Media Independent Transport Service for Ambient Intelligence

Marcelo Lebre[1], Daniel Corujo [2], Diogo Gomes[3], Rui Aguiar[4]
Instituto de Telecomunicações
University of Aveiro
Aveiro, Portugal
{marcelolebre[1], dcorujo [2], dgomes[3], ruilaa[4]}@av.it.pt

Abstract—**The evolution on ambient intelligence technologies, such as sensor networks, propelled a universe of very diverse types of both data and hardware equipment creating one of the most heterogeneous network environments. This diversity brings to light the main issue we aim to address in this paper: the need for a common ground that enables communications between the different heterogeneous equipments and technologies. Starting from the well-established IEEE 802.21 Media Independent Handover standard, we propose its mechanisms and structure to be extended to provide the needed common ground for communication in ambient intelligence scenarios. In this work, we extend 802.21 to include sensor information, enabling different types of equipment and network technologies to communicate with each other under a common standard contributing to a truly heterogeneous network framework. To conclude, we address its viability through a comparison with other known solutions for communication on sensing devices.**

Keywords- IEEE 802.21, Media Independent Transport, M2M, Abstraction, Sensor Service Access Point, Ambient Intelligence, Heterogeneous Networks, Sensor Networks.

I. INTRODUCTION

As social and inquisitive human beings, all of our senses are continuously stimulated by our surroundings, enabling us to perceive the changes around us in different ways. With the ever-growing integration of technological devices into our everyday environment, it becomes necessary to streamline the information flow and control of such devices, optimizing and facilitating their incorporation into existing (and future) underlying communication and technological frameworks. This motivated the proliferation of various communication technologies and sensing devices, as well as the means to access and distribute the information provided by them. In fact, the variety of sensor node design, architectures and interfaces is such that the practical deployment of different sensor technologies creates extremely complex scenarios, since there are no common abstraction or interaction methods.

In our everyday life we encounter sensing devices in almost every piece of technology: to control pollutants in the air, to analyze humidity levels in the garden and optimize the activation of the sprinklers or to control the power consumption from our home, for instance. It is then natural that communications between sensor nodes can vary in many aspects such as technology, protocol or even application. Due to this variety, interoperability has become a problem: different devices can provide different interfaces and be accessed by different protocols via different access technologies, creating complex heterogeneous deployment scenarios.

Recently, and pressured by technology and society developments, the availability of multi-mode terminals, supporting different kinds of access technologies such as IEEE802.11, IEEE802.16 or 3GPP, led the IEEE to release in 2009 the IEEE 802.21 Media Independent Handover (MIH) standard [1]. It aims to abstract the specificities of different link layers to higher layer entities, facilitating and optimizing their control and information retrieval. We argue that its mechanisms can be also used to improve decision-making with accurate smart-environment information, empowering ambient intelligence scenarios with handover (and more) mechanisms supported by a multitude of information sources.

In this paper we enhance IEEE 802.21 enabling it to be used as the technology that integrates not only different access link technologies, but also several sensor network technologies, under a single ambient intelligence framework. The middleware created by this framework aims to empower a myriad of uses, enriching environments and aiding decision-making with the shared view of Ambient Intelligence [13].

The remainder of this article is as follows. In Section II we portray different sensor technologies and their role in heterogeneous environments, while also describing the 802.21 framework and related work. Section III presents the proposed Media Independent Handover Sensor extended (MIHS) and the Sensor Service Access Point, describing the integration of MIH mechanisms into sensor technologies. This is followed by Section IV which presents protocol operation, with performance results being presented in Section V. Finally, we conclude in Section VI.

II. STATE OF THE ART

Related to ambient intelligence and intervening sensing capabilities, the rapid evolution of hardware technology supported the development of sensor devices with cheaper components and a greater variety of choice [6]. These two features propelled the sensor network area to great advances in all directions and applications. A great number of diverse types of sensors, sensor nodes and sensor network technologies have been created. Many manufacturers have even developed specific sensor families like Sun SPOTS [4] or MicaZ [5]. This leaves developers and deployers with a plethora of devices that, not only use different software and hardware, but are also used for different ends [7], presenting the ideal opportunity for the integration of technology abstraction mechanisms.

The IEEE 802.21 Media Independent Handover Services standard [1] provides a cross-layer entity, the Media Independent Handover Function (MIHF) which abstracts the specificities of link layers to higher layer entities (dubbed MIH-Users). The MIHF also provides a set of core MIH services. The Media Independent Event Service (MIES) allows link layers to send events towards registered MIH-Users, such as indicating that a link has crossed a pre-defined threshold. The Media Independent Command Service (MICS) allows MIH-Users to issue commands towards the links, such as link actions and parameter configuration. Finally, the Media Independent Information Service (MIIS) provides queryable Information Elements (IEs) about neighboring networks, adding criteria to optimize the handover candidate selection.

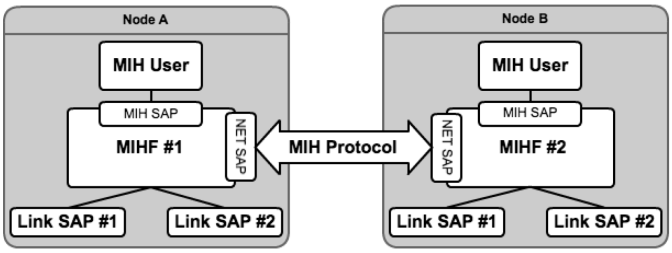


Figure 1 - IEEE 802.21 Framework

As can be seen in Figure 1 these services are accessed through Service Access Points (SAPs). The MIHF provides the MIH Service Access Point (MIH_SAP) to MIH-Users and translates the information into actions specific to the different technology links via a respective LINK_SAP. It also provides the NET_SAP for remote interaction enabling MIH-Users in other nodes to access other services remotely. This is achieved through the usage of the MIH Protocol, which can be transported over layer 2 (i.e., management frames) or layer 3 (UDP, TCP or SCTP).

The 802.21 framework facilitates and optimizes handover operation by enabling handover decision nodes to register to the MIHF of both mobile terminals and network end-points, enabling them to obtain a view of both the mobile terminal and the network usage. An example of such a framework is given in [3] where a network handover decision node is able to collect 802.21 events from a dual-mode mobile node (e.g., Wi-Fi and 3G), and initiate handover procedures in an optimized way. It also shows that the 802.21 signaling has a negligible impact on the network bandwidth, while providing opportunistic information for triggering optimal handovers at the appropriate times.

Bringing such abstraction framework into the sensor networks and ambient intelligence worlds seems a highly promising solution. Early work has been explored in [9], but the authors there do not consider that sensor devices can be low powered devices with restricted capabilities (i.e., processing, memory, battery) and thus requires the definition of sensor-specific signaling messages, which we have defined as the MIHS Protocol. Established international projects, from both academia and industry, such as SENSEI [10], Airnet [11] or ETSI M2M [12], have started to address this issue. Approaches described in [14] and [15] propose specific protocols between nodes to share event information and device status details. This provides a reference baseline that allows us to validate our solution through a cross-comparison of performance, network and structural impact as explained in Section V.

In the next section we discuss Media Independent Handover Sensors (MIHS), a middleware based on 802.21, which can be used as the overlaying protocol on top of heterogeneous sensor networks enabling different equipment to exchange sensor information in a media independent way, and therefore facilitate access to the different sensor devices existing in a sensor framework deployment.

III. MIHS AND MIH SENSOR SAP

In this paper we aim to fill the gap between different sensor technologies by introducing media independent sensor mechanisms, whose abstract functionality facilitates operations involving such devices. The information provided by sensors is easily adaptable to the information structure defined in 802.21, enabling our extensions to be used in already existing MIH scenarios [8].

In order to support context information such as the one provided by sensors, 802.21 requires extensions. Our proposed MIHS extended protocol is a generic protocol extension, which means it is not tied to any specific sensor implementation and supports a vast amount of information that can work with any sensor technology. Therefore, this approach abstracts all implementation and specificity of sensor hardware for operation in a heterogeneous networks environment. Our approach preserved the message structure, encoding rules and general frame format outlined by the 802.21 standard. This approach keeps the MIH main guidelines and maintains the protocol skeleton while supporting new messages and new sensor oriented datatypes.

A. Adaptations to the 802.21 MIH standard

Proposing the use of 802.21 MIHS in sensor networks requires two major adaptations to the original standard. The first one is the extension of already existing messages and subsequent datatypes for sensor network information support. The 802.21 standard does not contemplate the exchange of sensing data, meaning that the development of new messages and datatypes is required. The second adaptation is the creation of another functional entity, the Sensor SAP, which translates sensor interaction into 802.21 messages and vice-versa. The conjunction of these two adaptations composes the core concepts of our MIHS framework, creating an abstraction layer for sensor networks that enables the interface with disparate heterogeneous elements in a normalized fashion.

B. *Sensor SAP Concept*

The proposed architecture involves a Sensor SAP that enables the control and information gathering of sensor devices, and provides it to upper layers in different entities. We took into consideration the fact that sensors can be entities with low memory and processing abilities. As such, imposing a scenario composed of sensor nodes with MIHFs and Sensor SAPs was just too demanding for most families of sensor nodes. To overcome this problem, we extended the 802.21 framework even further by allowing the communication between MIHF and Sensor SAPs to occur in a remote way, re-using the MIH protocol as if it were a MIHF-to-MIHF communication. This also allowed us to explore the sensors networking abilities, such as 802.15.4, for transporting the MIH frames between the Sensor SAP residing at the sensor node, and the MIHF at a respective gateway node. In this way, the processing required by 802.21 mechanisms is handled by the gateway (which has more processing capabilities), while the sensors only need to specify the sensing information in terms of 802.21 MIHS.

In order to contemplate the concerns regarding the power consumption of wireless sensor networks, our framework develops the concept of Light 802.21. Here, we enable the Sensor SAPs existing in sensor nodes to send MIH Protocol messages without requiring a MIHF. In this way, sensors are free of unnecessary service processing, sending the messages to nodes with more resource capabilities where a MIHF forwards and manages communications with other entities.

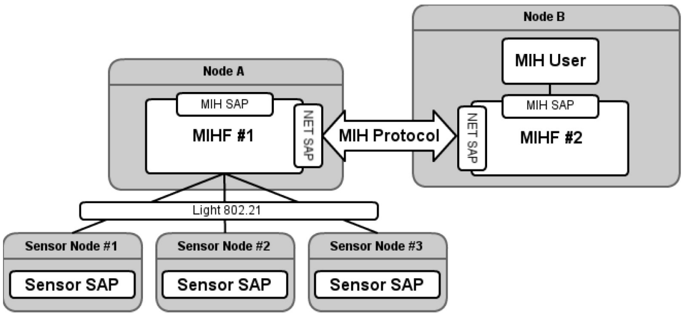


Figure 2 - MIHS Sensor SAP Structure

As Figure 2 depicts, Sensor SAPs are embedded in each Sensor Node. The gateway (Node A) is able to collect sensor information from different manufacturers and technologies in an abstract way, via MIHS extensions developed over 802.21. Whenever an external entity (such as a MIH-User depicted in Node B) intends to access sensor information, it does so using the MIHF in the gateway node, which acts as a MIHF-intermediary on behalf of the node devices, for MIH Protocol interactions. This architecture allows the creation of a totally heterogeneous compliant sensor network, with an abstraction layer that provides context information to remote entities, empowering them with the ability to process and communicate with different technologies of sensors. Also, events originated in the Sensor SAP are created in MIHS format. This procedure saves the MIHF, which is a energy-demanding entity, from having to parse every event, thus only having to forward events, turning the MIHS into a lightweight framework.

C. *802.21 MIHS protocol*

As previously mentioned, 802.21 had to be extended to support the exchange of sensor information. For this purpose we have added the following new messages to the standard 802.21 protocol, as seen in Table 1.

Category	Messages
Management	• MIH_Sensor_Capability_Discover.request • MIH_Sensor_Capability_Discover.response • MIH_Event_Subscribe.request • MIH_Event_Subscribe.response • MIH_Event_Unsubscribe.request • MIH_Event_Unsubscribe.response
Commands	• MIH_Sensor_Configure_Thresholds.request • MIH_Sensor_Configure_Thresholds.response • MIH_Sensor_Action.request • MIH_Sensor_Action.response
Events	• MIH_Sensor_Event.indication • MIH_Sensor_Parameter_Report.indication

Table 1 - MIHS added messages

These new primitives contain commands able to address three different categories. The Management category composes commands that allow the discovery of the sensor capabilities (e.g., type of sensing phenomena, sensing frequency), as well as the subscription and unsubscription of sensor events. The Commands category composes primitives to execute actions at the sensors (e.g., activate or deactivate sensors, force sleep mode), as well as threshold configuration (e.g., define a specific value than, when crossed, triggers the designated sensor event, instead of forcing a query/response mechanism to be deployed for obtaining the sensor information). Lastly, the Events category defines the primitive which is used to disseminate the sensor events.

To support the information provided by sensors, we have also extended the set of 802.21 protocol datatypes, as indicated in Table 2.

IV. PROTOCOL OPERATION

The next section describes the MIHS protocol operation in terms of its supported mechanisms and involved message sequence diagrams.

A. *Description*

In a given situation (exemplified by Figure 3) multiple sensor entities with different requirements can co-exist in the same environment. For instance, multiple sensor nodes can exist, each with a Sensor SAP, a gateway, composed by a MIHF and a MIH User to retrieve sensing information and issue commands, or even servers that just record data.

For this situation, in terms of 802.21 entities, the gateway is the point of attachment (PoA), which is the network termination to which the sensors, Ambient Intelligence Sensor and Consumer Devices are connected to. The gateway also acts as a Point of Service (PoS), since it contains the network-side

MIHF accessed by the consumer devices. This architecture allows the gateway to be a proactive entity and the server to be a passive entity. More powerful sensors could merge the Sensor SAP into the MIHF functionality as well, becoming gateways themselves, enabling even more complex scenarios. Our architecture also allows the support of both active and passive sensors. The architecture and deployment of sensor networks may vary considerably, which will not be a problem to our framework, which is based on an inherently flexible protocol (802.21 has been designed for mobility scenarios).

TLV Name Type	Definition
Sensor Identifier	Sensor identification (Variable)
Req. MIH Sensor Event List	List of supported sensor events (32bit Bitmap)
Req. MIH Sensor Command List	List of support sensor commands (32bit Bitmap)
Sensor Event Configuration List	Configurations List for each sensor type (Variable)
Sensor Parameter Report List	List of sensor parameters to report (Variable)
Sensor Identifier List	List of sensor identifiers (Variable)
Sensor Device States Response	Used to report the device status (Variable)
Sensor Configure Request List	List of configuration parameters (Variable)
Sensor Configure Response List	List of configuration status (Variable)
Sensor Action	Definition of the required action to be performed (Unsigned Integer (8bits))

Table 2 - MIHS added parameters

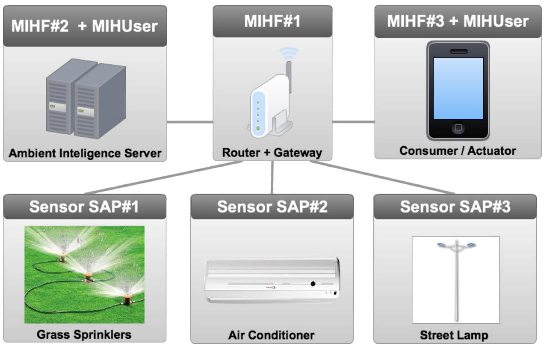


Figure 3 - Example of a MIH Deployment Scenario

B. *Mechanisms*

In order to access the operations and information made available by our MIHS primitives, it is necessary for sensor devices to announce their capabilities to nearby entities, when they become active. This enables potentially interested MIH-Users in the network to be informed that MIHS-enabled sensors are present, and which commands and information they support. As soon as the discovery process is completed, the sensor nodes are able to receive commands and event subscriptions. Event subscriptions allow for sensor nodes to identify which MIH-Users intend to be notified of sensor information events, when these become available.

There are two available mechanisms for event configuration: i) the Threshold Configuration, where a threshold is set for each specific phenomenon, and ii) the Event Subscription, which enables the subscription of periodic events. In this mechanism a specific time period is set for each action.

Sensor nodes are also able to receive action commands allowing for sensor control and real-time information about the status of the node or specific sensor information. There are multiple types of actions that can be sent to a sensor node, such as power down, perform a scan, power up, etc. Although this action is specific to each type of sensor and node hardware, it can be perfectly integrated in our framework by means of instantiation of the Generic Sensor SAP, as it provides a generic approach to sensor technologies supported by our MIHS framework.

Security aspects are currently not addressed in our framework. However, we can consider that security procedures can be executed as part of the link layer attachment procedure (e.g., using IEEE 802.1X for authenticated Wi-Fi connections). Also, specific security-enabled MIH-Users can be coupled to entities in our framework to execute different security measures, acting as out-of-band authenticators for enabling access to the sensor devices. The base IEEE 802.21 standard itself does not provide any specific considerations on security and authentication aspects. Currently, such considerations are being addressed in a separate on-going workgroup, the IEEE 802.21a *Security Extensions to Media Independent Handover Services*.

C. *Message Sequence Diagrams*

We will use two sequence diagrams to illustrate the framework operation. The first diagram represents the sequence of events and commands when they are triggered by sensor node activation. A second diagram illustrates the same operations but having origin at a remote server.

In the **Sensor Activated** Sequence (Diagram 1), an active MIH User becomes aware of a context information source (i.e., sensor nodes) and begins its usage of the sensor network based on events, commands and resulting actions.

The Sensor SAP is activated and sends an unsolicited MIH Sensor Capability Discover to allow the MIHF to know its capabilities (step 1). If the Sensor SAP receives any management message it will continue to function as depicted in Diagram 1. If not, it will wait a small configurable period of time for a response and then later will retry this procedure. Once the sensor node registers with the MIHF, it is ready to receive configuration of thresholds and event subscriptions (steps 2, 3). A MIH Sensor Action mechanism is also available so actions can be performed (step 4) over the sensor device. Information being sent to MIH-Users regarding periodic events or event thresholds will commence at this stage (step 5). The MIH User in the gateway is considered an active user because its messages have direct impact on the behavior of the sensor.

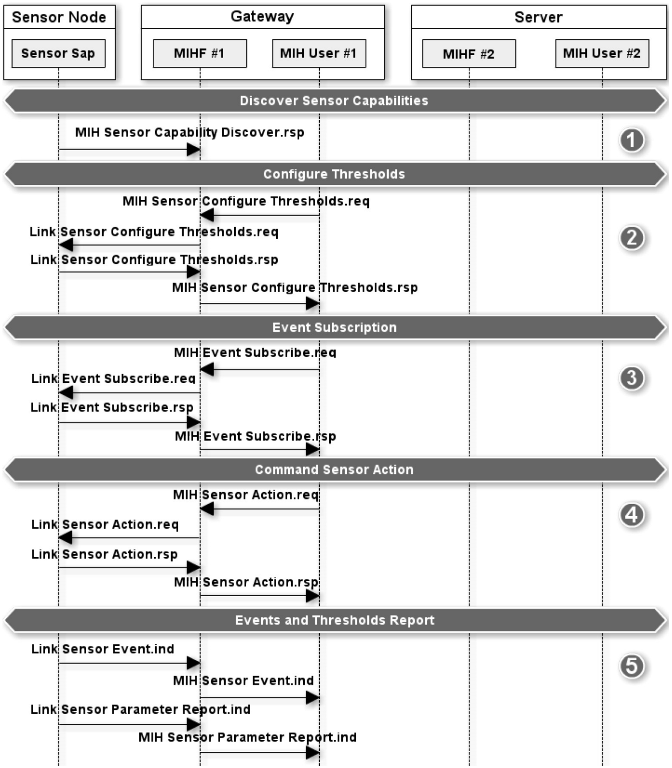


Diagram 1 – Simplified Sequence: Sensor Activated

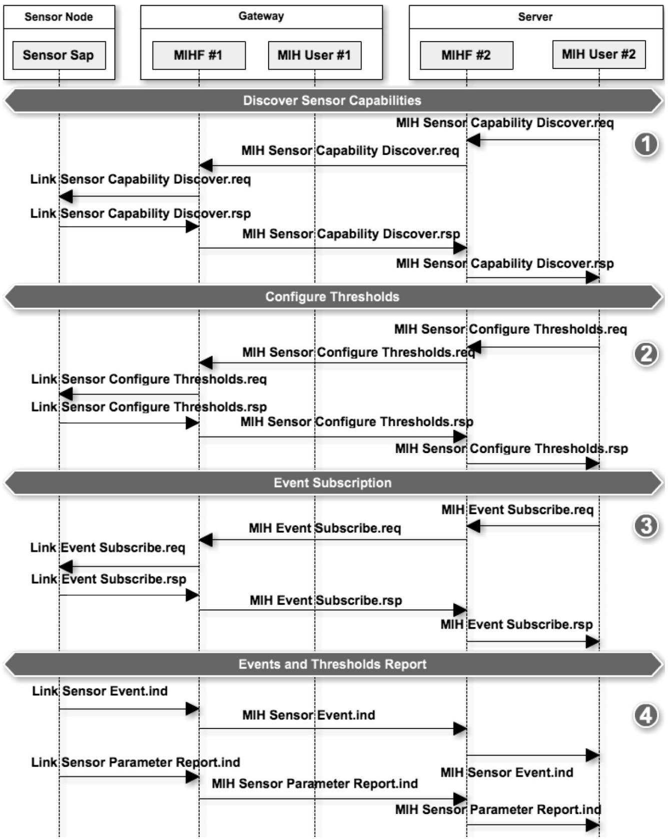


Diagram 2 – Simplified Sequence: Remote Server

The **Remote Server** sequence (Diagram 2), involves a passive MIH User in a remote Server. In this specific example, this MIH User has been developed with the aim of accessing the information from sensors and locally store it for history logging and future characterization of a possible context, but does not issue any action request.

Diagram 2 starts with a MIH Sensor Capability Discover message from the MIH User so it can learn about the offered capabilities of surrounding sensors (step 1). These messages can either be sent in broadcast (to which all MIHS-enabled sensors can reply, identifying their supported capabilities), or be sent in unicast when the MIH User has been pre-provisioned with the addresses of sensors (or has other alternate discovery means). Then the configuration and subscription processes take place (steps 2, 3). As soon as these are completed, the MIH User begins to receive events from sensors (step 4). In this sequence diagram the Sensor Action mechanism is not represented because the MIH User is a passive user, meaning that its actions will not affect the operation of the sensor nodes.

V. EVALUATION

The validation of MIHS as an approach to abstract sensor information communication was performed through a bipartite analysis: structural frame analysis comparing the energy impact using different access technologies, and a study of the impact on the network overhead and processing performance.

For our structural frame analysis comparison, we used protocol data from [14] and [15], which we briefly analyze here. With this data we can provide a common usage example to allow the comparison with our framework, by analyzing the frame, energy impact and signaling required to send an event for three types of sensor readings (i.e., temperature, light and acceleration).

In [14], a Context Base Event (CBE) message is used to convey context information and (as can be inferred in Figure 4) it represents the same types of information as the event message of Figure 6. This XML message is composed as according to the structure defined in [14] and its size is approximately 1300 bytes. This protocol has no header/payload differentiation. All information is inserted in the XML message following schema-based encoding, and is designed to operate at Layer 3.

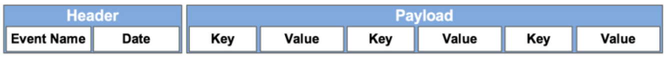
In [15], the DASIMA framework relies on a message, whose structure is shown in Figure 5. The message is composed by a header featuring an event name with a respective date, and a payload with a {key,value} (KV) pair for each sensor phenomena, as the means to convey context information. With this structure, it generates an event message with 69 bytes and operates at layer 3.

In our MIHS framework, all message encodings and datatypes are defined as stated in the MIH protocol standard [1]. The header is composed by a field with 8 bytes, and the rest is considered payload. In this message we encapsulate sensor readings in the Sensor Parameter Report parameters.

Every parameter is encoded in TLV (Type Length Value). The total message size is 48 bytes. This protocol can operate at Layer 2 or Layer 3.

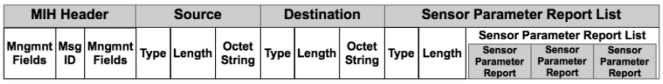
```
<?xml version="1.0" encoding="UTF-8"?>
<CommonBaseEvents xmlns="<xmlnsAddress>"
xmlns:xsi="<xmlSchemaInstanceAddress>" xsi:schemaLocation="<xsdAddress>">
    <CommonBaseEvent creationTime="2001-12-31T12:00:00" extensionName="MIH">
      <extendedDataElements name="" type="noValue">
           <children name="temperature">
           <values>28</values>
           </children>
           <children name="light">
           <values>100</values>
           </children>
           <children name="accelerometer">
           <values>0</values>
           </children>
       </extendedDataElements>
       <reporterComponentId componentType="Transport"
           component="mihsensor#1" componentIdType="Unknown"
           location="0000.0000.0000.0000" locationType="Unknown"
           subComponent="Event"/>
       <sourceComponentId componentType="Transport"
           component="mihsensor#1" componentIdType="Unknown"
           location="0000.0000.0000.0000" locationType="Unknown"
           subComponent="Event"/>
       <msgDataElement msgLocale="EN">
           <msgId>10-3-2</msgId>
           <msgIdType>MIHS</msgIdType>
       </msgDataElement>
       <situation categoryName="ReportSituation">
           <situationType reportCategory="STATUS"/>
       </situation>
    </CommonBaseEvent>
</CommonBaseEvents>
```

Figure 4 - Common Base Event Message



Header		Payload					
Event Name	Date	Key	Value	Key	Value	Key	Value

Figure 5 - DASIMA Event Message



MIH Header			Source			Destination			Sensor Parameter Report List				
Mngmnt Fields	Msg ID	Mngmnt Fields	Type	Length	Octet String	Type	Length	Octet String	Type	Length	Sensor Parameter Report List		
											Sensor Parameter Report	Sensor Parameter Report	Sensor Parameter Report

Figure 6 - 802.21 MIH S - Sensor Event Message

A. *Frame Analysis*

A simple comparison of the three protocols shows that the DASIMA message is the simplest. This fact can greatly reduce the amount of processing required to parse the messages. However, unlike our framework, this same aspect reveals a static nature that prevents it from supporting complex or dynamic data types, reducing its ability to abstract most hardware/software specific details. Another relevant aspect is the message size, in which the CBE message has 1300 bytes, DASIMA 69 bytes and MIHS 48 bytes. A CBE message is approximately 200% larger than MIHS, which directly impacts on performance and network overhead. The CBE framework presents a dynamic structure, able to comprise complex and abstract data, allowing its extension at any given point without the need to alter message-parsing routines on applications. The payload from DASIMA is encoded in KV format, where every insertion has a static and predefined size. Also, an extensive header with a event name and date of variable size, prevent this protocol from creating smaller messages. MIHS provides a best of both cases when considering message length and flexibility, with a TLV format that leads to a small message size while retaining a dynamic structure that allows simple and fast parsing of messages.

B. *Energy Impact of Technologies*

In [16], a study is presented showing energy consumption measurements for transferring a certain amount of bytes using different technologies on a mobile phone: 3G, GSM and WiFi.

Technology	Equation (J)
3G	$\boldsymbol{E_{3G}(x)} = 0.025(x) + 3.5$
GSM	$\boldsymbol{E_{GSM}(x)} = 0.036(x) + 1.7$
WiFi	$\boldsymbol{E_{WiFi}(x)} = 0.007(x) + 5.9$

Table 3 - Transfer Energy Equations

Based on those measurements, the energy consumption for transferring "x" bytes is translated into the equations shown in Table 3, which we used to compare the impact of each of the three mentioned protocols.

Analyzing Figure 7, it is clear that the CBE messages have the highest energy consumption, providing very distant values when compared to DASIMA and MIHS in all the three technologies. The messages from DASIMA also create a slightly higher impact than those from MIHS. These results were expected and are a direct result of the different message size.

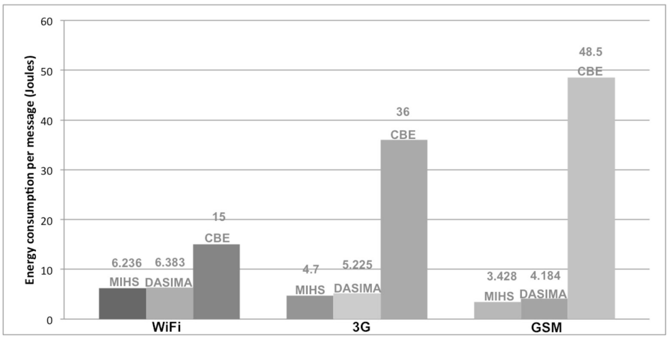


Figure 7 - Energy Consumption Comparison

In all technologies, MIHS has shown to be the most energy-efficient protocol always presenting the smallest energy consumption.

C. *Signaling Evaluation*

We compared overhead and Process Time (composed by total time of sending a command, execute configuration and receiving the response) between the standard MIH Protocol messages and our MIHS, verifying their usefulness in both local and remote handover management scenarios.

1. *Sensor SAP implementation over ODTONE*

This study was done by using ODTONE[1] [2] (Open Dot Twenty ONE) which is an open-source implementation of the IEEE802.21 standard developed at the Instituto de Telecomunicações, Aveiro, Portugal by the Advanced Telecommunications and Networks Group (ATNoG). This implementation stands out from other available implementations [17][18] by allowing its deployment to be made independently of the operating system. To achieve this, the MIHF is implemented using C++ and Boost libraries, particularly Boost.Asio which allowed for state-of-the-art

---

[1] ODTONE, Open Dot Twenty ONE, http://atnog.av.it.pt/odtone

cross-platform asynchronous networking. Another particularity of the ODTONE implementation is the way the MIH_SAP and the specific technology LINK_SAPs are implemented. Instead of developing the SAP primitives as an API, ODTONE implements the SAPs as separate modules coupled with sockets. For interfacing the MIHF with these SAPs, the MIH Protocol is used internally between the MIH-Users and the MIHF, as well as between the MIHF and the LINK_SAPs. As such, developers building MIH-Users and LINK_SAPs just need to import the MIH Protocol libraries and use them for formatting intended behavior.

Under these considerations, we developed a prototype Sensor SAP implementing the 802.21 extensions for our MIHS framework, using the ODTONE implementation. The Generic Sensor SAP was developed using JAVA, allowing the translation between MIHS primitives and a SUN Spot sensor base station. To facilitate the deployment using the sensor devices, a simplified version of the ODTONE MIHF was developed in JAVA as well.

2. *Testbed deployment*

For comparing the signaling performance of our MIHS framework with the base 802.21 mechanisms, we deployed our Generic Sensor SAP and a base 802.21 Link SAP able to operate over 802.11 links. Two nodes were setup as seen in Figure 8, connected through a 100Mb/s switch. Both nodes ran Ubuntu Linux 10.10 with the ODTONE extended API for MIHS and were the single entities in the network. The tests executed involved the MIH-User (located in one node) sending a Configure Threshold message (for testing the base 802.21 signaling) and a Sensor Configuration Threshold (for testing our MIHS signaling) towards the respective SAPs in a remote node.

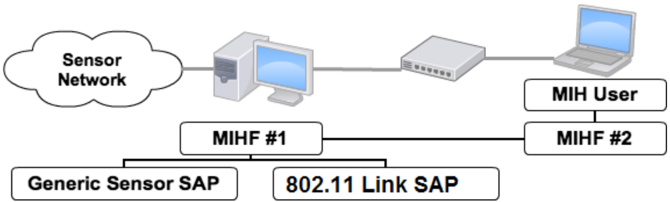


Figure 8 - Experimental Example

3. *Results Evaluation*

Regarding overheads, standard threshold configuration request messages were issued with a size of 84 bytes and the response message sized 39 bytes. For the Generic Sensor SAP a threshold configuration mechanism was also used, but this time the request message sized 63 bytes and the response message 28 bytes. Although these sizes can vary depending on the information, in this case the information passed was static in both mechanisms. The different size of the two sets of messages is due to the nature of the information in hand. The datatypes from the sensor information message are not as large as the ones from the network.

We analyzed the total Process Time, measuring 20 message exchanges with the Configure Thresholds and Sensor Configure messages. Their mean times revealed that the processing time for the Configure Tresholds message was 4.45ms (±0.59) and 4.20 ms (±0.75) for the Sensor Configure Thresholds, with a confidence of 95% considering a T-student distribution. Through these results, the new sensor context information messages do not seem to impact performance and are on par with standard 802.21 messages behavior.

VI. CONCLUSION

We proposed MIHS, an extension for the IEEE 802.21 standard able to transport sensor information, creating an abstraction layer that integrates both heterogeneous elements and networks with low resource requirements. We have compared its frame structure and energy consumption with two protocols specialized in event sharing and sensor communication (CBE and DASIMA), showing that our framework is both able to provide a simpler structure and low energy consumption. We have also compared the signaling processing time and size between our new messages and the base IEEE 802.21 messages. Results shown that the new sensor messages are on par with the base standard messages, allowing their utilization with no performance impact when compared to IEEE 802.21.

This study shows that MIHS is a resource efficient framework whose dynamic structure supports both complex and simple data types, while creating an adequate deployment for a standard media independent transport protocol in heterogeneous environments. Presently, as MIHS derivates from the IEEE802.21 MIH protocol, we are deploying it in integrated mobility and context-aware scenarios, obtaining results of more extensive performance tests including mobile devices and mechanisms to enhance the energy-efficiency of the presented protocol. Likewise, we are deploying the framework over different kinds of sensor devices, with the aim of obtaining performance results under a full wireless sensor network.

ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project).

REFERENCES

[1] IEEE 802.21 Standard, “Local and Metropolitan Area Networks – Part 21: Media Independent Handover Services”, January 2009.

[2] Corujo, D., Guimarães, C., Santos, B., Aguiar, R. L., "Using an Open-Source IEEE 802.21 Implementation for Network Based Localized Mobility Management" Chapter in IEEE Communications Magazine, Special Issue on "Communications Middleware for Mobile Devices and Applications", Sep 2011

[3] Melia, T.; Corujo, D.; de la Oliva, A.; Vidal, A.; Aguiar, R.; Soto, I.; , "Impact of Heterogeneous Network Controlled Handovers on Multi-Mode Mobile Device Design," Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE , vol., no., pp.3884-3889, 11-15 March 2007

[4] Sun SPOT, “Sun SPOT World”, http://www.sunspotworld.com

[5] Crossbow, “Crossbow Technology Inc.”, http://www.xbow.com

[6] Marcos A. M. Vieira, Claudionor N. Coelho, Diógenes C. S. Junior, José Mata, “Survey on Wireless Sensor Network Devices”, Proc. ETFA ’03 IEEE Conference, vol. 1, pp 537-544., September 2003

[7] Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y., Cayirci, E., “A survey on sensor networks”, IEEE Communications Magazine, pp 102-113, vol. 40, Issue 8, November 2002

[8] Lebre, M.; Corujo, D.; Gomes, D.; Aguiar, R.; “Context Transport based on 802.21 MIH protocol”, “1st Portuguese Conference on Wireless Sensor Networks” CNRS ‘11, Coimbra, Portugal, March, 2011.

[9] C. Dannewitz, S. Berg, and H. Karl, "An IEEE 802.21-based Universal Information Service", in Proc. of the Wireless World Research Forum Meeting 16, April 2006.

[10] ICT-SENSEI, FP7-ICT, “Sensei – integrating the physical with the digital world of the network of the future”, “http://www.ict-sensei.org”

[11] IST-Airnet, FP6-IST, “Airport Network for Mobiles, Surveillance and Alerting”, “http://www.airnet-project.com”

[12] ETSI TR 102681, “Machine-to-Machine communications (M2M); Smart Metering Use Cases”, http://www.etsi.org, May 2010

[13] J. Schwarz da Silva, “Future Internet Research: The EU framework”, ACM SIGCOMM, Volume 37, Number 2, April 2007

[14] I. Grønbæk; P.K. Biswas; , "Ontology-based abstractions for M2M virtual nodes and topologies," Ultra Modern Telecommunications & Workshops, 2009. ICUMT '09. International Conference on , vol., no., pp.1-8, 12-14 Oct. 2009

[15] Kessis, M.; Roncancio, C.; Lefebvre, A.; "DASIMA: A Flexible Management Middleware in Multi-Scale Contexts," Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on , vol., no., pp.1390-1396, 27-29 April 2009

[16] Balasubramanian, N.; Balasubramanian, A.; Venkataramani, A., “Energy Consumption in Mobile Phones: A Measurement Study and Implications for Network Applications”, Proc. 9th ACM SIGCOMM on Internet Measurement Conference, pp. 280-293, 2009, New York, U.S.

[17] E. Piri and K. Pentikousis, “Towards a GNU/Linux IEEE 802.21 Implementation,” IEEE ICC ’09, June 2009, pp.1–5, 14–18.

[18] Y. Lopez and E. Robert, “OpenMIH, an Open-Source Media-Independent Handover Implementation and Its Application to Proactive Pre-Authentication,” Social Informatics and Telecommun. Eng., vol. 32, part 1,2010, pp. 14–25.