Different Pre- Authentication Schemes for Achieving Security of Handover in WiMax Network

Ms. Rushali V. Nikhar,
ME student
RAIT,
NERUL,
NAVI MUMBAI
nikhar.rushali@gmail.com

Mrs.Puja Padiya
Professor
RAIT,
NERUL,
NAVI MUMBAI
puja.padiya@gmail.com

***Abstract*:-**The world wide interoperability for microwave access (WiMAX) is used for the 4th generation technology for wireless network by using IEEE 802.16e standard. The demand for mobile wireless network is growing rapidly. The Mobile WiMAX technology is the technologies that is used to provide continuous service and that is also used for roaming anywhere. The mobile station have one of the challenging issues which is handover (HO).When a mobile station change from one base station to another it should be authenticate again. When mobile authenticate the basic approach is reduction of inactivity and minimize the handover delay with faster performance. When mobile WIMAX does the process of handover it does not transmit the packet or receive any packet, which results the loss of packet during handover and affects the performance of services. The service provider does not guarantee the quality of service. The pre-authentication based handover techniques are used to provide the fast and secure handover service. Different schemes are used to improve the performance of handover.

Keywords:-*IEEE 802.16e, WiMAX, Handover, EAP-TLS, Pre-authentication.*

*****

1. INTRODUCTION

WiMAX stands for Worldwide Interoperability for Microwave Access. It is a technology which is used for fixed broadband system and mobile broadband wireless systems. It is the technology which is used to provide long distance connectivity with higher speed. IEEE 802.16e network are generally used for long distance connectivity with high speed and better performance in wireless system. It provides centralized wireless access in mobile network. It allows transmission though certain obstacles. The main advantage of IEEE 802.16e is its high data rates, built-in support and low cost of deployment for mobility. WiMAX (Worldwide Interoperability for Microwave Access) has been recognized as one of the important innovative thing for mobile wireless network. When a mobile moves from one ASN (Access Service Network) to other, WiMAX is used to provide handover process from one base station to another base station. WIMAX also establish new connection and for this connection it requires a authentication process. When mobile station moves from one base station to another base station handover procedure is done and for handover authentication procedure is required. This process occurs for obtaining higher signal and good quality of service. Whenever handover process is done it require authentication and when it moves from one base station to another then it require the steps like re-authentication, encryption key exchange and network registration. For all these steps some time delay is required .That means it affect the performance of service and security. Handovers are generally divided into two categories depending on technology: horizontal handovers and vertical handover. Horizontal handovers are homogeneous intra-network that is used for city network or for area network, while the vertical ones are heterogeneous inter-network that is generally used for roaming like network. For example, handovers between multiple WiMAX networks are horizontal handovers and that one in WiMAX and 3G or WLAN are vertical handovers. The WiMAX system includes three types of handover that is used to support all types of WIMAX network.

2. RELATED WORK

H.M.Sun, S.Y.Chang, Y.H.Lin, and S.Y. Chiou[1] the authors have proposed the EMSK and MSK obtained from EAP authentication to calculate a shared key so that the faster shared key-based EAP approach can be used in the authentication. Hung-Min Sun, Shih-Ying Chang, Yue-Hsun Lin, and Shin-Yan Chiou[2], proposed solution for EAP-based early authentication through IETF HOKEY working group which proposes a pre-authentication model where the MS pre-authenticates itself with multiple candidate authenticators before a HO happens. Mohammad M.Shurman, Mamoun F.AI-Mistarihi, and Shehab A. Nasser [3] propose an efficient group-based handover authentication scheme for mobile WiMAX networks. The service provider base station (BS) transmit all the handover group members' security context to the target base station (BS). The scheme is used to achieve the security requirements in handover technique. Subhashini. S [5]has proposes an EAP-TTLS based protocol to prevent an unauthorized access to the wireless broadband network as well as assures the confidentiality of the transmitted data over the network. Ms. Bhanupriya M. Nikhar and Prof. Kapil N. Hande [6] Proposes the Extensible Authentication Protocol (EAP), defined in RFC 3748, provides support for authentication methods. Transport Layer Security (TLS) provides for mutual authentication, integrity protected cipher suite negotiation, and key exchange between two endpoints. They define EAPTLS, which includes symmetric key support for encryption and key derivation.

3. METHODOLOGY

EAP-based Authentication uses a backend authentication server (AS) which is used for selection of authentication process. The EAP is used for authentication in each handover technique.

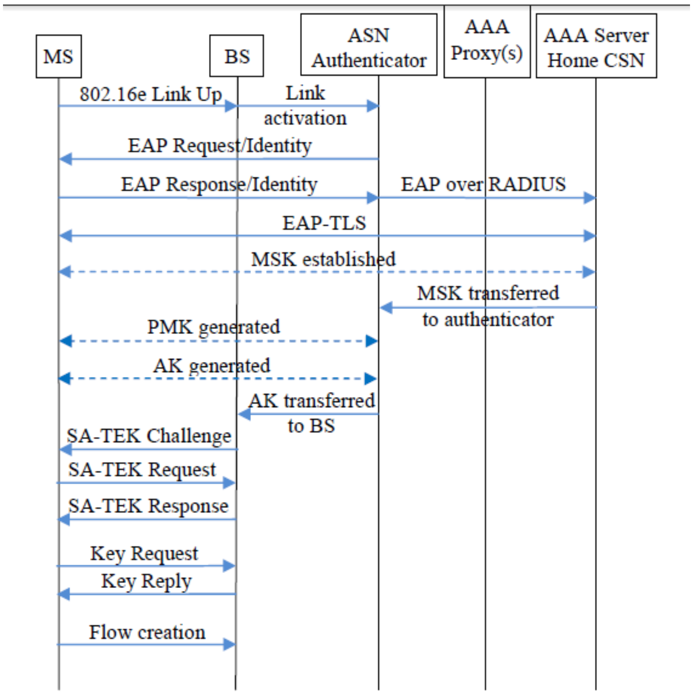


Figure 1. EAP-TLS based Authentication

The flexibility of EAP-based authentication is the popular choice for the authentication of each mobile WiMAX systems in HO. To reduce the EAP-based authentication delay during HOs without compromising security requirements, two approaches have been followed as re-authentication and pre-authentication approaches.Fig.1 shows the EAP-TLS authentication that is required for each handover procedure.

3.1 Secure Handover Scheme

Hung-Min Sun, Yue-Hsun Lin, Shuai-Min Chen, Yi-Chung Shen proposed scheme the pre-authentication scheme EAP-TLS with PKI(public key infrastructure)are used that provide more security and fast handover. By using the radius mobile station mutually authenticate with AAA server through EAP-TLS. In PKI architecture, the Certificate Authorization (CA) is used to organization key pairs to each user: a public key and a private key. The public key is stored in a public area accessible to everyone for secure hand over authentication procedure in 802.16/ WiMAX infrastructure, based on pre-authentication schemes combining with PKI architecture. It can be used to apply a macro-hand over during different ASN networks is used HO technique.

3.2 Message Exchange And Key Derivation At Initial Network Entry

The Pairwise master key generation is modified to link the identifications of the MS and BS, and the PMK is delivered to the related BS. In pre-authentication technique the authentication server generates a unique PMK that is in the diversity set and used for each base station (BS) and distribute it to each HHO pre-authentication. Then BS receives PMK from each diversity set in MS that perform 3-way handshake and gives TEK to each BS.

3.3 An Efficient Method To Reduce Handover Delay

In the HO procedure MS trying to minimize the Handover delay and reduce the number of target base stations (TBS) when it transmit from one BS to another BS. When it transmits it scan the minimum BS and find the suitable target BS. When numbers of BS scan are reduced it gives better performance in minimum time.

3.4 Pre- Authentication Protocol with symmetric key procedure

The scheme is aimed to reduce handover delay occurring in the communication.

Symmetric keys have been used for the encryption of the secret key, the origin authentication and the integrity protection of the pre-authentication messages. The scheme can reduce the HO delay with much less resource by allowing the MS and the AS to exchange the secret key used for the HO authentication session before the HO happens. As the result, during the HO, the MS does not need to perform EAP authentication with the AS and can proceed with the SA-TEK 3-way handshake straight away. The authentication scheme is both secure and efficient, which makes it to be a competitive candidate for the efficient handover schemes.

4. COMPARATIVE ANALYSIS

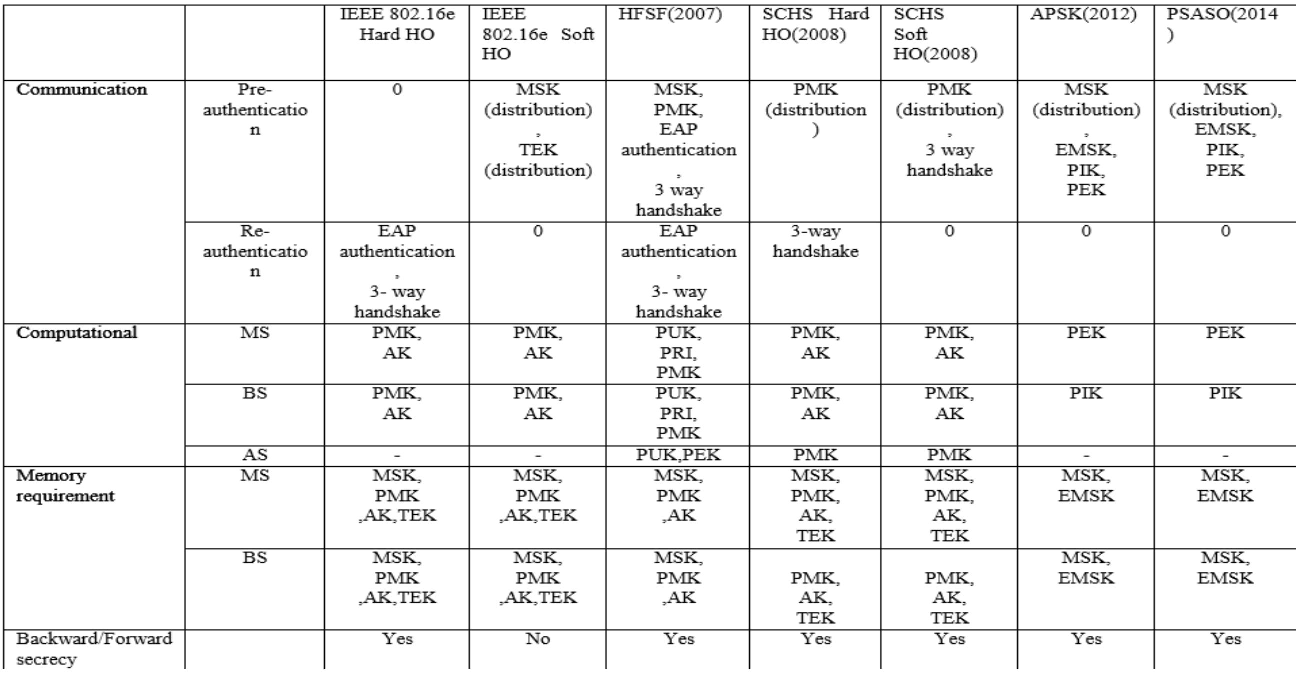
The different technique gives the result and more secure handover procedure. Different parameters should be considered for comparison of different techniques. The table shows the analysis of all the techniques as follows in Table 4.1.

So far we have discussed all the Authentication procedure in Mobile WiMAX Network. Table4.1 describes comparative analysis of five types of Authentication, IEEE 802.16e, HFSF, SCHS, APSK and PSASO. Every protocol is designed for special environment. Every handover procedure has generates its own key like MSK, TEK, PMK. These keys used to support pre-authentication and re-authentication of handover procedure. Communication based on communication of different keys like PMK, EMSK, MSK etc. In computation, MS, BS and AS are described. Each MS, BS and AS generates a key like PMK, PRI, AK, etc. Each is used to communicate and authenticate with different BS by using AS. For each communication in BS and MS different keys are generated .these key are used to authenticate different BS. Numbers of keys are generated then its memory requirement is more. In each authentication process the number of keys generated is different. The pre-authentication techniques, the different schemes are used to make a handover and reduced the time in handover. For each HO the schemes use the key like MSK, EMSK to reduce the HO delay.

In re-authentication for each HO re-authentication is required but it requires time and in place of this some scheme uses the pre-authentication and gives better result. EAP authentication and 3-way handshake gives better result for security.

Each is used to provide the secrecy and latency for handover procedure. In different techniques the handover time require is less and provides more security.

Table 4.1: Comparative analysis of authentication process



		IEEE 802.16e Hard HO	IEEE 802.16e Soft HO	HFSF(2007)	SCHS Hard HO(2008)	SCHS Soft HO(2008)	APSK(2012)	PSASO(2014)
Communication	Pre-authentication	0	MSK (distribution) , TEK (distribution)	MSK, PMK, EAP authentication , 3 way handshake	PMK (distribution)	PMK (distribution) , 3 way handshake	MSK (distribution) , EMSK, PIK, PEK	MSK (distribution), EMSK, PIK, PEK
	Re-authentication	EAP authentication , 3- way handshake	0	EAP authentication , 3- way handshake	3-way handshake	0	0	0
Computational	MS	PMK, AK	PMK, AK	PUK, PRI, PMK	PMK, AK	PMK, AK	PEK	PEK
	BS	PMK, AK	PMK, AK	PUK, PRI, PMK	PMK, AK	PMK, AK	PIK	PIK
	AS	-	-	PUK,PEK	PMK	PMK	-	-
Memory requirement	MS	MSK, PMK ,AK,TEK	MSK, PMK ,AK,TEK	MSK, PMK ,AK	MSK, PMK, AK, TEK	MSK, PMK, AK, TEK	MSK, EMSK	MSK, EMSK
	BS	MSK, PMK ,AK,TEK	MSK, PMK ,AK,TEK	MSK, PMK ,AK	PMK, AK, TEK	PMK, AK, TEK	MSK, EMSK	MSK, EMSK
Backward/Forward secrecy		Yes	No	Yes	Yes	Yes	Yes	Yes

5. CONCLUSION

Thus, the Pre-authentication scheme should provide fast and secure authentication for moving from one base station other and should reduce the communication delay in between two. We can conclude that the authentication between MS and AS is done by an EAP-TLS authentication procedure and this is the process followed by each mobile station. After authentication process the re-authentication is done by using PIK and PEK and also performs encryption for security purpose. A pre-authentication scheme is used to reduce the authentication delay in the HO process for the mobile WiMAX networks. In the pre-authentication technique the HO is done and during HO the MSK is generated and MSK is exchange between tASN and AS. Thus the additional key exchange will not introduce any extra delay to HO latency. As a result, the delay occurring previously is reduced. Symmetric keys have been used for the encryption of the secret key

6. REFERENCES

[1] Tuomas Aura and Michael Roe, "Reducing Reauthentication Delay in Wireless Networks", IEEE 2005.

[2] Hung-Min Sun, Yue-Hsun Lin, Shuai-Min Chen, Yi-Chung Shen, "Secure and Fast Handover Scheme Based on Pre-Authentication method for 802.16/WiMAX Infrastructure Networks", IEEE ,2007 .

[3] Hung-Min Sun, Shih-Ying Chang, Yue-Hsun Lin, and Shin-Yan Chiou, "Efficient Authentication schemes for Handover in Mobile WiMAX", IEEE ,pp . 235-240, 2008.

[4] Junbeom Hur, Hyeongseop Shi, Pyung Kim, Hyunsoo Yoon, Nah-Oak Song, "Security Considerations for

Handover Schemes in Mobile WiMAX Networks",IEEE , pp .2531-2536, 2008.

[5] Ahmed M. Taha AmrT. Abdel-Hamid , and Sofiene Tahar, "Formal Analysis of the Handover Schemes in Mobile WiMAX Networks",IEEE 2009.

[6] Sanjay P. Ahuja, Nicole Collier, "An Assessment of WiMax Security" Communications and Network",IEEE 2010.

[7] Mohammad M. Shurman, Mamoun F. AI-Mistarihi, and Shehab A. Nasser, "Hard Handover Optimization in Mobile Wimax Networks",The 5th International Conference on Communications, Computers and Applications (MIC-CCA2012);Istanbul, Turkey: 12-14 October 2012.

[8] Thuy Ngoc Nguyen and Maode, "An Pre-authentication Protocol with Symmetric Keys for Secure Handover in Mobile WiMAX Networks",IEEE , pp. 863-867, 2012.

[9] Subhashini.S, "Active EAP Protocol for Secure Inter ASN Handover in Mobile WiMAX Networks", IJREAT International Journal of Research in Engineering Advanced Technology, Volume 1, Issue 2, April-May, 2013. 24

[10] Ms. Bhanupriya M. Nikhar and Prof. Kapil N. Hande, "Pre-authentication Scheme for Achieving Security and Optimization of Handover in Mobile WiMAX Network",International Journal of computer Organization Trends-Volume 10 Number 1-Jul 2014 ,pp.11-18.

[11] Ms. Bhanupriya M. Nikhar and Prof. Kapil N. Hande, "A Survey on Secure Handover Optimization in Mobile WiMAX Network", IJREAT International Journal of Research in Engineering Advanced Technology, Volume 1, Issue 2, April-May, 2013.International Journal of Computer Science and Engineering (JCSE) 1- Feb 2014,pp . 21-27.