2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications

Knowledge acquisition and management architecture for mobile and personal Health environments based on the Internet of Things

Antonio J. Jara, Miguel A. Zamora, and Antonio F. Skarmeta
Clinical Technology Lab - Research Institute for Oriented Information and Communications Technologies
Regional Campus of International Excellence "Campus Mare Nostrum", Murcia, Spain
{jara, mzamora, skarmeta}@um.es

***Abstract*—Personalized health capability is limited to the available data from the patient, which is usually dynamic and incomplete. Therefore, it is presenting a critical issue for knowledge mining, analysis and trending. For that reason, this work presents a knowledge acquisition and management platform based on the Internet of Things (IoT). IoT is presenting the capability to connect any object to Internet. These Smart Objects are providing an enormous quantity of data. This work is focused on the personal and mobile health areas, where the integration of clinical devices in the patient's environment, this will enable new services with capabilities to predict health anomalies in real time, send alerts, reminders and offer an enriched feedback to the patient. This feedback will help and motivate to the patients with the treatments adherence and compliance and to follow a healthy lifestyle. In order to reach these services and feedback capabilities, it is required a full integration of the clinical devices and efficient processing of the collected data. The presented knowledge acquisition and management architecture is composed of, on the one hand, a gateway and a personal clinical device used for the integration of clinical devices, wireless transmission of continuous vital signs through 6LoWPAN, and patient identification through RFID. On the other hand, it is complemented with a data model and pre-processing module called YOAPY, which analyses the data from the sensors at the personal devices level. This offers an enriched data to the knowledge-based systems, and this also aggregate the data acquired in order to improve the performance of the communications to the constrains from the Smart Objects in aspects such as low bandwidth, frame size and power consumption. This architecture is being evaluated with an extended set of sensors required for patients with breathing problem in the framework of the AIRE project, it has evaluated the capabilities to provide knowledge acquisition and management from continuous monitored vital signs, the capabilities for diagnosis and detection of anomalies, and finally the support for security and privacy.**

***Index Terms*—Technologies of data management and integration; Internet of Things; mHealth; Identification technologies; knowledge acquisition architecture; Ambient Assisted Living.**

I. Introduction

Internet of things (IoT) is the result of the efforts to provide connectivity and intelligence to convert small devices and common things into Smart Objects [1]. These Smart Objects present high capabilities to integrate and transfer enriched data from environmental sensors, parking, activities, behaviours and clinical devices from mobile health [2] and Ambient Assisted Living (AAL) environments [3]. This huge and enriched data is what defines the Big Data [4]. Big Data brings a lot of opportunities for a wide range of application areas. Particularly, this work is focused on the personalized healthcare, which enables patients to monitor their own environments, i.e. the deployment of custom remote monitoring (remote assistance) and mobile health solutions. This offers the capability to send alerts, predict possible anomalies in real time, and transfer the collected data to an information system, in order to allow the subsequent study of patients and even, thanks to the large amount of data collected may help future researchers improve treatments for diseases or finding new cures. These systems and solutions require more intelligent physiological sensors, highlighting the low power consumption and with advanced wireless communications that allow continuous communication without losing efficiency. Therefore, advance in wireless communications is required in order to connect the health monitoring sensor deployed in patient's AAL, and even integrated into a wearable wireless body area network. We present a system for knowledge acquisition from clinical devices through technologies for communication and ubiquitous access to the data, such as wireless personal devices, embedded systems and smart objects, together with the capabilities presented by the Future Internet with IPv6 protocol and its extension to small and smart devices through technologies such as IPv6 over Low Power Area Networks (6LoWPAN) [5]. In addition, this system has been powered with Radio Frequency Identification (RFID) [6] for the identification of objects, and patients. These technologies are making it feasible to identify sense, locate, and connect all the people, machines, devices and things surrounding us. These new capabilities for linking Internet with everyday sensors and devices, forms of communication among people and things, and exploitation of data capture, define an extension of the usual Intranet of Things to a more Internet of Things [7]. The presented solution is based on the aforementioned integration of clinical devices in the patient's environment. This is presented a pre-processing module at the level sensor in order to offer that intelligence in the clinical devices to enable new advanced services with capabilities to predict health anomalies in real time, send alerts, reminders and offer a better a more enriched feedback to the patient about the health evolution. This feedback will help and motivate to the patients with the treatments adherence and compliance and

978-0-7695-4745-9/12 $26.00 © 2012 IEEE
DOI 10.1109/TrustCom.2012.194

to follow a healthy lifestyle. In order to reach these services and feedback capabilities, it is required a full integration of the clinical devices and efficient processing of the collected data. The pre-processing of the collected data at the sensor-level offers directly a enriched data model, called YOAPY. This data model is required in order to facilitate and offer an efficient knowledge mining in these ubiquitous computing solutions, where thousands of clinical sensors are continuously transmitting data with medical relevant knowledge. Therefore, this sensor-level pre-analysis and the capability to offer a more simplified knowledge representation make these solutions more scalable face to big deployments in nursing houses and patients' environments. This simplified and aggregated knowledge representation is required to minimize the amount of information sent to increase its lifetime, since the constraints from the Smart Objects, such as low bandwidth, low memory, and low power capabilities, since they are mainly powered with batteries. Finally, this data aggregation brings the opportunity to introduce security, integrity, and privacy capabilities, since it is reduced the payload requirements, leaving space for the security overload, and also reducing the number of packets to transmit per second. Thereby, it also leaves CPU time to complete the cryptographic tasks.

The next section presents the architecture for knowledge acquisition and management in the patient's environment. This architecture is integrated in the developed home gateway (Monere), and clinical device integrator (Movital). Then, it is presented the YOAPY module. Finally, it is analyzed the integration of YOAPY in the use case of the proposal for assisted living of fragile patients with serious breathing problems from AIRE project.

II. Architecture Overview

The architecture is presented in Figure 1. This shows the integration of the clinical devices with the tele-health enterprise information and knowledge infrastructure. This architecture is composed of, on the one hand, the home gateway platform, called Monere. This home gateway is located at the patient's house to provide a global connectivity and management capacity. On the other hand, the key element from this architecture is the Movital module. Movital functionality is focused on the integration of the devices for medical purpose from different vendors, which are not following any common standard such as Continua Alliance. The main reason because it has been required the integration of the clinical sensors through Movital instead of consider Continua Alliance solutions has been because the required sensors for patients with serious breathing problems are not available in the market with this standard. Since, they are usually complex patient's monitors in order to carry out accurate capnography, pulse-oximetry linked with electrocardiogram, and finally spirometry.

In addition, the mentioned platforms are not limited to transmitting vital signs data, these elements offer administrative functions for medical error reduction, fault detection, remote device management and, the pre-processing of the gathered data, which are also properties not supported by common clinical devices.

The architecture also presents as is integrated with existing information systems from the tele-health enterprise, such as:

- **Electronic Personal Record (EPR):** EPR is the version of the common Hospital Information System (HIS) for the personalized healthcare.
- **Pro-active monitoring and alerting:** The pro-active monitoring is a track and trend application that enables the triage, the assessment of the measurements coming from the continuous data transmission from a set of clinical devices, and the escalation based on work-flows driven by the measurement values assessment.
- **Remote diagnosis:** This analyses the pre-diagnosis and analyses carried out by the Movital nodes through the YOAPY module, such as it will be presented in the following sections. This remote diagnosis has mainly the goal of guarantee the delivery of an established treatment plan to the chronic patients with breathing problems, that it has in charge, in order to provide them with a real comprehensive care, outside of the hospital.
- **Other Services from the Service Providers Platform:** In addition, to the mentioned modules from the experiences in the AIRE project, it can be integrated with the rest of the developed services from the healthcare providers, as well as with other systems for context management, and external knowledge-bases systems for the intelligent analysis of patient status.

III. Hardware Platforms

The descriptions of Monere and Movital are presented in Sections III-A and III-B, respectively. They are the key elements to introduce the IoT in clinical environments. Monere is the gateway and manager to support ubiquitous data collection and access, whereas Movital is the combination of the IoT-based communication and identification technologies for wireless and mobile integration of clinical devices.

A. MONERE: Home Gateway

Monere is a word from ancient Latin that means watching, advertising and alerting. These are our goals after continuous monitoring through this multi-protocol card which connects a set of clinical devices, environmental sensors and systems through various communication protocols, so as to provide the capabilities to support ubiquitous data collection and global access. This also facilitates the retrieval of information from the different clinical sources, as well as the integration of information with the Information Infrastructure. For that reason, it is considered as the gateway between the sensors and patient, i.e. front-end system with the external information systems, i.e. backend system.

Monere offers a new dimension of networked and scalability capabilities to reach a higher interoperability, medical error reduction, and remote device management (monitor and repair). It also connects all kinds of devices such as sensors, and patient monitors, and collects context information such

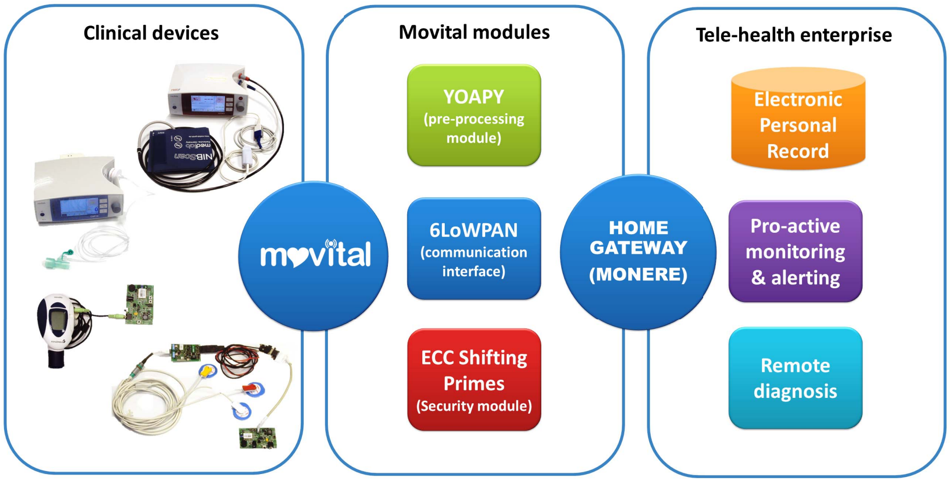

Fig. 1. Architecture overview: clinical devices integration with the tele-health enterprise Information and Knowledge Infrastructure.

as patient's activity, including factors such as environmental status.

A previous version of Monere has been deployed already in a building automation solution [12], and it is being piloted at a hospital. This offers the capacity for continuous monitoring and logging by using the Information Infrastructure through Internet and, at a local level, by having the support of the mentioned compact flash for offline deployments, or in case of connection disruption.

This system has a very flexible and open connectivity support for clinical devices, via RS232 and Bluetooth Health Device Profile (HDP) compliance. Additionally, clinical devices are adapted to 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks), a protocol defined by the Internet Engineering Task Force (IETF) which extends Wireless Sensor Networks to Internet, adding IEEE 802.15.4 a layer to support IPv6. 6LoWPAN presents advantages as regards previous solutions based on Bluetooth, because with this protocol the value is transmitted directly without any user interaction, i.e. user does not need to set up a mobile phone or similar. That feature is interesting for elderly patients who are not accustomed to new technologies, as well as for the extension of coverage from a range of 10-15 to over 100 meters, allowing monitoring of users during usual activities at home, i.e. Activities Daily Living (ADL).

B. MOVITAL: Mobile personal health device

This architecture needs to support the integration and adaptation of clinical devices to IoT technologies, since it is required to provide ubiquitous connectivity. For that reason, Monere platform is completed with a mobile and wireless device in order to integrate clinical devices, Movital (mobile vital sign monitoring). It is presented in Figure 2.

Movital adapts basic communication technologies such as USB/RS232/IrDA (A) to 6LoWPAN, to allow interaction of the collected data with other entities of the architecture. It also integrates RFID technology to allow the identification of patients to personalize the services, and identification of physician for responsibility issues, which is required for environments with multiple patients, such as senior residence, to link data to patient and physician identity.

As a result, Movital is the combination of the mentioned new generation technologies, including SkyeModule M2, from SkyeTek (B) for contactless identification (RFID and NFC), and module Jennic JN5139 for 6LoWPAN (C).

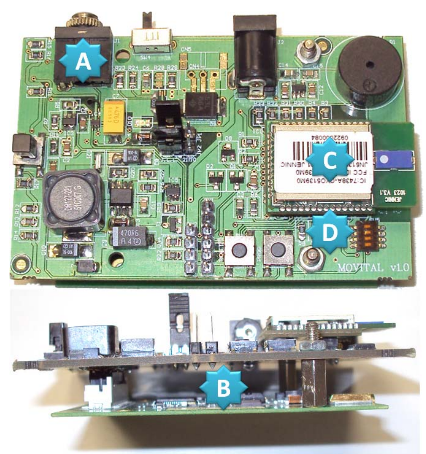

Fig. 2. Movital device to adapt the devices to the Internet of Things, top picture is top view and bottom picture is cross view.

The size of Movital has been minimized to a credit card size for an easier integration. Furthermore, it is powered with reachable lithium batteries to optimize lifetime. This leads to a compact module which acts as an efficient information exchange gateway between clinicians, patients and information infrastructure.

In order to ensure the Quality of Privacy (QoP) and Security, Movital offers security capacities through symmetric-key encryption AES 128 bits, integrity based on CRC16-ITT, and asymmetric-key encryption based on Elliptic Curve

Cryptography (ECC) with the optimization of the Shiting Primes, in order to adapt public key algorithms and support low cost, high performance, and secure authentication [11]. These capacities are required since privacy is the most relevant issues in healthcare and IoT, due to openness and ubiquity features.

Movital also presents a flexible use with a unique module of several sensors; for that reason, we have included a switch to select the device in a determined moment (D).

Specifically, Movital is offering a new generation of clinical devices with advanced capabilities. The usual sensors found in the market are denominated **"simple"**, i.e. a clinical device which offers a single function with low network impact, administration and integration, such as the 3-lead electrocardiogram (Figure 1), which, in turn, is extended with Movital in order to reach **"complex"** clinical devices. **"Complex"** clinical devices not only integrate some administrative functions, they also offer high network capabilities. The next level which is not usually considered for this solution is the **"compound"**, i.e. patient monitors, which presents a multifunction device evolving medium technology, with medium integration, management requirements, and network capabilities. For example, the PEARL100 and CAP10 patient monitors in top of the Figure 1. They monitor multiple vital signs, from pulse-oximeter, electrocardiogram and capnography.

These modules have been extended with the version of Movital in the communications box (A), which includes the 6LoWPAN transceiver by Jennic (B), and a RFID reader to identify patient/nurse (C), see Figure 3.

Fig. 3. Movital device integrated in one of the patient monitors.

Finally, the **"compound-complex"** defines a multiple function system, with highly evolving technology, high administrations, networks and integration capabilities, and even supports clinical decision making. This level is only reached with the Movital and the Monere platforms, since they are able to carry out local and remote processing with intelligent information systems to detect anomalies and evaluate patient's status.

C. Tele-health enterprise platform

The Tele-health enterprise platform integrates of inherited systems from current deployments, such as the Electronic Personal Record (EPR) through an adaptation of the common Hospital Information System, to the definition of new personalized services from healthcare providers, e.g. health status monitoring, e-booking services etc.

The pro-active monitoring, alerting and remote diagnosis are services enhanced with the vital sign data from the physiological sensors connected through the communication architecture proposed. These services based on Knowledge offer a global vision of all the knowledge generated from each node level. It is a critical element to underpin remote consultations of large communities of patients. There are existing low-level data fusion techniques for automated pre-processing of data to identify and model important trends and anomalies in data from the devices. For that reason, this work proposes the pre-processing module, called YOAPY, which is presented in the following section, i.e. Section IV.

IV. Knowledge analysis and management

Personalized and ubiquitous healthcare presents a set of challenges for the definition of the protocols and communication models for reaching a suitable integration, interoperability, security and high performance in terms of lifetime (power consumption) and Quality of Service (delivery delay/latency). In monitored signals, the additional latency incurred by the security operations and pre-process of the RAW data from the clinical sensors is unacceptable. This requires optimizing communication protocols in order to reach a trade-off among lifetime, security level and pre-process of the data from the sensors.

Since, the recent advancements of the wireless communication technologies increase in memory capacity of the Smart Objects and extension to Internet with 6LoWPAN make end-to-end security desirable in these contexts. The communication model is based on UDP traffic type over IPv6 adapted following the last 6LoWPAN specification, i.e. RFC 6282 [5]. This defines an optimized header compression for global addressing based on contexts. 6LoWPAN presents a payload of 92 bytes, which is the result of 127 bytes from IEEE 802.15.4 MAC frame, less 25 bytes from MAC header, and 9 bytes from the IP and UDP compressed headers.

The clinical sensors are adapted from their original protocol to 6LoWPAN, in order to provide Internet connectivity to reach the global and ubiquitous communication capabilities, and treatment of the data provided by the sensors. This pre-processing and data aggregation of the collected RAW data is presented in the following section.

The clinical sensors are adapted from their original protocol to 6LoWPAN, in order to provide Internet connectivity to reach the global and ubiquitous communication capabilities, and treatment of the data provided by the sensors, and finally carry out an analysis of the data gathered by the sensor in order to detect anomalies at a sensor level.

This pre-processing and data aggregation of the collected RAW data is presented in the following sub-sections.

A. YOAPY Data model

The communication between Movital and Monere is carried out with the data model defined by the YOAPY pre-processing and data aggregation module based on domain knowledge in order to reduce overload and optimize payload size. This module is required, since it was initially concluded that the native RAW mode transmission from the clinical sensors presents an intensive quantity of information [13]. Therefore, this produces a delay for real-time and continuous monitoring of vital signs. Since, this generates more information that technologies such as 6LoWPAN and Bluetooth Low Energy are able to transmit. For that reason, YOAPY carries out a pre-processing to analyse the relevant parts from the vital sign to compress the gathered RAW data, and make feasible its continuous and real-time transmission, YOAPY also presents optimizations regarding power consumption through data aggregation, and this introduces security, integrity, and privacy capabilities to the communication.

This section presents three examples of YOAPY for continuous sensors. First, a wearable electrocardiogram, second a patient monitor with electrocardiogram and pulse-oximetry, and finally a patient monitor for capnography. Regarding to discrete sensors such as temperature and peak flow sensor, it is only requiring a byte for temperature value, and the peak flow sensor only two bytes for PEF value, since this version is not calculating FEV, therefore they present a very low requirements (see Figure 1 with the clinical devices integrated).

B. YOAPY for a wearable electrocardiogram

Electrocardiogram (ECG) data compression methods can be found in current research literature. Some of the most relevant studies are based on wavelet-based methods. They reach compression ratios of 18:1 [14]. They focus on the QRS complex, which is a group of waves depicted on an ECG signal. The QRS complex is the most important clinical part of the cardiology system and determines the normal or abnormal arrhythmia occurring in the heart (see Figure 4 for QRS complex identification). The problem is that wavelet-based method is not suitable for the constrained chips located at the platforms from the Internet of Things such as Movital.

For that reason, this work proposes a simpler pre-processed based on representations of the waveform with the amplitude and times of each one of the significant points from the curve [13], i.e. P, Q, R, S and T points, since it is really the relevant information. Figure 4 presents the mentioned significant points, which are transmitted when it is considered the use of YOAPY.

1) Arrhythmia Analysis: An analysis of the ECG wave is carried out in order to determine possibly relevant medical conditions (such as heart arrhythmia) on the patient. This does not replace the diagnosis process from a specialist, but still offers an initial approximation of the patient's health status.

The arrhythmia analysis is carried out through the reconstruction parameters of the PQRST complex (see Figure 4). The complex is pre-processed in order to obtain the segments, ranges, amplitudes and polarities for each one of its curves.

There are several features from the signal that are used to reconstruct the ECG wave: the P wave starting point (P), the

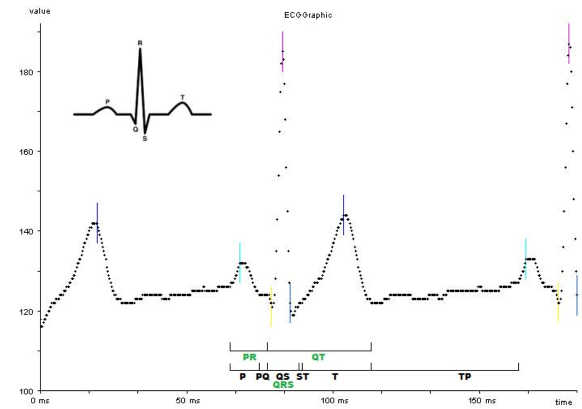

Fig. 4. Patient monitor with an adapted version of Movital integrated, and in the bottom: wearable, portable clinical devices

interval between P and Q (PQ), the interval between S and Q (QS), the interval between S and T (ST), the T segment which presents the beginning of wave T until its end (T), and finally the segment between T and P from the next heartbeat (TP). In addition, a set of intervals with clinical relevance were also considered: the PR interval is the combination of the P and PQ segments, the QT interval is similar to the former and represents the addition of the segments QS, ST and T. Finally, the QRS interval coincides with QS segment, which is calculated for the reconstruction. These intervals can be observed in Figure 4. The signal analysis is carried out directly over the reconstruction parameters, making it less complex and computationally lighter than more traditional approaches. The described intervals and their respective amplitudes and polarities are evaluated according to the following set of rules, which determine the possibility of a patient suffering of some arrhythmia or cardiology disease [16]:

- *Interval QRS > 0.12 sec*: Ventricular hypertrophy, necrosis, BCRD, BCRI, pacemakers, cardiomyopathies, electrolyte abnormalities.
- *Sign U <> Sign T*: Ischemic heart disease, hypokalaemia.
- *Interval PR > 0.20 secT*: Ischemic heart disease, hypokalaemia.
- *Interval PR < 0.12 sec*: Tachycardia, WPW, manners or headphones low rates.
- *Interval QT > 0.45 sec*: Antiarrhythmic medicines, ischemic heart disease, cardiomyopathies, hypocalcemia, mixedema, long QT syndrome.
- *Interval QT < 0.35 sec*: Hypercalcemia, hyperkalemia, early repolarization, digoxin.

C. Time analysis

We chose the EG 01000 ECG module from Medlab, which provides a continuous data channel through a serial interface. This transmits the wave trace of the called V2 in cardiology. V2 is the result wave depending of ECG lead position on the patient, in this case in the fourth intercostal spaces (between ribs 4 and 5) just to the left of the sternum.

In the following we assume a time series x, from the RAW data from the clinical devices such as the electrocardiogram, whose elements are $x^{(k)}$, with k = 1, . . . ,K.

In order to get the analysis and pre-processing of the time series x, we divide the signal into **B**, not equally spaced segments of variable length (L_i), where 1 < i < K.

$$x(1:L_1), x(1{+}L_1:L_1{+}L_2), ..., x(1{+}...{+}L_{K-1}:L_1{+}...{+}L_K) \tag{1}$$

Each segment represents a heartbeat, and **B** is the total of heartbeats from the time-series x. Since, the ECG original protocol has a sampling rate of 300 samples/second (Hz), and a high resolution mode with an accuracy of 150 values per mV. Then, according to the heartbeat rate, i.e. Beats Per Minute (BPM), the sensor will send variable length frame sizes of L_i, such as it can be seen in the Figure 5.

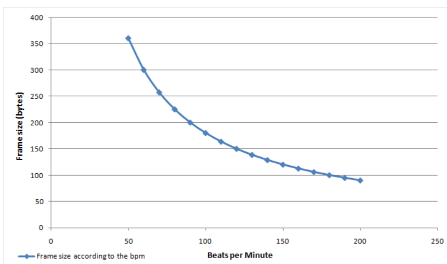

Fig. 5. Size of the frame according to the Beats Per Minute (BPM).

Thus, let us consider a sampling frequency (ω) with a value of 300 Hz. It requires a total of L_i bytes or samples, since each sample has a byte length for each pulse. This $L_i = 236\ bytes$ for the case of $\beta = 76bpm$ (beats per minute), following the equation 2.

$$\frac{60 * \omega}{\beta} = L_i\ bytes, where\ \beta\ is\ the\ heartbeat\ rate\ (BPM) \tag{2}$$

In addition, it is important to determine the interval of time required for each byte measurement, in order to calculate relevant medical intervals used for a pre-diagnosis analysis. The time required per byte, i.e. , it can be determined by following equation 3.

$$\frac{1\,byte/1\,sec}{\omega\,byte/1\,sec} = 3,3\,ms/byte,\ where\ \omega =\ 300\ Hz \tag{3}$$

This means that a electrocardiogram wave, whose elements are the mentioned time series $x^{(k)}$, with k = 1, . . . ,K. has a total transmission requirements equal to Δ, which is defined by the following equation.

$$\Delta = \sum_{i=1}^{K} L_i\ bytes \tag{4}$$

The overload is reduced by YOAPY, for example for a single heartbeat, it is required $L_i = 236\ bytes$, which depends on the heartbeat rate (bpm). This variable byte rate is reduced to a constant byte rate of $L_i = 10\ bytes\ without\ bpm$ and $L_i = 11\ bytes\ with\ bpm$ (see top of the Figure 6). This reduction means that 6 samples are transmitted in a single 6LoWPAN frame, instead of the 4 6LoWPAN frames required per sample in the original RAW format. Therefore, this new format allows the inclusion of 5 samples in a single frame. Therefore, we have a practical reduction of 24 times.

In addition for electrocardiogram wave composed of a set of heartbeats these results are more significant. For example, a electrocardiogram wave composed of 10 heartbeats, with the original RAW format requires 32 frames (see equation 5), but with YOAPY requires less than 2 frames (see equation 6).

$$\Delta_{RAW} \;=\; 2360\ bytes \;=\; 2360/76 \;\simeq\; 32\ frames \tag{5}$$

$$\Delta_{YOAPY} \;=\; 110\ bytes \;=\; 110/76 \;\simeq\; 2\ frames \tag{6}$$

FORMAT FOR ECG

0	1	2	3	4	5	6	7
BPM	P	Q	R	S	T	S_TP	S_PQ
68 0x44	132 0x84	121 0x79	185 0xB9	122 0x80	144 0x90	151 0x97	9 0x09
S_QS	S_ST	S_RS	Other samples … (until a total of 5 samples, it is a fix number to avoid counters)				
32 0x20	3 0x03	71 0x47					

FORMAT FOR CAP10

0	1	2	3	4	5	6	7
etCo2	Breaths per minute (BPM)	Point left X	Point left Y	Point right X		Point right Y	Diag.
12 0x0B	16 0x10	37 0x25	23 0x17	230 0x00E6		28 0x1B	0 0x00
Distance		Other samples					
300 0x012C							

FORMAT FOR PEARL100

0	1	2	3	4	5	6	7
BPM	P	Q	R	S	T	S_P	S_PQ
82 0x52	6 0x44	-4 0xFC	53 0x35	-4 0xFC	15 0x0F	34 0x22	4 0x04
S_QRS	S_ST	S_T	S_TP	SPo2	Diag.		
35 0x23	4 0x04	63 0x3F	56 0x38	99 0x63	0 0x00	Other samples	

Fig. 6. YOAPY data model for the modules ECG, PEARL10 and CAP10.

D. Patient monitor with ECG and Pulse-oximeter

Patient monitor PEARL100 from medlab. This offers a different format, since this offers the ECG wave and SPo2 value. In this occasion, it is also analysed the wave processing peaks from the QRS complex. YOAPY format for PEARL100 clinical sensor is presented in the bottom of the Figure 6. This presents a YOAPY size of 14 bytes per heartbeat, since this includes additional relevant points for the diagnosis. Specifically, this pre-process makes the development of health status monitoring solutions easier, since this is able to include a diagnosis and status byte inferred during the pre-processing, such as it will be analysed for the PEARL100 and CAP10 patient monitors.

E. Capnography

The capnography CAP10 module from medlab offers three relevant values, breath per minute, etCO2, and the etCO2 wave. The wave for each breath has a size of 300-350 bytes. Therefore, it is already required to compress it. The relevant points from the etCO2 wave are the beginning of the inspiration (point left) and the end of this (point right). For this is required, 2 bytes for the left point, and 3 bytes for the right point (since it is over 300 the value, therefore this requires 2 bytes).

The last byte for diagnostic is defined in a similar way that for the electrocardiogram and PEARL100, since the capnographic waveform with its main description features (slope of phase and alpha angle) allow to determinate the status of the treatment. In addition, the etCO2 value determinate, with low level, anomalies such as a diminution of the CO2, hypothermia, reduction of cardiac activity, an excess of alveolar ventilation, or hyperventilation- With a high level determinates excessive production of CO2, hyperthermia, sepsis, a decrease in alveolar ventilation, hyperventilation, or malfunction of the ventilator or a combination thereof [15]. Therefore, the considered values for YOAPY allow the calculation of the slope of phase and alpha angle. Thereby, it is being transmitted, following the domain knowledge, a pre-processing of the monitored data, which allows the aggregation and compression of the data to be transmitted.

V. Evaluation

This work has evaluated the capabilities from 6LoWPAN to support continuous monitoring of vital signs through physiological sensors. This has not only limited to the transmission, else it has also addressed high level requirements such as Quality of Privacy and Quality of Service. For that reason, it has been evaluated, on the one hand, the security capabilities with and without the YOAPY pre-processing module, and on the other hand, the performance based on latency from the different modules.

A. Security evaluation

The presented aggregation models allow to include security support. Specifically, it is considered two security levels; ECDSA, which requires a field of 16 bytes for the digital signature, and AES-CCM-128 Link Layer Security, which requires 21 bytes. They offer integrity and confidentiality, and an additional timestamp is considered to ensure freshness. Overload is summarized in the Figure 7.

The time it takes AES-CCM-128 to encode 51 bytes from payload (64 bytes, since 16 bytes multiple is required) is 61 ms. This is not suitable for the RAW data, since it only can transfer 16 frames per minute and 420 frames are required. But, it is suitable with the 14 frames per minute required after YOAPY module pre-processing.

It is concluded the suitability for continuous data transmission applying symmetric key cryptography based on AES, and the Elliptic Curve Cryptography, also proposed under AIRE project in [11], for establishing the session, since the

Security Level	Security Overload + Timestamp	Available Payload	#frames with RAW data	#samples in a frame with YOAPY less 1 packet per sample
AES-CCM 128bits Layer Security	23bytes + 2bytes = 25bytes	76bytes − 25bytes = 51bytes	257/51 ≈ 6 packets for a sample	(51-1)/10 ≈ 5 samples in one packet
ECDSA 160bits based on ECC	16bytes + 2bytes = 18bytes	76bytes - 18bytes = 58bytes	257/58 ≈ 5 packets for a sample	(58-1)/10 ≈ 5 samples in one packet

Fig. 7. Overload evaluation by security levels and YOAPY.

digital signature with the optimized ECC stack is 765 ms. This latency makes ECDSA unsuitable for the continuous monitoring.

B. Performance evaluation of continuous transmission

The evaluation for the latency and performance for continuous transmission has been carried out with a client-server communications scheme, where it has been sent all the 6LoWPAN packets required by the physiological sensor for a sample through the Movital to the Monere, it has been replied by the Monere with an acknowledgement. Therefore, it is measured the round trip times for the different aggregations modes, i.e. RAW (no aggregation mode) and with YOAPY.

This is also measured with the use of or not of encryption. Since, it has been concluded in the previous section that it is only feasible the continuous data transmission applying cryptography is only feasible with symmetric key cryptography; the following tests are based on AES 128 bits.

1) Evaluation of the PEARL100 (ECG and SPo2): PEARL100 is an evolution of the previously presented electrocardiogram, since this is also considering pulse-oximetry, i.e. SPo2. This offers a variable byte rate between 250 and 300 bytes per heartbeat with $\omega = 300\ Hz$ such as for the presented ECG.

The main results is that the transmission of the RAW format requires a mean time of 43,83 milliseconds for a single sample (breath), i.e. 4 6LoWPAN frames. In addition with encryption it is increased requiring 5 frames and presenting a mean time of 64,78 seconds per sample, This increase of time is coming, on the one hand, because the additional packet, and on the other hand, because the encryption tasks.

This is presenting a high overload. For that reason, it has been proposed YOAPY. This offers the transmission of 5 samples in a single packet, and this requires only 19,67 ms each 5 samples. In addition, it can be encrypted considering 4 samples, and this spends 27,72 ms. This increase is coming specially by the encryption task, which is spending a mean time of 7,5 ms for a packet.

Finally, it can be seen as for RAW data, at the end it starts to accumulate some delay, starting to reach over 500 ms for some transmissions. It is caused because the flooding of the network with the overload presented by the continuous monitoring.

2) Evaluation of the CAP100 (Capnography): This evaluation is also carried out with a capnography monitor, which is one of the sensors from the presented use case for continuous breathing monitoring.

RAW data from CAP10 has a size of 300 bytes per breath. This requires 4 6LoWPAN packets, and this presents a mean time of 38,95 ms for the transmission of the 4 frames and the return of a acknowledgement from the Monere to Movital.

RAW data encrypted requires 5 frames, since it is required to add 23 bytes for each 53 bytes (76 bytes of the payload less the 23 bytes from the checksum code because the AES security overload). This presents a mean time of 46,83 milliseconds. Since, this presents a high overload; it is also used YOAPY aggregation and pre-processing module.

This reduces for the CAP10 to 10 bytes, such as presented in the middle of the Figure 6. Thereby, this is able to transfer until 7 samples in a 6LoWPAN frame for the simple YOAPY version of 10 bytes for the electrocardiogram. This presents a mean time of 19,61 ms.

YOAPY with encryption, based on AES, allows 5 samples in a single frame, i.e. $5 \cdot 10\ bytes = 50\ bytes + 23\ bytes\ of\ security\ overload = 73\ bytes$. This presents a mean time of 27,15 ms. The main difference is the encryption task, which is meaning an overload of around 7.5 ms.

VI. Conclusions

This work has presented a knowledge acquisition architecture, which integrates and transfers enriched data from clinical devices to the knowledge-based information systems.

This architecture is composed physically of the Monere and Movital hardware resources. They make feasible this integration through seamless communication flows between heterogeneous devices, hiding the complexity of the end-to-end heterogeneity to communication service, and supporting security. In addition, it has been defined the YOAPY pre-processing and data aggregation module, in the Movital, in order to generate the enriched data at the clinical device-level.

YOAPY analyses the continuous vital signs from the patient in order to detect anomalies, and reduce the overload. This reduction is required for the IoT, since the constrains in power consumption, bandwidth and memory from technologies such as NFC and 6LoWPAN. In addition, it has been demonstrated that the transmission of the RAW data from the sensor is not feasible with security. However, it is totally suitable for the transmission of the packets with the data model defined by YOAPY with the simplified knowledge representation.

Finally, this knowledge representation offers the most relevant points for representation and diagnosis from the monitored data, and a pre-diagnosis byte, which indicates if it has been detected any anomaly at the sensor level. Thereby, Knowledge Based Systems work over the pre-processed data in order to be more scalable for the management of the huge volumes of data (big data) provided by the sensors.

Ongoing work is focused on the analysis of the overload for a light version of IPv6 for Wireless Sensor Networks called GLoWBAL IPv6 [17], and for new IoT technologies such as Bluetooth Low Energy.

Acknowledgment

This work has been made possible by the means of the Excellence Researching Group Program (04552/GERM/06) from Foundation Seneca, the FP7 European Project IoT6 (grant agreement no: 288445), the Spanish ministry for Industry, Tourism and infrastructure for sponsoring these research activities under the grant "Architecture for Intelligent Respiratory Evaluation (AIRE)" (TSI-020302-2010-95), and the grant from the Spanish ministry for education under the FPU program (AP2009-3981).

References

[1] Atzori, L.; Iera, A.; Morabito. G.; "The Internet of Things: A survey". Computer Networks, Vol. 54, No. 15, pp. 2787-2805, 2010.

[2] Istepanian R.S.H.; Jara, A.; Sungoor, A.; Philips, N.: "Internet of Things for M-health Applications (IoMT)", AMA IEEE Medical Tech. Conf. on Individualized Healthcare, Washington (USA), 2010.

[3] Dohr, A.; et al.; "The Internet of Things for Ambient Assisted Living,", ITNG, pp .804-809, Seventh International Conference on Information Technology, 2010.

[4] J Bughin, M Chui; "Clouds, big data, and smart assets: Ten tech-enabled business trends to watch", McKinsey Quarterly, IT Global Services, 2010.

[5] J. Hui, P. Thubert; "Compression Format for IPv6 Datagrams over IEEE 802.15.4 Based Networks". IETF 6LoWPAN Working Group, RFC6282, 2011.

[6] Shuenn-Yuh Lee; Liang-Hung Wang; Qiang Fang; "A Low-Power RFID Integrated Circuits for Intelligent Healthcare Systems," Information Technology in Biomedicine, IEEE Transactions on , vol.14, no.6, pp.1387-1396, Nov. 2010.

[7] Zorzi, M.; Gluhak, A.; Lange, S.; Bassi, A.; "From today's INTRAnet of things to a future INTERnet of things: a wireless- and mobility-related view", Wireless Comm., IEEE, Vol. 17, no. 6, pp.44-51, 2010.

[8] Jara, A. J.; Zamora, M.A.; Skarmeta, A.F.G.; "An internet of things-based personal device for diabetes therapy management in ambient assisted living (AAL)", Personal and Ubiquitous Computing, Vol. 15, no. 4, pp. 431-440, 2011.

[9] Perakis, K.; Haritou, M.; Koutsouris, D.; "ALADDIN A technology platform for the Assisted living of Dementia elderly INdividuals and their career", International Workshop of Ambient Assisted Living, IWAAN 2009, Part 2, LNCS 5518, pp. 878-881, 2009.

[10] Chung-Chih Lin; Ming-Jang Chiu; Chun-Chieh Hsiao; Ren-Guey Lee; Yuh-Show Tsai; "Wireless Health Care Service System for Elderly With Dementia," Information Technology in Biomedicine, IEEE Transactions on , vol.10, no.4, pp.696-704, Oct. 2006.

[11] Marin, L.; Jara, A.J.; Skarmeta, A.; "Shifting Primes: Extension of pseudo-Mersenne primes to optimize ECC for MSP430-based Future Internet of Things devices". Multidisciplinary Research and Practice for Business, Health Information Systems, Springer, LNCS, 2011

[12] Zamora, M.A.; Santa, J.; Skarmeta, A.F.G.; "An integral and networked Home Automation solution for indoor Ambient Intelligence", IEEE Pervasive Computing, Vol. 9, pp. 66-77, 2010.

[13] Jara, A.J.; Marin, L.; Zamora, M.A.; Skarmeta, A.F.G.; "Evaluation of 6LoWPAN capabilities for secure integration of sensors for continuous vital monitoring", V International Symposium on Ubiquitous Computing and Ambient Intelligence (UCAmI'11), 2011.

[14] R. S. H. Istepanian and A A. Petrosian, "Optimal zonal wavelet based ECG data compression for a mobile telecardiology system", IEEE Trans. Infor. Tech. in Biomedicine, vol.4, no. 3, pp. 200–211, 2000.

[15] John E Thompson, and Michael B Jaffe. "Capnographic Waveforms in the Mechanically Ventilated Patient", Respiratory Care, Vol 50, No 1, January 2005.

[16] A.J. Jara, F.J. Blaya, M.A. Zamora, A.Skarmeta, "An ontology and rule based intelligent information system to detect and predict myocardial diseases",IEEE Inf. Tech. in Biomedicine, ITAB, 2009.

[17] A. J. Jara, M. A. Zamora and A. F.Skarmeta., "GLoWBAL IPv6: An adaptive and transparent IPv6 integration in the Internet of Things", Mobile Information Systems, IOS Press, ISSN: 1574-017x, 2012.