Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>
Title	**Relay MAC Subheader/Header Protection**
Date Submitted	**2008-01-14**
Source(s)	Ryoji Ono, Toshiyuki Kuze **Mitsubishi Electric Corp** Voice: 81-467-41-2085 E-mail: Ono.Ryoji@aj.MitsubishiElectric.co.jp Zhifeng (Jeff) Tao, Jinyun Zhang **Mitsubishi Electric Research Lab** Voice: 1-617-621-7557 E-mail: tao@merl.com
Re:	Response to the IEEE 802.16 Working Group Letter Ballot #28a (i.e., IEEE 802.16-07/059).
Abstract	This contribution proposes a mechanism to protect relay MAC subheader/header.
Purpose	To adopt the relay MAC subheader/header protection mechanism proposed herein into IEEE 802.16j.
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>.

Relay MAC Subheader/Header Protection

Ryoji Ono, Toshiyuki Kuze
Mitsubishi Electric Corp

Zhifeng (Jeff) Tao, Jinyun Zhang
Mitsubishi Electric Research Lab

1. Introduction

Subheaders are considered as a part of payload in IEEE 802.16 [2] and thus are encrypted if EC bit in generic MAC header (GMH) is turned on. Moreover, the GMH is used as a part of nonce N during the encryption, and its authenticity is therefore also protected.

In the current IEEE 802.16j draft D2 [1], however, relay subheaders are transmitted as plaintext on relay link, and no protection for their authenticity is provided.

This contribution proposes a mechanism to protect the authenticity of the relay subheaders. As a by-product, the proposed mechanism can also provide protection to the authenticity of relay MAC header and relay extended subheaders.

2. Summary of Proposal

We propose an optional feature to protect relay MAC PDU against forgery.

As an optional function, R-MPDU should be able to carry the HMAC/CMAC digest over its relay MAC header, extended subheaders and subheaders. The digest is carried by the newly defined subheader called *HMAC/CMAC subheader*. The HMAC/CMAC subheader also contains HMAC/CMAC PN against replay attack.

Derivation and validation of the HMAC/CMAC digest is done hop-by-hop. The MR-BS or RS who receives the R-MPDU that contains an HMAC/CMAC subheader shall validate it as in management messages. In non-transparent RS system, the station may update the contents of subheaders and extended subheaders. The station then re-calculates HMAC/CMAC digest for the next hop.

HMAC/CMAC_KEY_RL* shall be used to derive the HMAC/CMAC digest.

To indicate the existence of the HMAC/CMAC subheader, an Authentication Control bit shall be included in relay MAC header.

3. Proposed Text Changes

6. MAC Common Part Sublayer

6.3.2.1.1.1 Relay MAC header format

[Change Figure 22a as indicated:]

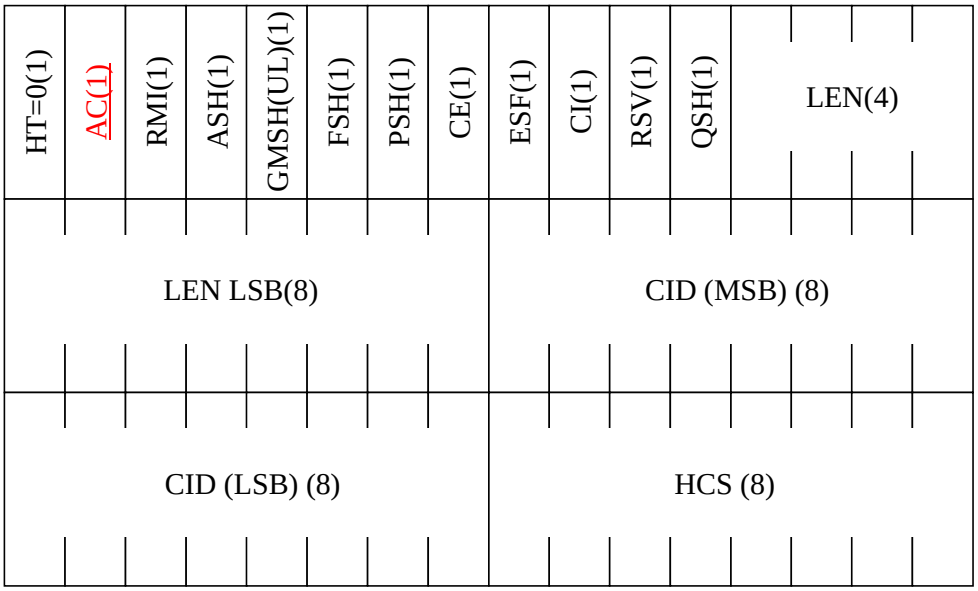

Figure 22a—Header format of relay MAC PDU with payload

[Change Table 7a as indicated:]

Table 7a—Description of relay MAC header fields

Syntax	Size	Notes
Relay MAC Header() {		
HT	1 bit	Shall be set to zero.
AC	1 bit	Authentication control. 1=headers are authenticated, 0=headers are not authenticated
RMI	1 bit	Shall be set to 1.
ASH	1 bit	Allocation subheader 1=present; 0=absent
GMSH	1 bits	UL: grant management subheader (GMSH) 1 = present, 0 = absent DL : reserved, shall be set to 0.
FSH	1 bit	Fragmentation subheader (FSH) 1=present; 0=absent
PSH	1 bit	Packing subheader (PSH) 1=present; 0=absent
CE	1 bit	CID encapsulation 1 = present, 0 = absent
ESF	1 bit	Extended subheader field If ESF=0, the extended subheader is absent. If ESF=1, the extended subheader is present and immediately follows the relay MAC header. The ESF is applicable in both the DL and UL.
CI	1 bit	CRC indicator. 1 = CRC is included in the PDU by appending it to the PDU payload after encryption, if any. 0 = No CRC is included.

RSV	2 bits	Shall be set to 0
QSH	1 bit	QoS subheader (QSH) 1=present; 0=absent
LEN	12 bits	Length. The length in bytes of the relay MAC PDU including the relay MAC header and the CRC if present.
CID	16 bits	T-CID or MT-CID.
HCS	8 bits	Header Check Sequence
}		

6.3.2.2.8 Relay MAC PDU subheaders

[Change the first paragraph as indicated:]

~~Four~~ Five types of subheaders may be present in a Relay MAC PDU: Fragmentation subheader, Packing subheader, QoS subheader, ~~and~~ Allocation subheader, and HMAC/CMAC subheader. The Packing and Fragmentation subheaders are mutually exclusive and shall not both be present within the same MAC PDU. When multiple subheaders are present in the same Relay MAC PDU, they shall be ordered as follows: QoS subheader, Fragmentation or Packing subheader, ~~and~~ Allocation subheader, and HMAC/CMAC subheader.

[Insert new subclause 6.3.2.2.8.3:]

6.3.2.2.8.3 HMAC/CMAC subheader

When the AC field in the relay MAC header is set to 1, the relay MAC header, the relay extended subheaders and the relay subheaders except the HMAC/CMAC subheader are authenticated hop-by-hop, by the HMAC/CMAC digest calculated over them. Upon receipt of the relay MAC PDU whose AC field is set to 1, the receiver should validate the HMAC/CMAC value and the HMAC/CMAC Packet Number Counter as per subclauses 7.5.3, 7.5.4.4 and 7.5.7. In this case, data to be authenticated are the relay MAC header, the relay extended subheaders and the relay subheaders except the HMAC/CMAC subheader, instead of management messages. The HMAC/CMAC subheader format is specified in Table 37c.

Table 37c—HMAC/CMAC subheader format

Syntax	Size	Notes
HMAC/CMAC subheader() {		
Reserved	4 bits	Shall be set to zero.
HMAC/CMAC Key Sequence Number	4 bits	HMAC/CMAC key sequence number
RSID	48 bits	RSID of the station who generates HMAC/CMAC value
HMAC/CMAC Packet Number Counter HMAC/CMAC_PN_RL*	32 bits	Replay counter
HMAC/CMAC Value	*variable*	64 bits for CMAC with AES-128 64, 80 or 96 bits for Short-HMAC with SHA-256
}		

7. Security sublayer

7.3.3.1 SZK usage

[Change the second and the third paragraphs as indicated:]

SZK is used by the MR-BS and RS to derive security zone message authentication keys, i.e. HMAC/ CMAC_KEY_SZU and HMAC/CMAC_KEY_SZD. SZK is updated periodically via relay multicast rekeying algorithm (see subclause 7.8.4).

The MR-BS shall use HMAC/CMAC_KEY_SZD to generate MAC for the relay management messages (except for PKMv2 messages); and MAC for relay MAC header, relay MAC extended subheader and relay MAC subheader. The MR-BS shall use HMAC/CMAC_KEY_SZU to validate MAC of the relay management messages; and MAC of relay MAC header, relay MAC extended subheader and relay MAC subheader..

An RS shall use HMAC/CMAC_KEY_SZD to re-generate or validate MAC of the downlink relay management messages and MAC of relay MAC header, relay MAC extended subheader and relay MAC subheader sent by the MR-BS or its superordinate RS (except for PKMv2 messages). An RS shall use HMAC/CMAC_KEY_SZU to re-generate or validate MAC of the relay management messages and MAC of relay MAC header, relay MAC extended subheader and relay MAC subheader sent by its subordinate RS.

11. TLV Encodings

11.8.4 Security Negotiation Parameters

[Insert new subclause 11.8.4.8:]

11.8.4.8 Relay MPDU authentication mode support

Type	Length	Value
TBA	1	Bit #0: Indication of support of relay MAC PDU protection if set to 1 Bit #1 - #7: reserved

4. Reference

[1] “Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Multihop Relay Specification”, IEEE P802.16j/D2, December 2007

[2] “IEEE Standard for Local and Metropolitan Area Networks − Part 16: Air Interface for Fixed Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands,” IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, February 2006.