Proposal on removing standalone signaling header authentication

IEEE 802.16 Presentation Submission Template (Rev. 9)

Document Number:

IEEE C80216m-09/0182r1

Date Submitted:

2009-01-08

Source:

Youngkyo Baek, Anil Agiwal, Jungje Son

Voice : +82102797321

Samsung Electronics

E-mail :youngkyo.baek@samsung.com

Venue: IEEE 802.16m-08/052 - Call for Comments and Contributions on Project 802.16m SDD

Topic: Security, standalone signaling header authentication

Base Contribution:

N/A

Purpose:

For adopting proposed text or modification into 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:

Remove standalone signaling header authentication(1/2)

- comments

  When integrity check is applied to a standalone signaling header, ABS has to allocate more bandwidth to AMS than standalone signaling header without integrity check. But, standalone signaling header authentication can not be applied until security context is shared between AMS and ABS. So when ABS receives BR ranging , the ABS has to distinguish whether the AMS wants to add authentication part(i.e. integrity check) or not. It could make system complicate. In addition, standalone signaling header protection makes non-negligible size of security overhead considering the size of the standalone signaling header, and AMS is still unsafe from attack because BR ranging is not secure.

- Proposed text changes in SDD

[modify the following text at page46 line 24]

------------------------------- Text Starts -------------------

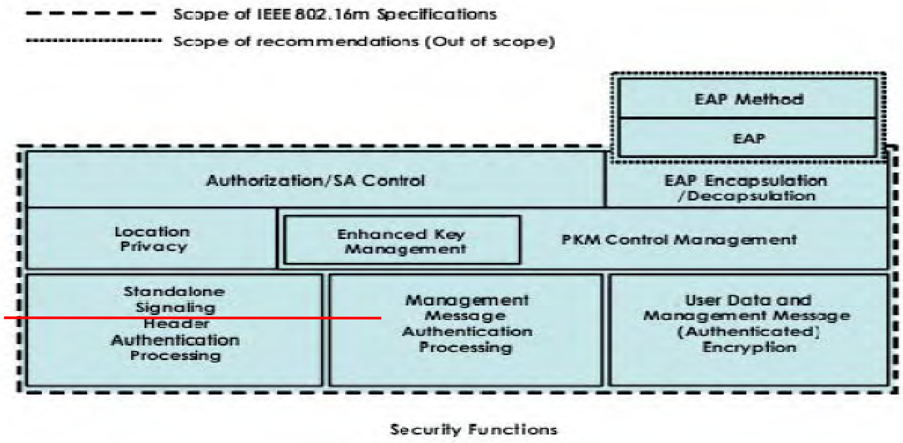
It does this by applying cryptographic transforms to transport and management MAC PDUs ~~and standalone signaling headers~~ carried across connections between AMS and ABS.

------------------------------- Text Ends -------------------

Remove standalone signaling header authentication(2/2)

[modify the following figure 17 in section 10.5.5.1 at page47 line 1]

------------------------------- Text Starts -------------------



Scope of IEEE 802.16m Specifications
Scope of recommendations (Out of scope)
EAP Method
EAP
Authorization/SA Control
EAP Encapsulation /Decapsulation
Location Privacy
Enhanced Key Management
PKM Control Management
~~Standalone Signaling Header Authentication Processing~~
Management Message Authentication Processing
User Data and Management Message (Authenticated) Encryption
Security Functions

Figure 17 Functional Blocks of IEEE 802.16m Security Architecture

------------------------------- Text Ends -------------------

[modify the following text at page54 line 22]

------------------------------- Text Starts -------------------

~~**10.6.5.3.2 Standalone Signaling Header Authentication**~~

~~**Integrity protection is applied to standalone MAC signaling header.**~~

~~**Method for providing standalone signaling header protection is FFS.**~~

------------------------------- Text Ends -------------------