Project	**IEEE 802.16 Mobile Broadband Wireless Access Working Group** <**http://ieee802.org/16**>
Title	**Flexible Data Encryption Location**
Date Submitted	**[2004-05-07]**
Source(s)	Yong Chang Samsung Elec. 416, Maetan-3dong, Youngtong-gu Suwon-si, Gyeonggi-do Korea
Re:	Working Group Review of P802.16-REVe_D2
Abstract	Enhance the Privacy sublayer for P802.16-REVe_D2 to allow the flexible data encryption location
Purpose	Propose the text in Privacy sublayer for IEEE802.16REVe/D2-2004
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>.

1. Introduction

The current IEEE P802.16-REVe/D2-2004 assumes that the data encryption has to be performed after packing and fragmentation of a MAC PDU. This assumption may cause some kinds of limitations and a little performance degradation.

- A little performance degradation

It is noted that a little performance degradation, increased consumption of encryption processing power caused by the repetition of the same data encryption whenever the frame of a encrypted MAC PDU is lost under ARQ situation.

However, if we allow encrypting a data before packing and fragmentation of a MAC PDU, a little gain of encryption processing power is achieved. The following comparison table shows how much gain can be obtained comparing to the current data encryption mechanism.

- Assumptions
  1. Type I : The data encryption on a MAC PDU is performed after packing and fragmentation
  2. Type II : The data encryption on an IP packet is performed before packing and fragmentation
  3. Traffic Types : Voice, Packet Data
     - Since voice traffic is requesting a constant bandwidth, the RTP/UDP/IP packet with voice encoder bits are almost the same. We assume that the IP packet is 40 bytes. MAC PDU size of this IP packet is constant, just adding bytes of MAC header in addition to the IP packet as MAC SDU. ARQ is not applied to voice.
     - For Packet data, we assume that the IP packet size is 1500 bytes, and this packet is fragmented to 5 MAC PDUs of 300-byte size.
  4. Block retransmission overhead or ARQ block error rate is assumed 10%
  5. Metric is the number of how many encryption is performed

	Type I	Type II
Voice	One MAC PDU is to be encrypted.	One IP packet is to be encrypted. No gain comparing to Type I. Reason: Since one IP packet is encapsulated into one MAC PDU, no gain is achieved.

Data	The encryption is to be performed 5.5 times than Type II. 5 MAC PDUs and 0.5 retransmitted MAC PDU under 10% FER ARQ are to be encrypted	One IP packet as MAC SDU is to be encrypted. Even 10% FER ARQ is to be performed, there is no need to retry to encrypt an IP packet.

- Inefficiency of broadcast service support

Now, broadcast service with mobility is being deployed over the world, e.g., DMB(Digital Multimedia Broadcast service), MBMS(Multicast Broadcast Multimedia Service) of 3GPP and BCMCS(Broadcast and Multicast service) of 3GPP2. We make sure that 802.16e will provide the broadcast service as soon as possible. What feature we have to keep in mind for broadcast service support is that the same broadcast content is to be transferred in the secure manner from the broadcast content server to all subscribers locating anywhere. That is, the same broadcast content encrypted by the same encryption key is to be transmitted over the air from all BS to all registered subscribers for broadcast service at the same time. Therefore, the most architecture for broadcast service support is designed in the centralized manner because it's efficient for a centralized network entity to encrypt the content, transfer the same content to all subscribers.

Now, if the encryption for broadcast service is performed after packing and fragmentation, the encryption key shall be transferred from the network entity generating the encryption key to network entity encrypting MAC PDU. This is inefficient because the encryption key has to be transferred whenever the encryption key is refreshed hour-by-hour, day-by-day. The efficient way is that the network entity generating encryption key is to encrypt the broadcast content as well before packing and fragmentation.

- Inefficiency of handover

It is well known that one of ways to reduce handover latency is to use the same encryption key without duplicate authentication and authorization during the handover. For this, the serving BS has to send the key and user's parameters for authentication and authorization to the target BS before the association between SS and target BS by inter-BS communication or a centralized network entity to manage the security key and user's parameters, e.g., ASA server is introduced in network reference model.

In this architecture with a centralized network entity, it is better for this network entity to encrypt the data as well as to manage the key. That is, if the network entity encrypts the data with the encryption key managed by itself, the encryption key does not need to be sent on handover. This network entity is similar to BSC of 3G.

- Limitation of various BS product (e.g, centralized, de-centralized product)

The IETF CAPWAP WG is discussing the split of WLAN MAC to support the centralized architecture. Mainly two network entities dealing with non-real time process and real time process respectively, like BSC-BTS in 3G. It is evident there are pros and cons between the centralized architecture and the de-centralized architecture. However, the current 802.16d has a limitation to support the centralized architecture because the non-real time data encryption is performed after real-time packing and fragmentation. This is unnatural. If the data encryption in non-real time is performed before packing and fragmentation in real time, the centralized architecture is easily deployed and the current CAPWAP architecture can be applied into 802.16 network.

Conclusively, this contribution proposes that the data encryption may be performed after or before packing and fragmentation.

2. Proposed Text changes

6.4.3. Construction and Transmission of MAC PDUs

[Except the followings, Refer to IEEE P802.16-REVe/D2-2004]

The construction of a MAC PDU is illustrated in Figure 26 or Figure XXX. The encryption payload may be performed after or before the packing and the fragmentation.

6.4.3.1 Conventions

[Refer to IEEE P802.16-REVe/D2-2004]

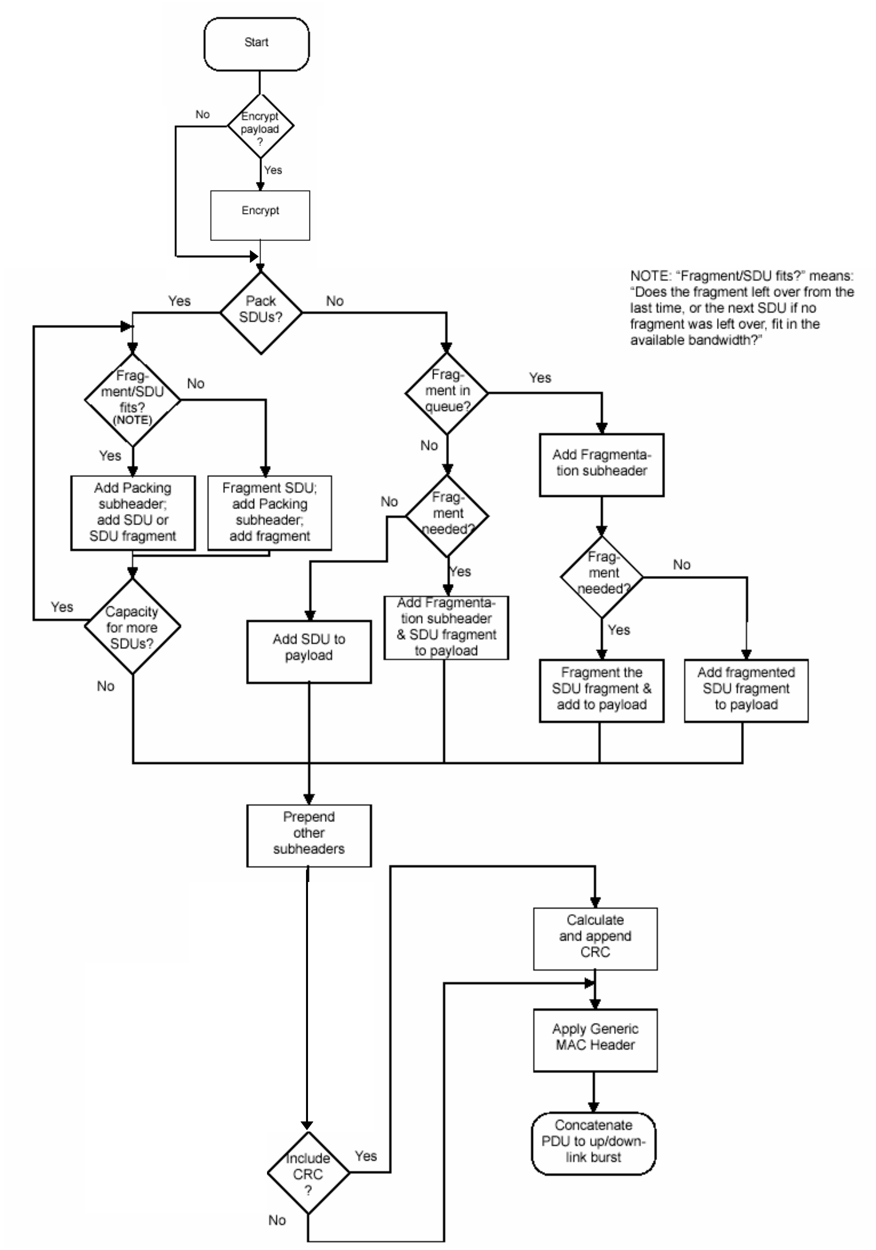

Start
Encrypt payload ?
No
Yes
Encrypt
Pack SDUs?
Yes
No
NOTE: "Fragment/SDU fits?" means: "Does the fragment left over from the last time, or the next SDU if no fragment was left over, fit in the available bandwidth?"
Frag-ment/SDU fits? (NOTE)
No
Yes
Add Packing subheader; add SDU or SDU fragment
Fragment SDU; add Packing subheader; add fragment
Frag-ment in queue?
Yes
No
Add Fragmenta-tion subheader
Frag-ment needed?
No
Yes
Add Fragmenta-tion subheader & SDU fragment to payload
Add SDU to payload
Frag-ment needed?
No
Yes
Fragment the SDU fragment & add to payload
Add fragmented SDU fragment to payload
Capacity for more SDUs?
Yes
No
Prepend other subheaders
Calculate and append CRC
Apply Generic MAC Header
Concatenate PDU to up/down-link burst
Include CRC ?
Yes
No

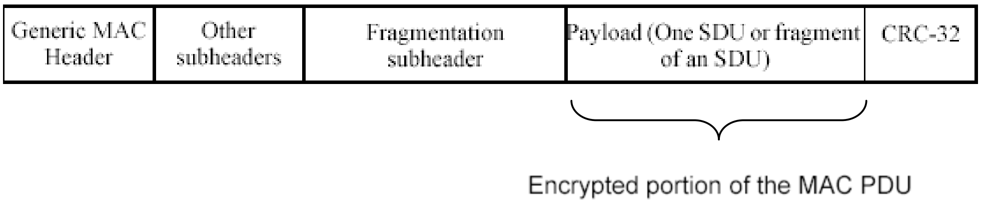
Figure XXX. Construction of a MAC PDU

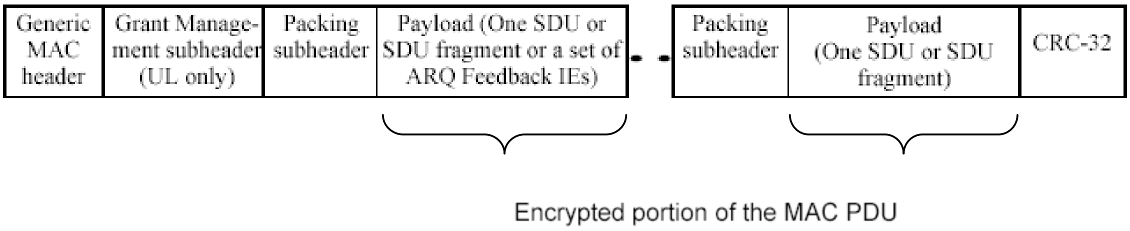
6.4.3.6 Encryption of MAC PDUs

When transmitting a MAC PDU on a connection that is mapped to an SA, the sender shall perform encryption and data authentication of the MAC PDU payload or MAC SDU as specified by that SA. When receiving a MAC PDU on a connection mapped to an SA, the receiver shall perform decryption and data authentication of the MAC PDU payload or MAC SDU, as specified by that SA.

The generic MAC header shall not be encrypted. The MAC subheader may not be encrypted. The Header contains all the Encryption information [EC Field, encryption key sequence (EKS) Field, and CID] needed to decrypt a Payload or MAC SDU at the receiving station. This is illustrated in Figure 34.

Two bits of a MAC Header contain a key sequence number. Note that the keying material associated with an SA has a limited lifetime, and the BS periodically refreshes an SA's keying material. The BS manages a 2 bit key sequence number independently for each SA and distributes this key sequence number along with the SA's keying material to the client SS. The BS increments the key sequence number with each new generation of keying material. The MAC Header includes this sequence number to identify the specific generation of that SA keying material being used to encrypt the attached payload. Being a 2-bit quantity, the sequence number wraps around to 0 when it reaches 3. If SA specifies MAC SDU encryption, all SDU fragments in a MAC PDU should be encrypted with a same keying material. Comparing a received MAC PDU's key sequence number with what it believes to be the "current" key sequence number, an SS or BS can easily recognize a loss of key synchronization with its peer. An SS shall maintain the two most recent generations of keying material for each SA. Keeping on hand the two most recent key generations is necessary for maintaining uninterrupted service during an SA's key transition. Encryption of the payload is indicated by the EC bit field. A value of 1 indicates the payload is encrypted and the EKS field contains meaningful data. A value of 0 indicates the payload is not encrypted. Any unencrypted MAC PDU received on a connection mapped to an SA requiring encryption shall be discarded.


Generic MAC Header
Other subheaders
Fragmentation subheader
Payload (One SDU or fragment of an SDU)
CRC-32
Encrypted portion of the MAC PDU


Generic MAC header
Grant Management subheader (UL only)
Packing subheader
Payload (One SDU or SDU fragment or a set of ARQ Feedback IEs)
Packing subheader
Payload (One SDU or SDU fragment)
CRC-32
Encrypted portion of the MAC PDU

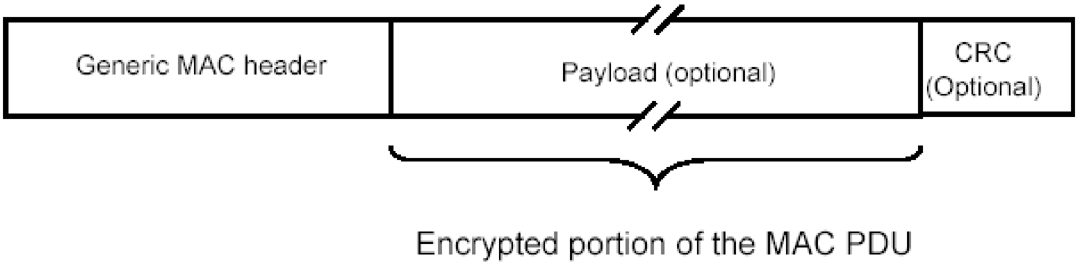


Figure 32—MAC PDU encryption

7. Privacy sublayer

7.1 Architecture

[Except the following changes, Refer to IEEE P802.16-REVe/D2-2004]

Security has two component protocols as follows:

a) An encapsulation protocol for securing packet data across the BWA network. This protocol defines (1) a set of supported cryptographic suites, i.e., pairings of data encryption and authentication algorithms, and (2) the rules for applying those algorithms to a MAC PDU payload or MAC SDU.

b) A key management protocol (PKM) providing the secure distribution of keying data from BS to SS. Through this key management protocol, SS and BS synchronize keying data; in addition, the BS uses the protocol to enforce conditional access to network services.

7.1.1 Packet data encryption

Encryption services are defined as a set of capabilities within the MAC Security Sublayer. MAC Header information specific to encryption is allocated in the generic MAC header format.

Encryption is always applied to the MAC PDU payload or MAC SDU when required by the selected ciphersuite; the generic MAC header is not encrypted. All MAC management messages shall be sent in the clear to facilitate registration, ranging, and normal operation of the MAC . The format of MAC PDUs carrying encrypted packet data payloads is specified in 6.4.3.6.