Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Corrections for PKMv2 Group-Key-Update-Command Message**
Data Submitted	**2006-09-21**
Source(s)	Seokheon Cho 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	This contribution provides a resolution for technical problems in the PKMv2 Group-Key-Update-Command message.
Purpose	Adoption of proposed changes into IEEE Std 802.16e-2005
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>.

Corrections for PKMv2 Group-Key-Update-Command Message

Seokheon Cho and Chulsik Yoon

ETRI

Introduction

There are several technical problems in the definition of the PKMv2 Group-Key-Update-Command message.

1. According to the value of Key Push Modes sub-field (refer to sub-clause 11.9.28), the Key-Sequence-Number included in the PKMv2 Group-Key-Update-Command message may be AK sequence number or GKEK sequence number.

2. The PKMv2 Group-Key-Update-Command message may be transmitted to refresh the MBS-related keys.

Proposed Changes to IEEE Std 802.16e-2005

[Change sub-clauses 6.3.2.3.9.26 as follows]

6.3.2.3.9.26 PKMv2 Group-Key-Update-Command message

This message is sent by BS to refresh and push ~~the GTEK and/or GKEK parameters~~ the GKEK-related parameters (for GKEK update mode) or the GTEK-related parameters (for GTEK update mode) to MSs served with the specific multicast service, ~~or~~ broadcast service, or MBS.

Code: 28

Attributes are shown in Table 37p.

Table 37p PKMv2 Group-Key-Update-Command attributes

Attribute	Contents
Key-Sequence-Number	AK sequence number, for GKEK update mode GKEK sequence number, for GTEK update mode
GSAID	Security Association ID
Key Push Modes	Usage code of PKMv2 Group-Key-Update Command message
Key Push Counter	Counter one greater than that of older generation
GTEK-Parameters	“Newer” generation of GTEK-related parameters relevant to GSAID. The GTEK-Parameters is the TEK-Parameters for multicast, ~~or~~ broadcast service, or MBS.
GKEK-Parameters	“Newer” generation of GKEK-related parameters for multicast, ~~or~~ broadcast service, or MBS.
HMAC/CMAC-Digest	Message integrity code of this message

Key Sequence Number is the sequence number of the ~~synchronized~~ shared AK (Authorization Key) between an MS and a BS in this message for GKEK update mode. Key Sequence number is the GKEK sequence number in this message for GTEK update mode.

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 a PKMv2 Group-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~~ broadcast service, or MBS. Key Push Modes indicates this usage code of the PKMv2 Group-Key-Update-Command message. The PKMv2 Group-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 PKMv2 Group-Key-Update-Command message shall not be used according this Key Push Modes attribute's value. See 11.9~~.33~~.28 for details.

Key Push Counter is used to protect for replay attack. This value is one greater than that of older generation. If the CMAC-Digest is included in this message, then Key Push Counter may not be included.

A PKMv2 Group-Key-Update-Command message contains only newer generation of key parameters, because this message informs an MS of ~~next traffic~~ key material to be used for next lifetime. The GTEK-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 GTEK, the GTEK's remaining key lifetime, the GTEK's key sequence number, the associated GKEK 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~~ a network entity (i.e., an ASA server or an MBS server). The GKEK should be identically shared within the same multicast group, ~~or~~ broadcast service group, or MBS group. The GTEK is encrypted with GKEK for the multicast, ~~or~~ broadcast service, or MBS. GKEK parameters contain the GKEK encrypted by the KEK, ~~and~~ GKEK lifetime, and GKEK sequence number. See 7.5.4~~.4~~.5 for details.

The HMAC/CMAC-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 PKMv2 Group-Key-Update-Command message. The HMAC/CMAC-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~~ 7.2.2.2.9 for details.