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.

# 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 Case Descriptions

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.
* Need for cyphering. This characteristic shows the need for cyphering mechanisms in the use case.
* Authentication of the source of the message. This characteristic shows the use case need for authentication of the source of the message.
* Non-repudiation capabilities. This characteristic presents the use case need for providing non-repudiation features.
* Tampering detection. 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

### Need for cyphering

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

The valid values for this feature are:

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

### Authentication of the source of the messages

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.

### Non-repudiation capabilities

This characteristic expresses the use case need for providing non-repudiation features. With non-repudiation we mean a service that provides proof of the integrity and origin of the data and an authentication of the sender that with high assurance can be asserted to be genuine.

The valid values of this characteristic are:

* Required: Non repudiation features are required for the use case.
* Desired: Non repudiation features are desired for the use case.
* Not required: Non repudiation features are NOT required for the use case.

### Tampering detection

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

The valid values are:

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

# 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.

|  |  |  |
| --- | --- | --- |
| Characteristic | Value | Key Renegotiation |
| Differentiated Group Management | Not Required/Desired | - |
| Rate of group modification | Low | - |
| Need for cyphering | Not Required | - |
| Authentication of the source | Required | Medium/Low |
| Non-repudiation | Desired | Medium/Low |
| Tampering Detection | 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 cyphering since there is no sensible information being exchanged, although it requires authentication and tampering detection 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 tampering detection and authentication, the requirements in terms of key renegotiation are low, unless the serving PoS changes.

## 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.

|  |  |  |
| --- | --- | --- |
| Characteristic | Value | Key Renegotiation |
| Differentiated Group Management | Required | - |
| Rate of group modification | High/Medium | - |
| Need for cyphering | Not Required | - |
| Authentication of the source | Required | Medium/Low |
| Non-repudiation | Desired | Medium/Low |
| Tampering Detection | 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 cyphering is not needed. With respect to the authentication, non-repudiation and tampering detection, the same comments as in the previous use case apply.

## Configuration 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. One special case considered is the use of multicast group communication for firmware update on sensor networks.

|  |  |  |
| --- | --- | --- |
| Characteristic | Value | Key Renegotiation |
| Differentiated Group Management | Required | - |
| Rate of group modification | Medium/Low | - |
| Need for cyphering | Desired | High |
| Authentication of the source | Required | Medium/Low |
| Non-repudiation | Required | Medium/Low |
| Tampering Detection | 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 modification of configuration parameters require the maximum security. Cyphering can be required depending on what kind of parameters we are updating, for example if we are updating a media specific key or any sensitive parameter, we may want to opt for cyphering. The requirements in terms of authentication and tampering detection are the same as in the previous scenarios. In all cases the node source of the message must be authenticated in order to execute its commands. Finally in this case it is also desirable to have non-repudiation capabilities, since this enable the operator to account for failures or wrong commands.