Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>
Title	**Multicast Key Usage and Update on IEEE 802.16.1a**
Date Submitted	**2011-11-09**
Source(s)	Eunkyung Kim, Sungcheol Chang, Won-Ik Kim, Seokki Kim, Sungkyung Kim, Miyoung Yun, Hyun Lee, Chulsik Yoon, Kwangjae Lim ETRI Voice: +82-42-860-5415 E-mail: ekkim@etri.re.kr scchang@etri.re.kr Wai Leong Yeow, Joseph Teo Chee Ming Institute For Infocomm Research wlyeow@i2r.a-star.edu.sg cmteo@i2r.a-star.edu.sg
Re:	"IEEE 802.16n-11/0020," in response to Call for Comments on GRIDMAN AWD
Abstract	Multicast key management on GRIDMAN Amendment Draft Standard
Purpose	To discuss and adopt the proposed text in the draft amendment document on GRIDMAN
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.
Copyright Policy	The contributor is familiar with the IEEE-SA Copyright Policy <http://standards.ieee.org/IPR/copyrightpolicy.html>.
Patent Policy and Procedures	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>.

Multicast Key Usage and Update on IEEE 802.16.1a

Eunkyung Kim, Sungcheol Chang, Won-Ik Kim, Seokki Kim, Sungkyung Kim, Miyoung Yun, Hyun Lee, Chulsik Yoon, Kwangjae Lim
ETRI

Wai Leong Yeow, Joseph Teo Chee Ming
Institute for Infocomm Research

1. Introduction

In IEEE 802.16.1a[3], multicast security key is described and hierarchy and how to derived MTEK and MCMAC key from the MAK. To support multicast operation, MAK is defined as a pre-shared key and shared by MSs in a multicast group. However, MTEK may be updated (or re-keyed) in the event of following cases:

- when new MAK is re-established. However, how to update/re-establish is outside scope of IEEE 802.16
- prior to expiry of lifetime
- in response to request by HR-MS using either PKM-REQ or RNG-REQ
- when a member of group has been unsubscribed (i.e., leaved) or joined

To update MTEK, HR-BS may transmit either PKM-RSP or RNG-RSP, including following parameters:

- Multicast Group ID
- FID
- MEKS
- COUNTER_MTEK

Thus, this contribution provides how to update multicast security key (i.e., MTEK).

2. References

[1] IEEE 802.16n-10/0048r2, 802.16n System Requirement Document including SARM annex, July 2011.
[2] IEEE 802.16n-11/0024, P802.16n Draft AWD, October 2011.
[3] IEEE 802.16n-11/0025, P802.16.1a Draft AWD, October 2011.
[4] IEEE P802.16Rev3/D2, IEEE Draft Standard for Local and metropolitan area networks; Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," October 2011.
[5] IEEE P802.16.1^{TM}/D2, [Draft] WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems, October 2011.

[6] IEEE C802.16n-11/0177r1, Multicast Key Usage and Update, September 2011.

3. Proposed Text on the IEEE 802.16.1a Amendment Draft Standard

[----------Start of Text Proposal----------]

[*Remedy1: Change Table 684-AAI-RNG-REQ message Field Description in line 1, page 17 (section 6.2.3.1) in the 802.16.1a AWD as follows*:]

Field	Size(bits)	Value/Description	Conditions

Ranging Purpose Indication	4	0b0000 = Initial network entry 0b0001 = HO reentry 0b0010 = Network reentry from idle mode 0b0011 = Idle mode location update 0b0100 = DCR mode extension 0b0101 = Emergency call setup (e.g., E911) 0b0110 = Location update for updating service flow management encodings of E-MBS flows 0b0111 = Location update for transition to DCR mode from idle mode 0b1000 = Reentry from DCR mode, coverage loss or detection of different ABS restart count. 0b1001 = Network reentry from a Legacy BS 0b1010 = Zone switch to MZONE from LZONE 0b1011 = Location update due to power down. 0b1100 = Interference mitigation request to a CSG Femto ABS when experiencing interference from the CSG Femto ABS 0b1101 = NS/EP call setup ~~0b1110–0b1111 = reserved~~ 0b1110 = HR multicast service ~~flow update~~ location update 0b1111 = reserved	-
.....	...	.....	
}else if (Ranging Purpose Indication == 0b1101) {		//NS/EP call setup	
AMS MAC address	48	AMS's real MAC address	
MAC version	8	see 11.1.3	

Initial Offset for uplink power control (OffsetInitial)	5	The bit size represents power level ranging from -15dB (0x00) to 16dB(0x1F) with 1dB step. The value is determined by AMS after successful initial ranging process.	
}else if (Ranging Purpose Indication == 0b1110) {		// HR multicast location update	
action code	3	bit0: multicast service flow update bit1: location update due to multicast zone change bit2: multicast security key update	
} //end of Ranging Purpose Indication			

[*Remedy2: Insert the following rows after "New FID" in Table 685-AAI-RNG-RSP message Field Description in 5th row, page 19 (section 6.2.3.2) in the 802.16.1a AWD.*]

New FID	4		
}			
Multicast Group ID	12	Multicast Group ID to update METK	Shall be present if needed to update MTEK in HR-Network
FID	4	FID to update MTEK	Shall be present if needed to update MTEK in HR-Network
COUNTER_MTEK	16	COUNTER_MTEK used for deriving current MTEK	Shall be present if needed to update MTEK in HR-Network
MEKS	2	Encryption key sequence number for current MTEK	Shall be present if needed to update MTEK in HR-Network

} // end of If (Location Update Response == 0x0)			

[*Remedy3: Add the following rows after "New FID" in Table 685-AAI-RNG-RSP message Field Description in 2th row from the bottom, page 20 (section 6.2.3.2) in the 802.16.1a AWD.*]

New FID	4		
}			
Multicast Group ID	12	Multicast Group ID to update METK	Shall be present if needed to update MTEK in HR-Network
FID	4	FID to update MTEK	Shall be present if needed to update MTEK in HR-Network
COUNTER_MTEK	16	COUNTER_MTEK used for deriving current MTEK	Shall be present if needed to update MTEK in HR-Network
MEKS	2	Encryption key sequence number for current MTEK	Shall be present if needed to update MTEK in HR-Network
} // end of If (it is under network reentry for HO)			

[*Remedy4: Replace "MCMAC-MTEK Prekey = Dot16KDF(MAK, MAK COUNT|"MACMA-MTEK prekey", 16)" by MCMAC-MTEK Prekey = Dot16KDF(MAK, MulticastGrpID|MCNonce|"MACMA-MTEK prekey", 160)" in Figure 934, page 185 (section 6. 12.10.2) in the 802.16.1a AWD.*]

**[*Remedy5: Change Table 1223 - The MAK context in line 4, page 186, in the 802.16.1a*

AWD as follows:]

Parameter	Size (bit)	Usage
MAK	160	Shared by HR-MSs in a multicast group
MAK Lifetime	32	MAK Lifetime
MAKID	64	Identifies the authorization key.
~~MAK_COUNT~~	~~16~~	~~A value used to derive the MCMAC key and MTEK~~
MulticastGrpID	16	The identifier of the multicast group 12bits of MSB is MGID and 4bit LSB is FID of the multicast group
MCNonce	128	A random number used to derive the MCMAC-MTEK Prekey
MCMAC_KEY_D	128	The key which is used for signing DL MAC control messages.
MCMAC_PN_D	24	Used to avoid DL replay attack on the control connection before this expires, reauthorization is needed. The initial value of MCMAC_PN_D is zero and the value of MCMAC_PN_D is reset to zero whenever MAK_COUNT is increased.
Next available counter_MTEK	16	The counter value to be used in next MTEK derivation, after derivation this is increased by 1.

[*Remedy6: Insert the following text into the end of 6.2.10.2 in the 802.16.1a AWD.*]

6.2.10.2.a Multicast Key Derivation

The multicast key hierarchy defines what keys are present in the system for secure multicast operations and how the keys are generated.

6.2.10.2.a.1 MAK Key Derivation

The 160bits MAK is the pre-established shared key among the HR-BS and a group of HR-MSs in a secure HR-multicast group. The generation and transport of the MAK is outside the scope of the IEEE 802.16 standard. The MAK is a 160-bit key.

The MAK is used to derive the MCMAC-MTEK Prekey as follows:

MCMAC-MTEK Prekey = Dot16KDF(MAK, MulticastGrpID|MCNonce| “MCMAC-MTEK prekey”, 160)

The MCMAC-MTEK Prekey is used to derive the :

- Multicast Cipher-based Message Authentication Code (MCMAC) key

- Multicast Traffic Encryption (MTEK) Key

6.2.10.2.a.2 MCMAC Key Derivation

The 128bits MCMAC key is derived from MCMAC-MTEK Prekey and used for message authentication for the multicast messages sent during secure multicast operation.

MCMAC key is derived as follows:

MCMAC = Dot16KDF(MCMAC-MTEK Prekey, “MCMAC_KEYS”, 128)

6.2.10.2.a.3 MTEK Derivation

The 128bits MTEK is the multicast transport encryption key used to encrypt data for secure multicast operations.

MTEK is derived as follows:

MTEKi = Dot16KDF(MCMAC-MTEK Prekey, MSAID|COUNTER_MTEK=i|“MTEK”, 128)

6.2.10.2.x Key usage

6.2.10.2.x.1 MTEK usage

Each MSA maintains MTEK marked as DLE.

The $MTEK_{DLE}$ key is used for encrypting DL multicast data by the HR-BS. The decryption is done according to the MEKS so basically, in transition times.

Each MTEK has its own PN counter size 22bits.

The PN is used for DL multicast traffic and its range is 0x000000-0x1FFFFF.

6.2.10.2.x.2 MTEK update

The MTEK update is triggered by $MTEK_{DLE}$ running out the relevant PN space. In particular, HR-BS derives new MTEK when the DL PN space of $MTEK_{DLE}$ is exhausted.

The HR-BS shall indicate the new MEKS, COUNTER_MTEK, and MTEK lifetime in the AAI-PKM-RSP message when the current MTEK lifetime expires. If the COUNTER_MTEK or MEKS are updated, the HR-MS updates its MTEK accordingly. Unless the COUNTER_MTEK and MEKS are updated, it means the HR-BS did not derive new MTEK yet and the HR-MS shall maintain the current MTEKs but reset the value of MTEK lifetime.

[----------End of Text Proposal----------]