Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Authentication Tuples in Mobility Management Messages**
Date Submitted	**2005-03-10**
Source(s)	Jaesun Cha, Sungcheol Chang , and Chulsik Yoon jscha@etri.re.kr ETRI 161, Gajeong-dong,Yuseong-Gu, Daejeon, 305-350, Korea
Re:	Contribution on comments to IEEE P802.16e/D6
Abstract	In this contribution, we propose to clarify the use of authentication tuples in mobility management messages.
Purpose	Adoption
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 text 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 (Version 1.0) <http://ieee802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing 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:r.b.marks@ieee.org> as early as possible, in written or electronic form, of any patents (granted or under application) that may cover technology that is under consideration by or has been approved by IEEE 802.16. The Chair will disclose this notification via the IEEE 802.16 web site <http://ieee802.org/16/ipr/patents/notices>.

Authentication Tuples in Mobility Management Messages

Jaesun Cha, Sungcheol Chang, and Chulsik Yoon

ETRI

1. Problem Statement

The purpose of this contribution is to clarify the use of authentication tuples in mobility management messages because there are several problems in the current 802.16e/D6

- HMAC tuple is used as a TLV in MOB_SLP-RSP, while it is used as a fixed parameter in the other mobility management messages. There is no consistency of using HMAC tuple.
- In case OMAC or short-HMAC tuple is negotiated to be supported by MS and BS, then HMAC tuple is appeared with OMAC or short-HMAC tuple in the same message because HMAC tuple is used as a fixed parameter and the other is used as a TLV in the mobility management messages. That means one of them is a redundant parameter.
- The field declared for HMAC tuple may be used for OMAC or short-HMAC tuple to solve the above redundant problem. However, it may induce an error when MS or BS decodes messages. For example, if the first byte of any authentication tuple has the same value as the type of Resource Retain Time TLV, then the authentication tuple may be decoded as Resource Retain Time TLV because MS or BS doesn't know the total length of the TLV encoded information.

In order to solve the aforementioned problems, we proposed to use authentication tuples as TLVs.

2. Proposed Text Changes

[*Modify the contents of Table 108c as indicated:*]

Table 108c-Sleep-Request (MOB_SLP-REQ) message format

Syntax	Size	Notes
}		
~~HMAC Tuple~~	~~21 bytes~~	
TLV encoded information	*variable*	
}		

[*Delete the description of HAMC Tuple and add a new paragraph in section 6.3.2.3.44*]

CID

CIDs of unicast connections comprising the Power Saving Class. CID = 0 denotes set of all management connections associated with the MS

~~HMAC Tuple (see 11.1.2)~~
~~The HMAC Tuple shall be the last item in the message.~~

The MOB_SLP-REQ shall include the following parameters encoded as TLV tuples:

HMAC Tuple (see 11.1.2)

[*Modify section 6.3.2.3.48 as follows*]

6.3.2.3.48 Scanning Interval Allocation Request (MOB_SCN-REQ) message
A MOB_SCN-REQ message may be transmitted by an MS to request a scanning for the purpose of seeking available and determining their suitability as targets for HO. An MS may request the scanning allocation to perform scanning with Scan type = 0, or non-contention Association ranging with Scan type =1.

An MS shall generate MOB_SCN-REQ messages in the format shown in Table 108j:

Table 108j-MOB_SCN-REQ message format

Syntax	Size	Notes
MOB_SCN-REQ_Message_Format() {		
Management Message Type = 54	8 bits	
Scan duration	8 bits	Units are frames.
If (Scan duration =!= 0) {		
~~HMAC Tuple~~	~~21 bytes~~	
~~} else {~~		
Scan Type	1 bit	0: Scanning 1: Association
Reserved	3 bits	Shall be set to zero
Interleaving interval	8 bits	Units are frames.
For (j=0;j<N_Recommended_BS_Scanning;j++) {		N_Recommended_BS can be derived from the known length of the MAC message
Recommended BS ID Scanning	48 bits	
}		
If (Scan type == 1) {		
N_Recommeded BS_Association	4 bits	
For (j=0;j<N_Recommended_BS_Association;j++) {		
Recommended BS ID Association	48 bits	
}		
}		
~~HMAC Tuple~~	~~21 bytes~~	~~See 11.1.2.~~
}		
TLV encoded information	*variable*	
}		

The following parameters shall be included in the MOB_SCN-REQ message,

Scan duration
Duration (in units of frames) of the requested scanning period. If the BS sets this field to zero to disapprove the MSS' scan or association request, all other parameters except ~~HMAC Tuple~~TLV encoded information shall be omitted in the message.

Scan type
Signals presence of information on BSs with which MS intends to perform Association.
~~HMAC Tuple (see 11.1.2.)~~
~~The HMAC Tuple Attribute contains a keyed message digest (to guarantee the origin and integrity of the message)~~
Interleaving Interval
The period of MS's Normal Operation which is interleaved between Scanning Durations.
N_Recommended_BS_Setting
Number of BSs which the MSS plans to scan only
Recommended BS ID Scanning
BS IDs of those BSs the MSS plans to scan
N_Recommended_BS_Association
Number of BSs which the MSS plans to scan and try association
Recommended BS ID Association
BS IDs of those BSs the MSS plans to scan and try association This field may be included only if an MS has a candidate available BS. It means that MSS calls Serving BS for assistance to make appointment with the Recommended BS for noncontention based ranging opportunity to perform association.

The MOB_SCN-REQ message shall include the following parameters encoded as TLV tuples:
HMAC Tuple (See 11.1.2.)

[*Modify section 6.3.2.3.49 as follows*]

6.3.2.3.49 Scanning Interval Allocation Response (MOB_SCN-RSP) message
A MON_SCN-RSP message shall be transmitted by the MS either unsolicited or in response to an MOB_SCN-REQ message sent by an MS. A BS may request the scanning allocation for MS scanning with Scan type = 0, or MS non-contention Association ranging with Scan type = 1. The message shall be transmitted on the Basic CID.

The format of the MOB_SCN-RSP message is depicted in Table 108k.

Table 108k-MOB_SCN-RSP message format

Syntax	Size	Notes
MOB_SCN-RSP_Message_Format() {		
Management Message Type = 55	8 bits	
Scan duration	8 bits	Units are frames.
If (Scan duration =!= 0) {		
~~HMAC Tuple~~	~~21 bytes~~	
~~} else {~~		
Start frame	4 bits	
Scan_type	1 bit	0: Scanning 1: Association
Reserved	7 bits	Shall be set to zero
Interleaving interval	8 bits	Units are frames.
Scan iteration	8 bits	
Report mode	2 bits	0b00: no report ob01: periodic report 0b10: event triggered report 0b11: reserved

Scan report period	8 bits	Available when the value of Scan Report is set to 0b01. Scan report period in frames.
reserved	2 bits	Shall be set to zero.
N_Recommended_BS_String	4 bits	
For (j=0;j<N_Recommended_BS_Scanning;j++) {		N_Recommended_BS can be derived from the known length of the MAC message
Recommended BS ID Scanning	48 bits	
}		
If (Scan type == 1) {		
N_Recommeded BS_Association	4 bits	
For (j=0;j<N_Recommended_BS_Association;j++) {		
Recommended BS ID Association	48 bits	
Rendevouz_time	16 bits	
}		
~~HMAC Tuple~~	~~21 bytes~~	~~See 11.1.2.~~
}		
}		
TLV encoded information	variable	
}		

The following parameters shall be included in the MOB_SCN-RSP message:

Scan duration
Duration (in units of frames) where the MS may perform scanning or association for Available BS. If the BS sets this field to zero to disapprove the MSS' request, all other parameters except ~~HMAC Tuple~~TLV encoded information shall be omitted in the message.

Start Frame
Measured from the frame in which this message was received. A value of zero means that first Scanning Interval starts in the next frame.

Scan type
Signals presence of information on BSs with which Serving BS recommends to perform Association.

Interleaving interal
The period interleaved between Scanning Intervals when MS shall perform Normal Operation.

Scan Iteration
The number of iterating scanning interval

Report mode
Action code for an MS's report of CINR measurement:
00: The MS measure channel quality of the Available BSs without reporting.
01: The MS reports the result of the measurement to Serving BS periodically. The period of reporting is different from that of scanning.
10: The MS reports the result of the measurement to Serving BS after each measurement.
11: *reserved*

Scan report period
The period of MS's report of CINR measurement when the MS is required to report the value periodically.

N_Recommended_BS_Scanning
Number of BSs which the BS recommends to scan only
Recommended BS ID Scanning
BS IDs of those BSs the BS recommends to scan

If Scan type is set to '1', the follwing parameters shall be included in the MOB_SCN-R~~EQ~~SP message:
N_Recommended_BS_Association
Number of BSs which the MSS plans to scan and try association
Recommended BS ID Association
Recommended BS ID list of Association. Serving BS may request, over the backbone, from Recommended BS allocation of non-contention based ranging opportunity for MS Association activity. When conducting initial ranging to Recommended BS, MS shall use allocated non-contention based ranging opportunity, if available.
Rendezvous time
This is offset, measured in units of frame duration (of Serving BS), when the corresponding Recommended BS is expected to provide non-contention based ranging opportunity for the MSS. The offset is calculated from the frame where MON_SCN-REQ message transmitted. In case Scan type = 0, the parameter is not applicable and shall be encoded as 0. The recommended BS is expected to provide non-contention based Ranging opportunity within 5 frames interval starting from the fram specified by Rendezvous time parameter.

The MOB_SCN-REQ message shall include the following parameters encoded as TLV tuples:
HMAC Tuple (See 11.1.2.)

[Modify the contents of *Table 108m as indicated:*]

Table 108m-MOB_BSHO-REQ message format

Syntax	Size	Notes
Action time	8 bits	
padding	variable	Padding bits to ensure byte aligned
~~HMAC Tuple~~	~~21 bytes~~	~~See 11.1.2~~
TLV encoded information	variable	
}		

[*Delete the description of HAMC Tuple on page*]

Action Time
For HHO, this value is defined as number of frames until the Target BS allocates a non-contention based ranging opportunity for the MSS. For SHO/FBSS, this is the time of update of Anchor BS and/or Active Set. A value of zero in this parameter signified that this parameter should be ignored.
~~HMAC Tuple (see 11.1.2)~~
~~The HMAC Tuple Attribute contains a keyed Message digest (to guarantee the origin and integrity of the message.) The HMAC Tuple shall be the last item in the message.~~

[Add a new paragraph at the *end of section 6.3.2.3.51*]

The MOB_BSHO-REQ may contain the following TLVs:

Resource Retain Time (see 11.16.1)

The MOB_BSHO-REQ message shall include the following parameters encoded as TLV tuples:
HMAC Tuple (see 11.1.2)

[*Modify the contents of Table 108n as indicated:*]

Table 108n-MOB_MSHO-REQ message format

Syntax	Size	Notes
Estimated HO start	8 bits	The estimated HO time shall be the time for the recommended target BS.
~~HMAC Tuple~~	~~21 bytes~~	~~See 11.1.2~~
Padding	variable	Padding bits to ensure byte aligned.
TLV encoded information	variable	
}		

[Delete *the description of HMAC Tuple on page to 105*]

Estimated HO start
Estimated number of frames starting from the frame following the reception of the MOB_BSHO-RSP message
~~HMAC Tuple (see 11.1.2)~~
~~The HMAC Tuple Attribute contains a keyed Message digest (to guarantee the origin and integrity of the message). The HMAC Tuple shall be the last item in the message~~
Comp_NBR_BSID_IND
This bit indicates whether neighbor BSIDs are compressed or not. MS can compress BSID, only when NBR_BS_Index_Validity_Time is larger than the difference of MOB_SCAN_REPORT message transmitting time and MOB_NBR_ADV message receiving time (MOB_NBR_ADV message should be referred in order to compress neighbor BSIDs). This difference time is calculated from Frame number of DL-MAP PHY Synchronization Field).

[Add a new paragraph at the end of section 6.3.2.3.52]

The MOB_MSHO-REQ message shall include the following parameters encoded as TLV tuples:
HMAC Tuple (See 11.1.2.)

[Modify the contents of *Table 108o as indicated*]

Table 108o-MOB_BSHO-RSP message format

Syntax	Size	Notes
Action Time	8 bits	
Resource Remain Type	1 bit	0: MS resource release 1: MS resource retain
Padding	variable	Padding bits to ensure byte aligned.
TLV encoded information	variable	TLV specific

~~HMAC Tuple~~	~~21 bytes~~	~~See 11.1.2~~
}		

[Delete *the description of HMAC Tuple on page110*]

Resource Remain Type

The Resource Remain Type flag indicates whether the serving BS will retain or delete the connection information of the MS upon receiving MOB_HO-IND with HO_IND_type=00. If the flag is set to 1, the serving BS will retain the MS's connection information during the time in Resource Retain Time field. If Resource Remain Type=1 and Resource Retain Time is not included as a TLV item in the message, then the serving BS and MS shall use the System Resource Retain Time timer. If the flag is set to 0, the serving BS will discard the MS's connection information.

~~HMAC Tuple (see 11.1.2)~~

~~The HMAC Tuple Attribute contains a keyed Message digest (to guarantee the origin and integrity of the message).~~

[Modify the last paragraph as indicated and Add a new paragraph at the end of section 6.3.2.3.53]

The MOB_MSHO-R~~EQ~~SP may contain the following TLVs:

Resource Retain Time (11.16.1)

The MOB_BSHO-RSP message shall include the following parameters encoded as TLV tuples:

HMAC Tuple (See 11.1.2.)

[Modify the contents of *Table 108p as indicated:]*

Table 108p-MOB_HO-IND message format

Syntax	Size	Notes
Preamble index/Subchannel Index	8 bits	For the SCa and OFDMA PHY this parameter defines the PHY specific preamble for the target BS. For the OFDM PHY the 5 LSB contain the active DL subchannel index for the target BS. The 3 MSB shall be Reserved and set to '0b000'
Padding	variable	Padding bits to ensure byte aligned.
~~HMAC Tuple~~	~~21 bytes~~	~~See 11.1.2~~
TLV encoded information	variable	TLV specific
}		

[Delete *the description of HMAC Tuple on page 113 and add a new paragraph in section 6.3.2.3.54*]

An MS shall generate MOB_HO-IND messages in the format shown in Table 108p. The following parameters shall be included in the message:

Target_BS_ID

Same as the Base Station ID parameter in DL-MAP message of target BS. This may include the serving BS.

Preamble Index/Subchannel Index

For the SCa and OFDMA PHY this parameter defines the PHY specific preamble for the target BS. For the OFDM PHY the 5 LSB contain the DL subchannel index (as defined in Table 211) used in the target BS sector. The 3 MSB shall be Reserved and set to '0b000'.

~~HMAC Tuple (see 11.1.2)~~

~~The HMAC Tuple Attribute contains a keyed Message digest (to guarantee the origin and integrity of the message).~~

The MOB_HO-IND message shall include the following parameters encoded as TLV tuples:
HMAC Tuple (See 11.1.2.)

[*Add a new paragraph in section 11.1.2]*

11.1.2 Authentication Tuples

An authentication tuple shall be the last item in management messages.

[*Change the contents of Table 347 as indicated:*]

Type	Length	Value	Scope
149	21	See Table 348	DSx-REQ, DSx-RSP, DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-CMD, TFTP-CPLT, MOB_SLP-REQ, MOB_SLP-RSP, MOB_SCN-REQ, MOB_SCN-RSP, MOB_BSHO-REQ, MOB_MSHO-REQ, MOB_BSHO-RSP, MOB_HO-IND

[*Change the contents of Table 348a as indicated:*]

Type	Length	Value	Scope
	12	See Table 346a	DSx-REQ, DSx-RSP,DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-CMD, TFTP-CPLT, MOB_SLP-REQ, MOB_SLP-RSP, MOB_SCN-REQ, MOB_SCN-RSP, MOB_BSHO-REQ, MOB_MSHO-REQ, MOB_BSHO-RSP, MOB_HO-IND