Implementation of Reserved CID Based Passport Handover and PKMv2 Protocol in IEEE802.16e Network Entry Process

B. Sridevi, V. S. Sudharsana, R. Pavithra, N. Karthika, and S. Rajaram

***Abstract*—Mobility management being a decisive role in wireless communication networks which effectively distribute the services to the relevant users on the move. A wireless network which is richer and fixed in bandwidth is specified as IEEE802.16 and is promoted and launched by an industrial forum Worldwide Interoperability for Microwave Access (WiMAX). WiMAX has the challenge of prolonged Handover Delay time. In our proposed method, to minimize the time delay passport handover using Reserved CIDs (RCID) are used which is common and unique to all BSs of that particular ASN. MS with RCID can roam around all BSs within ASN without any authentication for six handovers. By this the handoff delay can be reduced by 33.33%. In IEEE 802.16, however, security has been considered as the main issue during the design of the protocol but some issues still need to be solved on threats, risk and vulnerability in real situations. IEEE 802.16 employs an authenticated client/server key management protocol in which the BS, the server, controls the distribution of keying material to the client SS and is based on the PKMv2 (Privacy Key Management Version 2) protocol. This paper discusses about the implementation of RSA and EAP based PKMv2.This mechanism is analyzed in mobile WiMAX model and the protocols are developed in MATLAB GUIDE.**

***Index Terms*—IEEE 802.16, WiMAX, key caching, authentication cost, MSK utilization.**

I. Introduction

Mobile WiMAX (IEEE 802.16e) is a hasty growing broadband access technology which facilitates low-cost mobile internet application. The advancement in this technique is Mobile WiMAX is combined with Orthogonal Frequency Division Multiplexing Access (OFDMA) and advanced Multi Input and Multi Output (MIMO) schemes with the most expected flexible bandwidth and required fast link adaption. WiMAX creates an elevated and efficient air interface that exceeds the facility of existing and emerging 3G radio access networks [1] .This provides broadband wireless services that enable wide service coverage, high data throughput and high mobility. In Passport Handover, the serving BS broadcasts all the basic information about the MS to the target BS. This reduces the delay during the handover process. Bearing in mind regarding the secured network access, AAA (Authentication Authorization and Accounting) mechanism is utilized in the WiMAX architecture [2]. The two challenges faced are referred as roaming cost and handoff cost. Pre-authentication is performed in WiFi and WiMAX. It uses EAP-TLS based authentication[11]. The authentication is divided Pre-authentication phase and Re- authentication phase. Pre-authentication is used as the initial stage and then re-authentication begins. It can reduce the authentication delay less than 150ms.In this EAP authentication is skipped, MS handovers occurs within the same network hence the handover delay is abridged .TBS is selected in which has largest bandwidth and also minimum usage. Collision resistant hash function is used to generate credentials.IEEE802.16e has the setback of low spectrum utilization and also frequent handoff. RS Grouping is the optional technique in the 802.16j standard to overcome these problems .By using this RS grouping algorithm with centralized-scheduling, for fixed user's groupings with a small in group sizes has improved throughput results. Its verified that throughput depends on the group size. During this handoff process, the mobile station has to accomplish the authentication procedure every time during the handoff from one base station to another. The overall network may be divided logically into three parts [3]:

- **Mobile station MS** used by the end user to access the network.
- **Access Service Network (ASN)**, which comprises one or more base stations and one or more ASN gateways that form the radio access network at the edge.
- **Connectivity Service Network (CSN),** which provides IP connectivity and all the IP core network **functions**.

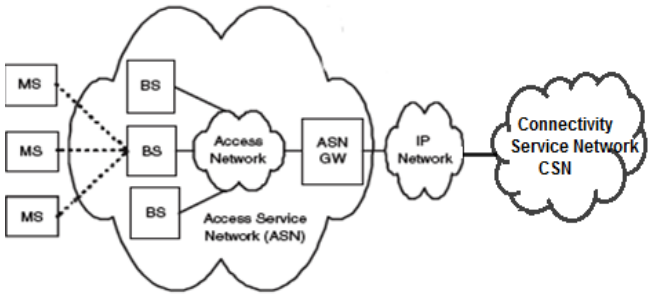

Fig. 1. WiMAX network reference model

In WiMAX, MS typically makes the final decision, whereas BS makes recommadations towards the candidate which target itself for handoff [4]. The rest of the article is organised as follows.In section II wimax network entry process is discussed .Section III provides WiMAX key management is confered. In section IV privacy key management version 2 is discussed.In section V results and

Manuscript received October 4, 2012; revised December 24, 2012.

B. Sridevi, V. S. Sudharsana, R. Pavithra, N. Karthika are all with Department of ECE, Velammal College of Engineering and Technology, Madurai, India (e-mail: aisveriya@yahoo.com).

S. Rajaram was with the Department of ECE,Thiagarajar College of Engineering,Madurai (e-mail: sudharsana92@gmail.com).

discussion is performed.

II. WIMAX NETWORK ENTRY PROCESS

The network entry process is a set of procedures that MS must follow in order to enter the network and to get the network services. The initial network entry procedure mainly consists of four processes: initial ranging process, MS basic capability negotiation process, PKM authentication process and registration process. The important point that is to be noted here is that, depending on the current status of the MS, the network entry process can be different. This process is the most security perceptive process in IEEE 802.16 network. Fig. 2 given below describes the initial network entry procedure. A mobile station which is just powered on must perform initial network entry process[5]. The steps for initial network entry process are given below:

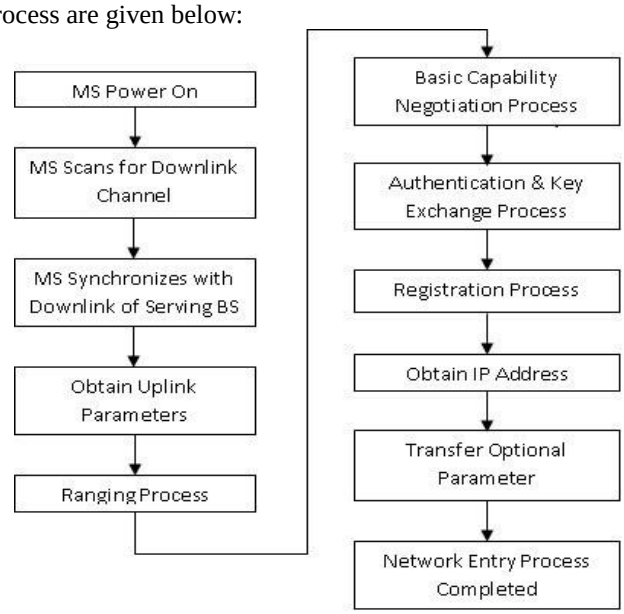

Fig. 2. WiMAX Network Entry Process

Step 1: When it is powered on, it firsts scans the downlink channel to determine whether it is currently in the coverage of base station.

Step 2: Each MS stores the list of optional parameters, such as DL frequency. So in next step MS synchronizes with the stored DL frequency of most suitable BS.

Step 3: Once the DL synchronization is completed, MS can listen to the various control messages from which it obtains the UL parameters. Based on these UL parameters, MS decides whether the channel is suitable or not.

Step 4: If the channel is suitable MS performs next step, otherwise it goes back to the scanning step that is step 1.

Step 5: Next step is to perform ranging process. Ranging is the process to acquire timing and power level adjustment to maintain the UL connection with the BS. To perform initial ranging, MS send a RNG-REQ message to the BS with the CID parameter.

Step 6: In response to this message, BS sends the RNG-RSP message to the MS with the basic and primary CID.

Step 7: After initial ranging, next step is to perform basic capability negotiation process. Here MS firsts sends the SBC-REQ message to the BS through which MS informs the BS about its basic capabilities.

Step 8: When BS receives this message, it responds with the SBC-RSP message consisting of the parameters required for the UL and DL transmission.

Step 9: After negotiating the basic capabilities, authentication and key exchange process will be performed.

Step 10: Once the key exchange process is completed, MS registers itself with the BS, for which it sends the REG-REQ message to the BS.

Step 11: In response to this message, BS sends the REG-RSP message to the MS. When MS receives this message, it can obtain the IP address.

Step 12: Finally the service flow will be established, which is either initiated by the MS or BS.

Some researchers are going on in the view of reducing the authentication cost in Network Entry Process [7], [9]

III. WIMAX KEY MANAGEMENT

TABLE I: DESCRIPTION OF KEYS

Key	Bits	Description
AK	160	Authentication of an MS/SS by BS. Lifetime between 1 and 70 days
KEK	128	3-DES key used for the encryption of the TEK
TEK	128	Traffic encryption key. Lifetime between 30 min and 7 days
HMAC_ KEY_D	160	Used for authenticating messages in the downlink direction
HMAC_ KEY_U	160	Used for authenticating messages in the uplink direction

The IEEE 802.16e standard, also referred to as mobile WiMAX, supports fixed and mobile services for both enterprise and consumer markets and remedies most of the security weaknesses of its predecessors. The security sublayer of 802.16e consists of two component protocols, namely the encapsulation protocol and key management. As already mentioned, here we focus on key management performed by the PKMv2 protocol. Key management procedures in 802.16e are part of the PKM protocol and define how the keys are created, which keys are available and for what purpose. Specifically, the keys used for the integrity protection of management frames and secure transmission of Traffic Encryption Keys (TEK) are produced from master keys. Master keys may be derived from two distinct sources (procedures), namely RSA and EAP or a combination of two. The key generation procedure based on Public Key Certificates (PKC) ends with a pre-Primary Authorization Key (pre-PAK), while the 802.1X/EAP procedure ends with a Master Session Key (MSK). In addition, PKM is used to apply conditional access to network services, making it the authentication protocol, defending them from theft of service (or service hijacking) and providing a secure key exchange.

IEEE802.16 standard security uses many encryption keys.

The encryption keys defined in 802.16-2004 are listed in Table 15.1 where the notation and the number of bits in each key are given. A nonexhaustive list of the keys used in the PKMv2 protocol, taking into account the 802.16e amendment, is proposed in Table I.

IV. PROPOSED WORK

A. Passport Handover

WiMAX has the challenge of prolonged Handover Delay time. In regular Handover when a Mobile station(MS) moves from Service Base Station (SBS) to Target Base Station(TBS) steps such as Initialization, synchronization, ranging, authentication takes place and new CID is generated to the MS thereby increasing the delay time which is shown in Figure 1.The scope of the CID is within the that base station. In our proposed method, to minimize the time delay Reserved CIDs (RCID) are used which is common to all BSs of that particular ASN[10] .The MS has to send a request to ASN for acquiring RCID. To avoid illegitimate user, ASN verifies validity of MS with AAA server and the unique RCID is generated and distributed to the MS. MS switching between BSs with same CID is called Passport Handover and it avoids the repetitive steps done for the generation of CID. The algorithm for obtaining RCIDs by MSs is shown in figure 3.

Algorithm 1: Obtaining Reserved CID by MS:
Step1: MS request ASN for Reserved CID
Step 2: ASN Response to MS.
Step 2.1: ASN checks the validity of MS by accessing MS details from AAA.
Step 2.2: Provides Reserved CID .
Step 3: Acknowledgement sent by MS.

Fig. 3. Algorithm for obtaining RCID by MS

Let the maximum number of BSs be **N**
The possible number of CIDs will be **2^16.**
The maximum number of users is **65536N (N*2^16).**
The number of RCIDs will be **1% of maximum number of users**
Hence the number of RCIDs will be **0.01*65536N.**

Fig. 4. Calculation of RCID

Algorithm 2: Passport Handover
Step1: MS request Handover to BS with Reserved CID.
Step2 :Assign res= Decimal(first 4 bits of MSB of Reserved CID)
Step3 : if(res==15)
if(priority==‘7’)
allow Passport Handoff
else if(priority<6)
allow Passport Handoff
priority =priority + 1
else
do not allow Passport Handoff and normal handoff takes place
else
Allow Normal / existing Handoff process

Fig. 5. Algorithm for passport handover

Priority is a 3-bit field followed by RCID to limit the number of hops by MS in the ASN. The Algorithm for Passport Handover process is shown in figure 5.

B. Privacy Key Management Version 2

Security of connections access in WiMAX is done with respect to the Privacy Key Management (PKM) protocol. The protocol is responsible for the usual and periodical authorization of SSs and distribution of key material to them, as well as reauthorization and key refresh. It also manages the application of the supported encryption and authentication algorithms to the exchanged MAC Protocol Data Units (MPDUs).The PKMv1 supports only the device authentication and had many critical drawbacks. Therefore IEEE 802.16e released the second version of Privacy and Key Management (PKM) protocol called PKMv2. It has many security features like message authentication codes, key ids, certificates, etc.

PKMv2 which allows for three types of authentication:

- RSA based authentication
- EAP based authentication
- RSA based authentication followed by EAP authentication

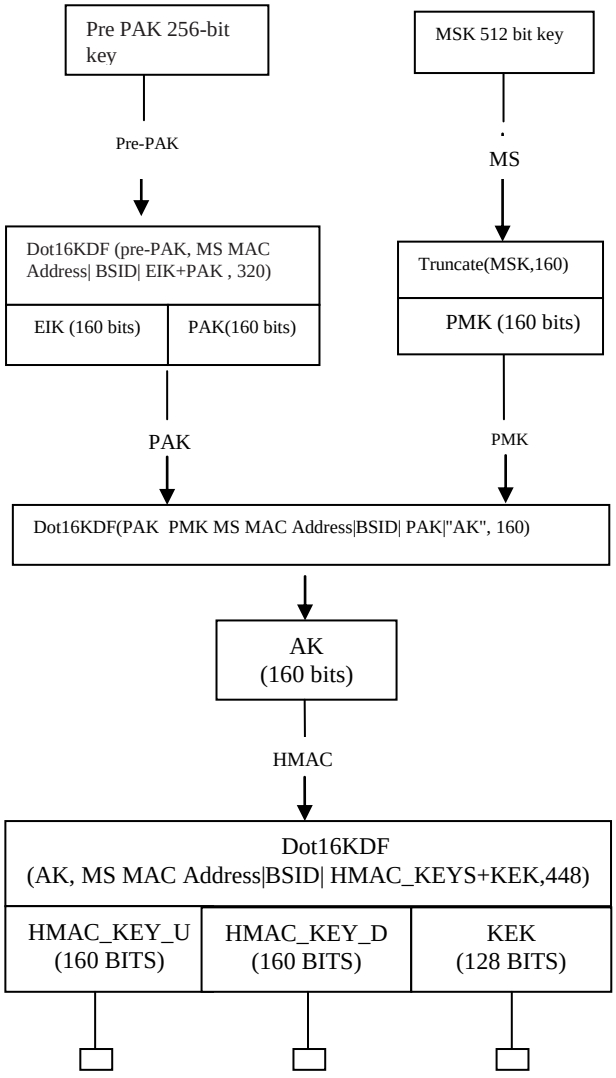

Fig. 6. PKM V2-EAP&RSA

Figure 6 shows the structure of PKM V2 protocol based on EAP & RSA.

The PKM V2 supports both mutual authentication and unilateral authentication and enables periodic reauthentication/reauthorization and key update. To do so, it employs either EAP in combination with an operator-selected EAP method such as EAP-TLS, or X.509 digital certificates together with RSA public-key encryption or a mixed procedure starting with RSA authentication and followed by EAP authentication. In contrast to its precursor, PKMv2 offers strong encryption algorithms to perform key exchanges between an MS and the corresponding BS. After establishing a shared secret (the AK) between the MS and the BS, PKMv2 uses it to secure subsequent exchanges of TEKs between the two parties. Several issues of Key management are listed in [5].

C. PKM V2 –RSA and EAP

The RSA-based authorization process yields the Pre-PAK (Pre-Primary AK). The Pre-PAK is sent by the BS to the MS encrypted with the public key of the MS certificate. Pre-PAK is used to generate the PAK. The EAP-based authentication process yields the MSK and then the other keys such as the Key Encryption Key (KEK) and HMAC/CMAC key are derived from the MSK. EAP and RSA are combined in this protocol. If RSA-based and EAP-based authorization then, AK=Dot16KDF (PAK x or PMK, SS MAC address |BSID|PAK|"AK,"160).

V. Results And Discussion

As in section IV, the RCID is generated for Passport Handover by ASN which is shown in Figure 7. The keys generated for authentication, encryption and authorization are AK, HMAC uplink, HMAC downlink, KEK .If RSA based authorization, then AK=Dot16KDF(PAK, SSMAC address |BSID| PAK"AK,"160).

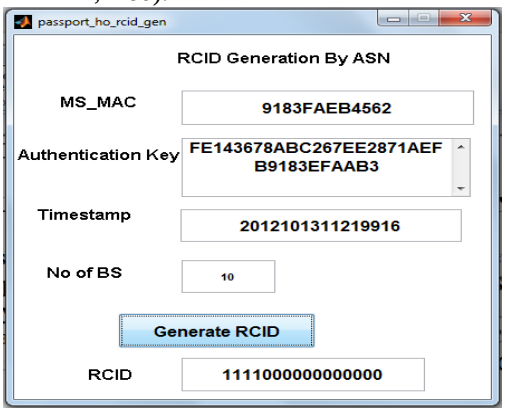

Fig. 7. Generation of RCID by ASN

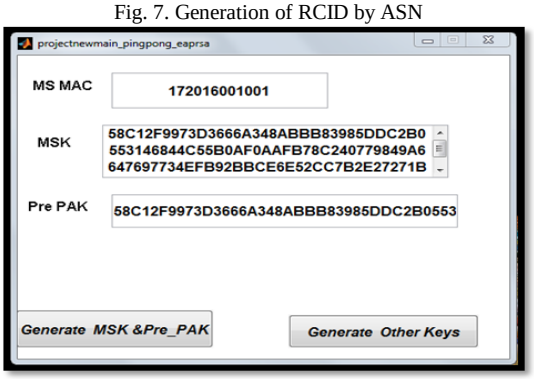

Fig. 8.

In Figure 8, both MSK and pre-PAK are generated during network entry process based on EAP & RSA based authorization. PMK, PAK keys are derived from the MSK and pre-PAK respectively and this is shown in Figure 9.

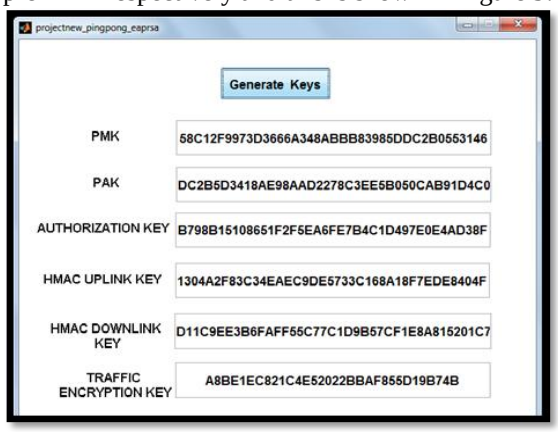

Fig. 9.

In normal handover, delay time is calculated as

$$\mathbf{D_{conventional} = T_{sync} + T_{cont\_resol} + T_{rng} + T_{auth} + T_{reg}}$$

In passport handover, authentication and registration process do not take place and so the delay time is calculated as

$$\mathbf{D_{passport\ handover} = T_{sync} + T_{cont\_resol} + T_{rng}}$$

Thus the delay time is reduced approximately by 33.3%.

VI. Conclusion

In this paper, we have discussed about three types of key management techniques which strengthen the authentication in WiMAX network entry process. The key idea of our work is to bestow WiMAX users and providers a detailed comparative analysis with respect to authentication time, key generation time using simulation results obtained from MATLAB GUIDE. Results depict the implementation of PKMv2 protocols and their impact on WiMAX network. Our Future work will be focused in enhancing PKMv2 protocol to overcome the limitation of the traffic in the network and analyzing various attacks and their impacts so that ASN and BS can differentiate the hackers from users.

References

[1] J. J. Andrews, A. Ghosh, and R. Muhamed, *Fundamentals of WIMAX understanding broadband wireless networking*, Prentice Hall, 2007.

[2] L. Nuaymi, *WiMAX technology for broadband wireless access*, John Wiley & Sons Ltd, 2007.

[3] S. Y. Tang, P. Muller, and H. R. Sharif, *Wimax security and quality of service*, John Wiley & Sons Ltd, 2010.

[4] W. M. Lang, R. S. Wu, and J. Q. Wang, "A simple key management scheme based on WiMAX," *IEEE computer society*, 2008.

[5] S. Xu, M. Matthews, and C. T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16," ACM SE, 2006.

[6] Y. W. Chen, J. T. Wang, K. H. Chi, and C. C. Tseng, "Group - Based authentication and key agreement," *Springer Science and Business Media*, LLC, 2010.

[7] M. Hollick, P. S. Mogre, C. Schott, and R. Steinmetz, "Slow and steady: Modelling and performance analysis of the network entry process in IEEE 802.16," *IEEE communication society*, 2007.

[8] J. Mandin, "Enhancement of 802.16e to support EAP based Authentication/key distribution," 2004.

[9] S. F. Hsu and Y. B. Lin, "A key caching mechanism for reducing WiMAX authentication cost in Handoff," *IEEE Trans. Veh. Tech.*, vol. 58, no. 8, October 2009.

[10] W. H. Jiao, P. Jiang, and Y. Y. Ma, "Fast handover scheme for real-time applications in mobile Wimax," *IEEE Communication Society*, 2007.
[11] L. M. Hou and K. X. Miao, "A pre-authentication architecture in WiFi and WiMAX integrated system," *IEEE proceedings of communications and Networking*, pp. 1-5, 2009.

B. Sridevi is an ssistant professor of ECE Department of Velammal College of Engineering & Technology, Madurai, obtained her B.E., degree from A.C.C.E.T Karaikudi, Madurai Kamaraj Univeristy, Madurai and M.E. degree from Anna University, Chennai. She has 2 years of Industrial experience, 10 years of Teaching, and Research experience. Pursuing Ph.D. in Anna Universit in Networking. She published many research papers in International journals, national and international conferences.

V. S. Sudharsana is a student of Velammal College of Engineering and Technology pursuing Under Graduation in Electronics and Communication, final year. We are doing a project in Mobile WiMax and have attended many National Conferences.

R. Pavithra is a student of Velammal College of Engineering and Technology pursuing Under Graduation in Electronics and Communication, final year. We are doing a project in Mobile WiMax and have attended many National Conferences.

N. Karthika is a student of Velammal College of Engineering and Technology pursuing Under Graduation in Electronics and Communication, final year. We are doing a project in Mobile WiMax and have attended many National Conferences.

S. Rajaram is working as Associate Professor of ECE Department of Thiagarajar College of Engineering, Madurai. He was awarded Ph.D by Madurai Kamaraj University in the field of VLSI Design. He was awarded PDF from Georgia Institute of Technology, USA in 3D VLSI. He has 16 years of experience of teaching and research. His area of research includes VLSI Design, Network Security.