Project	**IEEE 802.16 Broadband Wireless Access Working Group <**http://ieee802.org/16**>**	
Title	**Relay MAC PDU Construction in Distributed 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 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 traffic en/decryption and message authentication functions and MS SDUs are visible to access RS. In this contribution, the MPDU and R-MAC PDU construction are proposed.	
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 Distributed 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 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 traffic en/decryption and message authentication functions and MS SDUs are visible to access RS. Therefore, in DL, all SDUs to MSs attached to an access RS can be viewed as SDUs targeting to the access RS. In UL, all received MAC SDUs from MSs by an access RS can be viewed as the SDUs originated from this RS.

In transmission using tunnel or destination RS CID, for MS SDUs forwarding,
One is that

- for MS SDUs, per MS transport connection MPDUs are created
- each such a MPDU is encrypted using the security materials of the corresponding access RS
- One or multiple such MPDUs are encapsulated into one R-MAC PDU for forwarding purpose

One alternative way is that

- establish a transport connection between MR-BS and an access RS
- MS SDUs from the same or different service flows are encapsulated into a single MPDU of the RS
- each such a MPDU is encrypted using the security materials of the corresponding access RS
- such a MPDU is encapsulated into a R-MAC PDU for forwarding purpose

The main reason of introducing the second method is to utilize the benefit of distributed security (RS is able to process MS traffic at SDUs level) to minimize the encryption overhead.

Since each encrypted MPDU has the overhead related to encryption (12 bytes for AEC CCM) and CRC (4 bytes). When N MS SDUs can be forwarded together using R-MAC PDU, the encryption and CRC overhead in first method would be N times of that of second method. This overhead issue becomes severer for short SDUs (VoIP) case.

In this contribution, the MPDU and R-MAC PDU construction are proposed when the second method is implemented.

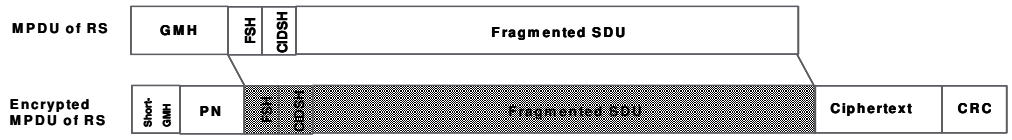
2. Proposal

Between a MR-BS and an access RS with distributed security, one DL transport connection and one UP transport connection shall be established during network entry. The DL transport connection of this RS is used for carrying SDUs targeting to MSs attached to this RS. The UL transport connection of this RS is used to carry MS SDUs received from MSs by an access RS. These transport connections of an RS are different from transport tunnels connections assigned to the same RS. The transport connections are used to carry MSs SDUs in MPDU format while the tunnel connections are used to carry MPDU in R-MAC format.

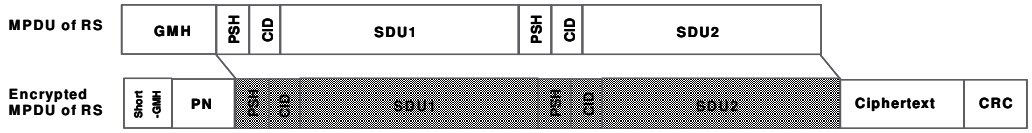
2.1 Construction of MPDU on transport connection between MR-BS and an access RS

The construction of transport connection MPDU of an access RS is the same as that of MS MPDU except that a MPDU of an RS can encapsulate MS SDUs from difference service flows. In order to indicate the service flow of a SDU, a 2-byte CID sub-header shall precede a SDU. The CID is corresponding to the SFID of the SDU. The CID sub-header will always present in such a MPDU and no CID sub-header flag in GMH is needed. This sub-header presents immediately after a fragmentation sub-header or a packing sub-header whichever presents. When neither of these two sub-headers presents, the CID sub-header will present as the last sub-header. The CID field in GMH of such a MPDU is the CID of transport connection assigned to the RS. In DL, the CPS sub-layer on R-link of MR-BS shall create MPDU of an access RS. In UL, The CPS sub-layer on R-link of the access RS shall create its transport connection MPDU.

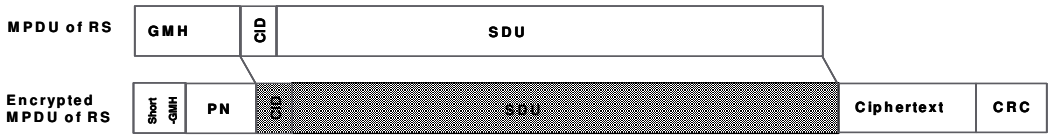
The MPDU construction is illustrated by Figure 1.



(a) Format of MPDU of RS (fragmentation case)



(b) Format of MPDU of RS (packing case)



(c) Format of MPDU of RS on (no fragmentation/packing case. AEC CCM encryption assumed)

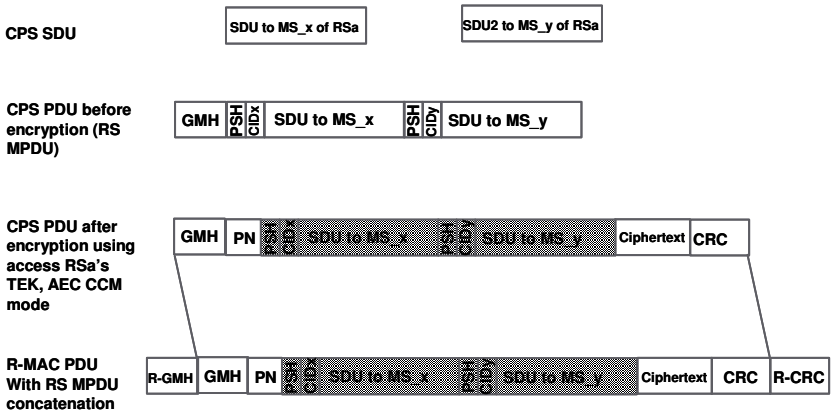
Figure 1. The RS MAC PDU of an access RS in distributed security scenario.

2.2 Construction and process of R-MAC PDU

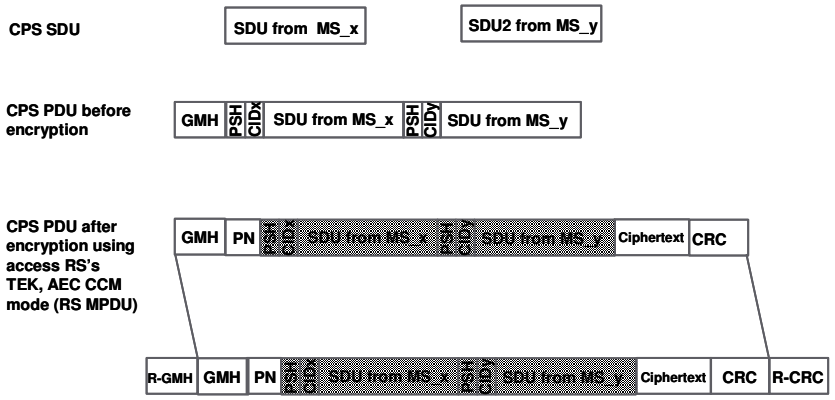
For DL, in transmission using tunnel or destination RS CID case, the security sub-layer on R-link of MR-BS (DL) or access RS (UL) shall provide the encrypted RS transport connection MPDU to R-MAC sub-layer. R-MAC sub-layer shall encapsulate one or a fragment of an RS MPDU into R-MAC PDU. The intermediate RS, if any in the forwarding path, shall process an R-MAC PDU in the same way as in a centralized security scenario. The R-MAC sub-layer on R-link of access RS (DL) or MR-BS (UL), after receiving an R-MAC PDU, shall de-capsulate the R-MAC PDU and recover any fragmented MAC PDU and provide MAC PDU to security sub-layer on R-link.

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

The R-MAC PDU construction is illustrated in figure 3. Please note that this figure only shows the case where there is fragmentation and packing of MPDU by R_MAC sub-layer. Packing and fragmentation of MPDU by R-MAC are possible.



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



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

Figure 3. R-MAC PDU construction in distributed 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

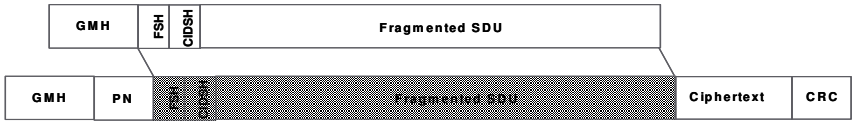
6.3.3.8.3.2 MAC PDU and R-MAC PDU construction in distributed security scenario

In the distributed security mode, the security materials of a MS are accessible and kept by the access RS of the MS. Since the access RS has the MS security materials, the RS process MSs' traffic can be at MAC SDU level, instead of on MS encrypted MPDU level like in centralized security scenario. Therefore, in DL, all SDUs to MSs attached to an access RS shall be viewed as SDUs targetting to the access RS. In UL, all received MAC

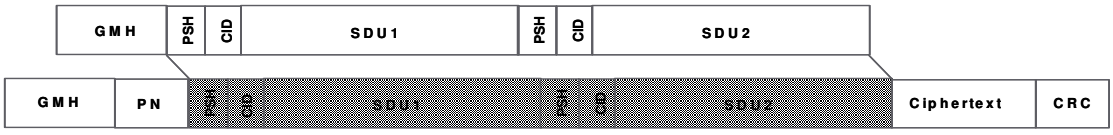
SDUs from MSs by an access RS can be viewed as the SDUs originated from this RS. For MS SDU forwarding by an access RS, one DL transport connection and one UP transport connection shall be established during network entry. These transport connections of an RS are different from transport tunnels connections assigned to the same RS. The transport connections are used to carry MSs SDUs in RS MPDU format while the tunnel connections are used to carry RS MPDU in R-MAC format.

6.3.3.8.3.2.1 Construction of MPDU on the connection between MR-BS and an access RS

The construction of transport connection MPDU of an access RS is the same as that of MS MPDU except that a MPDU of an RS can encapsulate MS SDUs from difference service flows. In order to indicate the service flow of a SDU, a 2-byte CID sub-header shall precede a SDU. The CID is corresponding to the SFID of the SDU. The CID sub-header will always present in such a MPDU and no CID-sub-header flag in GMH is needed. This sub-header presents immediately after a fragmentation sub-header or a packing sub-header whichever presents. When neither of these two sub-headers presents, the CID sub-header will present as the last sub-header. The CID field in GMH of such a MPDU is the CID of transport connection assigned to the RS. In DL, the CPS sub-layer on R-link of MR-BS shall create MPDU of an access RS. In UL, The CPS sub-layer on R-link of the access RS shall create its transport connection MPDU. The MPDU construction is illustrated by Figure xxx.

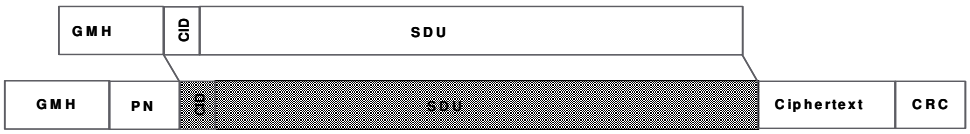


(a) Format of MPDU of RS (fragmentation case before and after encryption)



(b)

(b) Format of MPDU of RS (packing case before and after encryption)



(c) Format of MPDU of RS on (no fragmentation/packing case before and after encryption)

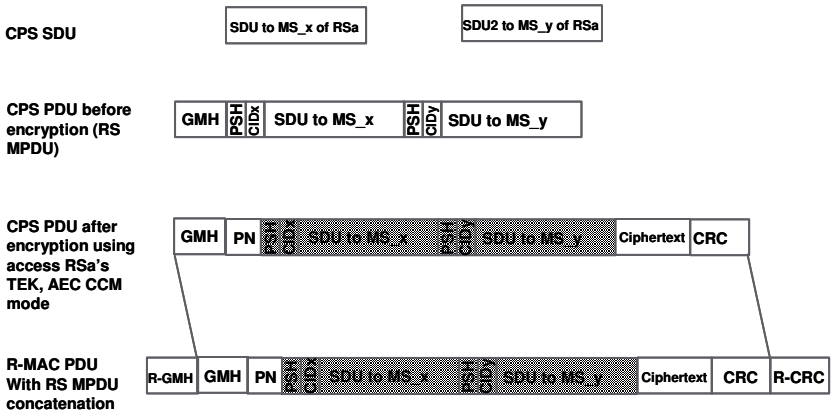
Figure xxx. The RS MAC PDU of an access RS in distributed security scenario.

6.3.3.8.3.2.2 Construction and process of R-MAC PDU

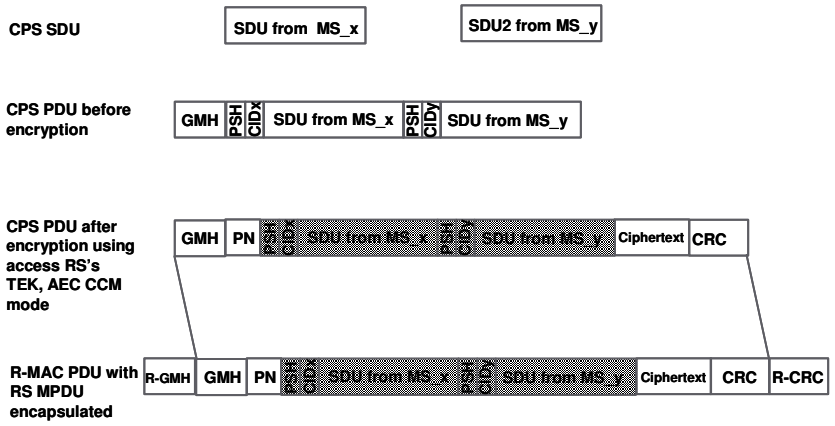
For DL, in transmission using tunnel or destination RS CID case, the security sub-layer on R-link of MR-BS (DL) or an access RS (UL) shall provide the encrypted RS MPDU to R-MAC sub-layer. R-MAC sub-layer shall encapsulate one or a fragment of an RS MPDU into R-MAC PDU. The intermediate RS, if any in the forwarding path, shall process an R-MAC PDU in the same way as in a centralized security scenario. The R-MAC sub-layer on R-link of access RS (DL) or MR-BS (UL), after receiving an R-MAC PDU, shall de-capsulate the R-MAC PDU and recover any fragmented MAC PDU and provide MAC PDU to security sub-

layer on R-link.

In the last hop of a forwarding path, the RS transport connection MDPU may be sent without using R-MAC PDU. The R-MAC PDU construction is illustrated in Figure xxx.



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



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

Figure XXX. R-MAC PDU construction in distributed security scenario (no packing/fragemention case).

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

[Add the section 6.3.2.2.8 as indicated]

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

6.3.2.2.8 CID sub header

The CID sub-header is used to indicate the CID assigned to the service flow of following SDU in MAC PDU of RS with distributed security function. This sub-header will always present and no CID sub-header flag In GMH

is needed. This sub-header immediately follows either the fragmentation sub-header or packing sub-header whichever presents, or presents as the last sub-header if neither fragmentation sub-header nor packing sub-header presents.

The CID sub-header field encoding is show in Table xxx.

Table xxx. Local CID sub-header field encoding

Name	Length (bits)	Description
CID	16	CID assigned to the corresponding service flow of the following SDU in a RS MPDU

++++++++++++++ End text ++