| | |
|---|---|
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>** |
| Title | The enhancement of PKM identifier in PKM message for replay attack |
| Date Submitted | **2005-01-07** |
| Source(s) | [Rui Li] [Feng Tian] [Dongxin Lu] [zte] [ZTE Plaza , Keji Road South , Hi-tech Industrial Park , Nanshan District , Shenzhen , P.R.China , 518057] Voice: [86-0755-26772016] Fax: [86-0755-26772004] [mailto:li.rui2@zte.com.cn] |
| Re: | 802.16e/D5 |
| Abstract | This document contains new Group TEK management for Multicast and Broadcast Service |
| Purpose | Adopt |
| 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>. |

# The enhancement of PKM identifier in PKM message for replay attack

*Rui Li*
*Feng tian*
*Dongxin lu*

## 1. Problem Statements

There is not description about how to prevent replay attack of SS's Key request and Authorization request messages in BS in IEEE 802.16e/D5a. An SS uses the PKM identifier in PKM message to match a BS response to the SS's requests. We may expand the function of the PKM identifier and use it to prevent replay attack in the BS. The capability of PKM identifier for preventing replay attack is weak because the size of PKM identifier in PKM message is 8 bits and many PKM messages make use of it together. So it is necessary to extend the size of PKM identifier for replay attack and supply some contents about how to prevent replay attack in the BS in this specification.

[add the following as show]

## 2. Proposed Text adds

### 6.3.2.3.9 Privacy key management (PKM) messages (PKM-REQ/PKM-RSP)

PKM employs two MAC message types: PKM Request (PKM-REQ) and PKM Response (PKM-RSP), as described in Table Table 23—.

**Table 23—PKM MAC messages**

| Type Value | Message name | Message description |
|---|---|---|
| 9 | PKM-REQ | Privacy Key Management Request [SS -> BS] |
| 10 | PKM-RSP | Privacy Key Management Response [BS -> SS] |

These MAC management message types distinguish between PKM requests (SS–to–BS) and PKM responses (BS–to–SS). Each message encapsulates one PKM message in the Management Message Payload.

PKM protocol messages transmitted from the SS to the BS shall use the form shown in Table Table 24—. They are transmitted on the SSs Primary Management Connection.

**Table 24—PKM request (PKM-REQ) message format**

| Syntax | Size | Notes |
|---|---|---|
| PKM-REQ_Message_Format() { | | |
| **Management Message Type = 9** | 8 bits | |
| **Code** | 8 bits | |
| **PKM Identifier** | ~~8 bits~~ 16bits | |
| **TLV Encoded Attributes** | *variable* | TLV specific |
| } | | |

***[Insert the following text directly below Table 24 - PKM request (PKM-REQ) message format table as shown]***

PKM protocol messages transmitted from the BS to the SS shall use the form shown in Table 25. They are transmitted on the SSs Primary Management Connection. When the BS sends PKM-RSP message in key push mode for the multicast service or the broadcast service, it may be carried on the Broadcast connection.

**Table 25—PKM response (PKM-RSP) message format**

| Syntax | Size | Notes |
|---|---|---|
| PKM-RSP_Message_Format() { | | |
| **Management Message Type = 10** | 8 bits | |
| **Code** | 8 bits | |
| **PKM Identifier** | ~~8 bits~~ 16 bits | |
| **TLV Encoded Attributes** | *variable* | TLV specific |
| } | | |

***[Change the text between Table 25 and Table 26 as indicated:]***

The parameters shall be set as follows:

**Code**

The Code is one byte and identifies the type of PKM packet. When a packet is received with an invalid Code, it shall be silently discarded. The code values are defined in Table 26.

**PKM Identifier**

The Identifier field is one byte. An SS uses the identifier to match a BS response to the SS's requests.

The SS shall increment (modulo 256) the Identifier field whenever it issues a new PKM message. A "new" message is an Authorization Request or Key Request that is not a retransmission being sent in response to a Timeout event. For retransmissions, the Identifier field shall remain unchanged. The BS can use the PKM identifier to prevent replay attack.

The Identifier field in Authentication Information messages, which are informative and do not effect any response messaging, shall be set to zero. The Identifier field in a BS's PKM-RSP message shall match the Identifier field of the PKMREQ message the BS is responding to. The Identifier field in TEK Invalid messages, which are not sent in response to PKMREQs, shall be set to zero. The Identifier field in unsolicited Authorization Invalid messages shall be set to zero. The Identifier field in Key Update Command messages, which are used to distribute the updated GTEK and traffic keying material, shall be set to zero.

On reception of a PKM-RSP message, the SS associates the message with a particular state machine (the Authorization state machine in the case of Authorization Replies, Authorization Rejects, and Authorization Invalids; a particular TEK state machine in the case of Key Replies, Key Rejects, ~~and TEK Invalids~~ TEK Invalids, Key Update Commands).

An SS shall keep track of the identifier of its latest, pending Authorization Request. The SS shall discard Authorization Reply and Authorization Reject messages with Identifier fields not matching that of the pending

Authorization Request.

An SS shall keep track of the identifiers of its latest, pending Key Request for each SA. The SS shall discard Key Reply and Key Reject messages with Identifier fields not matching those of the pending Key Request messages.

A BS shall keep track of the identifier of its latest, pending Authorization Request from an SS. The BS shall discard the new receiving Authorization Request message with identifier field which is less than or equal to that of the pending Authorization Request.

A BS shall keep track of the identifier of its latest, pending Key Request for each SA from an SS. The BS shall discard the new receiving Key Request message with identifier field which is less than or equal to that of the pending Key Request.

**Attributes**

PKM attributes carry the specific authentication, authorization, and key management data exchanged between client and server. Each PKM packet type has its own set of required and optional attributes. Unless explicitly stated, there are no requirements on the ordering of attributes within a PKM message. The end of the list of attributes is indicated by the LEN field of the MAC PDU header.