Proposal on AMS ID and location Privacy

IEEE 802.16 Presentation Submission Template (Rev. 9)

Document Number:

IEEE C80216m-09/0181r1

Date Submitted:

2009-01-08

Source:

Youngkyo Baek, Anil Agiwal, Jungje Son

Samsung Electronics

Voice : +82102797321

E-mail :youngkyo.baek@samsung.com

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

Topic: Security, AMS privacy, sub section 10.6.2.1

Base Contribution:

N/A

Purpose:

For adopting proposed text or modification into 16m SDD

AMS ID and location privacy(1/2)

- Comments

  There is no remedy for AMS privacy in SDD yet. If relationship between MS MAC address and normal station ID is hidden, AMS privacy can be achieved even though the MS MAC address is transmitted as a plaintext. We suggest using Temporary station ID, which the ABS assigns the AMS, to hide the relationship.

- Suggested Remedy

  This is the steps for hiding the relationship between MS MAC address and normal station ID during initial Network entry. (see Figure xxx)

  1. The AMS sends AMS ID(e.g. MS MAC address) for MS identification to ABS.

  2. ABS allocates a temporary station ID, which is used until the AMS obtains a normal station ID.

  3. During the authorization/authentication procedure, ABS and AMS become to share security keys which is used to encrypt management message. (During the authorization/authentication procedure AMS may transmit the MS MAC address to ABS for device authentication.)

  4. ABS assigns securely normal station ID to AMS, which is sent through the encrypted management message.

  5. The assigned normal station ID is used from a negotiated time.

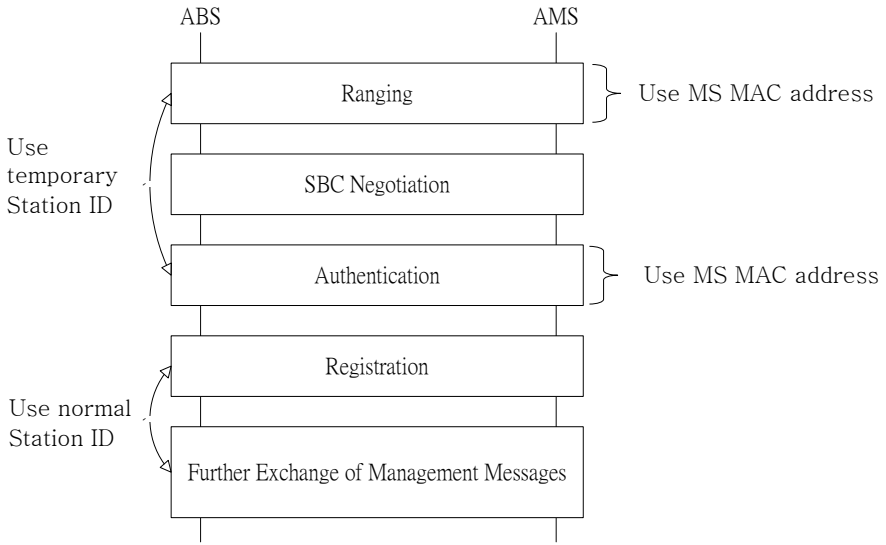

Figure 1. AMS Privacy during NW entry

AMS privacy(2/2)

[insert the following text in section 10.6.2.1 at page48 line14]

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

10.6.2.1 AMS Privacy

~~In reference system there is no explicit means by which identity of user is protected. During initial ranging and certificate exchange during authorization MS MAC Address (MS ID) is transmitted in the clear. Hence, the identity or location information can be easily inferred from fixed MS MAC address, result of which violates the security aspects of IEEE 802.16m SRD. Detailed method for providing AMS ID privacy is FFS.~~

AMS privacy is provided by hiding relationship between MS MAC address and normal station ID.

During initial network entry, the AMS and ABS use MS MAC address for MS identification . When the AMS sends MS MAC address to ABS for MS identification, the ABS allocates a temporary station ID, which is used until the AMS obtains a normal station ID. During the authorization/authentication procedure, ABS and AMS share security keys which is used to encrypt management message. ABS assigns station ID to AMS, which is sent through the encrypted management message, and the station ID is used from a negotiated time. Figure xxx.yyy illustrates an example of identity privacy and location privacy.

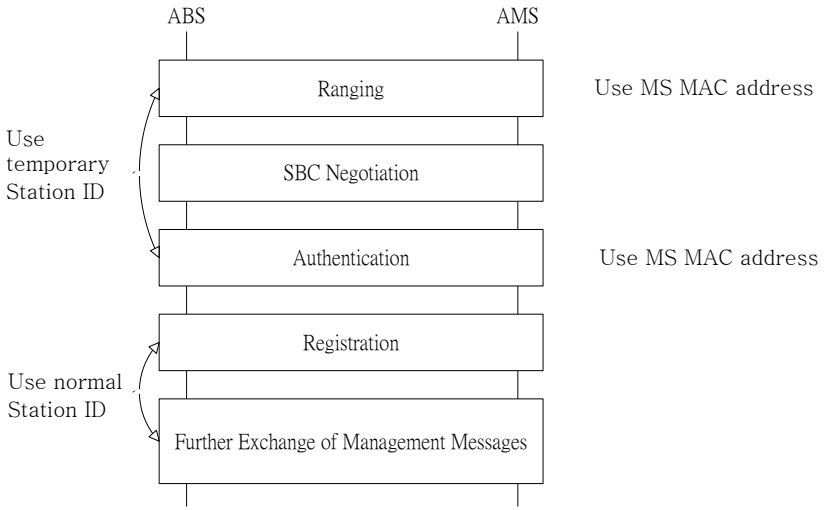

Figure xxx.yyy AMS Privacy during NW entry

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