Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>	
Title	**Data Encryption and PDU format using AES-CCM**	
Date Submitted	**2008-09-05**	
Source(s)	Masato Okuda, Yanling Lu and Wei-Peng Chen Fujitsu	E-mail: okuda@jp.fujitsu.com *<http://standards.ieee.org/faqs/affiliationFAQ.html>
Re:	Security: MAC; in response to the IEEE 802.16m-08/033, Call for Contributions and Comments on Project 802.16m System Description Document (SDD)"	
Abstract	To propose Payload format and Nonce construction in AES-CCM.	
Purpose	To propose Payload format and Nonce construction in AES-CCM to the 802.16m SDD	
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups.* It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who 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	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.	

Data Encryption and PDU format using AES-CCM

Masato Okuda, Yanling Lu and Wei-Peng Chen
Fujitsu

Introduction

This contribution proposes a new Nonce definition and PDU payload format for AES-CCM mode.

Figure 1 shows the encrypted payload format in AES-CCM mode specified in the current 16e standard.

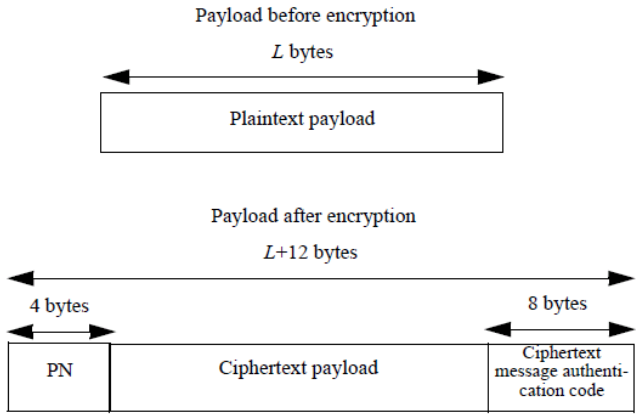

Figure 1 Encrypted Payload format in AES-CCM mode (Figure 170 in Rev2/D6)

In the figure, any PN (Packet Number) value shall not be used more than once for a given encryption key (TEK). And PN (Packet Number) is used as a part of Nonce in CCM algorithm in the 16e. And

Figure 2 shows Nonce (13-byte) construction using PN.

Byte number	0 4	5 8	9 12
Field	Generic MAC header	*Reserved*	PN
Contents	Generic MAC header omitting HCS	0x00000000	PN field from payload

Figure 2 Nonce construction (Figure 171 in Rev2/D6)

As shown in the figure 1, each encrypted PDU payload contains 4-byte long PN even if payload length is very small. Therefore, overhead due to PN is not negligible.

Proposed Scheme

Principle rule of Nonce is that a Nonce value shall not be used more than once for a given encryption key. To ensure this rule, Packet Number is used in the 16e. However we can use any other values for encryption as long as principle rule of Nonce is ensured.

So, we propose to use ‘Frame Number’ and ‘PDU index’ as a part of Nonce instead of Packet Number to omit PN.

Figure 3 shows the proposed Nonce Construction.

There is no need to attach ‘Frame Number’ and ‘PDU index’ to each PDU, because the sender and the receiver of a PDU can identify those information related to the PDU.

AS a result, we can omit PN from the legacy PDU.

Figure 4 shows the proposed Encrypted Payload format in AES-CCM.

Byte Number	0 - 4	5 – 7	8	9-11	12
Field	Generic MAC header	*Reserved*	Frame Number Iteration	Frame Number	PDU Index

Figure 3 Proposed Nonce Construction

Generic MAC Header (Byte#0-#4): Generic MAC header omitting HCS. (GMH is subject to change)

Reserved (Byte#5-#7): set to 0. 0x000000.

Frame Number Iteration (Byte#8): Initial value shall be 0x00. Every time the frame number goes around, Frame Number Iteration is incremented by one.

Frame Number (Byte#9-#11): The Frame Number in which the PDU is transmitted or received.

PDU Index (Byte#12): The order of PDU appearance within the frame.

Ciphertext Payload	Message authentication code

Figure 4 Proposed Encrypted Payload format in AES-CCM

Proposed Text to the SDD

[Insert the following new subclause to the section 12 (Security)]

12.X Data encryption with AES- CCM mode

12.X.1 PDU payload format

The plaintext PDU shall be encrypted and authenticated using the active TEK, according to the CCM specification. This includes appending an 8-byte integrity check value (ICV) to the end of the payload and encrypting both the plaintext payload and the appended ICV.

The processing yields a payload that is 8 bytes longer than the plaintext payload. See Figure X-1.

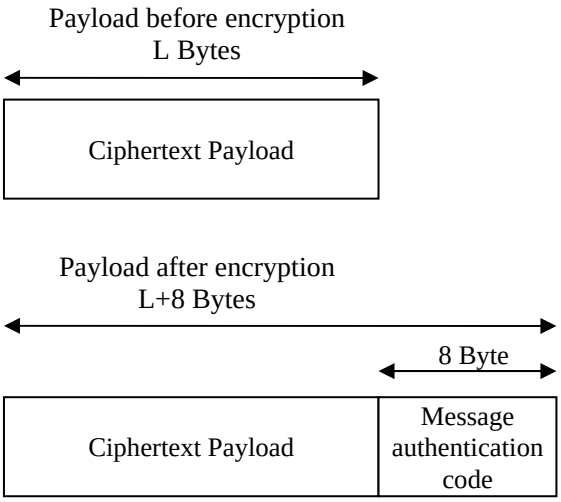

Figure X-1 Encrypted Payload format in AES-CCM

12.X.2 Nonce construction for CCM algorithm

The nonce shall be 13 bytes long as shown in Figure X-2. Bytes 0 through 4 shall be set to the first 5 bytes of the generic MAC header (thus excluding the HCS). The HCS of the generic MAC header is not included in the nonce since it is redundant. Bytes 5 through 7 are reserved and shall be set to 0x000000. Byte 8 shall be set to the value of the Frame Number Iteration. The initial value of the Frame Number Iteration shall be 0x00. Every time the frame number goes around, the Frame Number Iteration is incremented by one. Bytes 9 through 11 shall be set to the value of the Frame Number. The Frame Number indicates the frame in which the PDU is transmitted or received. Byte 12 shall be set to the value of the PDU Index. The PDU Index indicates the order of PDU originated by sender's MAC PDU construction function to /from an SS within the frame.

(Editor's note: The number of bytes may change due to new definition for the 16m)

Byte Number	0 - 4	5 – 7	8	9-11	12
Field	Generic MAC header	*Reserved*	Frame Number Iteration	Frame Number	PDU Index

Figure X-2 Proposed Nonce Construction

[1] P802.16Rev2/D6