I. J. Computer Network and Information Security, **2012, 6, 56-64**
Published Online June 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2012.06.08

Dynamic Inter Arrival Time Based Seamless Handoff for Mobile WIMAX Ping-Pong Calls Bypassing PKMv2 EAP Authentication

B.Sridevi, Dr.S.Rajaram
Department of ECE, Velammal College of Engineering and Technology,
Department of ECE, Thiagarajar College of Engineering, India
aisveriya@yahoo.com

Abstract **—** The rapid growth of wireless communication and its persistent use influences all walks of life. Mobile WiMAX IEEE 802.16e standard enabled convergence of mobile and fixed broadband networks through a common wide-area radio-access technology and flexible network architecture. It aims to provide seamless support to its users but an inevitable is that the long delay which occurs during the handoff management in every network process. This paper proposes a Dynamic Interval based Processing Algorithm to separate ping-pong users from the pool of users and to process them separately thus reducing the overhead of network re-entry process. Incoming users are divided into three categories like new user, old user and ping pong user. New user should undergo all the phases of network entry process, old user is provided with authentication key which leads to skipping of steps in generation of keys. Proposed algorithm deals with identifying the ping pong users by calculating the inter arrival duration and rate with same base station. When assured authenticated ping-pong users enter the network next time within the allotted time they will be provided with last used Traffic Encryption Key (TEK) thus bypassing key generation phase . It is observed that the proposed work performs the authentication phase and cancels the key generation phase which leads to minimum network entry delay and it saves to the maximum of 80% processing time. The network model was developed using Network Simulator and the algorithm was implemented in MATLAB GUIDE which gets connected to the database developed in MYSQL.This approach is justified through its timing analysis result which proves the efficient swift in the handoff processes.

Index Terms **—** IEEE802.16, WiMAX Handoff Delay, Authentication cost, Ping Pong, TEK utilization

I. INTRODUCTION

This is the era where a requirement is needed to replace the usage from fixed to the wireless medium without limiting the user to their time, place or any parameters. One such technology is WiMAX which provides ubiquitous access to the users. The WiMAX architecture is based on the use of standardized IP protocols and is compatible with service frameworks such as the IP Multimedia Subsystem (IMS). The WiMAX Forum charter also aims to deliver a framework for a high-performance end-to-end IP network architecture to support fixed, nomadic, portable and mobile users. Mobile WiMAX was the first mobile broadband wireless-access solution based on the IEEE802.16e .Next-generation mobile WiMAX will build on the success of the existing WiMAX technology and its time-to-market advantage over other mobile broadband wireless access technologies [1] .The backward compatibility feature will allow smooth upgrades and an evolutionary path for the existing deployments. One of the major goals of the 802.16e amendment is to introduce mobility in WiMAX. Here, we consider AAA (Authentication Authorization and Accounting) mechanism is utilized in the WiMAX architecture [2] .The two challenges faced by Mobile WiMAX are roaming cost and handoff cost. Consequently, Mobile WiMAX problems are based on IEEE802.16e. The Handover can be due to mobile subscribers migrates, to radio channel condition changes or to cell capacity considerations. During this handoff process, the mobile station has to accomplish the authentication procedure every time during the handoff from one base station to another.

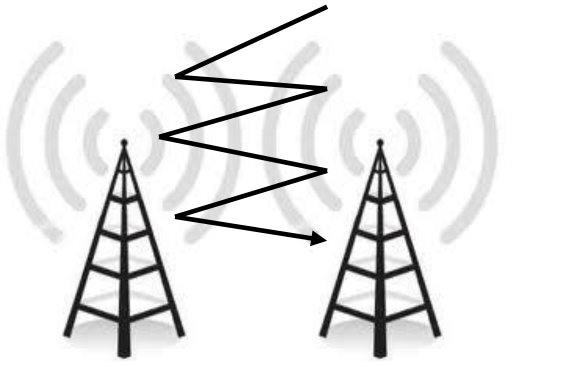


Fig1:Ping-Pong Effect

In WiMAX, the Mobile Station (MS) typically makes the final decision, whereas the Base station (BS) makes recommendations towards the candidate who target itself for handoff. BS may also assist in this process by providing the MS with a received signal strength or signal to interference plus the noise ratio may be used. They need security requirements, as some attacks are possible on the occasion of the handover procedure. Finally, the handover does not have only Layer 2 considerations. Layer 3 considerations are also needed. In a WiMAX network the ping-pong handover is a very common phenomenon to degrade the network performance. The ping-pong handover means handover to and fro between a pair of BS frequently. As shown in Fig1. Ping-pong effect occurs due to the frequent movement of mobile units between the two BS and high signal fluctuation at the common boundary of the BS .Since the ping-pong handover increases the occurrences of handover and thus the loading of the network, it is necessary for network operators to reduce this undesirable effect. Hence, the handover is not independent of the architecture. Ping pong is defined as the case that the MSS, while moving to a Target BS and performing network re-entry procedures with the Target BS, tries to return to its Serving BS and resume the communication with the BS as shown in Fig 1. When the MSS has detected the ping pong, it shall transmit MSS_PINGPONG_Report message to the Target BS for reporting its ping pong situation and attempt a fast call resuming with its Serving BS.

Even though WiMAX is mounting against its competing technologies, it experiences some setbacks with the existing procedure .One among them is unnecessary Handoff which leads to the rise in authentication cost. Several researches are proceeding with the objective of reducing handoff delay.To resolve this issue [4] proposes a key caching mechanism to eliminate the non necessary IEEE 802.1X authentication cost in WiMAX handoff which also discusses about the analysis of time to be fixed for key caching .[5] Introduces the relay station (RS) grouping as one optional mechanism in the IEEE 802.16j Multihop Relay standard to overcome handoff problems. The concept of RS grouping is to group neighbouring RSs together to form an RS group, which acts as a logical RS with larger coverage. This paper investigates RS grouping performance enhancement in terms of throughput and handoff frequency and it also proposes RS grouping algorithm to minimize handoffs by utilizing a greedy grouping policy .[6]Reduces the handover delay in the Multicast and Broadcast Services (MBS), the IEEE 802.16e standard by introducing MBS zone which is a group of base stations that are broadcasting the same multicast packets .It presents an MBS architecture that is based on location-management areas (LMAs), which can increase the sizes of MBS zones to reduce the average handover delay without too much bandwidth waste.A proxy mobile IP based layer-3 handover scheme for mobile WiMAX based wireless mesh networks was discussed .Proposed handover scheme performs layer-3 handover using handover anticipation information prior to completion of layer-2 handover in order to reduce handover latency [7].

[8] proposes a location aware fast handover technique for vertical handover between WiMAX and WiFi networks to minimize target network detection delay, select proper target network for handover and eliminate Ping-Pong effect .To prevent a handover ping-pong effect between base-station in WiMAX-compliant networks, a priority level is firstly assigned to the trigger causes for handover, and the prioritized causes are coded [9]. Additionally [10] proposes a triple-layer location management strategy to eliminate the generalized ping-pong effect with location areas in three different layers. Three layers are placed in such a way that any boundary or corner in one layer could be covered by a location area of another layer. If a mobile terminal moves out of the location area of the current layer, it could register with any of two location areas of the other two layers. To keep the Mobile Terminal (MT) away from another location update in a shorter time period, the MT will choose the layer whose boundary is farther away from the MT.

The rest of the article is organized as follows. Section II gives an overview of WiMAX network entry process Section III explains security negotiation and key derivation in PKM v2 – EAP authentication . Section IV briefly about the proposed work with NS2 WiMAX model,Fixed key caching and Dynamic Inter arrival time based Ping-Pong Seamless Handoff and Section V demonstrates the proposed techniques with corresponding results.

II. WIMAX NETWORK ENTRY PROCESS

We consider the basic architecture which includes the Mobile station (MS), the Base station (BS) and the Access Service Network-Gateway (ASN-GW). It is desirable to follow certain standard process to handle the network entry [2], [3] and hence the WiMAX authentication is carried as shown in Fig.2. Initially, when MS gets linked to the Wireless network, the following processes are done.

Step 1) Negotiation of security and authorization policy.

Step 2) The part of the authenticator is to send an EAP request message to the MS .

Steps 3) The function of the MS is to reply with an EAP response message with the user identity to the authenticator

Step 4) Authenticator forwards the EAP response message to the AAA server .

Step 5) Upon receipt of the user identity, the AAA server performs the SIM-based EAP authentication.

Step 5.1) Extensible Authentication Protocol Request comes into process mode without random key.

Step 5.2) The Response is carried away and the random key is generated.

Step 5.3) Complete Authentication procedure is conceded.

Step5.4) Request from the server is processed under the authenticated approach to the BS.

Step 5.5) Response is sent over to the AAA server for the further procedure.

Step 6) EAP Verification

Steep 7) Authentication Key Generation

Step 8) The ASN-GW forwards the EAP success message to the BS with AK .Upon receipt of this message, the MS generates its version of AK.

Step 9) Traffic Encryption Key (TEK) Generation.

This encryption key is used to afford data integrity and confidentiality for a communication session between the MS and the BS. The BS passes the generated TEK to the MS. If the MS switches from the old BS to the new BS connecting to a diverse authenticator (ASN-GW), a new MSK must be generated in this inter-ASN-GW handoff process, which is similar as the initial network access progression .In this case, the authenticator (ASN-GW) of the old BS will eradicate the MS key record (i.e., MSK, the MSK lifetime, and the MS authorization profile). When the MS budges back to the old ASN-GW again, another inter-ASN-GW handoff procedure should be performed, which may incur a long delay.

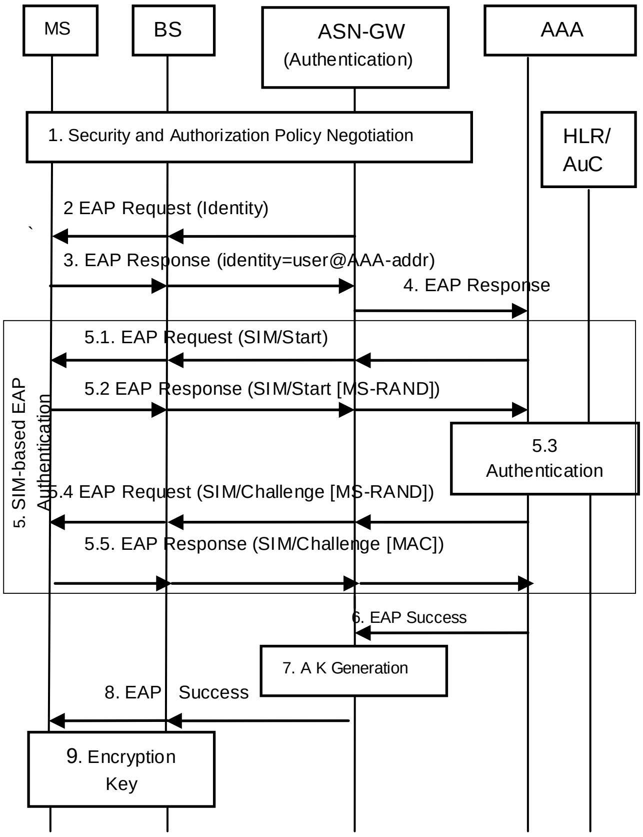

MS
BS
ASN-GW
(Authentication)
AAA
1. Security and Authorization Policy Negotiation
HLR/
AuC
2 EAP Request (Identity)
3. EAP Response (identity=user@AAA-addr)
4. EAP Response
5.1. EAP Request (SIM/Start)
5.2 EAP Response (SIM/Start [MS-RAND])
5. SIM-based EAP Authentication
5.3
Authentication
5.4 EAP Request (SIM/Challenge [MS-RAND])
5.5. EAP Response (SIM/Challenge [MAC])
6. EAP Success
7. A K Generation
8. EAP Success
9. Encryption
Key

Fig2: WiMAX Network Entry Process

III. SECURITY NEGOTIATION AND KEY DERIVATION IN PKM V2 – EAP AUTHENTICATION

The security sub layer of 802.16e consists of two component protocols namely the encapsulation and key management. As already mentioned, this paper focuses on key management performed by the PKMv2 protocol in IEEE 802.16e. Actually PKMv1 is a subset of PKMv2 in its function .Additionally PKMv2 supports mutual authentication, unilateral authentication and enables periodic re-authentication, reauthorization and key update. The MS to BS mutual authentication can occur in one of two modes of operation. First mode only mutual authentication while the second with mutual authentication followed by an EAP authentication as in Fig 3.

Step 1: MS → BS (PKMv2 RSA-Request message): This message follows an Authentication Information message immediately. By sending this message to the BS, the MS applies for an MSK (Master Session Key).

Step 2:BS → MS (PKMv2 RSA-Reply message): Upon receipt of the previous message, the BS performs the following actions: attests the identity of the client MS, generates an MSK and encapsulates it using the MS's public key and send it back to the MS using this message.

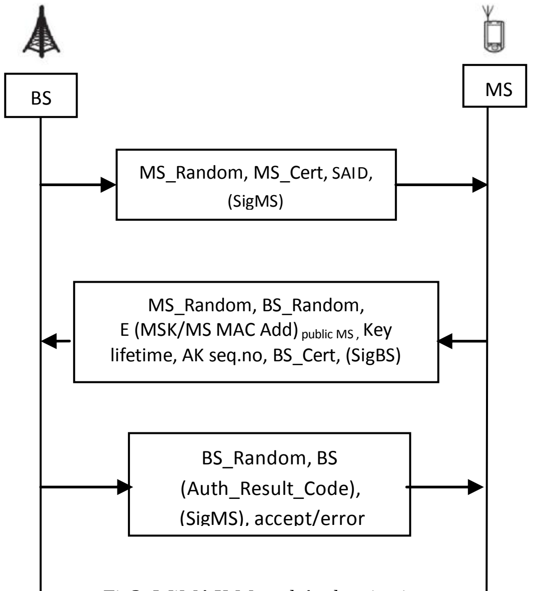

BS
MS
MS_Random, MS_Cert, SAID,
(SigMS)
MS_Random, BS_Random,
E (MSK/MS MAC Add) public MS , Key
lifetime, AK seq.no, BS_Cert, (SigBS)
BS_Random, BS
(Auth_Result_Code),
(SigMS), accept/error

Fig3: WiMAX Mutual Authentication

Step 3: MS → BS (PKMv2 RSA-Acknowledgement message): This message follows a PKMv2 RSA accept message or a PKMv2 RSA-Reject message. By this current message, the MS demonstrates to the BS that it is alive.

A successful execution of the EAP-based authentication mode is described in the following. At the initial entry, the MS and the Authentication Server (AS) mutually authenticate each other using an EAP-based authentication method.

The AS is an Authorization Authentication Accounting (AAA) Diameter or RADIUS server. The product of the EAP exchange is the 512-bit Master Session Key (MSK), known to both the AS and the MS. Then the MSK is securely transferred from the AS to the authenticator, i.e. the BS. Due to migration of the mobile subscribers the Handover get into account, by conditional changes in the radio channel or by cell capacity considerations. During this handoff process, the mobile station has to accomplish the authentication procedure every time during the handoff from one base station to another. Time variability and the unpredictability of the channel become more acute and the main challenge arise from the need to hand over sessions from one cell to another as the user moves across their coverage boundaries. During this handover process, it is still necessary to provide session continuity and to offer the previously negotiated end-to-end QoS and security levels [9]. The additional latency introduced by the handover process is an issue which needs to be tackled to minimize the impact of authentication procedure for the user who falls in the handoff process very frequently has need some measures to get an effective measurement by involving the Key-caching mechanisms (i.e. Increasing the processing time and therefore reduces authentication cost).

Key Derivation is handled by the RSA-based authorization produces the EAP-based MSK [10]. All PKMv2 key derivations are based on the Dot16 Key Derivation Function (Dot16KDF) which is an AES counter (CTR) mode construction used to derive an arbitrary amount of keying material from source keying material [11]. HMAC mode uses SHA-1 which is a secure hash standard algorithm which gives 160 bit output irrespective of any input [12].

A complete map of the 802.16e key hierarchy is depicted in Fig 4. For example, the EAP-based authentication process yields the MSK. MSK is given by ASN to BS by secured transmission and is transmitted to MS as explained earlier. MSK leads to the generation of other keys done independently in MS and BS [13].

Generation of various keys:

Master Session Key (MSK-512 bits): This key is generated by the ASN and sent to BS through secured channel .BS sends this key to MS after authenticating MS. MSK is generated by hashing MS_Random, BS_Random, MS_MAC,BS_MAC using SHA-512.

Pairwise Master Key (PMK 160bits): MSK is truncated in such a way that the First 160 bits is derived as PMK. Authorization Key (AK 160 bits): This is derived by

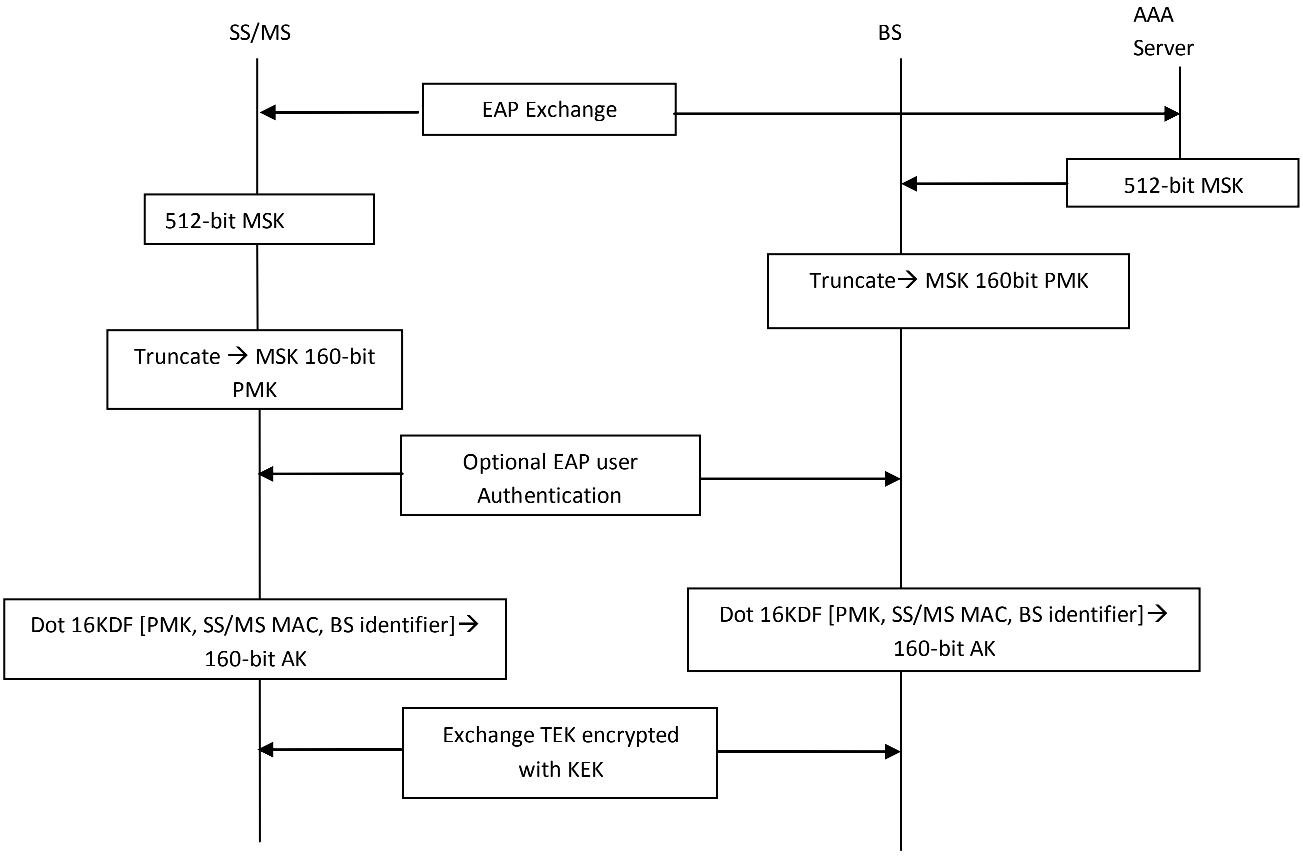

SS/MS
BS
AAA Server
EAP Exchange
512-bit MSK
512-bit MSK
Truncate→ MSK 160bit PMK
Truncate → MSK 160-bit PMK
Optional EAP user Authentication
Dot 16KDF [PMK, SS/MS MAC, BS identifier]→ 160-bit AK
Dot 16KDF [PMK, SS/MS MAC, BS identifier]→ 160-bit AK
Exchange TEK encrypted with KEK

Fig 4: Key Derivation

Dot16KDF (PMK, MS MAC Address |BSID| "AK", 160) *Integrated Key (HMAC mode Key 448bits*): This is derived by Dot16KDF ((AK, MS MAC Address |BSID| "HMAC_KEYS+KEK" , 448) *Uplink Key (HMAC_KEY_U 160 bits)* Integrated key is truncated in such a way that the First 160 bits is derived as HMAC_KEY_U.

Downlink Key (HMAC_KEY_U 160 bits): Integrated key is truncated in such a way that the second 160 bits i.e. 161th bit to 320th bit is derived as HMAC_KEY_U.

Key Encryption Key (KEK 128 bits): The remaining part of the Integrated key i.e. 321th bit to 448th bit is termed as KEK.

IV. PROPOSED METHOD

A. NS2 WiMAX Network model

A WiMAX 802.16 network model is developed in Network Simulator version 2 with two base station nodes which represents SBS and TBS, one sink node, five fixed nodes and ten mobile nodes as shown in Fig 5.

Ping–pong effect is analyzed with Mobile nodes which are programmed with random mobility. The overall objective is to reduce the authentication cost by avoiding repeated authentication steps to speed up handoff cost overloaded by ping-pong calls. As a solution, old users should be separated from the pool of users and from the pool of old users ping pong users should be identified and processed .Hence it is proposed to divide the large pool of users into three categories.

New user: User entering the network for the first time. This type of user should undergo all the phases of network entry process. Most valued key AK will be stored in ASN database for T seconds. While selecting the T value it should be noted that that it should not overload the ASN and not to be affected by various cryptanalytic attacks. We the authors of this paper have already discussed these and proposed compression using Huffman coding which yields fixed as well as variable length keys [14]. Numerical analyses of T value with both fixed and exponential case is provided by [6].

Old Users: Users entering the network within T seconds of first entry .This type of user need to undergo only authorization and authentication phases of network entry process as shown in Fixed key caching algorithm of Fig 6. AK is provided and others keys are generated from it. When the user enters after T seconds timer gets expired and the keys are deleted from ASN server and hence considered as new user .It was already discussed in detail in [15].

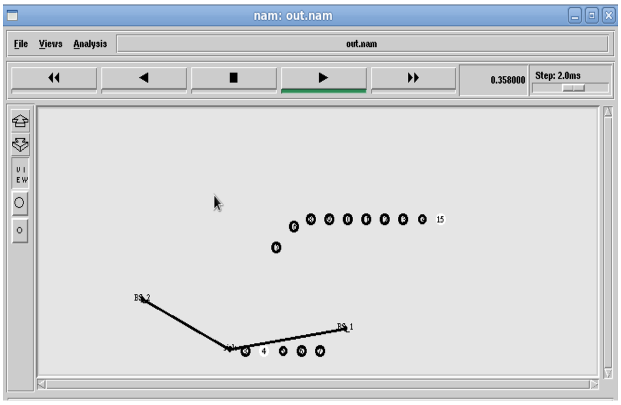


Fig.5. NS2 WiMAX Network Model

Ping-Pong User: Users entering the network more than three times with same inter arrival time with allowable tolerance as explained in Fig 7. They are provided with final key TEK which bypasses all the key generation steps. But it is essential to undergo authorization and authentication phase to enhance security.

B. Fixed Key Caching

Algorithm 1: Fixed key caching

```
    //MS to BS Authentication:
MS_request= MS_Random|MS_MAC|SAID|SigMS
// BS Verification
if $S \in U$
   Verify MS_MAC, SAID, SigMS
    if verification succeed
        if $AKASN(S) \neq NULL$
           allow as old user
          $AK = AKASN(S)$
 // Generate other keys HMAC_KEY_U,
HMAC_KEY_D,KEK,TEK
          HMAC mode Key= Dot16KDF (AK,MS MAC
         Address | BSID | "HMAC_KEYS +KEK", 448)
          HMAC_KEY_U =Truncate(HMAC mode    Key,160)
          HMAC_KEY_D =Truncate(HMAC mode
          Key  - HMAC_KEY_U, 160)
             KEK= Truncate( HMAC mode Key -
          (HMAC _KEY_U + HMAC_KEY_D),128)
          TEK=Dot16KDF(KEK, SAID,TEKNO, 128)
           start timer
        retain AKASN(S) for 20 seconds
         start session
        else
          accept as new user
//BS to MS Authentication:
BS_Response= MS_Random|BS_Random|
            Enc(MSK|MS_MAC)$_{Pubkey(MS)}$ |Key lifetime|
            Keyseq_no|BS_cert|SigBS
//MS Verification
 if Verification succeeds
//MS to BS Acknowledgement
 MS ACK=BS_Random |Success|SigMS
//Generate  keys PMK,AK
```

```
23.     PMK=Truncate(MSK,160);
24.     AK= Dot16KDF (PMK,MS
MACAddress|BSID|"AK",160)
// Generate other keys HMAC_KEY_U, HMAC_KEY_D,
KEK,TEK as in steps 9 to14
25.     AKASN(S)=AK
26.     start timer
27.     retain AKASN(S) for 20 seconds
28.     start session
29.     end
       else
30.     reject
31.     end
```

Fig.6. Algorithm 1 for Fixed Key Caching

In handling the handoff procedure the first approach is by holding the timer for the user who used to visit the region within the given time allocation which is watched by special timer . In the existing method the process get started from step 1 to step 9 for every handoff requirements for the user. In order to avoid the repetitions for the handoff the user is watched with the special timer which allocates time duration about T seconds .When the user visits the network within this time, he will be considered as old user and the process carries only Steps 1) and steps 6) to 9) to speed up the inter ASN-GW handoff process .The cache will be refreshed i.e. the timer starts again. If the user re enter beyond the caching time AK will not be available in the ASN and hence considered as new user.

Table 1: Terminology

Notation	Explanation
MS_Random	64 bit random number generated by MS
BS_Random	64 bit random number generated by BS
MS_MAC	MAC address of MS
SAID	Security Association Identity
Sig MS	RSA Signature of the authentication Message which contains the details.
S	Incoming MS
U	Collection of valid MSs
AKASN(S)	Authorization key of incoming MS stored in ASN Database
AK	Authorization key of S.
Pubkey(MS)	Public key of MS
BS_Cert	BS certificate usually its MAC address
BSID	Identification of BS
Enc()	AES Encryption
TEK NO	Represents the number of updated TEK.
TEKASN(S)	TEK of incoming MS stored in ASN Database
S_{IAT}	Inter Arrival Time of S

```
Algorithm3: Dynamic Inter arrival time based
algorithm
1.  Step 1 to 8 as in Algorithm 1
2.  if  TEKASN(S) ≠ NULL
3.  Allow as Ping-Pong User
//No need for Key Generation. Final key TEK
 is provided
4.  TEK= TEKASN(S)
5.  start session
6.  retain TEKASN(S) for 30 Seconds
7.  else if  AKASN(S) ≠ NULL
8.  Allow as old user
// proceed as in algorithm 1 from step 8 to step 25
9.  count=count +1
10. S_IAT =Difference in time between current entry and
    previous entry
 //Initially count=0 and Incremented by 1 for each
entry
11. if count>3 and S_IAT ≤ 10 seconds
12. Insert MAC address and TEK in ping-pong table
    in ASN database
13. start session
14. retain TEKASN(S) for 30 Seconds
15. end
16  else
17  reject
18  end
```

Fig 7: Algorithm 3 for Dynamic Ping-Pong Decision

V. RESULTS AND DISCUSSION

A. NS2 Ping-Pong Model

Mobile nodes move randomly from BS1 to BS2 .From the simulation it is inferred that the mobile nodes Switching between base stations is identified by change of color in nodes i.e yellow for BS1 and green for BS2. Network scenario is shown in Fig8.

Various components used in this implementation are User's inputs – the details of the user are acquired and processed through MATLAB GUI (ASN Gateway).

Database –Here we consider the standard MY SQL database which acts as the AAA Server in our proposed method.

Let us discuss the results with three categories of user

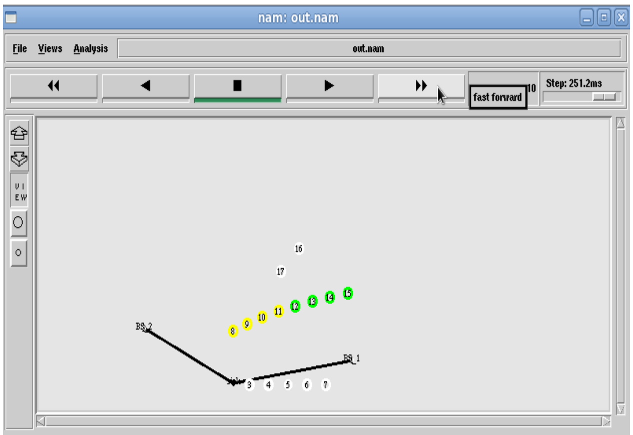
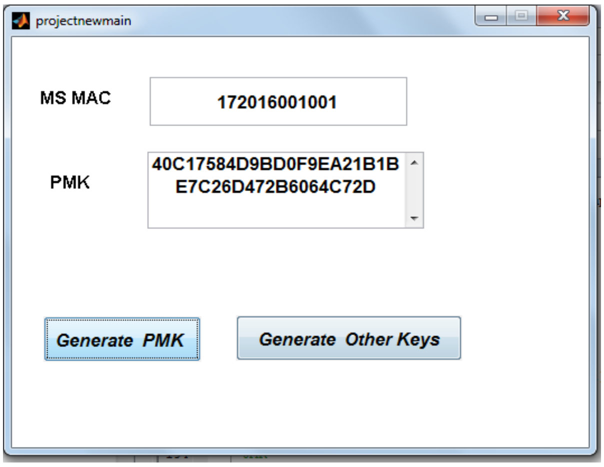


Fig 8 : NS2 model for Ping-Pong Effect

B. New user

User enters the network randomly and his validity is checked by corresponding with the existing IP addresses in the database. If not matched then affirmed as 'Unauthorized User'. If affirmed as Authorized User MSK is generated by ASN and send to BS .BS sends it to MS and derives PMK from MSK as in Fig 9. Other keys are generated in parallel by MS and BS which are shown in Fig 10.

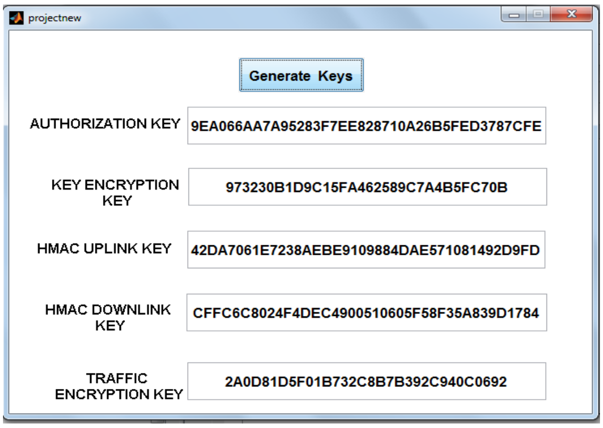

projectnewmain

MS MAC 172016001001

PMK 40C17584D9BD0F9EA21B1B E7C26D472B6064C72D

Fig 9: Check for validity for a new user

Moreover Authorization key (AK) is stored in the database against the corresponding MAC address. This key will be utilized when the MS comes back to the old ASN-GW within the allotted time i.e., AK lifetime so as to enable the user to bypass the steps. The connection with the database is prepared by the installation of ODBC driver. It is updated in real time with the changes occurring i.e., generated authentication key in the respected column .The connectivity between MATLAB GUI and the MySQL database provides the consideration of the ASN-GW.


projectnew

AUTHORIZATION KEY 9EA066AA7A95283F7EE828710A26B5FED3787CFE

KEY ENCRYPTION KEY 973230B1D9C15FA462589C7A4B5FC70B

HMAC UPLINK KEY 42DA7061E7238AEBE9109884DAE571081492D9FD

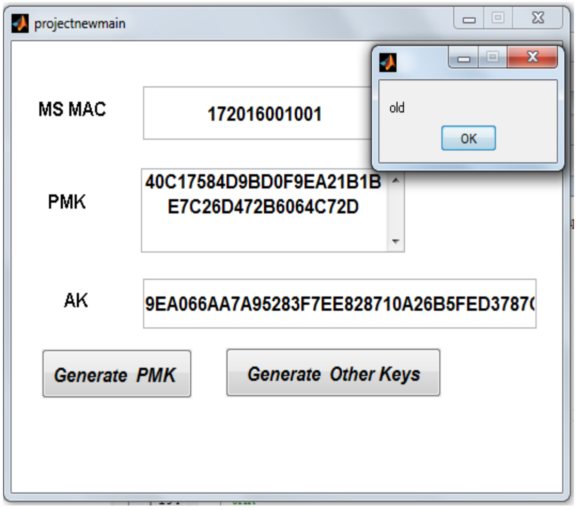
HMAC DOWNLINK KEY CFFC6C8024F4DEC4900510605F58F35A839D1784

TRAFFIC ENCRYPTION KEY 2A0D81D5F01B732C8B7B392C940C0692

Fig 10: Key Derivation for a new user

C. Old user

When the user re enters the network, the request is delivered to BS.


projectnewmain

MS MAC 172016001001

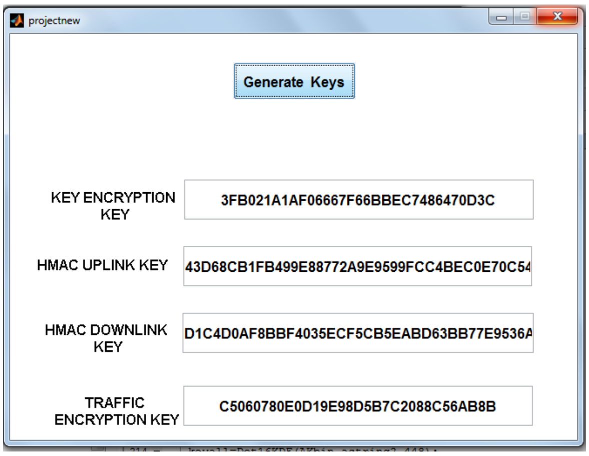
old

PMK 40C17584D9BD0F9EA21B1B E7C26D472B6064C72D

AK 9EA066AA7A95283F7EE828710A26B5FED3787(

Fig 11: Check for validity for an old user

BS checks the validity of MS and authenticates the MS and declares him as old user as in Fig 11. When MS is known to enter within its caching time, AK will be directly delivered bypassing all the steps. Other keys are derived in parallel by the BS and the MS as in Fig 12. This process saves upto 48.5% authentication cost compared to the user processing all the steps of network entry.



KEY ENCRYPTION KEY 3FB021A1AF06667F66BBEC7486470D3C

HMAC UPLINK KEY 43D68CB1FB499E88772A9E9599FCC4BEC0E70C54

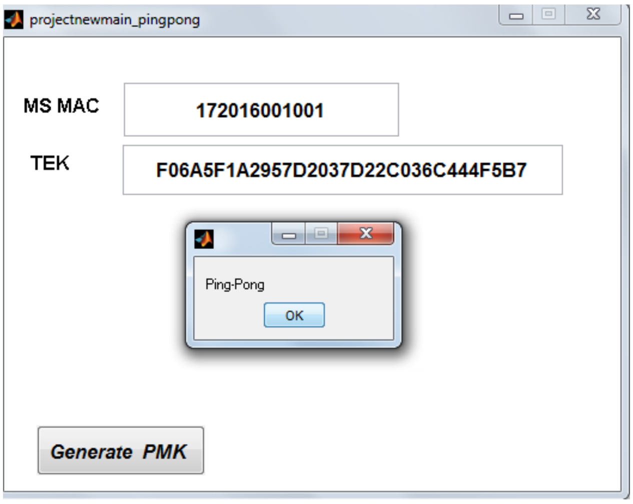
HMAC DOWNLINK KEY D1C4D0AF8BBF4035ECF5CB5EABD63BB77E9536A

TRAFFIC ENCRYPTION KEY C5060780E0D19E98D5B7C2088C56AB8B

Fig 12: Key Derivation for old user

D. Ping-Pong User

As per the algorithm shown in Fig 10 Ping-pong users are separated and the network entry process is made faster by providing the final key TEK. Fig 13 shows the process. As soon as the uses enters the network MAC address of the MS is examined with the authentication process and when it succeeds as ping-pong user, TEK is issued directly .It is observed that this proposed work saves 77.78% of processing time. By implementing proposed algorithm in the existing architecture, handoff delay paid for ping-pong calls will be reduced and thus reduces the authentication cost.



MS MAC 172016001001

TEK F06A5F1A2957D2037D22C036C444F5B7

Ping-Pong

Fig 13: Key Derivation for a ping-pong user

Table 2: Comparison of Performance

Type of User	Execution time in seconds
New User	10.5
Old User	5.4
Ping-Pong User	1.2

Execution time of different type of user for single attempt is given in Table 2 .Also the simulation is studied with 10 arrivals with all types of user and result is plotted in Fig 14. It shows the authentication cost reduction which enhances seamless handoff for old users and ping-pong users.

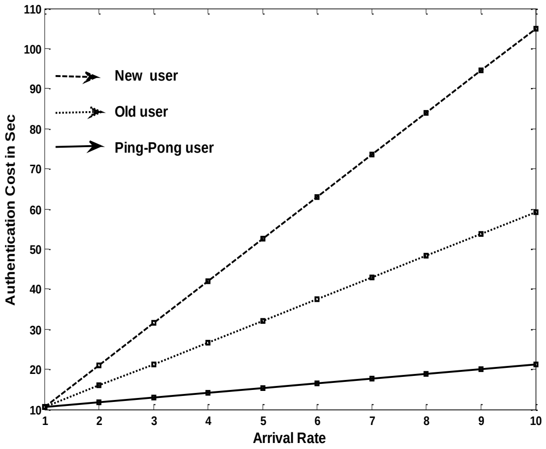


Fig 14: Authentication Cost Comparison

VI. CONCLUSION

In this paper, PKM v2 EAP protocol is implemented and the proposed ping pong separation technique to reduce authentication cost in WiMAX network entry process is incorporated .If the MS ensues to the old ASN-GW before the AK lifetime expires, it can reuse the AK without accomplishing the IEEE802.1X authentication .If the MS re-enters again and again to the same BS it is identified as ping pong call and key generation phase is bypassed to the reduction in authentication cost. A WiMAX network model is developed and simulated in NS2 with 15 users. The network entry process of this model with key caching technique is developed in MATLAB and their performance was analyzed. It is supported by our yielded observations

1) The Fixed Key caching mechanism speeds up the authentication process by saving 48.5% of the message exchange time.
2) Authentication cost reduction inferred by the proposed dynamic inter arrival based technique is of 77.78% compared to old users and 88.57% compared to new users.

Our Future work will be focused in enhancing to overcome the limitation of the traffic in the network and analyzing various attacks and their impacts so that ASN can differentiate the hackers from users. This approach will also be compared with other cost effective hand off techniques such as cross layer paradigm and vector accessing.

REFERENCES

[1]. Jeffrey J.Andrews,Arunabha Ghosh,Rias Muhamed , "Fundamentals of WIMAX Understanding Broadband Wireless Networking", *Prentice Hall*, 2007

[2]. Loutfi Nuaymi "WiMAX Technology For Broadband Wireless Access", *John Wiley & Sons Ltd,2007*

[3]. B. Rong, Y. Qian, K. Lu, H.-H.Chen, and M. Guizani, "Call admission control optimization in WiMAX networks," IEEE *Transactions on Vehicular Technology*, vol. 57, no. 4, pp. 2509–2522, Jul. 2008.

[4]. Shih-Feng Hsu and Yi-Bing Lin, Fellow, IEEE, "A Key Caching Mechanism for Reducing WiMAX Authentication Cost in Handoff ",*IEEE Trans. Veh. Tech.* vol 58 no 8, october2009.

[5]. Shun-Ren Yang, Chien-Chi Kao, Wai-Chi Kan, and Tzung-Chin Shih "Handoff Minimization Through a Relay Station Grouping Algorithm With Efficient Radio-Resource Scheduling Policies for IEEE 802.16j Multihop Relay Networks" IEEE Transactions On Vehicular Technology, Vol. 59, 2010

[6]. Ji Hoon Lee, Sangheon Pack, *Member*, Taekyoung Kwon and Yanghee Choi "Reducing Handover Delay by Location Management in Mobile WiMAX Multicast and Broadcast Services" IEEE Transactions On Vehicular Technology, Vol. 60, 2011

[7]. Kheya Banerjee, Sheikh Md. Rabiul Islam, Zulkernine Ibne Tahasin, Rokon Uddin "An Efficient Handover Scheme for PMIPv6 in IEEE 802.16/WiMAX Network" International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 ,2011

[8]. Jianlin Guo, Tsutomu Tsuboi, Jinyun Zhang "Location Aware Fast Handover Between WiMAX and WiFi Networks" MITSUBISHI ELECTRIC RESEARCH LABORATORIES , http://www.merl.com, 2010.

[9]. Alessandro De Sanctis, Marco Rastell, Daniele Tortora "METHOD FOR PREVENTING PING-PONG HANDOVER EFFECT IN MOBILE WIMAX NETWORKS",*United States Patent Application Publication*,2009

[10]. Guangbin Fan,Ivan Stojmenovic, and Jingyuan Zhang "Elimination of Generalized Ping-Pong Effects Using Triple-Layers of Location Areas in Cellular Networks", Computer Science and Information Systems Vol. 5, No. 1, June 2008

[11]. Lin, P. Shin-Ming Cheng Wanjiun Liao,"Modeling Key Caching for Mobile IP Authentication, Authorization, and Accounting (AAA) Services " *IEEE Transactions on Vehicular Technology*, vol. 58,pp. 3596 – 3608, Sept. 2009

[12]. Alina Olteanu, Yang Xiao,Yan Zhang Optimization Between AES Security and Performance for IEEE 802.15.3 WPAN" , *IEEE Transactions On Wireless Communications*, Vol. 8, 2009

[13]. Jung Je Son, Changai Koo," Enhancement of BS Initiated Handoff Algorithm for 802.16e", *IEEE 802.16 Broadband Wireless Access Working Group http://ieee802.org/16*

[14]. B.Sridevi and Dr.S.Rajaram ,"Compressed Key Exchange and Key Caching in PKMv2-EAP Mobile WiMAX Authentication" , European Journal of Scientific and Research, March 2012

[15]. B.Sridevi and Dr.S.Rajaram ,"GUI based cost effective handoff management in WiMAX Network entry process using key caching mechanism", SEISCON 2011, IEEE explore, Feb.2012

B.Sridevi, Assistant 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 University ,Tirunelveli in Networking. She published many research papers in International journals, national and international conferences. Her area of research includes Network Security, Wireless Networks. Email id: aisveriya@yahoo.com

Dr.S.Rajaram working as Associate Professor of ECE Department of Thiagarajar College of Engineering, Madurai, obtained her B.E., degree Thiagarajar College of Engineering from Madurai Kamaraj Univeristy, Madurai and M.E. degree from A.C.C.E.T Karaikudi. 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, Wireless Networks. He has published many research papers in International journals, national and international conferences.