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 section10.6.5.1

Base Contribution:

N/A

Purpose:

Discuss and approve the proposed text changes into SDD document

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.

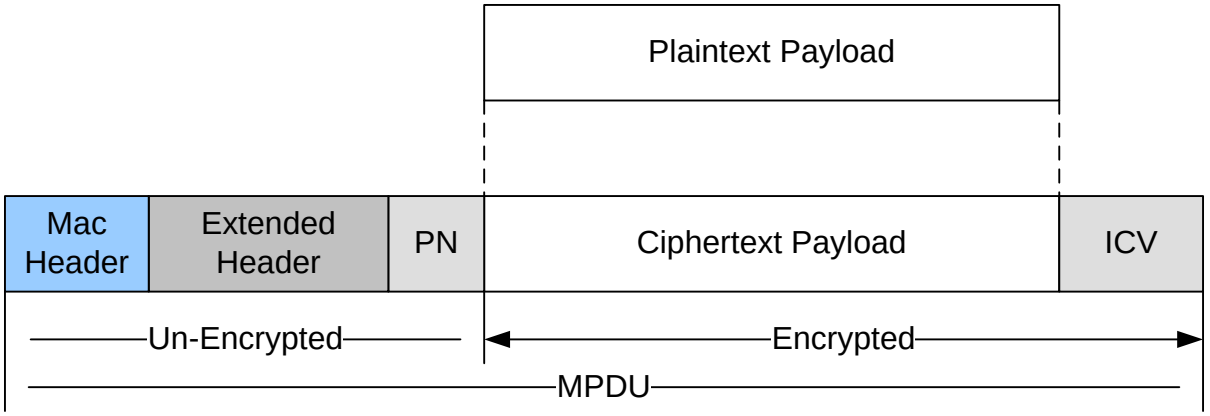

Figure 1 - Encrypted payload format in AES-CCM mode

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* ----------