Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>	
Title	**SZK Generation Algorithm**	
Date Submitted	**2007-08-25**	
Source(s)	Sheng Sun; Guo-Qiang Wang; Hang Zhang; Nortel 3500 Carling Avenue Ottawa, Ontario K2H 8E9	Voice: +613-763-4460 E-mail: guoqiang @nortel.com Voice: +613-765-4159 E-mail: pyzhu@nortel.com
Re:	IEEE P802.16j/D1: IEEE 802.16j working group letter ballot #28	
Abstract		
Purpose	To incorporate the proposed text into the P802.16j/D1 Baseline Document	
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups.* It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who 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	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.	

SZK Generation function

Sheng Sun, G.Q Wang ,Hang Zhang, Peiying Zhu, Mo-Han Fong, Wen Tong, David Steer, Gamini Senarath, , Derek Yu, Israfil Bahceci, and Mark Naden

Nortel

1. Introduction

This contribution is to specify the SZK generation function and associated algorithm

Within the SRZ which is identified by the SRZ GSA generated by the MR-BS. Following the existing 802.16e PKMv2 principle, MR-BS shall be responsible for the generation of the SRZ. There are two solutions

1.1 Centralized SZK Generation

MR-BS randomly generated the 128bits of SZK and distributed to each RS when the RS sends the PKM request message during the authentication process. This SZK has unique value that can only be bound to the SRZ. SZK has the characteristics of :

- MR-BS is the only trusted Key distribution Center (KDC) responsible for generating the RGK
- A member join/leave will trigger the updates/refresh of the RGK
- RGK should be re-keyed periodically
- A group member must not have knowledge of keys before it joins the group or after it leaves the group

1.2 EDH SZK Generation

Compared to the centralized SZK generation, EDH SZK has the attributes of dynamic membership updates and stronger security assurance. In solution 1, because the SZK is centrally generated and distributed to each RS via the air transmission, a single point of attack or eavesdropping will compromise the group's security. Also in order to achieve the mobility in the relay network, a node has to re-key the secrets during the hand-off process, the group where the RS leaves has to update its group key as well. However we can not rely on the RS that is honest enough to inform the MR-BS to update the group key. Therefore, solution with EDH SZK Generation algorithm dictate the following benefits

- Support of dynamic add/delete of members
- Less reliance on the security of the key distribution channel
- Support dynamic re-keying
- Reduce the need to re-key while the intra-roaming
- Diffie-Hellman algorithm provides the assurance of the security
- Against the passive attack
- Against the active attack

1.2.1 EDH SZK Algorithm

The notions for the EDH SZK algorithm are as:

- RS*i* : denotes the *i* RS
- *p : A large prime*
- *q : A prime with q|p-1*
- *g : A generator of G*
- *m: the size of the Secure Relay Group*
- *r : Random integer, chosen by RSi*
- *Ki : g mod p*

The process for generating a SZK is :

- Based on Diffie-hellman protocol
- Each RS sends a random number r_i to MR-BS who is the centralized KDC
- MR-BS generates its own random number R
- The SZK=$g^{(r_1 r_2 r_3 \cdots r_m) R}$
- MR-BS sends back $g^{(r_1 r_2 r_3 \cdots r_m R) r_i^{-1}}$ to RS*i*

Figure 1 illustrates the key generation process

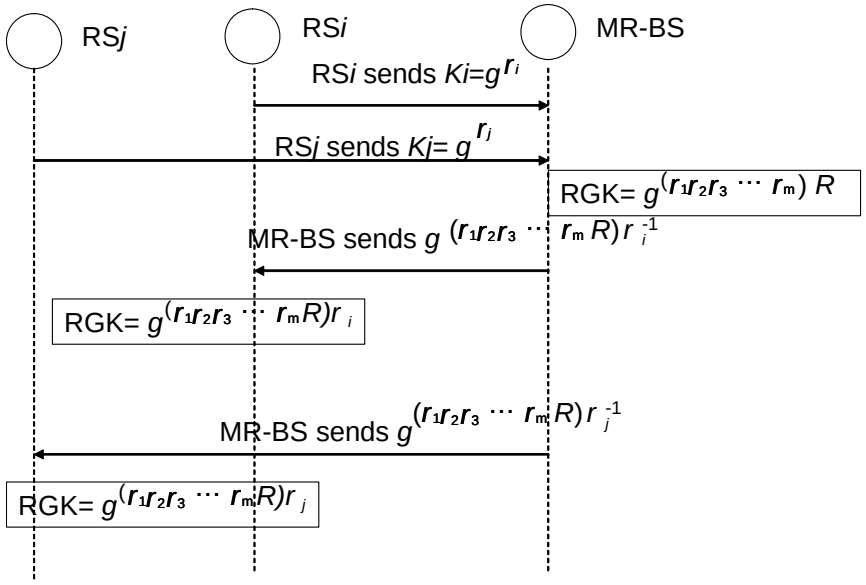

Figure 1

3. Proposed text change

++++++++++++++++++++++ Start Text ++++++++++++++++++++++++++++++++

[Add the following clause into section 7.4.4]

Within the SRZ which is identified by the SRZ GSA generated by the MR-BS. Following the existing 802.16e PKMv2 principle, MR-BS shall be responsible for the generation of the SRZ. There are two solutions

[Add the following clause into section 7.4.4.1]

Centralized SZK Generation

MR-BS randomly generated the 128bits of SZK and distributed to each RS when the RS sends the PKM request message during the authentication process. This SZK has unique value that can only be bound to the SRZ. SZK has the characteristics of :

- MR-BS is the only trusted Key distribution Center (KDC) responsible for generating the RGK
- A member join/leave will trigger the updates/refresh of the RGK
- RGK should be re-keyed periodically
- A group member must not have knowledge of keys before it joins the group or after it leaves the group

[Add the following clause into section 7.4.4.2]

EDH SZK Generation

Compared to the centralized SZK generation, EDH SZK has the attributes of dynamic membership updates and stronger security assurance. In solution 1, because the SZK is centrally generated and distributed to each RS via the air transmission, a single point of attack or eavesdropping will compromise the group's security. Also in order to achieve the mobility in the relay network, a node has to re-key the secrets during the hand-off process, the group where the RS leaves has to update its group key as well. However we can not rely on the RS that is honest enough to inform the MR-BS to update the group key. Therefore, solution with EDH SZK Generation algorithm dictate the following benefits

- Support of dynamic add/delete of members
- Less reliance on the security of the key distribution channel
- Support dynamic re-keying
- Reduce the need to re-key while the intra-roaming
- Diffie-Hellman algorithm provides the assurance of the security
- Against the passive attack
- Against the active attack

1.2.1 EDH SZK Algorithm

The notions for the EDH SZK algorithm are as:

- RS*i* : denotes the *i* RS
- *p : A large prime*
- *q : A prime with q|p-1*
- *g : A generator of G*
- *m: the size of the Secure Relay Group*
- *r : Random integer, chosen by RSi*
- *Ki : g mod p*

The process for generating a SZK is :

- Based on Diffie-hellman protocol
- Each RS sends a random number r_i to MR-BS who is the centralized KDC
- MR-BS generates its own random number R
- The SZK=$g^{(r_1 r_2 r_3 \quad r_m) R}$
- MR-BS sends back $g^{(r_1 r_2 r_3 \quad r_m R) r_i^{-1}}$ to RS*i*

++++++++++++ End text ++