Suggested Remedy for IEEE 802.21d Lb7b comments #79, #81, #82, #100

Antonio de la Oliva (UC3M)

* + - * 1. MIH user of a GMCS

Required components in an MIH User of a GMCS in a PoS relevant to group manipulation and group commands are listed as follows:

* A GKB Generator. This component is constructed from CreateCompleteSubtreeFragments (see 9.4.2.3), KeyDerivation (see 9.5) and MasterGroupKeyWrapping (9.4.2.1).
* A *Group Management Information Base* (of type GROUP\_MANAGEMENT\_BASE as defined in Table F.25). This information base contains the MIHF\_IDs and device keys of all nodes in the network.
* A *Command Center Information Base* (of type COMMAND\_CENTER\_BASE as defined in Table F.25). This information base contains the list of nodes that can be managed by groups.
* A *Group Information Base* (of type GROUP\_INFO\_BASE as defined in Table F.25). This information base stores the information about a group. It contains the MIHF Group ID, the different group members, the MGK used and the status of the group.

A Flow diagram of the generation process of the GKB parameters is given in Figure 24. The MIH User generates MIH\_Net\_Group\_Manipulate.request described in 7.4.3.2 as follows:

1. Define a group to manipulate:
	1. Decide a TargetGroupIdentifier which indicates a group to manipulate.
		* If it is a new group, choose the TargetGroupIdentifier by consulting with the *Group Information Base*.
	2. Decide group members belonging to the group from the *Command Center Information Base*.
		* The group members are the recipients of group addressed commands to the group.
	3. If contents of group addressed commands to the group shall be encrypted, the MIHF chooses an MGK for the group.
	4. Update with the new MGK and the new membership information the *Group Information Base.*
2. Define CompleteSubtree and SubgroupRange:
	1. Send MIHF IDs of the group member, the group management tree, and threshold for fragmentation to the CreateCompleteSubtreeFragments procedure, and receive CompleteSubtree and SubGroupRange.
	2. If the CompleteSubtree is not fragmented, SubgroupRange is removed.
3. (Optional) Define GroupKeyData:
	1. When MGK is not used, this process is skipped.
	2. Send the MGK and the CompleteSubtree to the MasterGroupKeyWrapping procedure, and receive GroupKeyData. The procedure accesses the *Group Management Information Base* to refer the group members’ device key.



1. — Flow diagram of the generation process of the GKB parameters
2. (Optional) Construct the UserSpecificData field.
3. Choose a DestinationIdentifier. A DestinationIdentifier is an MIHF Group ID, which represents an existing group. The group indicated by the DestinationIdentifier shall include all members who are manipulated by this command.
4. Generate an MIH\_Net\_Group\_Manipulate.request from the DestinationIdentifier, the TargetGroupIdentifier, the SubgroupRange (an option), the UserSpecificData (an option), the CompleteSubtree and the GroupKeyData (an option). Set the GroupKeyUpdateFlag if the MGK of the group designated by the TargetGroupIdentifier should be updated. Send it to the local MIHF.
5. Optionally, in case the CC obtains a Multicast Address to be used by the group (through any mean outside of this specification), it can choose to ask the MIHF to use it by including it in the MIH\_Net\_Group\_Manipulate.request.

Figure 25 shows a flow diagram summarizing the steps performed by the MIH User on a PoS, described in this Clause.



1. — Summary of steps performed by PoS MIH User
	* + - 1. MIHF of a GMCS

Required components relevant to group manipulation and group commands are listed as follows:

* A signing key (of type SIGNING\_KEY as defined in Table F.25). The key is for creation of a signature at the Command center.
* A *Recipient Information Base* (of type RECIPIENT\_MIHF\_BASE as defined in Table F.25)containing the set of device keys to retrieve a group key from a GKB which is received from the local MIH User. The certificate used to verify digital signatures, and the information required to send commands to the group, i.e., the MIHF Group ID, the transport address used, the MGK, the sequence number and the SAID associated to the group.

It is assumed that the MIHF is able to obtain in some way a multicast address associated with a Group MIHF ID. The multicast address may be contained in the MIH\_Net\_Group\_Manipulate.request received from the MIH User. In this case, if the TargetGroupIdentifier in the received request is not registered in the *Recipient Information Base*, obtain the multicast address associated with the TargetGroupIdentifier and update the *Recipient Information Base* with the DestinationIdentifier and the associated multicast address. The MIHF of the Command center receives an MIH\_Net\_Group\_Manipulate.request, which is generated by the MIH User, the MIHF generates and sends an MIH\_Net\_Group\_Manipulate indication message to a multicast group. Note that this behavior depends on the ResponseFlag parameter. When “ResponseFlag=1”, the MIHF will generate MIH\_Net\_Group\_Manipulate request message. When “ResponseFlag=0”, the MIHF will generate MIH\_Net\_Group\_Manipulate indication message.

In the following we detail the steps performed to generate the message:

1. Generate a Source MIHF ID TLV using its own MIHF ID.
2. Generate a Destination MIHF ID TLV from the DestinationIdentifier in the received MIH\_Group\_Manipulate.request.
3. If GroupKeyUpdateFlag = 0 and GroupKeyData is contained in the received MIH\_Group\_Manipulate.request, it generates Sequence Number TLV from a current SequenceNumber with respect to the TargetIdentifier in the MIH\_Group\_Manipulate.request. Else Sequence Number TLV is not generated.
4. The MIHF generates a Multicast Address TLV. If the MIH\_Net\_Group\_Manipulate.request contains a MulticastAddress parameter, the parameter is contained in the Multicast Address TLV. Otherwise, a multicast address determined by the MIHF is contained in the Multicast Address TLV.
5. If the MIH\_Net\_Group\_Manipulate.request contains a SubgroupRange, it generates a SubgroupRange TLV from the SubgroupRange.
6. If the MIH\_Net\_Group\_Manipulate.request contains a UserSpecificData, it generates an Aux Data TLV from the UserSpecificData.
7. Generate a Complete Subtree TLV from the CompleteSubtree in the received MIH\_Net\_Group\_Manipulate.request.
8. If the MIH\_Net\_Group\_Manipulate.request contains a GroupKeyData, it generates a Group Key Data TLV from the GroupKeyData.
9. If GroupKeyUpdateFlag = 0 , SAID TLV is not generated. Else decide new security association ID and generate SAID TLV from the security association ID.
10. If the GroupKeyUpdateFlag = 1, then process the GKB (the Complete Subtree TLV and the Group Key Data TLV) using the Device Key stored in own *Recipient Information Base*, and obtain the MGK.
11. Update own *Recipient Information Base* using the TargetIdentifier, the MulticastAddress, the MGK, and the SAID.
12. Generate a Signature TLV as shown in 9.4.1 using the signing key of the MIHF.
13. If ResponseFlag=0, generate an MIH\_Net\_Group\_Manipulate indication using the preceding TLVs, else generate an MIH\_Net\_Group\_Manipulate request using the preceding TLVs.

Figure 26, shows a flow diagram summarizing the steps performed by the MIHF at a PoS, described in this Clause.



1. —Summary of steps performed by PoS MIHF
	* + 1. Procedures for group manipulation command recipients (GMCR)

Required components relevant to group manipulation and group commands are listed as follows:

* A Device Key.
* A certificate of a Command Center which contains a verification key. The verification key is for verification of a signature made by the Command Center.
* A *Group Information Base* which stores a groups table, which has the following three columns at least: MIHF Group ID, MGK and Multicast Address. A row of the table specifies that this MN belongs to the group designated by the MIHF Group ID. The group has the MGK as the master group key and is associated with the Multicast Address. The Multicast Address may have an attribute which indicates if it defined at Layer 2 or 3 of the protocol stack.

When a client MN receives a group manipulation command, i.e., an MIH\_Net\_Group\_Manipulate indication/request message, issued by a Command center, the MIHF of the MN processes the command. Suppose at first that the GKB in the group manipulation command has a group key data element:

1. The MIHF obtains a Source Identifier from the Source MIHF ID TLV.
2. The MIHF verifies the Signature TLV using the verification key corresponding to the obtained SourceIdentifier. If the verification fails, the MIHF shall cancel the following steps and stop processing the command.
3. The MIHF checks the DestinationIdentifier in the Destination MIHF ID TLV. If the DestinationIdentifier does not match one of the following MIHF IDs, the MIHF shall cancel the following steps and stop processing the command: (i) An MIHF Group ID corresponding to a broadcast address, (ii) an MIHF Group ID which is registered with a multicast address in the Group Information Base, or (iii) the MN's own MIHF ID.
4. Decrypt the payload if it is encrypted, i.e., if it is a Security TLV. The decryption key is the one associated with the DestinationIdentifier in the Group Information Base.
	1. In case an MN cannot decrypt the Security TLV, the message will be silently discarded.
5. If a SubgroupRange TLV exists in the indication, the MIHF obtains a SubgroupRange and checks whether its own Leaf Number is contained in the SubgroupRange or not. If it is not, the MIHF shall cancel the following steps and stop processing.
6. The MIHF obtains the TargetIdentifier in the Group Identifier TLV.



1. —MGK generation process
2. A GKB is composed of the Complete Subtree TLV. The MIHF processes the Complete Subtree TLV as described in 7.4.32.2. If the MIHF succeeds to find a matching pair of GKB Indices, go to the next step. Otherwise, go to Step l).
3. The MIHF checks whether the TargetIdentifier obtained in Step f) has already been registered or not in the Group Information Base. If it has been, go to Step h) [Stay]. Otherwise, go to Step i) [Join].
4. [Stay] The MIHF throws an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field of the indication shall be “Unchanged successful” (5). The procedure of command processing terminates.
5. [Join] The MIHF obtains a multicast address associated with the TargetIdentifier and starts listening to it. The messages come through the multicast channel may be encrypted with the group key obtained in Step g). The multicast address may be obtained from a server (Note that this operation is out of the scope of this specification). Or, the received indication may accompany it in the Multicast Address TLV. Save in the *Group Information Base* the TargetIdentifier, the associated multicast address and the group key obtained in Step f).
6. The MIHF issues an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2. to the MIH User. The GroupStatus field must be “Join operation successful” (0). The procedure of command processing terminates.
7. [Leave] The MIHF finds the multicast address recorded on the same row as the TargetIdentifier obtained in Step f) and the MIHF stops listening to it. The MIHF removes the row that has the TargetIdentifier.
8. The MIHF throws an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field must be “Leave operation successful” (3). The procedure of command processing terminates.

Then, suppose that the GKB in the group manipulation command has no group key data part:

1. The MIHF obtains a Source Identifier from the Source MIHF ID TLV.
2. The MIHF verifies the Signature TLV using the verification key corresponding to the obtained SourceIdentifier. If the verification fails, the MIHF shall cancel the following steps and stop processing the command.
3. The MIHF checks the DestinationIdentifier in the Destination MIHF ID TLV. If the DestinationIdentifier does not match one of the following MIHF IDs, the MIHF shall cancel the following steps and stop processing the command: (i) An MIHF Group ID corresponding to a broadcast address, (ii) an MIHF Group ID which is registered with a multicast address in the *Group Information Base*, or (iii) the MN's own MIHF ID.
4. Decrypt the payload if it is encrypted, i.e., if it is a Security TLV. The decryption key is the one associated with the DestinationIdentifier in the *Group Information Base*.
5. If a SubgroupRange TLV exists in the indication, the MIHF obtains a SubgroupRange and check whether its own Leaf Number is contained in the SubgroupRange or not. If it is not, the MIHF shall cancel the following steps and stop processing.
6. The MIHF obtains a TargetIdentifier in the Group Identifier TLV.
7. A GKB is composed of the Complete Subtree TLV. The MIHF processes the Complete Subtree TLV as described in 7.4.32.2. If the MIHF succeeds to find a matching pair of GKB Indices, go to the next step. Otherwise, go to Step i).
8. The MIHF checks whether the TargetIdentifier obtained in Step f) has already been registered or not in the Group Information Base. If it has been, go to the Step j) [Stay]. Otherwise, go to Step k) [Join].
9. The MIHF checks whether the TargetIdentifier obtained in Step f) has already been registered or not in the *Group Information Base*. If it has been, go to Step m) [Leave]. Otherwise, go to Step j) [Stay].
10. [Stay] The MIHF issues an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field of the indication must be “Unchanged successful” (5). The process terminates.
11. [Join] The MIHF obtains a multicast address associated with the TargetIdentifier and starts listening to it. The multicast address may be obtained from a server. Or, the received indication may accompany it in the Multicast Address TLV. Save in the Group Information Base the TargetIdentifier, the associated multicast address.
12. The MIHF issues an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field must be “Join operation successful” (0). The procedure of command processing terminates.
13. [Leave] The MIHF finds the multicast address recorded on the same row as the TargetIdentifier obtained in f) and the MIHF stops listening to it. The MIHF discards the row that has the TargetIdentifier.
14. The MIHF issues an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field must be “Leave operation successful” (3). The procedure of command processing terminates.

Figure 28 summarizes the steps followed by the MIHF on the MN upon reception of an MIH\_Net\_Group\_Manipulation.indication.



1. —Summary of steps performed by the MN MIHF

Subclause 7.4.31 introduces a mechanism enabling the MN to trigger the Join/Leave operations controlled by the Command center. In order to do so, the MIH User located at the MN notifies the Command center of its desire to Join or Leave a group through the use of the MIH\_MN\_Group\_Manipulate primitive. The Command center, upon receiving the associated request message, performs the same process as defined in this Clause, for the use of the MIH\_Net\_Group\_Manipulate, although in this case, the group to be manipulated is provided by the MN. The resulting GKB parameters are returned to the MN in the MIH\_MN\_Group\_Manipulate response message.

|  |  |  |
| --- | --- | --- |
| GROUP\_INFO | SEQUENCE(MIHF\_ID,CHOICE(MGK,NULL),GROUP\_MEMBERS, GROUP\_STATUS) | The information base stores MIHF Group ID and its group members. |
| COMMAND\_CENTER\_BASE | MANAGED\_NODES | The information base stores information to issue group manipulation commands and group addressed commands. |