Secured Cost Effective Group based Handover Authentication Scheme for Mobile WiMAX Networks

Mohanaprasanth.P
PG Student
Department of Electronics & Communication Engineering,
Velammal College of Engineering & Technology
Madurai-625009
Tamilnadu, India.

B.Sridevi
Professor
Department of Electronics & Communication Engineering,
Velammal College of Engineering & Technology
Madurai-625009
Tamilnadu, India.

ABSTRACT
Technological improvement of Wireless Communication is important aspect of our daily life. Mobile WiMAX IEEE 802.16m standard aims at fulfilling the requirements on 4G Systems. Providing seamless handover authentication is a critical issue in this area. This paper proposes a grouping of mobile stations algorithm to reduce the handover latency including security considerations. In our scheme the MSs which have similar Signal to Interference-plus-Noise Ratio (SINR) are grouped into the same handover group. In that MS group, while the first MS of the same handover group leaves from the service base station (SBS) to target BS (tBS), the SBS transmits all the details of the handover group member's security context to the tBS. Hence the rest of the MS in that group avoids the Extensible Authentication Protocol (EAP) and Security Context Transfer phases and directly performs the handover authentication which reduces the handover latency.

General Terms
Algorithm for grouping of mobile stations, Algorithm for initial & Handover authentication phase, Key generation.

Keywords
WiMAX, Group, Handover authentication, Extensible Authentication Protocol (EAP), Key generation.

1. INTRODUCTION
WiMAX (World Worldwide Interoperability for Microwave Access) has been established as one of the important milestone for broadband wireless communication. It mainly focus on a high data rate, wide coverage and security. IEEE 802.16m new version can be issued to satisfy the requirements of 4G systems. In IEEE 802.16m network, we are in need of fast authentication to perform the handover request from the MS due to the users mobility. RSA and EAP is the two methods used for the authentication. EAP is the method which is mostly used for the authentication [1] due to its flexibility and ability to interact with authentication, authorizing and accounting. A full EAP authentication lasts a considerable time which is difficult to support real-time applications, such as video conference, in a handover process. Now a days many methods have been introduced to reduce the handover authentication delay by avoiding the implementation of the EAP authentication. In the paper [5], also presented a fast handover authentication method based on ticket for IEEE 802.16m network. While an MS leaves from the service Base Station (SBS) to a target BS (tBS) it shows its ticket to the target BS and then that BS can authenticate the MS without intermingling with any other third party. Though, all these methods have not considered the case of many correlated MSs leaving together. For example, users taking the same vehicle such as a bus or a train are always located in the same network and move in the same direction [6]. While correlated MSs Leave together in a group and handover from one BS to another at the same time, handover performance could be enhanced if the current group information is used.

Since wireless networks are open to all it is vulnerable to attacks. Due to this an external adversary can easily compromise the MSs Identity privacy due to the complex information exchanged in the handover authentication process. Even though the schemes [7], [8] shield the identity information from the adversary, the location privacy is uninvolved and stills a challenge issue. In [9], the location privacy preserving is realized at the cost of the time-consuming. For the purpose of a safe and effectual handover process, in this paper, an effective group detection handover authentication method with secrecy preservation for mobile WiMAX networks. This paper comprises of the following two aspects:

1) Our method transmits all the handover group members' details (security contexts) to the target BS using the Security Context Transfer (SCT) scheme during the first MS handover authentication phase. Then the rest of the MSs in the handover group can avoid both the EAP authentication and the SCT phase to perform directly the 2-way handshake with the target BS. Furthermore, not like the conventional SCT schemes [2], [3], the security context is not used as the key material for deriving new session key but served as a symmetric key of Hash-based Message Authentication Code (HMAC) to process mutual authentication for the 2-way handshake protocol.

2) In this scheme, MS only provides a pseudonym instead of its real identity in the initial authentication phase and changes its pseudonym in each handover authentication phase, so it can protect the MSs Identity privacy and avoid adversary from tracing its movement route. Unlike from the existing method [9], our scheme does not require MS to perform any complex operations.

2. SYSTEM MODEL
A typical topology of mobile WiMAX networks is shown in Fig. 1. In this network, the Access Service Networks (ASN) contains of ASN Gateway (ASNGW) and BS. An ASN-GW controls many BSs and is responsible for forwarding

authentication messages between the MS and the AAA server. A BS provides WiMAX radio access for the MSs authenticated by the AAA server. Assume that all the objects, AAA server, ASN-GW and BS, maintain trusted relations and have established secure connections. Note that the MSs may be a single user or some correlated users who take the same vehicle (such as a bus or a train). If MSs travel through the same BSs at the same points in time, it can be assumed that they move together and that their mobility patterns are correlated. According to MSs Signal-to-Noise Ratio (SNR) and history handover information etc., it can classify the correlated MSs into a handover group by some grouping algorithms. The grouping algorithm is outside the scope of this letter since many efficient schemes [10], [11] have been proposed and both of them can be used in our scheme by minor modifications.

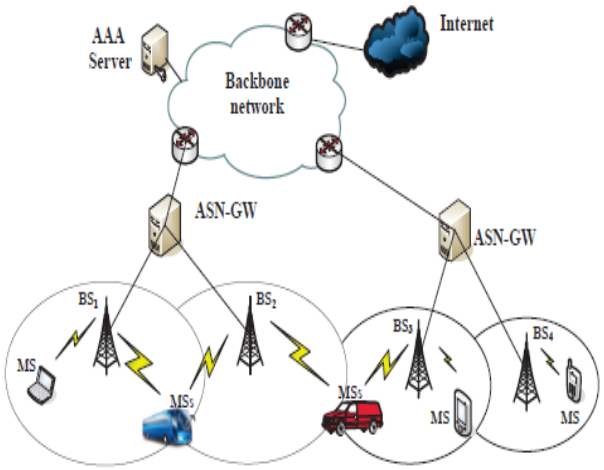

Fig 1: Architecture of Mobile WiMAX Networks

3. GROUPING OF MOBILE STATIONS

Grouping of mobile stations can be done by using the two following parameters signal to interference plus noise ratio (SINR) and interference to other interference plus noise ratio (IINR). These parameters can be used to find the correlated MSs. There is a SBS and 6 nearest tBSs, mobile stations in the BS1 have the six possible BS as shown in fig.2.

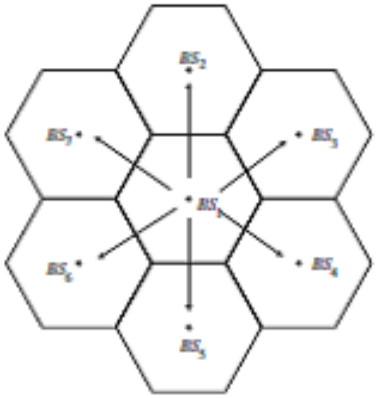

Fig 2: MS mobility model

The MSs can be grouped whose mobility patterns are similar and have the correlated SINR and IINR values. From this, the average SINR and IINR values can be calculated to eliminate the fading effects.

Algorithm 1: Grouping of MSs

Input:
{SI N R1,1(t), . . ., SI N Ri,1(t), . . ., SI N Rm,1(t)} is the set of average SINRs value between MSs and *BS*1; {I I N R1,∂ (t), . . ., I I N Ri,∂ (t), . . ., I I N Rm,∂ (t)} is the set of avg IINRs values between MSs and *BS*∂, where ∂ =2*to*7;

Output:
Output shows that, the MSs connected with each BSs

Initialization:
M ← {*MS*1, *MS*2, . . ., *MSm*}; / *M* indicates the *MSs* which are not grouped/
A ← ∅; / ∗ *A* represents the MSs Set which aren't joined in the current round of grouping
//Grouping procedure//
n ← 0; / ∗ *n* is the index of *Group* */
∂ ← 1; / ∗ ∂ is the index of a *BS* */
Procedure:
for(∂ = 1*to*6) do
∂ ← ∂ + 1;
n ← *n* + 1;
A ← *M*;
while(*A* _= ∅)
*BS*1 selects *MSi* from *A*;
if (*SI N Ri*,1*(t)* − *I I N Ri*,∂ *(t)* < −1 and *Di (t)* ≤ *D*)
then
*BS*1 adds *MSi* into *Grouping*;
*BS*1 removes *MSi* from *M*;
end
*BS*1 removes *MSi* from *A*;
end
end

Figure.3: Algorithm for Grouping of MSs.

The above algorithm 1 shows the grouping of MSs using the following factors such as SINR, IINR. In this algorithm M indicates that the MSs which are not grouped. Initially A should be empty which denotes the MSs are not joined in the current group.

4. PROPOSED HANDOVER AUTHENTICATION PHASE

4.1 Initial Authentication Phase

When an MS (MSi) first accesses to mobile WiMAX networks, it needs an initial authentication as shown in Fig. 2. Then a successful EAP authentication, the MSi and AAA server create a shared 512 bit Master Session Key (MSK). Then the AAA server issues MSK to ASN-GW. After receiving MSK. The ASN-GW derives Pairwise Master Key (PMK) from the MSK as formula (1) and then sends it to the authorized *BS*1.

PMK = Dot16KDF (MSK, BS1ID, 160) (1)

The BS1ID is the identity of BS1, and Dot16KDF refers to a keyed hash function defined in IEEE 802.16m standard [1]. After receiving the PMK, BS1 performs the 2-way handshake procedure with *MSi* to build security solutions, including,

including Authorization Key (AK), Transmission Encryption Keys (TEKs) and HMAC keys, in the following steps.

Step 1: BS1 first computes a Temporary HMAC Key (THK) as in (2) and chooses a random number $r1 \in Z*q$. Then it sends a key agreement request message (MSG#1) containing the current time *tt*, *r*1*P*, *BS*1*ID* and their HMAC value (HMAC using the *THKi*) to *MSi*. Note that the timestamp included in the message is to prevent the replay attack.

$$THKi = Truncate (PMK, 128) \quad (2)$$

Truncate(x, y) is defined as the last *y* bits of *x* if $y \leq x$ or entire *x* if $y > x$.

Step 2: After receiving MSG#1, *MSi* checks the current time *tt* and determines whether the received message is fresh or not. Assume the message propagation time limit is ε, we should have $tt - tt \leq \varepsilon$. If not, simply discard it. Otherwise, *MSi* computes *PMK* and *THKi* as in (1) and (2), respectively. Then it uses *THKi* to verify the HMAC value. If the HMAC value is valid, *MSi* further chooses a random number $r2 \in Z*q$ and then sends a key agreement response message (MSG#2) to *BS*1 that includes the MSiID, current time *tt*, and their HMAC value (HMAC using the *THKi*), where *MSiID*0 is a permutation of the *MSi*'s Media Access Control (MAC) as defined in IEEE 802.16m standard.

Step 3: After receiving MSG#2, *BS*1 also checks the current time *tt* and determines whether the received message is fresh or not. If not, simply discards it. Otherwise, *BS*1 verifies the HMAC value using the saved *THKi*. If the HMAC value is verified, *BS*1 judges *MSi* as a legitimate user and accepts its access request. Finally, both *MSi* and *BS*1 can obtain the same *AK* = *r*1*r*2*P* and then derive the TEKs and HMAC keys as defined in IEEE 802.16m [1].

Algorithm:2: Initial Authentication Phase

// EAP Authentication//

1) MS sends the EAP Authentication request message to AAA Server.
2) AAA server sends 512b MSK to BS via ASN GW
3) // Two way Handshake //
   - 3.1) BS derives THKϵ r1
   - 3.2) M1=(BS id,tt,r1p)(HMAC)
   - 3.3) MS derives the THKϵ r2
   - 3.4) **If** both HMAC are valid
     - 3.4.1) choose r2
   - 3.6) M2=(MS id,tt,r2p)(HMAC)
   - 3.7) If BS verifies received HMAC with already BS received HMAC Key.
   - 3.8) If verification succeeds both MS & BS generate same AK=r1r2P

Fig 4: Algorithm for Initial authentication phase

Algorithm 2 shows the Initial authentication phase between MS and AAA server. It shows the entire EAP authentication mechanism and two way Handshake method between the BS and MS.

4.2 Handover Authentication Phase

Handover authentication procedure for a group of MSs leaving from BS1 to BS2 can be explained by using the following algorithm3.

Algorithm 3: Handover Authentication phase:

//MS1 to BS1 Handover Initiation//

1) BS1 performs SCT to BS2.
2) BS1 generate THK for every MSs.
   - 2.1) THKi = H(AKi, MSi_id,BS1_id,BS2_id)
     Where i = 1 to n.
3) BS2 receives the THK and MS_id
4) BS1 to MS1 Handover Command message

// 2-way Handshake //

5) MS1 sends MSG#1 to BS2 via THK by choosing r3
   - 5.1) MSG#1=(MS1_id, tt, r2p)(HMAC)
6) BS2 verifies the received HMAC value & choose r4 and send MSG#2 to MS1
   - 6.1) MSG#2=(BS2_id, tt, r4p)(HMAC)
7) MS1 verifies the received HMAC value and compute AK
   - 7.1) AK = r3r4p
8) MS1 & BS2 Derive same AK = r3r4p

// MS2 to BS1 Handover Initiation//

9) MS2 performs the Handover from BS1 to BS2

// MSn to BS1 Handover Initiation //

10) MSn performs the Handover from BS1 to BS2

Fig 5: Algorithm for Handover authentication phase

Step 1: MS1 sends a Handover (HO) Initiation message, including the identifier of the target BS, to BS1.

Step 2: Upon receiving the HO Initiation message, BS1 uses the Grouping of MS algorithm to group MSs for the current serving BS1 and then searches the group in which the current handover BS is. Based on the searching results, it computes the new THKs of all MSs within the same handover group (we assume that the number of group members is *n*) as follows:

THK_1= H *(*AK1, MS1ID∗, BS1ID, BS2ID*)*
THK_2= H *(*AK2, MS2ID∗, BS1ID, BS2ID*)*
THK_n= H *(*AKn, MSnID∗, BS1ID, BS2ID*)*

Step 3: After the security context, are successfully transmitted to BS2, BS1 sends a HO Command message to MS1

Step 4: Upon receiving the HO Command message, MS1 initiates the 2-way handshake to BS2as follows:

a) MS1 computes THK_1= H *(*AK1, MS1ID∗, BS1ID, BS2ID*)* and chooses a random number *r*3 ∈ *Z*∗q. Then it sends a key agreement request message (MSG#1) containing the MS1ID∗, current time *tt*, *r*3*P* and their HMAC value (HMAC using the THK_1*)* to BS2.

b) Upon receiving MSG#1, BS2 checks the current time *tt* and determines if the received message is fresh or not. If not, simply discard it. Else, BS2 obtains the THK_1 according to MS1ID∗ and then uses it to verify the HMAC value. If the HMAC value is valid, BS2 judges the MS1 as a legitimate user. Then BS2 chooses a random number *r*4 ∈ *Z*∗q and sends a key agreement response message (MSG#2) to MS1 that includes the current time *tt*, *r*4*P*, *BS2I D* and their HMAC value.

c) After receiving MSG#2, MS1 also checks the current time *tt* and determines if the received message is fresh or not. If not, simply discard it. Otherwise, MS1 verifies the HMAC value. If the HMAC value is verified, MS1 judges the BS2 as a legitimate BS.

d) Both MS1 and BS2 calculate *AK*_1= *r*3*r*4*P* and then derive the TEKs and HMAC keys for the supported SAID as specified in the initial authentication phase.

5. RESULTS AND DISCUSSIONS

5.1. MATLAB Grouping model

Mobile stations move randomly from serving Base Station to target Base Station. The MSs can be grouped whose mobility patterns are similar and have the correlated SINR and IINR values. From this, the average SINR and IINR values can be calculated to eliminate the fading effects. Fig 6(b) shows that the mobile station group connected with different base stations. In every mobile station group first MS performs the authentication phases, other MS bypasses these phases.

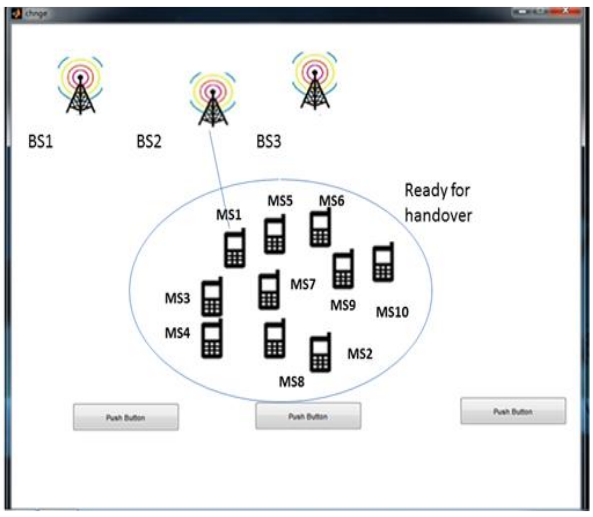

Fig 6(a): MSs before grouping

The SINR and IINR values of different MS between different BS can be shown in the following simulated results *Table 1, 2*. This result can be obtained by using the Grouping of Mobile Station algorithm (algorithm 1). *Table 3* shows that the MSs connected with the BSs in the form of grouping.

Figure 6(a) shows that the MSs Status before grouping.

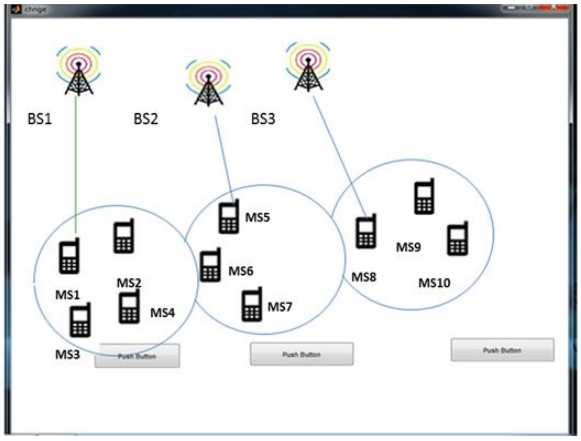

Fig 6(b): MATLAB model for grouping of MSs

5.2. GENERATION OF KEYS

Master Session Key (MSK-512 bits): This key is made by the ASN and sent to BS through secured channel .BS sends this key to MS after authenticating MS. MSK is created by hashing MS Random, BS Random, MS_MAC,BS_MAC via 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 Dot16KDF (eqn1).

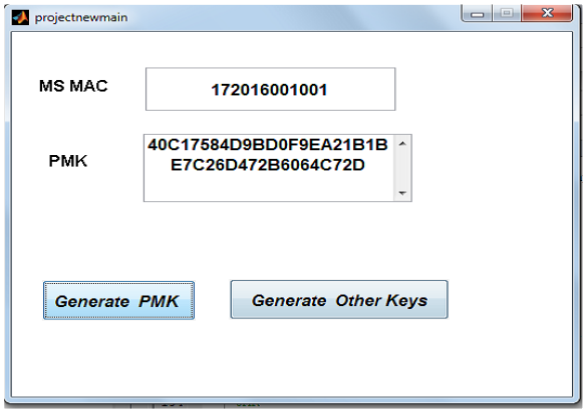

Fig 7: Generation of PMK

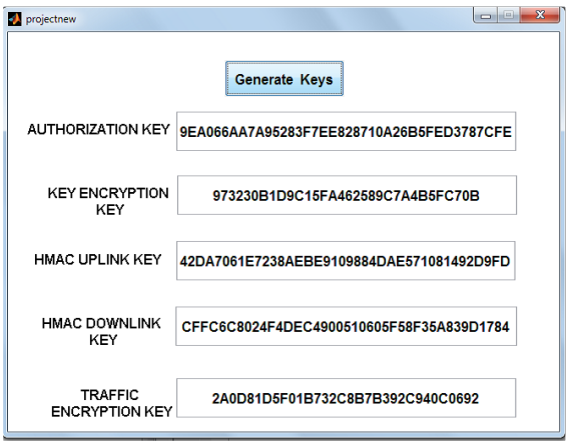

Fig 8: Key generations

5.3 SIMULATED MATLAB GROUPING TABLE

Table.1: SINR value between BS and MS

	MS1	MS2	MS3	MS4	MS5	MS6	MS7	MS8	MS9	MS10
BS1	37	37	26	31	38	39	33	22	33	19
BS2	27	33	39	36	29	35	27	40	40	37
BS3	26	28	23	36	38	39	30	31	21	38

Table.2. IINR Values between MS to BS

	BS1	BS2	BS3
MS1	28	38	38
MS2	35	38	24
MS3	33	33	20
MS4	27	24	34
MS5	24	38	37
MS6	26	29	33
MS7	37	32	31
MS8	25	28	34
MS9	38	34	18
MS10	33	28	28

Table.3: Grouping of Mobile Stations

	MS	MS	MS	MS
BS1	3	7	9	10
BS2	2	5	6	
BS3	1	8	4	

The above figure 7 and 8 shows the simulated output of different Key generations such as Authorization Key (AK), Transmission Encryption Key (TEK), HMAC uplink key, HMAC downlink key.

6. CONCLUSIONS

In this paper, we have proposed an effective group based handover authentication scheme for mobile WiMAX networks. The key idea of our method is that all the handover group members' security contexts are transmitted to the target BS during the first MS handover authentication phase. Thus the rest of the MSs in the same handover group can avoid not only the EAP authentication but also the SCT phases to perform directly the handover authentication. Compared to the existing schemes, the proposed scheme is very effective in reducing handover latency but with high security performance.

7. REFERENCES

[1] IEEE standard 802.16m-2011, "Air interface for broadband wireless access systems - Amendment 3: advanced air interface," May 2011.

[2] C. Politis, K. A. Chew, N. Akhtar, et al., "Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks," IEEE Wireless Commun., vol. 11, no. 4, pp. 76–88, Aug. 2004.

[3] C. M. Huang and J. W. Li, "A cluster-chain-based context transfer mechanism for fast basic service set transition in the centralized wireless LAN architecture," Wireless Commun. Mob. Comput. vol. 9, no. 10, pp. 1387–1401, Oct. 2009.

[4] J. Hur, H. Shim, P. Kim, et al., "Security considerations for handover schemes in mobile WiMAX networks," in Proc. 2008 WCNC, pp. 2531– 2536.

[5] A. Fu, Y. Zhang, Z. Zhu. et al., "A fast handover authentication mechanism based on ticket for IEEE 802.16m," IEEE Commun. Lett. vol. 14, no. 12, pp. 1134–1136, Dec. 2010.

[6] L. Shan, F. Liu, and K. Yang, "Performance analysis of group handover scheme for IEEE 802.16j-enabled vehicular networks," in Proc. 2009 Advances in Data and Web Management, pp. 653–658.

[7] F. Pereniguez, G. Kambourakis, R. Marin-Lopez, et al., "Privacy enhanced fast re-authentication for EAP-based next generation network," Comput. Commun. vol. 33, no. 14, pp. 1682–1694, Sep. 2010.

[8] Q. Jing, Y. Zhang, A. Fu, *et al.*, "A privacy preserving handover authentication schemes for EAP-based wireless networks," in *Proc. 2011 GLOBECOM*, pp. 1769–1774.

[9] C. Zhang, R. Lu, P. Ho, *et al.*, "A location privacy preserving authentication scheme in vehicular networks," in Proc. 2008 WCNC, pp. 2543–2548.

[10] L. Lee, D. Kim, B. Chung, et al., "Adaptive hysteresis using mobility correlation for fast handover," IEEE Commun. Lett. vol. 12, no. 2, pp. 152–154, Feb. 2008.

[11] H. H. Choi, J. B. Lim, H. Hwang, *et al.*, "Optimal handover decision algorithm for throughput enhancement in cooperative cellular networks," in Proc. 2010 IEEE VTC – Fall, pp. 1–5.