Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Relay MAC PDU Construction in Centralized Security Scenario**	
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 centralized security mode, the security materials of a MS are kept by the MS and the corresponding MR-BS. The MR-BS performs traffic encryption and message authentication of a MS. This contribution further clarifies the MPDU and R-MAC PDU constructions in this scenario.	
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>.	

Relay MAC PDU Construction in Centralized Security Scenario

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

1. Introduction

In current baseline document, both centralized and distributed security modes are described. In centralized security mode, the security materials of a MS are kept by the MS and the corresponding MR-BS. The MR-BS performs traffic encryption and message authentication of a MS. In the current baseline document, the MPDU and R-MAC PDU constructions in this scenarios needs more detailed descriptions. This contribution is addressing this topic.

2. Proposal

In centralized security scenario, the security materials of a MS are kept by the MS and the corresponding MR-BS. The MR-BS performs MS traffic encryption and decryption. The access RS simply relay encrypted MS MPDUs.

In transmission using tunnel or destination RS CID case, the realy MAC (R-MAC) sub-layer is used to carry encrypted MS MPDUs over forwarding path.

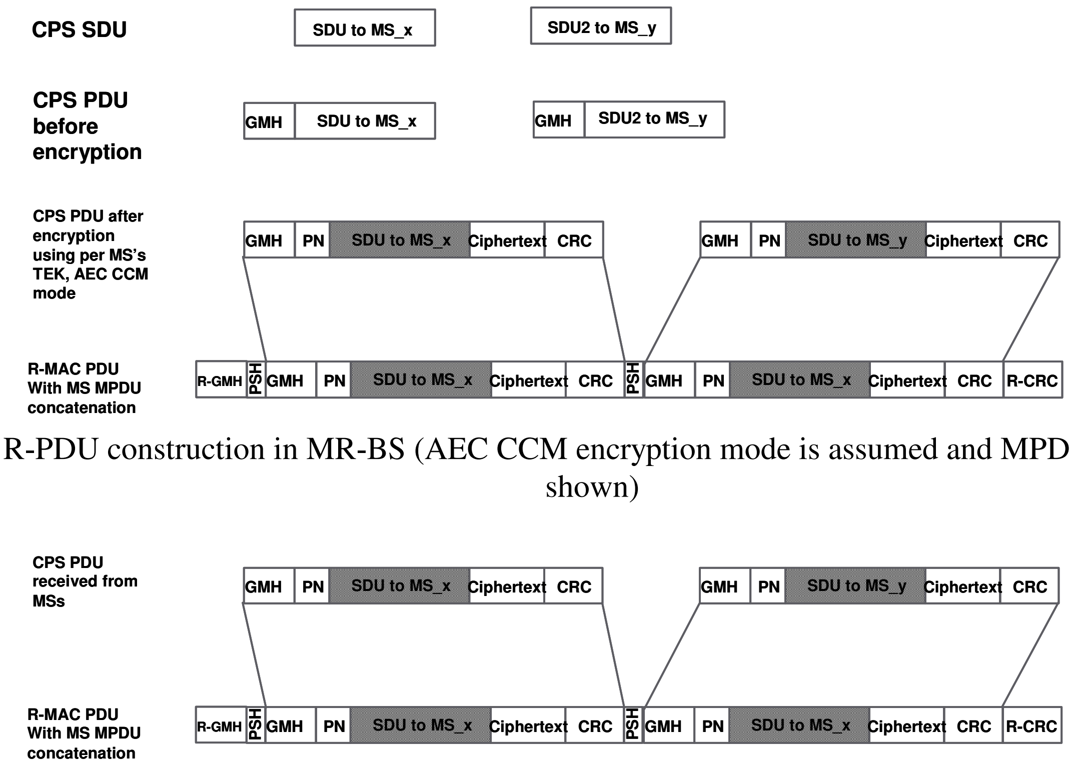
For DL, the MR-BS CPS sub-layer creates MS MAC PDUs encapsulating SDUs of MSs received from upper layer and encrypts the payload of the MPDU using MSs security materials. R-MAC sub-layer then encapsulates one, multiple or a fragment of such MPDU in a R-MAC PDU. The R-MAC PDU is transmitted on R-link and the intermediate RS, if any in the forwarding path, receives the R-MAC PDU and shall de-capsulate the R-MAC PDU and recover any MPDU within the payload which is fragmented by the sender. The intermediate RS reconstructs an R-MAC PDU in the similar way of a MR-BS and send the R-MAC PDU to the next hop RS. The access RS, after receiving an R-MAC PDU over its R-link, the RS shall de-capsulate the R-MAC PDU and recover any MPDU which is fragmented by the sender. Those MPDUs then are sent to MSs over access link of this access RS. Finally, MSs will decrypt MPDUs using their individual security materials and recover SDU carried by MPDUs.

For UL, the access RS receives UL MPDUs from MS over access link. The R-MAC sub-layer of the access RS over R-link encapsulates one, multiple or a fragment of such MPDU in an R-MAC PDU. The processes of R-MAC PDU of intermediate RS(s) are the same as those for DL. The MR-BS, after receiving R-MAC PDUs, shall de-capsulate the R-MAC PDU and obtain MS MPDU(s). Those MS MPDUs are then decrypted by MR-BS using security materials of MSs and the recovered SDUs are delivered to the upper layer.

The R-MAC PDU construction, i.e., fragmentation and packing of MS encrypted MPDUs, follows the same rules defined for MS MPDU construction. The only difference is that the definition of fragment sequence number (FSN) in fragmentation sub-header (FSH) and packing sub-header (PSH). In MPDU, the FSN is meaningful for one MS service flow. In R-MAC PDU, the FSN is meaningful for a particular QoS class or a transport tunnel which could carry an aggregated MS service flow. The FSN is set to each encrypted MS MPDU by R-MAC sub-layer of the source station in the forwarding path and is used to keep the order of MS MPDUs between the two ends of forwarding path.

In the last hop of a forwarding path, the MS MDPU may be sent without using R-MAC PDU.

The R-MAC PDU construction with packing multiple MS MPDUs is shown in Figure 1.



(a) DL R-PDU construction in MR-BS (AEC CCM encryption mode is assumed and MPDU packing is shown)

(b) UL R-MAC PDU construction in access RS (AEC CCM encryption mode is assumed and MPDU packing is shown)

Figure 1. R-MAC PDU construction in centralized security scenario

3. Proposed text change

[Add the following section 6.3.3.8.3 as indicated]

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

6.3.3.8.3 R-MAC PDU construction in relay network

6.3.3.8.3.1 R-MAC PDU construction and forwarding in centralized security scenario

In centralized security scenario, the security materials of a MS are kept by the MS and the corresponding MR-BS. The MR-BS performs MS traffic encryption and decryption. The access RS simply relay encrypted MS MPDUs.

In transmission using tunnel or destination RS CID case, the realy MAC (R-MAC) sub-layer is used to carry encrypted MS MPDUs over forwarding path.

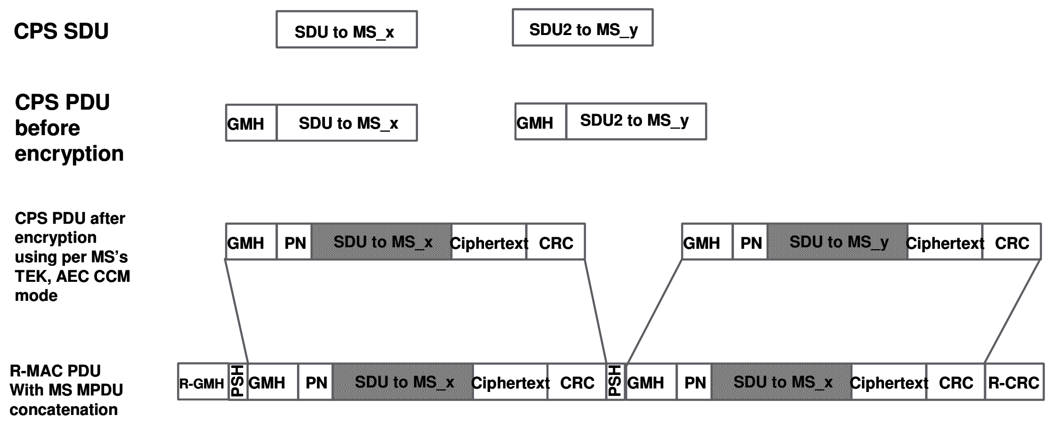
For DL, the MR-BS CPS sub-layer creates MS MAC PDUs encapsulating SDUs of MSs received from upper layer and encrypts the payload of the MPDU using MSs security materials. R-MAC sub-layer then encapsulates one, multiple or a fragment of such MPDU in a R-MAC PDU. The R-MAC PDU is transmitted on R-link and the intermediate RS, if any in the forwarding path, receives the R-MAC PDU and shall de-capsulate the R-MAC PDU and recover any MPDU within the payload which is fragmented by the sender. The intermediate RS reconstructs an R-MAC PDU in the similar way of a MR-BS and send the R-MAC PDU to the next hop RS. The access RS, after receiving an R-MAC PDU over its R-link, the RS shall de-capsulate the R-MAC PDU and recover any MPDU which is fragmented by the sender. Those MPDUs then are sent to MSs over access link of this access RS. Finally, MSs will decrypt MPDUs using their individual security materials and recover SDU carried by MPDUs.

For UL, the access RS receives UL MPDUs from MS over access link. The R-MAC sub-layer of the access RS over R-link encapsulates one, multiple or a fragment of such MPDU in an R-MAC PDU. The processes of R-MAC PDU of intermediate RS(s) are the same as those for DL. The MR-BS, after receiving R-MAC PDUs, shall de-capsulate the R-MAC PDU and obtain MS MPDU(s). Those MS MPDUs are then decrypted by MR-BS using security materials of MSs and the recovered SDUs are delivered to the upper layer.

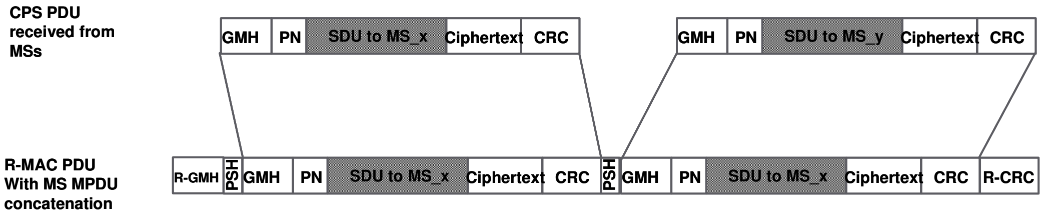
The R-MAC PDU construction, i.e., fragmentation and packing of MS encrypted MPDUs, follows the same rules defined for MS MPDU construction. The only difference is that the definition of fragment sequence number (FSN) in fragmentation sub-header (FSH) and packing sub-header (PSH). In MPDU, the FSN is meaningful for one MS service flow. In R-MAC PDU, the FSN is meaningful for a particular QoS class or a transport tunnel which could carry an aggregated MS service flow. The FSN is set to each encrypted MS MPDU by R-MAC sub-layer of the source station in the forwarding path and is used to keep the order of MS MPDUs between the two ends of forwarding path.

In the last hop of a forwarding path, the MS MDPU may be sent without using R-MAC PDU.

The R-MAC PDU construction with packing multiple MS MPDUs is shown in Figure xxx.



a) DL R-PDU construction in MR-BS (AEC CCM encryption mode is assumed and MPDU packing is shown)



b) UL R-MAC PDU construction in access RS (AEC CCM encryption mode is assumed and MPDU packing is shown)

Figure xxx. R-MAC PDU construction in centralized security scenario.

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