# Proposal on PN overhead reduction in AES-CCM

Document Number: C80216m-09/0177r1

Date Submitted: 2009-01-08

Source:

Youngkyo Baek, Anil Agiwal, Jungje Son
Samsung Electronics*

Voice: +82102797321
E-mail: youngkyo.baek@samsung.com
anilag@samsung.com

*<http://standards.ieee.org/faqs/affiliationFAQ.html>

Venue:

IEEE 802.16m-08/052 - Call for Comments and Contributions on Project 802.16m SDD
Topic: Security, AES CCM Mode sub section 10.6.5.1.1

Base Contribution:

N/A

Purpose:

Discuss and approve the proposed text changes into SDD document

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 >.

# Proposed PN Overhead Reduction Scheme (1/3)

- Problem - How to share the information in initial CCM block between MS and BS when AES-CCM is used for data encryption?
  - In 16e, PN(4byte),GMH & length of plaintext payload are parameters present in initial CCM block
  - PN is explicitly included in encrypted MPDU for decrypting cipher text
  - ISSUE : To reduce the encryption (4 byte PN) overhead
- Motivation - Sequence number (SN) per flow (e.g. ARQ_SN or FSN) is present in each MPDU
  - The SN increments by 1 per MPDU
- Define a ROC (roll-over counter; 2bytes) of the SN
  - ROC is included in the MPDU format explicitly
    - Encryption overhead : ROC+ICV = 2+8 bytes
    - EKS could be included as 2bits of ROC (e.g. 2bits EKS +14bits ROC)
  - SN and ROC are used as input values of initial CCM block.
  - SN & ROC in a MPDU are not encrypted

# Proposed PN Overhead Reduction Scheme (2/3)

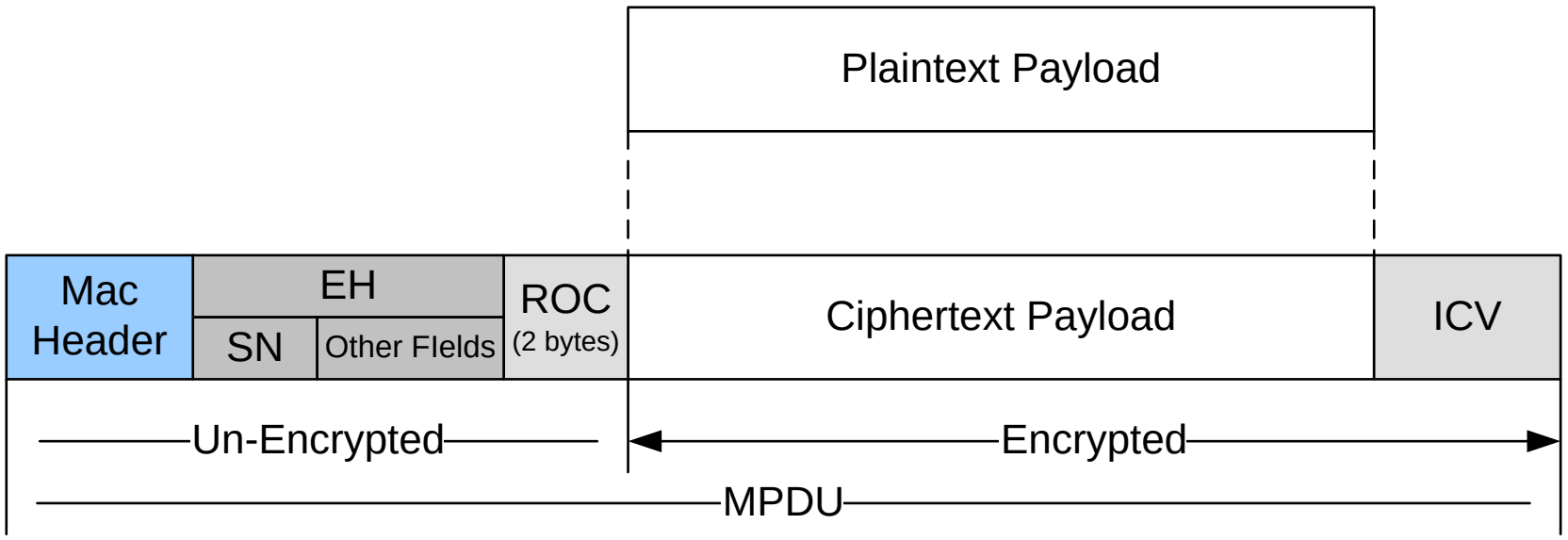


**Figure 1. Proposed Encrypted Payload Format in AES CCM Mode**

# Proposed PN Overhead Reduction Scheme (3/3)

- ROC maintained per flow
  - The ROC is the rollover counter for the SN
    - When the SN is changed from its Max to 0, the ROC is incremented by 1.
    - Sequence number (e.g. ARQ_SN or FSN) is not applied at a MPDU, ROC is incremented at each PDU.
  - Before the ROC of a Flow overflows, the TEK of the SA to which this flow is mapped is updated
  - If TEK is updated, then the flows mapped to the related SA reset their ROC by 0.

| Byte number | 0 2 | 3 8 | 9 10 | 11 12 |
|---|---|---|---|---|
| Field | GMAC Header | Reserved | ROC | Sequence number |
| contents | GMAC Header omitting HCS | 0x000000000000 | ROC | 0x0000 + Sequence number |

**Table.1 NONCE Construction for AES CCM Mode**

# Proposed text change in SDD (1/2)

[ Insert the following text in section 10.6.5.1.1 in IEEE 802.16m-08/003r6]

**---------- Text Starts ----------**

10.6.5.1.1 AES in CCM mode

10.6.5..1.1.1 PDU payload format

~~The PN size is reduced in 802.16m from 4 bytes to 3 bytes. Further reduction in PN and supporting methods are FFS~~

For encryption of MPDU based on AES in CCM mode, ROC and Sequence Number of PDU(if present) is used as input values for nonce and ROC is appended at MAC PDU format.

ROC is maintained per flow.

When the Sequence number is rolled over, the ROC is incremented.

If Sequence number is not applied at a PDU, ROC is incremented at each PDU.

The MS shall ensure that a new TEK is requested and transferred before ROC overflows. If ROC overflows without new keys being installed, transport communications on that SA shall be halted until new TEKs are installed. If the TEK is updated, then the flows mapped to the related SA reset their ROC by 0. Any tuple value of {Flow ID,ROC, Sequence number , TEK} shall not be used more than once for the purposes of transmitting data.

~~The nonce construction for the CCM algorithm defined in IEEE 802.16e is used also for 802.16m~~

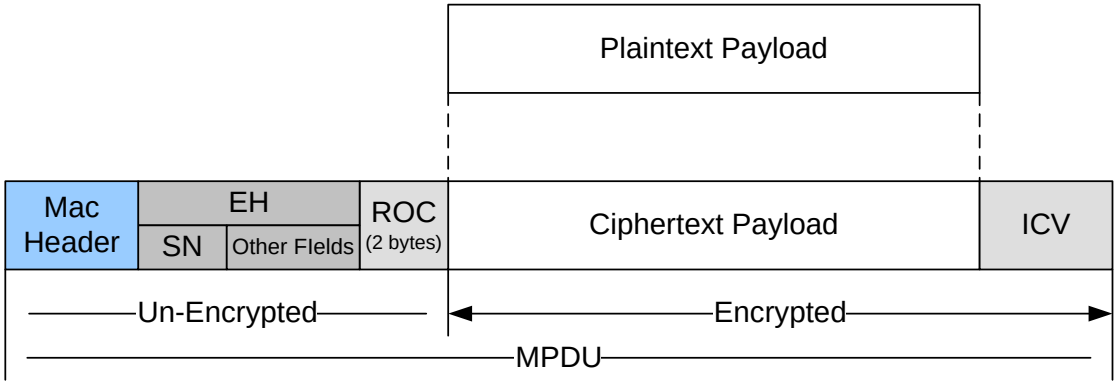


**Figure xx. Proposed Encrypted Payload Format in AES CCM Mode**

# Proposed text change in SDD (2/2)

~~The nonce construction for the CCM algorithm defined in IEEE 802.16e is used also for 802.16m~~

The nonce shall be 13 bytes long as shown in table xx. Bytes 0 through 2 shall be set to the first 3 bytes of the generic MAC header (thus excluding the HCS). Bytes 3 through 8 are reserved and shall be set to 0x000000000000. Bytes 9 through 10 shall be set to the value of the ROC. Bytes 11 through 12 shall be set to the value of the Sequence number if present .

| Byte number | 0 2 | 3 8 | 9 10 | 11 12 |
|---|---|---|---|---|
| Field | GMAC Header | Reserved | ROC | Sequence number |
| contents | GMAC Header omitting HCS | 0x000000000000 | ROC | 0x0000 + Sequence number |

Table.xx. Example of NONCE for CCM

---------- Text ends ----------