International Journal of Artificial Intelligence,
Spring 2011, Volume 6, Number S11
ISSN 0974-0635;

A Telemonitoring System for Healthcare Using Heterogeneous Wireless Sensor Networks

Dante I. Tapia, Ricardo S. Alonso, Juan F. De Paz, Carolina Zato and **Fernando De la Prieta**

Department of Informatics
University of Salamanca
Plaza de la Merced s/n, 37008, Salamanca, Spain
{dantetapia, ralorin, fcofds, carol_zato, fer}@usal.es

Abstract

E-healthcare has acquired great importance in recent years and requires the development of innovative solutions. This paper presents a telemonitoring system aimed at enhancing remote healthcare for dependent people at their homes. The system deploys a service-oriented architecture over a heterogeneous Wireless Sensor Networks infrastructure to create smart environments. Such architecture can be executed over multiple wireless devices independently of their microcontroller or the programming language they use. Furthermore, the system allows the interconnection of several networks from different wireless technologies, such as ZigBee or Bluetooth. This approach provides the system better flexibility to change its functionalities and components after deployment than other analyzed proposals. The system description, its architecture, and preliminary results of the system prototype implemented in a real environment are presented.

Keywords: *Wireless Sensor Networks, Healthcare, Telemonitoring, Service-Oriented Architectures.*

Computing Classification System: C.2.1. J.3

1. INTRODUCTION

There is an ever growing need to supply constant care and support to the disabled and elderly, and the drive to find more effective ways of providing such care has become a major challenge for the scientific community. The World Health Organization has determined that in the year 2025 there will be 1 billion people in the world over the age of 60 and twice as many by 2050, with nearly 80% concentrated in developed countries (WHO, 2007). Furthermore, over 20% of those people over 85 have a limited capacity for independent living, requiring continuous monitoring and daily assistance (Erickson, *et al*., 2000). The importance of developing new and more reliable ways of providing care and support for the elderly is underscored by this trend, and the creation of secure, unobtrusive and adaptable environments for monitoring and optimizing healthcare will become vital.

Home healthcare telemonitoring systems allow a patient's state and vital signs to be supervised by specialized personnel from a remote medical center. Such telemonitoring systems usually consist of a home monitoring subsystem, a remote monitoring subsystem in the medical center and a network which interconnects both (Bai, *et al*., 2000). A telemonitoring system for healthcare needs to continuously keep track of context information about patients and their environment. The information may consist of many different parameters such as location, the building temperature or vital signs (*e.g.*, heart rhythm or blood pressure). Most of the context information can be collected by distributed sensors throughout the environment and even the patients themselves. To facilitate the deployment of these sensors, it is preferable to use Wireless Sensor Networks (WSNs) (Yick, *et al*., 2008) instead of wired networks (Sarangapani, 2007) (Ahmed, *et al*., 2006). In existing smart environments (*i.e.*, environments that interact with users through sensors and actuators in a pervasive and ubiquitous way) (Weiser, 1999), wiring the location is more uncomfortable and difficult than using wireless devices. In the case of the biomedical sensors that monitor the patient's vital signs, it could be quite bothersome for patients to wear a mesh of wires. One solution would be to use a Wireless Body Area Network (WBAN) formed by sensors and wearable computers (Jurik and Weaver, 2008) (Narayanaswami and Raghunath, 2002).

Whether in home automation, healthcare telemonitoring systems or hospitals, WSNs are used for collecting information from the users and their environment. WSNs are formed by a set of devices called sensor nodes, each of which is habitually formed by a microcontroller, a radio transceiver and a sensor or actuator mechanism (Sarangapani, 2007). Some nodes act as routers that can forward data that must be delivered to other nodes. Traditional networks are aimed at providing high QoS (Quality of Service) (Chen, 2007), while WSN protocols must focus primarily on saving power (Correia, *et al*., 2007). Examples of wireless technologies for building WSNs are ZigBee/IEEE 802.15.4, Bluetooth and Wi-Fi.

Nonetheless, the development of software for remote telemonitoring that integrates different subsystems demands the creation of complex and flexible applications. As the complexity of an application increases, it needs to be divided into modules with different functionalities. Since different applications could require similar functionalities, there is a trend towards the reimplementation of such functionalities (Costa, *et al*., 2008). Although it implies more development time, it is generally the easiest and safest solution. Nevertheless, reimplementation can lead to duplicated functionalities and more difficult system migration. An alternative to such an approach is the reutilization of resources that can be implemented as part of other systems. This trend is the best solution in the long-term and can be realized using a common platform. However, it is difficult to perform because the systems in which those functionalities are implemented are not always compatible with other systems. An alternative for solving this problem is to use distributed architectures.

This paper presents a context-aware telemonitoring system aimed at enhancing healthcare for dependent people at their homes. The system utilizes the SYLPH (*Services laYers over Light PHysical devices*) experimental architecture that integrates a SOA (Service-Oriented Architectures) approach with heterogeneous WSNs. The architecture provides the telemonitoring system with a flexible distribution of resources and facilitates the inclusion of new functionalities in highly dynamic smart environments. Unlike other SOA-WSNs architectures, SYLPH allows both services and services directories to be embedded into nodes with limited computational resources regardless of the radio technology they use.

The next section introduces the problem description and explains why there is a need for defining a new telemonitoring system. Then, the main functionalities and capabilities of the system and its architecture are described. Finally, the results and conclusions are presented, including future lines of work.

2. PROBLEM DESCRIPTION

One of the key aspects for the construction of telemonitoring systems is obtaining information about the patients and their environment through sensor networks. This section presents the strengths and weaknesses of existent telemonitoring developments and analyzes the feasibility for implementing a distributed architecture for integrating heterogeneous WSNs. This section also discusses some of the most important problems of existent functional architectures for WSNs, including their suitability for constructing intelligent environments.

As a result of extensive research, biomedical sensors have become more inexpensive, accurate and reliable (Cote, *et al*., 2003). Moreover, biomedical sensors are now wearable and even implantable (Lymberis, 2005). Nevertheless, biomedical sensors (*e.g.*, electrocardiogram, blood pressure, etc.) and automation sensors (*e.g.*, temperature, light, etc.) differ significantly in how they collect data. On the one hand, biomedical sensors obtain continuously information about vital signs that is important and should not be lost (Fazel-Rezai, *et al*., 2007). On the other hand, automation sensors obtain information at a lower frequency than biomedical sensors (Sarangapani, 2007) because this information is generally less important than vital signs. In a telemonitoring scenario, it is necessary to interconnect WSNs from different technologies (Jurik and Weaver, 2008), so having a distributed platform for deploying applications over different networks facilitates the developers' work and the integration of the heterogeneous devices.

There are several telemonitoring healthcare developments based on WSNs (Jurik and Weaver, 2008) (Varshney, 2008) (Andreasson, 2002) (Gonçalves, 2008). However, they do not take into account their integration with other architectures and are difficult to adapt to new scenarios (Satyanarayanan, 2002). This is because such approaches do not allow sensors and actuators to communicate directly with one another, and instead gather data in a centralized way. Excessive centralization of services negatively affects system functionalities, overcharging or limiting their capabilities (Ardissono, *et al*., 2004) (Voos, 2006). Figure 1 shows a centralized versus a distributed model for integrating heterogeneous WSNs. A centralized model consists of a central component that gathers all the data forwarded by the nodes connected to it. The main component can be a computer with several wireless hardware interfaces (*i.e.*, wireless network cards). Each of these interfaces is connected to one or more of the WSNs deployed in the system. This way, this central component can be, in fact, formed by more than a physical network node, as that shown in Figure 1, represented by two green nodes. At a physical or hardware interface level, the central component in Figure 1 acts as two network nodes, but at a logical or software level, this main component performs as just one node, being aware of the different networks to which it is connected. Furthermore, the central component can be even a distributed computer network formed by several logical nodes, but centralizing anyway the knowledge of network nodes inside it. One of the main problems in this kind of model is that most of the intelligence of the system is centralized. That is, the central component is the responsible for knowing what nodes are in all WSNs. Thus, it gathers the required data from the nodes and, based on such data, decides what commands will be sent to each node. That means that a node belonging to a certain WSN does not know about the existence of another node forming part of a different WSN, although this WSN is also part of the system. This problem can be seen in Figure 1a. In such centralized model, if a certain measurement in a sensor in the WSN #2 has to provoke an action to be performed by an actuator in the WSN #3, the responsible of taking the decisions and invoking the commands in the actuator will be the central nodes. The thinner broken lines between nodes on Figure 1 represent links at each network layer level, whilst thicker lines represent the communication at the application layer level between the nodes implied in the given example. The thinner broken lines around the WSNs represent the knowledge area at the application level. That is, nodes sited inside one of this knowledge area can communicate amongst them directly at the application level. In this centralized model, it is difficult for the system to dynamically adapt its behavior to the changes in the environment, because the decision logic on the central nodes has to be changed every time a new functionality (*i.e.*, sensor or actuator) is added to the system.

Nonetheless, this model can be improved using a common platform where all the nodes in the system can know about the existence of any other node in the same system no matter the technology they use. This is achieved by adding a middleware logical layer over the existing application layers on the nodes. Figure 1b shows a distributed model for integrating heterogeneous WSNs. It can be seen how only one knowledge area now covers all the WSNs. That is, following the previous example, the sensor node in the WSN #2 knows about the existence of the actuator node in the WSN #3, so the sensor node can send a command to the actuator node directly at the application layer level. A service-oriented approach is adequate for being implemented in wireless sensor nodes due to it allows distributing the functionalities of the system into small modules. Such small modules are ideal for being executed by devices with limited computational resources as wireless sensor nodes. This platform covers aspects relative to services such as registration, discovering and addressing. The code executing in a certain node can invoke functionalities (*i.e.*, services) offered by any other node in the system, regardless the latter node is in the same WSN or not. This way, the central component now only has to act as a gateway amongst the distinct WSNs connected to it. Thus, it has not to keep track of either the nodes in the system or the functionalities they offer. Some nodes in the system can integrate services directories for distributing the registration and discovering of services. A node can know about the existence of other nodes and services offered by them. Therefore, it can directly communicate with other nodes in order to execute commands or gather data. Moreover, a node belonging to the system can react to a certain change in the environment with no need of having into account all the factors involved on the system. In addition, the node registration is done in the corresponding WSN and the service registration is maintained by the service directories. Consequently, the process of connecting a new node offering additional functionalities to the system is performed in a dynamical way.

In classic functional architectures their modularity and structure are oriented to the systems themselves. However, modern functional architectures such as SOA allow functionalities to be created outside the system, as external services linked to it. Thus, distributed architectures look for the interoperability amongst different systems, the distribution of resources and the independency of programming languages (Cerami, 2002). SOA proposes a model based on a collection of services and a communication way between them. The communication can involve a simple interchange of data, two or more services coordinating a certain activity, etc. A service can be defined as a function that must be well-defined, self-contained, and non-dependent of the context or the state of other services (Cerami, 2002). Services are integrated through communication protocols that have to be used by applications to share resources in the network (Ardissono, *et al.*, 2004). The compatibility and management of messages that the services generate to provide their functionalities are important and complex elements in any of these approaches. Some developments try to reach integration between devices by implementing some kind of middleware, which can be implemented as reduced versions of virtual machines (Simon and Cifuentes, 2005), middleware (Souto, *et al.*, 2005) or multi-agent approaches (Freitas, *et al.*, 2008). However, these developments require devices whose microcontrollers have large memory and high computational power, thus increasing costs and physical size. These drawbacks are very important regarding WSNs, as it is desirable to deploy applications with reduced resources and low infrastructural impact, especially in healthcare telemonitoring scenarios.

There are different technologies for implementing WSNs, such as ZigBee or Bluetooth. The ZigBee standard allows operating in the ISM (Industrial, Scientific and Medical) band, which includes 2.4GHz almost all over the world (Huang and Pang, 2007). The underlying IEEE 802.15.4 standard is designed to work with low-power and limited resources nodes (Singh, *et al.*, 2008). ZigBee incorporates additional network, application and security layers over IEEE 802.15.4 and allows more than 65,000 nodes to be connected in a mesh topology network (Baronti, *et al.*, 2007). Another common standard to deploy WSNs is Bluetooth. Bluetooth allows multiple WPAN (Wireless Personal Area Network) or WBAN (Wireless Body Area Network) applications for interconnecting mobile devices or biomedical sensors. Bluetooth also operates in the 2.4GHz band and allows creating star topology networks (called *piconets*) of up to 8 devices, one acting as master and the rest as slaves, but it is possible to create more extensive networks, known as *scatternets*, through devices that belong simultaneously to several networks (Ilyas and Dorf, 2003). However, it is not easy to integrate devices from different technologies into a single network (Marin-Perianu, *et al.*, 2007) (Rogers, *et al.*, 2009) (Lei, *et al.*, 2006). The lack of a common architecture may lead to additional costs due to the necessity of deploying non-transparent interconnection elements amongst different networks. Moreover, the developed elements are dependent on the application to which they belong, complicating their reutilization.

The architecture for the telemonitoring system presented in this paper tackles some of these issues by enabling an extensive integration of WSNs and providing a greater simplicity of deployment, optimizing the reutilization of the available resources in such networks. The architecture integrates a SOA approach for facilitating the distribution and management of resources (*i.e.*, services). A distributed architecture provides more flexible ways to move functions to where actions are needed, thus obtaining better responses, autonomy, services continuity, and superior levels of flexibility and scalability than centralized architectures (Cerami, 2002) (Camarinha-Matos and Afsarmanesh, 2007). Unfortunately, the difficulty in developing a distributed architecture is higher (Rigole, *et al.*, 2002). It is also necessary to have a more complex system analysis and design, implying more time to reach the implementation stage. There are several developments to integrate WSNs and a SOA approach (Marin-Perianu, *et al.*, 2007) (Meshkova, *et al.*, 2008) (Song and Lee, 2008) (Prinsloo, *et al.*, 2006). However, those developments do not consider the necessity of minimizing the overload of the services architecture on the devices. In contrast, our solution allows the services to be directly embedded in the WSN nodes and invoked from other nodes either in the same network or another network connected to the former. It also specifically focuses on using devices with small resources to save CPU time, memory size and energy consumption, which is very useful to design and construct smart environments. Furthermore, as previously mentioned, the system contemplates the possibility of connecting WSNs based on different technologies.

3. A NEW TELEMONITORING SYSTEM FOR HEALTHCARE

This section describes the main features of a telemonitoring system designed and developed with the aim at improving healthcare of dependent people at their homes. The system utilizes WSNs for obtaining context information about users (*i.e.*, patients) and their environment in an automatic and ubiquitous way.

The system uses a network of ZigBee devices placed throughout the home of each patient to be monitored. Figure 2 shows the basic schema of the telemonitoring system. The patient carries a remote control (a small ZigBee device embedded in a wristband) that includes an alarm button which can be pressed in case of emergency or the need for remote assistance. There is a set of ZigBee sensors that obtain information about the environment (e.g. light, smoke, temperature, etc.) and react to changes (e.g. light dimmers and fire alarms). Each ZigBee node includes an ATmega1281 microcontroller with only 8KB of RAM and 128KB of Flash memory and an AT86RF231 transceiver, working at 2.4GHz band and consuming only a few µA in sleep mode (n-Core, 2010). There are also several Bluetooth biomedical sensors placed over the patient's body. Biomedical sensors allow data about the patient's vital signs to be acquired continuously. Each patient carries an Electrocardiogram (ECG) monitor, an air pressure sensor acting as respiration monitor, and a triaxial accelerometer for detecting falls. These Bluetooth devices use a BlueCore4-Ext chip with a RISC microcontroller with 48KB of RAM. All ZigBee and Bluetooth devices can offer and invoke services (*i.e.*, functionalities) within the network. There is also a computer connected to a remote healthcare center via Internet for forwarding possible alerts to caregivers and allowing them to communicate with patients. This computer acts as a ZigBee coordinator and is also the master of a Bluetooth network formed by the biomedical sensors as slaves. Thus, the computer works as a gateway interconnecting both WSNs. If the size of the patient' home were be too large, it could be possible to add more gateways for allowing Bluetooth sensors to not lose their connection with the system and to transmit continuously the patient's biomedical data to it.

Figure 3 shows an example of the system operation. In this case, a smoke sensor detects a higher smoke level than a previously specified threshold (1). Then, it invokes a service offered by the node which handles the fire alarm, making it to ring (2). At the same time, it also invokes a service offered by the computer that acts as both ZigBee master node and Internet gateway (3). Such gateway sends an alert through the Internet towards the remote healthcare telemonitoring center (4). At the remote center, the alert is received by a monitoring server (5), which subsequently queries a database in order to obtain the information relative to the patient (6) (*i.e.*, home address and clinical history). Then, the monitoring server shows the generated alert and the patient's information to the caregivers (7), which can establish a communication over VoIP (Voice over Internet Protocol) or by means of a webcam with the patient's home in order to check the incidence. The patient can also ask for assistance by pressing its manual alert button (using the personal remote control) or making a call through the VoIP terminal. In the example in Figure 3, the caregiver decides to request the monitoring server to start a voice and video communication with the patient's home (8). The monitoring server starts such communication through VoIP (10). As the gateway in the patient's home accepts it automatically (11), now the caregiver can see the patient and talk with him (12). Several webcams can be deployed through the patient's home to assure the chance of establishing the communication with the patient. If the patient is conscious, he can also talk with caregivers and explain the situation (13). If necessary, caregivers will call the fire department, send an emergency ambulance to the patient's home and give the patient instruction about how he should act.

Although the system is mainly focused on monitoring tasks, it also provides useful features to patients and caregivers. For example, the remote center can consult RSS (Really Simple Syndication) sources to obtain weather reports or entertainment options for patients and inform them of their scheduled medical staff visits. This information is shown on a graphical user interface on a display connected to the computer at home. Moreover, the system is not only restricted to teleassistance but also performs home automation tasks, so that a light sensor can dim a lamp by invoking a service stored in the dimmer actuator node connected to the lamp. Furthermore, patients are not only monitored at their home, but also at the medical center when they arrive for an appointment with the doctor. The ZigBee remote control carried by each patient has a unique identifying electronic label. There are ZigBee and Bluetooth networks throughout the medical center so that the ZigBee identification label and its Bluetooth biomedical sensors can automatically connect to the corresponding patient. Moreover, the same wireless devices are useful for patients checked into the medical center because the system receives all the data gathered by the Bluetooth sensors located on the patient's body, and the caregivers will be warned if a patient is at risk. Furthermore, medical personnel as doctors and caregivers also carry ZigBee devices with identifying electronic labels, so the system keeps track of their location and movements. This allows obtaining information relevant to optimize the number of personnel necessary for taking care of each area in the center.

As previously mentioned, the system implements a distributed architecture specially designed for integrating heterogeneous WSNs. The next section describes the main characteristics of the architecture.

3.1. SYLPH; A Distributed SOA-Based Architecture for Integrating Heterogeneous WSNs

The described telemonitoring system makes use of SYLPH (*Service laYers over Light PHysical devices*), an experimental architecture developed by the BISITE Research Group at the University of Salamanca, Spain. This architecture integrates a SOA approach over WSNs for building systems that combine devices from different network technologies, such as ZigBee or Bluetooth. A node in a WSN of a specific technology can then be connected to a node in another WSN of a different technology. In this case, both WSNs are interconnected through a set of intermediate gateways connected simultaneously to several wireless interfaces. SYLPH allows applications to work in a distributed way and does not depend on the lower stack layers related to the WSN formation (*i.e.*, network layer) or the radio transmission (*i.e.*, data link and physical layers) amongst the nodes that form part of the network. Given that neither developers nor users have to worry about what kind of technology each node in the system uses, the experience is transparent for everybody involved. The applications can be executed over multiple wireless devices independently of their microcontroller or the programming language they use. A SOA approach was chosen because such architectures are asynchronous and non-dependent on context (*i.e.*, previous states of the system) (Cerami, 2002). Thus, devices working on them do not continuously take up processing time and are free to perform other tasks or consume less energy.

SYLPH implements an organization based on a stack of layers (Sarangapani, 2007). Each layer in one node communicates with its peer in another node through an established protocol. The SYLPH layers are added over the application layer of each WSN stack, allowing SYLPH to be reutilized over different WSN technologies (*i.e.*, standards). Figure 4 illustrates the basic communication schema between two ZigBee devices using SYLPH whereby SYLPH implements the SYLPH Message Layer (SML), the SYLPH Application Layer (SAL) and the SYLPH Services Directory Sub-layer (SSDS). The SML offers the upper layers the possibility of sending asynchronous messages between two wireless devices through the SYLPH Services Protocol (SSP). Such messages specify the origin and target nodes and the service invocation in a SYLPH Services Definition Language (SSDL) format. The SSDL describes the service itself and the parameters to be invoked. The SAL layers on two different nodes can directly communicate each other using SSDL invocations and responses which will be delivered encapsulated in SML messages through SSP. The SSDS is used by nodes for locating services on other nodes in the network. A SYLPH Directory Node (SDN) acts as directory of the services offered by other nodes. Thus, any node in the network can request a SDN for the location of a certain service by sending it a SSDL search request embedded in a SML message over SSP.

The behavior of SYLPH is essentially similar to other SOA-based approaches. However, SYLPH has several distinctive characteristics. The first step in SYLPH begins when a service registers itself on the SDN and informs the network of its location, the parameters it requires and the output values returned in the response message after its execution. To do that, SSDL is used because it has been specifically designed to work with limited computational resources nodes. SSDL is the IDL (Interface Definition Language) used by SYLPH. Unlike other IDLs such as WSDL (Web Services Definition Language) (Cerami, 2002), SSDL does not use as many intermediate separating tags and the order of its elements is fixed. Once the service has been registered in the SDN, it can be invoked by any application in the network. Both the SDN and the services can be stored in any node of the created network.

The next example shows the operation of SYLPH when registering, searching and invoking a service. A simple service called “registerServiceOnFireAlarm” is defined. This service is stored in a smoke sensor device that belongs to a WSN with SYLPH running over it. The service can be invoked by any other node in the network to register another service that will act as a *callback*. Thus, when the smoke sensor obtains a read above the specified threshold, the node where it is stored will invoke the service labeled as “callback” in the interface definition. The sequence diagram of the fire alarm using the defined “registerServiceOnFireAlarm” service is shown in Figure 5. First, node #2 registers the mentioned service on node #0 (SDN). Node #1 asks node #2 for the service location and definition. Then, node #1 invokes the service through a message to node #2. In that message, node #1 registers a service to act as *callback*, as previously defined. When the smoke sensor on node #2 detects a fire, it invokes “callback” on node #1.

As mentioned above, several heterogeneous WSNs can be interconnected using SYLPH. For this, a special node called SYLPH Gateway is used, which is connected to WSNs through different network interfaces. Thus, it can forward messages amongst the different networks to which it belongs. From the SAL layer’s point of view, there is no difference between invoking a service stored in a node in the same WSN and invoking another one stored in a remote node in a different network. Figure 6 shows a ZigBee and a Bluetooth network working together using SYLPH. In this example, if a ZigBee node invokes a service in a Bluetooth node, the ZigBee node will look for the service in the SDN belonging to the ZigBee network. In fact, the entry stored in the services table of the SDN points to the SSP address of the SYLPH Gateway. When the ZigBee node invokes the service in the Bluetooth node, the SYLPH Gateway forwards the call message to the Bluetooth node through its Bluetooth hardware interface.

3.2. Experiments and Results

Two experiments were realized to evaluate the overall performance of a telemonitoring system prototype. The system’s functionalities were compared with a previous system in a healthcare institution in Salamanca (Spain). The name of this institution is omitted in this paper due to confidentiality. The previous system consisted of a VoIP (Voice over IP) infrastructure connected between the remote center and the patients’ homes. Patients were 20 elderly people with a relative risk of having a fall or home accident due to their limited mobility capabilities. With this system, each patient carried a bracelet with an alarm button that could be pressed to initiate a VoIP conversation between the home and the remote center. The panic button transmitted the alarm via Bluetooth to a USB dongle connected to a mini barebone (*i.e.*, a personal computer) which forwarded the alert to the center through the Internet. This system was substituted by the telemonitoring system prototype described in this paper. With the new system each patient carried the three biomedical sensors previously described (id and fall detector, ECG and breath monitors). The patients selected had similar home characteristics (*i.e.*, 5 rooms, including bathroom and kitchen). In each home, 5 smoke sensors, 5 light sensors, 5 light dimmers and 1 fire alarm were installed. Both systems were subjected to observation during a period of four weeks in order to gather information and make comparisons.

The data tracked were relative to the alerts registered by the system from the patients' homes. These alerts could come not only from the alarm button but also from any of the other sensors that constituted the new telemonitoring system. As a result, more risks sources, including the fall detector, the fire alarm or the heart pulse, were taken into account in the new system data. The precise measured variables were: average response time to incidents (the time spent from the risk situation is detected by the sensors, even the panic button, to the moment the help is sent to the patient's home, including the time spent to guess what kind of help the patient needs); average assisted incidents per day; average number of false positives per day; and the time employed by the medical staff to attend to an alert (the time spent from the help is sent to the moment the risk situation has been solved, carrying the patient to a medical center if necessary).

Table 1 illustrates how the new telemonitoring system reduced the average response time to incidents. However, it was unable to reduce the false positives, increasing them instead, because the number of sensors is greater than in the former system and, consequently, the number of alarm sources. These results demonstrate that the prototype still needs more development in this aspect. It is important to mention that the new system does not reduce the time employed by the medical staff to attend to an alert, but does allow patients to be attended earlier. Moreover, the new system allowed caregivers to detect some situations that the older system could not have. For instance, one diabetic patient tracked with the new system fainted due to a hypoglycemia situation, and was unable to press her alert button. However, the new system detected the risk with the fall detector, prompting caregivers to assist her at home, since they could not contact her through VoIP. Furthermore, the SYLPH architecture allowed the new system to merge biomedical and automation sensors from different radio technologies and at a low deployment cost.

In addition, several experiments were carried out to evaluate the performance of SYLPH, mainly to test how it handled the network formation and the services registration, as well as the services searches, invocations and responses in homogeneous and heterogeneous SYLPH networks. To make it possible, it was developed an application for monitoring all the traffic (*i.e.*, service invocations, responses, registrations or searches) in the SYLPH network.

The first experiment consisted of trying to form a ZigBee WSN using SYLPH. The network was made up of 30 ZigBee nodes using the same microcontroller and transceiver as in the telemonitoring system, two of them acting as SDNs. Each node was instructed to try to register one service on each SDN after joining the network. This experiment was run 50 times in order to measure the success ratio of the network formation and the services registration. The second experiment consisted of a dual SYLPH network made up of one 15-node ZigBee network and another 15-node Bluetooth network, both of them interconnected through a SYLPH Gateway, in this case a computer. The 15-node Bluetooth network was, in fact, a scatternet formed by two piconets. Each of these two piconets had a master node and seven slave nodes, having a common slave node forming part of both piconets simultaneously. All Bluetooth nodes had BlueCore4-Ext chips as in the telemonitoring system. There were also two SDNs in this experiment, one in each WSN (*i.e.*, a SDN in the ZigBee network and another one in the Bluetooth network). In the first experiment, the success ratio of network formation reached 97.2% while the success ratio for registration of services was 96.2%. In the second experiment, the success ratios were 84.1% and 97.4% respectively. These results demonstrate that the inclusion of the SYLPH Gateway makes the formation of the whole SYLPH network (a difference of 13.1%) much harder. However, once the network is successfully formed, there is a small difference of 0.8% in the service registration mechanism.

Two additional experiments were done using the SYLPH networks from the two previous experiments. These experiments were run 50 times to calculate average measurements of the performance of services searches, invocations and responses in SYLPH networks. Once each network was completely formed and all the services were correctly registered, each node in the network was instructed to search all the registered services in the SDNs and then invoke each one of them once. Three factors were measured: the SDN query success ratio (*i.e.*, the number of times the SDN answers correctly to the service searches from the nodes with respect to the total number of service searches done), the service invocation success ratio and the service response success ratio. In the ZigBee network, the SDN query success ratio was 98.3%, the service invocation success ratio was 99.1% and the service response success was 99.6%. In the hybrid SYLPH network the results were 94.9%, 96.6% and 98.1%, respectively. These results and the obtained in the previous experiment are showed in Figure 7. It is possible to observe how the introduction of the SYLPH Gateway slightly affects the performance of the services searches, invocations and responses.

4. CONCLUSIONS AND FUTURE WORK

The system presented in this paper allows wireless devices from different technologies to work together in a distributed way in smart environments. Because such devices do not require large memory chips or fast microprocessors to exploit their functionalities, it is possible to create a more flexible system and reduce the implementation costs in terms of development and infrastructure support compared to other analyzed telemonitoring approaches (Jurik and Weaver, 2008) (Varshney, 2008). The distributed approach of this system makes it possible to add new components in execution time. In this respect, this model goes a step further in designing dynamic systems in wireless communications scenarios (*e.g.*, E-healthcare). In addition, the system includes features that make it easy an adaptation amongst heterogeneous networks and technologies through SYLPH.

Future work includes the addition of new automation and biomedical sensors to the system to obtain additional context information. The suggestions and the necessities of patients and caregivers have been taken into account. Plans are being made to include new automation sensors to measure ambient humidity and gas detectors in order to improve patient comfort and avoid accidents. Regarding biomedical sensors, we are expecting to add electro-dermal sensors to track the cognitive activity in patients with certain brain pathologies. Other planned biomedical sensors include peripheral body temperature to detect fevers, and surface Electromyography (sEMG) sensors to monitor muscle activity. Thus, both the comfort of home automation and the vital signs gathered from patients will increase.

In addition, some improvements are under development to enhance the overall system operation. An indoor Real-Time Location System is intended to be implemented both in patient homes and medical centers. Patients will continue to carry the ZigBee wristbands as identification tags, and more ZigBee presence detectors will be present both in center and homes. Thus, if a patient suffers an accident at home, the system will warn caregivers about what room the patient is in, and activate a corresponding webcam. At the medical center, the system will keep track of the location of each patient, alerting the medical personnel if anyone leaves the center or accesses to a restricted area.

Future work on SYLPH includes an improved SYLPH Gateways performance and support for other WSN technologies as Wi-Fi. These changes will facilitate the interconnection of more WSNs technologies and in a more efficient way. To reduce design and implementation times, it is in progress the development of a tool for generating code skeletons from the human-readable SSDL language, so that the building and delivering of SSDL frames will be coded directly from the services definitions.

Nevertheless, the main efforts on improving SYLPH are aimed at increasing the service registration, SDN query, service invocation and service response success ratios to nearly achieve the 100%. This is very important for the use of SYLPH in healthcare applications as such applications work with critical data and the actions performed on them can have serious consequences.

Acknowledgements

This work has been supported by the Spanish Ministry of Science and Technology project TIN2006-14630-C03-03.

REFERENCES

Ahmed, A., Ali, J., Raza, A., and Abbas, G., 2006, Wired vs Wireless Deployment Support for Wireless Sensor Networks, Proceedings of TENCON 2006, 2006 IEEE Region 10 Conference, Hong Kong, 1-3.

Andreasson, J., Ekstrom, M., Fard, A., Castano, J., and Johnson, T., 2002, Remote System for Patient Monitoring using Bluetooth™, Proceedings of 1st IEEE International Conference on Sensors (Sensors 2002), Orlando, FL, USA, 1, 304-307.

Ardissono, L., Petrone, G., and Segnan, M., 2004, A Conversational Approach to the Interaction with Web Services, Computational Intelligence, 20(4), 693-709.

Bai, J., Zhang, Y., Cui, Z., and Zhang, J., 2000, *Home Telemonitoring Framework based on Integrated Functional Modules,* Proceedings of 22nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Chicago, IL, USA, 1, 778-781.

Baronti, P., Pillai, P., Chook, V.W.C., Chessa, S., Gotta, A., and Hu, Y.F., 2007, *Wireless Sensor Networks: A Survey on the State of the Art and the 802.15.4 and ZigBee Standards,* Computer Communications, 30(7), 1655-1695.

Camarinha-Matos, L.M., and Afsarmanesh, H., 2007, *A Comprehensive Modeling Framework for Collaborative Networked Organizations,* Journal of Intelligent Manufacturing, 18(5), 529-542.

Cerami, E., 2002, *Web Services Essentials: Distributed Applications with XML-RPC, SOAP, UDDI & WSDL (1st ed.),* O'Reilly Media, Inc.

Chen Z., 2007, *A Customizable QoS Strategy for Convergent Heterogeneous Wireless Communications,* IEEE Wireless Communications, 14(2), 20-27.

Correia, L.H.A., Macedo, D.F., Santos, A.L.D., Loureiro, A.A.F., and Nogueira, J.M.S., 2007, *Transmission Power Control Techniques for Wireless Sensor Networks,* Computer Networks, 51(17), 4765-4779.

Costa, C.A.D., Yamin, A.C., and Geyer, C.F.R., 2008, *Toward a General Software Infrastructure for Ubiquitous Computing,* IEEE Pervasive Computing, 7(1), 64-73.

Cote, G., Lec, R., and Pishko, M., 2003, *Emerging Biomedical Sensing Technologies and their Applications,* IEEE Sensors Journal, 3(3), 251-266.

Erickson, P., Wilson, R., and Shannon, I., 2000, *Years of healthy life,* Healthy People 2000 Statistical Notes / National Center for Health Statistics, 7, 1-9.

Fazel-Rezai, R., Pauls, M., and Slawinski, D., 2007, *A Low-Cost Biomedical Signal Transceiver based on a Bluetooth Wireless System,* Proceedings of 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Lyon, France, 5711-5714.

Freitas, E.P.D., Wehrmeister, M.A., Pereira, C.E., and Larsson, T., 2008, *Reflective Middleware for Heterogeneous Sensor Networks,* Proceedings of 7th workshop on Reflective and adaptive middleware, Leuven, Belgium, 49-50.

Gonçalves, B., Filho, J.G.P., Andreão, R.V., and Guizzardi, G., 2008, *ECG Data Provisioning for Telehomecare Monitoring,* Proceedings of the 2008 ACM symposium on Applied computing, Fortaleza, Ceara, Brazil, 1374-1379.

Huang, Y., and Pang, A., 2007, *A Comprehensive Study of Low-Power Operation in IEEE 802.15.4.,* Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems, Chania, Crete Island, Greece, 405-408.

Ilyas, M., and Dorf, R.C. (Eds.), 2003, *The Handbook of Ad Hoc Wireless Networks*. CRC Press, Inc.

Jurik, A.D., and Weaver, A.C., 2008, *Remote Medical Monitoring,* Computer, 41(4), 96-99.

Lei, S., Xu, H., Xiaoling, W., Lin, Z., Cho, J., and Lee, S., 2006, *VIP Bridge: Integrating Several Sensor Networks into One Virtual Sensor Network,* Proceedings of International Conference on Internet Surveillance and Protection (ICISP'06), 2-2.

Lymberis, A., 2005, *Progress in R&D on Wearable and Implantable Biomedical Sensors for Better Healthcare and Medicine,* Proceedings of 2005 3rd IEEE/EMBS Special Topic Conference on Microtechnology in Medicine and Biology, 296-298.

Marin-Perianu, M., Meratnia, N., Havinga, P., de Souza, L., Muller, J., Spiess, P., Haller, S., Riedel, T., Decker, C., and Stromberg, G., 2007, *Decentralized Enterprise Systems: a Multiplatform Wireless Sensor Network Approach,* IEEE Wireless Communications, 14(6), 57-66.

Meshkova, E., Riihijärvi, J., Oldewurtel, F., Jardak, C., and Mähönen, P., 2008, *Service-Oriented Design Methodology for Wireless Sensor Networks: A View through Case Studies,* Proceedings of the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008), Taichung, Taiwan, 146-153.

Narayanaswami, C., and Raghunath, M.T., 2002, *Designing a New Form Factor for Wearable Computing,* IEEE Pervasive Computing, 1(4), 42-48.

n-Core, 2010, *n-Core: A Faster and Easier Way to Create Wireless Sensor Networks*, Retrieved October 24, 2010, from http://www.n-core.info

Prinsloo, J.M., Schulz, C.L., Kourie, D.G., Theunissen, W.H.M., Strauss, T., Heever, R.V.D., and Grobbelaar, S., 2006, *A Service Oriented Architecture for Wireless Sensor and Actor Network Applications,* Proceedings of the 2006 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT research in Developing Countries, Somerset West, South Africa, 145-154.

Rigole, P., Holvoet, T., and Berbers, Y., 2002, *Using Jini to Integrate Home Automation in a Distributed Software-System,* Distributed Communities on the Web, Lecture Notes in Computer Science, 2468, 185-232, Springer Berlin / Heidelberg.

Rogers, A., Corkill, D. D., and Jennings, N. R., 2009, *Agent Technologies for Sensor Networks,* IEEE Intelligent Systems, 24(2), 13-17.

Sarangapani, J., 2007, *Wireless Ad hoc and Sensor Networks: Protocols, Performance, and Control (1st ed.).,* CRC Press.

Satyanarayanan, M., 2002, *Pervasive Computing: Vision and Challenges,* IEEE Personal Communications, 8(4), 10-17.

Simon, D., and Cifuentes, C., 2005, *The Squawk Virtual Machine: Java™ on the Bare Metal,* In Companion to the 20th annual ACM SIGPLAN Conference on Object-oriented programming, Systems, Languages, and Applications, San Diego, CA, USA, 150-151.

Singh, C.K., Kumar, A., and Ameer, P.M., 2008, *Performance Evaluation of an IEEE 802.15.4 Sensor Network with a Star Topology,* Wireless Networks, 14(4), 543-568.

Song, E.Y., and Lee, K.B., 2008, *STWS: A Unified Web Service for IEEE 1451 Smart Transducers,* IEEE Transactions on Instrumentation and Measurement, 57(8), 1749-1756.

Souto, E., Guimarães, G., Vasconcelos, G., Vieira, M., Rosa, N., Ferraz, C., and Kelner, J., 2005, *Mires: a Publish/Subscribe Middleware for Sensor Networks,* Personal Ubiquitous Computing., 10(1), 37-44.

Varshney, U., 2008, *Improving Wireless Health Monitoring Using Incentive-Based Router Cooperation,* Computer, 41(5), 56-62.

Voos, H., 2006, *Agent-Based Distributed Resource Allocation in Technical Dynamic Systems,* Proceedings of IEEE Workshop on Distributed Intelligent Systems: Collective Intelligence and Its Applications, Los Alamitos, CA, USA, 157-162.

Weiser, M., 1999, *The Computer for the 21st century,* SIGMOBILE Mobile Computer and Communications Review, 3(3), 3-11.

Yick, J., Mukherjee, B., and Ghosal, D., 2008, *Wireless Sensor Network Survey,* Computer Networks, 52(12), 2292-2330.

World Health Organization, 2007, *Global Age-Friendly Cities: A Guide (illustrated edition.),* World Health Organization.

Table 1. Comparison between both telemonitoring systems

Factor	New telemonitoring system	Previous telemonitoring system
Average response time to incidents (minutes)	10	14
Average assisted incidents per day	5.7	3.1
Average number of false positives per day	3.3	1.6
Time employed by the medical staff to attend to an alert (minutes)	75	75

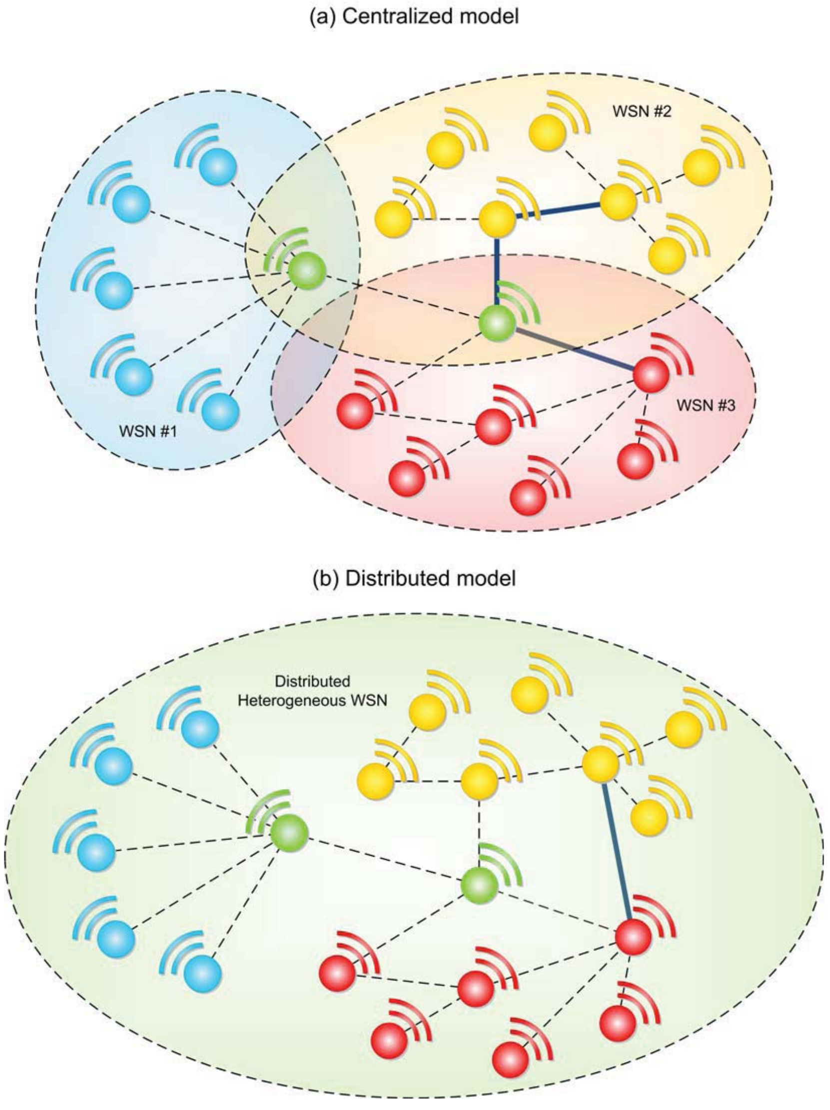

Fig. 1. A centralized versus a distributed approach for integrating heterogeneous WSNs.

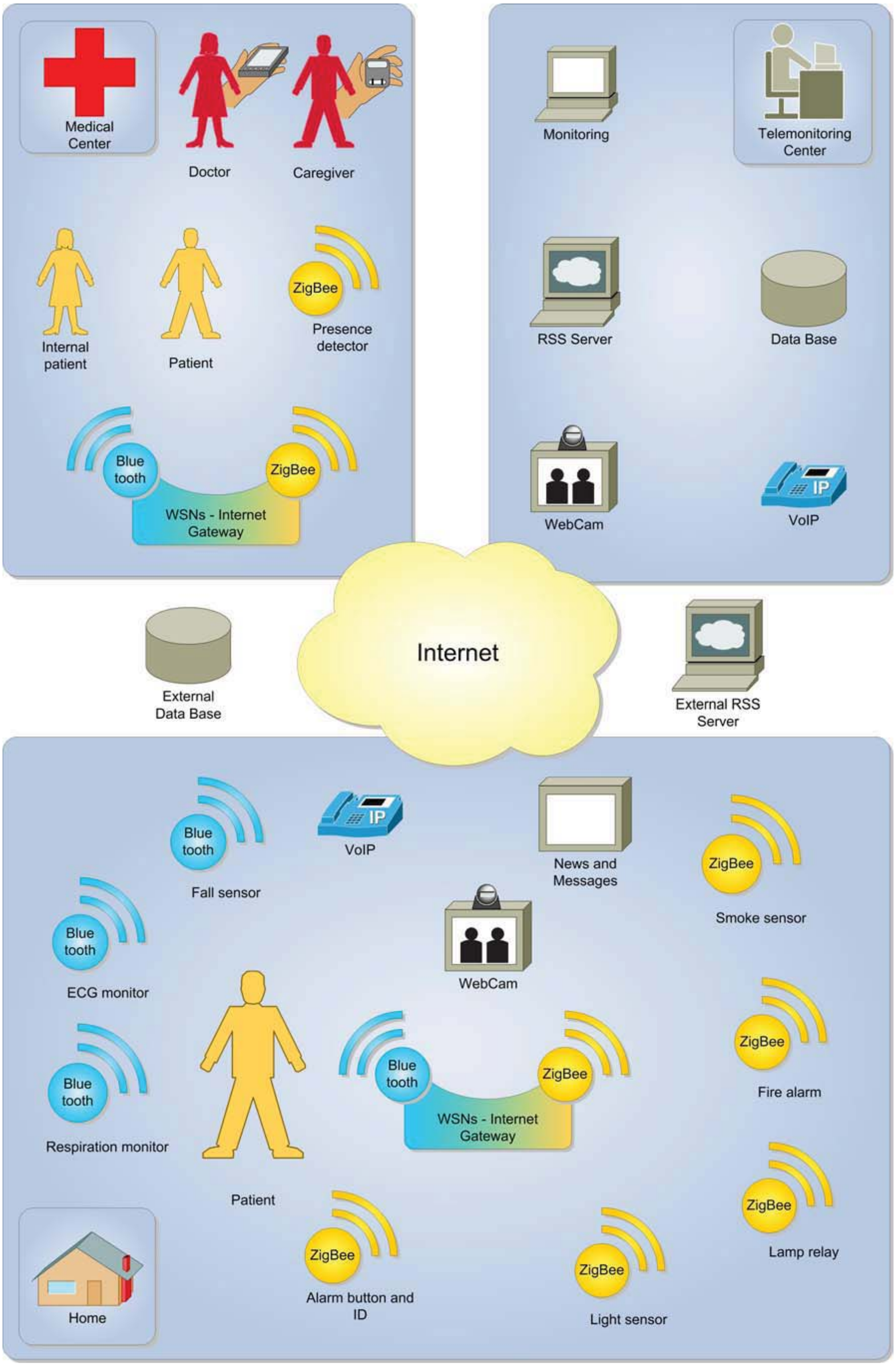

Fig. 2. Schema of the telemonitoring system.

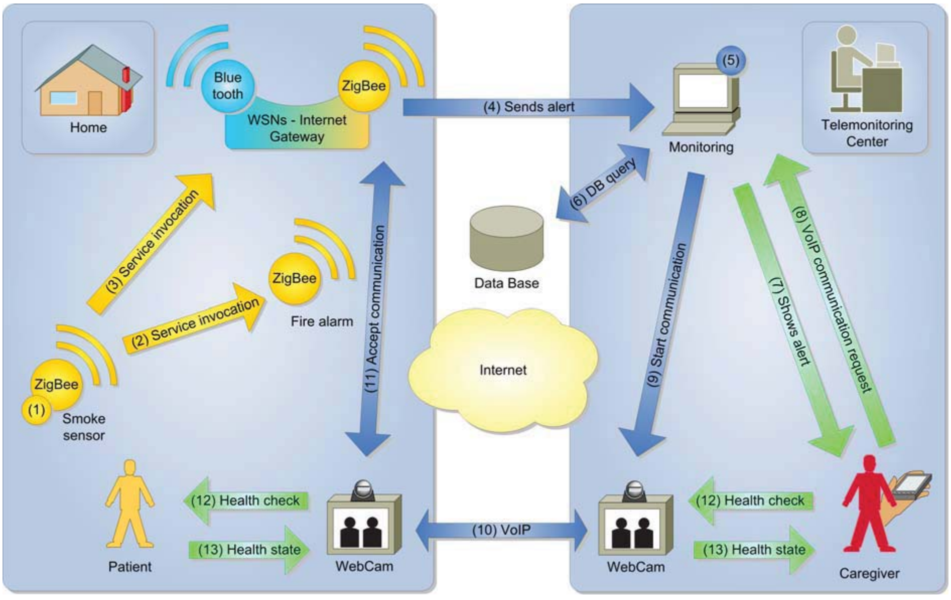

Fig. 3. Example of the system operation.

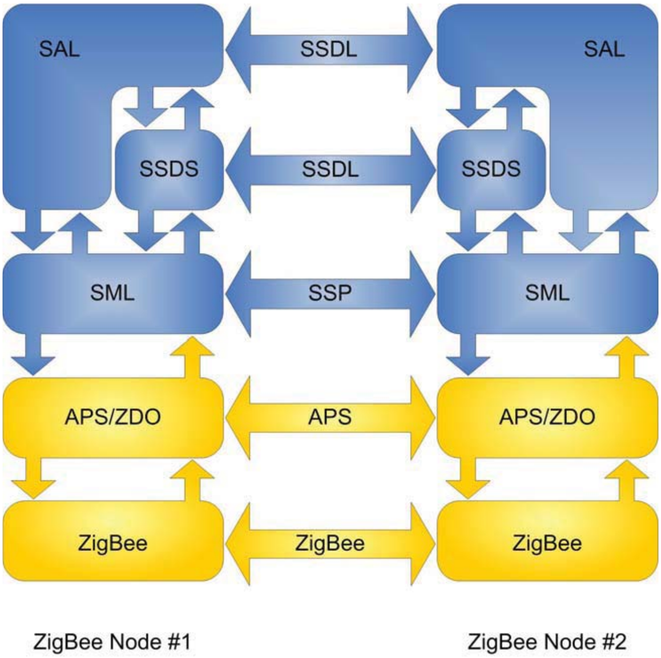

Fig. 4. Communication between two ZigBee devices using SYLPH.

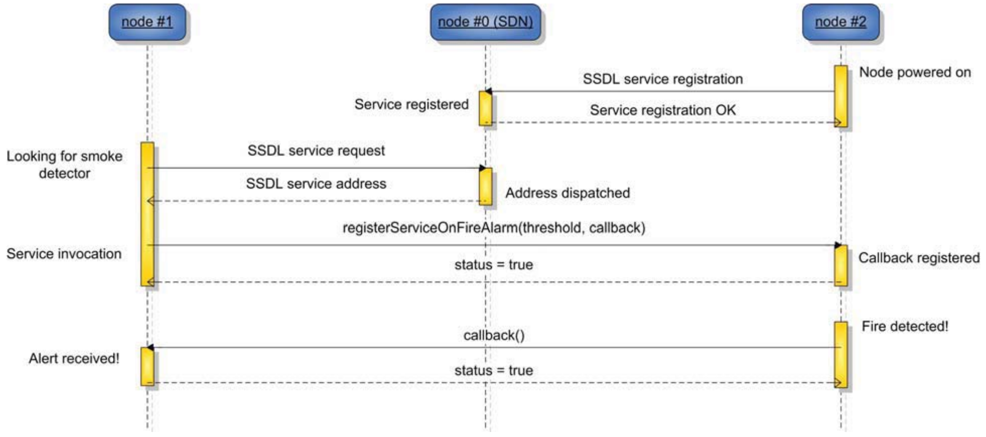

Fig. 5. Example of service registration, search and invocation.

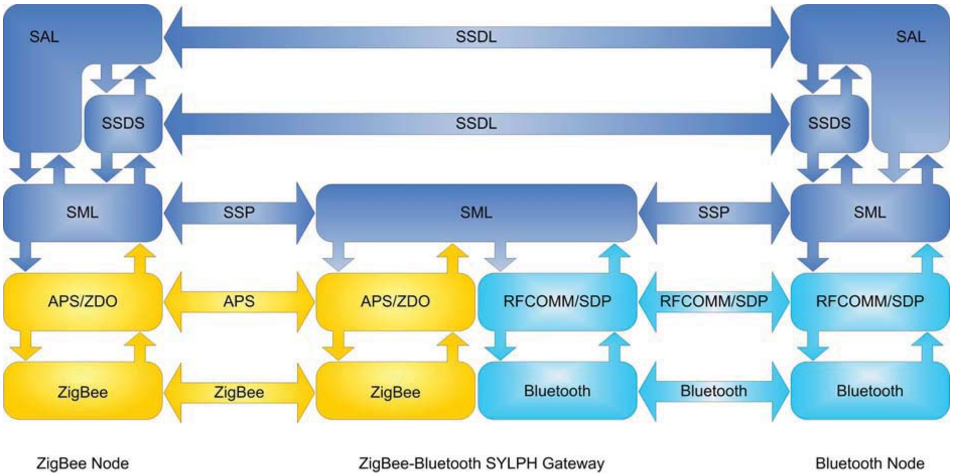

Fig. 6. SYLPH over a ZigBee and a Bluetooth network.

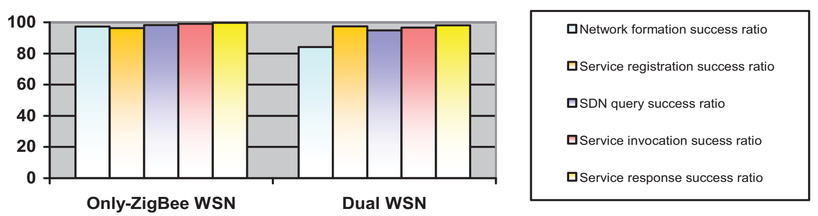

Fig. 7. Comparative of average network formation, service registration, SDN query, service invocation and service response success ratios in only-ZigBee and dual SYLPH WSNs.