Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**	
Title	**Location Management for supporting IDLE mode in IEEE P802.16e**	
Date Submitted	**2004-07-15**	
Source(s)	Jungje Son, and Yong Chang, Samsung Electronics	jungje.son@samsung.com, youngchang@samsung.com
	Chulsik Yoon, ETRI	csyoon@etri.re.kr
	Mo-Han Fong, Nortel	mhfong@nortelnetworks.com
	BJ Kim	beom@lge.com
Re:	IEEE P802.16e/D3-2004	
Abstract	This contribution describes Location Management for supporting IDLE mode in IEEE P802.16e/D2-2004.	
Purpose	Review and Adopt the suggested changes into P802.16e/D3	
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>.	

History

Revision	Changes
Rev 0.	C80216e-04/198
Rev 1.	C80216e-04/198r1 Following Reply Comments are reflected more clearly. ・ The explanation of location update on timer expiry is added ・ Paging Controller as an logical network entity instead of ASA server or BS ・ Paging Cycle Request in RNG-REQ and Paging Information in RNG-RSP are deleted. ・ MAC Key is deleted. ・ Typo is corrected.

Location Management for supporting IDLE mode in IEEE P802.16e

Jungje Son and Yong Chang, SAMSUNG Electronics, Ltd

ChulSik Yoon, ETRI

Mo-Han Fong, Nortel

BJ KIM, LGE

1. INTRODUCTION

A MSS in Idle mode shall update its location to the network when the MSS enters a new paging-group or the MSS is requested to update its location by the BS through MOB_PAG_ADV message. The paging groups of Idle Mode are designed to trade-off between paging overhead and location update signaling overhead. If the paging group size is small, the paging overhead will be small. However, there will be frequent location update which increases the associated signaling overhead. On the other hand, if the paging group size is large, the paging overhead will be large. However, the signaling overhead associated with location update will be reduced.
In the current standard, the location update procedure is similar to that of an initial ranging. In fact, the purpose of location update is to inform the network of a MSS' location, instead of a network entry. Therefore the current location update procedure can be simplified to eliminate unnecessary overhead and delay.

In this contribution, we propose the light and secure location update procedures in IDLE mode. While a MSS in IDLE mode crosses the boundary of a paging group or its timer is expires, the MSS shall perform location update operation instead of doing network re-entry. This location update procedure should be designed in order to protect the fake location update from the malicious user.

2. SUMMARY OF PROPOSAL

2.1 Security Information for authentication in idle mode

At the 16e #31 meeting, we made a consensus on that the security information for authentication in idle mode is required to protect reply attack. The mechanism to make a security key in idle mode is being discussed in the Security Ad Hoc.

In our proposal, we assume that an MAC Key(Message Authentication Code Key) in idle mode, what we called, is maintained between ASA(or BS) and MSS. Based on this assumption, when the MSS sends the DREG-REQ message to the Serving BS with the HMAC Tuple, and then the Serving BS replies the DREG-CMD with ASA server ID or BS-ID with the function to control the paging and location management for IDLE mode.

2.2 Location update procedure in IDLE mode

The MSS in IDLE mode shall perform location update operation if the update condition is met. We propose two location update conditions as following:

- Zone-based update

  The MSS performs location update when the paging group is changed. The MSS can detect the change of paging

group by monitoring the paging group identifier, PG_ID, which is transmitted on the **MOB_PAG-ADV** message.

- Timer-based update

  The MSS periodically performs location update whenever a predefined timer expires. This scheme enables the ASA server or BS to ascertain a MSS in IDLE mode to keep alive.

If the MSS in IDLE mode needs to update its location, the MSS sends to a RNG-REQ message with some TLV information like HMAC Tuple, ASA server ID, Location Update Indication, etc. After receiving RNG-REQ for location update purpose, the BS performs the location update backbone procedure with ASA server or previous BS controlling the MSS. The ASA server or previous control BS will update the MSS's location information provided that the HMAC Tuple is correctly verified.

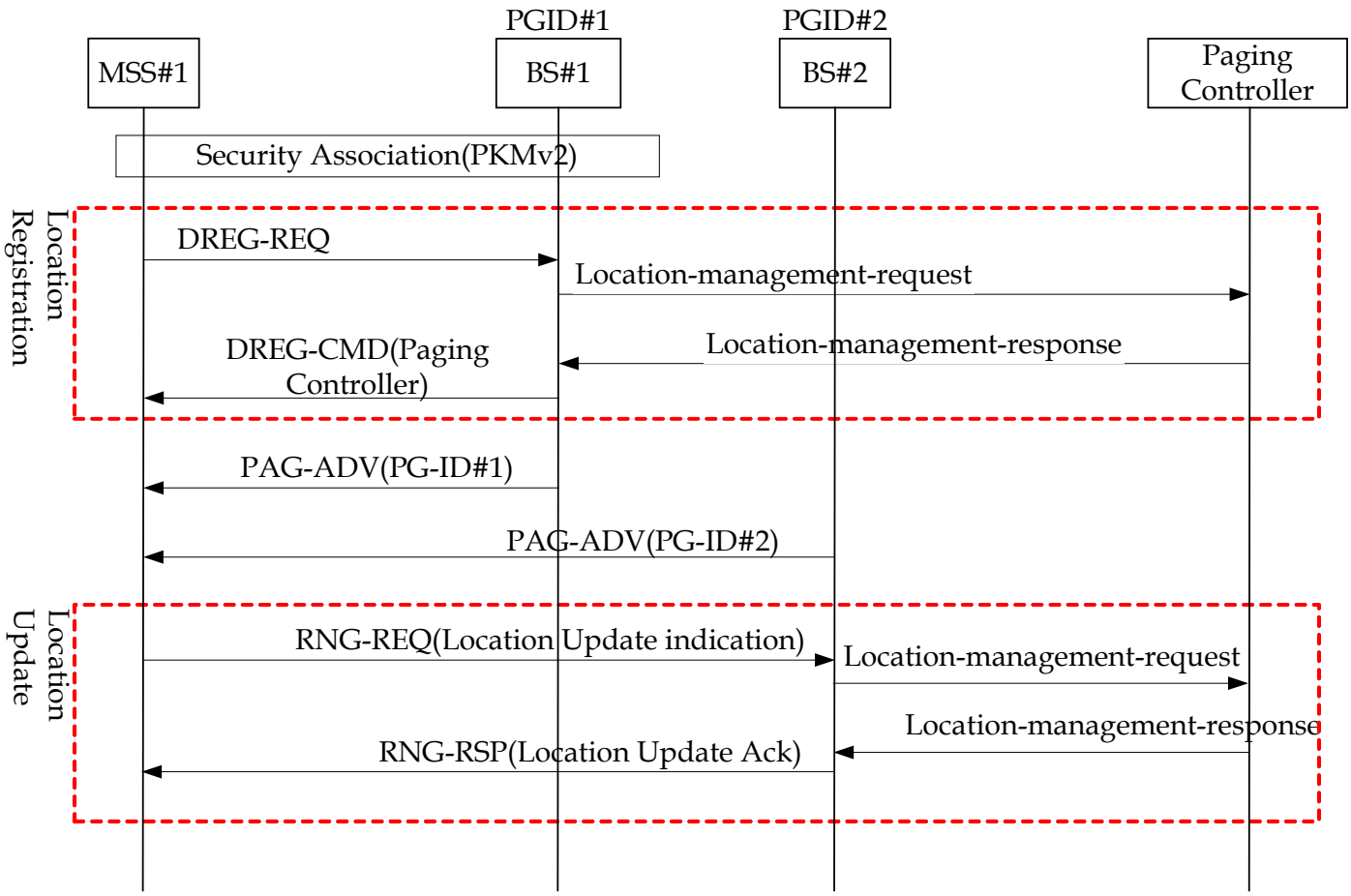

Figure xx. Location management for IDLE mode

3. Proposed Text Changes to 16e/D3

[Insert the following text after REQ-duration section : in 6.3.2.3.26 De/Re-register Command (DREG-CMD) message]

PAGING Controller (e.g., ASA Server ID or BS ID)

This is an logical network identity identifier which takes charge of the location of the MSS in IDLE mode. The network element may be the current serving BS, or ASA server, or new network element. This is 48 bits.

[Add the following text after Serving BS ID in 6.3.2.3.5 RNG_REQ]:

6.3.2.3.5 Ranging Request (RNG_REQ) message

[…]

The following parameters as TLV shall be included in the RNG-REQ message when the MSS in idle mode is attempting to perform the location update:

Location Update Indication

Location Update indication 2 bits are set as followings:

0x00 = Location update by detection of new Paging Group ID

0x01 = Location update by Timer expiry

0x10, 0x11 = reserved

The timer is the MSS's timer corresponding to the AGING_TIMER at the Serving BS. If the MSS wants to keep alive based on the timer, it sends the RNG-REQ for keeping alive with the location update indication when its timer is expired.

PAGING Controller (e.g., ASA Server ID or BS ID)

This is an logical network identity identifier which takes charge of the location of the MSS in IDLE mode. The network element may be the current serving BS, or ASA server, or new network element. This is 48 bits.

Paging Cycle Request

PAGING_CYCLE requested by MSS. This is 16 bits.

HMAC Tuple

The HMAC-Tuple attribute, This is 176 bits.

[Add new table 318a in Section 11.5 RNG-REQ Meesage Encodings]:

Table 318a—RNG-REQ Message Encodings

Name	Type	Length	Value
Serving BS ID	4	6	The unique identifier of the former Serving BS
Request Type	5	1	#Bit0: Reserved for HO indication #Bit1 : Reserved for another purpose of RNG-REQ #Bit2~3 Location Updates #Bit4~Bit7: Reserved
Location Update Indication of Request Type	6	1	0x00 = Location update by detection of new Paging Group ID 0x01 = Location update by Timer expiry 0x10, 0x11 = reserved
PAGING Controller (e.g., ASA Server ID or BS ID)	7	6	This is an logical network identity identifier which takes charge of the location of the MSS in IDLE mode. The network element may be

			the current serving BS, or ASA server, or new network element.
HMAC Tuple	8	22	

[Add the following text after Servce Level Prediction in 6.3.2.3.6 RNG_RSP]:

6.3.2.3.6 Ranging Response (RNG-RSP) message

[…]

The following parameters as TLV shall be included in the RNG-RSP message when the BS is attempting to response the location update from the MSS

Action Code

Action code identifying the type of location update request:

0x00= Success of Location Update

0x01= Failure of Location Update. The MSS should perform network re-entry.

0x10, 0x11: Reserved

When the Action Code = 00, the following TLV shall be included:

HMAC- Tuple

The HMAC-Tuple shall be the last attribute in the message

[Add new section 6.3.21.9 with the following sentences after section 6.3.21.8.2]

6.3.21.9.Location Update

The MSS in IDLE mode shall perform location update operation if the location update condition is met. The location update procedures are the followings:

- Zone-based update

  The MSS performs location update when the paging group is changed. The MSS can detect the change of paging group by monitoring the paging group identifier, PG_ID which is transmitted on the **MOB_PAG-ADV** message.

- Timer-based update

  The MSS periodically performs location update whenever a predefined timer expires. This scheme enables the ASA server or BS to ascertain a MSS in IDLE mode to keep alive. If the ASA server or BS ascertains a MSS in IDLE mode to be died, the ASA server or BS may delete all information for the MSS.

If the MSS in IDLE mode needs to update its location, the MSS sends to a RNG-REQ message with some TLV information like HMAC Tuple, ASA server ID, Location Update Indication, etc. After receiving RNG-REQ for location update purpose, the BS performs the location update backbone procedure with ASA server or previous BS controlling the MSS. The ASA server or previous control BS will update the MSS's location information provided that the HMAC Tuple is correctly verified.

This Location Update procedure is initiated by sending the RNG-REQ with location update indication from the MSS. At this time, MSS may send another code(e.g., handover ranging code), different from the current ranging code.

[Add new table 320a in Section 11.6 RNG-REQ Meesage Encodings]:

Table 320a—RNG-RSP Message Encodings

Name	Type	Length	Value
Action Code	21	1	0x00= Success of Location Update 0x01= Failure of Location Update. The MSS should perform network re-entry. 0x10, 0x11: Reserved
HMAC Tuple	8	22	

[Add new sections D.2.11 and D.2.12. The sections will include the following text]:

D.2.11Location-management-request message

This message may be sent from one BS to another (or to the ASA server) to request registration or update of MSS location information. The message contains the following information,

Table Cxxx— Location-management-request Message Format

Field	**Size**	**Notes**
IDLE-location-management-request_Message_Format() {		
Global Header	152 bits	Message Type=??
For (i=0; i<Num_Records; i++) {		
MSS ID	48 bits	
Action Code	8 bits	0x00 : Location Registration 0x01 : Location Update 0x02-FF: reserved
TLV-Paging Cycle Request	16 bits	
TLV_Previous PG-ID	24 bits	
TLV_HMAC- Tuple	176 bits	~~Only valid if Action code = 0x01.~~ This value is equal to the HMAC-Tuple in MOB_LU-REQ message.
}		
Security field	TBD	BS-BS Security Information
}		

D.2.12 Location-management-response message

This message may be sent from one BS to another BS (or to the ASA server), typically in response to a Location-management-request message. This message serves to provide the BS that sent the Location-mamagement-request message with information about the result of location registration or update. The message contains the following information,

Table Cxxx— Location-management-response Message Format

Field	Size	Notes
IDLE-location-management-response_Message_Format() {		
Global Header	152 bits	Message Type=??
For (i=0; i<Num_Records; i++) {		
MSS ID	48 bits	
Action Code	8 bits	0x00 : Location Registration 0x01 : Successful Location Update 0x02 : Failed Location Update 0x03-FF: reserved
TLV-Paging Information	16 bits	
TLV_HMAC-Tuple	176 bits	The HMAC- Tuple is calculated with IDLE authentication key
}		
Security field	TBD	BS-BS Security Information
}		