

Project	IEEE 802.16 Broadband Wireless Access Working Group < http://ieee802.org/16 >	
Title	Shared Management Message in MR system: Format, Transfer and Security	
Date Submitted	2007-04-25	
Source(s)	Shulan Feng, Yanling Lu, Ting Li, Liangliang Zhang Hisilicon Technologies Harbour Building, No.8, Dongbeiwang West Road, HaiDian District, Beijing, China	Voice: 86-10-82829010 Fax: 86-10-82829075 mailto:fengsl@huawei.com luyanling@hisilicon.com
	Masato Okuda and Yuefeng Zhou Fujitsu	mailto:okuda@jp.fujitsu.com Yuefeng.Zhou@uk.fujitsu.com
Re:	This contribution is a response to " IEEE 802.16j-07/013 Call for Technical Comments regarding IEEE Project 802.16j" (2007-04-02) .	
Abstract	This contribution describes shared management message format and transfer, as well as security on shared management message	
Purpose	This document is provided in response for Call for Technical Comments and Contributions regarding IEEE Project 802.16j .	
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 >.	

Shared Management Message in MR system: Format, Transfer and Security

Shulan Feng, Yanling Lu, Ting Li, Liangliang Zhang

Hisilicon Technologies

Masato Okuda and Yuefeng Zhou

Fujitsu

1. Introduction

This contribution describes a method how a shared management message can be sent by the MR-BS only once while it can be read and authenticated by the MS/RS and its access RS in a centralized MR system with distributed scheduling. This method includes the shared management message format and transfer, as well as security on the shared management message.

2. Problem Statement

In a centralized MR system with distributed scheduling, the MR-BS and MS perform the system procedures, for example, create/modify/delete service flow, handover, sleep mode and so on, while the RS and MR-BS allocate the bandwidth on the relay and access link. In some cases, it's desirable that the messages sent by the MR-BS can be read and authenticated by the access RS on the multi-hop link, so that the RS can allocate the bandwidth more efficiently based on the information from the management messages sent by the MR_BS. We call this kind of management message "shared management message". However, the shared management message can all applied in the uplink.

However, in the 16e system, although the management messages are not encrypted, they are protected by the CMAC/HMAC Tuple to validate their integrity, so the message can't be authenticated by the nodes except the sender and receiver. To solve this problem, one way is to let the sender send duplicate messages to each node on the multi-hop link. Obviously, this way reduces available bandwidth and can't ensure these duplicate messages are all received successfully, which may further lead to the information inconsistency among the receivers. So this contribution proposes a method by which a shared management message is sent by the MR-BS only once while the message can be read and authenticated by the MS/RS and its access RS on the multi-hop.

3. Suggested Solution

3.1 Shared Management Message Format

Shared management message format is consistent with management message format in 16e system, as indicated in Figure 1. Within management message payload of 16e system, the HMAC/CMAC Tuple is the last attribute if it exists. Here we only modify 16e's HMAC/CMAC Tuple in the 16e system as HMAC/CMAC Tuple Sequence in the MR system.

Shared Management Message format is defined as following:

- 1) Management Message Type.
- 2) Shared Management Message Payload, the management message payload with exception of HMAC/CMAC Tuple Sequence.
- 3) HMAC/CMAC Tuple Sequence, which consists of two HMAC/CMAC Tuples . The first HMAC/CMAC Tuple in the HMAC/CMAC Tuple Sequence is originated **by** using the key shared between the MR-BS and last hop node on the multi-hop link. The second HMAC/CMAC Tuple in the sequence is originated **by** using the key shared between the MR-BS and last two hop node on the multi-hop link..

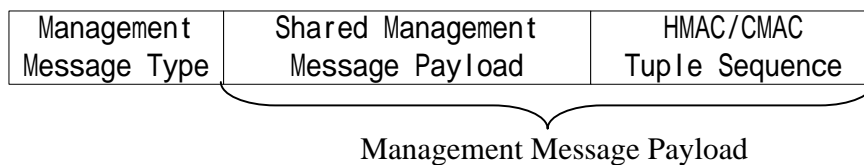


Figure-1 Shared management message format

3.2 Procedure of Shared Management Message Transfer

Assuming the last hop node on the multi-hop link is a MS, before the MR-BS sends a shared management message ,the MR-BS shall add the HMAC/CMAC Tuple Sequence as the last attribute in the shared management message. The HMAC/CMAC Tuple Sequence consists of two HMAC/CMAC Tuples. One is originated by the shared key between the MR-BS and the MS, the other is originated by the shared key between the MR-BS and the access RS.

When the management message is received by the intermediate RS on the multi-hop link, the RS can determine whether the message needs to be authenticated or not. The method used is out of this contribution's scope. If RS needs to do it, the RS validates this message's integrity based on the key shared with the MR-BS. If the message is legal, the RS reads the message and deletes the last HMAC/CMAC Tuple in the HMAC/CMAC

Tuple Sequence and relays the shared message to the MS. The message received by the MS has the same format as that in the 16e system, so there is no change for the MS.

Figure 2 is an example of transferring shared management message.

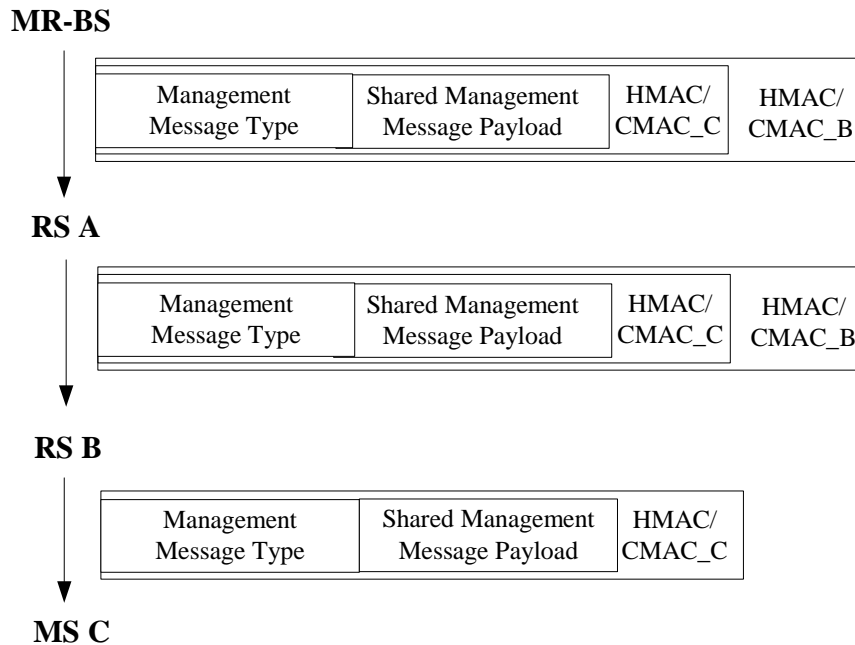


Figure-2 An example of transferring shared management message.

3.3 Security on Shared Management Message

In a centralized MR system with distributed scheduling, the PKM may be unchanged. The algorithms used to calculate the HMAC-Digests and CMAC valued remain unchanged. The only modification is the field over which the HMAC/CMAC digest is calculated.

3.3.1 Calculation of HMAC–Digest

The HMAC digest shall be calculated using the authentication key shared between the MR-BS and a node on the multi-hop link over a field consisting of the part protected by the HMAC Tuple originated using the authentication key shared between the MR-BS and this node’s subordinate node(this HMAC Tuple is included). If the HMAC digest is calculated using the key shared with MS, this field consists of Management Message Type and Shared Management Message payload.

3.3.2 Calculation of CMAC Value

The CMAC digest shall be calculated on the authentication key shared between the MR-BS and a node over a field consisting of the AKID followed by the CMAC Packet Number Counter, followed by the 16-bit Connection ID on which the message is sent, followed by 16-bit of zero padding, followed by the part protected by the CMAC Tuple originated using the authentication key shared between the MR-BS and this node's subordinate node (this CHMAC Tuple is included). If the CMAC digest is calculated using the key shared with MS, this field consists of Management Message Type and Shared Management Message payload.

Upon calculation of CMAC value in CMAC Tuple in the CMAC Tuple Sequence, the CID will be the Connection ID in the generic header on which connection the shared management message is transmitted when the message is received.

3.4 Advantages

In brief, the method proposed has the following advantages:

- 1) Shared management message will be sent by the MR-BS only once while it can be read and authenticated by the node and its access RS, which saves the rare bandwidth of the multi-hop link and keeps the information consistent among the sender and receivers.
- 2) Shared management format is consistent with management message format in 16e system.
- 3) Keep the security in 16e system almost unchanged only with simple modifications to the field over which the HMAC/CMAC digest is calculated, when originating HMAC/CMAC Tuples in the shared management message.

4. Proposed Text

[Insert the followings at the end of section 3]

3.xx Shared management message: A kind of management message which are be read and authenticated by multiple node on the multi-hop link.

6.3.2.3 MAC management message

[Insert new subclause before 6.3.2.3.1 Downlink Channel Descriptor (DCD) message]

Shared Management Message format is defined as following:

- 1) Management Message Type:
- 2) Shared Management Message Payload, the management message payload with exception of HMAC/CMAC Tuple Sequence.
- 3) HMAC/CMAC Tuple Sequence, which consists of two HMAC/CMAC Tuples . The first HMAC/CMAC Tuple in the HMAC/CMAC Tuple Sequence is originated by using the key shared between the MR-BS and

last hop node on the multi-hop link. The second HMAC/CMAC Tuple in the sequence is originated by using the key shared between the MR-BS and last two hop node on the multi-hop link..

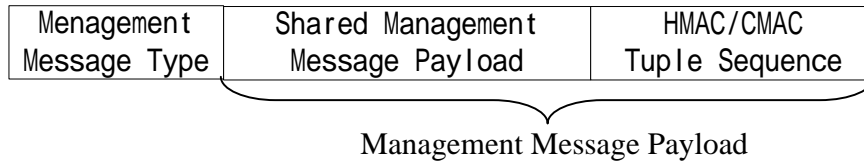


Figure-xx Shared management message format

7.5.3 Calculation of HMAC-Digests

[Insert new subclause 7.5.3.1 at the end of this subclause:]

7.5.3.1 Calculation of HMAC-Digests in the MR system

The HMAC digest shall be calculated using the authentication key shared between the MR-BS and the node on the multi-hop link over a field consisting of the part protected by the HMAC Tuple originated using the authentication key shared between the MR-BS and this node's subordinate node (this HMAC Tuple is included). If the HMAC digest is calculated using the key shared with MS, this field consists of Management Message Type and Shared Management Message payload.

7.5.4.4 Cipher-based MAC (CMC)

[Insert new subclause 7.5.4.4.2 at the end of this subclause:]

7.5.4.4.2 Cipher-based MAC in the MR system

The CMAC digest shall be calculated on the authentication key shared between the MR-BS and a node over a field consisting of the AKID followed by the CMAC Packet Number Counter, followed by the 16-bit Connection ID on which the message is sent, followed by 16-bit of zero padding, followed by the part protected by the CMAC Tuple originated using the authentication key shared between the MR-BS and this node's subordinate node (this CHMAC Tuple is included). If the CMAC digest is calculated using the key shared with MS, this field consists of Management Message Type and Shared Management Message payload.

Upon calculation of CMAC value in CMAC Tuple in the CMAC Tuple Sequence, the CID will be the Connection ID in the generic header on which connection the shared management message is transmitted when the message is received.