IEEE P802.21
Media Independent Handover Services

|  |
| --- |
| Clause 9.4 and Clause 9.5 restructure proposal |
| Date: 2013-11-xx |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Lily Chen | NIST | 100 Bureau Dr. Gaithersburg, MD 20878 | +1 (301) 975-6974 | Lily.Chen at nist.gov |

Abstract

This contribution proposes an outline to restructure clause 9.4 and 9.5 in IEEE P802.21d/D2.0 to resolve the comments received in ballot 7a.

**Background:**

Based on the comments received in ballot 7a, clause 9.4 and clause 9.5 in IEEE P802.21d/D2.0 need to be restructured. Here is a summary about the issues with the current structure.

1. Without introducing the tree structure for device keys, the content is hard to understand (see comment #107).
2. Subclause 9.4.1 is titled as protection mechanisms. However, 9.4.1 is more on some basic assumptions about the command center.
3. Subclauses 9.4.1 and 9.4.2 have content overlap about the command center. The descriptions are inconsistent (see comments #33, #97, etc.).
4. Subcluse 9.4.2.4 is misplaced. The content is needed for the description of the commend center in 9.4.2.1-9.4.2.3.
5. Subclause 9.4.3 and subclause 9.4.4 have the same title.
6. Clause 9.5 shall not be a stand alone clause.

Therefore, a new structure is proposed for clause 9.4 and 9.5. The basic idea is to separate the manipulation part and group command protection part. The new proposed clause 9.4 will address the group manipulation, while 9.5 will specify group command protection.

**New Structure Proposal**:

----------

**9.4 Group manipulation for multicast MIH messages**

A multicast MIH message is an MIH message sent to a group of recipients. A multicast recipient can be a mobile node (MN) or a point of service (PoS). Each group is identified by an MIHF group ID. A group is dynamic in the sense that some of the group members may leave, while the new member may join. The group is managed through group manipulation commands. A series of group commands may follow a group manipulation command that defines a target group of MNs.

**9.4.1 Key distribution for multicast MIH message protection**

9.4.1 can use the text in document #199 and [Yoshi’s algorithm]].

**9.4.1.1 Device key assignment through a key tree**

**9.4.1.2 Complete subtree**

**9.4.2 GKB generation by the complete subtree method**

[Use the original content in 9.4.2.4. Some text needs to be modified a little bit to use the introduction provided in the new clause 9.4.1].

**9.4.2.1 Master group key wrapping**

[This should use the content in 9.4.2.5.1 encapsulation. But new text is needed. The current text is just an example. It needs to be more general.]

**9.4.2.2 Key unwrapping**

[This should use the content in 9.4.2.5.2 decapsulation.]

**9.4.2.3 Fragmented GKB**

[This should use the content in original 9.4.1. Subgroup range needs to be introduced. Then use the paragraph above the Table 26 and the table. The last column of Table 26 does not seem right. The expected behavior is not join or leave. It is to process the GKB or not.]

**9.4.3 Secure group manipulation procedures**

[This should use the content in 9.4.2.]

**9.4.3.1 Procedures for group manipulation command sender (GMCS)**

[Here we assume that group manipulation command sender is a PoS, where the MIH user is the command center.]

**9.4.3.1.1 MIH user of a GMCS**

[This can use the content in 9.4.2.1. Here MIH user of a GMCS is a command center.]

**9.4.3.1.2 MIHF of a GMCS**

[This can use the content in 9.4.2.2.]

**9.4.3.2 Procedures for group manipulation command recipients (GMCR)**

[Here a recipient can be an MN or a PoS. Only the MIHF is involved. ]

**9.5 Multicast MIH message protection**

**9.5.1 Group session key derivation**

[This can use the content in 9.4.3.]

**9.5.2 Multicast message encrypton**

[This can use the content in 9.4.3.]

**9.5.3 Signature and credential management**

[This can use the content in 9.4.5.]

**9.5.4 Common procedures**

[This can use the content in 9.5. The question is: common for what?]

**9.5.4.1 Sending**

**9.5.4.2 Receiving**