Integrity protection of MAC Signaling Header

IEEE 802.16 Presentation Submission Template (Rev. 9)

Document Number:

IEEE C802.16m-08/1141r1

Date Submitted:

2008-09-05

Source:

Shashikant Maheshwari, Haihong Zheng, Yousuf Saifullah
Nokia Siemens Networks E-mail: shashi.maheshwari@nsn.com

Jan Suumaki E-mail: jan.suumaki@nokia.com
Nokia

Venue:

Re: Security: IEEE 802.16m-08/033, “Call for Comments and Contributions on Project 802.16m System Description Document (SDD)”.

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:

Introduction

- In IEEE 802.16-REV2, Standalone MAC Signaling headers are neither authenticated nor encrypted.
- The MAC management messages or Headers are sent without encryption between BS and MS.
- A rogue station could read these messages and could send a false response and distort the information relevant to the procedure in BS/MS.
- Bandwidth Request header is not authenticated, a malicious user could send a wrong BR header which may cause following problems:
  - deprivation of bandwidth in the system for the legitimate users (denial of Service attack) or
  - wastage of UL bandwidth.

Proposal: Authenticated HCS

- In IEEE 802.16-REV2, HMAC/CMAC tuple is used for authentication that has large overhead.
- HMAC tuple is 21 bytes, and CMAC tuple is 13-19 bytes. It seems inappropriate to send so many bytes in the HMAC/CMAC tuple for protecting few bytes of header (e.g. 6 bytes in 802.16REV2).
- We propose that Bandwidth Request and other signalling headers shall be authenticated, by replacing HCS with Authenticated HCS (A-HCS).
- With this method, the A-HCS (Authenticated HCS) **provides both error detection and integrity protection** at the same time.
- A-HCS field is only 8 bits long, which may not provide same level of integrity protection as HMAC/CMAC mechanism.
- However, the proposed scheme is bandwidth efficient and useful in preventing malicious uplink bandwidth wastage and reducing the chance of replay attack and denial of service attack.

Example implementation: Authenticated BR Header

- In 802.16-REV2, the checksum is computed as the residue of the generator polynomial (D8+D2+D+1).
- Propose to compute the checksum using the message authentication code as mentioned below:

  A-HCS = CMAC(CMAC_KEY_U⊗counter, 5-byte-checksum) mod (D8+D2+D+1)
- Counter is a monotonically increasing number. 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.

Example: 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">STId MSB (8)</td></tr>
<tr><td colspan="4">STId LSB (4)</td><td colspan="4">Flow Identifier (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
- STId: Station identifier of the MS
- Flow identifier: Flow identifier of the connection requesting for b/w
- A-HCS: Authenticated HCS

Proposed text changes for 802.16m SDD

[insert following text in section 12.x]

12.x.x MAC Header security

Header Check Sum (HCS) of standalone MAC signaling header provides both error detection and integrity protection