Project	**IEEE 802.16 Broadband Wireless Access Working Group <**http://ieee802.org/16**>**
Title	**Data Encryption Location & PN Header Compression for IEEE 802.16m**
Date Submitted	**2008-01-~~16~~**
Source(s)	Kiran Thakare, Per Ernström Ericsson AB SE-164 80 Stockholm, Sweden Voice: +46 8 58532591 E-mail: kiran.thakare@ericsson.com
Re:	IEEE 802.16m-07/040 - Call for Contributions on Project 802.16m System Description Document. For protocol architecture
Abstract	This contribution proposes the location for Data Encryption & authentication functionality. It also proposes DE header compression functionality. This proposal considers the future requirements on system evolution and still optimize the air resource use in robust manner for IEEE 802.16m
Purpose	To include: 1. Data Encryption functionality in the CS layer of protocol architecture for IEEE 802.16m. 2. Authentication & compression of PN header 3. Simple compression method (SCM) We propose to include the contributions in the protocol architecture section of the 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	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>.

Data Encryption Location & DE Header Compression for IEEE 802.16m

Kiran Thakare, Per Ernström
Ericsson AB Sweden

1. Introduction

This contribution proposes progression of the security sub-layer specified in WirelessMAN OFDMA system while retaining backward compatibility [1]. We propose that the Data Encryption and authentication functionality be located at the CS layer protocol architecture for IEEE 802.16m. Additionally, we propose the use of PN header authentication and PN compression using SCM[1] method.

2. Background

The IEEE 802.16e [2] uses the protocol architecture as shown below in Figure 1. Figure 2 shows the proposed logical protocol architecture for 16m reference [3].

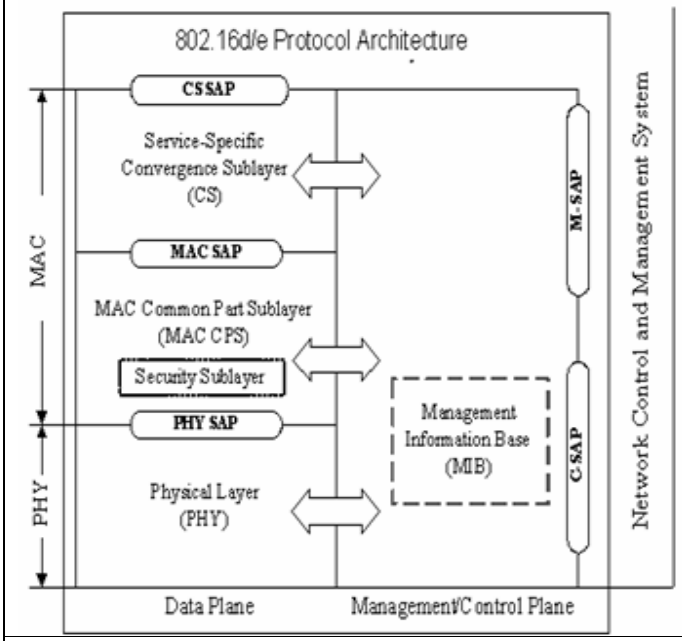

Figure 1 Showing Logical Protocol Architecture for the Reference WirelessMAN OFDMA system

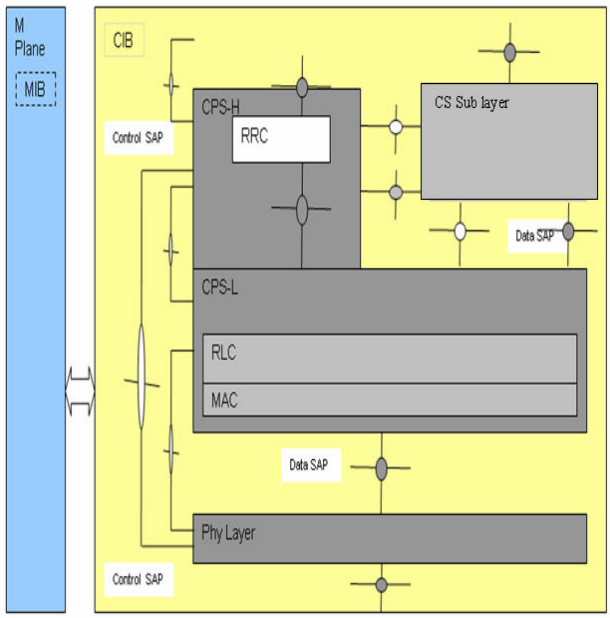

Figure 2 Showing Logical Protocol Architecture for the IEEE 802.16m system

The MAC CS layer specifies three service specific convergence sub-layers (CS) such as ATM CS, Packet CS and generic packet CS. The service specific CS provides SDU classification of higher layer SDUs and associating them to the service flow IDs and connection IDs (CID). The CS provides, as an option, functionality for packet-header-compression and multiplexing of upper layer PDUs for specific services.

The MAC-CPS performs the core MAC functionalities. It receives SDUs from the CS and processes them. The MAC Security sub-layer is responsible for encryption of PDUs, data authenticity and privacy key management between the BS and MS. The IEEE 802.16e standard specifies four distinct encryption methods [2] as follows: DES in CBS Mode, AES in CCM mode, AES in CTR mode and AES in CBC mode.

[1] SCM Simple Compression method

HMAC/CMAC are specified for the control/management messages for optional integrity protection. However, the WiMax forum profile [4] specifies only AES in CCM mode with 128bit for data encryption.

3. Problem Statement

The encryption & authentication functionalities are located at the MAC CPS layer as shown in the figure 1. This location of the DE functionality is an implausible position since the needed traffic/data characteristics, are available at CS layer. The CS layer allocates CIDs and associates the CIDs to various types of security association (SA) of the service flow used by a user. This results in significant inter-layer communication for efficient operation of the security sub-layer. Additionally encryption & authentication functionality at MAC layer is inadequate for the reason of future traffic growth & mobility aspect of the service flows. Accordingly, we believe that the security sub-layer at MAC layer is an inefficient solution.

The AES CCM mode with 128bit used for data encryption provides the encrypted payload with a 4-byte PN (packet number) header.

It is to be noted that PN header is not authenticated [2], subjecting it to security attacks. The overhead due to the PN header affects the efficiency and throughput of the system.

This contribution provides advancement to the security mechanism dealing the three issues raised above.

4. Proposed Location for the DE & Authentication for 802.16m

We propose to move the security functionalities, in particular, the data encryption and authentication to the CS layer. New DE & authentication functionality is shown in figure 3 & 4 below.

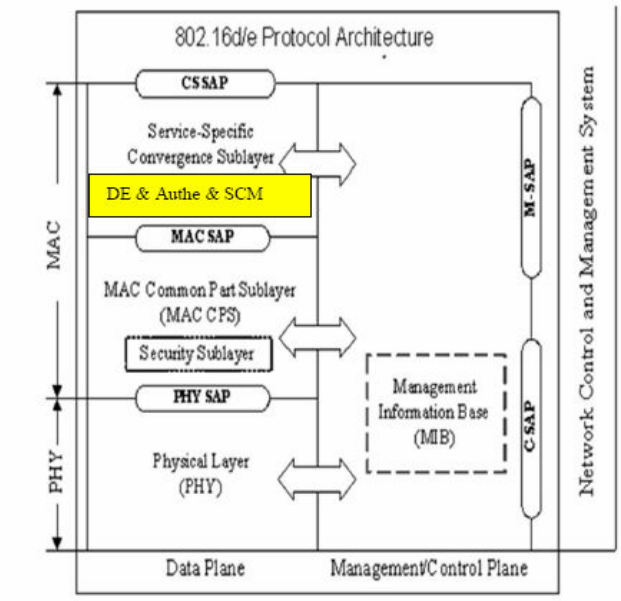

Figure 3 shows the security sub-layer functionalities moved to convergence sub-layer

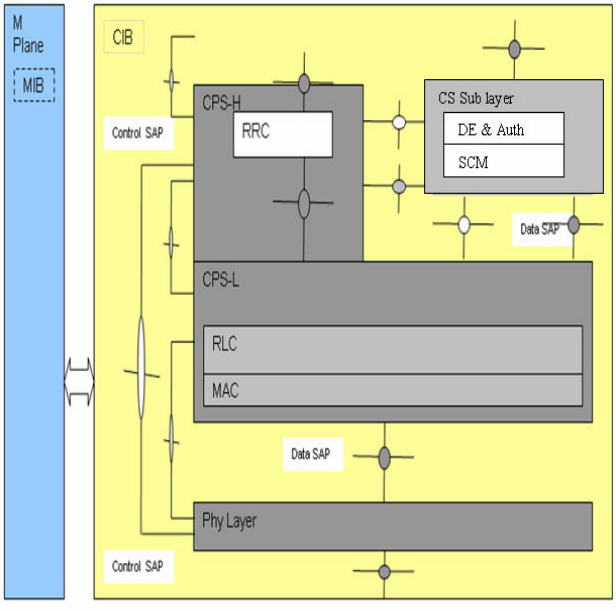

Fig 4 Showing logical architecture for 16m showing DE & Authentication & CS with SCM method

The CS layer generates the PN (packet number). Additionally, the bit 'EC' (Encryption control) is needed for the generic MAC header and is communicated over 'MAC-SAP'/'control SAP' in case of figure 3/4 respectively.

5. Proposed PN authentication & compression for 802.16m

AEC CCM mode [4] for data encryption uses the PN header, which is 4 bytes long, wasting the precious air interface resources. AEC CCM authenticates only the ciphered payload without authentication of the PN header. This will subject the PN header to fraudulent attacks. In order to solve these two problems we propose two robust solutions as follows:

a. Authentication of the PN header in addition to the ciphered payload
b. Compression of the authenticated PN header using SCM method described below.

Figure 5 shows the PN header authentication and header compression functionality applied to PN, thus protecting the PN integrity, providing optimization of the air resource use and making the PN compression more robust.

Figure 5 illustrates the order of execution at CS layer is as follows:

1. Compress SDU header using RoHC
2. Add PN header
3. Authenticate both PN and payload
4. Apply Encryption
5. Compress PN using SCM, as proposed below

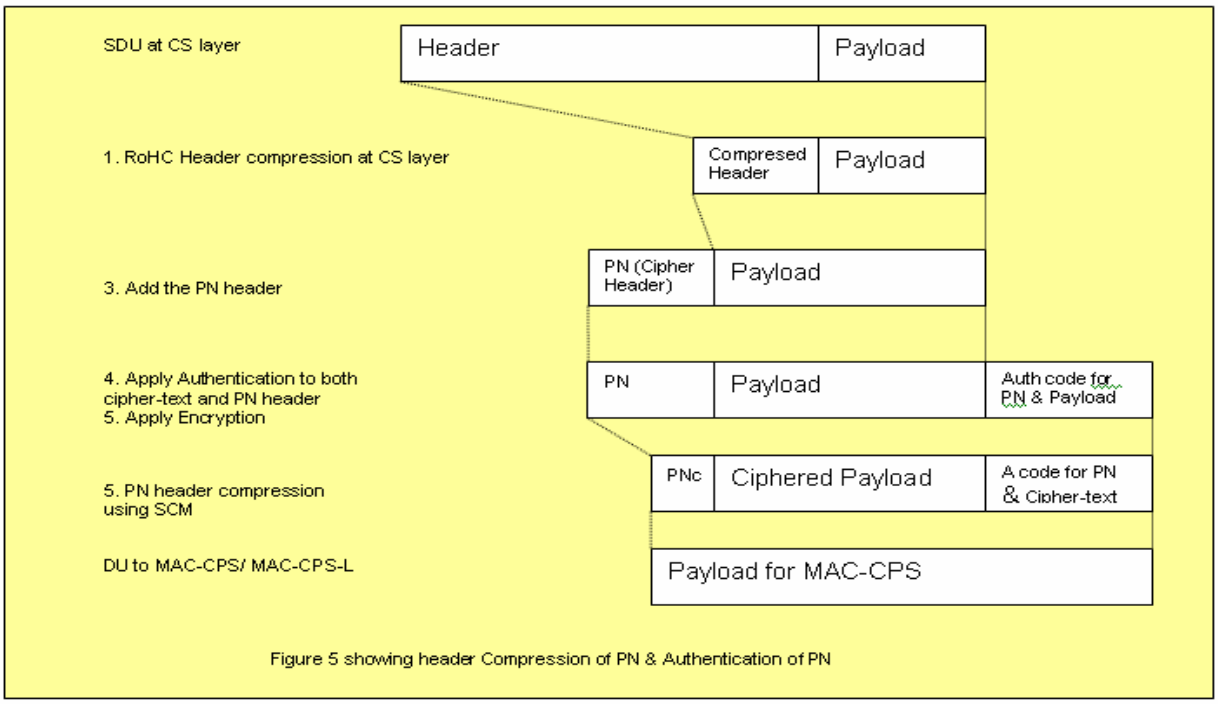

Figure 5 showing header Compression of PN & Authentication of PN

A simple and effective compression method is proposed to reduce the size of the PN header, as described below.

5.1 Simple Compression Method (SCM)

The SCM is described as follows: The PN header is four bytes long and fixed. Instead of sending the 4 bytes long header with each packet, SCM (Simple compression method) relies on sending only the LSB (least significant bits). The number of LSBs to be transmitted can be defined in a service specific fashion, for delay tolerant and delay non-tolerant services, the number of LSB bits sent could be different. The number of LSB bits is defined as 4 or 8 bits to cover the nature of the services. At the time of service flow creation UE requests either 4bit, 8bit or full header based on UE capability and is granted by BS in the service flow creation response message. A 2-Bit indicator is needed in service creation request & response message.

This header compression algorithm (SCM) should be located in the CS layer if ciphering & authentication is at CS layer, or at MAC security sub-layer, in case that ciphering, authentication remains in the existing security layer, as in of Figure 1.

5.1.1 SCM Indexing & Sequence estimation scheme

The transmitting end determines the indexing scheme and the receiver estimates the index of the packet based on received LSB bits (referred as 'n' bits hereupon). This indexing scheme takes care of replay attack, packet reordering. Indexing scheme for packet sequencing is defined below.
Both the sender and receiver maintains a ROC, roll over counter. Number of bits in ROC is 'r'
When the session starts the sender sets the ROC to zero. Each time the LSB sequence number LB_seq, wraps modulo 2^n, the sender side MUST increment ROC by one, modulo 2^r.
The sender's packet index is then defined as follows:

i = 2^n * ROC + LSB_Seq

Receiver-side implementations use LSB sequence number LSB-Seq to determine the correct index of a packet, which is the location of the packet in the sequence of all packets. Out-of-order packets with sequence numbers close to 2^n or zero must be properly handled. The index estimate is based on the receiver's locally maintained ROC and S_1 values. At the setup of the session, the ROC MUST be set to zero. S_1 is the highest received and properly authenticated packet sequence number.
On consecutive packets, the receiver should estimate the index as

i = 2^n * v + LSB_Seq

where v is chosen from the set { ROC-1, ROC, ROC+1 } (modulo 2^r) such that i is closest to the value 2^n * ROC + S_1
This scheme only requires that the LSB-Seq is sent over the air /communication link. ROC is locally maintained at both receiver and transmitter end. Also S_1 is maintained at receiver end, for bidirectional traffic at both ends.

Proposal

We propose to include following in the protocol architecture section of the SDD.

1. DE and Authentication functionalities at CS layer, as proposed in section 4
2. PN Authentication shall be carried out, as proposed in section 5
3. PN Compression using SCM as proposed in section 5.1
4. SCM Indexing & sequence estimation scheme as proposed in section 5.1.1

References

1. IEEE 802.16m Requirements Specification
2. IEEE 802.16e Standards
3. Ericsson Contribution 'logical protocol architecture for 802.16m
4. WiMax Forum profile