Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	AES in CTR mode clarifications
Date Submitted	**2005-05-04**
Source(s)	Ilan Zohar ilan.zohar@intel.com Yigal Eliaspur yigal.eliaspur@intel.com **Intel Corporation**
Re:	IEEE802.16e/D7
Abstract	This contribution clarifies use of AES in CTR.
Purpose	To incorporate the text changes proposed in this contribution into the 802.16e/D8 draft.
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:chair@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>.

AES in CTR mode

Ilan Zohar (Intel corp.)

1 Introduction

Section 7.8.4.1.1 prescribe how AES in CTR should be used and how the NONCE and Initial counter should be constructed. Despite clarifications in D7 the text still contains ambiguities that only examination of the test code can resolve. This contribution amends the text relieving the need for code review. It also remove a portion of which appears twice in the text (annex F).

2 Proposed Text Change

[modify section 7.8.4.1.1 as follows]

7.8.4.1.1 PDU payload format

Counter mode requires a unique initial counter and key pair across all messages. This section describes the initialization of the 128-bit initial counter, constructed from the 24-bit PHY synchronization field or frame number and a new 8-bit Rollover counter (ROC).

NOTE—When we start to deal with a new PDU we have a new frame number and therefore reinitialize the counter. When the frame number reaches 0x000000 (from 0xFFFFFF), we increment ROC.

The PDU payload for AES-CTR encryption shall be prepended with the 8-bit ROC , i.e., the ROC is the 8 MSBits of the 32-bit nonce. ~~The ROC shall be transmitted in little endian order.~~ The ROC shall not be encrypted.

Any tuple value of {AES Counter, KEY} shall not be used more than once for the purposes of encrypting a block. MS and BS shall ensure that a new MTEK is requested and transferred before the ROC reaches 0xFF.

A 32 bit nonce NONCE = n0 | n1 | n2 | n3 (n0 being the MSByte and n3 the LSByte) is made of ROC and 24bits frame number in the following way: n0=ROC and n1, n2 , n3 are the byte representation of frame-number in MSB first order. ~~The 32bit nonce made out of ROC and 24bits frame number~~

NONCE shall be repeated four times to construct the 128-bit counter block required by the AES-128 cipher. (initial counter = NONCE|NONCE|NONCE|NONCE). When incremented, this 16 byte counter will be treated as a Big Endian number.

This mechanism can reduce per-PDU overhead of transmitting the full counter. In other words, at the most 2^32 PDUs can be encrypted with a single MTK.

The plaintext PDU shall be encrypted using the active MBS_Traffic_key (MTK) derived from MAK and-MGTEK, according to CTR mode specification. A different 128-bit counter value is used to encrypt each 128-bit block within a PDU.

The processing yields a payload that is 8 bits longer than the plaintext payload.

[delete annex F]