Standard-based and Distributed Health Information Sharing for mHealth IoT Systems

Danilo F. S. Santos, Angelo Perkusich and Hyggo O. Almeida
Embedded Systems and Pervasive Computing Lab.
Federal University of Campina Grande, Brazil
Emails: {danilo.santos, perkusic, hyggo}@embedded.ufcg.edu.br

***Abstract*—The increasing availability of connected Personal Health Devices (PHDs) enables a new type of information to be available in the Internet: health information. Most of these devices have specific ways to connect and share information to the Internet through gateways or health managers, creating vertical solutions where one device just talks to one health service. In this context, this paper proposes an architecture that considers the use of different types of health managers and gateways, but keeping interoperability by the use of widely adopted standards. The main contribution of this work is the distribution of health managers in different locations, such as mobile devices and cloud applications, enabling the use of a single health service for different types of PHDs. The ISO/IEEE 11073 standard is used as core technology, enabling the transport of PHD information over different technologies and protocols. We also present a new classification of health managers based on requirements of legacy m-health services. In conclusion, the results of the integration with a real cloud-based connected health system are presented and evaluated.**

***Index Terms*—mHealth, Personal Health Devices, ISO/IEEE 11073**

I. INTRODUCTION

The increasing use of mobile and smart devices to monitor our health creates new opportunities for healthcare services. In this scenario, patients collect data using their Personal Health Devices (PHDs) and share it with their doctors remotely using smartphones, tablets or even TV sets [1]. Based on this scenario, we are starting to witness PHDs with wireless connectivity technologies, such as Bluetooth and Bluetooth Low Energy, which enable automatic sharing of information with just a few clicks.

Following this trend, patients are the ones that take control of their health and wellness by being responsible for monitoring themselves using connected devices and the Internet, enabling a true scenario for the Internet of Things (IoT) for healthcare. Considering mobility aspects created by the frequent use of personal devices such as smartphones, patients can share health information anytime and anywhere. From the health device point of view, these patients can use personal (or wearable) health devices, or share health devices available at home or in hospitals, such as weighing scales or non-invasive Blood Pressure monitors. Another important limitation of most connected health devices is the need of third party devices to share information, for example, a Bluetooth Blood Pressure monitor needs a smartphone to send its measurements to the Internet. Therefore, it is necessary to create an infrastructure that supports the use of different types of health devices in the Internet, but keeping shared health information personal.

Based on the previous description, interoperability between devices and services is a natural concern. In this front, some effort groups created standards and specifications for exchanging health information. One of these groups created the ISO/IEEE 11073 set of standards, which declares how those devices should talk to each other (IEEE 11073-20601 [2] [3]) and how each entity should behave. The most important feature of ISO/IEEE 11073 is its transport independency, meaning that IEEE 11073 message can be carried over almost any transport technology or protocol.

In the IoT context some related work has been done within mobile and pervasive healthcare systems. In [4] it is discussed and presented a new concept of m-IoT (Internet of m-health Things). In [5] it is discussed how to apply service science model to integrate IoT and eHealth solutions. Other research works, such as [6] and [7], also propose systems, challenges or solutions for mobile healthcare systems. In common, all these works need to communicate with PHDs to collect sensor's data and share it with services through the use of specific health gateways or manager devices. Most of these previous works do not discuss communication aspects related to the standardization of health information on the Internet, as also, how a single and integrated solution could solve interoperability problems. In the standardization research [8] presented a personalized middleware based on ISO/IEEE 11073 standard, however, it just considers a single type of data manager or aggregator device.

Based on these communication and interoperability requirements, in [9] we proposed a solution for the use of ISO/IEEE 11073 standard in IoT context, where ISO/IEEE 11073 messages are carried over transport and application protocols, such as TCP/IP and CoAP [10]. Based on results of [9] and new scenarios presented by mobile technologies, this paper presents a new architecture that takes into account standardization needs, different types of health and mobile devices, and legacy connected health systems, creating a distributed and personal connected health architecture. The main contribution of this proposal is the potential to share information in a standardized way, using different connected health devices and health managers distributed in personal devices and in the cloud. We also present a set of requirements and definitions used in the design process of the architecture.

II. Technology Overview and Definitions

Before presenting the proposed architecture and how it was designed, it is necessary to understand some key technologies, and define some ground concepts and requirements. In the design process of connected health systems, it is important to understand and answer the following questions: (a) How health data is transmitted and transported by a PHD? (b) How health data is carried by health protocols over the Internet? (c) How health data is managed and distributed over health services? The following sections present technologies and concepts that will help us answer these questions.

A. PHD Wireless Transport Technologies

Personal Health Devices (PHD), wearable or not, are devices with constrained resources, specially related to energy supply and processing power. Therefore, it is natural the use of low-power communication technologies, such as 802.15.4 or Bluetooth. Having in mind personal and Consumer Electronic (CE) devices, Bluetooth is a well-deployed technology on smartphones, smart TVs, personal computers, etc. In this context, Bluetooth should be a natural choice for deployment of personal e-Health systems and devices. It is possible to use two approaches for Bluetooth health devices: use of the Health Device Profile (HDP) or use of the Bluetooth 4.0 Low Energy mode. HDP profile defines specific channels to transport Health Information over Bluetooth links. HDP specification is application-neutral, however the only protocol currently supported is IEEE 11073, and HDP architecture is clearly aimed towards IEEE 11073 needs. Bluetooth 4.0 Low Energy (BTLE) is a new specification that aims to exchange information consuming low power. The main protocol of BTLE is the GATT protocol, which define ways to exchange attributes between BTLE devices in a simple and efficient way. Over GATT protocol it is possible to define a set of specific profiles, including profiles for health and fitness devices. As also, an effort from multiple organizations is preparing BTLE for carry IPv6 packets, that way paving the way for IoT on Bluetooth devices.

B. Personal Health Protocol

One key concept of connected health solutions is make possible share health information using personal devices. Health information can come from multiple sources, such as PHDs, manual input in smartphones or even your CE device in your living room. Therefore, it is necessary to use a standardized way to represent and carry health data. In the context of this work, the ISO/IEEE 11073 family of specifications was chosen. Two types of devices are defined in the ISO/IEEE 11073: agents and managers. Agents are data producers (sources), therefore, they are Personal Health Devices. Managers are data sinks, thus, they are the ones that receive data from agents. ISO/IEEE 11073 is based upon the idea that agents are low-powered devices and have few processing resources, while managers are typically powerful devices connected on a main power source. Therefore, most of IEEE 11073 complexity is placed on managers. From a broader architecture point-of-view, we can consider that managers are the ones that know where personal health data should be sent and stored.

Many devices available at the market use Bluetooth HDP as transport layer. Besides physical communication technologies, it is also possible to carry ISO/IEEE 11073 messages over transport or applications protocols, such as TCP/IP, UPnP [11] or the new Constrained Application Protocol (CoAP). CoAP is designed to be used over UDP, and its model is similar to a client/server HTTP model. Although CoAP is designed to be carried by UDP packets, it supports confirmable messages, which is a requirement for health data transport. CoAP can also be used over different transport technologies, such as IEEE 802.15.4, Bluetooth Low Energy [12] and even SMS (more details at http://tools.ietf.org/ wg/core/). This could enable a new set of applications and services for embedded and mobile devices, especially in the healthcare field.

C. Gateways, Managers, Devices and Services

In the context of this work, it is important to understand the difference between *Gateways*, *Health Managers* and *Health Service*. In our work, a *Gateway* is the entity that forward health data to a different destination. By definition, a *Gateway* does not understand the device specialization of the health data, e.g. it does not know if a specific packet is from a Blood Pressure Monitor or Thermometer device. A *Health Manager*, otherwise, knows the specialization of a specific PHD. For example, the *Health Manager* knows what type of data a Blood Pressure Monitor is sending, e.g. systolic and diastolic blood pressure. Therefore, a *Health Manager* have an internal database with information about device specializations or, as an IEEE 11073 Manager, it can dynamically learn what type of data has been sent by a PHD. In terms of purpose, the *Gateway* receives health data and forwards to somewhere else, and the *Health Manager* receives health data and interprets it. Based on this definition, when a *Health Manager* is placed together with a *Gateway*, we called it a *Health Gateway*.

Looking at each end-point, we have the *Health Service*, which receives Personal Health Information from a user, and shares it to other healthcare actors. At the other end-point, as presented on [9], we have two types of PHDs classified based on the type of *Gateways* they use: (a) *Gateway-Based PHDs*, which are devices that uses *Health Gateways*; (b) *Internet-Ready PHDs*, which are devices that uses *Internet Gateways*.

III. Architecture Description

Before describe the proposed architecture, we defined the following requirements during our design process:

- Personal and CE devices, such as smartphones, should be able to read health data, and take actions;
- Internet Gateways should be part of the architecture;
- Users must be able to use personal or shared health devices together with their own Health Services;

Based on the definitions and requirements presented before, we propose an architecture where *Health Managers* could be distributed in different locations. Therefore, the main contribution of this architecture is in the definition of how *Health Managers* are used. *Health Managers* can be personal and installed in smartphones where, for example, it can control sensors and actuators on a Body Area Network. In this setup, healthcare applications installed into the user's smartphone can use health information without the dependence of external *Health Services*. In a different setup, the user can use *Internet-ready* PHDs where the *Health Manager* is integrated with *Health Services* in the cloud. This setup allows the user to use shared PHDs in different locations, but keeping use their own personal *Health Manager* in the cloud. The base architecture is illustrated in Figure 1.

In the core of the proposed architecture we used the ISO/IEEE 11073 standard. Using ISO/IEEE 11073 managers and agents, the architecture naturally supports different transport technologies, such as Bluetooth or TCP/IP. As also, it is possible to distribute managers over different locations keeping interoperability and using the same *Health Service*. As illustrated in Figure 1, we define two types of managers: Personal Health Managers and Internet Health Managers.

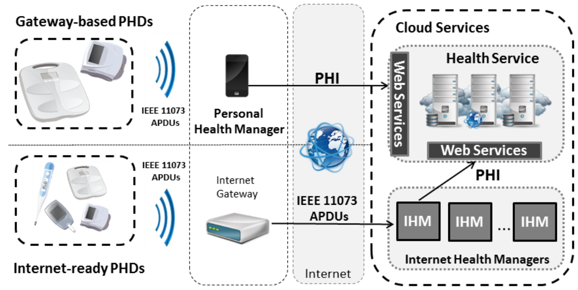

Fig. 1. Base Architecture.

A. Personal Health Manager

Personal Health Managers (PHM) are based on the idea that PHDs are usually used by only one user, and these devices do not have any identification information about the user. In a Body Area Network, for example, body sensors are attached to the same user all the time, and sensor's measurements can only be identified in the *Health Manager*, where it becomes Personal Health Information (PHI). Therefore, the PHM is an important part of our architecture because it makes possible for simple PHDs to send measurements to the *Health Service*. This type of manager is widely used by current connected health solutions, where PHDs use technologies such as USB, Bluetooth HDP or BTLE, and share information to the cloud through smartphones, tablets or hubs. A reference architecture for this type of manager is presented on Continua Health Alliance Guidelines [1]. Continua Health Alliance is a non-profit association that promotes the standardization of Personal Health Devices, envisioning a market of standard, affordable and readily connectable sensors.

B. Internet Health Manager

One of the main advantages of the proposed architecture is the use of distributed Internet Health Managers (IHM). IHM makes possible to Internet-Ready PHDs to send information direct to the Internet through standard Internet gateways. One important point to notice is the transport protocol configuration used by the IHM. Although ISO/IEEE 11073 transport flexibility, it is necessary to choose a base communication model for each ISO/IEEE 11073 IHM in the Internet. For example, based on the work presented in [9], it is possible to adapt IEEE 11073 communication model to REST model. Based on this new model, two base protocols can be used: HTTP and CoAP, creating a different IHM for each type of transport protocol in the cloud. With IHMs, it is possible to have Wi-Fi enabled PHDs using TCP/IP messages, such the ones presented in [6], and BTLE enabled PHDs using CoAP messages, both accessing the same *Health Service*. And, in the *Health Service*, it is possible to have CoAP-ready ISO/IEEE 11073 Managers and TCP/IP-ready IEEE 11073 managers. It is important to notice the possibility to use CoAP-HTTP proxies, keeping just one Internet Health Manager per user for both CoAP and HTTP protocols.

IV. Prototype Implementation and Evaluation

For the prototype implementation, a complete connected health system developed by Signove, namely SigHealth (more details at http://health.signove.com), was used. This system is complaint to Continua Health Alliance Guidelines, and its architecture is illustrated in Figure 2(a). The objective behind the use of SigHealth is to have an already deployed system based on Personal Health Managers. In this platform, managers are deployed on different mobile platforms, such Google Android, Apple iOS and Linux. As also, the PAN (Personal Area Network) communication interface is based on ISO/IEEE 11073 standards, over Bluetooth HDP, USB or transcoding Bluetooth Low Energy profiles to ISO/IEEE 11073.

Therefore, SigHealth provides the Personal Health Manager side of the architecture. In order to complete the proposed architecture, a proof-of-concept system for Internet Health Managers was developed and integrated to SigHealth. For this development, an Internet Health Manager was implemented and integrated to SigHealth using web services provided by the platform, as illustrated in Figure 2(b). This Internet Health Manager implements a CoAP-ready ISO/IEEE 11073 Manager and receives measurements from CoAP-ready ISO/IEEE 11073 Agents [9].

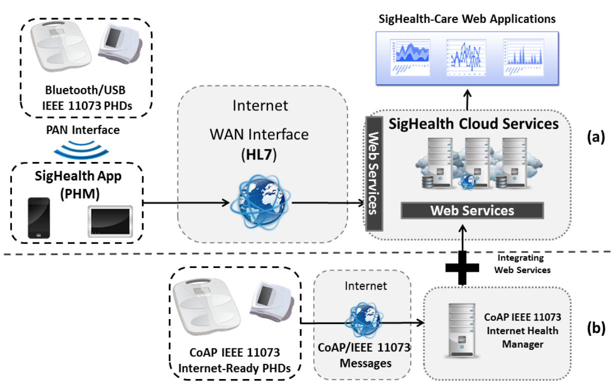

Fig. 2. Extended SigHealth Architecture.

In the implementation of the IHM end-point two open-source tools were used: Antidote IEEE 11073 Library (more details at http://oss.signove.com) and CoAP.NET (more details at http://open.smeshlink.com/CoAP.NET/). Antidote is a portable and lightweight software framework for development of ISO/IEEE 11073:20601 applications. It has a plugin-based architecture which makes possible to add new transport technologies, such as Bluetooth HDP and TCP. Based on this plugin-based architecture, a CoAP plugin for Antidote was developed, creating a CoAP 11073Server. To simulate a PHD, a ISO/IEEE 11073 application, namely 11073Client, was created in a Linux OS platform using the open-source library libCoAP and Antidote. The 11073Client application is the same used in [9], where prior evaluation results showed the feasibility of CoAP and ISO/IEEE 11073 integration, as also, its advantages over TCP/IP sockets.

In this work, we deployed our IHM implementation in the same cloud infrastructure of SigHealth Server. Tests were executed to validate the proposed architecture, focusing on the integration between an already deployed platform based on PHM and a new system based on IHM. In the IHM module we implemented a SigHealth integration module, and created a dynamic simple authentication CoAP service, that creates a new CoAP resource for each new connected 11073Client.That way, we can interpret each new IHM resource as a new virtual manager for each user. Each virtual IHM makes a translation between ISO/IEEE 11073 messages to SigHealth web services format, and sends it to SigHealth Service. As a result, each virtual IHM has the same functionality as a PHM running in a smartphone, creating a flexible solution where it is possible to run health managers on different locations. Figure 3 illustrates the flow between IHMs and SigHealth cloud services.

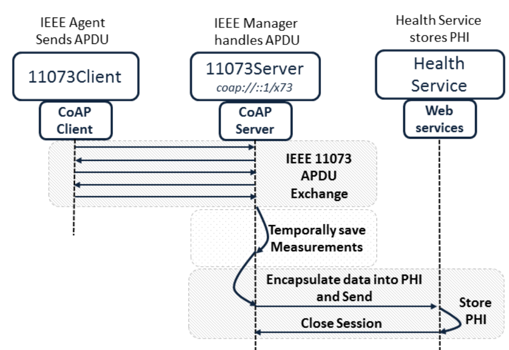

Fig. 3. SigHealth Integration Procedure.

A. Evaluation Tests

We executed tests to validate the integration between PHM-ready SigHealth server, and our new IHM implementation. For PHM tests, we used an Android Smartphone as PHM and a Bluetooth-HDP enabled Oximeter device. For IHM tests, we used as PHD a portable computer running Linux OS and 11073Client application with support to different wireless interfaces, such as Wi-Fi and 3G cellular networks.

In our tests the same user sent messages from different PHDs using both types of managers (PHM and IHM), and all data was received and consolidated at SigHealth Recorder Server and displayed on SigHealth Care Web applications. These tests showed the viability of the integration of different types of managers using the same connected health service.

To validate the IHM implementation based on CoAP we executed a set of tests to evaluate how CoAP/IEEE 11073 integration would behave in a real scenario. The results presented in [9] showed the advantages of CoAP/IEEE 11073 integration against other transport protocols, such as TCP/IP. Now, we evaluated how CoAP/IEEE 11073 integration behaves in real-case scenarios using different physical interfaces, such as Wi-Fi, 3G and 2G cellular networks. As introduced before, we deployed our IHM service in the same cloud infrastructure of SigHealth to minimize the delay overhead between both services. For tests we executed a sequence of simple transactions between the 11073Client and our cloud-based IHM until we reach a confidence level of 95% in our results. Each ISO/IEEE 11073 transaction has a total of 6 packets exchanged between entities. Table 1 resumes the results for each physical transport used.

TABLE I
COAP/IEEE 11073 TRANSACTIONS

PHY	Mean Duration (s)	Retransmissions (%)
Wi-Fi (30Mbps)	0.762s	0 %
3G HSDPA	1.444s	3.2%
2.5G EDGE	5.358s	40.91%

All ISO/IEEE 11073 transactions were completed using retransmission of packets or not, meaning that it complies with ISO/IEEE 11073 communication requirements. Also, based on the results and ISO/IEEE 11073 QoS requirements [13], the CoAP/IEEE11073 integration using Wi-Fi and 3G connections fulfill the latency requirements to be used in a monitoring system that indicates patient state changes in real-time (*delay* $<$3s).

V. CONCLUSIONS

This paper presented an architecture that distributes health managers over different locations, creating a flexible scenario for m-Health solutions. In the core of the proposed architecture is the ISO/IEEE 11073 standard, which enables the use of different transport and application protocols keeping interoperability between different PHDs and Health Services.

We presented concepts and requirements that helped the building process of the proposed architecture, showing the meaning of distributed managers and how this distribution helps building a flexible connected health scenario. A proof-of-concept implementation was developed based on previous works, and a real connected health platform available in the market was integrated. This integration validated the feasibility of the proposed architecture, showing how Internet Health Managers can be integrated with legacy systems that use Personal Health Managers. As a future work, we expect to develop Internet-Ready PHDs using CoAP and Bluetooth Low-Energy interface. We have plans to evaluate security features of CoAP use on healthcare domain, as also, execute scalability studies for the deployment of CoAP in cloud services using HTTP-proxies or not.

ACKNOWLEDGMENT

The authors would like to thank CAPES, Signove and the Embedded/UFCG for the partial support in the development of this work.

REFERENCES

[1] R. Carroll, R. Cnossen, M. Schnell, and D. Simons, “Continua: an interoperable personal healthcare ecosystem,” *IEEE Pervasive Computing*, pp. 90–94, 2007.

[2] *ISO/IEEE 11073-20601: Health informatics - Point-of-care medical device communication - Part 20601:Optimized exchange protocol Standards*, First edition ed., IEEE.

[3] D. Bogia, “Supporting personal health devices through standardization and collaboration,” in *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*, June 2011, pp. 338–343.

[4] R. S. Istepanian, A. Sungoor, A. Faisal, and N. Philip, “Internet of m-health things ”m-iot”,” in *Assisted Living 2011, IET Seminar on*. IET, 2011, pp. 1–3.

[5] P. Swiatek and A. Rucinski, “Iot as a service system for ehealth,” in *e-Health Networking, Applications Services (Healthcom), 2013 IEEE 15th International Conference on*, Oct 2013, pp. 81–84.

[6] L. carvalho, R. Campos, and M. Ricardo, “Context-aware low-energy wi-fi sensor networks for e-health,” in *e-Health Networking, Applications Services (Healthcom), 2013 IEEE 15th International Conference on*, Oct 2013, pp. 361–365.

[7] P. Swiatek, P. Schauer, A. Kokot, and M. Demkiewicz, “Platform for building ehealth streaming services,” in *e-Health Networking, Applications Services (Healthcom), 2013 IEEE 15th International Conference on*, Oct 2013, pp. 26–30.

[8] Z. Ji, X. Zhang, I. Ganchev, and M. O’Droma, “A personalized middleware for ubiquitous mhealth services,” in *e-Health Networking, Applications and Services (Healthcom), 2012 IEEE 14th International Conference on*, Oct 2012, pp. 474–476.

[9] D. Santos, F. Bublitz, H. Almeida, and A. Perkusich, “Integrating ieee 11073 and constrained application protocol for personal health devices,” in *Proceedings of the 2014 ACM Symposium On Applied Computing*. ACM, 2014.

[10] B. F. Shelby, K. Hartke, “Constrained application protocol (coap) draft-ietf-core-coap-13,” *IETF work in progress*, 2013.

[11] D. Santos, A. Martins, H. Almeida, and A. Perkusich, “Upnp and ieee 11073: Integrating personal health devices in home networks,” in *Proceedings of 11th IEEE Consumer Communications and Networking Conference*. ACM, 2014.

[12] M. Isomaki, J. Nieminen, C. Gomez, Z. Shelby, T. Savolainen, and B. Patil, “Transmission of ipv6 packets over bluetooth low energy,” *IETF work in progress*, 2012.

[13] *ISO/IEEE 11073-10101: Health informatics - Point-of-care medical device communication - Part 10101:Nomenclature*, First edition ed., IEEE.