| | |
|---|---|
| Project | IEEE 802.16 Broadband Wireless Access Working Group<br><http://ieee802.org/16> |
| Title | New 802.16e Privacy Capability |
| Date Submitted | 2004-11-04 |
| Source(s) | Mo-Han Fong, Bill Gage, Haixiang He<br>mailto:mhfong@nortelnetworks.com |
| Re: | IEEE 802.16e Privacy Sublayer |
| Abstract | Define a new privacy capability to enable rapid MAC signalling in a mobile environment, to reduce overhead and to support multiple network architectures. With this new capability, MAC subheaders are not encrypted and encryption is performed on a MAC SDU rather than on a MAC PDU. |
| Purpose | Review and adopt the suggested additions into P802.16e/D6. |
| 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 Problem Statement

Figure 24 of [1] “Construction of a MAC PDU” indicates that encryption is the last operation performed before addition of the Generic MAC Header to a frame. As a consequence, all of the optional MAC PDU subheaders (grant management, fragmentation control, fast feedback, mode selection feedback) and the packing SDU subheaders are deemed to be part of the MAC PDU payload and are encrypted if security is enabled on a transport CID[1]. This is illustrated in Figure 1.

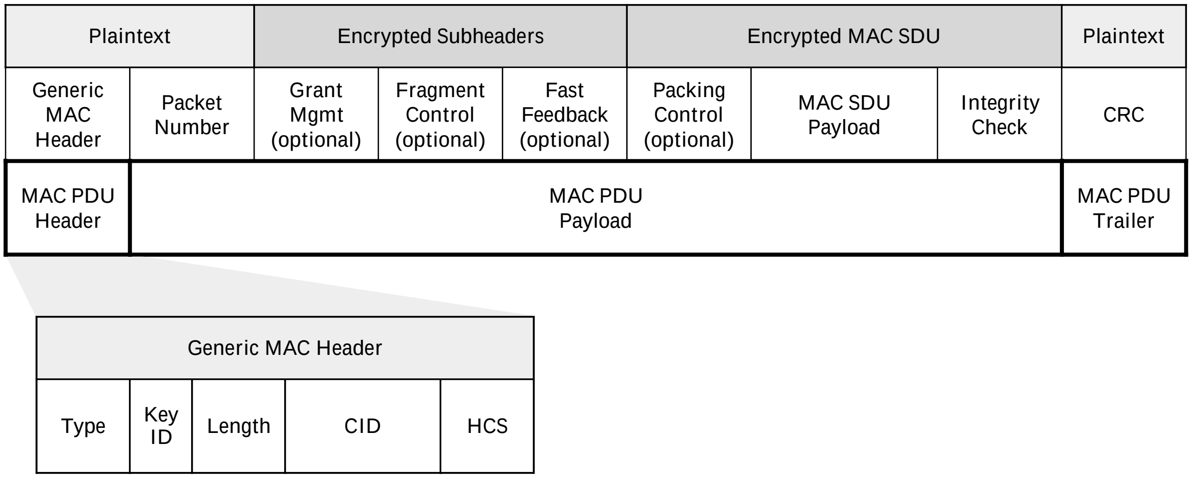

**Figure 1 : Encrypted MAC Frame in [1]**

The impacts of this encryption policy include:

- *Increased delays in MAC layer scheduling.* Processing of grant and fast feedback subheaders must occur after decryption of the MAC PDU. The delay incurred in encrypting the frame at the transmitter and decrypting the frame at the receiver negatively impacts the responsiveness of the system.
- *Increased delays for ARQ-enabled connections.* Processing of fragmentation subheaders must occur after decryption of the MAC PDU. The delay incurred in decrypting the frame at the receiver negatively impacts the responsiveness of the system.
- *Increased overhead for fragmented packets.* Each fragment is encrypted separately and has its own packet number and integrity check value (ICV) added to the fragment.
- *Increased processing requirements in the BS.* Encryption/decryption functions require significant computing resources. As a result, these functions are often implemented using specialised hardware encryption accelerators.
- *Increased system cost.* The current encryption policy forces the encryption/decryption functions to be incorporated into every BS and precludes alternate network architectures aimed at reducing the cost of implementing these functions.

[1] IEEE 802.16 management frames are never encrypted.

# 2 Proposed Solution

This contribution provides an alternate solution for the Privacy Sublayer in IEEE 802.16e to ensure that all MAC subheaders are transmitted as plaintext. In particular, this proposal defines a new capability that indicates encryption is to be applied on a per-SDU basis rather than on a per-PDU basis. The ability to support this capability is signalled through a new TLV included in REG-REQ/RSP messages. The privacy method used in a frame is signalled through a new flag in the Generic MAC Header.

This new capability results in the following changes with respect to the Security Sublayer defined in [1]:

- The transmitter in [1] encrypts each MAC PDU and its subheaders; the transmitter using this new capability encrypts at the MAC SDU level and leaves all subheaders as plaintext.
- The transmitter in [1] performs fragmentation and then applies encryption, adding an ICV and packet number to each of the resulting MAC PDUs; the transmitter using this new capability encrypts the MAC SDU and then performs fragmentation on the resulting encrypted SDU.
- The receiver in [1] decrypts each MAC PDU (SDU fragment) and then reconstructs the original SDU; the receiver using this new capability reconstructs the encrypted MAC SDU from the received fragments and then performs decryption of the entire SDU.
- [1] includes volatile information from the Generic MAC Header (i.e. the Type flags) and from the subheaders in the initialisation vector; this proposal includes only non-volatile information associated with the connection in its initialisation vector.

# 3 References

[1] IEEE Standard 802.16-REVd (2004 Edition), “Local and Metropolitan Area Networks: Air Interface for Fixed Broadband Wireless Access Systems”.

[2] IEEE Proposed Standard 802.16e/D5 (September 2004), “Local and Metropolitan Area Networks: Air Interface for Fixed Broadband Wireless Access Systems (Draft Amendment Combined Fixed and Mobile Operation in Licensed Bands)”.

# 4 Recommended Text Changes

## [2] 6.3.2 MAC PDU Format

*[Modify Table 4 as indicated:]*

**Table 4a**

| Syntax | Size | Notes |
|---|---|---|
| MAC Header () { | | |
| HT | 1 bit | 0 = Generic MAC Header<br>1 = Bandwidth Request Header |
| EC | 1 bit | If HT = 1, EC = 0 |
| if (HT == 0) { | | |
| .Type | 6 bits | |
| .if UL frame { | | |
| ..Mode Selection Feedback | 1 bit | |
| .} else { | | |
| ..Reserved | 1 bit | Shall be set to zero. |
| .} | | |
| .CI | 1 bit | |
| .EKS | 2 bits | |
| .if (EC == 1) { | | |
| ..Privacy Mode | 1 bit | |
| .} else { | | |
| ..Reserved | 1 bit | Shall be set to zero |
| .} | | |
| .LEN | 11 bits | |
| } | | |
| … | | |
| CID | 16 bits | |
| HCS | 8 bits | |

*[Modify Figure 19a as indicated:]*

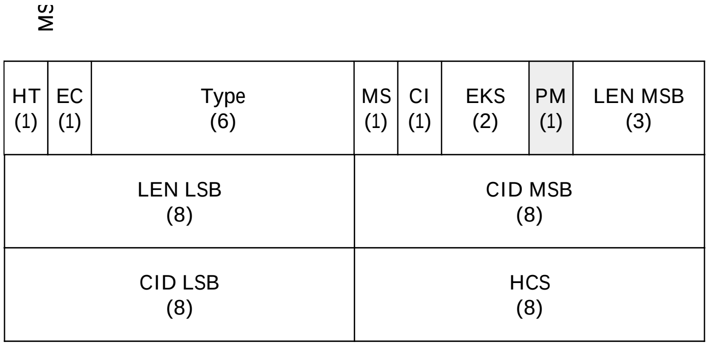

**Figure 19a – MAC PDU Format**

*[Modify Table 5 as indicated:]*

**Table 5a**

| Name | Length (bits) | Description |
|---|---|---|
| CI | 1 | CRC Indicator |
| CID | 16 | Connection Identifier |
| EC | 1 | Encryption Control |
| EKS | 2 | Encryption Key Sequence |
| HCS | 8 | Header Check Sequence |
| HT | 1 | Header Type |
| LEN | 11 | Length |
| MS | 1 | Mode Selection Feedback |
| PM | 1 | Privacy Mode<br>0 = PDU payload and subheaders encrypted<br>1 = SDU encrypted |
| Type | 6 | |

## [2] 6.3.2.3.7 Registration Request (REG-REQ) message

*[Insert the following text to the end of Section 6.3.2.3.7:]*

For MSS that support SDU-level privacy mode (Privacy Mode = 1), the REG-REQ shall contain the following TLV:

Privacy Mode support (section TBD)

## [2] 6.3.2.3.8 Registration Response (REG-RSP) message

*[Insert the following text to the end of Section 6.3.2.3.8:]*

For BS that support SDU-level privacy mode (Privacy Mode = 1), the REG-RSP shall contain the following TLV:

Privacy Mode support (section TBD)

## [1] 6.3.3 Construction and Transmission of MAC PDUs

*[Modify text as follows:]*

The construction of a MAC PDU when Privacy Mode is set to "0" is illustrated in Figure 24. The construction of a MAC PDU when Privacy Mode is set to "1" is illustrated in Figure 24a.

**Figure 24 – Construction of a MAC PDU (PM = 0)**

*[Add Figure 24a as follows:]*

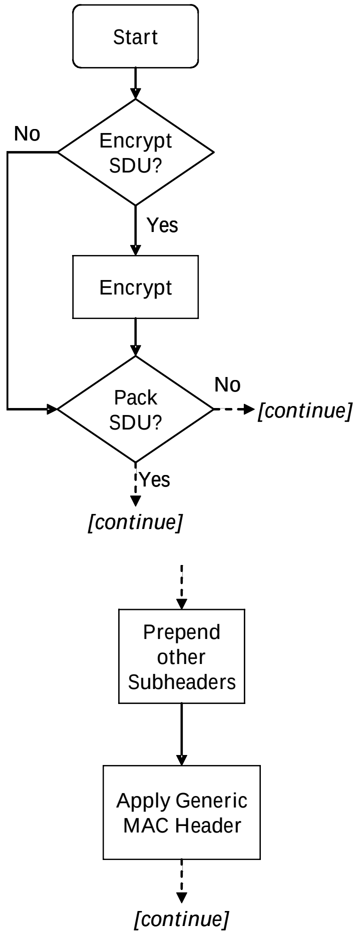

**Figure 24a – Construction of a MAC PDU (PM = 1)**

## [1] 6.3.3.6 Encryption of MAC PDUs

*[Modify the text as indicated:]*

The generic MAC header shall not be encrypted. The Header contains all the Encryption information [EC Field, privacy mode (PM) Field, encryption key sequence (EKS) Field, and CID] needed to decrypt a Payload at the receiving station. If EC is set to "1" and PM is set to "0", the entire MAC payload (including MAC PDU subheaders) is encrypted. This is illustrated in Figure 31. If EC is set to "1" and PM is set to "1", the MAC SDUs and/or fragments thereof are encrypted but the MAC PDU subheaders are not encrypted. This is illustrated in Figure 31a.

*[Add Figure 31a as follows:]*

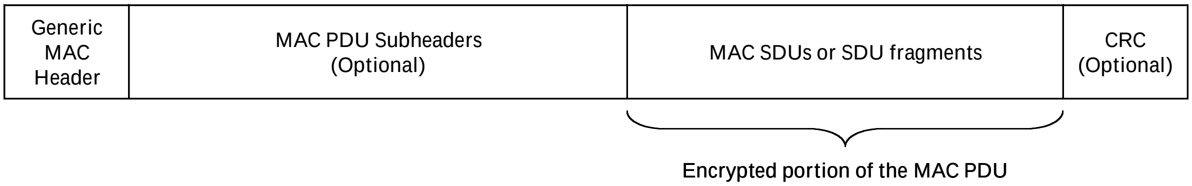
Generic MAC Header
MAC PDU Subheaders (Optional)
MAC SDUs or SDU fragments
CRC (Optional)
Encrypted portion of the MAC PDU

**Figure 31a –MAC PDU Encryption**

## [2] 7.1.1 Packet Data Encryption

*[Modify the text as indicated:]*

Encryption is applied to the MAC PDU payload when required by the selected ciphersuite; the generic MAC header is not encrypted. All MAC management messages ~~described in subclause 6.3.2.3~~ shall be sent in the clear to facilitate registration, ranging, and normal operation of the MAC. If Privacy Mode is set to “1”, all MAC PDU subheaders shall be sent in the clear to facilitate normal operation of the MAC.

## [1] 7.5.1.2.1 PDU Payload Format

*[Modify the text as indicated:]*

When Privacy Mode is set to “0”, the PDU payload shall be prepended with a 4-byte PN (Packet Number). The PN shall be transmitted in little endian byte order. The PN shall not be encrypted.

*[Add the following text and Figure 135a after Figure 135:]*

When Privacy Mode is set to “1”, the SDU shall be prepended with a 4-byte PN (Packet Number). The PN shall be transmitted in little endian byte order. The PN shall not be encrypted.

The plaintext SDU shall be encrypted and authenticated using the active TEK, according to the CCM specification. This includes appending an 8-byte ICV (Integrity Check Value) to the end of the SDU and encrypting both the plaintext SDU and the appended ICV. The ciphertext ICV is transmitted in little endian byte order. The processing yields an encrypted SDU that is 12 bytes longer than the plaintext SDU. The encrypted SDU may then be fragmented or packed as necessary to fit into a MAC PDU payload. This is illustrated in Figure 135a.

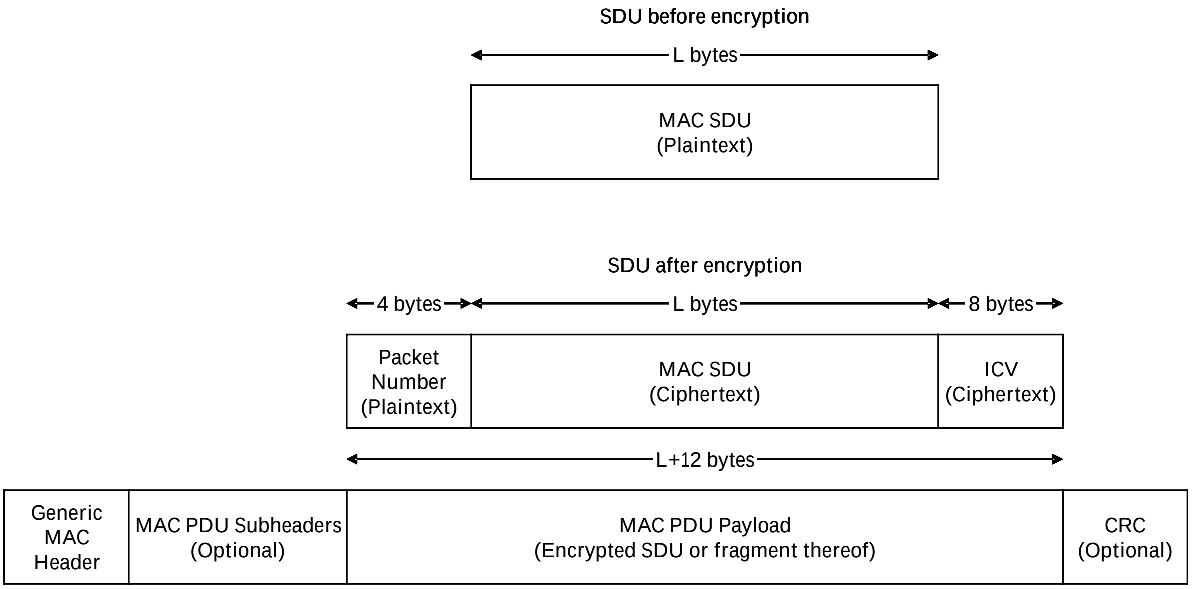

**Figure 135a – TEK Management in BS and MSS (PM = 1)**

## [1] 7.5.1.2.3 CCM Algorithm

*[Modify the text as indicated:]*

The nonce shall be 13 bytes long. When Privacy Mode is set to “0”, bytes 1 through 5 shall be set to the first five bytes of the GMH (thus excluding the HCS)~~. B~~; bytes 6 through 9 are reserved and shall be set to 0x00000000. When Privacy Mode is set to “1”, bytes 1 through 4 shall be set to the SFID and bytes 5 through 6 shall be set to the SAID associated with this connection; bytes 7 through 9 are reserved and shall be set to 0x000000.

Bytes 10 through 13 shall be set to the value of the PN. Byte 10 shall take the least significant byte and byte 13 shall take the most significant byte.

Consistent with the CCM specification, the initial block $B_0$ is formatted as shown in Figure 136 when Privacy Mode is set to “0”.

*[Add the following text and Figure 136a after Figure 136:]*

Consistent with the CCM specification, the initial block $B_0$ is formatted as shown in Figure 136a when Privacy Mode is set to “1”.

| Byte within MIC-IV | 0 | 1 4 | 5 6 | 7 9 | 10 13 | 14 15 |
|---|---|---|---|---|---|---|
| Bytes | 1 | 4 | 2 | 3 | 4 | 2 |
| Field | Flag | SFID | SAID | *reserved* | PN | DLEN |
| Contents | 0x19 | SFID associated with connection | SAID associated with connection | 0x000000 | Packet number associated with SDU | Length of data part, not including padding |

**Figure 136a – Initial CCM Block $B_0$ (PM = 1)**

*[Modify the text as indicated:]*

Consistent with the NIST CCM specification the counter blocks Ai are formatted as shown in Figure 137 when Privacy Mode is set to “0”.

*[Add the following text and Figure 137a after Figure 137:]*

Consistent with the CCM specification, the counter blocks Ai are formatted as shown in Figure 137a when Privacy Mode is set to “1”.

| | | | | | | |
|---|---|---|---|---|---|---|
| Byte within CTR(i) | 0 | 1 4 | 5 6 | 7 9 | 10 13 | 14 15 |
| Bytes | 1 | 4 | 2 | 3 | 4 | 2 |
| Field | Flag | SFID | SAID | *reserved* | PN | C |
| Contents | 0x01 | SFID associated with connection | SAID associated with connection | 0x000000 | Packet number associated with SDU | Length of data part, not including padding |

**Figure 137a – Construction of $A_i$ (PM = 1)**

## [2] 11.7 REG-REQ/RSP management message encodings

*[Insert the following text to the end of Section 11.7:]*

### 11.7.x Privacy Mode encodings

This field indicates which privacy mode the MSS will use – encryption of MAC subheaders and PDU payload or encryption of SDU only.

| **Type** | **Length** | **Value** | **Scope** |
|---|---|---|---|
| TBD | 1 | 0 = encryption of MAC subheaders and PDU payload. (PM=0 in GMH)<br>1 = [default] encryption of SDU only (PM=1 in GMH) | REG-REQ<br>REG-RSP |

**[End of Document]**