| | | |
|---|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** | |
| Title | **Centralized Security in Multi-hop Relay System** | |
| Date Submitted | **March-5-2007** | |
| Source(s) | Haihong Zheng, Yousuf Saifullah, Shashikant Maheshwari<br>Nokia<br>6000 Connection Drive, Irving, TX | Voice: +1 972 894 5000<br>Haihong.1.Zheng@nokia.com,<br>Yousuf.Saifullah@nokia.com,<br>Shashikant.Maheshwari@nokia.com |
| | Aik Chindapol<br>Siemens Corporate Research<br>755 College Road East, Princeton, NJ | Voice: + 1 609 734 3364<br>aik.chindapol@siemens.com |
| | Sheng Sun; Guo-Qiang Wang; Hang Zhang; Peiying Zhu; Wen Tong; Mo-han Fong<br>3500 Carling Avenue<br>Nortel Networks<br>Ottawa, Ontario K2H 8E9 | Voice: 1-613-763-1315<br>[mailto:wentong@nortel.com]<br>[mailto:pyzhu@nortel.com]<br>[mailto:shengs@nortel.com] |
| | Kanchei (Ken) Loa, Yi-Hsueh Tsai, Chih-Chiang Hsieh, Yung-Ting Lee, Hua-Chiang Yin, Shiann-Tsong Sheu,<br>Frank C.D. Tsai, Youn-Tai Lee, Heng-Iang Hsu<br>Institute for Information Industry, 8F., No. 218, Sec. 2, Dunhua S. Rd., Taipei City, Taiwan. | Voice: +886-2-2739-9616<br>loa@iii.org.tw |
| Re: | This is in response to the call for proposal, 80216j-07_7r2.pdf, sent out by 802.16j TG. | |
| Abstract | This contribution proposes path management procedures in multi-hop relay system. The path management procedures include path calculation, path establishment and path selection. The relevant changes to the specification are also defined. | |
| Purpose | Add proposed spec changes. | |

| | |
|---|---|
| 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://ieee802.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://ieee802.org/16/ipr/patents/notices>. |

# Centralized Security in Multi-hop Relay System

## 1. OVERVIEW

In the 802.16e system, security association is established between the MS and BS. The AK for the MS is distributed to the BS by the authentication server, which is used to derive the other keys such as KEK. In this proposal, we propose to apply the same security model in the multi-hop relay system, i.e., the security association is established between MS and MR-BS without the involvement from the intermediate RS. With such centralized security model, all the PKM messages are exchanged between MS and MR-BS..In order to prevent man-in-middle attack, the access RS may add HMAC/CMAC tuple using the SA established between itself and the MR-BS into the PKM-REQ and PKM-RSP that are not protected by the message authentication code generated by MS. For all the other cases, the access RS and the intermediate RSs just simply relay the PKM messages (as shown in Figure 1). All the keys are stored and maintained at the MS and MR-BS, and RS doesn't have any key information associated with the MS. An RS does not try to decrypt the user data or authenticate the MAC management message it receives from the MS, but simply relays it. An RS uses the same security architecture and procedures as an SS to provide privacy, authentication and confidentiality between itself and MR-BS.

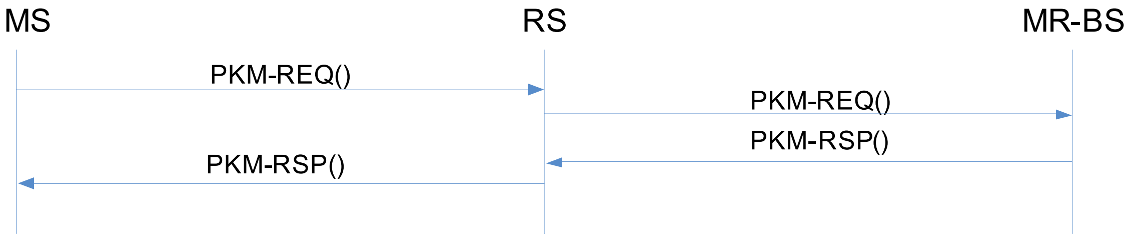

Figure 1: Relaying of PKM Protocols in Intermediate RSs

With this centralized security model, RS can be kept simple and there is no need for MR-BS to distribute user sensitive information such as AK to any RS over the air interface. Note that this contribution doesn't exclude a distributed security model if becoming available.

## 2. CHANGES TO THE SPECIFICATION

***Insert following paragraph before section 7.1.1***

In multihop relay system, RS,uses the same security architecture and procedures as an SS to provide privacy, authentication and confidentiality between itself and the MR-BS.

***Add following paragraph in section 7.1.6***

7.1.6 Centralized Security Control in Multi-hop Relay System

With centralized security control residing in the MR-BS in the multihop relay system, the security association is established between MS and MR-BS without the involvement from the intermediate RS. RS does not try to decrypt the user data or authenticate the MAC management message it receives from the MS, but simply relays it.

Similar to other MAC management messages, all the PKM messages are exchanged between MS and MR-BS. For the PKM messages that are not protected by the message authentication code from the MS (termed as non-MS-authenticated PKM messages, e.g., Authorization Request, Authorization Reply, PKMv2 RSA-Request, PKMv2 RSA-Reply), the following procedure may be applied. For all the other cases, the access RS and the intermediate RSs just simply relay the PKM messages.

- Upon receiving a non-MS-authenticated PKM message, the access RS may add the HMAC/CMAC tuple based on the SA established between itself and the MR-BS into the message.
- Upon receiving a non-MS-authenticated PKM message with the presence of HMAC/CMAC tuple, the MR-BS authenticates the message based on the shared SA between itself and the access RS.
- When the MR-BS generates a non-MS-authenticated PKM message to the MS, it may add the HMAC/CMAC tuple based on the SA established between itself and the access RS.
- Upon receiving a non-MS-authenticated PKM message with the presence of HMAC/CMAC tuple, the access RS authenticates the message based on the SA between itself and MR-BS. If the message is valid, it then removes the HMAC/CMAC tuple, and then sends the PKM message to the MS.

All the keys are stored and maintained at the MS and MR-BS, and RS doesn’t have any key information associated with the MS.