CrossMark

MOBILE SYSTEMS

A Standard-Based and Context-Aware Architecture for Personal Healthcare Smart Gateways

Danilo F. S. Santos[1] · Kyller C. Gorgônio[1] · Angelo Perkusich[1] · Hyggo O. Almeida[1]

Abstract The rising availability of Personal Health Devices (PHDs) capable of Personal Network Area (PAN) communication and the desire of keeping a high quality of life are the ingredients of the Connected Health vision. In parallel, a growing number of personal and portable devices, like smartphones and tablet computers, are becoming capable of taking the role of health gateway, that is, a data collector for the sensor PHDs. However, as the number of PHDs increase, the number of other peripherals connected in PAN also increases. Therefore, PHDs are now competing for medium access with other devices, decreasing the Quality of Service (QoS) of health applications in the PAN. In this article we present a reference architecture to prioritize PHD connections based on their state and requirements, creating a healthcare Smart Gateway. Healthcare context information is extracted by observing the traffic through the gateway. A standard-based approach was used to identify health traffic based on ISO/IEEE 11073 family of standards. A reference implementation was developed showing the relevance of the problem and how the proposed architecture can assist in the prioritization. The reference Smart Gateway solution was integrated with a Connected Health System for the Internet of Things, validating its use in a real case scenario.

Keywords e-Health · Personal health devices · Personal area networks · IEEE 11073

This article is part of the Topical Collection on *Mobile Systems*

✉ Danilo F. S. Santos
danilo.santos@embedded.ufcg.edu.br

Kyller C. Gorgônio
kyller@embedded.ufcg.edu.br

Angelo Perkusich
perkusic@embedded.ufcg.edu.br

Hyggo O. Almeida
hyggo@embedded.ufcg.edu.br

1 Embedded Systems and Pervasive Computing Laboratory, Federal University of Campina Grande, Campina Grande, PB, Brazil

Introduction

Nowadays, a new set of portable sensor devices are available to make it easier the way we take care of our health. Personal Health Devices (PHDs), from wearable sensors to portable and wireless devices, enable patients to share Personal Health Information (PHI) from anywhere at any time. Thus, patients can take care of their health using PHDs at home, and seamlessly share information using Internet services to all their health actors, including caregivers, physicians and family. For example, physicians can define specific monitoring routines based on each patient profile, creating a direct and customized connection with the patient.

This scenario describes what a Connected Health system can provide to end-users [25]. A Connected Health system is composed of multiple components, from a PHD to the Health Service in the cloud. In a general view, the first step is to collect PHI from PHDs using communication technologies, for example, collect blood pressure information from a PHD using a Bluetooth connection. From this starting point, a manager or gateway device forwards PHI to Health Services in the cloud. These gateways are usually personal and portable devices, such as smartphones or tablet computers. Therefore, from the PHD to a Health Service, PHI passes through multiple paths to its destination.

The focus of this work is on the first path, where PHDs connect to Personal Gateway devices through a Personal Area Network (PAN). A PAN can use different technologies, such as Bluetooth or Zigbee. Bluetooth is widely available in different Consumer Electronics and Personal devices. Bluetooth is always evolving, and its latest specifications presented the Bluetooth 4.0 Low Energy (BLE) [4]. Considering the Internet of Things (IoT) paradigm, a new BLE profile was presented enabling the use of the Internet Protocol over BLE [23]. This new profile should increase the number of smart sensors using Bluetooth technology in different contexts, from healthcare to entertainment.

In the Connected Health context, a Personal Gateway device creates a PAN, like a Bluetooth network, and connects itself to multiple devices. Therefore, the PAN is not only used by health-related devices. Other services and devices also share the medium, like audio services, human-interface services, among others. The network sharing usually leads to a decrease in bitrate of some devices, delays in the delivery of packets, and other common congestion limitations. In most of healthcare monitoring situations, these limitations are not relevant; however, during a special situation where information from PHDs is essential for a remote diagnostic purpose, it is necessary that all health sensors participating in a monitoring task share information in an efficient way. For example, during a monitoring task, different types of devices could be used, like a wearable ECG monitor, implantable glucose meter devices and a oximeter. Figure 1 illustrates a scenario where a Personal Gateway connects with multiple devices in the same PAN.

For that reason, it is necessary to understand the healthcare context to identify that a monitoring task is running at a specific moment. Based on this scenario, this article presents a healthcare-aware architecture for PAN Gateways. This architecture enables the prioritization of health streams when necessary, creating a healthcare Smart Gateway. The main scenario of this Smart Gateway is its use at home for Remote Patient Monitoring Services. Therefore, it is important to evaluate the use of these healthcare services in conjunction with other daily and personal services.

For the architecture presented in this article, health context information is extracted from the application layer to support the gateway to identify if a set of PHDs is in a special monitoring situation or not. Based on this context identification, the gateway can decrease the bitrate of some peripheral PAN devices, or even disable them, in order to keep QoS requirements for health devices participating in the monitoring task. One of the main contributions of this work is the use of a standard-based and seamless context information extractor based on the ISO/IEEE 11073 family of standards [13]. By the use of a standardized language, it is possible to identify healthcare monitoring tasks regardless of the devices in the network. Finally, the Smart Gateway
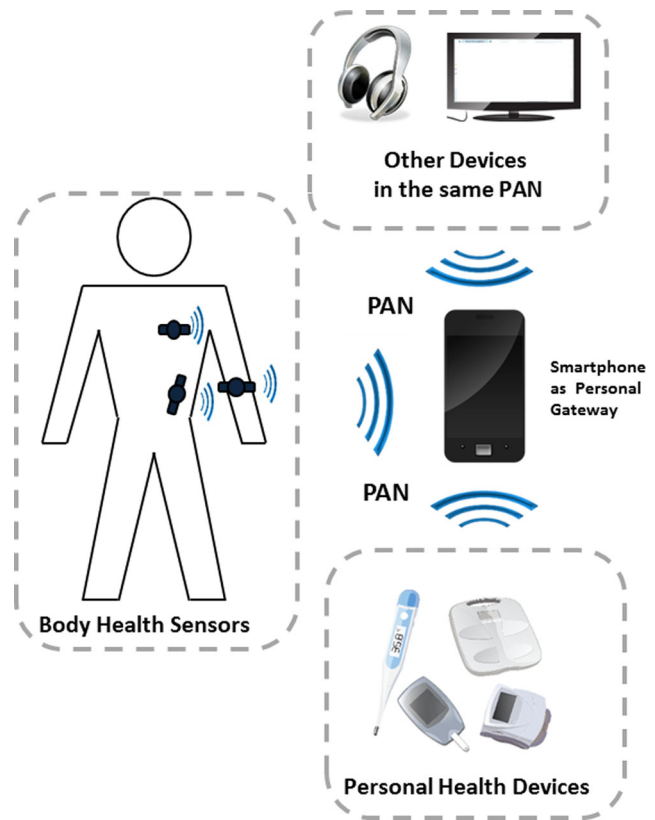
Fig. 1 General view of a personal area network

also uses information acquired during the device registration phase, such as its type and optimal data rate.

The remainder of this article is organized as follows. In Sections "Related works and Standards, technologies and previous work" we present a review of related works, technologies and our previous work. Section "Building the smart gateway for an IoT solution" describes the Smart Gateway architecture and how it works. The architecture evaluation is presented and discussed in Section "Smart gateway development and evaluation" in details. Section "IoT system integration" describes how the Smart Gateway can be used together with a healthcare monitoring system in the Internet of Things. Finally, an overall discussion, current challenges and future works are presented.

Related works

Connected Health systems and technologies have been discussed by the industry and research community for a while, especially when the topic is the adoption of standards and reference architectures. Associations such as IHE (Integrating Healthcare Enterprise)[1] and Continua Health

---

[1] http://www.ihe.org

Alliance[2] work in the definition of guidelines to promote the standardization of communication protocols and interfaces, envisioning a market of standard, affordable and readily connectable health sensors. They define interfaces and profiles to interchange health information, where standards as ISO/IEEE 11073 and HL7[3] are used for comprehensive sharing of personal health data across different services and devices [22].

When the subject is the use of healthcare monitoring systems in Personal Area Networks, some work has been done in the prioritization streams in wireless networks. Rezaee et al. [20, 21] presented a congestion control mechanism based on intermediary nodes placed between the gateway and the Health Service. The work of Niyato [18] also presents a traffic scheduling mechanism from the gateway to the Health Service. Zhou et al. [30] presented a system based on a virtual MAC layer that adjusts QoS parameters for sensors in a Body Area Network using a polling mechanism. A similar transport-agnostic and polling mechanism was used in the work of Ren et al. [19]. Considering the Internet, in [3] an IoT middleware with a use case for healthcare is presented, and in [29], medical applications on IoT are discussed and analyzed. Finally, in [15], a new concept of m-IoT (Internet of m-health Things) is proposed. More challenges and Internet-based architectures and proposals for Wireless Body Area Networks (WBAN) are presented in [9] and [11].

The work of Almashaqbeh et al. [1] presents a cloud-distributed architecture that prioritizes healthcare monitoring streams in WBANs based on QoS requirements. Prioritization is also discussed in the work of Chen et al. [7] where a distributed schedule mechanism is used based on the current patient condition. Lin et al. [17] present metrics for the quality-of-experience (QoE) of health monitoring systems, and use these metrics to create resource allocation schemes in wireless healthcare networks.

In common, all these works do not consider the use of healthcare context information in the application layer to prioritize connection streams in a personal gateway in a PAN. Also, most of these works do not discuss communication aspects related to the standardization of health information on the Internet, and how this standardization can be used to identify healthcare monitoring situations.

In terms of classification and design, smart health monitoring systems are classified in the work of Baig et al. [2], where systems are divided into three main groups: wearable, mobile and remote health monitoring systems. The Smart Gateway presented in this article can be used in any of these systems, as it can be the bridge between wearables and mobile devices. Also, considering Personal Health Devices

with Internet connectivity, the Smart Gateway can be an enabler for remote health monitoring systems in the Internet of Things.

Standards, technologies and previous work

Based on our previous work presented in [27] and [26], an IoT ready architecture for connected health systems was developed and validated. The main characteristic of this architecture is how its PHDs communicate with healthcare services in the Internet. On these previous works, PHDs can communicate directly with services in the cloud using IPv6 as transport, where two types of gateways are defined:

– Health-Gateways, which receives health information from PHDs using specific protocols, and then prepares and forwards this data to the Internet.
– Internet-Gateways, which receives information already formatted in an IP friendly way, and forwards this information to the Internet without changing it.

Thus, one of the main contributions of these previous works is a proposal and evaluation of how health information can be transported by Internet-Gateways. The system uses an integrated solution, where the Constrained Application Protocol (CoAP) [24] is used to carry ISO/IEEE 11073 packets between the PHD and a remote ISO/IEEE 11073 health manager placed in an Internet Health Service. CoAP is a lightweight protocol based on the Representational State Transfer (REST) model and can be considered a real enabler for IoT.

For PHD data communication, the ISO/IEEE 11073 set of standards was used. The ISO/IEEE 11073 declares how medical devices should talk to each other, how each entity should behave, and how medical device information is written and represented. The base standard is the ISO/IEEE 11073:20601 [13], which defines the base-exchange protocol between medical devices and aggregators. Another important standard is the ISO/IEEE 11073:10101 [12], which defines the base nomenclature for medical devices communication. This set of standards was chosen because it is widely adopted by manufacturers and international associations, such as Continua Health Alliance [5] and the IHE (Integrating the Healthcare Enterprise) [22]. The main guideline used by both associations is the Patient Care Device (PCD)[4] domain, which addresses the integration of medical devices into the healthcare enterprise. For example, the PCD part 01 (PCD-01) document addresses communication data formats, and is based on HL7 format, where its semantic is also based on the ISO/IEEE 11073:10101 standard.

---

[2]http://www.continuaalliance.org

[3]http://www.hl7.org

[4]http://www.ihe.net/

Based on these standards and protocols, the previous works presented a scenario illustrated in Fig. 2, where it is possible to identify two types of services presented in a personal gateway, namely Health Manager and Internet Gateway services.

Looking at Fig. 2a it is possible to identify that the Health Manager Service provides Health Data to applications installed on the Personal Gateway. These applications share Personal Health Information with Health Services in cloud. It is important to notice that a single Health Manager Service is shared by all applications. The Health Data generated by the medical sensors are prepared to the Internet by those applications. For example, Health Data can be received using the Bluetooth Health Device Profile [4] or one of GATT Health Profiles of Bluetooth 4.0, and the health application encapsulates it to be transmitted to the Internet in a Simple Object Access Protocol (SOAP) or RESTful message.

In Fig. 2b, Health Data is generated ready for the Internet using IP based protocols, such as using the Constrained Application Protocol (CoAP). In this setup the Internet Gateway Service works over the Personal Area Network module in order to route packets directly to Health Services in cloud. It is important to notice that the Internet Gateway Service is also shared by non-health related PAN devices.

Building the smart gateway for an IoT solution

Considering the scenario described for a congested PAN and the goal of this work, a Gateway is considered a *Smart*
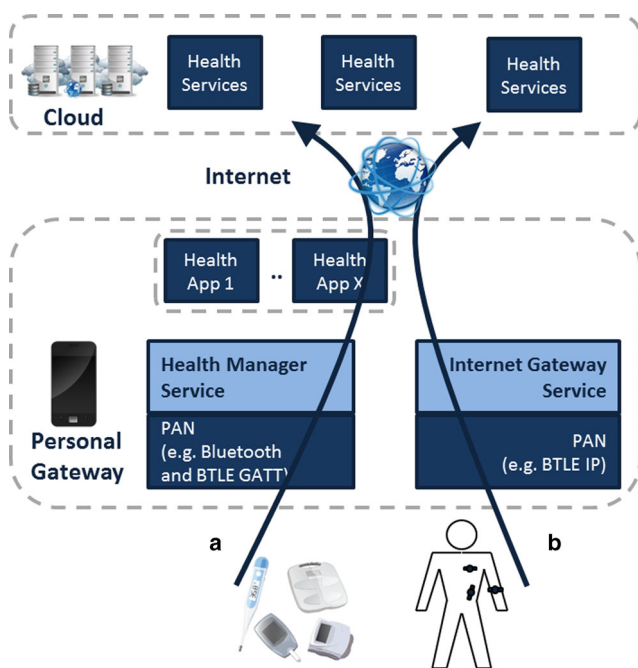
Gateway when it is capable of: identifying a situation that a user or system is experiencing; and adapting the data flow based on that situation. Therefore, some basic requirements have been considered to define the Smart Gateway architecture:

– The Smart Gateway must be able to seamless evaluate the data flow in order to identify a user or system situation;
– The Smart Gateway must be able to identify devices that are part of monitoring process based on information provided by upper layers, such as applications;
– The Smart Gateway must be able to adapt the underlying data flow for devices that are part of a monitoring process based on their network requirements.

Architecture description

Based on the requirements mentioned before and the health information flow described on previous works, where multiple devices share the same wireless PAN, the use of a Healthcare QoS Monitor (HQM) in the Personal Smart Gateway is proposed, as illustrated in Fig. 3. The main objective of HQM is to seamlessly analyze the network traffic from health sensors, and identify situations where they need prioritization against other devices sharing the same PAN. For example, real-time ECG streams generate a considerable data flow in the PAN and, during critical monitoring tasks, it is necessary to prioritize those streams compared to other data-flows, such as multimedia flows and even other medical devices that are not part of the specific monitoring task. The HQM is also responsible to access the PAN module and send commands to disable other services and devices sharing the medium. Disabling these
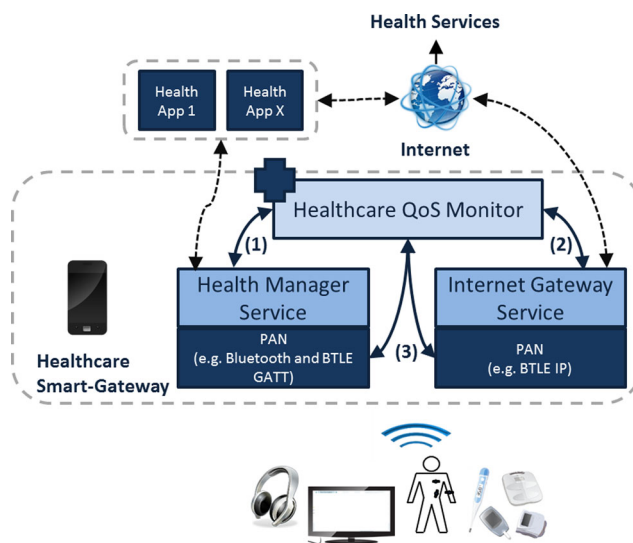

Fig. 2 Health information flow in a personal gateway

Fig. 3 Healthcare Smart gateway overview

services releases the wireless medium, avoiding congestion and delays, making possible to devices participating in the monitoring task to complete their job offering the best Quality of Service for Health Services and end-users.

The main feature of HQM is the use of healthcare context information to identify specific monitoring tasks. A monitoring task happens when a set of health sensors and actuators act together to share health information with Health Services and applications, usually when a specific action or diagnostic is necessary.

In the HQM, context information is extracted from the network traffic of the Health Manager Service and the Internet Gateway Service. In order to understand the health context information, it is necessary to define a standardized language for Health Information generated by medical devices. HQM uses the ISO/IEEE 11073 family of standards as base language and protocol. As introduced before, the ISO/IEEE 11073:10101 standard is used as base semantic for health messages and, therefore, it is used by HQM to understand what type of information is being carried at a specific moment. With ISO/IEEE 11073:10101 nomenclature it is also possible to understand IHE PCD-01 messages, which, for example, is used on Continua Health Alliance WAN interface.

Figure 4 presents a detailed view of the HQM. Three components integrate the core of HQM, namely Health Monitor Evaluator (HME), Device Register (DR) and Monitoring Rules (MR) module. The MR has the base rules to identify monitoring tasks. These rules can be loaded by health applications or services, or they can be extracted observing the behavior of the Smart Gateway over the time. Rules must follow a very simple condition/actions format, describing a series of events and conditions that happens during a monitoring task. After all these events and conditions happen, it means that the Smart Gateway is executing a monitoring task. The DR stores information about health devices, which are collected during a registration phase, such as its optimal stream bitrate requirement and type of data. Finally the HME uses the information from DR and MR to identify a monitoring task and estimate an optimal throughput necessary for each device in the monitoring task.

Two platform-dependent modules are necessary to complete the HQM, namely ISO/IEEE 11073 Extractors (11073Ex) and the Health Medium Controller module (HMC). 11073Ex is the component that receives information from the Health Manager and Internet Gateway services. This module must be compliant with the interfaces provided by those services in order to receive data packets from them. HMC receives commands from HME and decides which peripherals must be disconnected or not. For example, HMC would receive a list of devices that are part of a monitoring task and their respective requirements.

Fig. 4 Healthcare QoS monitor overview
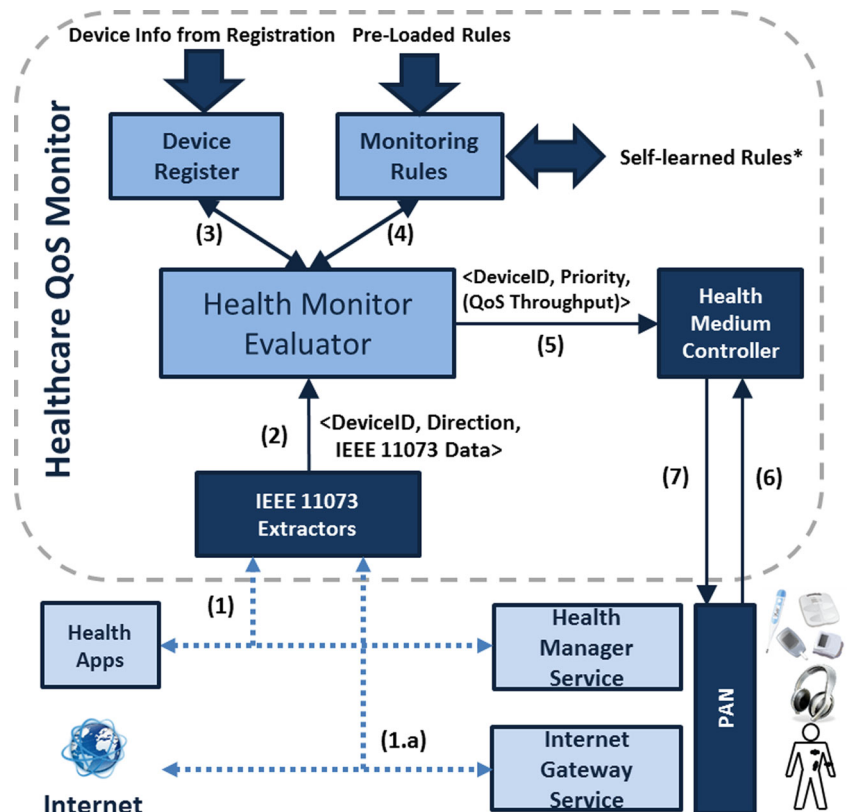
Based on this information and PAN available resources at that specific moment, HMC decides if other peripherals that are not part of the monitoring task must be disconnected or not. HMC is platform-dependent because it must have direct access to the PAN controller in order to disconnect other devices.

Execution flow of the monitor

The execution flow is illustrated in Fig. 4. After listening to packets in the PAN interface (1), 11073Ex extracts ISO/IEEE 11073 data from them, and forwards to the HME (2). HMC uses information about the device from the DR (3) and evaluates rules stored on the MR module (4). HME updates the HMC about the requirements of the current monitoring task (5) sending information about the participating devices, its QoS throughput requirements and priority. HMC compares these requirements with the current PAN status (6), and decides if an action is necessary or not (7).

Internally, the ISO/IEEE 11073 data is extracted using two mechanisms: a packet-capture mechanism (PCAP) in one of the network interfaces, such as the Bluetooth interface in the Internet Gateway Service; and using an ISO/IEEE 11073 Manager that shares formatted data from the Health Manager Service. For example, data can be shared using a DataList XML message like the one presented in Listing 1.

Some points can be highlighted in the message presented in Listing 1. For example, a human-readable version of unit is used to help a simple client application show measurements without any knowledge of ISO/IEEE 11073 unit code numbers. These codes are also available in the message in order to follow ISO/IEEE 11073 semantic.

It is also possible to capture packets that are forwarded directly to Internet Services and are formatted using the HL7 ORU (HL7 *Observation Response Unit*) [22]. This format is used by PCD-01 and Continua Health Alliance WAN

```
<entry>
<meta-data>
<meta name="unit-code">544</meta>
<meta name="unit">%</meta>
</meta-data>
<simple>
<name>Basic-Nu-Observed-Value</name>
<type>float</type>
<value>29.00000</value>
</simple>
</entry>
```

Listing 1 ISO/IEEE 11073 XML DataList Sample

```
MSH|^~\\&|Embedded^ACDE48234567ABCD^EUI
    -64|||20090713090030+0000||ORU^R01^ORU_R01|
    MSGID1234|P|2.6|||NE|AL|||||IHE PCD ORU-R01 2006^HL7
    ^2.16.840.1.113883.9.n.m^HL7\r
PID|||{USERID}^^^Imaginary Hospital^PI ||Doe^John^Joseph
    ^^^^L^A|||M\r
OBR|1|AB12345^AcmeAHDInc^ACDE48234567ABCD^EUI-64|CD12345
    ^AcmeAHDInc^ACDE48234567ABCD^EUI-64|182777000^
    monitoring of patient^SNOMED-CT|||{DATE}+0000\r
OBX|1||528388^MDC_DEV_SPEC_PROFILE_PULS_OXIM^MDC
    |1||||||||X|||{DATE}+0000||||1234567890AABBCCDDEEFF^
    EUI-64\r
OBX|2|NM|150456^MDC_PULS_OXIM_SAT_O2^MDC
    |1.0.0.1|80.5|262688^MDC_DIM_PERCENT^MDC||DEMO^ALINH
    |||R|||{DATE}+0000\r
OBX|3|CWE|67911^MDC_ATTR_MSMT_STAT^MDC|1.0.0.1.1|1^demo-
    data(5)||||||R\r
OBX|4|NA|150452^MDC_PULS_OXIM_PLETH^MDC
    |1.0.0.2|12^123^24^12^234^55^66^77^88^99|262656^
    MDC_DIM_DIMLESS^MDC|||||R|||{DATE}+0000
```

Listing 2 PCD-01 HL7 ORU Sample

interface, and carry ISO/IEEE 11073 words. An example of this format is presented in Listing 2.

The *MDC* prefix identifies regular ISO/IEEE 11073 semantic words, and is widely used in different levels of a connected health system. This type of prefix is a word representation of ISO/IEEE 11073 data fields, which can be translated to codes, as the ones presented in the Listing 1.

An important process is the registration of devices in the Device Register (DR). The registration process is based on the type of device. A regular PHD will be registered by applications, where a regular PHD is a device that does not use an extra description Bluetooth service. These applications register the PHD identification (such as its MAC address), its ISO/IEEE 11073 type (such as blood pressure device), and its network requirements (such as its maximum bandwidth requirement).

For new IPv6 BLE PHDs, it is possible to use an extra service for device registration. These devices will have an extra Bluetooth Low Energy (BLE) GATT[5] service for device requirements registration. This GATT service offers GATT descriptors with additional information about the device, such as its network requirements and its maximum bandwidth requirement. If the device has this GATT service in its BLE list of services, the connection procedure in the Smart Gateway is executed as illustrated in Fig. 5. The procedure starts when a new device is connected to the Smart Gateway. In the master device, a BLE enabled application developed for registration will look for all GATT services presented in the new connected device. If the registration service is presented, the application reads its requirement descriptors and sends this data to the DR service.

---

[5]GATT is the Generic Attribute Profile of Bluetooth Low-Energy

Figure 5 Procedure for device registration using GATT Service
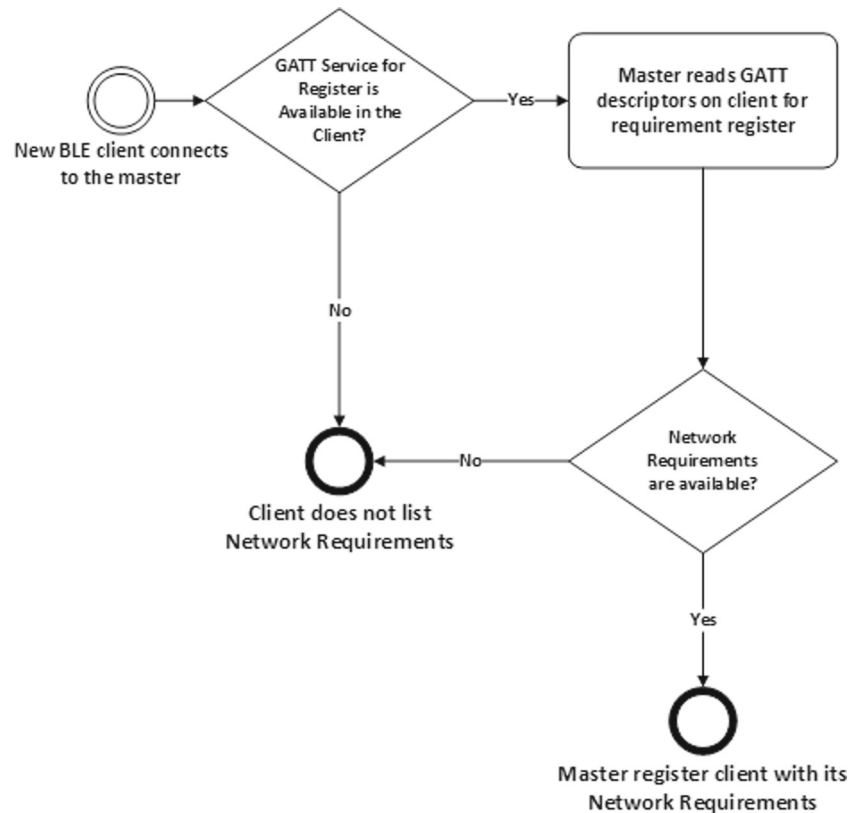
Smart gateway development and evaluation

For evaluation of the proposed solution, firstly it was implemented a prototype version of HQM in a development Linux platform to show the relevance of the problem. It was used the Health Manager Service, namely healthd, provided by the Antidote ISO/IEEE 11073 Library.[6] Antidote is a portable and open-source implementation of ISO/IEEE 11073, which offers a service and data encoder that shares information with applications using different data formats, such as XML and JSON, by a well-defined communication interface.

Although the Smart Gateway is designed for personal devices, such as smartphones, the prototype was implemented in a development Linux platform to simplify data acquisition using development tools, such as Wireshark Network Protocol Analyzer.[7] As the Linux operating system is used underlying mobile platforms, such as Android Platform, the results obtained in the next sections would also apply for these mobile platforms.

For the first prototype, data listening is executed by the Health Manager Service only, using Antidote Health Manager and the DataList format described in the previous sections. In the Smart Gateway, a specific Bluetooth controller application was developed to list connected devices and disable connection streams based on the information received from the Health Monitor Evaluator (HME). HME receives data from the Health Manager as an extractor, and compares it to stored rules.

For this Smart Gateway prototype, a test environment was deployed to create a congested PAN. For the test environment four (4) peripheral devices were used:

– A portable tablet computer used to share audio over Bluetooth (Device A);
– A portable computer simulating a generic oximeter health device sharing information over a serial Bluetooth connection (Device B);
– A fitness heart-rate belt sharing data over Bluetooth 4.0 Low-Energy (Device C);
– A portable computer simulating an ECG body sensor sharing data streams over Bluetooth HDP (Device D).

The Health Manager Service connects with devices B, C and D. Device B and C do not generate ISO/IEEE 11073 directly, however, using a transcoding mechanism [10], the Health Manager Service shares information with HQM using ISO/IEEE 11073 nomenclature and Antidote's Data Encoder format.

---

[6] http://oss.signove.com

[7] https://www.wireshark.org/

To emulate a congested PAN, devices A and B create a constant data-flow of approximately $35\,Kbytes/s$ in the network. Although Bluetooth supports bigger data rates, the threshold of $35\,Kbytes/s$ using multimedia streams demonstrated to be a good disturbed test environment for our purposes.

As a requirement, device D needs constant bitrate of $16.5\,Kbytes/s$ to provide real-time ECG data streams. This information is shared with HQM during the registration phase, which could happen just after the Bluetooth pairing process. If device D is not able to share its ECG streams with this bitrate, its internal data buffers would overflow and, after a specific amount of time, the connection is dropped. If the network is congested, device D will not have access to the medium with the necessary frequency and, therefore, it will not reach the desired bitrate. For example, considering a PHD with data channel with the following definitions:

Definition 1 (PHD Throughput)

Throughput = Tx_{min} in bytes/seconds
Internal Buffer = B_{in} in bytes

Definition 2 (Available Channel)

Available bandwidth = $Tx_{channel}$ in bytes/seconds
Where: $Tx_{channel} < Tx_{min}$

Therefore, the internal buffer B_{in} will be filled after the following time period:

Definition 3 (Internal Buffer Threshold)

Time to internal buffer fill:
$$P_{max} = B_{in}/(Tx_{min} - Tx_{channel}) \text{ in seconds}$$

After the internal buffer fill, the PHD has the following options:

```
when  MDC_DIM_BEAT_PER_MIN  >  100
and  MDC_DEV_SUB_SPEC_PROFILE_ECG  starts
```

Listing 3 Sample Smart Gateway Rule

– Reduces its data reading in the sensors. However, this approach can lead to a reduced precision.
– Discards collected data from sensors until the channel offers bandwidth.
– Disconnects and wait for available bandwidth in the channel.

A test case was executed to demonstrate this buffer overflow scenario, and its results are presented in the graph of Fig. 6. The overall capacity of the network is $C_{max} = 50\,Kbytes/s$, which is shared with all connected devices. In Fig. 6 point (a), device D starts its ECG stream, reaching a bitrate of approximately $15\,Kbytes/s$, as $35\,Kbytes/s$ are used by third-party devices. However, the Tx_{min} for device D is $16.5\,Kbytes/s$ and its internal buffer B_{in} is $8\,Kbytes$, which is the same internal buffer of the Bluetooth hardware. Therefore, after approximately 5.3 seconds, its internal buffer overflows, and the device disconnects, as illustrated in Fig. 6 point (b).

After this test case of failure, a test with HQM implementation was executed. A simple rule was created to identify a critical monitoring task. The rule is presented in Listing 3.

This rule describes that every time a heart rate value bigger than 100 bpm is identified, the ECG device will start a real-time stream. The nomenclature with MDC prefix used in the description is the same as the one used by ISO/IEEE 11073:10101, which is also used by IHE PCD-01 messages. It is important to notice that this rule does not mean that HQM will start the monitoring task; it means that some of the external Health Services or Applications will ask for an ECG stream after that specific heart rate value, and this is probably a diagnostic or critical situation.

Figure 6 Streams without HQM
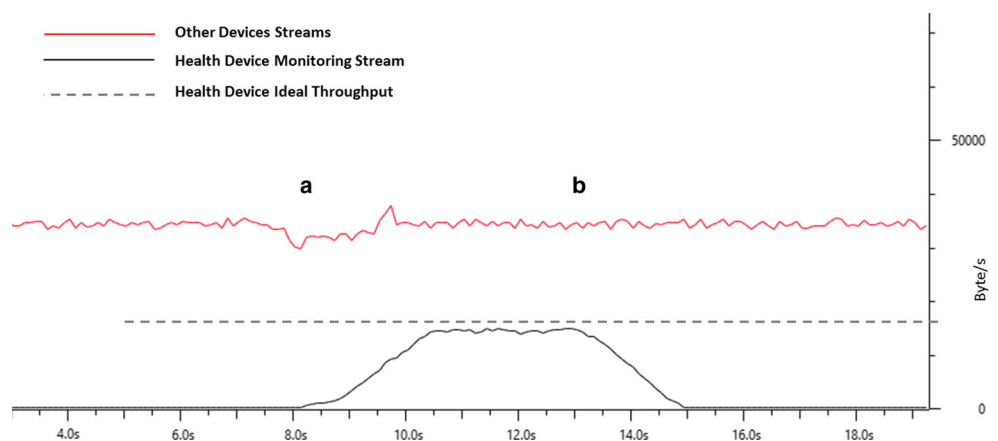
Figure 7 Streams using HQM Prototype
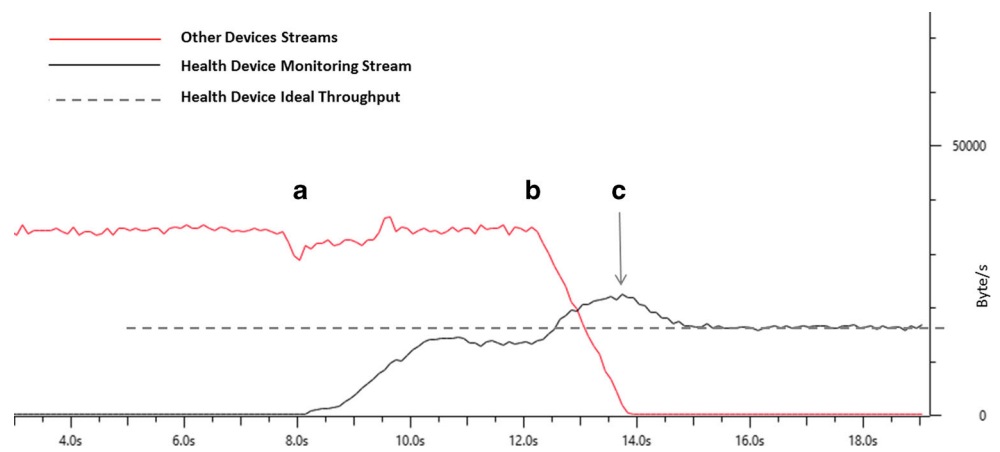
The HQM has additional context information about device D, as its bitrate requirement is $Tx_{min} = 16.5 Kbytes/s$ and its internal buffer is $B_{in} = 8 Kbytes$. An extra parameter is configured in the HMC, which is a hold-on period of $P_{limit} = 80\%$ of P_{max}, where P_{max} is defined in Definition 3. The P_{limit} is the maximum amount time to wait for the desired bandwidth of Tx_{min} in the channel. Results of the use of HQM are presented in the graph of Fig. 7. In Fig. 7 point (a) HQM identifies a heart-rate value bigger than 100 bpm, and just after this point the ECG stream is started, therefore, the Personal Smart Gateway is under a monitoring task. In the prototype implementation, HQM starts listening to bitrate information after a monitoring task is identified. After a time window of two (2) seconds with bitrate below the required for device D, HQM decides to shut down all other peripheral connections in Fig. 7 point (b). After that, the required bitrate is reached for device D, enabling it to share ECG streams in real time, and providing the necessary QoS requirements for the PAN layer. It is important to notice that ECG information is not lost. Figure 7 point (c) indicates that after the wireless medium is free, device D pushes all its buffered data packets, generating a slighting bigger bitrate during a small amount of time.

IoT system integration

To validate the use of the Smart Gateway in an IoT-ready health monitoring system, the proposed gateway was integrated with the previously developed system presented in [27] and resumed in Section "Standards, technologies and previous work". Also, in this integrated system, the ISO/IEEE 11073 nomenclature is still used, therefore, allowing the Smart Gateway to understand its carried data.

In this new system, the focus is on transport health information using Internet Gateway Services. Thus, in the integrated system, the PAN is designed towards the 6LoWPAN protocol, where CoAP messages are carried over different technologies, such as Bluetooth Low Energy [14]. Based on this, it was developed a Bluetooth Low Energy Internet Gateway using an open source implementation of Bluetooth 6LoWPAN module for the Linux Operating System. The merged new standard-based IoT Healthcare System is now integrated with the proposed Smart Gateway as illustrated in Fig. 8. It is important to notice that in this new system, two main paths can be evaluated: between the PHDs and Smart Gateway; and between the Smart Gateway and the Internet Service. Considering that the main purpose of the Smart Gateway is to control the congested PAN, the

Figure 8 IoT healthcare system integrated with a Smart Gateway
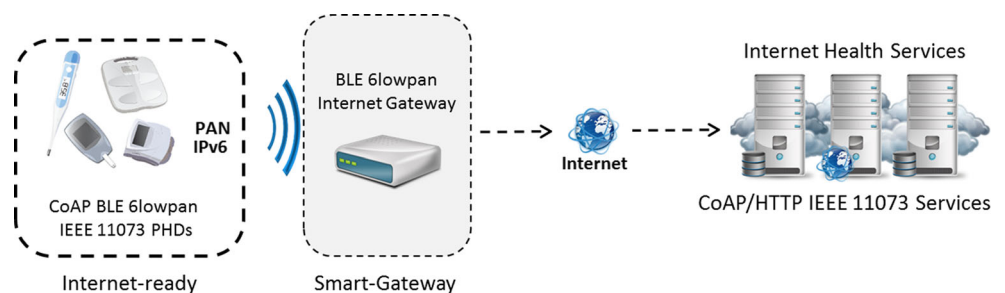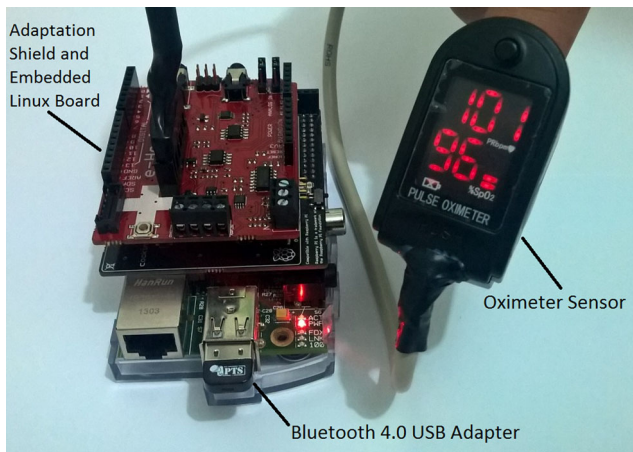
Figure 9 Prototype Personal Health Device with Bluetooth LE 6LoWPAN

rest of this article focuses on the evaluation of this network level.
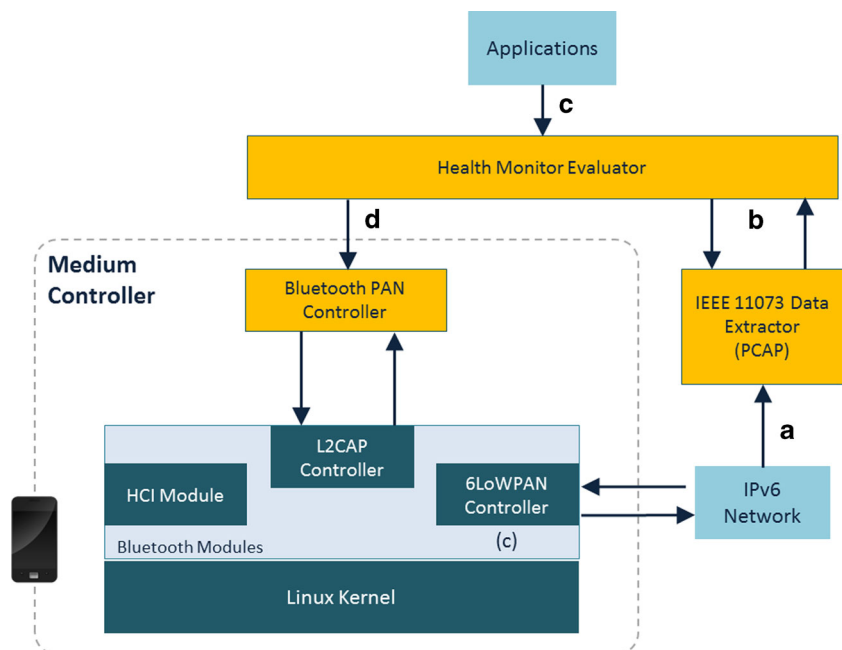
Before adapt the Smart Gateway for IPv6 traffic, test PHD clients using Bluetooth 6LoWPAN and CoAP were developed. In special, the prototype oximeter sensor developed in [27] was adapted to work with Bluetooth 6LoWPAN module on an embedded Linux board, as depicted in Fig. 9. One of the main advantages of using the Bluetooth 6LoW-PAN module on Linux in the client oximeter PHD is that it is possible to keep the same CoAP/IEEE 11073 model adaptation validated and presented in the previous work.

After enabling Bluetooth 6LoWPAN communication on clients, it was necessary to enable it in the Smart Gateway and implement an ISO/IEEE 11073 data extractor from IP

packets. This extractor listens to IP traffic over the Bluetooth 6LoWPAN interface, named btx. During a registration phase, where Bluetooth 6LoWPAN clients register with the Internet Gateway, it is defined the type of device connected to the gateway based on procedures described before. Therefore, the extractor knows beforehand if a Bluetooth 6LoWPAN client is a PHD or not. To be able to listen for all IP traffic passing through the gateway, the extractor has administration privileges, as also, the gateway has permissions to listen the traffic from PHDs. In this first version of the gateway, these permissions are granted offline during a manual configuration phase. In future versions of the gateway, an automatic procedure must be defined due to security and privacy restrictions.

In the Smart Gateway platform, the Linux Kernel Bluetooth Module was enabled to work with 6LowPAN communication, which is a feature available since Linux Kernel version 3.19. To control applications connections, the link layer controller L2CAP module was changed. For IPv6 communication over BLE, a new flow control mechanism based on credits was specified by Bluetooth SIG [4]. This credit control mechanism makes possible to the master device controls when a client is allowed to send packets or not. Thus, instead of the Smart Gateway disconnects a client when its connection is not allowed, the Smart Gateway can refuse renew its credits, forcing this client to wait. This approach is more lightweight comparing with the procedure of disconnection and connection. Based on this new approach, a change in the Linux Kernel L2CAP controller module was developed to make possible to the Health Monitor Evaluator stops the distribution of credits for a specific

Figure 10 Diagram with Implementation Architecture of the Smart Gateway for IPv6 Traffic

client. The overall architecture of the new Smart Gateway for IPv6 traffic is illustrated in Fig. 10.

For the ISO/IEEE 11073 extractor, a service application was developed, which uses a Linux PCAP module to listen to Bluetooth interface. This application was developed to listen and identify traffic based on PCD-01 messages, as described in previous sections. For that reason, the previous developed PHD clients were adapted to send PCD-01 messages, which use ISO/IEEE 11073 semantics.

The execution flow can be described based on Fig. 10. After extracting ISO/IEEE 11073 data from IP packets in Fig. 10a, the IP extractor forwards this information to the HME in Fig. 10b. HME receives rules and device registration information from external applications in Fig. 10c. After evaluate the rules as presented in the previous section, the HME sends a prioritization information to the Bluetooth PAN Controller in Fig. 10d, which sends a message to the L2CAP controller to disable a connection if necessary. It is important to notice that all information regarding the IP enabled PHD is exchanged during the registration phase in the gateway. This information is necessary to execute the calculations exemplified in the previous section.

After this integration, tests were executed to evaluate the use of mixed traffic control in the Smart Gateway, where traffic from Bluetooth 6LoWPAN devices is transported in the wireless medium and through the gateway. In these tests, we were able to use the prototype client PHDs with Bluetooth 6LoWPAN to send measurements to a health service, showing how the Smart Gateway can be seamlessly integrated with already deployed connected health systems.

For these tests, it is necessary to firstly define the maximum bandwidth supported by the master node. When enabling the Smart Gateway for IPv6 over BLE usage, a new Bluetooth hardware controller was necessary. This hardware controller has a different bandwidth threshold if compared with the one used for the first prototype. To determine this

threshold, experiments were executed with the Smart Gateway. These experiments consist of connecting new devices in sequence, and observing when the Bluetooth Controller enters in an unstable state and disconnects. A sample result is presented in the graph of Fig. 11. Evaluating these results, it is possible to observe that in point Fig. 11a, when the third device connects, the master controller enters in an unstable state, and all connections are dropped. As it can be observed, this Bluetooth controller has a maximum supported transmission rate of approximately $2.5 Kbytes$.

Using this information, the Health Monitor Evaluator knows the limit of the Smart Gateway, and based on its rules can prioritize streams using the Bluetooth PAN Controller. A test scenario was developed, when three devices are connected, and the results are presented in Fig. 12. In this test scenario, a *non-health client* is streaming data to the Internet using approximately half of the available bandwidth. At point Fig. 12a, the Health Monitor Evaluator identifies that *health client-1*, which is a 1-derivation ECG emulator, needs more bandwidth because it will change its sample frequency for a period of *30 seconds*. Therefore, in point Fig. 12a, the Health Monitor Evaluator decides to disconnect the *non-health client* by not renewing its BLE credits. After *30 seconds*, *health client-1* disconnects in point Fig. 12b and *health client-2*, which is an oximeter device, can use extra bandwidth to send its data.

It is important to notice that all connected devices are streaming data directly to Web Services, and the Smart Gateway executes its operations just listening through the passing traffic.
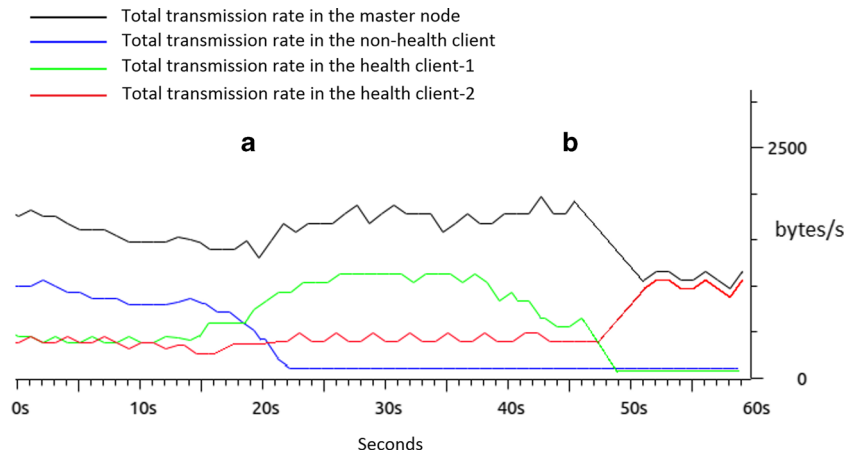
Results and discussion

The objective of this work was to explore how healthcare context information can be used to better adapt network

Figure 11 Streams in a BLE controller using IPv6 connections over 6LowPAN
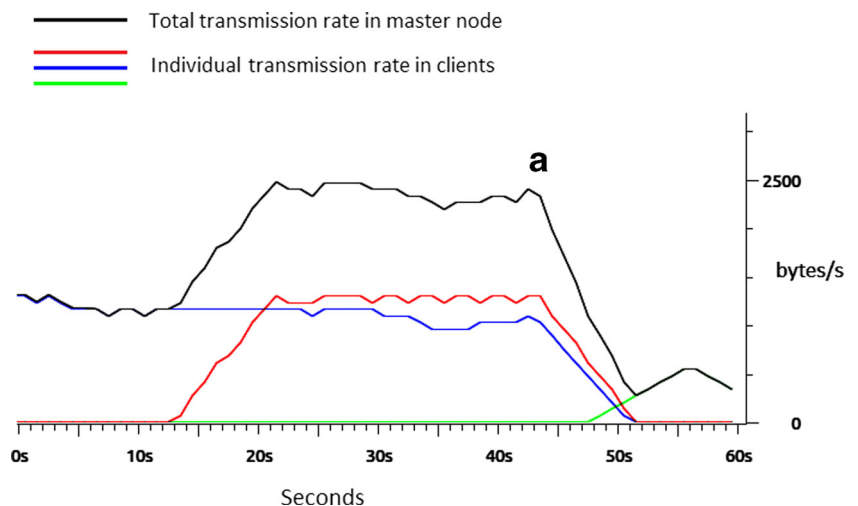
Figure 12 Streams in a Smart Gateway BLE controller using IPv6 connections over 6LowPAN

streams on a PAN in a dynamic way. We observed the advantages of health streams prioritization during a monitoring task. Also, the use of ISO/IEEE 11073 language proved to help in the identification of healthcare flows in a seamless way by the gateway.

Comparing the results presented in this article with related works presented in Section "Related works", we can identify important improvements. Some works present approaches using a virtual MAC, where they can adapt the network data flow based on the context of each connected sensor, such as the BodyT2 [19] and BodyQoS [30] works. However, these proposals make use of a polling mechanism, where the master node requests data from each sensor based on its context. This approach differs from the one presented in this article, where the data flow is adapted in the master node without an active control mechanism for the clients, such as polling. Comparing works that use a multilayer approach for data flow adaptation, the work presented by Carvalho et al. [6] presents an approach where the data flow adaptation is executed at the transport layer using TCP/IP. Although proper for some scenarios, limitations in lower layers, such as the link layer, could create restrictions for the TCP/IP control. As discussed in our work, considering networks with high bandwidth restrictions, such as a BLE PAN, flow control in lower levels must be considered, such as control the data flow using the credit mechanism of Bluetooth 4.1, as developed and evaluated in our Smart Gateway.

When considering the use of context information for data flow adaptation, works such as the ones presented in [16, 20, 21, 28] and [8], present solutions where the data flow adaptation is executed after the gateway, therefore, outside the PAN. The Smart Gateway presented in this article focuses on the data flow control inside the PAN.

Based on the results of the current Smart Gateway, one procedure under definition is the registration channel between the PHD and the Smart Gateway. In the current proposal, during the registration, extra information is exchanged in a simple way, such as buffer size of sensors and maximum streaming throughput for each device. Dynamic network requirements can also be used to reach an optimal throughput for all connected devices based on their current requirements. However, a signaling channel would be necessary to keep this requirement information updated over the time.

Another important point is the use of monitoring rules to identify monitoring tasks. In the current version, rules are loaded by Health Applications and Services into the Smart Gateway. The use of ISO/IEEE 11073 as base standard is also applied in the definition of the rules, making them independent of the available devices and applications. In the future, the Smart Gateway could also be able to learn monitoring patterns based on observation using machine learning methods. This feature would make the Smart Gateway independent of third party Health Applications.

Some challenges still need to be studied. For example, when two monitoring tasks are executed at the same time, it is necessary to prioritize one of them. For this, it is necessary to identify which one is more important than other. Our first approach is to predefine which type of device and connection mode has priority over the other. For example, streams usually have real-time restrictions, and therefore, should have priority over event observation reports. Also, ECG monitors usually have more critical information than a fitness device.

In terms of security, when dealing with Internet Gateways Service, the registration process must be extended. When the PHD generates IP packets ready to be sent to the Health Service, such as in the Bluetooth 6LoWPAN case, usually the body of the message is encrypted due privacy restrictions, for example, using SSL. Therefore, it is necessary to register the Smart Gateway with the Health Service in order to share keys. With these keys, the Smart Gateway would be able to seamlessly monitor the packets from the Internet Gateway Service that goes to a specific Health Service.

From the end-user point of view, some usability challenges should be considered in a final product. Peripheral devices will be disconnected automatically, and this action must be reported to the user in a friendly-way. For example, when a monitoring task is under execution, and the Smart Gateway decides to shutdown other peripherals, an end-user wireless headphone will stop working, and the end-user must be reported about the reason.

Conclusion

In this article we presented a healthcare Smart Gateway for personal and portable devices. It was detailed the motivation of the work as well as the details about concepts and the operation of the Smart Gateway. A reference architecture for healthcare Smart Gateways was described, focusing on how the use of healthcare context information can be extracted from the underlying traffic, and how this information can be used in the prioritization of connections. For this reference architecture, a new component, namely Healthcare QoS Monitor, was introduced and implemented. A prototype was developed to show the relevance of congestion problems in Personal Area Networks, and how the use of healthcare context information could help the prioritization of connections by the use of Health QoS Monitor. This prototype was integrated with an Internet of Things ready health monitoring system, showing how the Smart Gateway can be used with real systems.

As future work we plan to define a self-learning module for the identification of monitoring tasks in order to make the Health QoS Monitor independent of third party applications. Also, we are developing a dynamic Bluetooth Smart controller, which uses the credit-based flow control mechanism of Bluetooth 4.1 to control the maximum bandwidth of connected clients dynamically.

References

1. Almashaqbeh, G., Hayajneh, T., Vasilakos, A. V., and Mohd, B. J., Qos-aware health monitoring system using cloud-based wbans. *J. Med. Syst.* 38(10):1–20, 2014.
2. Baig, M. M., and Gholamhosseini, H., Smart health monitoring systems: an overview of design and modeling. *J. Med. Syst.* 37(2):1–14, 2013.
3. Bazzani, M., Conzon, D., Scalera, A., Spirito, M., and Trainito, C., Enabling the iot paradigm in e-health solutions through the virtus middleware. In: *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 660–665, 2012.
4. Bluetooth SIG: Bluetooth specification version 4.2. Bluetooth Special Interest Group, 2014.
5. Carroll, R., Cnossen, R., Schnell, M., and Simons, D., Continua: an interoperable personal healthcare ecosystem. *IEEE Pervasive Comput.* 90–94, 2007.
6. Carvalho, L., Campos, R., and Ricardo, M., Context-aware low-energy Wi-Fi sensor networks for e-health. In: *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, pp. 361–365, 2013.
7. Chen, B., and Pompili, D., Transmission of patient vital signs using wireless body area networks. *Mobile Netw. Appl.* 16(6):663–682, 2011.
8. Cheng, S., Huang, C., and Tu, C. C., RACOON: a multiuser QoS design for mobile wireless body area networks. *J. Med. Syst.* 35(5):1277–87, 2011.
9. Fortino, G., Di Fatta, G., Pathan, M., and Vasilakos, A. V., Cloud-assisted body area networks: state-of-the-art and future challenges. *Wireless Netw.* 20(7):1925–1938, 2014.
10. Gonzalez Gomez, R., Hughes, R. D., Bogia, D., Shingala, K., Kermes, L., Lima, M., Herbster, R., Pfutzenreuter, E., Ott, L., Barr, J. R., Schatz, G., and Strickland, R., Personal health devices transcoding white paper, v1. 4. Bluetooth SIG, 2012.
11. Hayajneh, T., Almashaqbeh, G., Ullah, S., and Vasilakos, A. V., A survey of wireless technologies coexistence in wban: analysis and open research issues. *Wireless Netw.* 20(8):2165–2199, 2014.
12. IEEE: ISO/IEEE 11073-10101: Health informatics - Point-of-care medical device communication - Part 10101:Nomenclature, first edition edn, 2008.
13. IEEE: ISO/IEEE 11073-20601: Health informatics - Point-of-care medical device communication - Part 20601:Optimized exchange protocol Standards, first edition edn, 2010.
14. Isomaki, M., Nieminen, J., Gomez, C., Shelby, Z., Savolainen, T., and Patil, B., Transmission of IPv6 Packets over Bluetooth Low Energy. IETF, 2014.
15. Istepanian, R. S., Sungoor, A., Faisal, A., and Philip, N., Internet of m-health things - m-iot. In: *IET Seminar on Assisted Living 2011*, pp. 1–3. IET, 2011.
16. Karla, P., Saffer, S. I., Gurupur, V. P., and Suh, S. C., Identification of class of services in the Internet and a proposed approach to traffic prioritization at layer 3. In: *2012 Proceedings of IEEE Southeastcon*, pp 1–5, 2012.
17. Lin, D., Labeau, F., and Vasilakos, A. V., Qoe-based optimal resource allocation in wireless healthcare networks: opportunities and challenges. *Wireless Netw.* 1–18, 2015.
18. Niyato, D., Hossain, E., and Camorlinga, S., Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization. *IEEE J. Selected Areas Commun.* 27(4):412–423, 2009.
19. Ren, Z., Zhou, G., Pyles, A., Keally, M., Mao, W., and Wang, H., BodyT2: Throughput and time delay performance assurance for heterogeneous BSNs. In: *2011 Proceedings IEEE INFOCOM*, pp. 2750–2758, 2011.
20. Rezaee, A. A., Yaghmaee, M. H., and Rahmani, A. M., Optimized congestion management protocol for healthcare wireless sensor networks. *Wire. Personal Commun.* 75(1):11–34, 2013.
21. Rezaee, A. A., Yaghmaee, M. H., Rahmani, A. M., and Mohajerzadeh, A. H., HOCA: healthcare aware optimized congestion avoidance and control protocol for wireless sensor networks. *J. Netw. Comput. Appl.* 37:216–228, 2014.
22. Rhoads, J. G., Cooper, T., Fuchs, K., Schluter, P., and Zambuto, R. P., Medical device interoperability and the Integrating the Healthcare Enterprise (IHE) initiative. *Biomed. Instrum. Technol.* 21–7, 2010.

23. Savolainen, T., Kerai, K., Berntsen, F., Decuir, J., Heydon, R., Zhodzishsky, V., and Callaway, E.: Internet protocol support profile. Bluetooth Special Interest Group - SIG, 2014.

24. Shelby, Z., Hartke, K., Bormann, C., and Frank, B., RFC 7252: The constrained application protocol (CoAP). Internet Engineering Task Force, 2014.

25. Simons, D. P., Consumer electronics opportunities in remote and home healthcare. In: *2008 Digest of Technical Papers - International Conference on Consumer Electronics*, pp. 1–2, 2008.

26. de Souza Santos, D. F., Perkusich, A., and Almeida, H., Standard-based and distributed health information sharing for mhealth iot systems. In: *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 94–98, 2014.

27. de Souza Santos, D. F., Perkusich, A., and Almeida, H., A personal connected health system for the internet of things based on the constrained application protocol - (accepted for publication). Comput. Electr. Eng. J., 2015.

28. Ullah, S., and Kwak, K. S., An ultra low-power and traffic-adaptive medium access control protocol for wireless body area network. *J. Med. Syst.* 36(3):1021–30, 2012.

29. Zhao, W., Wang, C., and Nakahira, Y., Medical application on internet of things. In: *IET International Conference on Communication Technology and Application (ICCTA 2011)*, pp. 660–665, 2011.

30. Zhou, G., Li, Q., Li, J., Wu, Y., Lin, S., Lu, J., Wan, C. Y., Yarvis, M. D., and Stankovic, J. A., Adaptive and radio-agnostic qos for body sensor networks. *ACM Trans. Embed. Comput. Syst* 10(4), 2011.