and System, Faculty of Science, University Mohammed V-Agdal, Avenue Ibn Batouta, B.P.1014, Rabat, Morocco
e-mail: youneselhajjaji@gmail.com

mechanism. Network operators must provide end users with three essential security services: authentication, confidentiality and integrity [3]. WiMAX architecture is designed to avoid IEEE 802.11 WLAN security issues. The open-air nature of radio propagation in WiMAX networks introduces an additional security challenge that does not exist in wired network. The WiMAX forum defines a set of security requirements to be respected by User Equipment (UE) and network operators. On the one hand, UE must be able to verify that the accessed network is the legal serving operator and informs the selected Serving core network (CSN) by its identity, capabilities and credentials. UE should protect the exchanged wireless traffic with the connected BS by using a secure wireless link. On the other hand, the WiMAX operator needs to provide secure communication with legitimate UE by using strong cipher and integrity algorithms. In addition, it must offer to UE an efficient mobility service and allows access to the IP-based service only for legitimate UE via a secure connection.

Figure 1 represents WiMAX network model. Before a UE accesses to WiMAX network, a mutual authentication between the UE and WiMAX network is needed. The Access Service Network Gateway (ASN) controls a set of Base Station (BS). UE connected to BS is authenticated by Authentication, Authorization and Accounting server (AAA) in WiMAX Home Network (HN). User authentication is deployed by using Extensible Authentication Protocol (EAP) [4] in Initial Network Entry Authentication process (INEA). EAP presents a flexible authentication framework able to interact with AAA infrastructures. However, it introduces some drawbacks when mobility is taken into consideration. UE mobility presents two security challenges for WiMAX architecture. The first is the UE authentication by Target Base Station (TBS), while the second is the restoration of UE pre-existing security credentials. WiMAX architecture offers to UE the possibility to make handover in connected mode. UE can make a hard handover from Serving Base Station (SBS) to TBS when it receives high signal quality from the TBS [5]. The handover must be seamless for UE to avoid service interruption and Quality of Service (QoS) degradation. However, UE performs full INEA process with AAA when it handovers from one BS to another in different ASN. This results high authentication delays and signaling cost [6–11].

WiMAX defines three types of handover [8]: Hard Handover (HHD), Macro Diversity Handover (MDHD) and Fast Base Station Switching (FBSS). HHD is mandatory in WiMAX systems, while the other two are optional. HHD adopts the break-before-make technique in which the connection with the old BS is broken and the traffic is interrupted while the handover is in progress. Then, UE communicates with only one BS at each time. HHD is simple to use, meets WiMAX security requirements but introduces high handover delay due to the execution of full INEA by AAA. MDHD and FBSS belong to the group of soft handovers. Each UE maintains a list of BSs which are involved in handover procedure "Diversity set". UE communicates and shares its security context simultaneously with all the BSs in the diversity set via more radio channels. These types of handovers introduce an additional traffic, require complex user equipment and do not satisfy the WiMAX security requirements [7,8].

To resolve the handover delay issue, WiMAX architecture proposed an additional handover optimization [1]. TBS bypasses the request of UE capabilities and UE re-authentication, and re-uses key materials from previous authentication [1]. The omission of the mutual authentication is based on the type of network architecture and the trust relationship between UE, BS and the CSN. The absence of a trust connection between UE and BS impacts negatively this optimization, because in the absence of a mutual authentication UE cannot detect a rouge target BS. Consequently, this optimization does not much with the WiMAX security requirements.

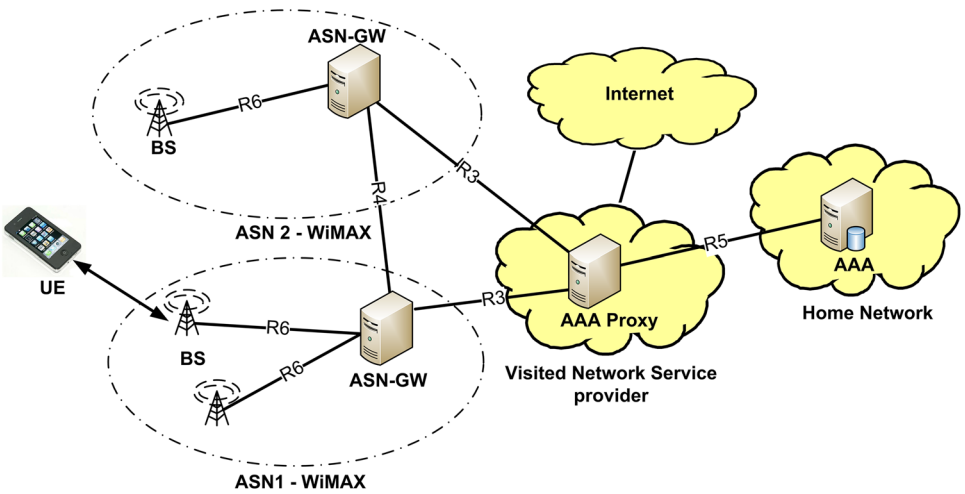

Fig. 1 WiMAX network model

In this paper, we propose a new handover pre-authentication scheme to simplify UE handover in WiMAX network. Our authentication method does not require any Public Key Infrastructure (PKI) and matches with WiMAX security requirements. The proposed handover protocol requires the execution of only one INEA round. A new key framework is proposed to authenticate UE locally by ASN during the handover process. In addition, this method reduces authentication delay and the number of generated authentication keys. It also achieves mutual authentication and protects the user identity. The rest of the paper is organized as follows. In Sect. 2, we present the standard authentication methods and we detail our proposed method in Sect. 3. In Sects. 4 and 5, we analyze the performance of our methods and we evaluate the security in Sect. 6. We conclude in Sect. 7.

2 Standard Handover Protocols

UE authentication in WiMAX architecture is based on the EAP protocol. WiMAX forum recommends three EAP methods: EAP-AKA, EAP-TLS and EAP-TTLS [11]. In practice, certificate-based authentication EAP-TLS and EAP-TTLS need high cost for computation and communication than shared key-based authentication EAP-AKA. This later is based on Pre-shared Symmetric Key (PSK) between UE and authentication server AAA. It is also used for interworking between 3GPP and WiMAX networks. The INEA process is executed when UE enters in ASN domain for the first time [8]. Figure 2 illustrates an example of INEA process in WiMAX network. EAP authentication run takes place between UE and AAA server through ASN. If the authentication is successful, UE and AAA drive the Master Session Key (MSK—512 bit) and Extended Master Session Key (EMSK). The AAA server forwards the resulting MSK key to the ASN without saving a copy of the MSK. ASN and UE use MSK to generate the Pairewise Master Key (PMK—160 bit). The PMK serves to generate the Authentication Key (AK—160 bit). PMK and AK are generated as follows:

$$\text{PMK} = \text{Truncate (MSK, 160)} \quad (1)$$

$$\text{AK} = \text{Truncate (PMK, UEMAC}\,||\text{IDBS}||\ \text{“AK”, 160)} \quad (2)$$

where Truncate (x, y) is a key derivation function defined as the last y bits of x. UEMAC is UE MAC address. AK is used to create lower-level keys. A three-way handshake protocol is executed to ensure that both UE and serving BS have the same AK [1]. This key will be used to secure the communications between UE and BS. The exchanged messages between UE and BS are carried by using the PKMv2 [7]. While the exchanged packets between ASN and AAA are carried by RADIUS protocol [10].

UE performs handover across different WiMAX BSs to seek a stronger signal. Handover procedure can be started by UE or connected BS. An intra-handover, called R6 handover, is realized when the UE wants to move from the SBS to a TBS belonging to the same ASN domain. The inter-handover, called R3 handover, is executed when the selected TBS is controlled by another ASN. In the case of R6 handover, AK sent by ASN to TBS for further authentication

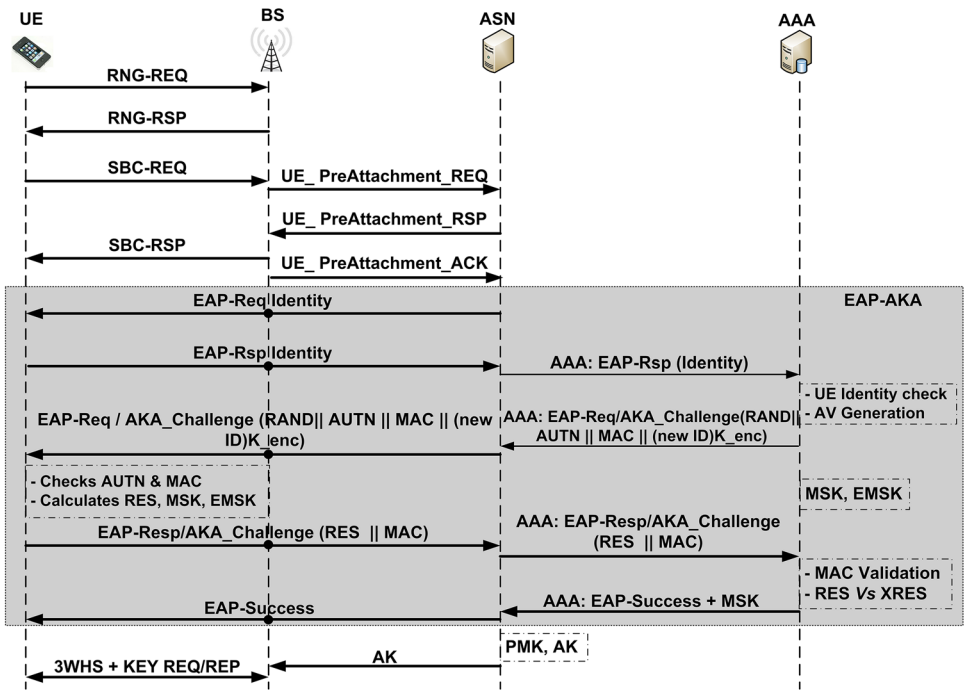

Fig. 2 Initial Network Entry Authentication (INEA)

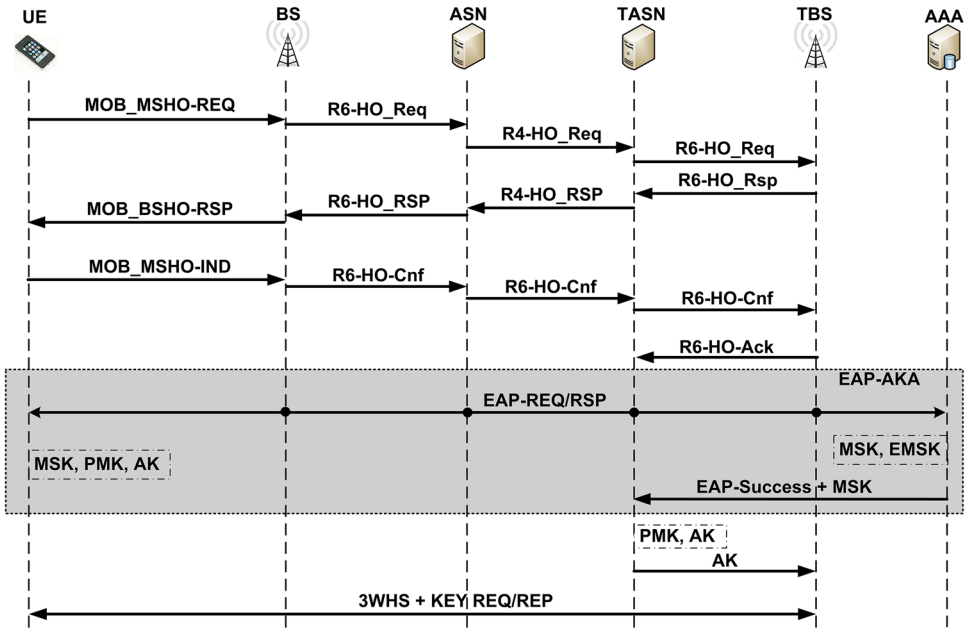

Fig. 3 Default R3 handover protocol

and key generation. As result, ASN does not need to execute EAP authentication since the old AK will be used to derive new authentication keys. But, this impacts negatively WiMAX key framework and creates the domino effect [9]. This means that if the security of one BS is compromised, it can lead to the security compromise of all previous BSs (backward secrecy) and following BSs (forward secrecy).

When the TBS is controlled by another ASN, R3 handover is invoked. Figure 3 illustrates an example of R3 handover process. The UE initiates the handover process by sending an MOB_MSHO-REQ request to SBS. SBS sends a handover request message over R6_HO_REQ/RESP to its ASN controller. The ASN selects candidate handover TBS, which are controlled by other ASN, and sends a handover request message over the R4_HO_REQ/RESP to the TASN. The TASN generates handover request for TBS. Then, UE and AAA execute the INEA process which leads to communication delay and signaling overhead due to key re-generation and distribution.

To improve the handover performance, a seamless handover option is defined by WiMAX forum. The TBS can suggest omitting the EAP-AKA execution by requesting the use of Handover Process Optimization (HPO) [2–11]. All secret keys used before the handover will be reused after the handover. UE and TBS generate the new authentication key AK by using the old (PMK, MSK) and only TBS identity is changed in Eq. 2. However, the improvement of performance bypassing the EAP-AKA execution creates critical security issues such as a lack of valid entity authentication leading to Man-In-the-Middle (MITM) and Denial of Service (DoS) attacks and domino effect problem [11].

In literature, significant volume of research has proposed an enhancement of WiMAX authentication procedure. The main goal of these researchers was to achieve fast handover without impact on network security. These solutions may be classified into two categories: pre-authentication and re-authentication. In pre-authentication handover, UE and TBS authenticate each other prior to the completion of the handover. In [12], Thuy et al. propose an enhanced EAP-based pre-authentication (EPA) method, which reduces the authentication delay and overcomes DoS and replay attacks during R3 handovers. But this method requires high computation and communication overheads, due to the exchange of unnecessary keys between UE and BSs that the UE never roams to. In [13], a promising solution for secure handover in WiMAX network was proposed. The authors propose an efficient pre-authentication scheme that follows the least privilege principle to solve the domino effect. However, this pre-authentication scheme is not efficient and degrades WiMAX security level.

Re-authentication methods can avoid full EAP-based authentication in handover by reusing the information exchanged between UE and ASN in the previous authentication. The authors in [14,15] propose a key caching mechanism to eliminate the non-necessary IEEE 802.1X authentication cost. To speed the handover process, the old ASN re-uses the MSK when the UE revisits the ASN in the future. The old ASN still keeps the UE key MSK and profile until the end of the key lifetime. This approach can improve authentication performance, but constraints UE mobility to the old ASN and consumes extra storage (512 bits for the MSK, 32 bits for the MSK lifetime and 1,024 bits for the UE authorization profiles) to keep UE key records at the old ASN. In addition, this approach does not respect WiMAX security requirements due to the absence of a fresh round of mutual authentication between UE and ASN. In [6], Chang et al.

propose to reduce the authentication period by overlooking few authentication steps. In this approach, Mobile IPv6 Fast Handover (FMIPv6) protocol is combined in the EAP authentication procedure and security keys are transferred from SBS to TBS. Therefore, the major key material was shared among BSs, which do not satisfy the backward and forward secrecy concept. Other handover schemes are proposed in [16,17], these new authentication schemes achieve mutual authentication by using public key process. This has a negative impact on handover delay compared to standard handover process. To address handover drawbacks, Kim et al. [18] have proposed a mutual authentication and key agreement method by using a public-key cryptosystem. This method requires a public key infrastructure, does not respect the WiMAX architecture and suffers from the high handover delay compared with the symmetrical key-based scheme.

In summary, the limitations of existed methods are listed as follows: standard authentication procedures (INEA, R6 and R3) introduce high authentication delay, are vulnerable to MITM and DOS attacks and create a domino effect problem. The pre-authentication schemes [12,13] are inefficient and insecure. The re-authentication methods [6,14–17] constraint the UE mobility, do not respect the WiMAX architecture and they violate the WiMAX security requirements. Therefore, to reduce authentication delay and respect WiMAX security requirements, we propose a new optimized pre-authentication model. In the next section, we present novel handover pre-authentication methods in WiMAX network that simplify the INEA process, reduce the authentication delay during R3 handover, are robust to MITM and DOS attacks and that can eliminate the domino effect in R6 handover. In comparison with the schemes mentioned above, our proposed methods are more practical since they necessitate less modification in the standard WiMAX architecture. They require only one round of INEA between local UE and AAA and expand the scoop of ASN to cover the authentication function during the handover process. Our authentication methods match with WiMAX security recommendations and do not require PKI infrastructure. These are guaranteed by a new hybrid key framework which permits to authenticate UE locally by the ASN during the handover process. Lastly, our methods reduce authentication delay and number of authentication keys, achieve mutual authentication and protect the user identity.

3 Proposed Handover Protocols

The new pre-authentication methods propose an enhanced R6 and R3 handover protocol in WiMAX architecture. These protocols eliminate the need for third party to authenticate UE during handover process. An enhanced INEA protocol is proposed to facilitate the execution of handover protocols. Our protocols introduce less signaling overhead, reduce handover delay, respect WiMAX security requirements and guaranty data confidentiality by using hybrid cipher cryptosystem, which combines Elliptic Curve Cryptography (ECC) with symmetric key.

It is known that ECC is an attractive public-key cryptosystem that offers the same security strength as prevalent cryptosystems such as RSA with reduced key sizes and encryption /decryption time. For example, the ECC offers the same security strength with a key of 163 bits as 1,024 bits in RSA [19]. Security in ECC is based on the hardness of elliptic curve discrete logarithm problem (ECDLP). The elliptic curve equation $E_q(a, b)$ can be defined as follows [20]:

$$y^2 = x^3 + ax + b \quad (a, b \in F_q, \quad \Delta = 4a^3 + 27b^2 \neq 0) \quad (3)$$

The ECDLP problem is defined as follows: Given a $P \in F_q$ with order n and Q with order n over E_q. It is intractable to find r such that $Q = r \times P$.

To use the ECC algorithm, WiMAX operator selects a finite field F_q over a large odd prime $q > 2^{160}$ and defines elliptic curve equation $E_q(a, b)$. In addition, it selects public point Q with order n over $E_q(a, b)$. Each authentication server AAA has a known public encryption key $U_H = d_H \times Q$ (with d_H indicates the private key). Every UE and ASN has a pre-shared secret key with AAA composed by $(U_E, d_E)(U_E = d_E \times Q)(U_{\text{ASN}}, d_{\text{ASN}})(U_{\text{ASN}} = d_{\text{ASN}} \times Q)$. By using this key framework, three simple authentication protocols are proposed: modified INEA protocol (MINEA), fast R6 handover (FR6H) and fast R3 handover (FR3H) authentication protocol. A list of symbols used in describing the proposed protocols is shown in Table 1.

3.1 Modified INEA (MINEA)

Full EAP-AKA protocol is executed during standard INEA process, which introduces high authentication delay and signaling cost. To bypass this limitation, we propose a new authentication method "Modified INEA protocol (MINEA)". Figure 4 describes the proposed authentication process MINEA. After user identification, AAA generates a random number RAND, randomly selects an integer $r_H \in Z_q^*$, computes $R_H = r_H \times U_H$, $R'_H = r_H \times U_E$ and creates the UE Temporary Authentication Key $\text{TAK} = d_H \times R'_H$. Furthermore, it calculates the next UE identity ID_{NTE}, MAC_{HU} and authentication token AUTH_{HU} as follows:

$$\text{ID}_{\text{NTE}} = \text{Dot16KDF(IDE, TAK)} \quad (4)$$

$$\text{MAC}_{\text{HU}} = \text{Hash (TAK, RAND, ID}_{\text{NTE}}) \quad (5)$$

$$\text{AUTH}_{\text{HU}} = R_H || \text{MAC}_{\text{HU}} \quad (6)$$

The AAA sends the AV and TAK to the ASN. AAA defines for each TAK a valid lifetime after which the MINEA must be

Table 1 Notation definition

$E_q(a, b)$	Elliptic curve defined over F_q
$X \times Y$	Denotes the point multiplication over $E_q(a, b)$
$X\|\|Y$	Concatenation of X and Y
TAK	Temporary authentication key
THK	Temporary handover key
PMK	Pairwise master Key
AK	Authorization Key
d_X	Private key of X
$U_x = d_x \times Q$	Public key of X
(U_x, d_x)	Pre-shared key between X and authentication server ($U_x = d_x \times Q$)
Dot16KDF	Key hash function
Hash	Public cryptographic one-way secured hash function
Truncate (x, n)	Result of truncating x to its leftmost n bits
fK (X)	Encrypt X using key K
$AUTH_X$	Message authentication token generated by X
MACx	Message integrity check generated by X
ID_X	Identifier of X
ID_{NTX}	Next Identifier of X

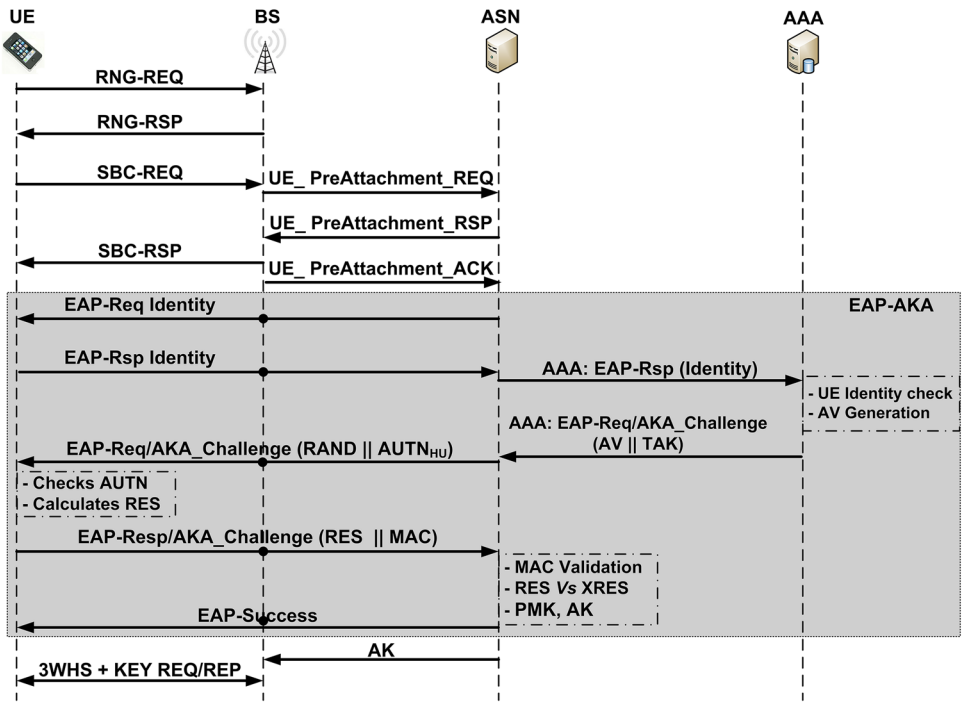

Fig. 4 Modified Initial Network Entry Authentication (MINEA)

re-invoked. After reception of EAP request message by UE, it computes the authentication key by using the received R_H and his secret key d_E(TAK $= d_E \times R_H$), next authentication ID, a local MAC_{HU} and verifies the calculated MAC with the received one. In positive check, the UE calculates the response message RESP and MAC in this way:

$$\text{MAC} = \text{Hash (TAK, RAND)} \tag{7}$$

ASN receives UE response message and checks the received RESP with the expected one XRESP. In positive check, ASN derives the session key MSK from TAK and sends an EAP success message to UE. ASN and UE use MSK to generate PMK and AK as described in (1) and (2). The MINEA proposes a new key hierarchy. For each handover operation, TAK will be used by ASN to generate UE coming authentication and handover key THK. ASN will use this key as a

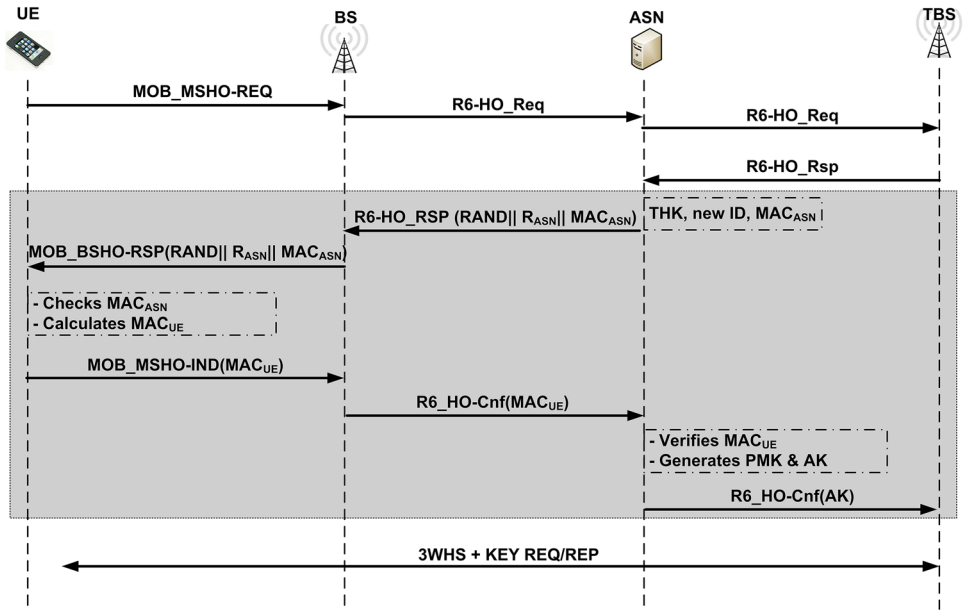

Fig. 5 Fast R6 handover protocol (FR6H)

UE shared key and generates the handover key THK by using the ECC algorithm. This key hierarchy offers to the ASN the possibility to authenticate UE without intervention of AAA and without knowing the pre-shared key of UE.

3.2 Fast R6 Handover Protocol

To avoid the domino effect problem detected in the standard R6 handover, we propose a new FR6H protocol. During FR6H, ASN locally authenticates UE by using the previous received key TAK. Figure 5 illustrates the proposed FR6H protocol. All authentication traffics are carried by the control message. UE initiates handover process, by sending a MOB_MSHO-REQ message, which contains UE identity. ASN validates UE identity ID_E, verifies the lifetime of TAK and prepares the TBS to the handover by using the R6-HO_REQ/RES messages. After this, it generates a random number RAND and new handover key THK in this way: Randomly selects an integer $r_{\mathrm{ASN}} \in Z^*$, calculates $R_{\mathrm{ASN}} = r_{\mathrm{ASN}} \times U_{\mathrm{ASN}}$, $R'_{\mathrm{ASN}} = r_{\mathrm{ASN}} \times \mathrm{TAK}$ and handover key $\mathrm{THK} = U_{\mathrm{ASN}} \times R_{\mathrm{ASN}}$. Also ASN computes the next UE local $\mathrm{ID}_{\mathrm{NTE}}$ and $\mathrm{MAC}_{\mathrm{ASN}}$ as follows:

$$\mathrm{ID}_{\mathrm{NTE}} = \mathrm{Dot16KDF}\ (\mathrm{ID}_{\mathrm{NTE}},\ \mathrm{ID}_{\mathrm{ASN}},\ \mathrm{THK}) \tag{8}$$

$$\mathrm{MAC}_{\mathrm{ASN}} = \mathrm{Hash}\ (\mathrm{RAND}\ ||\mathrm{ID}_{\mathrm{NTE}}||\ \mathrm{THK}) \tag{9}$$

ASN sends to UE the RAND, R_{ASN} and $\mathrm{MAC}_{\mathrm{ASN}}$ in the MOB_MSHO-REQ message through serving BS. After reception of authentication request, UE computes authentication handover key $\mathrm{THK} = d_E \times R_{\mathrm{ASN}}$, next authentication $\mathrm{ID}_{\mathrm{NTE}}$, a local $\mathrm{MAC}_{\mathrm{ASN}}$ and verifies it with the received one. The authentication procedure is stopped in the case of negative check, otherwise, UE replies with an MOB-HO-IND message which contains a message integrity check $\mathrm{MAC}_{\mathrm{UE}}$ in this way:

$$\mathrm{MAC}_{\mathrm{UE}} = \mathrm{Hash}\ (\mathrm{ID}_{\mathrm{NTE}}||\mathrm{THK}) \tag{10}$$

After getting authentication response, ASN calculates a local $\mathrm{MAC}_{\mathrm{UE}}$. If the values of calculated $\mathrm{MAC}_{\mathrm{UE}}$ and received one are equal, the ASN is assured that UE is legitimate. ASN and UE derive the new session keys PMK and AK from the THK in this way:

$$\mathrm{PMK} = \mathrm{Dot16KDF}(\mathrm{THK},\ \mathrm{ID}_{\mathrm{NTE}}||\mathrm{ID}_{\mathrm{ASN}}||\text{“PMK”},\ 160) \tag{11}$$

$$\mathrm{AK} = \mathrm{Dot16KDF}(\mathrm{PMK},\ \mathrm{UE}_{\mathrm{MAC}}||\mathrm{ID}_{\mathrm{BS}}||\text{“AK”},\ 160) \tag{12}$$

3.3 Fast R3 Handover Protocol

In WiMAX architectures, UE is authenticated by AAA server during R3 handover. Novel pre-authentication protocol is proposed to improve R3 handover. This is achieved by piggybacking authentication information on handover control messages without using INEA protocol. Figure 6 illustrates an example of our FR3H process. UE initiates the handover by sending an MOB_MSHO-REQ request message to SBS. The SBS sends a handover request message over the R6_HO_REQ to its ASN controller. After this, the ASN starts the handover negotiation with target ASN (TASN) through R4_HO-REQ. R4_HO_REQ contains $\mathrm{ID}_{\mathrm{UE}}$ and authentication key TAK. TASN sends R6_HO-REQ to TBS, which accepts the handover by using a R6_HO-RES. At the same time, TASN generates handover key THK in the same way as R6-handover, next local ID, $\mathrm{MAC}_{\mathrm{ASN}}$ and sends an authentication request to UE via the R4/R6_HO-REQ. After reception of authentication request, UE computes the handover

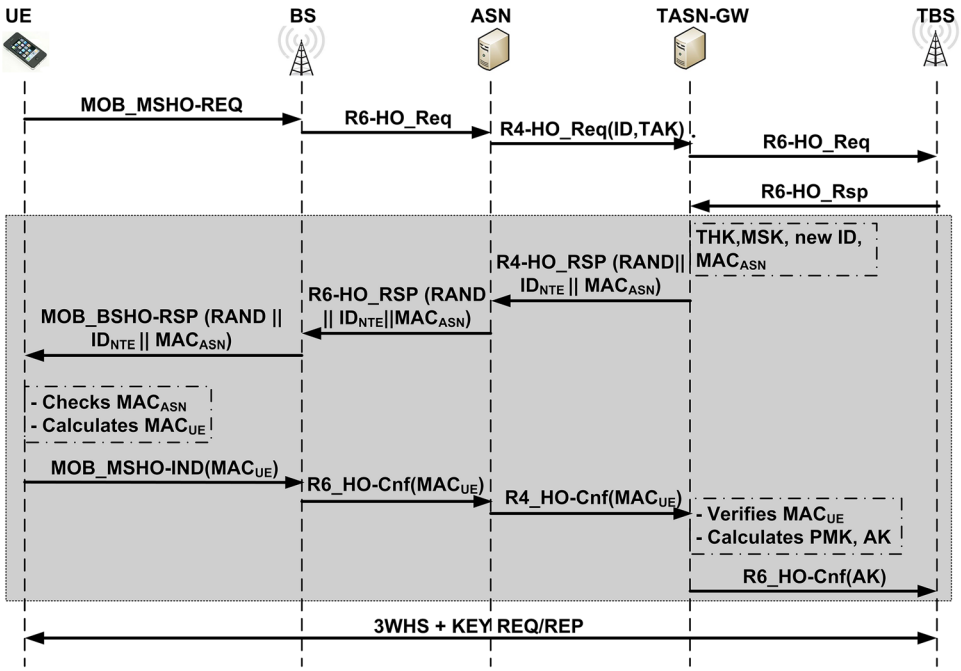

Fig. 6 Fast R3 handover protocol (FR3H)

authentication key THK, next authentication ID_{NTE}, a local MAC_{ASN} and verifies it with the received one. If MACs are identical, the TASN is legal. Then, UE sends a MOB-HO-IND message which contains message integrity check MAC_{UE} as follows:

$$MAC_{UE} = \text{Hash}(ID_{NTE}||THK) \tag{13}$$

TASN calculates a local MAC_{UE} and compares it with received one in R4_HO_Ack. In positive check, TASN drives a new MSK, PMK and AK and sends an R6_HO-Ack with the AK to the TBS.

4 Performance Evaluation of the Proposed Handover Protocols

In this section, we analyze and evaluate the performance of proposed handover protocols (FR6H/FR3H) compared to the standard ones and re-authentication mechanism proposed in [14]. The performance comparison is based on the bandwidth consumption, authentication delay and depends on UE movement in the specified network model following three handovers scenarios:

SC1 UE makes R3 standard handover followed by R6 standard handover, and then returns to the old ASN by executing standard R3 handovers.

SC2 UE makes handover by using key caching mechanism [14]. It executes R3 standard handover followed by R6 standard handover, and then returns to the old ASN by executing the key caching mechanism [14].

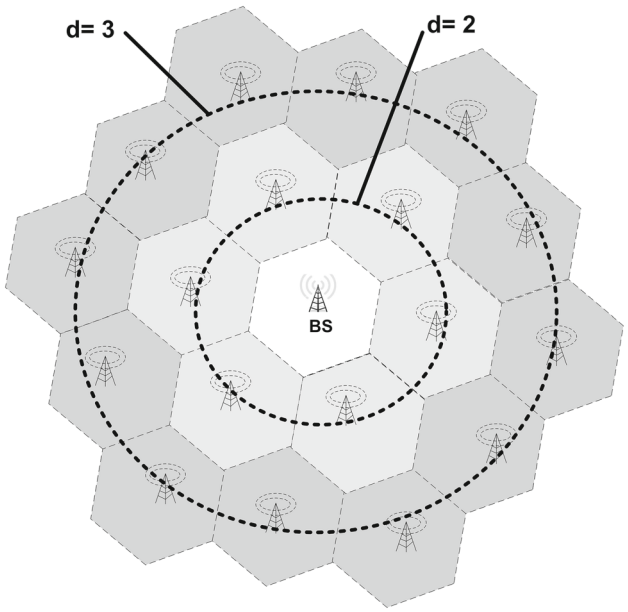

Fig. 7 WiMAX network structure

SC3 UE makes a fast R3 handover followed by R6 handover, and then returns to the old ASN by fast R3 handovers protocol.

4.1 UE Movement in Network model

Performance evaluation of the proposed authentication methods depends basically on WiMAX network model. Usually hexagonal structure is used in the wireless network performance evaluation [8]. We use the same network model as [21–23]. Figure 7 illustrates the proposed network model.

Table 2 List of used symbols

Symbol	Definition
d	ASN domain
t	Hexagon side length
v	Average velocity of users in a uniformly distributed direction over [0, 2p]
n	Number of UEs by cell
ρ	UEs density by area (mobile/m^2)
Rr6	Intra-handover rates
Rr3	Inter-handover rates
N_{wl}	Number of messages exchanged between two nodes in wireless network
N_{wd}	Number of messages exchanged between two nodes in wired network
H	Number of hops separating two nods

Our network is composed of several hexagonal cells. Each cell sector represents the coverage area of a single BS. The ASN domain regroups a number of adjacent BSs and is represented by a pointed circle d. a list of used symbols is presented in Table 2.

The number of BS for an R6 handover in an ASN is represented by:

$$\text{Br6} = 6\,(d-1) \tag{14}$$

The number of total BS for an R3 handover inside the WIMAX network is represented by:

$$\text{Br3} = \sum_{x=1}^{d} 6\,(x-1) + 1 = 3d\,(d-1) + 1 \tag{15}$$

The area coverage and the perimeter of a single BS for R6 and R3 handovers are represented by:

$$\text{Ar6} = 3/2\sqrt{3}t^2, \text{Lr6} = 6t \tag{16}$$

$$\text{Ar3} = 3/2\sqrt{3}t^2(3d\,(d-1)+1),$$

$$\text{Lr3} = 6t\,(2d-1) \tag{17}$$

We use a fluid flow mobility model to represent the UE handover rate in the network model [22–24]. In this model, the n UEs residing in a node are moving at an average velocity of v (m/s) in uniformly distributed directions over $[0.2\pi]$. The R6 and R3 handover rates are expressed by:

$$\text{Rr6} = \frac{\rho v l}{\pi} = \frac{n v \text{Lr6}}{\pi \text{Ar6}} \cdot \text{Br6} \tag{18}$$

$$\text{Rr3} = \frac{\rho v l}{\pi} = \frac{n v \text{Lr3}}{\pi \text{Ar3}} \cdot \text{Br3} \tag{19}$$

4.2 Authentication Signaling Cost

In this section, we evaluate the handover authentication signaling cost for all scenarios. The signaling cost can be defined as the total authentication signaling message traffic during a communication session [25]. Since the BS scanning messages and the UE registration are the same for all handovers protocols, our study is focused only on the handover control messages. The handover signaling costs of the three scenarios are represented by:

$$C_{\text{SC1}} = S_{\text{INEA}} + R_{\text{r3}} \cdot S_{\text{R3}} + R_{\text{r6}} \cdot S_{\text{R6}} + R_{\text{r3}} \cdot S_{\text{R3}} \tag{20}$$

$$C_{\text{SC2}} = S_{\text{INEA}} + R_{\text{r3}} \cdot S_{\text{R3}} + R_{\text{r6}} \cdot S_{\text{R6}} + R_{\text{r3}} \cdot S_{\text{KC}} \tag{21}$$

$$C_{\text{SC2}} = S_{\text{MINEA}} + R_{\text{r3}} \cdot S_{\text{FR3}} + R_{\text{r6}} \cdot S_{\text{FR6}} + R_{\text{r3}} \cdot S_{\text{FR3}} \tag{22}$$

where S_{protocol} is the total size of messages exchanged between all nodes during the handover protocol. INEA and MINEA are included, respectively, in (SC1, SC2) and SC3, because firstly R6 and R3 can only take place if they were previously executed, and secondly to indicate the impact of INEA in the coming handover process. We consider that the message average size is 250 bytes [8].

4.3 Authentication Delay

Studying handover delay is essential in evaluating the efficiency of handover protocols. Authentication delay (D_{auth}) can be defined as the delay taken by an authentication protocol to complete authentication process. In this section, we compare the D_{auth} for the three handover scenarios. Only handover authentication delay will be considered. Other handover related delays such as BS scanning or packets retransmissions are assumed to be the same in all scenarios. Handover delay is calculated starting from the MOB_MSHO-REQ request by UE and ends by sending AK by ASN to TBS. The total authentication delays introduced by the three handover scenarios are expressed as:

$$D_{\text{auth(SC1)}} = D_{\text{auth(INEA)}} + 2R_{\text{r3}} \cdot D_{\text{auth(R3)}} + R_{\text{r6}} \cdot D_{\text{auth(R6)}} \tag{23}$$

$$D_{\text{auth(SC2)}} = D_{\text{auth(INEA)}} + R_{\text{r3}} \cdot D_{\text{auth(R3)}} + R_{\text{r6}} \cdot D_{\text{auth(R6)}} + R_{\text{r3}} \cdot D_{\text{auth(KC)}} \tag{24}$$

$$D_{\text{auth(SC2)}} = D_{\text{auth(MINEA)}} + 2R_{\text{r3}} \cdot D_{\text{auth(FR3)}} + R_{\text{r6}} \cdot D_{\text{auth(FR6)}} \tag{25}$$

$D_{\text{auth}(X)}$ represents the delay time experienced when executing the specified X handover protocol. In the same way as authentication signaling cost, $D_{\text{auth(INEA)}}$ and $D_{\text{auth(MINEA)}}$ are included, respectively, in (SC1, SC2) and SC3 because R6 and R3 can only take place if INEA and MINEA were previously executed. D_{auth} can be divided into four components: delay of messages transmission D_{trans}, the nodal processing delay D_{pc}, propagation delay D_{pp} and additional delays related to special operation D_{sp}. According to [26] the transmission, delay in WIMAX is insignificant compared to D_{pc} and D_{pp}. D_{sp} regroups the delay experienced by AAA and UE when generating Authentication Vector D_{AV} [27], the delay for encryption/decryption D_{ED}, the delay caused by calculating and verifying message authentication codes D_{MAC}, the delay practiced by ASN and UE for ECC key generation D_{ECC} and the delay induced by key derivation D_{Key}. Authentication delay for different authentication protocols is expressed as follows:

$$D_{\text{auth(X)}} = N_{\text{wl}}\left(D_{\text{pp(UE-BS)}} + 2D_{\text{pc}}\right) + N_{\text{wd(A-B)}}\left(D_{\text{pp(A-B)}} + 2D_{\text{pc}}\right) + D_{\text{sp}(X)} \quad (26)$$

We assume that we have the same propagation delay between ASN-AAA and ASN-TASN ($D_{\text{pp(ASN-AAA)}} = D_{\text{pp(ASN-TASN)}} = H \times D_{\text{pp(Wired)}}$) and $D_{\text{pp(BS-ASN)}} = D_{\text{pp(Wired)}}$ with $D_{\text{pp(Wired)}}$ is the wired propagation delay. Also we note that $D_{\text{pp(UE-BS)}}$ is the wireless propagation delay $D_{\text{pp(Wrl)}}$. $D_{\text{sp(protocol)}}$ is represented as follows: $D_{\text{sp}(X)} = \overrightarrow{T}_{\text{sp}(X)} \cdot \overrightarrow{E}$, where $\overrightarrow{E}$ is a vector that represents $[D_{\text{AV}}, D_{\text{ED}}, D_{\text{MAC}}, D_{\text{ECC}}, D_{\text{key}}]$ while $\overrightarrow{T}_{\text{sp(X)}}$ represents the number of execution of each special operations in $\overrightarrow{E}$ by specified handover protocol. $\overrightarrow{T}_{\text{sp(X)}}$ is calculated as follows:

$$\begin{aligned}
\overrightarrow{T}_{\text{sp(INEA)}} &= [2, 2, 4, 0, 7],\\
\overrightarrow{T}_{\text{sp(R6)}} &= [0, 0, 0, 0, 1],\\
\overrightarrow{T}_{\text{sp(R3)}} &= [2, 2, 4, 0, 7],\\
\overrightarrow{T}_{\text{sp(MINEA)}} &= [2, 2, 4, 2, 7],\\
\overrightarrow{T}_{\text{sp(FR6)}} &= [0, 2, 4, 2, 1],\\
\overrightarrow{T}_{\text{sp(FR3)}} &= [0, 2, 4, 2, 1],\\
\overrightarrow{T}_{\text{sp(KC)}} &= [0, 0, 0, 0, 1],
\end{aligned}$$

4.4 Security Analysis

Network security should not be impacted by performance improvement of authentication method. The proposed protocols satisfy all network security requirements defined by the WiMAX. In this section, we examine the security of these protocols according to WiMAX security requirements.

Mutual authentication and key agreement The mutual authentication is used to protect UE against Man-In-The-Middle and rouge BS attacks. Our protocols propose a strong mutual authentication mechanism between UE and ASN. UE and ASN authenticate each other by proving the possession of the correct TAK and THK. UE authenticates ASN by verifying calculated MAC_{ASN} with the received one. ASN authenticates UE by checking MAC_{UE} with the received one. Moreover, no key is transmitted in clear and THK is one use key.

Forward and backward secrecy To avoid the domino effect problem, unnecessary distribution of key must be avoided. To achieve this goal, all generated keys must be used in a specific context. UE secret key (U_E, d_E) is hold only by UE and AAA. UE and ASN share the authentication key TAK with the help of the AAA and without knowing the secret key of each other. The TAK is used by the ASN as UE public key to derive the new session key THK for each handover process.

Protection to the replay and DOS attacks Our protocols are robust to the replay attack because the RAND_x, and r_x are generated randomly for each new handover and are used one time. In addition, all the exchanged messages are protected by a message integrity code.

Privacy protection To avoid UE identity disclosing, UE uses a pseudo identity ID_{NTE} generated by one-way function Dot16KDF in MINEA, FR6 and FR3 handover authentication phase. Therefore, it is difficult for strong global adversary and compromised BS to reveal the UE real identity from the ID_{NTE} overheard. In addition, UE changes its identity during every handover authentication process, and each ID_{NTE} is calculated by using the one-way function Dot16KDF with the new generated key THK.

5 Simulation Results

In our study, we use the same parameters as [2,27–29]. Table 3 summarizes the used handover parameters. All

Table 3 Value of used parameters

Parameter	Value
d	3
t	4 km
n	10 per/cell
v	5 m/s
Dpc	1 μs
DAV	12 μs
DMAC	3 μs
DED	5 μs
DKey	12 μs
DECC	0.54 ms
Dpp(Wired)	0.5 ms
Dpp(Wrl)	2 ms

numerical calculations are performed by using MATLAB based on the analysis in the previous section.

Figure 8 shows the authentication signaling cost for UE in three authentication scenarios by varying the UE velocity v. Our proposed protocols used in SC3 outperform standard and key caching mechanism used in SC1 and SC2. The differences in handover authentication signaling cost between SC1 and SC1/2 widen as v increases. This is mainly due to the increased handover frequency. This demonstrates that our authentication protocols (MINE, FR6H, FR3H) outperform the standard ones (INEA, R6, R3) and the key caching mechanism. When $v = 15$ m/s, the signaling cost is reduced by 31.7 % in SC3 compared to the SC1 and by 26.54 % compared to SC2. These differences are essentially due to the execution of full EAP-AKA by R3 handover in SC1 and in the new ASN in SC2. However, full EAP-AKA is executed one time in SC3. Improved performance results can be reached when the lifetime of the authentication key TAK is increased.

Figure 9 shows authentication delay of the three scenarios by varying the number of hops between ASN, TASN and AAA. Our authentication protocol reduces authentication delay in SC3 compared to SC1 and SC2 which uses only the standard protocols and key caching mechanism. Authentication delay in SC3 is not impacted by new ECC keys generation by ASN and UE in the handover proposed protocols. The authentication delay is reduced by 49.47 % in SC3 compared to SC1 and by 34.49 % compared to SC2. In conclusion, our scheme achieves huge performance results compared to the standard schemes and key caching technique in terms of computation and communication overhead.

6 Security Evaluation

Formal methods for protocol analysis and verification have so far been successfully used to check for correctness in communication protocols and complex sequential circuit designs. Model checking technique verifies whether a given model specification satisfies given properties by using checking tool. Different tools have been successfully implemented to

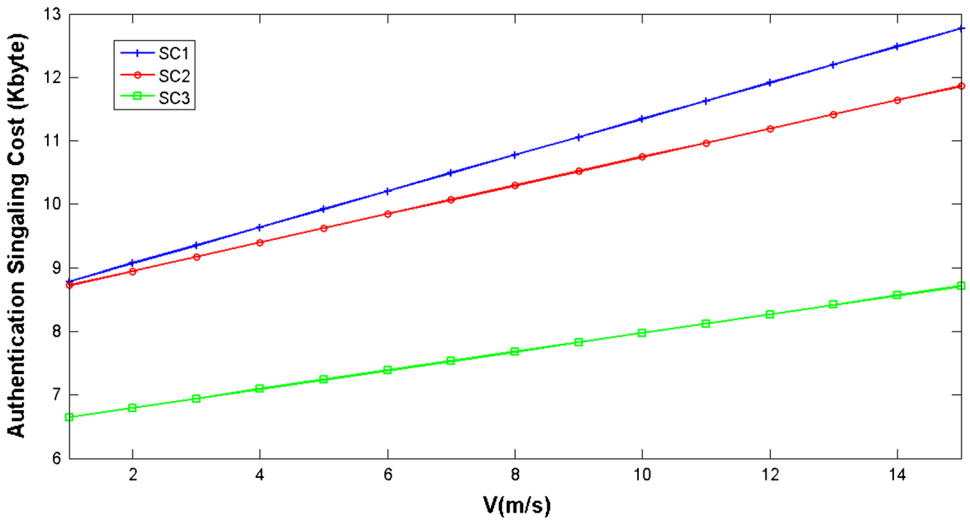

Fig. 8 Authentication signaling cost of SC1, SC2 and SC3

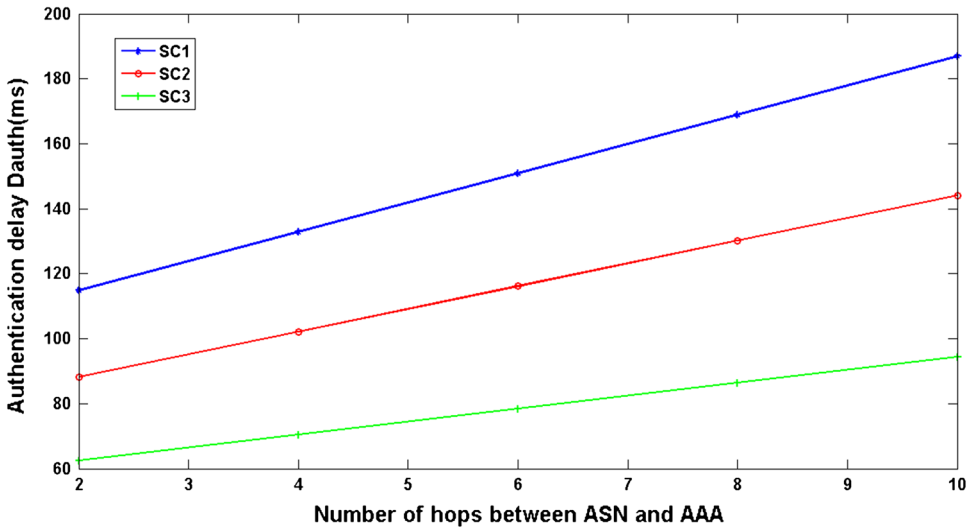

Fig. 9 Authentication delay of SC1, SC2 and SC3

expose vulnerabilities that may still exist in security protocols especially in WiMAX. Automated Validation of Internet Security Protocols and Applications (AVISPA) [30] is a model formal checking tool for internet security protocols. AVISPA is widely used by developers of security protocols and by academic researchers to analyze possible attacks on security protocols. It is based on sending and receiving messages, and on 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 protocols, its semantics is based on Lamport's Temporal Logic of Actions (TLA). Each protocol is divided into a set of basic roles representing the actions of one single agent in the protocol. Composition Roles (session and environment) represent the entire protocol and instantiate the basic roles. Each role is modeled 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 checker to find possible attacks on the protocol by using attacker. The attacker implemented in AVISPA is a DoleveYao intruder, which can overhear, intercept, modify or inject messages in communication channel. In general, authentication goals are modeled by these words: witness, request, wrequest and secret. Once the protocol is modeled in HLPSL, AVISPA translates them into a lower-level language Intermediate Format (IF) by a translator called hlpsl2if. IF is executed directly by the backends tools (OFMC, CL-AtSe, SATMC and TA4SP) to verify whether the security goals are satisfied or violated.

AVISPA and HLPSL are a very popular formal verification pack. However, the definitions role by role and not message by message make this pack difficult to use. For this, a new tool called "Security Protocol Animator" (SPAN) was created to facilitate the specification phase by allowing the animation of the language HLPSL [31]. SPAN helps in building Message Sequence Charts (MSC) of the protocol execution and implements an active intruder attacks on the verified protocol. Additionally, generation of nonce values and message texts can also be verified using SPAN. It can also be used to interactively find and build attacks on protocols.

Since the authentication messages are generated only by UE and ASN, BS role can be omitted in the formal specification. Exchanged authentication messages between UE and ASN are similar in both fast handovers (R6/R3). For this, we will focus only on verification of R6 handover protocol. Our protocol is defined in Peer (UE) and Server (ASN) role model and is expressed in the formal language HLPSL used in AVISPA. Figure 10 illustrates the role of server ASN in R6 handover protocol. We use the request and witness goal specification to check the mutual authentication between UE and ASN. The assertion witness (ASN,P,at_rand,AT_RAND′) means that ASN should be authenticated by UE by agreeing on the value AT_RAND. While the assertion request (P, ASN, at_rand, AT_RAND′) indicates that the UE authenticates the ASN and agrees on the value AT_RAND. The statement secret (THK,sec_TK,{ASN,P}) validates the confidentiality of the key THK between ASN and UE. Figure 11 shows the R6 protocol simulation by SPAN. This proves that our protocol specification is correctly written and interpreted by AVISPA.

```
role server (     P,ASN      : agent,
                  F1         : hash_func,
                  HASH       : hash_func,
                  TAK        : symmetric_key,
                  Q          : public_key,
                  Multi      : hash_func,
                  SND,RCV    : channel (dy))
played_by ASN def=
 local
     AT_RAND, RAND2,Rw        : text,
     MOB_MSHO_REQ             : text,
     Rasn,R1wu,THK,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 := 1
 transition

 1.  State  = 1      /\ RCV(MOB_MSHO_REQ) =|>
     State' := 3     /\ Rw'          := new()
                     /\ Rasn'        := Multi(Rw'.Multi(Dw.Q))
                     /\ R1wu'        := Multi(Rasn'.TAK)
                     /\ THK'         := Multi(R1wu'.Dw)
                     /\ AT_RAND'     := new()
                     /\ IDnte'       := (F1(user_id.THK'))
                     /\ AT_MAC1'     := HASH(AT_RAND'.IDnte'.THK')
                     /\ SND(Rasn'.AT_RAND'.AT_MAC1')
                     /\ witness(ASN,P,at_rand,AT_RAND')

 2.  State  = 3      /\ RCV(AT_MAC2')
                     /\ AT_MAC2' = HASH(AT_RAND'.THK) =|>
     State' := 5     /\ SND(success)
                     /\ request(ASN,P,at_rand2,AT_RAND)
end role
```

Fig. 10 ASN role description with HLPSL language

The mutual authentication and the confidentiality of handover keys in our protocols are checked by using OFMC and CLATSE. All tests are passed, and no attacks or vulnerabilities have been found. These confirm the secure key management and mutual authentication service of the proposed protocols. Figure 12 shows the messages returned by OFMC and CLATSE tools. Our protocol achieves mutual authentication, assures the confidentiality of shared keys TAK and THK between UE and ASN and is safe to use by both verification check tools. Test results did not reveal any exposed attacks. Therefore, AVISPA cannot produce any attack on our proposed scheme.

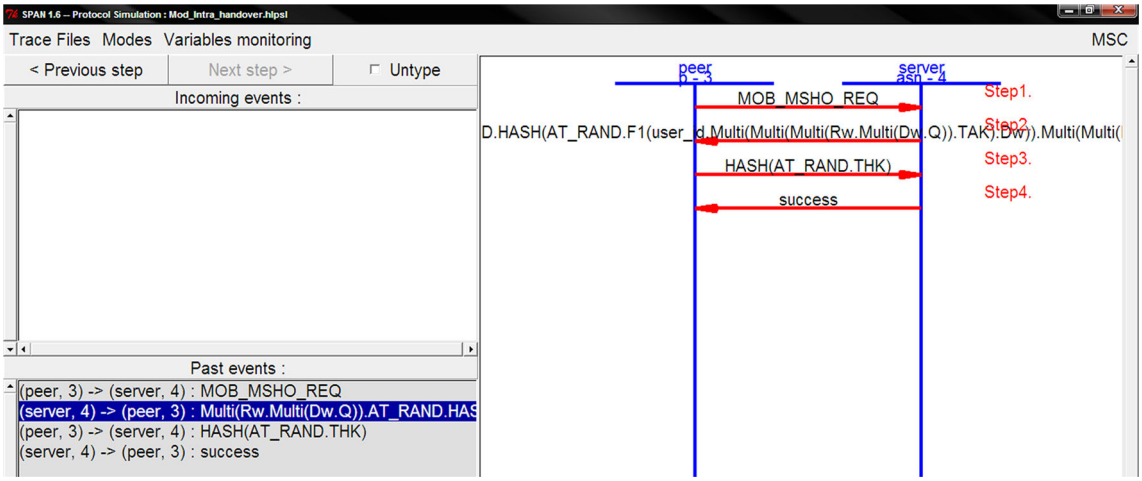

Fig. 11 R6 handover protocol simulation in SPAN

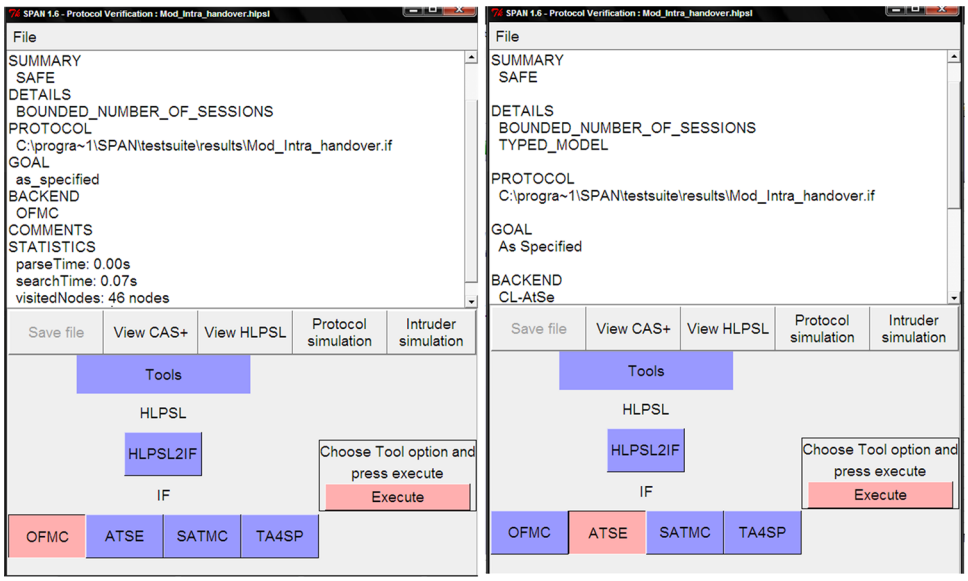

Fig. 12 R6 handover check message returned message by OFMC and CLATSE

7 Conclusion

A seamless handover in WiMAX architecture is absolutely required. The authentication delay has an impact on handover delay. A simplified authentication scheme will reduce handover delay and will increase the network performance. In this paper, we identified and analyzed the performance and security of the current WiMAX architecture. The proposed authentication method improves the performance of the handover protocol and reduces the authentication delay during the R6 and R3 handovers. This protocol also shows superior performance results in comparison to the standard handover method in terms of signaling cost and authentication delay. The security properties of our method are verified by using AVISA, which proves that it is safe to use and resists to all known attacks.

References

1. IEEE Standard for local and metropolitan area networks.: Air Interface for Fixed Broadband Wireless Access Systems. Part 16. Amendment 2 and Corrigendum 1. IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor1 (2005)
2. IEEE Standard for local and metropolitan area networks.: Air interface for broadband wireless access systems. Part 16. Amendment 3: Advanced air interface. IEEE Std 802.16m-2011. 6 May (2011)
3. Stallings, W.: Cryptography and Network Security, Principles and Practices, 3rd edn. Prentice Hall, Englewood Cliffs (2003)
4. Aboba, B.; Blunk, L.; Vollbrecht, J.; Carlson, J.; Levkowetz H.: Extensible Authentication Protocol. RFC 3748. June (2004)
5. ETEMAD, K.; LAIWiMAX, M.: Technology and Network Evolution. IEEE COMMUNICATIONS SOCIETY. (2010)
6. Chang, C.K.; Huang, C.T.: Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks. ICPPW. Xian. China. Sept (2007)

7. IEEE Standard for Local and Metropolitan Area networks.: Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems. IEEE Press (2004)
8. WiMAX Forum Network Architecture: Stage 2 Architecture Tenets. Reference Model and Reference Points. WMF-T37-001-R010v03. 1. January (2008)
9. IEEE Standard for local and metropolitan area networks: Mobility Sensitive Master Key Derivation and Fast Re-authentication for 802.16m. C802.16m-07/029. February (2007)
10. Rigney; Willens, C.; Rubens, S.; Simpson, A.: Remote Authentication Dial in User Service (RADIUS). IETF. RFC 2865. Jun (2000)
11. WiMAX Forum Network Architecture.: Stage 3 Detailed Protocols and Procedures. WiMAX Forum. Rel. 1, ver. 1.2. Jan. (2008)
12. Nguyen, T.N.; Ma, M.: Enhanced EAP-based pre-authentication for fast and secure inter-ASN handovers in mobile WiMAX networks. IEEE Trans. Wirel. Commun. **11**(6), 2173–2181 (2012)
13. Junbeom, H.; Hyeongseop, S.; Pyung, K.; Hyunsoo, Y.; Nah-Oak, S.: Security considerations for handover schemes in mobile wimax networks. In: IEEE WCNC 2008, Las Vegas, USA. March 31–April 3, pp. 2531–2536 (2008)
14. Hsu, S.F.; Lin, Y.: A key caching mechanism for reducing WiMAX authentication cost in handoff. IEEE Trans. Veh. Technol. **58**(8), 4507–4513 (2009)
15. Sridevi, B.; Rajaram, S.: Performance analysis of proposed cost reduction mechanisms for authentication in mobile WiMAX network entry process. Arab. J. Sci. Eng. (2014). doi:10.1007/s13369-014-1199-z
16. Cai, L.; Machiraju, S.; Chen, H.: CapAuth: a capability-based handover scheme. INFOCOM. March (2010)
17. Zhang, C.; Liu, R.; Chen, A.: A location privacy preserving authentication scheme in vehicular networks. WCNC 2008, pp. 2543–2548 (2008)
18. Kim, Y.; Ren, W.; Jiang, Y.; Zheng, J.: SFRIC: a secure fast roaming scheme in wireless LAN using ID-based cryptography. ICC, pp. 1570–1575 (2007)
19. Shahid, H.; Naeem, M.; Ibrahim, M.: A security architecture for wimax networks. Int. J. Comput. Appl. **50**(9), 35–39 (2012)
20. HankersonMenezes, D.; Vanstone, A.: Guide to Elliptic Curve Cryptography. Springer, New York (2004)
21. Al Shidhani, A.; Victor, C.M.: Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers. IEEE Trans. Depend. Secure Comput. **8**(5) (2011)
22. Ian, F.; Akyildiz; Wenye, W.: A dynamic location management scheme for next-generation multitier PCS systems. IEEE Trans. Wirel. Commun. **1**(1), 178–189 (2002)
23. Kassab, M.; Bonnin, J.; Belghith, A.: Fast and secure handover in WLANs: an evaluation of the signaling overhead. In: IEEE CCNC, pp. 770–775 (2008)
24. Lam, D.; Cox, D.; Widom, C.: Teletraffic modeling for personal communications services. IEEE Commun. Mag. **35**(2), 1–18 (1997)
25. Choi, H.H.; Song, O.; Cho, D.H.: Seamless handoff scheme based on pre-registration and pre-authentication for UMTS-WLAN interworking. Wirel. Pers. Commun. **41**(3), 345–364 (2007)
26. Prasithsangaree, P.; Krishnamurthy, P.: A new authentication mechanism for loosely coupled 3G-WLAN integrated networks. In: IEEE 59th vehicular technology conference, Spring, 2998–3003 (2004)
27. Mahdi, M.; Abd-ELdayem, M.; Elgamal, S.; Wan, T.: Security analysis end enhancement of authentication in CDMA based on elliptic curve cryptography. Res. J. Inf. Technol. **4**(3), 106–123 (2012)
28. IEEE Standard for local and metropolitan area networks.: IEEE 802.16m System Description Document. IEEE 802.16m-08/0034r2. http://ieee802.org/16/tgm/index.html (2009)
29. Hess, A.; Scha, G.: Performance evaluation of AAA/Mobile IP Authentication. In: Proceedings of 2nd Polish-German teletraffic symposium, PGTS 02, Poland (2002)
30. Armando, A.; Basin, D.; Cuellar, J.; Rusinowitch, L.; Vigano, M.: The AVISPA tool for the automated validation of internet security protocols and applications. CAV. LNCS **3576**, 281–285 (2005)
31. Glouche, Y.; Genet, T.: SPAN: a Security Protocol Animator for AVISPA—User Manual. IRISA. University Rennes 1. http://www.irisa.fr/lande/genet/span (2006)