Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Piggyback Bandwidth Request Handling in Distributed Scheduling**
Date Submitted	**2007-04-25**

Source(s)	Masato Okuda and Yuefeng Zhou Fujitsu	okuda@jp.fujitsu.com Yuefeng.Zhou@uk.fujitsu.com

Re:	IEEE802.16j-07/013: “Call for Technical Comments Regarding IEEE Project 802.16j”
Abstract	This contribution proposes a distributed bandwidth request and allocation mechanism.
Purpose	To propose text to describe a distributed bandwidth request and allocation mechanism
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>.

Piggyback Bandwidth Request Handling in Distributed Scheduling

Masato Okuda and Yuefeng Zhou

Introduction

In distributed scheduling systems, an access RS shall cope with all kinds of bandwidth request from MSs. The current 16e standard specifies the following request schemes.

1) Signaling Header

- Bandwidth Request Header (Incremental/Aggregate)
- BR and UL Tx Power Report Header
- BR and CINR Report Header
- BR and Uplink sleep control Header

2) Grant Management Subheader

- Piggybacked Bandwidth Request

3) Contention based CDMA Bandwidth Request Mechanism

4) CQICH

- codeword (0b111011) for bandwidth request to ertPS connection.

Among the above bandwidth request schemes, RS may not be able to get directly piggybacked bandwidth request information from MS since the Grant Management Subheader may be encrypted.

However, the current baseline document does not mention this problem at all. So, it is necessary to describe clearly how to process the piggybacked bandwidth Request at the access RS in distributed scheduling systems.

Proposed Schemes

How to handle piggybacked bandwidth request depends on MAC-PDU decryption capability of RS. Focusing on MAC-PDU decryption capability of RS, we use the terms, distributed security where RS can decrypt MAC-PDUs and centralized security where RS cannot decrypt MAC-PDUs in this contribution. Therefore, distributed or centralized security may be used for other meanings in different contributions.

<Distributed Security>

Since RS can decrypt MAC-PDUs, RS can derive piggybacked bandwidth request information from the grant management subheader and handle it locally as other bandwidth request. So, all kinds of bandwidth requests shall be locally handled by the access RS in distributed security systems.

<Centralized Security>

In centralized security systems, all all kinds of bandwidth requests except for encrypted piggybacked bandwidth request shall be locally handled by the access RS.

As for encrypted bandwidth request, the MR-BS decrypts MAC-PDUs and forwards piggybacked bandwidth request information to the access RS since RS cannot decrypt MAC-PDUs. See Figure 1.

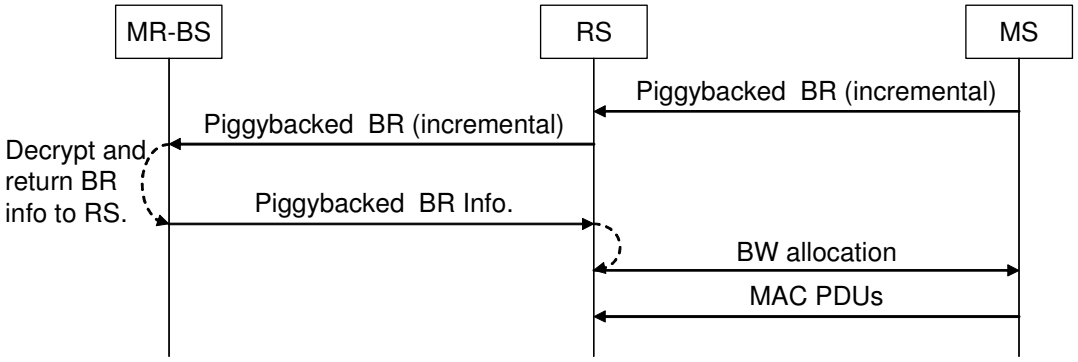

Figure 1 Forwarding PB-BR from MR-BS to RS

According to the current standard, MS must send BR header (Aggregate) periodically. Therefore, based on the Aggregate BR header, the RS may allocated all bandwidth requested by the MS before receiving PB-BR information from the MR-BS. In this case, bandwidth allocation based on the returned PB-BR information could be wasted. See Figure 2.

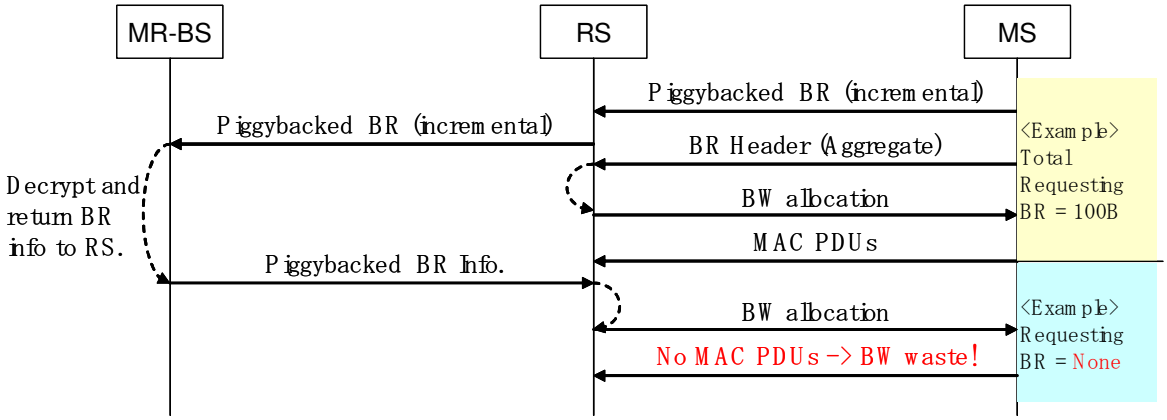

Figure 2 Aggregate BR Header Superseding incremental PB-BR

To prevent the above problem, Piggybacked BR Info sent by MR-BS shall contain packet number of MAC-PDU to which the Piggybacked BR request is attached. A MAC-PDU encrypted with AES-CCM shall contain unencrypted packet number. The access RS can use this value to manage ordering of bandwidth requests received from MS directly and via MR-BS.

Specific Text Changes

[Insert the following new subclause at the end of 6.3.2.3:]

6.3.2.3.X MR_PBBR-INFO message

This message is used to notify encrypted piggybacked BW request information to RS. This message is transmitted by MR-BS with using the RS's basic CID.

Table xx MR PBBR-INFO message Format

Syntax	Size	Note
MR_Piggybacked_Bandwidth Request Information Format(){		
Management Message Type = xx	8 bits	TBA
N_PB-BR_INFO	8 bits	Number of PB-BR Information
for (i=0; i<N_PB-BR_INFO; i++) {		
CID	16 bits	The CID shall indicate the connection for which uplink bandwidth is requested.
PN_Flag	1	0: indicates Packet Number field is invalid 1: indicates Packet Number field is valid
Packet Number	31 bits	Packet Number which is attached to MAC-PDU containing the grant management subheader
Grant Management Subheader Information	16 bits	See Table 9.
}		
TLV Encoded Information	variable	TLV Specific
}		

The MR_PBBR-INFO message shall include the following parameter encoded as TLV tuples:

HMAC/CMAC Tuple (See 11.1.2.)

[Add the following text at the end of 6.3.6.7.1 in the page 48 (line26)].

An access RS receives various types of bandwidth requests from MSs, such as signaling header, grant management subheader, CDMA bandwidth request code and so on. Among those request types, only Grant Management subheader may be encrypted and cannot be derived by the RS. Therefore, depending on RS capability of decrypting MAC-PDUs, there are two different ways to handle the Grant Management subheader. RS capable of decrypting MAC-PDUs shall locally handle all kinds of bandwidth requests from MS. Meanwhile, RS incapable of decrypting MAC-PDUs shall locally handle all kinds of bandwidth requests except for grant management subheader from MS. For this type of RS, the encrypted Grant Management header is decrypted by the MR-BS, and then forwarded to the RS using MR_PBBR-INFO message. When the RS receives MR_PBBR-INFO, it confirms whether content of the message is superseded by a standalone BW request header (aggregate) with checking Packet Number if PN_Flag is set to 1 (valid). MR-BS set PN_Flag to 0 (invalid) if the MAC-PDU does not contain Packet Number. When a RS incapable of decrypting MAC-PDUs detects Grant Management subheader on UGS connection from the type field of the GMH, it may allocate a small amount of bandwidth to the MS sending the subheader.