Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>	
Title	**Clarification on HMAC/CMAC tuples**	
Date Submitted	**2007-09-09**	
Source(s)	Sergey Seleznev, Hyoung Kyu Lim, Hyunjeong Kang, Jungje Son Samsung Electronics Rep. of Korea, Gyonggi-do, Suwon	Voice: +82312795968 E-mail: s.sergey@samsung.com
Re:	IEEE 802.16j-07/019	
Abstract	This contribution proposes text changes to apply HMAC/CMAC protection to relay control messages.	
Purpose	Discuss and adopt proposed text changes.	
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the “Source(s)” field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who 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	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.	

Clarification on HMAC/CMAC tuples

Sergey Seleznev, Hyoung Kyu Lim, Hyunjeong Kang, Jungje Son
Samsung Electronics

Introduction

Most of the newly proposed messages are not protected (i.e. does not include HMAC/CMAC tuple). This contribution proposes relevant text changes.

Proposed text changes

[*Add the following text at the end of subclause 6.3.2.3.56*]:

The MOB_PAG-ADV message transmitted over relay link shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.62*]:

The RS-CDC-REQ message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.63*]:

The MR_NBR-INF shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.64*]:

The MR_Code-REP message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.66*]:

The RS_Config-RCM message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.68*]:

The RS_NBR-MEAS-REP message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Change subclause 6.3.2.3.69.1 as follows*]:

The MR_LOC-REQ message shall contain the following TLVs:~~The following TLV parameters may be included in the MR_LOC-REQ message:~~

~~Short~~ **HMAC/CMAC Tuple (see 11.1.2)**
The ~~Short~~ HMAC/CMAC Tuple shall be the last attribute in the message.

[*Change subclause 6.3.2.3.69.2 as follows*]:

The MR_LOC-RSP message shall contain the following TLVs:~~The following TLV parameter shall be included in the MR_LOC-RSP when the BS or RS wishes to acknowledge a valid Short-HMAC/CMAC Tuple in the acknowledged MR_LOC-REQ management message:~~

~~**Short**~~ **HMAC/CMAC Tuple (see 11.1.2)**
The ~~Short~~ HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.70*]:

The MS_SCN-INF message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.71*]:

The MS_SCN-CLT message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.72*]:

The MS_INFO-DEL message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.73*]:

The RS-CD message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.74*]:

The CLK-SYNC message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.75*]:

The MR_ASC-REQ message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.76*]:

The MR_ASC-RSP message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.77*]:

The MOB_RSSCN-REP message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.78*]:

The MOB_RSSCN-RSP message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)
The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Change subclause 6.3.2.3.79 as follows*]:

Add the following text after the Table 183t:

The HARQ_CHASE_ER-REP message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

Add the following text after the Table 183u:

The HARQ_IR_ER-REP message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.81*]:

The STA-INFO message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.82*]:

The RS_path-REQ message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.83*]:

The RS-SCH message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.84*]:

The RS_Member_List_Update message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Add the following text at the end of subclause 6.3.2.3.87*]:

The COMP_AAS_DCD-UCD message shall contain the following TLVs:

HMAC/CMAC Tuple (see 11.1.2)

The HMAC/CMAC Tuple shall be the last attribute in the message.

[*Change subclause 11.1.2.2 as indicated*]:

Change Table 348a (.16e)/Table 597 (Rev2) as indicated:

Table 597—CMAC Tuple definition

Type	Length	Value	Scope
141	13 or 19	See Table 598	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, DREG-REQ, RNG-REQ, RNG-RSP, MR_LOC-REQ, MR_LOC-RSP, MOB_PAG_ADV, RS-CDC-REQ, MR_NBR-INF, RS_Config-RCM, RS_NBR-MEAS-REP, MS_SCN-INF, MS_SCN-CLT, MS_INFO_DEL, RS_CD, CLK-SYNC, MR_ASC-REQ, MR_ASC-RSP, MOB_RSSCN-REP, MOB_RSSCN-RSP, HARQ_CHASE_ER-REP, STA-INFO, RS_path-REQ, RS-SCH, RS_Member_List_Update, COMP_AAS_DCD-UCD

[*Change subclause 11.1.2.3 as indicated*]:

Change Table 348c (.16e)/Table 599 (Rev2) as indicated:

Table 599—Short-HMAC Tuple definition

Type	Length	Value	Scope
150	13 or 19	See Table 600	MOB_SLP-REQ, MOB_SLP-RSP, MOB_SCN-REQ, MOB_SCN-RSP, MOB_MSHO-REQ, MOB_BSHO-RSP, MOB_HO-IND, RNG-REQ, RNG-RSP, PKM-REQ, PKM-RSP, MR_LOC-REQ, MR_LOC-RSP, MOB_PAG_ADV, RS-CDC-REQ, MR_NBR-INF, RS_Config-RCM, RS_NBR-MEAS-REP, MS_SCN-INF, MS_SCN-CLT, MS_INFO_DEL, RS_CD, CLK-SYNC, MR_ASC-REQ, MR_ASC-RSP, MOB_RSSCN-REP, MOB_RSSCN-RSP, HARQ_CHASE_ER-REP, STA-INFO, RS_path-REQ, RS-SCH, RS_Member_List_Update, COMP_AAS_DCD-UCD