Message Encryption and MS Identity Privacy in 802.16m

IEEE 802.16 Presentation Submission Template (Rev. 9)

Document Number:

IEEE C802.16m-08/1087

Date Submitted:

2008-09-05

Source:

Haihong Zheng, Shashikant Maheshwari, Yousuf Saifullah Email: haihong.zheng@nsn.com
Nokia Siemens Networks

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

Venue:

Re: Security: MAC; in response to the TGm Call for Contributions and Comments 802.16m-08/033 for Session 57

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:

Motivation (1)

- In 802.16e, MAC management messages are sent over the air interface with clear text.
- HMAC or CMAC is applied to MAC management message to provide message authentication, but no encryption is used.
- An intruder can obtain the information carried in the MAC management message sent from/to other MSs by simply listening to the air interface and issue security attack.
  - Example 1: By listening to RNG-REQ/RSP messages, an intruder can obtain MS's MAC address, station identifier and mapping between them.
  - Example 2: By listening to DSA-REQ/RSP messages, the intruder can obtain what type of application an MS is running and their correspondent IP address and port number.
- Using the current 16e approach, the following 16m requirement cannot be reached.
  - "Confidentiality of user-related data (e.g., location privacy, user identity)"

Motivation (2)

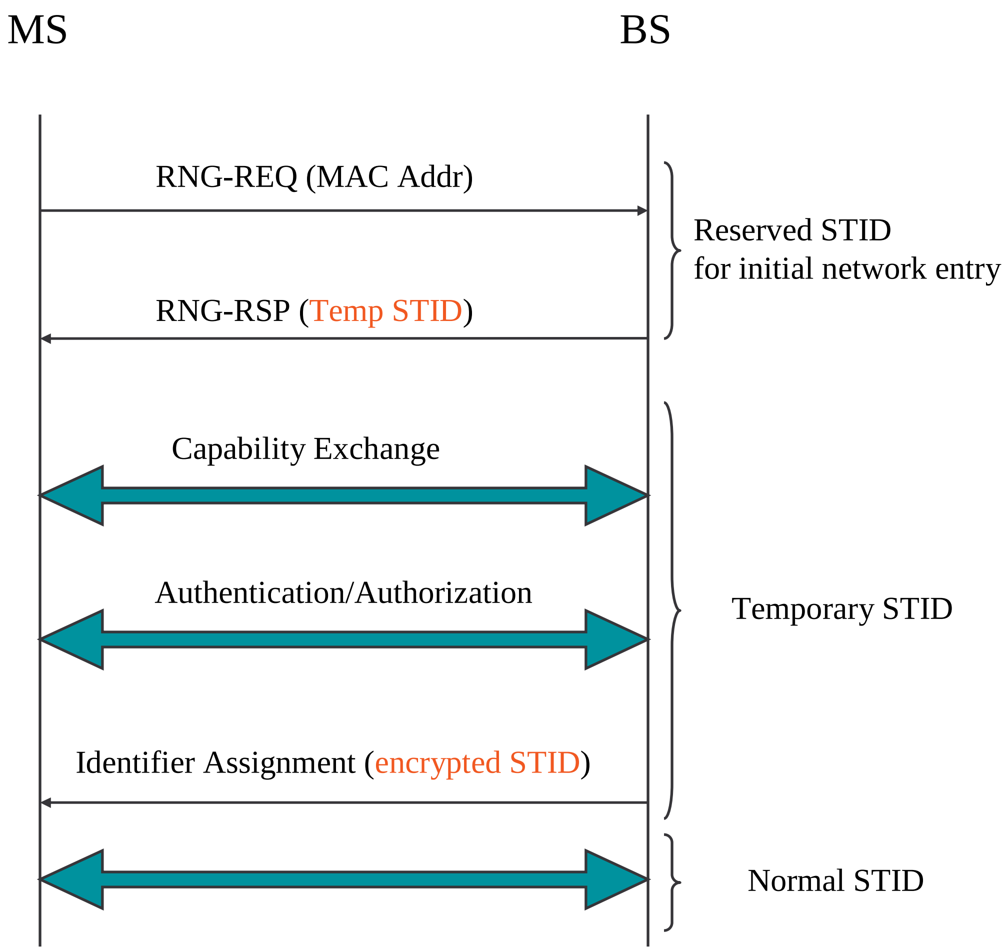
- Sending MAC address over the air is not an issue and cannot be completely avoided.
  - MAC address is needed for BS to obtain MS related information from other network entities.
  - MAC address is used by BS to generate various security keys.
  - Certificate which contains MAC address is sent over the air in clear text.
- Revealing the mapping between MAC address and Station ID is the real problem to be solved.
  - By monitoring the ranging procedures, an intruder can obtain the mapping between MAC address and Station ID, based on which perform specific attack to that specific user.

Proposed Solution – Encryption of MAC Management Messages

- MAC management messages that carry user-related data are encrypted.
- Special flow identifiers can be used to carry MAC management messages that are encrypted.
- The key used for encryption/decryption could be the same as TEK in 16e or a different key (FFS).

Proposed Solution - Temporary Station Identifier

- Temporary Station Identifier (STID) is assigned during initial ranging process.
- After being assigned, it is used for the subsequent network entry procedures until the normal STID is allocated.
- Normal STID is assigned during/after authentication process, and the assignment message shall be encrypted.
- The temporary STID is then released and normal STID is used for all the remaining transactions.



Proposed SDD Text

Section 10.12: Security

- MAC management messages that carry user-related data are encrypted. Different management connections are used to carry encrypted and non-encrypted MAC management messages.

Section 10.x: Network Entry

- Two types of station identifiers are assigned to MS during network entry process and one of them will be used for the certain time period.
- A temporary station identifier is assigned during initial ranging process, and is used during the subsequent network entry procedures until the normal station identifier is allocated.
- The normal station identifier is assigned during authentication process, and the assignment message is encrypted.
- The temporary station identifier is released after normal station identifier is assigned, and the normal station identifier is used for all the remaining transactions.