Security Architecture in Relay System

IEEE 802.16 Presentation Submission Template (Rev. 9)

Document Number:

IEEE C802.16m-08/1380

Date Submitted:

2008-10-31

Source:

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

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

Venue:

Re: TGm SDD: Relay; in response to the TGm Call for Comments and Contributions 802.16m-08/040

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:

Background

- Two security models are adopted in 802.16j
- Centralized security model
  - SA is established between BS and MS; No MS key is distributed to RSs; RS just forwards user traffic without decryption and re-encrytion
  - Pros: Simple; RS cannot see user data content
  - Cons: Doesn’t allow refragmentation/repacking and local bandwidth allocation based on piggybacked BR due to encrypted subheaders; Overhead due to ICV for each MS MAC PDU
- Distributed security model
  - SA is established between BS and MS; MS AK is distributed to access RS; Access RS generates/distributes TEK for access link; RS decrypts user traffic from access link using MS TEK and encrypt the tunnel packet using RS TEK
  - Pros: Enables refragmentation/repacking and local bandwidth allocation based piggybacked BR
  - Cons: MS AK (which is the base for all the other keys) is transferred to RS; RS can see user data content

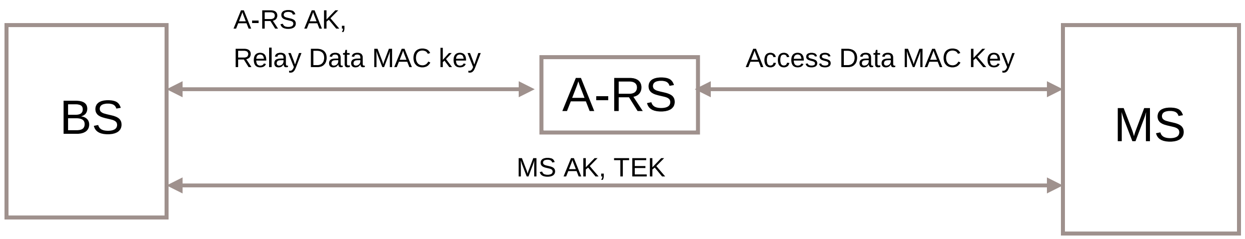
Motivation

- There are issues with both centralized and distributed security model in 16j.
- However with the 16j requirement of no change to MS, nothing can be done.
- We propose a new security model for .16m relay, which provides integrity protection for data sent over access link and end-to-end encryption between BS and MS. There is no need to transfer MS AK to RS.

Proposed Solution – Hybrid Security Model

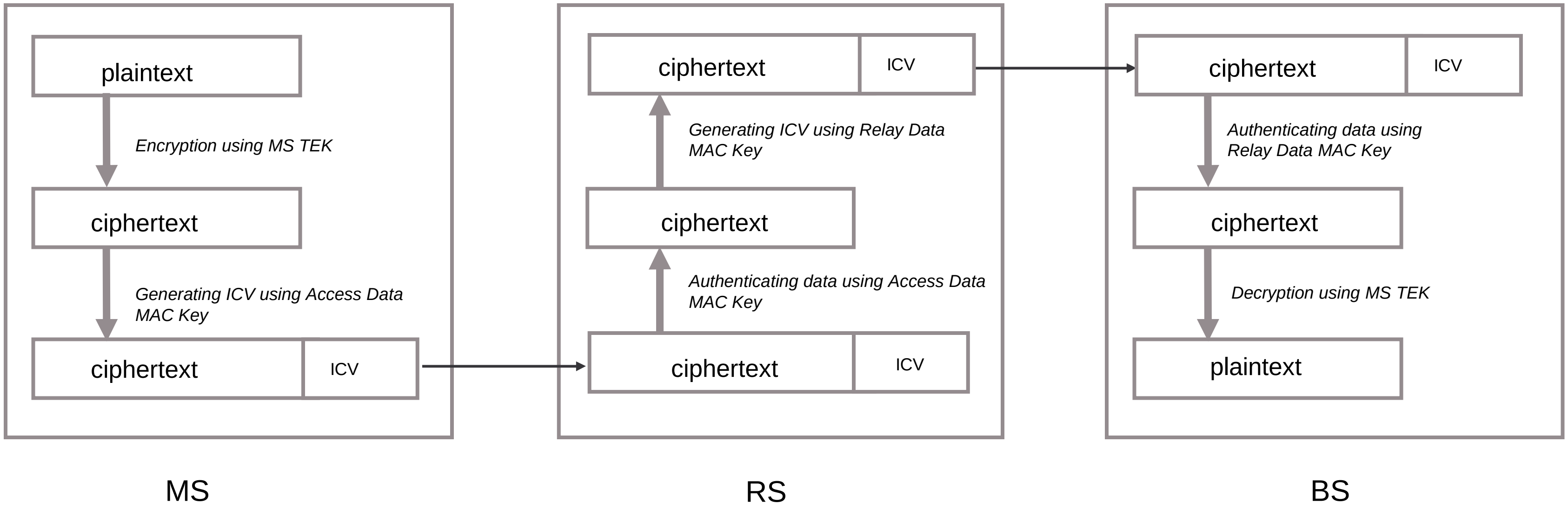
- MS is aware that it attaches to a BS or RS.
- MS Authentication is performed between MS and BS, w/o the involvement of RS.
- Subheaders are not encrypted but protected with ICV.
- Data traffic is encrypted/decrypted by MS and BS using TEK which is only known to MS and BS. RS cannot decrypt user data.
  - In order to reduce overhead, use the encryption algorithm that doesn't support integrity protection when refragmentation/repacking is used in relay link.
- ICV is added to the encrypted data to provide integrity protection of data sent over access link.
  - The key used to generate ICV is a key shared between MS and access RS, which could be generated and distributed by BS or RS.
  - ICV used over access link is removed after RS/MS verifies the data sent over access link.
- ICV is added to the end of payload of relay MAC PDU to provide integrity protection of data sent over relay link.
  - The key used to generate ICV is a key shared between BS and RS, and could be derived from RS AK, or generated and distributed by BS.

Keys Used for Different Links



- Between BS and MS
  - MS AK
  - TEK (generated and distributed by BS) – used to encrypt/decrypt user data
  - E2E MAC key (derived from AK) – used to authenticate MAC mgt msgs that are only processed by BS and MS
- Between BS and A-RS
  - A-RS AK
  - Relay Data MAC key (derived from A-RS AK or generated and distributed by BS) – used to provide integrity protection to the user data on relay link
- Between A-RS and MS
  - Access Data MAC key (generated and distributed by BS) – used to provide integrity protection to the user data on access link

Example Processing of UL User Data and Benefits


plaintext
Encryption using MS TEK
ciphertext
Generating ICV using Access Data MAC Key
ciphertext
ICV
ciphertext
ICV
Authenticating data using Access Data MAC Key
ciphertext
Generating ICV using Relay Data MAC Key
ciphertext
ICV
ciphertext
ICV
Authenticating data using Relay Data MAC Key
ciphertext
Decryption using MS TEK
plaintext
MS
RS
BS

- Benefits
  - No MS AK distribution to RS
  - RS is not able to see the content of user data
  - Allow local authentication at access link
  - All keys are generated at BS so that no security context transfer is needed at relay link during HO

Proposed Text

15 Support for multihop relay

15.x Security Model

- MS Authentication is performed between MS and BS, without the involvement of RS.
- Data traffic is encrypted and decrypted by MS and BS using TEK which is shared between MS and BS. RS doesn’t decrypt user data.
- Integrity protection of the user data sent over the access link is provided using the key shared between MS and access RS, which could be generated and distributed by BS or RS. The ICV used over the access link is removed from the MAC PDU after RS verifies the integrity of the UL data sent over access link.
- Integrity protection of the user data sent over the relay link is provided using the key shared between BS and access-RS, which could be derived from RS AK, or generated and distributed by BS. The ICV used over relay link is removed from relay MAC PDU after the access-RS verifies the integrity of the DL data sent over the relay link.