

Proposal on applying AES-CTR to unicast connection

Document Number: C80216m-09/0179r1

Date Submitted: 2009-01-05

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, Encryption methods sub section 10.6.5.1

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>>.

Encryption Methods in SDD

- AES-CCM mode
 - ✓ Support encryption and authentication
 - ✓ Encryption overhead:
 - 16e : PN(4bytes) + ICV (integrity check value ; 8bytes)
 - 16m : PN (less than 3bytes) + ICV(8bytes)
- AES-CTR mode
 - ✓ Support encryption only
 - ✓ Usage in 16e : for MBS traffic encryption with 1 byte encryption overhead.

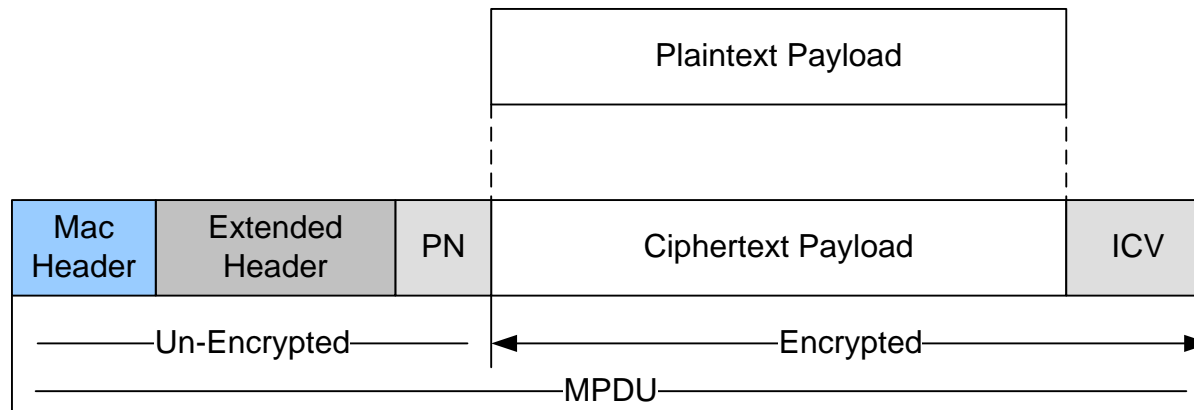


Figure 1 - Encrypted payload format in AES-CCM mode

Motivation and remedy

- Motivation

- ✓ Some applications (e.g. VoIP) are not required to check integrity because corrupt packets are regarded as noise by End users
- ✓ We can reduce at least 8bytes encryption overhead such as 'integrity check' etc.
 - VoIP payloads are small-size considering encryption overhead of AES-CCM

	VoIP (AMR full rate)	VoIP (AMR silence)
Plaintext MPDU	36 ~ 40 bytes	11 ~ 15 bytes
Encryption Overhead(CCM)	25~27%	67 ~ 91%
Encryption Overhead(CTR)	At least 5~5.6%	At least 13~18%

Table1. encryption overhead v.s. size of plaintext MPDU in 16e

- Proposed remedy: Use 'AES-CCM method without ICV for the flows which don't need integrity protection

Proposed text change in SDD

[insert the following text in section 10.5.5.1 at page52 line35]

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

10.6.5.1.2 AES in CTR mode

When integrity check is not required for an unicast connection, AES-CCM mode(10.5.5.1.1) excluding ICV part is used as a kind of AES-CTR mode.

10.6.5.1.~~2~~3 Multiplexing MPDUs

----- *Text Ends* -----