Multicast Group Membership Management in Media Independent Handover Services

Carlos Guimarães[a,*], Daniel Corujo[a], Antonio de la Oliva[b], Yoshihiro Ohba[c], Rui L. Aguiar[a]

[a] *Instituto de Telecomunicações, Universidade de Aveiro, Portugal*
[b] *Universidad Carlos III de Madrid, Spain*
[c] *Toshiba Corporate R&D Center, Japan*

Abstract

Currently we are witnessing an explosion of devices able to connect to a variety of wired and wireless access network technologies. This connectivity is increasingly integrating networks composed by sensors, actuators and even utility devices that use private and public networks to relay important information and measurements. The deployment of the so-called Smart Grid technologies allied to the rise of Machine-to-Machine communications require new mechanisms to optimally manage the change of point of attachment to the network of these huge clouds of nodes, assisting in tackling the scale of the problem. With this problematic in mind, the IEEE 802.21 WG started on March 2012 a new project, named IEEE 802.21d, Group Management Services. This amendment establishes the required changes to the original specification, in order to manage the mobility of groups of nodes. This work follows closely the progress of the Task Group on the use cases, requirements and gap analysis, providing in addition a potential solution, integrating new group mechanisms, extensions to the MIH Protocol and associated security enhancements. This solution has been implemented and validated in a custom built testbed, with results showing that the utilisation of Group Control procedures through multicast signalling achieves a lower cost when compared with unicast signalling, in group handover and sensor information dissemination scenarios.

Keywords: IEEE 802.21d, Handover, Multicast, Group Management

1. Introduction

In the last years we have been witnessing the explosion of multi-mode connected devices that take advantage of different technologies, aiming to improve the connectivity options of terminals. Although the use of several technologies is not something new, its current use is limited, since terminals are only able to connect to well known hotspots preconfigured by the user, without further intelligence. In order to overcome this limitation, providing new mechanisms for network selection and information sharing, the IEEE published at the end of 2008 the IEEE 802.21 specification [1]. The IEEE 802.21 standard on Media Independent Handover (MIH) Services aims at improving user experience in mobile terminals by providing a set of services that will help optimise the handover between IEEE 802-based and cellular technologies. In 2012, two new amendments to the base specification were published. The IEEE 802.21a [2] providing security services and the IEEE 802.21b [3] extending the basic functionality of the standard to support downlink only technologies. While developing this last amendment, several comments were received from Smart Grid/M2M related forums, pointing out the lack of a specific feature, corresponding to the mobility management of not a single node, but groups of nodes, addressing the requirements posed by

*Corresponding author. Address: cguimaraes@av.it.pt

these new applications and use cases.

In order to tackle this requirement, the IEEE 802.21d Task Group (TGd) was created in March 2012. Although the applicability of the group management extensions is not limited to it, the main use case that triggered the IEEE 802.21d work was centred on the management of networks composed by large numbers of sensor/actuator networks. The operators of such networks require mechanisms able to scale with the number of nodes in order to e.g., handover portions of the network to a separate maintenance network, a perfect match for the group management features to be developed by the TGd.

Framed by the progress of the specification, this paper presents initial research providing a solution to the challenges posed by the new amendment. An initial description on motivation and background work is presented in Section 2, followed by an explanation of the role of IEEE 802.21d within the IEEE 802.21 WG in Section 3. The scenarios, requirements and gap analysis of missing features are presented in Section 4. Section 5 details the design of the proposed solution, specifying the new features developed and the different options that can be taken while addressing the problem space. Section 6 reports the results obtained from a prototype of the proposed solution developed over a real open-source IEEE 802.21 implementation for the purpose of this work, showing the pros and cons of using multicast communication in the concerned scenarios. Finally, the paper concludes with Section 7.

2. Related Work and Motivation

As explained in Section 1, the work performed at the IEEE 802.21d TG was initiated to specifically address the communication requirements (in terms of mobility control protocol) of applications scaling to thousands of nodes.

In the context of Smart Grid and Machine to Machine (M2M) communications, due to the diversity and extreme large scale properties of the network, the characteristics of the data and control traffic are not well known, increasing the complexity of managing mobility. Sample scenarios of the use of Smart Grid are the distribution of energy consumption measurements in a neighbourhood, where hundreds to thousands of nodes may send measurements once every e.g., 10 minutes [4]. In order to understand the magnitude of the problem being tackled, Table 1 presents the expected number of nodes that will be active in Japan households for different areas and number of nodes per household (M). As Table 1 shows, the number of nodes is expected to be very high, with ranges in the order of the thousands. This expected value is in line with other reports such as [5], where it is stated that the expected aggregated traffic in an IEEE 802.16p sector might scale up to 35000 devices.

These new use cases require a reliable connection, hence nodes must be continuously searching for the best possible connection, involving a handover of Point of Attachment (PoA) in the cases where the current connection is poor. Due to the large amount of nodes involved in the communication, Group Control has been identified as one of the key challenges for this kind of network [6]. Mobility management in this scenario has several major challenges. Basically, the signalling required to move portions of these networks to a different point of attachment might increase the delay in the medium (since several messages, scaling with the number of nodes, are sent) and may also impact the accuracy of the measurements being reported by the sensors. This implications will be further elaborated in Section 6.

In these scenarios, the usage of multicast traffic capabilities increases the scalability of group information dissemination traversing the network [7][8], particularly at the network layer. However, group dynamics incur stringent conditions in the access layer, such as when concentrations of users occurring due to large numbers of passengers commuting in trains or buses leave the coverage of a wireless network, and have to select and handover to other networks. As another example, [5] also accounts for situations where surges in network access from a large number of devices, motivated by an outage or an alarm event in the network, can generate up to 35000 access attempts over periods of 10 seconds, in large cities, having to

	Area (Km^2)	# of Households (in 2012)	Avg. # of nodes per sq.km M=1	M=5	M=10
Special Wards of Tokyo	622	4,547,435	7,311	36,555	73,110
Tokyo	2,629	6,403,219	2,435	12,175	24,350
Japan	377,900	51,950,504	137	685	1,370

Table 1: Foreseen number of nodes in Japan based on 2012 household data[1].

maintain a 99% access success rate. These situations typically generate handover selection opportunities that occur simultaneous to all entities, where each node egotistically tries to select the best network based on individual information. As these situations create performance degradation and network congestion, they raise the need for controlling mechanisms operating over wireless networks, such as handover management procedures aiming to optimise wireless connectivity, while maintaining the need for operating in a media independent way.

Group Control implies that the system supports group addressing and handling of devices as clusters, imposing the same behaviour to group of nodes. Solutions for this issue, however, have been mostly concerned with increasing the level of awareness of the concurrency for optimal network selection. In [9] a comparison between mobile terminal and network controlled approaches was done, showing that the later one allowed for lower delays and handover rejection rates. The authors of [10] used an enhanced Proxy Mobile IPv6 message which aggregated the mobility information of different 6LoWPAN-enabled sensors, to reduce the number of control messages over the air. Other solutions, such as [11], used Fuzzy Clustering Method for combining the status of available networks with traffic characteristics of the users, optimising network selection and reducing handover blocking probability.

Moreover, enabling Group Control of a massive number of devices requires several changes to the architecture of the protocols used, such as multicast operation, group membership management and control signalling. Changes to network attachment and connection management protocols may also be necessary [12], including novel security mechanisms to provide authentication and privacy to communications within groups [13]. The handover of groups of sensors has already been tackled in the literature with works such as [14], although they mainly focus on enabling the use of well known mobility protocols to clusters of nodes, leaving apart the group management and the use of multicast signalling for addressing the different handover control messages. In this context, the use of handover control mechanisms such as the ones provided by IEEE 802.21 are of special value, since they allow nodes in a network to roam across heterogeneous networks, with its capability to provide and control link parameters for handover execution. Although previous works have already explored the possibility of using broadcast mechanisms for disseminating MIH signalling, such as [15] [16], they use a similar approach to 802.21b, not considering the usage of handover control procedures directly with groups of nodes. Other approaches, such as [17] [18], relate multicast mechanisms and MIH signalling, but only with the objective of increasing the performance of multicast session handovers, and thus do not provide any means for group handover control. As such, these mechanisms do not provide any enhancements in terms of media independent Group Control, which are at the base of upcoming M2M deployment scenarios and requirements [18] [19]. It is important to understand at this point, that the use of multicast MIH signalling before IEEE 802.21d was just not possible, since the MIHF_ID space did not allow it. Hence, previous works focus on trying to circumvallate this problem, which will be solved in the

[1]Source of data: `http://www.metro.tokyo.jp/INET/CHOUSA/2011/02/60l2p200.htm`

future specification.

3. The role of IEEE 802.21d in the IEEE 802.21 ecosystem

Interworking and handover management across heterogeneous access network is a topic that has received a lot of attention in the last years, specially after the explosion in market penetration of multi-interfaced smartphones. Anticipating this trend, the IEEE 802 published at the end of 2008 the IEEE 802.21 specification. The IEEE 802.21 [20] [21] (or Media Independent Handover, MIH) technology is an enabler for the optimisation of handovers between heterogeneous IEEE 802 systems and between 802 and cellular systems. The goal is to provide the means to support and enhance the intelligence behind handover procedures, allowing vendors and operators to develop their own strategy and handover policies. For this purpose, IEEE 802.21 aims at improving handover procedures between heterogeneous networks by adding a technology independent function (Media Independent Handover Function, MIHF) which simplifies and abstracts the communication between different entities, either locally (mobile node, MN) or remotely (network functions).

Sharing information allows algorithms to provide seamless mobile node handovers while moving across different PoA and the establishment of standardised technology-independent services greatly simplifies algorithm design. The so-called Media Independent functionality is divided into Events (providing link layer information about the status of wireless connections), Commands (allowing the execution of configuration and handover related procedures at the link layers) and Information Services (enhancing handover decision processes with network configuration information). Through the usage of the MIH Protocol, information sharing becomes possible between remote entities which have executed an MIH Registration procedure with one another, using either Layer 2 (L2) or Layer 3 (L3) transport mechanisms.

However, uniform signalling was conceived considering unicast handover management only. The main objective of IEEE 802.21 was to manage the mobility of individual mobile terminals, hence the specific 802.21 identifiers, called MIHF_IDs (Media Independent Handover Function Identifiers), are defined for unicast or broadcast, without any support for addressing groups of nodes. In addition, although some broadcast mechanisms exist in the base specification, they only address MIH node discovery and capability exchanges, and not specifically the handover control signalling. Finally, the main specification does not consider the support of L2 or L3 native multicast transport.

Two different enhancement amendments have been released [2] [3], since the standard has been made available in 2008, with a third one on the way, focusing on single radio handover optimisations (IEEE 802.21c). Interestingly, 802.21b defines extensions to support downlink-only technologies, typically associated with massive broadcast mechanisms. However, the 802.21b evolutions to the signalling consist simply of relaxing the request/response mechanisms requirement of the original standard, for certain command messages. The group capabilities of this specification only provide mechanisms to select nodes receiving specific multimedia flows, identified by a certain URL. Hence, this approach is of no use for sending handover control messages, which are still limited to unicast destinations.

In this context, IEEE 802.21d was born to provide an answer to the industry of smart meters/actuators and M2M applications, providing a standardised way of dealing with the change of point of attachment of large groups of nodes. Although this functionality itself is already included in the product portfolio of the big players of this market, the lack of a standardised mechanism impacts negatively on the competence and possible deployment options of this technology. Hence, this new standard appears to fulfil a necessity identified by the market.

This situation set the stage for IEEE to create the 802.21d Task Group, addressing Group Management Solutions under scope of media independent handover mechanisms. In this work we

present an efficient solution to the 802.21d challenges, starting by describing its use cases and requirements, in the next section.

4. Furthering IEEE 802.21 With Multicast Signalling Capability

Taking the 802.21 architecture as described, in this section we focus on presenting the scenarios, requirements and missing features that highlight the lack of group management functionalities in IEEE 802.21.

4.1. Use cases

On its original design, IEEE 802.21 defines the signalling required by a control node located at the network (the so called Point of Service, PoS) to assist and manage a terminal handover process. As such, signalling was originally designed with a unicast point of view, in which the PoS establishes a peer to peer communication with the terminal. Currently, the importance of Smart Grid-like networks is growing and the technologies enabling their use are under heavy standardisation activities. Amongst the different problems tackled in the different standardisation fora, the issue of connectivity management is specially suited for IEEE 802.21 technologies, since a solution able to span through different technologies and access networks is required to ensure best connectivity for the network nodes. Due to this fact, within the IEEE 802.21 WG there have been several discussions regarding how to enable the use of MIH-based handover control for Wireless Sensor Networks (WSNs), whose characteristics are very different from traditional networks [22]. Within this scope, the key missing feature in order to address the connectivity management challenges of WSNs has been identified as the ability to control groups of nodes. The need of this feature is also acknowledged by other standardisation bodies as the Open Smart Grid[2], which defines on [23] the different use cases requiring group communication capabilities. Handover control for groups of nodes in IEEE 802.21 has several advantages over the base line specification for WSN networks:

- **Reduced signalling load:** IEEE 802.21 follows a request/response model for its signalling exchanges. This means that for every command sent to the nodes, a response is required. Hence, in the most simple handover case that requires just the exchange of one command for its execution, every node needs to reply this message. This creates not only extra-saturation in the air interface but also in the network connecting the access network to the PoS, a fact that is exacerbated when hundreds of nodes are addressed. A more detailed analysis of the gain obtained by using group communication for this case can be found in Section 6.2.

- **Reduced complexity in the PoS:** In the case multicast signalling is used, the PoS must maintain a separated message transmission state machine for each transaction. The result of this is higher memory and processing requirements in the PoS, which can be solved by introducing group communications, since with a single transaction all nodes in the network can be addressed.

- **Impact on the reliability and timeliness of data transmitted in the sensor network:** As analysed in Section 6.4, in case unicast signalling is used, the wireless medium must support the burden of the signalling required for the handover. Although the amount of bandwidth required for this signalling is not very high (in the magnitude of hundreds of Kbps in the case of 1000 nodes), the fact of having the channel busy with transmitting the control messages impacts the WSN by increasing the delay of the data packets in the network. Depending on the purpose of the network, this might have an impact on the reliability and timeliness of the network measurements.

Hence, taking as base these ideas and the use cases identified by the industry, the IEEE 802.21d TG has defined its own set of use cases and scenarios, highlighting the new features to be included in the standard. Hence, the TG document [24] iden-

[2] `http://www.opensg.org/`

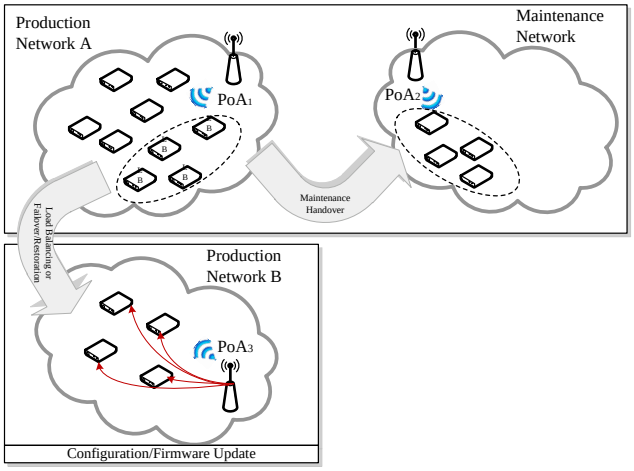

Figure 1: IEEE 802.21d Use Cases

tifies the following handover use cases to be tackled by the IEEE 802.21d solution: *i)* load balancing, *ii)* failover/restoration, *iii)* maintenance, as well as *iv)* configuration/firmware update, which are shown in Figure 1, and detailed next.

4.1.1. PoA Load Balancing

PoA Load Balancing may be required in order to free resources in the PoA serving the sensor network, hence decreasing its load and consequently reducing the probability of losing important measurement information from the nodes. The PoA may be overloaded due to a sudden request for information from the control centre or just because too many nodes are attached to it due to e.g., a failure in another PoA. The need of this scenario is already presented in the literature, identifying specific problems to wireless sensor networks, such as the *hot spot problem*, where nodes with a better channel quality to the sink manifest a faster battery depletion in nodes, since they become overloaded with traffic from the rest of the network [25]. Another example of such a scenario is provided in [12], where the access conditions at a WLAN hotspot degrade rapidly when a group of users starts to broadcast and receive video traffic. With available access alternatives in the vicinity, a network decision point can issue a handover command towards part of the users, moving them to another hotspot (or even to another technology due to the media independent capabilities of 802.21), balancing the load in the network area.

There are several advantages when comparing group control with per-node control for load balancing scenarios. On the one hand, the generation of a single message able to address a group of nodes does not further burden the network with more signalling overhead. On the other hand, sending individual handover commands for load balancing, and respectively waiting for their responses after the handover has been executed, can delay the load balancing convergence process (i.e., the rate at which the nodes are being balanced can be lower than the rate at which the load in the AP increases). Figure 1 illustrates such a scenario, where a subset of MNs/sensors attached to Production Network A execute a handover towards Production Network B, for load balancing purposes.

4.1.2. Failover/Restoration

The second example, Failover/Restoration, corresponds to a forced handover being triggered due to a failure in the PoA, generally forcing the whole sensor network to hand off to a second PoA in order to keep connectivity. Similar to the previous scenario in Figure 1, the network controlling framework would benefit as well from existing IEEE 802.21 events (i.e., *MIH_Link_Going_Down.indication*) signalling that PoA_1 is shutting down due to a failure, triggering a handover of the affected MNs/sensors towards Production Network B. Incrementally, the reverse scenario is also enhanceable with IEEE 802.21 signalling, with the network controlling point able to receive events about PoA_1 being back on-line and detected by the MNs/sensors (i.e., through *MIH_Link_Detected.indication* events) as well as using the novel multicast signalling to handover the group of nodes back to Production Network A.

Here, the benefits of sending group commands are incrementally important, since only a single handover command is required to reach nodes connected to a PoA in imminent failure: when a fault is generated, the opportunity window to have the network react and maintain node con-

nectivity can be very small, and not long enough to support a sequence of individual commands towards each node.

4.1.3. Maintenance

Another usage example is the handover of portions of the MN/sensor network to a secondary maintenance network, in order to perform management operations, as shown in Figure 1. Akin to the previous handover situations, a group of selected nodes can simultaneously be instructed to handover towards a separate network where they can safely be subjected to maintenance procedures without affecting a production network (i.e., maintain information generating nodes without having to re-configure or re-calibrate sink nodes). In respect to the necessary support procedures, unicast events and commands could be used to have the nodes alert the network about maintenance needs (i.e., through a *MIH_Link_Parameters_Report.indication*), and to have the network controlling the handover procedures of each node independently.

Depending on the various situations that have the MNs/sensors require maintenance, different time constraints can be at stake as well in this kind of scenarios, with group signalling reducing the amount of messages required for the handover of the group of nodes towards the maintenance network, as well as the duration of the handover command sending procedures.

4.1.4. Configuration/Firmware update

Finally, a last example considers the use of IEEE 802.21 extensions to indicate to a sensor network that a change of configuration parameters or even a firmware update is available, such as in the *Open Mobile Alliance Device Management* protocol [26]. As shown in Figure 1, when a configuration or firmware update becomes available and affects a group of users, group commands can be used to convey this information simultaneously to all nodes. This not only simplifies the process of managing the update process (i.e., account for update actions for groups of users instead of individual users), as well as reducing the amount of information traversing the network for carrying the same information multiple times.

In addition, by integrating as well the IEEE 802.21 handover operations, optimisation procedures become available for moving the nodes into a network able to offer a greater performance for the configuration and firmware transfer.

4.2. Challenges

The previous section presented the scenarios and use cases being considered within the IEEE 802.21d TG. This section highlights the main challenges to be addressed in order to efficiently support such examples at the MIHF level. Currently four main areas of work have been identified, closely tied with multicast communication concepts:

- **Group addressing mechanisms:** The base IEEE 802.21 standard defines an unique identifier, called MIHF_ID, which identifies the source or destination of an MIH message. The current base specification has two modes of addressing within the MIHF identifiers space. It supports unicast addressing, where a message contains an MIHF_ID corresponding to the intended receiver of the MIH message, and supports the so called zero-length MIHF_ID. Messages addressed to the unicast MIHF_ID will be discarded by a receiving MIHF to which the unicast MIHF_ID does not belong to, while the zero-length MIHF_ID behaves as a broadcast wildcard, enabling any receiving MIHF to process a sent message. The group addressing mechanisms required by IEEE 802.21d are more complex than the ones already defined, hence we advocate for the creation of a new subspace of the current MIHF_ID space. This new multicast space must be compatible with the current MIHF_ID definition but the identifiers belonging to it must be clearly distinguishable from the unicast ones. In this way, destination groups can be clearly distinguishable and MIH Users will be able to identify groups of destinations by using standard MIHF formatted IDs.

- **Group management mechanisms:** In the current specifications there is no mechanism in place for group-management, since the concept of group is non-existent. In order to provide Group Management functionalities, new mechanisms enabling MIHFs to join and leave groups in a secure and authenticated way, must be designed.

- **Required changes to the MIH protocol:** The current specification defines a protocol based on request/response transactions. This model of communication is not the most suitable for multicast transmission and that is the reason why IEEE 802.21b defined a new handover command that does not require reply. Although basic support for multiple responses to a request message is already included in the main 802.21 specification, per-recipient response handling and accounting in multiple response transaction is not implemented. This is one of the major changes required from the 802.21 state machine point of view.

- **Security extensions:** The base IEEE 802.21 specification does not define any security mechanism, with all security related procedures specified in IEEE 802.21a. Basically, this amendment provides solutions for mutual authentication between a MN and a PoS, as well as protection of MIH messages, but considering in all cases a one-to-one communication between the MN and the PoS. Hence, new security mechanisms tailored for multicast communication must be defined. Moreover, in cases such as the firmware/configuration scenario updates, extra security mechanisms must be in place in order to avoid compromised firmware or unauthorised settings to be installed in sensor nodes.

4.3. Requirements

Building on the use cases and problems provided in previous sections, in the following we present the main requirements identified for a full IEEE 802.21d [27] solution:

R1 **Multicast Communication and Transport**: The solution shall support the exchange of MIH primitives between an MIHF located at a PoS and a group of MIHFs, using already established L2, L3 or application layer multicast mechanisms, in a transparent way for the MIH Users.

R2 **Addressing**: The solution shall provide an addressing mechanism suitable for identifying a group (i.e., a multicast MIHF_ID).

R3 **Group Management**: The solution shall provide functionalities for managing groups of nodes. These functionalities include the creation/destruction of groups, join and leave operations and modifications to the group subscription

R4 **Security Requirements**: The solution shall provide mechanisms to perform authentication, confidentiality and integrity protection at the receiving node.

In the following we present the key concepts behind our proposed solution to these challenges.

5. MIH Group Membership Mechanism

In order to explore the concept of multicast-enabled signalling for media independent handover support, we have conceived a framework that enhances the existing MIHF behaviour and integrates new mechanisms to address the problems and requirements identified in Section 4.

5.1. Group Addressing Mechanisms

In our framework, we reuse MIHF identifiers as the means for identifying MIH-enabled multicast groups. An identifier is used as the destination parameter for multicast 802.21 protocol messages, which are shared by all multicast 802.21-enabled nodes belonging to that group. In this way, besides its own MIHF identifier, a node can be associated to several multicast groups, each with its own multicast MIHF identifier (see Figure 2). As such, whenever an 802.21 message is sent to that group, all member nodes receive it, as long

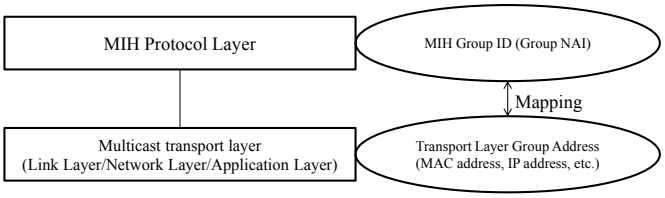

Figure 2: Relation between multicast identifiers at different layers of the protocol stack

as the multicast route has been previously setup in the routers along the way. In order to support that, whenever a node joins a MIH-enabled multicast group, it relies on already existing multicast procedures at the mobile node, triggering a IGMP or MLD message (if IPv4 or IPv6 is being used, respectively) towards its access router, or any L2 multicast mechanism if adequate. Following this approach, the interaction with multicast procedures are based on already existing multicast tree establishment and reconfiguration mechanisms, and do not incur any added operations affecting scalability at involved multicast routers. At the same time, the node is still able to receive unicast messages sent to its unique MIHF_ID.

5.2. Group Management Mechanisms

In order to control and to support the reception of multicast 802.21 signalling, our framework employs group membership management mechanisms. We assume three possible solutions for group management control in a multicast-enabled MIH framework, which are depicted in Figure 3, and described in the following sub-sections. In Section 6.3, we evaluate the cost of executing the different group management alternatives.

5.2.1. Unicast Network-Initiated Group Management Command

Using a new set of 802.21 protocol group management messages (network-initiated request), a PoS is able to command the creation, joining, leaving and destruction of multicast groups. Such messages carry multicast MIHF identifiers towards individual mobile nodes, enabling them to execute the necessary underlying multicast procedures, and individually relaying a response back to the PoS, indicating the outcome of the command (Figure 3a).

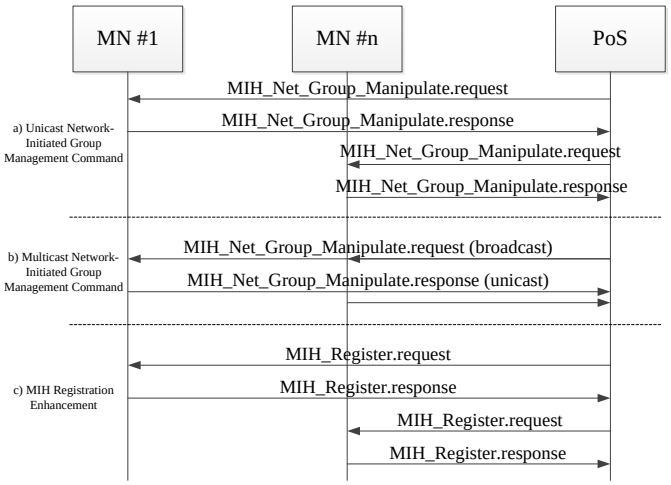

Figure 3: Group Management Mechanisms Signalling

5.2.2. Multicast Network-Initiated Group Management Command

This method is similar to the previous one, but this new group management command is sent using existing 802.21 broadcast mechanisms (network-initiated request). The multicast group management command uses the zero-length MIHF_ID as destination, which is able to reach all MIH-enabled nodes in broadcast range. Each node that receives the request replies in a unicast way (Figure 3b). This command also comes coupled with a list issued by the PoS, indicating the intended multicast group for each mobile node. This, of course, still requires the unicast Register phase to occur (i.e., the PoS needs to be made aware of each mobile node specific MIHF_ID).

5.2.3. MIH Registration Enhancement

The interaction between two MIH-enabled nodes requires that they register with one another. This approach can be enhanced by including in the *MIH_Register.request* message, sent by the PoS, the multicast group(s) for the recipient to join (Figure 3c). This enhancement is independent of using a unicast or a multicast join method, because it is done at the MIH registration phase, which is required in both methods.

5.3. Enhancements to the MIH protocol operation mode

The MIH protocol is based on request/response transactions, relying on a set of state machines

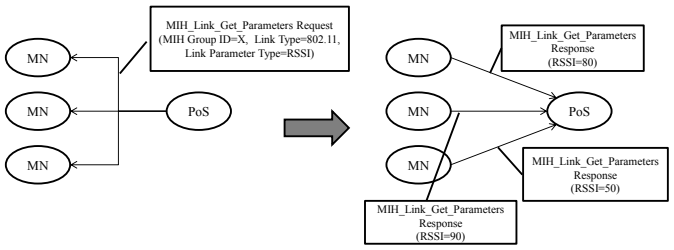

Figure 4: Example of the use of multicast request and multiple unicast responses

to manage them. These are unable to distinguish multicast messages from regular broadcast messages, which are typically used for MIH discovery procedures. Moreover, due to the request/response mechanism, the different multiple targets of a multicast request message sent by the PoS need to send their individual responses using unicast, generating different message exchanges. As such, in our framework, the state machines were enhanced to support multicast signalling, and matching of unicast responses to multicast requests. To illustrate this idea, Figure 4 presents an example of the use of a multicast request message to gather information regarding the link quality of a network of nodes, while the reporting is performed using unicast responses.

Note that not all of the existing 802.21 standard messages make sense in multicast environments, with several messages including parameters that target individual nodes. However, we verified that all commands which are not originated on the MN or the PoA are able to be used in a multicast way, which fits perfectly with the IEEE 802.21d scenario where the PoS is always the source of the multicast messages. Commands triggering specific actions in the destination, such as *MIH_Link_Get_Parameters* and *MIH_Link_Configure_Thresholds* messages, may be useful to be sent in multicast, but still require the indication of the link identifier of the destination, which makes no sense while using multicast communication. So we propose the definition of a generic link identifier (e.g., per technology) in order to take advantage of these commands requiring specific link identifiers.[3]

Moreover, the group operation capability added to the PoS enables it to interact with other network-based link admission control mechanisms, allowing it to not only support but actually enhance strategies for assisting Group Control scenarios. For example, in order to avoid having multiple nodes associating simultaneously after a handover, our primitives can be coupled with the definition of a random time after which the group performs the handover, allowing a back-off mechanism. The flexibility added by 802.21 node design allows it to be integrated into different kinds of solutions.

Finally, when connecting to a PoA, nodes can actively select for a multicast-supporting network, based on discovery and MIIS info, knowing that they will need to support multicast, and help the network in optimising control traffic. In this way, the *MIH_Capability_Discover* messages and the MIIS were extended in our solution to provide this information to the nodes, by adding new parameters and Information Elements identifying their multicast capability. We restrict the multicast delivery to occur unidirectionally, having the network PoS acting as the multicast tree source towards the mobile nodes. Bi-directional multicast trees are known to pose complex issues, particularly when mobile nodes are involved, and are not needed for the scenarios addressed in TGd.

5.4. Security Enhancements

Regarding the security aspects of the solution, the TGd has identified three main issues to tackle; *i)* key management, *ii)* encryption and *iii)* authentication. This work focuses on the modifications to the messages required to carry the security payload and on studying the suitability of several well known cypher suites for the scenario being analysed. Hence, key management functionality is out of the scope of this paper. Security in the IEEE 802.21 specification has been tackled by the IEEE 802.21a amendment [2]. As such, for backward compatibility, we propose to extend

[3]The proposed generic link identifier is based on a generic Link Type which can be used as a wildcard. For more information please refer to [28]

MIH header (S=1)	Source MIHF Identifier TLV	Destination MIHF Identifier TLV	SAID TLV	MIH service specific TLVs Security TLV (Encrypted payload)	Security TLV (Authentication payload)

Figure 5: Protected MIH PDU

the secure message format defined by the security amendment to include an optional signature which can be used for authenticating the messages. The proposal message format is presented in Figure 5. Through the use of this extended message format, the PoS controlling the multicast communication is able to secure and authenticate the communication with the nodes. Section 6.5 is focused on comparing the requirements in terms of memory and CPU time required for different cyphering suite options.

6. Framework Evaluation

In order to evaluate the feasibility of our multicast-enabled 802.21 framework, we modified the ODTONE[4] open-source IEEE 802.21 implementation [29] according to the proposals in Section 5, and used this as a tool for performance comparison.

6.1. Scenario description

Our evaluation scenario was built over the AMazING wireless network testbed [30], located on the rooftop of the Instituto de Telecomunicações building. As can be seen in Figure 6, a set of 10 physical wireless mobile nodes, connected to one of two possible wireless PoAs, were deployed. Each PoA served a different IP network and was, in turn, connected to a third network where the handover-controlling PoS was situated. For both the multicast and unicast cases, the scenario consists of a handover preparation signalling exchange between the PoS and the MNs, which are moved between Network A and Network B.

The proposed multicast signalling is depicted in Figure 7. The procedure assumes that the mobile nodes have joined the multicast group using the enhanced MIH Register procedure described in Section 5.2.3. This procedure was selected,

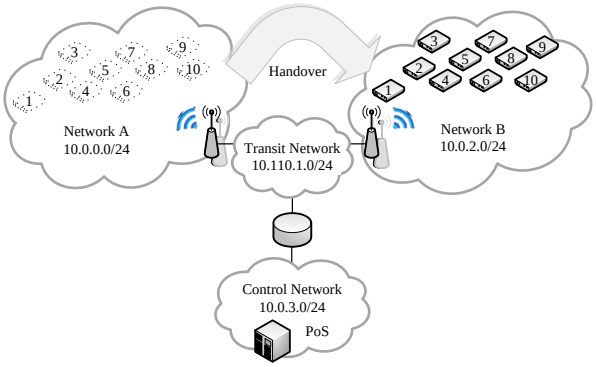

Figure 6: Handover Evaluation Scenario

since it is shared by both unicast and multicast cases, simplifying their performance comparison. Moreover, for this section we are not addressing security since the size of the key and the cypher mechanism will change the size of the messages. As such, our results present a lower bound, and assume that an authentication phase has already occurred. The security overhead evaluation is presented in Section 6.5.

The experiment relates to having the MNs (e.g., sensor nodes) handover to another PoA, for load balancing reasons or to connect with a better signal to the network. This work focuses on the required handover signalling and, as such, does not explore the triggering conditions. When such a trigger occurs, the PoS sends to all nodes the primitive *MIH_Net_HO_Bcst_Commit.indication* (message 1 in Figure 7). This message, belonging to the IEEE 802.21b amendment, is used to broadcast the handover commit command to all nodes, without requiring a response message. In our work, we have implemented this message in ODTONE and extended its behaviour to reach the nodes subscribed to a multicast group. When the mobile nodes receive this message, they initiate the handover procedures and send a *MIH_MN_HO_Complete.request* message (message 2 in Figure 7) back to the PoS, indicating handover completeness. The PoS collects the messages from all the nodes, and issues an *MIH_MN_HO_Complete.response* (message 3

[4]Open Dot Twenty ONE - `http://atnog.av.it.pt/odtone`

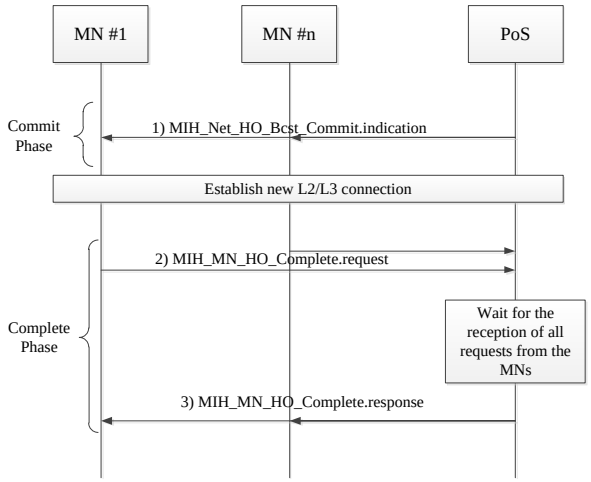

Figure 7: Evaluated Multicast Signalling

in Figure 7) in multicast as a response.

For the unicast case, the signalling structure remains the same. However, all messages for the handover phase are sent in unicast and require a request/response mechanism between the PoS and all nodes.

Regarding the size of the MIHF_IDs, the evaluation scenario considers 3 bytes for the MIHF_IDs of the mobile nodes and PoS, and 12 bytes for the multicast group, out of a maximum of 253 bytes allowed by the 802.21 standard. Note that the presented results are affected by the size of the messages sent, hence the results are sensible to the length of the MIHF_IDs used.

To avoid all MNs performing the handover at the same time, the MIH protocol allows the definition of a time interval, which the MNs use to calculate a random delay before starting the handover (in all experiments this value is 100ms). Each physical node is configured with a VIA Eden 1GHz processor with 1GB RAM, a 802.11a/b/g/n Atheros 9K wireless interface, and a Gigabit wired interface. Each node runs the Linux OS (Debian distribution) with kernel version 3.2.0-2-686-pae, with ODTONE installed. Each experiment was run 100 times, showing here averaged results.

6.2. Handover Control Signalling Comparison

This test aims to study the footprint of the proposed multicast signalling, making a comparison with its unicast version. For brevity, we focus on the measurement of the amount of data exchanged and the total time required. All the analysis performed regarding signalling costs is presented collapsed in Figure 8, due to space constraints.

The experimental results for the amount of information exchanged in multicast and unicast signalling is depicted in the lines denoted as "Total signalling cost" in Figure 8, which represents the overhead caused by the MIH signalling. These values consider not only the size of the MIH protocol but also the size of the UDP and IP headers. As can be seen, for an increasing number of mobile nodes, the amount of bytes from the multicast signalling required to control the handover is less than the unicast signalling. Concretely, for a single node, the difference is of 61 bytes, increasing to ≈2Kb for 10 nodes and to ≈213Kb for 1000 nodes (values for 100 and 1000 nodes have been analytically computed, hence they are not shown in the graphs). Multicast signalling also increases with the amount of mobile nodes, due to the existence of unicast messages in the signalling scenario, such as message 2 of Figure 7. On the other hand, multicast gains are justified with the fact that the *Commit Phase* (message 1 in Figure 7) is not affected by the number of MNs that perform the handover, since the request is sent in a single multicast message and there are no responses messages. Also, the use of a single multicast complete response message reduces by half the value of the *Complete Phase* (messages 2 and 3 in Figure 7) when compared with the unicast. As such, for the whole scenario, the multicast signalling accounts for 66 percent of the whole exchange for a single node, but with the increase of the number of nodes it becomes insignificant (≈2 percent and 0.2 percent for 100 and 1000 nodes).

As referred previously, these values do not consider the layer 2 size, however, the technology used also impacts the amount of information exchanged. If we assume the handover of 1000 MNs to be performed over WiFi, we will get a total size of 434Kb for the unicast signalling and 112Kb multicast signalling. Moreover, using Ethernet, the total exchanged information will be 346Kb for

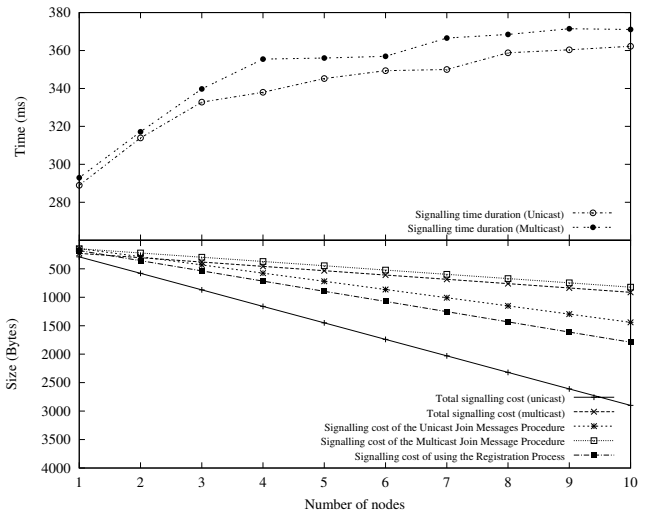

Figure 8: Evaluation of the different group management mechanisms and their comparison with unicast

unicast and 90kb for multicast.

The plots denoted as "Signalling time duration" in Figure 8 present the total time required to complete each type of signalling. Although the multicast signalling requires less information, it demands more time to complete the handover procedure of all MNs. The reason for this behaviour is the waiting period (proportional to the number of nodes) implemented in order to send message 3 in Figure 7, as well the lower bit rate associated with wireless multicast transmissions [31]. Moreover, these times are significantly increased by the L2/L3 handover procedure, which takes most of the total time. For a single MN it takes about 95% and 76% for 10 MNs.

6.3. Group Management Signalling Impact

In this section we assess the cost of the Group Management signalling procedures required to have the mobile nodes join the multicast group, enabling the multicast 802.21 handover signalling. The lines denoted as "Signalling Cost" in Figure 8 present a comparison of the three methods proposed in Section 5.2.

Analysing the results, we can observe that the enhancement of the MIH registration is the procedure that requires more information exchange. However, this procedure is a special case since only 25.7 percent of the information is related with the group management, while the remaining is related with the normal MIH registration procedure.

Comparing the unicast and the multicast join command procedures results, the unicast requires the exchange of more information than the multicast (except for a single node), mostly due to the fact that the unicast procedure requires that a different request message is sent to each node, contrary to the multicast procedure that only sends a unique multicast message. In both cases, the MNs reply to the join command and, therefore, the multicast procedure only saves bytes in the request message.

As described in Section 5.2, the multicast join procedure enables the PoS to request several nodes to join a multicast group by specifying their MIHF_IDs in the message. Considering the MIHF_IDs used, the maximum number of MIHFs that can be handled in just one message is 356 and 363 for UDP and L2 respectively.

6.4. Large-scale Group Control Impact

We also aim at measuring the impact that large-scale Group Control signalling operations have as transients in the network. For this, each node was configured to periodically send *MIH_Link_Parameters_Report.indication* messages to the PoS, every 100ms in average. This considers the case of sensors providing periodic sampling of a certain magnitude to the PoS, which is in front of a potential sink node. Meanwhile, the PoS also acts as handover management entity, requesting several nodes to move to another network every 5 seconds. This exemplifies a situation with highly dynamic network conditions, with the PoS making sure that the mobile nodes are always connected to the optimal wireless PoA. This experiment was performed using the unicast and the multicast signalling, for comparison.

Figure 9 shows the delay between events received in the PoS. The vertical dashed lines illustrate the time moments where the handover procedures were triggered. As can be seen, the proposed multicast procedure does not affect the delivery of the

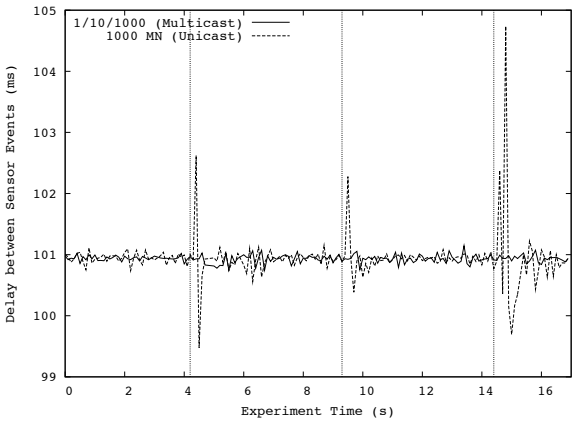

Figure 9: Handover Control Signalling Impact on Event Reception Delay

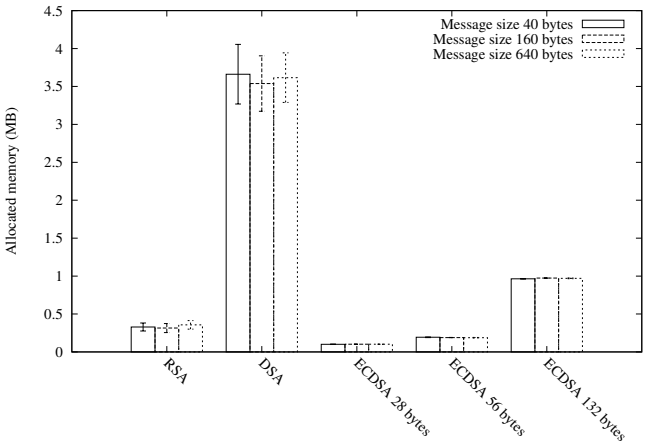

Figure 10: Memory allocation for signature generation and verification of a multicast MIH message

MIH_Link_Parameters_Report.indication message, as the unicast does. Independently of the number of nodes that perform the handover, the multicast handover procedure requires only a single message to be sent, thus causing no impact in the delay of the event messages reception. In contrast, the unicast procedure needs to send a different message to each node involved in the handover, creating overhead in the network and affecting the periodic reports from the remaining nodes. Its impact in the periodic is clearly visible if a large number of nodes (1000 MNs) is moving.

The effect observed in Figure 9 represents a good example of the benefits that an approach such the one being designed in IEEE 802.21d can bring to the management of large networks. While a unicast control approach has a noticeable impact on the system, e.g., the measurement transmission is being delayed, the multicast control does not produce any negative impact on the network performance.

6.5. Security Overhead

To evaluate the impact of using the proposed security mechanisms, we measured the processing time and the amount of memory required to perform the signature generation and signature verification of a multicast MIH message, using the most popular digital signature algorithms such as RSA, DSA and ECDSA. For taking the results related with the amount of allocated memory we used the Valgrind[5] software tool. In addition, and since one of the use cases is the management of networks composed by large numbers of sensor/actuator, we measured the impact of the proposed security mechanisms in low-power devices. For this, we setup a scenario different from the one described in the section 6.1, on which we used a RaspberryPi (Model B rev 2) to perform signing and verification of multicast MIH messages using RSA, DSA and ECDSA algorithms. The RaspberryPi is composed by an ARMv6 running at 700Mhz with 512MB RAM.

The results regarding processing time are depicted in Table 2, while the results regarding memory allocation are presented in Figure 10. The measurements for the ECDSA algorithm take into account different signature sizes, ranging from 28 bytes to 132 bytes. However, due to the similarity of results we present only a subset of all obtained experimental values.

Analysing the results, we can observe that the processing time and memory allocation is not affected by the message size. Results show that the ECDSA algorithm, for a signature size of 28 bytes, is the fastest message signing algorithm (about 8.65 ms), while the RSA is the algorithm that requires less processing time to verify a message (about 2.47 ms). A common characteristic of all

[5]http://valgrind.org/

Table 2: Processing time (ms) for signature generation and verification of a multicast MIH message

Operation	Algorithm		Message Size		
			40 bytes	160 bytes	640 bytes
Signing	DSA		24.52 ± 0.44	24.37 ± 0.41	24.42 ± 0.12
	RSA		59.55 ± 0.28	59.40 ± 0.23	59.78 ± 0.41
	ECDSA	28 bytes	8.48 ± 0.28	8.64 ± 0.21	8.74 ± 0.23
		56 bytes	25.23 ± 0.76	25.49 ± 0.36	25.39 ± 0.42
		132 bytes	582.98 ± 13.48	569.00 ± 14.56	581.03 ± 12.76
Verification	DSA		27.45 ± 1.03	27.11 ± 0.43	27.17 ± 0.18
	RSA		2.42 ± 0.04	2.47 ± 0.04	2.53 ± 0.06
	ECDSA	28 bytes	12.13 ± 0.20	12.24 ± 0.16	12.25 ± 0.17
		56 bytes	50.47 ± 0.58	50.80 ± 0.97	50.79 ± 0.53
		132 bytes	779.00 ± 2.87	778.92 ± 4.05	776.21 ± 2.60

algorithms, besides the RSA algorithm, is that the the computation time needed for the message signing is higher than the time required to verify the authenticity of the message's sender, which fits our scenario where the signing entity is the PoS (with typically less CPU constraints than the sensor nodes). In terms of memory allocation, ECDSA is the algorithm with the lowest signature key size, needing about 97.3 Kbytes to generate and verify the signature of a single message, being the algorithm that requires less memory. On the other hand, the most memory demanding algorithm is the DSA, requiring about 3.46 Mbytes to compute and to verify the message's signature.

The size of the elliptic curve of the ECDSA algorithm defines the complexity of computing the signature. Thus, with the increase of the signature size in the ECDSA algorithm, the computational overhead, in terms of processing time and memory for signing and verification operations, also increases, having an higher impact for signatures sizes of 96 and 132 bytes.

Comparing the ECDSA algorithm with the RSA, the principal advantage of ECDSA is that it offers equivalent security for a smaller key size [32] and, therefore, allows a reduction on the processing overhead, which may be crucial when low-power devices are considered. Moreover, ECDSA is able to provide smaller signature sizes when compared with RSA and DSA algorithms, reducing the overhead introduced in the transmission of authenticated multicast MIH messages.

7. Conclusions and Future Work

The work presented in this article has been framed by the challenges present in recent standardisation activities within IEEE 802.21d. After the identification of key requirements to support common use cases, the work delves into a first version of a proposal to address these challenges, and provides a thorough performance analysis of the different approaches that can be used in order to support complex scenarios with sensor networks, and provide Group Management capabilities within the constraints of IEEE 802.21. This paper shows the benefits that this solution brings in terms of network performance, efficiency and security impact.

Acknowledgement

This work has been partially funded from the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project), and by the project Cloud Thinking (CENTRO-07-ST24-FEDER-002031), co-funded by QREN, "Mais Centro" program. The work of Antonio de la Oliva has also been funded by the Spanish Government, MICINN, under research grant TIN2010- 20136-C03.

References

[1] LAN/MAN Committee of the IEEE Computer Society, IEEE Std 802.21-2008, Standards for Local and Metropolitan Area - Part 21: Media Independent Handover Services, 2008.

[2] LAN/MAN Committee of the IEEE Computer Society, IEEE Std 802.21a-2012, Standards for Local and Metropolitan Area - Part 21: Media Independent Handover Services Amendment for Security Extensions to Media Independent Handover Services and Protocol, 2012.

[3] LAN/MAN Committee of the IEEE Computer Society, IEEE Std 802.21b-2012, Standards for Local and Metropolitan Area - Part 21: Media Independent Handover Services Amendment for Extension for Supporting Handovers with Downlink Only Technologies, 2012.

[4] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, W. H. Chin, Smart grid communications: Overview of research challenges, solutions, and standardization activities, Communications Surveys Tutorials, IEEE 15 (1) (2013) 21–38. doi:10.1109/SURV.2011.122211.00021.

[5] Himayat, N., Talwar, S., Johnsson, K., Andreev, S., Galinina, O., Turlikov, A., Proposed 802.16p Performance Requirements for Network Entry by Large Number of Devices, iEEE 802.16 C80216p-10/0006 (2010).

[6] G. Wu, S. Talwar, K. Johnsson, N. Himayat, K. D. Johnson, M2m: From mobile to embedded internet, Communications Magazine, IEEE 49 (4) (2011) 36–43.

[7] H. Boujelben, O. Gaddour, M. Abid, Enhancement and performance evaluation of a multicast routing mechanism in zigbee cluster-tree wireless sensor networks, in: Systems, Signals Devices (SSD), 2013 10th International Multi-Conference on, 2013, pp. 1–8. doi:10.1109/SSD.2013.6564164.

[8] C.-H. Feng, W. Heinzelman, Rbmulticast: Receiver based multicast for wireless sensor networks, in: Wireless Communications and Networking Conference, 2009. WCNC 2009. IEEE, 2009, pp. 1–6. doi:10.1109/WCNC.2009.4917931.

[9] S. Lei, T. Hui, H. Zheng, Group vertical handover in heterogeneous radio access networks, in: Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd, 2010, pp. 1–5. doi:10.1109/VETECF.2010.5594539.

[10] Y.-S. Chen, C.-S. Hsu, H.-K. Lee, An enhanced group mobility protocol for 6lowpan-based wireless body area networks, in: Wireless Communications and Networking Conference (WCNC), 2013 IEEE, 2013, pp. 1003–1008. doi:10.1109/WCNC.2013.6554701.

[11] L. Ning, Z. Wang, Q. Guo, K. Jiang, Fuzzy clustering based group vertical handover decision for heterogeneous wireless networks, in: Wireless Communications and Networking Conference (WCNC), 2013 IEEE, 2013, pp. 1231–1236. doi:10.1109/WCNC.2013.6554740.

[12] D. Corujo, S. Figueiredo, R. L. Aguiar, Media-independent multicast signalling for enhanced video performance in the MEDIEVAL project, in: IEEE Future Network & Mobile Summit (FutureNetw), 2011, pp. 1–9.

[13] P. Sakarindr, N. Ansari, Security services in group communications over wireless infrastructure, mobile ad hoc, and wireless sensor networks, Wireless Communications, IEEE 14 (5) (2007) 8–20.

[14] A. J. Jabir, S. K. Subramaniam, Z. Z. Ahmad, N. A. W. A. Hamid, A cluster-based proxy mobile ipv6 for ip-wsns, EURASIP Journal on Wireless Communications and Networking 2012 (1) (2012) 1–17.

[15] M. Wetterwald, T. Buburuzan, G. Carneiro, Combining mbms and ieee 802.21 for on-the-road emergency, in: ITS Telecommunications, 2008. ITST 2008. 8th International Conference on, 2008, pp. 434 –438. doi:10.1109/ITST.2008.4740301.

[16] T. Buburuzan, G. May, T. Melia, J. Modeker, M. Wetterwald, Integration of broadcast technologies with heterogeneous networks - an ieee 802.21 centric approach, in: Consumer Electronics, 2007. ICCE 2007. Digest of Technical Papers. International Conference on, 2007, pp. 1 –2. doi:10.1109/ICCE.2007.341356.

[17] I.-S. Jang, W.-T. Kim, Y.-J. Park, An efficient mobile multicast mechanism based on media independent handover, in: Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, 2009, pp. 501 –505. doi:10.1109/MICC.2009.5431610.

[18] S. J. Koh, M. Gohar, Multicast handover agents for fast handover in wireless multicast networks, Communications Letters, IEEE 14 (7) (2010) 676 –678. doi:10.1109/LCOMM.2010.07.100558.

[19] ETSI TS 102.690 V1.1.1, Technical Specification Machine-to-Machine communications (M2M); Functional architecture, 2011.

[20] A. De La Oliva, A. Banchs, I. Soto, T. Melia, A. Vidal, An overview of IEEE 802.21: media-independent handover services, IEEE Wireless Communications 15 (4) (2008) 96–103.

[21] S. Das, M. Tauil, Y. Cheng, A. Dutta, D. Baker, M. Yajnik, D. Famolari, et al., IEEE 802.21: Media independent handover: Features, applicability, and realization, IEEE Communications Magazine (2009) 113.

[22] Z. Zhou, X. Xiang, X. Wang, J. Pan, A holistic sensor network design for energy conservation and efficient data dissemination, Comput. Netw. 55 (1) (2011) 131–146. doi:10.1016/j.comnet.2010.08.002. URL http://dx.doi.org/10.1016/j.comnet.2010.08.002

[23] SG-Network committee, Smart Grid Networks System Requirements Specification, release Version 5 (2013).

[24] A. de la Oliva, D. Corujo, C. Guimaraes, Use case Reference for TGd, https:

//mentor.ieee.org/802.21/dcn/12/21-12-0090-01-MuGM-use-case-reference-for-tgd.docx (July 2012).

[25] D. Puccinelli, M. Haenggi, Arbutus: Network-layer load balancing for wireless sensor networks, in: Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE, 2008, pp. 2063 –2068. doi:10.1109/WCNC.2008.366.

[26] N. Gligoric, S. Krco, D. Drajic, S. Jokic, B. Jakovljevic, M2m device management in lte networks, in: Telecommunications Forum (TELFOR), 2011 19th, 2011, pp. 414 –417. doi:10.1109/TELFOR.2011.6143576.

[27] A. de la Oliva, D. Corujo, C. Guimaraes, Requirements Document, https://mentor.ieee.org/802.21/dcn/12/21-12-0091-06-MuGM-requirements-document.docx (September 2012).

[28] A. de la Oliva, D. Corujo, C. Guimaraes, Proposal for IEEE 802.21d solution, ProposalforIEEE802.21dsolution (January 2013).

[29] D. Corujo, C. Guimaraes, B. Santos, R. Aguiar, Using an open-source ieee 802.21 implementation for network-based localized mobility management, Communications Magazine, IEEE 49 (9) (2011) 114 –123. doi:10.1109/MCOM.2011.6011742.

[30] J. P. Barraca, D. Gomes, R. L. Aguiar, AMazING - Advanced Mobile wIreless Network playGround, International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops.

[31] LAN/MAN Committee of the IEEE Computer Society, IEEE Std 802.11-1997, Standards for Local and Metropolitan Area - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1997.

[32] S. Ray, G. P. Biswas, An ecc based public key infrastructure usable for mobile applications, in: Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, CCSEIT '12, ACM, New York, NY, USA, 2012, pp. 562–568. doi:10.1145/2393216.2393310.