Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>	
Title	**PN management in multi-hop relay**	
Date Submitted	**2007-09-09**	
Source(s)	Sergey Seleznev, Hyoung Kyu Lim, Hyunjeong Kang, 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 proposes text changes to clarify PN management in MR.	
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>.	

Packet Number management in MR

Sergey Seleznev, Hyoung Kyu Lim, Hyunjeong Kang, Jungje Son
Samsung Electronics

Introduction

In multi-hop relay system, RSs in a security zone use group key for authentication of control messages transmitted over relay links. Current spec defines a UL and DL PN pair to be used with a key. However, since PN is not shared between multiple sources of messages, that will create inconsistency between PNs included in HMAC/CMAC tuples. Thus MR-BS shall maintain separate PNs for UL and DL connections with every RS. RS shall maintain a proper PN for connections it shares with the MR-BS.

In addition, the RS may generate and send a message (i.e. DSAx and DSCx) to its subordinate or super-ordinate station. RS shall send a message using destination RS's primary CID. MR-BS can also send a message to any RS using its primary CID. In the meantime, PN shall be incremented for every new message. In order to avoid inconsistency in PN used by source RS and the MR-BS, RS shall implement two sets of UL/DL PN: for connections it holds with the MR-BS and for connections it hold with its subordinate and super-ordinate stations.

Destination RS shall also be able to differentiate which PN is included into HMAC/CMAC tuple. This can be achieved by using one of the 'reserved' bits in HMAC/CMAC tuple as 'PN type' bit.

Proposed text changes

[*Insert the following subclause 7.5.7*]

7.5.7 Calculation of HMAC/CMAC digests in a security zone

RS follows the HMAC or CMAC calculation procedure as that for the MS. However, packet number management is different within security zone.

In MR, the MR-BS shall maintain separate Security Zone HMAC/CMAC Packet Number Counter, HMAC/CMAC_PN_SZ*, with every RS within security zone. Any tuple value {HMAC/CMAC_PN_SZ*, HMAC/CMAC_KEY_SZ*, CID} shall not be used more than once. HMAC/CMAC_PN_SZ* shall be used for messages transferred between RS and the MR-BS under the SZK.

RS shall maintain HMAC/CMAC_PN_SZ* with the MR-BS. In addition, RS shall maintain Relay Link HMAC/CMAC Packet Number Counters, HMAC/CMAC_PN_RL*, with it subordinate and superordinate RSs. HMAC/CMAC_PN_RL* shall be used by RS to send one-hop relay management messages (such as DSAx and DSCx messages) under the SZK.

The following CMAC_PAD values shall be used for the purpose of replay protection:

- CMAC_PAD = 0x7E in case of CMAC_PN_SZ*;
- CMAC_PAD = 0x7D in case of CMAC_PN_RL*.

[*Delete the following text from subclause 7.5.4.4.1*]

~~Insert the following after the second paragraph of 7.5.4.4.1:~~

~~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.~~

[*Change table 598 as follows*]

Table 598—CMAC Tuple definition

Field	Length (bits)	Note
Reserved	3	Set to 0
PN type	1	0 – Security zone PN, 1 – Relay Link PN
CMAC Key Sequence Number	4	CMAC key sequence number
BSID	48	Only used in case of MDHO zone—optional
CMAC_PN_*, CMAC_PN_SZ* or CMAC_PN_RL*	32	This context is different UL, DL
CMAC Value	64	CMAC with AES-128

[*Change table 600 as follows*]

Table 599—Short-HMAC tuple definition

Field	Length (bits)	Note
Reserved	3	Set to 0
PN type	1	0 – Security zone PN, 1 – Relay Link PN
HMAC Key Sequence Number	4	CMAC key sequence number
HMAC Packet Number Counter HMAC_PN_*, CMAC_PN_SZ* or CMAC_PN_RL*	32	Replay counter
Short-HMAC digest	*variable*	0—Truncate HMAC to 8 bytes in Short HMAC Tuple 1—Truncate to 10 bytes 2—Truncate to 12 bytes