UNIONE EUROPEA
Fondo europeo di sviluppo regionale

PON Ricerca e Competitività 2007-2013

Ministero dell'Istruzione dell'Università e della Ricerca

Ministero dello Sviluppo Economico

investiamo nel vostro futuro

UNIVERSITA' DELLA CALABRIA

Dipartimento di Fisica

Scuola di Dottorato
"Archimede" in Scienze, Comunicazione e Tecnologie
Indirizzo
Scienze e Tecnologie dei Sistemi Complessi
CICLO
XXVIII

Smart Homes and Smart Objects: "Internet of Things" for energy-aware monitoring and controlling systems

Settore Scientifico Disciplinare ING-INF/03

Direttore: Ch.mo Prof. Pietro Pantano
Firma Pietro Pantano

Supervisore: Ch.mo Prof. Salvatore Marano
Firma

Correlatore: Ing. Floriano De Rango
Firma Floriano De Rango

Dottorando: Dott. Domenico Barletta
Firma Domenico Barletta

Acknowledgements

> *"Around here, however, we don't look backwards for very long.*
> *We keep moving forward, opening up new doors*
> *and doing new things, because we're curious. . .*
> *and curiosity keeps leading us down new paths."*
> *Walt Disney*

I would like to thank my family for always having supported, inspired and motivated me during the years.

I would like to thank the PhD School "*Archimede*" for the opportunity of being a research fellow of the University of Calabria.

I would like to thank *DIMES* (Department of Informatics, Modeling, Electronics and Systems Engineering) and the *Culture TeleLab*, especially my supervisors Prof. Salvatore Marano and Eng. Floriano De Rango for their academic encouragement.

I would like to thank the company "*Spintel Srl*" for giving shape to the results of my research.

I would like to thank all my friends and colleagues with whom I have shared these years in Cosenza.

Table of contents

Abstract in English

In recent years, the design and implementation of Home Automation Systems followed the spread of Internet of Things and its intent to make every home smart for end-users through Internet and Wireless connectivity. Ambient intelligence is an emerging discipline as well that aims to bring intelligence to environments making them sensitive to people through the use of embedded smart objects. Together, Automation Systems, Internet of Things and Ambient Intelligence make great interaction between people and the environments they live in possible. The enhancing of these interactions was one the main goals of this thesis whose intent was to improve the classic concept of Home Automation System through Internet Of Things philosophy.

The first research objective was the design and implementation of a basic Internet of Things architecture that can be used for several Home Automation and Monitoring applications such as lighting, heating, conditioning or energy management. In particular, besides controlling features, the system can optimize energy consumptions by increasing awareness of users that have full control of their house and the possibility to save money and reduce the impact of energetic consumption on the earth, matching the new "green" motto requirements. According to IoT, innovative plug-and-play and ready-to-use smart devices were designed and implemented as part of this reactive automation system that offers a user-friendly web application and allows users to control and interact with different plans of their house in order to make life more comfortable and be aware of their energy consumptions. Control and awareness were two important key points for the first stage of research activity.

The next challenge was to enhance IoT with intelligence and awareness by exploring various interactions between human beings and the environment they live in. The system was progressively enhanced evolving from a reactive system to a proactive system where the knowledge of human needs, in addition to the current environment status, constitute a new input for the system whose further objective is to find the right automations that can satisfy human needs in real-time. This advanced proactive system can sense and infer the user's and the environment's context and consequently decide autonomously how to affect the environment and actuate smart actions.

It was experienced by many researchers that, for several reasons, some users might not appreciate these kinds of proactive actuations so, another challenge was the design of a system

which is able to learn from user's context and feedbacks history and, subsequently, to adapt itself to always up-do-date users' expectations and keep the rules for triggering smart actuations constantly updated. The system was at a later time transformed into a "Inferactive" system.

Another important scope of the research was the in-depth examination of the motivations for energy-efficient communications in wireless systems by highlighting emerging trends and identifying the challenges that need to be addressed to enable novel, scalable and energy-efficient wireless communications. One of the most important issues for researchers that must be addressed in designing communication protocols for wireless networks is how to save devices' energy while meeting the needs of applications. For this reason, the architecture proposed was also enhanced at a communication level with energy-awareness in order to minimize energy consumption by communication devices, protocols, networks, end-user systems and data centers. To do this, some smart devices have been designed with multiple communication interfaces, such as RF and Wi-Fi, by using open-source technology such as Arduino. They have been analyzed under different working conditions and network topology. Communication parameters, data size and device status have been changed dynamically according to different scenarios and specific quality of service required, such as the speed of response, in order to find the best hardware and software configuration that offers the most benefits in terms of energy cost/quality ratio, lowest energy consumption and extended lifetime for battery-powered devices.

The last challenge was to improve energy consumption of battery-powered smart devices provided with Wi-Fi that is commonly considered a very energy-expensive communication interface if compared to Bluetooth or ZigBee. Research focused on social IoT solutions for Home Automation Systems where devices are socially connected to Internet and can communicate through social applications like Facebook, Twitter or Google+ with a community of users that usually interact with that device itself. A fuzzy-based solution was proposed to classify the social community interaction with the system in order to implement an adaptive energy saving mode for social Wi-Fi devices according to users' current context, behavior, habits and feedbacks.

Test and performance evaluation regarding energy consumption and efficiency in real world scenario with real hardware devices were performed to prove the efficiency of the solution in terms of electricity consumption, battery lifetime, CPU utilization and increase of comfort and satisfaction levels for community users.

The thesis is organized as follows. Chapters 1,2 and 3 contains the basics for a better understanding of the solutions proposed such as Internet of Things, Ambient Intelligence, Smart Homes and Smart Devices energy level issues. Chapter 4 describes the solution proposed, in particular, the system architecture and how the system evolved from reactive, to proactive and finally to “inferactive”. Chapter 5 examines how to deal with energy-aware communication and how Wi-Fi communication was improved in terms of energy consumption through social IoT awareness and fuzzy logic. In closing, Chapter 6 presents the test and the results achieved.

Abstract in Italiano

Negli ultimi anni, la progettazione e l'implementazione dei sistemi di automazione in ambito domestico sono stati guidati dalla diffusione di Internet delle Cose e dal suo intento di rendere ogni casa intelligente tramite l'utilizzo di Internet e della connettività wireless. L'intelligenza ambientale è una disciplina emergente che ha lo scopo di rendere gli ambienti intelligenti e reattivi alla presenza degli utenti tramite l'utilizzo di oggetti intelligenti di tipo "embedded". Sistemi di automazione, Internet delle Cose ed Intelligenza ambientale hanno reso possibile una grande ed innovativa interazione tra l'ambiente e le persone presenti al loro interno.

Uno degli obiettivi del lavoro di tesi è stato quello di studiare e migliorare l'interazione uomo-ambiente cercando di estendere il classico concetto di automazione mediante l'approccio ed il paradigma di Internet delle Cose. L'ambito di ricerca è stato pertanto quello di Internet delle Cose e dei sistemi di automazione per il controllo ed il monitoraggio energetico. Il primo obiettivo di ricerca è stato progettare ed implementare un'architettura base da poter utilizzare nel contesto delle Smart Home. Oltre alla funzionalità base di controllo di diversi impianti domestici, quali ad esempio illuminazione o condizionamento, il sistema è stato ideato per essere di grado di ottimizzare il consumo energetico degli impianti educando gli utenti al risparmio energetico ed alle politiche "green". In collaborazione con l'azienda *Spintel Srl* sono stari progettati, altresì, l'hardware ed il firmware dei diversi dispositivi Smart in grado di controllare e monitorare gli impianti secondo il paradigma di Internet delle Cose.

L'obiettivo successivo è stato quello di definire un livello di intelligenza nel sistema in grado di dedurre le esigenze degli utenti introducendo nuovi input di analisi come ad esempio il contesto utente, l'interpretazione semantica di un discorso, il grado di utilizzo del sistema e il consumo energetico attuale. La ricerca ha permesso l'evoluzione da sistema reattivo a sistema proattivo in grado di effettuare azionamenti mirati in maniera autonoma. La ricerca ha evidenziato che, per diversi motivi, alcuni azionamenti proattivi potrebbero non soddisfare le aspettative di alcuni utenti. E' stato pertanto ideato un nuovo sistema, chiamato "Inferattivo/Inferactive" in grado di apprendere nuovi azionamenti dal contesto utente e da una serie di feedback in modo che ogni singolo azionamento autonomo possa soddisfare quanto più possibile le esigenze e le aspettative degli utenti stessi, a volte mutevoli nel tempo.

Un altro obiettivo di ricerca è stato progettare ed implementare protocolli di comunicazione wireless energicamente efficienti ed in grado massimizzare il tempo di vita di dispositivi intelligenti wireless alimentati a batteria. Sono stati creati diversi scenari di test, utilizzando tecnologie open source (come ad esempio Arduino) e diverse interfacce di comunicazione wireless come ad esempio WiFi e Radio Frequenza e facendo variare in maniera dinamica alcuni parametri di comunicazione in modo da definire la configurazione ottimale che offre il miglior compromesso in termini di rapporto costo/qualità di comunicazione, il minor consumo di energia ed il più lungo tempo di vita.

Infine, la ricerca ha avuto come obiettivo quello di migliorare la comunicazione WiFi di dispositivi alimentati a batteria che è comunemente considerata essere poco efficiente in termini di consumo energetico se paragonata ad altri tipi di comunicazione wireless come ad esempio Bluetooth o ZigBee. L'attività di ricerca si è focalizzata su soluzioni che prevedono l'utilizzo di dispositivi Smart connessi tramite social networks (Facebook, Twitter o Google+) a comunità di utenti. E' stata progettata ed analizzata una soluzione che prevede l'utilizzo della logica fuzzy per classificare il grado di interazione della comunità di utenti con il dispositivo in modo da realizzare una nuova modalità di risparmio energetico per dispositivi che comunicano tramite interfaccia WiFi.

I test e la validazione dei risultati sono stati effettuati tramite dispositivi e scenari reali realizzati in collaborazione con l'azienda *Spintel Srl* al fine di valutare l'efficienza della soluzione in termini di consumo elettrico, durata della batteria, utilizzazione della CPU ed aumento del comfort per una comunità di utenti.

Il lavoro di tesi è organizzato in sei capitoli. I capitoli 1, 2 e 3 contengono i concetti teorici che stanno alla base delle soluzioni proposte come ad esempio Internet delle Cose, Intelligenza Ambientale, Smart Homes, il consumo energetico di dispositivi alimentati a batteria, ecc. Il capitolo 4 descrive la soluzione proposta, in particolare l'architettura di sistema e l'evoluzione da sistema reattivo a proattivo ed "Inferattivo". Il capitolo 5 analizza le problematiche legate alla comunicazione energicamente efficiente e come la comunicazione Wi-Fi è stata migliorata in termini di consumo energetico tramite l'utilizzo di dispositivi socialmente connessi e l'implementazione di algoritmi secondo la logica fuzzy. Infine, il capitolo 6 presenta i test ed i risultati raggiunti.

List of Figures

List of Tables

CHAPTER 1

INTERNET OF THINGS

Internet of Things (IoT) is a concept encompassing numerous objects and communication modes for the exchange of information. The term IoT describes a vision in which everything is connected to the Internet. In the future, the IoT will be essential as it creates opportunities for both new services and new innovations. All objects will be connected and will communicate with each other while operating in environments which are unprotected. Currently, the IoT requires standardisation together with clear architectures describing how to implement this technology and how IoT devices securely interact with each other. In the sense of IoT, "things,", can refer to an extensive range of devices such as heart monitoring implants, livestock biochip transponders, electric clams in coastal waters, vehicles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring or field operation devices that assist firefighters in search and rescue operations. Legal scholars suggest considering "Things" as an "*inextricable mixture of hardware, software, data and service*". These devices gather useful data with the aid of several existing technologies; they subsequently autonomously flow the data between other devices. Some current market examples include home automation (also known as smart home devices) for instance the control and automation of lighting, or heating (like smart thermostat), ventilation, air conditioning (HVAC) systems, and appliances such as washer/dryers, ovens or refrigerators/freezers that use Wi-Fi for remote monitoring. In the near future, it is feasible that the majority of people will inhabit a connected universe of smart cities, smart transportation, smart homes, and more, where not only electrical appliances are connected, but also stores and the trucks. Currently, the smart home is representative of the most tangible aspect of the IoT vision. At the cutting edge of IoT, the smart home market is a sector experiencing rapid growth. IHS Technology[1] forecasts that the smart home market will grow by 56% per year for some years. Moreover, by 2018 approximately 224 million homes will possess at least one type of installed smart home system installed according to Strategy Analytics.

1.1 Origin and diffusion

The Internet of Things (IoT) is paradoxically both a new and old term. In 1999, it was mentioned by Kevin Ashton during a presentation at Proctor & Gamble[2]. Ashton used the term to connect the concept of radio frequency identification (RFID)[3] to the then new topic of the Internet [1]. Since 1999, the use of the term IoT has flourished and major companies have forecasted an increase in IoT [2, 3, 4]. One forecast is that there will be a thirtyfold increase in the number of connected things globally between 2009 and 2020, consequently, it is estimated that by 2020 there will be approximately 26 billion things that connected to the Internet [2]. The reason that IoT has become so significant can be attributed, in part, to two things: Moore's law and Koomey's law. According to Moore's law, the number of transistors on a chip doubles approximately every two years [5] which has allowed the development of computers which are much more powerful on the same sized chip. In 1971, Intel, a well-known semiconductor chip maker, had 2300 transistors on a processor and in just over forty years this number had reached 1.4 billion transistors [6]. This is an increase of approximately 610 000 % and this trend is expected to continue. Koomey's law states that the number of computations per kilowatt-hour roughly doubles every one and a half years [7]. According to Ashton , these two laws together have allowed the creation of computers which are both powerful and energy efficient. By turning the graph for Moore's law upside down we can interpret it as the size of a computer (of a fixed capacity) is halved every two years. By doing the same thing to Koomey's law, we can interpret it as the amount of energy required to perform a computation is dropping rapidly [8]. The combination of these interpretations informs us that it is possible for the same amount of computations to be performed on an ever smaller chip whilst consuming ever decreasing amounts of energy; consequently, computations are becoming ever more energy efficient. The potential result is a small, powerful, energy efficient computer which can provide

---

[1] IHS Technology is the world's leading source for research, analysis, and strategic guidance in the technology, media, and telecommunications industries.

[2] Procter & Gamble Co., also known as P&G, is an American multinational consumer goods company.

[3] Radio-frequency identification (RFID) uses electromagnetic fields to automatically identify and track tags attached to objects.

more advanced services while using a lesser chip area whilst consuming lower energy that previously possible.

The definition of the term IoT may be complex as its definitions vary depending upon the person defining the term [9]. The basic idea of the IoT is to interconnect things, thus enabling communication between these "things" and enabling users to communicate with them [10]. The nature of these things varies depending upon the context in which the term is used and the aim of use of the thing. The following definition of IoT is proposed by ITU's Telecommunication Standardization Sector[4]:

> *"... a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*".

Interconnecting the physical world with the virtual world and applying this concept to all things creates a myriad of new possibilities in the sense of being able to access anything at any time from any place. The provision of new possibilities is likely to lead to the generation of new threats, security risks and it could expose vulnerabilities in the, as yet, unexplored arena of interconnected everything. In the physical world, "things" are objects that physically exist and which, from an IoT user perspective, can sense, operate and connect to these things. Instead, in the virtual world, "things" are storable, accessible and processable [11]. The IoT uses sensors for information collection. These sensors are currently used in daily life, yet the majority of people may, in fact, be unaware of their use. Smartphones contain several different types of sensors, for instance accelerometers, cameras, and GPS receivers. Built-in sensors are not a novelty in today's society. Ashton stated that the IoT is already happening, but it cannot be compared to Smartphones which are both visible and tangible. RFID is an example of an IoT technology which exists but which may not necessarily be visible; therefore, IoT development may need to significantly progress prior to becoming visible to everyone [8].

---

[4] The International Telecommunication Union (ITU; French: Union International des Telecommunications), originally the International Telegraph Union, is a specialized agency of the United Nations (UN) that is responsible for issues that concern information and communication technologies.

1.2 Reference model and application areas

A reference model for the IoT has been defined by the ITU-T[5]. This reference model consists of four distinct layers, namely application layer, service support and application support layer, network layer and device layer. Management and security capabilities are included in each of these layers. These capabilities include both generic and specific capabilities that can cut across multiple layers as shown in Figure 1.1.

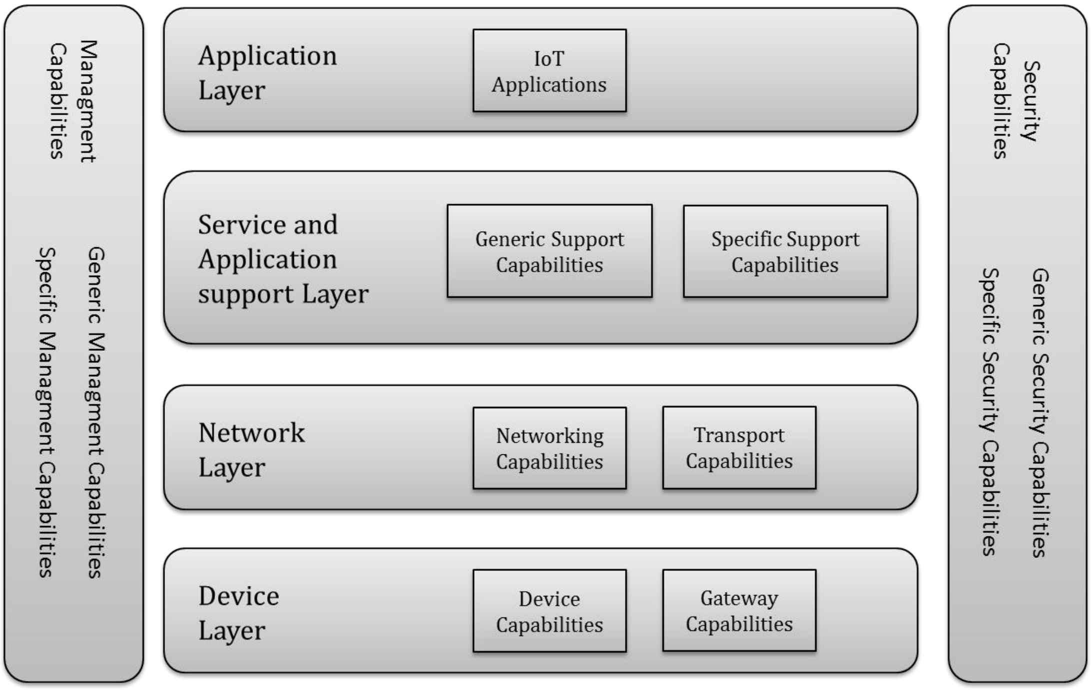


Figure 1.1 - ITU-T reference model for IoT.

IoT applications requiring certain support from the underlying layer for functioning are contained in the application. Generic support capabilities for use by IoT applications are constituted by the service and application support layer; data processing or storage are just two examples of such capabilities. Instead, specific support capabilities are those beyond the generic capabilities which are required to provide support for diversified applications [11]. The network layer is divided into networking and transport capabilities. The networking capabilities provide relevant control functions for network connectivity, while the transport capabilities focus on the IoT service transport and application specific data. At the bottom of the model, there is the device layer in which the device capabilities include direct and indirect interaction

---

[5] ITU Telecommunication Standardization Sector.

with the communication network. Unlike direct interaction, indirect interaction requires a gateway or the sending and receiving off information via the network. Two other capabilities are ad hoc networking and sleeping and waking up which enable devices to connect in an ad hoc manner and save energy (respectively) [11]. The device layer also includes gateway capabilities to support devices connected via different types of wired and wireless technologies through the support of multiple interfaces. In some situations, protocol conversion is required in order to support communication between devices that use different protocols at the device and network layer [11]. Generic management capabilities include device management (such as remote device activation, de-activation, diagnostics, and firmware or software updates) and local network topology, traffic, and congestion management [11]. The generic security capabilities are independent of the application and include authorization and authentication at the application, network, and device layer. Moreover, all the layers have their own individual capabilities. These include:

- at the application layer: application data confidentiality and integrity protection, privacy protection, security audit and anti-virus;
- at the network layer: signalling data confidentiality and integrity protection;
- at the device layer: device integrity validation, access control, data confidentiality, and integrity protection.

Both the specific management and security capabilities are closely tied with application specific requirements, such as mobile payment [11].

The term IoT is currently being used in different contexts, such as the body, homes, cities, industry, and the global environment:

- in terms of the **body**, the IoT enables sensing and connectivity. It can be used to track activity, health status, and other relevant information. It could improve not only the user's daily life, but also their future health by preventing bad habits. However, this could occur at the cost of a significant decrease in both personal integrity and personal autonomy. There are, therefore, both individual and societal issues that must be tackled with this type of IoT;
- when talking about the **home**, the IoT is often considered in terms of both remote and local monitoring as well as the management of different domestic electrical appliances and lights, or simply to keep plants in the garden alive by using an automatic watering system. Today this has become an increasingly important area as globally more and

more areas are faced with water shortages thus traditional house and garden plant watering approaches may no longer be feasible;

- with regard to **cities**, the term IoT describes the systems that effectively collect and elaborate information that is generated by different infrastructures such as, for example, the monitoring of centres for traffic lights, street lights, camera surveillance and the power grid. These systems offer the possibility to enhance flows of vehicles and people through the city centres ; furthermore they can also improve transport system energy efficiency whilst improving both personal and societal safety;
- the principal goals of IoT solution applications in **industry** are typically operations optimization, productivity increase, resource saving and cost reduction. In industry, the IoT can be used to monitor business assets, to improve environmental safety and for quality and consistency maintenance in production processes. The use of IoT, in these instances, is not only motivated by companies being motivated by environmental issues but also because significant economic advantages are to be had through a better understanding of improved process control (in terms of quality maintenance), while also limiting detrimental effects on the environment;
- last, but not least important, is **environmental monitoring** where the IoT can be an aid in the better understanding of and better management of resources. Sensors can be used to help protect wildlife, monitor water usage and flows, monitor local weather, monitor use of natural resources, or provide warnings prior to and after natural disasters to help people prepare [12]. In fact, an increasing use of technology (be it in production, consumption, recycling or post-recycling phases) appears to be necessary in order to achieve high environmental efficiency.

The IoT includes different objects with different capabilities, which, however, share a common mode of communicating (a communication chain through a communication network) to enable the transfer of information in which two or more objects understand the information to render a process more efficient, often by minimizing both human factors and interaction. Objects are both virtual and physical objects which are not limited to electronic devices (such as computers, mobile phones, televisions, machines, and robots) and sensors (connected either through devices or gateways). Communicating includes different protocols and technologies for the sending of digital or analogue signals through nodes (e.g. Constrained Application Protocol, File Transfer Protocol, Hypertext Transfer Protocol, etc. in Local Area Networks, Wide Area Networks, Body Area Networks, Wi-Fi, Ethernet, fibre optic links, radio etc.). Whereas, capabilities include, but are not limited to information gathering, information processing, information storage and information presentation. A process could consist of the tracking of health information, home heating, street lighting or the monitoring of assets

An example of non-IoT is formed by a single object speaking its own language (even using protocols) which is potentially connected to a communication network (e.g. Internet), yet no other object can interpret this data and, consequently, no other object can contribute with any functionality or usefulness to this non-IoT device. However, as soon as there is another device at the end of the communication path that is able to use the same protocols, it is subsequently possible to establish communication and potentially increase efficiency. A practical example of IoT is the *Bigbelly smart waste and recycling system*, shown in Figure 1.2. In this system, stations (objects) produced for waste collection, monitor (capability) and report (communicate) station fullness and station-specific data remotely, in this case to the Bigbelly cloud (object). This is of assistance in informing refuse collectors of when and where a station needs to be emptied (process) which to date has been a guessing game [13].

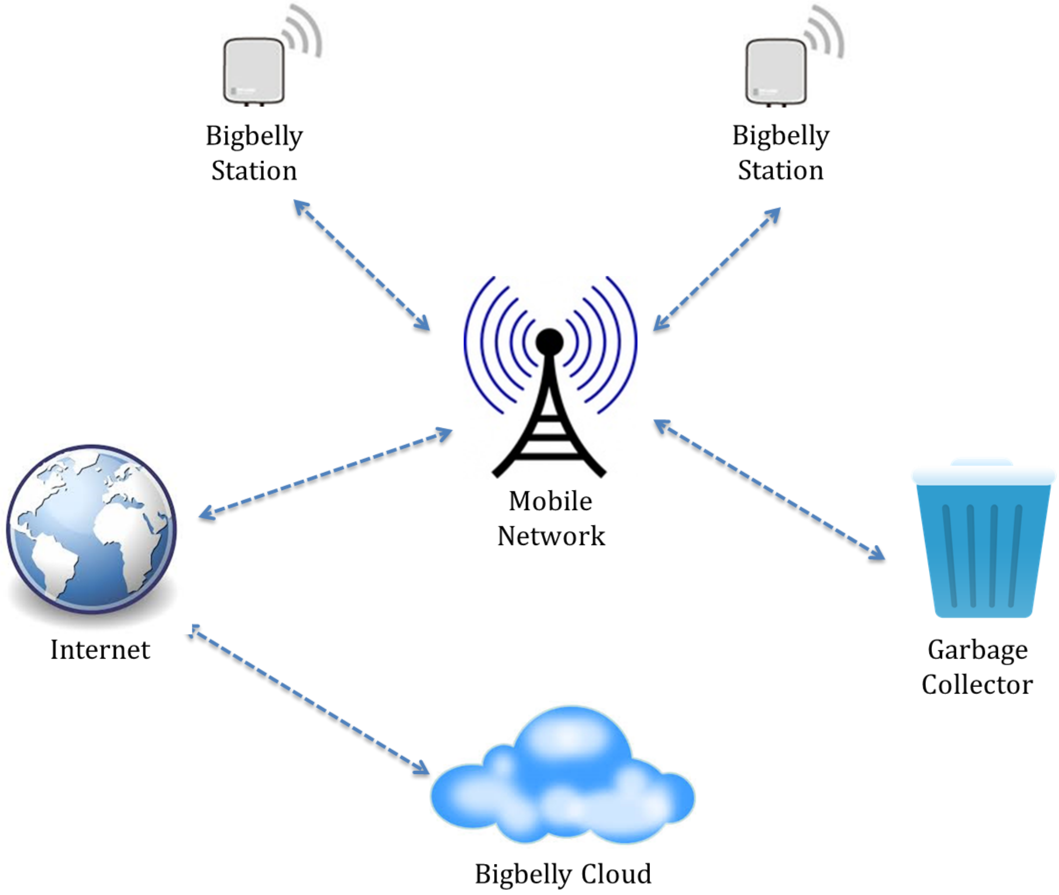


Figure 1.2 - Bigbelly IoT example.

1.3 Interoperability and protocols convergence

The evolution of the future internet is being shaped by the IoT . After connecting people anytime and everywhere, the next step is to interconnect heterogeneous things / machines / smart objects both between themselves and with the Internet; enabling the creation of value added open and interoperable services/applications, enabled by their interconnection, so that they can be integrated with both actual and new business and development processes. As for the IoT, future networks will continue to be heterogeneous, multivendor, multi-services and widely distributed. Subsequently, the risk of non-interoperability will increase. This could lead to the unavailability of some services for end-users that could have catastrophic consequences regarding applications related to emergencies or health, etc. Furthermore, it could also mean that users/applications could possibly lose key information from the IoT due to this lack of interoperability. Therefore, it is essential to guarantee that network components will interoperate to release the full value of the Internet of Things. Interoperability is a key challenge in the realms of the Internet of Things . This is due to the intrinsic fabric of the IoT as:

- **high–dimensional**, with the co-existence of many systems (devices, sensors, equipment, etc.) in the environment that have to communicate and exchange information;
- **highly-heterogeneous**, where these large systems are conceived by a plethora of manufacturers and are designed for many different purposes and target diverse application domains, rendering it highly difficult (if not impossible) to establish global agreements and widely accepted specifications;
- **dynamic and non-linear**, where new Things (that were not even initially considered) are entering (and leaving) the environment continuously which support new unforeseen formats and protocols but that need to communicate and share data in the IoT;
- **hard to describe/model** due to the existence of many data formats, described in many different languages, that can share (or not) the same modelling principles, and that can be interrelated in many ways with one another. This qualifies interoperability in the IoT as a complex issue.

Furthermore, the Internet of Things can be considered as being both the first and the last frontier of interoperability. It can be considered as the first frontier of interoperability in that it is the initial mile of a sensing system where interoperability has the potential to enable Things to talk and collaborate altogether for a higher purpose. It can be considered as the final frontier as it may be the place where interoperability is more difficult to tackle due to the unavoidable complexities of the IoT. Thus, there is a need for some novel approaches and understandings of interoperability for the IoT, ensuring that it endures and that it is sustainable. Thus a sustainable interoperability is required in the IoT There is, therefore, a need to cope both with the complex nature and the sustainability requirement of IoT interoperability. In order to do so, a framework for sustainable interoperability is required which targets the Internet of Things taking into consideration both its specifics and constraints. This framework may and ought to learn from the best-of-breed interoperability solutions from related domains (e.g. enterprise interoperability), to select their good approaches and principles of these while understanding the differences and particulars posed by the Internet of Things. The framework for sustainable interoperability in Internet of Things applications needs, at least, to address the following aspects:

- **Management of Interoperability in the IoT**: in order to correctly support interoperability in the Internet of Things, interoperability resources need to be efficiently and effectively managed. It is necessary to understand what needs to be managed, to what extent and how, in respect to interoperability in the Internet of Things;
- **Dynamic Interoperability Technologies for the IoT**: for enduring interoperability in the complex IoT environment, it is necessary for Things to be permitted to enter and dynamically interoperate without needing to be remanufactured. Therefore, it is necessary to understand the approaches and methods needed to create IoT dynamic interoperability;
- **Measurement of Interoperability in the IoT**: in order to properly manage and execute interoperability in the IoT it is necessary to quantify and/or qualify interoperability itself. As Lord Kelvin stated: “If one cannot measure it, one cannot improve it”. Then, what methods and techniques are required to provide an adequate measurement of Interoperability in the Internet of Things?
- **Interaction and integration of IoT in the global Internet**: IPv6 integration, global interoperability, IoT-Cloud integration, etc. namely, how to bridge billions of smart things globally, while respecting their specific constraints.

There are different areas in interoperability such as at least four areas on technical interoperability, syntactic, semantic interoperability and organizational interoperability. Technical Interoperability is usually associated with hardware/software components, systems and platforms that enable machine-to-machine communication to occur. This kind of interoperability is often centred on both the (communication) protocols and the infrastructure needed for them to operate and it is necessary to pay specific attention as many protocols are developed within SDOs and they will necessitate a market proof approach to validate and implement these protocols leading to the obtainment of IoT products which are truly interoperable and global.

Validation is an important aspect of interoperability (also in the Internet of Things). Both testing and validation provide assurance that interoperability methods, protocols, etc. are able to cope with the specific nature and requirements of the Internet of Things. The main way, among others, is to provide test suites which are efficient and accurate and associated interoperability testing methodology (with associated test description/coding languages) that help in thoroughly testing both the underlying protocols used by interconnected things / machines / smart objects and the embedded services / applications. It is essential that the testing features and facilities are built into design and deployment process, as the conditions of communication means, object/things availability and accessibility may change over time or location. It is extremely important that these new testing methods consider the real context of future communicating systems where these objects will be deployed. Indeed, contrary to most of the existing testing methods, interconnected things / machines / smart objects in the IoT are distributed naturally. As they are distributed, the usual and classical approach of a single centralized testing system dealing with all these components and the test execution is no longer applicable. The distributed nature of the tested components requires a shift towards distributed testing methods. Testing must be conducted in a (close to) real operational environment in order for there to be increased confidence in the real interoperability of these components when they will be deployed in real networks. In this context of IoT where objects are connected through radio links, the communicating environment may be unreliable and non-controllable if it fails to seriously address interoperability testing challenges with the same intensity and complexity of the IoT research itself. In order to use the full potential of the IoT paradigm, interconnected devices need to communicate using lightweight protocols that do not demand extensive CPU resource use. C, Java, MQTT, Python and some scripting languages are the preferred choices used by IoT applications. The IoT nodes use separate IoT gateways if protocol conversion, database storage, or decision making is required to supplement the low-intelligence node. One of the most important aspects for a convergence protocol that supports information exchange between domains, is the ability to convey the information (data) contained in a particular domain to other domains. This section provides an overview of the existing data exchange protocols that can be applied for data exchange among various domains. Today there are two dominant architectures for data exchange protocols:

- **bus-based**: clients publish messages for a specific topic which are directly delivered to the subscribers of that topic. There is no centralized broker or broker-based services. Examples of bus-based protocols include Data Distribution Service (DDS), Representational State Transfer (REST) and Extensible Messaging and Presence Protocol (XMPP);
- **broker-based architecture**: the broker controls information distribution. For example, it stores, forwards, filters and prioritizes publish requests from the publisher (the source of the information) client to the subscriber (the information consumer) clients. Clients switch between publisher and subscriber roles depending on their objectives. Examples of broker –based protocols include Advanced Message Queuing Protocol (AMPQ), Constrained Applications Protocol (CoAP), Message Queue Telemetry Transport (MQTT) and Java Message Service API (JMS).

Another important way to classify these protocols is whether they are message-centric or data-centric. Message centric protocols such as AMQP, MQTT, JMS and REST focus on message delivery to the intended recipient(s), regardless of the data payload it contains. A data-centric protocol such as DDS, CoAP and XMPP focuses on delivering the data and assumes that the data is understood by the receiver. Middleware understands the data and ensures that the subscribers have a synchronized and consistent view of the data. Yet another fundamental aspect of these protocols is whether it is web-based like CoAP or application-based such as with XMPP, and AMQP. These aspects have a fundamental effect on the environment, performance and tools available for implementers.

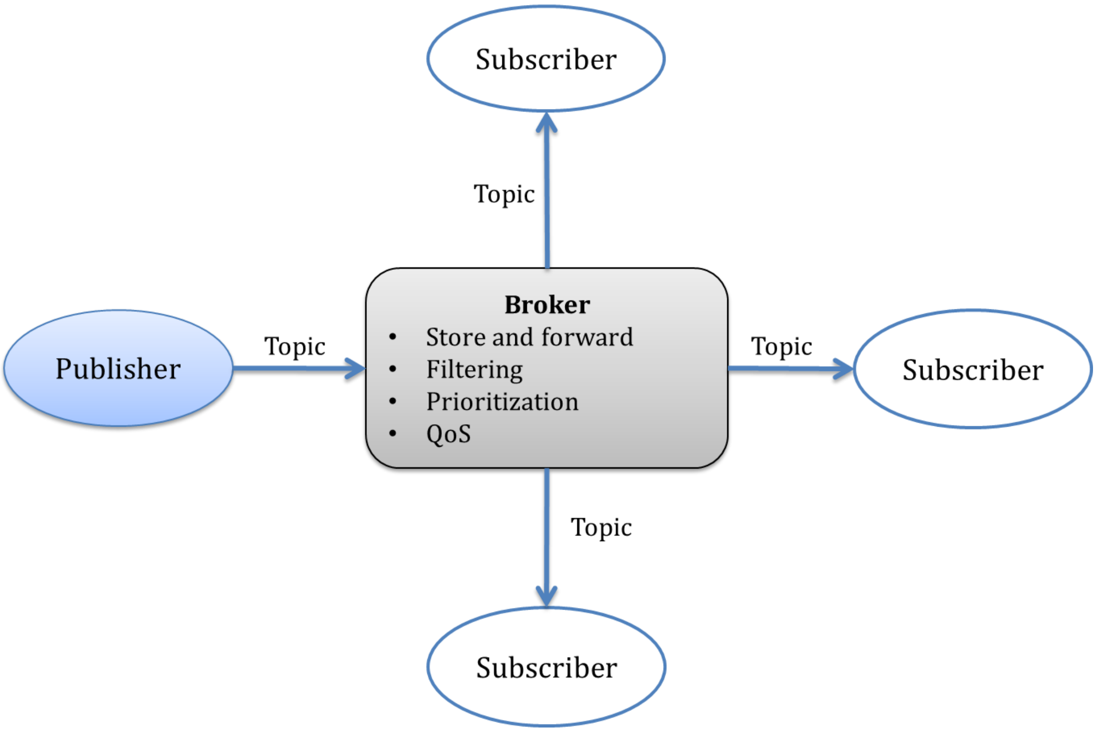


Figure 1.3 – Broker-based architecture for data exchange protocols.

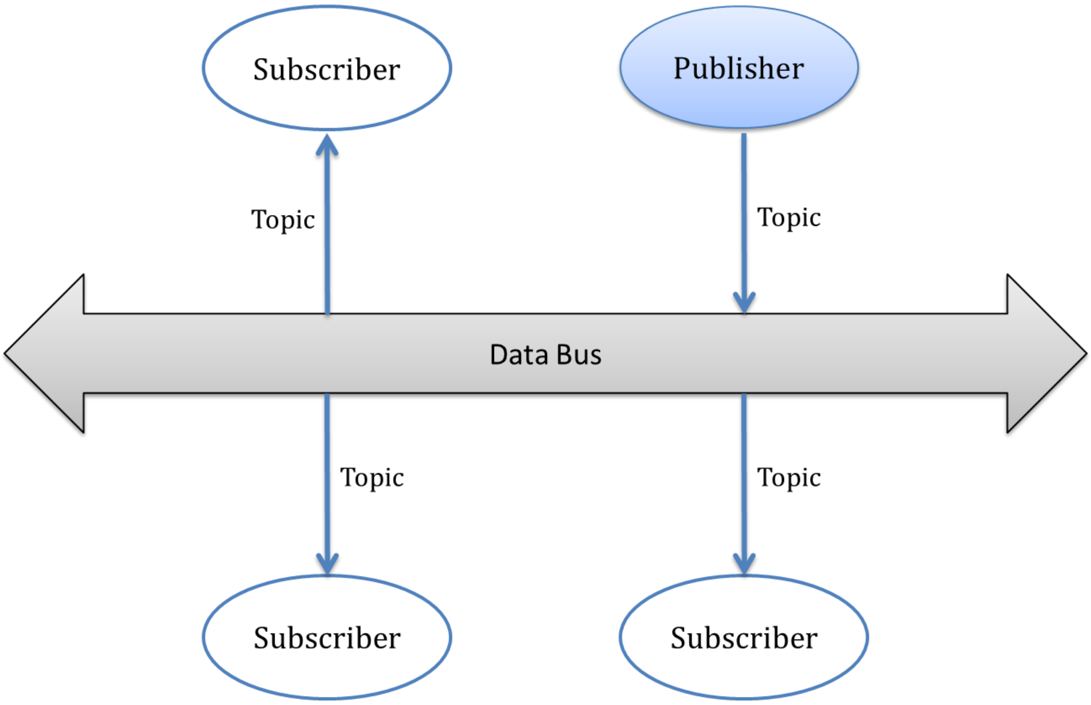


Figure 1.4 - Bus-based architecture for data exchange protocols.

1.4 Communication models

From an operational perspective, it is useful to consider how IoT devices connect and communicate in terms of their technical communication models. In March 2015, the Internet Architecture Board (IAB)[6] released a guiding architectural document for the networking of smart objects[7]. It outlines a framework of four common communication models used by IoT devices. The discussion below presents this framework and explains key characteristics of each model in the framework.

1.4.1 Device-to-Device Communications

The device-to-device communication model represents two or more devices that directly connect and communicate between one another, instead of through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. However, these devices frequently use protocols such as Bluetooth [15], Z-Wave [16], or ZigBee [17] to establish direct device-to-device communications, as shown in Figure 1.5.

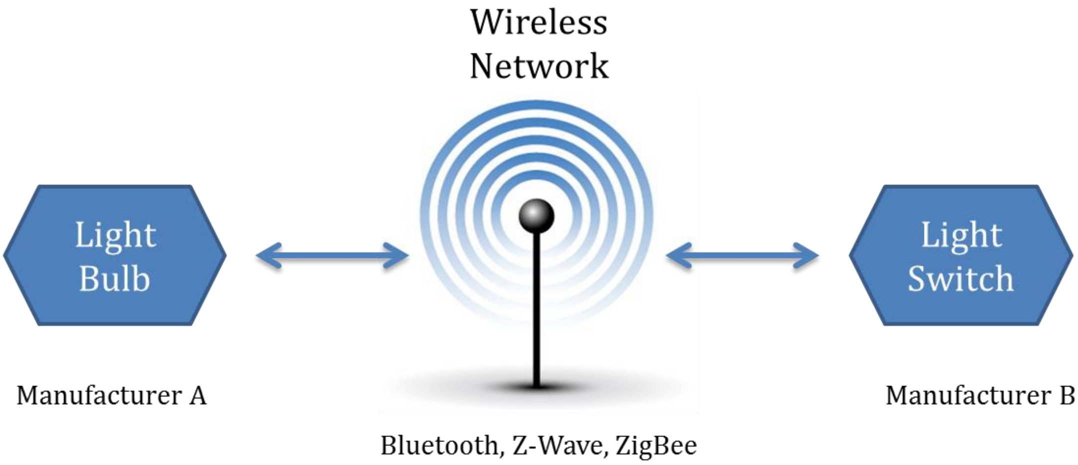


Figure 1.5 - Example of device-to-device communication model.

---

[6] Committee of the Internet Engineering Task Force (IETF) and an advisory body of the Internet Society (ISOC). Its responsibilities include architectural oversight of IETF activities, Internet Standards Process oversight and appeal, and the appointment of the Request for Comments (RFC) Editor. The IAB is also responsible for the management of the IETF protocol parameter registries

[7] RFC 7452 [14]

These device-to-device networks allow devices adhering to a particular communication protocol to communicate and exchange messages to achieve their function. This communication model is commonly used in applications like home automation systems, which typically use small data packets of information to communicate between devices with relatively low data rate requirements. Residential IoT devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other (e.g. a door lock status message or turn on light command) in a home automation scenario. This device-to-device communication approach illustrates many of the interoperability challenges discussed later in this work. As an IETF Journal article describes:

"…These devices often have a direct relationship, they usually have built-in security and trust mechanisms, but they also use device-specific data models that require redundant development efforts by device manufacturers" [18].

This means that device manufacturers ought to invest in development efforts to implement device-specific data formats rather than open approaches that enable use of standard data formats. From the user's point of view, this frequently means that underlying device-to-device communication protocols are incompatible, obliging the user to select a family of devices which use a common protocol. For example, the family of devices using the Z-Wave protocol is not natively compatible with the ZigBee family of devices. While these incompatibilities limit user choice to devices within a particular protocol family, the user benefits from knowing that products within a particular family tend to communicate well.

1.4.2 Device-to-Cloud Communication

In a device-to-cloud communication model, the IoT device connects directly to an Internet cloud service such as an application service provider to exchange data and control message traffic. This approach frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service. This is shown in Figure 1.6.

Figure 1.6 - Device-to-cloud communication model diagram.

Some popular consumer IoT devices, such as the Nest Labs Learning Thermostat [19] and the Samsung Smart TV [20] use this communication model. In the case of the Nest Learning Thermostat, the device transmits data to a cloud database where it can be used for the analysis of home energy consumption. Moreover, through its cloud connection , the user can access their thermostat remotely via their smartphone or Web interface, and thermostat software updates are also supported. A similar scenario occurs with Samsung Smart TV technology. The television uses an Internet connection to transmit user viewing information to Samsung to analyse and to enable the TV interactive voice recognition features. In the aforementioned cases, the device-to-cloud model provides additional value to the end user as the device's capabilities reach beyond its native features. However, challenges regarding interoperability may occur when attempts are made to integrate devices produced by other manufacturers. Often, both the device and cloud service are provided by the same vendor [18]. If proprietary data protocols are used between the device and the cloud service, then the device owner or user could find himself tied to the use of a cloud service, which can limit, or even prevent, the use of alternative service providers. This situation is usually referred to as "vendor lock-in'', a term that also includes other elements of the relationship with the provider such as data ownership and access. Concurrently, users may be safe in the knowledge that they can integrate devices designed for the specific platform.

1.4.3 Device-to-Gateway Model

In the device-to-gateway model, or more typically, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a conduit to reach a cloud service. In other words, this basically means there is application software operating on a local gateway device; it is an intermediary between the device and the cloud service providing security and other functionality such as data or protocol translation. The model is shown in Figure 1.7.

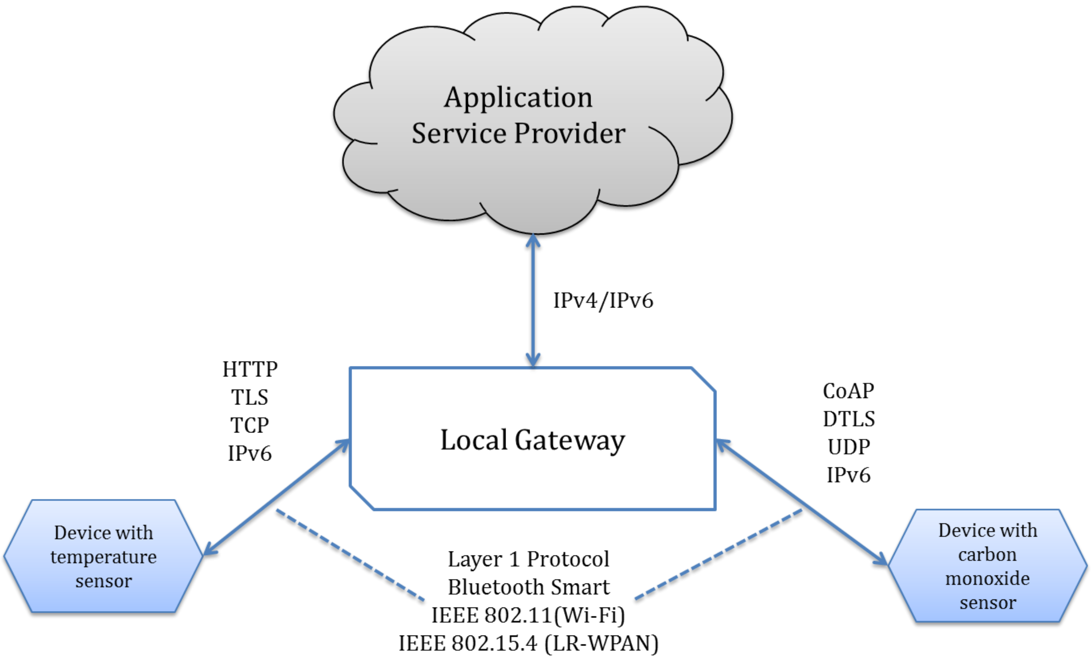


Figure 1.7 - Device-to-gateway communication model diagram.

Several variations of this model are to be found in consumer devices. Often, , the local gateway device consists of a smartphone running an app to communicate with a device and transmit data to a cloud service. Personal fitness trackers are one such popular consumer items that often use this model. These devices do not possess the native ability to connect directly to a cloud service, therefore, they often depend on smartphone app software to act as an intermediary gateway connecting fitness device to the cloud. Another form of this device-to-gateway model is found in the use of “hub” devices in home automation applications. These are devices serving as a local gateway between individual IoT devices and a cloud service, yet they are also capable of bridging the interoperability gap between devices themselves. For instance, the SmartThings hub is a stand-alone gateway device that has both Z-Wave and ZigBee transceivers installed to communicate with both device families [21]. Then, it connects to the SmartThings cloud service, which allows the user to access the devices using a smartphone app and an Internet connection. From a broader technical perspective, the IETF Journal article explains the benefit of the device-to-gateway approach:

“This communication model is used in situations where the smart objects require interoperability with non-IP devices. Sometimes this approach is taken for integrating IPv6-only devices, which means a gateway is necessary for legacy IPv4-only devices and services”. [18]

Essentially, this communications model is frequently employed to integrate new smart devices into a legacy system with devices that are not natively interoperable with them. However, a negative aspect of this approach is that complexity and cost is added to the overall system due to the necessary development of the application-layer gateway software and system. The IAB's RFC7452 document suggests the outlook for this model:

> *"It is expected that in the future, more generic gateways will be deployed to lower cost and infrastructure complexity for end consumers, enterprises, and industrial environments. Such generic gateways are more likely to exist if IoT device designs make use of generic Internet protocols and not require application-layer gateways that translate one application-layer protocol to another one. The use of application-layer gateways will, in general, lead to a more fragile deployment, as has been observed in the past…" [22].*

Device-to-gateway communication systems evolution and its more extensive role in addressing the challenges of interoperability between IoT devices is still unfolding.

1.4.4 Back-End Data-Sharing Model

The back-end data-sharing model refers to a communication architecture which allows users to export and analyse smart object data from a cloud service together with data from other sources. This architecture supports "the user's desire for granting access to the uploaded sensor data to third parties" [23]. This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where "IoT devices upload data only to a single application service provider'' [23]. A back-end sharing architecture allows aggregation and analysis of the data collected from single IoT device data streams. For instance, a corporate user in charge an office building could be interested in the consolidation and analysis of energy consumption and utilities data provided by all the IoT sensors and Internet-enabled utility systems located in the offices. It is often the case that in the single device-to-cloud model, the data produced by each IoT sensor or system remains in a stand-alone data silo. An effective back-end data sharing architecture would effectively allow the cloud data produced by the entire range of devices in the premises, to be easily accessed and analyzed. Moreover, this type of architecture facilitates data portability needs. Effective back-end data-sharing architectures allows data to be moved by users when they change IoT services, removing traditional data silo barriers. The back-end data-sharing model suggests that in order to achieve cloud hosted smart device data interoperability, a federated cloud services approach[8] or cloud applications programmer interfaces (APIs) are required [24]. Figure 1.8 shows a graphical representation of this design.

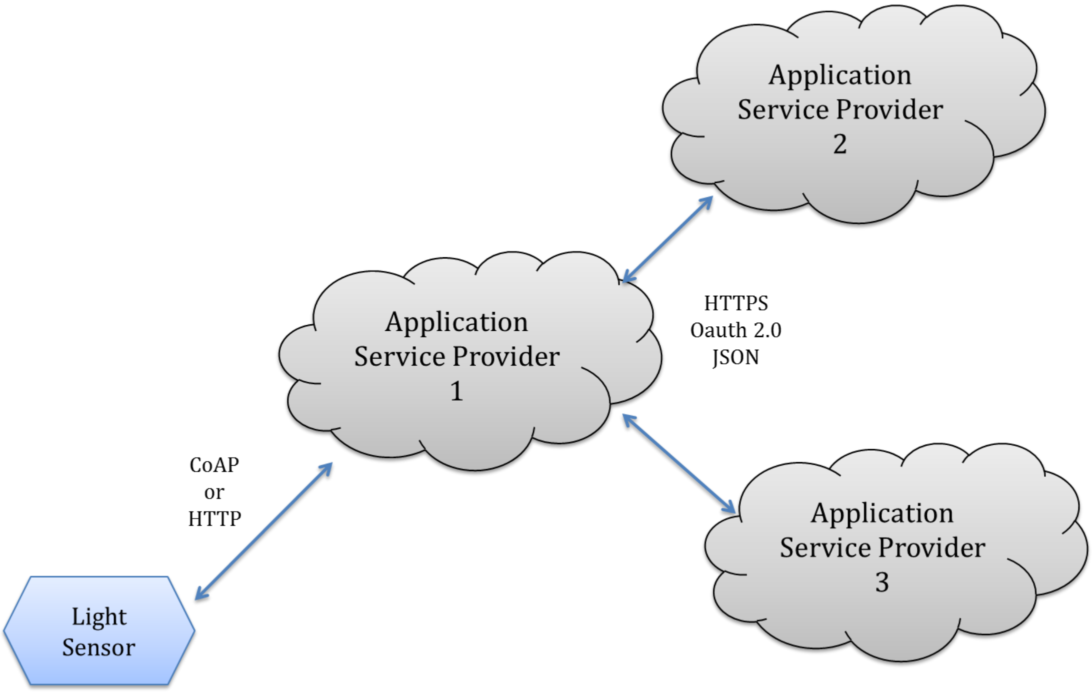


Figure 1.8 - Back-end data sharing model diagram.

This architecture model constitutes an approach to achieve interoperability between these back-end systems. As suggested by the IETF Journal:

“Standard protocols can help but are not sufficient to eliminate data silos because common information models are needed between the vendors.” [25]

In other words, this communication model effectiveness depends on the underlying IoT system designs. Back-end data sharing architectures are not able to fully overcome closed system designs.

The underlying strategies used which enable IoT device communication are demonstrated by the four basic communication. Besides some technical considerations, the open versus proprietary nature of the networked IoT devices significantly influences the use of these models. Moreover, in the case of the device-to-gateway model, an ability to surpass proprietary device

---

[8] A federated cloud services approach is one that combines the resources of separate cloud service providers to meet a larger business need.

restrictions in connecting IoT devices constitutes its primary feature. Consequently, device interoperability and open standards are key considerations in both the design and development of internetworked IoT systems. From a general user perspective, these communication models help highlight the ability of networked devices to add value to the end user. The total value of the device is increased by its capacity to enable the user to achieve improved access to an IoT device and its data. For instance, in three of the four communication models, a cloud computing setting is used to provide connection to data analytic services. Through the creation of data communication conduits to the cloud, the users, and service providers employment of data aggregation, big data analytics, data visualization, and predictive analytics technologies is facilitated which, in turn, permits for the obtainment of more value from IoT data than that which can be achieved in traditional data-silo applications. Namely, effective communication architectures can be considered as an important driver of value to the end user by creating possibilities of using information in new ways. It is, however, necessary to note that these networked benefits are accompanied by trade-offs. Careful consideration of the incurred cost burdens placed on users to connect to cloud resources when considering an architecture is needed, particularly in locations where user incur high connectivity costs. . Even though the end user benefits from effective communication models, it is necessary to state that effective IoT communication models can also enhance technical innovation and create opportunities for commercial growth. It is possible to design new products and services to exploit IoT data streams that did not previously exist, thus acting as a catalyst for further innovation.

CHAPTER 2

WIRELESS IOT CONNECTIVITY AND ENERGY ISSUES

Different types of wireless technologies exist that are relevant for the IoT; these different technologies span a variety of spaces from just a few centimetres to many kilometres. Wireless Personal and Local Area Network technologies (WPAN\LAN) such as: Bluetooth, ZigBee, 6LowPAN, and Wi-Fi are recommended for short to medium range communication. Whereas, for long range communication Wireless Wide Area Network technologies (WWAN) are recommended; these which can be divided into two types, namely whether to use licensed (Cellular 2G/3G/4G and 5G in future) or licensed-exempt technologies (LPWA LoRa, SIGFOX, and other). As shown in Figure 2.1 connectivity is the foundation for IoT, and the nature of the type of application determines the type of access required. Radio technologies operating on the unlicensed spectrum which had been designed for short-range connectivity with limited QoS and security requirements that are typically applicable for a home or indoor environment, serve many IoT devices.

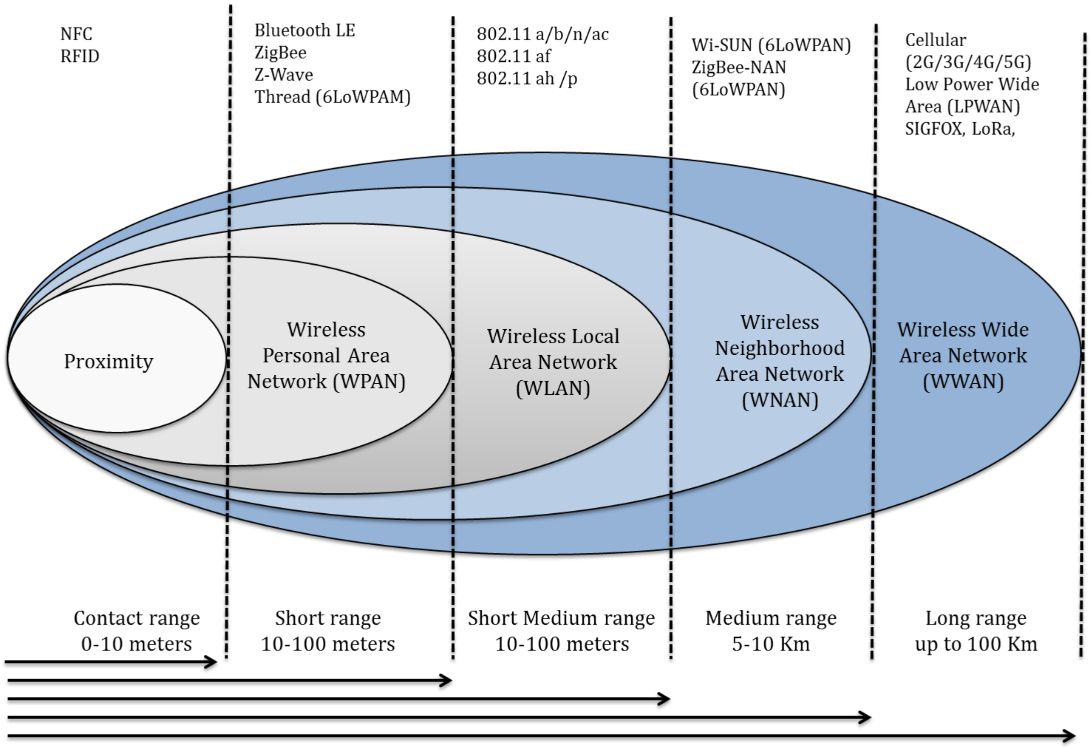


Figure 2.1 - Wireless IoT connectivity technologies.

2.1 Short Range Connectivity Technologies

Wi-Fi is a prime candidate that can ensure connectivity in IoT applications due to its significant growth over the past years, despite it consuming greater energy. Nowadays, most places where people may wish to send something or transmit data, has Wi-Fi coverage. Unfortunately, Wi-Fi has been beyond the reach for sensor communications due to the significant high energy consumption with its traditional protocols. However, this has changed as since 2006, the Wi-Fi community started applying a well-known technology such as duty cycling, which consists of putting chips into sleep mode for most of the time and low power Wi-Fi module lights such as the Microchips RN171 module which is a standalone module, embedded 802.11 b/g Wireless Local Area Network (WLAN) module [131]. IEEE 802.15.4 technology is another suitable candidate for short range connectivity . IEEE 802.15.4 has been implemented by several leading radio manufacturers. The Internet Engineering Task Force (IETF) introduced the 6LowPAN protocol and ZigBee alliance produced the ZigBee protocol over low power IEEE802.15.4 protocol. In particular, the IETF 6LowPAN defines both the frame format and several mechanisms required for IPv6 packets on IEEE 802.15.4 networks. 6LowPAN is the acronym for IPv6 over low-power personal area networks. The concept behind

6LowPAN is the aim to bring the Internet Protocol (IP) directly into small, low-cost sensor devices. Since there are insufficient addresses in IPv4, 6LowPAN starts from the premise of IPv6, with the aim of providing an address to each device [132]. Early optimization efforts have shown that Wi-Fi may be 10 times more energy efficient than ZigBee, given the broad spectrum of data rates required for IoT applications. IEEE has started working on a low power Wi-Fi version, which is standardized in IEEE 802.11ah.

2.2 Long Range Connectivity Technologies

Currently, there are two alternative connectivity tracks for the many IoT applications that are dependent on wide-area coverage:

- **Cellular Technologies**: 3GPP technologies like GSM, WCDMA, LTE and future 5G. These WANs operate on the licensed spectrum and in the past, have primarily targeted high-quality mobile voice and data services. However, they are now rapidly evolving with new functionality and the new radio access technology narrowband IoT (NB-IoT) specifically tailored so that it constitutes an attractive solution for emerging low power wide area (LPWA) applications [133];
- **Unlicensed LPWA**: new proprietary radio technologies, such as those provided by SIGFOX and LoRa, have been developed and designed solely for machine-type communication (MTC) applications addressing the ultra-low-end sensor segment, with extremely limited demands on throughput, reliability or QoS. IoT applications can be segmented through their categorization according to coverage needs and performance requirements (such as data speed or latency demands). The different types of technologies that can be used for the IoT with different coverage areas and within the unlicensed spectrum are shown in Figure 2.2 [133]. Cellular connectivity applications are concentrated in traditional applications such as transportation, automotive, and location management. Cellular 2G connectivity provides the benefit of the world-wide web; nevertheless, cellular connectivity is not without limitations which are addressed by LPWA. Two key issues are at the center of these limitations: high power consumption that denies battery operation over an extended time period reaching into years, and the cost of service including device cost, as well as the cost of the supporting infrastructure that factors into the return on investment for the service provider. In brief, existing cellular mobile networks and short range technologies are complemented by LPWA, enabling wide area communications with lower cost points and with better

power consumption properties. However, it is important to note that as recently as early 2013, the term “LPWA” did not yet exist. Since then, the LPWA space has become one of the fastest developing areas of the Internet of Things (IoT) market, bearing witness the incredible potential for LPWA technologies [134]. Low-Power Wide-Area (LPWA) is an umbrella term for a group of technologies that have the following key properties:

- long battery life, often more than 10 years;
- wide area connectivity characteristics, allowing for out-of-the-box connected solutions;
- low cost chipsets and networks;
- limited data communications throughput capacity.

LPWA technologies tend to be narrowband (with some exceptions) and operate in the ISM license-exempt spectrum bands. Recently, GERAN and 3GPP standards organizations launched on a process of standardizing narrowband technology for use in the mobile spectrum. Several proponents of LPWA technologies have put forward their technologies. The competition in the standards race extends to 3GPP, where the roadmap for a cost reduced LTE module for IoT applications is currently being developed (LTE-M). Instead, some other standard organizations are currently focusing on 5G technologies. Market forecasts for LPWA vary between a low of 1 billion and a high of 3 billion connected devices by 2020, most of which will be in North America, Europe and the Asia Pacific region deployed in leading applications such as smart cities, smart buildings, agriculture and the environment, as well as utilities [134, 135].

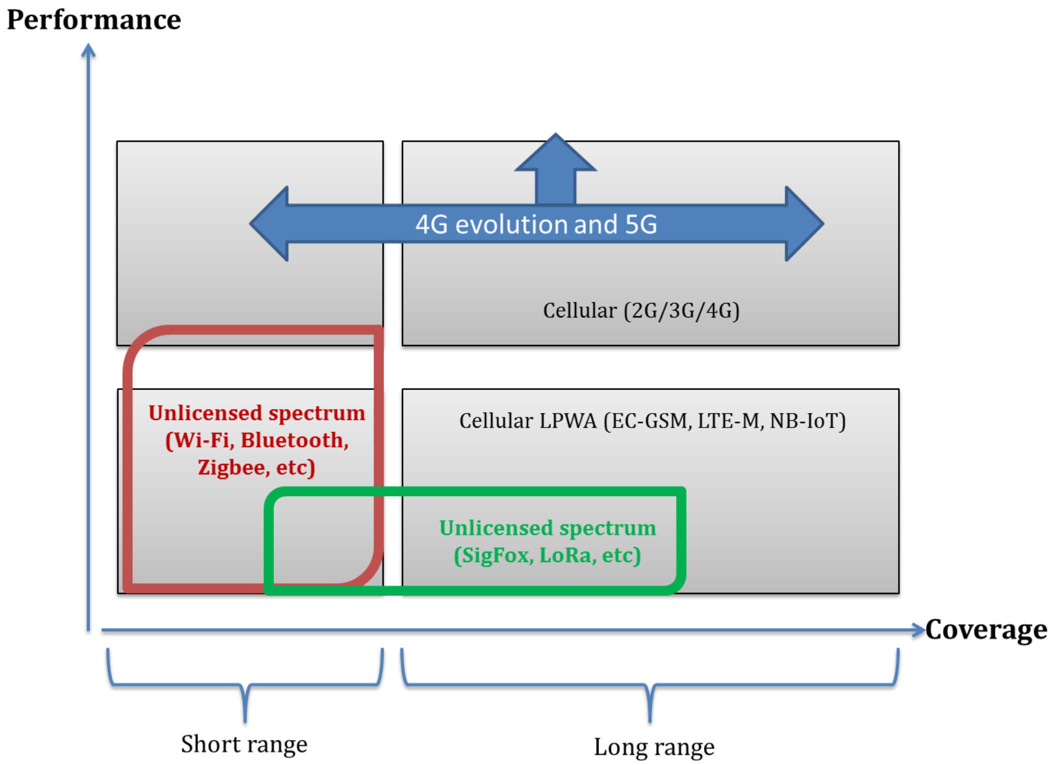


Figure 2.2 - Technologies addressing different segments.

For several years, Sigfox and LoRa have been competitors in the LPWAN space. While the two companies have quite different business models and technologies, their ultimate goals are actually very similar. The goal of the LoRa Alliance, LoRaWAN adopters, and Sigfox is for their technology to be adopted by mobile network operators for IoT deployments over both city and nationwide low power, wide-area networks (LPWANs). However, there are some significant differences as to how each technology aims to meet this objective and which applications the technology is best suited for.

2.2.1 LoRa

LoRa is proprietary LPWA technology that typically operates in the unlicensed spectrum i.e. ISM band. While the LoRa physical layer is proprietary, the rest of the protocol stack, known as LoRaWAN, is kept open, and its development is conducted by the LoRa Alliance, led by IBM, Actility, Semtech, and Microchip. As shown in Figure 2.3, the LoRa network is deployed in accordance with star-of-stars topology, in which the leaf nodes (end devices) are connected to one or multiple LoRa gateways, via a single-hop LoRa link. The gateways are connected, over standard IP protocols, to a network server (NetServer). The technology employs a spreading technique, in accordance with which a symbol is encoded in a longer sequence of bits, thus increasing both the signal-to-noise (SNR) and interference ratios required for correct reception, without altering the frequency bandwidth of the wireless signal. LoRa technology has made the provision of variable data rates possible, offering a trade-off between throughput and coverage range or energy consumption [136].

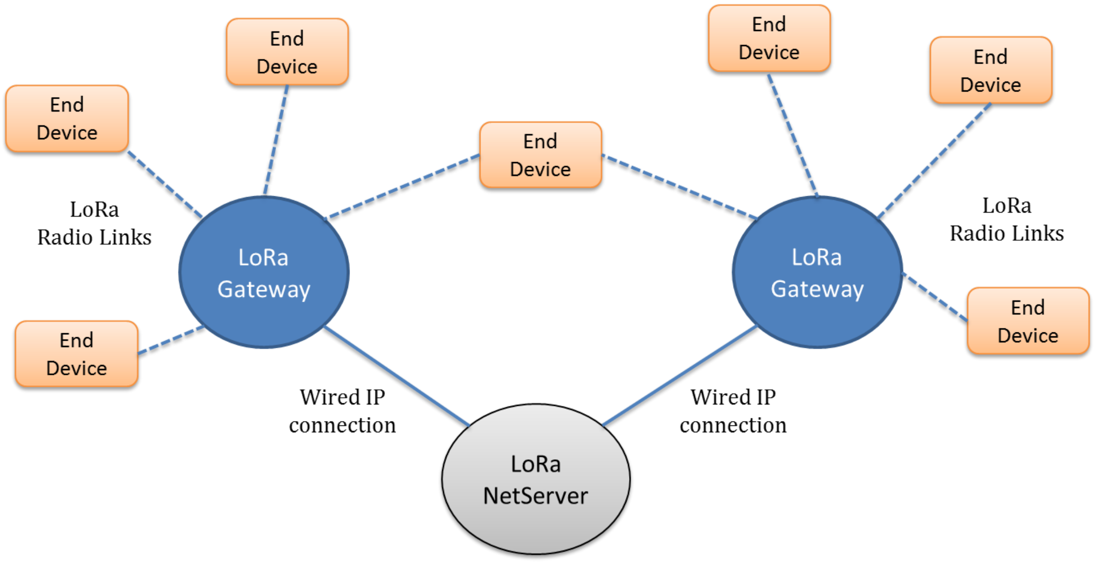


Figure 2.3 – Overview of LoRa Architecture.

LoRa offers three type of devices, each intended for different purposes.

- **Class A (for all) Devices**: are devices which have been designed for deployment in monitoring applications, where a centralized controlling entity can accommodate the data generated by all leaf nodes;
- **Class B (for beacon) Devices**: are devices synchronized with the NetServer in order to receive commands from a controller to perform a specific function. Examples include actuators and switches etc.;
- **Class C (continuous listening) devices:** are devices that always keep the receive windows open; they operate without any strict constraints on energy requirements. Examples are devices connected to power grids.

Advantages are:

- the ability to trade-off between range and data rate, allowing the devices to work in a harsh environment with a lesser data rate but a robust link connection owing to spreading technology;
- coverage of a greater area with less gateways compared to cellular networks [136].

Disadvantages are:

- the use of gateways for communicating with end devices could lead to the creation of a bottleneck due to a single failure point;
- LoRa operates in the un-licensed band which sets a limitation of 1% on the duty cycle. Consequently, LoRa lacks predictability as the protocol has a highly variable frame length, the transmission time depends on the data-rate when the network controls the data-rate and not the device.

Table 2.1 – Specifications of LoRa.

Specification/feature	**LoRa support**
Frequency range	ISM band 868 MHZ 915 MHZ
Data Rate	< 10 kbps
Channel Bandwidth	< 500 KHz
Coverage	< 11 km
Energy need	Low
Battery Life	> 10 years

2.2.2 Sigfox

Sigfox is a pioneer in LPWA technology which was introduced in IoT market in 2009 and which has continued to grow since. Sigfox, like LoRa, is proprietary and offers a much lesser data rate, about 100-1000 times less than other IoT technologies. Sigfox devices use ultra-narrowband modulation while the network level protocols are proprietary. Sigfox is developing this technology with the aim of deploying a controlled network dedicated to IoT, much like a cellular network. Employment of the Sigfox certified transmitter in devices is a solution for the customer. Device transmitted data is first routed to the Sigfox server to be scrutinized for data integrity and security. Successively, it is routed back to the application’s IT network, thus it is easier for the user to collect data from the deployed devices.

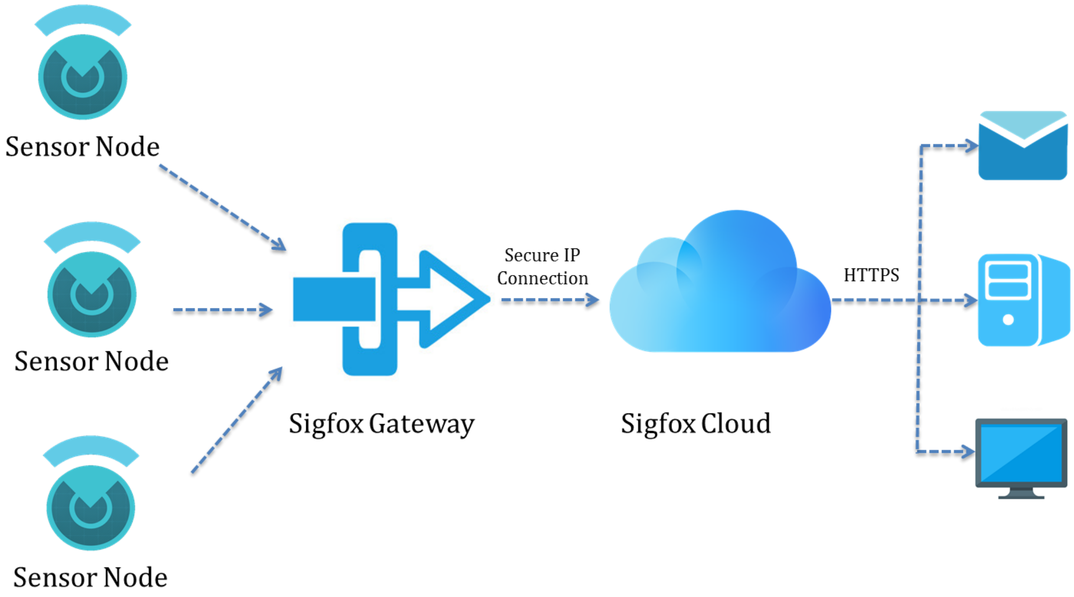


Figure 2.4 – Overview of Sigfox Architecture.

A unique global cellular connectivity solution, from the customers' devices to their software applications is provided by Sigfox. Sigfox devices have been designed to capture markets such as agriculture and environment, automotive, buildings, consumer electronics. A Sigfox certified local cellular operator sells a customer a subscription and they can deploy the smart embedded devices – connected all over the internet.

Advantages are:

- extremely low data rate (100 bps) offers good sensitivity in long range communication spanning multiples of kilometres;
- Sigfox states that each gateway has the potential to handle up-to millions of connected devices and cover a rural area of 30-35 km rural and an urban area of 3-10 km.

Disadvantages are:

- Sigfox does not implement any collision avoidance, fair use, and listen-before-talk mechanism. Consequently, multiple Sigfox devices working in the ultra-narrowband spectrum could offer the worst kind of interference for any wide-band system in the locality;
- a very low data rate is impractical for many devices. For instance, with 100bps, a mere 12 bytes payload takes 1.2 seconds;
- the Sigfox deployed devices currently offer one way communication without acknowledgment. In order to achieve reliability in this scenario, redundant

transmission, that may prove to be inefficient for resource constrained device, is required;

- in order to operate on ultra-narrowband, it is necessary that devices are equipped with precise temperature compensated crystals with a subsequent higher cost than regular devices.

Table 2.2 – Specifications of Sigfox.

Specification/feature	**LoRa support**
Frequency range	Unlicensed 900 MHz
Data Rate	< 100 bps
Channel Bandwidth	< 100 Hz
Coverage	< 13 km
Energy need	Very Low
Battery Life	> 10 years

2.3 Smart Energy Management

Energy management in the current environment in which there is ever-increasing demand constitutes an issue with a significant profound economic, environmental, and social impact. Since homes and office buildings represent more than 70% of total grid electricity consumption today [63], particular attention has focused on 'smart grid' initiatives with the specific focus on the reduction or optimization of building energy consumption. There are multiple challenges involved in the design of energy-aware smart homes and a model-based approach has been proposed to tackles these challenges. Smart buildings use demand-side energy management to in order to self-regulate their energy footprint to obtain a reduction in overall energy consumption and peak power usage, while better aligning consumption with renewable generation [64]. Demand-side management requires buildings to

- continuously monitor the power consumption of electrical loads;
- remotely control when and how much power each load consumes, e.g., to enable automated demand response.

Although load monitoring and control are closely connected in demand-side management, two distinct sets of technologies have evolved to execute these smart home tasks. On the monitoring front, numerous techniques have been developed by researchers to enable finegrain tracking of electric usage at different spatial and temporal dimensions, e.g., [65, 66, 67, 68, 69]. Numerous past efforts have focused on outlet-level monitoring and, in some cases control, of electric loads using wireless technologies, such as 802.15. These technologies continue to be costly for typical homes, which can contain several tens to hundreds of power outlets. For instance, , Acme meter components cost $85 plus time for assembly and calibration although they are not commercially available [70, 71]; instead, Tweet-a-watt components cost $60 per meter plus time for assembly [72]. Similarly, the commercial PloggSE plug meter costs $215 per outlet [73]. Other issues include maintenance, communication interference, and aesthetic concerns when high numbers of meters are deployed [74]. A more economical option is that of deploying a single sensor at a home's electric panel for the monitoring of aggregate usage, and the using of NILM or load tracking techniques to disaggregate individual loads. However, on its own, this approach is insufficient for the development of such techniques given that it does not possess the capacity for ground-truth data which is necessary for evaluation. High-quality dataset collection has been the focus of interest for many researchers in sustainability [75, 76, 77] and can be considered as representative of another goal of smart home deployments. On the control front, Home Automation (HA) protocols, such as X10 and Insteon [78, 79], were designed explicitly for remote load control. The protocols enable programmatic actuation of outlets and switches that are hard-wired into a building and which are controlled from a central server, via command-line or remote web/smartphone interfaces, using the building's powerlines for communication. HA protocols are considered as mature standards: X10 was introduced in 1975 and Insteon in 2005. Many of these protocols communicate over building power-lines, which has been proposed as a path towards smart buildings [80]. Increasingly, it is possible to combine monitoring and control capabilities via 'smart outlets' such as the Belkin WeMo Insight Switch [81], which integrates both sensing and actuation capabilities into a single outlet-like device.. The use of HA devices for outlet- and switch-level energy monitoring adds to our proposed smart home architecture, which is based around a whole-house smart meter and low-power controller for the performance of local data processing. Notably, in contrast to HA protocols, many previous efforts have focused on outlet- and switch-level energy monitoring using wireless technologies, such as Z-Wave, ZigBee, and Wi-Fi. Wi-Fi is particularly attractive due to existing Wi-Fi networks and relatively high bandwidth for fine-grained monitoring. However, since outlet and switch boxes are embedded in walls and can be behind large appliances, wireless communication often presents interference that severely degrades both its performance and reliability. One of the key challenges in IoT is how to interconnect "things" in an interoperable way whilst considering energy constraints, in the awareness that communication is the most energy consuming task on devices. RF solutions for an extensive field of applications in the Internet of Things have been issued over the course of the last decade, led by a requirement of integration and low power consumption.

2.3.1 Low Power Communication

Different standardisation bodies have proposed several low power communication technologies. The most common ones are:

- **IEEE 802.15.4** has developed a low-cost, low-power consumption, low complexity, low to medium range communication standard at the link and the physical layers [82] for devices that are resource constrained;
- **Bluetooth low energy** (Bluetooth LE [83]) is the ultra-low power version of Bluetooth technology [84] that is up to 15 times more efficient than Bluetooth;
- **Ultra-Wide Bandwidth (UWB)** Technology [84] is an emerging technology in the domain of IoT that transmits signals across a much larger frequency range than conventional systems. UWB, in addition to its communication capabilities, can allow for high precision ranging of devices in IoT applications;
- **ISO 18000–7 DASH7 standard** developed by DASH7 Alliance is a low power, low complexity, radio protocol for all sub 1GHz radio devices. It is a non-proprietary technology based on an open standard, and the solutions may contain a pool of companion technologies each operating in their own way. All these technologies share their use of a Sub 1 GHz silicon radio (433 MHz) as their primary communicating device [85]. The applications using DASH7 include supply chain management, inventory/yard management, manufacturing and warehouse optimization, hazardous material monitoring, smart meter and commercial green building development;
- **RFID/NFC** proposes a variety of standards to offer contactless solutions. Proximity cards can only be read from less than 10 cm and follow the ISO 14443 standard [86]; it also constitutes the basis of the NFC standard. RFID tags or vicinity tags dedicated to identification of objects have a reading distance which can reach a distance of 7 to 8 meters.

Nevertheless, front-end architectures have stayed traditional and there is currently a need for innovation. Regarding the ultra-low consumption target, super-regenerative architectures have proven to be very energetically efficient and they are used for wake-up receivers. It is permanently active with very low power consumption, and can trigger a signal to wake up a complete/standard receiver [87, 88]. Standardization is required in this field, as currently only proprietary solutions exist, for an actual gain in the overall market to be significant. On the other hand, power consumption reduction of an RF full-receiver can be envisioned, with a target well below 5mW to enable very small form factor and long life-time battery. Indeed, targeting below 1mW would consequently enable support from energy harvesting systems thus enabling energy autonomous RF communications. In addition to this improvement, lighter communication protocols should also be considered as the frequent synchronization requirement makes frequent activation of the RF link mandatory, thereby overhead in the power consumption. It is also necessary to consider that recent advances in the field of CMOS technology beyond 90 nm, even 65 nm nodes, leads to new paradigms in the RF communication field . Applications requiring RF connectivity are growing as rapidly as the Internet of Things, and it is currently economically viable to propose this connectivity solution as a feature of a wider solution. This is already the case for the micro-controller in which a ZigBee or Bluetooth RF link can now easily be embedded, and this will expand to meet other large volume applications sensors. Progressively, portable RF architectures are facilitating the addition of an RF feature to existing devices. This will lead to RF significantly exploiting digital blocks and limiting analogue ones, like passive / inductor silicon consuming elements, as these are rarely easy to port from one technology to another. Nevertheless, the same performance will be required so receiver architectures must efficiently digitalize the signal in the receiver or transmitter chain [89]. In this direction, Band-Pass Sampling solutions are promising as the signal is quantized at a much lower frequency than the Nyquist one, related to deep under-sampling ratio [90]. Consequently, consumption is therefore greatly reduced compared to more traditional early-stage sampling processes, with a much lower sampling frequency. Continuous-Time quantization has also been regarded as a high-integration and easy portability solution. It is also an early-stage quantization, but without sampling [91]. Thus, there is no added consumption due to the clock, only a signal level which is considered. These two solutions are clear evolutions which can pave the way to further digital and portable RF solutions. It is not expected that cable-powered devices will be a viable option for IoT devices as they are both complex and expensive to deploy. In many IoT deployment scenarios, device battery replacements can be either impractical or extremely expensive. Consequently, for large scale and autonomous IoT, alternative energy sourcing using ambient energy ought to be considered. The radio transceiver is one of the most power/consuming components on typical IoT platforms. Idle listening is as expensive as receiving packets. For energy to be saved, he radio transceiver must be switched completely off for most of the time. Numerous types of Internet of Things devices will always be connected to the energy grid; whereas, on the other hand a significant subset of Internet of Things devices will need to depend on their own limited energy resources or energy harvesting throughout their lifetime. Given this range of possible implementations and the expected importance of minimum-energy Internet of Things devices and applications, an important topic of research could be the search for minimum energy, minimum computation, slim and lightweight solutions through all Internet of Things communication and applications layers.

2.3.2 Energy Harvesting

Mechanical energy, thermal energy, radiant energy and chemical energy are the four main ambient energy sources that can be present in an environment. The power consumption can vary depending on the communication protocols and data rate used to transmit the date. The approximate power consumption for different protocols is as follows: 3G-384kbps-2W, GPRS-24kbps-1W, Wi-Fi-10Mbps-32–200mW, Bluetooth-1Mbps-2.5–100 mW, and Zigbee-250kbps-1mW. Ambient light, thermal gradients, vibration/motion or electromagnetic radiation can be harvested to power electronic devices. The major components of an autonomous wireless sensor are the energy harvesting transducer, energy processing, sensor, microcontroller and the wireless radio. There are three key areas in the energy processing stage that must be addressed for successful energy harvesting implementations, namely: energy conversion, energy storage, and power management. Harvesting 100 µW over 1 year corresponds to a total amount of energy equivalent to 1 g of lithium. Considering this approach of examining energy consumption for one measurement instead of average power consumption, it results that, today:

- sending 100 bits of data consumes about 5 µJ;
- measuring acceleration consumes about 50 µJ;
- making a complete measurement: measure + conversion + emission consumes 250–500 µJ. Therefore, with 100 µW harvested continuously, a complete measurement can be performed every 1–10 seconds. This duty cycle can be sufficient for many applications. For other applications, basic functions' power consumptions are expected to be reduced by 10 to 100 within 10 years; which will enable continuous running mode of EH-powered IoT devices.

Despite the developments of the last 10 years, energy harvesting (except PV cells) remains an emerging technology that has not yet been adopted by industry. Nevertheless, further improvements of present technologies should enable the meeting of IoT needs.

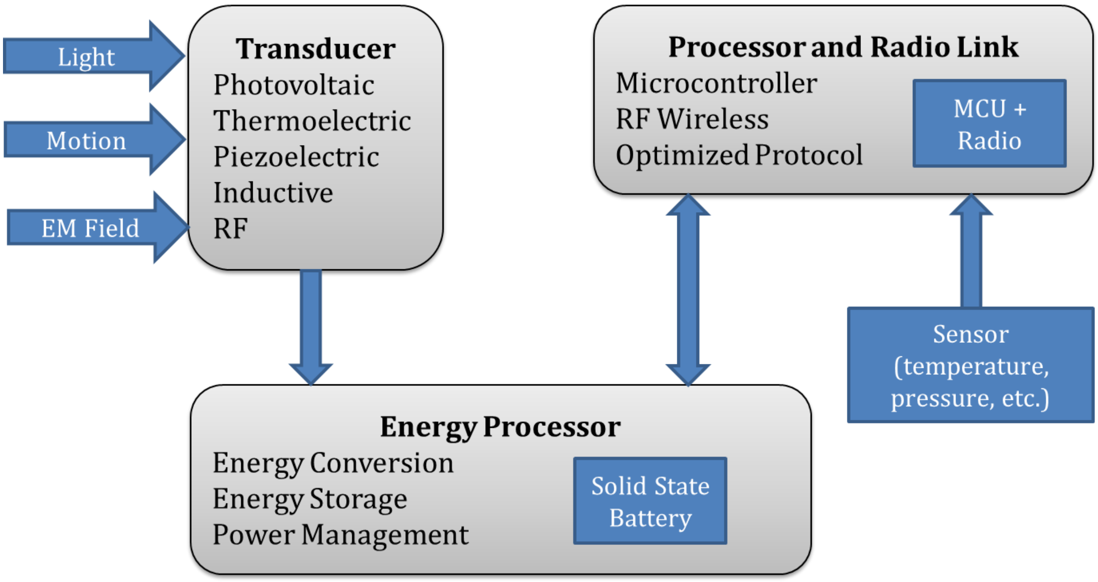
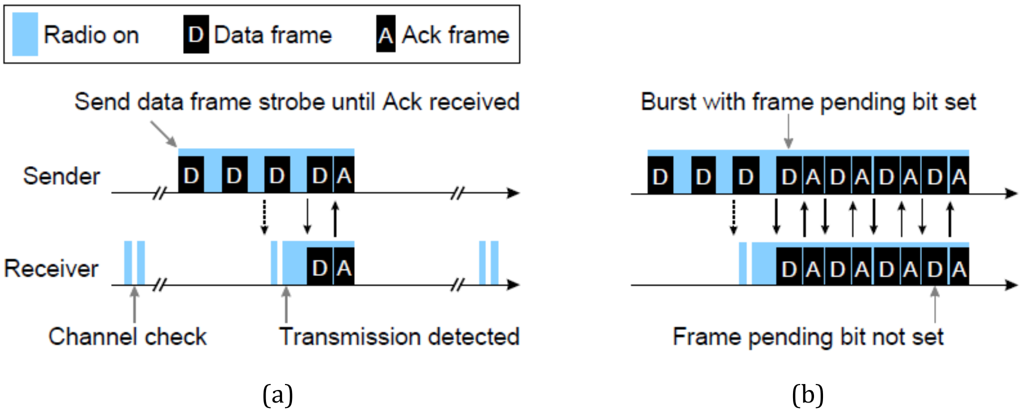


Figure 2.5 - Energy harvesting and components of an autonomous wireless sensor

An example of interoperable wireless standard that allows switches, gateways and sensors produced by different manufacturers to combine seamlessly and wireless communicates with all major wired bus systems such as KNX, LON, BACnet or TCP/IP is presented in [92]. The development of energy harvesting and storage devices is key in the realization of the ubiquitous connectivity that the IoT proclaims and the potential market for portable energy storage and energy harvesting could lie in distributed smart swarms of mobile systems for the Internet of Things. The energy harvesting wireless sensor solution can generate a signal from an extremely small amount of energy. From just 50 μWs a standard energy harvesting wireless module can easily transmit a signal over a distance of 300 meters in a free field.

2.3.3 Sleepy nodes and radio duty cycling (RDC)

The extended sleep mode mechanism often called ‘sleepy nodes’ has been the object of industry focus. The sleep periods can range between seconds and weeks and are completely controlled by the application layer. The business logic (i.e., the code that implements the actual functionality on top of the operating system (OS) and protocols) is able to define suitable moments to go into sleep mode (e.g., after data was uploaded to the cloud) and at which events to wake up (e.g., a sensor stimulus). This strategy is of particular use for communications other than IEEE 802.15.4 such as Wi-Fi or cellular. Low-power Wi-Fi, for instance, is mainly based on long sleeping periods and short wake-up cycles [93]. Often devices must re-synchronize and perhaps even re-associate with the network. . For this, power save services to coordinate sleeping intervals are provided by IEEE 802.11v [94]. Since the devices are unavailable during sleep mode, the business logic placed under a burden in order to maintain connectivity and continuous operation. Furthermore, it is hard to create a response infrastructure that can be inquired and re-configured at any time. In contrast, radio duty cycling (RDC) strategies provide virtual always-on semantics that are transparent for the application [95, 96, 97, 98, 99]. Several RDC algorithms have been designed that allow nodes to keep the radio chip off for more than 99% of the time while still being able to send and receive messages [96, 97]. For instance, the ContikiMAC RDC protocol [100] is a low-power listening MAC protocol that employs an efficient wake-up mechanism to attain a high power efficiency: with a wake-up frequency of 8 Hz, the idle radio duty cycle is only 0.6%. Figure 2.6 shows its operation principle. Nodes periodically wake up to check the radio channel for a transmission from a neighbour. If a radio signal is sensed, the node keeps the radio on to listen for the packet. If the frame is not addressed to the checking node, it goes back to sleep. When the data frame is correctly received the receiver sends an acknowledgment frame. To send a packet, the sender repeatedly sends the data frame in a so-called strobe until it receives an acknowledgment, or until the packet is sent for an entire channel-check interval without receiving an acknowledgment. This can be optimized by storing the wake-up times for each neighbour. The so-called phase lock starts the strobe just prior to the receiver awakening and minimizes the active transmit time, which also reduces channel utilization. ContikiMAC can easily be combined with link-layer bursts. When a sender has several frames to send, it first wakes up its neighbours with a ContikiMAC strobe and sets the frame pending bit in the 802.15.4 frame header to inform the receiver that another frame will follow.



(a) (b)

Figure 2.6 - (a) ContikiMAC senders wake their neighbours up by sending a strobe of data frames until receiving an acknowledgment. Only the addressed node stays awake to receive the frame. (b) Link-layer bursts use the frame pending bit in the 802.15.4 frame structure to signal the receiver to keep the radio on.

2.3.4 Ultra-Low Power Efficiency

Since last-inch devices typically perform limited tasks, their architectures tend to be fairly simple architectures focusing on basic data collection, calculation and connectivity functionality. Whether such a device needs an 8-bit or 32-bit microcontroller (MUC) is primarily dependent on the types of calculations to be performed by the device The wider bus and advanced peripherals of 32-bit MCUs also enable substantially faster data movement and computational power than 8-bit MCUs, thus devices can return to sleep faster for better power efficiency. For many last-inch applications, such as motion and light sensors placed throughout a house, the cost of the installation of new wiring to power these devices is prohibitive when compared to the cost of the device and the function it is to perform. Consequently, these devices must offer superior power efficiency so they can operate using a battery or by harvesting energy from their environment. In addition, these devices must be easy to install, even in difficult-to-reach spaces, and they must also be able to operate for years without requiring battery replacement or other servicing. MCUs need to support ultra-low power operation while enabling ubiquitous control and connectivity. To achieve this exceptional power efficiency, A variety of advanced capabilities must be integrated by MCUs. For instance, an on-chip, high-efficiency dc-dc buck converter can enable higher efficiency while allowing devices to operate all the way down to the lowest usable voltage of the batteries. A 32-bit microcontroller with an integrated dc-dc buck converter, such as Silicon Labs' 32-bit SiM3L1xx Precision32™ device, can achieve an active mode power that is 40 percent lower compared to a similar microcontroller without a buck converter, as shown in Figure 2.7 [101].

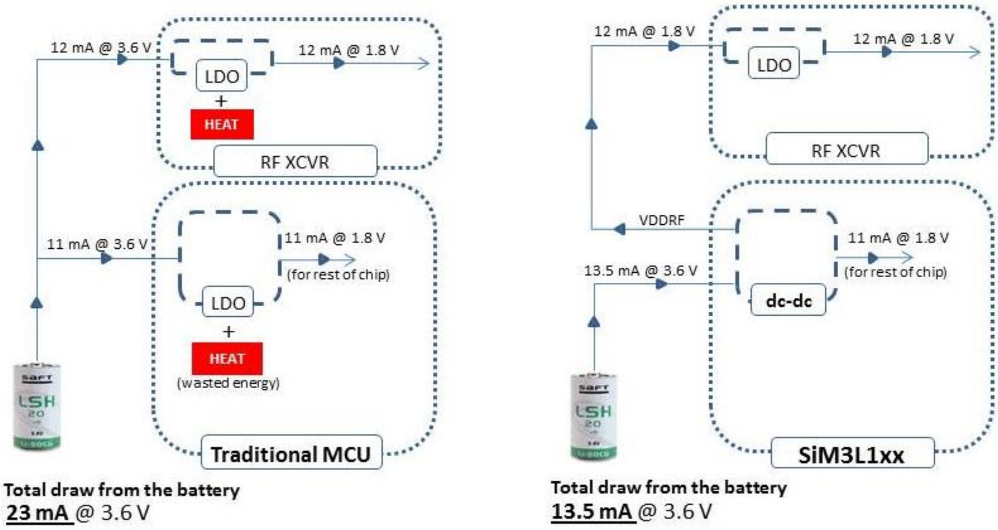


Figure 2.7 - An Integrated DC-DC buck converter that can reduce active power by up to 40%.

Ideally, MCUs used in devices at the edge of the IoT support multiple power domains, which enable peripherals to operate autonomously at different frequencies with the CPU powered down. For example, direct memory access (DMA) can be used to collect sensor data and wake the CPU only when there is a full buffer of data to process. This results in a greater sleep-to-wake ratio and higher power efficiency. These architectures are also highly specialized to transition in and out of standby more rapidly to reduce the power wasted while the CPU wakes. Silicon Labs' SiM3L1xx 32-bit microcontroller family, for example, features a dedicated, programmable Data Transfer Manager (DTM) hardware block that allows the embedded designer to fix together a complex set of tasks that execute autonomously without relying on the MCU core. In these instances, the core is maintained in its lowest power state until all the tasks have completed. The DTM is especially useful in wireless data transfers. In wireless systems, for example, raw data is processed through multiple operations prior to being delivered to the radio for transmission. The microcontroller must encrypt the raw data, add error correction, encode the packet and pass the packet to a serial interface in one or more bursts, such a process is shown Figure 2.8.

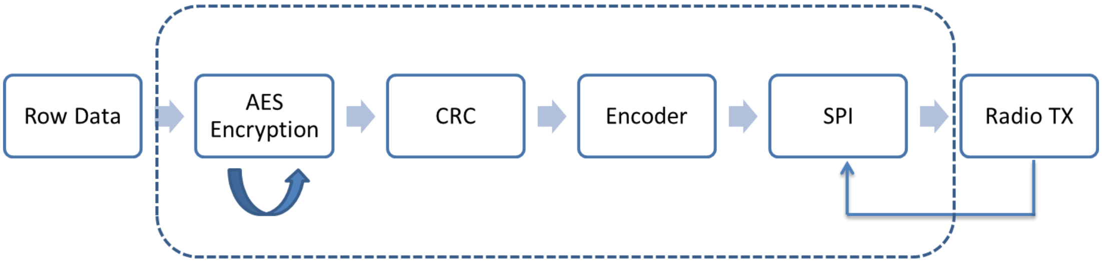


Figure 2.8 - Silicon Labs' data transfer manager that enables autonomous data transfers of radio

Application-specific circuitry can further offload the CPU. For example, an on-chip pulse counter for utility meters is able to efficiently measure pulse trains or fluid flow as a background operation while integrated capacitive touch-sensing capabilities are able to reduce active time power consumption for devices with a UI. The availability of hardware-based accelerators that speed processing and decrease active current, such as dedicated packet processing engines (DPPEs), can significantly improve RF message processing while allowing the CPU to remain idle during transactions.

CHAPTER 3

SMART HOME & SMART BUILDING

Within their homes, humans usually interact with environment settings like light, air, etc., and regulate them accordingly. If it is possible to make environment settings respond to human behaviour, there may be several advantages. The automation of home settings so that they act in accordance with the requirements of inhabitants is referred to as an intelligent home automation system. Ambient intelligence [9] responds to inhabitant behaviours in domestic settings and provides them with various facilities [35]. In computing, *Ambient Intelligence (AmI)* refers to electronic environments that are both sensitive and responsive to the presence of people. Ambient intelligence constitutes a future vision of consumer electronics, telecommunications and computing that originally developed in the late 1990s with reference to the 2010-2020 time frame. In an ambient intelligence world, people are supported in executing their daily life activities, tasks and rituals in a natural manner using both information and intelligence hidden in the network connecting devices that work together to support people. As these devices become smaller, , more connected and more integrated into our environment, the technology progressively disappears into our surroundings until only the user interface is perceived by users. The ambient intelligence paradigm builds upon several elements including pervasive computing, ubiquitous computing, profiling, context awareness, and human-centric computer interaction design; it is characterized by systems and technologies that are:

- **embedded**: the environment integrates many networked devices
- **context aware**: the user and situational context can be recognised by these devices
- **personalized**: they can be tailored to the user’s needs

---

[9] In computing, Ambient Intelligence (AmI) refers to electronic environments that are sensitive and responsive to the presence of people.

- **adaptive**: they can change in response to the user
- **anticipatory**: they can anticipate the user's desires without conscious mediation.

A typical ambient intelligence environment context is a Home environment. In general, an intelligent home automation system consists of a cluster of sensors, which collect different data types relating to the occupiers and domestic utility consumption. Systems with computing capabilities analyse the gathered data in order to recognize the activities of inhabitants or events. They can effectively automate domestic utilizations and can also support the inhabitant through cost reduction and living standard improvement. Recently, several research activities have actively studied the IoT such as [36, 37, 38]. However, to date, most of the research activities on the IoT are limited to the management of resource constraint devices [39], and different interconnection mechanisms [40, 41]. In the future, it is likely that cyber-age networked infrastructures of domestic household appliances will be reliant on sensors embedded in/on the infrastructure. Such technologies will act as a catalyst in the evolution of a new generation services that will significantly impact both the social and technological eco-system. According to [35], it is possible to consider that next generation systems and services will encompass several domains such as e-Governance, Health Care, Transportation, Waste Management, Food Supply Chains, and Energy & Utilities. New technologies and applications built on top of smart devices may fulfil the vision of Intelligent Infrastructure. There are numerous examples of intelligent home automation or “Smart Home Monitoring” in research labs around the world, such as the GatorTech Smart House [42], Casas Smart Home [43], iDorm [44], Georgia Tech Aware Home [45], and Place Lab [46], etc. Yet, to date, a complete development of a monitoring smart home from a commercial perspective is lacking, nor have there been any investigation into how such a house is perceived either by the inhabitants or their carers. The smart homes designed so far serve different purposes namely information collection and decision support system for inhabitant wellbeing [47, 48], multimedia data storage and retrieval [48] and surveillance, where the data is captured from the environment and processed to obtain information that can be used to raise the alarm to protect the home and safeguard its inhabitants from burglaries, theft and natural disasters [48]. In order to obtain low-power However, it has limitations on network and application layer functionalities such as addressing, routing and interoperability with the Internet. Alternatively, adapting to IPv6 Low Power Personal Area Network (6LoWPAN) protocol, allows the obtainment of better end-to-end communication with sensing devices. However, translation mechanisms such as SOAP/REST, GRIP [49] will increase the complexity of the network system. The concurrent impact of wireless sensor networks on IEEE 802.15.4 devices was assessed in [50]. Studies in [51] have theoretically proven that WSN performance is more susceptible to reduction when interference with other radio networks and likelihood of faults in the 802.15.4 network is high. In [52], the authors have studied the coexistence of IEEE 802.15.4 and other radio networks, based on outage probability, packet loss rate and changes in RSSI value. Research for internetworking 802.15.4 with IP networks has been conducted. 6LowPAN [53] provides a well-defined method for transferring IPv6 packets over an 802.15.4 network. However, deployment complexity in 802.15.4 network nodes is very challenging [54]. IPv6 over 6LoWPAN is proposed by the Internet Engineering Task Force (IETF) working group to accomplish the concept of IP-based WSN. A new layer is incorporated between the IPv6 network layer and the 802.15.4 MAC layer, which is an entitled adaptation layer. It was observed that the adaptation layer, specifically the fragmentation process, may increase the energy consumption of a sensor node by 5 to 10 percent [55]. As mentioned above, there are numerous issues related to integrating IPv6 with the WSN. The advantages of interconnecting WSN with IoT model is for remote monitoring of a contextual environment, in which heterogeneous data can work together and provide collective facilities. According to an internetworking perception, a WSN can be fully integrated into the IoT by the type of integration approach used for both the infrastructures.

3.1 Components and modules

It is possible to classify Smart Home components into five components. There are five discrete units of a Smart House, we will consider them as a single unit and more focusing will be placed on their application.

- **Sensors**: are the most vital integral unit of a smart home. Sensors monitor and submit messages in case of changes. A variety of sensors can be used for the monitoring of specific data which are discussed in detail in the successive chapters;
- **Actuators**: perform physical actions; automatic light switches and relays are examples of actuators. Environmental control system components are mostly actuators;
- **Controllers**: make choices on the basis of programmed rules and occurrences. Controllers are microprocessors which are often built- in with sensors and actuators. Values from the sensor or other controllers are received and processed;
- **Central Unit**: it acts as a data repository of all the vital information from the various types of sensors. This central unit can also be used;
- **Communication Modules**: they facilitate the information flow in and out of a Smart Home. The communication module is totally dependent on the communication technology type used for the specific purpose.

Sensors are electronic devices which measure a physical quantity such as temperature, pressure or loudness; they convert it into an electronic signal of some kind. Smart Sensors, which are the topic of interest, are, instead, sensors which provide additional functions beyond those necessary for generating a correct representation of the sensed quantity. A variety of Smart Home applications use sensors and they constitute their backbone structure. The key purpose of a sensor is to collect data or measure a variable. The applications of sensors used in Smart Homes in this thesis can be classified mainly into three types:

- sensors in relation to the subjects (the occupants of the house are referred to as subjects);
- sensors in relation to the environment;
- hybrid sensors that are inter-related to both the environment and the subjects.

3.2 Layers and services

Home automation is computerization of the home, housework or household action. Home automation may incorporate a control unit for the control of lighting, HVAC (warming, ventilation and aerating and cooling), machines, and different frameworks, to deliver enhanced accommodation, solace, better energy saving, productivity and security. The concept of home automation has existed for some time and items have been available for a considerable number of years; however, not one arrangement has yet arrived at the standard. Home computerization for the elderly and debilitated has the potential to provide extended personal satisfaction to people who may generally need parental figures or institutional consideration. It can also provide a remote interface to home apparatuses or the automation system itself, through a phone line, remote transmission or the web, to give control and allow observation and monitoring with either a smart phone or a web explorer program. [56].

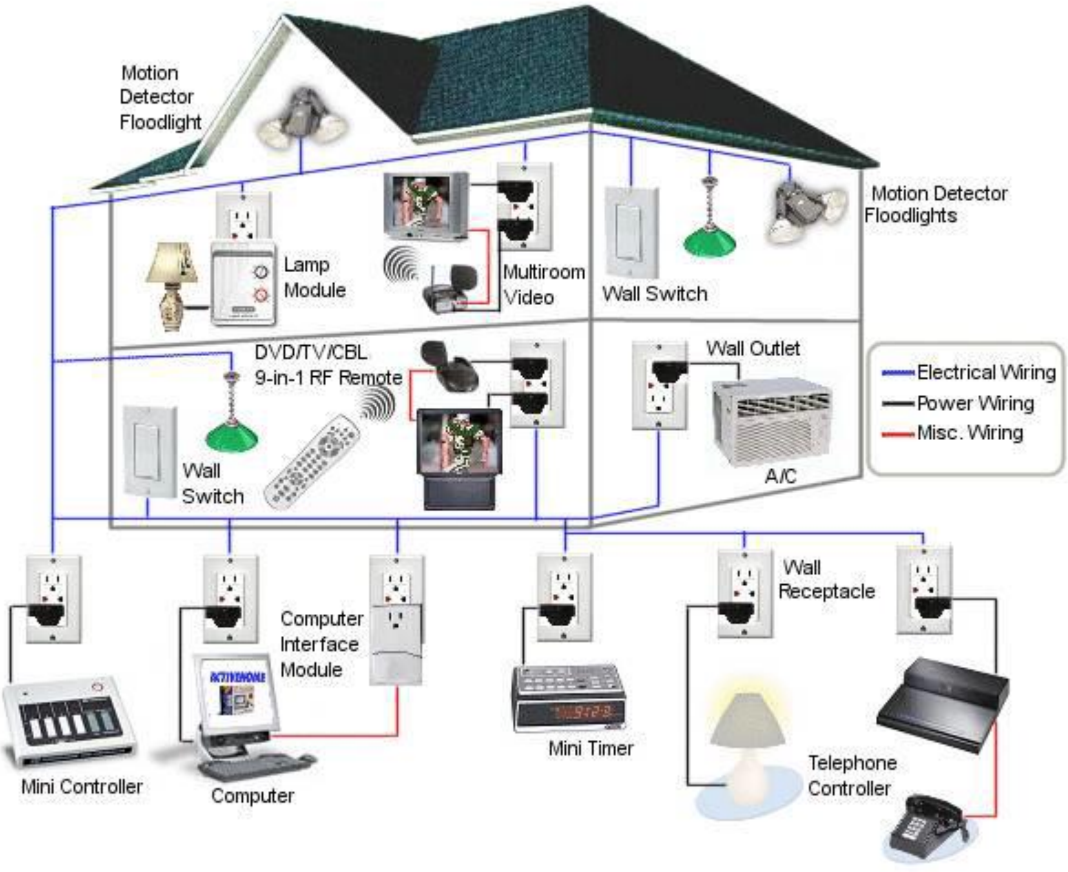


Figure 3.1 - Home Automation System.

The rise of the role of Wi-Fi in home automation has primarily occurred due to the networked nature of deployed electronics where electronic devices (TVs and AV receivers, mobile devices, etc.) have started to become part of the home IP network and also due the increasing adoption rate of mobile computing devices (smartphones, tablets, etc.). Several organizations are working on equipping homes with technology enabling the occupants to use a single device to control all electronic devices and appliances. The focus of the solutions is primarily on environmental monitoring, energy management, assisted living, comfort, and convenience. The solutions are based on open platforms that use an intelligent sensor network to provide information about the state of the home. These sensors monitor a variety of systems such as energy generation and metering; heating, ventilation, and air conditioning (HVAC); lighting; security; and environmental key performance indicators. A number of access methods such as touch screens, mobile phones and 3–D browsers [57] process and render information available.

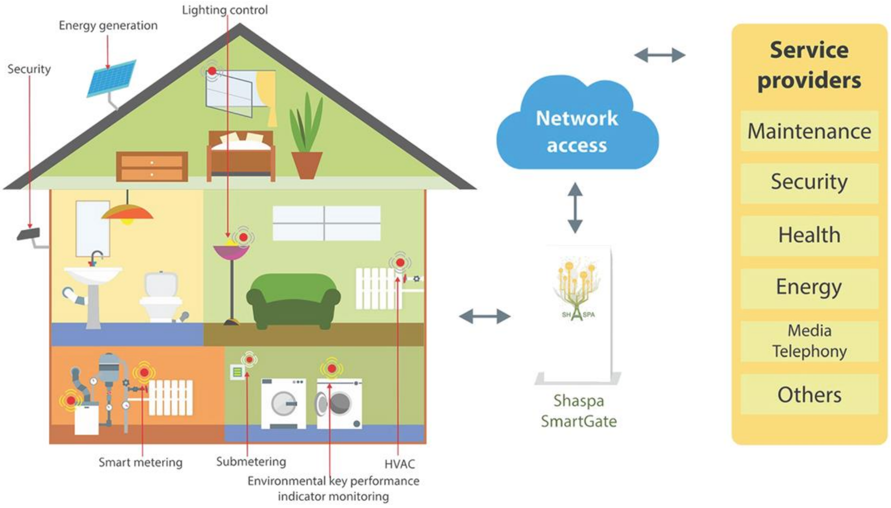


Figure 3.2 - Integrated equipment and appliances [58].

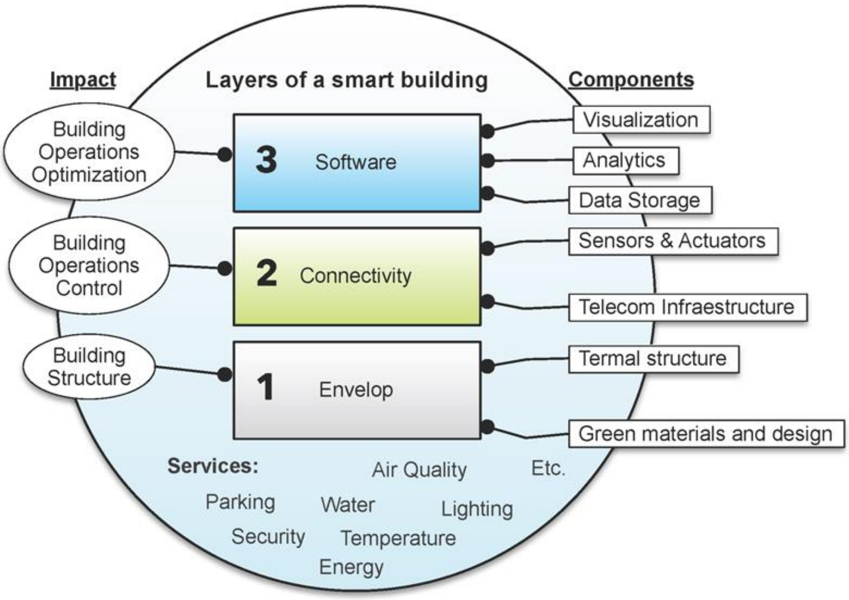


Figure 3.3 - Smart Buildings Layers [59].

The networking aspects consist of providing online streaming services or network playback, while becoming a means of control of the device functionality over the network. Contemporaneously, mobile devices ensure that consumers can access a portable 'controller' for the network connected electronics. Both types of devices can be used as gateways for IoT applications. In this context, many companies are currently considering building platforms that integrate building automation with entertainment, healthcare monitoring, energy monitoring and wireless sensor monitoring in both home and building environments. IoT applications using sensors for the collection of information regarding operating conditions combined with cloud hosted analytics software that analyse disparate data points can help facility managers to become significantly more proactive in the management of buildings at peak efficiency. From a technological viewpoint, we can identify the different layers of a smart building in more detail, to better understand the correlation of the systems, services, and management operations. For each layer, it is essential to understand the implied actors, stakeholders and best practices in order to implement different technological solutions [59]. Issues of building ownership (i.e., building owner, manager, or occupants) present a challenge for integration with issues regarding as who is responsible for covering the initial system cost and who collects the benefits over time. Poor collaboration between the different subsectors of the building industry hampers the adoption of new technology and can even prevent new buildings from meeting energy, economic and environmental performance targets. From the layers of a smart building there are many integrated services that can be seen as subsystems. The set of services are managed to create the best conditions for building occupant activities. The figure below presents basic services taxonomy. The integration of cyber physical systems both within the building and with external entities, such as the electrical grid, necessitates stakeholder cooperation in order to achieve true interoperability. As in all sectors, security maintenance presents a critical challenge to be overcome [60].

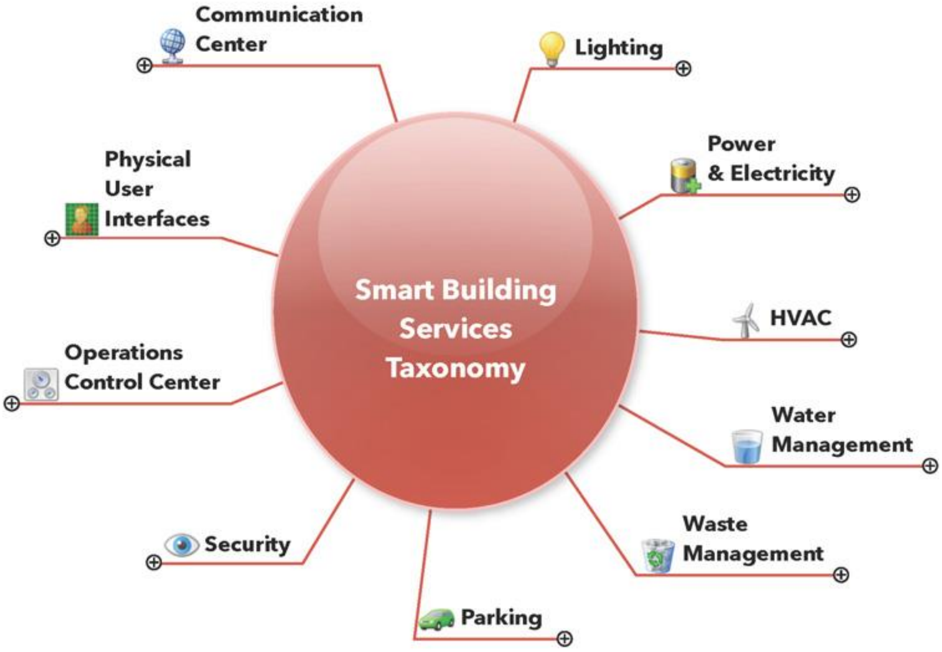


Figure 3.4 - Smart Building Services Taxonomy [59].

Within this field of research, the exploitation of the potential of *Wireless Sensor Networks (WSNs)* to facilitate intelligent energy management in buildings which, in turn, increases occupant comfort while reducing energy demand, is extremely relevant.

3.3 Internet of Buildings

Other positive effects will be achieved from the introduction of intelligent energy management in buildings in addition to the obvious economic and environmental gains from its introduction.

Figure 3.5 - Internet of Buildings concept.

One of the most important positive effects is building control; the placement of monitoring, information feedback equipment and control capabilities in a single location will lead to the buildings' energy management system being easier to handle for several users, including building owners, building managers, maintenance crews and other users of the building.

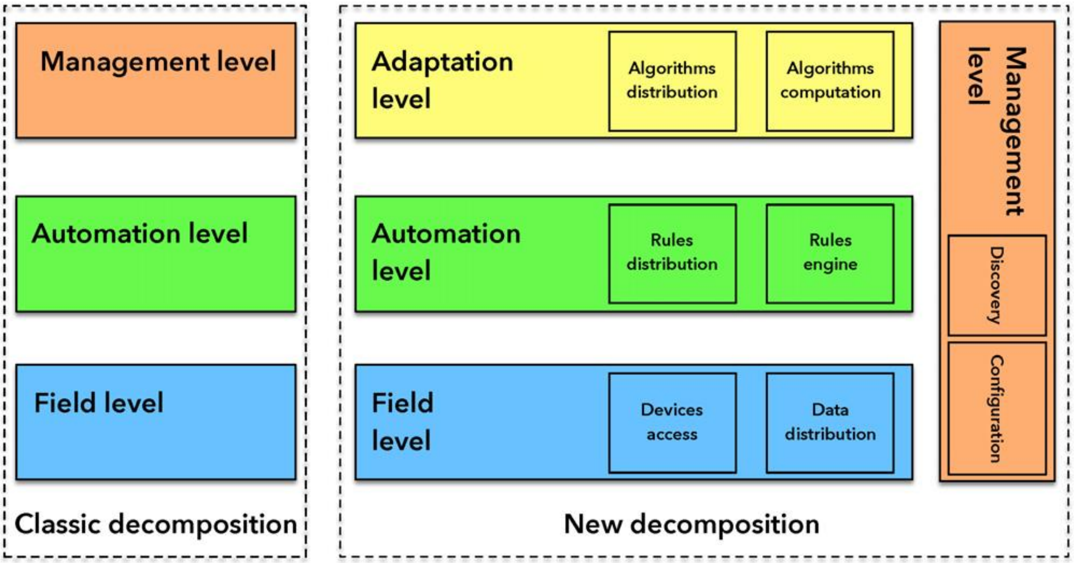


Figure 3.6 – Level-based architecture of building automation systems [46].

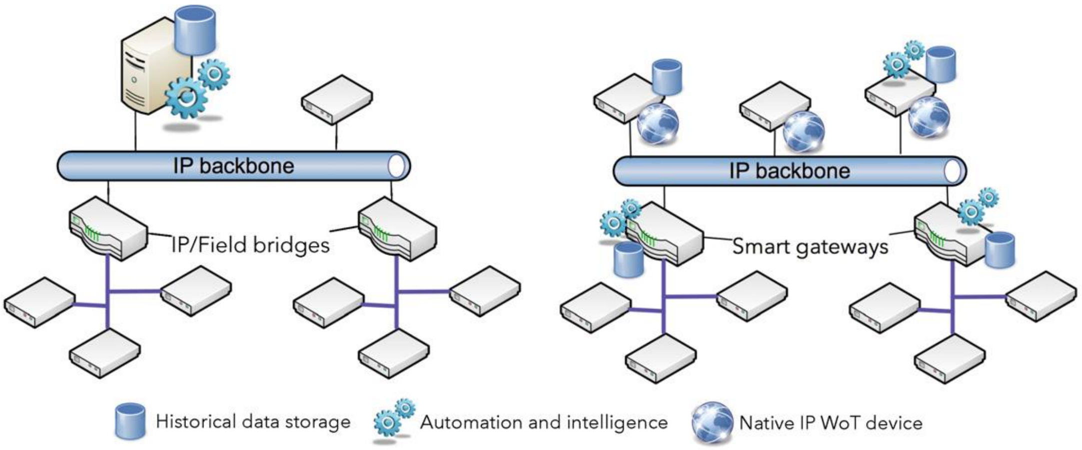


Figure 3.7 - Role distribution for a classical building automation system and for a Web-of-Things architecture [61].

Using the Internet alongside energy management systems also offers an opportunity to access a buildings' energy information and control systems from a laptop or a Smartphone located anywhere in the world. This has an impressive potential to provide building managers, owners and residents with energy consumption feedback and the ability to act on that information. The perceived evolution of building system architectures includes an adaptation level that will dynamically feed the automation level with control logic, i.e. rules. Furthermore, in the IoT approach, the management level must be made transversally available as configuration, discovery and monitoring services must be made accessible to all levels. It is also necessary to consider algorithms and rules as Web resources in a similar way as for sensors and actuators. The repartition of roles for a classical building automation system to the new web of things enabled architecture differs and in this context, it will be necessary to execute future works with the aim of identifying solutions which will minimize the transfer of data and the distribution of algorithms [61]. In the context of the future 'Internet of Things', we may consider Intelligent Building Management Systems part of a much larger information system. This system is used by building facilities managers to manage both energy use and energy procurement as well as to maintain buildings systems. It is based on the infrastructure of existing Intranets and the Internet, and it, therefore, utilises the same standards as other IT devices. Reductions in the costs and reliability of WSNs in this context are transforming building automation, by rendering energy maintenance of energy efficient, healthy, productive work spaces in buildings increasingly cost effective [62].

3.4 Web of Things

Building upon the notion of the IoT, the Web of Things (WoT) has recently been proposed [26, 27], promising to seamlessly interconnect devices and their functionalities. The WoT reuses well accepted and understood Web principles to interconnect the expanding ecosystem of embedded devices. While the IoT focuses on interconnecting heterogeneous devices at the network layer, the WoT can be considered as a promising practice to achieve interoperability at the application layer. It consists of taking the Web as it is currently known and extending it so that anyone can plug devices into it. The WoT follows the concept of resource-oriented architectures and *REpresentational State Transfer* (REST) [28, 29], proposing the use of uniform patterns, influenced by the HTTP protocol, for the management of and communication with pervasive smart home devices. REST is an architectural style that defines how HTTP should be properly used as an application protocol. While this may provide enhanced interoperability between heterogeneous devices and services, it is a commonly held belief that Web standards are inappropriate for building pervasive applications. Furthermore, many issues arise in enabling the devices in a dynamic, plug and play way to the Web. Issues such as local device discovery, service description, uniform and transparent interaction with embedded devices, service sharing, notifications in event-based scenarios etc. must be effectively and efficiently addressed. Finally, Web-enabled smart homes will play a crucial role in current and future technological and societal challenges. Energy awareness of home inhabitants, energy saving through advanced automation and social approaches, the forth-coming integration of smart homes to the smart grid of electricity, and even the contribution of smart homes towards the digitization of the urban environment are just some examples of the many challenges encountered by both smart homes and their residents. This key role of smart homes in relation to the physical and urban environment is deserving of investigation, highlighting and promotion. Technologies, protocols and architectures must be defined, which permit the smooth and flexible adaptation of smart home solutions to meet these challenges, ensuring satisfactory security and user privacy levels. It will be necessary to develop numerous case studies need to illustrate the abovementioned benefits and consequently encourage the adoption of Web technologies in smart homes. Given the above, the main research challenges encountered in this PhD thesis, for which solutions will be sought, are:

- of Smart Home solutions and technologies hardware and software heterogeneity, as well as incompatible, vendor-specific approaches for home automation;
- support from multiple family members who may interact concurrently with their smart home environment;
- failures concerning device unavailability and message transmission losses, which may occur in the unpredictable embedded home environment and consequently decrease smart home operations reliability;
- possible degradation of performance, caused by utilizing the IoT for interconnecting physical devices and their services, mainly due to the IP overhead of exchanged messages;
- performance in terms of response time, especially in scenarios involving domestic safety and health applications;
- energy consumption performance of embedded home devices, in particular when incorporating the IP stack;
- complicated, vendor-specific closed smart application development, that is not based on any standards nor well-known techniques;
- issues encountered during the process of dynamically enabling physical devices and their services to the Web;
- the role of smart homes in current and future technological and societal challenges and the flexible adaptation of smart homes to these challenges.

Extending the concept of the IoT, the Web of Things [26, 27] is a notion where everyday devices and sensors are connected by fully integrating them to the Web. Based on the success of the Web 2.0, this concept regards the reuse of well-accepted and understood Web standards to connect constrained devices. The WoT offers significant benefits in the ubiquitous computing society. It brings a new application development paradigm, where applications can be easily built on top of embedded devices, utilizing the same techniques that are used in Web development, such as Web mashups involving physical things. Furthermore, many features of the Web can by employed very easily. These features include searching, securing, blogging, caching, linking, bookmarking etc. Finally, the Web has been proven to be a highly scalable and ubiquitous platform, and, consequently, researchers believe it is appropriate for the interconnection of millions of embedded devices and everyday objects under uniform and interoperable interfaces. The WoT practice mainly follows steps:

1. Connect embedded devices to the Internet, through IPv4 or IPv6;
2. Embed Web servers on these devices;
3. Model the services, offered by these devices, in a resource-oriented way;
4. Expose these services as RESTful Web resources.

It is possible to perform the Web-enabling process in two ways, namely through the embedding of Web servers directly on physical devices (indicated way) or by employing gateways, which perform protocol translation, from the TCP/IP protocol to the dedicated protocol used by the physical device (e.g. Bluetooth, ZigBee). Gateways are used when the TCP/IP protocol stack cannot be integrated to embedded devices (e.g. RFID tags, QR codes). Smart meters and smart power outlets are not yet capable of supporting the direct embedding of Web servers on them, however, this is expected to change in the near future. Directly embedding Web servers on sensors is a recent development [30, 31]. Examples of embedded Web servers that can be integrated in resource-constrained devices are NanoHTTPD [32] and the Nokia mobile Web server [33]. The important properties of the WoT can be summarized as follows:

- it uses HTTP as an application protocol rather than as a transport protocol as in the world of Web Services [34];
- it exposes the synchronous functionality of smart objects through a REST interface and respects the blueprints of resource-oriented architectures;
- it provides the asynchronous functionality (i.e. events) of smart objects through the use of largely accepted Web syndication standards such as Atom or server-push Web mechanisms such as Comet.

Open research questions of the WoT include:

- local/global discovery of physical devices and services;

- complete description of these services using standardized languages and semantic techniques;
- uniform interaction with embedded devices using standard protocols;
- asynchronous, Web-based interaction with devices that sense the environment for sporadic events.

CHAPTER 4

ACHITECTURE AND SOLUTIONS PROPOSED

Great interaction between humans, environments and smart devices can be achieved with a home automation system. The enhancing of these interactions was one of the main goal of this thesis whose intent was to improve the classic concept of home automation system. The framework that was designed and developed can be used for several applications such as lighting, heating, conditioning or energy management. In particular, the proposed system can optimize energy consumptions by rising awareness in users that have full control of their house and the possibility to save money, reduce the impact of the energy consumption and meet the new "green" motto requirements. In this way, the overall system also aims to match the central concept of IoT. From this point of view, a complex automation system with smart devices makes a more efficient way to produce, follow and manage home automation policies possible. Following the spread of IoT, new plug-and-play and ready-to-use smart devices were designed and implemented as part of a complex automation system that offers a user-friendly web application and allows users to control and interact with different plans of their house in order to make life more comfortable and be aware of their energy consumptions. There has been a significant increase of home automation systems in recent years due to the spread of both smart phones and tablets that allow connectivity everywhere at any time. Furthermore, with the introduction of IoT and the design of uniquely identifiable objects and their virtual representations in an Internet-like structure, the research and implementation of home automation systems is becoming more popular [102] . Different household devices and home appliances such as lightings, air conditioners, home security and entertainment systems can be connected to the Internet and controlled remotely using smart phones or tablets. Home environments can also be continuously monitored to maintain a certain desired temperature or a certain consumed energy [103]. This can contribute to overall cost reduction and energy saving which is one of the key concerns today. Home Automation Systems can be seen as a subset of Building Automation Systems with particular focus on living spaces on an apartment or family house scale. The main purpose of this system is to make everyday life more comfortable, safe and energy-efficient.

4.1 System Architecture

The challenge was to build a scalable and reliable automation system equipped with some different and distributed plug-and-play and ready-to-use smart objects that are able to change the current environmental state according to user preferences and energy saving policies. Many of the functions and devices related to Smart Homes already exist, like motion detectors, sensitive air conditioners, automatic heating adjusters or automatic sunlight-sensitive blinds. The challenge was to enhance some of these functionalities by designing an inter-operable system with flexible interfaces that can be accessed by users from everywhere and anytime allowing them to always be aware of their energy consumes. Most of the currently available systems are proprietary products and this involves a series of constraints for end users such as long term support, maintainability, future development, system compatibility and cost. To go beyond these issues open source solutions were adopted. Moreover, to deal with devices, vendors, communication protocols and technology heterogeneity, scalability, extensibility, reliability, load concentration, simultaneous use, easy mutual data exchange between devices, lower development and maintenance costs and reusable services, a multi-layers *Service Oriented Architecture (SOA)* [104, 105] was adopted to separate the physical hardware devices from the application software and services. In particular, four layers were designed: Application Layer, Service Layer, Controlling Layer and Controlled Layer.

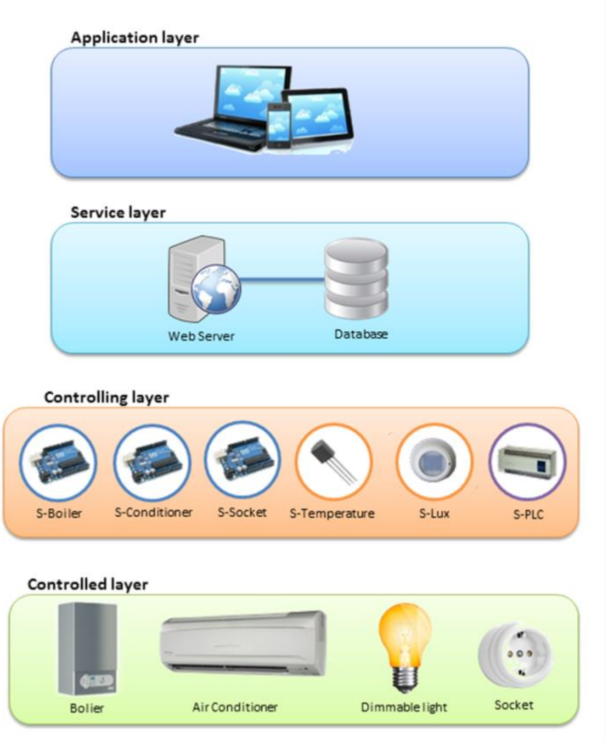


Figure 4.1 - Reference architecture proposed.

All the devices that can be controlled by higher level in order to change the current environmental state belong to the Controlled Layer. For testing purposes, the heating control, the lighting system and the power consumption were contemplated; therefore devices that were integrated in the environment are the boiler, the air conditioner, the dimmable light and the socket. Instead, the smart objects capable of observing and storing the current environmental state belong to the Controlling Layer. They are also the actuators of the commands coming from the higher level. For this layer three smart objects were designed using the open source single-board microcontroller called *Arduino* [106, 107] to control the boiler, the air conditioner and the socket. A *Programmable Logic Controller (PLC)* was integrated to control the lighting system. All devices must be connected to the Internet so smart devices are equipped with a Wi-Fi interface whereas the PLC is connected to the Internet through Ethernet. The Service Layer is both the brain and the heart of the system since it determines the functionality, the scalability, user-friendliness, stability, efficiency and, therefore, the success of automations. For this layer, a Java Web Server was implemented to communicate with other layers through HTTP protocol. This protocol provides an interaction mechanism between heterogeneous devices. The calling application does not know about the internal details of the service whereas the service does not know about the calling application. A database implemented with *MySql* in which are stored the current state of the controlled environments and all the commands that must be executed by the

Controlling Layer also belongs to this layer. An end-user application was implemented for the Application Layer that allows interaction with the system from everywhere at any time. In particular a Web Application (*HTML5* pages with *JavaScript* and *PHP*) for desktop devices (PC) or mobile devices (tablets and smartphones) was implemented.

4.1.1 Smart monitoring and controlling IoT devices

The following devices were designed and implemented for the Controlling Layer:

- **S-Boiler** for the house heating: it is directly connected to the boiler. It can turn the boiler on/off and set the desired temperature;
- **S-Conditioner** for the heating of one room: it can control any model of air conditioners through infrared signals by replicating the original signal from the remote controller;
- **S-Socket**: is directly plugged in to the socket and it is able to measure how much current is used by the load. It can also stop or allow the flow of the electrical current. The energy consumption detected is sent and computed by the Service Layer;
- **S-Temperature**: it can read the current temperature of the environment in which it is installed. This temperature is sent and computed by the Service Layer. The same temperature sensors are integrated in the S-Conditioner for indoor temperature detection, others in the S-conditioner for outdoor temperature detection since boilers are usually placed outside the house;
- **S-Lux**: it can detect the current light intensity of the environment in which it is installed. Some are placed inside the environment for indoor lux detection, others outside for outdoor lux detection. Lux measured are sent and computed by the Service Layer;
- **PLC:** this controller can turn on or off the lights and change the brightness of dimmable lights. It is remotely controlled through HTTP protocol.

4.1.2 Inter-layer communication

The application layer offers a graphic interface that, during the installation and configuration phase, allows users to create their own environments and connect one or more smart devices to Internet through a Wi-Fi interface. The environments and user profiles created are stored in the database of the Service Layer. Once the devices are connected to the local network, they start sending sensing data (temperature, lux, and energy consumption) and start asking the Service Layer for possible commands that must be executed. These commands are generated from users with the Web Application of the Application Layer according to their preferences about the state of the environment. Users can:

- turn on/off the devices;
- display the current temperature of the house;
- display indoor or outdoor lux;
- change the desired temperature;
- display the real time energy consumption;
- change the light intensity of dimmable lights;
- interrupt the flow of current from a socket that corresponds to the switch-off of an appliance such as the washing machine, the hair dryer or the oven.

The commands are stored to the Service Layer so that they can be taken from the Controlling Layer. Users are always aware if the commands have been executed through feedback/ack mechanism.

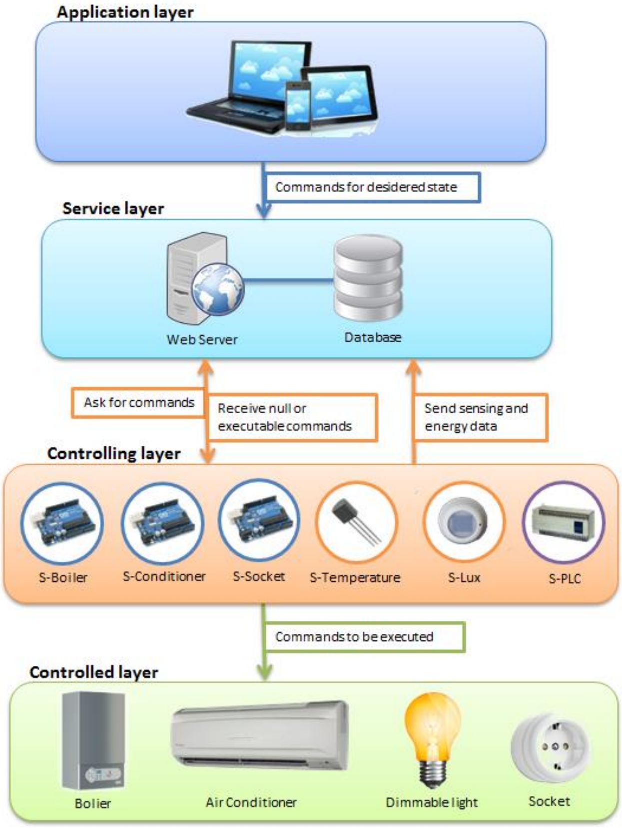


Figure 4.2 - Interlayer communication.

4.2 Speech recognition and semantic interpretation for smart actuations

Another important challenge was to enhance IoT with intelligence and awareness by exploring various interactions between human beings and the environment in which they live . To reach this goal, the core of the system was formed by an automation system, which is made up of a home automation control unit and several sensors installed in the environment. The task of the sensors is to collect information from the environment and to send it to the control unit. Once the information is collected, the core combines it in order to infer the most accurate human needs. The knowledge of human needs and the current environment status constitutes the inputs of the intelligence block whose main goal is to find the right automations to satisfy human needs in a real time way. The system also provides a Speech Recognition Service which allows users to interact with the system by their voice so human speech can be considered as additional input for smart automatisms. Speech recognition and semantic interpretation are both two key factors for *Ambient intelligence (Aml)*, an emerging discipline that brings intelligence to environments making them sensitive to people. This discipline has developed following the spread of sensors devices, sensor networks, pervasive computing and artificial intelligence. The term Ambient Intelligence was coined by the European Commission in 2001 and, in recent years, its intended goals have been adopted worldwide within research programs [108]. It refers to a system in which people are surrounded by distributed sensors and computational electronic devices embedded in common objects. These smart objects make the environment sensitive, adaptive and responsive to people [109], as they allow identification of and recognization of the actions, emotions, intentions, preferences and needs of the occupants. AmI also makes it possible to detect:

- **Who** are the actors of the environment by tracking and identifying processes;
- **Where** and **When** something happened by providing a time frame to a specific context;
- **What** is happening by recognizing activities interactions, time-space relations, linguistic and non-linguistic messages, signals, and signs;
- **Why** something is happened by associating actions, tasks and behaviour patterns with semantic meaning;
- **How** something is happening by tracing the information flow, recognizing expressions, movements and gestures.

The spread of AmI in domestic environments has been driven by the desire to reduce labour and improve the quality of time the spent at home. Today, this is one of the main reasons why AmI is also related to the home with the term *Smart Homes (SH)* which describes a system consisting of:

- **sensors**: they are the eyes and the ears of the system. They can measure a physical quantity and convert it into a signal which can be read and interpreted by the core of the system;
- **activators**: they can control the sensors;
- **computing facilities** to which the sensors and activators are linked.

Many researchers agree [109] that sensor information requires additional computational processing to produce useful data for the system, such as people location, the task the resident is trying to achieve or the behaviour patterns of the occupant. Much of the work on SH concentrates on hardware development (sensors and devices) even though several authors have argued that the evolution of SH can only be possible by bringing more complexity to the processing of information provided by devices and sensors. This processing can be enhanced for example through the learning of user profiles or by determining whether a deviation from routine is a matter of concern, on advising whether or not a rescheduling of normal activities is possible after a deviation or combining elements of temporal and probabilistic reasoning to provide a more powerful setting for monitoring and intervening. Others have argued that a rational and reactive agent architecture may be more appropriated for smart home applications as it can be designed for dynamic environments and it can be used to provide the required reasoning and adaptability.

According to the research conducted, it is possible to state that smart home applications and AmI require integration and development of different techniques, different kinds of devices for different kinds of purpose with very few constraints for end-users. These are the basics that have led to the development of the proposed system to meet human needs. The Service Layer was enhanced by introducing new inputs for the system and a sort of intelligence that allows the system to infer human needs in order to autonomously perform smart automatisms. Furthermore, a speech recognition service was developed that let the system understand the semantic meaning of the speech that is taking place in the environment. In this sense human participation was considered as sensor operator and data source. For the Controlling Layer a smart microphone was designed using the open source single-board microcontroller called *Arduino* [106, 107] that is able to detect and compute the speech of the occupants. To provide appropriate data and services able to satisfy human needs, the system must be aware of both the current environmental state and occupants needs in a machine understandable format. This led to the design of the following:

- a **Data Integrator** in the Service Layer whose task is to collect and combine different inputs in order to establish the most accurate automatism that can satisfy human needs;
- a **Semantic Interpreter** in the Service Layer that is able to transcribe an audio file and deduct its semantic meaning. The interpreter invokes an undocumented Google Web Service [110] to obtain a transcription from the speech which accepts audio data and returns a transcription through HTTPS protocol;
- A **Smart Microphone** in the Controlling Layer whose task is to detect speech from the environment and send it to the Service Layer. The microphone compresses the vocal signal in *Free Lossless Audio Codec (FLAC)* format [111], which works like MP3 but it is lossless, non-proprietary and it is open source and a reference implementation documentation is supplied as well. Furthermore, the microphone helps the Service Layer to understand if someone is in the environment.

The Semantic Interpreter requires an initialization phase in which different semantic domains must be defined with the use of key words. Different semantic domains correspond to different automatisms. Once the domains are set, when a transcription is received, the interpreter is able to determine if there is a univocal correspondence between the received data and one of the contemplated domain. The interpreter is also capable of understanding that “I'm cold” or “I'm too cold” or “It's not so cold” or “'m not cold” have different meaning so they belong to different semantic domains. The result of this process is sent to the Data Integrator.

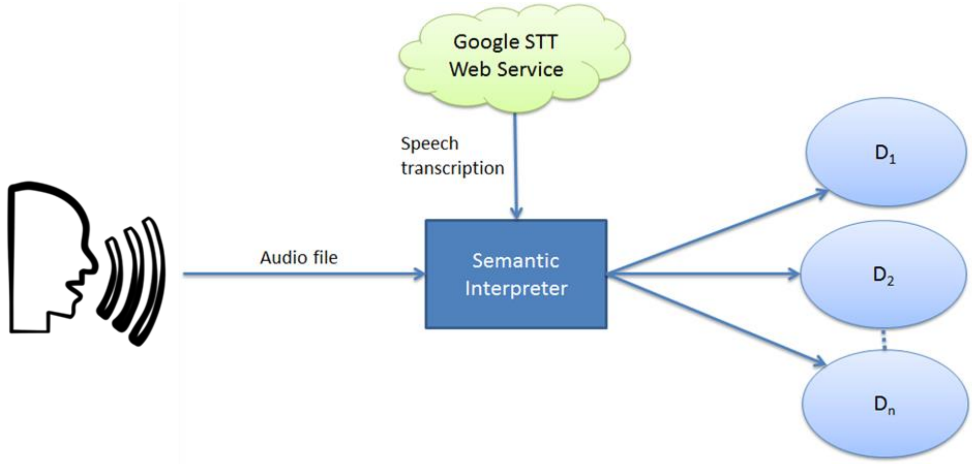


Figure 4.3 - Semantic interpretation.

For the purpose, eleven semantic domains were defined that correspond to eleven automatisms the system is able to perform. The Data Integrator computes different input including the result of the semantic interpretation:

- information if someone is in the environment from the microphone;
- indoor and outdoor temperature;
- lux from the environment;
- power consumption from the socket;
- semantic interpretation of current speech.

The brain of the system is the Data Integrator which defines the automatism that best matches all inputs and thus the human needs. The smart automatisms the system is able to execute are:

- turn the boiler or conditioner on/off or set a higher/lower temperature according to the value of the indoor/outdoor temperature detected or the presence of someone in the environment. This automatism also takes into consideration the user's preferences that are set during a configuration phase;
- Stop/permit the flow of electrical current to the socket according the current energy consumption. This automatism requires a configuration phase in which users can set energy thresholds and costs of suppliers;
- Turn on/off the light or increase/decrease the intensity of dimmable light according to the lux measured or the presence of someone in the environment.

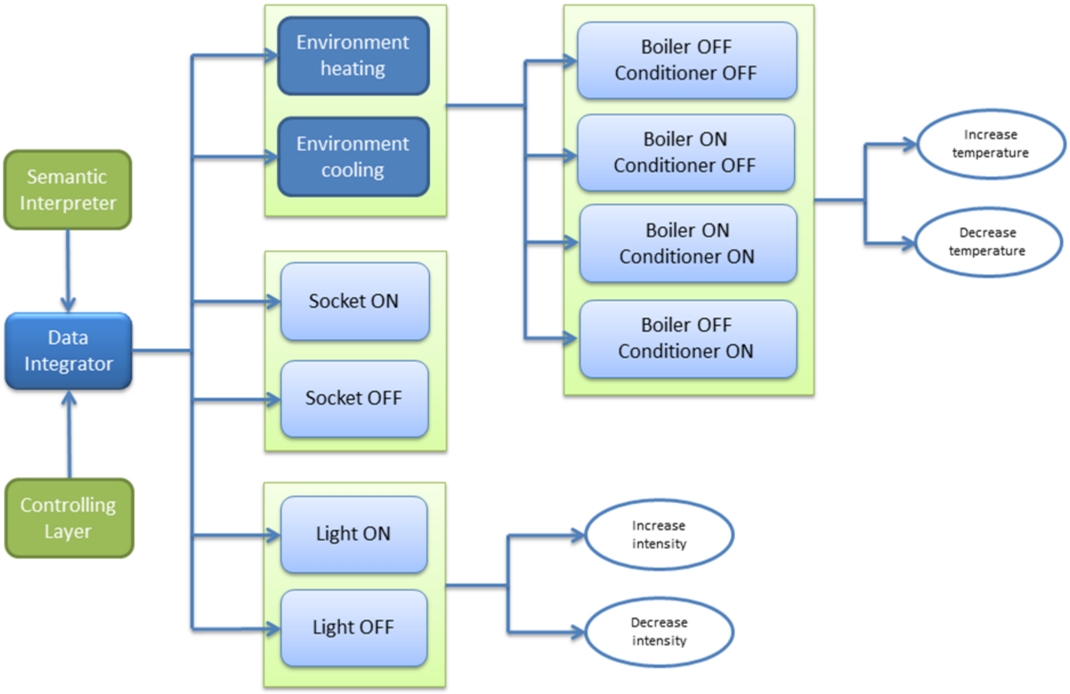


Figure 4.4 - Data integration for smart actuations.

The system is able to automate many actions that are usually manual. Experiments have been conducted with the collaboration of volunteers in an environment where the system was installed. The system showed a high degree of comfort and reliable speech recognition. Experiments have also shown that by adding human speech as an input to the system, the choice of the automatism becomes more accurate. In order to evaluate the performances of the whole system several tests were conducted. The main goal of these tests was the evaluation of the system sensibility in different scenarios considering ambient noise and other kind of disturbances such as normal human activities and background speech. The results have shown that the system needs to recognize master speech with a certain quality in order to obtain a good percentage of success in speech recognition. Moreover, it is possible to go forward making habit recognition possible by teaching the system to use unconventional methods such as Neural Network, Game Theory, Genetic Algorithm and Fuzzy Logic. These phases are still under development and are considered future developments for the moment such as the choice of better approach in term of resource allocation, latency and learning time. Another planned future development is the distribution of intelligence in the sensors, to create a mesh network that can learn user habits and to add new inputs to the data integrator (from more smart devices or processed from Internet). Furthermore, from the Controlling Layer to the Service Layer, speech could be coded as VoIP data-stream using a VoIP client-server architecture [112, 113]. This approach certainly opens the doors for the development and integration of new services with greater potentials for new distributed application and Network Layer protocols. Of course the *Quality of Service (QoS)* and *Quality of Experience (QoE)* have to be guarantee by the networking in order to reach a good *Mean Opinion Score (MOS)* level. This allows to fix users recognized speech also when it comes from a remote position. Nowadays, it is important to allow *Machine-to-Machine (M2M)* communication in order to enhance the overall performances of the system.

4.3 Human-centric applications and devices

Today *Cyber-Physical Systems (CPSs)*[10] are becoming very popular [114] since they allow both the sensing and control of physical phenomena through a network of interconnected and cooperating devices. Today both the Internet of Things and Cyber-Physical Systems concepts can be considered inherently complementary and synonymous. With the spread of smart homes it has been also possible to implement advanced and proactively operating systems called "*Proactive Context-Aware Systems*" which can sense and infer the user's and the environment's context and consequently decide autonomously how to affect the environment and actuate some smart actions. One very common problem is that for several reasons some users might not appreciate these kinds of proactive actuations so the human-feedback-in-the-loop concept and the idea of "Inferactive" system were also a topic of research in order to introduce a system that is able to learn from the user's context and feedback history and, subsequently, to adapt itself to always up-to-date users' expectations and keep the rules for triggering smart actuations constantly updated. Devices from Smart Home can collect sensing data and receive or send controlling messages according to the inhabitants' activities, requests, expectations or preferences. The environment, which is controlled by a computing system, can adjust itself using adaptation mechanisms to meet user preferences so it can offer an unobtrusive and better support for users' activities. A home adapting to its inhabitants' living style is much more suitable than a user adapting to the home's services. In recent years, the design and implementation of home automation systems followed the spread of IoT [102]; moreover, the introduction of wireless communication and *Wireless Sensors Networks (WSN)* in a wide variety of applications led research activities to add intelligence to home environments in order to increase users' level of comfort, to reduce energy consumption and to prolong lifetime of

---

[10] A cyber-physical system (CPS) is a mechanism controlled or monitored by computer-based algorithms, tightly integrated with internet and its users. In cyber physical systems, physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a myriad of ways that change with context.

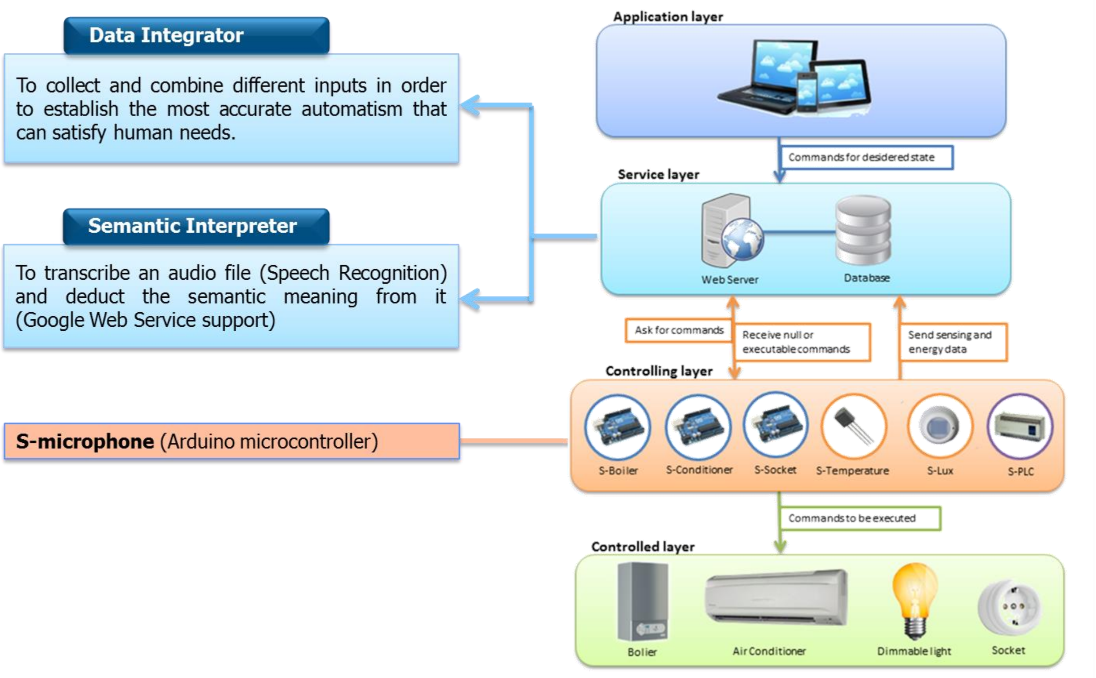
battery-powered devices. CPSs technology requires skills in robotics, wireless sensor networks, mobile computing and the Internet of Things to implement constantly monitored and reliably controlled and adaptable environments. IoT and CPSs can be considered closely related concepts: IoT was initially related to a computer science perspective and the objective was to create an Internet network of computers connected to objects with self-configuring capabilities; instead the idea of CPSs was related to an engineering perspective and the objective was the control and monitoring of physical environments and phenomena through distributed computing devices that belong to a sensing and actuation systems. To model physical phenomena, CPSs require interdisciplinary skills on smart devices and services, effective actuation, security, privacy, integration, communication and data processing and a strong foundation in mathematical abstractions. For the above discussed reasons, IoT focuses more on interconnected smart devices while CPSs are more about problem solving issues and modelling of physical processes through closed-looped systems. Although the core focus of both concepts were initially different they have many affinities such as thorough data processing, smart services and devices, reliable devices interconnection and data exchange, so in literature the two terms are often used interchangeably as they have become inherently complementary and synonymous.

While many CPSs and smart automation system can be considered *human-centric* applications meaning that humans in the system are an essential part, unfortunately, they are an external part and an unpredictable element in the process management system designed to maintain a process variable at a desired set point that is called "*control loop*" which includes sensors, control algorithms and actuators. To better meet human needs, these systems need to be strictly connected with the human element through the "*Human-in-the-Loop controls"* concept which takes account of human actions and intents, psychological and emotional states that are inferred from data acquired by interconnected sensors. In [115] a novel framework is proposed to improve the learning process through the introduction of emotion/learning sensors. The framework has a set of components and roles that emphasizes the contents and the contexts involved in the acquisition of knowledge. This is a very recent and new concept that requires multidisciplinary skills and currently, as far as is it concerned, in literature there is a lack of general understanding about requirements, principles and theory. Human in-the-loop IoT is also identified as an enabler for machine-to-machine, human-to-machine, and human-with-environment interactions. With the spread of smart devices and the adoption of new communication protocols, such as IPv6, IoT is expected to shift toward the fusion of smart and autonomous networks of Internet-capable objects equipped with the ubiquitous computing paradigm. Human in the loop IoT offers a number of advantages for a wide range of applications, such as healthcare, security, energy management, smart home etc.

4.3.1 "*Inferactive*" system and human-feedback in the loop

Automatic systems for the monitoring and control of environments are today adopted in many applications [114]; there are industrial applications for several factory processes, social applications for metropolitan reduction of pollution and traffic, body networks for health-care and disease management that may integrate user's vital signs and activity information with environmental information to recommend a healthier footpath. In [116] cooperation between wireless sensor networks and existing consumer electronic infrastructures can assist in the areas of health care and patient monitoring to improve the quality of life of patients, provide early detection for certain ailments and improve doctor-patient efficiency. In [117] authors have presented a new laboratorial prototype based on wireless sensor networks to measure patient weight. The implemented platform monitors the weight of each bedfast patient, triggering an alarm every time an unusual situation occurs. It also provides a complete suite of tools to manage, access and control all situations related to each patient. Also in the transportation domain there are modern vehicles with cruise control systems to maintain the vehicle's speed or assist in parking manoeuvres. Large urban areas are nowadays covered by millions of wireless devices and several ubiquitous and pervasive platforms are used to monitor and/or actuate on a variety of phenomena in the city area [118]. All these modern and innovative systems combine sensor data, actuator capability and computational intelligence of the devices to accomplish the predetermined goals. Traditional embedded and wireless systems are usually designed for a specific application domain; the main task is to collect data from sensors and to analyse it for a specific purpose; this restriction is called "target-application driven development" which is a limit for the spread of the technology, mass production and cost reduction [119]. Some authors believe that these restricted deployments are only the first step towards a future with interconnection in massive and non-centralized networks of smart devices. In fact, in [120] authors discuss ubiquitous, pervasive and distributed systems where users can access heterogeneous data information provided by large number of homogenous and heterogeneous sensors. The authors believe users should be free to use these data without a central-controlled authorization so data acquisition, processing and visualization should be focused on users not on administrators. Furthermore, data should be localized and delivered preferentially to local users. What has been discussed above introduces the need for a stochastic system about unpredictable sensor data and actuation. Heterogeneity is due to different types of sensor hardware, firmware, smart devices, applications, user interfaces, actuators, data flows, and usage patterns that are constantly increasing and evolving. However, this point of view, can be controversial in terms of privacy and security. A reactive system is the one that responds and reacts to external events. For example, a light consisting of a bulb and a switch is a reactive system, reacting to the user changing the switch position. On-Off control is one of the simplest types of control; another example is the thermostat used on household appliances. Reactiveness is the basic feature for any automation systems.

The logical representation of the system introduced and discussed in Section 4.1 includes all the necessary elements and functions for reactive actuations.. When the system operates proactively it means that it can sense and infer the user’s context, decide autonomously how to affect the environment and trigger actuations. An example of a proactive system is the one presented in Section 4.2, starting from the basic architecture presented in Section 4.1, where IoT was enhanced with intelligence and awareness by exploring various interactions between human beings and the environment they live in. As discussed, the knowledge of *human needs* and the *current environment* status form the inputs of the intelligence block whose main goal is to find the right automations to satisfy human needs in a real time way. To introduce the proactive feature, the Service Layer was enhanced by introducing new inputs for the system and a sort of intelligence that allows the system to infer human needs in order to autonomously perform smart automatisms. Furthermore, a speech recognition service was developed that let the system understand the semantic meaning of the speech that takes place in the environment. In this sense, human participation is considered as sensor operators and data sources. For the Controlling Layer a smart microphone was designed using the open source single-board microcontroller called Arduino that is able to detect and compute the speech of the inhabitants.


Data Integrator

To collect and combine different inputs in order to establish the most accurate automatism that can satisfy human needs.

Semantic Interpreter

To transcribe an audio file (Speech Recognition) and deduct the semantic meaning from it (Google Web Service support)

S-microphone (Arduino microcontroller)

Figure 4.5 - Extended proactive system starting from basic architecture.

One very common problem is that some users might not appreciate some proactive actuations for the following reasons:

- some errors during context sensing or inferences could trigger unreasonable actions;
- the user sometimes might appreciate something opposite to what the system autonomously trigger;
- the action, even if matching the user's desires, might be unexpected and unwanted;
- the user might feel a lack of control of his house.

Researchers have long argued that users should be active agents rather than passive recipients [121]. Considering a thermostat that automatically lowers the temperature to avoid wasteful heating when cold air comes inside through an open window. Most users would accept the proactive adjustments of closing the windows, other maybe not. In [121] a soft-actuation loop is presented. Authors assume a sense-and-react application that does not actuate, instead it generates non-imposing hints suggesting the user to perform a specific actuating actions: reaching to a nearby object and performing on it a simple, manual operation. A hint specifies both the target object and the operation (such as "close the window"). The delivery of such hints is called soft actuation because the purpose of a hint is to trigger actuation, but the decision as well as the execution is left to the user, now a part of the control loop. The idea of soft actuation was put forward quite some time ago, but, to the author's knowledge, it has not yet been systematically elaborated.

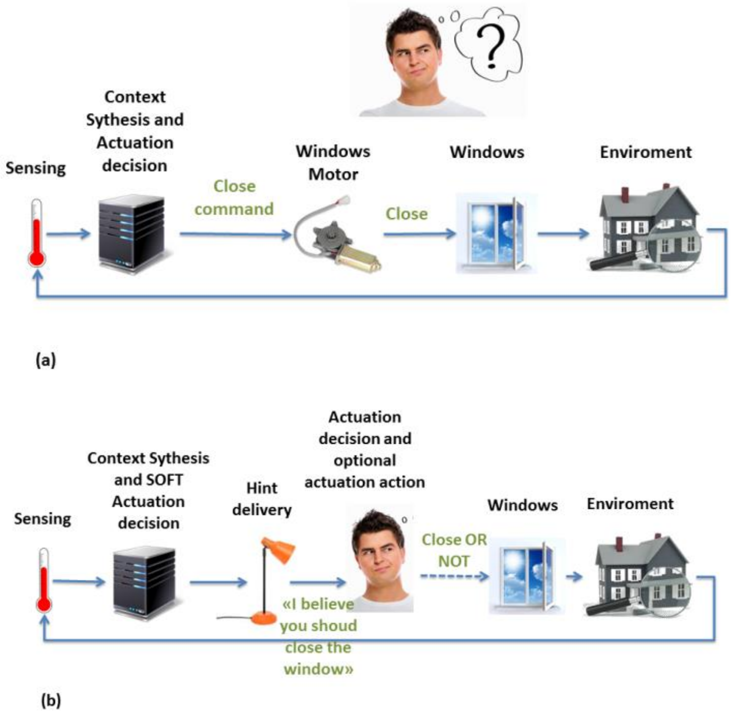


Figure 4.6 - Sense-and-react loop with proactive actuation (a) and soft actuation (b) [121].

When designing and developing these systems, some ongoing challenges must be taken into consideration [114]:

- **energy constraints** related to permanent sensing, which require intelligent mechanisms to dynamically adapt sampling rates according to the user's context;
- **data processing and inference mechanisms** to accurately extract information on human behaviour from raw sensor data;
- **classification mechanisms** for uniform inferences about widely different kinds of users;
- **privacy** about sensitive data such as user's locations and activities. People's informed consent should be provided for example to capture the voice through some environmental microphones or from the smartphone.

To go beyond the reasons why some users might not appreciate some proactive actuations, a new human role in the controlling process has been defined. A new concept of system is introduced, called "*Inferactive* System", where some information processed by the system is used to trigger actuations; the decision as well as the execution is not left directly to the user but is inferred (the origin of the name *Inferactive*) from a feedback history of that actuation related to a specific user's context; this is what has been named *human-feedback-in-the-loop*.

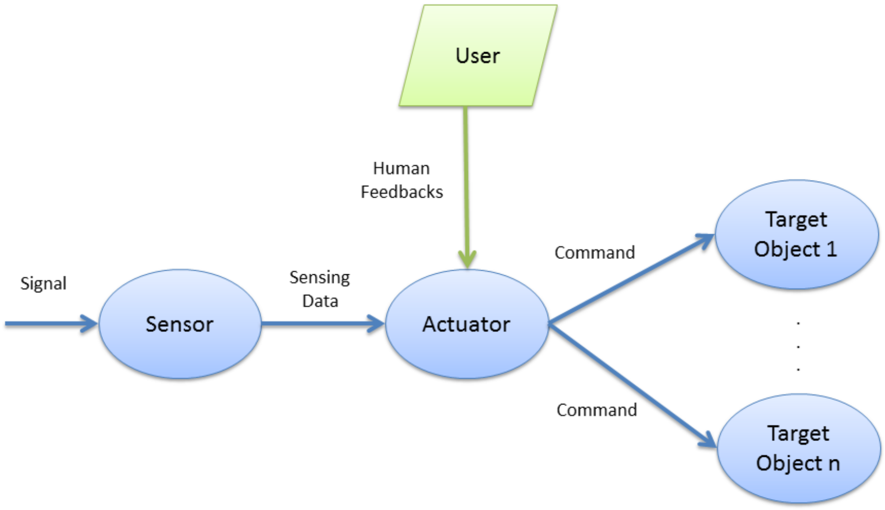


Figure 4.7 - Human-feedback-in-the-loop.

Environmental data is acquired by the sensor and is sent to the actuator; according to this information some commands can be sent to a specific target object if they match some controlling rules: for example, the heating air conditioner (target object) is turned on by the actuator when the inside temperature is below a threshold and the desired temperature will be proportional to the inside temperature according to some formula or relationship.

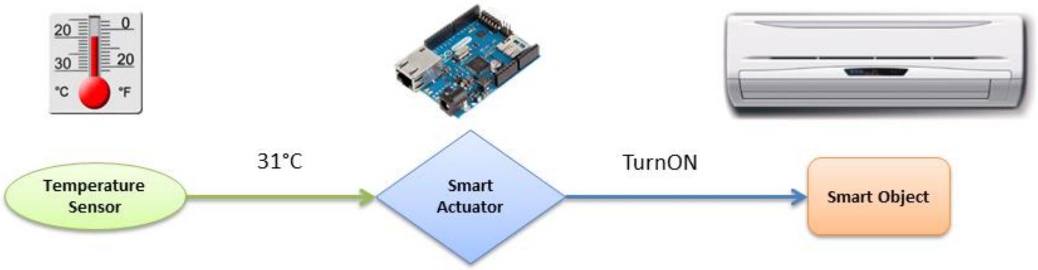


Figure 4.8 - Smart actuation.

This actuation can be considered smart if it aims to improve some specific parameters defined during the design process such as quality of life, energy efficiency, comfort and security. Other smart actuations can be, for example, the closing of the window when it starts to rain, the switching off of the light when nobody is in the room, etc. The problem is still the same: some user may not welcome energy saving and they may want to keep the light on also when nobody is at home, for example to simulate human presence in the house to discourage burglars.

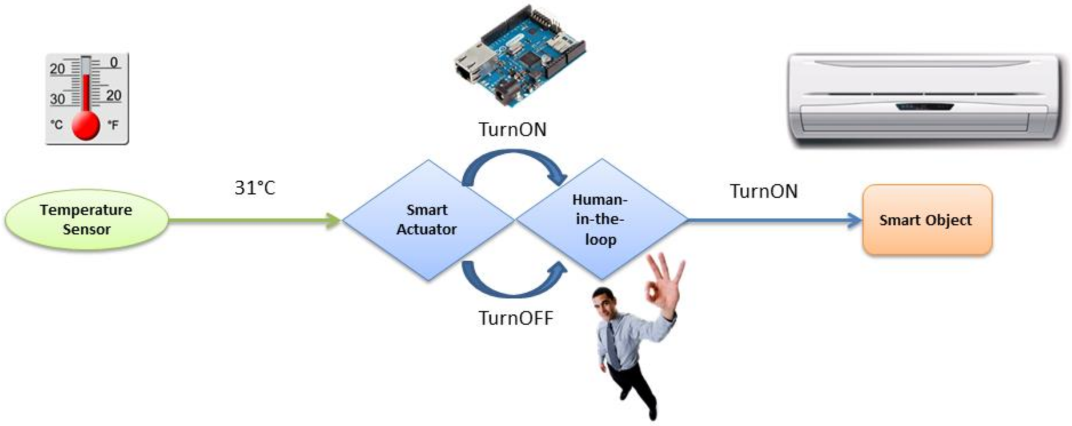


Figure 4.9 - Inferactive system.

To avoid such situations and to fully meet user needs and requirements two solutions were examined:

1 ask the users directly before command execution . This is considered a low quality solution as proactive features can be weakened, strong delays can be introduced and it can turn the system into a reactive one;
2 infer the right command to execute according to the user's feedback. If no feedback history is available, the feedback story will start from that moment. A feedback can be left in two ways:
    - **feedback from opposite triggered actuation**: after the execution of an action (or command), the user can freely contradict the actuation by changing it physically (using switches, remote controller, buttons) or using the smartphone/tablet/PC. This is the way the system can learn if a specific actuation is good or not for that specific user's context so next time at the same user's context a different actuation will be triggered. Let us assume the user's home, the season is summer and the inside temperature is 30°C. The system turns the air conditioner on and sets temperature to 25°C. However, the user is sick, he has a cold so when he notices the air conditioner is on, he immediately turns it off. The system stores this new action as negative feedback since this new actuation goes against the one triggered by the system itself. The controlling system in now updated with this new rules that overwrite the old one, so when in user's home, the season is summer and the inside temperature is 30°C, the air conditioner will not be turned on anymore;
    - **feedback from social network**: the concept of social structure made up of a set of social actors, that are users and devices, sets of dyadic ties, and other social interactions between actors can be used to create some community relationship between users and devices. Common tools, like recommendation buttons, can be used to leave feedbacks to the system about some actuations in order to establish if that actuation is meeting the user's needs and requirements.

Using the concepts of *Inferactive System* and *human-feedback-in-the-loop*, there will not be a steady relationship between the inputs and the output of the system but the output will depend on the user as it can change over time as the user's needs and requirements can change over time as well. How the *feedback history* is computed by the system is a design control process: for example, for a new rule only the last feedback can be taken into consideration, or each feedback can weigh differently, or the system can mediate among the last 10 or more feedbacks or, can even mediate among the whole history.

Feedbacks can also be collected using the concept of social communities while human-feedback-in-the-loop can be used as input for the proposed fuzzy algorithm (see Chapter 5.3). Using fuzzy logic, the user's feedback can not only be positive or negative, but it can assume different values such as excellent, very good, average, poor or terrible. The output is a numeric value that can represent, for example, the status of the light: 1 or 0 that is ON or OFF.

CHAPTER 5

ENERGY-EFFICIENT COMMUNICATION DISCOVERED

5.1 Energy-aware communication

Another important issue that was addressed in designing communication protocols was how to save sensor node energy while meeting the needs of applications. Recent researches have led to new protocols specifically designed for sensor networks where energy awareness is an essential consideration. Integration of sensing and actuation systems, connected to the Internet, means integration of all forms of energy consuming devices such as power outlets, bulbs, air conditioners, etc. Sometimes the system can communicate with the utility supply company and this can lead to the achievement of a balance between power generation and energy usage or in general is likely to optimize energy consumption as a whole. The past decade has witnessed a significant growth in the usage of Internet and wireless handheld devices. Today's handheld devices are equipped with different wireless interfaces such as 2G, 3G, Wi-Fi, RF and Bluetooth for a variety of applications. Handheld devices are commonly powered with rechargeable batteries to support mobility. Small and light devices require the battery to be proportionately small so the supply budget is limited. To keep the device running, the battery needs to be recharged before the remaining energy falls under a specific threshold.

Some electrical devices have been designed with multiple communication interfaces, such as RF or Wi-Fi, using open source technology and they have been analysed under different working conditions. Some devices are programmed to communicate directly with a Web Server, others to communicate only with a special device that acts as a bridge between some devices and the web server. Communication parameters, data size and device status have been changed dynamically according to different scenarios and specific quality of service required, such as the speed of response, in order to have the most benefits in terms of energy cost/quality ratio and to extend battery lifetime. The way devices communicate with the Web Server or between each other and the way they try to obtain the information they need to be always up-to-date, change dynamically in order to guarantee always the lowest energy consumption, a long lasting battery lifetime, the fastest responses and feedbacks and the best quality of service and communication for end-users and inner devices of the system. The spread of IoT is over multiple disciplines such as healthcare, industry, transport, and home appliances where the main objective is to maximize the communication of hardware objects with the physical world and to convert the data collected into useful information without any human intervention. The more data collected and analysed, the greater the accuracy of extracted information and the energy consumed of the limited battery power; therefore a trade-off between quality of information extracted and energy consumption is required in order to prolong lifetime of resources and the effective operation of the system. Using the architecture described in Section 4.1, different scenarios were explored and energy consumption of battery powered devices was tested under different conditions.

D_i is assumed to be the generic device of the Controlling Layer where $i=1 \ldots n$. The enhancement introduced regarded how devices communicate with the Web Server of The Service Layer and between each other. Three types of Di were designed:

- D_1: device equipped only with Wi-Fi interface that can communicate with the Service Layer through HTTP protocol;
- D_2: device equipped only with RF interface that can communicate with other devices of the same layer through RF protocol;
- D_3: device equipped with both Wi-Fi and RF interfaces so it can communicate with other devices of the same layer through HTTP and RF protocols and with the Service Layer through HTTP protocol.

Devices were implemented with 8-bit low power ATMEGA328p Microcontroller (MCU). Energy consumption is 0.2 mA in active mode (1MHz, 1.8V, 25°C) and it can reach 0.1 uA in power-down mode. Low power RF interface consumes 0.4mA in active mode. The RF interface used is AM OOK transmitter module with *Surface Acoustic Wave (SAW)* resonator. It contains a buffer stage for enhanced power and low harmonics on output allowing high immunity against disadjustments. A printed circuit version of the well-established long available, TX-SAW MID 3V assembled on alumina substrate was used. Energy consumption of RF and Wi-Fi interfaces is shown in Tables 5.1, 5,2, 5.3.

Table 5.1 - Energy consumption of RF Rx interface.

RF Rx Parameters	**Value**	**Unit**
Carrier frequency	433.92	MHz
Supply voltage	3.3	V
Supply current	0.4	mA

Table 5.2 - Energy consumption of RF Tx interface.

RF Tx	**Value min**	**Value typical**	**Value Max**	**Unit**
Carrier frequency	433.92	433.92	434.02	MHz
Supply voltage	1.8	3.3	3.5	V
Supply current with modulation	2.4	5.5	7	mA
RF output power	3	10	11	dBm

Table 5.3 - Energy consumption of Wi-Fi interface.

Wi-Fi	**Value**	**Unit**
Tx 802.11b,CCK 11Mbps, P.Out = +17dBm	170	mA
Tx 802.11g,OFDM 54Mbps, P.Out = +15dBm	140	mA
Tx 802.11n,MCS7, P.Out = +13dBm	120	mA
Rx 802.11b, 1024 bytes packet length, -80dBm	50	mA
Rx 802.11g, 1024 bytes packet length, -70dBm	56	mA
Rx 802.11n, 1024 bytes packet length, -65dBm	56	mA
Modem Sleep	15	mA
Light-sleep	0.9	mA
Deep-sleep	10	uA
Power Off	0.5	uA

Using these different types of devices it is possible to test different scenarios and different network topologies of the controlling layer like star network or cluster/tree network. For the star network only D_1 devices are used. The centre of the star is the Service Layer and no communication between devices of the same layer is provided. For Cluster/Tree network both D_2 and D_3 device are used and both Wi-Fi and RF communications are provided.

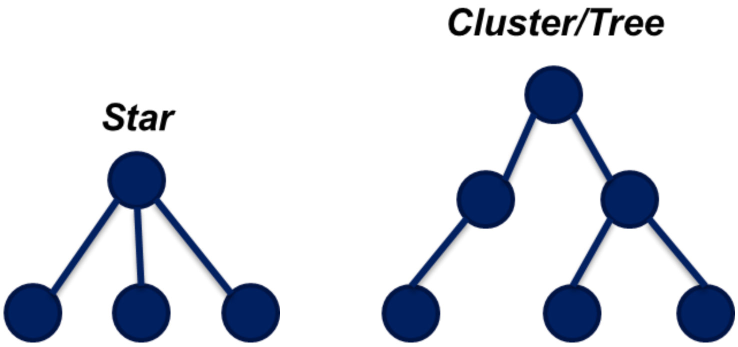


Figure 5.1 - Star topology and Cluster/Tree topology.

The way devices communicate has been analysed in order to reduce energy consumption and prolong system lifetime. Devices equipped with Wi-Fi and RF interfaces were analysed under different scenarios by setting different communication parameters, such as data size, in order to evaluate the best device configuration and the longest lifetime of devices. The communication protocol from the Controlling Layer to the Application Layer was enhanced in order to collect and store monitoring data from the sensor of the Controlled Layer. The main focus was on the way devices communicate between each other to transfer the information the system requires to always be up-to-date and to guarantee the lowest energy consumption and a long lasting battery life. For the Controlling Layer, a hierarchical organization of devices was assumed devices: a sink node is equipped with both Wi-Fi and RF interfaces so it can communicate with other devices of the same layer through HTTP or RF protocols and with the Service Layer through HTTP protocol; sensor nodes are equipped only with RF interface so they can communicate with the sink node only through RF protocol. The sink node collects and manages data aggregation and data transfer from the Controlling Layer to the Service Layer. Controlling Layer topology is represented in Figure 5.2.

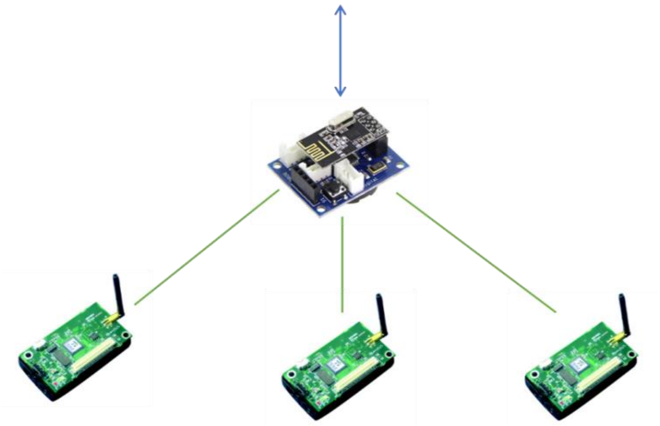


Figure 5.2 - Controlling layer topology.

Both sink nodes and sensors node were implemented with an 8-bit low power ATMEGA328p Microcontroller (MCU) where energy consumption is described in Table 5.1, 5.2, 5.3. Chapter 6 presents a discussion of the test and results of energy consumption according to these topological configurations.

5.2 Energy-efficient Wi-Fi social communication

The design and implementation of Wi-Fi sensors and actuators have also been inspected as a social IoT solution for home automation systems where devices are socially connected to the Internet and can communicate through social applications like Facebook, Twitter or Google+ with a community of users that usually interact with that device. A fuzzy-based solution was proposed to classify the social community interaction with the system in order to implement an adaptive energy saving mode for these social Wi-Fi devices according to the users' current context, behaviour, habits and feedbacks. Test and performance evaluation regarding energy consumption and efficiency in a real world scenario with real hardware devices are shown in Chapter 6 to prove the efficiency of the solution in terms of electricity consumption, battery lifetime, CPU utilization and increase of comfort and satisfaction levels for community users.

One of the most important issues in designing IoT systems is how to save the devices' energy and meet applications requirements at the same time. The development of energy efficient schemes for IoT is a challenging issue for complex and large-scale IoT systems since current techniques of wireless sensor networks cannot be applied directly to IoT devices [122]. Currently, smart homes implemented with Wireless Networks meet the Internet of Things paradigm. Often these systems can vary in their architectures, communication technologies, energy management and devices features and these issues can be addressed through the performing of a permanent monitoring of some energy parameters that can be adapted to energy requirements or the user's expectations in terms of battery lifetime and the response time of the system. Also, the integration of different electrical devices in the household is an open challenge because of the absence of an inexpensive and standardized communication protocol [123]. It is very common to find solutions using low power communication protocols such as Bluetooth or ZigBee [123, 124, 125]; the main drawback of these technologies is that a dedicated network is required for the applications to be deployed and sometimes this can be very unusual for the home environment where Wi-Fi technology is the one widely used and adopted in home and monitoring applications [126, 127, 128, 129]. Everybody owns a Wi-Fi router at home to enable Internet connection through computers, smart-phones, smart cameras or smart TVs. On the other hand, originally, the Wi-Fi protocol was not designed to be suitable for battery-powered devices or low power devices since energy consumption, compared to other wireless protocols such as ZigBee or Bluetooth, is proved to be moderately high. This is the reason why Wi-Fi protocol, with the spread of the Internet of Things, has undergone some revisions and changes in order to meet these energy requirements and to open the doors for new scenarios. Energy efficient architectures and protocols allow for the lifetime of smart devices' to be prolonged so that users are not compelled to constantly replaces dead batteries.

A new concept of device called "Social aware Wi-Fi device" was conceived, which is able to interact with a community of users by using social applications like Facebook, Twitter or Google+ in order to improve performances in terms of energy consumption; the device adapts its energy parameters to the user's feedbacks, context and the device's remaining battery percentage. Using a fuzzy-based algorithm, an adaptive energy saving mode and a dynamic requesting frequency were implemented to offer better energy management that takes device's status and users' levels of interaction and satisfaction during different interaction contexts into account. Information from a social community that interacts with the device is used as input for the fuzzy algorithm along with other parameters. Energy policies based on fuzzy-logic allow devices to impersonate human reasoning very closely so that any decision can be made with uncertain users' behaviour by taking into account users' feedbacks from the social community and the current device's level of energy. A star network for the Controlling Layer was implemented with Wi-Fi devices where the centre of the star is the Service Layer and no communication between devices of the same layer is provided. This configuration provides the system with good communication and data transfer performances in terms of reliability and response of the system but the problem is the high energy consumption due to Wi-Fi interfaces available on the market that are not optimized for batteries powered devices so energy consumption is higher than others low power interfaces such as Bluetooth Low Energy or ZigBee. The message flow in star topology is described in Figure 5.3:

(1) generation of command from the Application Layer;
(2) receiving command to the Service Layer with HTTP/HTTPS protocol;
(3) data capture of the command from Service Layer by Controlling Layer through Wi-Fi interface with a specific requesting frequency;
(4) processing data with Controlled Layer;
(5) sending ack to Service Layer through Wi-Fi interface;
(6) Send ack to Application Layer with HTTP protocol.

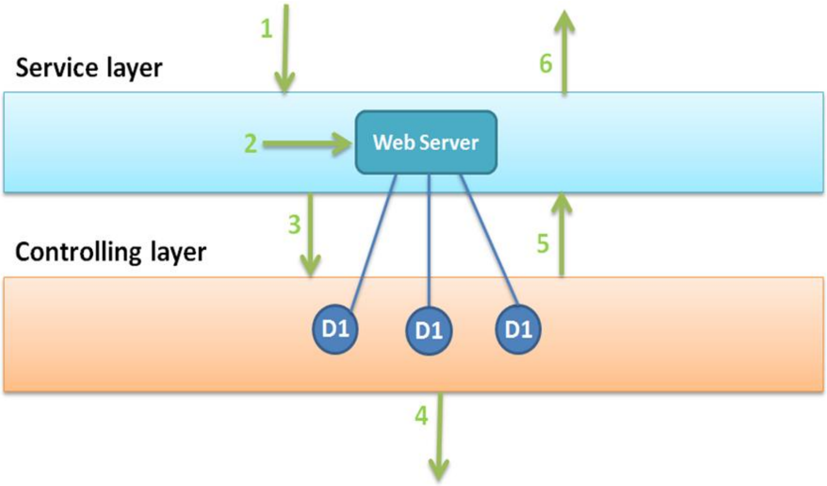


Figure 5.3 - Message flow in star topology.

REST Web Services provided by the Service Layer are invoked to send commands, such as HTTP POST or HTTP PUT. The command contains the identification of the actuator that is placed in the Controlled Layer and a coded message in HTTP body that contains the command to be executed (turn on the air conditioner is coded in an integer value). In Figure 5.4 an example of user interaction with the system and message delivery is shown. At the beginning a constraint for devices was a fixed requesting frequency for commands to be executed; for a better energy management and a longer lifetime of devices, a dynamic requesting frequency was introduced later by implementing a fuzzy-logic algorithm for the new type of Social Aware Wi-Fi Devices.

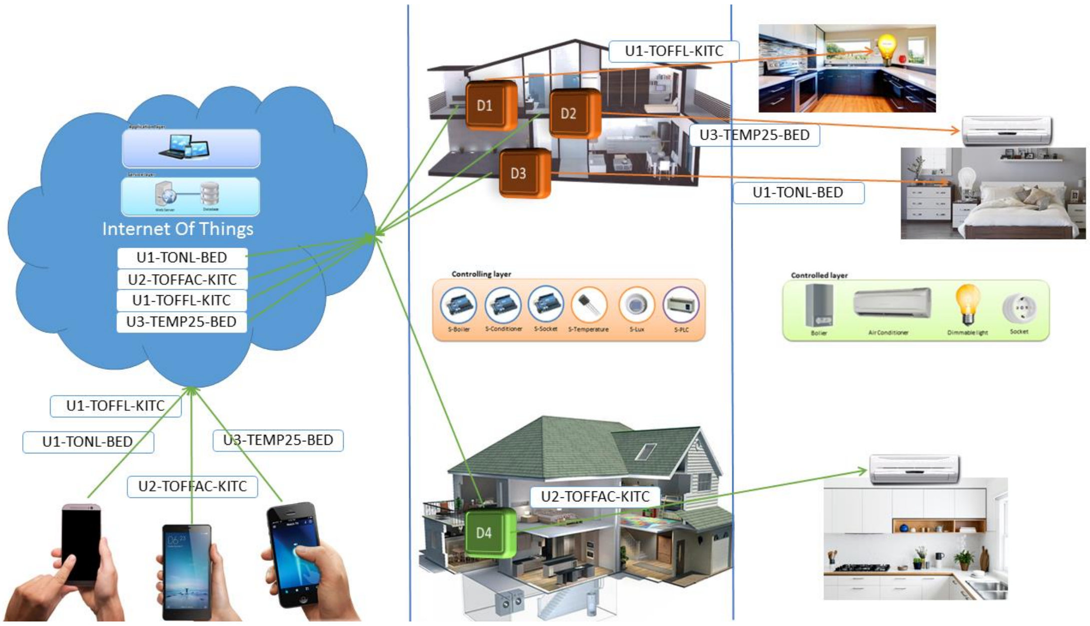


Figure 5.4 - System communication and users' interaction.

Social Aware Wi-Fi devices of the Controlling Layer have been implemented with an 8-bit low power ATMEGA328P_AU MEL Microcontroller (MCU) produced by AT and a Wi-Fi Al-Thinker module on an ESP8266 chip produced by ESPRESSIF. Energy consumption is 0.2 mA in active mode (1MHz, 1.8V, 25°C) and can reach 0.1 uA in power-down mode. The power supply circuit consists of four AAA batteries and an MCP1700 LDO (Low Dropout Voltage Regulator) produced by Microchip with stabilized voltage fixed to 3.3V. The device is equipped with one temperature sensor TMP36. Two buttons, an ICSP (In-Circuit Serial Programming) Interface, one micro-USB port and a radio frequency module have been designed and implemented for future works.

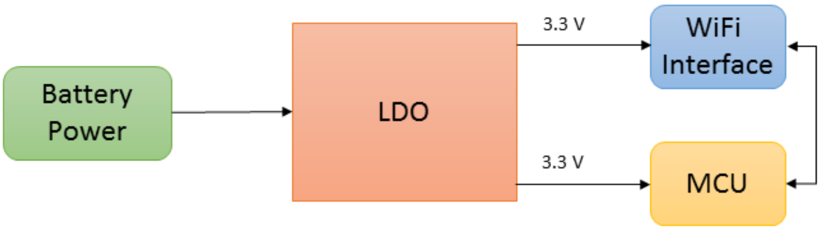


Figure 5.5 - Block diagram of the Social Aware Wi-Fi Device.

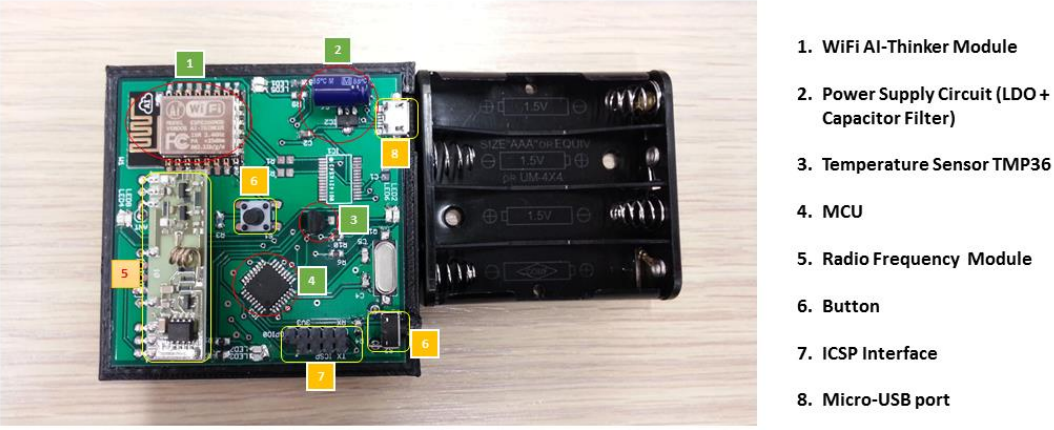


Figure 5.6 - Hardware implementation of the Social Aware Wi-Fi Device.

Firmware was designed taking into consideration low power strategies: all unused interfaces and peripheral devices go to sleep mode and only when necessary UART (Universal Asynchronous Receiver-Transmitter) is activated to enable communication with the Wi-Fi module. *ADC (Analog to Digital Converter)* is activated only when sensor data acquisition is required. As shown in Figure 5.7, MCU works at 512KHz low frequency during sensing procedure, then it goes to sleep mode (128KHz internal RC oscillator). When it is time for request, MCU wakes up to high speed (16MHz), the Wi-Fi interface is activated and initialized, then sensing data are sent along with the request for commands to be executed.

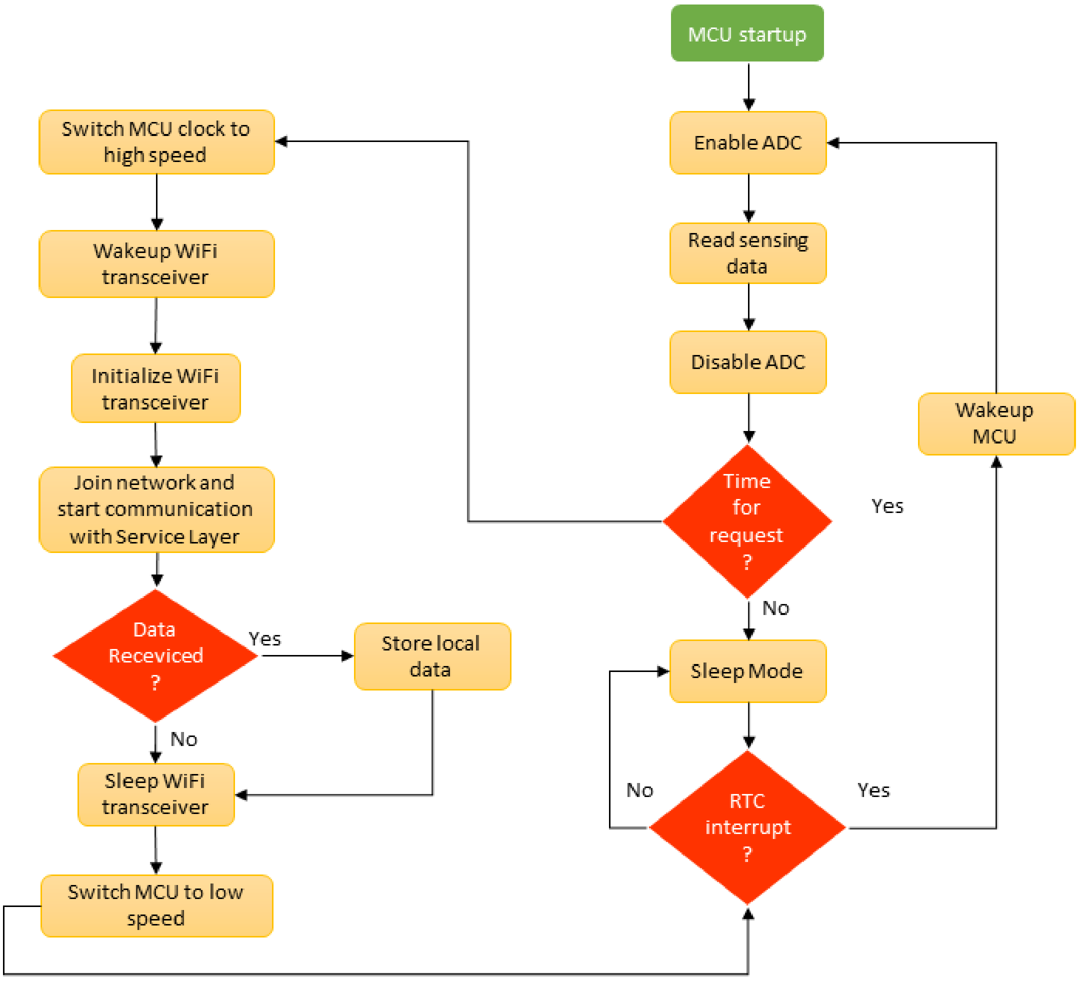


Figure 5.7 - Workflow diagram of the Wi-Fi sensors and actuators.

5.3 Social communities for Smart Wi-Fi Devices

To interact with the automation system, users are required to login to a mobile application by using a system account. The service Layer of the systems offers the possibility to create a new system account, otherwise a Facebook or Google+ account can be used. Accessing through the interfaces of the Application Layer, it is possible to configure the device that users want to control and link it to their own account. During this configuration phase, the device's serial number and home Wi-Fi information are required to enable Internet connection for the device. Once configuration is complete, the system automatically creates a social community for that device that is identified with the serial number; the user automatically becomes a member of that community. If the community for that device already exists, there will be no need to create another one so user will just be added to the community or invited to join in. The community should enable the possibility for people to be organized into groups or lists for sharing information with the system. One easy way to share information is by using a "*Like Button*" or "*Recommend button*" that is a widespread feature in communication software such as social networking services, Internet forums, news websites and blogs: using this button, users can express if they like, enjoy or support certain content and thus constitutes an alternative to other methods of expressing reaction to content, like writing a reply text. A dislike button could be implemented to vote against some content although a negative feedback is actually deduced from a missing positive feedback. The system is able to create some posts to share with community users in order to collect their likes or dislikes and take advantage of this information for energy management decisions. Social communication and community are managed by the Service Layer. A device that implements this social awareness feature is called "Social Aware Wi-Fi Device". A community is a group of people that usually interact with a specific social device; two or more communities can live together in the same house but can interact with different devices such as D1 to control the air conditioner, D2 to control a smart socket and D3 to control a dimmable light.

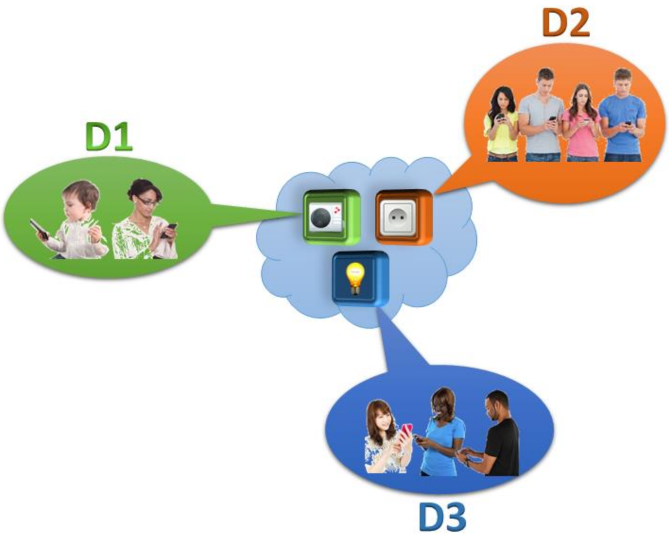
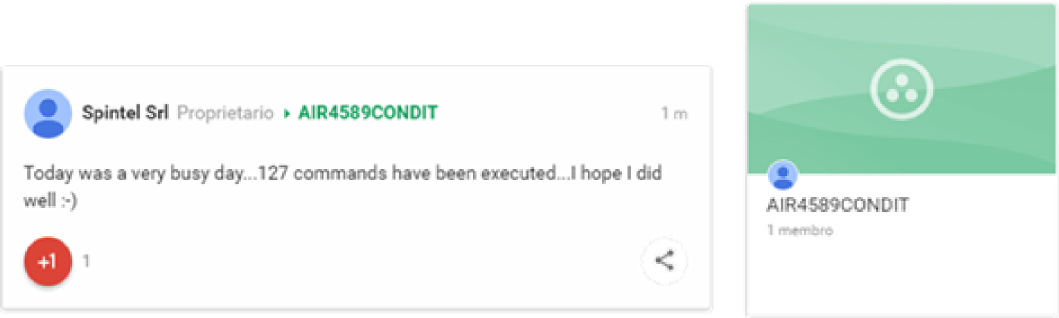


Figure 5.8 - Social Community around different devices D1, D2 and D3.



Spintel Srl Proprietario ▸ AIR4589CONDIT 1 m

Today was a very busy day...127 commands have been executed...I hope I did well :-)

Figure 5.9 – Social community linked to the smart actuator and feedback from social network.

For testing purposes, Google+ is used as the social network to implement the conceived social awareness feature. A Google administration account is required for the Service Layer and users are required to login to a mobile application by using a Google account. After the configuration phase, a Google+ Community for that device must be automatically created by the Service Layer using official or thirty party Google APIs and users must be invited to join in. If the devices' serial number matches an existing community ID, the user will be automatically invited to join that community by the system administration account and will be authorized to share information with other members of the community or with the system. Communities can be implemented with "Google+ Communities" that allow any account to create ongoing conversations about particular topics; for the social awareness about automation systems the topic could be a daily survey about numbers of interaction the devices of the system had dealt with during the day. If users join the device community, they become members of that community. Users can use +1 button to express if they like or dislike the topic of the day. All +1 likes for that topic can be used to evaluate the degree of satisfaction about the system response time that depends on the requesting frequency (numbers of requests sent in a time interval to the Web Server of the system to ask about commands to execute). The only disadvantage in using an existing social network, is that some official or third party API may not be available so interaction with the social network could be rather difficult or sometimes impossible. All the likes collected with +1 button will be mathematically computed to be used as one possible input for the proposed fuzzy algorithm discussed in Section 5.3.1.

5.3.1 Fuzzy-Based algorithm for energy saving mode

The objective of the proposed fuzzy algorithm is to classify user interaction with social aware Wi-Fi devices in different contexts in order to adapt requesting frequency for any pending actuating commands; this dynamic requesting frequency can avoid frequent requests of commands to the Web Server in hours of the day with low or missing interactions and so the device can prolong sleep mode and, consequently, its lifetime. The knowledge of users habits and regular usage of the system helps in energy saving strategies and the reduction of energy wastage. Information about how often users interact with the system are computed with a fuzzy logic algorithm. User interaction can vary during the day and can differ according to a specific context; for example, it is reasonable to state that in an outdoor context commands are less frequent and the speed of system response to commands is a weak constraint. A *Fuzzy Logic Controller (FLC)* can be used where classical control methods do not achieve favourable results. A general representation of FLC is depicted in Figure 5.10 where some input parameters are used to evaluate and update the requesting frequency to the Server that is the output of the FLC. An FLC fuzzification phase is based on a *Membership Function (MF)* which maps each point of the input space to a membership value which represents the degree of membership between zero and one.

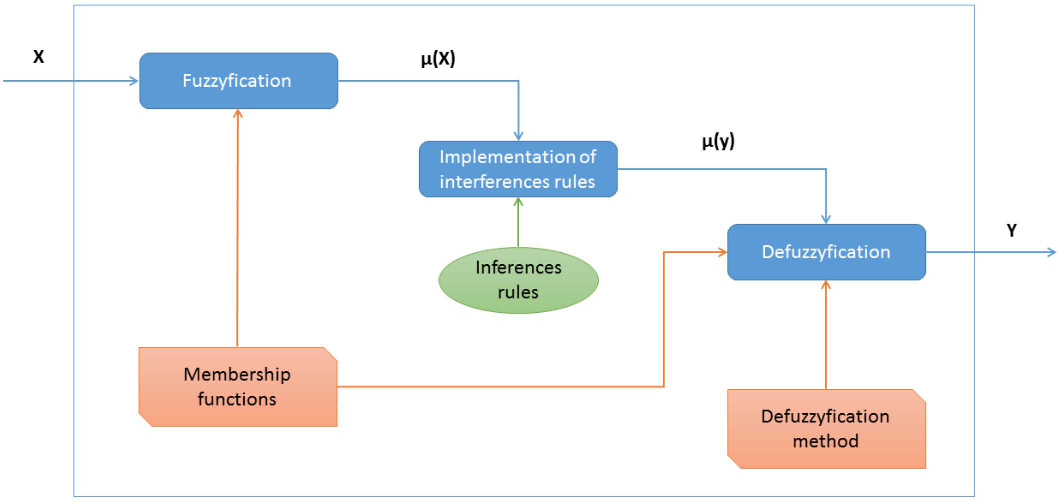


Figure 5.10 - Fuzzy algorithm for logic controller.

One common method for inference is the four-steps Mamdani method [130]:

1. **Fuzzification**: evaluation of membership value for crisp inputs;
2. **Inferences rules**: setting up of IF-THEN rules with antecedents using AND/OR fuzzy operators;
3. **Aggregation**: unification of all the antecedents of the rules to make a fuzzy set for each output variable;

4. **Defuzzification**: reconversion of fuzzy values in crisp values by using membership function and one of the defuzzification methods available in literature such as centre of area, mean of maxima, centre of gravity, etc. The output is a numeric value.

To evaluate the new requesting frequency, the inputs for the algorithm are community context and feedback, remaining battery, community interaction.

Community context is a numeric value between 0 and 1 that is used to distinguish between:

- **Indoor context**: quick response of the system is preferable;
- **Outdoor context**: delayed response of the system is accepted.

The value is evaluated as follows:

$$C_c = \frac{\sum_{i=1}^{n} IH_i}{n} \quad \text{with} \quad C_c \in [0,1] \qquad (1)$$

where
IH = IsHome variable related to user or member i-th with n = number of community members

$$IH_i = 1 \text{ if member i} - \text{th is home}$$
$$IH_i = 0 \text{ if member i} - \text{th is not home}$$

A value close to 1 means that all members are home so a quick response is preferable; as the value decreases, a delayed response is more suitable. The more the community context value is close to zero, the more the delay in the command execution is accepted. The system is able to understand if users are home by using different localization techniques. One easy way is offered by the Wi-Fi interface of mobile devices where the client application is installed: usually the system's developing library offers the possibility to scan all surrounding Wi-Fi networks; if the home Wi-Fi network signal, previously stored as the user home network during the configuration phase, is detected it means that the user is home, otherwise the user is not home. If no information is available about the user's location, some assumptions can be made or the user's location can be inferred by the user's interaction rate with the system assuming that interaction is high when the user is home.

Community feedback is a number between 0 and 1 that is evaluated as follows:

$$\mathrm{C_f} = \frac{\sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{pf_i}}{\mathrm{n}} \quad \text{with} \quad C_f \in [0,1] \qquad (2)$$

where

pf = positive feedback variable related to user i-th and n = number of community members

$$\mathrm{pf_i} = 1 \text{ if } \mathrm{member_i} \text{ left a positive feedback}$$
$$\mathrm{pf_i} = 0 \text{ if } \mathrm{member_i} \text{ left a negative feedback}$$

A value close to 1 means that all members left a positive feedback so energy management is working well and all users are satisfied; the more the value is close to zero, the more users are unsatisfied so energy policies must change as soon as possible.

Remaining battery is a number between 0 and 1 that is evaluated as follows;

$$\mathrm{B_i} = \frac{\mathrm{B_{i\%}}}{100} \quad \text{with} \quad B_i \in [0,1] \qquad (3)$$

where

$$\mathrm{B_{i\%}} = \text{Quantity of remaining battery for device i}$$
$$0 \le \mathrm{B_{i\%}} \le 100$$
$$0 \le \mathrm{B_i} \le 1$$

$\mathrm{B_i} = 1$ means 100%of battery for device i,$\mathrm{B_i} = 0.5$means 50% and so on.

Community interaction is a number between 0 and 1 that represents the amount of actuations commands sent during the last hour by the community and is evaluated as follows:

$$\mathrm{I_i} = \frac{\sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{cmd_i}}{60} \qquad (4)$$

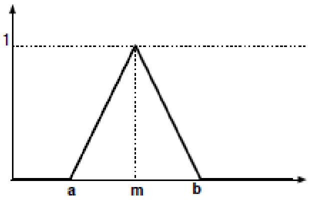
where

n = number ofcommunity members

$\mathrm{cmd_i}$ = numbers of actuation commands sent during the last hour by member i

The output of the algorithm is the new requesting frequency. The proposed FLC considers three membership functions (Low, Medium, High) for the inputs and the output that are shaped with a triangular function:

$$\mu_A(x) \begin{cases} 0 & \text{if } x \le a \\ \frac{x-a}{m-a} & \text{if } a < x \le m \\ \frac{b-x}{b-m} & \text{if } m < x < b \\ 0 & \text{if } x \ge b \end{cases} \tag{5}$$



During the configuration phase, users can set different values of maximum allowable delay for each device, according to their preferences or habits.

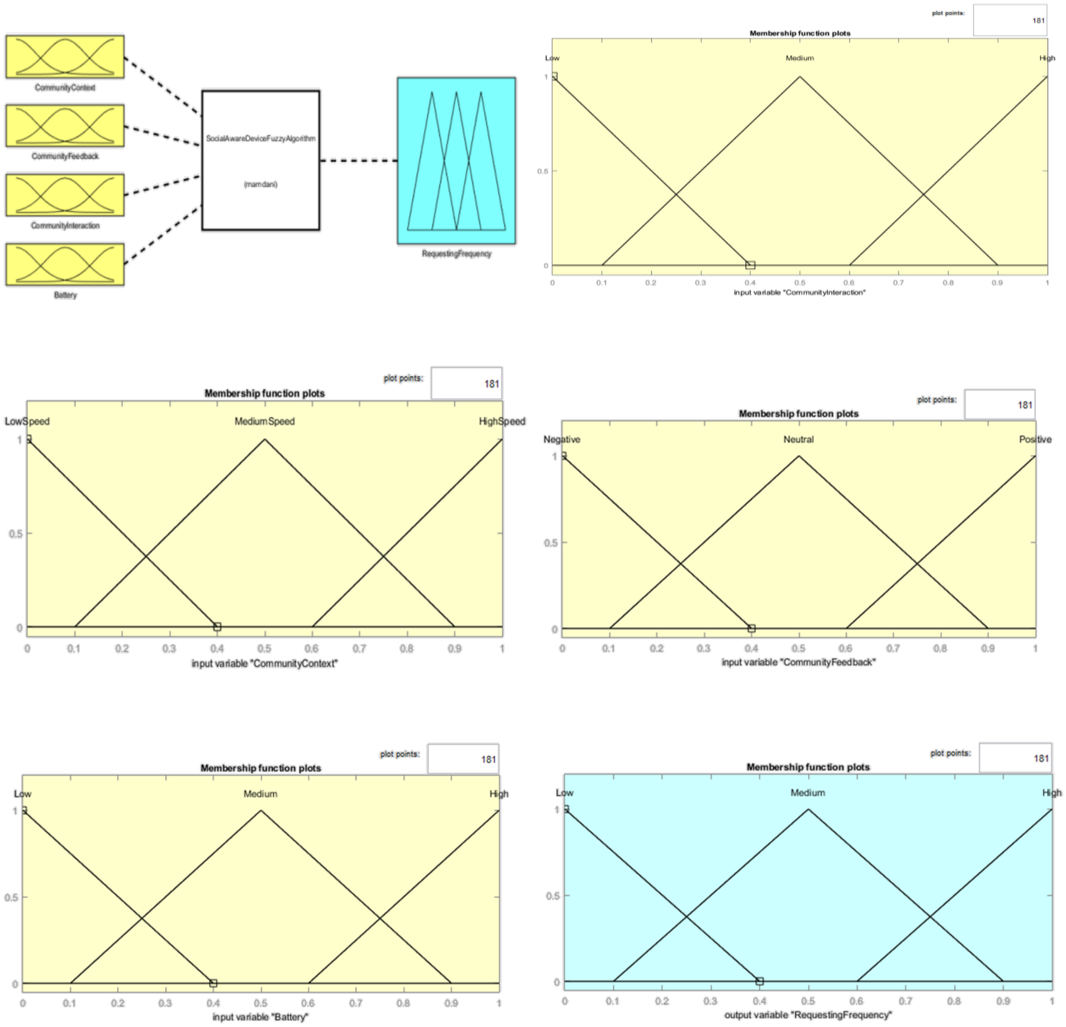


Figure 5.11 - MATLAB Fuzzy Logic Design.

The output value is evaluated through the following fuzzy rules based on IF-THEN statements and listed in Tables 5.4, 5.5 and 5.6.

Table 5.4 - (A) Fuzzy Rules for Social Aware Devices.

Rule	**IF Community Context**	**AND Community Interaction**	**THEN Requesting frequency RF1**
1	Low Speed	Low	Low
2	Low Speed	Medium	Low
3	Low Speed	High	Low
4	Medium Speed	Low	Low
5	Medium Speed	Medium	Medium
6	Medium Speed	High	Medium
7	High Speed	Low	Medium
8	High Speed	Medium	High
9	High Speed	High	High

Table 5.5 - (B) Fuzzy Rules for Social Aware Devices.

Rule	**IF RF1**	**AND Battery**	**THEN Requesting frequency RF2**
10	Low	Low	Low
11	Low	Medium	Low
12	Low	High	Low
13	Medium	Low	Low
14	Medium	Medium	Medium
15	Medium	High	Medium
16	High	Low	Low
17	High	Medium	Medium
18	High	High	High

Table 5.6 - (C) Fuzzy Rules for Social Aware Devices.

Rule	IF RF2	AND Community Feedback	THEN Requesting frequency RF
19	Low	Negative	Medium
20	Low	Neutral	Medium
21	Low	Positive	Low
22	Medium	Negative	High
23	Medium	Neutral	Medium
24	Medium	Positive	Medium
25	High	Negative	Medium
26	High	Neutral	Low
27	High	Positive	High

Three types of fuzzy inference methods are proposed in literature: Mamdani, Sugeno and Tsukamoto [130]. All of these three methods can be divided into two processes: the first consists in fuzzifying the crisp values of input variables into membership values according to appropriate fuzzy sets and these three methods are exactly the same in this process. The difference of the three methods is the second process that is when the results of all rules are integrated into a single precise value for output. In Mamdani inference, the consequence of the IF-THEN rule is defined by fuzzy set. The output fuzzy set of each rule will be reshaped by a matching number, and defuzzification is required after aggregating all of these reshaped fuzzy sets. In Sugeno inference, the consequence of IF-THEN rule is explained by a polynomial with respect to input variables, thus the output of each rule is a single number. Then a weighting mechanism is implemented to work out the final crisp output. Although Sugeno inference avoids the complex defuzzification, the work of determining the parameters of polynomials is inefficient and less straightforward than defining the output fuzzy sets for Mamdani inference. Tsukamoto inference is a kind of combination of Mamdani and Sugeno method but it is less transparent than the other two. For social aware Wi-Fi device the Mamdani model has been implemented. Defuzzification is performed by using *Centroid Of Area (COA)* method so the final output that is the new requesting frequency is evaluated as follows:

$$R_f = \frac{\sum_{i=1}^{n} O_i * C_i}{\sum_{i=1}^{n} C_i} \qquad (6)$$

where O_i is the output of rule i and C_i is the center of the output membership function. This is the most widely adopted defuzzification strategy which is reminiscent of the calculation of expected values of probability distributions. The results are discussed in Chapter 6

CHAPTER 6

TEST AND RESULTS

In this Chapter, the results obtained are discussed according to scenarios and test environments set up and discussed in Chapters 4 and 5.

6.1 Energy savings for end-users

One of the main goals of the thesis was to design a very user-friendly monitoring and controlling system with ready-to-use smart devices that allow users to interact with their house and be aware of energy waste. In order to evaluate system performances, a testbed based on typical use of appliances in a common home automation environment was set up. It was assumed that a typical family consists of four people that would like to take the advantages of a home automation system and control several devices. The architecture proposed aims to make an easier control of home automation devices offering a very smart and friendly client application based on modern technologies that allow communication between the central control unit, devices and users. The design and development was based on the intent to raise user awareness about their energy consumption, showing the waste of energy during the day. As shown in Figure 6.1, users after a learning time about all the features and advantages that can be taken from the system, they are encouraged to adopt a better behavior in terms of energy consumption, avoiding wastage and saving energy and money. The learning time and the slope of the trends demonstrate that users can take advantages from such useful tools that help them to perform the best actuation by consulting information containing real-time energy consumption. They become aware how small changes in their behaviors can reduce energy waste. Moreover, using a multi-layer Service Oriented Architecture allows the achievement of a high degree of interoperability between different software and smart devices avoiding direct implementation of service-oriented features on the devices' side. Thinking of a future commercialization of the system, having a modular architecture with layers would make it possible to entrust the Application and Service Layers to some Service Provider while the Controlling and Controlled Layers could be installed at the users' home. Another commercial solution could regard the installation of the Service and Application Layers at the users' house. The commercial solution will depend on the adopted marketing policies. Experimental results showed that if users are aware of their energy consumptions and have the possibility to control some household devices, after a period of training, they can save up to 20% on energy bills and correct misconduct about energy consumptions.

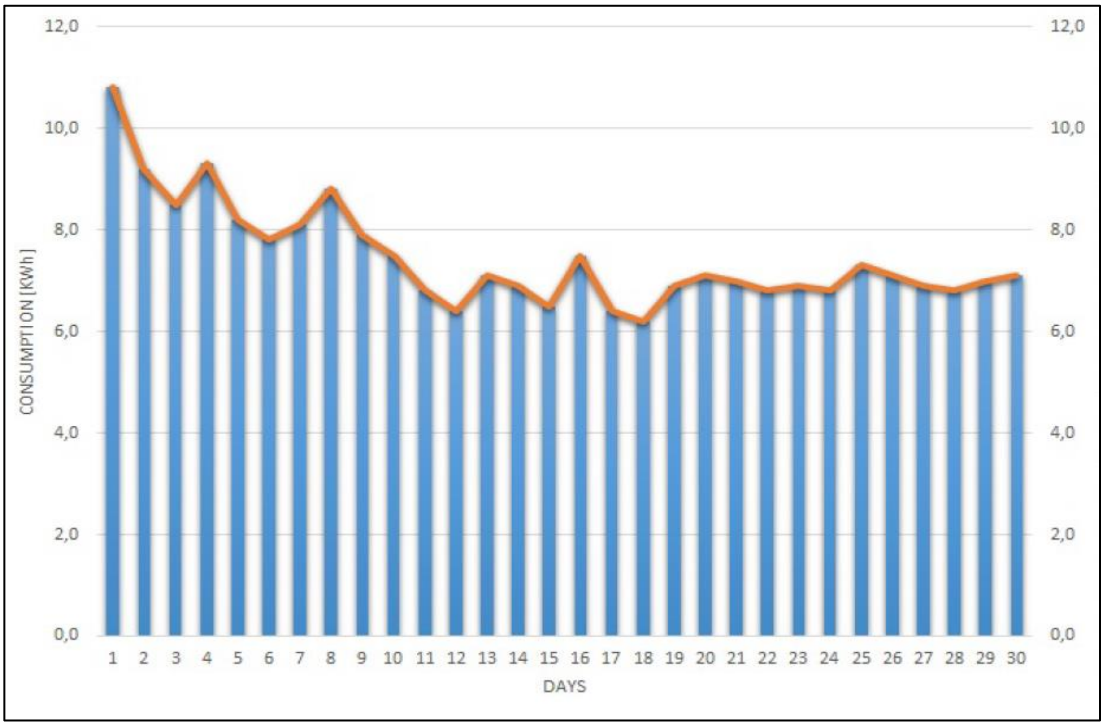


Figure 6.1 – Monthly energy saving for a common family composed of four adult people.

6.2 Energy-efficient communication for battery-powered IoT devices

According to the network topologies discussed in Chapter 5, first the star network was implemented and tested. This configuration provides the systems with good communication and data transfer performances in terms of reliability and response of the system but the problem is the high energy consumption due to Wi-Fi interfaces on the market that are not optimized for battery-powered devices so energy consumption is higher than other low power interfaces such as Bluetooth Low Energy or ZigBee. The response time of the system, defined as the difference of time between the timestamp of generated command from the Application Layer and the timestamp of received command to the Controlled Layer, in this scenario it is approximately 5 sec. The message flow in star topology is described in Figure 6.2:

(1) generation of command from the Application Layer (for example turn on the air conditioner of the kitchen);
(2) receiving command to the Service Layer through HTTP protocol;
(3) data capture of the command from the Service Layer by the Controlling Layer through the Wi-Fi interface;
(4) processing data with Controlled Layer sending ack to Service Layer through the Wi-Fi interface;
(6) sending ack to Application Layer through HTTP protocol.

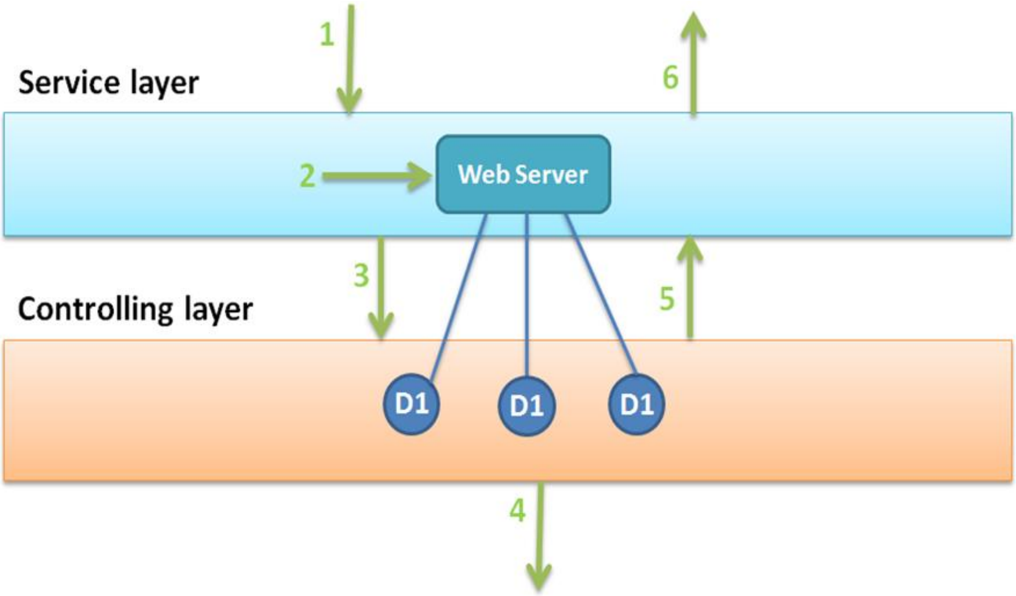
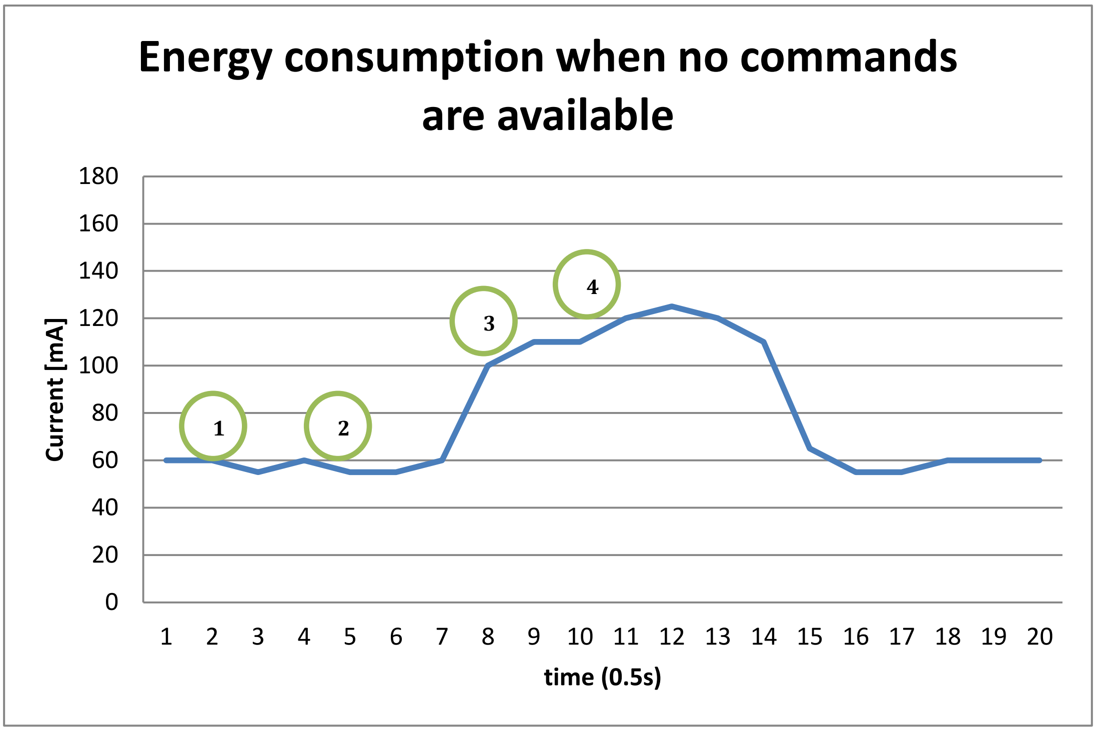
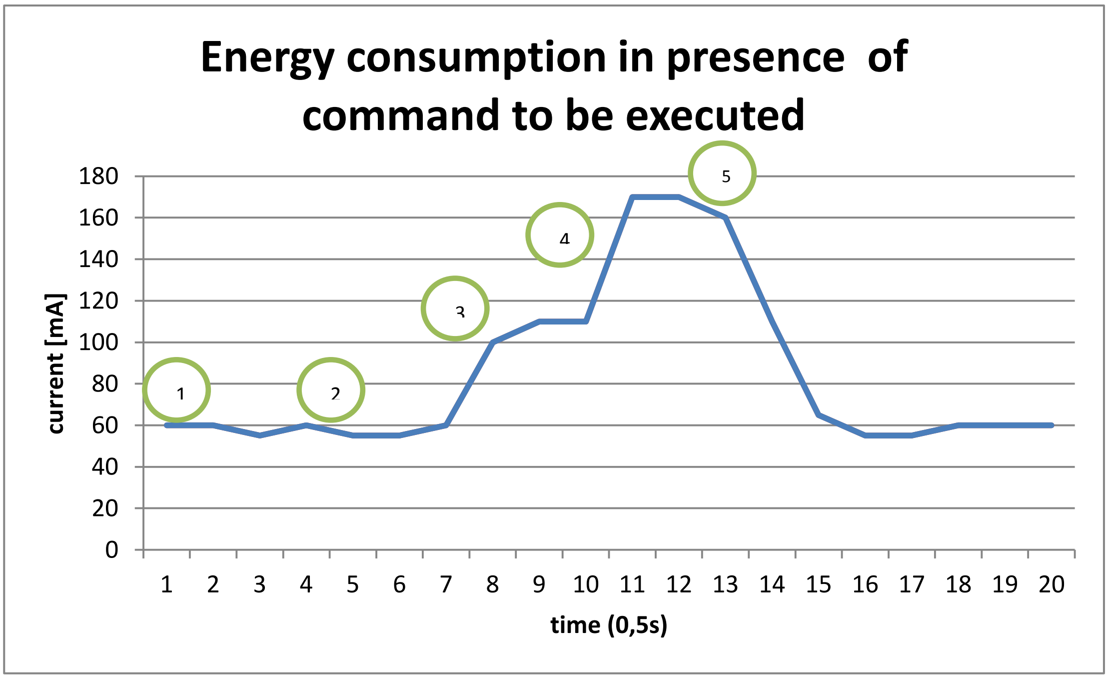


Figure 6.2 - Message flow in star topology.

Commands are sent by invoking the REST Web Services provided by the Service Layer through the HTTP protocol. The command contains the identification of the actuator that is placed in the Controlled Layer and a coded message in the HTTP body that contains the command to be executed (turn on the air conditioner is coded in a integer value). In Figure 6.3 the energy consumption of $D1$ during communications phases is shown. Energy consumption is higher when some commands need to be processed.



(a)



(b)

Figure 6.3 - Energy consumption of D_1 during communication phases when no commands are available (a) and in presence of commands to executed (b).

To break down Wi-Fi energy limitations and give the system the possibility to manage and execute more commands, the Cluster/Tree network topology was implemented. $D3$ acts as a master and $D2$ acts as a slave of $D3$. $D3$ communicates with the Service layer through Wi-Fi interface and pass possible commands to $D2$ through an RF interface. $D3$ is assumed to be plugged in to the energy supply whereas $D2$ is powered with batteries. The message flow in tree/cluster topology is described in Figure 6.4.

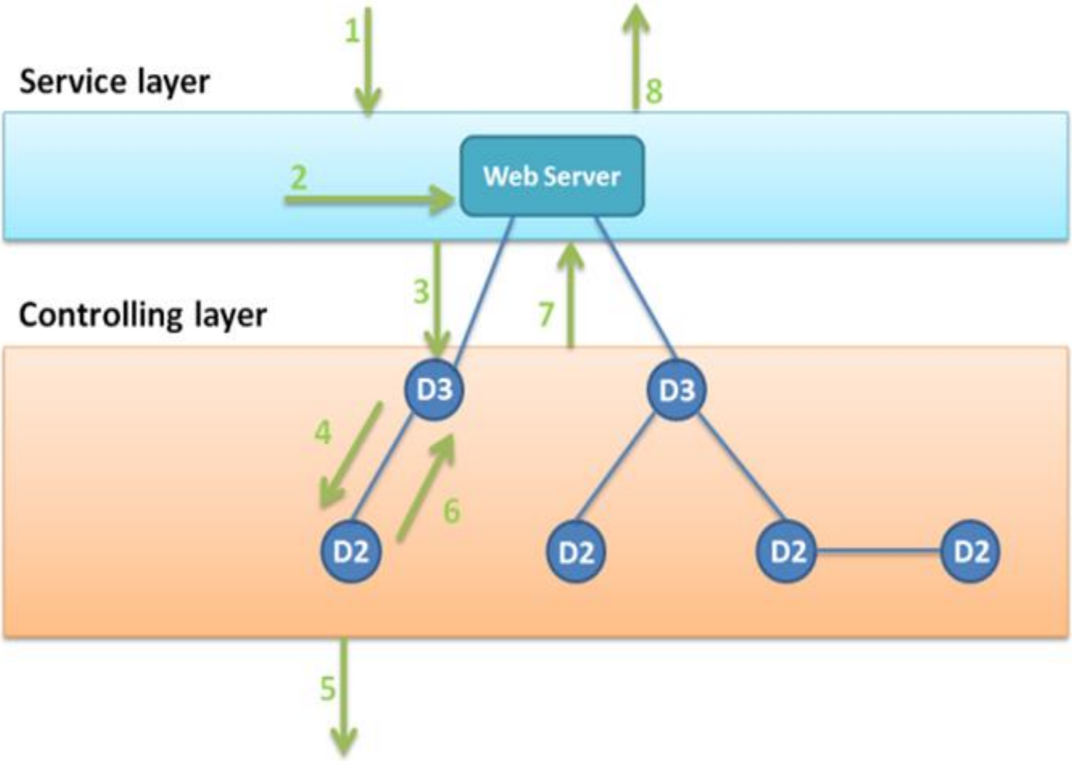


Figure 6.4 - Message flow in Cluster/Tree topology.

(1) generation of command from the Application Layer;
(2) receiving command to the Service Layer with HTTP protocol;
(3) data capture of the command from the Service Layer by the Controlling Layer via Wi-Fi interface;
(4) sending data to slave node through RF interface;
(5) processing data with the Controlled Layer;
(6) sending ack to the master node through RF interface;
(7) sending ack to the Service Layer via Wi-Fi interface;
(8) sending ack to the Application Layer with HTTP protocol.

Different configurations are used for testbeds, in particular, speed of MCU, sleep time, activity time of RF receiver and transmission time of RF transmitter when $D3$ collects some data to transmit to $D2$ were set with different values to create four different scenarios and evaluate energy consumption.

Table 6.1 - Scenarios for testbeds.

Variable	**Unit**	**Scenario1**	**Scenario2**	**Scenario3**	**Scenario4**
RF_TX_ON_if_receives_data	s	6	3	2	1
RF_RX_ON	T = 1 min	Always on	1/2	1/3	1/12
MCU_sleep	T = 1 min	NO	1/6	1/3	11/12
MCU_speed	Mhz	16	8	4	1

Experimental results show that the average time to execute the command (response time) is approximately 5 sec. with low variance in case of perfect network conditions. In Figure 6.5 the duty-cycle of D_3 is shown, where T_ON and T_OFF are respectively on_mode and off_mode time of Wi-Fi Interface.

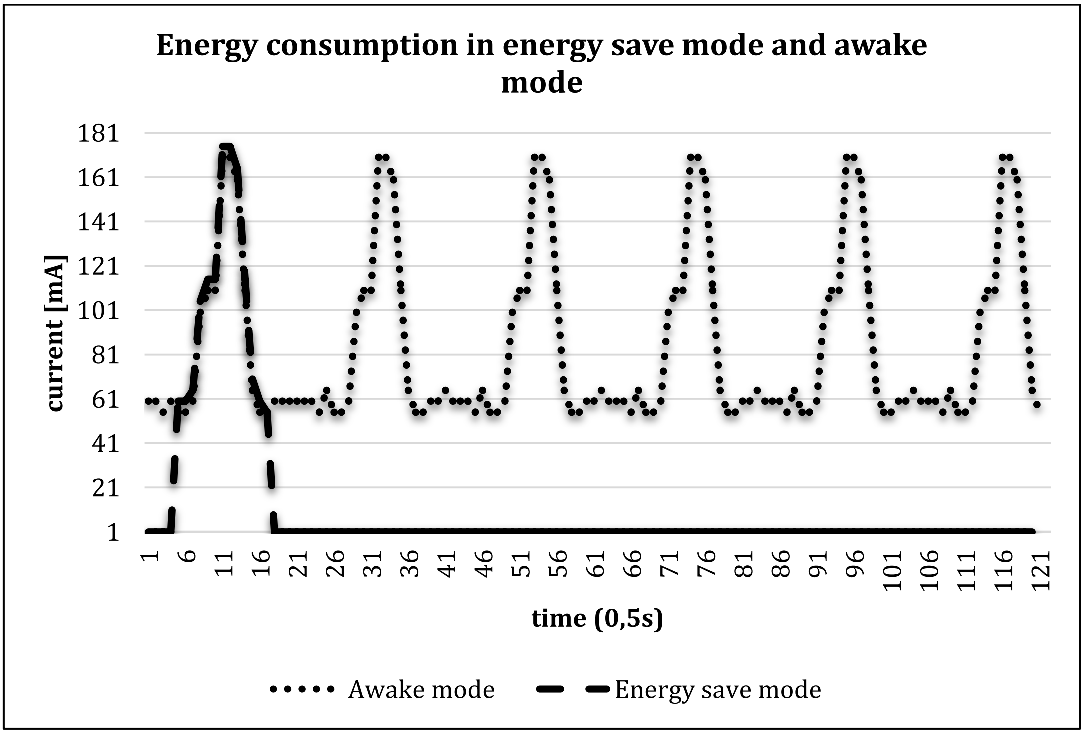


Figure 6.5 - Energy consumption of D_3 in energy save mode and awake mode.

Figure 6.6 shows how energy consumption changes according to the different scenarios listed in Table 6.1.

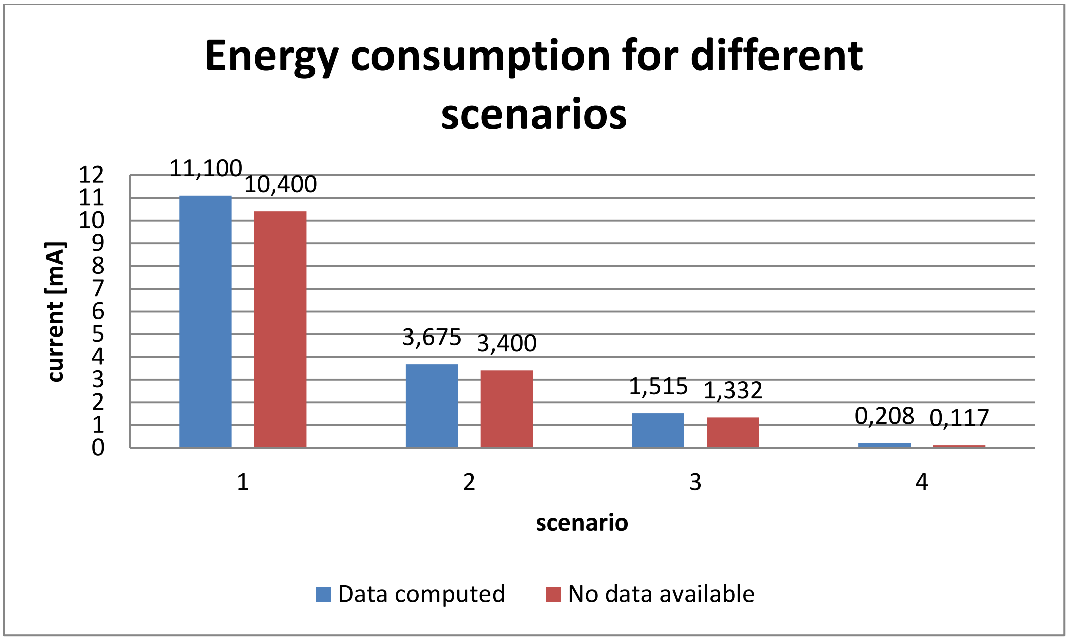


Figure 6.6 – Energy consumption in 4 different scenarios.

Two cases were analysed: a case in which some commands are available to be executed and a case in which no commands are available. Scenario 4 offers the best performance in terms of energy consumption.

A detailed communication model between sensor node and sink node is depicted in Figure 6.7. Sensors nodes observe the environmental status and when some important changes occur, sensing data are sent to the sink node. Sensing data are classified in two types and a threshold is used to establish if sensing data belong to one type or the other:

- **Priority sensing data**: data related to some alerting environment change, for example fire or gas detection. These data need to be immediately sent to the sink node. Sensing data must exceed a threshold to trigger an alerting communication;
- **Ordinary sensing data**: these data are about slight environmental changes, for example when temperature is increased by 0.1°C. This data can be collected by the sensor node and can be sent to sink node periodically (for example every 5 min.) or when the data buffer is full. Ordinary sensing data are under the established threshold.

When the sink node receives priority data, they are sent immediately to the Service Layer. Ordinary sensing data are also collected by the sink node and are sent to the Service Layer node periodically or when the data buffer is full. Users can access monitoring data by using the REST Web Services provided by the Service Layer through HTTP requests. The command inside the HTTP BODY contains the identification of dataset requested.

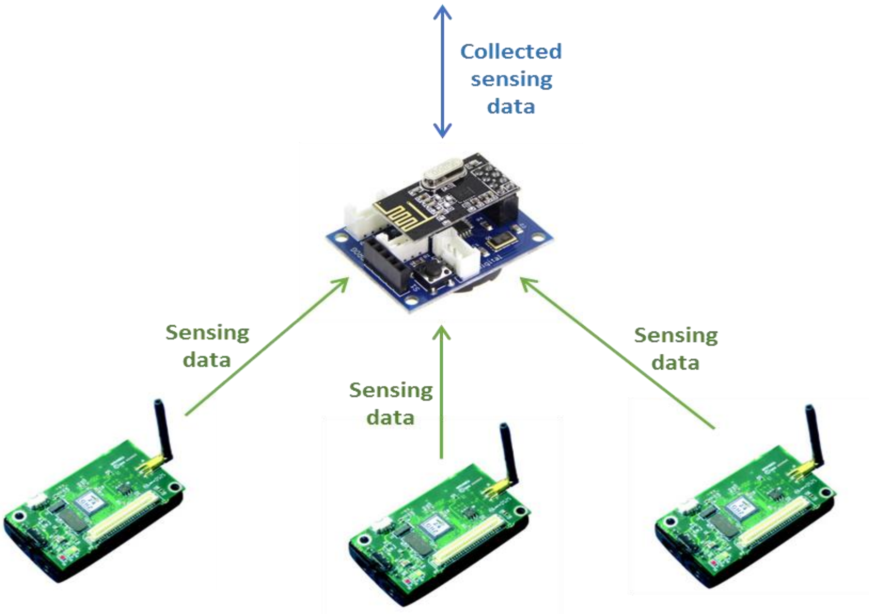


Figure 6.7 - Communication between sensor node and sink node.

Different configurations were used for testbeds, in particular different packet length, different numbers of packets and different values of average energy consumptions. Device energy consumption was analysed during the communication phase. The analysis of consumed current refers to a time interval of 10 sec. Intermediate phases, such as sleep mode, were not analysed in this testbed. Energy consumption of the sink node during Wi-Fi communication with the Service Layer was analysed. Scenarios are described in Table 6.2.

Table 6.2 - Different scenarios during Wi-Fi sink-node communication.

Variable	**Unit**	**Scenario1**	**Scenario2**	**Scenario3**	**Scenario4**	**Scenario5**
Packet length	byte	4096	2048	1024	512	256
Packet	number	4	8	15	30	60
Average Wi-Fi energy Consumption	mA	95	88.33	83.33	82.85	82.61

Figure 6.8 shows the numbers of packets that are sent in a hour assuming a fixed number of bytes per data. Data size corresponds to an assumed node buffer size that is dynamically changed. Increasing of data size involves decreasing of transmission rate. The first bar of the graph represents the first scenario, the second bar represents the second scenario and so on.

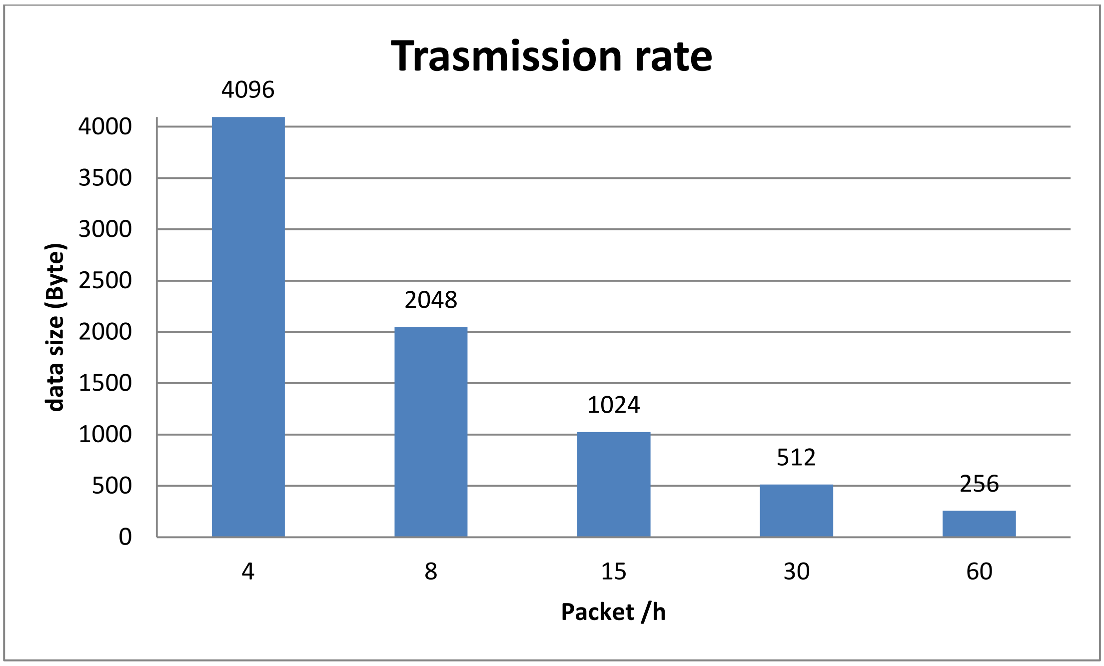


Figure 6.8 - Sink-node trasmisison rate during Wi-Fi communcation.

Sending data with a lower transmission rate involves less energy consumption as shown in Figure 6.9. The linear graph represents energy consumption as a ratio between average consumption in mA of first scenario and the others. Others scenarios are compared with the first because that is the one that consumes less energy in the time interval considered of one hour. Minimum transmission rate is 4 packets per hour; less transmission rate may not offer accurate monitoring data. An increasing transmission rate implies smaller data size that means information is split into more packets. An increasing transmission rate gives the possibility to send data in more packets; therefore, if transmission rate is low it is necessary to increase data size to send as much data as possible since the next transmission will happen not in a short while.

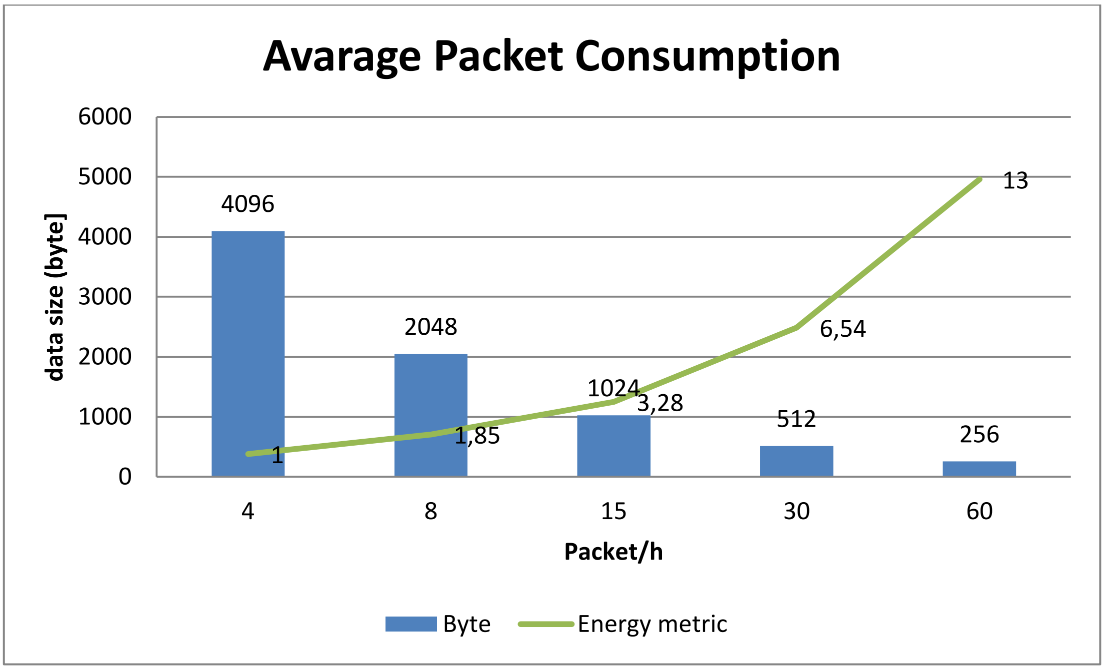


Figure 6.9 - Packets energy consumption during Wi-Fi communication.

Following figures show energy consumption of single packet during Wi-Fi communication using different packet length. Basis for comparison is 1024 byte. The shortest packet length (512 byte) consumes less energy.

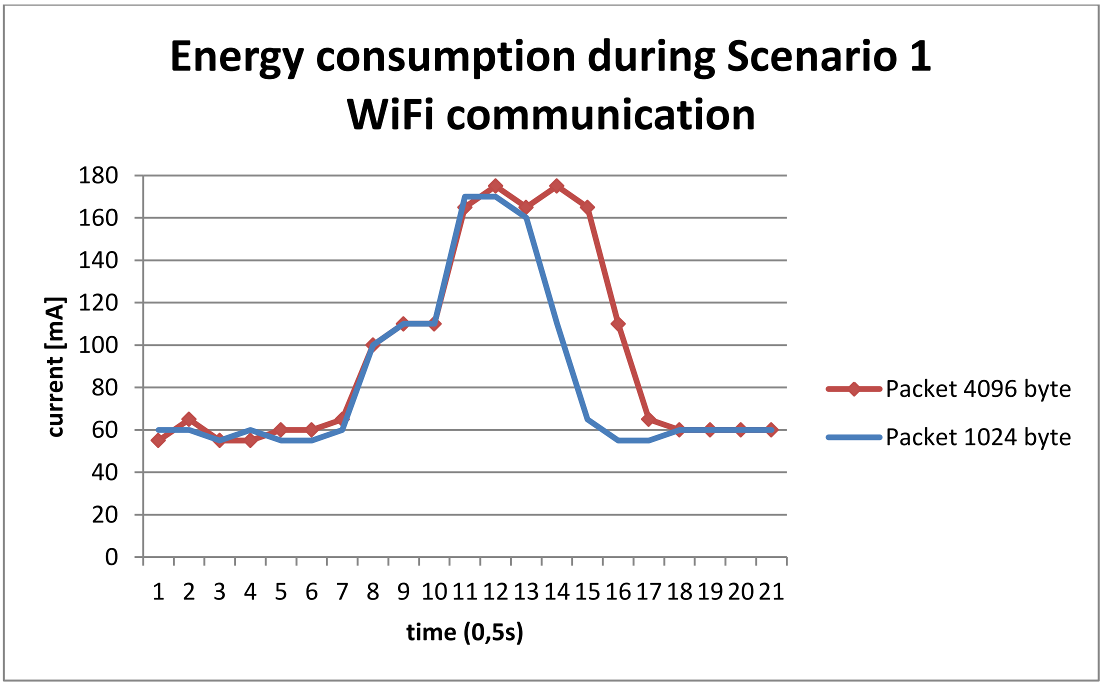


Figure 6.10 – Scenario 1 for Wi-Fi communication.

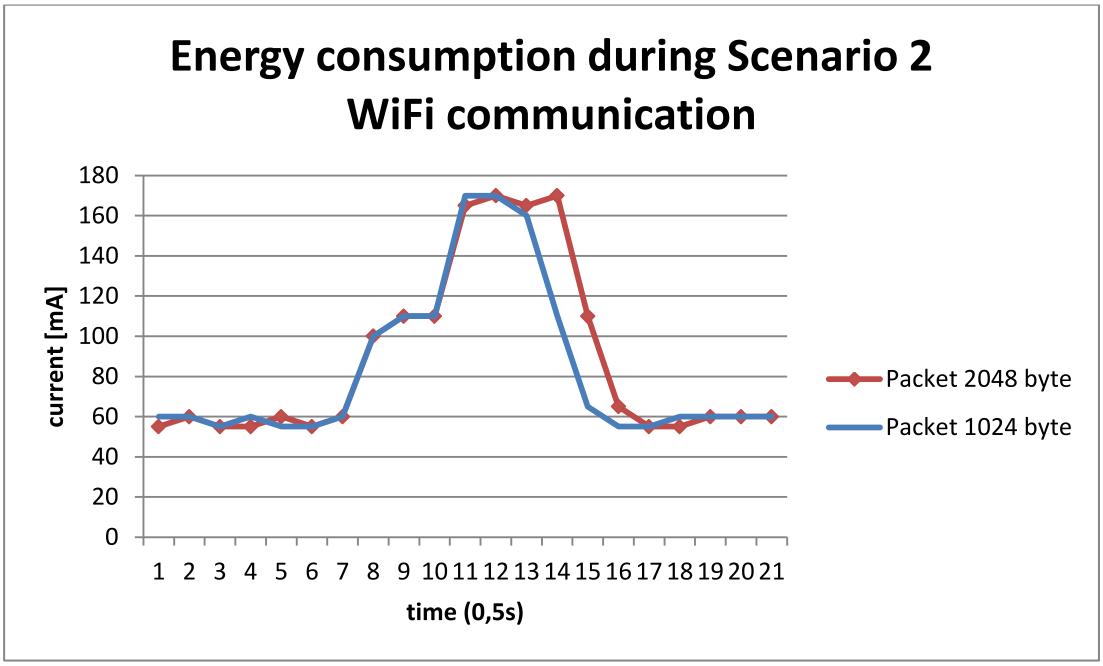


Figure 6.11 – Scenario 2 for Wi-Fi communication.

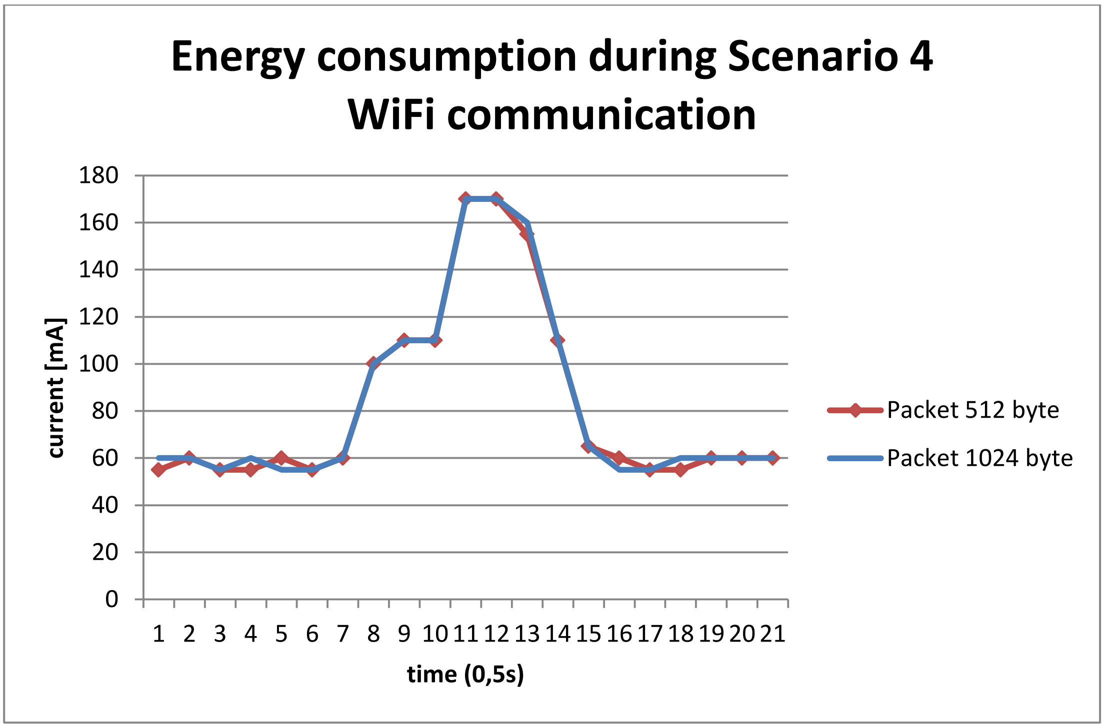


Figure 6.12 – Scenario 4 for Wi-Fi communication.

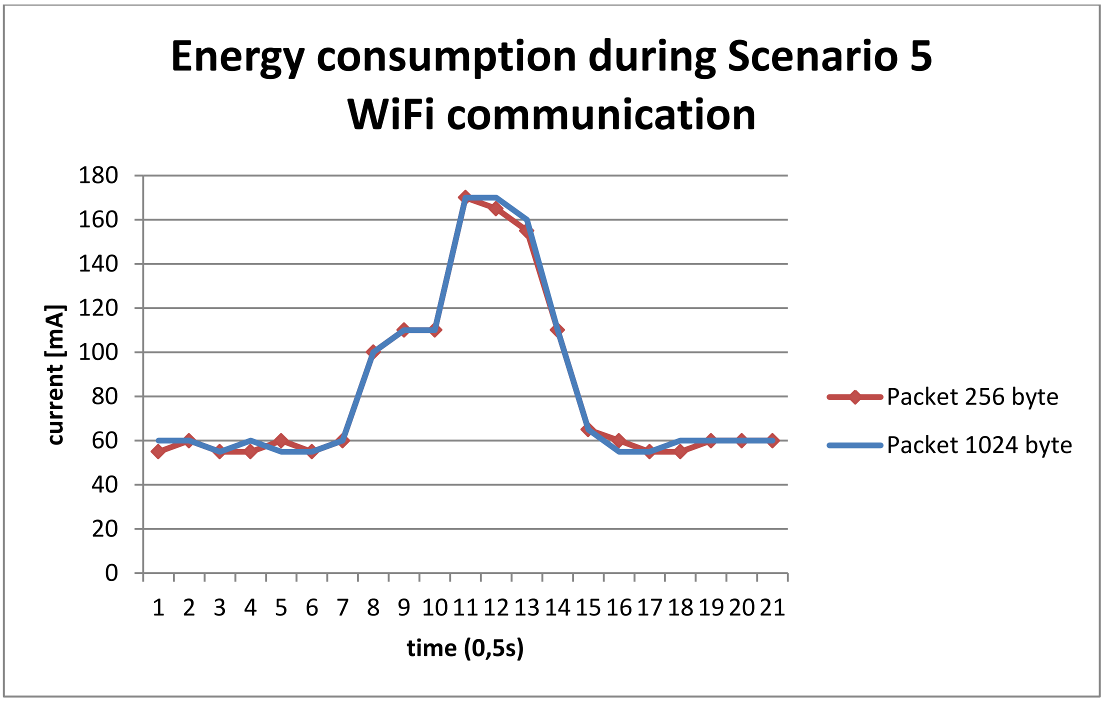


Figure 6.13 – Scenario 5 for Wi-Fi communication.

In this analysis, scenario 5 with 256 bytes consumes less energy. Starting from scenario 1 with 4096 bytes, it can be stated that energy consumption is proportional to packet length but, as depicted in the graphs, the relation is not linear. Scenario 1 is the best configuration for devices. A similar investigation is presented for RF communication. Uninterrupted monitoring and transmission communication is energy expensive, especially if devices are battery powered. The sensor node was implemented with a physical sensor and an RF module on a Low Power microcontroller. Data are received from the MCU and are collected or sent immediately according to data type, priority sensing data or ordinary sensing data. For energy analysis, a time window of 5 sec. was assumed and intermediate phases, such as sleep mode, were not analysed. Variable parameters are listed in Table 6.3.

Table 6.3 – Communication variables for energy analysis.

Variable	**Unit**	**Scenario1**	**Scenario2**	**Scenario3**	**Scenario4**	**Scenario5**
Packet length	byte	256	128	64	32	16
Packet	number	8	15	30	60	120
Average Wi-Fi energy Consumption	mA	3.65	3.486	3.114	3.055	2.958
TX	number	4	4	4	4	4

RF is a broadcast transmission and for reliability reasons, data are transmitted 4 consecutive times. This is because, in our scenarios, RF performs one way communication and no acknowledgment of received data is provided.

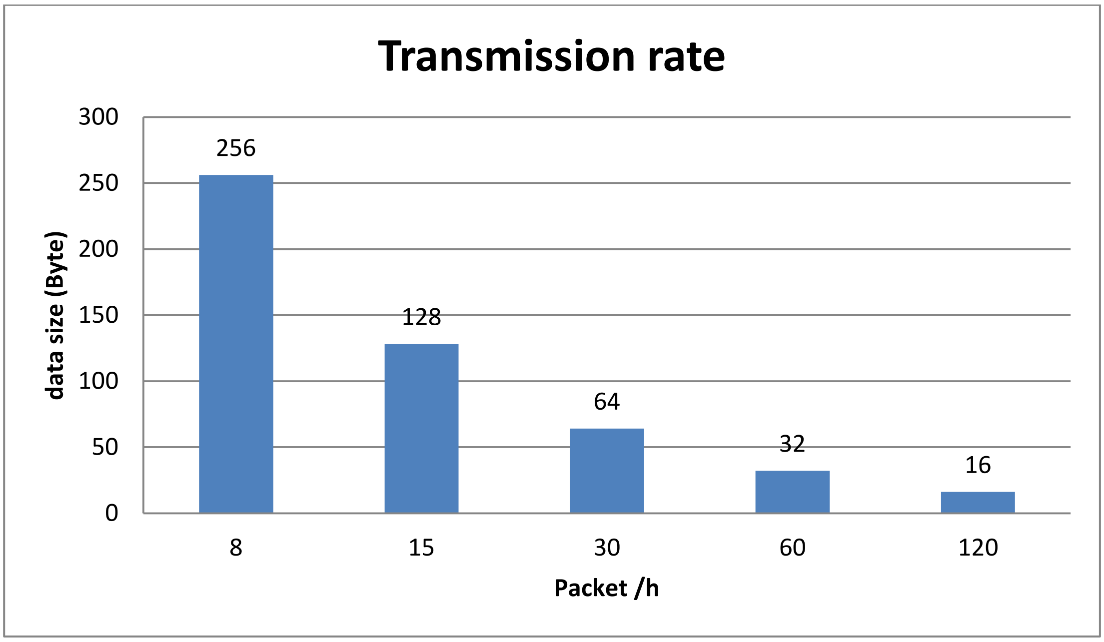


Figure 6.14 - Sink-node transmission rate during Wi-Fi communication.

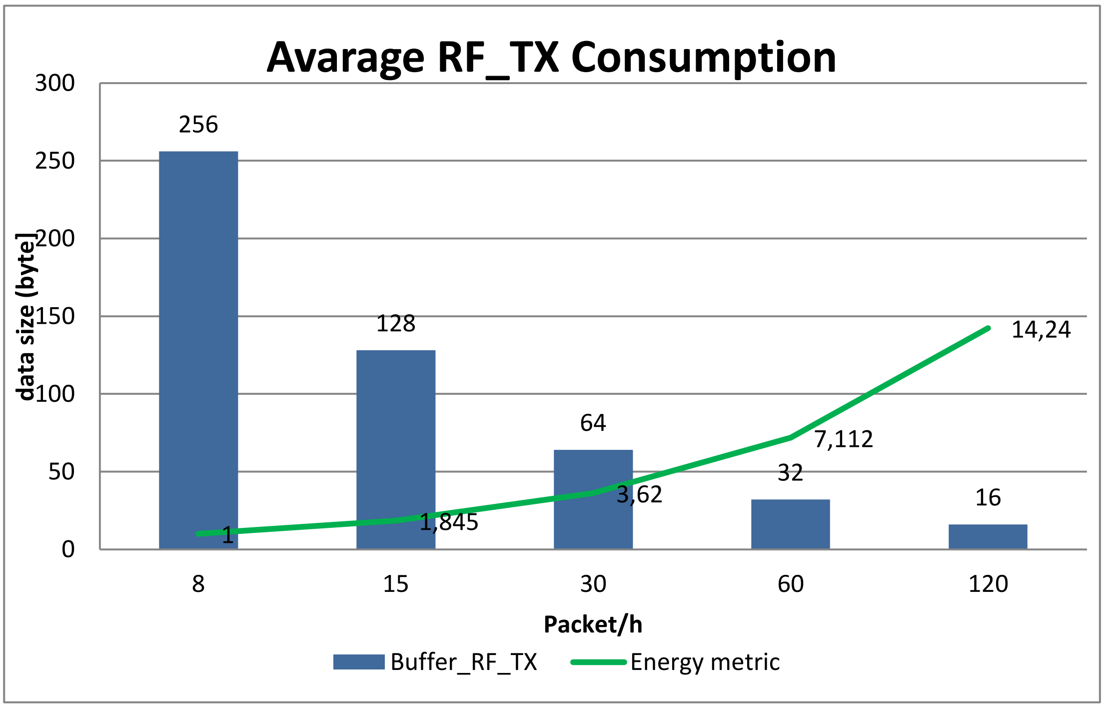


Figure 6.15 - Packets energy consumption during RF communication.

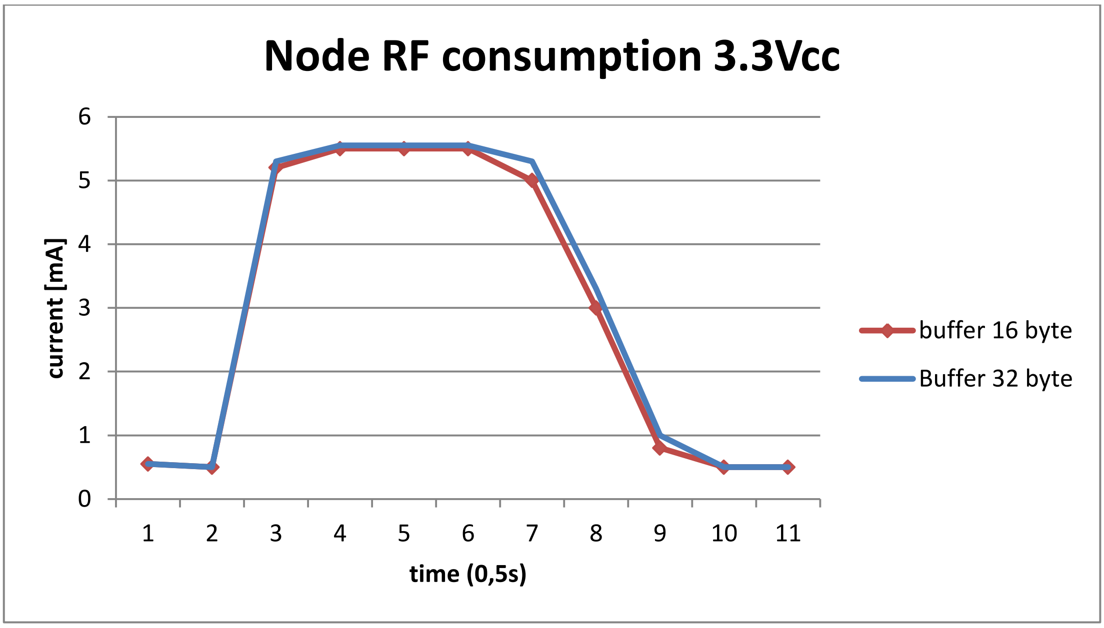


Figure 6.16 - Scenario 1 for RF communication.

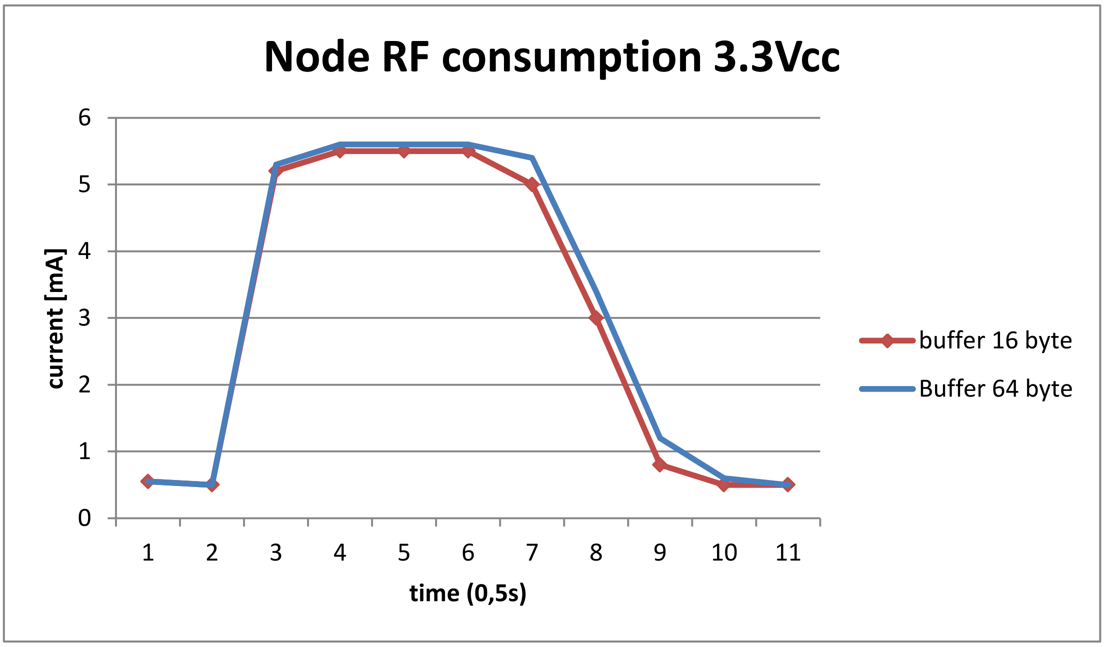


Figure 6.17 - Scenario 2 for RF communication.

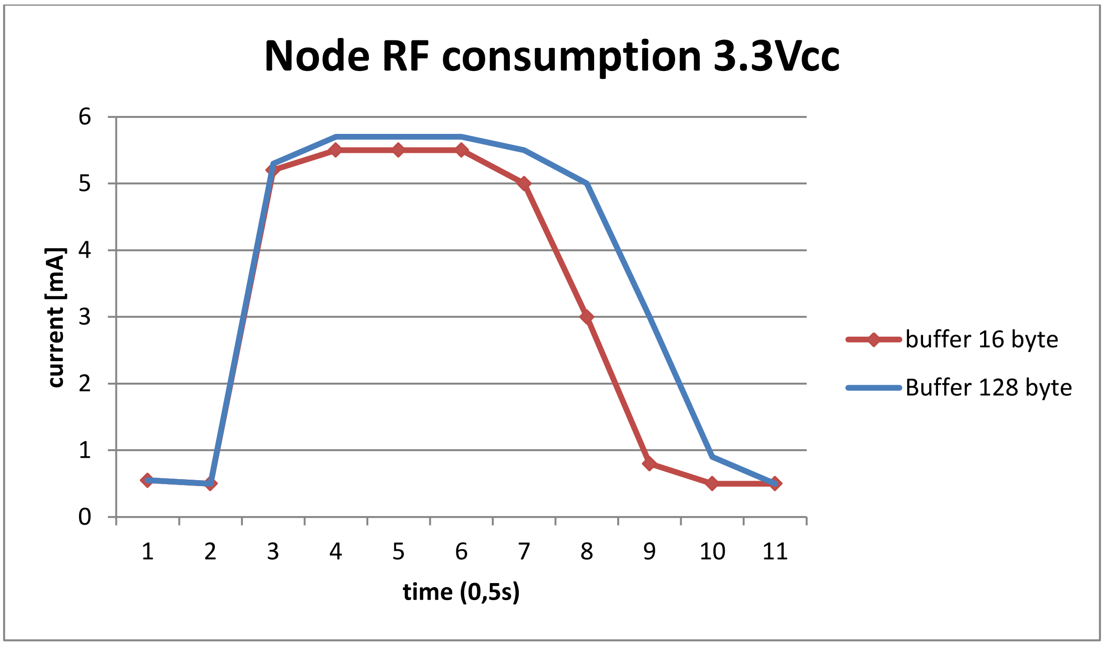


Figure 6.18 - Scenario 4 for RF communication.

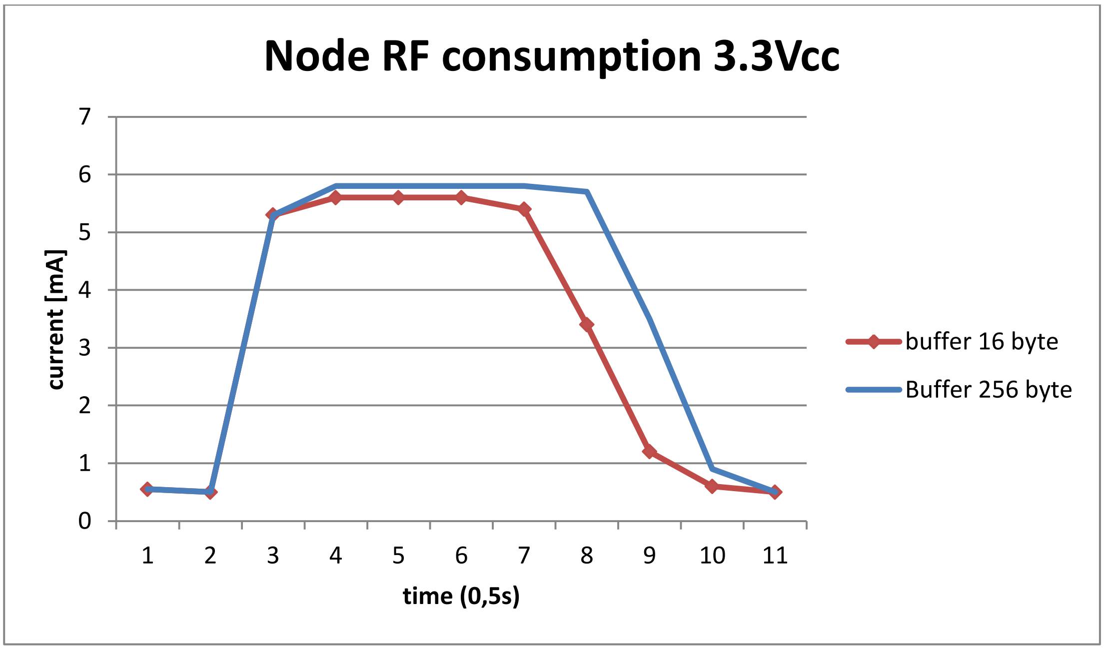


Figure 6.19 - Scenario 5 for RF communication.

In this analysis, scenario 5 with 16 bytes consumes less energy. The analysis is similar to the one presented for Wi-Fi scenarios but there is an important energy reduction. Starting from scenario 1 with 256 bytes, it can be stated that energy consumption is proportional to packet length but, as shown in the graphs, the relation is not linear. Maximum RF data legth is 256 bytes; this value is a good compromise for potential interferences in case of longer trasmission. In case of RF communication, the data buffer is smaller bacause of broadcast and one way communication so no extra controlling data are required; only *CRC (Cyclic Redundancy Check)* is performed. In both Wi-Fi and RF analysis, Scenario 1 is the best configuration for devices and the bigger data size implies less energy consumption, therefore the transmission rate plays an important role in energy optimization.

6.3 Battery life and server-side optimization

In this section, the performance evaluation of the proposed social Wi-Fi communication (Paragraph 5.3) is discussed and related to:

- **Battery lifetime**: to show the longest device's lifetime;
- **Transmission duration**: to show that useless daily transmissions are avoided;
- **Community feedback**: to show the level of comfort and satisfaction for community users;
- **Hourly CPU Server utilization and operations throughout**: to show energy and processing optimization also towards the system Web Server.

Energy parameters and performances are:

- Wi-Fi energy consumption:
  - when no commands are available;
  - in presence of commands to be executed.

The fuzzy algorithm presented in Paragraph 5.3.1 has been implemented in the Service Layer of the architecture described in Chapter 4; every time the device asks the Server for any command to be executed, the algorithm runs and the result is sent to the device so it can update the current requesting frequency. During the requesting phase, sensing data are sent to the Server to be stored and be available for users from Application Layer. The performance of the algorithm has been evaluated in a real scenario with real devices and real users making a comparison between devices with fixed requesting frequency and a social aware device with a dynamic requesting frequency. Four rechargeable batteries of 1000 mAh have been used for the power supply. By implementing the hardware and software design described in Paragraph 5.3, according to empirical results, the device needs on average 4 seconds for sensing and storing procedure and connection setup so the minimum requesting time interval is every 4 seconds. Upper and lower bounds are design variables since they depend on firmware design (according to firmware design sensing, storing and connection, setup could take a longer time then 4 seconds) and user preferences. The maximum allowable delay was set to 30 minutes thus the requesting frequency R_f can assume these values:

$$RF_{low} \le R_f \le RF_{high} \qquad (7)$$

where $RF_{low} = \frac{1}{60 \cdot 30}$ and $RF_{high} = \frac{1}{4}$; this means that $0.0005555 \le R_f \le 0.25$.

To calculate values between 0 and 1, R_f is divided by 0.25:

$$0.002222 \le R_f \le 1 \qquad (8)$$

Energy consumption of the Wi-Fi interface is shown in Table 6.4 :

Table 6.4 - Energy Consumption of Wi-Fi Interface.

Wi-Fi	**Value**	**Unit**
Tx 802.11b,CCK 11Mbps, P.Out = +17dBm	170	mA
Tx 802.11g,OFDM 54Mbps, P.Out = +15dBm	140	mA
Tx 802.11n,MCS7, P.Out = +13dBm	120	mA
Rx 802.11b, 1024 bytes packet length, -80dBm	50	mA
Rx 802.11g, 1024 bytes packet length, -70dBm	56	mA
Rx 802.11n, 1024 bytes packet length, -65dBm	56	mA
Modem Sleep	15	mA
Light-sleep	0.9	mA
Deep-sleep	10	mA
Power Off	0.5	mA

The energy consumption during message flow is described in Figures 6.20 and 6.21.

(1) generation of command from the Application Layer;

(2) receiving command to the Service Layer with HTTP protocol;

(3) data capture of the command from Service Layer by Controlling Layer through the Wi-Fi interface;

(4) processing data with the Controlled Layer;

(5) sending ack to the Service Layer through the Wi-Fi interface.

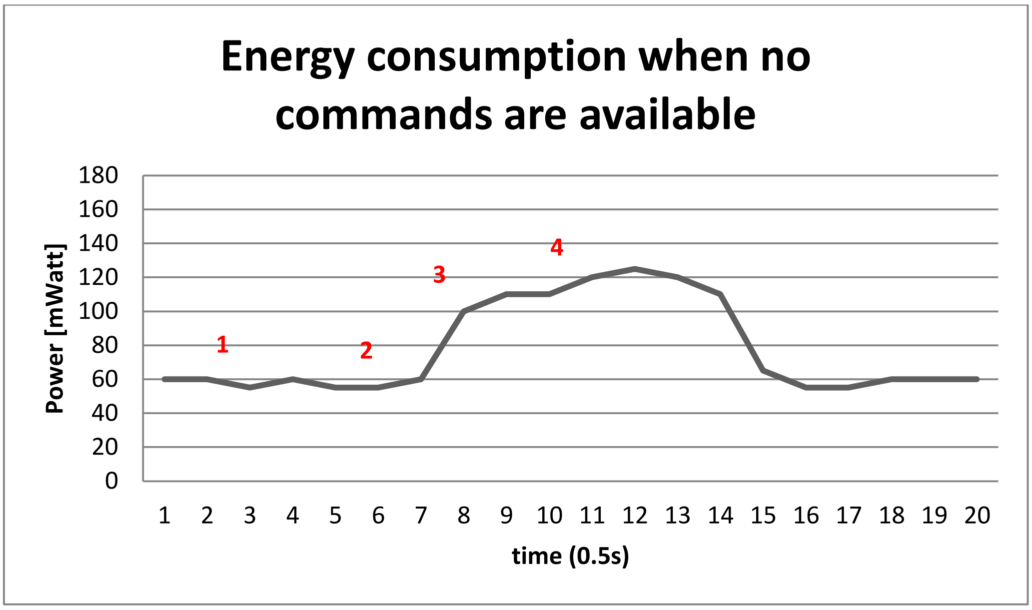


Figure 6.20 - Energy consumption of Social Aware Wi-Fi device during Wi-Fi communication when no commands are available.

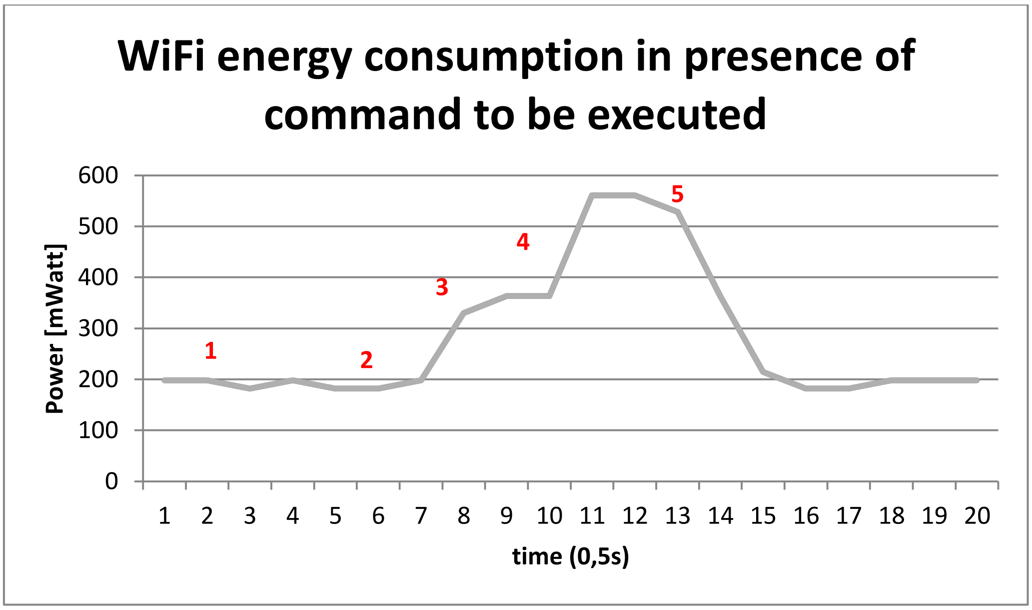


Figure 6.21 - Energy consumption of Social Aware Wi-Fi device during Wi-Fi communication in presence of commands to be executed.

In Figure 6.22 the duty-cycle of a social aware device is shown, both in standard mode, with fixed wake-up frequency and energy saving mode when the Wi-Fi Interface is dynamically turned OFF. Four devices have been installed in three different houses: one with 4 seconds requesting time interval, one with 1-minute requesting time interval, one with 5 minute requesting time interval and one social aware device with a dynamic requesting time interval that is evaluated through a fuzzy-logic algorithm. The fuzzy inputs and output are listed In Table 6.5.

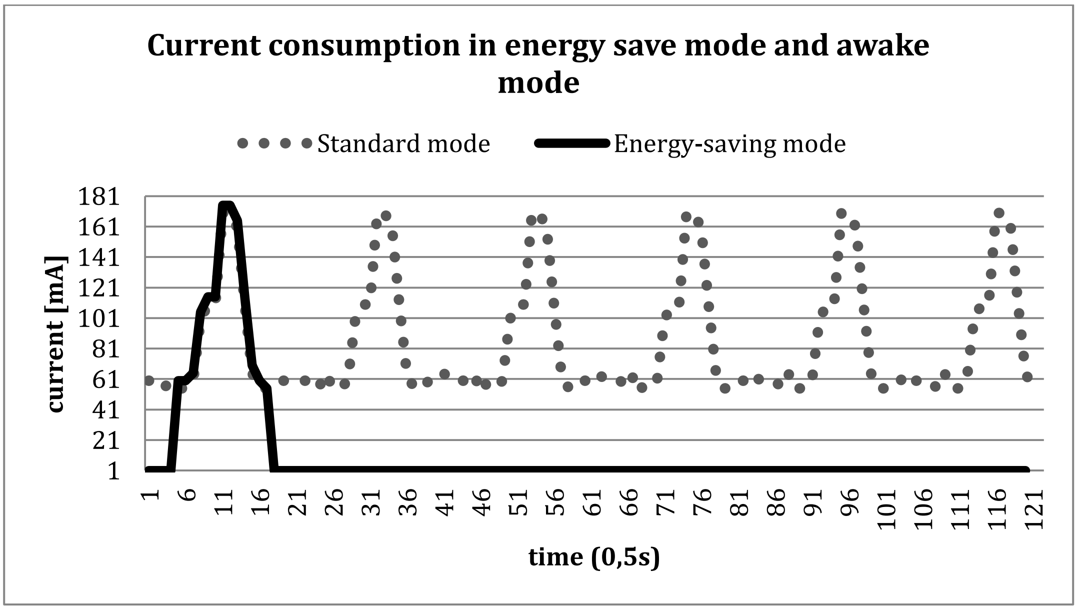


Figure 6.22 - Wi-Fi energy consumption in standard mode and energy-saving mode.

Table 6.5 - Fuzzy Inputs and output parameters.

Name	Formula
Community Context	$C_c = \frac{\sum_{i=1}^{n} IO_i}{n}$
Community Feedback	$C_f = \frac{\sum_{i=1}^{n} fb_i}{n}$
Remaining Battery	$B_i = \frac{B_{i\%}}{100}$
Community Interaction	$I_i = \frac{\sum_{i=1}^{n} cmd_i}{60}$
Requesting Frequency for Social Aware Device	$R_f = \frac{\sum_{i=1}^{n} O_i * C_i}{\sum_{i=1}^{n} C_i}$

Battery lifetime is correlated to the Server requesting frequency. Lower requesting frequencies correspond to longest battery lifetime. The dynamic server allows for the correlaring of battery lifetime to the daily mean requesting frequency and so to the hours in which device turns the Wi-Fi interface on and hours in which sleep mode is active.

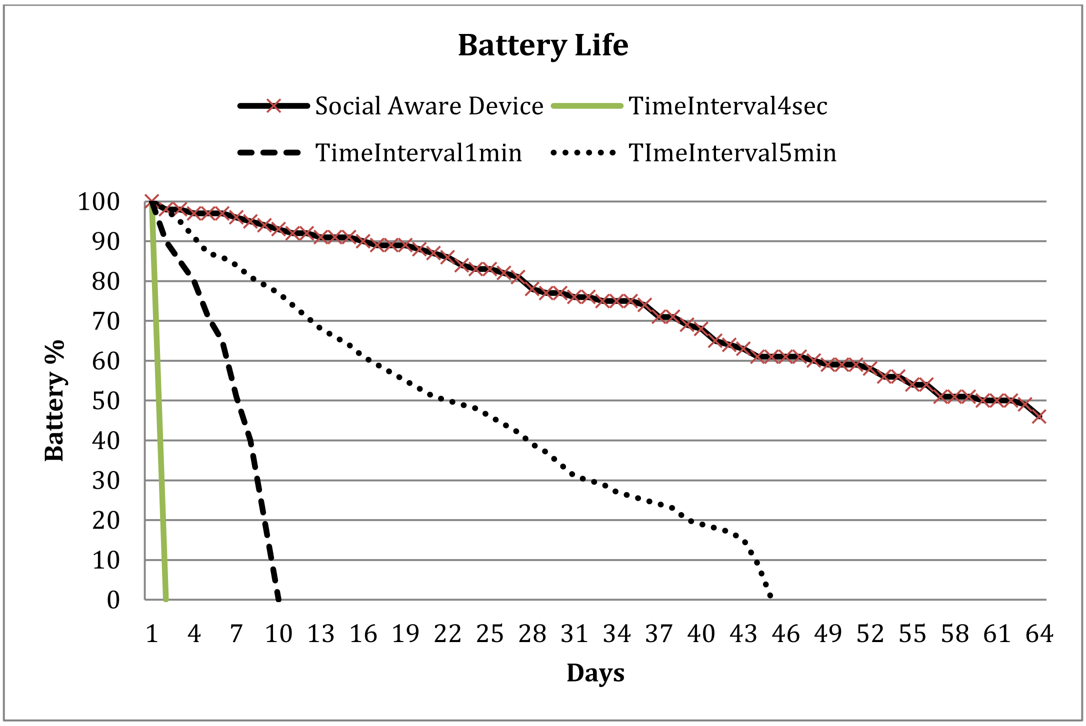
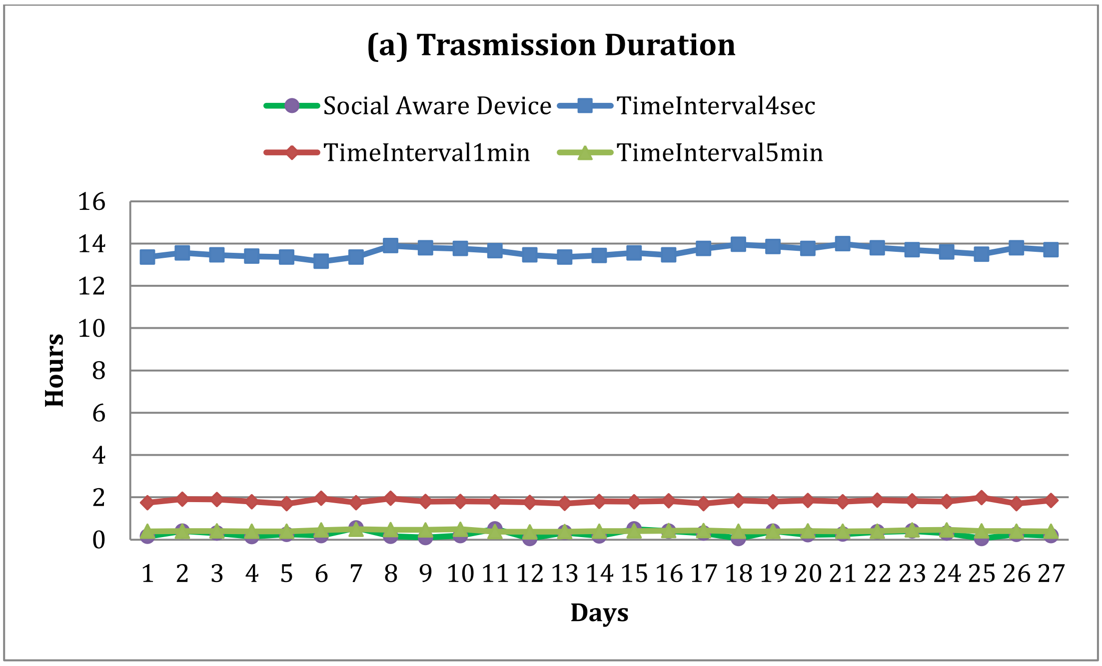


Figure 6.23 - Battery lifetime of Social-Aware Wi-Fi device.

In Figure 6.24, in case of fixed requesting frequency, the transmission time is approximately constant and some slight changes occur according to the numbers of commands to be executed that are inserted in the HTTP/HTTPS response: the more the commands, the more is the time that the connection is kept alive. In case of social aware devices, transmission duration lines fluctuate between different values but, on average, the mean time line lays under the Time Interval 5 min mean time line and this proves the longest battery lifetime. The maximum allowable delay was set to 30 minutes (the time between one request and the following) so, in the case of dynamic requesting frequency, a request can be performed every 30 minutes, especially when nobody is at home and community interaction is low.



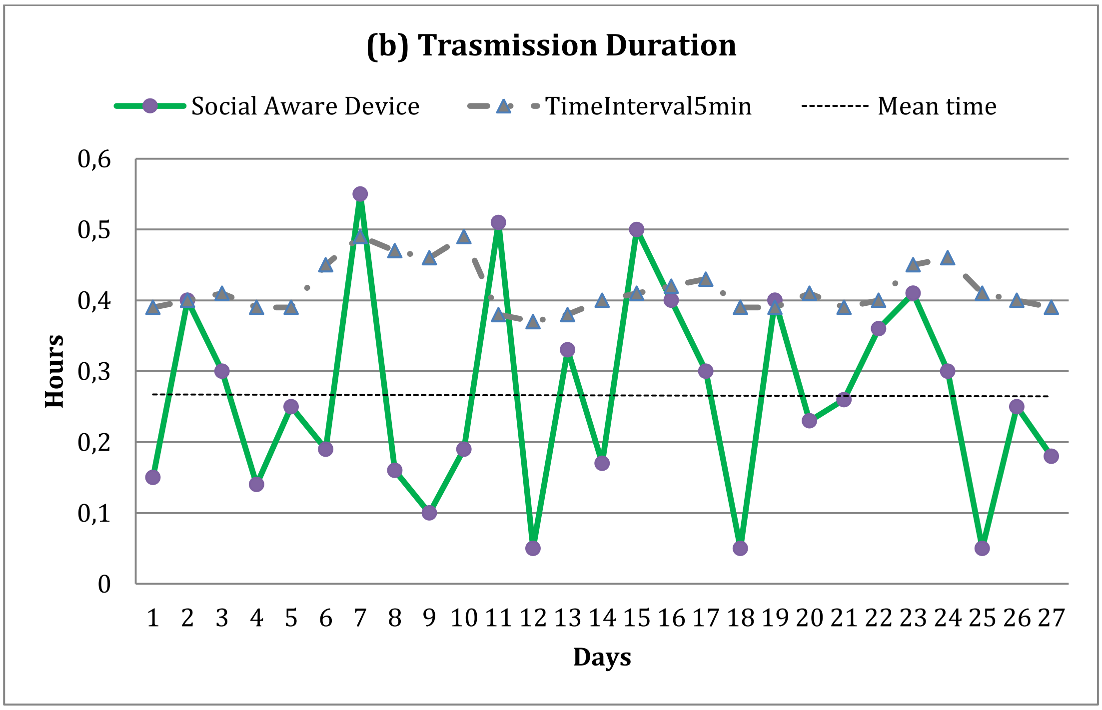


Figure 6.24 - Transmission duration.

The server's workload and capacity have been evaluated according to the related tasks carried out from the Web Server of the Service Layer. There are three variables that form the basic model of system capacity:

- **Observation time (T)**: the amount of time that the server is monitored for activity;
- **Busy time (B)**: the amount of time that the server was active during the observation time;
- **Completions (C)**: the number of transactions completed during the observation period.

Using these three variables, the most significant values have been calculated to develop a capacity planning model. On average, the Server takes 5 seconds to complete a request.

Table 6.6 - Energy variables of capacity planning model.

Variable	Description	Formula
CPU Utilization	The percentage of CPU capacity used during a specific period of time.	U = B/T
Transaction throughout of the system	The average number of transactions completed during a specified period of time.	X = C/T

Figures 6.25 and 6.26 show energy and processing optimization also towards the Web Server of the Service Layer: hourly CPU utilization and transaction throughout drastically decrease in the presence of social aware devices.

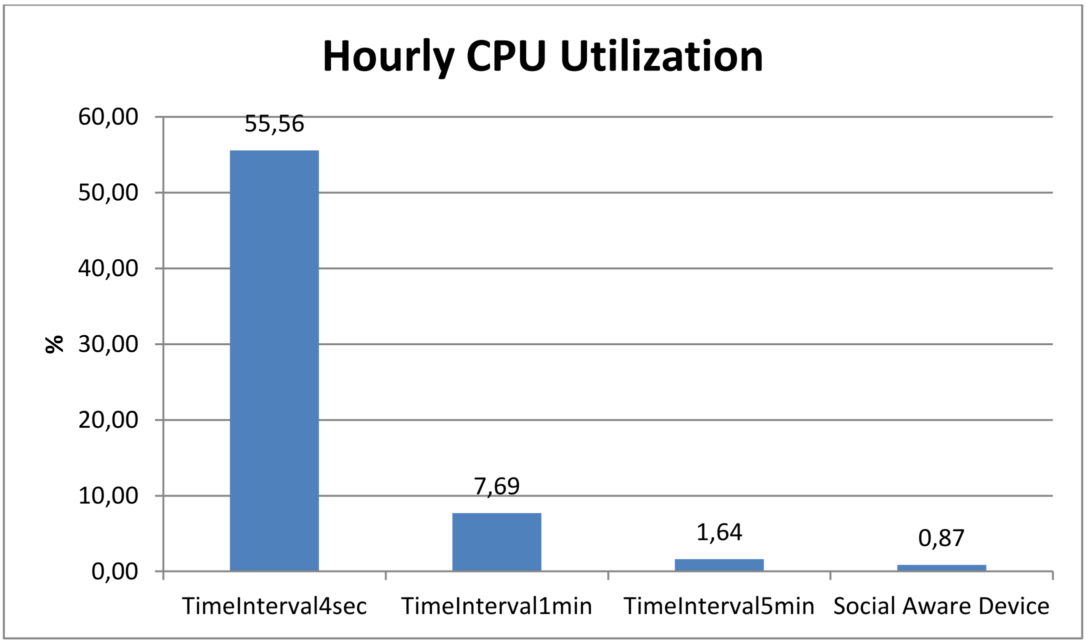


Figure 6.25 - Hourly CPU Server Utilization.

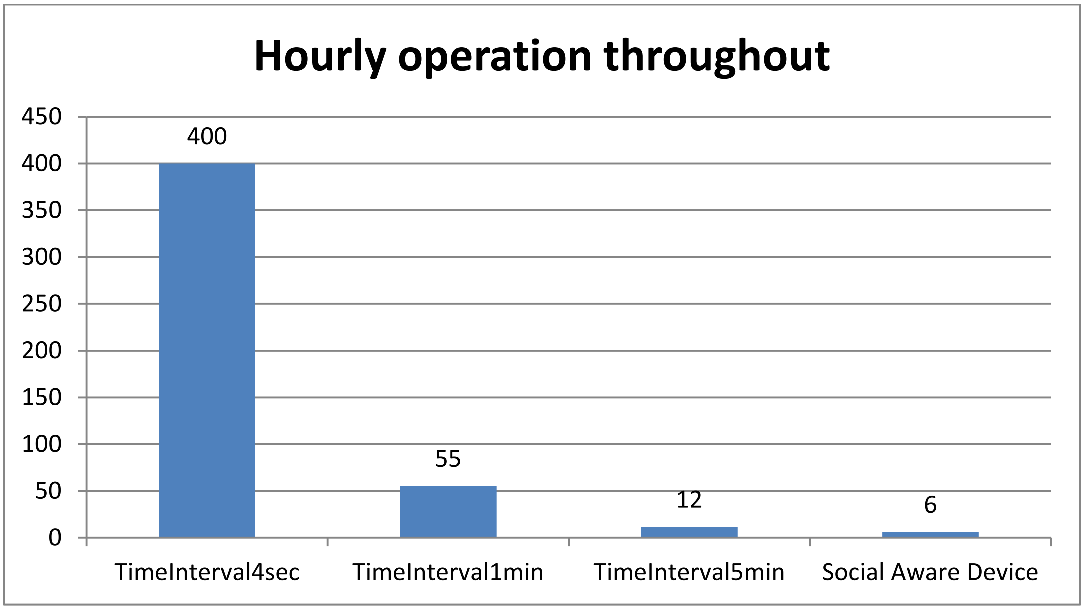


Figure 6.26 - Hourly operation throughout of the Web Server.

Figure 6.27 shows that community feedback is always kept high, sometimes it drops but on average is between 0.78 and 0.91 and this means that the new requesting frequency matches users' expectations rather well. In case of high requesting frequency, most of the requests are useless since, in most cases, the response contains no commands to be executed; using this new approach, it is more likely that a command will be received after a request. On average, community feedback increases with the passing of the days and this means that the algorithm gradually adapts to the users' behaviour and acts according to the users' expectations.

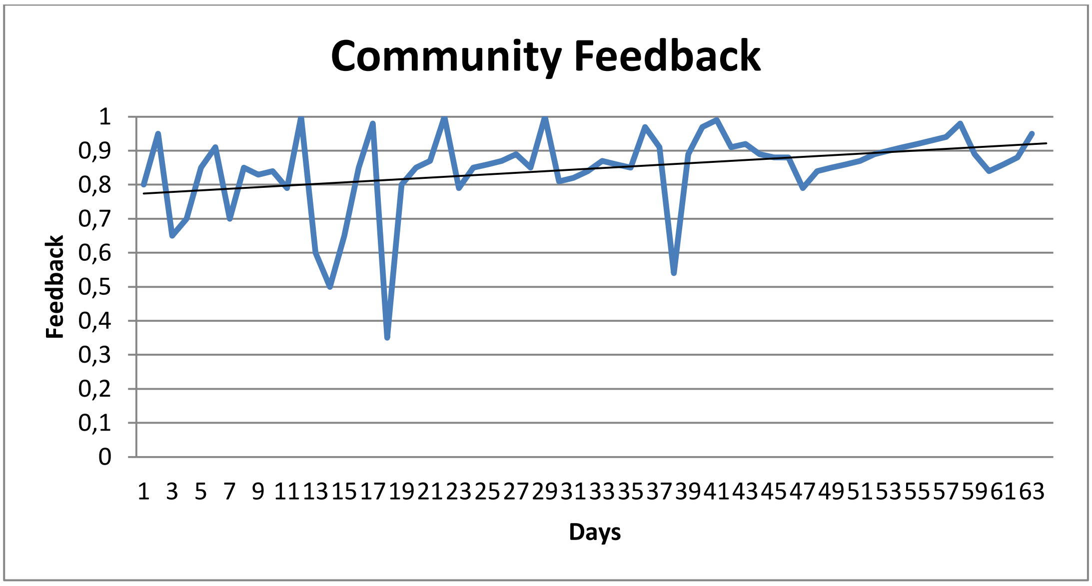


Figure 6.27 - Community feedback.

Conclusion

One of the main objective of this thesis was to design and develop e very user-friendly automation system with ready-to-use smart devices that allow users to interact with their house and be aware of energy waste. In order to evaluate system performances, a testbed based on typical use of appliances in a common home environment was set up. A typical family unit was assumed as consisting of four people that would like to benefit from an Automation System and control the lighting and heating systems of the house. The main goal of the basic architecture system was to create an easier control of smart devices through a user-friendly driving application that exploits the modern technologies to allow communication among central control unit, smart devices and users. The design and development of this framework was based on the intent to raise awareness to users about energy consumptions, showing the waste of energy during the day. According to experimental results, users after a learning time about all features and advantages can be taken from the system, they are encouraged to adopt better behavior in term of energy consumption, avoiding wastages and saving energy and money. The learning time and the slope of the trends demonstrate that users can take advantages from useful tools that help them to perform the best actuation by consulting information containing real-time energy consumption. They become aware how small changes in their behaviors can reduce energy waste. Moreover, using a multi-layer Service Oriented Architecture allowed for the achievement of a high degree of interoperability between different software and smart devices avoiding direct implementation of service-oriented features devices' side. Considering a future commercialization of the system, having a modular architecture with layers would make it possible to entrust the Application and Service Layers to some Service Provider while the Controlling and Controlled Layers could be installed at the user's home. Another commercial solution could regard the installation of the Service and Application Layers at the user's home. The commercial solution will depend on the adopted marketing policies. Experimental results showed that if users are aware of their energy consumptions and have the possibility to control some household devices, after a training period, they can save up to 20% on energy bills and correct misconduct about energy consumptions.

Experiments on the proactive system were made with the collaboration of volunteers in an environment where the system was installed. Results of the system that is able to automate many actions that usually are manual, showed a high degree of comfort and reliable speech recognition. Experiments have also shown that adding the human speech as an input to the system, the choice of the automatism becomes more accurate. One of the objective of these tests was the evaluation of the system sensibility in different scenarios considering ambient noises and other kind of disturbs such as normal human activities and background speech. The results showed the system needs to recognize master speech with a certain quality to have a good percentage of success in speech recognition. Future works could provide for speech, from the Controlling Layer to the Service Layer, to be coded as VoIP data-stream using a VoIP client-server architecture. This approach could certainly open doors for the development and integration of new services with great potentials for new distributed application and Network Layer protocols. Of course the *Quality of Service (QoS)* and *Quality of Experience (QoE)* have to be guaranteed by the networking in order to reach a good *Mean Opinion Score (MOS)* level. This will allow the correction of users' recognized speech also when it comes from a remote position. IoT devices have been designed using open source technology with multiple communication interfaces, such as Wi-Fi and RF, to communicate directly with a Web Server or to communicate only with a special device that acts as a bridge between IoT devices and the Web Server with Wi-Fi and RF interfaces. During the testbed, a sensor node was designed for monitoring application; sensor data were transmitted via RF to a sink node that was designed with RF and Wi-Fi interfaces to communicate with both sensors and the Web Servers. Communication parameters were changed according to different scenarios in order to obtain the most benefits in terms of energy cost and battery life. Through experimental results, specific configurations of devices both for Wi-Fi and RF communications were discovered to obtain the best energy optimization and reduce energy consumption. A nonlinear relation between data size and transmission rate was also discovered; bigger data size implies a lower transmission rate and a lower energy consumption; therefore, the transmission rate plays an important role in energy optimization. A real "Inferactive" System was implemented by extending the basic reactive architecture in order to evaluate the level of comfort and satisfaction for users about proactive automations. Four real devices were installed in a home environment to control the lighting and the heating systems. The results show that during the day, user feedback is always kept high, sometimes it drops but on average is between 0.78 and 0.91 and this means that proactive commands match users' expectations with a fair degree of success. The connection between the Internet Of Things and the Cyber-Physical Systems was explored, in particular the connection with Smart Homes and Automation Systems. The evolution from Reactive to Proactive Automation System was examined, focusing on the reasons why some users might not appreciate some proactive actuations. To take a step towards designing a system that can match every kind of user's needs and requirements, the *Human-feedback-in-the-loop* concept was introduced besides the idea of an "*Inferactive*" system which is able to learn from the user's context and feedback history in order to adapt itself to always up-to-date users' expectations and keep the rules for triggering smart actuations constantly updated. Finally, the design and implementation of Wi-Fi sensors and actuators were presented as a social IoT solution for Home Automation Systems where devices are socially connected to Internet and can communicate through social applications like Facebook, Twitter or Google+ with community users that usually interact with that device. A fuzzy-based solution was proposed to classify the social community interaction with the system in order to implement an adaptive energy saving mode for social Wi-Fi devices according to users' current context, behavior, habits and feedbacks. Test and performance evaluation regarding energy consumption and efficiency in a real world scenario with real hardware devices showed the efficiency of proposed dynamic requesting frequency compared with the fixed requesting frequency solution in terms of electricity consumption, battery lifetime and increase of comfort and satisfaction levels for community users. The proposed solution also produces a good processing optimization towards the Web Server of the system reducing CPU utilization and number of operations per hour.

References

[1] K. Ashton, "*That 'Internet of Things'*" 22 June 2009. http://www.rfidjournal.com/articles/view?4986.

[2] Gartner, *"Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020*" Gartner, 12 December 2013. http://www.gartner.com/newsroom/id/2636073.

[3] Cisco, "*Connections Counter: The Internet of Everything in Motion*", Cisco's The Network, Cisco, 29 July 2013. http://newsroom.cisco.com/feature/1208342/Connections-Counter-The-Internet-of-Everything-in-Motio_2.

[4] EMC & IDC, "*The Internet of Things: Data from Embedded Systems Will Account for 10% of the Digital Universe by 2020 | The Digital Universe of Opportunities: Rich Data and Increasing Value of the Internet of Things*" EMC & IDC, April 2014. http://www.emc.com/leadership/digital-universe/2014iview/internet-of-things.htm.

[5] G. E. Moore, "*Cramming More Components onto Integrated Circuits*" [Online]. http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf.

[6] Intel, "*Intel Chips*" 7 December 2013. http://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/history-intel-chips-timeline-poster.pdf.

[7] J. G. Koomey, S. Berard, M. Sanchez and H. Wong, "*Assesing Trends In The Elecritcal Efficiency Computation Over Time*" 2009.

[8] K. Ashton, "*Kevin Ashton. The Internet of Things. Seoul, June 19, 2014 - YouTube*", 19 June 2014. https://www.youtube.com/watch?v=xSYkp8_Dn2E.

[9] Postscapes, "*Internet of Things Definition- Postscapes*", Postscapes. http://postscapes.com/internet-of-things-definition.

[10] O. Vermesan and P. Friess, "*Internet of Things - From Research and Innovation to Market Deployment*", Aalborg Ø: River Publishers, 2014.

[11] ITU Telecommunication Standardization Sector, "*ITU-T Recommendation database*" 2012. http://handle.itu.int/11.1002/1000/11559-en?locatt=format:pdf&auth.

[12] Postscapes, "*Internet of Things Examples - Postscapes*". http://postscapes.com/internet-of-things-examples/.

[13] Bigbelly, "*Bigbelly*" 2015. http://bigbelly.com/.

[14] Tschofenig, H., et. al., “*Architectural Considerations in Smart Object Networking. Tech*”, no. RFC 7452. Internet Architecture Board,Mar. 2015. https://www.rfc-editor.org/rfc/rfc7452.txt

[15] http://www.bluetooth.com and http://www.bluetooth.org

[16] http://www.z-wave.com

[17] http://www.zigbee.org

[18] Duffy Marsan, Carolyn. "*IAB Releases Guidelines for Internet-of-Things Developers*" IETF Journal 11.1 (2015): 6-8. Internet Engineering Task Force, July 2015. https://www.internetsociety.org/sites/default/files/Journal_11.1.pdf

[19] “*Meet the Nest Thermostat | Nest*” Nest Labs. Web. 31 Aug. 2015. https://nest.com/thermostat/meet-nest-thermostat/

[20] “*Samsung Privacy Policy--SmartTV Supplement.*” Samsung Corp. Web. 29 Sept. 2015. http://www.samsung.com/sg/info/privacy/smarttv.html

[21] “*How It Works*” SmartThings, 2015. http://www.smartthings.com/how-it-works.

[22] Tschofenig, H., et. al., p. 6.

[23] Tschofenig, H., et. al., p. 9.

[24] “*An example of a generic (non-IoT) off-the-shelf*”, federated cloud-sharing tool is ownCloud, produced by ownCloud.org. https://owncloud.org/blog/faster-easier-file-sync-and-share-with-federated-self-hosted-owncloud-8-0/

[25] Duffy Marsan, Carolyn. p.7

[26] Erik Wilde. “*Putting things to REST*”. Technical Report UCB iSchool Report 2007-015, School of Information, UC Berkeley, November 2007.

[27] Dominique Guinard, Vlad Trifa, and Erik Wilde, “*Architecting a Mashable Open World Wide Web of Things*”, Technical Report No. 663, Dept. of Computer Science, ETH Zurich, February 2010.

[28] Roy Thomas Fielding, “*Architectural Styles and the Design of Network-based Software Architectures*”, PhD thesis, University of California, Irvine, Irvine, California, 2000.

[29] Leonard Richardson and Sam Ruby, “*RESTful Web Services*”, O’Reilly, 2007.

[30] Lars Schor, Philipp Sommer, and Roger Wattenhofer, “*Towards a Zero-Configuration Wireless Sensor Network Architecture for Smart Buildings*”, in First Workshop On Embedded Sensing Systems For Energy-Efficiency In Buildings (BuildSys), Berkeley, California, USA, November 2009.

[31] Dogan Yazar and Adam Dunkels, "*Efficient Application Integration in IP-based Sensor Networks*", in First Workshop On Embedded Sensing Systems For Energy-Efficiency In Buildings (BuildSys), Berkeley, California, November 2009.

[32] Jarno Elonen. "NanoHTTPD embeddable HTTP server in Java", http://elonen.iki.fi/code/nanohttpd/ (accessed in December 2012).

[33] Nokia Research Center. "*Nokia Mobile Web Server*". http://research.nokia.com/page/231 (accessed in December 2012).

[34] Gustavo Alonso, Fabio Casati, Harumi Kuno, and Vijay Machiraju, "*Web Services: Concepts, Architectures*", Springer-Verlag, 2004.

[35] M. Eisenhauer, P. Rosengren and P. Antolin, "*A Development Platform for Integrating Wireless Devices and Sensors into Ambient Intelligence Systems*", in 6th Annual IEEE Communications Society Sensor, Mesh and Ad Hoc Communications and Networks Workshops, SECON, Rome, 2009.

[36] S. Hong, D. Kim, M. Ha, S. Bae, S. Park, W. Jung and J. Kim, "*SNAIL: an IP-based wireless sensor network approach to the internet of things*" IEEE Wireless Communications, vol. 17, no. 6, pp. 34-42, 2010.

[37] N. Bui, A. Castellani, P. Casari and M. Zorzi, "*The internet of energy: a web-enabled smart grid system*" IEEE Network, vol. 26, no. 4, pp. 39-45, 2012.

[38] A. Iera, C. Floerkemeier, J. Mitsugi and G. Morabito, "*The Internet of things*" IEEE Wireless Communications, vol. 17, no. 6, pp. 8-9, 2010.

[39] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton and T. Razafindr alambo, "*A survey on facilities for experimental internet of things research*" IEEE Communications Magazine, vol. 49, no. 11, pp. 58-67, 2011.

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

[41] A. Sehgal, V. Perelman, S. Kuryla and J. Schonwalder, "*Management of resource constrained devices in the internet of things*" IEEE Communications Magazine, vol. 50, no. 12, pp. 144-149, 2012.

[42] S. Helal, W. Mann, H. El-Zabadani, J. King, Y. Kaddoura and E. Jansen, "*The gator tech smart house: A programmable pervasive space*" IEEE Computer, vol. 38, no. 3, pp. 50-60, 2005.

[43] D. Cook, "*Learning Setting-Generalized Activity Models for Smart Spaces*" IEEE Intelligent Systems, vol. 27, no. 1, pp. 32-38, 2012.

[44] F. Doctor, H. Hagras and V. Callaghan, "*A fuzzy embedded agent-based approach for realizing ambient intelligence in intelligent inhabited environments*" IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, vol. 35, no. 1, pp. 55-65, 2005.

[45] J. Kientz, S. Patel, B. Jones, E. Price, E. Myantt and G. Abowd, "*The Georgia Tech aware home*" in Proceedings of the Extended Abstracts on Human Factors in Computing Systems, 2008.

[46] I. S. Larson, K. Tapia, E. Beaudin, J. Kaushik, P. Nawyn and J. R. Rockinson, "*Using a Live- In Laboratory for Ubiquitous Computing Research*" in Pervasive Computing, Lecture Notes in Computer Science, Berlin, Springer Berlin Heidelberg, 2006, p. 349–365.

[47] N. K. Suryadevara and S. C. Mukhopadhyay, "*Wireless Sensor Network based Home Monitoring System for Wellness Determination of Elderly*" IEEE Sensors Journal, vol. 12, no. 6, pp. 1965-1972, 2012.

[48] L. C. DeSilva, M. Chamin and M. P. Iskandar, "*State of the art of Smart Homes*" Engineering Applications of Artificial Intelligence, vol. 25, no. 7, pp. 1313-1321, 2012.

[49] I. Howitt and J. A. Gutierrez, "*IEEE 802.15.4 low rate - wireless personal area network coexistence issuues*" in Proceedings of the IEEE-Wireless Communications and Networking, New Orleans, 2003.

[50] L. Angrisani, M. Bertocco, D. Foortin and A. Sona, "*Assessing coexistence problems of IEEE 802.11b and IEEE 802.15.4 wireless networks through cross-layer measurements*" in Instrumentation and Measurement Technology Conference Proceedings, Warsaw, 2007.

[51] H. Khaleel, C. Pastrone, F. Penn a, M. A. Spirito and R. Garello, "*Impact of Wi-Fi traffic on the IEEE 8022.15.4 channels occupation in indoor environments*" in International Conferrence on Electromagneticcs in Advanced Applications, 2009.

[52] N. Kushalnagar, G. Montenegro, J. Hui and D. Culler, "*Transmission of IPv6 Packets over IEEE 802.15.4 Networks, IETF RFC 4944*" September 2007. http://tools.ietf.org/rfc/rfc4944.txt.

[53] K. Lee, J. Won and C. Bae, "*IGN2IP: Internetworking Intelligent Gadget Network based on 802.15.4 with IP Network*" in Proceedings of the International Conference on Consumer Electronics, ICCE 2008, Digest of Technical Papers, Las Vegas, 2008.

[54] F. Mesrinejad, F. Hashim F, N. K. Noordin, M. F. A. Rasid and R. S. A. R. Abdullah, "*The Effect of Fragmentation and Header Compression on IP-Based Sensor Networks (6LoWPAN)*" in Proceedings of the 17th Asia-Pacific Conference on Communications (APCC), Sabah, 2011.

[55] J. Beutel, "*Metrics for Sensor Network Platforms*" in ACM Workshop on Real-World Wireless Sensor Networks (REALWSN'06), ACM Press, New York, 2006.

[56] Deepali Javale, Mohd. Mohsin, Shreerang Nandanwar and Mayur Shingate, "*International Journal of Electronics Communication and Computer Technology (IJECCT)*", Volume 3 Issue 2 (March 2013).

[57] "*Connected Devices for Smarter Home Environments*", IBM Data Magazine, 2014. http://ibmdatamag.com/2014/04/connecteddevices-for-smarter-home-environments/

[58] "*Autonomic Computing: IBM's perspective on the state of Information Technology*", 2001, http://www.research.ibm.com/autonomic/manifesto/autonomic computing.pdf

[59] Larios V.M., Robledo J.G., Gómez L., and Rincon R., "*IEEE-GDL CCD Smart Buildings Introduction*". http://smartcities.ieee.org/images/files/ images/pdf/whitepaper phi smartbuildingsv6.pdf

[60] "*Foundations for Innovation in Cyber-Physical Systems*", Workshop Report, NIST, 2013. http://www.nist.gov/el/upload/CPSWorkshopReport-1–30-13-Final.pdf

[61] G. Bovet, A. Ridi and J. Hennebert, "*Toward Web Enhanced Building Automation System*", in Eds. N. Bessis and C. Dobre – Big Data and Internet of Things: A Roadmap for Smart Environments, ISBN: 978–3-319–05028-7, Studies in Computational Intelligence, Volume 546, 2014 pp. 259–283. http://hal.archivesouvertes.fr/docs/00/97/35/10/PDF/BuildingsWoT.pdf

[62] H. Grindvoll, O. Vermesan, T. Crosbie, R. Bahr, et al., "*A wireless sensor network for intelligent building energy management based on multi communication standards – a case study*", ITcon Vol. 17, pg. 43–62, http://www.itcon.org/2012/3

[63] U.S. Department of Energy, "*Building Energy Data Book*". http://buildingsdatabook.eere.energy.gov/, 2010.

[64] Taneja, J., Culler, D., and Dutta, P., "*Towards Cooperative Grids: Sensor/Actuator Networks for Renewables Integration*", in SmartGridComm (2010).

[65] Gupta, S., Reynolds, M., and Patel, S., "*ElectriSense: Single-Point Sensing Using EMI for Electrical Event Detection and Classication in the Home*", in Ubicomp (September 2010).

[66] Hart, G., "*Nonintrusive Appliance Load Monitoring*", in Proceedings of the IEEE vol. 80, n.12 (December 1992).

[67] Jiang, X., Ly, M. Van, Taneja, J., Dutta, P., and Culler, D., "*Experiences with a High-Fidelity Wireless Building Energy Auditing Network*", in SenSys (2009).

[68] Kim, Y., Schmid, T., Charbiwala, Z., and Srivastava, M. ViridiScope, "*Design and Implementation of a Fine Grained Power Monitoring System for Homes*", in Proceedings of the Conference on Ubiquitous Computing (UbiComp) (Orlando, Florida, September 2009), pp. 245{254.

[69] Marchiori, A., and Han, Q. "*Using Circuit-Level Power Measurements in Household Energy Management Systems*", in BuildSys (2009).

[70] Jiang, X., Dawson-Haggerty, S., Dutta, P., and Culler, D., "*Design and Implementation of a High-Fidelity AC Metering Network*", in IPSN (2009).

[71] Lanzisera, Steven, "*The "Other" Energy in Buildings: Wireless Power Metering of Plug-in Devices*", Environment Energy Technologies Division Seminar, Lawrence Berkeley National Labs, June 17 2011.

[72] Tweet-a-Watt. http://www.ladyada.net/make/tweetawatt/.

[73] Plogg Wireless Energy Management. http://www.plogginternational.com.

[74] Hnat, T., Srinivasan, V., Lu, J., Sookoor, T., Dawson, R., Stankovic, J., and Whitehouse, K., "*The Hitchhiker's Guide to Successful Residential Sensing Deployments*", in SenSys (November 2011).

[75] Kolter, J., and Johnson, M. REDD, "*A Public Data Set for Energy Disaggregation Research*", in SustKDD (August 2011).

[76] Anderson, K., Ocneanu, A., Benitez, D., Carlson, D., Rowe, A., and Berges, M. BLUED, "*A Fully Labeled Public Dataset for Event-Based Non-Intrusive Load Monitoring Research*", in SustKDD (August 2012).

[77] Barker, S., Mishra, A., Irwin, D., Cecchet, E., Shenoy, P., and Albrecht, J. Smart, "*An Open Data Set and Tools for Enabling Research in Sustainable Homes*". In SustKDD (August 2012).

[78] Insteon: The Details. www.insteon.net/pdf/insteondetails.pdf, 2005.

[79] Insteon for the Smart Grid. http://www.insteonsmartgrid.com.

[80] Pannuto, P., and Dutta, P., "*Exploring Powerline Networking for the Smart Building", I*n IP+SN (2011).

[81] Wemo insight switch. http://www.belkin.com/us/F7C029-Belkin/p/P-F7C029/.

[82] IEEE Std 802.15.4TM-2006, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-RateWireless Personal Area Networks (LR-WPANs). http://www.ieee802.org/15/pub/TG4.html

[83] Bluetooth Low Energy (LE) Technology. http://www.bluetooth.com/English/Products/Pages/low energy.aspx

[84] The Official Bluetooth Technology. http://www.bluetooth.com/

[85] DASH7 Alliance. http://www.dash7.org

[86] ISO, International Organization for Standardization (ISO), Identification cards – Contactless integrated circuit(s) cards – Vicinity cards, ISO/IEC 14443, 2003

[87] N. Pletcher, S. Gambini, and J. Rabaey, "*A 52 µW Wake-Up Receiver With 72 dBm Sensitivity Using an Uncertain-IF Architecture*", in IEEE Journal of Solid-State Circuits, vol. 44, no1, January, pp. 269–280. 2009

[88] A. Vouilloz, M. Declercq, and C. Dehollain, "*A Low-Power CMOS Super-Regenerative Receiver at 1 GHz*", in IEEE Journal of Solid-State Circuits, vol. 36, no3, March, pp. 440–451, 2001

[89] J. Ryckaert, A. Geis, L. Bos, G. van der Plas, J. Craninckx, *"A 6.1 GS/s 52.8 mW 43 dB DR 80 MHz Bandwidth 2.4 GHz RF Bandpass S-? ADC in 40 nm CMOS*", in IEEE Radio-Frequency Integrated Circuits Symposium, 2010

[90] L. Lolis, C. Bernier, M. Pelissier, D. Dallet, and J.-B. Bégueret, “*Bandpass Sampling RX System Design Issues and Architecture Comparison for Low Power RF Standards*”, IEEE ISCAS 2010

[91] D. Lachartre, “*A 550 µW inductorless bandpass quantizer in 65 nm CMOS for 1.4-to-3 GHz digital RF receivers*”, VLSI Circuits 2011, pp. 166–167, 2011

[92] T. Mitchell, Machine Learning, McGraw Hill, 1997

[93] B. Ostermaier, M. Kovatsch, and S. Santini, “*Connecting Things to the Web using Programmable Low-power Wi-Fi Modules*”, in Proceedings of the 2nd International Workshop on the Web of Things, WoT, pages 1–6, San Francisco, CA, USA, 2011.

[94] IEEE Draft Standard for Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks-Specific requirements-Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications-Amendment 8: IEEE 802.11 Wireless Network Management. IEEE P802.11v, Feb. 2012.

[95] M. Buettner, G. V. Yee, E. Anderson, and R. Han. X-MAC, “*A Short Preamble MAC Protocol for Duty-cycled Wireless Sensor Networks*”, in Proceedings of the 4th International Conference on Embedded Networked Sensor Systems, SenSys, pages 307–320, 2006.

[96] A. Dunkels, L. Mottola, N. Tsiftes, F. Osterlind, J. Eriksson, and N. Finne. The Announcement Layer, “*Beacon Coordination for the Sensornet Stack*”, in Proc. EWSN, Bonn, Germany, 2011.

[97] P. Dutta, S. Dawson-Haggerty, Y. Chen, C.-J. M. Liang, and A. Terzis, “*Design and Evaluation of a Versatile and Efficient Receiver-initiated Link Layer for Low-power Wireless*”, in Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems, SenSys, pages 1–14, 2010.

[98] J. Polastre, J. Hill, and D. Culler, “*Versatile Low Power Media Access for Wireless Sensor Networks*”, in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, SenSys, pages 95–107, Baltimore, MD, USA, 2004.

[99] W. Ye, J. Heidemann, and D. Estrin, “*An Energy-efficient MAC Protocol for Wireless Sensor Networks*”, in Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, pages 1567–1576, 2002.

[100] A. Dunkels, “*The ContikiMAC Radio Duty Cycling Protocol”,* Technical Report T2011:13, SICS Swedish ICT, 2011

[101] Silicon Laboratories Inc., “*Overcoming Challenges of Connecting Intelligent Nodes to the Internet of Things*”. (2012)

[102] Y. Liu, "*Study on Smart Home System Based on Internet of Things Technology*" in Informatics and Management Science IV. vol. 207, W. Du, Ed., ed: Springer London, pp. 73-81, (2013).

[103] C.H. Chen, C.-C. Gao, and J.-J. Chen, "*Intelligent Home Energy Conservation System Based On WSN*" International Conference on Electrical, Electronics and Civil Engineering, Pattaya, (2011).

[104] Muhammad Waqar Aziz, "*Service-Oriented Layered Architecture for Smart Home*", International Journal of Smart Home Vol.7, No.6 (2013), pp.409-418, (2013).

[105] M. ONakamura, H. Igaki and H. Tamada, "*Implementing integrated services of networked home appliances using service oriented architecture*", second Int. Conf. on Service Oriented Computing, ACM, New York, NY, USA, (2004).

[106] M. Margolis, Arduino Cookbook,O'Reilly, CA, USA, (2011).

[107] Arduino at http://www.arduino.cc/

[108] Fariba Sadri, "*Ambient Intelligence: A Survey*" ACM Comput. Surv. 43, 4, Article 36, (2011).

[109] Eric J. Pauwels,Albert A. Salah, Romain Tavenard, "*Sensor Networks for Ambient Intelligence*", Multimedia Signal Processing - MMSP, (2007)

[110] Google Speech To Text Web Service. https://www.google.com/intl/it/chrome/demos/speech.html.

[111] Free Lossless Audio Codec (FLAC). https://xiph.org/flac/.

[112] F. De Rango, M. Tropea, P. Fazio, S. Marano, "*Overview on VoIP: Subjective and objective measurement methods*", International Journal of Computer Science and Network Security, pp.140-153, (2006).

[113] F. De Rango, P. Fazio, F. Scarcello, F. Conte, "*A New Distributed Application and Network Layer Protocol for VoIP in Mobile Ad Hoc Networks*", IEEE Transaction on Mobile Computing, Vol.13, (2014).

[114] David Sousa Nunes, Pei Zhang, Jorge Sá Silva, "*A Survey on Human-in-the-Loop Applications Towards an Internet of All*", IEEE Communications Surveys & Tutorials (Volume:17, Issue: 2), 2015.

[115] F. Gaudencio, T. Camilo ; J. S. Silva ; F. Boavida, "*Sensitive learning: A new framework proposal in learning contexts*", Intelligent Environments, 2008 IET 4th International Conference on, 2008.

[116] Chris R. Baker, Kenneth Armijo, Simon Belka, Merwan Benhabib, Vikas Bhargava, Nathan Burkhart, Artin Der Minassians, Gunes Dervisoglu, Lilia Gutnik, M. Brent Haick, Christine Ho, Mike Koplow, Jennifer Mangold, Stefanie Robinson, Matt Rosa, Miclas Schwartz, Christo Sims, Hanns Stoffregen, Andrew Waterbury, Eli S. Leland, Trevor Pering, Paul K. Wright, "*Wireless Sensor Networks for Home Health Care*", Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference on (Volume:2), 2007.

[117] R. Silva, J. S. Silva ; A. Silva ; F. C. Pinto ; M. Simek ; F. Boavida, "*Wireless Sensor Networks in Intensive Care Units*", 2009 IEEE International Conference on Communications Workshops, 2009.

[118] Ricardo Silva; Jorge Sa Silva ; Fernando Boavida, “*A symbiotic resources sharing IoT platform in the smart cities context*”, Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2015 IEEE Tenth International Conference on, 2015.

[119] P. Rawat, K. Singh, H. Chaouchi, and J. Bonnin, “*Wireless sensor networks: A survey on recent developments and potential synergies*”, J. Supercomput., vol. 66, no. 1, pp. 1–48, Oct. 2013.

[120] A. D. Wood and J. A. Stankovic, “*Human in the loop: Distributed data streams for immersive cyber-physical systems*”, SIGBED Rev., vol. 5, no. 1, pp. 20:1–20:2, Jan. 2008.

[121] Jaroslaw Domaszewicz, Spyros Lalis, Aleksander Pruszkowski, Manos Koutsoubelias, Tomasz Tajmajer, Nasos Grigoropoulos, Michele Nati, Alexander Gluhak, “*Soft Actuation: Smart Home and Office with Human-in-the-Loop*”, IEEE Pervasive Computing (Volume:15, Issue: 1), 2016.

[122] Shalli Rani, Rajneesh Talwar, Jyoteesh Malhotra, Syed Hassan Ahmed, Mahasweta Sarkar, Houbing Song, “*A Novel Scheme for an Energy Efficient Internet of Things Based on Wireless Sensor Networks*”, Sensors 2015, 15, 28603-28626; doi:10.3390/s151128603.

[123] Tiago D. P. Mendes, Radu Godina, Eduardo M. G. Rodrigues, João C. O. Matias, João P. S. Catalão, “*Smart home communication technologies and applications: Wireless protocol assessment for home area network resources*”. Energies 2015, 8, 7279.

[124] Mario Collotta, Giovanni Pau, “*A Solution Based on Bluetooth Low Energy for Smart Home Energy Management*”, Energies 2015, 8, 11916-11938.

[125] R. Al-Ali; Murad Qasaimeh; Mamoun Al-Mardini; Suresh Radder; I. A. Zualkernan, “*ZigBee-based irrigation system for home gardens*”, Communications, Signal Processing, and their Applications (ICCSPA), 2015 International Conference on.

[126] C. A. Trasviña-Moreno, R. Blasco, R. Casas, and A. Marco, “*Autonomous Wi-Fi Sensor for Heating Systems in the Internet of Things*” Journal of Sensors, vol. 2016, Article ID 7235984, 14 pages, 2016. doi:10.1155/2016/7235984.

[127] Xingyue Han; Chunhui Zhao, “*Distributing Monitor System Based on WI-FI and GSM Supporting SCPI*”, Distributed Computing and Applications to Business, Engineering and Science (DCABES), 2014 13th International Symposium on.

[128] Yan Wenbo; Wang Quanyu; Gao Zhenwei, “*Smart home implementation based on Internet and Wi-Fi technology*”, Control Conference (CCC), 2015 34th Chinese.

[129] Fagui Liu, Hongjie Zhao, “*The Design of Wi-Fi-Based Smart Home Communication Hardware Adapter*”, 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC).

[130] Arshdeep Kaur, Amrit Kaur , “*Comparison of Mamdani-Type and Sugeno-Type Fuzzy Inference Systems for Air Conditioning System*”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[131] Microchip Technology Inc., 2.4 GHz IEEE Std. 802.11 b/g Wireless LAN RN171 Module Specification Sheet, 2014.

[132] Colitti, W., "*State-of-the-Art: Communication, Technology, Interoperability*", Version: 0.3, ISN, Interoperable Sensor Networks, 2011.

[133] Ericsson White Paper, "*Cellular Networks for Massive IoT*", 2006.

[134] Semtech Corporation Whitepaper, "LPWA Technologies—Unlock New IoT Market Potential", Machina Research, 2015.

[135] Rayal, F. "Shaping Cellular IoT Connectivity—Emerging Technologies in Wide-Area Connectivity", Xona Partners Team. www.xonapartners.com, 2015

[136] Marco Centenaro, Lorenzo Vangelista, Andrea Zanella, and Michele Zorzi, "*Long-range communications in unlicensed bands: the rising stars in the iot and smart city scenarios*", arXiv preprint arXiv:1510.00620, 2015.