Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**MBRA (Multicast & Broadcast Rekeying Algorithm) for PKMv2**
Data Submitted	**2004-06-23**
Source(s)	Seokheon Cho SungCheol Chang Chulsik Yoon, ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea David Johnston, Intel Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr
Re:	TGe
Abstract	The efficient method of rekeying for the multicast service and the broadcast service
Purpose	The document is submitted for review by PKMv2 Working Group and/or 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>.

MBRA (Multicast & Broadcast Rekeying Algorithm) for PKMv2

Seokheon Cho, SungCheol Chang, and Chulsik Yoon
ETRI
David Johnston
Intel

0. Introduction

As I presented the contribution ("IEEE C802.16e-04_23r2") in the Orlando meeting, the current TEK refreshment exchange method for the multicast service and the broadcast service has some problems, such as instantaneously excessive load in a BS, use of unnecessary signaling resources, collision with other SS's bandwidth request code, and no data transmission during key refreshment.

Therefore, we should solve these problems. The summary of my ex-contribution is as follows.

0.1 Summary of ex-contribution (IEEE C802.16e-04-23)

The ex-proposed structure of the TEK management for the multicast service is shown in Figure 0.1.

An SS tries to get the TEK before an SS is served with the specific multicast service. The first TEK distribution procedure is executed by using the Key Request and Key Reply messages that are carried on the primary management connection.

The BS manages the M&B (Multicast & Broadcast) TEK Grace Time for the respective SA-ID in itself. This M&B TEK Grace Time is defined only for the multicast service or the broadcast service in the BS. This parameter means time interval (in seconds) before the estimated expiration of an old distributed TEK. Since the M&B TEK Grace Time is longer than the TEK Grace Time in an SS, the BS starts rekeying for a new TEK earlier than an SS does. The BS shall periodically begin to refresh TEK for the multicast service or the broadcast service at the M&B TEK Grace Time. The BS shall send only one Key Reply message, containing updated TEK, to all SSs being served with the relevant service through not the primary management connection but the broadcast connection.

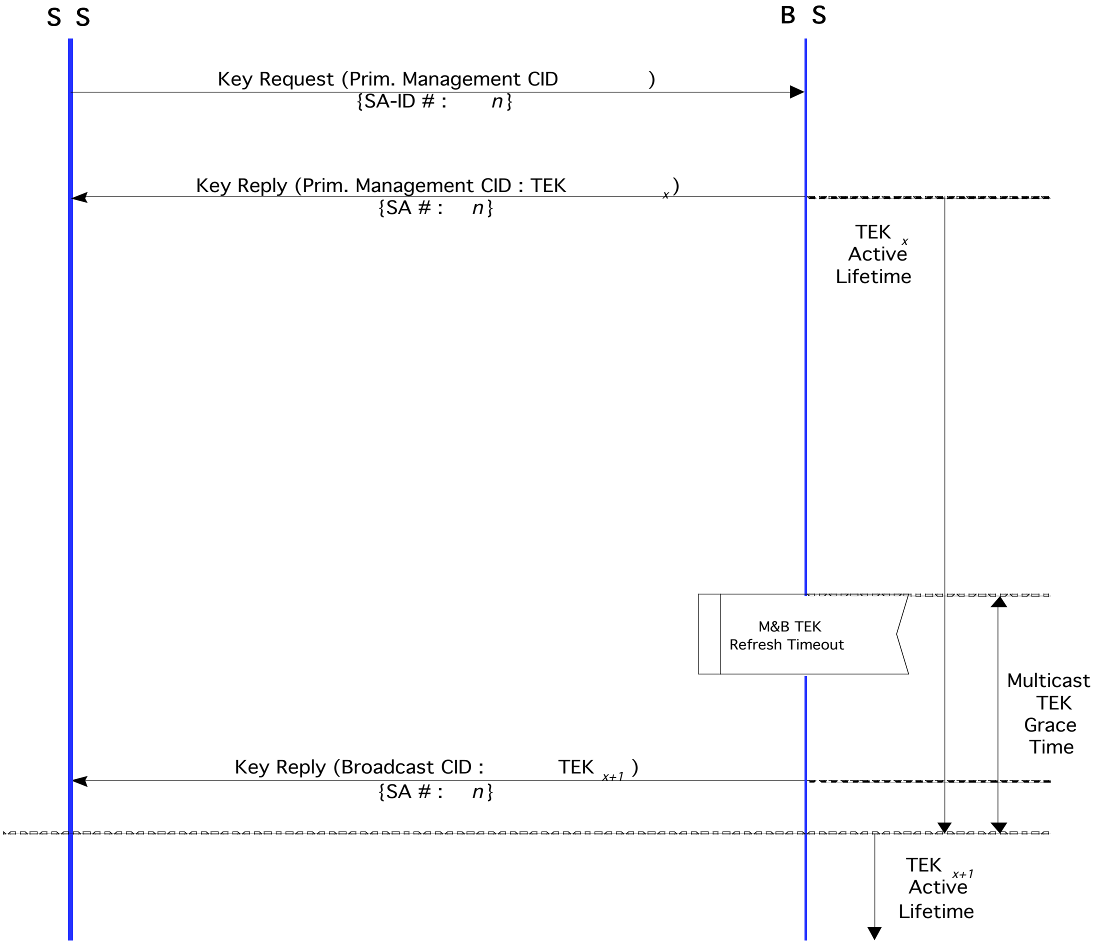

Figure 0.1 TEK management for the multicast and broadcast service

In the sent Key Reply message, the newly updated TEK should be encrypted, because the new TEK itself is safely provided to SSs. Two input keys in the 3-DES are the KEK, when the Key Reply message is carried on the primary management connection. However, two input keys are two old distributed TEKs, when the Key Reply message is carried on the broadcast connection. The common input keys should be used to encrypt the new TEK, because a new identical TEK is transmitted to all served SSs carried on the broadcast connection. In addition, these common input keys should be known to only SSs served with the specific service, because the new encrypted TEKs are transmitted to the authorized SSs as well as the unauthorized SSs for that service. Owing to satisfaction of these requirements, old distributed TEKs for the multicast or broadcast service is proper as the input keys of the 3-DES. The used input key according to connection transmitted the Key Reply message is described as shown in the Table 0.1.

Table 0.1 Used input key according to the transport connection

Connection	Input key
Primary management connection	KEK
Broadcast connection	Old distributed TEK

However, it occurs the chaining problem, because the newly updated TEK is encrypted with the old distributed TEK. In other words, even though an SS knowing the current TEK attempts to delete the specific service, that SS can continuously decode the newly updated TEK and be served with service.

In order solve this chaining problem, I propose new MBRA (Multicast & Broadcast Rekeying Algorithm).

0.2 Summary of new propose MBRA (Multicast & Broadcast Rekeying Algorithm)

An SS tries to get the TEK before an SS is served with the specific multicast service or the broadcast service. The first TEK distribution procedure is executed by using the Key Request and Key Reply messages that are carried on the primary management connection.

The BS manages the M&B (Multicast & Broadcast) TEK Grace Time for the respective SA-ID in itself. This M&B TEK Grace Time is defined only for the multicast service or the broadcast service in the BS. This parameter means time interval (in seconds) before the estimated expiration of an old distributed TEK. That is, the Multicast TEK Grace Time is longer than the TEK Grace Time in an SS.

A BS distributes updated TEK by using two Key Update Command messages around the M&B TEK Grace Time. Those messages are distinguished according to a parameter included in Key Update Command message, “Key Push Modes.”

A BS transmits the first Key Update Command message to each SS served with the specific service before the M&B TEK Grace Time. The first Key Update Command message is carried on the primary management connection. A BS intermittently transmits the first Key Update Command message to each SS in order to reduce the BS’s load for key refreshment. The purpose of the first Key Update Command message is to distribute the GKEK (Group Key Encryption Key). This GKEK is needed to encrypt the newly updated TEK. The GKEK is also encrypted with the SS’s AK. The GKEK can be randomly generated in a BS or an ASA server.
A BS transmits the second Key Update Command message carrying on the broadcast connection after the M&B TEK Grace Time. The aim of the second Key Update Command message is to distribute the TEK. This TEK is encrypted with already transmitted GKEK.

New MBRA mechanism is shown in the Figure 0.2.

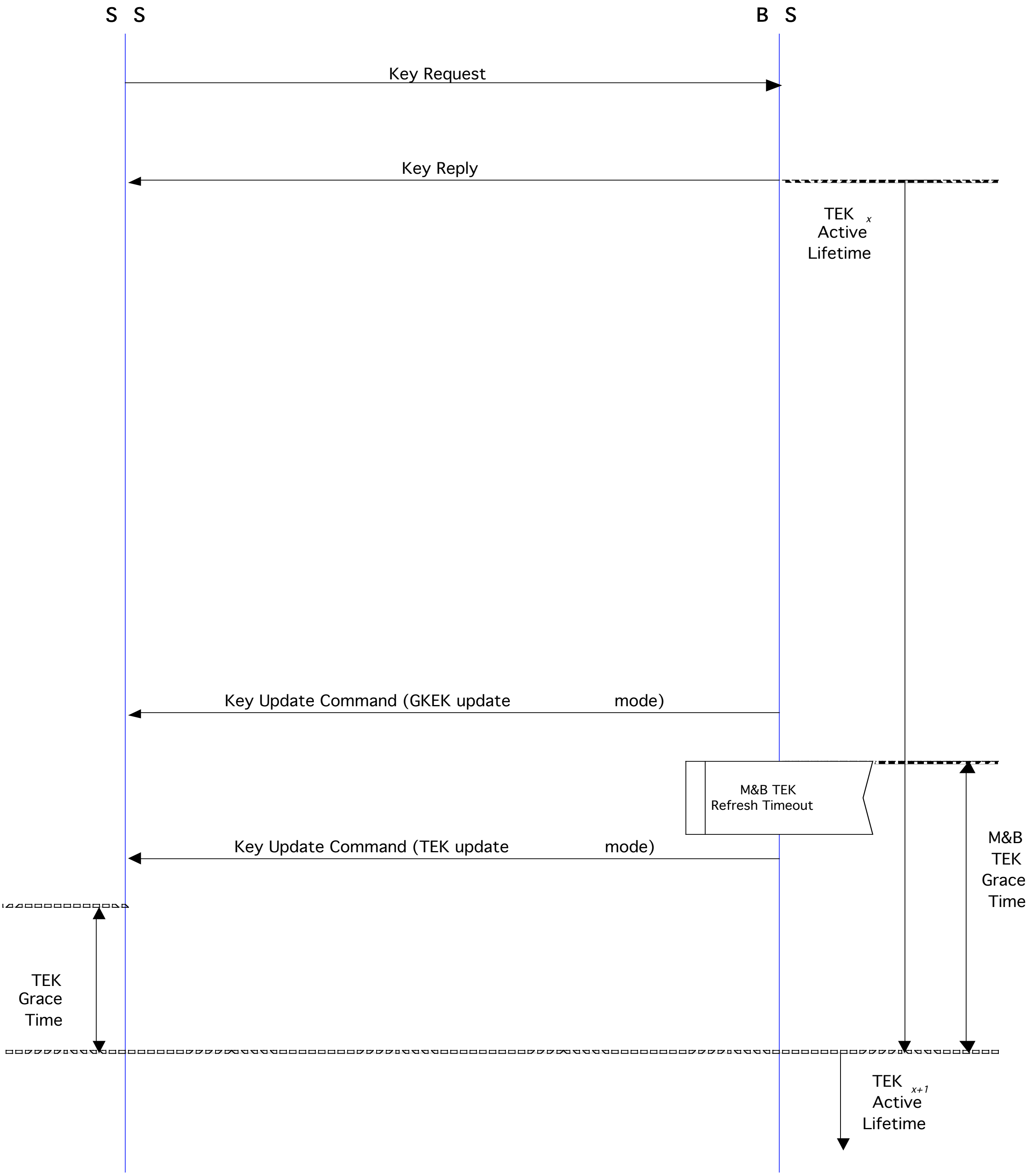

Figure 0.1 TEK management of the MBRA

If an SS doesn't receive at least one of two Key Update Command message, then that SS tries to refresh TEK by sending Key Request message to a BS. A BS responds to Key Request message with Key Reply message. In other words, if an SS doesn't get updated TEK, then the SS' TEK request exchange is executed like the existing key refreshment structure. This abnormal case of the MBRA is described in the Figure 0.3.

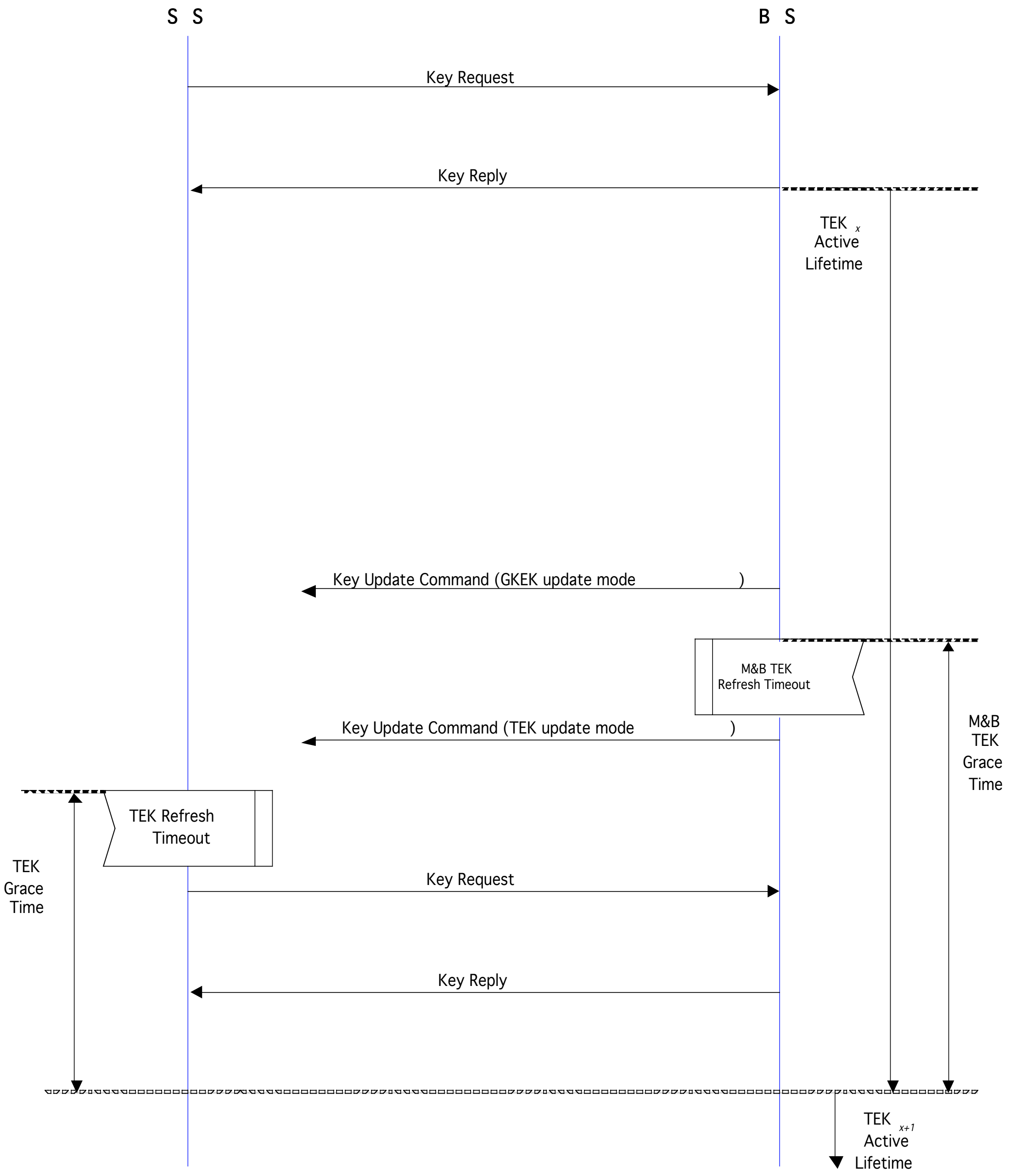

Figure 0.3 Abnormal case of the MBRA

[Insert the following documentation into section 7 and renumber as necessary]

1. MBRA (Multicast & Broadcast Rekeying Algorithm)

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 SS.
- Provide strong protection for the replay attack.

1.1 MBRA Flow

The MBRA overall flow is shown in the Figure 1.

1.1.1 BS usage of GTEK

An SS tries to get the GTEK before an SS is served with the specific 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.

A BS shall be capable of maintaining two successive sets of traffic keying material per authorized GSAID. That is, a BS manages the M&B (Multicast & Broadcast) TEK Grace Time for the respective GSA-ID in itself. Through operation of its M&B TEK Grace Time, a BS shall push a new set of traffic keying material. This M&B TEK Grace Time is defined only for the multicast service or the broadcast service in a BS. This parameter means time interval (in seconds) before the estimated expiration of an old distributed GTEK. That is, the M&B TEK Grace Time is longer than the TEK Grace Time managed in an SS.

A BS distributes updated GTEK by using two Key Update Command messages around the M&B TEK Grace Time, before the already distributed GTEK is expired. Those messages are distinguished according to a parameter included in that message, "Key Push Modes."

A BS transmits the first Key Update Command message to each SS served with the specific service before the M&B TEK Grace Time. The first Key Update Command message is carried on the primary management connection. A BS intermittently transmits the first Key Update Command message to each SS in order to reduce the BS's load for key refreshment. The purpose of the first Key Update Command message is to distribute the GKEK (Group Key Encryption Key). This GKEK is needed to encrypt the updated GTEK. The GKEK is also encrypted with the SS's AK. The GKEK can be randomly generated in a BS or an ASA server.

A BS transmits the second Key Update Command message carrying on the broadcast connection after the M&B TEK Grace Time. The aim of the second Key Update Command message is to distribute the GTEK to the specific service group. This GTEK is encrypted with transmitted GKEK before the M&B TEK Grace Time.

1.1.2 SS usage of GTEK

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

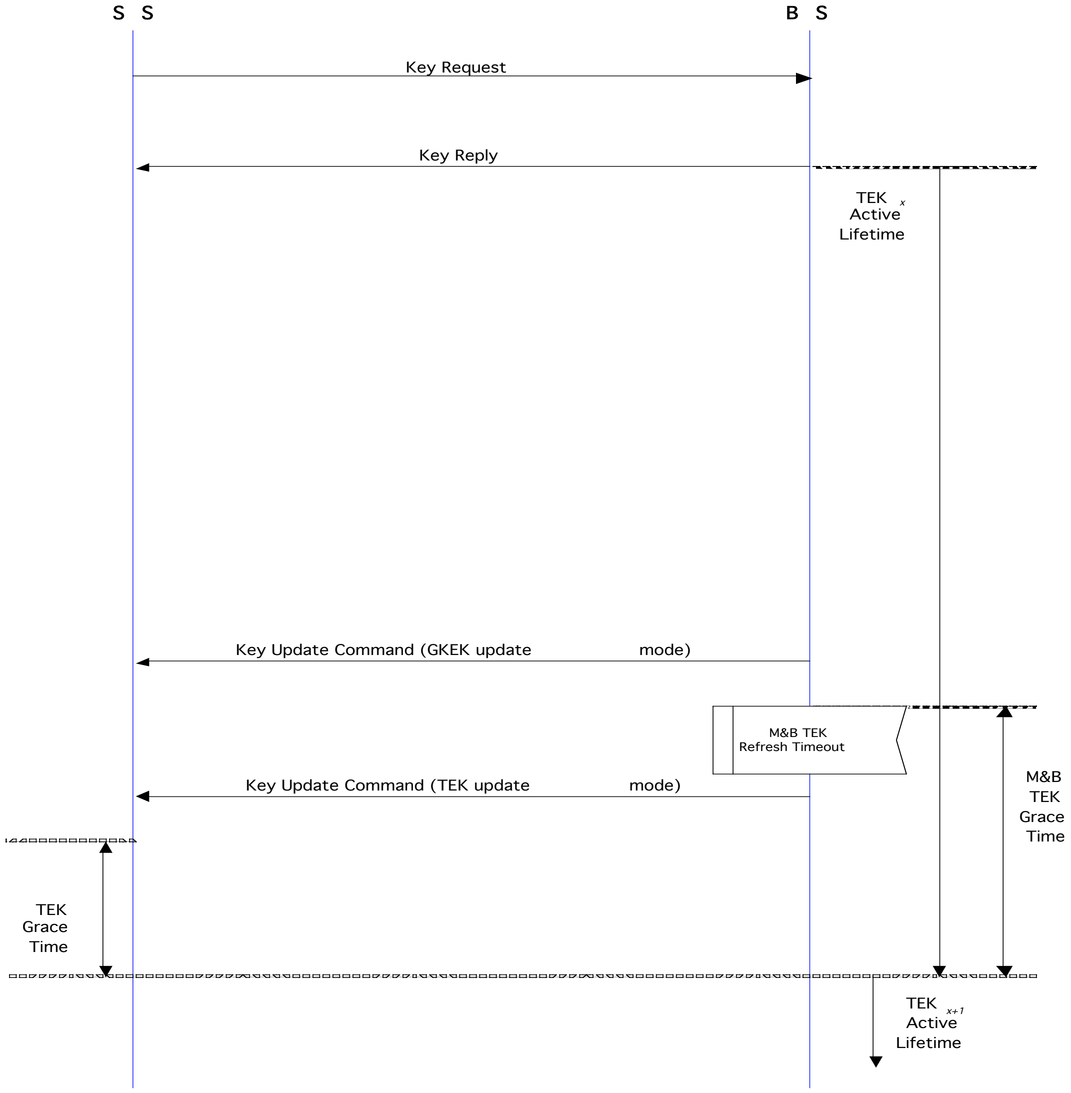

Figure 1 MBRA management

1.2 Messages

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

- Key Request
  Refer to subsection 6.3.2.3.9.11.

- Key Reply
  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 1 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. 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. The lifetime and sequence number of GKEK are identical to ones of GTEK.
This message is carried on the primary management connection.

- Key Update Command
  A BS transmits Key Update Command message to initiate and push newly updated GKEK and GTEK to an SS.
  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.

1.3 Attributes of Key Update Command message

1.3.1 Key Push Modes

The field, key push modes, is used to distinguish usage code of Key Update Command message
This parameter is shown in Table 3

Table 3 Key Push Modes

Type	Length	Value
30	1	0, GKEK update mode (1st Key Update Command message) 1, GTEK update mode (2nd Key Update Command message) 2-255, reserved

The first Key Update Command message is to update GKEK to each SS carried on the primary management connection. The Key Push Modes' value of the first Key Update Command message is "GKEK update mode, 0."
The second Key Update Command message is to update GTEK to all SS carried on the broadcast connection. The Key Push Modes' value of the second Key Update Command message is "GTEK update mode, 1."

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

Table 4 Attribute of Key Update Command message

Attribute	GKEK update mode 1st Message (Primary)	GTEK update mode 2nd Message (Broadcast)
Key-Sequence-Number	_	_
GSAID	_	_
Key Push Modes	_	_
Key Push Counter	_	_
TEK-Parameters		
> GKEK	_	_
> GTEK	_	_
> Key-Lifetime	_	_
> Key-Sequence-Number	_	_
> CBC-IV	_	_
HMAC-Digest	_	_

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

1.3.2 Key Push Counter

Key Push Counter is used to protect for replay attack. This value is one greater than (modulo 65536) that of older generation.
This parameter is shown in Table 5.

Table 5 Key Push Counter

Type	Length	Value
30	2	16-bit counter

1.3.3 Used input key for HMAC-Digest

HMAC-Digest attribute is used for Key Update Command message authentication.
Input key used to generate HMAC-Digest of Key Update Command message is different according to Key Push Modes as shown in Table 6.

Table 6 Input key of the HMAC-Digest

Key push modes	Input Key
GKEK update mode	KEK, derived from AK
GTEK update mode	GKEK

1.3.4 GKEK (Group Key Encryption Key)

128-bit GKEK may be randomly generated in a BS or an ASA server.
This field is shown in Table 7.

Table 1 GKEK

Type	Length	Value
31	20	GKEK, encrypted with AK

1.4 Encryption of GKEK

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 SS 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