Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Corrections for the MBRA**
Data Submitted	**2006-09-21**
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 Std 802.16e-2005
Abstract	The contents of the Multicast and Broadcast Rekeying Algorithm to fully adapt to the PKMv2
Purpose	Adoption of proposed changes into IEEE Std 802.16e-2005
Notice	
Release	
Patent Policy and Procedures	

Corrections for the MBRA

Seokheon Cho, SungCheol Chang, and Chulsik Yoon

ETRI

Introduction

A commentary (# 5144) which was made a resolution at the TGe Chicago June meeting was accepted. The corresponding contribution is the IEEE C802.16e-05/278, "Clarification of GKEK-related Parameters for the MBRA."

The main idea of that contribution is that the GKEK lifetime is different from the GTEK lifetime in order to use radio resource more efficiently. By increasing the GKEK lifetime, the transmission number of the PKMv2 Group-Key-Update-Command message for the GKEK update mode is decreased. On the contrary, by decreasing the GTEK lifetime, the update number of the GTEK is increased. Hence, there are advantages that the security level for the GTEK is stronger and the radio resource used to update the GKEK and the GTEK is decreased.

However, the existing contents of section 7.9 are based that the GKEK lifetime is equal to the GTEK lifetime.

Therefore, it is necessary to change the existing contents so that the MBRA can operate well with the independent GKEK lifetime from the GTEK lifetime.

Proposed changes

[Change section 7.9: as follows]

7.9 ~~Optional multicast~~ Multicast and broadcast rekeying algorithm (MBRA)

When MBRA is supported, the MBRA shall be used to refresh traffic keying material efficiently not for the unicast service, but for the multicast service, ~~or~~ the broadcast service, or the MBS.

[Change section 7.9.1: as follows]

7.9.1 MBRA Flow

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

An SS may get the traffic keying material before an MSS is served with the specific multicast service, ~~or~~ the broadcast service, or the MBS. The initial GTEK request exchange procedure is executed by using the PKMv2 Key-Request and PKMv2 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 SS shares the traffic keying material with a BS, an SS doesn't need to request the new traffic keying material. A BS updates and distributes the traffic keying material periodically by sending two PKMv2 Group-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, or the MBS. 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 SS.

A BS distributes updated traffic keying material by sending two PKMv2 Group-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 PKMv2 Group-Key-Update-Command message.

A BS transmits the PKMv2 Group-Key-Update-Command message for the GKEK update mode in order to distribute the new GKEK. Moreover, a BS transmits the PKMv2 Group-Key-Update-Command message for the GTEK update mode in order to distribute the new GTEK.

In general, the GKEK lifetime corresponds to the **n** (integer being bigger than 1) times of the GTEK lifetime. That is, the GKEK shall be updated once while the GTEK is updated *n* times.

A BS transmits the PKMv2 Group-Key-Update-Command message for the GKEK update mode to each SS served with the specific multicast service or the broadcast service before the current GKEK expires and the last M&B TEK Grace Time of the corresponding current GKEK starts. The purpose of the Key Update Command message for the GKEK update mode is to distribute the GKEK (Group Key Encryption Key). The PKMv2 Group-Key-Update-Command message for the GKEK update mode is carried on the Primary Management connection. A BS intermittently transmits the PKMv2 Group-Key-Update-Command message for the GKEK update mode to each SS 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 a network entity (i.e., an ASA server or an MBS server).

A BS transmits the PKMv2 Group-Key-Update-Command message for the GTEK update mode carrying on the Broadcast connection after the each M&B TEK Grace Time starts. The aim of the PKMv2 Group-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 randomly generated in the same node which generates the GKEK and encrypted with already transmitted GKEK.

An SS shall be capable of maintaining two successive sets of traffic keying material per authorized GSA-ID. 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 at a configurable amount of time, the TEK Grace Time, before the SS's latest GTEK is scheduled to expire.

If an SS receives the valid two PKMv2 Group-Key-Update-Command messages and shares new valid GKEK and GTEK with a BS, then that SS doesn't need to request a new set of traffic keying material.

If an SS doesn't receive at least one of two PKMv2 Group-Key-Update-Command messages, then that SS sends the PKMv2 Key-Request message to get a new traffic keying material. A BS responds to the PKMv2 Key-Request message with the PKMv2 Key-Reply message. In other words, if an SS doesn't get valid new GKEK or GTEK, then the GTEK request exchange procedure initiated by a SS shall be ~~is executed~~ shall be performed.

[Delete Figure 137d and add the following figure as the Figure 137d]

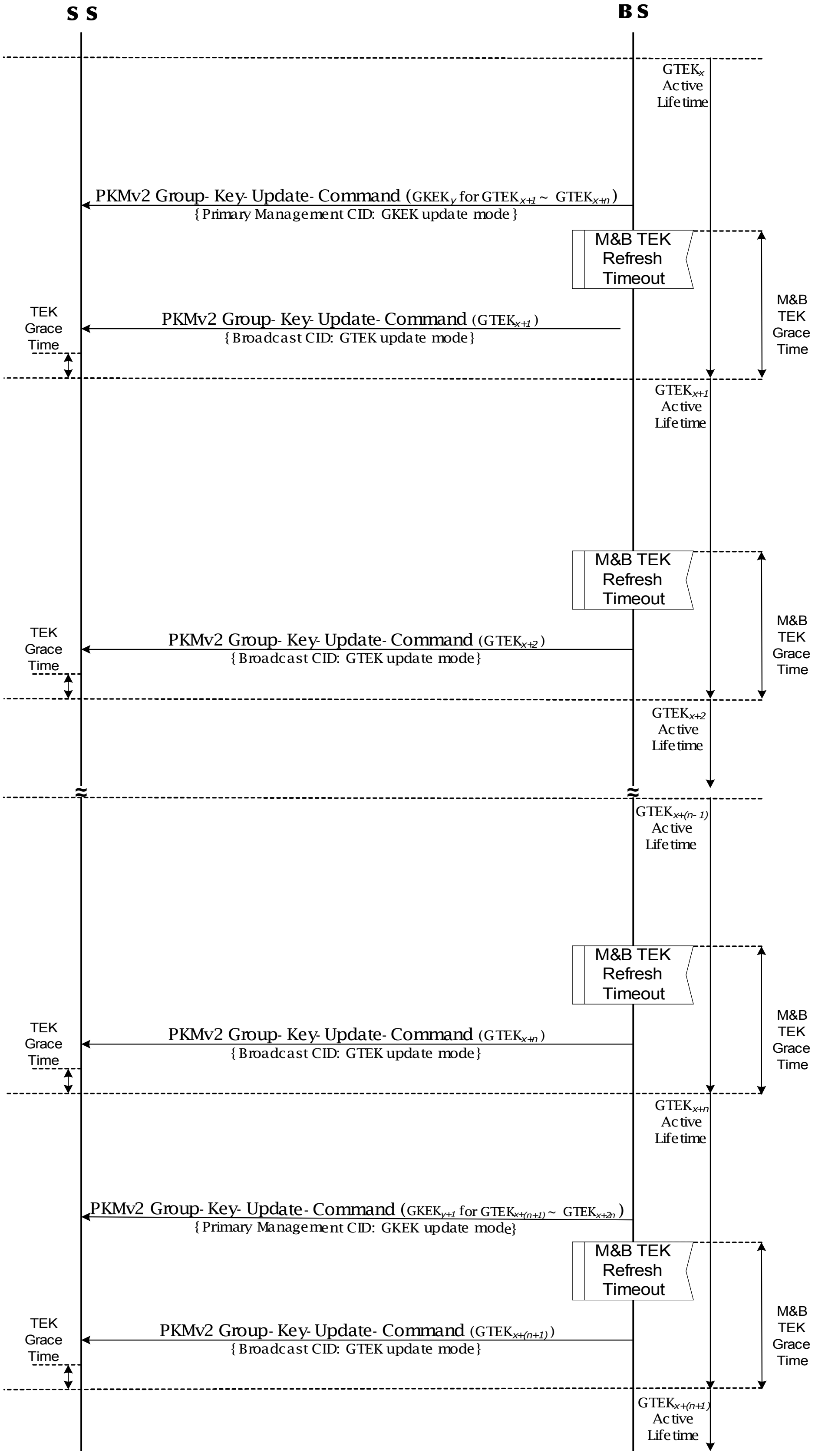
S S
B S
GTEK$_x$ Active Lifetime
PKMv2 Group-Key-Update-Command (GKEK$_y$ for GTEK$_{x+1}$ ~ GTEK$_{x+n}$)
{Primary Management CID: GKEK update mode}
M&B TEK Refresh Timeout
TEK Grace Time
PKMv2 Group-Key-Update-Command (GTEK$_{x+1}$)
{Broadcast CID: GTEK update mode}
M&B TEK Grace Time
GTEK$_{x+1}$ Active Lifetime
M&B TEK Refresh Timeout
TEK Grace Time
PKMv2 Group-Key-Update-Command (GTEK$_{x+2}$)
{Broadcast CID: GTEK update mode}
M&B TEK Grace Time
GTEK$_{x+2}$ Active Lifetime
≈
≈
GTEK$_{x+(n-1)}$ Active Lifetime
M&B TEK Refresh Timeout
TEK Grace Time
PKMv2 Group-Key-Update-Command (GTEK$_{x+n}$)
{Broadcast CID: GTEK update mode}
M&B TEK Grace Time
GTEK$_{x+n}$ Active Lifetime
PKMv2 Group-Key-Update-Command (GKEK$_{y+1}$ for GTEK$_{x+(n+1)}$ ~ GTEK$_{x+2n}$)
{Primary Management CID: GKEK update mode}
M&B TEK Refresh Timeout
TEK Grace Time
PKMv2 Group-Key-Update-Command (GTEK$_{x+(n+1)}$)
{Broadcast CID: GTEK update mode}
M&B TEK Grace Time
GTEK$_{x+(n+1)}$ Active Lifetime

Figure 137d-MBRA Management Flow

[Change section 7.9.1.1: as follows]

7.9.1.1 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 PKMv2 Key-Request and PKMv2 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, when GKEK has been changed 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 PKMv2 Group-Key-Update-Command messages when the current GKEK is about to expire ~~has been changed~~, or by using ~~one (the second)~~ PKMv2 Group-Key-Update-Command message for the GTEK update mode ~~otherwise, around the M&B TEK Grace Time starts,~~ after the M&B TEK Grace Time starts and ~~before the already distributed GTEK is expired~~ before the current GTEK expires. Those messages are distinguished according to a parameter included in that message, “Key Push Modes.”

A BS transmits the ~~first~~ PKMv2 Group-Key-Update-Command message for the GKEK update mode to each SS served with the specific service before the current GKEK expires and the last M&B TEK Grace Time of the corresponding current GKEK starts. The ~~first~~ PKMv2 Group-Key-Update-Command message for the GKEK update mode is carried on the primary management connection. A BS intermittently transmits the ~~first~~ PKMv2 Group-Key-Update-Command message for the GKEK update mode to each SS in order to reduce the BS’s load for key refreshment. The purpose of the ~~first~~ PKMv2 Group-Key-Update-Command message for the GKEK update mode 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 KEK. The GKEK may be randomly generated in a BS or a network entity (i.e., an ASA server or an MBS server).

A BS transmits the PKMv2 Group-Key-Update-Command message for the GTEK update mode carried on the broadcast connection after the M&B TEK Grace Time. The aim of the ~~second~~ PKMv2 Group-Key-Update-Command message for the GTEK update mode is to distribute the GTEK to the specific service group. ~~This GTEK is encrypted with transmitted GKEK before the M&B TEK Grace Time.~~ This GTEK is encrypted with the GKEK identified by the associated GKEK sequence number. The associated GKEK sequence number is included in the GTEK-Parameters attribute.

[Change section 7.9.1.2: as follows]

7.9.1.2 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 does not have that, then an SS shall request a new set of traffic keying material at a configurable amount of time, the TEK Grace Time, before the SS's latest GTEK is scheduled to expire.

[Change section 7.9.2: as follows]

7.9.2 Messages

Messages used in the MBRA are the PKMv2 Key-Request, PKMv2 Key-Reply, and PKMv2 Group-Key-Update-Command messages.

- PKMv2 Key-Request
  An SS may request the traffic keying material with the PKMv2 Key-Request message in the initial GTEK request exchange procedure or the GTEK refresh procedure. Refer to 6.3.2.3.9.~~5~~.21.
- PKMv2 Key-Reply
  A BS responds to the PKMv2 Key-Request message with the PKMv2 Key-Reply message including the traffic keying material. PKMv2 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 distributed to an SS.GTEK is encrypted with the GKEK for the multicast service or the broadcast service. The GKEK is encrypted with the KEK. See 7.5.4.5.2 and 7.9.3 for details. This message is carried on the primary management connection. Refer to 6.3.2.3.9.~~6~~.22.
- PKMv2 Group-Key-Update-Command
  A BS transmits PKMv2 Group-Key-Update-Command message to initiate and push newly updated GKEK and GTEK to every SSs served with the specific multicast or broadcast service.