IEEE P802.21  
Media Independent Handover Services

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Use Case Reference for TGd | | | | |
| Date: 2012-07-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Antonio de la Oliva | UC3M | Avda. Universidad 30,28918, Leganes, Madrid |  | aoliva@it.uc3m.es |
| Daniel Corujo | ITAv | Campus Univesirátio de Santiago, 3810-193 Aveiro, Portugal | +351 234 377 900 | dcorujo@av.it.pt |
| Carlos Guimaraes | ITav | Campus Univesirátio de Santiago, 3810-193 Aveiro, Portugal | +351 234 377 900 | cguimaraes@av.it.pt |

Abstract

The most current version of this document contains the descriptions of the use cases that will be used to evaluate submissions to TGd.

Table of Contents

1 Terminology 4

2 Introduction 5

3 Use cases 6

3.1 Failover/Restoration 6

3.2 Load Balancing 6

3.3 Configuration Parameters Update 6

3.4 Firmware Update 6

3.4.1 Firmware update over MIH protocol 6

3.4.2 Firmware update indication over MIH protocol 6

4 Use Cases Characterization 7

4.1 Use Case characteristics for TGd 7

4.1.1 Differentiated group management 7

4.1.2 Rate of group modification 7

4.1.3 Confidentiality 8

4.1.4 Authentication 8

4.1.5 Integrity Protection 8

4.1.6 Key renegotiation dynamicity 8

4.2 Per use case characterization 8

4.2.1 Failover/Restoration 8

4.2.2 Load Balancing 9

4.2.3 Configuration Parameters Update 9

4.2.4 Firmware Update 10

# Terminology

TBD

# Introduction

IEEE 802.21 enables the optimization of the handover process by providing the network and the terminal with extended handover information and control mechanisms. On its original design, IEEE 802.21 defined the signaling required by a control node located at the network (the so called Point of Service, PoS) to assist and manage a terminal handover process, and prepare network link resources. As such, the signaling was originally designed with a unicast point of view, in which the PoS establishes a peer to peer communication with the terminal. This mechanism works well when the number of nodes performing simultaneous handover is reduced but does not scale as the number of nodes increases.

The goal of this document is to serve as reference for the use cases submitted to the TGd, and to be used as reference while deriving the requirements of the solution.

# Use cases

This section shows the generic description of each use case followed by an analysis of the characteristics defined in the previous section.

## Failover/Restoration

This use case corresponds to a handover being triggered due to optimization or preventive procedures (i.e., a failure in the PoA), forcing the whole network, in general, to hand off to a second PoA in order to maintain connectivity.

In general, due to the reason for the handover, the complete set of nodes attached to the serving PoA (which is about to fail) are hand off to another PoA. After handover, the group of nodes that has just moved may join the group of nodes already attached to the target PoA.

## Load Balancing

This use case refers to a handover triggered in order to free resources in the Point of Attachment (PoA) serving the network. In this way, the load on the PoA is decreased, while also reducing the probability of losing some important message (e.g., reducing call block probability or lost measurements from sensors) from the nodes. This use case can also contemplate the scenario of executing the handover to a PoA where the nodes are expected to obtain a better signal strength, contributing to a better energy efficiency. Another useful scenario is the handover of portions of the network to a secondary maintenance network, in order to perform management operations.

## Configuration Parameters Update

This use case corresponds to the use of the multicast group communication to update a certain configuration parameter in all nodes belonging to the group. Envisioned usages for this scenario encompass the configuration of handover related parameters, such as signal level thresholds, or even the configuration of other **application** specific parameters, such as Smart Grid information on the rate of the electricity.

## Firmware Update

This use case corresponds to the use of a multicast group to convey the nodes the information regarding a new firmware update. This use case can be implemented in two ways with different requirements in term of security.

### Firmware update over MIH protocol

In this case, the firmware image itself is transported to the nodes through MIH protocol messages.

### Firmware update indication over MIH protocol

In this case, the information carried by the MIH protocol only contains a pointer to the location of the firmware image, e.g., an URL. This information is passed to the application, which takes care of downloading the image through application specific mechanisms.

# Use Cases Characterization

The purpose of this document is to gather all use cases that will be considered in the evaluation of proposed updates to IEEE 802.21 that would provide multicast group management and communication capabilities. TGd may determine that some of the use cases contained in this document are required to be satisfied, while others may be desired but optional. In any case, no requirements for technical solutions are required to address issues other than those stated or implied by the use cases in the most current version of this document.

## Use Case characteristics for TGd

The basic methodology to the use case description follows. For each of the use cases six different characteristics will be analysed. These six characteristics are the following:

* Differentiated Group Management. With this characteristic we express the use case need for managing several groups in a differentiated way.
* Rate of group modification. With this characteristic we express the flexibility required by the use on the creation/deletion and modification of groups of nodes.
* Confidentiality. This characteristic shows the need for encryption mechanisms in the use case.
* Authentication. This characteristic shows the use case need for authentication of the source of the message.
* Integrity protection. This characteristic relates to the use case need for detecting the modification of a message.

For each of the security related characteristic we add an attribute that aims at expressing the requirement in terms of the dynamicity of the key used for each security feature:

* Key renegotiation dynamicity: Expresses the dynamicity of the key renegotiation per security mechanism

For each of the use cases we present an analysis of the previous characteristics, showing the expected values for the specific functionality on each use case.

In the next subsections we show which are the valid values for each of the characteristics presented above that will be used on this document.

### Differentiated group management

The differentiated group management characteristic is used to express if a certain use case requires different behaviours to be provided towards different groups of nodes within the network.

The values valid for this characteristic are:

* Required: The use case is expected to encompass different groups of nodes with different behaviours.
* Desired: The use case might encompass different groups requiring different behavior if the feature is available.
* Not required: The use case is only composed of one group or the behavior for all groups is the same.

### Rate of group modification

Through this characteristic we express the dynamicity of the scenario in terms of the need for creation/deletion or modification of groups and subscription to groups.

The valid values for this characteristic are:

* High: Individual nodes move across the network
* Medium: A mix of complete networks and individual nodes move across the network boundaries
* Low: Complete networks of nodes join the network at the same time

### Confidentiality

This characteristic aims at expressing the need for providing encryption characteristics to the group.

The valid values for this feature are:

* Required: Encryption of all communication between the source of the communication and the nodes belonging to the group is required.
* Desired: Encryption of all communication between the source of the communication and the nodes belonging to the group is desired.
* Not required: Encryption of all communication between the source of the communication and the nodes belonging to the group is NOT required.

### Authentication

This characteristic expresses the need for authentication of the source of the message.

The valid values are:

* Required: Proof of authentication of the source of the message is required in order to process the content of the message.
* Desired: Proof of authentication of the source of the message is desired.
* Not required: Proof of authentication of the source of the message is NOT required in order to process the content of the message.

### Integrity Protection

This characteristic aims at showing the need for proof of integrity of the messages exchanged to the group.

The valid values are:

* Required: Integrity detection features are required for the use case.
* Desired: Integrity detection features are desired for the use case.
* Not required: Integrity detection features are NOT required for the use case.

### Key renegotiation dynamicity

This attribute shows per use case the dynamicity expected in terms of renegotiating the keys used for security features.

The valid values are:

* High: The key needs to be renegotiated each time the group membership changes
* Medium: The key needs to be renegotiated based on certain events such as handover, timer expiration, number of nodes changing membership etc..
* Low: The key needs does not need to be renegotiated periodically.

## Per use case characterization

### Failover/Restoration

|  |  |  |
| --- | --- | --- |
| Characteristic | Value | Key Renegotiation |
| Differentiated Group Management | Not Required/Desired | - |
| Rate of group modification | Low | - |
| Confidentiality | Not Required | - |
| Authentication | Required | Medium/Low |
| Integrity Protection | Required | Medium/Low |

This scenario in general does not require differentiated group management functionalities, since all nodes in the network need to perform handover before the PoA stops working. If this feature is available, it can be used to provide different alternative PoAs to the nodes, based on technologies available or for load balancing in case of a fail in the serving PoA.

The rate of group modification in this use case is low, since the complete network in general is performing the handover, hence no partition or creation of new groups is required.

This use case does not require confidentiality since there is no sensible information being exchanged, although it requires authentication and integrity protection in order to avoid any malicious node impersonating the PoS and commanding the complete network to handover to a compromised PoA (or performing DoS attacks).

In all cases, since the key is only needed to integrity protection and authentication, the requirements in terms of key renegotiation are low, unless the serving PoS changes.

### Load Balancing

|  |  |  |
| --- | --- | --- |
| Characteristic | Value | Key Renegotiation |
| Differentiated Group Management | Required | - |
| Rate of group modification | High/Medium | - |
| Confidentiality | Not Required | - |
| Authentication | Required | Medium/Low |
| Integrity Protection | Required | Medium/Low |

This use case in general requires differentiated group management, since the nodes will require to be moved to the most appropriate target network accordingly to their different characteristics. The difference with the previous use case resides on performing group handover in a differentiated way, providing to each group the best possible PoA.

Following the previous idea, this use case needs to classify all nodes in different groups, and not using just one big group to perform a failover handover as in the previous use case. Hence the rate of group modification is expected to be high or at least medium.

Regarding the security, in this use case the information exchanged to the group is also not sensitive hence confidentiality of the information exchanged is not needed. With respect to the authentication and integrity protection characteristics, the same comments as in the previous use case apply.

### Configuration Parameters Update

|  |  |  |
| --- | --- | --- |
| Characteristic | Value | Key Renegotiation |
| Differentiated Group Management | Required | - |
| Rate of group modification | Medium/Low | - |
| Confidentiality | Not required | - |
| Authentication | Required | Medium/Low |
| Integrity Protection | Required | Medium/Low |

This use case requires of the management of different groups that might require the configuration of different technologies depending on their characteristics. As different groups will be used and nothing is limiting the amount of users per group, this scenario can exhibit a moderate amount of modifications of the groups.

Regarding security, the update or modification of configuration parameters requires the maximum security in terms of authentication and integrity of the messages. It is also worth to mention that this use case requires also the log of the commands received in order to provide non-repudiability.

In all cases the node source of the message must be authenticated in order to execute its commands, and the messages must be check in order to be sure the message has not suffer any modification.

### Firmware Update

As in the use case description, here we present two tables of characteristics depending on the implementation of the Firmware Update.

Regarding the non-security related characteristics, both use cases share the same characteristics as the Configuration Parameters Update. In the following subsections we highlight the differences in terms of security requirements between the different implementations of the use case.

#### Firmware update over MIH protocol

|  |  |  |
| --- | --- | --- |
| Characteristic | Value | Key Renegotiation |
| Differentiated Group Management | Required | - |
| Rate of group modification | Medium/Low | - |
| Confidentiality | Required | High/Medium |
| Authentication | Required | Medium/Low |
| Integrity Protection | Required | Medium/Low |

This use case shows the transport of the firmware binary image on top of the MIH protocol, between an MN and the PoS. In this case, confidentiality is required since the binary image of the firmware should not be made public while being transported. As the transport is performed at the MIHF level, application layer security mechanisms and protocols cannot be used, requiring of new security mechanisms to be defined at the MIHF level.

#### Firmware update indication over MIH protocol

|  |  |  |
| --- | --- | --- |
| Characteristic | Value | Key Renegotiation |
| Differentiated Group Management | Required | - |
| Rate of group modification | Medium/Low | - |
| Confidentiality | Not Required | - |
| Authentication | Required | Medium/Low |
| Integrity Protection | Required | Medium/Low |

This use case corresponds to the transport of an indication and a pointer to a new firmware image through the MIH protocol. In this case, the binary file of the image is uploaded in some online repository. The solution uses the multicast MIH protocol to indicate the application layer of the existence of such image, using any higher layer protocol to perform the download of the image. As such, in this use case, confidentiality is not required since application layer specific mechanisms can be used to secure the image transport, such as e.g., https.