Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Crypto synchronized HMAC**	
Date Submitted	**2004-05-17**	
Source(s)	JunHyuk Song, Lim Geunhwi, Yong Chang Samsung Electronics	Voice: +82-31-xxx-xxxx Fax: mailto: junhyuk.song@samsung.com
Re:	This is a response to a Call for Comments IEEE 802.16e-03/58 on IEEE 802.16e-03/07r5	
Abstract	This document contains suggestions to provide crypto synchronized HMAC to protect certain MAC management messages against reply attack	
Purpose	The document is submitted for review by 802.16e Working Group members.	
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>.	

802.16e Crypto Synchronized HMAC Message Authentication

Samsung Electronics

1 Scope of this document

This document outlines how to provide Crypto Synchronized HMAC Message Authentication

2 Background

Current Message Authentication Code, HMAC-Digest doesn't include any time related information for HMAC calculation that may open vulnerability for replay attacks for some MAC Management messages such as Location Update, Key Request, DASx and Registration message. In this contribution we propose to add PHY_SYNC in DL_MAP in computation for HMAC-DIGEST (see figure-1) in case of Crypto synchronized HMAC is supported in both SS and BS and negotiated during SBC Capability negotiation.

3 Attack Scenario

Rogue SS could capture MAC management messages and replay it later on to produce-unauthorized effect.

4 Proposed solution

Crypto Synchronized HMAC Digest shall be computed as below:

- HMAC (160bits) = SHA1 (HMAC_KEY_D/U XOR opad, SHA1(HMAC_KEY_D/U XOR ipad, text))

  - ipad (512 bits) = 0x36 repeated 64 times
  - opad (512 bits) = 0x5c repeated 64 times
  - text = DL_MAP PHY Synchronization field (32bits) XOR LSB 32bits of MAC Management messages

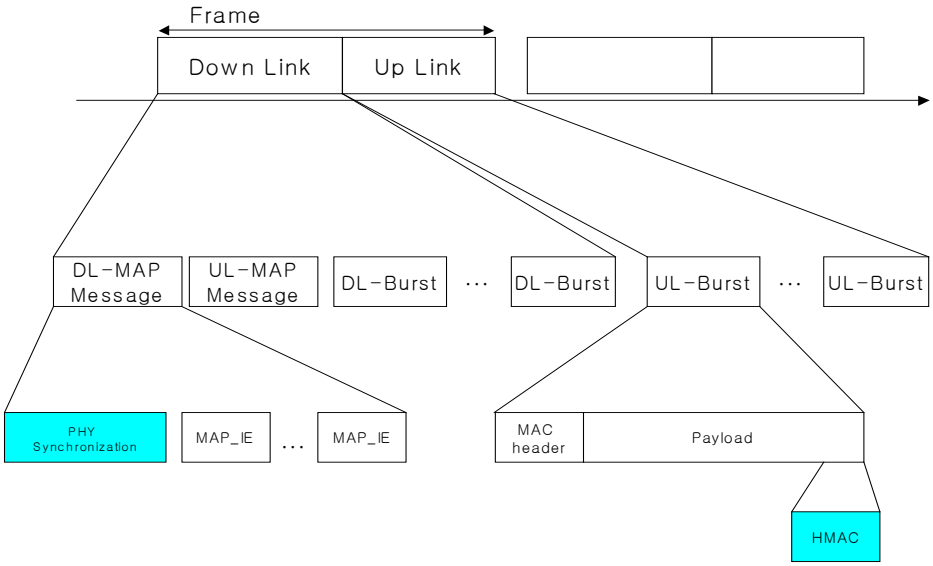

Figure-1

Proposed Text Change

[Add following as shown]

7.5.3 Calculation of HMAC-Digests

The calculation of the keyed hash in the HMAC-Digest attribute and the HMAC Tuple shall use the HMAC (IETF RFC 2104) with the secure hash algorithm SHA-1 (FIPS 180-1). The downlink authentication key HMAC_KEY_D shall be used for authenticating messages in the downlink direction. The uplink authentication key HMAC_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). The HMAC Sequence number in the HMAC Tuple shall be equal to the AK Sequence Number of the AK from which the HMAC_KEY_x was derived.

In Mesh Mode HMAC-Digests calculated with the key HMAC_KEY_S shall be supported. When calculating the digest with this key the HMAC sequence Number in the HMAC tuple shall be equal to the Operator Shared Secret Sequence Number.

The digest shall be calculated over the entire MAC Management message with the exception of the HMAC_Digest and HMAC Tuple attributes.__
HMAC-Digest calculation for certain types MAC Management messages shall include PHY_Synchronized field in DL_MAP for protection against replay attack. The text of HMAC-SHA-1, the entire MAC message shall be initialized with the exclusive-OR (XOR) of the PHY Synchronized field of the latest DL-MAP.

11.3.2.11 Authorization Policy Support

This field indicates authorization policy that both SS and BS need to negotiate and synchronize. A bit value of 0 indicates “not supported” while 1 indicates “supported.” If this field is omitted, then both SS and BS shall use the IEEE 802.16 essential privacy method, constituting X.509 digital certificates and the RSA public key encryption algorithm, as authorization policy.

Type	Length	Value	Scope
5.25	1	Bit# 0: IEEE 802.16 essential privacy (Legacy PKM) -Default Bit# 1: Authorization via PKM EAP Bit# 2: Crypto Synchronized HMAC Bit# 3-7: Reserved for open privacy. Set to 0	SBC-REQ (see 6.4.2.3.23) SBC-RSP (see 6.4.2.3.24)