Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Minimization of Handoff interruption time skipping Reauthorization procedure**
Date Submitted	**2004-05-17**
Source(s)	Dongkie Lee, DongIl Moon, DongRyul Lee, JongKuk Ahn, Sungho Ha SK Telecom 15F, Seoul Finance Center, 84, Taepyungpro 1 ga, Chung-gu, Seoul, 100-768, Korea Voice: +82-2-6323-3147 Fax: +82-2-6323-4493 [mailto: {galahad,dimoon,drlee,jgahn,ss23}@sktelecom.com]
Re:	Response to IEEE 802.16-04/19 (Recirculation Ballot #14a Announcement)
Abstract	To minimize the handoff interruption time, short-hand authentication procedure is suggested which doesn't use normal re-authorization procedure. Sending Ranging-Request message with HMAC Tuple attached, SS can be authenticated by the BS implicitly without the full reauthorization procedure. In order to do this short-hand authentication, security context shall be transferred from serving BS to target BS.
Purpose	Discuss and Adopt as the enhanced handoff authentication procedure
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Minimization of Handoff interruption time skipping Reauthorization procedure

Dongkie Lee, DongRyul Lee, DongIl Moon, JongKuk Ahn
SK Telecom

1. Problem Statements

Current IEEE 802.16e/D2 specify reauthorization procedure after handoff. Considering the fact that asymmetric encryption like RSA is computationally complex and therefore CPU-intensive, generating AK and encrypting it using the X.509 certificate of SS adds additional overload to the target BS. Additionally, there is no doubt about the security concerns about the HMAC Tuple of Key Request/Reply messages. Replacing reauthorization procedure with the short-hand authorization procedure will reduce unnecessary authorizations from SS-BS and will reduce latency due to handoff.

2. Overview of Proposed Solutions

Firstly, security context from serving BS to target BS should be transferred which is piggybacked on HO-pre-notification backbone message.

Table 1 Security Context Information

Type	Content
AK Related	Older/Newer {AK, Remaining lifetime, Key Sequence Number}
TEK Related	Older/Newer {TEK Parameters(TEK, Remaining Key-Lifetime, Key-Sequence-Number, CBC-IV), SAID} per SAID

Table 2 Session Context Information

Type	Content
CID	Basic/Primary Management/Secondary Management CID, Transport Ids, Service Flow IDs
etc	IP Address, NAI(Network Address Identifier), MAC Address

Secondly, current re-authorization procedure which is supposed to be performed just after handoff is not performed. By sending Ranging Request with HMAC Tuple instead of re-authorization procedure after handoff, MSS is implicitly authorized by BS. HMAC Tuple, which is calculated with the AK issued by serving BS, is added to the Ranging Request for MSS which undergoes handoff. The rational behind this is during the stay in Serving BS, HMAC Tuple is good enough to verify the validity of the MSS when MSS sends Key Request/Reply/Reject/TEK Invalid and the other messages listed in Table 1 of P80216-REVd_D4. And HMAC-Digest's authentication key is derived from the Authorization Key, which is transferred with the other security context information from serving BS to target BS according to the first step. If the target BS had not previously received security context from Serving BS over the backbone, target BS may request SS to perform full reauthorization using the indicator in Ranging Response message.

Table 3 HMAC Tuple Definition(P80216-REVd_D4)

Type	Length	Value	Scope
27	21		DSx-REQ, DSx-RSP, DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-CMD, TFTP-CPLT

3. Proposed Changes to IEEE 802.16e/

6.3.2.3.8 Registration Rosponse(REG-RSP) message

Unless otherwise indicated in this section, MSS mobile network entry/re-entry is processed according to 6.4.9. For purposes of this process, MSS network re-entry and hand-over are synonymous.

For mobile networks, Target BS may include CID_update TLVs and SAID_update TLVs in the REG-RSP for MSS recognized by the Target BS as performing HO or network re-entry by the presence of a Serving BS ID in the RNG-REQ.

CID_update - The CID_update is a compound TLV value that provides a shorthand method for renewing active connections used by the MSS in its previous Serving BS. The TLVs specify CID in the Target BS that shall replace active CID used in the previous Serving BS. Multiple iterations of these TLVs may occur in the REG-RSP suitable to re-creating and re-assigning all active Service Flows for the MSS from its previous Serving BS including Basic, Primary and Secondary CIDs. If any of the Service Flow parameters change, then those Service Flow parameters and CS parameter encoding TLVs that have changed will be added. Only active Service Flows are transferred in this manner.

These TLVs enable the Target BS to renew connections used in the previous Serving BS, but with different QoS settings.

SAID_update - The SAID_update is a compound TLV value that provides a shorthand method for renewing active SAs used by the MSS in its previous Serving BS. The TLVs specify SAID in the Target BS that shall replace active SAID used in the previous Serving BS. Multiple iterations of these TLVs may occur in the REG-RSP suitable to re-creating and re-assigning all active Security Associations for the MSS from its previous Serving BS including Primary, Dynamic and Static SAIDs. If any of the Security Associations parameters change, then those Security Associations parameters encoding TLVs that have changed will be added.

6.3.20.4 Network entry/re-entry

Unless otherwise indicated in this section, MSS mobile network entry/re-entry is processed according to 6.4.9. For purposes of this process, MSS network re-entry and hand-over are synonymous.

MSS and Target BS shall conduct Ranging per 6.4.9.5 to begin network entry/re-entry except as MSS may take advantage of a non-contention based MSS Initial Ranging opportunity if present. If MSS RNG-REQ includes an Serving BS ID and Target BS had not previously received MSS information over the backbone (see section Backbone network HO procedures), then Target BS may make an MSS information request of Serving BS over the backbone network and Serving BS may respond. Regardless of having received MSS
information from Serving BS, Target BS may request MSS information from another network management
entity via the backbone network. Network re-entry proceeds per 6.4.9.5 except as may be shortened by Target
BS possession of MSS information obtained from Serving BS over the backbone network.

If MSS RNG-REQ included an Serving BS ID, HMAC-Digest and Target BS had previously received an backbone message (see section Backbone network HO procedures) containing MSS information and security context information, Target BS shall skip

~~use the embedded TLV PKM-REQ information and~~ the re-authorization process as defined in 7.2 and authenticates MSS using HMAC-Digest which is calculated with the AK of the serving BS. But Target BS may request MSS to re-authorize setting Authorization Required field in RNG-RSP.

If Target BS had previously received an backbone message (see section Backbone network HO procedures), Target BS may use the embedded TLV REG-REQ & DSA-REQ information to build and send an unsolicited REG-RSP message. The REG-RSP message may include New_CID, Old_CID, New_SAID, Old_SAID, and Connection_Info TLVs. If the post-handoff shortcut HMAC authorization is performed and full reauthorization is skipped, SAID's shall be updated by SAID_update contained in REG-RSP. Target BS may ignore only the first REG-REQ message received if it sends an unsolicited REG_RSP message. MSS is not required to send an REG-REQ if it receives an unsolicited REG-RSP prior to MSS attempt to send REG-REQ.

If MSS RNG-REQ included an Serving BS ID, MSS and Target BS may skip Time of day process.

If MSS RNG-REQ included an Serving BS ID, MSS may skip the MSS configuration file download procedure.

If MSS received a REG-RSP message that included New_CID, Old_CID, and Connection_Info TLVs, MSS and Target BS may skip the establish connections procedure.

Network entry/re-entry process completes with establishment of MSS Normal Operations.

Figure 141j shows the SDL of an MSS initiating handoff with the BS.

[Change the following as shown below:]

6.3.2.3.5 Ranging Request (RNG_REQ) message

The following parameters shall be included in the RNG-REQ message when the MSS is attempting to perform re-entry, association or hand-over:

Serving BS ID
The BS ID of the BS to which the MSS is currently connected (has completed the registration cycle and is in Normal Operation). Serving BS ID shall not be included if interval timer is timed-out (Serving BS ID AGINGTIMER, see Table 264a). Inclusion of Serving BS ID in the RNG-REQ message signals to the Target BS that the MSS is currently connected to the network through the serving BS and is performing association or is in the process of either hand-over or network re-entry.

HMAC Tuple
The HMAC Tuple is calculated with HMAC_KEY_S derived from AK issued by serving BS. Inclusion of the keyed digest allows the target BS to implicitly authenticate MSS and allows skipping authorization just after handoff. The HMAC Tuple attribute shall be the final attribute in the message's attribute list.

6.3.2.3.6 Ranging Response (RNG-RSP) message

[Add the following to section 6.4.2.4.6:]
When a BS sends a RNG-RSP message in response to a RNG-REQ message containing Serving BS ID, the BS may include the following TLV parameter in the RNG-RSP message:

Service Level Prediction — This value indicates the level of service the MSS can expect from this BS. The following encodings apply:

0 = No service possible for this MSS.
1 = Some service is available for one or several Service Flow authorized for the MSS.
2 = For each authorized Service Flow, a MAC connection can be established with QoS specified by the

AuthorizedQoSParamSet.
3 = No service level prediction available.

Service Level prediction may be accompanied by a number of Service Flow Encodings as specified in 11.4.913 sufficient to uniquely identify the AuthorizedQoSParamSet associated with the predicting SLP. If Service Flow Encodings are included, then the SLP response is specific to the presented AuthorizedQoSParamSet defined by the associated encodings. Included Service Flow Encodings are restricted to the following parameters only:

— Global Service Class Name
— Service Flow QoS parameter set encodings as defined in 11.13 such that the combination of Global Service Class Name and any Service Flow modifying parameters fully defines an AuthorizedQoSParamSet profile being assessed
— Service Flow Identifier

If individual AuthorizedQoSParamSet profiles are provided for multiple Service Level Predictions, then each Service Level Prediction is specific to its associated AuthorizedQoSParamSet profile and shall include only response options ‘0’ or ‘2’.

Authorization Required
This indicates whether the authorization is required or not. If the target BS did not receive security context information from serving BS, HMAC-Digest validation fails, or operator’s policy mandates, authorization is required.

11.5 RNG-REQ message encodings

[Add the following rows to table 318:]

Table 318a-RNG-REQ Message Encodings

Name	Type(1 byte)	Length	Value
Serving BS ID	4	6	The unique identifier of the former Serving BS
Basic CID	6	2	Basic CID allocated from the formar Serving BS
HMAC-Digest	7	20	Keyed SHA message digest

11.5 RNG-RSP TLV for re-establishment of Service Flows

[Add the following rows to table 320:]

Table 318a-RNG-RSP Message Encodings

Name	Type(1 byte)	Length	Value
QoS Parameters	[145/146].Variable	Variable	Compound TLV incorporating one or more 11.13 QoS Paramater Set definition encodings
SFID	[145/146].1	4	
Resource Retain Flag	20		This value indicates whether the former Serving BS retains the connection information of the MSS. 0 = the connection information for the MSS is deleted 1 = the connection information fo the MSS is r
Authorization Required	21	1	This indicates whether the authorization is required or not 0 = authorization not required 1 = authorization required

11.7 REG-REQ/RSP management message encodings

[Add the following rows to the end of 11.7.10.1:]

11.7.11 SAID update encodings

This field provides a translation table that allows an MSS to update its security associations so that it may continue security service after a hand-over to a new serving BS.

Name	Type (1 byte)	Length (1 byte)	Value (Variable length)
SAID_update	20	variable	Compound

The following TLV values shall appear in each SAID_update TLV.

Name	Type (1 byte)	Length (1 byte)	Value (Variable length)
New_SAID	20.1	2	New SAID after hand-over to new BS
Old_SAID	20.2	2	Old SAID before hand-over from Old BS

D.2.5 HO-pre-notification message

This message is sent by a BS to advertise an MSS intention to perform HO. The message is typically sent to neighbor BS referenced in the MOB-BSHO-REQ or MOB-MSSHO-REQ message. The message serves to query the Target BS whether it can serve the HO requesting MSS. The message contains the following information:

Table D6—HO-pre-notification Message

Field	Size	Notes
Global Header	152-bit	
For (j=0; j<Num Records; j++) {		
MSS unique identifier	48-bit	48-bit unique identifier used by MSS (as provided by the MSS or by the *I-am-host-of* message)
Estimated Time to HO	16-bit	In milliseconds, relative to the time stamp. A value of 0 indicates that the estimated time is unknown.
Required BW	8-bit	Bandwith which is required by MSS (to gurarantee minimum packet data transmission)
For (i=0; i<Num_SFID_Records; i++) {		
SFID	32-bit	
For (i=0; i<Num_QoS_Records; i++) {	Variable	
Required QoS		11.13 QoS Parameter definition encodings that in combination define an AdmittedQoSParamSet specific to the SFID
}		
}		
N_SAIE		**Number of Security Association Information Elements**
For(k=0;k<N_SAIE;k++){		
Field Size	**16-bit**	**Size, in bytes, of TLV encoded information field below**
TLV encoded information	**Variable**	**TLV information as allowed on a PKM-xxx MAC messages**
}		
Old AK Remaining key Lifetime		

__Old AK Key Sequence Number		
__New AK		
__New AK Remaining key Lifetime		
__New AK Key Sequence Number		
__N_SAIE		**Number of Security Association Information Elements**
__For(k=0;k<N_SAIE;k++){		
____Old AK		
____Old TEK Remaining key Lifetime		
____Old TEK Key Sequence Number		
____Old TEK CBC Init Vector		
____NEW TEK		
____New TEK Remaining key Lifetime		
____New TEK Key Sequence Number		
____New TEK CBC Init Vector		
__}		
}		
Security field		A means to authenticate this message