|  |  |
| --- | --- |
| Project | **IEEE 802.16 Broadband Wireless Access Working Group <**<http://ieee802.org/16>**>** |
| Title | **Efficient and Secure Change of Multicast Group Service Flow on IEEE 802.16.1a**  |
| Date Submitted | **2012-07-09** |
| Source(s) | Chulsik Yoon, Sungcheol Chang, Miyoung Yun, Hyun Lee, Won-Ik Kim, Eunkyung Kim, Seokki Kim, Sungkyung KimETRI | E-mail: csyoon@etri.re.krscchang@etri.re.kr |
| Re: | Letter Ballot #38b on P802.16.1a/D3 |
| Abstract | This provides AWD text proposals for fast management of multicast group service flow in IEEE p802.16.1a. |
| Purpose | To discuss and adopt the proposed text in the draft amendment document on GRIDMAN |
| 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. |
| Copyright Policy | The contributor is familiar with the IEEE-SA Copyright Policy <http://standards.ieee.org/IPR/copyrightpolicy.html>. |
| 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>>. |

**Efficient and Secure Change of Multicast Group Service Flow on IEEE 802.16.1a**

Chulsik Yoon, Sungcheol Chang, Miyoung Yun, Hyun Lee, Won-Ik Kim, Eunkyung Kim, Seokki Kim, Sungkyung Kim

ETRI

# Background

Currently, AAI-DSC-REQ/AAI-DSC-RSP messages are used to change the service flows to an HR-MS with unicast fashion. It is because the service flow update information shall be securely transported and authenticated. If the AAI-DSC-REQ/AAI-DSC-RSP messages are transmitted, then the message shall be encrypted by TEK for the basic unicast connection and message authenticated by using CMAC\_KEY\_D/CMAC\_KEY\_U, respectively. Since the AAI-DSC-REQ/AAI-DSC-RSP messages contain change (update/ add/ delete) information for multiple service flows (identified by their combinations of MGID and FID), it cannot be transmitted by multicast connections.

According to the PKMv3 Key Hierarchy, corresponding multicast keys for each multicast connection shall be generated and applied with each multicast connection, differently. When we need to change the service flow information for a multicast service, the unicast signaling by AAI-DSC-REQ/AAI-DSC-RSP for multiple HR-MSs is inefficient.

So, we propose to define a new multicast-based management messages (AAI-HR-DSC-CMD) for multicast service flow changes on the HR network. If this type of message is used, it shall be transmitted all the HR-MSs with the multicast connection on the same multicast group zone, and encrypted with the current MTEK for confidentiality, and contain the MCMAC attribute for MCMAC verification which is computed from MCMAC\_KEY. Therefore, we can get a more secure (encrypted and message authenticated) and efficient (just one message transaction for multiple HR-MSs) service flow change procedure.



The above concept can be used for the dynamic service flow deletion. When a circumstance for a bulk deletion for multiple HR-MSs of a service flow happens, a multicast command type of service deletion (using AAI-HR-DSD-CMD) will be better operated.

# Proposed Text for the 802.16.1a AWD

Note:

The text in **BLACK** color: the existing text in the IEEE P802.16.1a/D3

The text in **~~RED~~** color: the removal of existing IEEE P802.16.1a/D3.

The text in **BLUE** color: the new text added to the IEEE P802.16.1a/D3.

 [-------------------------------------------------Start of Text Proposal---------------------------------------------------]

**[*Adopt the following changes in Section 6.2.3 in IEEE P802.16.1a/D3.*]**

***[Page# 11, Line# 1]***

***Change (Add the MAC Control Messages for Multicast Services) Table 29 as indicated:***

**Table 29 —MAC control messages**

| **No.** | **Functional Areas** | **Message names** | **Message description** | **Security** | **Connection** |
| --- | --- | --- | --- | --- | --- |
| 116 | Multicast | AAI-HR-DSC-CMD | Multicast-based Service Flow Change | Encrypted/ICV by Multicast Key | Multicast |
| 117 | Multicast | AAI-HR-DSD-CMD | Multicast-based Service Flow Delete | Encrypted/ICV by Multicast Key | Multicast |

***Newly define the following MAC Control Messages for Multicast Services:***

* + - * 1. AAI-HR-DSC-CMD message

An HR-BS may use AAI-HR-DSC-CMD message to change a service flow (identified by a combination of MGID and FID) to all the HR-MSs with multicast command in the multicast group zone during the multicast group service.

When the AAI-HR-DSC-CMD message is used, it shall be encrypted with the current MTEK for confidentiality, and contain the MCMAC attribute for MCMAC verification which is computed from MCMAC\_KEY.

**Table ?? —** **AAI-HR-DSC-CMD message field description**

| **Field** | **Size (bits)** | **Value/Description** | **Condition** |
| --- | --- | --- | --- |
| Current Multicast Group ID | 12 |  |  |
| Current FID | 4 |  |  |
| New Multicast Group ID | 12 |  |  |
| New FID | 4 |  |  |
| MCMAC Digest |  | Message Digest Calculated using MCMAC Key by HR-BS |  |

* + - * 1. AAI-HR-DSD-CMD message

An HR-BS may use AAI-HR-DSD-CMD message to delete a service flow (identified by a combination of MGID and FID) to all the HR-MSs with multicast command in the multicast group zone during the multicast group service.

When the AAI-HR-DSD-CMD message is used, it shall be encrypted with the current MTEK for confidentiality, and contain the MCMAC attribute for MCMAC verification which is computed from MCMAC\_KEY.

**Table ?? —** **AAI-HR-DSD-CMD message field description**

| **Field** | **Size (bits)** | **Value/Description** | **Condition** |
| --- | --- | --- | --- |
| Multicast Group ID | 12 |  |  |
| Current FID | 4 |  |  |
| MCMAC Digest |  | Message Digest Calculated using MCMAC Key by HR-BS |  |

[-------------------------------------------------End of Text Proposal---------------------------------------------------]