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	2007-03-05
Source(s)	Shulan Feng,Yanling Lu, Ting Li, Liangliang Zhang Hisilicon Technologies Harbour Building, No.8, Dongbeiwang West Road, HaiDian District, Beijing, China Masato Okuda and Yuefeng Zhou Fujitsu Voice: 86-10-82829010 Fax: 86-10-82829075 mailto:luyanling@hisilicon.com. fengsl@huawei.com mailto: okuda@jp.fujitsu.com Yuefeng.Zhou@uk.fujitsu.com
Re:	This contribution is a response to ” IEEE 802.16j-07/007r2 Call for Technical Comments and Contributions regarding IEEE Project 802.16j” (2007-02-19) .
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	
Patent Policy and Procedures	

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 each node on the multi-hop link 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, it is the MR-BS and MS which determine to 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 by the 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 message shared management message.

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 each node 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 replace the HMAC/CMAC Tuple in the 16e system with the HMAC/CMAC Tuple Sequence in the MR system.

Each shared management message has a corresponding management message of 16e system. The shared management message has the same message type with that of its corresponding management message and its shared management message payload is the same as the message payload with the exception of HMAC/CMAC Tuple of its corresponding management message.

HMAC/CMAC Tuple Sequence consists of HMAC/CMAC Tuples originated by using the authentication key shared between the MR-BS and each node on the multi-hop link respectively. 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 second hop node on the multi-hop link and so on.

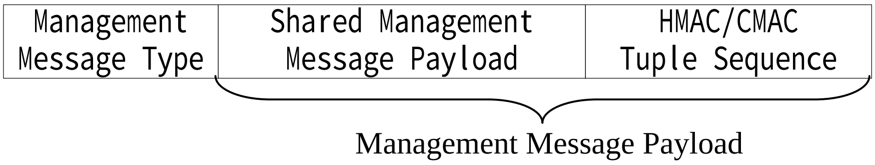

Figure-1 Shared management message format

As for the construction of the MAC PDU with the shared management message, there may be some solutions. One of them is a method proposed in [1] is a potential one.

3.2 Procedure of Shared Management Message Transfer

If a shared management message will be sent by the MR-BS to the nodes on the multi-hop link, the MR-BS shall add the HMAC/CMAC Tuple Sequence as the last attribute in the shared management message.

When the shared message is received by the RS on the multi-hop link, 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, leaving the part protected by HMAC/CMAC Tuple originated by using the authentication key shared between this RS's subordinate node and the MR-BS. At last, when the message is received by the MS, the message 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 the MAC PDU with shared management message.

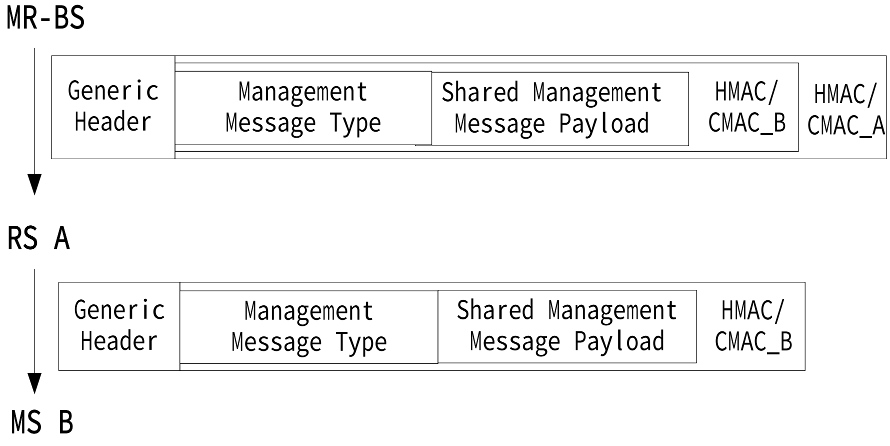

Figure-2 An example of transferring the MAC PDU with shared management message.

3.3 Security on Shared Management Message

In a centralized MR system with distributed scheduling, the PKM may be unchanged: The MR-BS distributes the keying data to the RS and MS respectively, so the RS and MS can synchronize keying data to the MR-BS. The management messages should be protected by the CMAC/HMAC Tuple. The message authentication keys used to generate the CMAC value and HMAC-Digest are also derived from the AK. The algorithms used to calculate the HMAC-Digests and CMAC valued remain unchanged. From the point view of security, 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 by 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 by 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 by using the key shared between the MR-BS and 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 by 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 by using the key shared between the MR-BS and 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 nodes on the multi-hop, which saves the rare bandwidth of the multi-hop link and keeps the information consistent among the sender and receivers.
2) Shared management message can only be read and authenticated by the necessary nodes which need the information in the shared management message, for the MR-BS can only add the HMAC/CMAC Tuples. They are originated by using the key shared between the MR-BS and these necessary nodes into the HMAC/CMAC Tuple Sequence.
3) Shared management format is consistent with management message format in 16e system.
4) 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

6.1 PMP

6.1.1 Relay extension

[Insert new subclause 6.1.1.x at the end of this subclause:]

6.1.1. Shared Management Message format

Shared management message is a kind of management message which are sent by the MR-BS only once while they can be read and authenticated by each node on the multi-hop link.

Shared Management Message format is consistent with management message format in 16e system, as indicated in figure xx.

Each shared management message has a corresponding management message of 16e system. The shared management message has the same message type with that of its corresponding management message and its shared management message payload is the same as the message payload with the exception of HMAC/CMAC Tuple of its corresponding management message.

HMAC/CMAC Tuple Sequence consists of HMAC/CMAC Tuples originated by using the key shared between the MR-BS and each node on the multi-hop link respectively. The first HMAC/CMAC Tuple in the HMAC/CMAC Tuple 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 is originated by using the key shared between the MR-BS and last second hop node on the multi-hop link and so on.

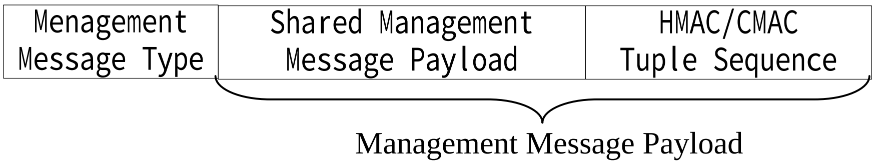

Figure-xx Shared management message format

When the shared message is received by the RS with distributed scheduling on the multi-hop link, the RS shall determine the message type based on the CID in the generic MAC header and Management Message Type in the payload and validate this message's integrity based on the authentication key shared with the MR-BS. If the message is legal, the RS reads the message, deletes the last HMAC/CMAC Tuple in the HMAC/CMAC Tuple Sequence and relays the shared management message to its subordinate node.

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 by 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 by 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 by using the key shared between the MR-BS and MS, this field consists of Management Message Type and Shared Management Message payload.

7.5.4.4 Ciper-based MAC (CMC)

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

7.5.4.4.2 Ciper-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 by 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 by using the key shared between the MR-BS and 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.

References

[1] IEEE 802.16j-07/189, “Construction of MAC PDU with Shared Management Message”, Shulan Feng, Yanling Lu, Ting Li, Liangliang Zhang, Hisilicon Technologies.

.