Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Relaying of Messages of MS(s) by RS with Distributed Security**
Date Submitted	**2007-09-09**
Source(s)	Hang Zhang, Peiying Zhu, Mo-Han Fong, Wen Tong, David Steer, Gamini Senarath, G.Q. Wang, Derek Yu, Israfil Bahceci, Robert Sun and Mark Naden Nortel 3500 Carling Avenue Ottawa, Ontario K2H 8E9 Voice: +613-763-1315 E-mail: wentong@nortel.com Voice: +613-765-8983 E-mail: pyzhu@nortel.com
Re:	IEEE P802.16j/D1: IEEE 802.16j working group letter ballot #28
Abstract	For the distributed security mode, the security materials of a MS are accessible and kept by the access RS of a MS. Such an access RS implements MS message authentication functions. Such an access RS can locally process MS management message. In this contribution, the relaying of this information by an access RS with distributed security is discussed.
Purpose	To incorporate the proposed text into the P802.16j/D1 Baseline Document
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>.

Relaying of Messages of MSs by RS with Distributed Security

Hang Zhang, Peiying Zhu, Mo-Han Fong, Wen Tong, David Steer, Gamini Senarath, Derek Yu, Mark Naden, G.Q. Wang

Nortel

1. Introduction

In current baseline document, both centralized and distributed security modes are described. In the distributed security mode, the security materials of a MS are accessible and kept by the access RS of a MS. Such an access RS implements MS message authentication functions. Such an access RS can locally process MS management message. However, information carried in some management messages needs to be relayed by the RS for between MR-BS and MS. In this contribution, the relaying of this information by an access RS with distributed security is discussed.

2. Proposal

There are number of methods for MS message relay in transmission using R-MAC sub-layer:

One way is similar to the way of an access with centralized security, where the MS MPDU carry message is encapsulated into an R-MAC PDU. In the distributed security case, the authentication field (PN, HMAC/CMAC) in MS message is replayed by authentication field calculated using security materials of the access RS. The issue with this method is the redundant authentication overhead when multiple such MS MPDUs are packed together. The benefit brought by distributed security is not fully utilized.

Another way is to encapsulate one or multiple plain MS MPDUs carrying messages into a R-MAC PDU with a authentication tailor which is calculated using the security materials of the access RS. The issue with this method is that no fragmentation during forwarding is possible. It is difficult to prohibit fragmentation over a wireless multi-hop system due to time-variant radio resource availability.

In fact, since an access RS can authenticate the MS message, the some of MS message body which carries the information that needs to be relayed by the RS between MR-BS and MS can be included in a new message called as RS_MSG_Relay REQ/RSP message. A single such message can include more than one MS message body. The RS_MSG_Relay REQ/RSP messages are management message of RS which can be transmitted over the basic or primary connection of the RS, depending on the connection type of included message bodies. By using this method, the information from multiple MS massage can be easily included in one single RS_MSG_Relay message and only one authentication field is needed. This MPDU carrying this message then is encapsulated into R-MAC PDU. Fragmentation could be performed by any intermediate RS in the forwarding path if needed. Using this method, an access RS can easily to insert some new TLV if needed.

The RS shall create RS_MSG_Relay message in the following way:

- for UL, after receives MS management message(s), RS shall authenticates the sender(s). If the contents need to be forwarded to MR-BS, the RS shall extract the content of available messages and may add some additional TLVs for control purpose and finally add CMAC/HMAC TVL using the RS's security material.

- For DL, MR-BS will do the similar thing. After an RS receives such a message, the RS shall extract the contents, create corresponding types of MAC management message with CMAC using MS's security material.

This message can also be used by other type of access RS to aggregate multiple management messages before authentication performed.

The benefits of above include the low authentication overhead, enabling fragmentation over the forwarding path and easily insert new TLV for control purpose.

3. Proposed text change

[Modify the last row in Table 38 as following]

++++++++++++++++++++++ Start Text +++++++++++++++++++++++++++++++++

Type	Message name	Message description	Connection
98~~-255~~	RS_MSG_Relay-REQ	-	Basic/primary connection Depending on the type of relayed message
99	RS_MSG_Relay-RSP		Basic/primary connection Depending on the type of relayed message
100-255	reserved		

++++++++++++++++++++++ End Text +++++++++++++++++++++++++++++++++

[Add the following section 6.3.2.3.91 as indicated]

++++++++++++++++++++++ Start Text +++++++++++++++++++++++++++++++++

6.3.2.3.91 MS message relay request (RS_MSG_Relay-REQ)

This message is used by MR-BS to forward contents of MS DL unicast management messages to an access RS with distributed security. This message can aggregate contents from multiple MS management messages to be sent on MSs' basic connections or multiple MS management messages to be sent on MSs' primary connections.

The message is also used by an access RS to relay contents of MS UL unicast message to MR-BS. This message can aggregate contents of multiple MS management messages received on MSs' basic connections or multiple MS management messages received on MSs' primary connections. The format of RS_MSG_Relay-REQ is shown in Table XXX.

Table XXX. RS_MSG_Relay request message format.

Syntax	Size	Notes
RS_MSG_Relay request format {		
Management Message Type = 98	8 bits	
Transaction ID	8 bits	Transaction ID of this message
Number of relayed messages	4 bits	Indicates the number of messages whose contents are includes

for (i = 0; i < Number of relayed messages; i ++) {		
CID	16 bits	Basic CID of management connection of MS
Message type	8 bits	Type of message
Length	11 bits	Indicates the length of Message contents in bytes
Message contents	variable	The fields in the message relayed and TLVs (not including MS authentication TLV)
RS specific TLV	Variable	RS specific TLV
}		
Authentication TLV	Variable	CMAC/HMAC TLV
}		

Transaction ID

The transaction ID of this message to coupling this message and corresponding response message RS_MSG_Relay-RSP

Number of relayed messages

The number of MS messages whose contents are included in this message

CID

The CID of management connection on which the MS message is received or to be sent

Message type

The type of MS message carrying the following contents

Length

The length of "Message contents and RS specific TLV" for one relayed message in length

Authentication TLV

Authentication TLV calculated by using the security materials of access RS

++++++++++++++++++++++ End Text ++++++++++++++++++++++++++++++++

[Add the following section 6.3.2.3.92 as indicated]

++++++++++++++++++++++ Start Text ++++++++++++++++++++++++++++++++

6.3.2.3.91 MS message relay request (RS_MSG_Relay-RSP)

This message is used by MR-BS to response RS_MSG_Relay-REQ message sent by an access with distributed security. This message includes contents of MS DL unicast management messages which is to be used for the access RS to create MS management message. The message is also used by an access RS as a response to RS_MSG_Relay-REQ sent by MR-BS. The format of RS_MSG_Relay-RSP is shown in Table XXX.

Table XXX. RS_MSG_Relay response message format.

Syntax	**Size**	**Notes**

RS_MSG_Relay response format {		
Management Message Type = 99		
Transaction ID	8 bits	Transaction ID in the corresponding request message
Number of relayed of messages	4 bits	Indicates the number of messages whose contents are includes
for (i = 0; i < Number of relayed messages; i ++) {		
CID	16 bits	Basic CID of management connection of MS
Message type	8 bits	Type of message
Length	11 bits	Indicates the length of Message contents in bytes
Message contents	variable	The fields in the message relayed and TLVs (not including MS authentication TLV)
RS specific TLV	Variable	RS specific TLV
}		
Authentication TLV	Variable	CMAC/HMAC
}		

Transaction ID

The transaction ID in the corresponding request message RS_MSG_Relay-REQ

Number of relayed messages

The number of MS messages whose contents are included in this message

CID

The CID of management connection on which the MS message is received or to be sent

Message type

The type of MS message carrying the following contents

Length

The length of “Message contents and RS specific TLV” for one relayed message in bytes

Authentication TLV

Authentication TLV calculated by using the security materials of access RS

++++++++++++++++++++++ End Text ++++++++++++++++++++++++++++++++