Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Secure Message Transfer Between BSs in the Backbone network**	
Date Submitted	**2004-11-12**	
Source(s)	Sangho Park, Pyung-Su Park, Inkyu Paek Hanarotelecom 470-9, Sindaebang-dong, Dongjak-gu, Seoul, Korea	Voice: +82-2-6266-5291 Fax: +82-2-6266-5309 mailto: [pasang,pspark,inkyu]@hanaro.com
	DaeHun Nyang InHa University Yonghyun-dong, Incheon, Korea	Voice: +82-32-860-8242 mailto: nyang@inha.ac.kr
Re:	IEEE 802.16 NetMan Task Group Call for Contribution	
Abstract	To expedite the handover procedure, backbone messages transfer security context and HO related information. To protect the security context and backbone messages, shared keys between BSs are required. In this contribution, method to share the keys dynamically is presented.	
Purpose	FYI	
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>.	

Secure Message Transfer between BSs in the Backbone network

Sangho Park, Pyung-Su Park, Inkyu Paek
Hanaro Telecom
DaeHun Nyang
Inha University

1. Vulnerabilities in MSS Security Context Transfer Message

HMAC Tuple of RNG_RSP in 6.3.2.3.6 expedites security authentication by notifying MSS through the HO Process Optimization TLV that the PKM_REQ/RSP sequence may be omitted for the current HO re_entry attempt. Thus, BS must obtain security context before sending RNG_RSP to compute the HMAC Tuple.

After a HO_REQ/RSP exchange, an MSS may seek to use pre_authentication to effect a fast handover. An MSS seeking to use pre_authentication shall transmit a PKM_PREAUTH_REQ with OMAC Tuple. Thus, target BSs must obtain security context before receiving PKM Pre_Authentication Request message to validate the OMAC Tuple.

To this end, MSS Security Context Transfer Request/Response messages are defined in ANNEX D.2.15. Unfortunately, only authentication for messages in backbone network is provided, but confidentiality is not serviced for messages in ANNEX D.2. Thus, an attacker can obtain AK and TEK in non_negligible probability by monitoring BSs interested to capture an MSS Security Context Transfer Response message for a enough time period. Thus, it is required to provide confidentiality service for MSS Security Context Transfer Response message. To provide the confidentiality service for an MSS Security Context Transfer Response message and authentication service of the security field for all inter_BS messages, it is necessary to share a key between communicating BSs. The key may be provisioned in each BS, but it is more desirable to dynamically generate a key in every session in view of security and convenience.

2. Solution

If Backbone network communication protocol accommodates some underlying security protocol such as IPSec, the key distribution problem between BSs is resolved and also we do not need any more the security field of backbone messages. Also, timestamp field is not required for prevention of replay attack because IPSec already prevents replay attack effectively. Similarly, Task Group F of IEEE 802.11 has recommended IPSec to protect messages of Inter-Access-Point Protocol (IAPP).

3. Proposed text changes

We propose to change the annex named by "Annex D. Backbone network HO procedures" in IEEE 802.16e-D4.

[Remove the timestamp field in Table D4 at section D.2.1, page 211:]

Table D4_Global Message Header

Field	Size	Notes
Message Type = ?	8-bit	
Sender BS-ID	48-bit	Base station unique identifier (Same number as that broad-casted on the DL-MAP message)
Target BS-ID	48-bit	Base station unique identifier (Same number as that broad-casted on the DL-MAP message)
~~Time Stamp~~	~~32-bit~~	~~Number of milliseconds since midnight GMT (set to 0xffffffff to ignore)~~
Num Records	16-bit	Number of MSS identity records

[Change Table D5 at section D.2.2, page 211:]

Table D5_I-am-host-of Message

Field	Size	Notes
Global Header	~~152-bit~~ 120 bit	
For (j=0; j<Num Records; j++) {		
MSS unique identifier	48-bit	48-bit unique identifier used by MSS on initial network entry
Reason	8-bit	#0: Network Attached #1: Successful Handover #2: Handover Failure #3:-7: *reserved*
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~

[Change Table D6 at section D.2.3, page 212:]

Table D6_MSS-info-request Message

Field	Size	Notes
Global Header	~~152-bit~~ 120 bit	
For (j=0; j<Num Records; j++) {		

MSS unique identifier	48-bit	48-bit unique identifier used by MSS (as provided by the MSS or by the *I-am-host-of* message)
Action flag	8-bit	0 – Request information 1 – MSS arrived from Idle mode 2 – MSS has transitioned to another paging group 3 – MSS request handover 4-7 – *reserved*
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~

[Change Table D7 at section D.2.4, page 212:]

Table D7_MSS-info-response Message

Field	Size	Notes
Global Header	~~152-bit~~ 120 bit	
For (j=0; j<Num Records; j++) {		
MSS unique identifier	48-bit	48-bit unique identifier used by MSS (as provided by the MSS or by the *I-am-host-of* message)
N_NSIE		Number of Network Service Information Elements
For (k=0; k<N_NSIE; k++) {		
Field Size	16-bit	Size, in bytes, of TLV encoded information field below
TLV encoded information	Variable	TLV information as allowed on a DSA-REQ MAC message
}		
N_SAIE		Number of Security Association Information Elements
For (k=0; k<N_SAIE; k++) {		
Field Size	16-bit	Size, in bytes, of TLV encoded information field below
TLV encoded information	Variable	TLV information as allowed on a PKM-xxx MAC messages
}		
N_MSS_CAP		Number of MSS Capabilities
For (k=0; k<N_MSS_CAP; k++) {		
Field Size	16-bit	Size, in bytes, of TLV encoded information field below
TLV encoded information	Variable	TLV information as allowed on a SBC-REQ MAC message
}		
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~

[Change Table D8 at section D.2.5, page 213:]

Table D8_HO-pre-notification Message

Field	Size	Notes
Global Header	~~152-bit~~ 120 bit	
For (j=0; j<Num Records; j++) {		
MSS unique identifier	48-bit	48-bit unique identifier used by MSS (as provided by the MSS or by the *I-am-host-of* message)
Estimated Time to HO	16-bit	In milliseconds, relative to the time stamp. A value of 0 indicates that the estimated time is unknown.
Required BW	8-bit	Bandwidth which is required by MSS (to guarantee minimum packet data transmission)
For (i=0; i<Num_SFID_Records; i++)		
SFID	32 bits	
For (i=0; i<Num_QoS_Records; i++) {		
Required QoS	Variable	11.13 QoS Parameter definition encodings that in combination define an AdmittedQoSParamSet specific to the SFID
}		
}		
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~

[Change Table D9 at section D.2.6, page 214:]

Table D9_HO-pre-notification-response Message

Field	Size	Notes
Global Header	~~152-bit~~ 120 bit	
For (j=0; j<Num Records; j++) {		
MSS unique identifier	48-bit	48-bit unique identifier used by MSS (as provided by the MSS or by the *I-am-host-of* message)
BW Estimated	8-bit	Bandwidth which is provided by BS (to guarantee minimum packet data transmission) TBD how to set this field

QoS Estimated	8-bit	Quality of Service level — Unsolicited Grant Service (UGS) — Real-time Polling Service (rtPS) — Non-real-time Polling Service (nrtPS) — Best Effort
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~

[Change Table D10 at section D.2.7, page 214:]

Table D10_HO-confirm Message

Field	Size	Notes
Global Header	~~152-bit~~ 120 bit	
For (j=0; j<Num Records; j++) {		
MSS unique identifier	48-bit	48-bit universal MAC address of the MSS (as provided to the BS on the RNG-REQ message)
BW Estimated	8-bit	Bandwidth which is provided by BS (to guarantee minimum packet data transmission) TBD how to set this field
QoS Estimated	8-bit	Quality of Service level — Unsolicited Grant Service (UGS) — Real-time Polling Service (rtPS) — Non-real-time Polling Service (nrtPS) — Best Effort Service (BE)
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~

[Change the table at the end of section D.2.8, page 215:]

Field	Size	Notes
Message Type = ?	**8-bit**	
Sender BS-ID	48-bit	Base station unique identifier (Same number as that broadcasted on the DL-MAP message)
Target BS-ID	48-bit	Base station unique identifier (Same number as that broadcasted on the DL-MAP message)
Time Stamp	32-bit	Number of milliseconds since midnight GMT (set to 0xffffffff to ignore)
Action	4-bit	0 – Assign target BS to paging groups 1 – Remove target BS from paging groups 2 – Query (which paging groups target BS belongs to?) 3 – Information (paging groups sender BS belongs to)
Num Records	4-bit	Number of paging-group-ID records
For (j=0; j<Num Records; j++) {		
Paging-group-ID	16-bit	Paging-group-ID
PAGING_CYCLE	16-bit	Cycle in which the paging message is transmitted within the paging group
PAGING OFFSET	8-bit	MSS PAGING OFFSET parameter
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~
CRC field	32-bit	IEEE CRC-32

[Change the table at the end of section D.2.9, page 216:]

Field	Size	Notes
Message Type = ?	8-bit	
Sender BS-ID	48-bit	Base station unique identifier (Same number as that broadcasted on the DL-MAP message)
Recipient BS-ID	48-bit	Set to 0xffffff to indicate broadcast
Time Stamp	32-bit	Number of milliseconds since midnight GMT (set to 0xffffffff to ignore)
Num MSS	8-bit	Number of MSSs to page
For (j=0; j<Num MSS; j++) {		
MSS MAC address	48-bit	
Paging Group ID	8-bit	The identifier of the paging group to which the MSS belongs.
PAGING CYCLE	16-bit	MSS PAGING CYCLE parameter
PAGING OFFSET	8-bit	MSS PAGING OFFSET parameter
Action code	3-bit	0=MSS enters Idle Mode 1=MSS exits Idle Mode 2=MSS should be paged to perform ranging to establish location and acknowledgement message 3=MSS should be paged to enter network 4-7= *Reserved*
Reserved	5-bit	
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~
CRC field	32-bit	IEEE CRC-32

[Change the table at the end of section D.2.10, page 217:]

Field	Size	Notes
MSS_PINGPONG_Notification_Message_Format() {		
Global Header	152 bits	
MSS unique identifier	48 bits	48-bit unique identifier of the MSS
Estimated PP time	8 bits	Same value in MSS_PINGPONG_Report message
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~
CRC field	32 bits	IEEE CRC-32
}		

[Change the table at the end of section D.2.11, page 217:]

Field	Size	Notes
Global Header	~~152-bit~~ 120 bit	
for (i=0; i<NUM_Records; i++) {		
MSS unique identifier	48 bits	48-bit universal MAC address of the MSS (as provided to the BS on the RNG-REQ message)
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~

[Change the table at the end of section D.2.12, page 217:]

Field	Size	Notes
Message Type = ?	8-bit	
Server BS-ID	48 bits	BS unique identifier (same number as that broadcast on the DL-MAP message)
Target BS-ID	48 bits	Set to 0xFFFFFF to indicate broadcast
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~

[Change the table at the end of section D.2.13, page 218:]

Field	Size	Notes
Message Type = ?	8 bits	
Sender BS-ID	48 bits	BS unique identifier (same number as that broadcast on the DL-MAP message)
Target BS-ID	48 bits	Set to 0xFFFFFF to indicate broadcast
Time Stamp	32 bits	Number of milliseconds since midnight GMT (set to 0xFFFFFF to ignore)
Configuration Change Count	8 bits	Incremented each time the information for the BS has changed.
TLV Encoded information	Variable	TLV information as allowed on DCD, UCD messages.
~~Security field~~	~~TBD~~	~~A means to authenticate this message.~~

[Change the table at the end of section D.2.14, page 218:]

Field	Size	Notes
Global Header	152 bits	
Message Type = ?	8 bits	
for (j=0; j<NumRecords; j++) {		
MSS Unique identifier	48 bits	48-bit unique identifier of the MSS
}		
~~Security field~~		~~A means to authenticate this message.~~

[Change the table at the end of section D.2.15, page 219:]

Field	Size	Notes
Global Header	~~152-bit~~ 120 bit	
Message Type = ?	8 bits	
for (j=0; j<NumRecords; j++) {		
MSS Unique identifier	48 bits	48-bit unique identifier of the MSS
"Older" AK	160 bits	
"Older" AK Remaining Key Lifetime	32 bits	
"Older" AK Key Sequence Number	8 bits	
"Newer" AK	160 bits	
"Newer" AK Remaining Key Lifetime	32 bits	
"Newer" AK Key Sequence Number	8 bits	
N_SAIE	8 bits	Number of Security Association Information Elements
for (k=0; i<N_SAIE; k++) {		
SA Descriptor	Variable	These properties include the SAID, the SA type, and the cryptographic suite employed within the SA.
"Older" TEK		
"Older" TEK Remaining Key Lifetime	32 bits	
"Older" TEK Key Sequence Number	8 bits	
"Older" TEK CBC Init Vector	Equal to block length of cipher	
}		
}		
~~Security field~~	~~TBD~~	~~A means to authenticate this message~~

[Change Table D11 at section D.2.17, page 223:]

Table D11_MSS-Data-Forwarding Message

Syntax	Size	Notes
Global Header	~~152-bit~~ 120 bit	
Length	16 bits	The length in bytes of the MAC SDU including the Global Header, MSS unique identifier, and Security field.
MSS unique identifier	48 bits	48-bit unique identifier used by MSS on initial network entry
MAC SDU	*variable*	
~~Security Field~~	~~TBD~~	~~A means to authenticate this message.~~

[Change Table D12 at section D.2.18, page 223:]

Table D12_Stop-Data-Forwarding Message

Syntax	Size	Notes
Global Header	~~152-bit~~ 120 bit	
MSS unique identifier	48 bits	48-bit unique identifier used by MSS on initial network entry.
Action	TBD	TBD
~~Security field~~	~~TBD~~	~~A means to authenticate this message.~~

[Add the following at section D.3, page 223:]

D.3 Backbone network communication protocol

Backbone network communication protocol is run on top of the IPSec. All the backbone messages are transferred in the secure channel between BSs using IPSec that provides message authentication and confidentiality services. Transport mode rather than tunnel mode of IPSec should be used. Only for the message authentication, AH(Authentication Header) should be used, and MSS Security Context Transfer Request and MSS Security Context Transfer Reply must be transferred in ESP(Encapsulating Security Payload) of IPSec.