CHAPTER 6

AUTHENTICATION COST REDUCTION BY PRE-AUTHENTICATION AND PASSPORT HANDOFF

6.1 INTRODUCTION

As the mobile WiMAX is challenged by the unwanted handoff delay, previous chapters 4 and 5 detailed the proposed work in reducing the authentication cost for re-entering MSs and re-entering ping-pong MSs which in turn reduces the handoff delay. This chapter proposes the algorithms in the perspective of reducing the authentication cost of newly entering MSs to the Base Station (BS). This is challenged by the cost affective existing handoff process which undergoes authentication and Connection Identifier (CID) generation. As these processes cannot be skipped because of their importance in providing security, measures can be taken to advance them independently of handoff. This chapter proposes a secured pre-authentication technique and Reserved CID (RCID) based passport handover to reduce the handoff delay and increase the speed of the intra-ASN handoff.

The proposed pre-authentication method is intended to reduce the authentication delay in getting authenticated by the Pre Authentication Authority (PAA) which is assumed to be included as a function of ASN-GW. Due to this, a major part of authentication phase can be skipped in handoff process. RCID based passport handoff enables the pre-authenticated MSs to receive RCIDs from the ASN-GW on their initial entry to ASN. This method
enhances the authentication cost reduction by skipping the generation of CIDs in each handoff.

6.2 AUTHENTICATION IN MOBILE WIMAX

Authentication occupies a substantial amount of handoff processing time (Anmin Fu 2010) and it is essential to ensure the security. Since the authentication phase of handoff process is independent, it can be performed separately before the actual handoff takes place. Hence the time consumed by authentication phase can be saved during the handoff process. As explained in chapter 3, authentication of mobile WiMAX can be processed according to PKM V2 by any one of the methods like RSA method, EAP and RSA followed by EAP.

6.2.1 Pre-Authentication

With the prior knowledge of authentication & the key exchange phase and the handoff process of mobile WiMAX already explained in chapter 3 & chapter 4 respectively, this section details the role of pre-authentication in handoff process. As shown in Figure 4.2, MS authorization, authentication and key exchange are processed as the sixth step of handoff process. EAP authentication is shown in Figure 6.1 which explains the process of authentication done between the MS and BS with the help of ASN and AAA server or ASN server (Aboba et al 2004).

Initially the EAP request is sent from ASN to MS through the BS. The response is sent from MS to ASN which is forwarded to the AAA server for checking the identity of MS with AAA server using the EAP protocol. After completing the EAP process, key generation starts according to PKMV2 protocol and the distribution of keys follows it (Ram Dantu et al 2007). Before generating TEK, security associations should be exchanged with SA request,
SA responses and then finally results in the generation of TEK as shown in Figure 6.1 (Jeffrey et al 2007).

![Figure 6.1 Message Exchange and Key Derivation in initial network entry](image)

When the MS requests for pre-authentication, ASN checks the validity of MS by EAP message transfer and then generates the root key MSK and sends it to both the SBS and the MS. During the handoff process, MS and BS derive the other keys PMK and AK mutually from MSK. Security association can be generated after this step and exchanged between the MS.
and BS to derive the final key TEK which is used to encrypt the user data. Although this method reduces handoff delay, MSK delivery is not convincing in the perspective of secured key exchange as the MSK generation does not bind the Base Station Identifier (BSID) and the identification of the MS (Seok-Yeung Tang et al 2010). Any fraudulent BS that receives the MSK from the ASN can derive the PMK and AK of other NBSs with the known identifications of the BS and the MS.

6.2.2 Passport Handoff

As one of the main objectives of this research is to reduce handoff delay, various techniques having the scope to reduce handoff delay are analyzed. Reviews of research with the similar objective induced to study about Connection identifier (CID) generation during handoff at each BS.

Role of CID in Mobile WiMAX

Before any data transmission happens, the BS and the MS establish a unidirectional logical link, called a connection, between the two MAC-layer peers. MS can have several connections to a BS for different services, like network management or data transport. Each connection is identified by a CID, which serves as a temporary address for data transmissions over the particular link. In MAC, all associations use different parameters for priority, bandwidth and security. CID is used in all MAC level QoS functions such as classifier and QoS scheduler to identify and differentiate traffic in order to maintain service level and fairness between connections (Mobile WiMAX PartI, WiMAX forum 2006). As soon as a MS joins a network, three different CIDs are allocated to it. Moreover, each CID has separate QoS requirements, which are used by different management connection levels like Primary, Basic and Secondary Management connections (Ramjee Prasad & Fernando 2010). Both basic and primary management connections are created when a MS is
joined to a BS network (Andrews et al 2007). All MAC connections for IEEE 802.16 are identified by a 16-bit CID. Once all the management connections are established, an MS can set up transport connections. The BS computes the value of ‘m’ (affordable amount of MSs) which decides the range of various CIDs in mobile WiMAX as shown in Table 6.1 and explained as follows:

- An initial ranging connection identifier is a code that is used during the initial connection to a wireless system to determine how much transmission timing adjustment is required.

- A basic CID (BCID) is a logical channel that is assigned during the initial ranging process. Basic CID connections are used for time sensitive MAC control messages such as RF power control and time alignment.

- A primary management CID (PCID) is a logical channel that is used to transfer link control messages.

- A secondary management CID (SCID) is a logical channel that is used for upper layer control messages such as Dynamic Host Configuration Protocol (DHCP) and Trivial File Transfer Protocol (TFTP) messages.

- A transport CID (TCID) is a logical channel that is used to transfer user data. Transport connections can use different CIDs in the uplink and downlink directions.

- Multicast polling CID (MCID) are used to prompt subscriber stations which are part of a multicast group that have data to transmit their data using a contention control process.

- A broadcast CID (BrCID) is used to transfer broadcast messages to all devices that are listening to the radio channel.
Table 6.1 Range of CID

<table>
<thead>
<tr>
<th>S.No</th>
<th>Type of CID</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IRCID</td>
<td>0000 or FEFF</td>
</tr>
<tr>
<td>2</td>
<td>BCID</td>
<td>0001 to m</td>
</tr>
<tr>
<td>3</td>
<td>PCID</td>
<td>m to 2m</td>
</tr>
<tr>
<td>4</td>
<td>TCID &amp; SCID</td>
<td>2m to FE9F</td>
</tr>
<tr>
<td>5</td>
<td>MCID</td>
<td>FF00 to FFFC</td>
</tr>
<tr>
<td>6</td>
<td>BrCID</td>
<td>FFFF</td>
</tr>
</tbody>
</table>

Service Flow is a MAC transport service and provides unidirectional transport of UL packets or DL packets. A service flow is characterized by a set of QoS parameters such as latency, jitter and throughput assurances. In order to standardize the communication between the MS and BS, these attributes include the details of MS requests for uplink bandwidth allocations and the expected behaviour of the BS uplink scheduler. CID maps to a Service Flow Identifier (SFID), which provides the QoS parameters of the service flow associated with that connection.

The MS initiates the ranging process with Initial Ranging CID (IRCID) whose value is 0000H (in Hexadecimal). Only after the successful completion of ranging process, BCID and PCID are generated by BS and sent to MS as shown in Figure 6.2. Then the negotiation of capabilities of BS and MS are done mutually followed by authorization and key exchange process. After the successful completion of key exchange, MS is registered as an authorized user and TCID & SCID is allocated by BS. Network entry of MS into the BS needs the compulsory generation of BCID, PCID, TCID and SCID. Allocation of each CID indicates the successful completion of the process upto that level. The scope of CIDs is only within the BS, hence they need to be generated randomly with the available pool of CIDs (Byeong Gi Le et al 2008).
6.3 REVIEW OF PREVIOUS RESEARCH WORKS

Hur et al (2008) secured the pre-authentication by the derivation of PMK and AK for each BS. PMK and AK pair is distributed to the corresponding BS as well as MS. Since PMK has the information about BSID, it cannot be used by other fraudulent BSs. But, this work burdens the ASN-GW by deriving many keys and also the keys thus generated will not be fresh during handoff. The point to be noted here is that AK has its limitation of key lifetime and the pre-authentication makes the key to lose its lifetime before the actual usage in the handoff. The HOKEY working group has proposed an EAP based pre-authentication model (Ohba et al 2010) called Handover Early Authentication (HOEA) protocol for Mobile IPv6 network. 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 can be applied only when the link layer
supports proactive signalling and there are chances for the handover to get started before the pre-authentication phase completes which results in a failed pre-authentication (Yi-Bing Lin & Yuan-Kai Chen 2003).

An EAP-based Pre-Authentication scheme (EPA) was proposed to reduce the authentication delay in inter-ASN handovers (H. M. Sun et al 2007 and Mohammed Awadh Ben-Mubarak et al 2009). In this scheme, the MS exchanges the key materials with different neighbour ASN-GWs (nASNs) of the serving ASN-GW and home ASN-GW (hASN). Thus it can proceed directly with the 3-way handshake during handoff instead of performing a full EAP authentication. The advantage of EPA over HOEA is that proactive signalling is not required and the pre-authentication with the nASN-GWs is performed immediately after the MS attaches to the current hASN-GW which ensures the completion of pre-authentication before the handoff. However, the EPA is vulnerable to security threats like DoS attacks and replay attacks and also it leads to the wastage of unnecessary effort for key exchange between the MS and those nASN-GWs that the MS never roams to.

Thuy Ngoc Nguyen & Maode Ma (2012) proposed fast and secure inter-ASN handovers by Enhanced EAP Method (EEP) and compared it with EAP and HOEA. The EEP scheme not only detect & prevent the DOS and the replay attacks, it also significantly reduce pre-authentication delay as well as computing power required. But the handover latency of the EEP is the same as that of the EPA and other pre-authentication based schemes such as the HOEA.

Ejaz Ahmed et al 2011 reduced the handoff delay by re-authentication which can be used only inside the same ASN. It derives AK from the previous one using hash function for intra-ASN handoff. This function can be used by man in the middle who knows the previous AK to derive the AK at any instant. More importance should be given to secure AK
since it plays a vital role in the key exchange process. Liming Hou & Kai (2009) proposed pre-authentication in WiFi and WiMAX Integrated system based on EAP-TLS authentication which divides pre-authentication phase and re-authentication phase. The pre-authentication stage is executed at the network entry and it remains valid for all the handoffs. When the MS roams from the coverage of a WiFi to a WiMAX BS or vice versa, then the re-authentication phase should be performed.

Al Shidhani & Leung (2010) proposes secured pre-authentication in the UMTS-WLAN interworking architectures. Although it reduces handoff delay with no compromise on security, it is limited by WLAN focused architecture which needs to be improved to apply in WiMAX. Yong Change et al (2004) introduced the concept of updating CID on handoff from one BS to another. Passport handover with the same CID between NBSs is proposed by Wenhua Jiao et al (2007) and Mohammed Awadh Ben-Mubarak et al (2009). The CID can be used in the initial process of handoff till the new CID is generated. The usage of same CID in SBS as well as TBS is possible by the restriction of fractional reuse of frequency by which NBS will not use the same frequency. Above mentioned review of research have directly or indirectly helped the development of proposed methodology of this chapter

6.4 PROPOSED METHODOLOGY

6.4.1 Pre – Authentication Certificate based Proposed Handoff

Existing WiMAX handoff spends its channel resources for authorization, authentication and key exchange and it also leads to handoff latency. The motive behind the pre-authentication technique is to authenticate the MS before the handoff, thus reducing the handoff latency by skipping the authentication phase during handoff (Thuy Ngoc Nguyen & Maode Ma 2012). This section proposes the secured time limited Pre-Authentication Certificate (PAC) based handoff. The proposed technique reduces handoff delay and also
defends from impersonation, MITM and replay attacks. The sequential flow of PAC based handoff is shown in Figure 6.3 and its implementation requires the following sub modules.

1. PAC Request & Response.

2. Distribution of PAC to MS and NBSs.

3. Handoff request & Response between MS and TBS.

![Diagram of PAC based Handoff](image)

**Figure 6.3 Proposed PAC based Handoff**

**PAC Request and Response:**

The proposed algorithm explains the process of PAC request and response to yield PAC from PAA function of ASN-GW. Pre-authentication can be initiated by the MS at its entry into the new ASN. PAC request/response should be forwarded between MS and PAA by the SBS.
<table>
<thead>
<tr>
<th>Terms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS-X.509</td>
<td>Mobile Station X.509 certificate</td>
</tr>
<tr>
<td>E_{UPAA}</td>
<td>Encrypted with PAA public key</td>
</tr>
<tr>
<td>E_{PAC}</td>
<td>Encrypted with PAC</td>
</tr>
<tr>
<td>N()</td>
<td>Nonce - a random string or number used only once</td>
</tr>
<tr>
<td>BS_i-X.509</td>
<td>Base Station <em>i</em> X.509 certificate</td>
</tr>
<tr>
<td>E_{UMS}</td>
<td>Encrypted with MS public key</td>
</tr>
<tr>
<td>E_{UBSi}</td>
<td>Encrypted with BS_i public key</td>
</tr>
<tr>
<td>PAA-X.509</td>
<td>Pre-Authentication Authority -X.509 certificate</td>
</tr>
<tr>
<td>HMAC()</td>
<td>Hash based MAC algorithm</td>
</tr>
<tr>
<td>MSPAC</td>
<td>Mobile Station Pre-Authentication Certificate</td>
</tr>
<tr>
<td>MSCET</td>
<td>Mobile Station Certificate Expiry Time</td>
</tr>
</tbody>
</table>

PAC request from MS consists of its X.509 certificate, previously used AK with SBS and it is encrypted using the public key of PAA. PAA on receiving this request, decrypts with its private key and validates the identity of MS with the hASN. If MS succeeds the verification, PAA prepares the response with PAC which is encrypted using the public key of MS as in Figure 6.4. PAA also sends the Certificate Expiry Time (CET) which fixes the lifetime of PAC. This avoids the long time usage of pre-authentication functionality which can be misused once attacked. After the acknowledgement of MS is completed, EAP authentication phase is carried over (Loutfi Nuaymi 2007).
//MS sends PAC Request/
M1=MSX.509 cert, AK, T1, N1(MS)
Msg1=E_{UPAA}(M1)
// PAA verification
/*PAA decrypts the request with its private key and Verifies
T (MS), N (MS), Validity of MS*/
//PAA sends PAC Response
if valid then
    M2=PAAX.509 cert∥T2∥ N1(PAA) ∥N1(MS) ∥ MSPAC ∥ CET
    (MS)
    Msg2=E_{UMS}(M2)
else
    Access denied
end
//MS sends ACK//
Msg3=E_{PAC}(N1 (PAA) ∥T3∥ N2(MS))
//EAP Authentication to generate MSK
//PAA sends MSK
Msg4 = E_{PAC}(MSK∥ N2(PAA) ∥T4)
//MS sends ACK for MSK
Msg5=HMAC(MSK∥N2(PAA)∥T5.64)

Figure 6.4 Algorithm for Pre-Authentication Request from MS to PAA

EAP involves symmetric cryptography and is based on the use of
EAP (RFC 5247) which is an authentication protocol for remote or local
network access. The mobile can be authenticated using a credential issued by
the operator or an X.509 digital certificate. Several EAP authentication
methods are supported by PKM v2, including EAP-TLS (X509 based
authentication), EAP-AKA (Authentication and Key Agreement), and EAP-
CHAPv2 (Microsoft Challenge Handshake Protocol). The output of EAP
exchange is 512-bit key, called the Master Session Key (MSK), which is the
root of key hierarchy. Thus the derived MSK is sent to MS by encrypting with
PAC. This phase demonstrates the secured generation of MSK and its
acknowledgement by sending the 64 bits HMAC of MSK. The above
mentioned message exchanges are processed along with nonces and
timestamps.
Distribution of PAC:

After generating MSPAC, PAA distributes them to NBSs of MS in a secured manner which is explained in Figure 6.5. Selection of potential NBSs to be the TBS of MS discussed in previous research works (Sayan Kumar Ray et al 2012) and (Ejaz Ahmed et al 2011) can also be used to efficiently utilize the bandwidth in message exchanges.

![Algorithm](algorithm.png)

**Figure 6.5 Algorithm for the Distribution of PAC to NBSs**

PAA sends the MSPAC along with the MAC address, CET and its digital certificate for mutual authentication. Above mentioned parameters are sent by encrypting with the public key of corresponding BS. The BS acknowledges PAA when the verification of the validity of PAA is a success otherwise access is denied. PAA in turn sends the encrypted MSK of the corresponding MS using the PAC. BS acknowledges the receipt of MSK by sending 64 bits HMAC of MSK. All the message exchanges include a timestamp and nonce to ensure the freshness of process and to protect from
security threats. When the task of pre-authentication is completed, the MSs possessing the PAC are treated as pre-authenticated MS and this allows the handoff process for these MS to skip the authentication phase within the ASN.

**Proposed Handoff with PAC:**

The proposed algorithm is explained in Figure 6.6. At the instant of handoff, MS sends the handoff request message to the TBSs through SBS. This message has the MS Validity with time limited PAC and this can be encrypted by neighbouring Base Station’s public key. The selected TBS decrypts the message and verifies the PAC with the PAC received from PAA. CET gives the expiry time of pre-authentication after which pre-authentication should not be allowed by TBSs.

```
Algorithm 6.3: PAC based handoff
// MS sends handover request message to BS //
for i=1 to n
    MS sends BSi, i=1,2,……n
    M1=MSX.509 cert, MSMAC, T(MS),N(MS), PAC(MS)
    Msg1=EUBSi (M1)
end
// BSi verification //
BSi verifies T(MS),N(MS), Validity of MS
if verified
    /* BSi sends handover response message accept or wait or reject to MS */
    M2=BSi-X.509 cert, BSI-MAC, N(BSi), T(BSi),
        N(MS), ACC/WAIT/REJ
    Msg2=EUMS(M2)
end
Connection established
```

*Figure 6.6 Algorithm for PAC based Handoff*

BS responds to MS by sending accept/wait as a response to MS when the verification of PAC is a success and also CET will not be expired. BS
rejects the request when the above condition is not satisfied. After the acceptance of PAC, both MS and BS start deriving other keys like PMK and AK mutually. Thus the proposed work overcomes the security issue in distributing MSK as well as generating other keys only during handoff so that the lifetime of the keys is not wasted.

6.4.2 RCID Based Passport Handoff

The chances of reducing the handoff delay of MS entering the BS for the first time is analyzed in this chapter. As the first step, secured pre-authentication is proposed. The proposed pre-authentication technique reduces intra-ASN and inter-ASN handoff delay by skipping the authentication phase MSs. In this section, a passport handover based on the Reserved CID (RCID) is proposed by which the CID generation phase during each handoff is saved and thus minimizes the handoff delay.

After successful completion of the authorization and key exchange phase, next phase to be processed is the registration phase which generates TCID as shown in Figure 6.7. The proposed RCID based passport handoff reserves the TCID after pre-authentication and uses for all handoffs. Passport handoff is about the same meaning as the passport by which anyone can be allowed to roam around the world. As handoff is the switching of MS from one BS to another BS, passport handoff is defined as the handoff which can be allowed by all BS of the ASN without any unwanted delay.

On successful selection of TBS by scanning process, request for ranging process is sent by MS to BS with the reserved CID instead of IRCID. BS sends the acknowledgement of usage of RCID after the verification of pre-authentication and its validity. If valid, BS starts the registration process of MS skipping the generation of BCID, PCID and mutual message exchanges
performed before registration. It is followed by the registration process. Figure 6.8 shows the sequential flow of the proposed method.

![Diagram](image.png)

**Figure 6.7 Proposed RCID based Passport Handoff**

MSs passes through many ASN on their mobility and the handoff from one ASN to another ASN is done with the help of SBS of one ASN from which the handoff initiated and the TBS of another ASN to which the handoff is intended. Initially when the MS enters into the ASN, it can request for RCID to ASN-GW through the TBS. The request is acknowledged after the verification of MS at ASN-GW and followed by the allocation of next available RCID.

![Diagram](image.png)

**Figure 6.8 RCID based passport handoff**
On receiving RCID, MS is now eligible to process handoff to any BS of that ASN bypassing the CID generation. Thus MS get the benefit of seamless mobility at all TBS on its move with the help of passport handoff. Since the scope of RCIDs is within the ASN, it cannot be used in handoffs between different ASNs. Because of this RCID is automatically released and surrendered to ASN-GW when the MS initiates a handoff from SBS of current ASN to TBS of another ASN. The proposed technique can be implemented sequentially in three phases:

1. Adaptive decision about number of RCID by ASN-GW
2. RCID Request and Response for RCID allocation
3. Passport handoff by MS

**Adaptive decision about number of RCID by ASN-GW:**

Analysis of RCID deals with finalizing the decision about the amount of RCID in an ASN of mobile WiMAX network. RCIDs are unique and are not allowed to be reused like CIDs. RCID once provided will be used for all handoffs between BSs of that particular ASN. Limited users selected on the basis of priority or ‘first come first served’ are allowed to utilize this facility. Remaining users have to follow the existing process of acquiring CID from each BS on their handoff. The maximum number of possible CIDs in a BS which is 64K is limited by the number of RCIDs. If the number of RCIDs is N, then the maximum number of CIDs of each BS will be only 64K - N. Increase in number of RCIDs increases the number of MS utilizing fast handoff but decreases the number of MS processed by BS at a particular time.

Analysis should be made on the basis of traffic rate, capacity of ASN and the time of call admission (peak hour or normal hour) to fix the allowed number of RCID in each ASN. It can be varied in such a way that the amount
of RCID enhances seamless handoff without being hurdle to admission of MS at each BS. Variation in the amount of RCID if any should be intimated to all BSs of that ASN.

![Algorithm 6.4: Decision of amount of RCIDs](image)

**Algorithm 6.4: Decision of amount of RCIDs**

- P\_RCID=Percentage of MS allowed to use RCID
- N\_BS= Number of BS in ASN
- TR\_i=Average Traffic rate of BS\_i
- N\_RCID= Number of RCIDs

\[\text{for } i=1 \text{ to } N\_BS\]
\[\text{TR\_AVG} = \frac{\sum_{i=1}^{N\_BS}TR\_i}{N\_BS}\]

\[\text{if } \text{TR\_AVG}>30,000\]
\[\text{P\_RCID}=0.1\]
\[\text{else if } \text{TR\_AVG}>20,000\]
\[\text{P\_RCID}=0.15\]
\[\text{else}\]
\[\text{P\_RCID}=0.2\]
\[\text{end}\]

\[\text{N\_RCID}=\text{P\_RCID}*\text{TR\_AVG}\]
\[\text{end}\]

Send N\_RCID to all BS of that ASN

**Figure 6.9 Algorithm for Decision of amount of RCIDs**

The proposed algorithm Figure 6.9 demonstrates the method of finalizing the number of RCID by computing average traffic rate (TR\_AVG) taking into account of all BS in an ASN. Depending on TR\_AVG, percentage of RCID is 1%, 1.5% and 2% respectively for high, medium and low traffic over a period of time (for each hour). This should be informed to all BS of that particular ASN through the interface R6.

**RCID Request and Response for RCID allocation:**

Any MS enters into the new ASN from the old ASN through the SBS of old ASN and TBS of new ASN. As shown in Figure 6.10, MS sends its request (RCID\_REQ\_MS) for RCID to ASN-GW through its initial TBS of
ASN. On receiving the request, RCID is allotted to the MS as per the algorithm shown in Figure 6.11. RCID should be released automatically to ASN-GW when MS exits to another ASN through last TBS. Such RCIDs can be allotted to other MS so that RCIDs are efficiently utilized.

![Figure 6.10 RCID Request and Response](image)

The Figure 6.11 depicts the way of allocating RCID when an MS enters the ASN. First the validity of the MS is verified and then allowed for getting RCID. A random RCID from the available RCID is provided in the range of starting RCID (RCID_st) and (RCID_end) excluding the already allotted RCIDs. This is done to avoid sequential allotment of RCID which can be easily detectable by security attacks. All RCIDs are represented in binary notation with a length of 16 bits and is linked to a SFID.

After allocating all available RCID, declaration of unavailability of RCID should be intimated to the incoming MS so that they can adapt the existing process. Allocation of RCID can be made as first come first serve basis in this proposed work. It can also be made on a priority basis (military, emergency and government sectors) which is out of scope of this research.
RCID_list=empty
while ASN_GW receives RCID_REQ from MS_i through TBS_i
   Verify validity of MS_i
   if verification succeeds
      if N_RCID-Length(RCID_list) $\neq$ 0
         RCID_st=Binary(FE9F-N_RCID,16)
         RCID_end=Binary(FE9F,16)
         RCID_MS_i=Random(RCID_st, RCID_end)-RCID_list
         Update RCID_list by adding RCID_MS_i
      else
         No RCID available
      end
   else
      Not a valid user
   end
end
while MS_i exits ASN
   Update RCID_list by adding RCID_MS_i
end

Figure 6.11 Algorithm for Allocation of RCID

Passport handoff by MS:

After receiving RCID from ASN-GW through the TBS by which MS entered into the ASN, MS is now eligible to request for passport handoff. ASN-GW distributes the value representing the maximum number of possible RCIDs and Pre-Authentication Certificate (PAC) of MSs who have completed their pre-authentication to all the BSs within the ASN.
BS receives N_RCID and PAC_list from ASN_GW
RCID_st=Binary (FE9F-N_RCID, 16)
RCID_end=Binary (FE9F, 16)
MS sends RNG_REQ with RCID and MS_PAC
if RCID > RCID_st AND RCID ≤ RCID_end
   if MS_PAC ∈ PAC_list
      Accept Passport Handoff
      Start MS Registration
   else
      Reject passport handoff
      Start Existing Handoff
   end
else
   Invalid RCID
   Reject passport handoff
   Start Existing Handoff
end

**Figure 6.12 Algorithm for Passport Handoff**

When MS sends the passport handoff request, it should also include RCID and PAC. If it finds a match with the available RCIDs and PAC, then passport handoff can be allowed which leads to seamless handoff by skipping CID generation at each BS as illustrated in Figure 6.12. Similarly MS initiates the handoff from SBS$_i$ to TBS$_i$ within the particular ASN. TBS which is requested for handoff is processed with the same specification throughout the ASN. Messages like RNG_RSP, MS registration which needs to generate CID can use the RCID already allotted by ASN-GW. Since the scope of RCID is within the ASN, TBS strictly allocates CID other than RCID to the remaining MS which sends the handoff request without RCID.
6.5 RESULTS AND DISCUSSION

The proposed PAC based handoff and RCID based passport handoff decreases the handoff latency and enhances the seamless connectivity without compromising security. This section describes the simulation results of the proposed work implemented in MATLAB Release 2010 with GUIDE.

6.5.1 PAC Based Handoff

PAC Request and Response:

The mobile WiMAX network is simulated with 5 BSs, MS and PAA. Initially MS is connected with the SBS as shown in Figure 6.13. MS initiates the PAC Request to PAA before handoff with TBS of the same network. Parameters of Message exchange as per are shown in the listbox. Actual message exchange is passed only through SBS which it is shown between MS and PAA to depict that MS is initiating.

![Figure 6.13 Pre-Authentication Request](image-url)
Figure 6.14 PAC Request and Response

The detailed message exchange between MS and PAA is shown in Figure 6.14 with the request and response in encrypted format. PAC and CET derived from the encrypted response are shown separately. This is accomplished only when the MS is valid. After getting the acknowledgement from MS for the receipt of PAC, EAP authentication to generate MSK is completed. PAA sends the response encrypted by PAC as the shared key. MS derives MSK from the response is shown separately. In turn MS acknowledges the receipt of MSK HMAC digital signature. GUI representation of the pre-authentication response is shown in Figure 6.15 with the parameters exchanged are shown in the listbox on the right side. All the transactions between MS and PAA are sent along with a timestamp and nonce to ensure its freshness to avoid MITM and replay attacks.
Figure 6.15 Pre-Authentication Response

Distribution of PAC

Figure 6.16 PAC Distribution to BS
After the successful completion of PAC request and response, now the MS is eligible to request for PAC based handoff. Thus, the authentication process and the generation of MSK can be skipped for such MS which leads to reduction in handoff delay. The information about pre-authenticated MS should be intimated by PAA to the potential BSs which can act as TBS during the handoff process. The implementation of secured message exchanges involving the distribution of PAC to BS and the acknowledgement from the corresponding BS is shown in Figure 6.16.

PAA encrypts the details of pre-authenticated MS and sends to authorized BSs. Since the certificate details is encrypted by the public key of corresponding BS, it can be decrypted only by the authorized BS with its private key. BS then can derive PAC and CET of the MS from the certificated details and sends the encrypted acknowledgement using the public key of PAA. Receipt of this acknowledgement from BS initiates PAA to send the MSK encrypted with PAC. BS derives MSK and acknowledges by sending 64 bits of HMAC of MSK.

**Handover Process:**

PAA thus successfully completes the PAC & MSK generation for the requested MS and the distribution of the same to BSs. At the time of handoff, MS sends its handoff request along with its PAC to potential TBSs. The GUI implementation of handoff request is shown in Figure 6.17. The request shown is initiated from MS to indicate the MS but the actual handoff request is forwarded only through SBS.
This request is encrypted with the public key of corresponding BS and can be decrypted only by the valid BS possessing the private key. The parameters involved in the message exchange are shown in Figure 6.18 and the processing is done. BS checks the validity of the MS and verifies whether the request is initiated before the expiry of PAC using CET. When these validation result is true, then it responds with the indication of accept or wait along with nonce and timestamp.

The existing handoff process is started except for the authentication process and MSK generation is skipped. GUI implementation of Handoff response with the status of the TBS who received the PAC based handoff request from MS. GUI window depicts that one BS accepts the request and the other expects the MS to wait. If the validation fails, then the MS is not allowed for PAC based handoff. It can be allowed for existing handoff when the MS is valid and the connection is terminated when the user found to be invalid. The parameters involved in the handover are listed in the right side listbox.
The decision of allowing PAC based handoff purely depends on the current status of the BS with respect to its capacity, number of MS currently
served and the MS arrival rate. This analysis is not in the scope of this
research. The GUI implementation of occurrence of handoff with the TBS
which sends the 'accept response is shown in Figure 6.19.

![Figure 2: Pre Authentication](image)

**Figure 6.20 Handover Process**

Simulation results plotted in Figure 6.20 shows the contribution of
the automated proposed PAC based handoff technique. It saves 79.5% without
CET limit and 69.25% of the authentication cost with CET limit compared
with the existing authentication process. In spite of limitation obligatory by
CET, it is suitable to have CET to avoid users enjoying the benefit of pre
authentication all the time. It also avoids security threats like MITM attack and
Replay attack. Pre-Authentication without CET limit can be provided to
exceptional cases like military and emergency medical services.

### 6.5.2 Proposed RCID based Passport Handoff

This section discusses the results of Reserved CID (RCID) based
passport handoff which reduces the handoff delay by saving the time taken for
generating the CIDs. This can be accomplished for the MSs who have already
received their PAC in their pre-authentication process. This is to ensure the secured handoff with RCIDs. Hence the proposed RCID based passport handoff is not an independent process and it relies on the usage of PAC to avoid security threats.

**CID Generation by ASN:**

![CID Generation by ASN](image)

**Figure 6.21 Successful Generation of RCID by ASN**

The first phase in the RCID based passport handoff is the generation of RCID for the MS. The MS is required to send the request for RCID to ASN through SBS. The authority of the MS and validity of PAC &CET is checked and if satisfied RCID is generated. ASN can reject the request for any dispute in satisfying the conditions. RCID is generated for the MS and its GUI implementation is shown in Figure 6.21, 6.22 and 6.23. GUI implementations show the derived results from the encrypted request. Encryption is processed similar to that of pre-authentication request and response. The number of base stations is also shown which plays a vital role in calculating number of RCIDs.

The ASN possesses the details of CET and PAC in a database for all the MS who are pre-authenticated. Once the request for RCID generation is
received by ASN, PAC and CET will be matched with the existing record in
the database for the corresponding MS. Figure 6.22 shows the successful
RCID generations when a match found for PAC & CET and also checks
whether the lifetime of CET still exists. Figure 6.23 shows the denial of RCID
generation by ASN because of the invalid PAC due to mismatch with the
records in the database for the respective MS. Figure 6.24 shows the denial of
RCID generation due to the expiry of CET even when the PAC is valid.

![Figure 6.22 Denial of RCID generation due to Invalid PAC](image1.png)

![Figure 6.23 Denial of RCID generation due to the expiry of CET](image2.png)

Figure 6.22 Denial of RCID generation due to Invalid PAC

Figure 6.23 Denial of RCID generation due to the expiry of CET

After successfully received the RCID from ASN, MS is now eligible
to undergo passport handoff with the same RCID in all BSs. MS sends its
RCID and Authorization Key (AK) along with handoff request. RCID and AK show the completion of both RCID generation and authentication of the MS. As the processing of request for RCID generation is done after the PAC generation of MS, request for passport handoff should also be processed after the successful authentication phase of MS. This request is sent to Target BS with whom the handoff is processed.

![Figure 6.24 Successful Consent for Passport handoff](image)

**Figure 6.24 Successful Consent for Passport handoff**

On receiving the request from MS through SBS for Passport handoff, TBS initially checks the validity of MS using its digital certificate and AK. This is followed by the matching of RCID with that of the list of RCID received from ASN. If match found, MS is allowed for passport handoff which straight away goes to registration phase. Thus the time taken for handoff is reduced when compared to the existing handoff. A successful handoff is shown in Figure 6.25 which is allowed after verifying the details of incoming MS possessing RCID. Figure 6.26 shows the denial of passport handoff for the MS because of the mismatch of RCID. Decision about number of RCIDS allowed should be adapted depending on the status of the network.
Figure 6.25 Denial of Passport handoff

Figure 6.26 Authentication cost with respect to number of RCIDs

Performance analysis of the authentication cost of both existing and proposed techniques with increasing number of handoffs is plotted in Figure 6.27. From the given analysis it is proved that percentage of RCIDs reduces the handoff delay to certain extent. These results are taken by maintaining the number of handoffs as 200 and increasing the number of RCID from 0 to 2.5% of MSs in a base station. Random mobility is provided to MSs and tracked within an ASN. Increasing RCIDs above 2% does not have any impact on performance and it also wastes the resources of the BS if the
MS does not enter into the corresponding BS. Thus, allocating more RCIDs needs an analysis about the network so that it will not be a burden to the BSs. It is concluded that the percentage of RCIDs can be varied from 1% to 2%.

![Graph showing authentication cost with respect to handoff](image)

**Figure 6.27 Authentication cost with respect to handoff**

<table>
<thead>
<tr>
<th>S. No</th>
<th>Existing handoff (X10^4 secs)</th>
<th>Passport handoff (X10^4 secs)</th>
<th>Handoff Delay Reduction in %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>3.61</td>
<td>2.64</td>
<td>26.74</td>
</tr>
<tr>
<td>2.</td>
<td>3.23</td>
<td>2.38</td>
<td>26.27</td>
</tr>
<tr>
<td>3.</td>
<td>3.49</td>
<td>2.55</td>
<td>26.83</td>
</tr>
<tr>
<td>4.</td>
<td>3.28</td>
<td>2.41</td>
<td>26.38</td>
</tr>
<tr>
<td>5.</td>
<td>2.79</td>
<td>2.04</td>
<td>26.88</td>
</tr>
<tr>
<td>6.</td>
<td>2.97</td>
<td>2.21</td>
<td>25.43</td>
</tr>
<tr>
<td>7.</td>
<td>3.30</td>
<td>2.54</td>
<td>23.04</td>
</tr>
<tr>
<td>8.</td>
<td>2.87</td>
<td>2.11</td>
<td>26.32</td>
</tr>
<tr>
<td>9.</td>
<td>2.96</td>
<td>2.24</td>
<td>24.13</td>
</tr>
<tr>
<td>10.</td>
<td>3.23</td>
<td>2.44</td>
<td>24.44</td>
</tr>
</tbody>
</table>

**Table 6.3 ASN Handoff Delay Reduction for 10 simulations**

*Average 25.65*
Performance analysis is also made by fixing the RCIDs and varying the number of handoffs as shown in Figure 6.28. RCIDs are fixed as 1.5% of average of MSs served by a BS at a particular time and the number of handoffs is varied from 50 to 300. A random mobility model of MSs is simulated with RCIDs fixed as per the proposed algorithm and the results of proposed passport handoff for 10 different simulations are listed in Table 6.3 and plotted in Figure 6.28.

![Figure 6.28 Performance analysis of RCID based Passport handoff](image)

**Figure 6.28 Performance analysis of RCID based Passport handoff**

### 6.6 CONCLUSION

The main objective of this research work is to establish a secured seamless Mobile WiMAX network. Handover is inevitable in mobile WiMAX and it is delayed by authentication and CID generation which cannot be avoided because of its role in protection of network from security threats. The main contributions of this chapter are as follows:

- A Certificate based Pre-Authentication followed by handoff technique which assures the MS as authenticated before the handoff and thus saves the time for authentication upto 69.25% during the time of handoff.
- A RCID based passport handoff is also proposed which follows the pre-authentication. The MS gets allocated with RCID from ASN-GW in their initial entry to the ASN and thus travels throughout the network with the same RCID saving 25.65% of time for CID generation in each BS.

Future enhancement of this proposed work can be concentrated towards the implementation of these techniques in an integrated platform for handoff between other technologies like WiFi & UMTS and WiMAX. Implementation of these proposed techniques in Inter ASN handoff can be analysed.