Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Enhancement of the Multicast & Broadcast Rekeying Algorithm**
Data Submitted	**2004-11-15**

Source(s)	Seokheon Cho Sungcheol Chang Chulsik Yoon, ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr

Re:	IEEE 802.16e Security Ad Hoc
Abstract	The supplementary contents for the efficient rekeying method for the multicast service and the broadcast service
Purpose	The document is submitted for review by 802.16 Working Group members
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:chiar@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>.

Enhancement of the Multicast & Broadcast Rekeying Algorithm

Seokheon Cho, Sungcheol Chang, and Chulsik Yoon
ETRI

Introduction

The MBRA (Multicast & Broadcast Rekeying Algorithm) is defined in the IEEE P802.16e/D5.

However, some contents for the MBRA are not considered in the IEEE P802.16e/D5 as the following:

* The Key Update Command message used for the MBRA is not added into the PKM message codes.
* The usage of the Key Update Command message is not defined.
* The generation method of the HMAC authentication keys is not defined.
* A few PKM-REQ/PKM-RSP encoding parameters for the MBRA are not defined.

In this contribution, we suggest some contents needed to be supplemented so that the MBRA is fully operated for the multicast service and broadcast service.

Proposed changes

[Modify in the Table 14]
6.3.2.3 MAC Management messages

Table 14- MAC Management messages

Type	Message name	Message description	Connection
10	PKM-RSP	Privacy Key Management Response	~~Primary Management~~ Primary Management or Broadcast (optional)

[Insert as following below the Table 14]

In general, the PKM-RSP message is carried on the Primary Management connection. However, in order to send the PKM-RSP message in key push mode for the multicast service or the broadcast service, it may be carried on the Broadcast connection.

[Modify as the following in section 6.3.2.3.9]
6.3.2.3.9 Privacy key management (PKM) messages (PKM-REQ/PKM-RSP)

PKM employs two MAC message types: PKM Request (PKM-REQ) and PKM Response (PKM-RSP), as described in Table 23.

Table 23 - PKM MAC messages

Type Value	Message name	Message description
9	PKM-REQ	Privacy Key Management Request[SS->BS]
10	PKM-RSP	Privacy Key Management Request[BS->SS]

These MAC management message types distinguish between PKM requests (SS–to–BS) and PKM responses (BS–to–SS). Each message encapsulates one PKM message in the Management Message Payload.

PKM protocol messages transmitted from the SS to the BS shall use the form shown in Table 24. They are transmitted on the SSs Primary Management Connection.

Table 24 - PKM request (PKM-REQ) message format

Syntax	Size	Notes
PKM-REQ_Message_Format () {		
Management Message Type = 9	8 bits	
Code	8 bits	
PKM Identifier	8 bits	
TLV Encoded Attributes	variable	TLV specific
}		

PKM protocol messages transmitted from the BS to the SS shall use the form shown in Table 25. They are transmitted on the SSs Primary Management Connection. When the BS sends PKM-RSP message in key push mode for the multicast service or the broadcast service, it may be carried on the Broadcast connection.

Table 25 - PKM request (PKM-RSP) message format

Syntax	Size	Notes
PKM-REQ_Message_Format () {		
Management Message Type = 10	8 bits	

Code	8 bits	
PKM Identifier	8 bits	
TLV Encoded Attributes	variable	TLV specific
}		

The parameters shall be as follows:

Code

The Code is one byte and identifies the type of PKM packet. When a packet is received with an invalid Code, it shall be silently discarded. The code values are defined in Table 26.

PKM Identifier

The Identifier field is one byte. An SS uses the identifier to match a BS response to the SS's requests.

The SS shall increment (modulo 256) the Identifier field whenever it issues a new PKM message. A "new" message is an Authorization Request or Key Request that is not a retransmission being sent in response to a Timeout event. For retransmissions, the Identifier field shall remain unchanged.

The Identifier field in Authentication Information messages, which are informative and do not effect any response messaging, shall be set to zero. The Identifier field in a BS's PKM-RSP message shall match the Identifier field of the PKM-REQ message the BS is responding to. The Identifier field in TEK Invalid messages, which are not sent in response to PKM-REQs, shall be set to zero. The Identifier field in unsolicited Authorization Invalid messages shall be set to zero. The Identifier field in Key Update Command messages, which are used to distribute the updated GTEK and traffic keying material, shall be set to zero.

On reception of a PKM-RSP message, the SS associates the message with a particular state machine (the Authorization state machine in the case of Authorization Replies, Authorization Rejects, and Authorization Invalids; a particular TEK state machine in the case of Key Replies, Key Rejects, ~~and TEK Invalids~~ TEK Invalids, and Key Update Commands).

An SS shall keep track of the identifier of its latest, pending Authorization Request. The SS shall discard Authorization Reply and Authorization Reject messages with Identifier fields not matching that of the pending Authorization Request.

An SS shall keep track of the identifiers of its latest, pending Key Request for each SA. The SS shall discard Key Reply and Key Reject messages with Identifier fields not matching those of the pending Key Request messages.

Attributes

PKM attributes carry the specific authentication, authorization, and key management data exchanged between client and server. Each PKM packet type has its own set of required and optional attributes. Unless explicitly stated, there are no requirements on the ordering of attributes within a PKM message. The end of the list of attributes is indicated by the LEN field of the MAC PDU header.

Table 26 - PKM message codes

Code	PKM message type	MAC Management message name
0-2	reserved	-
3	SA Add	PKM-RSP
4	Auth Request	PKM-REQ
5	Auth Reply	PKM-RSP
6	Auth Reject	PKM-RSP
7	Key Request	PKM-RSP
8	Key Reply	PKM-RSP
9	Key Reject	PKM-RSP
10	Auth Invalid	PKM-RSP
11	TEK Invalid	PKM-RSP
12	Auth Info	PKM-REQ
13	EAP Transfer	PKM-REQ/PKM-RSP
14	EAP Establish-Key Request	PKM-RSP
15	EAP Establish-Key Reply	PKM-REQ
16	EAP Establish-Key Reject	PKM-REQ
17	EAP Establish-Key Confirm	PKM-RSP
18	Pre-Auth-Request	PKM-REQ

19	Pre-Auth-Reply	PKM-RSP
20	Pre-Auth-Reject	PKM-RSP
21	PKMv2 Auth Request	PKM-REQ
22	PKMv2 Auth Reply	PKM-RSP
23	Key Update Command	PKM-RSP
24-255 ~~13-255~~	Reserved	-

Formats for each of the PKM messages are described in the following subclauses. The descriptions list the PKM attributes contained within each PKM message type. The attributes themselves are described in 11.9. Unknown attributes shall be ignored on receipt and skipped over while scanning for recognized attributes.

The BS shall silently discard all requests that do not contain ALL required attributes. The SS shall silently discard all responses that do not contain ALL required attributes.

[Add the following to section 6.3.2.3.9:]

6.3.2.3.9.21 Key Update Command messages

The BS transmits the Key Update Command message in order to distribute the new GKEK, GTEK, and traffic keying material. This message is defined only for the multicast service or the broadcast service.

Code: 23

Attributes are shown in Table 37k.

Table 37k Key Update Command attributes

Attribute	Contents
Key-Sequence-Number	Authorization key sequence number
GSAID	Group Security Association ID
Key Push Modes	Usage code of Key Update Command message
Key Push Counter	Counter one greater than that of older generation
TEK-Parameters	"Newer" generation of key parameters relevant to GSAID
> GKEK	GKEK, encrypted with GKEKEK derived from the SS's AK
> GTEK	GTEK, encrypted with the GKEK
> Key-Lifetime	GTEK Remaining Lifetime
> Key-Sequence-Number	GTEK Sequence Number
> CBC-IV	Cipher Block Chaining (CBC) Initialization Vector (conditional with value of the cryptographic suite)
HMAC-Digest	Keyed SHA message digest (conditional with value of the authorization policy support)
OMAC-Digest	Message Digest calculated using OMAC_KEY (conditional with value of the authorization policy support)

Key Sequence Number is the sequence number of the synchronized AK (Authorization Key) between the MSS and the BS.

GSAID is SAID for the multicast group or the broadcast group. The type and length of the GSAID is equal to ones of the SAID.

There are two types in the Key Update Command message, GKEK update mode and GTEK update mode. The former is used to update GKEK and the latter is used to update GTEK for the multicast service or the broadcast service. Key Push Modes indicates this usage code of the Key Update Command message. The Key Update Command message for the GKEK update mode is carried on the Primary Management connection, but one for the GTEK update mode is carried on the Broadcast connection. A few attributes in the Key Update Command message shall not be used according this Key Push Modes attribute's value. See 11.9.33 for details.

Key Push Counter is used to protect for replay attack. This value is one greater than that of older generation.

The Key Update Command message contains only newer generation of key parameters, because this message inform an MSS of

next traffic key material. The TEK-Parameters attribute is a compound attribute containing all of the keying material corresponding to a newer generation of a GSAID's GTEK. This would include the GKEK, the GTEK, the GTEK's remaining key lifetime, the GTEK's key sequence number, and the cipher block chaining (CBC) initialization vector. The GTEK is TEK for the multicast group or the broadcast group. The type and length of the GTEK is equal to ones of the TEK. The GKEK (Group Key Encryption Key) can be randomly generated from a BS or an ASA server. The GKEK should be identically shared within the same multicast group or the broadcast group. Contrary to the unicast service, for which the TEK is encrypted with KEK derived from the AK, the GTEK is encrypted with GKEK for the multicast service or the broadcast service. The GKEK is also encrypted by the GKEKEK that is derived from the AK. See 7.5.4.4 for details.

The HMAC-Digest attribute shall be the final attribute in the message's attribute list. Inclusion of the keyed digest allows the receiving client to authenticate the Key Update Command message. The HMAC-Digest's authentication key is derived from the AK for the GKEK update mode and GKEK for the GTEK update mode. See 7.5.4.3 for details.

[Modify as following in section 7.5.4.3]
7.5.4.3 HMAC authentication keys

The HMAC authentication keys are derived as follows:

HMAC_KEY_D = SHA(H_PAD_D|AK)
HMAC_KEY_D = SHA(H_PAD_D|GKEK) : only for the Key Update Command message for the GTEK update mode
HMAC_KEY_U = SHA(H_PAD_U|AK)
HMAC_KEY_S = SHA(H_PAD_D|Operator Shared Secret).

with

H_PAD_D = 0x3A repeated 64 times
H_PAD_U = 0x5C repeated 64 times.

[Add the following section]
7.5.4.4 Encryption of GKEK

The BS encrypts the value fields of the GKEK in the Key Update Command message for the GKEK update mode and sends the encrypted GKEK to each SS served with the specific multicast service or the broadcast service. This field is encrypted using 128 bit AES Key Wrap Algorithm.

7.5.4.4.1 Encryption of GKEK with AES Key Wrap

The GKEK is encrypted using 128 bit AES Key Wrap Algorithm.

Encryption: C,I = Ek[P]
Decryption: P,I = Dk[C]
P = Plaintext 128-bit GKEK
C = Ciphertext 128-bit GKEK
I = Integrity Check Value
k = the 128-bit GKEKEK
Ek[ ] = AES Key Wrap encryption with key k
Dk[ ] = AES Key Wrap decryption with key k

7.9 MBRA (Multicast & Broadcast Rekeying Algorithm)

[Change from … to …]
[From]

If GTEK update exchange method for the multicast service and the broadcast service is identically applied to one for the unicast service, then that multicast and broadcast rekeying is resource inefficient.

Therefore, GTEK refreshment for the multicast service and the broadcast service should be different from one for the unicast

service. The new MBRA (Multicast & Broadcast Rekeying Algorithm) to efficiently refresh GTEK is needed. The MBRA is restricted to the multicast service and the broadcast service.

The aims of the MBRA are satisfied with the following:
• Provide efficient rekeying method for multicast group and broadcast group.
• Provide a BS's key push mode to an MSS.
• Provide strong protection for the replay attack.

[To]

This MBRA shall be used to refresh traffic keying material efficiently not for the unicast service, but for the multicast service or the broadcast service.

~~If GTEK update exchange method for the multicast service and the broadcast service is identically applied to one for the unicast service, then that multicast and broadcast rekeying is resource inefficient.~~

~~Therefore, GTEK refreshment for the multicast service and the broadcast service should be different from one for the unicast service. The new MBRA (Multicast & Broadcast Rekeying Algorithm) to efficiently refresh GTEK is needed. The MBRA is restricted to the multicast service and the broadcast service.~~

~~The aims of the MBRA are satisfied with the following:~~
~~• Provide efficient rekeying method for multicast group and broadcast group.~~
~~• Provide a BS's key push mode to an MSS.~~
~~• Provide strong protection for the replay attack.~~

[Modify as the following in section 7.9.1]
7.9.1 MBRA Flow

The MBRA overall flow is shown in the Figure 137b.

An MSS may get the traffic keying material before an MSS is served with the specific multicast service or the broadcast service. The initial GTEK request exchange procedure is executed by using the Key Request and Key Reply messages that are carried on the Primary Management connection. Once an MSS shares the traffic keying material with a BS, an MSS doesn't need to request the new traffic keying material. A BS updates and distributes the traffic keying material periodically by sending two Key Update Command messages.

A BS manages the M&B (Multicast & Broadcast) TEK Grace Time for the respective GSA-ID in itself. This M&B TEK Grace Time is defined only for the multicast service or the broadcast service. This parameter means time interval (in seconds), before the estimated expiration of an old distributed GTEK. In addition, the M&B TEK Grace Time is longer than the TEK Grace Time managed in an MSS.

A BS distributes updated traffic keying material by sending two Key Update Command messages before old distributed GTEK is expired. The usage type of these messages is distinguished according to the Key Push Modes included in the Key Update Command message.

A BS transmits the Key Update Command message for the GKEK update mode to each MSS served with the specific multicast service or the broadcast service before the M&B TEK Grace Time starts. The purpose of the Key Update Command message for the GKEK update mode is to distribute the GKEK (Group Key Encryption Key). The Key Update Command message for the GKEK update mode is carried on the Primary Management connection. A BS intermittently transmits the Key Update Command message for the GKEK update mode to each MSS in order to reduce the BS's load in refreshing traffic key material. The GKEK is needed to encrypt the new GTEK. The GKEK can be randomly generated in a BS or an ASA server.

A BS transmits the Key Update Command message for the GTEK update mode carrying on the Broadcast connection after the M&B TEK Grace Time starts. The aim of the Key Update Command message for the GTEK update mode is to distribute new GTEK and the other traffic keying material to all SSs served with the specific multicast service or the broadcast service. This GTEK is encrypted with already transmitted GKEK.

If an MSS receives the valid two Key Update Command messages and shares new valid GKEK and GTEK with a BS, then that MSS doesn't need to request a new set of traffic keying material.

If an MSS doesn't receive at least one of two Key Update Command messages, then that MSS sends the Key Request message to get a new traffic keying material. A BS responds to the Key Request message with the Key Reply message. In other words, if an MSS doesn't get valid new GKEK or GTEK, then the GTEK request exchange procedure initiated by a MSS is executed.

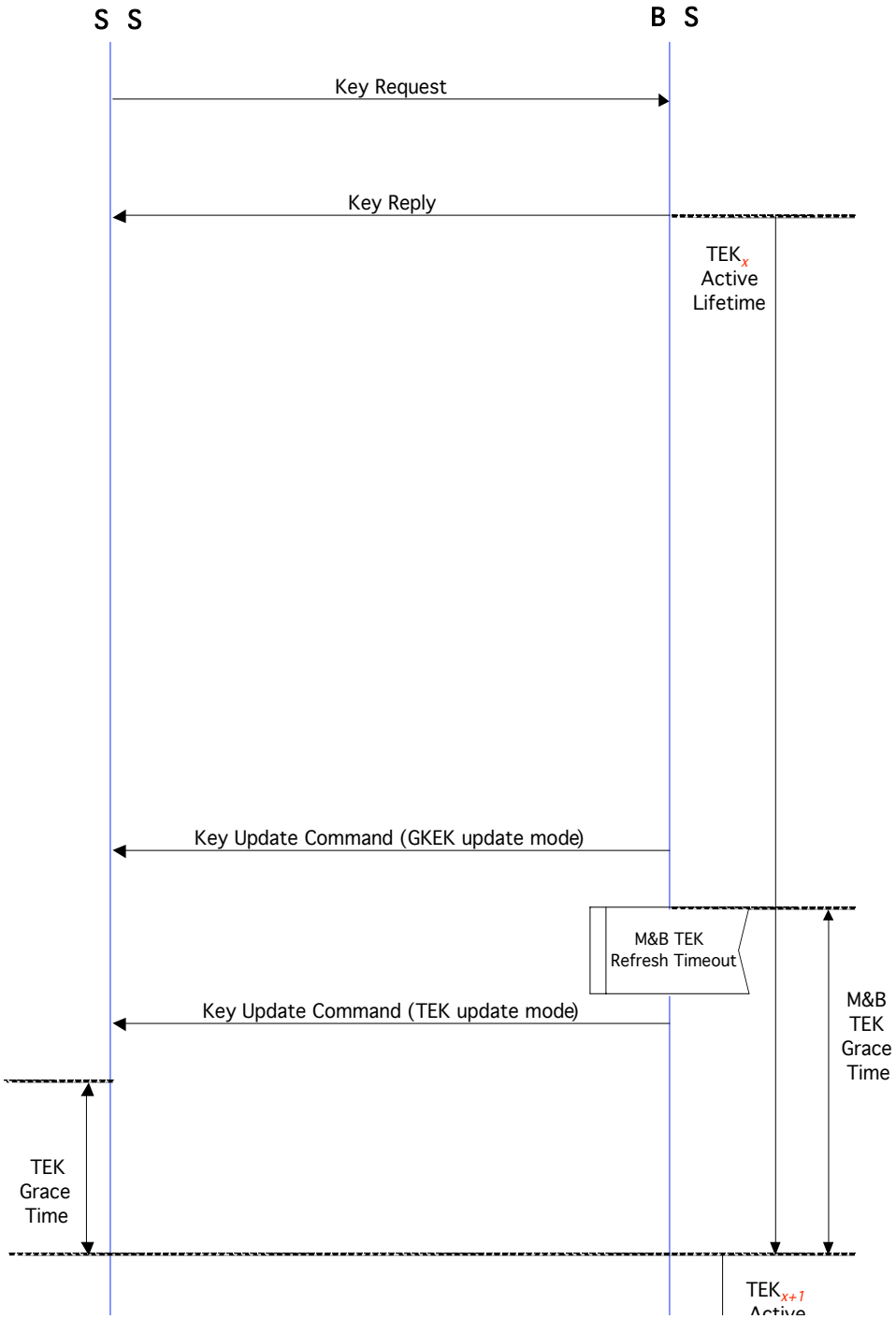

Figure 137b- MBRA management

[Modify as the following in section 7.9.3]
7.9.3 Encryption of GKEK

The BS encrypts the value fields of the GKEK in the Key Update Command message for the GKEK update mode and sends the encrypted GKEK to each SS served with the specific multicast service or the broadcast service. This field is encrypted using 128 bit AES Key Wrap Algorithm. See 7.5.4.4 for details.

~~The 160-GKEK used to encrypt GTEK is encrypted using 128-bit AES KEY WRAP.~~

~~A BS encrypts the value fields of the 128-GKEK in the first Key Update Command messages (GKEK update mode) and sends to each MSS served.~~

~~Encryption: C = AES_KEY_WRAP_ENCRYPT(k1, P)~~
~~Decryption: P = AES_KEY_WRAP_DECRYPT(k1,C)~~
~~P = Plaintext GKEK 160-bit~~
~~C = Ciphertext GKEK 160-bit~~
~~k1 = GKEKEK~~
~~I = AES_KEY_WRAP_DECRYPT(k1, C)~~
~~I: AES Key Wrap Integrity Value~~

[Add as the following in section 7.9:]
7.9.4 HMAC authentication keys for the Key Update Command message

HMAC-Digest attribute is used for Key Update Command message authentication.

Input key used to generate HMAC authentication keys of Key Update Command message is different according to the value field of the Key Push Modes. The AK shall be used for generation of HMAC-Digest included in the Key Update Command message for the GKEK update mode and the GKEK shall be used for generation of HMAC-Digest included in the Key Update Command message for the GTEK update mode. See 7.5.4.3 for details.

10.2 PKM parameter values
[Add the following above the Table 341]

The M&B TEK Grace Time is longer than the TEK Grace Time. The value of the M&B TEK Grace Time is vendor-specific.

[Add the following in the Table 341]

System	Name	Description	Minimum value	Default value	Maximum value
BS	M&B TEK Grace Time	Time prior to current GTEK expiration BS begins to push new traffic keying material. This time is longer than the TEK Grace Time. This is defined only for the multicast service or the broadcast service	Vendor-specific value	Vendor-specific value	Vendor-specific value

[Add to Table 368a-PKM attribute types:]
11.9 PKM-REQ/RSP management message encodings

Table 368a – PKM attribute types

Type	PKM attribute

41	Key Push Modes
42	Key Push Counter
43	GKEK

[Modify as following text in the Description in section 11.9.3:]
11.9.3 TEK

Description: This attribute contains a quantity that is a TEK key, encrypted with a KEK derived from the AK. The TEK for the multicast service or the broadcast service is the GTEK.

[Modify as following text in the Description in section 11.9.7:]
11.9.3 SAID

Description: This attribute contains a 16-bit SAID used by the Privacy Protocol to identify the SA. The SAID for the multicast service or the broadcast service is the GSAID.

[Modify as following text in the section 11.9.8]
11.9.8 TEK parameters

Description: This attribute is a compound attribute, consisting of a collection of subattributes. These subattributes represent all security parameters relevant to a particular generation of an SAID's TEK. A summary of the TEK-Parameters attribute format is shown below. The GTEK and GKEK are defined only for the multicast service or the broadcast service. The GTEK is the TEK for the multicast service or the broadcast service.

Type	Length	Value(compound)
13	variable	The Compound field contains the subattributes as defined in Table 370

Table 370 – TEK-parameters subattributes

Attributes	Contents
TEK	TEK, encrypted with the KEK GTEK, encrypted with the GKEK
GKEK	Group Key Encryption Key, encrypted with GKEKEK derived from AK
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequence Number
CBC-IV	CBC Initialization Vector

[Insert new sections in the section 11.9:]
11.9.33 Key Push Modes

Description: The field, key push modes, is used to distinguish usage code of the Key Update Command message.

Type	Length	Value
41	1	0, GKEK update mode 1, GTEK update mode 2-255, reserved

The Key Update Command message for the GKEK update mode is to distribute new GKEK to each SS carried on the Primary Management connection. The BS transmits this message before the M&B TEK Grace Time starts.

The Key Update Command message for the GTEK update mode is to distribute new GTEK to all SS carried on the Broadcast connection. The BS transmits this message after the M&B TEK Grace Time starts.

Attributes of Key Update Command message are different according to the value of the Key Push Modes as shown in Table 4.

Table 4 Attribute of Key Update Command message

Attribute	GKEK update mode	GTEK update mode
Key-Sequence-Number	_	_
GSAID	_	_
Key Push Modes	_	_
Key Push Counter	_	_
TEK-Parameters		
> GKEK	_	_
> GTEK	_	_
> Key-Lifetime	_	_
> Key-Sequence-Number	_	_
> CBC-IV	_	_
HMAC/OMAC-Digest	_	_

AK's Key-Sequence-Number, GSAID, Key Push Modes, and HMAC-Digest fields are included in two Key Update Command message regardless of the value of the Key Push Modes. Some subattributes of TEK-Parameters, GKEK and GTEK's Key-Sequence-Number, should be contained in the Key Update Command message for the GKEK update mode. And, GTEK, GTEK's Key-Lifetime, GTEK's Key-Sequence-Number, and CBC-IV should be contained in the Key Update Command message for the GTEK update mode.

11.9.34 Key Push Counter

Description: Key Push Counter is used to protect for replay attack. This value is one greater than (modulo 65536) that of older generation.

Type	Length	Value
42	2	16-bit counter

11.9.35 GKEK (Group Key Encryption Key)

Description: 128-bit GKEK may be randomly generated in a BS or an ASA server. This field is used to encrypt the GTEK for the multicast service or the broadcast service.

Type	Length	Value
43	16	GKEK, encrypted with GKEKEK derived from AK