Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	**Preventing replay attack using Paging Group Update information in RNG-REQ in idle mode**
Date Submitted	**2005-01-24**
Source(s)	Yongmao Lee, Zhengfei Xiao Huawei Pudong Eshan Road #98,Lane 91,Shanghai,China. Voice: +86-21-68644808 Fax: +86-21-50898375 xiaozhengfei@huawei.com
Re:	Contribution on comments to IEEE P802.16e/D5a
Abstract	Preventing replay attack using Paging Group Update information in RNG-REQ in idle mode
Purpose	Discussion, Decision and Adoption
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>.

Preventing replay attack using Paging Group Update Information in idle mode

Yongmao Lee, Zhengfei Xiao
Huawei

1. Introduction

In the current IEEE 802.16e/D5a, the Paging Controller reserves the relative information of the MSS in idle mode. The MSS in idle mode shall perform Paging Group Update periodically in order to demonstrate MSS continued network presence and re-validate Paging Controller retention of the MSS's service and operational information. In the current draft, MSS initiates Paging Group Update request through a RNG-REQ and been responded by a RNG-RSP. There is a TLV code in RNG-REQ and RNG-RSP, which indicates the information used in Paging Group Update.

MSS doesn't perform network re-entry and authentication during roam under idle mode, so the information reserved in the Paging Controller is related with MSS and the BS where MSS enters into idle mode. When MSS roams to a new paging group, the first Paging Group Update request initiated by MSS might be delivered to the previous Paging Controller. After validating the HMAC of the message, the previous Paging Controller may deliver the reserved MSS information through backbone network. At the same time, Paging Controller may report the paging group information of MSS to a central server.

According to the current protocol, an attacker could intercept the Paging Group Update information in RNG-REQ when MSS enters into the scope of BS_m and save it. The Paging Controller identifier information in this message is n and BS_m does not belong to this Paging Group. When MSS roam to the paging group n again, if the attacker replay the reserved message to the BS_m, it will make the gloss that MSS has roam to the paging group that BS_m belongs to. So the network could not page the MSS.

2. Proposed Solution

In order to avoid the replay attack above, we need to modify Paging Group Update information in RNG-REQ. A direct method is to add time-stamp or sequence number in RNG-REQ to prevent replay attack. The additive information ensures that Paging Group Update information in RNG-REQ will not be repeated in a long time. Even if a attacker intercept a Paging Group Update information in RNG-REQ, Paging Controller can distinguish whether the received RNG-REQ include a new Paging Group Update information or a replaying one by comparing the time-stamp or sequence number.

3. Proposed Text Changes

Insert the following text in

6.3.2.3.5 page 40, line 29

The following TLV parameter may be included in RNG_REQ message when a MSS is performing Paging Group Update to the selected target BS:

Sequence_Number

Insert the following text in

6.3.2.3.5 page 42, line 19

The following TLV parameter may be included in RNG_RSP message when a MSS is performing Paging Group Update to the selected target BS:

Sequence_Number

[Add the following rows to table 362:]

Name	Type (1 byte)	Length	Value
Sequence_Number		4	The sequence number increase after MSS sending a Paging Group Update information in RNG-REQ in idle mode.

[Add the following rows to table 365:]

Name	Type (1 byte)	Length	Value
Sequence_Number		4	The sequence number corresponding to the RNG-REQ message.

4. Reference:

[1] Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks C80216e-04_406
[2] IEEE 802.16-REVd_D5
[3] IEEE 802.16e_D5