Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>	
Title	**Authentication of management messages in a relay system**	
Date Submitted	**2007-07-05**	
Source(s)	Sergey Seleznev, Hyoung Kyu Lim, Jungje Son Samsung Electronics Rep. of Korea, Gyonggi-do, Suwon	Voice: +82312795968 E-mail: s.sergey@samsung.com
Re:	IEEE 802.16j-07/019	
Abstract	This contribution describes a problem of using a single shared key for authentication of management messages in a relay system. Alternative solution, referred as pairwise key approach, is proposed.	
Purpose	Discuss and adopt proposed text changes.	
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	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.	
Patent Policy	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.	

Authentication of management messages in a relay system

Sergey Seleznev
Samsung Electronics

Problem description

Security Zone Key (SZK) is a shared key which is used by RSs to compute HMAC/CMAC_KEY_GD and HMAC/CMAC_KEY_GU group keys. These keys are same for all RSs in a security zone and used for authentication of MAC management messages which are transmitted over relay links.

Each H/CMAC_KEY_* has it associated HMAC/CMAC Packet Number Counter (H/CMAC_PN_*) to control number of messages which can be signed with that key. When H/CMAC_PN_* reaches the end of its number space, either reauthentication or key update procedure should be initiated. Moreover, H/CMAC_PN_* must be unique for each MAC management message with the CMAC tuple or digest. Any tuple value of {H/CMAC_PN_*, H/CMAC_KEY_*} shall not be used more than once. Since RSs share the same H/CMAC_KEY_G* keys, they should also share their counter values. However, there is no real-time counter sharing scheme in the current draft, and its implementation does not seem to be trivial.

Sharing H/CMAC keys between pairs of RSs (pairwise keys) is an alternative to group key concept. This approach does not have problem with H/CMAC_PN_*, since keys are bind to a particular link. We are proposing to limit the scope of SZK to multicast messages, where the counter value is fully controlled by the MR-BS, and to apply pairwise key approach to unicast messages authentication.

Introduction to pairwise key approach

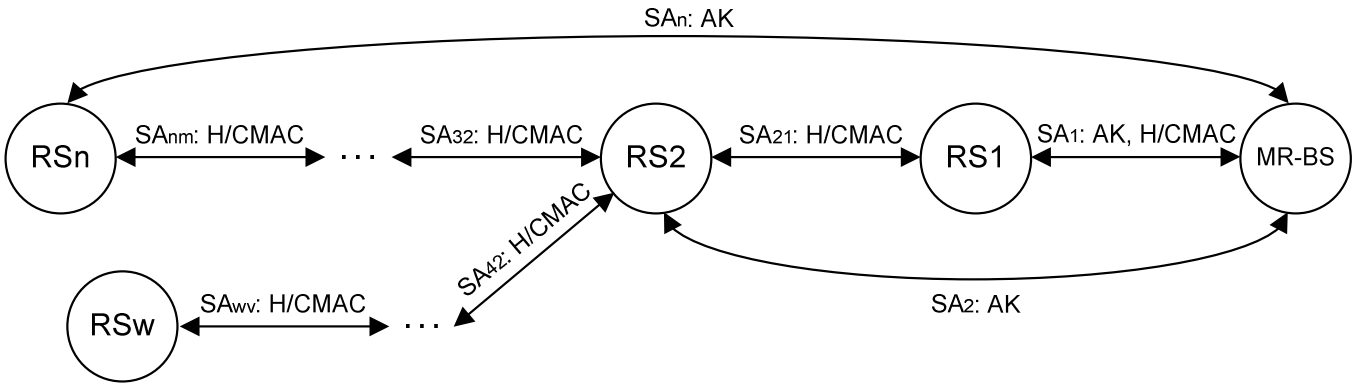

Fig.1 Security architecture

Security architecture is presented in Fig.1. SA is a Security Association between corresponding entities. SA_i exists for every BS and RS pair, and it is established during RS (re)authentication and authorization. SA_{ij} exists for every single-hop RS pair, and it is used for authentication of management messages transferred over relay links. SA_{ij} establishment is covered by this contribution.

Consider a pair of relay stations, e.g. RS_2 and RS_1, needs the security association SA_{21} (as depicted in Fig.1). RS_1 and RS_2 have already established SA_1 and SA_2, respectively, with MR-BS. SA_{21} establishment procedure should be performed right after PKMv2 SA-TEK 3-way handshake of RS_2.

At first, the RS_2 and MR-BS will derive HMAC/CMAC keys using EIK from SA_2 as follows:

CMAC_KEY_U2| CMAC_KEY_D2 <= Dot16KDF (EIK, RS MAC Address | BSID | “CMAC_LINK_KEYS”, 256)
HMAC_KEY_U2| HMAC_KEY_D2 <= Dot16KDF (EIK, RS MAC Address | BSID | “HMAC_LINK_KEYS”, 320)

Second, the MR-BS will transfer HMAC/CMAC_KEY_U2 and HMAC/CMAC_KEY_D2 to the RS_1. I.e. MR-BS will send PKMv2 Key Transfer message to RS_1 including SA_{21} keys encrypted by KEK from SA_2, RS_2 identifier (RSID) and associated security identifier.

Text proposal

[*Add the following subclause 7.1.7*]

7.1.7 Hop-by-hop authentication of management messages

Each pair of single-hop RSs share separate message authentication keys called CMAC_LINK_KEYS. During relay of management message, the RS should, first, shall validate appended Message Authentication Code (MAC) using the key it shares with previous hop RS on the path. If validation is successful, the RS shall remove old MAC and calculate another MAC using the key it shares with next hop RS on the path.

[*Change subclause 7.4.3 as follows*]:

The Security Zone Key (SZK) is a group key shared by the MR-BS and a group of RS within the same security zone. The membership of the security zone (i.e., which security zone(s) a RS should be belong to) is determined by the MR-BS. The SZK is used to authenticate multicast management messages within security zone. The SZK is randomly generated by the MR-BS and used as the GKEK to compute the HMAC/CMAC as defined in section 7.2.2.2.9. SZK is distributed by the MR-BS to a RS after the RS gets authenticated during initial network entry, using the same key distribution procedure defined for the GKEK distribution.

[*Change subclause 7.2.2.2.9 as follows*]:

MAC (message authentication code) keys are used to sign management messages in order to validate the authenticity of these messages. The MAC to be used is negotiated at SS Basic Capabilities negotiation.

There are different key for UL and DL messages. Also, a different message authentication key is generated for a multicast message (this is DL direction only) and for a unicast message.

In general, the message authentication keys used to generate the CMAC value and the HMAC-Digest are derived from AK.

The keys used for CMAC key and for KEK are as follows:

CMAC_KEY_U|CMAC_KEY_D|KEK<=Dot16KDF(AK, SS MAC Address|BSID|”CMAC_KEYS+KEK”,384)

CMAC_KEY_GD <= Dot16KDF(GKEK, “GROUP CMAC KEY”, 128) (Used for multicast MAC message such as PKMv2 Group-Key-Update-Command message). ~~and downlink unicast MAC message sent between RSs within the same security zone).~~

~~CMAC_KEY_GU <= Dot16KDF(GKEK, "GROUP CMAC KEY", 128) (Used for uplink unicast MAC message sent between RSs within the same security zone).~~

The keys used for HMAC key and for KEK are as follows:

HMAC_KEY_U|HCMAC_KEY_D|KEK<=Dot16KDF(AK, SS MAC Address|BSID|"HMAC_KEYS+KEK",448)

HMAC_KEY_GD <= Dot16KDF(GKEK, "GROUP HMAC KEY", 160) (Used for multicast MAC message such as PKMv2 Group-Key-Update-Command message). ~~and downlink unicast MAC message sent between RSs within the same security zone).~~

~~HMAC_KEY_GU <= Dot16KDF(GKEK, "GROUP HMAC KEY", 128) (Used for uplink unicast MAC message sent between RSs within the same security zone).~~

HMAC/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 SA are derived as follows:

CMAC_KEY_U2| CMAC_KEY_D2 <= Dot16KDF(EIK, RS MAC Address | BSID | "CMAC_LINK_KEYS", 256)

HMAC keys for RS to RS SA are derived as follows:

HMAC_KEY_U2| HMAC_KEY_D2 <= Dot16KDF(EIK, RS MAC Address | BSID | "HMAC_LINK_KEYS", 320)

[*Change subclause 7.5.4.4.1 as follows*]:

For authentication multicast message (in the DL only) a CMAC_KEY_GD shall be used (one for each group), group authentication key is derived from GKEK.

~~For an authentication unicast message transmitted between RSs within the same security zone, a CMAC_KEY_GU and CMAC_KEY_GD shall be used. The group authentication key is derived from GKEK, which is the same as SZK.~~

For an authentication of unicast message transmitted within relay zone, a HMAC/CMAC_KEY_U2 and HMAC/CMAC_KEY_D2 shall be used.

[*Change subclause 7.2.2.2.9 as follows*]:

[*Insert the following section 7.4.1*]:

7.4.1 RS to RS SA CMAC/HMAC key management

Upon successful authentication of the RS, MR-BS (or AR-RS) shall provide link keys for hop-by-hop authentication to its access RS. The MR-BS sends PKMv2 Key Transfer message, which includes HMAC/CMAC_KEY_U2 and HMAC/CMAC_KEY_D2 encrypted by KEK and authenticated, to the access RS. Upon reception of Key Transfer from MR-BS, the RS responds with PKMv2 Key Transfer Ack 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.

[*Add following rows in the Table 26*]:

Code	PKM message Type	MAC Management message name
Xx	PKMv2 Key Transfer	PKM-RSP
Xx	PKMv2 Key Transfer Ack	PKM-RSP
Xx-255	*Reserved*	-

[*Insert the following section 6.3.2.3.9.xx*]:

Table xx – PKMv2 Key Transfer attributes

Attribute	Contents
Key Sequence Number	AK sequence number
SAID	Security association identifier
RSID	RS ID to identify second RS of this SA
SAID	RS to RS security association identifier
CMAC -Parameters	HMAC/CMAC_KEY_U2, HMAC/CMAC_KEY_D2
Nonce	A random number generated in the MR-BS
CMAC Digest	Message authentication digest for this message

[*Insert the following section 6.3.2.3.9.xx*]:

Table xx – PKMv2 Key Transfer Ack attributes

Attribute	Contents
SAID	RS to RS SA ID
Nonce	A same random number included in the PKMv2 Key Transfer message
CMAC Digest	Message Digest calculated using CMAC_KEY_U_2.