Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Security ad-hoc – Minutes of the 1st 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 1st conference call

Sheng Sun

Chair: Sheng Sun

Date: Apr 4th, 2007, GMT 13:00

Attendees:

Haihong Zheng	Nokia	haihong.1.zheng@nokia.com
Yousuf Saifullah	Nokia	Yousuf.Saifullah@nokia.com
cancan huang	ZTE	chuang@zteusa.com
RT	ITRI	rtwang@csie.nctu.edu.tw
Sergey Seleznev	Samsung	s.sergey@samsung.com
Dan Brown	Motorola	ADB002@motorola.com
Roger Paterson	Motorola	r.peterson@motorola.com
Yanling Lu	Huawei	luyanling@huawei.com
Youn-Tai Lee	III	lyt@nmi.iii.org.tw
Kanchei(Ken) Loa	III	loa@nmi.iii.org.tw
Hua-Chiang Yin	III	hcyin@nmi.iii.org.tw
Yung-Ting Lee	III	lyd@nmi.iii.org.tw
Masato Okuda	Fijitsu	okuda@jp.fujitsu.com
Peiying Zhu	Nortel	pyzhu@nortel.com
Sheng Sun	Nortel	shengs@nortel.com

(Note: If I had missed out anyone's name or mis-spelled, please feel free to contact me for correction)

Contributions being reviewed

1: #C80216j-08_201 Centralized authentication for multi-hop relay system
Presenter : Haihong Zheng (Nokia)
Comments: - RS being transparent to authentication process could lead to expose the MR-BS to the attack (ZTE)
- The HMAC/CMAC tuple isn't enough to protect the PKM authentication information messages (Hisilicon and Motorola)

Resolutions: Open for improvements via discussion and harmonization for next conference

2: #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 (Nokia)
- The transfer AK down to RS is not safe as RS (Nokia)

Resolutions: Open for improvements via discussion and harmonization for next conference

3: #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 (Nokia)

- The concern w.r.t uplink message transporting based on the shared management scheme (Motorola)

Resolutions: Open for improvements via discussion and harmonization for next conference

4:#C80216j-08_149 TEK Transfer in Relay Systems
Presenter: Masato Okuda
Comments: - The insecure transfer of the TEK to RS given the RS has no track of the security association of the MS authentication (Nortel)
- The comprise of single RS which is vulnerable to attacks, could break the whole security system within the Relay network (Nokia and ITRI)

Resolutions: Open for improvements via discussion and harmonization for next conference

5: #C80216j-08_134 Security Zone Key generation and management for multi-hop relay system
Presenter: Sheng Sun
Comments: - Question regards whether the Group key applies to both Unicast and multicast management messages

Resolutions: Open for improvements via discussion and harmonization for next conference

Action items for all ad-hoc group participants :

- Send comments and questions for clarification to each contribution authors or utilize the security ad-hoc group email reflector

1: #C80216j-08_201 Centralized authentication for multi-hop relay system

Author : Haihong Zheng (haihong.1.zheng@nokia.com)

2: :#C80216j-08_098 Distributed authentication for .16j relay system
Author : Sheng sun(shengs@nortel.com)

3: #C80216j-08_188 Shared Management Message in MR system: Format, Transfer and Security for next conference
Author : Yanling Lu (luyanying@huawei.com)

4::#C80216j-08_149 TEK Transfer in Relay Systems
Author : Masato Okuda(okuda@jp.fujitsu.com)

5: #C80216j-08_134 Security Zone Key generation and management for multi-hop relay system
Author: Sheng Sun (shengs@nortel.com)

General Comments: Many security options may lead to bigger security problems (Can)