Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**CBC Mode and Initial Vector for the AES algorithm**	
Data Submitted	**2004-11-04**	
Source(s)	Sungcheol Chang Jaesun Cha Seokheon Cho Chulsik Yoon ETRI 161, Gajeong-dong, Yuseong-Gu, Daejeon, 305-350, Korea	Voice: +82-42-860-5456 Fax: +82-42-861-1966 scchang@etri.re.kr chosh@etri.re.kr jscha@etri.re.kr
Re:	This is a response to Sponsor Ballot 16e on P802.16e/D5..	
Abstract	The document contains suggestions on the changes in IEEE P802.16e-D1 that would support efficient key management method for the multicast service.	
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>.	

CBC Mode and Initial Vector for the AES algorithm

Sungcheol Chang, Jaesun Cha, Seokheon Cho and Chulsik Yoon
ETRI

Introduction

The US Advanced Encryption Standard (AES) algorithm [NIST Special Publication 800-38-C, FIPS-197] is generally adopted as a data encryption algorithm.

In the IEEE 802.16d/D5 the CCM mode is used to encrypt and authenticate MAC PDUs. The MAC PDU payload shall be prepended with a 4 byte PN (Packet Number), which is not encrypted. Both the initial block and the counter blocks consist of the PN and the GMH excluding the HCS.

In the IEEE 802.16e/D5 the CTR mode is generally described, principally to support MBS services. MBS contents are made independent of BSs. The MAC PDU payload shall be prepended with a 4 byte nonce, which is not encrypted. The 4 byte nonce is repeated 4 times to construct the 16 byte input nonce used in the CTR mode operation.

Both the CCM mode and the CTR mode of the AES require a 4 byte field to be followed by the MAC PDU payload. This nonce field, which is not the MAC PDU payload, reduces data efficiency.

Overview of Proposed Solution

Figure 1 shows the functionality of the CBC mode in which the plain text (PT) are encrypted to the cipher text (CT) with the inputs of both TEK and IV. In the IEEE 802d/D5 the DES algorithm may be used as block cipher algorithm. This contribution contains the CBC mode and IV generation for the AES algorithm.

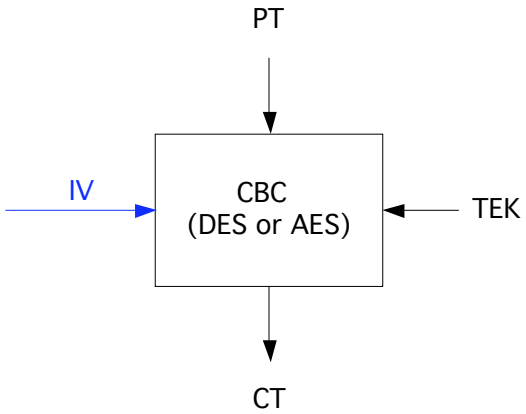
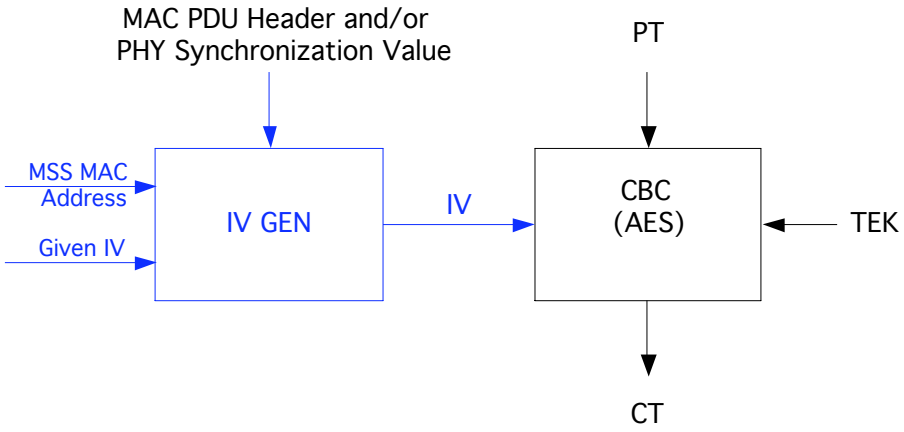


Figure 1 : Encryption in the CBC Mode.

The Cipher Block Chaining (CBC) mode of the AES algorithm requires different Initial Vectors (IVs) every MAC PDUs. If a IV value are used to encrypt the PT of a MAC PDU, the same IV must be used to decrypt the CT of the MAC PDU. To generate IVs every MAC PDUs, both the MAC header and the PHY Synchronization field are considered as input parameters. These input parameters may be changed every MAC PDUs. Also the MAC address and the given IV described at the PKM procedure, are used to add user-specific functionality. The IV generation per MAC PDU can reduce a 4 byte nonce field to be followed by the MAC PDU payload in both the CCM mode and the CTR mode.



IV = (MAC PDU Header (6 bytes)+PHY Synchronization Value (4 bytes)+MSS MAC Address (6 bytes))
XOR Given IV (16 bytes)

Figure 2 : IV Generation and Encryption.

If in HARQ operation the MAC PDU is decoded from several channel coded blocks transmitted through different frames, the MAC PDU payload must be decrypted with the IV value which are generated from the PHY Synchronization value when spid=0.

Proposed changes to IEEE 802.16e/D5

[Add section 7.8.2.3 in page 149 as follows]

7.8.2.3 Data encryption with AES in CBC mode

If the data encryption algorithm identifier in the cryptographic suite of an SA equals 0x03, data on connections associated with that SA shall use the CBC mode of the US Advanced Encryption Standard (AES) algorithm [NIST Special Publication 800-38C, FIPS 197] to encrypt the MAC PDU payloads.

7.8.2.3.1 CBC IV generation
The CBC IV shall be calculated with the exclusive-or (XOR) of (1) the IV parameter included in the TEK keying information, and (2) the 128-bits content which is a concatenation of the 48-bit MAC PDU Header, the 32-bit PHY Synchronization value of the MAP that a data transmission occurs, and the 48-bit MSS MAC address.

The CBC IV shall be updated every MAC PDUs.

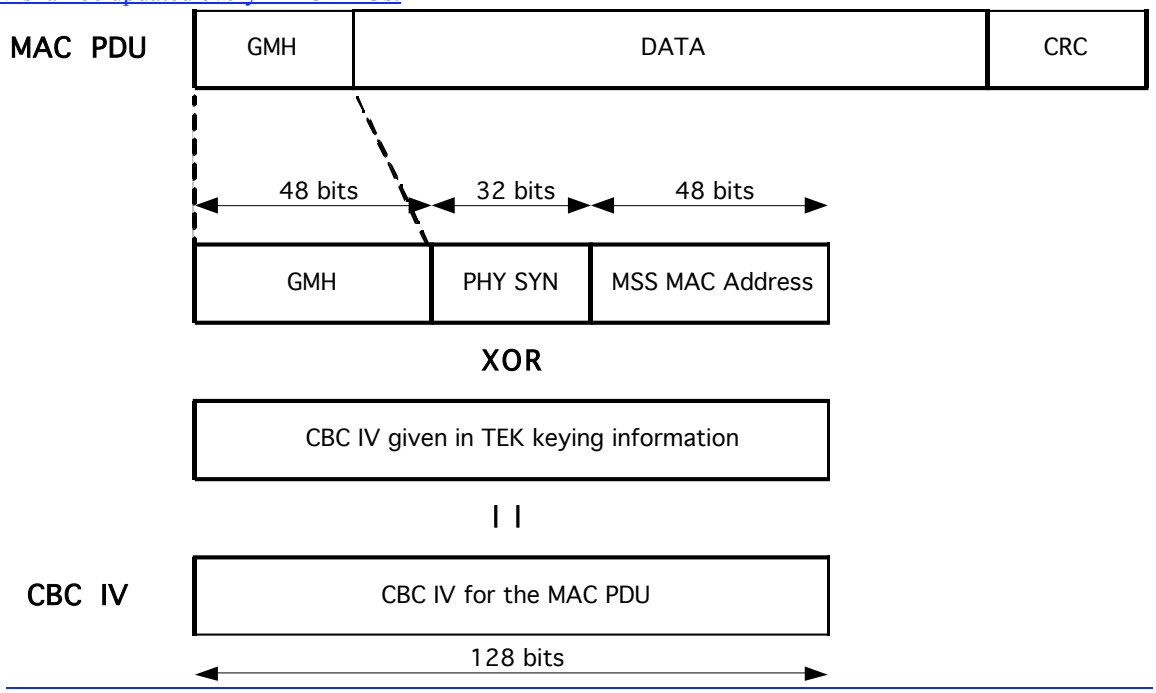


Figure xxx – CBC IV generation.

If the MAC PDU is decoded from several channel coded blocks transmitted at different frames in HARQ operation, the MAC PDU payload must be decrypted with the CBC IV value which are generated from the PHY Synchronization value of the MAP when spid=0.

[Modify text to section 11.9.8 in pages 295-296 as follows]

11.9.8 TEK parameters

The CBC-IV attribute is required when the data encryption algorithm identifier in the SA ciphersuite is 0x01 (DES in CBC mode) or 0x03 (AES in CBC mode).

The CBC-IV attribute is not required when the data encryption algorithm identifier in the SA ciphersuite is 0x02 (AES).

[Modify text to section 11.9.14 in pages 296-297 as follows]

11.9.14 Cryptographic suite

Table 373 - Data encryption algorithm identifiers

Value	Description
0	No data encryption

1	CBC-Mode, 56-bit DES
2	CCM-Mode, 128-bit AES
3	CBC-Mode, 128-bit AES
127	CTR-Mode 128 bits AES for MBS with 32 bits Nonce
3-126 & 128-255	Reserved

Table 374a - Data authentication algorithm identifiers

Value	Description
0	No data authentication
1	CCM-Mode, 128-bit AES
2-255	Reserved

Table 375a – TEK encryption algorithm identifiers

Value	Description
0	Reserved
1	3-DES EDE with 128-bit key
2	RSA with 1024-bit key
3	ECB mode AES with 128-bit key
4-255	Reserved

Table 376a – Allowed cryptographic suites

Value	Description
0x000001	No data encryption, no data authentication & 3-DES, 128
0x010001	CBC-Mode 56-bit DES, no data authentication & 3-DES, 128
0x000002	No data encryption, no data authentication & RSA, 1024
0x020002	CBC-Mode 56-bit DES, no data authentication & RSA, 1024
0x020103	CCM-Mode 128-bit AES, CCM-Mode, 128-bit AES, ECB mode AES with 128-bit key
0x030003	CBC-Mode 128-bit AES, no data authentication, ECB mode AES with 128-bit key
0x800003	MBS CTR Mode 128 bits AES with 32 bits nonce, no data authentication, AES ECB mode AES with 128-bit key
All remaining values	Reserved