Project	**IEEE 802.16 Broadband Wireless Access Working Group** <http://ieee802.org/16>	
Title	**SZK Definition and Management**	
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>.	

Security Zone Key Management

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 definition of SZK(Security Zone Key) concept and its operation in current .16j baseline document

1.1 SZK(Security Zone Key) Definition

SZK is the key in the SRZ (Secure Relay Zone) that are used to provide confidentiality (encryption), integrity and authenticity (MAC) within the relay group members.

There are a number of requirements while defining the SZK and its operation, such as:

- MR-BS is the only trusted Key distribution Center (KDC) responsible for generating the SZK
- A member join/leave the SRZ will trigger the updates/refresh of the SZK
- SZK 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

The SZK may be randomly generated by MR-BS or based on extended Diffie-Hellman algorithm to generate which will be discussed in section 7.4.4

1.2 SRZ(Secure Relay Zone) membership and trust model

The SRZ is consisting of a MR-BS who defines and identifies the SRZ , and a number of the RSs.

A RS member joins the group by authenticating itself to MR-BS. Implicitly, a RS who has completed the authentication with MR-BS will become the member of SRZ identified by MR-BS

- The RGK will be delivered to each member RS through AES-Key wrap protected by pair-wised KEK
- A RS should issue leave message to MR-BS to indicate it’s moving out of the SRZ

SZK Context

Parameter	Size (bits)	Usage
SZK	160	SZK is used to encrypt the MPDUs on UL/DL operations
SZK ID	64	RGKID=doc16KDF(RGK, RGK_SN|MR-BS MAC|BSID|"RGK", 64) The RGK_SN in the Dot16KDF function is an 8-bit number which consists of leading 4 zero bits and appending 4-bit AK_SN in MSB first order.
SZK SN	4	Sequence number of the RGK. Starts with 0 and incremented by 1
SZK Life time	-	This is the time this key is valid, when this expires, key refresh is initiated
GSA ID	16	GSA ID= Truncate(PathID1 XOR PathID 2 XOR PathIDm, 16)
GHMAC/GCMAC_KEY_U	160/128	The key which is used for signing UL management messages.
GHMAC/GCMAC_KEY_D	160/128	The key which is used for signing UL management messages

1.3 SZK Delivery

This method of encrypting the SZK shall be used for SAs with the RGK (TBD) encryption algorithm identifier in the cryptographic suite equal to 0x04.

The MR-BS encrypts the value fields of the SZK-128 in the Key Reply messages it sends to client SS. This field is encrypted using the AES Key Wrap Algorithm.

encryption: C,I = Ek[P]

decryption: P,I = Dk[C]

P = Plaintext 128-bit TEK

C = Ciphertext 128-bit TEK

I = Integrity Check Value

k = the 128-bit KEK (KEY Encryption Key between MR-BS and RS)

Ek[ ] = AES Key Wrap encryption with key k

Dk[ ] = AES Key Wrap decryption with key k

The AES key wrap encryption algorithm accepts both a ciphertext and an integrity check value. The decryption algorithm returns a plaintext key and the integrity check value. The default integrity check value in the

NIST AES Key Wrap algorithm shall be used.

1.4 SRZ (Secure Relay Zone) Group SA

SRZ GSA is the set of security information that a MR-BS and multiple of RS share authorization state in order to support secure and access controlled multicast management messages content reception across the IEEE

802.16 Relay network. Each MR-BS establish and provoke a SRZ Group SA during the RS initialization process.. A SRZ GSA's shared information shall include the Cryptographic Suite employed within the GSA and key material information such as SZKs.

The SRZ Group SAID, a 16-bit identifier for the GSA. The SAID shall be unique within a MR-BS and all RS clients.

Group SAID = Truncate(PathID1 XOR PathID2…XOR PathIDm, 16) ----- TBD

.

3. Proposed text change

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

[Updating description of 7.4.3]

SZK is the key in the SRZ (Secure Relay Zone) that are used to provide confidentiality (encryption), integrity and authenticity (MAC) within the relay group members.

There are a number of requirements while defining the SZK and its operation, such as:

- MR-BS is the only trusted Key distribution Center (KDC) responsible for generating the SZK
- A member join/leave will trigger the updates/refresh of the SZK
- SZK 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

[Updating description of 7.4.3.1]

This method of encrypting the SZK shall be used for SAs with the RGK (TBD) encryption algorithm identifier in the cryptographic suite equal to 0x04.

The MR-BS encrypts the value fields of the SZK-128 in the Key Reply messages it sends to client SS. This field is encrypted using the AES Key Wrap Algorithm.

encryption: C,I = Ek[P]

decryption: P,I = Dk[C]

P = Plaintext 128-bit TEK

C = Ciphertext 128-bit TEK

I = Integrity Check Value

k = the 128-bit KEK (KEY Encryption Key between MR-BS and RS)

Ek[ ] = AES Key Wrap encryption with key k

Dk[ ] = AES Key Wrap decryption with key k

The AES key wrap encryption algorithm accepts both a ciphertext and an integrity check value. The decryption algorithm returns a plaintext key and the integrity check value. The default integrity check value in the

NIST AES Key Wrap algorithm shall be used.

[Add the following section at end of 7.1.8]

SRZ(Secure Relay Zone) membership and trust model

The SRZ consisting of a MR-BS who defines and identifies the SRZ , and a number of the RSs that are requested to be part of the SRZ

- A RS member joins the group by authenticating itself to MR-BS. Implicitly, a RS who has completed the authentication with MR-BS will become the member of SRZ identified by MR-BS
- The RGK will be delivered to each member RS through AES-Key wrap protected by pair-wised KEK
- A RS should issue leave message to MR-BS to indicate it’s moving out of the SRZ

[Add the following section at end of 7.2.4]

SZK Context

Parameter	Size (bits)	Usage
SZK	160	SZK is used to encrypt the MPDUs on UL/DL operations
SZK ID	64	RGKID=doc16KDF(RGK, RGK_SN|MR-BS MAC|BSID|”RGK”, 64) The RGK_SN in the Dot16KDF

		function is an 8-bit number which consists of leading 4 zero bits and appending 4-bit AK_SN in MSB first order.
SZK SN	4	Sequence number of the RGK. Starts with 0 and incremented by 1
SZK Life time	-	This is the time this key is valid, when this expires, key refresh is initiated
GSA ID	16	GSA ID= Truncate(PathID1 XOR PathID 2 XOR PathIDm, 16)
GHMAC/GCMAC_KEY_U	160/128	The key which is used for signing UL management messages.
GHMAC/GCMAC_PN_UL	32	Used to avoid UL replay attack on the management connection—when this expires re-authentication is needed.
GHMAC/GCMAC_KEY_D	160/128	The key which is used for signing UL management messages
GHMAC/GCMAC_PN_DL	32	Used to avoid DL replay attack on the management connection—when this expires re-authentication is needed.

[Add the following section at end of 7.2.2.3.1]

SRZ (Secure Relay Zone) Group SA

SRZ GSA is the set of security information that a MR-BS and multiple of RS share authorization state in order to support secure and access controlled multicast management messages content reception across the IEEE

802.16 Relay network. Each MR-BS establish and provoke a SRZ Group SA during the RS initialization process.. A SRZ GSA's shared information shall include the Cryptographic Suite employed within the GSA and key material information such as SZKs.

The SRZ Group SAID, a 16-bit identifier for the GSA. The SAID shall be unique within a MR-BS and all RS clients.

Group SAID = Truncate(PathID1 XOR PathID2…XOR PathIDm, 16)

[Add the following parameters in the table in section 11.9 as following]

Table 370 PKM attributes types

Type	Attribute
48	SRZ Group SAID

[Add the following section at end of 11.9.38]

*Description:*16 bit SRZID should be randomly generated in a MR-BS and distributed to client RS

Type	Length	Value
48	16	Group SAID = Truncate(PathID1 XOR PathID2…XOR PathIDm, 16)

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