Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Enhancement of the MBRA for Adaptation to the PKMv2**
Data Submitted	**2005-01-10**

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 contents of the Multicast and Broadcast Rekeying Algorithm to fully adapt to the PKMv2
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 MBRA for Adaptation to the PKMv2

Seokheon Cho, SungCheol Chang, and Chulsik Yoon
ETRI

Introduction

The Key Hierarchical of PKM version 2 (IEEE C802.16e-04/217r1) was accepted last meeting.

So, there is the need for full adaptation of the MBRA to the PKM protocol, such as PKMv1 and PKMv2.

This contribution considers the following.

- Encryption method for the GKEK (Group Key Encryption Key)
- Message authentication keys for the Key Update Command message

Proposed changes

[Modify Table 37k and the last two paragraphs in section 6.3.2.3.9.21 as followings]
6.3.2.3.9.21 Key Update Command messages

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~~ , encrypted with the leftmost 128 bits of 160-bit AK (PKM version 1) , encrypted with the 128-bit GKEKEK derived from AK (PKM version 2)
> 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 cryptographic suite)
OMAC-Digest	Message Digest calculated using OMAC_KEY_D and OMAC_KEY_U (conditional with value of the cryptographic suite)

The Key Update Command message contains only newer generation of key parameters, because this message inform an MSS 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.~~ The GKEK is encrypted with leftmost 128 bits of 160-bit AK for PKM version 1 and the 128-bit GKEKEK derived from AK for PKM version 2. See ~~7.5.4.4~~ 7.5.5.5 for details.

~~The HMAC-Digest attribute~~ One of the HMAC-Digest attribute or the OMAC-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~~ 7.5.5.3 and 7.9.4 for details. In addition, the OMAC-Digest attribute is also derived from the AK for the GKEK update mode and GKEK for the GTEK update mode. See for details.

[Change section 7.5.4.3 as followings]
~~**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.~~

7.5.5.3 Message authentication keys

7.5.5.3.1 HMAC authentication keys

7.5.5.3.1.1 HMAC authentication keys for the PKM version 1

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.

7.5.5.3.1.2 HMAC authentication keys for the PKM version 2

The HMAC authentication keys are derived as follows:

HMAC_KEY_U || HMAC_KEY_D || KEK <= Dot16KDF(Input Key*, SSID || BSID || “HMAC_KEYS+KEK”, 448)

Input Key* is generally the AK. In case of sending the Key Update Command message for the GTEK update mode, however, the Input Key* is the GKEK.

See the key hierarchy for PKMv2 for details.

7.5.5.3.2 OMAC authentication keys

The OMAC Digests are defined only for PKM version 2. The OMAC authentication keys are derived as follows:

OMAC_KEY_U || OMAC_KEY_D || KEK <= Dot16KDF(Input Key*, SSID || BSID || “OMAC_KEYS+KEK”, 384)

Input Key* is generally the AK. In case of sending the Key Update Command message for the GTEK update mode, however, the Input Key* is the GKEK.

See the key hierarchy for PKMv2 for details.

[Change section 7.5.4.4: as followings]
~~**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~~

7.5.5.5 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. The following options for encryption of GKEK may be used. The encryption algorithm is determined according to the value of cryptographic suite. And, the value of cryptographic suite for GKEK encryption is identical to the one for GTEK encryption.

7.5.5.5.1 Encryption of GKEK with 3-DES

This method of encrypting the GKEK shall be used for SAs with the TEK (or GTEK) encryption algorithm identifier in the cryptographic suite equal to 0x01.

The BS encrypts the value fields of the GKEK in the Key Update Command messages (for the GKEK update mode) it sends to client SS. This filed is encrypted using two-key 3-DES in the EDE mode [B42]:

Encryption: $C = E_{k1}[D_{k2}[E_{k1}[P]]]$
Decryption: $P = D_{k1}[E_{k2}[D_{k1}[C]]]$
P = Plaintext 128-bit GKEK
C = Ciphertext 128-bit GKEK
k1 = leftmost 64 bits of the 128-bit Input Key*
k2 = rightmost 64 bits of the 128-bit Input Key*
E [ ] = 56-bit DES ECB mode encryption
D [ ] = 56-bit DES ECB mode encryption

Input Key* is the leftmost 128 bits of the 160-bit AK for PKM version 1. On the contrary, Input Key* is the 128-bit GKEKEK derived from the AK for PKM version 2.

7.5.5.5.2 Encryption of GKEK with RSA

The RSA method of encrypting the GKEK (PKCS #1 v2.1, RSA Cryptography Standard, RSA Laboratories, June 2002) shall be used for SAs with the TEK (or GTEK) encryption algorithm identifier in the cryptographic suite equal to 0x02.

7.5.5.5.3 Encryption of GKEK with ECB mode AES

This method of encrypting the GKEK shall be used for SAs with the TEK (or GTEK) encryption algorithm identifier in the cryptographic suite equal to 0x03.

The BS encrypts the value fields of the GKEK in the Key Update Command messages (for the GKEK update mode) it sends to client SS. This filed is encrypted using 128 bit AES in ECB mode.

Encryption: $C = E_{k1}[P]$
Decryption: $P = D_{k1}[C]$
P = Plaintext 128-bit GKEK
C = Ciphertext 128-bit GKEK
k1 = the 128-bit Input Key*
E [ ] = 128-bit AES ECB mode encryption
D [ ] = 128-bit AES ECB mode encryption

Input Key* is the leftmost 128 bits of the 160-bit AK for PKM version 1. On the contrary, Input Key* is the 128-bit GKEKEK derived from the AK for PKM version 2.

7.5.5.5.4 Encryption of GKEK with AES Key Wrap

This method of encrypting the GKEK shall be used for SAs with the TEK (or GTEK) encryption algorithm identifier in the cryptographic suite equal to 0x04.

The BS encrypts the value fields of the GKEK in the Key Update Command messages (for the GKEK update mode) it sends to client SS. This filed is encrypted using 128 bit AES Key Wrap Algorithm. This 128 bit AES Key Wrap Algorithm is defined only for PKM version 2.

Encryption: $C,I = E_k[P]$
Decryption: $P,I = D_k[C]$
P = Plaintext 128-bit GKEK

C = Ciphertext 128-bit GKEK
k = the 128-bit GKEKEK derived from the AK
$E_k[\ ]$ = AES Key Wrap encryption with key k
$D_k[\ ]$ = AES Key Wrap decryption with key k

[Change section 7.5.5 as followings]
7.5.5 Derivation of TEKs, KEKs, ~~and~~ message authentication keys, and GKEKs

[Modify section 7.9.1: as followings]
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. The GTEK (Group Traffic Encryption Key) is the TEK for multicast or broadcast service. 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. The GSA-ID (Group Security Association Identifier) is the SA-ID for multicast or broadcast service. 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.

An MSS shall be capable of maintaining two successive sets of traffic keying material per authorized GSA-ID. Through operation of its GTEK state machines, an MSS shall check whether it receives new traffic keying material or not. If an MSS get new traffic keying material, then its TEK Grace Time is not operated. However, if it doesn't has that, then an MSS shall request a new set of traffic keying material a configurable amount of time, the TEK Grace Time, before the MSS's latest GTEK is scheduled to expire.

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.

[Modify section 7.9.2 as followings]
7.9.2 Messages

Messages used in the MBRA are the Key Request, Key Reply, and Key Update Command messages.

- Key Request
  An MSS may request the traffic keying material with the Key Request message in the initial GTEK request exchange

procedure or the GTEK refresh procedure.

Refer to subsection 6.3.2.3.9.~~12.~~5.

- Key Reply
  A BS responds to the Key Request message with the Key Reply message including the traffic keying material.
  ~~Two subattributes in TEK-Parameters included in Key Reply message is added to <Table 370 TEK-Parameters subattributes>. Those subattributes are shown in Table 1.~~

~~**Table 133a TEK-Parameters subattributes**~~

~~Attribute~~	~~Contents~~
~~GKEK~~	~~GKEK (Group Key Encryption Key), encrypted by the GKEKEK that is derived from the AK.~~
~~GTEK~~	~~GTEK (Group Traffic Encryption Key), encrypted with the GKEK~~

Key Reply message includes GKEK as well as GTEK. The GTEK is the TEK for the multicast or broadcast service. GKEK and GTEK are encrypted to safely distribute to an SS. GTEK is encrypted with the GKEK for the multicast service or the broadcast service ~~and GKEK is encrypted with the SS's GKEKEK.~~ GKEK is encrypted with the MSS's AK or the MSS's GKEKEK according to the PKM version. See section 7.5.5.5 and section 7.9.3 for details. The lifetime and sequence number of GKEK are identical to ones of GTEK.
This message is carried on the primary management connection.

Refer to subsection 6.3.2.3.9.6.

- Key Update Command
  A BS transmits Key Update Command message to initiate and push newly updated GKEK and GTEK to ~~an SS~~ every SSs served with the specific multicast or broadcast service.

Refer to subsection 6.3.2.3.9.21.
~~Attributes of Key Update Command are shown in Table 2.~~

~~**Table 2 Key Update Command attributes**~~

~~Attribute~~	~~Contents~~
~~Key Sequence Number~~	~~Authorization key sequence number~~
~~GSAID~~	~~Security Association ID~~
~~Key Push Modes~~	~~Usage code of Key Update Command message~~
~~Key Push Counter~~	~~Counter one greater than that of older generation for replay attack~~
~~TEK Parameters~~	~~"Newer" generation of key parameters relevant to GSAID~~
~~> GKEK~~	~~GKEK, encrypted by the GKEKEK that is derived from the 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~~
~~HMAC Digest~~	~~Keyed SHA message digest~~

~~There are two types of Key Update Command message, GKEK update mode and GTEK update mode. Key Push Modes indicates the usage code of Key Update Command message.~~
~~Key Push Counter is used to protect for replay attack. This value is one greater than that of older generation.~~
~~Key Update Command message contains only newer generation of key parameters, because this message inform an SS of next key materials.~~

[Modify section 7.9.3 as followings]
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~~ 7.5.5.5 for details.

[Modify section 7.9.4 as followings]
7.9.4 ~~HMAC~~ Message authentication keys for the Key Update Command message

One of HMAC-Digest attribute or OMAC-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~~ 7.5.5.3 for details.

[Modify Table 370 in the section 11.9.8 as followings]
11.9.8 TEK parameters

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~~ , encrypted with leftmost 128 bits of 160-bit AK (PKM version 1) , encrypted with 128-bit GKEKE derived from AK (PKM version 2)
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequence Number
CBC-IV	CBC Initialization Vector

[Modify the section 11.9.33 as followings]
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~~ following table.

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/OMAC-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.

CBC-IV can be included only when the TEK encryption algorithm identifier in the cryptographic suite equal to 0x01.

One of HMAC-Digest or OMAC-Digest shall be used to authenticate the Key Update Command messages.

[Modify the following table in the section 11.9.35 as followings]
11.9.35 GKEK (Group Key Encryption Key)

Type	Length	Value
43	16	GKEK~~, encrypted with GKEKEK derived from AK~~ , encrypted with the leftmost 128 bits of the 160-bit AK (PKM version 1) , encrypted with the GKEKEK derived from AK (PKM version 2)