**IEEE P802.21  
Media Independent Handover Services**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Proposed Remedy for the 802.21d LB7 comment #150** | | | | |
| **Date:** 2013-09-16 | | | | |
| **Author(s):** | | | | |
| **Name** | **Affiliation** | **Address** | **Phone** | **Email** |
| Yoshikazu Hanatani | Toshiba |  |  | yoshikazu.hanatani@ toshiba.co.jp |

Abstract

This document contains proposed remedy for “the 802.21d ballot 7 comment #150.

**Remedy for the 802.21d LB7 comment #150**

9.4.1 MIH message protection mechanisms using GKB-generated SAs

Group Key Block (GKB) is a data field used to distribute master group keys (MGKs) to protect MIH multicast/broadcast commands. A GKB contains GroupkeyVerificationCode, CompleteSubtree and GroupKeyData (see 7.4.31.3 and 7.4.32.1). A group manipulation command accompanies a target MIHF Group ID and a GKB. An MN follows the procedure described in 9.4.2.2.2 to determine whether it should try to recover the key from the GKB. If an MN succeeds in recovering an MGK, the MN will keep the pair of the target MIHF Group ID and MGK, which means that the MN belongs to the group designated by the target MIHF Group ID. Otherwise, if an MN fails to derive an MGK from the GKB, it means that the MN does not belong to the group designated by the target MIHF Group ID. If an MN leaves the current group, the MN may destroy the pair of MIHF Group ID and MGK stored even though the key is not valid any more.

A series of group commands may follow a group manipulation command which defines a target group of MNs. A group command is issued, for instance, to instruct the group that the members should handover to a PoA or that they should update their configuration parameters. A payload of a group command can be protected (encrypted) using the SA derived from the MGK. The following two steps describe how group manipulation and command delivery are performed:

* Step 1: A Command center, which is an MIH PoS, issues a group manipulation command to instruct MNs to join or leave a group. A group manipulation command may also be used to update a group key stored at an MN. Group manipulation commands may be delivered to MNs through existing multicast channels. A multicast channel is associated with a group: If an MN joins a group then it starts listening to the multicast channel associated with the group. The address used by this multicast channel can be provided by the group manipulation command itself.
* Step 2: A Command center issues to a group of MNs a group command (not a group manipulation command) to instruct the MNs in the group to take an action. The target group is designated by the MIHF Group ID field in the group command. A group command is delivered through the multicast channel associated with the MIHF Group ID. A group command may alternatively take two types of payload: Encrypted and non-encrypted. If a payload is encrypted, it is encrypted with a key derived from the current group key.

Each MN has a Device Key, which is a sequence of AES keys. The number of keys in a Device Key is 8, 16, 24 or 32, which is a system-wide constant. All MNs which are managed by a Group Manager have the same number of device keys. The format of Device Key may vary depending on its implementation and is out of the scope of this specification. For convenience, an example format of a Device Key is described in clause 9.4.2.2 and Annex U. When confidentiality is not required for group manipulation, a GKB without GroupKeyData should be used. Note that an MN need not have a Device Key if the GKBs always have no GroupKeyData.

A Command center has a module called GKB Generator. A GKB Generator receives all the Device Keys assigned to all the MNs associated to a group, a set of MIHF IDs and a MGK. The set of MIHF IDs indicates the MNs that constitute a group. The MGK is a master group key for that group. MNs and the command center can generate a media independent group encryption key (MIGEK) and a media independent master group key verification key (MIGKCK) from MGK (see 9.4.3). The mechanism to provide all Device Keys to the GKB generator is out of the scope of this specification. This mechanism can just encompass the explicit provision of the Device Keys to the GKB or the random seed used to derive them. On receiving those data, a GKB Generator outputs a GKB, or several GKBs.

Although there are detailed procedures of an MIH User at a Command Center to prepare an MIH request for group manipulation, handover or configuration update depend on implementations of the User. An overview of the behaviors of an MIH User is given in 9.4.2, which also defines a series of actions to be performed by an MIHF which receives an indication message of group manipulation, handover or configuration update.

There are four modules involved in group manipulation operations: An MIH User of a Command center, an MIHF of a Command center, an MIH User of an MN and an MIHF of an MN. Indispensable components for each of the modules relevant to group manipulation and group commands are listed as follows:

MIH User of Command center:

* A GKB Generator.
* All the MIHF IDs and all the Device Keys each of which is uniquely associated with one of the MIHF IDs. As is described in 9.4.2.2, a number called Leaf Number is uniquely asssociated with a Device Key.
* A Group Management Database which stores a group management table, which has the following five columns at least: A Group MIHF ID, an MGK, a Device Key, a Leaf Number and an MIHF ID. An MN having the MIHF ID, the Device Key and the Leaf Number on a row belongs to the group designated by the Group MIHF ID recorded on the same row.

MIHF of Command center:

* A signing key. The key is for creation of a signature of the Command center
* A Group Database which stores a group table, which has the following four columns: An MIHF Group ID, a multicast address, SAID and MGK. The multicast address on a row is associated with the group designated by the MIHF Group ID recorded on the same row. Additionally the multicast address may have attributes, indicating if the multicast address is defined at layer 2 or 3 of the protocol stack.
* A Device Key for the Command center used to derive MGK by a GKB received from the MIH User of the Command center.

MIHF of an MN:

* A Device Key.
* Certificate of a Command center. The certificate contains a verification key. The key is for verification of a signature made by the Command center.
* A Group Database which stores a group table, which has the following three columns at least: An MIHF Group ID, an MGK and a multicast address. An MN concurrently belongs to the groups designated by the MIHF Group IDs recorded on the group table. The MGK for one of the groups is the one recorded on the same row as the MIHF Group ID, and the multicast address and a flag specifying a transport layer recorded on the same row is associated with the group.