Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Corrections for the OMAC-Digest and the OMAC-Tuple**	
Data Submitted	**2005-05-05**	
Source(s)	Seokheon Cho Taeyong Lee Chulsik Yoon ETRI Jicheol Lee Yong Chang SAMSUNG Yongjoo Tcha KT Li Rui and Tian Feng ZTE corporation Yigal Eliaspur Intel Corp.	Voice: +82-42-860-5524 Fax: +82-42-861-1966 chosh@etri.re.kr 161, Gajeong-dong,Yuseong-Gu, Daejeon, 305-350, Korea
Re:	IEEE P802.16e/D7	
Abstract	The document contains suggestions on the changes into IEEE 802.16e/D7 that would correct OMAC-Digest and OMAC-Tuple.	
Purpose	Adoption of proposed changes into P802.16e/D7	
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:chiar@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>.	

Corrections for the OMAC-Digest and the OMAC-Tuple

Seokheon Cho, Taeyong Lee, and Chulsik Yoon
ETRI

Jicheol Lee and Yong Chang
SAMSUNG

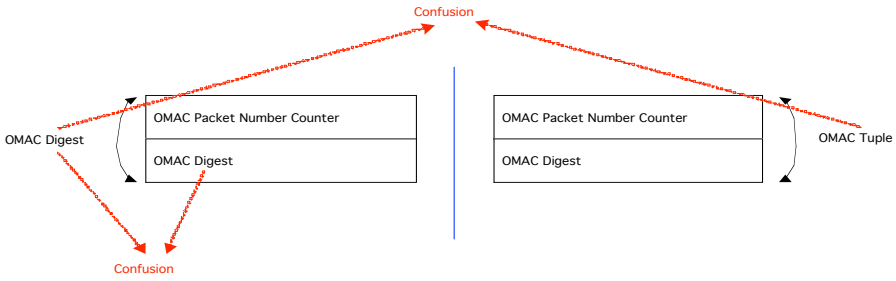
Yongjoo Tcha
KT

Li Rui and Tian Feng
ZTE corporation

Yigal Eliaspur
Intel Corp.

Introduction

The OMAC-Digest and OMAC-Tuple are defined in the P802.16/D7. However, those parameters have some problems as follows.



1. The OMAC-Digest defined in the sub-clause 11.9.32 causes confusion. The OMAC-Digest field contains the OMAC Packet Number Counter and the OMAC-Digest.

Table 381c-OMAC digest definition

Field	Length (bits)	Note
OMAC Packet Number counter, OMAC_PN_*	32	This context is different in UL, DL
OMAC Digest	64	OMAC with AES 128

However, the definition of the OMAC-Digest is generally a message authentication code just like the HMAC-Digest. It is necessary to avoid confusion between the OMAC-Digest field and the OMAC-Digest value and support backward compatibility to the HMAC-Digest field defined in the IEEE Std 802.16-2004. Therfore, the name of the OMAC Digest contained in the OMAC-Digest attribute should be changed like “OMAC Value.”

2. The OMAC-Tuple defined in the sub-clause 11.1.2.2. The OMAC-Tuple field contains the OMAC Packet Number Counter and the OMAC-Digest.

Table 348b-OMAC Tuple definition

Field	Length (bits)	Note

OMAC Packet Number counter, OMAC_PN_*	32	This context is different in UL, DL
OMAC Digest	64	OMAC with AES 128

There is no difference between the OMAC-Digest and the OMAC-Tuple as shown in Table 348b and Table 381c. In addition, the OMAC-Tuple field shall be included in the MAC messages (e.g., DSA-REQ/RSP/ACK) except the PKM-related MAC messages. Those MAC messages containing the OMAC-Tuple don't include a field such as OMAC Key Sequence Number to identify which the OMAC Key (OMAC_KEY_*) should be used to generate the OMAC-Digest, because both an SS and a BS shall be able to support up to two simultaneously active OMAC Keys. Therefore, the OMAC-Tuple should contain the OMAC Key Sequence Number.

Proposed changes to IEEE 802.16e/D7

11.9.32 OMAC Digest
[Modify the sub-clause 11.9.32 as follows:]

Description: This attribute contains a packet number counter OMAC_PN_* incremented per packet on each direction and the Message Authentication Code value used for message authentication. The OMAC algorithm is defined in draft SP 800-38B.

The OMAC digest includes

Type	Length	Value
40	12	See Table 381c

Table 381c-OMAC digest definition

Field	Length (bits)	Note
OMAC Packet Number counter, OMAC_PN_*	32	This context is different in UL, DL
OMAC ~~Digest~~ value	64	OMAC with AES 128

7.5.4 Calculation of OMAC ~~Digest~~ Value
[Modify the sub-clause 7.5.4 as follows:]

The calculation of the keyed hash value contained in the OMAC-Digest attribute and the OMAC Tuple shall use the OMAC Algorithm with AES. The downlink authentication key OMAC_KEY_D shall be used for authenticating messages in the downlink direction. The uplink authentication key OMAC_KEY_U shall be used for authenticating messages in the uplink direction. Uplink and downlink message authentication keys are derived from the AK (see 7.5.4 below for details).

For authentication multicast messages (in the DL only) a OMAC_KEY_GD shall be used (one for each group), group authentication key is derived from GKEK.

The OMAC-Digest and OMAC-Tuple attributes shall be only applicable to the PKM version 2. In the PKM version 2 protocol, The OMAC key sequence number in the OMAC tuple shall be equal to the ~~64-bit AKID~~ 4-bit AK sequence number of the AK from which the OMAC_KEY_x was derived. ~~In the PKM version 1 protocol, the 4 least significant bits of the OMAC sequence number in the OMAC tuple shall be equal to the 4-bit AK sequence number and the 44 most significant bits shall be equal to 0.~~

The OMAC Packet Number Counter (OMAC_PN_*) is a 4 byte sequential counter that is incremented in the context of UL messages by the MS, and in the context of DL messages by the BS,. The BS will also maintain a separate OMAC_PN_* for multicast packets per each GSA and increment that counter in the context of each multicast packet from the group. For MAC messages that have no CID e.g. ~~RNG-REG~~ RNG-REQ message, the OMAC_PN_* context will be the same as used on the basic CID.

The ~~OMAC_PN counters~~ OMAC Packet Number Counter, OMAC_PN_*, is ~~are~~ part of the OMAC security context and must be unique for each MAC management message with the OMAC tuple or digest.

The digest shall be calculated over a field consisting of the OMAC key sequence number followed by the OMAC Packet Number Counter ~~OMAC_PN~~, expressed as an unsigned 32-bit number, followed by the 16-bit Connection ID on which the message is sent, followed by 16-bit of zero padding (for the header to be aligned with AES block size) and followed by the entire MAC management message with the exception of the OMAC-TLV.

The least significant bits of the digest shall be truncated to yield a 64-bit length digest. ~~The OMAC key sequence number is identical to the KEYid it was derived from i.e AKID if derived from AK.~~ The OMAC key sequence number shall be equal to the 4-bit ~~AKID~~ AK sequence number of the AK from which the OMAC_KEY_x was derived.

I.e.,:

OMAC ~~digest~~ value <= Truncate64 (OMAC (OMAC_KEY_*, OMAC key sequence number | OMAC_PN_* | CID |16-bit zero padding | MAC_Management_Message))

If the message is included in an MPDU that has no CID, e.g. A RNG-REQ message, the CID used shall take the value of the basic

CID.

11.1.2.2 OMAC Tuple
[Modify the sub-clause 11.1.2.2 as follows:]

This parameter contains the OMAC key sequence number, the OMAC Packet Number Counter (OMAC_PN_*), and ~~concatenated with an~~ the OMAC value ~~OMAC Digest itself~~ used for message authentication. ~~The OMAC_PN_* is stored in the 32 least significant bits of the OMAC Tuple.~~ The OMAC-Tuple attribute format is shown in ~~Table 347 and Table 348.~~ Table 348a and Table 348b.

When included in a MAC management message, the OMAC tuple shall always be the final tuple in the message.

A message received, that contains an OMAC tuple, shall not be considered authentic if the length field of the tuple is not ~~12~~ 13, or if the locally computed value of the digest does not match the digest in the message.

Non authentic messages shall be discarded.

Informative note: It would be appropriate for a MIB to increment an error count on receipt of a non authentic message, so that management can detect an active attack.

Table 348a-OMAC Tuple definition

Type	Length	Value	Scope
150	~~12~~ 13 or 19	See Table ~~346a~~ 348b	DSx-REQ, DSx-RSP, DSx-ACK, REG-REQ, REG-RSP, RES-CMD, DREG-CMD, TFTP-CPLT

Table 348b-OMAC Tuple definition

Field	Length (bits)	Note
Reserved	4	Set to 0
OMAC Key Sequence Number	4	OMAC key sequence number
BSID	48	Only used in case of SHO zone - optional
OMAC Packet Number Counter ~~counter~~, OMAC_PN_*	32	This context is different in UL, DL
OMAC ~~Digest~~ Value	64	OMAC with AES 128