EUROSENSORS 2014, the XXVIII edition of the conference series

Wireless Sensor Networking in the Internet of Things and Cloud Computing Era

A. Flammini, E. Sisinni *

Department of Information Engineering, University of Brescia, via Branze 38, Brescia (25123), Italy

Abstract

In the recent past we have observed many technological revolutions, including the transition from the analog world into its digital counterpart and from centralized wired solutions to distributed and pervasive wireless systems. In particular, the advent of low-cost and low-power transceivers, together with the development of compact-size and open standard stacks, have made possible Wireless Sensor Networks (WSNs), largely adopted for both home/office and industrial monitoring applications. The nowadays ambitious goal is to sample, collect and analyze every piece of information around us, in order to improve production efficiency and ensure optimal resource consumption. The "Internet of Things" (IoT), i.e. the capability of connecting every possible device to the World Wide Web, is the practical answer to this request. The very large amount of information that is consequently generated could be profitably handled using "cloud" services, i.e. flexible and powerful hardware/software frameworks capable to deliver computing as a service. The aim of this work is to resume pros and cons of well-accepted WSN technologies, suggesting their possible extension towards already available cloud services.

1. Introduction

In the recent past, the availability of low-cost processors/microcontrollers allowed the advent of the so called "smart sensors", i.e. a device not only capable of transducing a physical quantity of interest, but also able to perform

* Corresponding author. Tel.: +39-030-3715445; fax: +39-030-380014.
  E-mail address: emiliano.sisinni@unibs.it

some post-processing on raw data in order to extract useful information. Consequently, it was possible to overcome some intrinsic limitations of the sensing element (e.g. non linearity) and to provide the measurement readout in a digital format (e.g. improving noise immunity), ready to be used by controllers, operators and so on. The next, obvious, step was the adoption of a (digital) communication interface, thus allowing to share a single communication media by several different devices and kind of information. Measurement solutions evolved from a centralized approach, where many analog connected sensors were linked with a central acquisition and processing system, toward a distributed approach, where the network "smartness" is spread across the network as a whole. In the latter, not only measurement readouts but also ancillary data, as diagnostic, can be remotely accessed. However, despite cabling reduction due to digital transmission by means of a bus, the actual frontier is the complete removal of wires, minimizing installations costs and troubleshooting. In fact, the availability of low-cost, low-power radio interfaces allow the replacement of traditional wired devices with wireless ones, without a sensible degradation in the obtainable performance. The actual main restriction is the tradeoff between latency and lifetime, dictated by the limited amount of on-board power source (often implemented by small dimensions batteries), due to the need of a truly autonomous device.

In this paper an overview of WSNs is provided, followed by a description of cloud computing services and their possible integration with WSNs. Finally, an example developed using the "Sensibility Testbed" is shown, including scenarios where smart devices and humans are used as sensors.

2. Wireless Sensors and Wireless Sensor Networks: an overview

A wireless sensor network can be roughly defined as the ensemble of spatially distributed, autonomous sensors that cooperate to monitor physical or environmental quantities of interest (e.g. as temperature, sound, vibration, pressure, pollutants, etc…) [1]. Originally motivated by military applications, such as battlefield surveillance, WSNs are now widely diffused in many civilian application scenarios, including home and building automation, health monitoring, environment and habitat monitoring, traffic control, and many others. Even a traditionally conservative world, as the industrial automation one, has been influenced by WSNs [2]. In particular, two standard communication protocols (i.e. WirelessHART, released by the HCF consortium, and ISA100.11a, released by the ISA association) have been proposed in the last few years, purposely designed for process monitoring and control [3]. Each node in a wireless sensor network is usually equipped with a sensor (transducing the physical quantity of interest into an electric signal), a small microcontroller (providing for analog to digital conversion and computational and storage capability), a radio transceiver device (providing for wireless communications capability), and a local energy source/storage element(usually in the form of an electrochemical battery) [1]. An optional power harvester or scavenger can be also present, whose aim is to convert the energy from an external source (e.g. solar, thermal, wind, and kinetic energy; salinity gradients; …) into electrical energy flanking/recharging the traditional power storage element. A simplified block diagram is sketched in Fig.1.
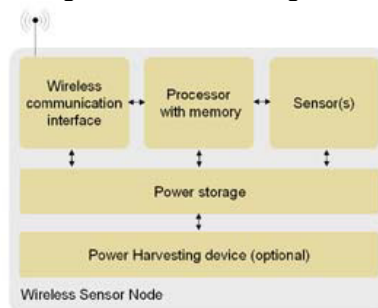

Fig.1.   Block diagram of a typical WSN node.

The development of these wireless sensor networks requires technologies from three very different research areas, i.e. technologies related to the development of the sensor, of the communication device, and of computing device

(not limited to the hardware, but also including software and algorithms). Combined and separate advancements in each of these areas have driven research in this field.

Depending on the actual implementation, the dimension of a sensor node can vary from shoebox down to a grain of dust. Similarly,the cost of a sensor device may vary from hundreds of dollars to a few pennies, mainly depending on the complexity of the embedded sensor and computational/storage requirements. Vice versa, size and cost constraints on sensor nodes dictated by the considered application, result in corresponding constraints on resources such as energy, computational power and bandwidth and storage capability [4]. In fact, if such smart sensor devices are small and inexpensive, they can be produced and deployed in large numbers, somehow "oversampling" the phenomenon of interest and improving overall performance exploiting cooperative capabilities. Formally speaking, such a large number of such wireless sensor nodes possibly interacting one with each other constitute a sensor network. Very different sensors can be adopted, such as pressure, vibration, optical, thermal, acoustic, sensors etc. capable to simultaneously monitor environmental conditions at different locations; locally extracted information can be consequently forwarder to a peculiar sink node for further processing.

In addition, smartdevice sensing capabilities are improving. For example, a smartphone includes sensors as accelerometers and GPS (Global Positioning System) and can communicate this information for further aggregation and processing using native wireless interfaces. Thanks to these devices, a human can communicate his feelings, his needs, also acting as a sensor (e.g. signaling failure in street lighting).

For sake of completeness, a summary of most important terms which are used widely in sensor network is provided in the following:

- Sensor: a transducer that converts a physical phenomenon such as heat, light, sound or motion into electrical or other signal that may be further processed by other devices.
- Sensor node: the basic unit constituting a sensor network; it embeds a processor, a memory, a wireless interface and a local autonomous power supply.
- Network Topology: a graph, where nodes are sensor nodes and edges are communication links.
- Routing: the process of forwarding data of interest along a network path from the source node to its final destination.
- Resource: this term is used to address the sensors, the communication links, the computational capabilities, the data storage and the energy amount of a node.

3. Cloud computing

Many formal definitions have been proposed in both the academia and the industry for describing the concept of "cloud computing". A well-known and widely-accepted is the one provided by the NIST (National Institute of Standards and Technology) [2], stating that "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned andreleased with minimal management effort or service provider interaction" [5]. Differently said, cloud computing is a term used to describe both a platform (including the underlying infrastructure) and a type of application.

In a cloud computing platform, instead of having local servers for collecting and managing information coming from applications, remotely located servers (implemented by means of virtual or physical machines) are dynamically provisioned and (re)configured, according to the actual needs. As an example, if we consider a wind or solar farm, the weather-related information collected by a WSN (e.g. exploiting light, wind sensors etc.), can be processed together with grid-related information (e.g. obtained from smart inverters) to improve plant efficiency and better satisfy the power demand. Cloud computing also describes those applications that can be remotely accessed through the Internet. Such cloud applications exploits large data centers and powerful servers similarly to Web applications and Web services we use every day.

3.1. Cloud computing features

In the following the most important features of cloud computing are briefly described for sake of completeness:

1. Service on demand: clients requests are satisfied automatically without the intervention of an human operator.
2. Elasticity of demand: available resources are used by the clients according to their own needs for a flexible period of time (i.e. there is not a formal agreement on such a time period).
3. Abstraction: Actual resources (hardware and/or software) are hidden to clients. Customers of the service exploits resources offered by the provider without knowing the locations from where processed data will arrive or where will be stored.
4. Service measurement: the provider exploits tools for measuring the actual usage (in terms of properly defined metrics) of offered services.
5. Resource pooling: Available services, constituting a pool of services, are assigned dynamically according to clients' requests.
6. Network access: The client application can run over various platforms by means of a (possibly ciphered) Internet access exploiting devices as mobile phones, tablets, laptops and so on.

3.2. Cloud computing services

According to its implementation, the cloud can provide different services levels hierarchically organized according to the following nomenclature (see Fig.2):

- IaaS (Infrastructure as a Service): This model provides basic storage and computing capabilities as standardized services over the network. Consequently the user (on the client side) does not need to buy its own hardware (e.g. servers, storage systems, networking devices, etc...) The user would typically execute its own applications exploiting the workload offered by the infrastructure. As an example, consider services offered by Amazon EC2.
- PaaS (Platform as a Service): This model provides application software and/or development environment as a service; in addition, other higher level software applications can be executed exploiting the same service. Consequently, the user (on the client side) has the freedom to create his own applications, that are executed by the infrastructure of the provider.As an example, consider the Google's App Engine or Windows Azure.
- SaaS (Software as a Service): This model provides services to clients according to their requests. A single instance of the service is executed on the cloud and can be used by multiple end users. There is no need for investment on the client side for hardware or software licenses. As an example, consider Google Apps ir Microsoft Office 365as a typical SaaS provider.

Fig.2. Different organization of cloud services: Iaas, Paas and SaaS

3.3. Cloud Computing Models

According to the way in which the cloud infrastructure is operated, different cloud computing models can be defined. Some well accepted and widely adopted definitions are:

- Private Cloud: In this case, the cloud infrastructure is completely managed by an organization. The goal for an organization in setting up a private cloud is to maximize the efficiency in the use of resources available in house. Advantages offered are in terms of increased security and lowered cost in transferring data.
- Public Cloud: a public cloud is one based on the standard cloud computing model, in which a service provider makes resources (applications, storage,…), available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model. The main benefits of using a public cloud service are the lower cost in setting up the system because hardware, application and bandwidth costs are handled/managed by the provider; the improved scalability and the improved efficiency, since you pay only for what you actually use.
- Hybrid Cloud: A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organization. All cloud computing services should offer certain efficiencies to differing degrees but public cloud services are likely to be more cost efficient and scalable than private clouds.
- Community Cloud: a community cloud is a multi-tenant infrastructure that is shared among several organizations from a specific group with common computing issues. The organizing principle for the community cloud will be different, but the members of the community generally share similar security, privacy, performance and compliance requirements.

4. WSNs and cloud computing

Once highlighted features and advantages of both WSNs and cloud computing, it is quite evident that these two paradigms can be mixed together to allow for easily sharing and analyzing real-time sensor data on-the-fly [6]. In addition, this mixture also allows for providing sensor data or sensor event as a service over the Internet, so that sensor data can be easily analyzed not only locally, but also from everywhere around the world. For these reasons, the terms "Sensing as a Service" and "Sensor Event as a Service" have been coined. The former describes the process of making the sensor data available to the clients across the cloud infrastructure; the latter, conversely, is related to events of interests provided by the cloud infrastructure.

Merging of these two technologies can be useful exploited for a largenumber of different applications, including:

- Transport Monitoring, e.g. for handling of systems for traffic control, automatic recognition of plates, toll-way management, emergency vehicle notification, dynamic traffic light management etc [7]. Sensors data collected by the cloud platform would allow to build a global traffic snapshot dynamically updated by user themselves. These data can be used in a large number of applications, as vehicle classification, collision avoidance systems, automatic toll gates and so on.
- Military Use; wireless sensor networks were originally designed for military applications (e.g. the smart dust concept) [8]. Private Cloud computing, as previously described, can be an answer to top level security requirements of these applications, requirements that cannot be easily provided using normal Internet connectivity [9].
- Weather Forecasting; data collected by environmental sensors represent an example of the so called "big data" issue, that cannot be easily maintained using the traditional database approaches [10], but could be profitably solved by low-cost large computational power of the cloud..
- Health Care; sensor networks are nowadays widely adopted in health care applications, not only limited to in hospital scenarios. In particular, there is an increasing interest in developing personal and portable devices for people's health continuous monitoring and consequently life quality improvement. For example, athletes can take advantage of such systems to get real-time warnings for a safe and more effective training; vital parameters of dismissed patients can be constantly and remotely monitored; and, more in general, all people can receive personalized advices to maintain a healthy lifestyle.

In particular, in the following section an application authors are developing on this subject is briefly resumed.

5. An example of cloud sensing for lifestyle monitoring

As stated in the previous section, health care is the application scenario authors consider for profitably applying cloud computing. Individual bio-signals continuous monitoring is a reality thanks to the increasing availability of non-invasive, low-cost wearable sensors [11]. However, the consequent collection of a very large amount of data from different and distributed sources needs a proper structure to manage the storing and analysis, suggesting the adoption of the cloud computing paradigm. Wearable sensors are usually organized into simple wireless networks due to cost limitations, thus cannot be directly connected to the Internet and for this reason gateways are needed. The massive introduction of smartphones in everyday life, flanked by the many native communication options (e.g. Bluetooth, Wifi, NFC…) suggests the utilization of this kind of devices to implement gateways toward the Internet in an easy way. In addition, what authors also proposed is to adopt smart devices also for acquiring different bio-data from a great amount of people exploiting already embedded sensors, and relying on the inherent distributed architectures for subsequent data processing. In this way, a wide range of statistical analysis can be easily conducted on a great amount of data from a large and heterogeneous population.

In particular, this section evaluates the use of the Sensibility Testbed framework, based on the Seattle project, to develop a cloud-based system for analyzing information acquired by smartphones' and tablets' accelerometers and GPS devices, obtaining useful data for studying the population lifestyle [12],[13],[14].

5.1. The Seattle project and the Sensibility Testbed

According to its developers, the "Seattle is a platform for networking and distributed systems research, offering a large deployment of computers spread across the world, whose resources can be used exploiting the Seattle Clearinghouse website". The Seattle framework has been recently made compatible with mobile devices, including Android, iOS, and other mobile operating systems. The Sensibility Testbed has been defined a post-desktop version of the Seattle cloud computing platform, thanks to the capability of nowadays available smartdevices it can do the same computation as regular PC-based application, and with embedded sensing capabilities. The system thus moves from the concept of cloud computing to the cloud sensing paradigm.

The Sensibility Testbed follows the Seattle Project approach, including three different stages in project handling, each one corresponding to a peculiar "player". The first player, called the Planner, customizes the execution environment, setting up the installer and allocating the available resources. Then the second one runs the installer on the target device we want to share resources, as set out by the planner; for this reason the corresponding player is called the Donor. At last, the Researcher exploits the resources exposed by the Planner on the Donor' systems for running experiments. In Fig.3 the Seattle system is shown.
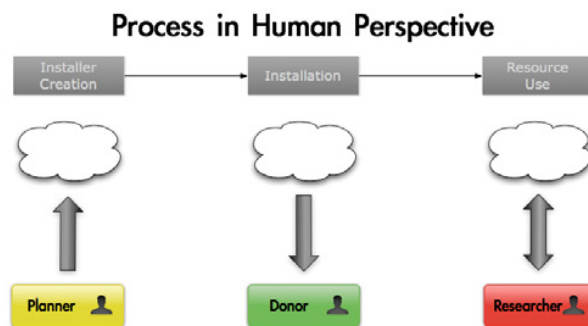

Fig.3.   The Seattle architecture (https://seattle.poly.edu/wiki/UnderstandingSeattle/SeattleComponents)

The aim of the Sensibility Testbed is to provide a unified programmable interface to sensors embedded in the smartdevices, so that the Researcher can easily and uniformly access the sensors on the device through the client side software. Currently, implemented sensor modules and the available contextual information are classified into three categories: device specific (i.e. parameters as the battery power level, the CPU and memory utilization),

location related (i.e. parameters as the geographical position, the altitude, and the speed if available), and network related (mobile network type and operator, neighborhood WiFi access points and Bluetooth devices in the nearby). All these information are natively provided by most of commercially available smartphones and tablets.

A scheme of the proposed architecture is shown in Fig.4; users' smartphone (resembling data sources) makes data accessible through the cloud, represented by the Seattle Clearinghouse server; a "Researcher terminal", e.g. owned by a doctor, can access the cloud in order to retrieve patient data of interest and execute further data processing. The logged data can be acquired through the cloud using the "sensibility testbed" software running on the Researcher terminal. In addition, the user's smartdevice also has the capability to communicate data directly to this "Researcher terminal", implementing server functionalities directly on the smartphone (if a public IP is available). However, a preliminary connection with the Seattle Clearinghouse server is still needed to affiliate the smartdevice to a "test group", constituted by all the monitored smartdevices. Furthermore, the "Sensibility testbed" also allows a Python software to be developed and downloaded/executed into the user smartphone. All these operations are implemented by means of an XML-RPC library added to the Android platform.
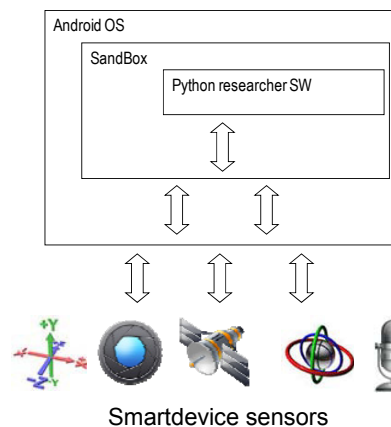

Fig.4.   The proposed.cloud-based architecture

Fig.5.   The sensibility testbed implemented in an Android smartdevice

The logging application on the smartdevice accesses the smartphone sensors through a SandBox, thus limiting potential damages by faulty software, as shown in Fig.5. The flexibility of the proposed system consists in the possibility of changing the sensor to be acquired by simply and remotely loading new software into the user smartphone. In particular, the potentialities of the Sensibility Testbed can be exploited to collect a large amount of data related the movements of the subjects under test and to realize various statistical analysis on the population physical activity. Many works available in literature propose algorithms to classify the user movements from the accelerometer data [15]; moreover, the use of GPS can help to better determine the type of activity the subject under test is performing, such as indoor or outdoor actions, walking or cycling and so on.

Some preliminary experiments with the proposed solution have been already carried out. One of the smartphones of the "test group" has been solidly fastened to a PC-controlled shaker, using a setup similar to the one described in [16]. The acquisition of the accelerometer data has been sent to the remote user terminal through the cloud-based system; results of two different basic (static) tests on the "Researcher terminal" are shown in Fig.6 and Fig.7. The simple experiment confirm that it is possible to remotely gather a (great) amount of sensor data, e.g. coming from embedded accelerometers, and to have data available in the cloud. It is worth noting that this is obtained without having any knowledge about the device, except its address within the "test group". The system is capable to collect about two samples per second; unfortunately, the jitter is relevant (on the order of ten milliseconds), but a timestamp is also automatically provided, so that readouts can be correctly ordered and further processing is still possible.
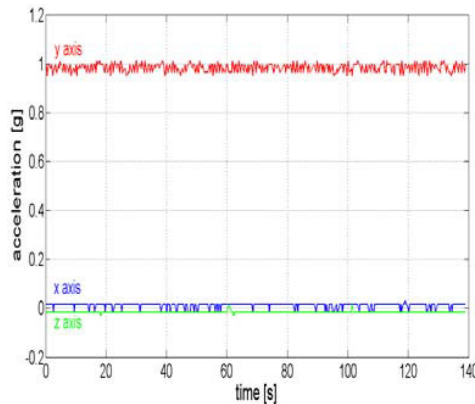
Fig.6.   In this experiment, the smartphone is arranged with vertical y axis parallel to the main axis and horizontal x and z axes are perpendicular to the main axis.
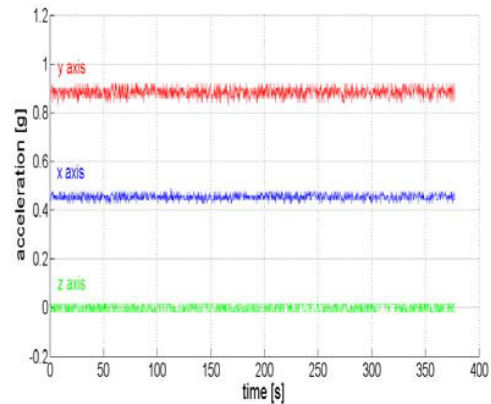
Fig.7.   In this experiment, the smartphone has a 30° offset between the y axis and the main axis; a 60° offset between the x axis and the main axis; the z axis is perpendicular to the main axis.

6. Conclusions

The IoT, i.e. the capability to interconnect every possible device, opens new scenarios in WSNs. Cloud computing services and the availability of powerful and inexpensive smartdevices allow to optimize information management, sharing measurement results and improving quality of services.

References

[1]   I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, August, 102-114(2002).
[2]   P. Ferrari, A. Flammini, D. Marioli, E. Sisinni, A. Taroni, "Wired and wireless sensor networks for industrial applications", Microelectronics Journal, September, 2009, Vol. 40, N. 9, pp. 1322-1336.
[3]   P. Ferrari, A. Flammini, M. Rizzi, E. Sisinni, "Improving simulation of wireless networked control systems based on WirelessHART", Computer Standards & Interfaces, November, 2013, Vol. 35, N. 6, pp. 605-615.
[4]   R. Kay; F. Mattern, "The Design Space of Wireless Sensor Networks", IEEE Wireless communications, 11 (6), Pp.: 54–61.
[5]   P. Mell, T. Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-145. Available on-line at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[6]   Sanjit Kumar Dash, Subasish Mohapatra, Prasant Kumar Pattnaik, "A survey on Application of Wireless sensor network using Cloud Computing", IJCSET, Vol. 1,Issue 4, Pp.50-55,December 2010.
[7]   P. Jaworski, T. Edwards, J. Moore, K. Burnham, "Cloud computing concept for Intelligent Transportation Systems", 2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC), pp.391,936, 5-7 Oct. 2011.
[8]   M. P. Durisic, Z. Tafa, G. Dimic, V. Milutinovic, "A survey of military applications of wireless sensor networks," 2012 Mediterranean Conference on Embedded Computing (MECO), pp.196,199, 19-21 June 2012.
[9]   J.M. Reddy, J.M. Monika, "Integrate Military with Distributed Cloud Computing and Secure Virtualization,", High Performance Computing, Networking, Storage and Analysis (SCC), pp. 1200-1206, 10-16 Nov. 2012.
[10]   D.K. Krishnappa, D. Irwin, E. Lyons, M. Zink, "CloudCast: Cloud computing for short-term mobile weather forecasts", 2012 IEEE 31st International Performance Computing and Communications Conference (IPCCC), pp.61-70, 1-3 Dec. 2012
[11]   A. Depari, A. Flammini, E. Sisinni, A. Vezzoli, "A Wearable Smartphone-Based System for Electrocardiogram Acquisition", 2014 IEEE International Symposium on Medical Measurements and Applications Proceedings, Lisbon, Portugal, June 11-12, 2014, pp.54-59.
[12]   "The Seattle platform"; available online: https://seattle.poly.edu/wiki
[13]   "The Sensibility Testbed", available online: http://seattlesensor.wordpress.com/
[14]   J. Cappos, Lai Wang, R. Weiss, Yi Yang, YanyanZhuang, "BlurSense: Dynamic fine-grained access control for smartphone privacy,"Sensors Applications Symposium (SAS), 2014 IEEE, pp.329,332, 18-20 Feb. 2014
[15]   S. Kaghyan, H. Sarukhanyan, "Accelerometer and GPS sensor combination based system for human activity recognition", Computer Science and Information Technologies (CSIT), p. 1-9, 2013
[16]   E. Sisinni, C. M. De Dominicis, A. Depari, A. Flammini, L. Fasanotti, M. Tomasini, "Performance assessment of vibration sensing using smartdevices", 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Montevideo, Uruguay, May 12-15, 2014, pp. 1617-1622.