UPnP for Wireless Sensor Networks in telemedicine applications

Silvano Mignanti, Francesco Delli Priscoli, Guido Oddi and Ivan Callian
Sapienza University of Rome”, Via Ariosto 25, 00185 Rome, Italy
{mignanti, dellipriscoli, oddi}@dis.uniroma1.it, callian@libero.it

Keywords: UPnP, Plug&Play, Sensors Network, Discovery Service, Bravehealth.

Abstract: The goal of this paper is to provide typical Sensor Networks with the management primitives (e.g.: discovery, control) offered by an UPnP-compatible framework. The idea is to extend the concept of Plug & Play to Sensor Networks: each network node should be able to discover other nodes’ functionalities, retrieve measured data and/or enforce actions on network’s actuators, (in case) compose services offered by several nodes to fulfill complex goals. The proposed sensor management architecture uses UPnP-compatible messaging and Wireless Sensor Networks, being these last ones the most challenging scenario due to their intrinsic limitations. Such an innovative approach revealed to be extremely useful for body area networks, like the one being developed within the Bravehealth FP7 project.

1 INTRODUCTION

Sensor networking is one of the most essential technologies for the implementation of ubiquitous computing. The sensor nodes are usually scattered in a sensor field and data are routed back to the sink by multi-hop. These sensor networks usually share the same communication channel. Sensor nodes have limited power, computational capacities, memory and short-range radio communication ability.

While they exist several protocols/standards for transport and lower layers of the ISO/OSI stack specific for wireless sensor networks, e.g. ZigBee (ZigBee Alliance, 2008), Bluetooth (Haartsen, 2000), 6LOWPAN (Shelby et al., 2009), usually at higher layers there is a lack of solutions, at least a lack of widely diffused ones, specific for the case of WSNs. In particular, usually sensed data and, in case, control messages, do use vendor-specific approaches, typically just row data or data with very limited scenario-specific formatting. This implies that, in most of the cases, communication among sensor of different vendors is impossible unless common semantics and meanings of data and messages are a-priori agreed, at application level, among the different vendors.

This, generally speaking, has obviously a great impact on the interoperability among different sensor and different sensor networks, negatively affecting all the applications require to use sensor networks: in particular, this is true for a medical scenario, where both wired and wireless sensor networks are used to retrieve medical data from patients in order to evaluate their health status, like in the Bravehealth (ICT FP7 European Commission Grant Agreement Number 248694) project.

In such a project, in fact, a so called “Wearable Unit” (WU), consisting in an extremely integrated system containing several sensors (ECG, temperature, 3-axis motion, pulse-oximetry…) in a “plaster” to be positioned on the chest in correspondence with the hearth, is used to measure patients’ medical data which is remotely reported to caregivers. Such a WU is designed to use standard communication protocols (Bluetooth and/or ZigBee) to interface with other devices: not only a so called “gateway” able to forward data to a remote management centre, but also to all other Bluetooth/ZigBee devices, in particular to other external sensors. Furthermore such a WU is also designed to support the connection to other wearable devices, implementing a sort of wireless body area network (WBAN).

The idea behind the presented work is to enable “Plug & Play” among those devices/sensors in such a WBAN, making them able to discover themselves, properly dispatch sensed data and/or control messages independently of vendor-specific solutions and approaches: each sensor will present itself as being able to offer certain services (sensing and/or
actuating) and, in case, being able to be controlled. All of this should require no manual intervention or manual (re-)configuration of any of the existing nodes: new nodes should “install” themselves in the WBAN transparently to the end users, just like new peripherals could be added to a standard PC without any configuration in most of the cases, thanks to the Plug & Play philosophy.

In order to avoid the most obvious objection could be moved to adding overhead to the data the WBAN should transmit, which, in case of the most common usage of wireless sensor networks means augmenting battery consumption so reducing the lifetime and the operability of the entire network, it is important to specify the field of application of such an approach. Whenever the main objective for the sensor network is to remain operative as long as possible, the proposed approach should not be followed: vice versa, if the main objectives are to guarantee interoperability among diverse sensors and sensor networks and/or the ease of use, the presented approach could be an effective solution. In particular, in a medical scenario, especially the one of patients with cardiovascular diseases (such as the one of the Bravehealth project) where most of the users will be elder people, the ease of use is a key requisite: surveys proposed to the patients revealed they prefer to be forced to recharge batteries of their sensors (which will be made obviously possible in such a case) up to once/twice a day instead than be forced to perform any kind of configuration of the sensors.

2 STATE OF THE ART

2.1 State of the Art in WSNs

The efficient design and implementation of wireless sensor networks become a challenging research area in the last years. By interconnecting large numbers of sensor nodes, it is possible to obtain data about physical phenomena that was difficult or impossible to obtain in more conventional ways. Furthermore the cost of manufacturing of sensor nodes is continuing to drop, so that increasing deployments of wireless sensor networks. Potential applications for such large-scale wireless sensor networks exist in a variety of fields, including medical monitoring, environmental monitoring, surveillance, home security, military operations, and industrial machine monitoring. To understand the potentialities connected to the usage of wireless sensor networks, consider the following example, strictly connected to the application scenario proposed in this paper.

A challenging application domain that can make use of wireless sensor network technology is medical monitoring. This field ranges, for example, from monitoring patients in the hospital using wireless sensors to monitoring people in their everyday lives to provide early detection and intervention for various types of disease. In these scenarios a plethora of sensors could be used: from miniaturised body-worn sensors to external ones such as cameras, or GPSs (adaptation from Perillo et al., 2005).

Another interesting potential field of application for (wireless) sensor networks is the domotics one; in this last particular scenario, anyhow, several protocols/standards are quite well established, so that the approach proposed in should take care of all of them: for such a reason, a short introduction of KNX and X10 is presented.

KNX is a standardized (CENELEC EN 50090, ISO/IEC 14543), OSI-based network communications protocol for intelligent buildings, and it was designed to be independent of any particular hardware platform. The most common form of installation of a KNX network is over a twisted pair medium. There are three categories of KNX device:

- A-mode or "Automatic mode" devices automatically configure themselves, and are intended to be sold to and installed by the end user.
- E-mode or "Easy mode" devices require basic training to install. Their behaviour is pre-programmed, but has configuration parameters that need to be tailored to the user's requirements.
- S-mode or "System mode" devices are used in the creation of building automation systems. S-mode devices have no default behaviour and must be programmed and installed by specialist technicians.

X10 (Rye, 1997) is an international and open industry standard for communication among electronic devices used for home automation (domotics). It primarily uses power line wiring for signalling and control, where the signals involve brief radio frequency bursts representing digital information. Although a number of higher bandwidth alternatives exist, X10 remains popular in the home environment with millions of units in use worldwide, and quite inexpensive availability of new components.
\section{State of the Art in Service Management}

In the literature have been proposed many approaches to service management (discovery, configuration, composition...): different protocols and/or standards propose different solutions, for example, for the sole aspect of service discovery, they exist a number of protocols such as UPnP, Jini, Salutation (Rekesh, 1999), SLP (Guttmann et al., 1999), UDDI (Ariba Corporation et al., 2000). Among these protocols/approaches, the one which best fits to the scenario presented in this paper is for sure UPnP (Universal Plug and Play): in fact it provides, at the same time, not only service discovery functionalities (like most of the other listed protocols) but also configuration/control mechanisms and even eventing. The main characteristics of UPnP are:

\begin{itemize}
\item Standardized: UPnP respects a number of standards and recommendations;
\item Scalable: it is suitable for working with networks of any dimension;
\item Plug and Play: it provides a standards-based communications environment that allows networked devices to be automatically discovered, configured and controlled;
\item Open Source: it is an open network architecture, defined by the protocols used, and independent of any programming language or physical support; furthermore they exist a lot of open source implementation of it in almost every programming language;
\item Limited Resources: the resources required by UPnP are extremely limited. This allows UPnP to work on PCs and on devices with limited computational capabilities and limited hardware resources, like sensors are.
\end{itemize}

This protocol is an extension of the Plug & Play concept, born for PC boards, to network devices and has been developed to support “zero-configuration” and the automatic detection of a wide range of device categories. With UPnP, devices can dynamically enter in a network, obtain an IP address, make available to it their functionalities and detect the presence and capabilities of other devices, without the need for any manual configuration/intervention. This technology uses well established standard like TCP/IP, UDP, HTTP, SSDP (UPnP Forum, 2008) and SOAP (Mitra et al., 2007), allowing a perfect integration into the existing networks. UPnP is open and the UPnP Forum defines, based on a common architecture, the “Device and Service Description”, which are the descriptions of devices and services in an XML (Bray et al., 2004) format, used in control messages and in the events’ generation.

\section{UPNP ENHANCEMENTS FOR THE WBAN SCENARIO}

As already indicated, the overall idea is to permit different nodes of a (wireless) sensor network, in particular a WBAN, to communicate each other with, possibly, a standard protocol in order to discover among themselves, exchange monitoring and control messages and, in case, intelligently compose their offered services in order to provide new ones. Among the existing protocols, the most promising for such a challenging objective was identified as the UPnP protocol, for its above mentioned specificities. Our tests revealed UPnP to be able to perfectly adapt, without any modification, also to WBANS: in any case, we decided to further investigate for some possible slight (optional) modifications to it as possible enhancements to the protocol, to better fit it to the WBANs scenario.

\subsection{Multi-hop UPnP}

\subsubsection{The proposal}

The most important proposed addition to the UPnP protocol is the possibility for nodes/control points to request to devices information of other (third) devices than the ones to which messages are directed (e.g. device A asks to device B information for device C): this is of particular importance in order to enable the possibility to obtain information of devices out of the reach of the applicant but located in the same sensor network (note, in this last sentence and in the following, unless differently specified, we group under the term “device” either UPnP devices and UPnP control points).

To support this additional functionality, it was necessary a minor modification to the SSDP M-SEARCH message allowing its body, within the “ST.” field, to support an additional type, namely “uuid_ext:device-UUID”. Remember that the M-SEARCH SSDP (Simple Service Discovery Protocol) messages are sent (usually in multicast) in order to discover devices and that the ST field is the field where the “search target” is specified, thanks to the “uuid/device-UUID” field: only the device of “device-UUID” has to respond to the M-SEARCH message. The new “uuid_ext:device-UUID” field indicates, to any receiver of the M-SEARCH
message containing that field, that the sender is looking for the device of UUID “device-UUID”, but, unlike the normal M-SEARCH messages, any device having information regarding to that “external” device of UUID “device-UUID” has to respond to the request. This new field will be not compliant with current UPnP specifications, causing receivers not allowed to interpret it to discard the message as a malformed one: this is actually not a problem, but an advantage. In fact, in order to support this functionality, also default behaviour of UPnP devices should be slightly changed, in order devices to store information also regarding “external” ones: in practice, in a network were both usual and “new” UPnP devices are present, only new ones could interpret and correctly respond to the new kind of message, as old ones were not present at all.

Prior to explain the modifications required to the behaviour of UPnP devices, it is useful to highlight the importance of additional functionality. Typically, in a sensor network, not all the nodes are directly reachable from each other, so that the UPnP devices related to a certain node could not be reachable from all other UPnP devices related to other nodes. In case the wireless sensor network does not support multi-hop transmission, such UPnP devices could never discover among themselves: the proposed addition to the UPnP protocol will resolve this kind of problem.

2.1.2 Implications

As already anticipated, in order to support the previously mentioned additional functionality, some modification to the usual functioning of UPnP devices should be performed, further than the one previously indicated.

First of all, if the WBAN does not support multi-hop, at least the Advertisement multicast messages should be properly forwarded by each UPnP node to the others, in order to guarantee all the nodes of the WBAN (or, at least the group of nodes reachable, with multiple hops, from the sender) are correctly informed of the activation of the node sending the Advertise message. Policies how to solve loops and similar issues are to be implemented as well, but this aspect is out of the scope of this paper.

Moreover, further than responding to M-SEARCH messages for third devices, each device should also take proper care of Time To Lives (TTLs) of the advertisements of those third devices. In fact, whenever a certain devices asks to a second one information for a third one, the second, in case the TTL of such a device is expired, should either respond to the first one that the requested device is no more available or try to contact the third one with a proper M-SEARCH message, in order to check its actual availability and, after this check, properly respond to the first device.

2.2 Further optimizations

Considering the particular application scenario, some further optimizations to the UPnP protocols were investigated.

First of all, UPnP specifications indicate some messages could/should be sent in multicast and some others could/should be sent in unicast. Unfortunately most of WBAN nodes have very limited computational power, so that it could be even not supported (for whatever reason: limited memory, limited number of ports…) the possibility to remain listening on two different sockets (one unicast and one multicast). For this reason, a possible optimization was identified for this particular situation (i.e. in case of the impossibility to open two listening sockets) was to force all the messages to be always sent in multicast. In such a case, it will be possible to use the “HOST” field to distinguish the addressee of the message: in case the value of such a field is the usual “239.255.255.250:xxx” (where xxx “MUST” be 1900 for the UPnP specifications, but could even be a different port number) the message is a normal multicast UPnP message and should be considered consequently; in case the value is different, it should be interpreted as the address of the addressee and only the device having that IP should read the message.

A second minor optimization proposal is intended to reduce messages’ size. For this reason, we propose to remove a field of the SSDP messages, namely the “SERVER” one. This field in fact contains information about the version of the Operating System, the UPnP version and product name and version, which are expected to be not fundamental in such a scenario: in any case, if, for whatever reason, the UPnP version information should be maintained, it could be moved, for example, at the end of the HTTP or NOTIFY fields.

4 CONCLUSIONS

The paper presents an approach could be used to ease the usage of medical devices which do use wireless sensor networks for their purposes, taking in particular care the interoperability aspect: th
proposed solution in fact permits interoperability and a “plug and play” like approach for the interaction among medical wireless devices, allowing devices’ auto configuration without any manual intervention. Such an idea, which could enormously boost the adoption of similar technological medical solution even for people with very limited technical skills, is based on a well-known and extremely diffused protocol, the Universal Plug and Play (UPnP), which results perfectly compatible even with devices with very limited computational resources and which also presents the best combination of functionalities for such a scenario, natively permitting discovery, advertisement and control of devices. For the above mentioned reasons, the UPnP protocol seems to be a really good candidate for the indicated medicine applications, in particular considering also the additional optimization proposed.

DISCLAIMER

The work described in this paper is partially based on the results of the ICT FP7 Integrated Project Bravehealth. The Bravehealth consortium receives research funding from the European Community's Seventh Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

REFERENCES


Protocols for Wireless and Mobile Networks, CRC Hall.
ZigBee Alliance, January 17 2008, ZigBee Specification.