Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Security proposal for multi-hop relay system**
Date Submitted	**2007-05-098**
Source(s)	Sergey Seleznev, Hyoung Kyu Lim Samsung Electronics Co., LTD. 416, Maetan-3dong, Youngtong-gu, Suwon-si, Gyonggi-do, Korea Voice: +82 31 279 5968 Fax: +82 31 279 5130 s.sergey@samsung.com
Re:	IEEE802.16j-07/007r2: “Call for Technical Comments and Contributions regarding IEEE Project 802.16j”
Abstract	This contribution proposes security architecture and related procedures
Purpose	To propose security architecture and procedures for .16j MMR control plane
Notice	
Release	
Patent Policy and Procedures	

Security Proposal for Multi-Hop Relay System

Sergey Seleznev and Hyoung Kyu Lim
Samsung

1. Introduction and scope

In this contribution we extend existing 802.16e security procedures to Mobile Multi-Hop Relay system. Mainly, we propose security architecture that allows MMR control messages authenticity and integrity: key management procedures are based on PKMv2 (with respect to 802.16e-2005); additional PKMv2 messages and the way to reuse existing key hierarchy are defined to allow relay links SAs bootstrapping based on existing SAs between RS and MR-BS (BS). Please note, that solution does not cover access link.

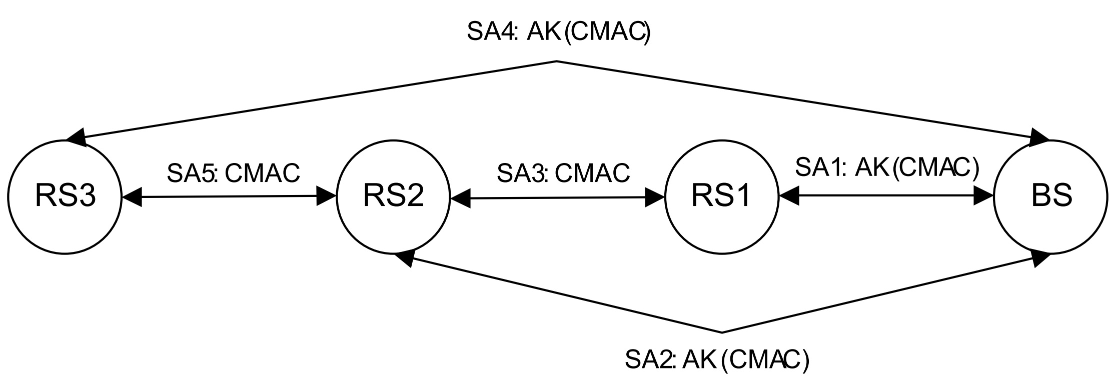
2. Objectives

In 802.16e MS and BS are mutually authenticated to each other. Any control message that is sent from MS to BS and backward is authenticated. Any data packet is authenticated and encrypted (if enabled).

In relay 802.16j relay system, relay station (RS) does not generate data plane traffic. Thus encryption procedures need not be implemented. However, management messages sent by RS still has to be protected including origin authentication and integrity protection. We assume that RS is able to send unicast control messages to another RS (1-hop away) and to BS. BS can send unicast control messages to any RS as well as BS can send broadcast and multicast messages to a set of RS under its control.

3. Proposed security architecture

Security architecture is presented on the following figure:



SA is a Security Association between corresponding entities. SAs exist for every BS and RS pair, and for every single-hop RS pair. This architecture is extendable to n-hop path.

AK and CMAC are keys used for the particular SA. For example, SA1 and SA2 have different AKs.

3.1 BS-RS SA

This SA is used to authenticate control messages between RS and BS. It is established during initial network entry and authorization, or during re-authentication. It is based on the Authorization Key (AK) with respect to 802.16e-2005. Authentication of the messages is based on CMAC function using CMAC_KEY_U and CMAC_KEY_D derived from AK as defined in the standard:

CMAC_KEY_U | CMAC_KEY_D | KEK ← Dot16KDF(AK, RS MAC Address | BSID |"CMAC_KEYS+KEK", 384)

KEK will be used for key transfer during RS to RS SA establishment.

3.2 RS-RS SA

This SA is used to authenticate the sender of a control message sent between single-hop RSs. It is newly defined association for the integrity protection of RS to RS wireless link. It uses the same CMAC function (which is more secure and thus preferable over HMAC).

3.2.1 Key derivation for RS-to-RS SA

Conceptually: key material is derived based on the preceding SA and distributed based on pre-preceding SA.

Consider two relay stations RS_n and RS_{n+1}, where $n = \{1...m\}$ is RS's position on the path, and RSs are sequentially ordered such that RS_1 is the closest to BS on that path, have to establish security association. RS_{n+1} derives SA keys as follows:

HMAC_KEY_U | HMAC_KEY_D | KEK <= Dot16KDF(AK, RS MAC Address | BSID |"HMAC_KEYS+KEK", 448)
$CMAC\_KEY\_U_2$| $CMAC\_KEY\_D_2$ <= Truncate (HMAC_KEY_U|HMAC_KEY_D, 256).

Then RS_{n+1} requests BS to generate and transfer this key to RS_n. BS generates $CMAC\_KEY\_U_2$ and $CMAC\_KEY\_D_2$ and sends it to RS_n using SA with that relay station.

Example: SA3 key material is bootstrapped from SA2 at RS2 and BS. ~~It is requested by RS2 from BS using SA2~~. Then it is transferred to RS1 using SA1.

4. Authentication, Authorization and Key Distribution

RS does not implement encryption procedures of 802.16e-2005.

Below procedures are described for two relay stations namely RS1 (as RS_n) and RS2 (as RS_{n+1}). RS2 is the RS which initiates RS1-RS2 SA establishment. RS1 plays passive role in this scenario.

4.1 Phase I: RS1 authentication and authorization

RS1 and BS perform legacy authentication procedures and key derivation. RS1-BS SA is established. See Fig. Phase I.

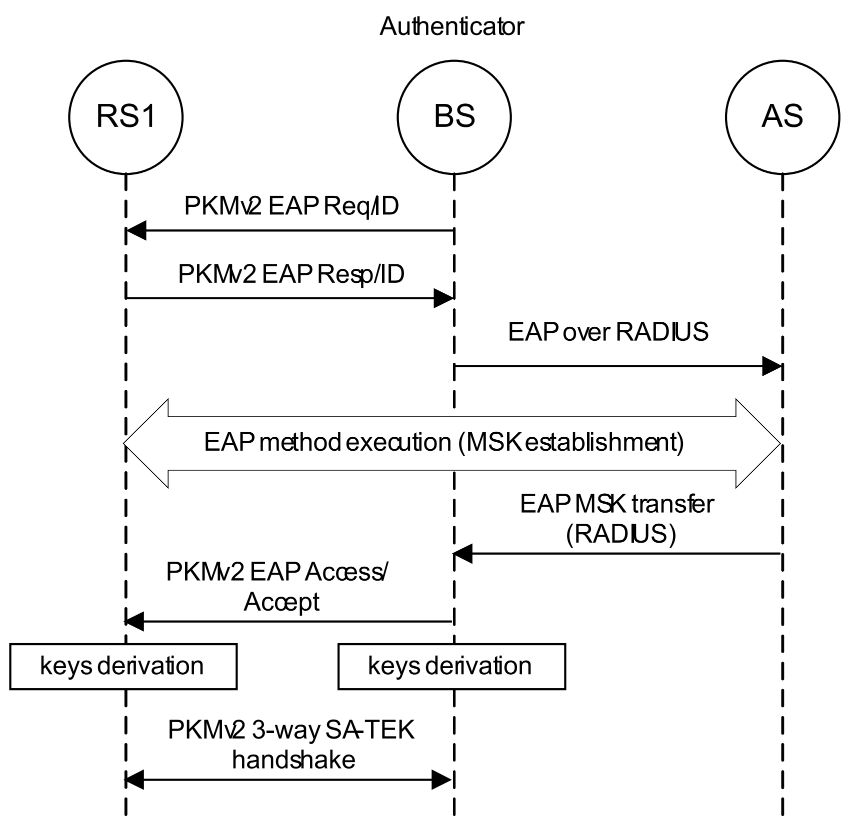
4.2 Phase II: RS2 authentication and authorization

RS2 and BS perform legacy authentication procedures and key derivation ($CMAC\_KEY\_U_2$ and $CMAC\_KEY\_D_2$ are also derived at RS2 and optionally at BS). RS2-BS SA is established. See Fig. Phase II.

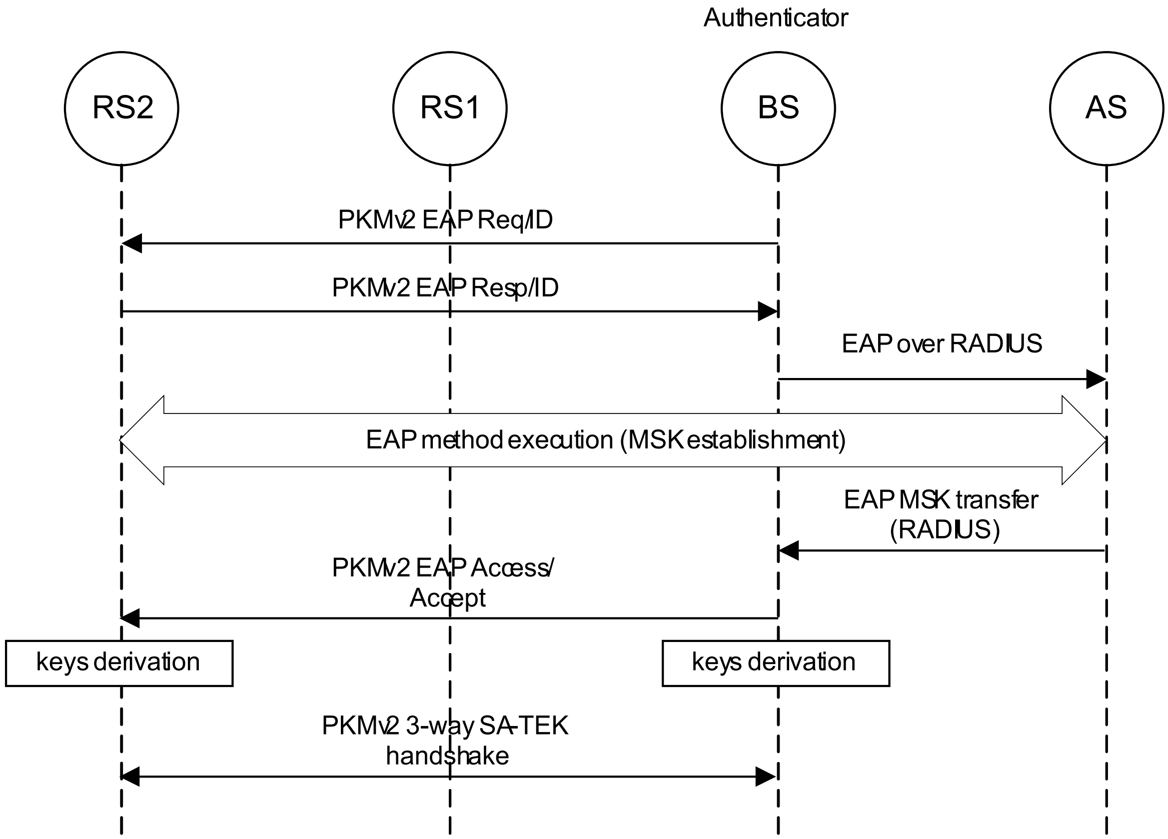
4.3 Phase III: RS2-RS1 SA establishment

Legacy 802.16e-2005 standard does not support key distribution for intermediate SA generation. We propose the following procedure and PKMv2 modifications to enable RS-to-RS key establishment.

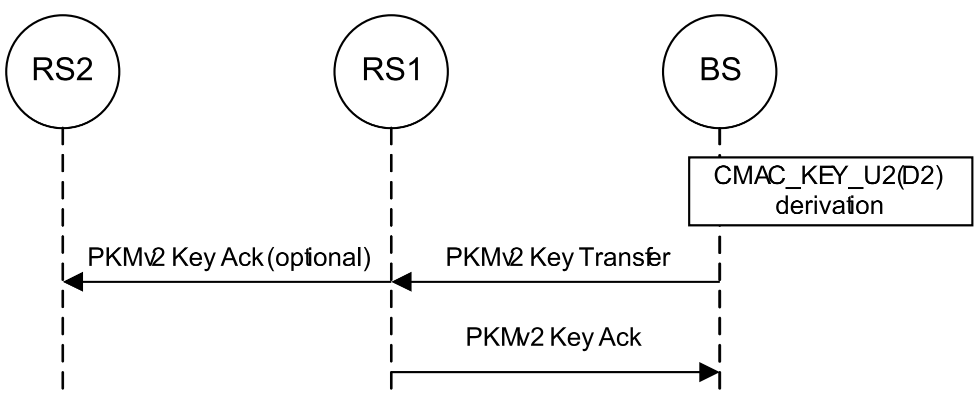
Upon successful authentication of RS2, BS sends PKMv2 Key Transfer message to RS1 as a preceding station. Key Transfer includes $CMAC\_KEY\_U_2$ and $CMAC\_KEY\_D_2$ corresponding to the keys RS2 has. Keys are encrypted by KEK of RS1. Upon reception of Key Transfer from BS, RS1 sends PKMv2 Key Acknowledgement message to RS2 and BS. This message should be protected by the key received in Key Transfer message. Thus RS2 and BS will be notified that RS2 and RS1 have established SA.



Phase I



Phase II



Phase III

4.4 PKMv2 Key Transfer and Key Acknowledgement

~~PKMv2 message codes:~~

~~Code~~	~~PKM message Type~~	~~MAC Management message name~~
~~31~~	~~PKMv2 Key Transfer~~	~~PKM-RSP~~
~~32~~	~~PKMv2 Key Acknowledgement~~	~~PKM-RSP~~
~~33-255~~	~~*Reserved*~~	~~-~~

~~PKMv2 Key Transfer attributes (includes additional parameters if used for other purposes):~~

~~Attribute~~	~~Contents~~
~~Key Sequence Number~~	~~RS AK sequence number~~
~~RS CID~~	~~RS's BCID~~
~~RS ID~~	~~Key Request originator's ID~~
~~SAID~~	~~Security association identifier~~
~~SAID~~	~~Key Request originator-BS SAID~~
~~CMAC -Parameters~~	~~- CMAC_KEY_U$_2$~~
~~CMAC -Parameters~~	~~- CMAC_KEY_D$_2$~~
~~CMAC Digest~~	~~Message Digest calculated using RS's AK~~

~~PKMv2 Key Acknowledgement attributes:~~

~~Attribute~~	~~Contents~~
~~*RS CID*~~	~~*RS's basic CID*~~
~~SAID~~	~~Key Request originator-BS SAID~~
~~Seee~~~~CMAC Digest~~	~~Message Digest calculated using CMAC_KEY_U$_2$~~

See proposed text for detail.

5. Usage scenarios

5.1 End-to-end security

Control messages are transferred between RS and BS. These messages are authenticated by CMAC_KEY_U and CMAC_KEY_D. Intermediate nodes are not able to modify or replay messages. They are not able to impersonate other RSs.

5.2. Hop-by-hop authentication

Control messages are signed and verified in hop-by-hop manner. Originator of the message calculates MAC using key from the SA it shares with the next hop on the path to destination. Upon reception of the message, next hop RS (intermediate RS) validates signature, removes old MAC and recalculates new MAC using the key it shares with the next hop.

Here, the ~~destination~~ originator of ~~the~~ message (i.e. BS in our case) should fully trust every RS on the path. ~~If one of them is compromised~~Compromised RS ~~it~~ can do any modifications to the message to be transferred to next RS. However, the whole system is not compromised.

Note: this scenario is applicable to either unicast or multicast authentication.

5.3 End-to-end security with hop-by-hop authentication

Management messages are signed by source RS with a key it shares with BS. In addition, they are signed and validated along the path as described in section 5~~4~~.2. In that case, every intermediate RS can check the validity of the message, while maintaining authenticity of the original message.

6. Summary

Proposed security solution provides fine security in relay system operation. That means, every entity is authenticated, and every message is authentic and integrity protected. RS to RS SAs are managed independently. In addition, we provide scenario for broadcast authentication.

7. Proposed text changes

+++++++++++++start text proposal+++++++++++++++++++

[*Insert the followings at the clause 7*]

The security sublayer provides relay system with authenticity and integrity by applying cryptographic transforms to control messages carried across connections between RSs, and between RSs and MR-BS.

The security sublayer employs an authenticated client/server key management protocol in which the MR-BS, the server, controls distribution of keying material to the client MS or RS.

Change section 7.1 as following

Security has the following components:

a) A key management protocol (PKM) providing secure distribution of keying data from the MR-BS to the RS or MS. Through this key management protocol, RS and MS synchronize keying data with MR-BS; in addition, the MR-BS uses the protocol to enforce conditional access to the network services.

Change section 7.2.1 as following

The PKM's authentication protocol establishes a shared secret (called an Authorization Key (AK)) between the SS and the BS, and between the RS and the BS. The shared secret is then used with PKM protocol as follows:

b) To establish a shared keys (called CMAC keys) between single-hop RSs.

Change the section 7.2.1.1 as following

A Security Association (SA) is the set of security information a MR-BS, RS and MS share in order to support secure communications across the IEEE 802.16j network. The following SAs are defined: MR-BS to RS, RS to RS, MR-BS to MS.

SAs are identified using SAID, except for RS to RS SAs. They are identified by the same SAID as requesting key RS shares with MR-BS.

Change section7.2.2.2.9 as following

CMAC keys are used to sign and verify management messages transferred between RSs in order to validate authenticity and integrity of these messages (i.e. for hop-by-hop message authentication).

CMAC keys for RS to RS communication are derived as follows:
CMAC_KEY_U2| CMAC_KEY_D2 <= Truncate (HMAC_KEY_U|HMAC_KEY_D, 256).

[*Insert the following section 7.4.1*]:

7.4.1 RS to RS SA CMAC key management

Upon successful authentication of RS, BS sends PKMv2 Key Transfer message to the right upstream RS of that just authenticated RS. Key Transfer includes CMAC_KEY_U$_2$ and CMAC_KEY_D$_2$ for RS to RS SA. Keys are encrypted by KEK of the right upstream RS. Upon reception of Key Transfer from BS, destination RS sends PKMv2 Key Acknowledgement message to the MR-BS and (optionally) to RS, whose ID is included in the Key Transfer message. This message should be protected by the key received in Key Transfer message. ~~CMAC keys for RS to RS link are requested by RS from BS for the right upstream RS using PKMv2 Key Request message. Upon reception of PKMv2 Key Request message, BS sends PKMv2 Key Transfer message to the right upstream RS of requesting RS. PKMv2 Key Transfer includes CMAC_KEY_U$_2$ and CMAC_KEY_D$_2$, and includes requesting RS identifier and SAID with BS to identify establishing link SA. Destination RS sends authenticated PKMv2 Key Acknowledgement message to the requesting RS, to enable secure message transfer between these two RSs.~~

Add following rows in the Table26:

Code	PKM message Type	MAC Management message name
31	*PKMv2 Key Transfer*	*PKM-RSP*
32	*PKMv2 Key Acknowledgement*	*PKM-RSP*
33-255	*Reserved*	-

[*Insert the following section 6.3.2.3.9.29*]:

Table xx – PKMv2 Key Transfer attributes

Attribute	*Contents*
~~*Key Sequence Number*~~	~~*RS AK sequence number*~~
RS CID	*RS's BCID*
RS ID	~~*Key request originator's ID*~~*RS ID to identify second RS of this SA*
SAID	*Security association identifier of the destination RS*
SAID	*RS to RS*~~*Key request originator-BS SAID*~~ *SA ID*
CMAC -Parameters	*- $CMAC\_KEY\_U_2$*
CMAC -Parameters	*- $CMAC\_KEY\_D_2$*
Nonce	A same random number included in the PKMv2 Key Request message
CMAC Digest	*Message Digest calculated using RS's AK.*

[*Insert the following section 6.3.2.3.9.30*]:

Table xx – PKMv2 Key Acknowledgement attributes

Attribute	*Contents*
RS CID	*RS's basic CID*
SAID	*RS to RS SA ID*~~*Key request originator-BS SAID*~~
Nonce	A same random number included in the PKMv2 Key Request message
CMAC Digest	*Message Digest calculated using $CMAC\_KEY\_U_2$.*

+++++++++++++end of text proposal+++++++++++++++++++