Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**The MBRA for the MBS**
Data Submitted	**2005-06-08**

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 P802.16e/D8
Abstract	The existing PKMv2 is somewhat unorganized and insecure security framework. This contribution provides a resolution for the efficient keying distribution for the MBS service.
Purpose	Adoption of proposed changes into P802.16e/D8

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>.

The MBRA for the MBS

Seokheon Cho, Sungcheol Chang, and Chulsik Yoon

ETRI

Introduction

0.1 IEEE P802.16e/D8 Status and Problems

Even though the MBS is defined, the keying distribution method for the encryption of the MBS traffic data is not defined.

There are several keys for the MBS, e.g., MAK (MBS Authorization Key), MGTEK (MBS Group Traffic Encryption Key), and MTK (MBS Transport Key).

The MAK may be generated and transported from the MBS application layer.

The MGTEK is used to derive the MTK, but the generation and transport methods of this key are not defined. Therefore, that method needs to be obviously specified.

In addition, the MTK used to encrypt the MBS traffic data is defined in the IEEE P802.16e/D7 as follows.

MTK <= Dot16KDF(MAK, MGTEK, 128)

The current derivation method for the MTK is not related to the SS's AK (Authorization Key). Since the MTK should be transmitted to the only authorized SS, the MTK should have relationship with the AK. It is reasonable that the MTK should be derived from a child key of the AK, such as the GTEK.

0.2 Proposed Solutions

Both an SS and BS have to share a new specific key, e.g., the MTK, to be used for encrypting the MBS traffic data. An SS shall send the Key-Request message to derive the MTK. A BS shall respond to the requesting SS with a PKMv2 Key Reply message. By exchanging these two messages, an SS can get a GTEK to be used for the derivation of the MTK. The MGTEK doesn't need any more.

In addition, the wrong current derivation method for the MTK shall be changed as follows:

MTK <= Dot16KDF(MAK, GTEK, 128)

Proposed Changes into IEEE P802.16e/D8

[Modify sub-clause 7.2.2.2.8 as follows:]

7.2.2.2.8 MBS Transport Key (MTK)

The generation and transport of the MAK (MBS AK) is outside the scope of the 802.16 standard. It is provided through means defined at higher layers. However the ~~keying~~ key such as the MTK is used in the link cipher, therefore its existence needs to be defined in layer 2.

The MTK is used to ~~protect MBS data~~ encrypt the MBS traffic data. It is defined as follows:

~~MTK <= Dot16KDF(MAK, MGTEK, 128)~~
MTK <= Dot16KDF(MAK, GTEK, 128)

The GTEK is the TEK for the MBS. An SS can get the GTEK by exchanging the PKMv2 Key Request message and the PKMv2 Key Reply message with a BS or receiving the PKMv2 Group Key Update Command message from a BS. The generation and transport of the GTEK is defined as in section 6.3.2.3.9 and 7.9.