Project	IEEE 802.16 Broadband Wireless Access Working Group <**http://IEEE 802.org/16**>	
Title	Security Zone Key generation and management for multi-hop relay system	
Date Submitted	2007-03-05	
Source(s)	Sheng Sun; Guo-Qiang Wang; Hang Zhang; Peiying Zhu; Wen Tong; Mohan Fong 3500 Carling Avenue Ottawa, Ontario K2H 8E9	Voice: [mailto:shengs@nortel.com]
	Haihong Zheng, Yousuf Saifullah, Shashikant Maheshwari Nokia 6000 Connection Drive, Irving, TX	Voice: +1 972 894 5000 Haihong.1.Zheng@nokia.com, Yousuf.Saifullah@nokia.com, Shashikant.Maheshwari@nokia.com
Re:	Response to a call for contributions.	
Abstract	Security elements and mechanisms for .16j MMR control plane	
Purpose	To propose the security mechanisms for .16j MMR control plane	
Notice	This document has been prepared to assist IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) 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 and Procedures	The contributor is familiar with the IEEE 802.16 Patent Policy and Procedures <http://IEEE 802.org/16/ipr/patents/policy.html>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for	

	delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <mailto:chair@wirelessman.org> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.16 Working Group. The Chair will disclose this notification via the IEEE 802.16 web site <http://IEEE 802.org/16/ipr/patents/notices>.

Security Zone Key Generation and Management for Multihop Relay

Sheng Sun; Guo-qiang Wang; Hang Zhang;
Peiying Zhu; Wen Tong; Mo-han Fong
Nortel

Haihong Zheng, Yousuf Saifullah, Shashikant Maheshwari
Nokia

1 Introduction

This contribution aims to introduce the security mechanisms into the .16j system to protect the confidentiality and integrity of the transmission of the MAC management messages among a group of RSs and MR-BS. The key distribution and management model are laid on the security principles of PKMv2 required with respect to the IEEE 802.16-2004 and IEEE 802.16e-2005.

1.1 Key Management

The SZK (Security Zone Key) 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 protect the integrity of the MAC management message transmitted between the RSs in the same security zone. It is generated by using the following options:

Option 1: Reuse the GKEK (Group Key Encryption Key) (Sec 7.2.2.2.7, IEEE 802.16e-2005)

Option 2: Randomly generated by MR-BS's RNG (Random Number Generator)

The SZK is distributed by the MR-BS to a RS after the RS gets authenticated during its initial network entry. The key itself is used to either encrypt the MAC management messages or at the minimum security defense by using HMAC/CMAC function to authenticate the message.

1.2 SZK Exchange

In order to securely distribute the Security Zone Key (SZK) to the RSs within one particular security zone, MR-BS would use security handshake to protect the attacks, i.e Replay attacks, interception attack. The TEK exchange 3-way handshake procedure specified in the PKMv2 could be used for such purpose.

2. Proposed text changes

++++++++++++ start text proposal ++++++++++++++++++++++++++++++++++++
[Insert the followings after the end of section 7.4]

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 the MAC management messages transmitted over the relay links. 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.

7.4.1 Security Zone Key Exchange

The TEK exchange 3-way handshake procedure specified in the PKMv2 is used for MR-BS to distribute the Security Zone Key (SZK) to the RSs within one security zone

Change section 7.2.2.2.9 as following

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

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

Change section 7.5.4.4.1 as following

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

+++++++++++++++++++ *End of text proposal* ++++++++++++++++++++++