J Supercomput (2016) 72:2734–2751
DOI 10.1007/s11227-015-1581-y

A symmetric key-based pre-authentication protocol for secure handover in mobile WiMAX networks

Jianhong Zhou[1,2] · **Maode Ma**[2] · **Yong Feng**[1] · **Thuy Ngoc Nguyen**[2]

Published online: 9 December 2015

Abstract Providing secured and seamless service is one of the most important aspects of mobile networks, particularly for mobile WiMAX systems. However, the long delay handover schemes brought by the time-consuming EAP-based authentication may cause service disruption when a mobile WiMAX user moves between the coverage areas of different base stations. In this paper, we propose a handover scheme using symmetric key cryptography and pre-authentication approach to shorten the delay while ensuring high security level for Mobile WiMAX handover. The scheme is proven by BAN logic to achieve the security goals of an authentication scheme. A performance analysis is also carried out to show the effectiveness of this scheme in reducing handover delay and saving computational resources.

Keywords Mobile WiMAX · Formal verification · Security · Handover · Pre-authentication

1 Introduction

Since 2005, the introduction of the IEEE 802.16e standard with mobility support [1] has enabled WIMAX users to get access to mobile broadband services. However, security has been the major concern in the deployment because many threats associated with different layers of the protocol stack exist in the mobile WiMAX systems. For instances, there are scrambling and jamming attacks at the physical layer and the

✉ Jianhong Zhou
zjh@e.ntu.edu.sg

1 Chengdu Information Technology of Chinese Academy of Science Co. Ltd, Chengdu, China

2 School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore, Singapore

issues of user authentication and data confidentiality at the MAC layer, while black-hole attacks and other miscellaneous attacks may impair the operations at the network layer etc…[2]. As a consequence, security issues become a vital requirement to prevent mobile WiMAX systems from the various attacks and to increase the reliability. Mobile WiMAX system allows a mobile station (MS) to handover between the coverage areas of different base stations (BSs) from the same or different access service networks (ASNs). For security purpose, the MS has to authenticate itself to the network through the target BS (tBS) or the target ASN gateway (tASN) before access to any service is granted. Currently, mobile WiMAX is using the extensible authentication protocol (EAP)-based authentication [3] for handover (HO) due to its flexibility and high security level. This authentication mechanism uses a backend authentication server (AS) and as a result, the authenticator does not need to be updated whenever there are new authentication methods. However, the EAP-based authentication involves time-consuming public key-based cryptographic operations and the authentication process requires several rounds of information exchange between the MS and the AS. As the result, the latency for a full EAP-based authentication can be 1000 ms, which is much longer compared to the recommended maximum HO latency of 150 ms for streaming applications.

Researchers have proposed various methods to reduce the authentication delay during WIMAX Hos without compromising security requirements. These methods mainly follow the two approaches, namely the re-authentication and the pre-authentication approaches. By re-authentication approaches [4–6], the authentication delay is reduced by reusing the secret information exchanged between the MS and the AS in the previous authentication session. In [4], the HOKEY working group has proposed the EAP-based re-authentication protocol (ERP), where the MS and the AS use the extended master session key (EMSK) from previous EAP authentication to derive the master session key (MSK) for the current authentication session. Thus, ERP has significantly reduced the delay caused by several rounds of EAP message exchange to the delay of a single round of ERP message exchange. Other proposals such as [5,6] allow the MSs to have instant access to the basic network services through a weak but fast authentication using previous credentials. The MS is then required to complete a stronger and more costly authentication in order to access services with higher security requirements. Re-authentication approaches focus on reducing the number of the messages exchanged and cryptographic operations, while by pre-authentication approaches [7–10], shared secret keys are computed by the MS and the AS before a HO so that only the TEK 3-way handshake is performed during the HO authentication. As the result, pre-authentication approach offers the shortest delay for the authentication signaling. Not only that, in this approach, the cryptographic material will not be reused, hence it is more secure compared to re-authentication approach. The HOKEY working group has proposed a pre-authentication model for the MS to pre-authenticate itself with multiple candidate authenticators before a HO happens [7]. Based on this model, an EAP-based pre-authentication scheme (EPA) is proposed for the inter-ASN Hos in [8]. Pre-authentication approach has also been applied into the intra-ASN Hos as in [9], by which the AS pre-distributes unique pair-wise master keys (PMKs) to neighbor BSs (nBSs) which are candidates for the future HO. One common drawback of these pre-authentication schemes is the wastage of unnecessary efforts for key exchange between

the MS and those neighbor ASNs/BSs which may be never roamed to. Recently, we have proposed a scheme called enhanced EAP-based pre-authentication scheme (EEP) [10] which overcome this drawback by allowing the MS to exchange the secret keys with the AS instead of the neighbor ASNs (nASNs). However, pre-authentication proposals such as the one in [8,10] have made use of public key cryptography, which can consume great amount of computational resources.

The authentication process may suffer negative effectiveness if its corresponding key management is weak in wireless networks. The key management issue has been addressed to allow users to generate public keys to achieve authentication, integrity, and confidentiality in WiMAX systems in [11]. Recent research works have focused on the interoperability between WiMAX systems and WiFi systems as the literatures [12–14] with different handover schemes designed to support WiFi-WiMAX integration in a heterogeneous network (HetNet). However, it is beyond the scope of this paper.

In this paper, as our major contribution, we propose a fast and secure Symmetric Keys for EAP-based pre-authentication protocol (SKEP) for the inter-ASN Hos. SKEP uses symmetric key cryptography to secure the pre-authentication message exchange with low demand of computational resource, thus making the HO authentication more efficient. By allowing the MS to exchange keying materials with the AS instead of nASNs, it can eliminate the wastage of unnecessary key exchanges. Moreover, since SKEP does not reuse secret key materials from the previous authentication session, it guarantees high level of security. BAN logic is used to prove that our proposed scheme can meet the security requirements of an authentication protocol.

The rest of this paper is organized as follows. In Sect. 2, we review the network model, Mobile WiMAX's standard HO procedure and the EAP-based authentication. The proposed SKEP scheme is presented in Sect. 3. The formal verification on the security functionality using BAN logic and the performance analysis of the proposed scheme are provided in Sects. 4 and 5 respectively. Finally, Sect. 6 concludes the paper. For the abbreviations of the terminologies used in our paper, please refer to the Appendix.

2 Background

2.1 Network model

The typical Mobile WiMAX system shown in Fig. 1 consists of three major types of equipment. They are the MSs, the ASNs owned by the network access provider (NAP), and the connectivity service networks (CSNs) owned by the network service provider (NSP). An ASN consists of multiple BSs and an ASN-GW. It offers radio access to the MSs. An ASN-GW is located at the boundary of the ASN to connect the BSs and the CSN which provides IP connectivity service to the MSs. It also acts as a proxy for the authentication between the MSs and the AS, which resides in the CSN. The IEEE802.16e standard specifies two types of Hos for Mobile WiMAX, namely intra-ASN HO and inter-ASN HO. The intra-ASN HO happens when a MS moves between BSs which belong to the same ASN. The inter-ASN HO happens when a MS

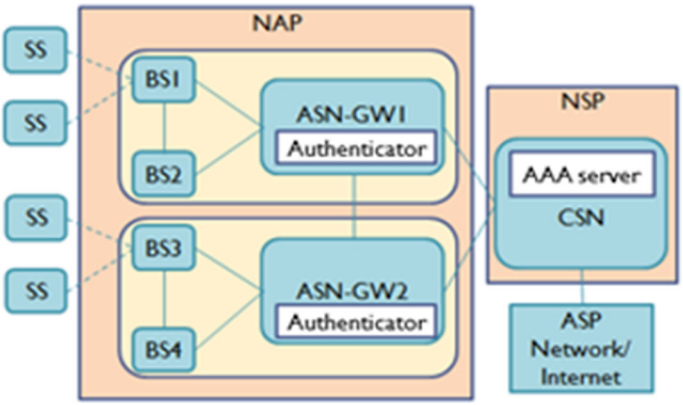

Fig. 1 The WiMAX network reference model

moves from the hBS in the coverage of the home ASN (hASN) to another BS in the coverage of a different ASN.

2.2 Standard handover procedure

In this section, the standard inter-ASN HO is described (Fig. 2). The HO decision can be triggered by a request from the MS or the hBS through MOB_MSHO-REQ or MOB_BSHO-REQ message, respectively. A list of nBSs which are candidates for HO is selected either by the MS or by the hBS. The hBS will send the HO notification messages to these candidates over the backbone network to notify that the MS intends to HO. Those nBSs which accept the HO request will send an accept response to the hBS and they become potential tBSs. The hBSs choose one from these potential tBSs and send a HO confirmation to the selected tBS. Thereafter, the hBS informs the MS of the selected tBS by sending the MS the MOB_BSHO-RSP message in the case of MS-initiated HO or the MOB_BSHO-REQ in the case of BS-initiated HO. Upon receiving this message, the MS makes its final HO decision and sends an MOB_HO-IND message to start the HO.

Upon receiving the MOB_HO-IND message, the hBS sets a timer to disconnect the MS and at the same time, the MS starts the synchronization and ranging process with the tBS, followed with the network re-entry procedure, which includes basic capability negotiation, authentication and registration. If the HO is successful, the MS can start using services provided by the new hBS.

2.3 The EAP-based authentication

The operation of the EAP transport layer security (EAP-TLS)-based authentication is shown in Fig. 3. The EAP-TLS-based authentication provides strong mutual authentication [15]. As a result, it has been selected by the WiMAX forum as one of the options for the MS-AS authentication. To start the authentication process, the MS

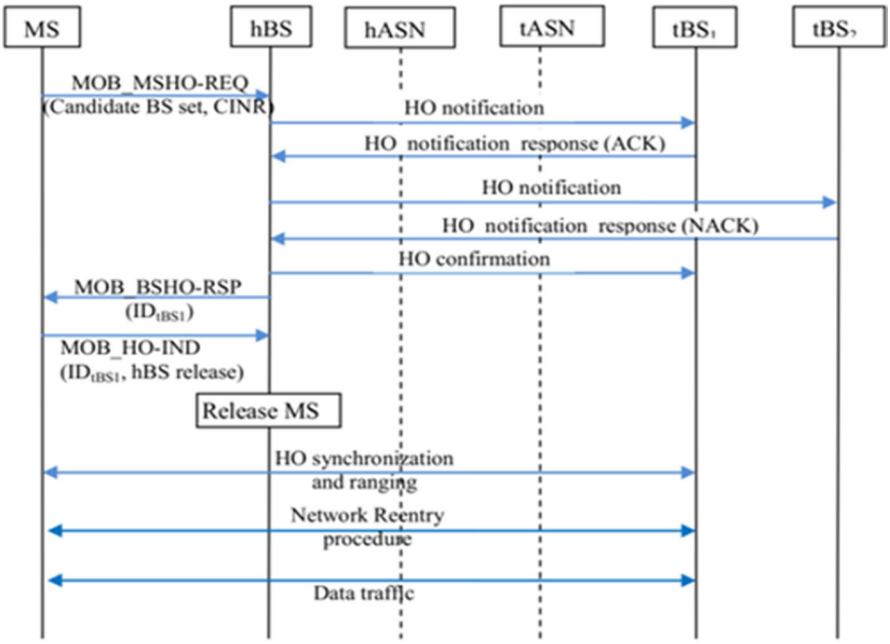

Fig. 2 The handover procedure in mobile WiMAX systems

sends a link-up requesting message to the BS, which is relayed to the authenticator in the ASN in order to notify the authenticator that a MS is connecting to the network. The authenticator acquires the MS's identity through the EAP Request/Identity and EAP Response/Identity messages and relays the response message to the AS over the RADIUS protocol [16]. From there, the MS and the AS exchange a few rounds of EAP-TLS authentication messages. If the MS is successfully authenticated, a 512-bit MSK is generated by both the MS and the AS and is transferred to the authenticator by the AS. The PMK is derived by truncating the MSK to 160 bits. The PMK is used to generate the authorization key (AK). The AK is transferred to the hBS, which is used for the security association-traffic encryption key (SA-TEK) 3-way handshake and key exchange. At the end of the authentication, the TEK for data encryption is shared between the MS and the hBS. The SKEP scheme is designed based on the EAP-TLS authentication.

3 The proposed solution

In this section, we present our solution of the SKEP scheme. Basically, our scheme is an EAP-based pre-authentication protocol where the MS and the AS exchange a 48-byte pre-master secret (PMS) and nonce through pre-authentication messages to generate the MSK for future HO. This MSK will be delivered to the tASN during the HO initialization process so that the tASN and the MS can straightaway generate the AK and proceed with the SA-TEK 3-way handshake. The MSK and EMSK from

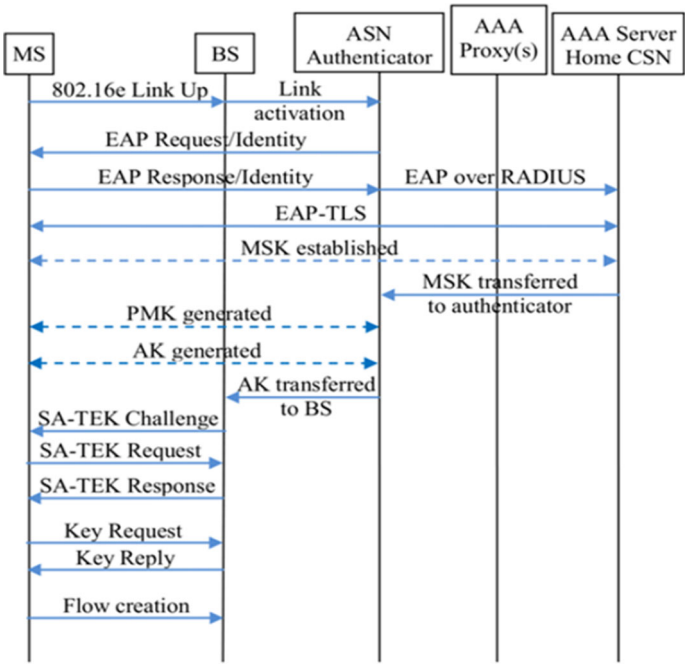

Fig. 3 EAP-TLS authentication

Table 1 Notations

Notation	Definition
$ENC_K(X)$	Encrypt X using K
$DEC_K(X)$	Decrypt X using K
$HMAC_K(X)$	Generate HMAC for message X using K
$VER_K(X, S)$	Verify message X with the corresponding message authentication code S using K
ID_A	Identifier of A
N_A	Nonce generated by A
$X \parallel Y$	Concatenation of X and Y

the current authentication session are used to derive symmetric keys to encrypt and protect the integrity of the pre-authentication messages. With the newly proposed scheme, we aim to reduce long HO latency which is a well-known bottle neck of the mobile WiMAX systems and, at the same time, ensure high security level of an authentication protocol. Compared to other pre-authentication protocols, the SKEP protocol uses symmetric cryptography instead of public key cryptography, resulting in low computational resource consumption and faster pre-authentication process. The notations used are shown in Table 1. The procedure of the SKEP scheme (Fig. 4) is as follows:

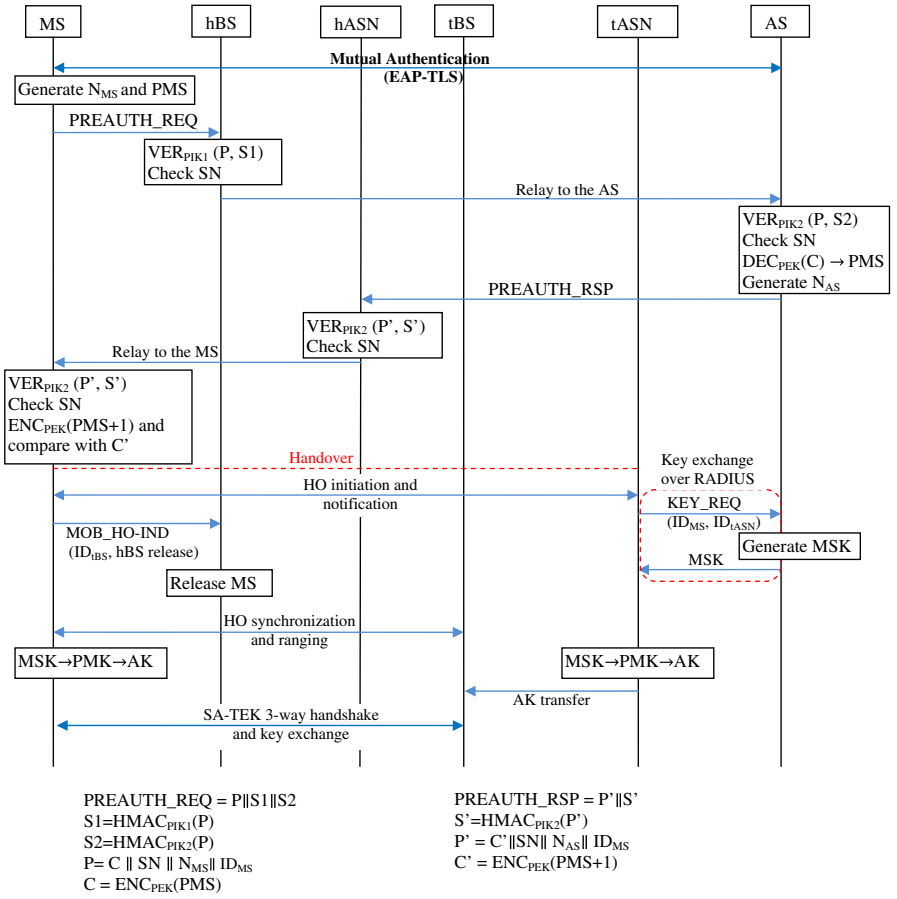

Fig. 4 The SKEP scheme

Initialization step: when a MS first joins in the network, it performs the full EAP-TLS authentication with the hASN. SKEP scheme can be used for the next and future authentication sessions. The SKEP scheme is an EAP-based pre-authentication protocol. It is designed in such a way that the secret keys shared among communication entities after each authentication session by the SKEP scheme will be same as those by using the EAP-TLS authentication protocol. How secret keys are shared among communication entities are specified in Table 2. In order to provide security for the SKEP scheme, we propose the derivation of three new keys: two pre-authentication integrity keys (PIK1 and PIK2) and a pre-authentication encryption key (PEK) from the AK, the MSK, and the EMSK, respectively using the Dot16KDF function, which is specified in [1]:

$$\text{PIK1} = \text{Dot16KDF (AK, “PIK1”, 160)} \tag{1}$$

$$\text{PIK2} = \text{Dot16KDF (MSK, “PIK2”, 160)} \tag{2}$$

$$\text{PEK} = \text{Dot16KDF (EMSK, “PEK”, 128).} \tag{3}$$

Table 2 Secret keys

Secret key	Entities that possess the key
EMSK, PEK	AS, MS
MSK, PIK2	AS, MS, hASN
AK, PIK1	MS, h ASN, hBS

The PIK1 is known by the MS, the hASN, and the hBS, and the PIK2 is known by the MS, the hASN, and the AS. They are used to calculate the Hash-based Message Authentication Codes (HMACs) to protect the integrity of the SKEP messages. The PEK is only known by the MS and the AS, and it is used to encrypt the PMS. The fact that each key is known to certain communication entities will make sure that each communication entity can only access certain information from the pre-authentication messages.

The PIK1 is known by the MS, the hASN, and the hBS, and the PIK2 is known by the MS, the hASN, and the AS. They are used to calculate the hash-based message authentication codes (HMACs) to protect the integrity of the SKEP messages. The PEK is only known by the MS and the AS, and it is used to encrypt the PMS. The fact that each key is known to certain communication entities will make sure that each communication entity can only access certain information from the pre-authentication messages.

Step 1: After a successful HO to the hASN, the MS initiates a pre-authentication procedure by sending the PREAUTH_REQ message to the hBS. The PREAUTH_REQ message is constructed as followed:

$$P = ENC_{PEK}\,(PMS) \parallel SN \parallel N_{MS} \parallel ID_{MS} \tag{4}$$

$$PREAUTH\_REQ = P \parallel HMAC_{PIK1}\,(P) \parallel HMAC_{PIK2}\,(P)\,. \tag{5}$$

In the above equation, the PMS and the nonce (N_{MS}) are generated by the MS. The PMS is the secret keying material to be sent to the AS and it is encrypted using the PEK. The ID_{MS} is the 48-bit MS' MAC address. The sequence number (SN) is 16 bits and aids in matching the PREAUTH_RSP with the corresponding PREAUTH_REQ. It is incremented whenever the MS initiates a new pre-authentication session. All communication entities maintain a record of the SN in the last request message received from the MS to prevent replay attacks.

Upon receiving the PREAUTH_REQ message from the MS, the hBS first checks the received SN, which must be greater than the SN stored in its memory for the message to be fresh. Next, it verifies the message's origin and integrity by calculating the HMAC using the PIK1 and compares it with the first HMAC in the message. If the HMAC is the same and the message is fresh, the hBS sends the message to the hASN, which will be relayed immediately to the AS. Otherwise, the message will be discarded.

Step 2: At the AS, the PREAUTH_REQ message is put through a verification process similar to that at the hBS. The only difference is that instead of using the PIK1

to calculate the HMAC, the AS uses the PIK2 and the calculated HMAC is compared with the second HMAC in the message. If the message is genuine, the AS decrypts the cipher text using the PEK to obtain the PMS and keeps a record of the PMS and the N_{MS}. The PREAUTH_RSP message is constructed as followed:

$$P' = ENC_{PEK}\,(PMS + 1) \parallel SN \parallel N_{AS} \parallel ID_{MS} \tag{6}$$

$$PREAUTH\_RSP = P' \parallel HMAC_{PIK2}\left(P'\right) \tag{7}$$

This message is sent to the MS to acknowledge that the AS has received the secret PMS, and also to deliver the nonce N_{AS} which is randomly generated by the AS. To prevent replay attack, the AS increments the PMS by 1 and encrypts it using the PEK.

This message is then sent to the hASN. Similar to the step 1, the hASN will verify the message and relay it to the hBS. We assume that the link between the hBS and the hASN is a secure-wired link; thus, the hBS does not have to check the message but relays it directly to the MS. The MS verifies the correctness of the received message and keeps a record of the N_{AS}. It also decrypts the cipher text using the PEK to confirm whether the AS has obtained the correct PMS.

Step 3: A HO begins with the MS's decision to HO from the hBS to a tBS. Following the standard HO procedure, the hBS chooses one from the potential tBSs and sends a HO confirmation to the tBS over the backbone. Since this message passes through the tASN, it serves as a notification to inform the tASN that it is selected for the HO. As soon as it receives this notification, the tASN sends a KEY_REQ message to the AS containing the ID_{MS} and ID_{tASN}. The AS will retrieve the PMS, N_{MS} and N_{AS} corresponding to the ID_{MS} and derive the MSK in a way similar to that of the EAP-TLS key derivation in [15].

$$\text{Master\_secret} = \text{TLS} - \text{PRF} - 48\,(\text{PMS}, \text{“master secret”}, N_{MS} \parallel N_{AS} \parallel ID_{tASN}) \tag{8}$$

$$\text{Key\_Material} = \text{TLS} - \text{PRF} - 128(\text{Master\_secret}, \text{“client EAP encryption”}, N_{MS} \parallel N_{AS} \parallel ID_{tASN}) \tag{9}$$

$$MSK = \text{Key\_Material}\,(0, 63) \tag{10}$$

More information on the TLS-PRF-X function can be found in [17]. By using the same key derivation algorithm as the EAP-TLS scheme, the SKEP scheme has guaranteed that the other keying materials such as the EMSK and the initialization vector (IV) can be derived so that the key hierarchy of EAP-based authentication is kept unchanged.

After deriving the MSK, the AS sends it back to the tASN. The KEY_REQ and the delivery of the MSK are protected using RADIUS-key wrap, which can be found in [18]. Meanwhile, the MS can derive the MSK using the same formula. After the above steps, the MS and the tASN share the same MSK to compute the AKand can start the SA-TEK 3-way handshake immediately after the ranging process. By using the SKEP, the long delay caused by EAP-based authentication can be omitted, thus making the HO significantly faster.

4 Formal verification

The BAN logic [19] is used for formal verification of SKEP. The BAN logic is a popular formal method to analyze and verify authentication protocols. By the BAN logic, the verification of the protocol follows three stages. The first stage is to transform the original protocol into an idealized one where the message exchange is expressed as a sequence of formal steps. The syntax for each formal step is A $\rightarrow$ B: X, where A and B are the communicating entities and X is a statement. The second stage is to identify and formally express the assumptions under the initial state of the protocol. The final step is to iteratively apply logical postulates using the given initial assumptions until meaningful results are obtained. The notation used throughout our verification follows the guideline in [19]. Since the BAN logic provides no notation and rule for the HMAC operation, we use $\langle P \rangle_K$ to express $HMAC_K(P)$.

4.1 Idealization of the protocol

The idealization of the protocol's message exchanges follows closely the syntax described previously. The hASN and the hBS are included in the protocol idealization so that we can verify the possibility of attacks on these entities. The PMS has been replaced by the statement that the PMS is a shared secret between the MS and the AS. ID_{MS} is omitted since it is a plain text which does not contribute to the logical properties of the protocol. However, the plain texts nonce N_{MS} and N_{AS} are still included since they are required for the generation of the MSK. Besides, it is also necessary to verify that both of the MS and the AS have the same nonce at the end of the pre-authentication process. PMS+1 is changed to PMS because the purpose of adding 1 to PMS is to prevent the same cipher text to be sent in the request and response message. The differentiation between two cipher text is reflected in the idealization in the "from" field.

M1: $\text{MS} \rightarrow \text{hBS} : \langle \{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{MS} \rangle_{\text{PIK1,PIK2}}$ from MS

M2: $\text{hBS} \rightarrow \text{AS} : \langle \{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{MS} \rangle_{\text{PIK1,PIK2}}$ from MS

M3: $\text{AS} \rightarrow \text{hASN} : \langle \{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{AS} \rangle_{\text{PIK2}}$ from MS

M4: $\text{hASN} \rightarrow \text{MS} : \langle \{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{AS} \rangle_{\text{PIK2}}$ from MS

4.2 Establishment of initial assumption

The initial assumptions are as followed:

A11: MS believes $\text{MS} \overset{\text{PIK1}}{\longleftrightarrow} \text{hBS}$
A12: hBSbelieves $\text{MS} \overset{\text{PIK1}}{\longleftrightarrow} \text{hBS}$
A21: MS believes $\text{MS} \overset{\text{PIK2}}{\longleftrightarrow} \text{hASN}$
A22: hASN believes $\text{MS} \overset{\text{PIK2}}{\longleftrightarrow} \text{hASN}$
A23: MS believes $\text{MS} \overset{\text{PIK2}}{\longleftrightarrow} \text{AS}$

A24: AS believes MS $\overset{\text{PIK2}}{\longleftrightarrow}$ AS
A31: MS believes MS $\overset{\text{PEK}}{\longleftrightarrow}$ AS
A32: AS believes MS $\overset{\text{PEK}}{\longleftrightarrow}$ AS
A41: MS believes MS $\overset{\text{PMS}}{\rightleftharpoons}$ AS
A42: MS believes N_{MS}
A43: AS believes N_{AS}
A51: AS believes (MS controls MS $\overset{\text{PMS}}{\rightleftharpoons}$ AS)
A61: MS believesfresh (SN)
A62: hBS believesfresh (SN)
A63: hASN believesfresh (SN)
A64: AS believes fresh (SN)

The first group of two assumptions (A11, A12) indicates that PIK1 is a shared secret key known by the MS and the BS. Although PIK1 is known by the hASN, since it is not used by this entity, there is no need to include this fact in the assumptions. The second group of 4 assumptions (A21–A24) indicates that PIK2 is a shared secret among the MS, the hASN, and the AS. The assumptions in the third group (A31, A32) indicate that PEK is only shared between the MS and the AS. Fourth group assumptions indicate that the MS knows the shared secret PMS between the MS and the AS. And the MS and the AS each generate a nonce, namely the N_{MS} and the N_{AS}, respectively. The assumption A51 shows that the AS trusts the MS to generate a good shared secret PMS. The last group (A61–A64) indicates that the freshness of the SN can be checked by all four communication entities.

4.3 Analysis of the protocol

After the idealized protocol and the initial assumptions are defined, the protocol can be analyzed as follows.

From M1, we can derive:

(1) hBS sees $\langle\{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{MS}\rangle_{\text{PIK1,PIK2}}$, by Annotation rule

(2) hBS believes MS said $(\{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{MS})$, by Message Meaning rule, using (1) and A12

(3) hBS believes MS believes $(\{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{MS})$, by Nonce Verification rule, using (2) and A62

From M2, we derive:

(4) AS sees $\langle\{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{MS}\rangle_{\text{PIK1,PIK2}}$, by Annotation rule

(5) AS believes MS said $(\{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{MS})$, by Message Meaning rule, using (4) and A24

(6) AS believes MS believes $(\{\text{MS} \overset{\text{PMS}}{\rightleftharpoons} \text{AS}\}_{\text{PEK}}, \text{SN}, N_{MS})$, by Nonce Verification rule, using (5) and A64

(7) AS believes MS believes MS $\overset{\text{PMS}}{\rightleftharpoons}$ AS, by Belief Conjuncatenation rule, using (6) and A32

(8) AS believes MS $\overset{\text{PMS}}{\rightleftharpoons}$ AS, by Jurisdiction rule, using (7) and A51

(9) AS believes MS believes N_{MS}, by Belief Conjuncatenation rule, using (8) and A32

Following the similar steps of the deduction from **M1** and **M2**, we can obtain the final results of the other two messages as follows.

MS believesMS $\overset{\text{PMS}}{\rightleftharpoons}$ AS

AS believesMS $\overset{\text{PMS}}{\rightleftharpoons}$ AS

MS believes AS believesMS $\overset{\text{PMS}}{\rightleftharpoons}$ AS

AS believes MS believesMS $\overset{\text{PMS}}{\rightleftharpoons}$ AS

MS believes AS believes N_{AS}

MS believes AS believes N_{MS}

It is shown from the above results that SKEP has achieved the ultimate goals of an authentication protocol. First, the PMS is verified to be the secret shared only between the MS and the AS which implies that no party except the MS and the AS knows or can deduce this secret. At the end of the pre-authentication process, both the MS and the AS have confirmed their possession of the PMS. The final two deductions indicate that both the MS and the AS possess the same nonce N_{MS} and N_{AS}.

On the other hand, we also derive that

From **M1:** hBS believes MS believes ($\{MS \overset{\text{PMS}}{\rightleftharpoons} AS\}_{PEK}$, SN, N_{MS})

From **M2**: AS believes MS believes ($\{MS \overset{\text{PMS}}{\rightleftharpoons} AS\}_{PEK}$, SN, N_{MS})

From **M3**: hASN believes AS believes ($\{MS \overset{\text{PMS}}{\rightleftharpoons} AS\}_{PEK}$, SN, N_{AS})

From **M4**: MS believes AS believes($\{MS \overset{\text{PMS}}{\rightleftharpoons} AS\}_{PEK}$, SN, N_{MS})

These derivation results show that it is not possible to perform the replay attack on any of these four messages. For the MSK key exchanged between the tASN and the AS, the security is guaranteed because it is protected using the RADIUS key wrap protocol, which has been used widely for the delivery of keying material from the server to the authenticator.

5 Performance evaluation

5.1 Performance analysis of the pre-authentication process

When analyzing the performance of pre-authentication-based protocols, two most important factors to be considered are the number of cryptographic operations

and the pre-authentication latency. The former factor defines how much computational resource has been consumed by the communication entities during the pre-authentication process as cryptographic operations are the main source of computational resource consumption. The latter factor defines how fast this process is. The faster the pre-authentication process, the higher possibility that the MS successfully exchanges the PMS with the AS before a HO happens. In this paper, we compare the SKEP with two other protocols, the EPA and the EEP.

5.1.1 Number of cryptographic operations

Cryptographic operations include the digital signature and verification, the certificate validation, the hash function, which is used to calculate the HMAC in the EEP and the SKEP, the encryption and decryption. In this analysis, the RSA-1024 algorithm is used to calculate digital signatures and for the public key encryption used in the EEP and the EPA. AES/CTR-128 is used for encryption of PMS in the SKEP. The number of nASNs is n.

The number of cryptographic operations is shown in Table 3. Compared to the EPA scheme which has the number of cryptographic functions performed by the hASN and the MS increases linearly with the number of nASNs, the EEP and the SKEP schemes provide a consistent performance with a constant and minimum number of cryptographic functions. The reason behind this improvement is that the EEP and the SKEP allow the MS to exchange keying materials with the AS and the AS will be responsible to distribute the MSK to the tASN upon the confirmation of a HO. Thus, they overcome the main drawback of the pre-authentication approach, which is that the MS wastes unnecessary power for the key exchange with other nASNs that it may never roam to. Similarly, the other nASNs would not waste their resources for the extra key exchanges.

Moreover, another enhancement of the SKEP compared to the EAP-TLS authentication as well as the EPA and the EEP schemes is that our proposed scheme makes use of symmetric key cryptography and hash function to protect the pre-authentication message exchange, which requires much less computational resource compared to the heavy public key operations such as certificates verifications, signature signing,

Table 3 Number of cryptographic operations

	EPA			EEP			SKEP			
	MS	hASN	nASN	MS	hBS	AS	MS	hBS	hASN	AS
Certificate verification	n	0	0	0	0	0	0	0	0	0
HMAC (SHA-1)	0	0	0	1	1	0	3	1	1	2
Asymmetric encryption	n	0	1	1	0	0	0	0	0	0
Asymmetric decryption	n	0	1	0	0	1	0	0	0	0
Symmetric encryption/decryption	0	0	0	0	0	0	2	0	0	2
Signature	n	0	1	1	0	1	0	0	0	0
Verification	n	$2n$	1	1	2	1	0	0	0	0

and verifications involved in the two other schemes. As mentioned before, the public key cryptographic operations consume great computational resource and processing power of the communication entities especially for the MS, because of the limited processing power due to its small physical size and less battery capacity. The computation required by public key cryptographic operations, especially digital signature operations and decryption [20], can significantly affect performance of the MS's other functions. Instead of performing 3 public key cryptographic operations and 1 hash function as the EEP, which would take several milliseconds, or even worse, $4n$ operations as the EPA, the SKEP only requires the MS to perform 3 hash functions and 2 symmetric cryptographic operations, which takes only several microseconds. This can effectively reduce the pre-authentication latency, which will be calculated in the next section.

5.1.2 Pre-authentication latency

The pre-authentication latency determines how fast the pre-authentication process can complete. It should be noted that the MS can perform pre-authentication and normal data transmission at the same time. Denoted as $l_{PREAUTH}$, it can be defined as the time elapsed between the moment of the transmission of the first pre-authentication message (the NBL message by the EPA, the PREAUTH_INIT message by the EEP and the PREAUTH_REQ message by the SKEP) until the moment of the reception of the last PREAUTH_RSP message. It consists of the delay of the computing process and the transmission and propagation delays of all pre-authentication messages. To evaluate the delay of the computing process, which is the time used for the cryptographic operations, we make use of the speed benchmark provided in [21] for the hBS, the hASN and the AS. We assume that the MS's processing power is half of the hBS's. The HMAC calculation delay for the EEP and the SKEP is different due to the different sizes of the input to the hash function.

In order to calculate the transmission delay, we make some assumptions to the network parameters. The uplink and downlink data rates are assumed to be 1.68 and 3.744 Mbps, respectively. All backbone connections among the BS, the ASN-GWs, and the AS are via wired links with bandwidth of 1000 Mbps. Each certificate has the size of 1 KB. All the messages are management messages, which include 6 bytes of MAC header, 14 bytes of Ethernet header, 20 bytes of IP header, 8 bytes of UDP header, 1 byte of management message type, 4 bytes of CRC, and other TLV attributes. Based on this, we can construct the size of each pre-authentication message and the total transmission time. The notation and corresponding values are summarized in Table 4.

For the EPA, the pre-authentication finishes when all secret keys are delivered from nASNs to the MS:

$$\begin{aligned} l_{PREAUTH\_EPA} &= n \times \left(t_{cert\_MS} + t_{RSAenc\_MS} + t_{RSAdec\_MS} + t_{sign\_MS} + t_{ver\_MS}\right) \\ &\quad + (2n+1) \times t_{ver\_ASN} + t_{RSAenc\_ASN} + t_{RSAdec\_ASN} + t_{sign\_ASN} \\ &\quad + (n+2) \times d_{MS-BS} + (n+1) \times (d_{BS-ASN} + d_{ASN}) + T_{EPA} \\ &= 80.93 \end{aligned} \tag{11}$$

Table 4 Notation in the expressions of pre-authentication latency

		MS	BS/ASN/AS
t_{cert}	Certificate verification delay	0.16 ms	0.08 ms
t_{EEP_HMAC}	HMAC calculation delay (SHA-1) for EEP	13.04 μs	6.52 μs
t_{SKEP_HMAC}	HMAC calculation delay (SHA-1) for SKEP	0.78 μs	0.39 μs
t_{RSAenc}	RSA 1024 encryption delay	0.16 ms	0.08 ms
t_{RSAdec}	RSA 1024 decryption delay	2.92 ms	1.46 ms
t_{AES}	AES/CTR 128 encryption/decryption delay	0.66 μs	0.33 μs
t_{sign}	Signature calculation delay	2.96 ms	1.48 ms
t_{ver}	Signature verification delay	0.14 ms	0.07 ms
T_{EPA}	Total transmission time for EPA	21.37 ms	
T_{EEP}	Total transmission time for EEP	4.38 ms	
T_{SKEP}	Total transmission time for SKEP	1.1 ms	
d_{MS-BS}	Average propagation delay between the MS and the BS	10 μs	
d_{BS-ASN}	Average propagation delay between the BS and the hASN-GW	2 ms	
d_{ASN}	Average propagation delay between two ASN-GWs	2 ms	
d_{ASN-AS}	Average propagation delay between the ASN-GW and the AS	2 ms	
n	Number of nASNs	5	

For the EEP and the SKEP, the PREAUTH_RSP message sent by the AS serves as the acknowledgement message to complete the pre-authentication. The pre-authentication latency is calculated as followed:

$$\begin{aligned} l_{PREAUTH\_EEP} &= t_{EEP\_HMAC\_MS} + t_{RSAenc\_MS} + t_{sign\_MS} + t_{ver\_MS} \\ &\quad + t_{EEP\_HMAC\_BS} + 3 \times t_{ver\_AS} + t_{RSAdec\_AS} + t_{sign\_AS} + 3 \times d_{MS-BS} \\ &\quad + 2 \times (d_{BS-ASN} + d_{ASN-AS}) + T_{EEP} = 21.76\,\text{ms} \end{aligned} \tag{12}$$

$$\begin{aligned} l_{PREAUTH\_SKEP} &= 3 \times t_{SKEP\_HMAC\_MS} + 2 \times t_{AES\_MS} \\ &\quad + 4 \times t_{SKEP\_HMAC\_BS} + 2 \times t_{AES\_AS} \\ &\quad + 2 \times (d_{MS-BS} + d_{BS-ASN} + d_{ASN-AS}) + T_{SKEP} = 5.13\,\text{ms} \end{aligned} \tag{13}$$

As shown in (Eqs. 11, 12 and 13), the proposed SKEP scheme has reduced significantly the total processing time for cryptographic operations compared to the EPA and the EEP scheme by using symmetric cryptography instead of public key cryptography. The SKEP scheme only requires one round trip of message exchange between the MS and the AS, while the EEP requires additional message sent from the BS to the MS to initialize the pre-authentication process and the EPA requires n round trips between the MS and the nASNs. Not only that, the number of bits of information exchanged

over the air is the smallest by the SKEP scheme since there is no certificate and only one key transmitted. As the result, SKEP has the shortest total transmission time as well as the shortest propagation delay among the three schemes.

In short, the pre-authentication latency has been significantly reduced by the SKEP scheme, more than 75 % compared to the EEP scheme and more than 90 % compared to the EPA scheme in the case of 5 nASNs. As explained before, it is extremely critical for a pre-authentication-based HO, as it is only successful if the pre-authentication can be completed before the HO starts. The shorter the pre-authentication latency is, the higher the possibility that the HO is successful.

5.2 Handover latency

During HO, the difference between SKEP and other pre-authentication schemes such as the EPA, the EEP, and the HOEA is the one additional exchange of MSK between the tASN and the AS upon the confirmation of HO, which is necessary to omit the consumption of communication resources required for distributing keying materials to possible nASNs that the MS may never roam to. However, this addition key exchange is performed in parallel with the HO synchronization and ranging process between the MS and the tBS. The recommended setting for a ranging duration in a HO is around 20 ms [22], which is longer than the time required for the MSK key exchange, which requires less than 10 ms. Thus, the additional key exchange will not introduce any extra delay to the HO latency. As the result, the HO latency of the SKEP is the same as that of other pre-authentication-based schemes such as the EPA, the EEP, and the HOEA. The common and most significant contribution of pre-authentication-based schemes is that they totally omit the long authentication latency of the full EAP authentication from the total HO latency. As the result, the authentication latency in HO is only the time required for the SA-TEK 3-way handshakes. Compared to re-authentication-based schemes such as the ERP which still require single or several round trips of authentication message exchange, our scheme still provides shorter HO latency.

6 Conclusion

In this paper, a pre-authentication scheme, SKEP, is proposed to reduce the authentication delay in the HO for the Mobile WiMAX networks. The proposed scheme uses symmetric key encryption for the delivery of the secret key, the mutual authentication of the MS and the AS, and the integrity protection of the pre-authentication messages. The SKEP is formally verified by the BAN logic and is proven to achieve high level of security and robustness. Through comparing with other pre-authentication schemes EPA and EEP, the SKEP has shown significant improvement in efficient usage of computational resources and in reducing the pre-authentication delay while keeping the minimum HO delay. We believe that the proposed authentication scheme is both secure and efficient, which makes it to be a competitive candidate for the efficient HO schemes.

Acknowledgments This paper is supported by National Natural Science Foundation of China (the Number is 11171053) and Major State Basic Research Development Program of China (973 program, the Number is 2011CB302402).

Appendix

The abbreviations of the terminologies

WiMAX	Worldwide interoperability for microwave access
MS	Mobile station
BS	Base station
AS	Authentic server
ASN	Access service networks
tBS	Target base station
tASN	Target access service networks
EAP	Extensible authentication protocol
HO	Handover
ERP	EAP-based re-authentication protocol
EMSK	Extended master session key
MSK	Master session key
EPA	EAP-based pre-authentication scheme
PMKs	Pair-wise master keys
nBSs	Neighbor BSs
EEP	Enhanced EAP-based pre-authentication scheme
HetNet	Heterogeneous network
SKEP	Symmetric keys for EAP-based pre-authentication protocol
NAP	Network access provider
CSNs	Connectivity service networks
NSP	Network service provider
EAP-TLS	EAP transport layer security
SA- TEK	Security association-traffic encryption key
PIK	Pre-authentication integrity key
HMACs	Hash-based message authentication codes
PEK	Pre-authentication encryption key
PMS	Pre-master secret
AK	Authorization key

References

1. IEEE Standard 802.16e (2005) In: Part 16: air interface for fixed and mobile broadband wireless access systems
2. Jatav VK, Singh V (2014) Mobile WiMAX network security threats and solutions: a survey. In: Proceedings of 2014 international conference computer and communication technology, pp 135–140
3. Aboba B, Blunk L, Vollbrecht J, Carlson J, Levkowetz H (2004, 7 September 2011) Extensible Authentication Protocol (EAP). [RFC 3748]. http://tools.ietf.org/pdf/rfc3748.pdf
4. Narayanan V, Dondeti L (2008, 09 December 2010) EAP Extensions for EAP Re-authentication Protocol (ERP). [RFC 5296]. http://www.rfc-editor.org/rfc/rfc5296.txt

5. Aura T, Roe M (2005) Reducing reauthentication delay in wireless networks. In: Proceedings of first international conference on security and privacy for emerging areas in communications networks (SecureComm 2005), Athens, pp 139–148
6. Kim Y, Bahk S (2008) Enhancing security using the discarded security information in mobile WiMAX networks. In: 2008 IEEE global telecommunications conference, New Orleans, 2008, pp 1–5
7. Ohba Y, Wu Q, Zorn G (2010, 09 December 2010) Extensible Authentication Protocol (EAP) early authentication problem statement. [RFC 5836]. http://www.rfc-editor.org/rfc/rfc5836.txt
8. Sun HM, Lin YH, Chen SM, Shen YC (2007) Secure and fast handover scheme based on pre-authentication method for 802.16/WiMAX infrastructure networks. In: TENCON—Proceedings of IEEE region 10th annual international conference, Taipei, pp. 1–4
9. Junbeom H, Hyeongseop S, Pyung K, Hyunsoo Y, Nah-Oak S (2008) Security considerations for handover schemes in mobile WiMAX networks. In: 2008 IEEE wireless communications and networking conference, 31 March–3 April 2008, Piscataway, 2008, pp 2531–2536
10. Thuy Ngoc N, Maode M (2012) Enhanced EAP-based pre-authentication for fast and secure inter-ASN handovers in mobile WiMAX networks. IEEE Trans Wireless Commun 11:2173–2181
11. Tiwari H, Chaurasia BK (2014) In: Proceeding of 2014 fourth international conference on communication systems and network technologies (CSNT 2014), pp 669–672
12. Sarma A, Chakraborty S, Nandi S (2015) Deciding handover points based on context aware load balancing in a WiFi-WiMAX heterogeneous network environment. IEEE Trans Veh Technol PP(99):1–10
13. Rajule N, Ambudkar B (2015) Seamless and optimised vertical handover algorithm. In: Proceeding of 2015 international conference on computing communication control and automation (ICCUBEA 2015), pp 195–199
14. Liu C-Y, Leu F-Y, Liu J-C, Castiglione A, Palmieri F (2015) Heterogeneous network handover using 3GPP AND SF. In: Proceeding of 2015 IEEE 29th international conference on advanced information networking and applications (AINA 2015), pp 171–175
15. Simon D, Aboba B, Hurst R (2008, 09 December 2010) The EAP-TLS Authentication Protocol. [RFC 5216]. http://www.rfc-editor.org/rfc/rfc5216.txt
16. Zorn G (2010, 09 December 2010) RADIUS attributes for IEEE 802.16 Privacy Key Management Version 1 (PKMv1) Protocol support. [RFC 5904]. http://www.rfc-editor.org/rfc/rfc5904.txt
17. Dierks T, Rescorla E (2008, 09 December 2010) The Transport Layer Security (TLS) Protocol Version 1.2. [RFC 5246]. http://www.rfc-editor.org/rfc/rfc5246.txt
18. Zorn G, Zhang T, Walker J, Salowey J (2011, 30th August 2012) Cisco Vendor-Specific RADIUS attributes for the delivery of keying material. [RFC 6218]. http://tools.ietf.org/pdf/rfc6218.pdf
19. Burrows M, Abadi M, Needham RM (1990) A logic of authentication. ACM Trans Comput Syst 8:18–36
20. Jonsson J, Kaliski B (2003, 11 December 2010) Public-key cryptography standards (PKCS) #1: RSA cryptography specifications Version 2.1. [RFC 3447]. http://www.rfc-editor.org/rfc/rfc3447.txt
21. (29 September 2012) Crypto++ 5.6.0 Benchmarks. http://www.cryptopp.com/benchmarks.html
22. Ye Y, Yi Q, Sharif H (2010) Performance analysis of IEEE 802.16e handover with RSA-based authentication. In: 2010 IEEE International Conference on Communications, ICC 2010 23-27 May 2010, Piscataway, p 5