Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Security ad-hoc – Minutes of the 2nd conference call**	
Date Submitted	**2007-05-04**	
Source(s)	**Sheng (Robert) Sun Chair, Security Ad-hoc Nortel 3500 Carling Avenue Ottawa, On K2H 8E9 Canada**	**Voice: +1 613 763 4460 shengs@nortel.com**
Re:		
Abstract	**Minutes of the first conference call of the Relay TG's Other MAC/PHY ad hoc, held on 4 April 2007.**	
Purpose	**Information**	
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>.**	

Security Ad-hoc: Minutes of the 2nd conference call

Sheng Sun

Chair: Sheng Sun
Date: Apr 19th , 2007

Attendees:

Haihong Zheng	**Nokia**	**haihong.1.zheng@nokia.com**
Yousuf Saifullah	**Nokia**	**Yousuf.Saifullah@nokia.com**
cancan huang	**ZTE**	**chuang@zteusa.com**
Sergey Seleznev	**Samsung**	**s.sergey@samsung.com**
Yanling Lu	**Huawei**	**luyanling@huawei.com**
Kanchei(Ken) Loa	**III**	**loa@nmi.iii.org.tw**
Masato Okuda	**Fijitsu**	**okuda@jp.fujitsu.com**
Hang Zhang	**Nortel**	**hazhang @nortel.com**
Sheng Sun	**Nortel**	**shengs@nortel.com**

(Please be advised that I may have missed out some of comments in the minutes, please feel free to add and correct me)

Review of new contributions

1: #C802.16j-07/274 Security proposal for multi-hop relay system
Presenter : Sergey Seleznev Sumsang
Comments: - This proposal shares the design purposes and some characteristics with #134 (Yousuf)
- This proposal has the scope with the relay network. how would it relate to the MS access authentication? (Hang)
Actions for Authors: Discuss with Nortel about the potential harmonization

2: #C80216j-08_283 Secure extended MAC header II
Presenter: Yousuf Saifullah (Nokia)
Comments: - The counter value added in the header will increase the header size, also it needs synchronization, otherwise, no consistence (Masato, Can)
- The A-HCS header is too short to protect the header, needs at 16/32bits (Sergey)
- The new MAC header type also needs thorough investigation from Ad-hoc group (Sheng)
- The new HCS bits algorithm needs more investigation (Hang)

Actions for Authors: - Also submit this proposal to PHY/MAC ad-hoc group
- Also investigate the strength of longer HCS protection

Update of existing contributions

1: #C80216j-08_201 Centralized authentication for multi-hop relay system
Presenter : Haihong Zheng (Nokia)
Updates: - RS being transparent to authentication process could lead to expose the MR-BS to the attack (Can)
- The MS-CID is also carried over the transparent RS which disallows the aggregation (Hang)

2 #C80216j-08_188 Shared Management Message in MR system: Format, Transfer and Security for next conference
Presenter: Yanling Lu (Hisilicon)
Comments: - The concern with the two-tier overhead with the addition of the HMAC/CMAC tuple (Haihong)
Actions for authors: Put the application bounds on this proposal

3 #C80216j-08_149 TEK Transfer in Relay Systems (Withdrawed and merged with #098)
Presenter: Masato Okuda(Fijitsu)

4 #C80216j-08_098 Distributed authentication for .16j relay system
Presenter: Sheng Sun (Nortel)
Comments: - The comprise of single RS which is vulnerable to attacks, could break the whole security system within the Relay network (Haihong/Sergey/Kan)
- The transfer AK down to RS is not safe as RS (Haihong/Sergey)

5: #C80216j-08_134 Security Zone Key generation and management for multi-hop relay system
Presenter: Sheng Sun
Comments: - Short of time to discuss in depth, will discuss over the emails

Stroll poll on the authentication scheme(s) that should be adopted in the 16j security

- **2/9 supports Centralized Authentication only**
- **1/9 supports Distributed authentication only**
- **5/9 supports Both authentication should appear in the security**
- **1/9 supports Centralized Authentication but willing to look at other distributed authentication scheme**

Chairman's recommedations: Suggest to adopt both authentication schemes which in essence still need improvements , in 16j baseline document so as to reflect majiority opinions since both schemes have strength and limitations in different application scenarios