TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

ALESSIA PANTANO

ENERGY HARVESTING SCHEMES FOR RADIO TECHNOLOGIES USED IN IOT: OVERVIEW AND SUITABILITY STUDY

Master of Science thesis

Examiner: Prof. Mikko Valkama
Dr. Ali Hazmi
Examiner and topic approved by the
Faculty Council of the Faculty of
Computing and Electrical Engineering
on 22nd January 2015

ABSTRACT

ALESSIA PANTANO: ENERGY HARVESTING SCHEMES FOR RADIO TECHNOLOGIES USED IN IOT: OVERVIEW AND SUITABILITY STUDY
Tampere University of Technology
Master of Science thesis,85 pages
October 2015
Master's Degree Programme in Information Technology
Major: Communication Systems and Networks
Examiner: Prof. Mikko Valkama
Dr. Ali Hazmi
Keywords: Internet of Things, Energy Harvesting, IEEE 802.11ah, Suitability

The number of devices connected to the Internet increases day by day. Moreover people start using the network in their everyday life to shopping, to control the house by remote, to check news or the weather forecast, to check the traffic, to call their friend or their family and so on. Their phones are interconnected all the time with other devices and sensors to gather all the information the users need. This network of object and the exchange of data are described with the Internet of Things idea. With the Internet of Thing concept all object are connected to the Internet and they are able to transmit data to each other. Thanks to sensors, inanimate object are able to understand the environment around them and to make decision and to interact with it. With this scenario the amount of data exchanged is huge. The main two challenges of the Internet of Things concept are the energy consumption and the portability of a given sensor or node in the network. In this way all the object and people can be connected everywhere and all the time.

To reach those aims it is important that the devices implement specific communication standards that require low energy to work and that guaranty, at the same time, quality and security to the transmission of the data. Batteries or cable are not suitable to satisfy the IoT requirements and new energy sources using energy harvesting schemes, are needed to power the devices. Moreover the communication protocols have to be faster and have to use as less power as possible to work.

In this thesis an overview on multiple energy harvesting schemes given and different communication standards used in the Wireless Sensor Networks are analyzed. The main focus is on the energy consumption of the Wireless Sensor Networks that im-

plements the communication standard IEEE 802.11ah. The aim was to understand whether it could be possible to power one node network or even a more complex one, only with the energy harvesting schemes described in the thesis.

Networks of different sizes are simulated and analyzed. All the networks present only one AP but they differentiate from each other by the number of nodes (STAs). Moreover two different scenarios are simulated to better understand the energy consumption in different traffic case. Both saturated and non-saturated traffic scenario were simulated and analyzed. To enhance the throughput and to decrease the energy needed to power the sensors, different Modulation and Code Schemes where implemented. To assess the performance of simulated scenarios, the throughput and the energy consumption where analyzed.

The results have showed that different networks required a small amount of energy to send and receive data. Therefore it is technically possible to power them only with some existing energy harvesting schemes.

PREFACE

This thesis is the conclusion of the Master of Science (MSc) degree in Ingegneria delle tecnologie della comunicazione e dell informazione (Telecommunication engineering) at the University of Roma TRE. The simulations and the results shown in the thesis where completely made in the department of Electronics and Communications Engineering at Tampere University of Technologies during the year 2014-2015.

I would like to express my thankfulness to my supervisor Professor Mikko Valkama for the huge and great opportunity he provided me. He allowed me to work on my thesis in a professional and innovative University. I would also like to really thank you my other supervisor Dr. Ali Hazmi for his time, his patience and his constant help. His support and the Skype call we had when I went back to Italy were important for the realization of this research.

I would also like to thank with all my heart my parents and my sister for the enthusiasm, the help and the patience they always had with me. I am really grateful for them always being on my side and for them inspiring me everyday. I owe them all my successes and I would have not reached this point in my life without their support and motivation.

I would also like to thank my grandmother, my aunt Stefania and my uncle Claudio for their help during my studies. They are always there to cheer me and to make my life better.

I would like to express my sincere appreciation and thanks to my boyfriend Georg. He supports and helps me everyday and I would have not reached my last achievements without him on my side.

The last thank goes to my friends in Italy and in Tampere. Their happiness and their support made my studies period better and funnier.

Tampere, 30.09.2015

Alessia Pantano

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The number of wireless and smart devices increased dramatically over the last years and more and more people started using technology in their everyday life. Smart and wearable devices as smart-phone, tablets and smart watches are using everyday to be connected anytime and everywhere. Moreover the idea of connecting objects from different networks brought up the concept of the Internet of Things (IoT). The Internet of Things consists of objects that have virtual personalities and that can interact both with human and other devices to create a smarter world. These smart and interactive objects are able to understand the environment around them and to send data captured by sensors. The IoT idea will bring to a reality where 50 to 100 billion devices will interact to each other and where the real word will be mapped into a virtual one by using RFID tags and QR codes [1].

One of the most important elements of the IoT is the Wireless Sensor Network (WSN) where nodes are densely distributed. These networks can be used everywhere, for instance, for home automation, for light control, temperature control, security and remote control of household appliances. They can also be used for industrial automation, sports, healthcare and much more applications.

Really important challenges for the node are its portability and its energy autonomy. That leads to the necessity of compact and low-cost energy sources and to the creation of new communication standards that work with low energy.

In this thesis different energy harvesting schemes to power the sensor nodes are illustrated. Moreover an overview of the communication standards used in these networks is given. In particular the energy consumption of the Wireless Sensor Network that implements the new standard IEEE 802.11ah is investigated. To understand the energy consumption of a single node or of a more complex network, different WSNs of different size are simulated using the OMNet++ tool. The data obtained is then used to understand if this kind of networks that use this standard can be completely powered by the energy harvesting schemes illustrated before.

The thesis consists of six chapters.

The second chapter gives an overview of the Internet of Things. The key factors on which it is based, the requirements that are needed to realize smart networks and the technical challenges and limitations that these networks have are discussed.

In the third chapter the radio technologies implemented in sensor networks used in the Internet of Things applications are described in detail. In particular the standard ZigBee, the Bluetooth Low Energy and the new standard IEEE 802.11ah (currently under development) are analyzed.

In the fourth chapter the concept of energy harvesting is explained. Using this technique it is possible to collect and use the energy that is present in the environment in which the device is located. Some of the energy harvesting schemes are analyzed in more detail. For each of them some examples are given and the amount of energy that they can gain is shown.

In the fifth chapter there is a brief introduction of the OMNeT++ tool used for the simulations and all them are explained in detail. The results obtained are then discussed.

In the final chapter the main conclusions obtained by analyzing the collected data are presented.

2. INTERNET OF THINGS

2.1 Introduction and overview

The Internet is a powerful network for communication. It has evolved in a way it has had a big influence on human life. The Internet started as the Internet of Computers, a global network with services such as the World Wide Web built on top of the original platform to allow people to send data or to search some information on the web. At that time most of the people were using Internet to look for answers and a few people were writing and providing the information. Over the last years the Internet has changed into an "Internet of People" evolving in the Social Web or also known as Web 2.0. In this Internet, the contents are created and read by people who want to be connected with others (an estimated 1 billion people make up the Internet of People). The Internet has become, in this way, a network for social relationships and it permits users to search not only information but also people. Forums and social websites were born. The development of new technology is expanding the boundaries of the Internet and a broadband Internet connectivity is becoming cheap and ubiquitous [2].

So, usually, Internet is most used by humans who want to interact with other people or who want to look for some knowledge. But with the development of new technologies, sensors and standards the Internet will be used also by objects to have human-thing and thing-thing communications [3]. In the future the main communications will not be in between humans and humans, but more and more objects will access the Internet to search information and to "talk" both with other objects and humans. Using appropriated communication protocols, designed for Web oriented architectures, the Internet will develop into the Internet of Things.

The name Internet of Things represents the development of the actual Internet network. Probably the first time someone told about the Internet of Things was in 1999 during a presentation hold by Kevin Ashton at Procter and Gamble and by

David L. Brock in 2001 [4-6]. The name was officially recognized in 2005 when the International Telecommunication Union (ITU), the authority that regulates all the universal telecommunication standards, published a report with the same name [5, 7].

It is possible to describe the Internet of Things as Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts [8]. So in the next future, animals, plants and even objects will be able to interact using Internet.

As shown in Figure 2.1, the Internet of Things represents a world where new technologies as the Radio Frequency Identifications (RFID), ZigBee, Bluetooth, IEEE 802.11 and smart programming can work together to create a network of interconnected devices for a different kind of applications.

The objects will be interactive and smart and they will be able to talk to each other by sending data that they can catch thanks to sensors. In this way there will be a network in which 50 to 100 billion devices will be connected to the Internet by 2020. Some projections indicate that in the same year, the number of mobile machine sessions will be 30 times higher than the number of mobile person sessions. If we consider not only machine-to-machine communications but communications among all kinds of objects, then the potential number of objects to be connected to the Internet arises to 100,000 billions [1].

It will then go towards a reality where especially the machines will communicate and the user will become more a spectator, who will benefit from this progress, than the actor.

With the new idea of Internet of Things the main amount of data will not be generated or accessed by humans but by devices.

Central issues are making a full interoperability of interconnected devices possible, providing them with an always higher degree of smartness by enabling their adaptation and autonomous behavior. It is also important to guarantee trust, privacy, and security [10]. In this big network every object will have also the power to understand where it is and the power to interact with the environment. It will also be able to think, or better, to calculate the data already collected. These smart objects will communicate their deductions and other information they have through

Figure 2.1 *Illustration of the Internet of Things [9].*

network that allows them to be connected with the world [8].

Regarding the place where they are placed and their porpoise the intelligent components will be able to fulfill different kind of tasks. An example of this is the future cars communicate with other cars and with the traffic lights to avoid accidents and to reduce traffic congestion. Another examples could be the smart doors that will sound the alarm if they undergo an intrusion attempt or a bunch of keys that reveals their position. There will be no limits to the actions and operations that these "smart things" will be able to perform. For example: the devices will have the power to direct their transport, self-heal, or the refrigerator will alert us if frozen foods are about to expire. The alarm, that will check traffic information or Google calendar events or the weather forecast, will sound earlier to avoid us being late at work [11] and the mirror will inform us about our weight and our health or about the weather forecast [12].

One of the aims of the Internet of Things (IoT) is to map the real word into a virtual one and this goal can be reached giving an identity to all the objects and to all the places [5]. The IoT will create a big and dynamic network combining Pervasive computer, Ubiquitous computer and Ambient intelligence. In a not too distant future, it is expected that a single system of numbering, such as IPv6, will make every single object identifiable and addressable [13]. The Internet of things

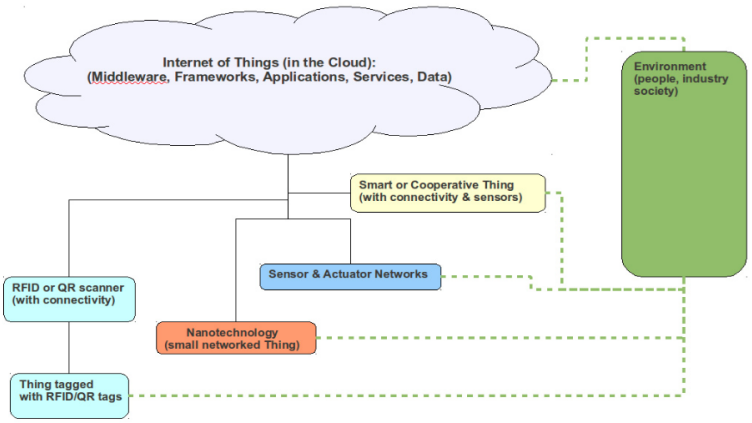

Figure 2.2 *The architecture of the Internet of Things [2].*

is based on three fundamental concepts: any time connection, any thing connection and any place connection [3, 8, 10, 14].

Let see them in details:

- Any Time Connection: everyone can be always connected, at all hours of the day and night, thanks to the mobile phone network
- Any Place Connection: that everyone can be connected anywhere, in door or outdoors or even on the move, thanks to portable devices such as PDAs, laptops, smart phones
- Any Thing Connection: it is introduced with the IoT and means that all objects can be connected, both among themselves and with humans

In order to realize the Internet of Things, these ideas have to be supported by an appropriate technology. As shown in Figure 2.2 ITU has identified 4 key components of this technology [14]:

- RFID technology: a tag is assigned to each object and a reader can read it and obtain all the info included in it;
- Sensors: they allow detecting changes in the physical state of the objects, their location or their temperature. Using the sensors also means that the

objects are able to change their status to respond to changes that occur in the surrounding environment [15]. (For example, an "electronic" jacket may detect temperature changes in the internal and/or external via special sensors, and to adjust the parameters of the same jacket);

- Embedded intelligence: it is obtained by delegating part of decision-making capacity from the central system to the objects (which must be equipped with sufficient processing power). In this way will be possible to create objects able to perform activities autonomously;
- Nanotechnology: using this technology more and more miniature-sized objects will be created.

2.2 Requirements

From the idea of the IoT, billion or trillion identifiable objects will communicate to each other [5]. That requires smaller and lighter devices that will need less energy to work, miniaturization of devices, new mobile communication protocols and a way to address all the objects. It should be easy to connect a big and dense amount of devices with high-energy efficiency. Also security and privacy have to be guaranteed for all the data transmitted.

2.2.1 Identification of the devices and traceability

One of the main points of the IoT is to identify objects and to get possible to know their positions and their movements. Just think of the use of the bar code that specifically identifies the product to which it is associated. Bar codes have two main limitations: they identify a product, but not a specific unit of the product, and they have to be read with a manual process [16].

To identify and trace objects it is possible to use all the technologies that use sensors, bar codes, smart cards, biometrics and so on. Each object will be labeled and addressed through codes. The code could be a QR code (Quick Response) or a RFID tag and, by using a portable reader, it is possible to access to more information about the object via the web. These technologies allow knowing the positions and the movements of some objects.

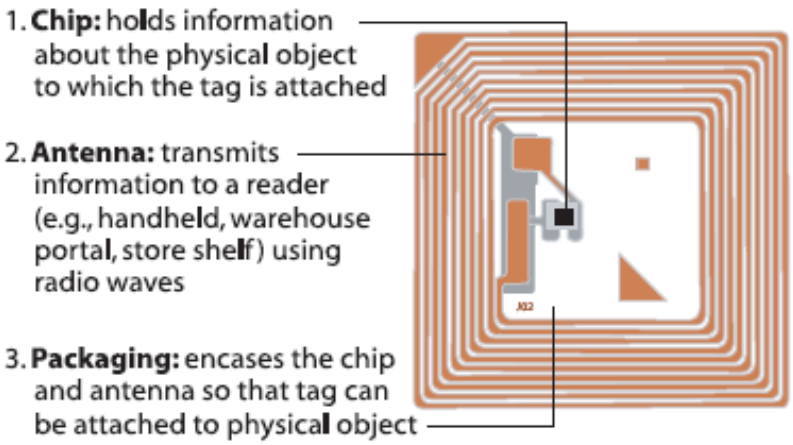

Figure 2.3 *Structure of RFID Tag [17].*

Radio Frequency IDentificator

The RFID technology is based on microchip in with is embedded a micro-antenna, called transponder or RFID tag.

The tags can be incorporated into objects and be updated or read automatically.

The RFID mechanism is quite simple: an antenna, positioned at a suitable distance from the tag (which also contains an antenna), is able to read the contents and the two systems are therefore able to communicate between them. The distance between the tag and the antenna is variable and is determined based on the specific application.

The tags can be active or passive: in case of the passive chip, the tag derives the energy needed to operate directly from the electromagnetic field that receives from the external system. The magnetic fields produced by the system are completely safe for the health of users, classified by three units less than the emissions of mobile phones.

The RFID systems, then, can be scanned without contact, and have the capacity to contain a large amount of data and have the characteristics of anti-counterfeiting.

Another advantage is that it can be applied anywhere and there are currently tags embedded in tissues, metals, food. In many cases, these tags can survive even

in an extremely inhospitable environment in which humans can hardly live or even survive. The tags can be used for keys, books, clothes, access control and banknotes. Over greater distances and higher frequencies, they may also be used for controlling containers or vehicles. The RFID tags could be applied on the operas in the museum so a tourist, who is visiting the area, can use a specific scanner (for example his/her smart-phone) and access, in real time, to all the possible information about that statue or paint [18].

To handle such amount of data an infrastructure (for example in the commercial field) that enables the use of tags between different companies that collaborate is needed to be created.

To use the RFID technology is necessary to develop at least two elements:

- A standardized system to uniquely identify products
- A standardized system to identify and to share information accompanying a single object

To identify items the technique of the EPC (Electronic Product Code) can be used. This is essentially an evolution of the UPC (Universal Product Code). The UPC is the code system used in the bar-code. Indeed tags with RFID technology are the most effectively adoptable device for identification and traceability of objects. That is possible because they are based on a memory that can be accessed passively via radio frequency by scanners. For example using the EPC, whoever is part of a chain of distribution, can locate and read or write the information on a single unit of product wherever it is placed.

They are different versions of the EPC code and it can be written in 64 bits, 96 bits and 256 bits. If companies want to use a 96-bit code, it provides unique identifiers for 268 million companies. Any company can have up to 16 million distinct classes of objects, with 68 billion serial numbers within each class of objects.

Unlike the UPC bar code, the EPC provides a unique identification for any physical object in the world and consists of (in the case of the 96-bit used in a company)[17]:

- Header (8 bits) that specifies the version number of the EPC
- EPC Manager (28-bit) that provides the name of the company

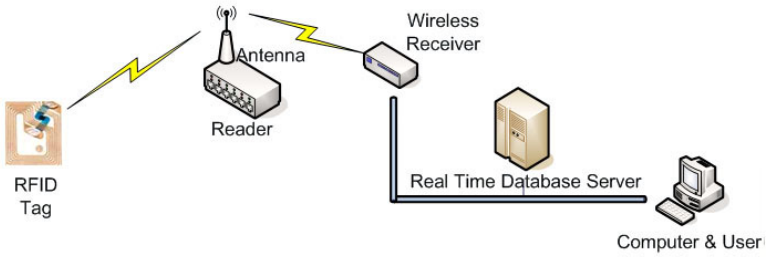

Figure 2.4 *How the RFID tag system work [20].*

- The class of objects (24 bits) that specifies the class of the product
- The serial number (36 bits) that uniquely identifies the individual item

The EPC is embedded in a microscopic tag that is applied to each item. Each tag will then be read along the way, from special sensors (RFID) and the data it contains will be stored in specific lists.

Companies, for example, need to exchange data about their products with other companies and to do that they need an infrastructure that is capable of handle a large amount of information and the EPC global Network has created the EPC Network [19].

The EPC Network is a network that, thanks to hardware (tags, readers) and software, can link the individual server/database of subscribers/users.

The EPC Network system allows the identification of each object across the network through the service ONS (Object Naming Service). The ONS is a global register that performs functions similar to the DNS (Domain Name Service). Based on the received EPC code, the ONS provides to the EPC Middle-ware the address of the EPC information Service. The EPC Middle-ware is a software that collect, store, and filter data received from the reader or the readers. In the EPC information Service (EPCIS) are stored the information about the product.

The EPC and all data relating to the product are registered within the local server (EPCIS) connected to the Web. Whenever companies will want to see the updated data they will be able to connect to the database and, if they have permissions, they can directly manage any kind of change on the information. Finally, the markup language PML (Physical Markup Language), which is specific for the communication

Figure 2.5 *How the QR code system work [25].*

via the web, is used to describe all the data related to products such as: lot number, date of manufacture, the proper use, proper preservation of the product, and so on. The PML language is written in XML and acts as an interface between readers and applications that wish to access the data via the EPC Network.

There are many solutions to integrate the RFID tags into the IPv6 addressing system [21]. The addresses in the IPv6 are written with 128 bits and that means that 1038 addresses can be used. A solution could be to use 64 bits of the IPv6 to indicate the RFID tag identifier and the other 64 bits to indicate the gateway between the RFID and the Internet[22]. This method cannot be used if the RFID identifier is longer than 96 bits. In this case an agent is introduced into the network, which will map the identifier into 64 bits becoming like an ID interface of the IPv6 addresses [23]. Other solution is to embed the header and the RFID message into the IPv6 payload [24].

QR Codes

The Quick Response codes are two-dimensional bar-codes (2D) or, better, a matrix composed of black modules arranged in a square pattern. It is used to store information that is generally intended to be read by a smart-phone with special application.

In only one cryptogram 7,089 numeric characters or 4,296 alphanumeric characters are contained. These codes can be applied everywhere, in magazines, on packaging, on posters and they give an huge potential to the advertising [26].

The QR Code was developed in 1994 by the Japanese company Denso Wave to track components of automobiles in the factories of Toyota. Later in 1999, the Denso Wave has released the QR codes freely licensed facilitating their widespread especially in Japan.

To read a QR code with the mobile phone it is really easy, the user has only to take a picture of the QR code and, using a specific application, he will be directed to the URL containing the entire specific item associated with the code. These codes can also contain text or phone numbers, and, in Japan, they also substituted the business cards.

In 2005, in the United States was born the Semapedia project that allows connecting, via QR code, the physical locations with their descriptions on Wikipedia. Now the project is offline, but it was one of the first try to connect real word with the virtual one [27].

From September 2012 has started in Italy an international photo contest, Wiki Loves Monuments, whose purpose is to collect images of the artistic heritage from the various regions with the porpoise to share them (with open license) on Wikipedia. Through this initiative it may be possible to make an estimation of the monuments on the Italian territory and assign, to each of them, an identification code [28].

Because QR codes are under a free license, on the Internet there are many free sites for reading (or better decoding) and writing (or better encoding) these codes. An example is the website where you can define the size of the cryptogram, the color, the content and the level of security (in terms of error correction). To read these codes just download the free software from the Internet on the smart-phone, take pictures of the cryptogram and then the device will automatically decode the content [29].

A variant of the QR code is the Micro QR code that is a reduced version. It is used for applications that require limited space and a smaller amount of information, such as the ID of the printed circuits. There are different forms of Micro QR codes and these can contain up to 25 alphanumeric characters [26].

2.2.2 Security and privacy

The IoT is quite easy to attack because usually all the components are left alone so it is easy to attack them. Moreover most of the communication are wireless and

they are exposed to eavesdropping. In addition the low energy capabilities and the low computer resources of the devices cannot calculate complex security schemes. The bigger problems concern the authentication and the data integrity.

The authentication is hard because, usually, a specific infrastructure is required and different authentication messages have to be exchanged before establishing a connection. But in the IoT sensors and RFID tags cannot exchange so many messages. Anyway there are some solutions for the sensor networks [30] and one of the solution can be to use a gateway between the sensor network and the Internet. Anyway it is still quite difficult to protect these networks from the man-in-the-middle attack.

The data integrity has to protect the data from modification, during the transmission, without the system recognize the change. Data are always exposed and they can be modified both when they are stored and while they are transmitted to the destination [31]. In the first case, it is a good solution to protect the memory both for the RFID tag and for the sensors, in the second one, an Keyed-Hash Message Authentication Code can be used [32]. Anyway all the solutions use cryptography and that requires bandwidth and energy consumption. Some light symmetric key cryptography solutions are illustrated in [30] [33] [34].

Other problem for the IoT is that people cannot control their personal data on the Internet. It is hard for them to know where the data are stored, who collect the data and for how long. The cost of the servers to store data is becoming so cheap that it is not a problem to store a huge amount of data. Anyway the personal info should be stored only until they are strictly necessary and the user should agree and set the privacy parameters. Moreover to guarantee that the provider of the system will access only to the personal data of the user that are strictly necessary, a privacy broker can be added to the system that operates like an interface between the services and the data [35].

In case of sensors network the problem of privacy is really difficult. An example could be a security system with cameras. In this case people´s faces will be recorder and, to provide privacy services to them, or the faces of the people are blurred [36] or people have not to be in that area to not be recorded [37].

In case of RFID tag, to be sure that the request to access to its info is coming from an authorized reader, authentication procedures can be used [38].

To avoid eavesdropping the signal transmitted by the reader can be manipulate to be similar to a pseudo-random noise that will be modulated by the tag [39]. Last problem is to delete the information from the web when they are not useful anymore and it is still an open question.

2.3 Technical challenges and limitations

2.3.1 Sensor network

One of the most important elements of the Internet of Things is the sensors network. A sensor network is a network formed by embedded devices that are able to capture the data, process them and transmit them for different kind of applications. The combination of: new technologies as MEMS (micro-electro-mechanical system); wireless communication standards and digital electronics permit to have a network based on low-power, low-cost, and multifunctional sensor nodes [40].

In a sensor network the nodes are densely distributed and each node uses a broadcast communication paradigm instead of a point-to-point one. Moreover this network it designed so its configuration can change easily and quickly. Creating a network of sensors that collaborate with others allow to observe better the phenomena because they can be placed next to the phenomena itself or even in it. Some examples could be founded in the medical field where the distributed wireless sensor nodes can be used to monitor the health of people in their everyday life or to constantly control people with chronically ills without use invasive instrumentation [41, 42]. The sensors can be placed into houses or buildings, on cars or trucks, on the bottom of the ocean or they can be attached to animals, which wanted to be studied, and so on. They have to be very resistant and they need to have a long lifetime and their accuracy cannot decrease.

- Sensor node architecture

  The sensor node architecture is shown in Figure 1.6 and it is composed by multiple pieces that are [43]:

  - Sensor
  - Processor

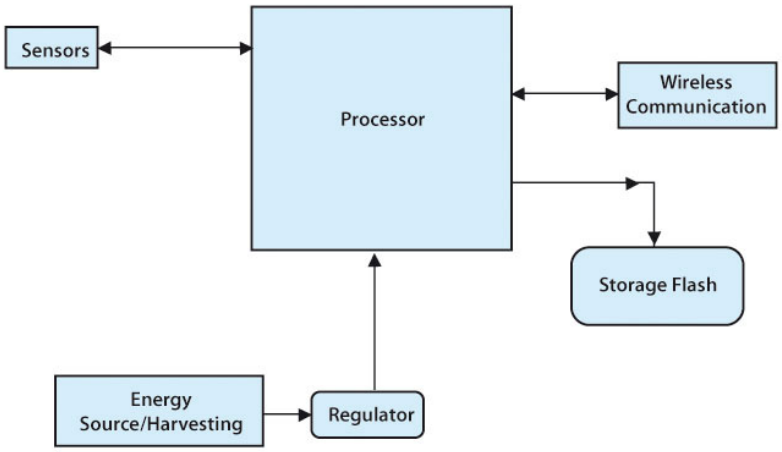

Figure 2.6 *Sensor node architecture [45].*

- Wireless communication system
- Storage system
- Energy harvesting or power source
- Regulator

To better understand how the sensor node works, its components are analyzed in details.

- The processor of the wireless sensor node is the core element where the data captured can be calculated and eventually processed directly into the node. If the processor has enough power and a storage system is included in the node, functions like statistical sampling, aggregation of data, and monitoring of system health and status can be done in the node itself [44]. In the processor can be included an algorithm for the energy management control.
- The storage system can be different from one node to another and it depends on the configuration of the net. If the network is conceived to sent data instantaneously to the other nodes or to the central one the storage data is not so important. Instead if the data are processed into the node and then only some results are sent to the central one a storage system is needed. Flash memory or nano-electronics-based MRAM can be used as a memory. The first one has the disadvantage of some limitation in terms of reuse [46] .

- The sensor is the part of the node that captures the data and that connect the real world with the digital one. There are so many different kinds of sensors in terms of size, price, accuracy, resolution and power usage.

- The wireless communication element has the task to receive and transmit data packets from/to other nodes. Usually it is the part of the device that uses the most part of the energy required by the node. The design of the radio part is based on three layers: physical layer, MAC (Media Access Control) and network layer. The first one sets the physical link between the transmitter and the receiver. The second one coordinates the access to the physical channel that is used at the same time by different radios. To decide how the transmitters use the channel is used the CSMA (Channel Sense Multiple Access).To transmit the data ZigBee or Bluetooth standard are used for short range communication and IEEE 802.11 can be used for a distance in a range of 50-100 m [47]. The third layer, the network one, has the task to decide the path that the data have to follow through the network to reach the destination from the sender [46].

- The power source/harvesting system supplies the power to the node. It can be made using both battery and fuel cells or harvesting energy from the environment around the sensor node. The energy storage can be used if the energy harvesting technique is used to store energy and to supply it in a second moment when the energy requirement from the node is bigger than the one harvested.

- The regulator is used to convert the DC power received from the energy system into a fixed input that will be used by the processor and the antenna [48].

As shown in Figure 2.7 the sensor networks can be used for volcano activities monitoring [49] or to study plans or animals behavior in environments where the presence of the humans is not so easy or where humans could modify the data collected [50]. The wireless sensor network can be used to detect the structure and the straight of a bridge to prevent it collapses [51] and to avoid a tragedy or it can be used to keep under observation the pressure of the tire (TPMS) of cars for safety aspect and control applications [52].

These kinds of networks have different requirements according to the wide range of applications that can be reached. Every sensor has different specification regarding

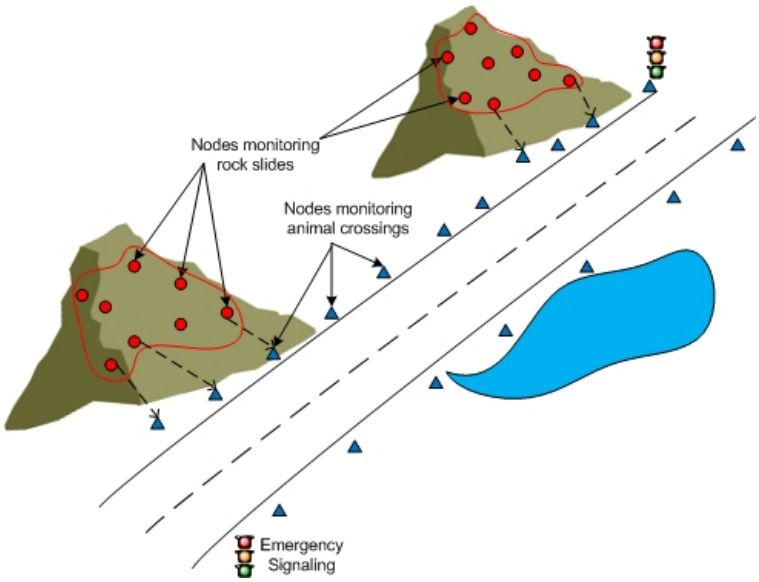

Figure 2.7 *Some sensor network applications [53, 54].*

the way they capture the data, the design dimensions and its sizes, the cost, the capabilities of storage and communication systems, the protocols implemented to communicate with other nodes of the network, the power sources and so on.

Depending on the application, the sensor has to work from 2 to 10 years. If an AA alkaline battery of 1.5V is used to power the wireless sensor network, the average power consumption of the node should be between 50?W and 250?W [55].

2.3.2 Connect a large amount of devices with high energy efficiency

There are some limitations for the sensors network because the nodes have a limited memory and finite computing capacity. Moreover other really important challenges for the node are its portability and its energy autonomy. That leads to the necessity of compact and low-cost energy sources. If the energy source is limited it is really hard to maximize all the parameters and the capabilities of the device at the same time. If the duty cycle (that is the fraction of time that an entity goes into an active state in proportion to the total time considered) is getting shorter the sensing reliability is decreased. Also, if there is an increment of the transmission rate, much more energy is required instead, if there is a lower transmission range, more hops

Battery type	Anode	Cathode	TGED[2] [Wh/kg]	PGED[3] [Wh/kg]	Fraction [%]
Lead-acid	Pb	PbO_2	252	30–50	12–20
Ni–Cd	Cd	Ni oxide	244	45–80	18–33
NiMH	MH[1]	Ni oxide	240	60–120	25–50
Li-ion	Li_xC_6	$Li_{(1-x)}CoO_2$	410	110–160	27–40
Li-polymer	Li_xC_6	$Li_{(1-x)}CoO_2$	410	100–130	24–32

1: MH, metal hydride, data based on 1.7% weight of hydrogen storage; 2: TGED, theoretical gravimetric energy density; 3: PGEd, practical gravimetric energy density.

Figure 2.8 *Gravimetric energy density of some battery systems [57].*

are needed so more nodes will work and that means more nodes have to be powered.

In conclusion the central question is to find an efficient way to power the network in a way that its operability will be not decreased. Let's see some ways to power the devices.

Battery

Most of the nodes are powered with batteries and this is a huge limitation for the wireless network. Using battery as a power source means that the nodes have a finite lifetime and that they will work until the batteries will be empty. Considering these limitations they support finite applications or their batteries need to be recharged or changed. Charging or changing batteries implies more costs for the maintenance of the network and sometimes it is not so easy to organize due to the complexity of certain network or the allocations of the nodes themselves. Moreover the energy density of the batteries has increased really slowly during the time, growing of a factor of three in the last fifteen years [56]. For these reasons the usage of the batteries is not so good and there are studies on how to power nodes in a more efficient way. To avoid frequent interventions on the nodes it is possible to use larger batteries or a low-power hardware. Both of these solutions are not perfect because, for the first one, having bigger batteries means to increase the size of the node and the cost as well and, for the second one, the computation capacity will decrease and the range of transmission will be reduced. Some example of different types of batteries and the amount of energy provided can be seen Figure 2.8.

A way to solve the problem it is to optimize the usage of the energy to make the battery lasts longer and to improve the lifetime of the nodes. Some examples of this solutions could be the usage of different kind of duty cycle strategy [58], or different routing and data transmission protocol [59, 60]. Moreover different MAC protocol

as SMAC [61], BMAC [62], XMAC [63] can used to reach the same aim. With these ideas it is possible to increase the lifetime of the application and to delay the replacement of the batteries and decrease the maintenance of the network. Anyway they don´t solve the problem of the main limitation of the battery so there are other ideas that have been still studied.

Fuel cells

A different solution could be the usage of energy storage system in combination with large energy system like the miniaturized fuel cells. The fuel cell is a device which converts chemical products as hydrogenous and oxygen, into electric energy without any thermal reaction. Skipping the thermal reaction allow to avoid the limits of Carnot´s theorem in which the maximum efficiency of a thermal machine is bound by the temperature in between it works [64].

As it is possible to see from Figure 1.9 the fuel cell is formed by three different components: the anode, the cathode and the electrolyte. On the cathode side we have oxygen (that is taken from the air of the room) and on the anode side the fuel (that could be the hydrogenous). The aim of the catalyst anode is to dissociate the hydrogenous into electrons and into positive ions. Then the protons will pass through the electrolyte and they will reach the cathode and react with the oxygen molecules and form water. The electrons, instead, are not able to pass the electrolyte that is made in a way to be electrically insulating and they will flow in an external circuit creating the current that will be used. Fuel cells produce more portable power than battery and they can reach a maximum power capability of 1-50W [64].

Both the battery and the fuel cell use the same principle to create the electricity but the difference is in where they store the energy. While in the battery the energy is created and store, in the fuel cell is not possible to store the energy but it only converts it and a reservoir is needed. Moreover the fuel cells are always refilled by the reactive elements that they need for the chemical reaction so, there is no need to substitute them [66]. The fuel cells can be used in three big categories: military area, health care area and portable electronics. They can be used to power portable devices as personal digital assistant (PDA), cellular, notebook or in military environment where more light and portable batteries are required.

Anyway the reality is that it is not easy to realize fuel cells. There are different king

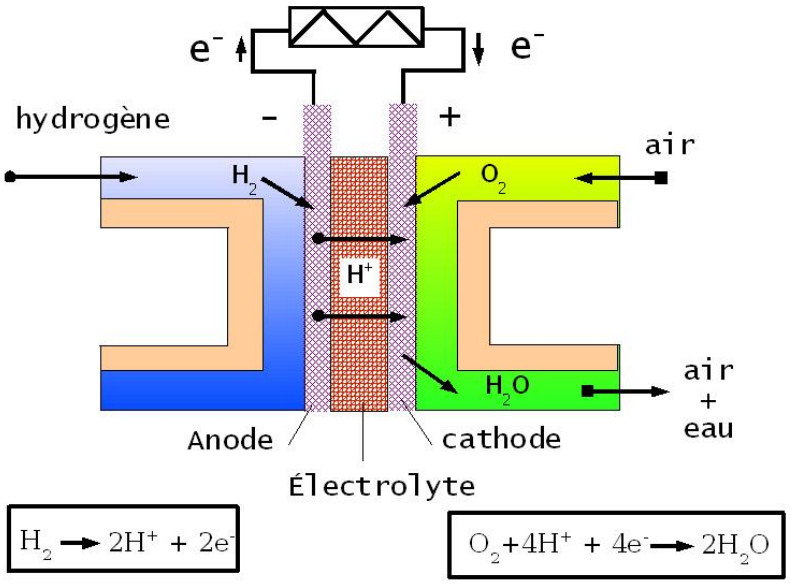

Figure 2.9 *Scheme of the hydrogenous fuel cell[65].*

of fuel cells regarding the type of electrolyte or the material to use for the electrodes. More over have a reliable fuel cell that is not expensive and efficient is quite difficult [53].

Both the battery and the fuel cells are not a good solution for nodes that have to operate for really long time in the wireless sensor networks. For this reason two different solution were thought to solve the energy problem of the node:

- Define new communication standards that require less energy to work
- Try to gather the energy needed by the node from the environment around the node

Both solutions are explained in more details in the next chapters.

3. RADIO TECHNOLOGIES

Sensors collect a huge amount of data that will be sent to the server or to other nodes. The transmission rate can reach billions or trillions bytes per day and that requires bandwidth and power. Moreover different nodes have to communicate to each other so new and more efficient standards are needed. Moreover less energy has to be used by the node to transmit and receive data.

The standards that will be analyzed in the following paragraphs are: the ZigBee; the Bluetooth Low Energy (BLE); the IEEE 802.11ah.

3.1 ZigBee

It is a high-level communication protocols that is used to create Personal Area Network (PAN). The IEEE 802.15.4 standard specifies the Physical layer (PHY) and the Media Access Control (MAC) layer upon which the ZigBee stack works. The ZigBee standard was thought for devices powered by battery and it is used for low-cost, low-power wireless Machine2Machine networks. It is really suitable for monitoring applications in environment as private home or industrial applications because the transmission distance can be 10 - 20m and, in the condition of line-of-sight, it is possible to reach 2000 meters.

3.1.1 Architecture

The ZigBee protocol stack is shown in Figure 3.1and it can be divided into 3 main levels:

1. Physical/Data level
2. ZigBee Stack level

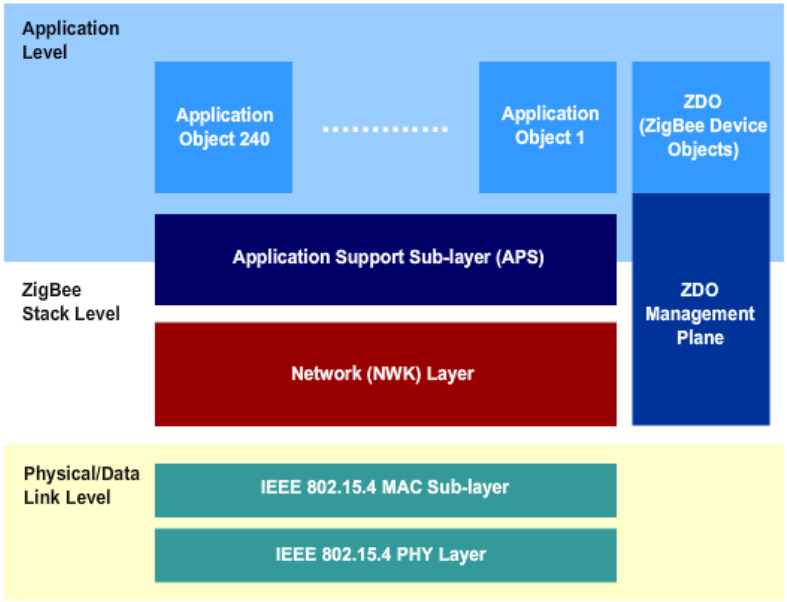

Figure 3.1 *ZigBee protocol stack [67].*

3. Application level

The topology of the network that implements the ZigBee standard can be: point-to-point, star, three or mesh. Each type of network requires a controller node that starts the network itself and manages it.

The main node of a star topology network is a Full Function Device (FFD) that becomes the coordinator of the network and manages the communications with both Reduced Function Device (RFD) and the FFD. To create the other topologies the FFD are connected to each other and the RFD can only be an end node of the network.

All the three main layers are analyzed in the following paragraphs. 1. Physical layer (PHY) The Physical and MAC layers work working in different bands depending on the country in which the devices are used. These bands are called ISM (Industrial, Scientific and Medical) bands. Sixteen channels compose the 2.4GHz band and each of them has 5MHz of bandwidth. They work at:

- 784 MHz in China
- 868MHz in Europe

- 915MHz in U.S.A
- 2.4GHz band is used everywhere

The air interface is based on the Direct Sequence Spread Spectrum (DSSS) and, in the 868 and 915MHz band, the BPSK (Binary Phase Shift Keying) modulation is used. The OQPSK (Offset Quadrature Phase-Shift Keying) is instead used in the 2.4GHz band [68]. Every channel has a data rate of 20 kbit/s for the 868MHz band, 40 kbit/s for the 915MHz band and 250 kbit/s for the 2.4GHz band. The PHY includes also other specifications as receiver Energy Detection (ED), Link Quality Indication (LQI) and Clear Channel Assessment (CCA). It is possible to address more than 65000 nodes for network [69].

MAC layer (Media Access Control)

It is responsible for the access of the media and uses the un-slotted CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) method to regulate the communications between the devices. For every transmission an acknowledgment is sent in order to control the flow, to validate frames, to retransmit data (in case of failure) and to synchronize the network. This layer is also responsible for the association of new networks and it uses the AES-128 bits encryption system to perform security services.

There are four different frames that are exchanged:

- Beacon frame that is used to transmit beacon messages
- Data frame to transmit the data
- Acknowledgment frame to be sure that the data were received correct
- MAC control frame for management information

The coordinator decides the format of the super-frame exchanged between the nodes and it is divided into 16 slots. The Beacon frame is sent in the first slot of the super-frame. In this way a super-frame is sent between two consecutive Beacon messages. The Beacon frames (shown in Figure 2.2) are used to send info regarding

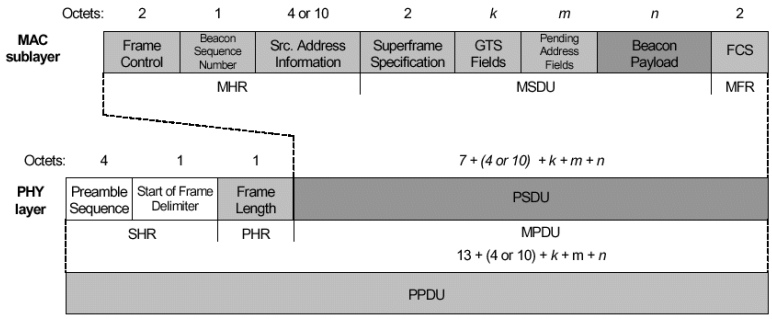

Figure 3.2 *Structure of a Beacon Frame [70].*

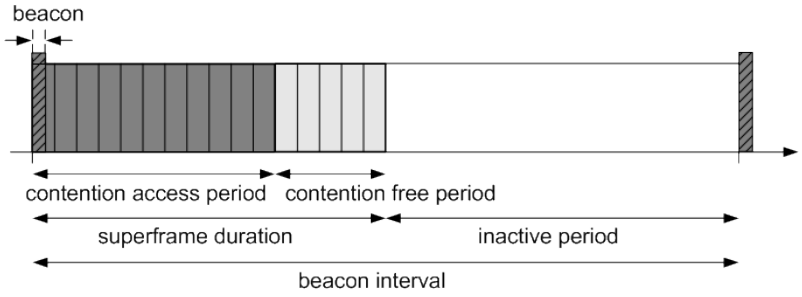

Figure 3.3 *Super-frame structure with GTS [71].*

the structure of the frame and the repetition interval of the Beacon frames. They are also used to identify the network and to allow the node to be synchronized with the coordinator before the start of a communication.

If a station wants to communicate with the coordinator it has to wait to receive two consecutive Beacons and, in this way, it will be synchronized with it.

The interval between two Beacons is called Contention Access Period (CAP). If the coordinator wants to set a transmit interval for a certain device, the ending part of the super-frame will contain a Contention Free Period (CFP). This procedure is called Guaranteed Time Slot (GTS) and it is used to avoid collisions during the transmissions. If there are still some collisions the Carrier Sense Multiple Access (CSMA/CA) protocol is used.

The transmission can occur:

- From a node to the coordinator

- From the coordinator to a node
- Between two nodes without the coordinator

In the first case, if the network is a Beacon-enabled, the node waits to receive two consecutive Beacon frames. After the reception of the second Beacon the station will be synchronized with the controller and it will transmit the data to it. The coordinator receives the packet and it can send an ack. If the network is a non Beacon-enabled, the station uses the CSMA/CA protocol and, as soon as the channel is free, it starts to transmit the data to the coordinator. If the data are correctly received, the coordinator ends the connection and eventually it sends an ack message.

In the second case is the coordinator that has to send data. In a Beacon-enabled network the node receives the beacons, then it send a data request to the coordinator. After that the coordinator sends first an ack for the data request and then the data that has to transmit. The node that receives the data ends the communication with an ack frame. In a non Beacon-enabled net the steps are the same except for the first one. The station uses the CSMA/CA to listen to the channel and transmit the data request as soon as no other nodes are transmitting.

The third option is the case of the point-to-point connection and, in this case, the devices use the CSMA/CA protocol to exchange data. If the network is more complex and bigger, usually a token is used to regulate the communications between the different stations.

Network layer

It is responsible for a variety of actions as routing, adding or removing devices from the network. Moreover it has the aim to start a new network and to assign network addresses. It also performs route discovering in mesh topologies.

Application Support Sub-layer (APS)

This layer allows the communications with the different applications and with the endpoints. Each node of the network can have different applications and each of

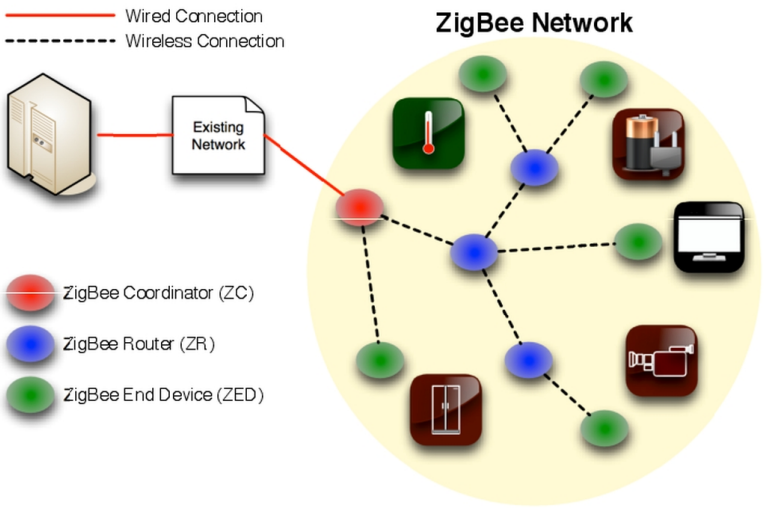

Figure 3.4 *Different type of nodes in a ZigBee network*

them is called endpoint. Each endpoint has a specific address and they are numbered from 1 to 240. The number 255 is instead used for the broadcast endpoint. In between the APS and the application object layer there is the Service Access Point (SAP) that implements four different kinds of operations: Request, Confirm, Response and Indication.

ZigBee Device Objects (ZDO) and Management Layer

The ZigBee Device Objects is an endpoint numbered with 0 and describes the type of the node of the device. As shown in Figure 2.4 there are three different kinds of nodes:

- Coordinator: it can connect different networks and has the task to start the network
- Router: forwards data from other devices
- End Device: can talk only with the other two nodes

The Management layer allows the communications between the ZDO and the Network and APS layers in order to access the network and perform security services (security key management, data stream de/encryption).

3.1.2 Energy consumption

The protocol can support beacon and non-beacon enabled network. Beacon enabled: the router sends periodically a beacon message to point out its presence. In between two transmissions the node will sleep so the duty cycle will be lower and the battery life will last longer. The sleep interval depends on the data rate. The nodes are awake only during the transmission. Non-beacon: the CSMA-CA mechanism is used and, usually, the routers have to listen the channels continuously. That means they have to be powered all the time so more energy supply is needed. It is possible to have heterogeneous network where some nodes receive continuously and some transmit only when they capture some input. In this case the power consumption is completely asymmetric for the two different kinds of devices. The devices using this protocol can run for 5-10 years.

3.2 Bluetooth Low Energy

The Bluetooth Low Energy was introduced in 2010 and allows the devices, which implement it, to have short-range communication with different kinds of peripherals. With the new BLE it is possible to extend the communication with devices used into sport and health care field. This protocol does not support streaming but it is perfect for sending a small amount of data. The devices that work with this standard can be single or dual mode. A dual mode node can implement both the BLE and the classic Bluetooth standard.

It is possible to use both point-to-point and star topology but the standard is thought to be used for point-to-point connections [72].

3.2.1 Architecture

As showed in Figure 3.5 the protocol stack can be divided into three main groups [73]:

1. Applications
2. Host
3. Controller

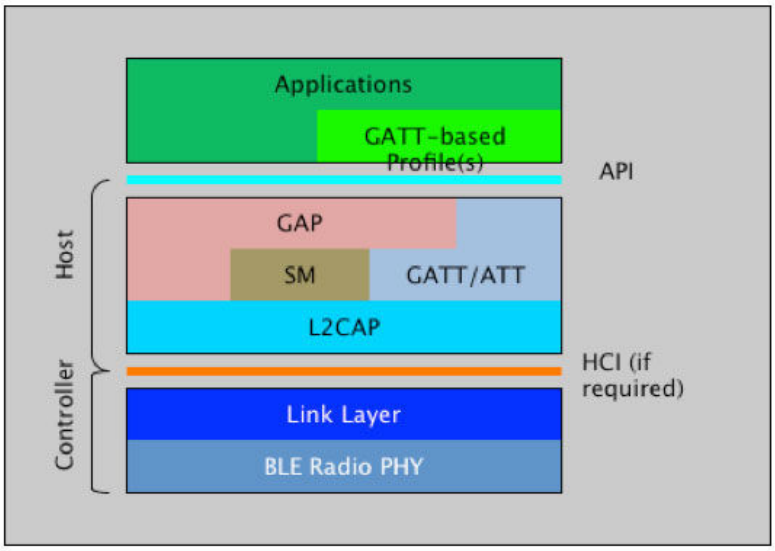

Figure 3.5 *BLE Protocol stack [73]*

Control layer

The control layer has different tasks as the organization of the low-level communication on the physical layer, the capture of packets and the managing of the radio link. It is also responsible, for the synchronization of the communications and the queue management of the data packets.

It operates in the 2.4GHz ISM band and, to access the channel, it uses two different schemes: the Frequency Division Multiple Access (FDMA) scheme and the Time Division Multiple Access (TDMA). In the TDMA scheme the communication is allowed only during pre-set slot intervals. In the other scheme instead, 40 channels spaced of 2MHz from each other are used.

Of these 40 channels, 3 are used to discover devices via advertising events and the other 37 to send data using the pseudo-random frequency hopping sequences. The nodes that belong to the same pico-net, during the connection request, will receive commands regarding how to change frequency [74]. After a connection request, the initial parameters are exchanged and set via the same channel already used for the Advertising messages. The data will be then transmitted using another channel.

The data rate is 1Mbit/s using a GFSK (Gaussian frequency-shift keying) modulation. It can also be used as a firewall to receive packets only from a specific

device.

As shown in the Figure 3.6 the packet has a variable length and can be of two different types:

- Data packet
- Advertise packet

The packet has 1 bytes of preamble, 4 bytes of Access Address to show the RF channel used, a PDU section which length can vary between 2-39 bytes and 3 bytes of CRC. The Access Address specifies the packet destination. If the packet has to be sent to a specific node, 32 bits will compose it otherwise, for the advertising links, a defined sequence of bits will be used.

For the 3 advertising channels, the header of the PDU specifies the length and the type of the payload and the address of the device that is sending the advertising message. The PDU section is used to send or the connection request or the parameters to set up the connection [74].

So the smallest packet will be 10 bytes and the longer one 47 bytes so the transmission time will be in the range of 80?s to 0.3ms. The 32 bits of the Access Address are used on each packet and, thanks to them, it is possible to connect millions of Slave nodes.

A sequence long 48 bits identify each device and it is divided into 3 fields:

1. Lower Address Part: it is 16 bits long and it is set by the constructor of the device and it is part of the Access Address that is in front of the header of the packet;
2. Upper Address Part: it is 8 bits long and it creates the Header Error Correct to correct the packet if an error occurs;
3. Non- significant Address Part: it is composed by 16 bits and, with the UAP, defines the Organizationally Unique Identifier that identifies the code of the constructor decided by the IEEE [74].

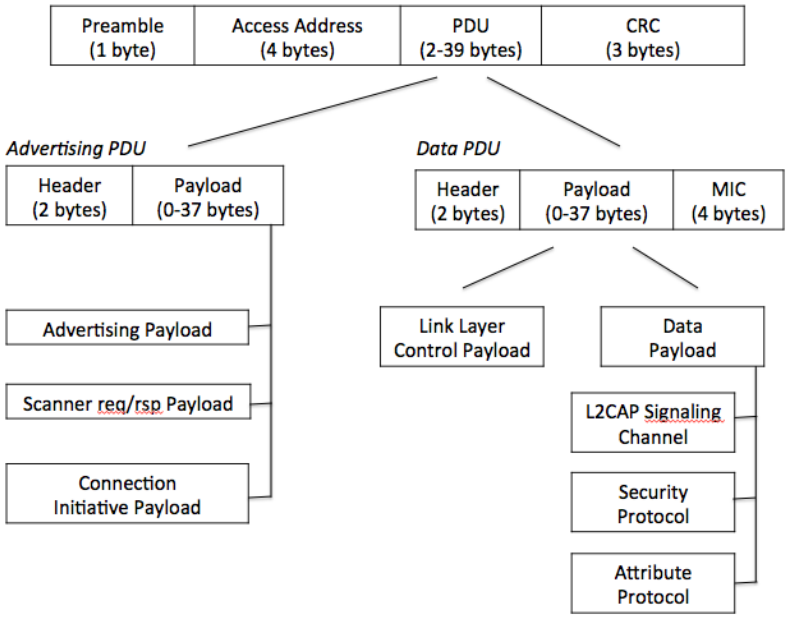

Figure 3.6 *BLE packets*

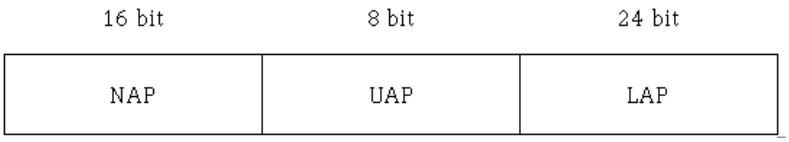

Figure 3.7 *Address of the device*

The BLE has an identification code for the different profiles of the device and it is called Universally Unique IDentifier (UUID) and it is 128 bits long.

The Host

It manages the upper part of the protocol stack and, sometimes, between the host and the Control, a Hardware Controller Interface (HCI) is needed in order to allow the communication in between them.

The host is organized into multiple sub-layers. They are: the L2CAP (Logical Link Control and Adaptation Layer), the SM (Security Manager), the GATT (Generic Attribute Profile), the ATT (Attribute Protocol), and the GAP (Generic Access Profile).

The L2CAP communicates directly or by the HCI with the Controller and its task is to segment and multiplex packets for the lower level.

The GAP is used to pair and link the devices and it is used by the Applications to perform the different Bluetooth modes.

There are 4 different modes a device can operate: Advertising mode, Scanning mode, Slave and Master modes.

- Advertising mode is used to send info to the device that are in the proximity and that can be linked at the node.
- Scanning mode captures and read the advertising packets.
- The device which sends the Advertising mode, will be the Slave one, instead, the one that will start the scanning, will assume the Master mode.

The device that is in the Scanner mode will receive all the advertising messages from the other nodes and, if it is in the ?active scan? mode, it can ask for more information. A device can be a scanner-only or an advertising-only. In the first case the device will passively receive all the advertising messages and, in the second case, it will just send advertising packets [75].

The Slave and Master mode organize the communication between devices by allow them to write or read or ask to each other information. The advertising is repeated on all the channels with a frequency between 10ms to 10s. A scan window and a scan interval characterize a scanner device. To start a conversation one device has to be in the Advertising mode and another one in the Initiator (active scan) mode. When the Scanner receives a packet, it sends a connection request using the same channel used for the advertising message received. The advertising event ends when the Advertising device accepts the request. Once the connection is established, the advertising node become the Slave and the scanner one assumes the Master role. The data are exchanged during the Connection event on a different channel from the one used for the advertising.

After the connection, to reduce the power consumption, the Master will send the connection interval and the slave latency to the slave. In this way the slave will know when to start the transmission, regarding the connection interval parameter,

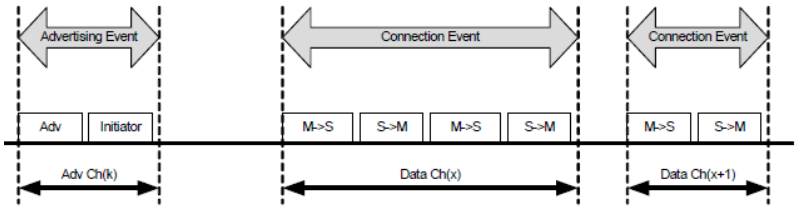

Figure 3.8 *Advertising and Connection events [74]*

and it will know how many connection interval it can ignore without loosing the link with the Master (slave latency).

The SM layer manages the authentication and encryption procedures. To encrypt the data AES-128 bit is used and the SM pairs and distributes the keys. This level is used by the Master device to start the security steps with the Slave device.

The ATT is a protocol to improve the transmission of small packets.

The GATT is the interface with the Application layer and, in order to allow the communication with it, it applies the application profiles. Each profile is specific for a certain application and it defines how the data has to be formatted and read by the applications in order to reduce the amount of data transmitted and to improve power efficiency.

3.2.2 Energy consumption

The BLE it is a good solution for sensors because the device that uses it can run for years using a standard coin-cell battery. That because the BLE implements a lower duty cycle compared with the normal Bluetooth and, in this way, the device will sleep more and be awake only sometimes to send or to receive data. Every time a connection is ended, the device goes to sleep and the link, used for the transmission, is ended as well. Another aspect that allows BLE to have a better power management is the use of the GATT profile.

Using this profile it is possible to send not a stream of data, but small amount of packets during small interval and so the devise is able to save power.

The power consumption depends on the devices and the applications but the transmission time, compared with the classic Bluetooth one, is much shorter (3ms against

Table 3.1 *Comparison between Bluetooth and BLE [76].*

Specification	**Bluetooth**	**BLE**
Range	100 m	50 m
Application	0.7-2.1 Mbit/s	0.27 Mbit/s
Active slaves	7	Implementation depending
Robustness	adaptive frequency	adaptive frequency
Latency (from a non connected stated)	100 ms	6 ms
Power consumption	1 V	0.06 to 0.5 V
Peak current consumption	<30 mA	<20 mA
Service discovery and Profile concept	Yes	Yes

100ms). Moreover, as we can see in Table 3.1, the power consumption of the BLE is 100 times smaller than the classic one and the peak current of BLE is about 10mA smaller than the Bluetooth one.

With this protocol the devices, that use battery, can run over 30 years but the battery usually exceed the cost of the device so it would be better harvest the energy. An example could be gathering the energy from the indoor light.

3.3 IEEE 802.11ah

The IEEE 802.11ah is a standard which operates at a frequency below 1GHz with the aim of reach the 1 Km transmission range and a data rate above 100Kbit/s [77].

Other challenges of this standard is to support a huge number of stations, up to 2000, for the outdoor application and it has to supply a power saving mechanism so the battery of the device will last longer [78]. So one of the aim is to provide a big amount of short packet transmissions made by stations that utilize limited power consumption.

The work on this standard should be finished in 2016 so there are not so much information about the protocol stack and its layers. At the moment the standard is still be studied and revised so some of the solutions, already know, can be changed before the final version. Anyway most of the draft already realized should be stable [79].

3.3.1 Architecture

Physic layer

The IEEE 802.11ah uses different channels: 1MHz, 2MHz, 4MHz, 8MHz, 16MHz but the sub bands of the ISM bands used are different and they depend on the country.

The standard uses an OFDM (Orthogonal frequency-division multiplexing) based modulation, Multiple Input Multiple Output (MIMO) and Downlink Multi-User MIMO (DL MU-MIMO).

For the 2MHz channel, 64 sub carriers are used including pilot, guard and DC sub carrier and 52 of them are used to transmit data. For the 1MHz channel the sub carriers are less than the 2MHz one and only 24 are used to send data. For channel which bandwidth is equal or bigger than 2MH, the OFDM symbol is 10 times longer than the one used in the IEEE 802.11ac [79]. There are different specifications, for the channelization, for U.S.A, for South Korea, for Europe, for China, Singapore and Japan [80].

- Europe uses a band limited in between 863MHZ and 868MHz and 5 channels of 1MHz are used and, later, 2 channels of 2MHz have been added.
- For the U.S.A. the band goes from 902MHz to 928MHz and it is possible to use 26 channels of 1MHz or 13 channels of 2MHz (composed by two adjacent 1MHz channels) and so on up to a maximum of 1 channel of 16MHz.
- For Japan the band goes from 916.5MHz to 927.5MHz. Japan has special rules for the spectrum regulation that says that the channelization starts with an off-set of 0.5MHz and it uses an LBT (Listen Before Talk) method to avoid mutual interferences [81].
- The South Korea has a band from 917.5MHz to 923.5MHz and it uses 6 channels of 1MHz, 3 channels at 2MHz and 1 channel of 4MHz. It used a 0.5 MHz shift of the band in the channelization to avoid mutual interference with wireless system working at low frequencies.

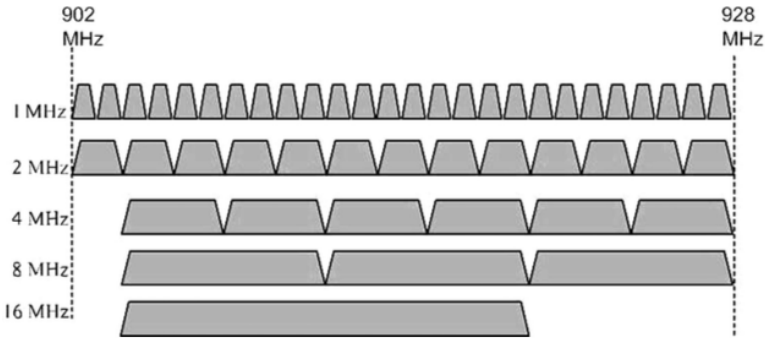

Figure 3.9 *Channelization of the U.S.A. standard [82]*

- For China there are different specifications and the band starts at 755MHz and end at 787MHz. For frequencies between 755MHz and 779MHz the maximum sending power is 5mW, for frequencies between 779MHz 787MHz the maximum power will be 10mW. In the higher frequencies 1 channel with 8MHz or 2 channels with 4MHz or 4 channels of 2MHz are used.
- For Singapore the band is 5MHz wide and starts at 920MHz and ends at 925MHz with 5 channels of 1MHz.

The standard .11ah uses the same 10 MSCs (Modulation and Coding System) of the .11ac and for the 2MHz channel the MCS9 is not available. The IEEE 802.11ah introduced a new MCS10 which is similar to the MCS0 but with 2x repetitions to enhance the reliability of the transmission [79].

MAC layer

The MAC layer is responsible for the management of collisions and defines how the various stations have to access the transmission channels. In case a collision occurs, the packet must be sent again and this will lead to a waste of bandwidth and a transmission delay. To avoid a collision, the protocol .11ah use the CSMA / CA (Carrier Sense Multiple Access with Collision Avoidance) protocol [83].

This protocol is important in networks where the detection of the transmissions of other stations is not very reliable or where the problem of hidden nodes is present. Let's see how the CSMA / CA works.

Before starts a transmission the station listens to the channel. If it is free, it waits a certain time interval called Distributed Inter Frame Space (DIFS), then it will listen again and, if the channel is still free, it starts transmitting the data. During an interval shorter than the DIFS, called Short Inter Frame Space (SIFS), the station waits to receive an ack package from the receiving station. Because the SIFS interval is shorter than the DIFS one, no one of the other stations is trying to transmit while an ack massage is sent.

If the station instead finds that the channel is busy, it calculates a random interval called back off and waits. To make the countdown a timer is decremented each time the channel appears inactive, while it is blocked if the channel is busy. When the timer reaches the value 0 the station will try to transmit again.

Other main tasks for this level are the limitation of power consumption and the reduction of the overhead. In the normal IEEE 802.11 standard each station has an AID (Association IDentifier) given by the Access Point during the handshake process. This ID is 14 bits long but some of them are reserved so only 2007 stations can be associated with an AP. Similar limit is given by the TIM (Traffic Indication Map) that represents the set of stations for which there are frames stored in the AP. The TIM length is 2008 bits. The .11ah standard allows having ID values from 1-2007 to 0-8191 and enlarge the number of the TIM bitmap from 2008 to 8192 [84].

Usually the overhead of the packets contains 3 addresses and it lasts 30 bytes plus 4 bytes of FCS (Frame Check Sequences). The IEEE 802.11ah standard allows using only 2 addresses so the overhead will be shorter. To identify 8000 stations is enough to use 6 bytes.

Beacons messages, sent by the AP, can improve the overhead as well and the solution is to divide them in two groups: short beacon and long beacon. The short ones are sent more often and don?t contain unessential information that can be asked with a probe message [79]. They don?t contain destination address because beacons are always broadcast, the BSSID because it is equal to the sender address and the sequence control. To notify stations about updates, short beacons contain a Change Sequence Field (1 byte) that is incremented with every update. The station knows when it will receive the next full beacon from the optional Next TBTT field. In this way the station could sleep till this moment and save energy.

To organize better and classified the stations this new standard uses a hierarchical

labeling model as shown in Figure 2.10. At the top level, the stations are grouped into 4 pages of 32 blocks each. A page is composed by 8 sub-blocks of 8 stations each. Thus, the first 2 bits of AID encode page number and the next 5 bits encode block, and so on.

So AIDs are assigned regarding to device type, power management mode, location, station's traffic, etc.

Instead of using the NAV mechanism (Network Allocation Vector) to avoid collisions, the .11ah uses the RID (Response Indication Deferral) mode to access the channels. The NAV mechanism was used to stop the other stations to send data while a station was already sending or waiting for an ACK. The neighbor stations know the duration of this time interval from the Duration field of the data frame. The Duration field is not sent anymore in the .11ah standard and that is why The RID mode is necessary.

The RID idles the channels from the stations that are not transmitting ad it is set as soon as the reception of the PHY header is received. The RID can estimated the duration of the interval, within the channel is idle, thanks to the type of response allocated in Response Indication field (2 bit) in the PHY header.

The responses can be [79]:

- Normal response: the RID interval is equal to the SIFS value plus the time to receive the ACK and depends on the data rate and the width of the channel;
- NDP response: The RID interval is equal to the SIFS plus the NDP (Non Data Packet) MAC frame duration;
- No Response: it is used for broadcast message so no ACK is expected and the RID is set to 0;
- Long response: the RID is set to SIFS plus the longest interval of transmission.

To reduce collisions, in networks where the number of the stations are up to thousands, RAW (Restricted Access Window) method is used.

RAW basically divides the stations in groups and the channels available in slots and each of them is used by a group of stations [79]. It is described more in details in the chapter below.

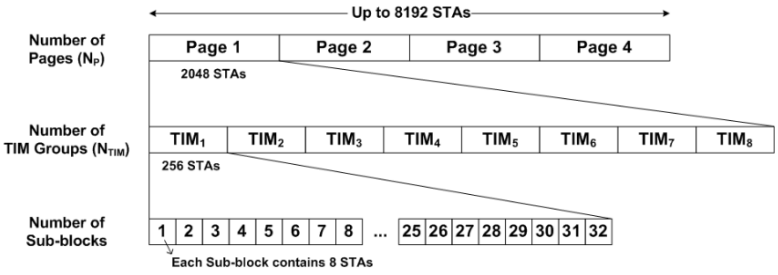

Figure 3.10 *AID hierarchy [85]*

3.3.2 Power management

The station can be in three different modes:

- Power save mode
- Active mode
- WNM-Sleep mode

In the Active mode the station is always receiving.

In the WNM-Sleep mode the station communicates to the AP for how long it will sleep but it will still receive beacon messages.

In the first case the station is awake for some periods and sleep for long interval. During the sleeping period the AP stores all the packets for this station and, in the beacon messages it includes the TIM value. As said before the TIM value indicates whether the Access Point has packets for the station. Periodically the station wakes up and checks the beacon message as soon as it receives it. In case the AP has packets for it, the station sends a PS-Poll frame to the AP asking for the packets. The AP then will send all the packets. If there are no packets stored in the AP the station start to sleep again.

The station sleeps for a long period but the Access Point will not disassociate it if it will receive a frame from the station before the end of the BSS Max idle period. The AP decides the value of the Max idle period and it is exchanged with the stations during the association procedure with the AP. The value is sent with 16 bits and

the maximum value is 18 hours [79]. There are some nodes or sensors that need to sleep longer and send only message to notify their presence is a waste of energy. So the Max idle mode can be modify using 2 methods:

- The AP set a bigger Max idle period for some stations or the stations themselves ask for a specific sleep time interval
- The 2 most significant bits of the Max idle period field are used as a scaling factor. These bits can assume the value 00, 01, 10, 11 and they indicate scaling factor 1, 10, 1000, 10000 and this allow to have a Max idle period 2500 times higher than the basic one

The station can work in two different ways to save the power and these are [85]:

- Non TIM station mode
- TIM station mode

In the first case the station is not receiving the TIM information element from the beacon. When the STA is awake, it sends a PS-Poll frame to the AP to ask if the AP has data in down-link for it. That mechanism is used because sometimes the sleeping mode of some stations is so long that it is easy to lost the synchronization with the AP. In the moment the station sends the PS-Poll message it stays awake and waits for the response from the AP.

In the other mode, the TIM one, the station is continuously receiving the beacon packets and when it recognize that the AP has packets for it, it sends the PS-Poll to the AP asking for the data.

As said before the RAW mechanism regulates how to access the channels for the stations that are allowed to transmit only in the RAW interval. In the Beacon message is transmitted the value of the duration and the time of starting of the transmit interval. Each RAW interval is used by a group of stations so, as soon as the station is awake during that interval, it can start to contend for the access of the medium [78]. To access the medium during its interval, the station uses the Enhanced Distributed Channel Access (EDCA).

It is also used the SFE (Speed Frame Exchange) protocol that allows an Access Point to send data in up-link or down-link in a certain slot of the time interval.

Because the transmission range of the .11ah is up to 1Km, to avoid collision during transmission, the stations are divided into groups called BSS (Basic Service Set). To divide the area covered by the stations to avoid the BSS overlapping problem, two different methods are used: group sectorization and TXOP-based (Transmission Opportunity-based) sectorization.

In the first one the AP allows stations to talk during an interval allocated by a TDM (Time Division Multiplexing) scheme. Each station receives an ID from the AP that indicates to which sector it belongs. If the station doesn't belong to the sector written on the Interval message, it cannot transmit.

In the second case the AP sends a TXOP to all the stations to set up the NAV (Network Allocation Vector) and wait for the ACK from the station it has to talk with. Then the AP switches to the sectorized beam transmission and receiving mode. There are 4 different way to transmit the data [79]:

1. The Access Point send the second frame with a longer PHY header
2. Instead of sending a longer PHY header, the AP sends two frames with short headers
3. Before starting the transmission the AP and the station first make a RTS/CTS handshake and then the AP sends one frame with long PHY header or two frames with short PHY headers
4. It is working as the first two ways but the AP starts the transmission after the reception of a PS-Poll from a station

To save more energy the IEEE 802.11ah standard divides the stations into two main groups [79]:

1. Sensor stations
2. Offloading stations

The sensor stations are all the nodes that send small amount of data and have limited amount of power. This kind of stations can set their own Max Awake time. In this way the sensor will sleep for long period, even months, and exchanges frames with the AP only in that interval. The Max Awake Interval is set during the associating process or later if the node changes its behavior. A maximum of 6000 sensors can be connected to one Access Points.

Moreover the sensors can refuse to receive beacon messages and the Target Wake Time mechanism is used. The station sleep always except for that interval of time. It will then operate in non-TIM mode. At the beginning of each TWT interval, the next one is set.

Due to the new energy harvesting schemes to power the sensors, this kind of nodes have the opportunity to send set a Recovery Intervals and sleep to recover. The offloading stations are the ones that send big amount of data as video streams and can includes cameras, laptops and so on.

4. ENERGY HARVESTING

The energy harvesting is the process used to convert and storage energy from alternative sources into electrical energy to be used by a sensor node. The alternative sources are the ones that are normally in the environment like the light, the thermal energy or the EM signals produced by TV, RF radio or Wi-Fi network [95, 96]. Other alternative sources can be collected from the human body using the body heat dissipation or the walking power [97].

When the energy is scavenged from the alternative sources there are three different situations that can occur for a limited interval of time:

1. Energy harvested $>$ energy required by the system
2. Energy harvested $=$ energy required by the system
3. Energy harvested $<$ energy required by the system

In the first case a storage system is required to allow the device to use the power scavenged when it needs it or better when the third situation occurs. In these cases the energy is harvested when it is possible and then it is used in a second time. In the first case two situations are possible: if the device doesn't need energy, it will be stored into a battery or a super capacitor; if the load is working, it can operate continuously. In the third one, the node has to wait until the storage system is full to work and so it will discontinuously operates [99]. If the energy output from the sources is the same amount of the one required by the load, there is no need for a storage system and the device can work continuously.

It is possible to classify the energy sources into two categories:

1. Device energy source

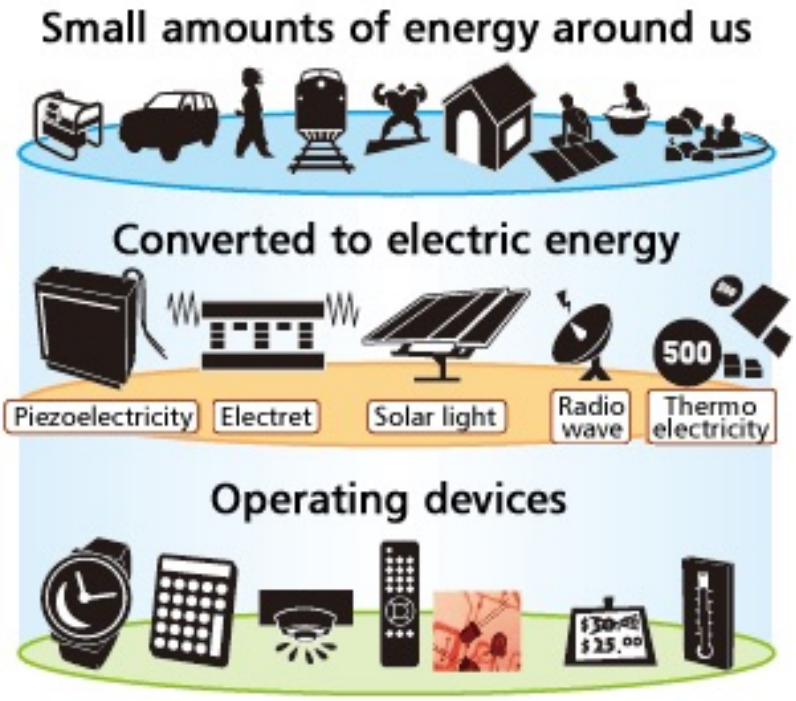

Figure 4.1 *How energy harvest works [98]*

2. Human sources

There are many different kinds of energy harvested by the ambient and they depend on where the sensor is placed and on the aim of the sensor.

They can be divided into four main groups:

- Natural energy:
  - Solar light power
  - Wind power
  - Water power
  - Tree power
- Thermal energy:
  - Seebeck effect
  - Pyro electric

  - Temperature changes

- Light energy
  - In door light power
- Electromagnetic energy:
  - RF -> DC
- Vibrational energy:
  - Electrostatic transducer
  - Electromagnetic transducer
  - Piezoelectric transducer

In the following paragraphs some or them are explained in details and some examples are shown.

4.1 Natural energy

4.1.1 Solar light power

Some examples of the battery storage system are Hydro Watch [100], the Fleck1 [101] and the Heliomote [102] and they all use NiMH batteries. Solar-Biscuit [103] and Sunflower [104] use a super capacitor to store the harvested energy. Prometheus [105] uses both of the sored system.

The Hydro Watch uses a solar panel of 5.84cm x 5.84cm and a TelosB platform. It has an output of 276mW at 3.11V. Two NiMH batteries, that have the capacity of 2500mAh, form the stored system. If the light hits the panel for 30 minutes the batteries receive more than 139mWh.

The Fleck1 use a 11.51cm x 8.51cm panel, an ATmega128 processor with a Nordic nRF903 radio chip. It has an output of 2100mWh/day. The Heliomote uses the Mica2 platform with a solar panel of 9.52cm x 6.35cm and has an output of 198mW with a 3.3V. This node is also capable to monitor the energy still available and its usage.

The Solar-Biscuit is an integrated node and it formed by a 5cm x 5cm solar panel a PIC 18LF452 microchip and a CC100 radio and a super capacitor of 1F at 5V. The solar cell can provide 20mA in fine weather.

The Sunflower instead uses four PIN diodes, a 0.2 F capacitors and a 2.29cm x 3.05cm panel and a MSP430F1232 micro-controller. It has an output of 540?W at 2.7V. Differently from the Solar-Biscuit the super capacitor is not directly connected to the panel and it has a switching regulator that charge the super capacitor from the diodes.

Prometheus uses two 22F super capacitors in series as first storage and a 200mAh Lithium polymer battery as a secondary one. It is formed by a 8.2cm x 3.68cm solar panel and present an output of 130mW to charge the super capacitors. If there is extra energy the super capacitor charges the battery and it has a mechanism, based on software, to monitor the charging state. The super capacitor is the primary storage system because, theoretically and differently from the battery, it has an infinite recharge cycle. Moreover it is better to use the Lithium-based batteries because they don?t have the memory effect of the recharge cycle presented by the NiMH batteries.

An application of a single storage battery similar to the Heliomote is ZebraNet [106] used to track the animal migration patterns by using the GPS technology. The ZebraNet is a collar formed by a comparator, a boost converter and has 14 solar modules and each of them has 3 solar cells in series. Each module produces 7mA at 5V and has an output of 400mW. As Sunflower it is an integrated system and the micro-controller monitor the Lithium battery voltage.

4.1.2 Tree energy

At the University of Washington a circuit was powered with energy coming from a tree. A student found out that, by hooking nails to a big leaf maples and connecting them to a voltmeter, it is possible to measure a continuously voltage. This voltage can be used to power a wireless sensor because it can reach the few millivolts. In fact, using a boost converter an output voltage of 1.1V can be achieved [107].

If an electrode is placed on a plant and a second one on the soil, the plants generate a voltage of up 200 mV [107]. The project aim was to find a way to slowly recharge a

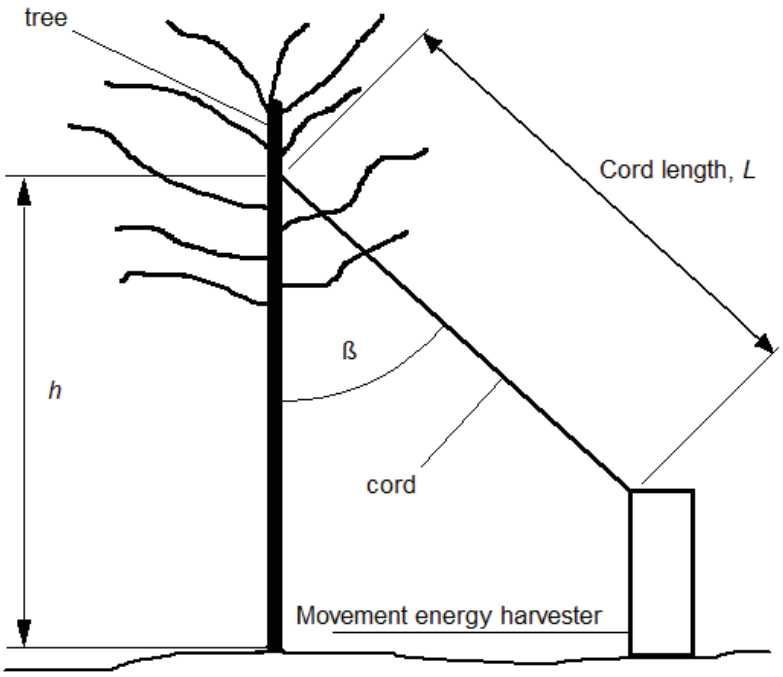

Figure 4.2 *Movement energy harvester scheme [109]*

battery in remote places as forest, for humidity and temperature sensors. The data are then sent, hop-by-hop, to a weather station. Other application could be prevention of blazes, agricultural sensing or border protection. The experiments lead to the opening of a company that is developing highly automated and environmentally responsible embedded system [108].

The trees movements can also be used to gather energy. The device capable of harvesting energy from tree movement, it is able to power a wireless sensor node continuously with an output energy of 0.5mW [109]. The movement of a 6m tall eucalypti tree recharges a nickel metal hydride battery. The energy gathered depends on the wind that makes the tree moves. The device is able to harvest in one day 152 J and it is shown in Figure 3.2.

4.2 Thermal energy

Thermal energy harvesting is based on the possibility to transform temperature variation directly into voltage and vice-verso [110].

If a voltage is applied to the device, a difference of temperature will be created. This

phenomenon can be used to generate energy or to measure temperature, so with this effect it is possible to create either sensors or power source. The thermoelectric effect can be based on the Seebeck effect and the pyro-electricity ability of certain materials.

4.2.1 Seebecks effect

If two junctions, made by different materials or better conductors, have different temperatures there will be a voltage in between them. A gradient of temperature create a heat flow and that means, in a conductive material, there will be a diffusion of charge carriers. This current flow through the hot region of the device to the cold region and it will create a voltage difference.

Thomas Johann Seebeck discovered this effect around 1821 and it is the base for thermocouple and thermopile. Every material has a Seebeck coefficient and the voltage generated by the thermocouple is proportionated to it and to the difference between the temperatures of the two different materials used to create the thermocouple. The voltage is totally not depending on the distribution of the temperature along the conductors.

$$V = \alpha_1 T_h - \alpha_2 T_c \tag{4.1}$$

T_h is the temperature of the hot side and T_c is the temperature of the cold side and α_1 is the Seebeck coefficient of the material A and α_2 is the coefficient of the material B.

The Seebeck coefficient is larger for semiconductors and the sign of the p- type semiconductor is opposite to the one in the n-type semiconductor. A thermocouple is shown in Figure 4.3.

Large thermal gradients are essential to produce practical voltage and power levels. A temperature differences bigger than 10°C are rare in a micro system, so this kind of systems can generate low voltage and power levels [111]. This energy harvest system is available for system that requires low power as remote wireless sensor nodes.

The most used material for thermoelectric generators is the Bi2Te3 [112]. A micro

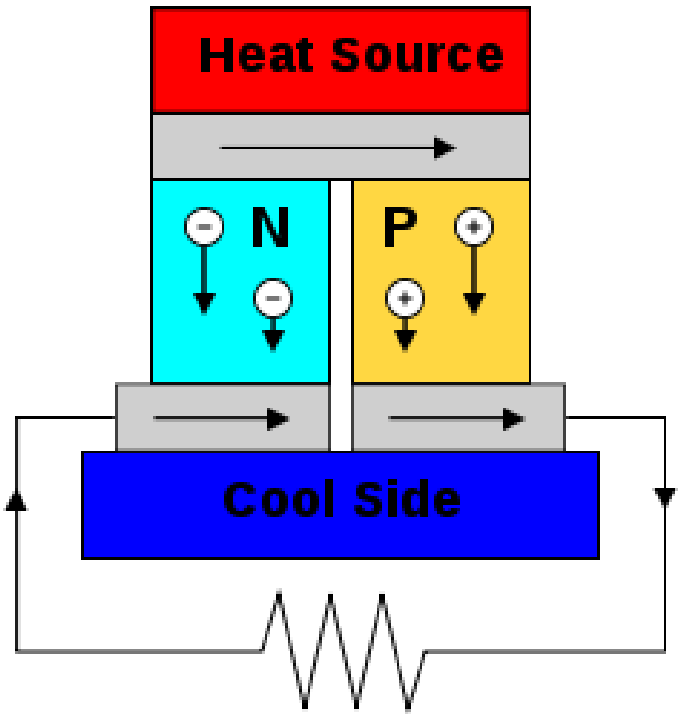

Figure 4.3 *Schematic of a thermocouple.*

machined poly-SiGe-based thermopile, made by poly-SiGe p-type and n-type thermocouple legs interconnected by aluminum pads, were used to power a wristband watch and it has a voltage output of about 1V [113].

An example of the thermoelectric energy harvesting is the wristwatch that converts the power heat into the electrical one that is needed to power the watch itself. Seiko designed this watch. When it is worn on the wrist, the watch absorbs body heat from the back case and dissipates it from the front of the watch to generate power with its thermal converter [114]. So as the temperature difference between the body and the ambient increases the power is generated as well. If the ambient temperature is equal or higher than the body one, the watch will stop working.

4.2.2 Pyroelectricity

The pyro-electricity is the property of a material to generate a voltage when it is cooled or heated for a certain interval of time. So temperature change in time causes a variation in the induced charge [115].

The current generated is:

$$I = \frac{dQ}{dt} = Sa\frac{dT}{dt} \tag{4.2}$$

where Q is the induced charge, S the electro surface of the electrode and a the pyro-electric coefficient that depends on the magnitude of the electrical polarization vector [116].

Using a pyro-electric cells it is possible to harvest enough energy (up to 1.5mJ) to power an autonomous sensor node. For 60°K of temperature variation in a time period of the order of 100s a current in the order of 10-7 A was generated [116].

4.2.3 Temperature air changes

A clock, the Atmos, was designed to be powered by a temperature changes in the atmosphere. An expansion chamber connected to a spiral composes the watch, called the counterweight. When there is an increment of the temperature the gas into the chamber expands and it compresses the spring. When the temperature decreases the chamber decreases its volume and the spring slackens. This movement is enough to power the watch and, because the charging system is based only on the temperature changes, it can last forever [117].

4.3 Radio frequency energy

The electromagnetic energy harvest consists in scavenging energy from the Radio Frequency sources. RF energy harvesting converts radio waves into DC power. To reach this aim the radio waves are captured with an antenna, then the signal is converted into a DC power and, after some conversions the output power is obtained. The block scheme diagram can be seen in Figure 3.4. There are a lots of factors

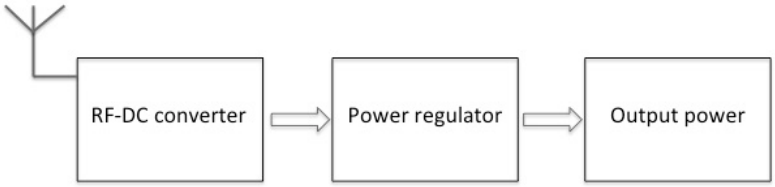

Figure 4.4 *RF harvesting scheme*

that can influence the amount of energy scavenged as antenna gain, distance from the source, conversion efficiency but it is possible to gather up to 250mW.

The radio source can be divided into three main groups [118]:

1. Intentional sources
2. Anticipated ambient sources
3. Unknown ambient sources

In the first group can belong the dedicated power transmitters and the sources in this group can be controlled. That is means that the amount of power scavenged can be increased or decreased tuning the radio transmitter. They can be used to recharge storage devices and keep them fully charged or to provide power for device activation (as RFID tags). Thanks to the control option, they can work continuously or not regarding the applications.

In the second group there are devices like mobile phones or radio and television stations. In this case it is not possible to tune the energy transmitted by the sources but the average amount of power to gather can be predicted. For example a bigger group of people that use their mobile phones is expected to be in a train or bus station in rush hour than during the night. In this way it is possible to harvest mW of power. This harvesting scheme can depend on the time of the day and of the time of the week.

In the last group, instead, there are these radio sources that are neither predictable nor controllable but they can be find everywhere. Some examples can be made in the house environment as microwaves or routers waves.

The broadcast radio and television, the mobile telephony, the wireless networks can be seen as examples of electromagnetic energy sources [95] [119].

If the aim is to use the GSM or WLAN band a really low power density levels have to be expected. For distances ranging from 25m to 100m from a GSM-900 base station it is possible to expect power density levels ranging from 0.1mW/m2 to 1mW/m2 for a single frequency. Instead from a GSM-1800 base station it is possible to receive 0.3mW/m2 to 3mW/m2. The measurements were taken in either two or three orthogonal directions, employing a bi-cone or log-periodic receive antenna in the range of 935-960MHz.

Other idea is to scavenge energy from a WLAN router and the EM field was measured using a printed dipole antenna. The results underline that the power density levels are at least one order of magnitude lower than the one obtained next to the GSM base station.

The company Powercast, using a dedicated RF source close to the device to power, is trying to create an universal chip to charge batteries of devices. The frequency used is in a range of 850-950MHz for a power of 2-5W [120]. In ideal conditions 15mW is received over a distance of 30cm. The maximum transmission power allowed is 3W so for a transmission power of 100mW from a distance of 20cm it is possible to receive 1.5mW [121] or 200 μW from 2m [122].

It is possible to harvest 1.9mW from 1m from a GSM-900 mobile phone that transmits at a power of 2W. These results have been taken using a rectenna with 100% of efficiency completely aligned with the phone antenna [123].

With a GSM-1800 mobile phone that transmits at 1W it is possible to power a led connected to a micro-strip patch rectenna from a distance of 20cm [124].

4.4 Vibrational energy

The vibrational, or better the kinetic energy, is the conversion of mechanical movement in the environment into electric energy. Regarding the mechanism used to produce the energy, it can be divided, into three main categories:

- Electromagnetic mechanism

- Electrostatic mechanism
- Piezoelectric mechanism

All of them require a transduction mechanism and the generator is a mechanical system that couples the transduction mechanism to the environmental phenomena. So the conversion is made in two steps: first the ambient vibration is transformed in motion between two elements and then it is changed into current or voltage with a mechanical to electrical converter.

4.4.1 Electromagnetic

The Electromagnetic induction is based on the generation of electric current in a conductor situated within a magnetic field. The conductor is usually in the shape of a coil and the electricity is generated by two phenomena: the relative movement of the magnet and coil; the change in the magnetic field. The amount of electricity generated depends on the strength of the magnetic field, the velocity of the relative motion and the number of turns of the coil [125].

The electromagnetic generator is formed, as shown in Figure 3.5, by a mass (m) attached to a spring (stiffness k) that vibrates when an external force is applied on it. The losses of the system are defined by the damping coefficient cr.

A resonant generator can be modeled as a second-order, spring?mass?damper system with base excitation. The inertial frame transmits the vibrations to a suspended inertial mass so it will produce a relative displacement between them. The input vibrations are represented as y (t). The relative motion between the housing and proof mass represents the relative motion between magnetic field and conductor. The resonant frequency of the system can be designed to match the characteristic frequency of the application environment [125].

The maximum power that can be generated is shown in the equation below and it is proportional to the coupling factor (k) and the quality factor (Q) and the velocity of the acceleration magnitude of the input vibration (A).

$$P = \frac{k^2 m (QA)^2}{4w} \tag{4.3}$$

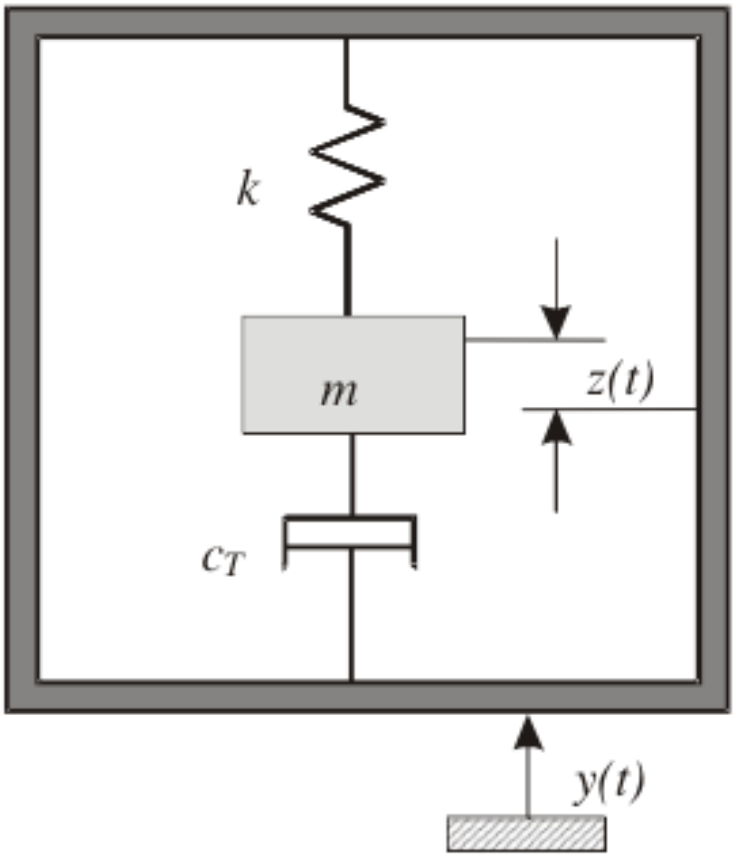

Figure 4.5 *General schematic of electromagnetic transducer [125]*

Electromagnetic generators tend to produce very low AC voltages. Furthermore, the voltage output scales down as the size scales down [126]. For a typical device, the predicted power generation was $1\mu W$ for an excitation frequency of 70 Hz, and 100?W at 330 Hz [127]. A device already on the market can be seen at [128] and can provide an output up to 24mW or 27mW.

This harvesting scheme allows having robustness, high output current and it can last for long period but has low efficiency in low frequencies and in small devices.

4.4.2 Electrostatic transducer

This harvesting scheme is based on the movement of the plates of a capacitor. The movement leads to a change in the electric charges and, this change, is then transformed into electricity. The converters can be divided into two main categories

[129]:

1. Electret-free converter
2. Electret-based converter

Electret-free converters

This converter is formed by a passive structure and by an external polarization source that make possible the mechanical-electrical conversion. The transformation can be reached thanks to a Charge-constrain cycle or thanks to a Voltage-constrained cycle.

- Charge-constrain cycle: when the structure is compressed the plates of the capacitor are closer and the capacitance reaches its maximum value. In this moment the cycle starts and the capacitor is charged with an electric charge under a given voltage. Then, the capacitance decreases because the structure moves back to the initial situation of minimal capacitance. During the process the charge stays constant so the voltage across the capacitor increases up to a maximum value. When the capacitance reaches its minimum value the charge is removed from the structure.
- Voltage-constrained cycle: The cycle starts, as the other, when the structure reaches the maximal capacitance. Thanks to a battery or a capacitor or another external source, the capacitor is charged using a voltage. This voltage stays constant while the capacitance of the structure will decrease (same steps of the previews method) and a current is then generated. As before, when the capacitance reaches its minimal value the charge is removed from the structure.

Some examples of power gathered from these devices can be seen in the next page in Table 5.

Electret-based converter

Instead of having an external source to charge the structure, these types of devices, presented a polarized layer that is attached to one or two plates to polarize them.

Table 4.1 *Some electret-free converters (adapted from [129]).*

Vibrations	Surface	Polarization Voltage	Output Power
10HZ	784mm2	2300V	24μW
1560Hz	4356mm2	6V	1.8μW
50Hz	1800mm2	3V	1.05mW
1300-1500Hz	30mm2	50V	3.5μW
250Hz	66mm2	8V	61nW

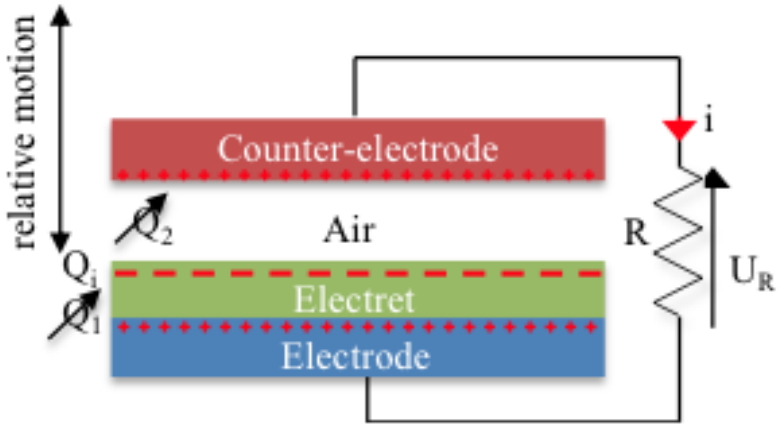

Figure 4.6 *Structure of a electret-based device [129]*

The structure can be seen in Figure 4.6.

The polarization can be achieved for years. To respect the Gauss?s law the charge into the electret has to be equal to the sum of the one stored into the two electrodes. In the moment one electrode moves away or gets closer to the other, the influence of the electret on counter-electrode changes. In this way the amount of charge on the two electrodes have to be reorganized through a resistance and a current is generated.

The advantage of these structures is that the deformation due to the vibrations is directly converted into electricity. The output power of some devices can be seen in Table 6.

This method of gather energy is cheap and, if the size of the capacitor is decreased, the capacitance increases. The coupling coefficient is easy to adjust and can reach high value.

Table 4.2 *Electret-based converters (adapted from [129]).*

Vibration or rotation	Surface	Electret Potential	Output Power
6000 rpm	730cm2	500V	25mW
5000 rpm	90cm2	363V	1.02mW
106 rpm	1.13cm2	200V	30.4W
60Hz	0.12cm2	850V	6μW
20Hz	4cm2	1100V	38μW
60Hz	4.84cm2	300V	2.26μW
500Hz	0.09cm2	10V	2nW

4.4.3 Piezoelectric transducer

These transducers have the piezoelectric properties and that means they can be used to create electrical charge when a mechanical strain is applied to them. When subjected to vibration, these transducers create a varying output voltage that can be converted and also stored to be used to power different devices. An advantage of these materials is that the electricity can be obtained directly using the properties of the materials. In fact the principal is based on the separation of charge within a material as a result of an applied strain. This charge separation leads to the creation of an electric field within the material.

As said before, it is possible to create electricity by applying a force to a piezoelectric material, but the phenomena can work in the other way round: applying an electromagnetic field creates a deformation in the material.

The piezoelectric materials can be divided into two main groups: ceramics and crystals.

Material as quartz, Rochelle salt and tourmaline have quite small piezoelectric effect.

The ferroelectric ceramics, instead, can generate higher voltage and some example of material are the zirconate titanate and the barium titanate [130].

Piezoelectric materials have a built-in polarization, and therefore respond differently to stressors depending on the direction. There are two different modes to convert the mechanical strain into an output voltage [131]:

1. 3-1 mode

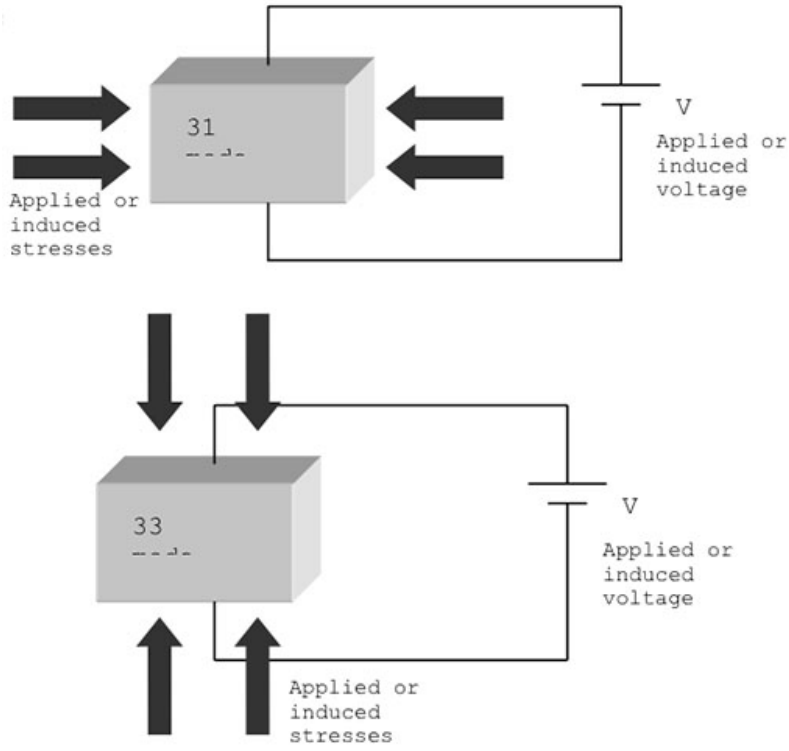

Figure 4.7 *The different mode how to harvest the energy. 3-1 mode (at the top) and 3-3 mode (at the bottom) [131]*

2. 3-3 mode

In the first case the electromagnetic field produced is generated on an axis that is orthogonal to the axis of the strain that is applied. In the second case, the axis of the strain is on the same axis of the field created. In the 3-3 mode the energy produced is higher but the design of these devices are more complex.

Using the vibrational energy it is possible to harvest $10\mu W$ to 100mW power [132].

For example a power of 1.8mW can be generated using a piezoelectric membrane of 25mm of diameter [133]

4.5 Human energy sources

Humans are a great source of energy and there are multiple ways to harvest energy from the body. Some of them and the relative power that can be generated are

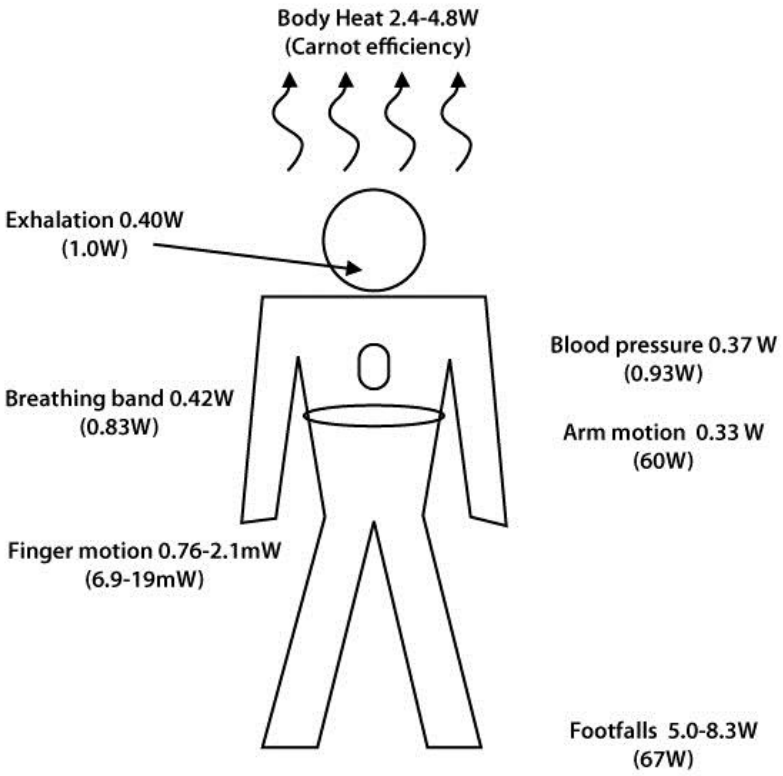

Figure 4.8 *Some ideas to harvest energy from the body [134]*

shown in the next page in Figure 4.8.

The sources for the energy harvesting from the human body can be divided into two main categories:

- Passive source:
  - Breathing;
  - Heat dissipation;
  - Organ movements;
  - Blood flows
  - Blood sugar. [135]
- Active source:
  - Movement of the limbs

4.5.1 Passive source

The passive one comes from the movement that are not under the control of the users [136] as breathing [137], or from the movement of the heart [138] or by placing a piezoelectric transducer located alongside moving organs [139].

The mechanical beating of the heart or the motion of the diaphragm from breathing do the pressing on a piezoelectric film and produce energy that can be used [140]. With this method, and using a living animal model, the researchers where able to charge a 3.8 V battery. Other way of utilizing the heart movement is made by using a new generator called SIMM (Self-energizing Implantable Medical Micro-system) placing two compressible bladders and a micro generator mounted on the wire that connects the pacemaker or defibrillator to the heart. It will be possible to harvest energy by insert a turbine into an artery to power devices, as drug delivery system or pacemaker, implanted into human body [141]. A blood pressure change of 40 mmHg at a frequency of 1 Hz can generate a theoretical value of $2.3\mu W$[142]. The same energy source finds out that using a circular diaphragm of 5.56 mm radius the optimum thickness of 9m produces 0.61W. Experimental tests using 28m thick membranes pulsed at 60 Hz can generate 0.34W and 0.25W for circular and square plates [143].

All these methods are still be studying and testing.

4.5.2 Active sources

The active one, instead, comes from the movements that a person can control as walking [144] [145] by insert a flexible piezoelectric piece under the insole to collect the energy.

Energy can me gathered from harm movements as the automatic watches [146] or by typing on a keyboard [147] which imply a little magnet generator under each key. An example of how to use the power of finger tap is studied in [148]a device that has a resonant frequency of 100 Hz. This device is capable to generate 0.16?W.

Using the walking power it is possible to harvest higher amount of energy up to 8.4mW. Two piezoelectric transducers located in the heel of a Navy work boot make this result. When the heel of the shoe hits the ground, the transducers will be

deformed and, as the heel is lifted, the transducers will go back to their original shape. An excitation of 0.9 Hz every step leads to the generation of the voltage [149]. It is possible to scavenge an amount of power up to 20 W [150].

The advantage of scavenging the energy from the human body is that the user can easily access to power whenever she/he wants and wherever she/he is without looking for a plug or changing the battery, or without having a new surgery to recharge the devices embedded in hers/his body.

4.6 Comparison of the energy harvesting schemes

Table 4.3 *Output energy harvested from different energy harvesting sources.*

Energy source	Output Power harvested	Information
Direct sun light	10-100mW/cm3	Depending on the amount of sun light
	μW to thousand of mW	
Indoor light	100mW/cm3	
Thermoelectric	Around 135mW/cm2 up to 1V	Seebeck effect
	Up to mJ	Pyroelectricity properties
Piezoelectric shoes	8.4mW	Normal walking speed
Electromagnetic RF	0.1 to 3mW	Depending on the device-antenna
Electromagnetic (vib.l)	2.5mW/cm3	miniaturization problem
	Generally μW to dozens of mW	
Vibrational	Machines: 800mW/cm3	frequency order Hz to KHz
	Humans: 4mW/cm3	
	10μW up to hundreds of 20 W	
Blood pressure	0.93W at 100mmHg	the power generated is around mW
	2.3μW at 40mmHg	
Wind	177mW/cm3	wind with average speed of 3m/s
	0.4-1mW/cm3	
Tree energy	Few mW up to hundreds mW	Movement of the trees

A storing system is usually needed because the amount of energy available in the environment changes from time to time and usually the power consumption of the sensor are bigger than the one harvested.

5. SIMULATOR ENVIRONMENT AND INVESTIGATED SCENARIOS

In this thesis different networks were simulated in order to investigate the compatibility between the energy consumption of a given network and the amount of power that can be supplied by the energy harvesting techniques presented in the previous chapters. The network simulator tool used in this investigation is the OMNeT++. In the paragraph 5.1 an overview of the simulation environment is given. In the paragraph 5.2 the simulation settings and the simulations performance results are given.

5.1 Overview of the OMNeT++ simulation environment

OMNeT++ is an object-oriented modular discrete event network simulation framework. Different tools that provide infrastructures to write simulations compose this program. OMNeT++ uses a set of modules that, connected to each others, define the models to simulate.

5.1.1 Hierarchical structure of the network

A model is nothing more than a hierarchical structure of different level of simple modules that exchange messages. The system module is the upper level or the hierarchy and it contains sub modules that can contain other sub modules as well. A compound module is a sub module and it is a group of simple modules. In the compound module the parameters can indicate the numbers of the modules, the number of the gates and of the connections and how they are made.

The simple modules are written in C++ language using the simulation class library. The communication between modules is made using connections and gates. Each

simple module has two interfaces: input and output one. The module is described by parameters that can be string, numbers or Boolean values or they can contain XML data trees.

A gate is the name of the interface used by the modules to send messages. An input gate and an output gate of different modules are connected by a link called connection.

The topology of the network is defined by using the NED language description (Network Description). The entire simulation objects, as messages, modules and so on, are part of the C++ classes.

A connection can link two modules or a module and a compound module. To reuse a model it is not allowed to use connection between different levels of the hierarchy. The connection is characterized by parameters like bit error rate, data rate and delay and packet error rate. A connection with specific parameters is called channel.

Two components form the simulation system and they are the simulation kernel and the user interface.

The simulation kernel contains the class library and the code to manage the simulation and is written in C++.

The user interface is used to run the simulation and to detect debugs and it is written in C++ as well. With the user interface is possible to see the structure of the model and to change objects or the parameters of a simulation. It is easy to control the simulation and the graphical user interface shows how the model behavior and how it works.

Due to its generic architecture it can be used to simulate different scenarios and different problems. It can be used to:

1. Model communication protocols
2. Model communication system both wired and wireless
3. Model distributed hardware system
4. Model any system described by discrete events and that communicates by exchanging messages.

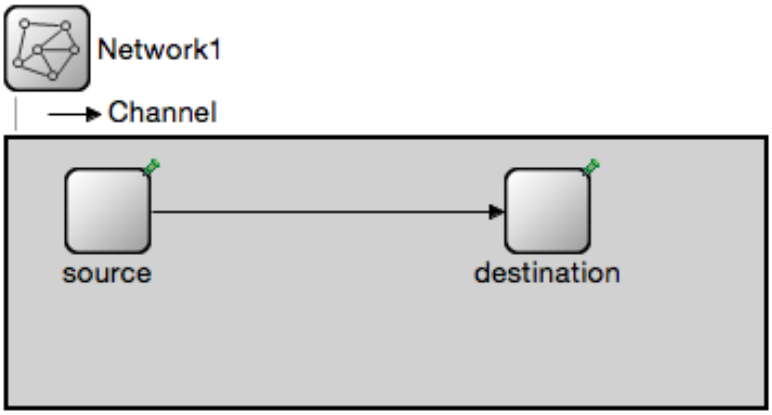

Figure 5.1 *Example of a simple network*

5. Evaluation of the performances of complex software systems

5.1.2 The NED language

The NED language is used to write and describe the simulation model and the user, using it, defines the simple modules, the connections and compound modules. The topology of the network is described with this language and the main components are:

1. The network
2. The compound modules
3. The simple modules
4. Channels
5. The network

The network file contains all the settings for the model. In the network all the nodes and the connections are defined and all the parameters are set. An example of a network definition is shown below.

```
network Network1
{
        @display("bgb=349,123");
    types:                  // here all the components of the network are defined

        channel Channel extends ned.DatarateChannel {
                datarate = 100Mbps;
        }
        submodules:
        source: Node1 {
                @display("p=46,33");
        }

        destination: Node2 {
                @display("p=249,33");
        }

        connections:
        source.out --> IdealChannel --> destination.in;

}
```

Figure 5.2 *Code of the network shown in Figure 5.1*

```
module Node
{
    parameters:         //Specify all the parameters of the node
        int capacity;
        volatile double sendIaTime @unit(s);
        int destAddress;

    submodules:         //Specify all the submodules of the node
        function: Node;
        function1: Node;
        function2: Node;

    connections:        //Specify all the connection of the submodules
        function.out --> IdealChannel --> function1.in;
        function.out --> IdealChannel --> function2.in;
        function1.out --> IdealChannel --> function.in;
        function2.out --> IdealChannel --> function.in;
    gates:              //Specify the interfache of the compound module
        inout gate;
}
```

Figure 5.3 *Code of a compound module*

The compound modules

Different simple modules form the compound module and, in the file, all the parameters and the sub modules are set and described. Comparing the compound and the simple module, in the compound model file there are two more sections: the sub modules section and the connection section. The connection section describes the topology of the node itself and how the simple modules are connected to each other. An example of the code can be seen in Figure 5.3.

```
simple NodeTrafficGenerator
{
    parameters:    // Specify all the variables of the simple module
        volatile double sendIaTime @unit(s);
        int destAddress;

    gates:       //Specify the king of gates of the simple module
        input in;
        output out;
}
```

Figure 5.4 *Code of a simple module*

The simple module

The simple module is the basic block of the network and it is the active component that, combined, forms the compound modules. The NED file contains the declaration of the parameters and the definition of the gates as it is shown in Figure 5.4. Each node (compound node) has different functionalities and each of them can be describe using a simple mode.

Examples of simple modules for a node are: the traffic generator, the routing and the one to queue up the packets that have to send.

Channels

In the channel file is written the behavior of the connections and all the specification. It is really rare to write new class of channels because there are predefined channel classes that can be used by the users. There are three different channels and they are: IdealChannel, DelayChannel and DatarateChannel.

The ideal channel has no parameter to define and, when a message is send through it, there are no delay and no loss.

The delay channel is used when a delay wants to be added to the simulation. The channel is defined by two parameters:

- The delay: it is the propagation delay of the message sent and has to be indicated with a time unit like s, ms, etc
- The disabled: it is a Boolean value set on false by default. When the value is

```
channel Channel extends ned.DatarateChannel {
        datarate = 100Mbps;
        delay = 100us;
}
```

Figure 5.5 *Definition of a new channel*

set on true the channel will drop all the messages

The data rate channel presents two more parameters compared to the delay one. The parameters are:

- Datarate: it is used to calculate the transmission duration of a packet and the unit is the bit per second or its multiples
- BER and PER: The Bit Error Rate and the Packet Error Rate are set to describe an error model. It is a double value set by default on 0

Extending the standard channel already in the tool, it is possible to design a channel with different parameters. A different DataRate channel is shown in Figure 5.5.

5.2 Simulations setting and results

5.2.1 General settings

To understand the energy efficiency of different networks implementing the standard IEEE 802.11ah, a simulation scenario was set and run with the OMNeT++ tool.

The fixed parameters of the simulation settings used are the constant parameters defined in IEEE 802.11ah standard. The Table 5.1 summarizes these fixed parameters and their corresponding values.

The parameters defined are:

- Tsym represents the duration of a symbol that is equal to 40μs

Table 5.1 *Fixed parameters used in the simulations.*

Tsym	40μs
MAC header	14x8 bits
PHY header	6xTsym
ACK	PHY header
Basic data rate	650kbps (MCS0)
SlotTime	52μs
SIFS	160 μs
DIFS	SIFS + 2 x SlotTime
Mshort	7
CWmin	15 SlotTime
CWmax	1023 SlotTime

- The RTS and CTS value are not used in the simulations in this thesis because the basic MAC access mode is used. The RTS and CTS are usually used to reduce the problem due to the hide nodes but, using them, the overhead is increased
- The SIFS represents the Short Inter Frame Space
- The DIFS is the Distributed Inter Frame Space
- Mshort parameter is related to how many times a packet is transmitted if it is not received correctly or not received at all
- The CWmin value represents the minimum contention window used in the simulations while the CWmax value represents the maximum connection window

Different Modulation and Coding Systems (MCSs) were applied to the data packets that are exchanged between the nodes in the network. In Table 5.2are shown the 9 possible MCS that can be used in 2 MHz mode with one spatial stream. For each of them, the corresponding data rate and the required minimum sensitivity level are also shown.

To evaluate the performance of the investigated networks in energy consumption point of view, that is generally calculated in mJ/bit, each state of the transceiver should have particular power consumption value.

In Table 5.3 summarizes the energy consumption in different modes of a station with respect to the transmission power that is equal to 1mW.

Table 5.2 *Sensitivity levels and data rate for different MCSs.*

MCS Index	Data Rate (Mbps)	Minimum sensitivity (dBm)
0	0.65	-92
1	1.30	-89
2	1.95	-87
3	2.60	-84
4	3.90	-80
5	5.20	-76
6	5.85	-75
7	6.50	-74
8	7.80	-69

- Transmission mode is only used for sending RTS and DATA
- Receiving mode refers to receiving Beacon, CTS and ACK
- Sleep mode refers to the times when station does not have anything to send and all the other timings are considered to be idle.

Table 5.3 *Energy consumption values in different state.*

Mode	Energy consumption (mW)
Transmission	255
Receive and channel sensing	135
Sleep	1.5

It should be noted that values corresponding to receiving and sensing modes are assumed to be the same since the base-band processing energy consumption, which is the additional energy in the receiving mode, is negligible compared to the whole receiving energy consumption.

The standard IEEE 802.11ah is thought to support very high number of stations (up to 6000) and, at the same time, it wants to achieve a data rate higher than 100 kbps. Another aim of this standard is to cover a transmission area of $1Km^2$. The scenarios simulated in this thesis are the ones defined in the TGah functional requirement and evaluation methodology document (IEEE802.11-11/0905r5) for basic mode case.

Different scenarios are considered in this thesis and are based on the the TGah functional requirement and evaluation methodology document (IEEE802.11-11/0905r5).

5.3 Results and comparison

5.3.1 IEEE 802.11ah results

In this thesis the energy performance of the IEEE 802.11ah standard is investigated. The aim is to compare the energy consumption of networks that implement this standard with the amount of power that can be gathered with different energy harvesting techniques. In this way it is possible to study the suitability of the energy harvesting schemes.

The performances are evaluated in terms of energy efficiency for both saturated and not saturated scenarios. Specific IEEE 802.11ah features like restricted access window (RAW) will be also considered, in order to improve the energy efficiency of the system, and therefore allow wide range of energy harvesting schemes to be deployed with IEEE 802.11ah.

Energy consumption in saturated traffic

In the saturated traffic each station has full buffer, meaning that it always has a packet to transmit. We assume an up-link traffic where the STA continuously sends DATA packets to the AP. Ideal channel (STAs are assumed to be on top of each others, meaning no path loss effects) and macro channel (here a typical playground of 100 m^2 is used, allowing the STAs to hear each others even when the largest MCS) are considered. Although this can seen as a very idealistic and not typical scenario, an idea of the asymptotic performance can be inferred though.

In the saturated scenario we assume that DATA packet size is 256 bytes.

The relevant simulated energy consumption results in the case of saturated traffic is shown in Figure 5.6 and in Figure 5.7 in the case of Ideal and macro channels

As can be seen in both figures, the total amount of the energy consumption to send successfully one packet increases if the size of the network becomes bigger. A noticeable difference can be achieved by using different MCS. We can also notice the energy efficiency improvement due to the use of RAW scheme.

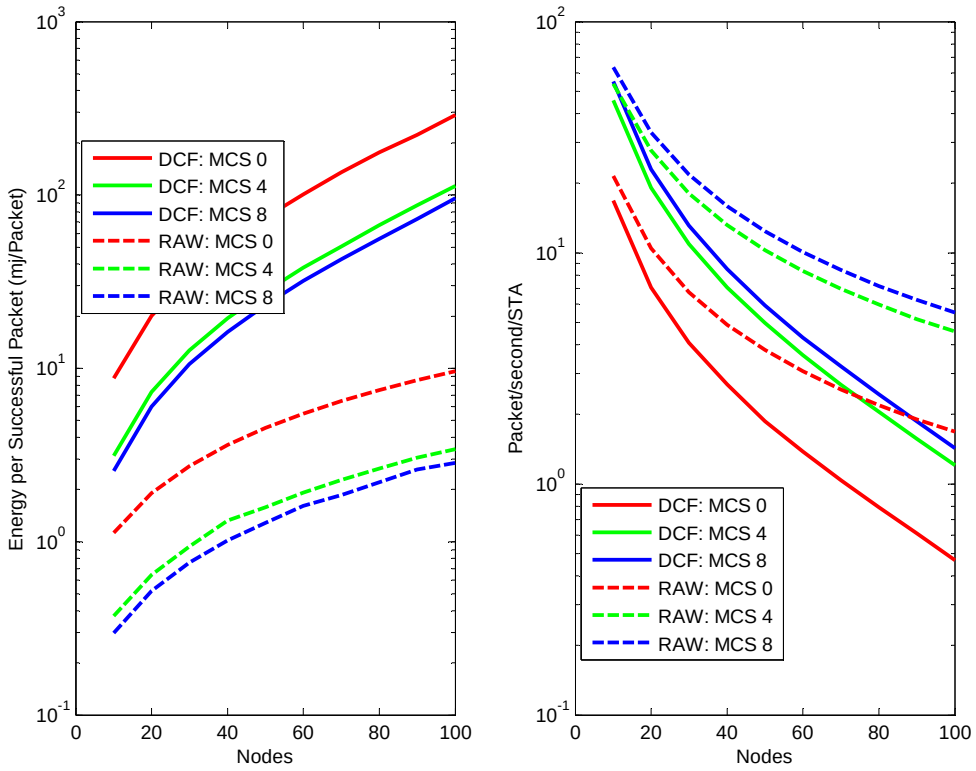

Figure 5.6 *DCF and RAW performances in ideal channel scenario for different MCSs: (left) Energy per successful packet, (right) successfully received packet per second per STA*

Energy consumption in un-saturated traffic

The unsaturated scenario is of more interest particularly because all practical use cases for the IEEE 802.11ah network have unsaturated traffic assumptions. In this section we consider three use cases of the IEEE 802.11ah amendment. The selected use cases encompass a wide range of applications and represent typical scenarios in which the IEEE 802.11ah networks will be deployed. The payload size and inter-arrival times of packets for stations's up-link data for each use case are given in Table 5.4.

Same in the Saturated traffic case, we can notice the energy efficiency improvement due to the use of RAW scheme. In the unsaturated scenario, and because of the low traffic settings, the overall throughput is clearly smaller. The energy efficiency however is not improved because the STAs are most of the time either listening,

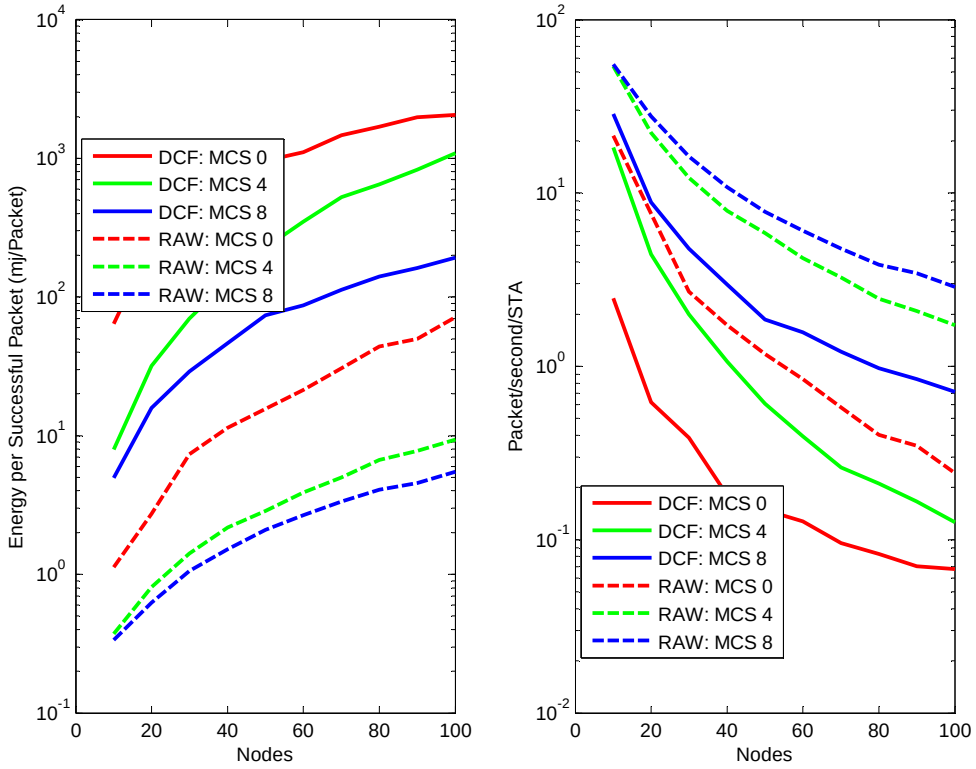

Figure 5.7 *DCF and RAW performances in macro channel scenario for different MCSs: (left) Energy per successful packet, (right) successfully received packet per second per STA*

Table 5.4 *Traffic parameters of IEEE 802.11ah use cases used in the simulation*

Use case	Packet Size (Bytes)	TX Period (sec)
Sensor Network (IoT)	256	10-60
Home/Building Automation	512	60
Healthcare/Clini c	2048	0.25

receiving or transmitting data.

Suitable energy harvesting schemes

By analyzing the results shown in Figures 5.6, 5.7, 5.8, 5.9 and 5.10 we can easily determine which of the energy harvesting schemes presented in the previous chapters are suitable in the case of IEEE 802.11ah based networks.

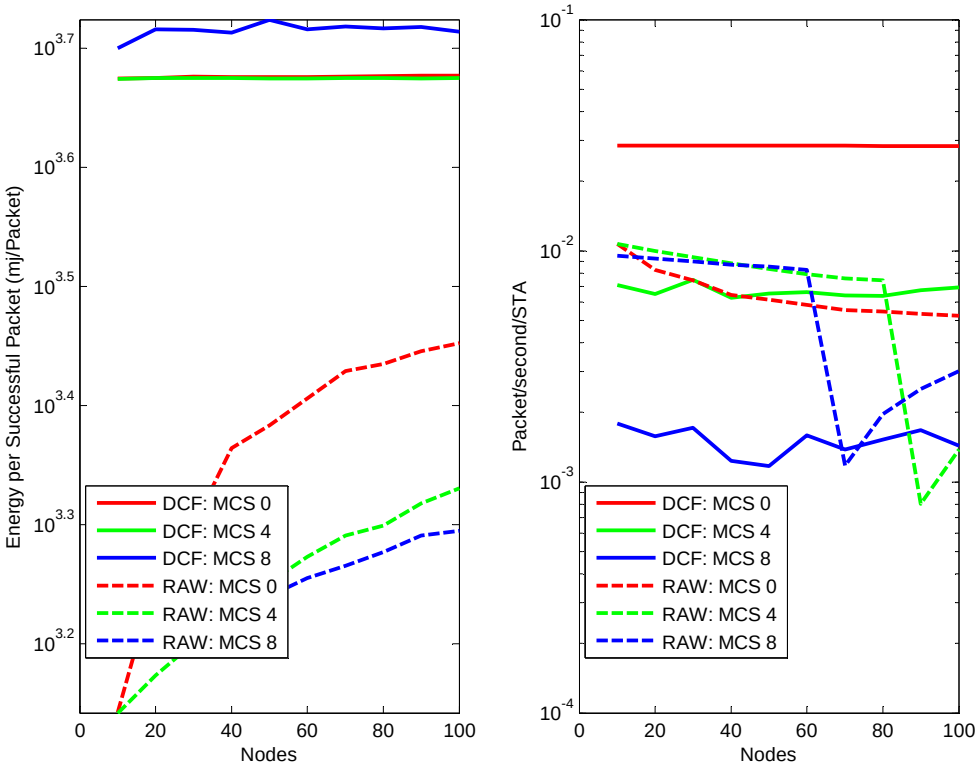

Figure 5.8 *DCF and RAW performances in sensor IoT traffic, macro channel scenario for different MCSs: (left) Energy per successful packet, (right) successfully received packet per second per STA*

For example in saturated scenario with ideal channel for a network formed by 10 (100) nodes and in the case of basic DCF with MCS0, we need around 10 (300) mJ per packet. We can also see that for the same network settings we can successfully transmit in average about 20 (0.5) packets per STA in a second, therefore we need 200 mW (150 mW) to be able to transmit those 20 (0.5) packets. By checking the Table 4.3 that includes the output energy harvested from different energy harvesting sources we can easily see that none of the listed scheme can achieve this goal.

If we use RAW, however, we can notice the improvement in energy efficiency and in throughput. Doing the same analysis as in the DCF case, we can see that we will need here around 2mW to 20 mW to guarantee the throughput performance illustrated in the Figure 5.6 (right). Checking again the Table 4.3, we can see that some of the listed energy harvesting schemes are now suitable for example using Direct sun light, and Tree energy techniques.

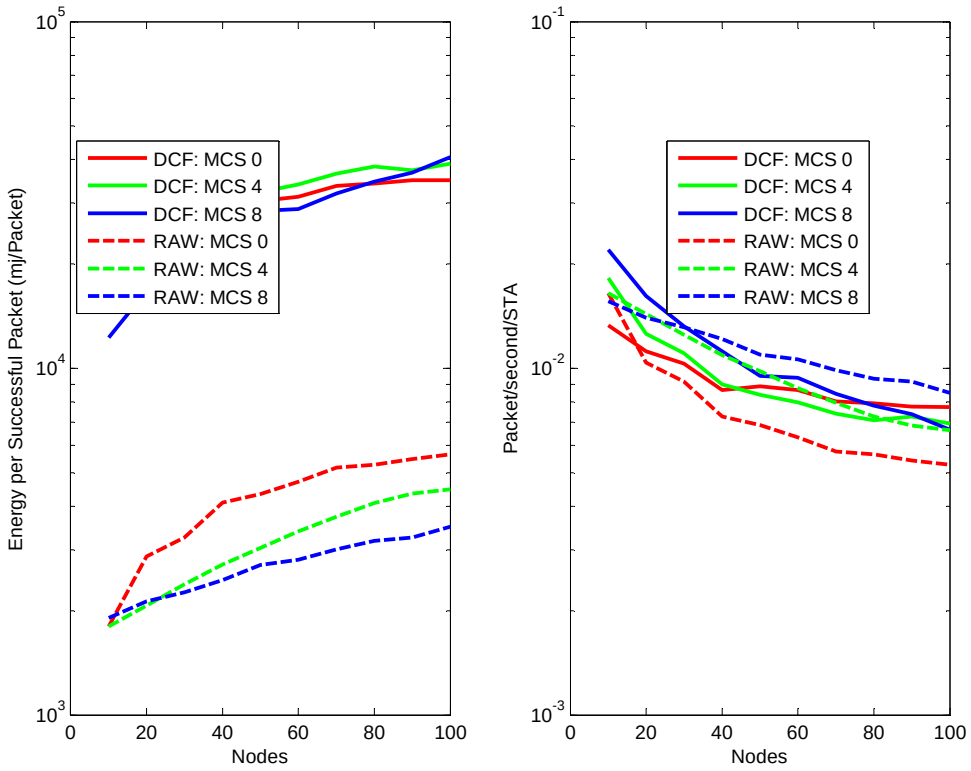

Figure 5.9 *DCF and RAW performances in Home/Building Automation traffic, macro channel scenario for different MCSs: (left) Energy per successful packet, (right) successfully received packet per second per STA*

Additional schemes can be also made suitable if higher MCSs are used.

Similar analysis can be done for the unsaturated traffic scenarios (Figures 5.8, 5.9, 5.10).

The main conclusion is that only some of the available energy harvesting schemes can be used to guarantee the same throughout achieved when no restrictions on the available power are applied.

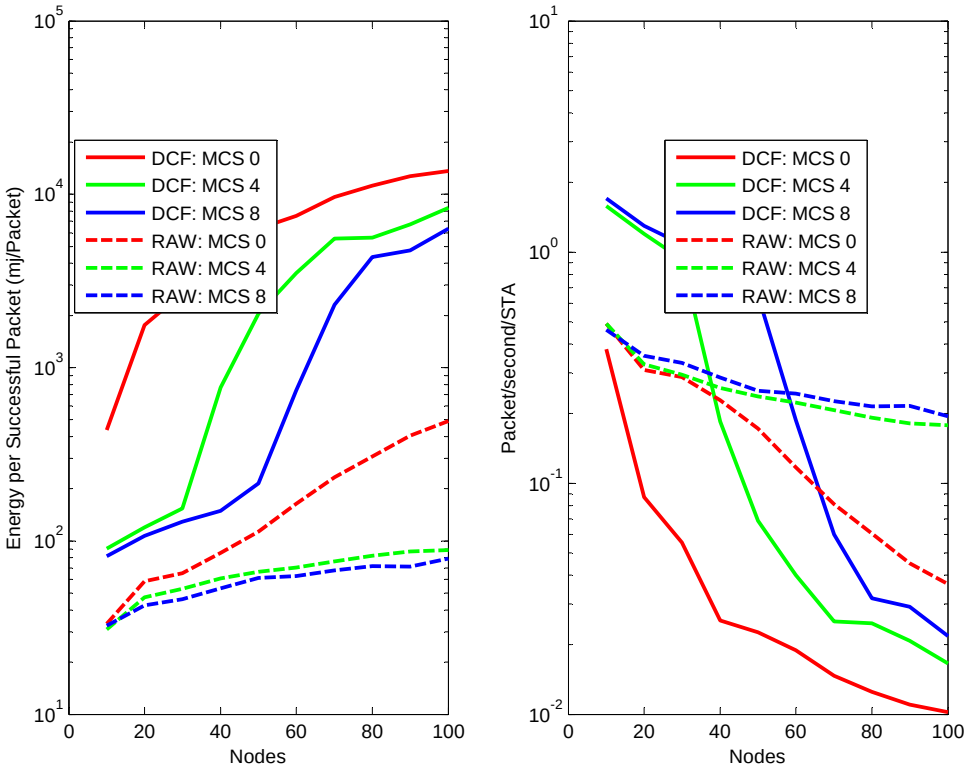

Figure 5.10 *DCF and RAW performances in healthcare traffic, macro channel scenario for different MCSs: (left) Energy per successful packet,(right) successfully received packet per second per STA*

6. CONCLUSIONS

In this thesis we gave an overview on multiple energy harvesting schemes that can represent a prospective power source for the Internet of Things networks. Additionally we presented a variety of radio technologies and communication standards used in current Wireless Sensor Networks.

The focus of the thesis was to study the suitability of these energy harvesting schemes in order to reliably power the Wireless Sensor Networks that implement the IEEE 802.11ah communication standard.

The IEEE 802.11ah is a standard operating at a frequency below 1GHz and aiming to reach the 1 km transmission range and a data rate above 100Kbit/s. Among the challenges of this standard is to support a huge number of stations, up to 2000, for the outdoor application and to provide a power saving mechanisms so the battery of the device can last for a longer period of time.

The main goal is to understand whether it could be possible to power one node network or even a more complex one, merely with one the presented energy harvesting schemes.

Networks of different sizes were simulated and analyzed. All the networks use only one AP but they differentiate from each other by the number of associated nodes (STAs). Moreover two different scenarios are simulated to better understand the energy consumption in different traffic cases. Both saturated and non-saturated traffic scenarios were simulated and analyzed. To enhance the throughput and to decrease the energy needed to power the sensors, different Modulation and Code Schemes were implemented. To assess the performance of simulated scenarios, the throughput and the energy consumption where analyzed.

Overall, the results have showed that different networks required a small amount of energy to send and receive data.

Specifically, in the saturated scenario, the total amount of the energy consumption to send successfully one packet increases if the size of the network becomes larger. A noticeable difference can be achieved by using different MCS. We can also notice the energy efficiency improvement due to the use of RAW scheme.

The unsaturated scenario is however of more interest particularly because all practical use cases for the IEEE 802.11ah network have unsaturated traffic assumptions. In the analysis of the unsaturated traffic we considered three use cases introduced by the IEEE 802.11ah amendment. These selected use cases encompass a wide range of applications and represent typical scenarios in which the IEEE 802.11ah networks will be deployed. For instance we considered the Sensor IoT, the Home/Building Automation and Healthcare use cases.

Similarly as in the saturated traffic case, we can notice easily the energy efficiency improvement due to the use of RAW scheme. In the unsaturated scenario, and because of the low traffic settings, the overall throughput is clearly smaller. In saturated scenario with ideal channel for a network formed by 10 to 100 nodes and in the case of basic DCF with MCS0, we need around 150 mW to 200 mW to be able to transmit those packets. These numbers are however higher than the values that can provide most of the presented energy harvesting scheme, therefore they are not suitable in this case.

If we use RAW, however we can notice the improvement in energy efficiency and in throughput. Doing the same analysis as in the DCF case, we can see that we will need here around 2mW to 20 mW to guarantee the throughput performance expected in the saturated traffic. Fortunately in this case, some of the presented energy harvesting schemes is suitable for example, direct sun light, and Tree energy techniques. Similar analysis can be done for the unsaturated traffic scenarios.

The main conclusion is that only some of the available energy harvesting schemes can be used to guarantee the same throughout achieved when no restrictions on the available power are applied.

REFERENCES

1. Gérald, S. *The Internet of Things: Between the Revolution of the Internet and the Metamorphosis of Objects*. in *Forum American Bar Association*. 2010.
2. Coetzee, L. and J. Eksteen. *The Internet of Things-promise for the future? An introduction*. in *IST-Africa Conference Proceedings, 2011*. 2011. IEEE.
3. Tan, L. and N. Wang. *Future internet: The internet of things*. in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*. 2010. IEEE.
4. *IoT First Time mensioned*. Available from: http://www.rfidjournal.com/articles/view?4986.
5. Sundmaeker, H., et al., *Vision and challenges for realising the Internet of Things*. 2010: EUR-OP.
6. Forbs. *Forbs IoT*. 2008 [cited 2014 22.10.]; Available from: http://www.forbes.com/global/2002/0318/092.html.
7. *IoT ITU*. Available from: http://it.emcelettronica.com/internet-delle-cose-che-cos%C3%A8.
8. Bassi, A. and G. Horn, *Internet of Things in 2020: A Roadmap for the Future*. European Commission: Information Society and Media, 2008.
9. *[Figure IoT]*. [cited 2014 22.10.]; Available from: http://launch.it/launch/iot-a-at-ceweek-2013.
10. Atzori, L., A. Iera, and G. Morabito, *The internet of things: A survey*. Computer networks, 2010. **54**(15): p. 2787-2805.
11. *Smart allarm clock*. Available from: http://hacknmod.com/hack/alarm-clock-syncs-to-google-calendar-weather-traffic-reports/.
12. *Smart mirror*. Available from: http://www.gizmag.com/toshiba-smart-mirror-concept-ces-2014/30574/.
13. Castellani, A.P., et al. *Architecture and protocols for the internet of things: A case study*. in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on*. 2010. IEEE.
14. Strategy, I. and P. Unit, *ITU Internet Reports 2005: The internet of things*. Geneva: International Telecommunication Union (ITU), 2005.
15. Conner, M., *Sensors empower the" Internet of Things"*. EDN (Electrical Design News), 2010. **55**(10): p. 32.
16. Hofmann, E., *Verso l'internet delle cose*. TENDENZE 2005. **N°50**: p. 2.
17. Khan, A. and S. Kurnia, *Exploring the Potential Benefits of RFID: A Literature-Based Study*. Department ofInformation Systems, University of Melbourne, 2006: p. 1-12.
18. Huang, Y.-P., S.-S. Wang, and F.E. Sandnes, *RFID-based guide gives museum visitors more freedom*. IT Professional, 2011. **13**(2): p. 25-29.
19. *EPC Network*. Available from: http://indicod-ecr.it/standard/gs1-epcglobal/epcglobal-network/.
20. Higazi, M. *RFID*. [cited 2015 06.03.]; Available from: http://m-higazi-ie673.tripod.com/assignment-5.html.

21. Ma, Y.-W., et al. *Mobile RFID with IPv6 for phone services*. in *Consumer Electronics, 2009. ISCE'09. IEEE 13th International Symposium on*. 2009. IEEE.
22. Lee, S.-D., M.-K. Shin, and H.-J. Kim. *EPC vs. IPv6 mapping mechanism*. in *Advanced Communication Technology, The 9th International Conference on*. 2007. IEEE.
23. Yoon, D.G., et al. *RFID networking mechanism using address management agent*. in *Networked Computing and Advanced Information Management, 2008. NCM'08. Fourth International Conference on*. 2008. IEEE.
24. Tech, L. *Using RFID & IPv6*. [cited 2014 15.11.]; Available from: http://ipv6.com/articles/applications/Using-RFID-and-IPv6.htm.
25. *QR Codes*. [cited 2015 06.03.]; Available from: http://www.mobilemarketinghelper.com/mobile-marketing/qr-codes/.
26. Liu, Y., J. Yang, and M. Liu. *Recognition of QR code with mobile phones*. in *Control and Decision Conference, 2008. CCDC 2008. Chinese*. 2008. IEEE.
27. *Semapedia*. Available from: http://www.merkwelt.com/people/stan/semapedia_offline/.
28. *[WikiLovesMonuments]*. [cited 2014 20.10.]; Available from: http://www.wikilovesmonuments.org.
29. *[QRcode generator]*. Available from: http://www.codmmunicator.com.
30. Eschenauer, L. and V.D. Gligor. *A key-management scheme for distributed sensor networks*. in *Proceedings of the 9th ACM conference on Computer and communications security*. 2002. ACM.
31. Karygiannis, T., et al., *Guidelines for securing radio frequency identification (RFID) systems.* NIST Special publication, 2007. **80**: p. 1-154.
32. Kumar, R., E. Kohler, and M. Srivastava. *Harbor: software-based memory protection for sensor nodes*. in *Proceedings of the 6th international conference on Information processing in sensor networks*. 2007. ACM.
33. Feldhofer, M., S. Dominikus, and J. Wolkerstorfer, *Strong authentication for RFID systems using the AES algorithm*, in *Cryptographic Hardware and Embedded Systems-CHES 2004*. 2004, Springer. p. 357-370.
34. Calmels, B., et al., *Low-cost cryptography for privacy in RFID systems*, in *Smart Card Research and Advanced Applications*. 2006, Springer. p. 237-251.
35. Lioudakis, G.V., et al. *A proxy for privacy: the discreet box*. in *EUROCON, 2007. The International Conference on &# 34; Computer as a Tool&# 34;*. 2007. IEEE.
36. Wickramasuriya, J., et al. *Privacy protecting data collection in media spaces*. in *Proceedings of the 12th annual ACM international conference on Multimedia*. 2004. ACM.
37. Chan, H. and A. Perrig, *Security and privacy in sensor networks.* Computer, 2003. **36**(10): p. 103-105.
38. Savry, O. and F. Vacherand, *Security and privacy protection of contactless devices*, in *The Internet of Things*. 2010, Springer. p. 409-419.
39. Savry, O., et al., *RFID Noisy Reader How to Prevent from Eavesdropping on the Communication?* 2007: Springer.
40. Akyildiz, I.F., et al., *Wireless sensor networks: a survey.* Computer networks, 2002. **38**(4): p. 393-422.
41. Yang, G.-Z. and M. Yacoub, *Body sensor networks.* 2006.

42. Ho, L., et al. *A prototype on RFID and sensor networks for elder healthcare: progress report*. in *Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*. 2005. ACM.
43. Feng, J., F. Koushanfar, and M. Potkonjak, *Sensor Network Architecture.* Handbook of Sensor Networks, 2004.
44. Estrin, D., et al. *Instrumenting the world with wireless sensor networks*. in *Acoustics, Speech, and Signal Processing, 2001. Proceedings.(ICASSP'01). 2001 IEEE International Conference on*. 2001. IEEE.
45. *Sensor node picture*. [cited 2014 22.10.]; Available from: http://www.eetimes.com/document.asp?doc_id=1279204.
46. Feng, J., F. Koushanfar, and M. Potkonjak. *System-architectures for sensor networks issues, alternatives, and directions*. in *Computer Design: VLSI in Computers and Processors, 2002. Proceedings. 2002 IEEE International Conference on*. 2002. IEEE.
47. Niyato, D., et al., *Wireless sensor networks with energy harvesting technologies: a game-theoretic approach to optimal energy management.* Wireless Communications, IEEE, 2007. **14**(4): p. 90-96.
48. Giuppi, F., et al. *Challenges in energy harvesting techniques for autonomous self-powered wireless sensors*. in *Microwave Conference (EuMC), 2013 European*. 2013. IEEE.
49. Werner-Allen, G., et al., *Deploying a wireless sensor network on an active volcano.* Internet Computing, IEEE, 2006. **10**(2): p. 18-25.
50. Mainwaring, A., et al., *Wireless sensor networks for habitat monitoring*, in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*. 2002, ACM: Atlanta, Georgia, USA. p. 88-97.
51. Chebrolu, K., et al. *Brimon: a sensor network system for railway bridge monitoring*. in *Proceedings of the 6th international conference on Mobile systems, applications, and services*. 2008. ACM.
52. Song, H.J., et al. *Modeling signal strength range of TPMS in automobiles*. in *Antennas and Propagation Society International Symposium, 2004. IEEE*. 2004. IEEE.
53. [cited 2015 08.01.]; Available from: http://en.wikipedia.org/wiki/Virtual_sensor_network -mediaviewer/File:Rock_Sliding_%26_Animal_Monitoring.jpg.
54. project, M. *volcano monitoring*. [cited 2015 08.01.]; Available from: http://miavita.brgm.fr/pressroom/PublishingImages/N5-INESCID/figure1.png.
55. Tan, Y.K. and S.K. Panda, *Review of energy harvesting technologies for sustainable wireless sensor network.* Sustainable Wireless Sensor Networks, INTECH Publisher, 2010: p. 15-43.
56. Vullers, R., et al., *Micropower energy harvesting.* Solid-State Electronics, 2009. **53**(7): p. 684-693.
57. Dunn-Rankin, D., E.M. Leal, and D.C. Walther, *Personal power systems.* Progress in Energy and Combustion Science, 2005. **31**(5): p. 422-465.
58. Ganeriwal, S., et al., *Estimating clock uncertainty for efficient duty-cycling in sensor networks.* IEEE/ACM Transactions on Networking (TON), 2009. **17**(3): p. 843-856.

59. Intanagonwiwat, C., R. Govindan, and D. Estrin. *Directed diffusion: a scalable and robust communication paradigm for sensor networks*. in *Proceedings of the 6th annual international conference on Mobile computing and networking*. 2000. ACM.
60. Desnoyers, P., et al. *PRESTO: A Predictive Storage Architecture for Sensor Networks*. in *HotOS*. 2005.
61. Ye, W., J. Heidemann, and D. Estrin. *An energy-efficient MAC protocol for wireless sensor networks*. in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*. 2002. IEEE.
62. Polastre, J., 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*. 2004. ACM.
63. Buettner, M., et al. *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*. 2006. ACM.
64. Kundu, A., et al., *Micro-fuel cells—current development and applications.* Journal of Power Sources, 2007. **170**(1): p. 67-78.
65. *Fuel cell figure*

. [cited 2014 07.10.2014]; Available from: http://commons.wikimedia.org/wiki/File:Fuell_cell.jpg.
66. Ellis, M.W., M.R. Von Spakovsky, and D.J. Nelson, *Fuel cell systems: efficient, flexible energy conversion for the 21st century.* Proceedings of the IEEE, 2001. **89**(12): p. 1808-1818.
67. *ZigBee Software Architecture*. [cited 2014 07.11.]; Available from: http://www.jennic.com/elearning/zigbee/files/html/module3/module3-4.htm.
68. ; Available from: http://www.embedded.com/design/industrial-control/4012593/ZigBee-SoCs-provide-cost-effective-solutions.
69. *ZigBee® Wireless Standard*. [cited 2014 07.11.]; Available from: http://www.digi.com/technology/rf-articles/wireless-zigbee.
70. *IEEE 802.15.4 (ZigBee)*. Available from: http://www.eng.yale.edu/enalab/courses/eeng460a/homeworks/hw1_results/zigbee.html.
71. *IEEE 802.15.4 CSMA-CA Protocol (ZigBee)*. [cited 2015 08.01.]; Available from: http://www.prismmodelchecker.org/casestudies/zigbee.php.
72. *The Low Energy Technology Behind Bluetooth Smart*. 2015 [cited 2015 1.1.]; Available from: http://www.bluetooth.com/Pages/low-energy-tech-info.aspx.
73. Galeev, M. *Taking advantage of Bluetooth LE advertising mode*. 2013 [cited 2014 7.11.]; Available from: http://m.eetasia.com/ART_8800684009_499488_TA_392c2fdd_3.HTM -.VG2m_4eXpFI

.
74. Enrico, F., *iBeacon Una nuova tecnologia per la localizzazione in ambienti chiusi.* 2013: p. 52.

75. Redazione, L. *BLE, Bluetooth Low Energy*. 2013; Available from: http://www.automazionenews.it/ble-bluetooth-low-energy/.
76. Villegas, J. *Bluetooth Low Energy Version 4.0*. [cited 2014 7.11.]; Available from: http://home.eng.iastate.edu/~gamari/CprE537_S13/project reports/Bluetooth LE.pdf.
77. Hazmi, A., J. Rinne, and M. Valkama. *Feasibility study of IEEE 802.11 ah radio technology for IoT and M2M use cases*. in *Globecom Workshops (GC Wkshps), 2012 IEEE*. 2012. IEEE.
78. Raeesi, O., et al. *Performance Enhancement and Evaluation of IEEE 802.11 ah Multi-Access Point Network Using Restricted Access Window Mechanism*. in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*. 2014. IEEE.
79. Khorov, E., et al., *A survey on IEEE 802.11 ah: An enabling networking technology for smart cities.* Computer Communications, 2014.
80. Aust, S., R.V. Prasad, and I.G. Niemegeers. *IEEE 802.11 ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi*. in *Communications (ICC), 2012 IEEE International Conference on*. 2012. IEEE.
81. Su, Y. and J. Soar. *Building an Information Quality Lab on e-health in the rural areas for healthcare education*. in *E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference on*. 2010. IEEE.
82. Churchill, S. *900MHz Standard for Smartwatches?* 2014 [cited 2014 2.12.]; Available from: http://www.dailywireless.org/category/applications/page/10/.
83. Ogawa, K., et al., *IEEE 802.11 ah based M2M networks employing virtual grouping and power saving methods.* IEICE Transactions on Communications, 2013. **96**(12): p. 2976-2985.
84. Group, I.W., *IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems–Local and Metropolitan Area Networks–Specific Requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments.* IEEE Std, 2010. **802**: p. 11p.
85. Adame, T., et al., *Capacity analysis of IEEE 802.11 ah WLANs for M2M communications*, in *Multiple Access Communcations*. 2013, Springer. p. 139-155.
86. *Libelium device*. [cited 2014 5.12.]; Available from: http://www.libelium.com/bluetooth-low-energy-ble-4-0-smart-connect-sensors-smartphone/ - !prettyPhoto.
87. *BR-Button-S3A Datasheet*. [cited 2014 5.12.]; Available from: http://www.blueradios.com/nBlue BR-BUTTON-S3A Summary Datasheet.pdf.
88. *BLE112 Datasheet*. [cited 2014 5.12.]; Available from: https://www.bluegiga.com/en-US/products/bluetooth-4.0-modules/ble112-bluetooth--smart-module/.
89. *CC2541 Datasheet*. [cited 2014 5.12.]; Available from: http://www.ti.com/lit/ds/symlink/cc2541.pdf.
90. *CC2420 Datasheet*. [cited 2014 5.12]; Available from: http://www.ti.com/lit/ds/symlink/cc2420.pdf.

91. *ETRX35x ZIGBEE® MODULES Datasheet*. [cited 2014 5.12.]; Available from: http://www.telegesis.com/downloads/general/tg-etrx35x-pm-010-100.pdf.
92. Lauzurica, D.B. *Development of a ZigBee Wireless Sensor Node*. 2012 [cited 2014 5.12.]; Available from: http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20120613DanielBlancoLauzurica.pdf.
93. *CC2430 Datasheet*. [cited 2014 5.11.]; Available from: http://www.ti.com/lit/ds/symlink/cc2430.pdf.
94. Liu, Z.-y., *Hardware Design of Smart Home System based on zigBee Wireless Sensor Network.* AASRI Procedia, 2014. **8**: p. 75-81.
95. Visser, H.J., A.C. Reniers, and J.A. Theeuwes. *Ambient RF energy scavenging: GSM and WLAN power density measurements*. in *Microwave Conference, 2008. EuMC 2008. 38th European*. 2008. IEEE.
96. Kawahara, Y., K. Tsukada, and T. Asami. *Feasibility and potential application of power scavenging from environmental RF signals*. in *Antennas and Propagation Society International Symposium, 2009. APSURSI'09. IEEE*. 2009. IEEE.
97. Donelan, J., et al., *Biomechanical energy harvesting: generating electricity during walking with minimal user effort.* Science, 2008. **319**(5864): p. 807-810.
98. MURATA. *Energy Harvesting explanation*. [cited 2015 08.01.]; Available from: http://www.murata.com/en-us/about/newsroom/techmag/metamorphosis16.
99. Mateu, L. and F. Moll. *Review of energy harvesting techniques and applications for microelectronics (Keynote Address)*. in *Microtechnologies for the New Millennium 2005*. 2005. International Society for Optics and Photonics.
100. Taneja, J., J. Jeong, and D. Culler. *Design, modeling, and capacity planning for micro-solar power sensor networks*. in *Proceedings of the 7th international conference on Information processing in sensor networks*. 2008. IEEE Computer Society.
101. Corke, P., et al. *Long-duration solar-powered wireless sensor networks*. in *Proceedings of the 4th workshop on Embedded networked sensors*. 2007. ACM.
102. Raghunathan, V., et al. *Design considerations for solar energy harvesting wireless embedded systems*. in *Proceedings of the 4th international symposium on Information processing in sensor networks*. 2005. IEEE Press.
103. Minami, M., et al. *Solar biscuit: A battery-less wireless sensor network system for environmental monitoring applications*. in *Proc. 2nd International Workshop on Networked Sensing Systems (INSS2005), San Diego, CA, USA*. 2005.
104. Stanley-Marbell, P. and D. Marculescu. *An 0.9× 1.2, low power, energy-harvesting system with custom multi-channel communication interface*. in *Proceedings of the conference on Design, automation and test in Europe*. 2007. EDA Consortium.
105. Jiang, X., J. Polastre, and D. Culler. *Perpetual environmentally powered sensor networks*. in *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on*. 2005. IEEE.
106. Zhang, P., et al. *Hardware design experiences in ZebraNet*. in *Proceedings of the 2nd international conference on Embedded networked sensor systems*. 2004. ACM.
107. Quick, D. *Power from a tree*. 2009 [cited 2014 15.10.]; Available from: http://www.gizmag.com/tree-powered-electricity/12772/.

108. *Voltree*. 2005 [cited 2014 15.10.]; Available from: http://voltreepower.com/companyInfo.html.
109. McGarry, S. and C. Knight, *Development and successful application of a tree movement energy harvesting device, to power a wireless sensor node.* Sensors, 2012. **12**(9): p. 12110-12125.
110. Blatt, F., et al., *Thermoelectric power of materials.* 1976.
111. Yildiz, F., *Potential ambient energy-harvesting sources and techniques.* 2009.
112. Strasser, M., et al., *Micromachined CMOS thermoelectric generators as on-chip power supply.* Sensors and Actuators A: Physical, 2004. **114**(2): p. 362-370.
113. Wang, Z., et al. *Micromachined thermopiles for energy scavenging on human body*. in *Solid-State Sensors, Actuators and Microsystems Conference, 2007. TRANSDUCERS 2007. International*. 2007. IEEE.
114. *Thermal wristband*. [cited 2014 15.10.]; Available from: http://www.roachman.com/thermic/.
115. Xu, Y., *Ferroelectric materials and their applications.* 1991.
116. Cuadras, A., M. Gasulla, and V. Ferrari, *Thermal energy harvesting through pyroelectricity.* Sensors and Actuators A: Physical, 2010. **158**(1): p. 132-139.
117. *Temperature changes clock*. [cited 2014 15.10.]; Available from: http://www.atmosadam.com/howitworks.html.
118. Ostaffe, H. *A brief introduction to RF energy harvesting: what it is, what it does, and how it enables wireless sensor networking applications.* 2013 [cited 2015 02.02.]; Available from: http://www.sensorsmag.com/sensors-mag/rf-energy-harvesting-enables-wireless-sensor-networks-6175.
119. Hagerty, J.A., et al., *Recycling ambient microwave energy with broad-band rectenna arrays.* Microwave Theory and Techniques, IEEE Transactions on, 2004. **52**(3): p. 1014-1024.
120. *Powercast*. [cited 2014 15.10.]; Available from: http://www.powercastco.com.
121. Vullers, R., et al., *RF harvesting using antenna structures on foil.* Proc. of PowerMEMS, 2008: p. 209-212.
122. Ungan, T. and L. Reindl. *Harvesting low ambient RF-sources for autonomous measurement systems*. in *Instrumentation and Measurement Technology Conference Proceedings, 2008. IMTC 2008. IEEE*. 2008. IEEE.
123. Ancey, P. *Ambient functionality in MIMOSA from technology to services*. in *Proceedings of the 2005 joint conference on Smart objects and ambient intelligence: innovative context-aware services: usages and technologies*. 2005. ACM.
124. Theeuwes, J.A., et al. *Efficient, compact, wireless battery design*. in *Wireless Technologies, 2007 European Conference on*. 2007. IEEE.
125. Beeby, S.P., M.J. Tudor, and N. White, *Energy harvesting vibration sources for microsystems applications.* Measurement science and technology, 2006. **17**(12): p. R175.
126. Roundy, S., *On the effectiveness of vibration-based energy harvesting.* Journal of intelligent material systems and structures, 2005. **16**(10): p. 809-823.
127. Williams, C., R.C. Woods, and R. Yates, *Feasibility study of a vibration powered micro-electric generator.* 1996.
128. Perpetuum. *Vibrational energy harvester*. [cited 2015 08.01.]; Available from: http://www.perpetuum.com/products/vibration-energy-harvester.asp.

129. Boisseau, S., G. Despesse, and B.A. Seddik, *Electrostatic conversion for vibration energy harvesting.* arXiv preprint arXiv:1210.5191, 2012.
130. *Fundamentals of Piezo Technology*. [cited 2015 12.01.]; Available from: http://piceramic.com/piezo-technology/fundamentals.html.
131. Townley, A., *Vibrational energy harvesting using MEMS piezoelectric generators.* 2009.
132. Zuo, L. and X. Tang, *Large-scale vibration energy harvesting.* Journal of intelligent material systems and structures, 2013. **24**(11): p. 1405-1430.
133. Ericka, M., et al. *Energy harvesting from vibration using a piezoelectric membrane*. in *Journal de Physique IV (Proceedings)*. 2005. EDP sciences.
134. Wang, B. *Human gait could soon power portable electronics*. 2011 [cited 2015 02.02.]; Available from: http://nextbigfuture.com/2011/08/human-gait-could-soon-power-portable.html.
135. MacVittie, K., et al., *From "cyborg" lobsters to a pacemaker powered by implantable biofuel cells.* Energy & Environmental Science, 2013. **6**(1): p. 81-86.
136. *passive Human sources*. 2011 [cited 2014 28.10.]; Available from: http://spectrum.ieee.org/biomedical/devices/swiss-scientists-design-a-turbine-to-fit-in-human-arteries.
137. Starner, T., *Human-powered wearable computing.* IBM systems Journal, 1996. **35**(3.4): p. 618-629.
138. *Heart movement*. [cited 2014 28.10.]; Available from: http://phys.org/news145533330.html - nRlv.
139. *Organ mouvement*. [cited 2014 28.10.]; Available from: http://ip.com/patapp/US20050256549.
140. *Organ movement piezoelectric*. [cited 2014 28.10.]; Available from: http://phys.org/news/2014-04-heart-powers-pacemaker.html - nRlv.
141. *blood flows*. 2011 [cited 2014 28.10.]; Available from: http://phys.org/news/2011-05-tiny-turbine-human-artery-harvests.html.
142. Ramsay, M.J. and W.W. Clark. *Piezoelectric energy harvesting for bio-MEMS applications*. in *SPIE's 8th Annual International Symposium on Smart Structures and Materials*. 2001. International Society for Optics and Photonics.
143. Sohn, J., S.B. Choi, and D. Lee, *An investigation on piezoelectric energy harvesting for MEMS power sources.* Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science, 2005. **219**(4): p. 429-436.
144. Paradiso, J.A. and M. Feldmeier. *A compact, wireless, self-powered pushbutton controller*. in *Ubicomp 2001: Ubiquitous Computing*. 2001. Springer.
145. Kymissis, J., et al. *Parasitic power harvesting in shoes*. in *Wearable Computers, 1998. Digest of Papers. Second International Symposium on*. 1998. IEEE.
146. Derr, K.W., *AUTOMATIC WATCH MAIN-SPRING WINDING MECHANISM*. 1956, Google Patents.
147. Crisan, A., *Typing power*. 1999, Google Patents.
148. Huang, W.-S., et al. *Design and fabrication of a vibrational micro-generator for wearable MEMS*. 2003. Institute of Electrical and Electronics Engineers.
149. Shenck, N.S. and J.A. Paradiso, *Energy scavenging with shoe-mounted piezoelectrics.* IEEE micro, 2001. **21**(3): p. 30-42.

150. *In step nano-power*. [cited 2015 02.02]; Available from: http://www.instepnanopower.com/2_Technology/Technology.aspx.
151. Siekkinen, M., et al. *How low energy is bluetooth low energy? comparative measurements with zigbee/802.15. 4*. in *Wireless Communications and Networking Conference Workshops (WCNCW), 2012 IEEE*. 2012. IEEE.