IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2, April-May, 2013
ISSN: 2320 - 8791
www.ijreat.org

Active EAP Protocol for Secure Inter ASN Handover in Mobile WiMAX Networks

Subhashini.S

Department of Computer Science and Engineering,
G.K.M.College of engineering and technology,
Chennai, Tamilnadu, India.

ABSTRACT

WiMAX, or Worldwide Interoperability for Microwave Access, is an emerging technology based on the IEEE 802.16 standard for a Metropolitan Area. For any wireless data transmission method, there are some issues relating to securing these transmissions that must be addressed in order to protect users and service providers to have confidence in the platform. Preventing unauthorized access to the wireless broadband network as well as assuring the confidentiality of data transmitted across the network should be given attention. An Enhanced Authentication protocol was proposed for mobile WiMAX networks achieve fast and secure inter-ASN handovers. However, it is shown to be vulnerable to Denial of Service (DoS) and replay attacks. In this paper, we propose an Enhanced EAP based TTLS(Tunnel Transport layer security) scheme to overcome the vulnerability of the above-mentioned scheme with much less requirements on the computation and communication resources.

Key Words*: Mobile WiMAX, EAP authentication, security, handover, preauthentication.*

I.Introduction

In IEEE 802.16e standard [1], Mobility support has been included that has extended the targeted customers to the mobile users in WiMAX systems..When a subscriber moves from one ASN(Access Service Network) to other, Mobile WiMAX system supports handover processes to make a mobile station (MS) find another base station(BS) to establish connection when moving out of coverage of the current serving BS (home BS or hBS). The MS and the target BS (tBS) or target ASN gateway, or ASN-GW (tASN) have to authenticate each other before the MS is granted access to the network to meet the security requirements.

In Mobile WiMAX, handover (HO) process is said to be an important element in supporting mobility and user roaming. The HO happens when the mobile station (MS) changes from one Base Station (BS) to another to obtain a higher signal quality or better quality of service (QoS) [8]. During the HO procedure, delay is added to the hand over process due to steps like re-authentication, encryption key exchange and network registration need to be implemented, all add delay to the handover process. Therefore, it is very necessary to minimize the handover latency while keeping the whole procedure secure. Among several authentication mechanism supported by the IEEE 802.16e,One of the authentication mechanism is the Extensible Authentication Protocol (EAP)-based authentication EAP based authentication that uses a backend authentication server (AS) such as an authentication, authorization, and accounting(AAA) server, This allows the mobile station to choose any of the authentication method without involving authenticator. The flexibility makes the EAP-based authentication a popular authentication method for mobile WiMAX systems.

There are two types of handover called Inter ASN and Intra ASN Handover. Inter-ASN handover is said to occur, when a MS handovers from one BS to another in different ASNs .A Security Association's traffic encryption key (SATEK) 3-way handshake was performed by Mobile station with the BS to distribute the TEK. However, an EAP-based authentication has been well known to be costly due to its time-consuming public key cryptography operations and the delay of several round-trips between the MS and the AS.

ERP(EAP based Reauthentication protocol) is proposed by HOKEY working Group which allows users to reuse Key materials.It allows several round trips to be reduced

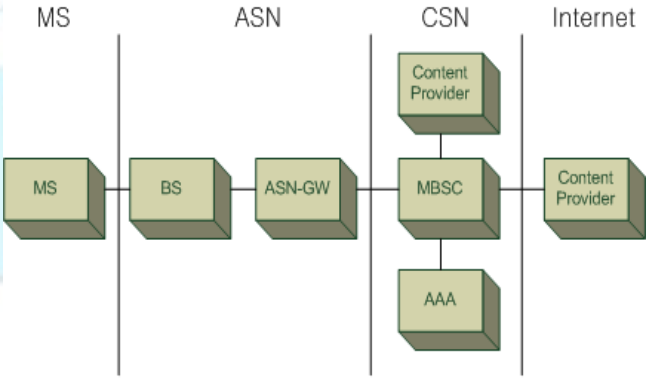
during handshake. In [5], a re-authentication scheme has been proposed that can be applied for handover between heterogeneous networks. The protocol makes use of an encrypted credential, which is given to a MS as a proof of its past honest behaviors and should be presented to the tBS for the handover. The main idea is to let the MS to have instant access to the network through a weak but fast authentication first followed by a stronger and more costly authentication. Based on the similar idea, the proposal in [6] has used the truncated 192 bits of the MSK in the subsequent EAP authentication as a temporary authentication root key for an inter-ASN handover.

By reducing the number of messages exchanged and simplifying the cryptographic operations, re-authentication techniques can lower the authentication signaling latency. By pre-authentication techniques in [7]–[9], a MS and the AS pre-compute the shared secret keys before a handover. Thus, the handover delay could be effectively reduced to the same amount of the time used by a 3-way handshake, resulting in the shortest authentication signalling delay. The main advantage of the pre-authentication is that the cryptographic material will not be reused, hence it becomes more secure. The HOKEY working group has proposed an EAP based pre-authentication model in [7] which has been adopted to Mobile IPv6 network in [8] and is called Handover Early Authentication (HOEA) protocol. HOEA utilizes proactive signalling to discover candidate access network where the MS potentially moves to and performs a full EAP authentication before it attaches to the candidate network. However, it only works when the link layer supports proactive signalling and there is a possibility that the handover has already started before the pre-authentication phase has completed, resulting in a failed pre-authentication. An EAP-based pre-authentication scheme (EPA) has been proposed to reduce the authentication delay in inter-ASN handovers [9]. By the EPA scheme, a MS exchanges the key materials with different neighbour ASNGWs(nASNs) of the serving ASN-GW, home ASN-GW or hASN, so that when it handovers to one of those nASNGWs, instead of performing a full EAP authentication, it can proceed directly with the 3-way handshake. The EPA has some advantages over the HOEA. Proactive signalling is not required in order to use EPA. Besides, the pre-authentication with the nASN-GWs is done right after the MS attaches to the current hASN-GW. As a result, the possibility that the pre-authentication completes before the handover is much higher compared to that by the HOEA. However, the EPA is vulnerable to DoS attacks and replay attacks, which greatly degrades its security level. Another drawback is the wastage of unnecessary effort for key exchange between the MS and those nASN-GWs that the MS never roams to. The HOEA also faces the same problem since proactive signalling can only be provided to the possible candidate networks. In this paper, in order to enhance the security functionality and the efficiency of the EPA, as our major contribution, we propose an Enhanced EAP-TTLS, or specifically, the EAP-Tunneled Transport Layer Security (EAP-TTLS) scheme which can prevent DoS and replay attacks with much less computational and communication resources and at the same time, can overcome the above mentioned drawbacks incurred in the EPA and the HOEA schemes.

System Background

A. Network Model

In this section, we have a brief introduction on the mobile WiMAX network reference model (NRM), which is the system under the study. A NRM consists of three logical parts: a MS, an ASN owned by a network access provider (NAP), connectivity service network (CSN) owned by network service provider (NSP). An ASN is formed by BSs and an ASN-GW to offer radio access to MSs. An ASN-GW is placed at the boundary of the ASN and connects the BSs to the CSN, which provides IP connectivity service to the MSs. The authenticator is located at the ASN-GW. The AS, which supports the authentication for the MSs, resides in the CSN.



MS - Mobile Station
BS - Base Station
ASN - Access Service Network
ASN-GW - Access Service Network Gateway
CSN - Connectivity Service Network
MBSC - Multicast Broadcast Service Controller
AAA - Authentication, Authorization, Accounting

III. The EEP Based Preauthentication Scheme

In this section, we present the EEP scheme (Existing System) for inter-ASN handovers, which fully utilizes the following information provided from the previous EAP-TLS mutual authentication and the centralized AS to prevent the above mentioned attacks and reduce the number of cryptographic operations required.

Firstly, it is assumed that the hBS always has an updated AS's certificate. This certificate can be obtained indirectly when the hBS relays the certification exchange during the EAP-TLS handshaking between the AS and the MS [16] or it can periodically request and check validation status of the AS's certificate.

Secondly, after the mutual authentication, the MS and the hBS share the message authentication code which is used to calculate Hash-based or cipher-based *MAC*.

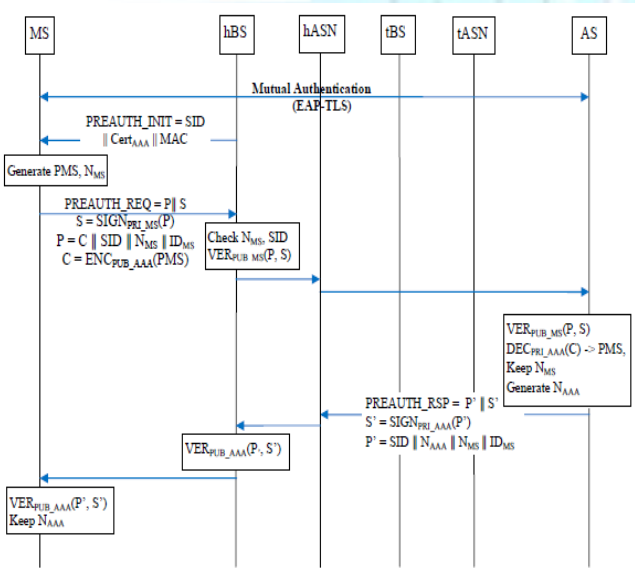


Fig. 2. The EEP pre-authentication scheme.

TABLE I
NOTATION DEFINITION

PUK_A	Public key of A
PRK_A	Private key of A
$ENC_K(X)$	Encrypt X using K
$DEC_K(X)$	Decrypt X using K
$SIGN_K(X)$	Generate Signature for message X using K
$VER_K(X, S)$	Verify message X with the corresponding signature S using K
ID_A	Identifier of A
TLS-PRF-X	TLS pseudo-random function computed to X octets
$X\|\|Y$	Concatenation of X and Y

Lastly, the ASN authenticator can communicate with the AS securely using the RADIUS protocol. The ASN authenticator and the AS share a secret key that can be used to protect data confidentiality. The AS can be employed to securely distribute the *MSK* to the nASN after it is confirmed to be the tASN for a handover. With the above facts, by the EEP scheme, the MS has only to exchange a pre-master secret (*PMS*) with the AS, which will use this *PMS* together with other available information to generate the corresponding *MSK* and send it over the RADIUS to the tASN.

• 0*th* Step: After the MS finishes the mutual authentication with the AS, the AS and the hBS are trusted by the MS.
The hBS shares the *MAC* key with the MS.

• 1*st* Step: The hBS sends a *PREAUTH INIT* containing a unique 16-bit session identifier (*SID*), the updated an verified AS's certificate and the *MAC* to the MS. The *SID* is incremented whenever the hBS initiates a new pre-authentication session with the same MS.

• 2*nd* Step: The MS checks the *SID* and the *MAC* to make sure that it is not a replayed message and is from the hBS. After that, it randomly generates a *PMS* and a nonce *NMS*. The *PMS* is encrypted using the AS's public key. It is concatenated with the *SID*, newly generated nonce and the *IDMS*. After that, the message is signed using the MS's private key and sent to the hBS. The Hbs verifies the signature using the MS's public key to check whether the message has been modified. It also checks the *SID* and the *NMS* to make sure it is the reply of the *PREAUTH_ INIT* sent previously and it is not a replayed message. After that, it relays the message to the AS.

• 3*rd* Step: The AS verifies the signature of the received message and the *NMS* to make sure it has not received this message before and the message has not been tampered.
If the message is genuine, the AS will decrypt the cipher text using its private key to obtain the *PMS*.
It will then generate a nonce *NAAA*, concatenate it with the *SID*, the *NMS* and the *IDMS*, sign the message and send it back to the hBS. Similar to the step 2, the hBSwill verify the message and relay it to the MS. The MScan verify the correctness of the receiving message and keep a record of the *NAAA*.
The handover phase (Fig. 3) begins with a decision for anMS to handover from the hBS to a tBS. The decision may originate either at the MS or the hBS using *MOB MSHOREQ* or *MOB BSHO-REQ* message, respectively. Before the handover decision is made, the hBS sends a notification containing the *IDMS*, *IDtASN* and the Carrier to Interference plus Noise Ratio (*CINR*) to the possible tBS over the backbone to notify the tBS of the MS intent for handover [17]. If the tBS accepts to handover, it will send a handover notification response through the backbone to the hBS. The message will go through the tASN. As it is informed that it is selected for the handover, the tASN will send a *KEY REQ* to the AS containing the *IDMS* and *IDtASN* to the AS. The AS will derive the *MSK* similar to the EAP-TLS key derivation in [11]. The *MSK* will be protected using the shared secret between the AS and the tASN and sent back over the RADIUS.

Master secret = *TLS-PRF*-48(*PMS,master secret,NMS_NAAA_IDtASN*)---- (1)

Key Material = *TLS-PRF*-128(*Master secret,client EAP encryption,NMS_NAAA_IDtASN*----(2)

MSK = *Key Material*(0, 63)---- (3)
More information on the TLS-PRF-X function can be found The MSK will be protected using the shared secret between the AS and the tASN and sent back over the RADIUS.

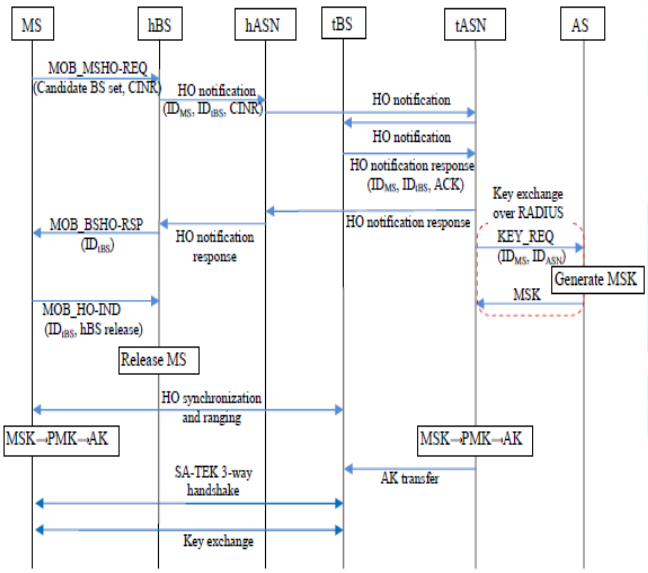
Meanwhile, the MS can derive the *MSK* using the similar formula. After above steps, the MS and the tASN share the same *MSK*, compute the *AK* and continue with the SA-TEK 3-way handshake as specified by IEEE 802.16e standard.

The EEP inherits EPA's ability to prevent eavesdropping, impersonation and MITM attacks. Firstly, the *PMS* is encrypted by using the public key of the AS, preventing an adversary from eavesdropping the secret. Secondly, it is impossible for an adversary to impersonate one honest party to send message to another party because each message is either signed using the transmitter's private key or protected by the *MAC*. A MITM attack is also impossible because the pre-authentication process is a mutual authentication, which implies that all communication parties are required to provide a proof of the identity by using a certificate, a digital signature or a *MAC*. The adversary cannot register itself as a legitimate MS or an ASN as long as it does not have the *MAC* key or the private key of the communication party whom it wants to impersonate.
Moreover, the EEP is more robust than the EPA because it can prevent the DoS attacks as well as the replay attacks, and at the same time, guarantee the backward and forward secrecy:
• Since the *PREAUTH _INIT* message is protected by using the *MAC* key which is shared between the MS and the hBS, an adversary cannot modify the message as it does not have the *MAC* key to create the correct *MAC*. The adversary cannot replay the message either, because the *SID* is incremented whenever the BS sends a new request and thus, can be used only once.
• The inclusion of the *SID* and randomly generated nonce *NMS* and *NAAA* prevents the adversary from replaying the *PREAUTH_ REQ* and the *PREAUTH_ RSP*. The *SID* relates the *PREAUTH RSP* with the corresponding *PREAUTH REQ* and the nonce can ensure the messages freshness.
• If a handover fails and the MS has to re-initiate a handover with a tBS from another tASN, it can still use the same *PMS* to generate a new *MSK* with the new tASN. Since the key derivation function uses *IDtASN* as one of the inputs and each ASN has a unique identifier,the *MSK* that the MS shares with the new tASN will be different from that shared with the previous tASN.As the result, the backward and forward secrecy can be guaranteed.
On the performance aspect, the EEP scheme performs better as follows:
• Only the AS's certificate is sent. The MS does not need to verify the certificate since the certificate has been verified by the hBS and sent to the MS. The certificate cannot be modified in transmission since it is integrity-protected by the *MAC*.
• The MS only needs to generate one *PMS*. As the result, it has to encrypt only one *PMS* while the EPA scheme needs to generate and encrypt a key for each nASN.
• Only the tASN needs to request the *MSK* from the

AS while other ASNs will not be involved in this preauthentication process. It helps to reduce the work load of the hBS, who is in charge of verifying signature and relaying all key exchange messages.

• There is no secret key sending back from the AS to the MS. Thus, there will be no public key encryption in the *PREAUTH_ RSP*.

• Even though there is one additional key exchange between the AS and the tASN, the process is performed while the MS and the tBS are proceeding with the handover synchronization and ranging, thus will not introduce any extra delay to the handover.



(Fig:3) The handover when EEP is used.

• The hBS is in charge of sending the *PREAUTH_ INIT* message to those MSs under its management, which can reduce the workload to the hASN.The proposed scheme followed the same key hierarchy and key derivation procedure as that of the EAP-TLS, thus, not only the *MSK* but also the important *EMSK* and the Initialization Vector (*IV*) can be derived after this pre-authentication process, which cannot be done

IV. HANDOVER USING EAP-TTLS

Our Proposed EAP-TTLS starts with establishing TLS Channel, authenticate server (Optionally authenticate user too).If the user wasn't authenticated, use the TLS channel to authenticate user using an authentication protocol.

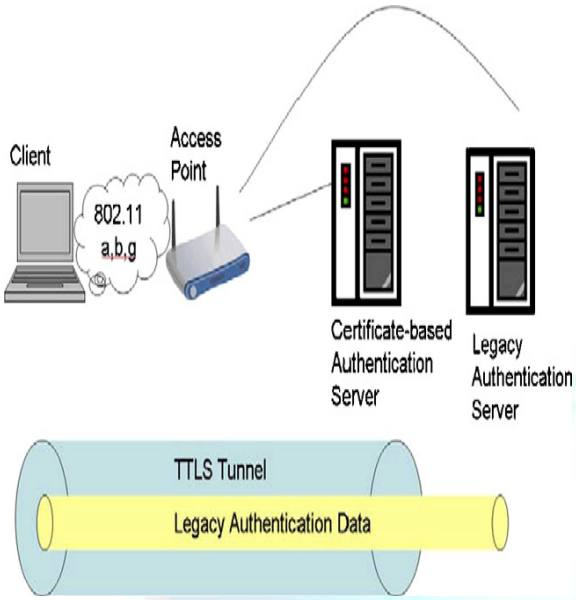
- EAP-TTLS Enables key distribution to the client and to the access point.
- The key is used for the communication between the AP and the client.

Supports exchange of Data cipher suite (cryptographic algorithm, key length) not the same as the suite used in the TLS phase,
Keying Material (from which the used keys will be generated) Supported by PEAP as well.

TTLS or tunneled TLS , is an extension on transport layer security. In this EAP method, a secure tunnel is established between the server and the client using a public key algorithm and certificates issued by a mutually trusted certificate authority. Once this tunnel is established, another authentication method is employed and that transaction is communicated via the secure tunnel. Because the authentication exchange now takes place via a secured tunnel, a less secure authentication method can be used. If the client is authenticated and authorized to join the network, another tunnel can be established to handle data encryption. This EAP method provides benefits of mutual authentication, secured cipher suite negotiation, the ability to use both passwords and certificates, and to keep the user's identity private since any password authentication would occur inside of a certificate-secured tunnel.

The client and the AP send their data cipher suite preferences to the TTLS server which select a cipher suite supported by both and sends it to both. If the client and/or the AP do not send their preferences, other means of negotiation should be used. (link layer. The client and TTLS server generate their keying material (as in EAP-TLS) and the TTLS sends the keying material to the AP

- Tunneling enables using existing protocols over a protected layer
- Provides client identity protection by passing Identity over the TLS channel.
  If the client is to be authenticated using a certificate, can be done after the TLS channel was established



.

V. RESULTS AND DISCUSSION

In our proposed system ,We can either Use digital certificate or Symmetric key for data encryption.It provides Strong authentication, resistant to attacks. Because the authentication exchange now takes place via a secured tunnel, a less secure authentication method can be used. If the client is authenticated and authorized to join the network, another tunnel can be established to handle data encryption. This EAP method provides benefits of mutual authentication, secured cipher suite negotiation, the ability to use both passwords and certificates, and to keep the user's identity private since any password authentication would occur inside of a certificate-secured tunnel.

RADIUS protocol is used for carrying authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.

VI.CONCLUSION

EAP-TTLS is increasingly seen as an extension of EAP-TLS. Proposed approach is used to perform handover securely by tunneling the data. This helps in preventing Identity exposure that happens in other protocols. This protocol is able to prevent other attacks like Dictionary attacks. Because the authentication exchange now takes place via a secured tunnel, a less secure authentication method can be used. This EAP method provides benefits of mutual authentication, secured cipher suite negotiation, the ability to use both passwords and certificates and to keep the user's identity private since any password authentication would occur inside of a certificate-secured tunnel.

There are a number of possibilities for extending this paper. Since public key cryptography is used for key generation, it may be somewhat difficult to implement and hence alternate solution can be applied that can reduce latency during handover.

REFERENCES

[1] IEEE Standard 802.16e-2005, in Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Feb. 2006.

[2] D. Q. Liu and M. Coslow, "Extensible authentication protocols for IEEE standards 802.11 and 802.16," 2008, pp. 1–9.

[3] A. M. Taha, A. T. Abdel-Hamid, and S. Tahar, "Formal analysis of the handover schemes in mobile WiMAX networks," in *Proc. 2009 IFIP International Conference on Wireless and Optical Communications Networks*, p. 5.

[4] V. Narayanan and L. Dondeti (2008, 09 December 2010), EAP extensions for EAP Re-authentication Protocol (ERP). [RFC 5296]. Available: http://www.rfc-editor.org/rfc/rfc5296.txt.

[5] T. Aura and M. Roe, "Reducing reauthentication delay in wireless networks," in *Proc. 2005 International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp. 139–148.

[6] Y. Kim and S. Bahk, "Enhancing security using the discarded security information in mobile WiMAX networks," in *Proc. 2008 IEEE Global Telecommunications Conference*, pp. 1–5.

[7] Y. Ohba, Q. Wu, and G. Zorn (2010, 09 December 2010), Extensible Authentication Protocol (EAP) early authentication problem statement. [RFC 5836]. Available: http://www.rfc-editor.org/rfc/rfc5836.txt

[8] L. Jong-Hyouk and C. Tai-Myoung, "Secure handover for Proxy Mobile IPv6 in next-generation communications: scenarios and performance," *Wireless Commun. and Mobile Comput.*, vol. 11, pp. 176–86, 2011.

[9] H. M. Sun, Y. H. Lin, S. M. Chen, and Y. C. Shen, "Secure and fast handover scheme based on pre-authentication method for 802.16/WiMAX infrastructure networks," in *Proc. 2007 IEEE Region 10th Annual International Conference*, pp. 1–4.

[10] C. Li, "Seamless mobility," M.S., Center for Information and Communication Technologies, Technical University of Denmark, 2006.