Project	IEEE 802.16 Broadband Wireless Access Working Group <**http://IEEE 802.org/16**>
Title	Key Hierarchy of the RRSP for the MMR Relay Network
Date Submitted	2007-01-08
Source(s)	Sheng Sun; Guo-Qiang Wang; Hang Zhang; Peiying Zhu; Wen Tong; Mo-han Fong 3500 Carling Avenue Ottawa, Ontario K2H 8E9 Voice: +1 613 7631315 [mailto:wentong@nortel.com] [mailto:shengs@nortel.com]
Re:	A response to a Call for Technical Proposal, http://wirelessman.org/relay/docs/80216j-06_034.pdf
Abstract	Security elements and mechanisms for .16j MMR control plane
Purpose	To incorporate the proposed text into the P802.16j Baseline Document (IEEE 802.16j-06/026r1)
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>.

Key Hierarchy of the RRSP for the MMR Relay Network

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

1 Introduction

This contribution aims to introduce the security mechanisms into the .16j MMR control plane to protect the confidentiality and integrity of the transmission of the MMR control messages. The encryption 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.

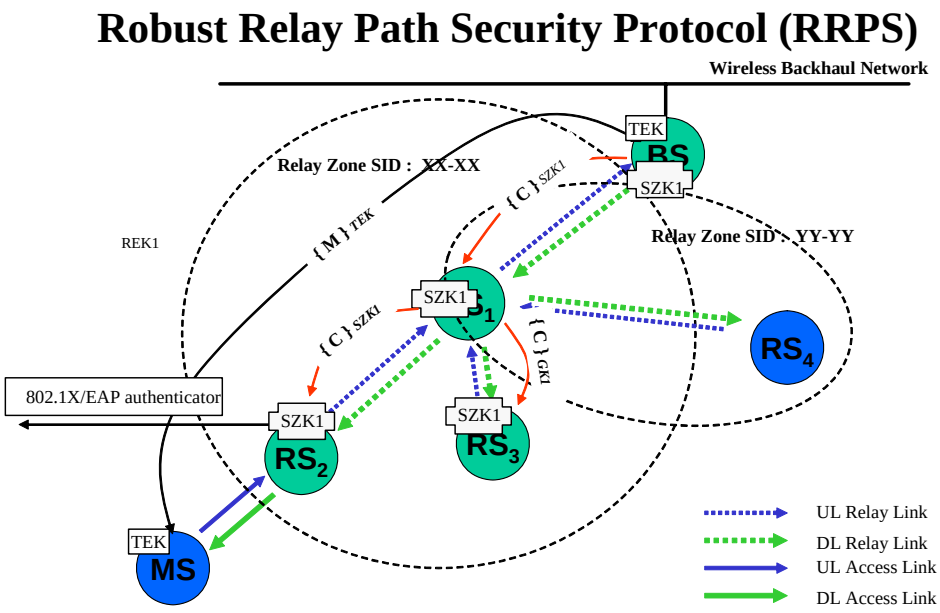

Figure 1 RRPS overview

1.1 RRPS (Robust Relay Path Security)

1.1.1 RRPS overview

Robust Relay Path Security (RRPS) service is used to permit efficient establishment of transmission between the Base Station (BS) and Relay Stations (RS) in a .16j MMR network.

Today's .16e network security services provide the minimum security protection to the control planes messages (Sec 7.1.1 of IEEE 802.16e-2005) in the Access link. The multi-hop based MMR relay network needs more complicated security model in order to satisfy both of the security objective and the performance objective. In other words, the security mechanism in the .16j MMR network should impose very minimum overhead onto the

control plane. Another metric of the security model required for .16j network is the fast link/path establishment and the fast re-association in the case of link failure or the handover operations.

RRPS is the security framework comprising the following security elements

Hybrid Association/Authentication Model

Encryption Keys and Keys distribution

The operation of RRPS relies on the BS which centralizes the authentication for the RSs within its Security Zone identified by the SZID (Security Zone ID). Each RS within the security zone becomes the Delegated Authenticator (DA) when it gets authenticated from its anchored authenticator as illustrated in the following diagram.

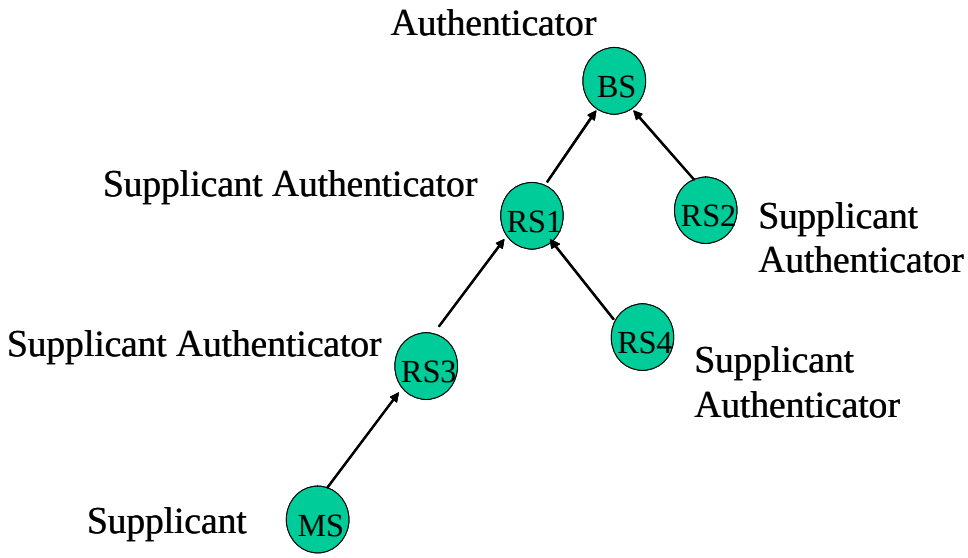

Figure 2 Authentication Hierarcy

This authentication hierarchy distributes the authenticator function to the perimeter of the security zone. Any RS assumes the authenticator role implements the full PKMv2 authentication function. The distributed authentication model virtually extends the BS's authentication function as closer to the .16e/d access link as possible, which brings the following characteristics:

- Basic uses IEEE 802.16e-2005 PKMv2
- Many relay operations are associated with paths, and these operations populate the same information to all RS along a given path
- MMR cell could be decomposed as security zones
- In each zone, the RSs share the same group key for path-oriented operations
- Group key is managed and distributed by BS
- Per Group SA associated HMAC/CMAC is used to authenticate the sender
- Group-cast signaling messages are defined to support path operations
- Greatly reduce the signaling overhead, especially in RS handover case

RRPS requires information to be exchanged during a RS's initial security association with a Authenticator, Subsequent security associations to other Authenticators within the same security zone may utilize the PKMv2 key hierarchy that is established during Initial RRPS Authentication.

Note: How to define security zone is out of scope of this contribution.

1.1.2 Key Management and Key Hierarchy

As per the Key hierarchy inherent from the PKMv2, RRPS may keep all the existing keys for each RS such as the MSK, AK, TEK, KEK etc with their original derivation hierarchy, and share Security Zone Keys (SZK) for path-oriented control plane messaging . There are two options to define SZK:

Reuse the GTEK (Group Traffic Encryption Key) (Sec 7.2.2.2.7, IEEE 802.16e-2005)

Randomly generated by MMR-BS's RNG (Random Number Generator) and distributed to the RS

The SZK is distributed by the MMR-BS at the first contact of any RS within its security zone. The key itself is used to either encrypt the Multicast based control messages or at the minimum security defense by using HMAC/CMAC data signature function to protect the message's integrity

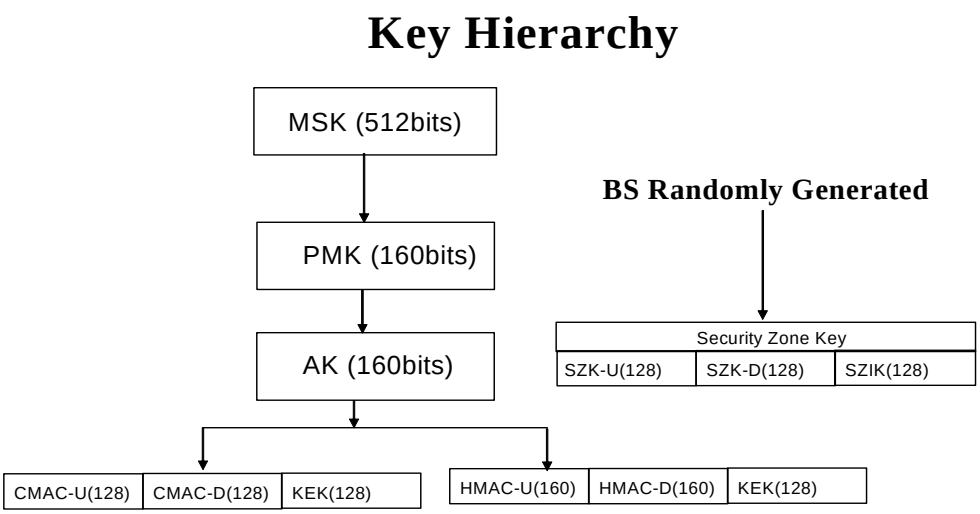

Figure 3 Key Hierarcy

1.1.4 Security Zone Key Exchange

In order to securely distribute the Security Zone Key (SZK) to the RSs within one particular security zone, MMR-BS would use security handshake to protect the attacks, i.e Replay attacks, interception attack. The bottom line is to reuse the TEK exchange 3-way handshake specified in the PKMv2

2. Proposed text changes

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

As per the Key hierarchy inherent from the PKMv2, RRPS may keep all the existing keys for each RS such as the MSK, AK, TEK, KEK etc with their original derivation hierarchy, and share Security Zone Keys (SZK) for path-oriented control plane messaging . There are two options to define SZK:

Reuse the GTEK (Group Traffic Encryption Key) (Sec 7.2.2.2.7, IEEE 802.16e-2005)

Randomly generated by MMR-BS's RNG (Random Number Generator) and distributed to the RS

The SZK is distributed by the MMR-BS at the first contact of any RS within its security zone. The SZK within each Security Zone is used to protect (by encrypting or signing) the control messages transmitted over the links between Relay Stations (RS) and the links between Relay Stations and the MMR-BS. There are two optional purposes of generation of the SZK: a) To encrypt the control messages among the RSs and the MMR-BS by using the AES-CCMP protocol specified in the PKMv2, b) to generate the HMAC/CMAC tuple to protect the integrity of the control messages.

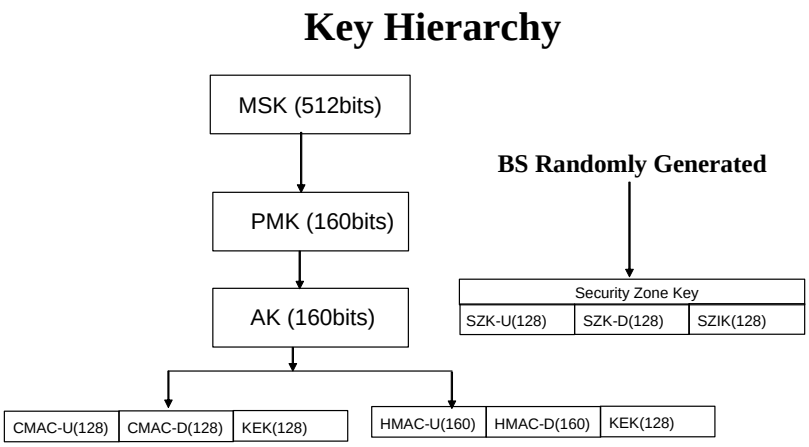

Figure P Key Hierarcy

7.4.1 Security Zone Key Exchange

In order to securely distribute the Security Zone Key (SZK) to the RSs within one particular security zone, MMR-BS would use security handshake to protect the attacks, i.e Replay attacks, interception attack. The bottom line is to reuse the TEK exchange 3-way handshake specified in the PKMv2

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