MAC PDU and GMH Design

IEEE 802.16 Presentation Submission Template (Rev. 9)

Document Number:

IEEE C802.16m-08/652r1

Date Submitted:

2008-07-11

Source:

Haihong Zheng, Shashikant Maheshwari, Adrian Boariu,
Yousuf Saifullah
Nokia Siemens Networks E-mail: haihong.zheng@nsn.com

Andrea Bacioccola E-mail: andrea.bacioccola@nokia.com
Nokia

Venue:

IEEE 802.16m-08/024, “Call for Comments and Contributions on Project 802.16m System Description Document (SDD)”.
Target topic: “Upper MAC concepts and methods - Addressing”.

Base Contribution:

This is the base contribution.

Purpose:

To be discussed and adopted by TGm for the 802.16m SDD

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:

Patent Policy:

Motivation

- 802.16e GMH and MAC PDUs include unnecessary overhead
  - Some fields in GMH are not needed, or can be signaled using other mechanisms
  - Using 16 bit CIDs to identify individual connections is a waste of resource
  - Encoding of subheader and extended subheader can be further optimized
  - Using HCS and CRC simultaneously is not necessary
- Optimization of GMH and MAC PDUs in .16m is needed
  - Reduce size of GMH
  - Remove unnecessary overhead in MAC PDUs
  - Introduce new features

MS Identifier and Connection Index

- Each MS is assigned with a 12-bit MS Identifier (MSId), which uniquely identifies the MS within the cell.
- A connection is a mapping between BS and MS MAC peers, and is uniquely identified by a 4-bit Connection Index (CI) within the MS.
  - The management connections (i.e., basic/primary/secondary connections) are automatically assigned with pre-defined Connection Index values.
  - A transport connection is assigned with a Connection Index during service flow setup.
  - Connection Index is bidirectional for management connections and uni-directional for transport connections.
- The combination of MSId and CI uniquely identifies a connection within the cell.
- For each UL or DL allocation, the MS Identifier is included in the MAP IE, while the Connection Index for the connection is included in the GMH.
- Refer to contribution C80216m-08_645 and later version for more details
- This contribution propose schemes on MAC PDU/header design including how to convey MS Identifier and Connection Index information in the MAC header.

GMH Optimization – Removal of EC bit

- Each transport connection is mapped to a Security Association (SA).
- The mapping is achieved during DSA/DSC procedure.
- Therefore, the connection index in the GMH already indicates whether the payload is encrypted or not, and there is no need to include EC bit.

GMH Optimization – CRC, HCS and CI bit

- When HARQ is enabled for a connection, the associated MAC PDUs are protected with HARQ CRC. In such case, there is no need to use CRC or HCS to protect the MAC PDU or GMH.
- It is the service flow requirement that whether or not CRC shall be enabled to protect the traffic. Therefore it shall be determined during service flow setup.
  - Such feature can be implemented by changing bit 6 in Request/Transmission Policy parameter in SF parameter to be “the service flow shall include CRC in MAC PDU”.
  - If such bit is set, then CRC shall be attached unless HARQ is enabled and HCS shall be omitted from the GMH.
- In general, the following default protection rules can be applied:
  - If HARQ is enabled for the connection, CRC for the MAC PDU and HCS for the GMH is not present.
  - If HARQ is not enabled for the connection and if CRC is enabled, CRC shall be attached to the MAC PDU and HCS in the GMH is not present.
  - If neither HARQ nor ARQ is enabled for the connection, HCS shall be present in GMH.
  - Using such default rule, there is no need to include CI bit in GMH.
- The management connections shall always be protected with CRC unless HARQ is enabled for these connections.

GMH/MPDU optimization – Masked CRC/HCS

- When power is not an issue for devices such as laptop, the MS can decode all the received MPDU to find out if the data is for itself or not. Therefore, no MSId needs to be included in DL-MAP.
- Possible issues: if MSId in DL-MAP is erroneous and not detected by the MAP CRC, the MS with the wrong MSId assumes the data is for itself.
- To address this issue, the HCS or CRC whichever is present can be masked with MSId.
  - If HARQ is enabled, HARQ CRC is masked with MSId.
  - If HARQ is not enabled and CRC is enabled, CRC is masked with MSId.
  - Otherwise, HCS is masked with MSId.
- Three possible schemes to mask CRC/HCS using MSId
  - Xor MSId with the LSBs of CRC (CRC16 or CRC32)
  - Xor first byte and second byte of MSId and then xor with HCS
  - MSId is appended to the end of GMH when CRC or HCS is calculated

GMH optimization – Subheader Presence Indication

- The Type field in .16e GMH indicates the presence of subheaders and extended subheaders.
- FSN size is defined in the FSN size TLV in DSA messages during service flow setup. Thus the connection index already indicate the size of FSN, and there is no need to have Extended Type bit in the Type field in GMH.
- Only 4 bit is needed to indicate the presence of Fragment subheader, Packing subheader, Extended Packing subheader, Grant management subheader/Fast-feedback allocation subheader, and Extended subheaders.
  - Bit #3: presence of Extended Subheader (see slide #12)
  - Bit #2 and #1: presence of fragmentation, packing and/or extended packing subheader
    - 00: fragmentation subheader
    - 01: packing subheader
    - 10: extended packing subheader
    - 11: reserved
  - Bit #0: presence of FFSH (DL) or GMSH (UL)

Proposed Normal GMH Format

<table>
<tr><td colspan="1">Hdr Type (1)</td><td colspan="1">Com (1)</td><td colspan="4">Subheader Presence (4)</td><td colspan="2">EKS (2)</td><td colspan="1">AFP (1)</td><td colspan="7">LEN MSB (7)</td></tr>
<tr><td colspan="4">LEN LSB (4)</td><td colspan="4">Connection Index (4)</td><td colspan="8">HCS (8) - optional</td></tr>
</table>

- Hdr Type: Header Type (0 - GMH, 1 - signaling header)
- Com: Indicate the GMH format (0 - normal GMH, 1- compressed GMH (see slide #9))
- Subheader Presence: Indicate presence of subheaders or extended subheader in the payload
- EKS: Encryption key sequence
- AFP: Indication of presence of ARQ feedback payload
- Connection Index (CI): Connection Index of the connection
- LEN: the length of the MAC PDU including MAC header and CRC if present
- HCS: header check sequence (only present when neither HARQ nor CRC is enabled for the connection)

GMH Optimization – Compressed GMH

- The resource assigned in persistent allocation is for a specific connection. Therefore, connection index is not needed in the GMH.
- Persistent allocation is normally used for periodical traffic such as VoIP with small size packet. Therefore, the length of MPDU is normally small.
- A compressed GMH can be used instead of normal GMH for persistent allocation to further reduce GMH overhead.

Proposed Compressed GMH Format

Hdr Type (1)	Com (1)	Subheader Presence (4)	EKS (2)	AFP (1)	LEN (7)
HCS (8) - optional					

- Hdr Type: Header Type (0 - GMH, 1 - signaling header)
- Com: Indicate the GMH format (0 - normal GMH, 1- compressed GMH)
- Subheader Presence: Indicate presence of subheaders in the payload
- EKS: Encryption key sequence
- AFP: Indication of presence of ARQ feedback payload
- LEN: the length of the MAC PDU including MAC header and CRC if present
- HCS: header check sequence (only present when neither HARQ nor CRC is enabled for the connection)

GMH optimization – Piggyback BR

- In 802.16e, the piggyback bandwidth request carried in grant management subheader can only be applied to the CID carried in the GMH
- It happens very often that MS needs b/w for other connections

<table>
<tr><td>Ext
(1) =1</td><td>Connection
Index (4)</td><td>Piggyback BR 1 MSB (3)</td></tr>
<tr><td colspan="3">Piggyback BR 1 LSB (8)</td></tr>
<tr><td colspan="3">….</td></tr>
<tr><td>Ext
(1) =0</td><td>Connection
Index (4)</td><td>Piggyback BR n MSB (3)</td></tr>
<tr><td colspan="3">Piggyback BR n LSB (8)</td></tr>
</table>

Optimization in .16m

- Each piggyback BR contains Ext bit, connection index and requested bandwidth
- Multiple piggyback BRs may be present in one grant management subheader
- Ext bit indicates if more piggyback BR follows

GMH Optimization – Extended Packing Subheader (1)

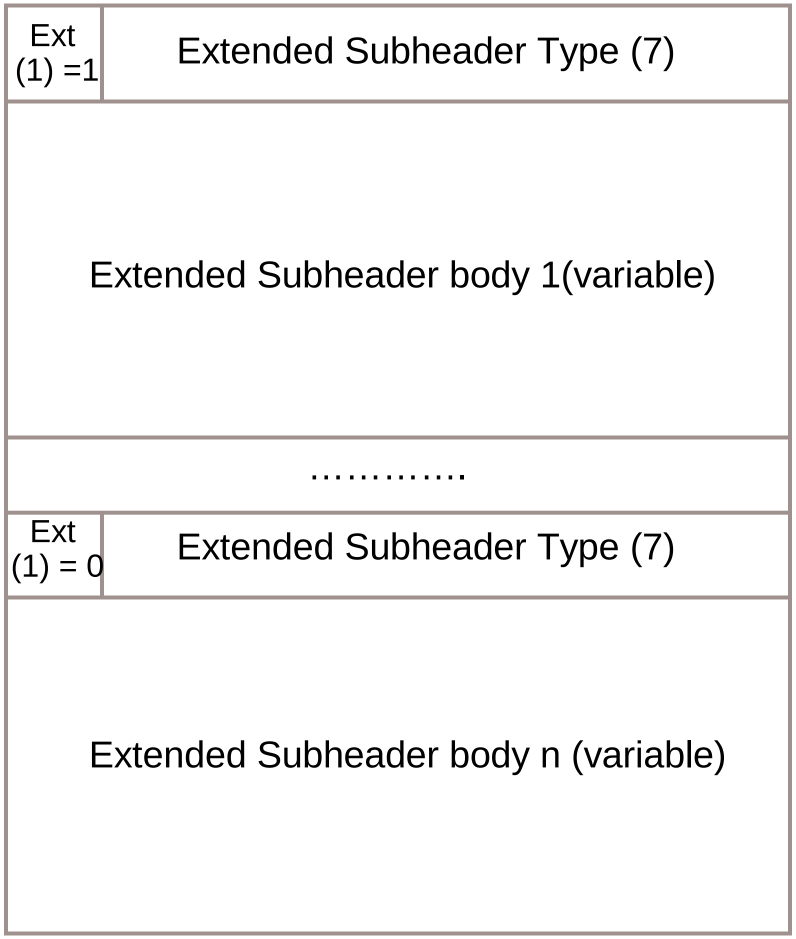
- In 802.16e, packing is only applied to the SDUs belonging to the same connection of an MS. If SDUs from different connections of an MS need to be sent in one burst, only concatenation can be used. This introduce overhead.
- In 802.16m, an Extended Packing Subheader (EPSH) can be used to pack SDUs from different connections of an MS into one MAC PDU.

Syntax	**Size**	**Notes**
Extended Packing Subheader() {		
FSI	1	First SDU Indication – indicate if it is the 1st SDU/SDU fragment for the same connection
If (First SDU Indication == 1) {		
Connection Index	4	Connection Index
EKS	2	Encryption Key Sequence
} else {		
Rsv	6	Reserved
}		
FC	2	Same as defined in PSH
If (ARQ-enabled Connection)	-	
BSN	11	Same as defined in PSH
else {	-	
if (Extended Type)	-	
FSN	3	Same as defined in PSH
else	-	
FSN	11	Same as defined in PSH
}	-	
Length	11	SDU/SDU fragment length including EPSH
Rsv	1	Reserved
}		

GMH Optimization – Extended Packing Subheader (2)

- The SDU/SDU fragments belonging to the same connection are packed adjacent to each other.
  - The first SDU/SDU fragment belong to the same connection uses the EPSH with the First_SDU_Indication (FSI) bit set to 1 and the CI and EKS fields in the EPSH contains the CI and EKS for the connection.
  - All the other SDUs/SDU fragments in the same connection is packed afterward, with the FSI bit in EPSH set to 0, and assumes that the same CI and EKS fields defined in the EPSH for the first SDU/SDU fragment with the same connection apply.
- When EPSH is present, the Connection Index and EKS fields in the GMH is not valid.
- If CRC is enabled for the connection, it is used to protect all the SDU/SDU fragment belonging to the same connection.
  - If CRC is enabled for the SDUs/SDU fragments for the first connection, the CRC shall protect the GMH and all the other subheaders/extended subheaders before the first EPSH plus SDUs/SDU fragments on the first connection; otherwise, HCS is included in the GMH.
  - If CRC is enabled for the following SDU/SDU fragments, the CRC shall protect the SDU/SDU fragments together with correspondent EPSH for the same connection.

GMH optimization – Extended Subheader



Ext (1) =1

Extended Subheader Type (7)

Extended Subheader body 1(variable)

………….

Ext (1) = 0

Extended Subheader Type (7)

Extended Subheader body n (variable)

- Use the Ext bit to indicate if there is another extended subheader follows
- There is no need to have Extended Subheader Group Length

Signaling Header optimization – BR Header

- Issues with .16e Bandwidth request and other signaling headers
  - Bandwidth Request and other signaling headers are not protected
    - Any entity can generate BR and other signaling header on behalf of another MS. BS cannot verify if the request is sent from a legitimate user.
    - Rogue SS could make false uplink bandwidth requests and waste precious uplink bandwidth.
    - Rogue MS could send BR header on behalf of other MS with bandwidth request of “ZERO” byte, which leads to Denial of Service attack.
  - Aggregate Bandwidth Request contains 19 bits
    - It’s not often for an MS to request for 512k bytes in one bandwidth request.
    - If more bandwidth is needed, a piggyback BR could be used.
    - Is 19 bit selected in .16e just for the purpose of byte alignment?
  - BR is in the unit of bytes
    - BS allocate resource in the unit of radio block in .16m. Thus it makes sense for MS to request for bandwidth in the unit of radio block.
  - Incremental BR is sent together with other signaling
    - How often does an MS sends BR and other signaling together?
    - If not, only aggregate BR is used and other signaling headers are sent by itself.

Authenticated BR Header

- Bandwidth Request and other signalling headers shall be authenticated, by replacing HCS with Authenticated HCS (A-HCS).
- The checksum for header is calculated as following:
  - A-HCS = CMAC(CMAC_KEY_U$\otimes$counter, 5-byte-checksum) mod (D8+D2+D+1)
- Therefore the BR header and other signalling header has error and integrity protection at the same time.
- Counter is a monotonically increasing number, which is of the same bit-length of CMAC/HMAC_KEY_U. The purpose to ensure that even though the A-HCS is only 8 bits long, it’s harder for the attacker to find a HCS collision and replay the message for bandwidth request.

Proposed Bandwidth Request Header Format

<table>
<tr><td colspan="1">Hdr Type (1)</td><td colspan="1">Sig Hdr Type (1)</td><td colspan="6">Counter LSB (6)</td><td colspan="8">BR MSB (8)</td></tr>
<tr><td colspan="8">BR LSB (8)</td><td colspan="8">MSId MSB (8)</td></tr>
<tr><td colspan="4">MSId LSB (4)</td><td colspan="4">Connection Index (4)</td><td colspan="8">A-HCS (8)</td></tr>
</table>

- Hdr Type: Header Type (1 for BR and other signaling header)
- Sig Hdr Type: Signaling Header Type (0 for BR and 1 for other signaling header)
- Counter LSB: the LSBs of counter
- BR: bandwidth requested in the unit of resource block
- MSId: MSId of the MS
- Connection Index: connection index for the connection requesting for b/w
- A-HCS: Authenticated HCS

Proposed text changes for 802.16m SDD (1)

- Section 10.x: MAC PDU Services and Functions
  - Each MAC PDU contains a MAC header, optional payload and optional CRC.
  - MAC header contains signalling information without payload or begins each MAC PDU containing either MAC management messages or user data. It only contains information that cannot be derived from DL control and signalling information or service flow information.
  - Multiple MAC PDUs from different MSs could be concatenated into a single transmission. One MAC SDU or MAC management message could be fragmented into one or more MAC PDUs. Multiple MAC SDUs or MAC management messages from the same MS could be packed into one MAC PDU.

Proposed text changes for 802.16m SDD (2)

- MAC PDU or MAC header could be protected using one type of error detection mechanism.
  - If PHY level error detection (e.g., HARQ) is enabled for the connection, no other error detection is applied to the MAC PDU and MAC header.
  - If no PHY level error detection is enabled, but CRC is enabled for the connection, no other error detection is applied for MAC header.
  - Otherwise, error detection on MAC header is applied.