Advance Metering Infrastructure for Smart Grid Real Time Energy Management Using Mesh Networks Based on IEEE802.15.4 and 6LoWPAN

by
Matias Ariel Kippke

Submitted to the Department of Electrical Engineering, Electronics, Computers and Systems
in partial fulfillment of the requirements for the degree of
Erasmus Mundus Master Course in Sustainable Transportation and Electrical Power Systems
at the
UNIVERSIDAD DE OVIEDO
September 2020

Certified by . . . .
Dr. Pablo Arboleya
Associate Professor
Thesis Supervisor

Certified by . . . .
Dr. Islam El Sayed
Associate Professor
Thesis Supervisor

Certified by . . . .
Dr. Adriano Mones Bayo
Phoenix Contact
Thesis Supervisor

Advance Metering Infrastructure for Smart Grid Real Time Energy Management Using Mesh Networks Based on IEEE802.15.4 and 6LoWPAN

by

Matias Ariel Kippke

Submitted to the Department of Electrical Engineering, Electronics, Computers and Systems
on September 1, 2020, in partial fulfillment of the
requirements for the degree of
Erasmus Mundus Master Course in Sustainable Transportation and Electrical Power Systems

Abstract

This thesis main goal is to propose an innovative method for smart meters infrastructure for real time data acquisition, focusing on smart grids application. Initial target was to measure energy readers performances, but later it could be demonstrated that the same communication interface is capable of interconnect any kind of sensors with a Serial Peripheral Interface, focusing on the integration of IoT devices into a common network. The development involves the comparison between different products available in the market, as well as comparing and selecting a proper communication protocol for the required task, taking into consideration required bandwidth and power consumption constrains. Simulations have been undertaken using Cooja simulator and coding has been done in C language using Contiki-NG development suite. Final deployment is done based on a mesh-topology network based on IEEE 802.15.4 standard with IPv6 over Low-Power, Lossy Networks IETF 6LoWPAN network structure. A series of test with two smart meters acting as UDP-clients, one data collector device acting as the network gateway and one device as a sniffer are shown, demonstrating the feasibility of the proposed network interface. Future work approach is also presented, where Blockchain applications and peer-to-peer energy trading are considered as the next steps towards a fully integration with smart cities emerging infrastructures.

Thesis Supervisor: Dr. Pablo Arboleya
Title: Associate Professor

Thesis Supervisor: Dr. Islam El Sayed
Title: Associate Professor

Thesis Supervisor: Dr. Adriano Mones Bayo
Title: Phoenix Contact

Acknowledgments

I would like to thank my supervisors, Dr. Pablo Arboleya and Dr. Islam El Sayed. Without their dedication and compromise during these strange times of home office and teleworking, this thesis would have taken much longer until it could see the sunlight.

Special thanks to Dr. Adriano Mones Bayo and Phoenix Contact company for their unconditional support, providing their solid knowledge in the industry and their high-quality equipment.

Thanks to the University of Oviedo, but most important to every university where I have the privilege to study during the last two years: Instituto Superior de Engenharia de Coimbra (ISEC) in my beloved Portugal and the University of Nottingham, where I started thinking about this project.

Special thanks to the Presidente do Departamento de Engenharia Eletrotécnica at ISEC, Cristina Faustino Agreira, who behaved like an gentle mother from the first moment I arrived to this continent. Being far away from home is not easy when affections are separated by thousands of kilometers. Finding people that make you feel at home is priceless.

To my parents, Liliana and Ariel, you both know I could not be here achieving my dreams without your sacrifice. With all my love for you both.

To my friends, from this side of the ocean and from the other, for all the time I stole from them. To the mighty *Glitterforce* born in the Kilbourn Street NG3 1BQ, from the UK to Spain, and hoping it will remain eternal. My deepest gratitude to you.

To *Lola*, *Chelo* and *Nina*. Without you three, this thesis could have been finished earlier for sure.

And mostly, thank you to my partner in crime, my dearest Belén, for her priceless company during this last year. I hope you are proud of what can be created together with love and dedication. The world awaits us.

Due to Coronavirus (COVID-19), all TCP applications are being converted to UDP to avoid handshakes...

Sincerely, 2020.

Contents

Figures

Tables

Chapter 1

Introduction

Data governance has become a key concept in the upcoming development in Smart Cities. The fact that end-users become not only aware of the data they consume, but also of the data they produce, creates a new paradigm in the awakening of *Internet of Things* (also known as IoT) infrastructures applied to cities. When it comes to the energy management field, the *data* as a concept starts to broaden its own boundaries: with the awakening of scalable, renewable energy sources, former consumers are given the chance not only to make use of the energy, but also to produce their own. This opens a new concept, where the end-user starts to become more than a mere *consumer*, taking the role of a *producer* as well, giving birth to the concept of a *prosumer* [17]. Thus, a new interrogate arises, whether the actual infrastructures are suitable of handling such amount of information. Truth is, former cities are based on outdated infrastructures. Energy structures are designed in a one-way path, making it extremely difficult to propose new alternatives. The development of fast, reliable communication interfaces nowadays in modern urban nuclei has become as important as having well paved, secure roads. These information highways may be determinant when it comes to improve life quality. For a former town to step up and transform itself into a *Smart City*, digital infrastructures are vital. This Masters' Thesis aims to develop the first steps towards the awakening of digital framework applied to cities, analysing concepts such as new IoT devices and revolutionary communication protocols, aiming to improve the way energy is monitored and consumed.

1.1 Awakening of Internet of Things

The term *Internet of Things* may sound as a new paradigm, but to be truth IoT has been around for many years in the process of building itself. The concept is based on data acquisition throughout a large variety of sensors, and later being able to transfer that information across a network [4]. Nowadays, the amount of sensors that can be integrated into an established network are increasing exponentially: energy smart meters, lighting sensors applied to smart lighting, residential water and gas readings, among others.

1.1.1 Factors for IoT development

Although they have been developing quietly in the first half of the XXI century, IoT technologies and devices application have shown a steep grown in the last couple of years. In other words, it may be not strictly excessive to define the awakening of IoT as a fourth Industrial Revolution right before after the steam engines, the mass production factories and embedded computers, given the positive impact it may have in transforming business and societies. The reasons behind this astonishing development may be seen in detail as follows, as illustrated in [4] there are mainly twelve strictly defined causes:

1. **The convergence between Operation Technology (OT) and Information Technology (IT):** As technology specializes, OT starts to depend more on trustworthy, real-time information due to safety concerns and to guarantee security and control.

2. **Multitude of companies based on Internet applications and making use of IoT devices information:** From Amazon to Uber, the amount of companies that depend on Internet services are exponentially increasing. Moreover, with the upcoming technology of self-driving vehicles stimulated by Tesla, the amount of interconnected sensors being used in the industry is expected to grow aggressively, which takes it to the next point.

3. **Awakening of a multiplicity of IoT devices, even mobile phones:** Telephones became part of societies' daily life. Even more, mobiles could be consider the precedent of IoT end-devices, given the fact that devices are connected in a network structure.

4. **The Era of Social Media and Social Networking:** Not only for communication but also for economics and tradings, social networks are the main background infrastructure that allows people and business to be interrelated. As depicted in the introduction, *prosumers* are the key-role players in the upcoming energy market business. Therefore, the development of suitable, social and business networking towards trading applications may show a rapid increment.

5. **Analytics and Big Data, the new paradigm of *data governance*:** Considering *structure data* or *unstructured data*, truth is that huge amounts of information are already being generated by a large amount of devices. Each piece of information might become extremely useful in the future, which also raises concerns about security and *data privacy.*

6. **Cloud applications incitement:** As networking infrastructures are evolving, same happens to storage and computing frameworks. From Microsoft Azure to Amazon AWS services, large amounts of data have finally found a place to be stored and processed accordingly. Nevertheless, this also propose a new challenge in the upcoming IoT networks, as data generation is expected to grow exponentially.

7. **New technology hype:** Developers have not only access to the Internet as a networking platform, but also the amount of development boards available in the market grown unexpectedly. Linux-based devices, such as Raspberries or Arduino based devices are available at low costs, as well as considering that new players are developing their own prototypes focused on the benefits of innovating in such a brand-new market, like the IoTs in general. Documentation, associated *know-how* and related developments are consistently thickening.

8. **Digital transformation of cities towards Smart Cities:** The tip of the iceberg is to combine IoT devices, with a strong network and storage infrastructure. Together with social networking and large amount of information exchange, the characteristics for a perfect storm are combined. The result is the awakening of brand developed cities, completely controllable and energy efficient.

9. **Ability to develop new user interfaces:** Smart Cities might be accepted by the society, but only if they manage to develop a friendly user interface with its inhabitants. Therefore, the awakening of Smart Cities and IoT must come hand-by-hand with the awakening of new ways of communications with the end-users. Energy-trading applications, *In-Home-Displays* (also known as IHD), information that is available to everyone. Infrastructures are important, but the right assimilation with the consumers is a key-factor in accepting technological changes.

10. **Fast adaptation and assimilation:** Interconnected devices began to outnumber the world back in 2010. Studies shown that acceptance of IoT has overcome the acceptance of electricity or telephone inventions in a 5:1 relation. Normally, adopting a new technology comes hand-by-hand with population expansion. Therefore, awareness of IoT devices and its impact in daily-life is expected to grow uncontrollably in the upcoming years. Proof of this is the growth in global IP traffic, as depicted by CISCO in [18].

11. **Security concerns:** As large amount of data is handled, also means that security and privacy protection is raising awareness among business and end-users. From financial transactions up to a possible environment where energy trading from *peer-to-peer* becomes a reality, sensible data is being used and must be safeguarded for privacy reasons. Moreover, the use of a large amount of domestic IoT devices, such as surveillance cameras or smart home appliances raises concerns about the impact that cyber-attacks might have in the near future.

12. **The beloved Moore's Law:** According to Moore's Law, *computing power will double approximately every 18 months.* Taking into consideration that the widest existing networks contain millions of nodes sending different kinds of information, the amount of data and new connections that are going to be developed in the upcoming years is astonishing. This illustrates a quite beneficial position for the developing of IoT technologies, but also proposes a set of interesting challenges, like the developing of strong, reliable digital infrastructures, among others.

1.2 Energy Management

Traditionally, the energy market has been conceived to be working as a *one-way* business: A couple of large power plants produce the electricity and dispatch it downstream towards industries and end-users. Generation and distribution of electrical power have been working under the same principles uninterruptedly for more than a century. Energy market is therefore based on projections: Key-role players bid a certain amount of energy for a 24-hour period, carefully considering estimations done by the habits of the consumers and the industries. On the other hand, producers compromise themselves to deliver the required amount of energy that the market demands. In that way, the energy market becomes one of the most precise, well-calculated and complex business of the modern-era.

1.2.1 Daily Consumption Curves Analysis

As it can be depicted from Figure 1-1, based in the electricity demand curve in Spain on a specific day of August, the daily electrical demand curve is based on estimations done by the market. As expected, the demand of energy is based on human activity, even differentiating the impact on consumption based on an specific period of the year. Basically, more energy is consumed during the winter, given the fact that it is used as a source of heating. In general, peaks of consumption are given around mid-day and in the afternoon, as there is a marked plunge in consumption after midnight.

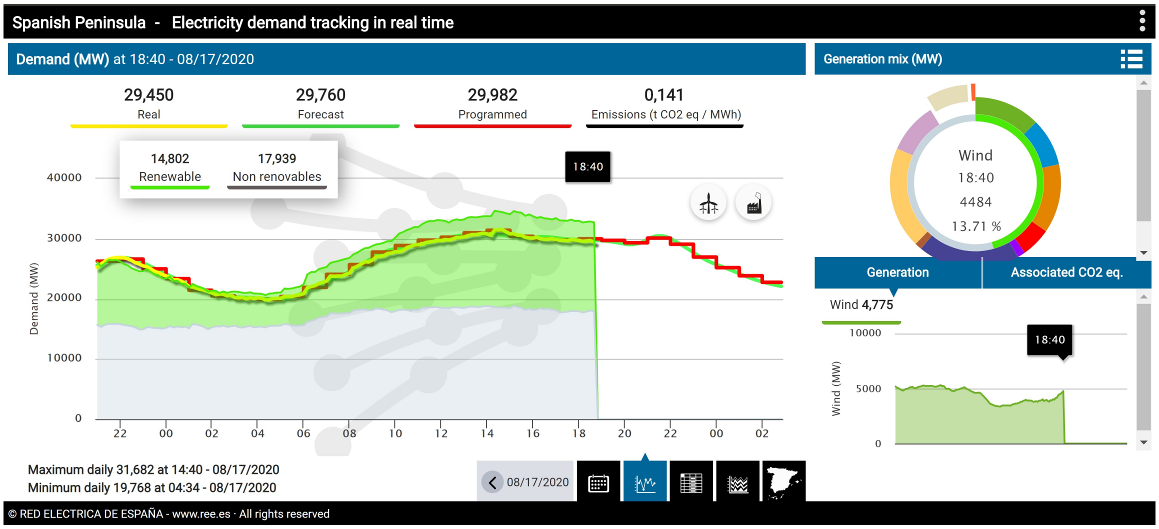

Figure 1-1: Daily electrical demand curve. Consumption and expected demand [1].

1.2.2 Issues and solutions

Energy market will face a complete transformation in the upcoming years. Reducing the political influence and the new regulations towards renewable energies were the first large steps. However, as new challenges arises, new answers and solutions need to be proposed [19]. As analyzed before in 1.2.1, large plunge and small fluctuations are common in the electrical market. As the first ones are easily predicted, the last ones are quite a challenge to manage. Not only they affect the overall prices in the market for both consumers and producers, but they also can be determinant factors for transmission lines overloads or energy surplus at the generating points of the system. Moreover, taking into consideration the awakening of renewable energy sources and their integration as a distributed generation system, fluctuations will not only have a large impact at the demand-side, but also at the generation offer. Although the promotion of renewables is encouraged in order to drastically reduce pollution and CO2 generation, the fact is that roper energy storage infrastructures have not been developed yet, and legal frameworks and regulations are far away from becoming a reality. Even worse, the uncontrollable demand and offer of electrical vehicles demands the development of a demand-side organised schedule, based on precise predictions, to prevent overloads or load shedding mechanisms.

1.3 Targets and Overall Vision

Designing a robust, trustworthy advance metering infrastructure (AMI) is the first step in order to guarantee the availability of reliable data to process. Nevertheless, design should not only focus on the metering infrastructure, but also in the data processing side, the interconnection with cities digital existing frameworks and the proper storage of the huge volume of data generated. Other factors, such as security and proper encryption are not being covered by the following thesis. In resume, the main targets of this thesis can be emphasised as follows:

1. **Building a *digital* infrastructure:** Such as *digital highways*, data generated by each device needs a solid framework to be transmitted. Communication protocols are analyzed, considering not only technical aspects such as *penetration constants* or *range*, but also more application factors such as *energy consumption* and *feasibility of application in cities and industrial environments*.

2. **Devices selection:** Market is flooded with new devices, capable of giving a huge amount of information. But the right tool for each task must be carefully chosen. Energy smart meters technologies are compared, taking into consideration how they can be correctly placed not only in residential environments, but also in industrial applications. Multiple manufacturers offer suitable products that can be implemented in order to create an A.M.I. system, so luckily the market is diverse enough.

3. **Practical applications and interconnection with existing infrastructures:** As the metering framework is developed, this also implies that it need to be integrated. Concepts such as *bandwidth*, *amount of data* and proper *sampling period* have to be analyzed, in order not to interfere or overload the preexisting infrastructures. Practical examples developed together with the City of Gijón are shown, given the fact that the city is implementing new communication protocols towards optimizing their lighting infrastructure's energy consumption [20].

4. **Integration with distributed generation:** As *consumers* become *prosumers*, the ability of a proper A.M.I. to foresee the consumption and generation of energy is analyzed. The fact that a system like the one proposed may be used to predict behaviours of end-users and industries is a key factor in order to generate a proper schedule that is useful to increase the effectiveness in the energy market. As depicted before in 1.2.2, this is the main goal in order to take awareness of the necessity of having a smart system that can not only predict, but also control the way energy is generated, stored and consumed.

5. **Security concerns:** Data is sensible. The fact that data processing and storage could be used to study human habits and predict behaviours implies a huge responsibility towards privacy. Although proper encryption in not covered by this thesis, the concern is taking into consideration and will be left as a future development that needs to be addressed before the implementation of A.M.I. becomes a reality.

As literally depicted in [17], main motivation behind the development for advance measurement infrastructures towards smart grids and IoT should be achieving for heterogeneity, openness, scalability and agility. As accurately depicted in [21], what is Internet of Things in practice? The most simplest way of explaining it is that IoT encompasses all devices and networks natively IP-enabled and Internet connected. Bearing that in mind, next section 2 focuses on the theoretical background, state-of-art, feasibility and technological aspects of this master's thesis.

Chapter 2

Literature Review

The application of advance metering infrastructures for energy management applied to industrial and residential buildings is not a brand new topic. There are multiple examples depicting the use of smart meters working under IEEE1888 communication standard as a data acquisition gateway for energy management systems [22], also being applied in industrial environments [3] or in smart grid applications overall [12]. Problem starts to arise when an specific communication protocol has to be selected for a certain application, given the amount of options that can be developed fulfilling the specific requirements. Many options have been proposed, being the most relevant the ones being used in industrial applications, given the fact that it not only implies the use of reliable communication infrastructures, but also transmitting information alongside Low Power and Lossy Networks, known as LLNs.

2.1 Advance Metering Infrastructures

Advance Metering Infrastructures, also widely known as AMIs, should not be confused with Automated Meter Reading (or AMR) application systems. While the last ones are interpreted as end-devices uploading information about consumption to an specific cluster of *servers*, the first group presents some differences, which can be enumerated as follows based on the description given in [12] and [13]. As AMI applications become more complex, it also means that control can be done in a much more assertive way:

- **Communication insights:** An advance metering infrastructure could basically not only measure, but also control the energy distribution given a two-ways communication framework between the smart meters as end-nodes, a data collector device also described as a Local Border Router (LBR) and the respective servers in the *cloud* which handle the storage and the process of information.

- **Programmable behaviour:** Data provided from the AMI could be accessed *at will*, which means that a schedule has to be carefully programmed in order to comply with the available communication channel data bandwidth, as well as not to overload the available information storing servers, as well as the devices acting as intermediate routers or border routers. Also, allowing remote configuration implies that energy supply to an specific end-user (understood as a physical end-user or a specif equipment in an industrial environment) can be controlled as commanded, which gives the possibility to easily shedding the corresponding energy demand.

- **Flexible network architecture:** Idea behind having an AMI is to being able to interconnect smart meters in close proximity using low-power links, creating a *mesh*-structured network. These kind of networks, compared with *star*-structured networks present several advantages, one of the most important lies on the fact that connections are *self-healed*, which means that there is not a single path from an end-node to an specific data collector, as communication routes are actively changing their configuration following routing protocols based on *metrics* and having a large impact in the ubiquitous part of the network. One of the most important routing protocols used in IPv6 applied to IoT is the Routing Protocol for Low-Power and Lossy Networks, also known as RPL, which will be analyzed in 3.6.

- **Multiple applications:** End-nodes in a *mesh* topology network could also be implemented on other types of meters apart from energy applications. The same topology might include gas and water meter devices, smart lighting communication nodes, home appliances sensors and charging stations for PEVs.

2.2 Wired Connections for AMIs

Main question arises between the use of wired connections alongside the already existing power network infrastructure or to develop new links using wireless technologies. First case shows some relevant advantages, as it can be depicted in [12]. Power Line Communication, also known informally as PLC proposes a reduced costs infrastructure for increasing the flexibility, security and control features to legacy power grids, which were created with the solely intention of delivering energy in a one-way path. As analyzed before in 1.2.2, demand growth and the advent of Plug-in Electric Vehicles, a.k.a. PEV, could uncover new possibilities to provide power to homes and valley-filling energy supply during demand peaks, as literally explained in [12]. Geographical impact for the proposed system has an unexpected impact as well: PLC technologies for IoT applications in the grid might be expensive in places where there are few consumers directly connected to a transformer. In the United States, the number of consumer per transformer is roughly five, which does not justifies the positive impact for the use of PLC infrastructures [23]. Nevertheless, in Europe the situation changes drastically, as the amount of consumers per transformer equipment is around 300, which encourages the development of the mentioned communication framework [24]. Distributions transformers, therefore, become one decisive element in smart grid applications and network monitoring, as punctually depicted in [25]. Considering traditional internet communication protocols like TCP/IP, adaptations have to be done in order to apply them for smart grid communications using other protocols such as ZigBee or 6LoWPAN infrastructures [2], as shown in Figure 2-1.

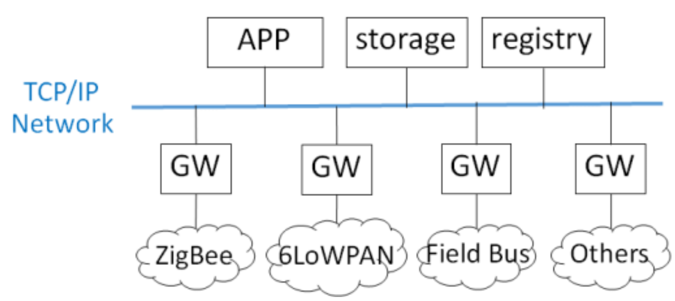

Figure 2-1: IEEE1888 proposed architecture [2]

.

Another main advantage of PLC application for smart grid communication lies on the fact that PLC development supports IPv6 packets structure without the need of data fragmentation [12], different from communication based on IEEE 802.15.4 protocol which proposes an adaptation layer to allow the transmission of IPv6 data packets as depicted in [26]. As in many cases smart meters are already being integrated in energy distribution networks, wired communication proposes a low-cost advantage, making it possible for them to also work as a multiple-sensing system towards estimation of power consumption, active price setting and quality-of-service information. Moreover, wired infrastructures have a significant advantage when it comes to analyze reliability of communication, reducing the need of strategical positioning of devices in order to avoid concrete walls or any kind of objects that may cause a disruption or attenuation. This points out a significant advantage in industrial environments, where LLNs have their major impact. As pointed out by the authors in [12], wireless communication experiences penetration losses and significant attenuation, even worse considering that devices are strongly recommended to be designed for low-power consumption, as it is further analyzed in 3.5.

Table 2.1: QoS and bandwidth requirements for AMI application [12],[13],[14],[15]

Traffic Class	**Services**	**Requirements characteristics**
High Priority and Critical	Power outage, pricing notification, event and emergency messages	$\geq$98% packet delivery within 5s Payload $\leq$ 100bytes
Critical	Power quality, meter service, connection and disconnection	$\geq$98% packet delivery within 10s Payload $\leq$ 150bytes
Normal Priority	System events: Faults, security, configuration	$\geq$98% packet delivery within 30s Payload $\leq$ 200bytes
Low Priority	Periodic meter reading	$\geq$98% packet delivery within 2hrs, 6 times/day Payload $\leq$ 400bytes
Background	Firmware/software download	$\geq$98% of devices processed within 7 days Update file $\leq$ 1MB

Although the numerous advantages in cost reductions and equipment positioning which may incline the scale for PLC applications, the truth is that it's main disadvantage from the use of wired connections in smart grid applications comes from the high latency and reduced bandwidth. In order to guarantee the Quality of Service (QoS), Table 2.1 enumerates the requirements as extracted from [15]. Latency, also interpreted as delay, is a key attribute for analysing AMI performance. Results shown in [12] demonstrate that latency parameters are worst in narrow-band PLC line interfaces, described as NBPLC, compared with Low-Powered Wireless Personal Area Networks, also known as LoWPAN, based on IEEE 802.15.4 standard. Following sections as 2.3 will address the main advantages for wireless networks, and why they are the chosen solution to implement AMI frameworks towards industrial and end-user applications.

2.3 Wireless Alternatives for AMIs

Breaking the dependency on electrical equipment such as power lines and distribution transformers also implies the development of new infrastructures in order to equip traditional transmission lines with brand new capabilities such as enhanced communication, Quality-of-Service (QoS) control and security. Several investments have to be made, but reduction in wired connections translates as more flexibility and ease-of-access for industrial applications mostly.

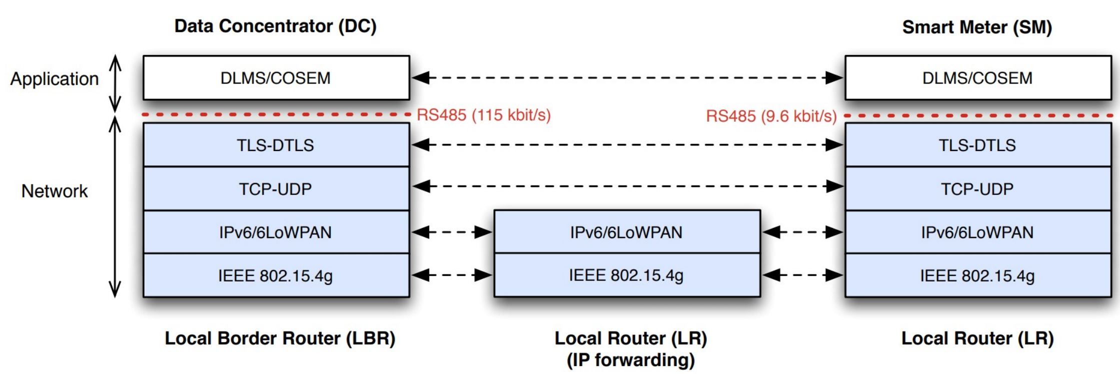

Figure 2-2: Proposed protocol stacks based on three types of equipment [3]

.

Awakening of IPv6 is not new, but it has found a perfect place to grow in IoT application field, where a multiplicity of devices must be interconnected. Principal advantages relies on the combination of IEEE 802.15.4 standard, together with RPL routing protocol and 6LoWPAN Internet Engineering Task Force (IETF) working group [3]. Structure for an AMI framework is composed by three key elements, depicted as follows from the example analyzed in [3] and shown in Figure 2-2:

- **Local Router (LR) applied as end-node solution:** With DLMS/COSEM smart grid metering applications in mind [27], the local router is the main infrastructure element to equip each of the smart meters with a network interface. Combination between a smart meter and a local router can be depicted as an end-node, which acts as an UDP or TCP client respectively, depending on the system's final configuration. Interconnection between the smart meter and the local router can be done in different ways, depending on the technology development of the smart meters as analyzed in 4.1. Normally, RS-232 or RS-435 are preferred protocols for implementing the physical layer between those two devices [3].

- **Local Router (LR) applied as IP forwarding:** For the sake of connectivity improvement, some local routers can be distributed alongside the infrastructure network acting solely as a router and forwarding IP packages between the end-nodes and the data concentrator. A local router can be deployed in a stand-alone operation, therefore providing the overall system with flexibility, as the location of smart meters can be done freely without compromising the performance and keeping latency between acceptable values. Basically, LRs do not process protocols above layer 3 from the OSI model described in 3.1, therefore do not work with protocols above IPv6/6LoWPAN [3].

- **Local Border Router (LBR) acting as a Data Concentrator (DC):** With an IP stack similar to a local router, the border local router acts not only as a data concentrator for the smart meter's information, but also provides connectivity to the internet environment and *cloud* applications.

Therefore, memory and processor requirements are larger in LBR than in LRs. Strategically, LBRs are generally located in power transformers. As wisely depicted in [12], AMI interfaces with LBRs require a relatively high up-link bandwidth to upload data from smart meters to utility servers. Therefore, LBRs election and design should also have high bandwidth interfaces, which may be linked with the awakening of 4G/5G applications for short-period bursts of large data packets.

2.4 Industrial and Smart Grid Applications

Results shown in [12] seem to be promising for using wireless solutions to interconnect end-nodes and data acquisition equipment. As presented in the analyzed simulations [3], having a multiple end-node infrastructure as the one proposed also implies that in 95% of the time the local routers where at a distance not further than 4 *hops* to the LBR/DC, as shown in Figure 2-3. Interpreting the Round Trip Time (RTT) as a measure of the latency in the network, and considering that each additional *hop* implies an increment of 15ms to the total RTT, an approximately value of 4 *hops* can be translated as a latency of not more than 60ms. As depicted in [3] in their results, all RTTs were below 160ms. Therefore, for a real-time system application, having such RTT values could be acceptable, thus giving an advantage for wireless connections.

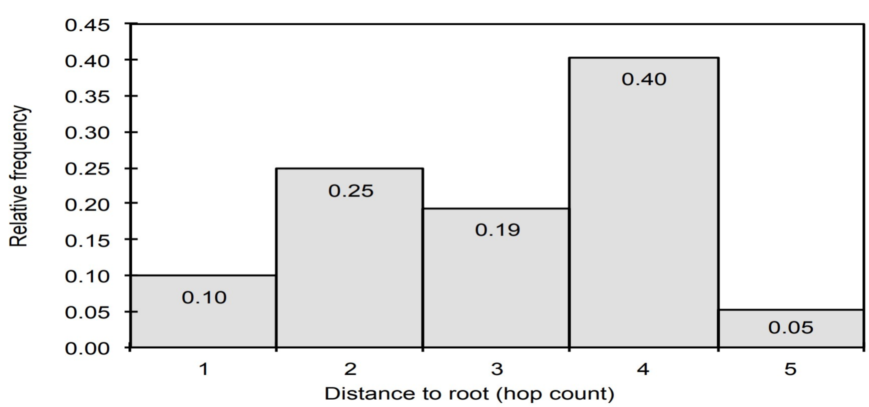

Figure 2-3: Histogram showing *hops* between LRs and LBR. Presented in [3].

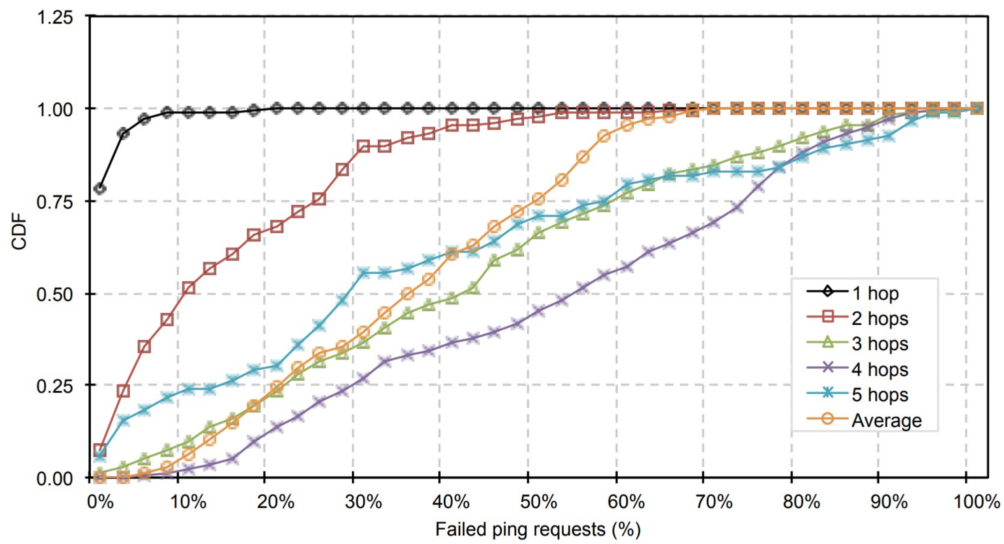

Figure 2-4: CDF of the *ping loss ratio* vs. distance. Presented in [3]

$$CDF : F_X(x) = P(X \leq x) \tag{2.1}$$

Moreover, the cumulative distribution function, depicted as in Eq. 2.1 shows that for 1 *hop* communication there is almost no loss of information, but increases significantly for more than 3 *hops* between LRs, as shown in 2-4. Ironically, in some cases links with 5 *hops* present less percentage of information losses than 3-4 *hops* links. This phenomena has an interesting background, as explained by [3]: RPL protocol encourages nodes to go up in the DAG look-up table and restrain them for going down as their link quality degrades. As the link quality tends to degrade or improve during the day given the uncertainty of wireless communication, many nodes that could have better service links for 4-5 *hops* end having worse service links for 3-4 *hops* given its position in the DAG tree, therefore presenting higher losses. Possible solutions to this kind of issues are presented in 5. Construction of DAG tree look-up table is extensively explained in 3.6.

2.5 Commercial Buildings and Home Appliances

Commercial building and Building Energy Management Systems (BEMS) are an emerging topic, where smart grids combined with IoT control and monitoring could improve significantly [22].

2.5.1 Power Quality Monitoring and QoS Applications

Given the importance around power quality monitoring in order to manage a smart grid accordingly, this used to be frequent in industrial applications, where dedicated, expensive equipment must be used. Deviations in power quality may lead not only to outages or malfunction, but also to severe damage of electric devices [17]. It was unimaginable for end-user and domestic appliances investing in such equipment, moreover considering the nonexistent profit for consumers [17]. The emergence of distributed generation systems also implies focusing on the quality of the provided service, therefore raising the awareness towards monitoring power quality. This demands the development of new structures which make use of low-cost, low-power equipment, making it accessible for end-users as well and providing enough amount of information to characterise the whole electrical network, towards the limits of what is known as *big data*. This is where several smart meters, forming a *mesh network* topology might find a perfect application [17]. One of the main challenges is to provide trustworthy measurements with lower latency and higher frequency, compared with traditional infrastructures. The FNET project is a perfect example of quality of power monitoring application, made for the U.S. power grid [28]. Nevertheless, the sophistication of the used equipment and the development costs makes this project unbearable for domestic appliances. Moreover, given the fact that the complexity of the grid is indeed growing with the awakening of PEV, which can also be considered as highly volatile consumption sources, thus degrading power quality if it is not correctly addressed. Nevertheless, the use of power quality indicators also means that end-users might know of they have malfunctioning devices connected to the network, which may cause not only disruptions to the grid, but also higher costs for consumers.

Smart meters combined with modern communication infrastructures, not only for data acquisition but also for using that information for quality improvement purposes has several advantages, based on the analysis presented in [17]:

1. **Increasing delivered power quality:** Several solutions have been proposed for smart grids towards improving efficiency and reducing losses in power lines: Static Synchronous Compensators (STATCOMs), Static Synchronous Series Compensators (SSSCs), Universal Power Flow Controllers (UPFCs), among a multitude of Flexible AC Transmission (FACTS) devices. Although being a feasible solution from the technological point of view, the truth is that the point has been always focusing on the generating-end of the whole system, but it has never took in account the other end of the electric market chain. A smart devices network, like the one analysed, could also have a positive impact on the efficiency from the consumers point of view, which also has a significant impact in the new paradigm of distributed generation: when *consumers* become *prosumers* as well, as mentioned in section 1.1.

2. **Clearer rules for the energy market:** Not only it gives the chance for the consumer to monitor its own consumption in a more *transparent* way towards data governance as detailed in 1, but also it promotes the creation of more decentralized rules for an extremely rigid electric market. There are projects which even propose the idea of *prosumers* to be able to sell and buy energy directly from each other, in a sort of *peer-to-peer* energy market [29]. This approach results not only curious, but also quite disruptive in the traditional rules of the market. Further analysis is made in section 6.

3. **Convergent solution with smart grid technologies:** Prediction based on energy consumption and habits are a fundamental aspect towards proposing a self-aware smart grid, which can prevent load shedding by relocating consumption towards *valley* hours, where the use of energy is reduced as it was shown previously in Figure 1-1 in subsection 1.2.1.

The energy being used by smart meters in domestic appliances is not accountable, and therefore not possible to make it billable. Moreover, the same happens for the communication devices used in data transmission towards the network. Therefore, the energy consumption for data acquisition and communication has to be reduced as much as possible [12]. Considering that every little amount of energy saved is accountable towards developing a near-zero energy consuming smart grid, Low-Power Wireless Personal Area Network (LoWPAN) devices emerged to the surface, founding themselves on the IEEE 802.15.4 standard. Section 3 will address the different communication protocols that found their place to flourish based on this standard. Nevertheless, as the right tool has to be chosen for the right work, same happens for smart meters application: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) ends up being the chosen protocol for this project towards its implementation for grid monitoring, which will be analyzed in particular in section 3.5.

Chapter 3

Protocols: Choosing the Right One

Once wireless protocols have proven to be preferred over wired connections given the technological advantages they present for networking, the main question that arises now is which protocol to choose for building a *mesh-network* applied to advance metering infrastructures. Following conditions have to be accomplished for a protocol to be considered in these kind of applications:

- **Low-Power Consumption:** As described previously in section 2.5, not only the energy consumption of the equipment itself, but also the energy cost consumed for transmitting data has to be addressed properly, moreover in domestic appliances given the fact that the energy consumed by the system is not billable. Type of protocols that must be considered should be designed considering low power consumption applications.

- **Acceptable Bandwidth:** Logically speaking, large burst of information consume more energy, given that each byte of information transmitted has an associated costs. Protocols with an acceptable MTU should be taken into consideration, although packet fragmentation and reassembly is a good strategy for achieving a compromise solution between low energy consumption and an acceptable bandwidth. Given the fact that smart meters technologies are diverse and could be designed for complex tasks as well, the decision regarding not only the type of data, but also the precision of it has to be taken into consideration.

- **Penetration Constant:** In order to get a profitable and trustworthy advance metering infrastructure, its behaviour in noisy environments has to be flawless. Industrial application devices have to overcome different type of obstacles that could have a direct impact in the quality and the range of the radio signals, thus conditioning the quality of the communication links or, even worse, forcing the design to have more devices in order to overcome this issues. The use of radio signals with a larger penetration constant means sacrificing bandwidth in exchange for range and reliability.

Low-power consumption protocols have been already developed, given the need of having standalone devices that can sustain operations with as little energy as possible. Moreover, with the emergence of IoT devices and applications and the little development in battery-storage based technologies, this point became a strong characteristic towards new developments, as depicted previously in section 2. Nevertheless, the first insight has to be made on the reliability of communications, and therefore the Open Systems Interconnection (OSI) standard is analyzed in section 3.1. Later, a deep analysis is made about the principles of the IEEE 802.15.4 standard, based on the use of sub-1GHz radio frequency, achieving not only the desired power consumption, but also a good behaviour in noisy, industrial environments and a reasonable bandwidth for the desired applications, as depicted in section 3.3. Once defined the importance behind the use of sub-1GHz communication infrastructures, two of the most prominent emerging protocols are analyzed. LoRaWAN is carefully depicted in section 3.4 as one of the first solutions offered to the new IoT world, considering low-power consumption and a global network application, following the LoRa Alliance [8]. Lately, the awakening of a new proposal, and the standard that is going to be used in the practical implementation of this project: 6LoWPAN, which is being addressed in section 3.5. Last but not least, a routing protocol for specific applications in LLNs is being deployed, as detailed in section 3.6, before jumping to the description of IoT devices, which compose the *hardware* infrastructure of this project.

3.1 OSI Model Insights

Reliable and efficient communication is one of the most difficult tasks that need to be fulfilled in large-scale networks applied to noisy environments [4]. The OSI model has been developed keeping in mind the standardization of protocols, regardless of underlying technological aspects. It literally breaks the network functionality into smaller functions, also descried as *layers*, in order to enable modular engineering developments [4]. Table 3.1 resumes its main aspects, highlighting its main functions, devices application that may be found in each one of them and protocols used.

Table 3.1: OSI model summarizing key functions, devices and protocols [4]
.

OSI Layer	Main Function	Examples of Main Devices	Examples of Main Protocol
Application	Provides network services to the end host's applications	Server, laptops, PCs	HTTPS, FTP, SSH, CoAP, MQTT
Presentation	Ensures the data can be understood between two end hosts	N/A	Data encoding Data formatting Serialization
Session	Manages multiple sessions between end hosts	N/A	Conn. management Error recovery
Transport	Establishes end-to-end connectivity and ensures reliable data delivery	Firewalls	TCP, UDP
Network	Connectivity and path selection based in logical addresses	Routers Firewalls	IPv4 IPv6 (6LoWPAN)
Data Link	Defines data format for transmission	Switches, APs	IEEE 802.1 IEEE 802.15.4
Physical	Defines physical media access and properties	Fiber optics Cat. 5 cables Coaxial cables	IEEE 802.3

OSI Model layers can be described as follows, as extracted from [4], starting from the top application layer down to the physical layer. The OSI model applied between two end-devices is depicted in Figure 3-1.

- **Layer 7 - Application:** This layers depicts where the users interact with network interfaces, using protocols such as DNS, HTTP, FTP, among others. In fact, it can be interpreted as an *abstraction* layer, specifying interfacing methods between end-users and networking environments.

- **Layer 6 - Presentation:** Operating systems services, such as Linux or Microsoft, work in this abstraction place. It is responsible for formatting information towards the application layer, as described before. It can also be interpreted as ensuring the data is understood by both sender and receiver.

- **Layer 5 - Session:** The session layer works with the communication protocol in order to manage and administrate one or multiple sessions between two network elements, which can be an end-node and a LBR, for example.

- **Layer 4 - Transport:** Basically, this layer establish and manages end-to-end communications between two end point devices. Data is being dissected into small unit called *segments*. It also ensures the reliability in data delivering, like error detection and packets re-transmission when it is needed. The most two well-known protocols used in this layer are TCP and UDP. While the first uses more bandwidth but ensures the delivery of information using *handshakes* and *acknowledgments* mechanisms, the last one is being used for repetitive and low-power, lossy networks. Re-transmissions are acceptable and data reception is not ensured in every case using UDP protocol.

- **Layer 3 - Network:** Provides connectivity and path selection, based on logical addresses (also known as IP addresses). For example, routing devices like LR or LBR operate in this layer. Data segments received from the *transport layer* are dissected in information packets, which are also known as IP datagrams.

Routing protocols are also specified in this layer, as for example the routing protocol for LLNs, as it will be later depicted in 3.6.

- **Layer 2 - Data Link:** Defines the format of data for final transmission, specifying communication *frames*. Data delivery is managed between devices on the same Local Area Network (LAN) by using Media Access Control (MAC) addresses, considering that the MAC address is unique for each device connected in the network acting as an identifier. Ethernet protocol and Point-to-Point protocol are being described in this layer.

- **Layer 1 - Physical:** The first layer in the OSI model describes the physical media access and its properties. It literally dissects the data received in binary signals, defining the electrical or mechanical interfaces. In other words, it defines how raw bytes are being transmitted over a physical link between two network devices, such as an end-node attached to a LR and a LBR. Radio carriers are defined in this layer as well, not only cabled interfaces.

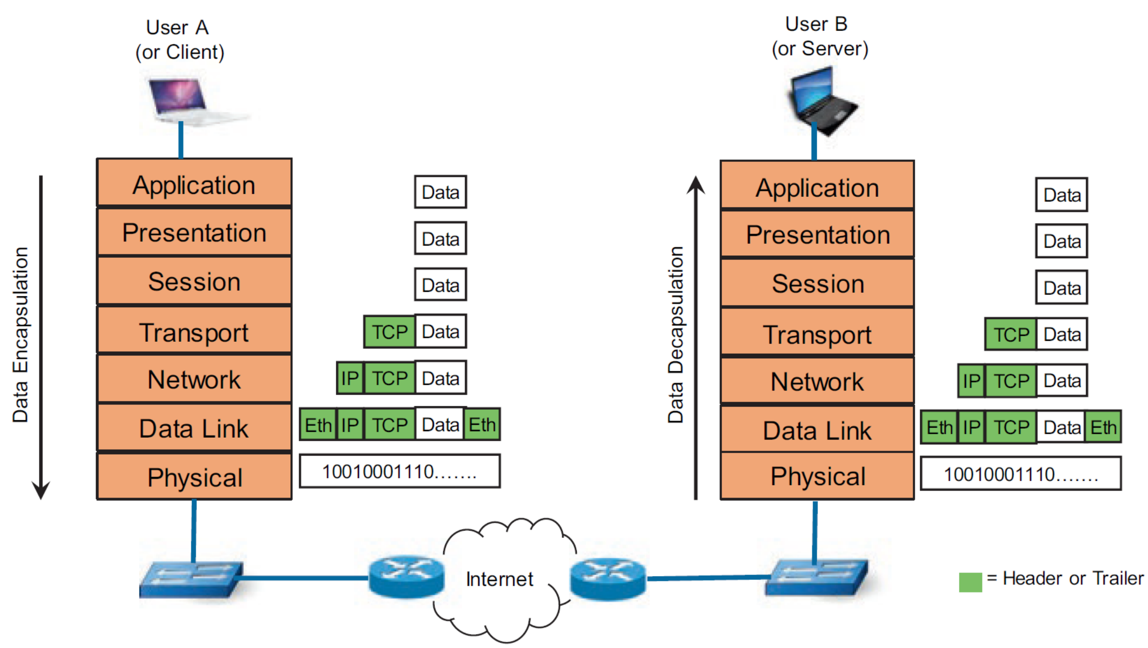

Figure 3-1: Depicting the OSI model between two end-devices [4]

.

3.2 IPv4 vs. IPv6

The IPv4 addressing protocol was the first emerging method to uniquely identify a specific network and an end-device inside that same network. It consist on 4-octets, 32-bit number separated by periods. With the raising awareness and the deploy of Internet of Things focusing on the hyper-connectivity and ubiquity of the network, IPv4 was not the optimal choice given the lack of available addresses (IPv4 has room available for 4.3 billion addresses) and given the fact that most of IPv4 addresses have been already assigned. Just for getting an idea, IoT devices are expected to grow up to 20 billion devices by the end of 2020 [4].

The new IPv6 was developed in order to address this problem in particular, allowing a multiplicity of intercommunication based devices. Nevertheless, given the increasing complexity of IPv6 compared with the former IPv4, devices running the new stack usually ended up consuming more energy [22]. In contrast with IPv4, IPv6 protocol uses 128-bit addresses, allowing in fact the overwhelming amount of $3.4x10^{38}$ available combinations. Nevertheless, this improvement also means that both IPv4 and IPv6 are not interoperable, which makes it more complicated to have an easy transition towards IPv6. In Figure 3-2, differences between both headers is shown.

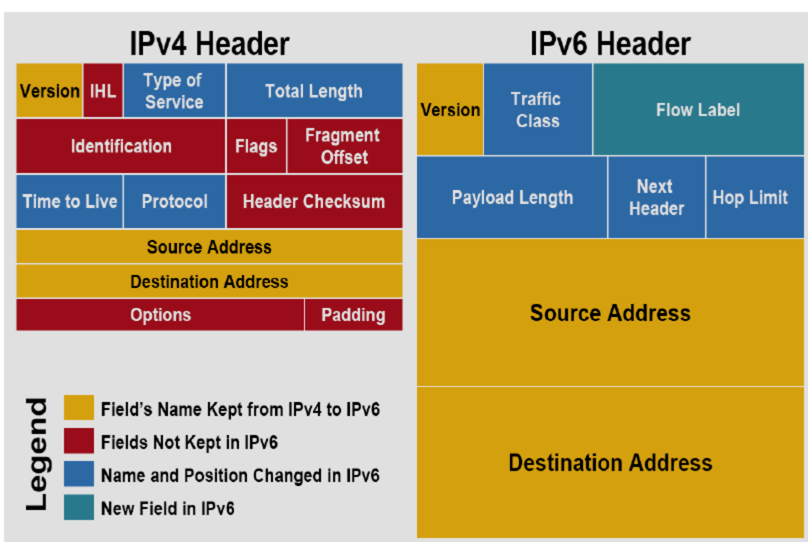

Figure 3-2: Comparison between IPv4 and IPv6 headers [5]

.

In order to make it more understandable, IPv6 addresses are normally expressed in 16-bit block in hexadecimal, and delimited with colons. Regularly, the leading zeros are removed, making it easier to comprehend. But the advantages of IPv6 addresses do not only resume down to the ability of having more devices connected to the IoT network environment. Device mobility features, security and configuration aspects have bee considered when the protocol has been created. Moreover, the use of hierarchical address allocation techniques simplifies the creation of routing tables accordingly.

IPv6 addresses can be classified in three well-defined categories:

- ***Unicast* addresses:** It acts as an identifier for a single interface. One packet sent to that type of address is delivered to the interface indicated by that same address only.
- ***Multicast* addresses:** It acts as an identifier for a group of interfaces, which may correspond to different nodes. Therefore, it can be delivered to multiple devices at once.
- ***Anycast* addresses:** It acts as an identifier for a set of interfaces that may belong to different nodes as well. Broadcasts messages as IPv6 packets are considered in this category.

3.3 IEEE 802.15.4 Principles

In this standard, physical layer (OSI model - layer 1) and MAC layer (OSI model - layer 2) are defined specifically for low-data-rate wireless connectivity with fixed, portable or moving devices with very limited battery consumption requirements [6]. As described before in section 3, the main goal behind finding a protocol suitable for IoT network development is to aim for low-power consumption, combined with an acceptable bandwidth. Therefore, IEEE 802.15.4 standard opens the door for a new IoT application developments, based on these characteristics.

Low-rate wireless personal area networks, also known as LR-WPAN, are defined as low-cost communication networks that are easy to install, provide reliable data transfer, have an extremely low cost and consume little battery power as the main source of power, maintaining a simple and flexible protocol. As depicted in [6], two or more devices communication on the same physical channel constitute a wireless personal area network (WPAN).

3.3.1 Proposed Network Topologies

Depending on the application design, LR-WPANs can operate as two different topologies: *star topology* or the *peer-to-peer topology*. The last one is also known as *mesh* topology, given the ability of its end-nodes to build relationships with multiple neighbors without addressing the Personal Area Network (PAN) coordinator. Both types can be graphically analysed in Figure 3-3.

Peer-to-peer topology, as graphically analysed, is able to communicate with any other device as long as they are within an acceptable range. This also allows the formation of more complex networking infrastructures, such as wireless sensor networks, industrial control and monitoring.

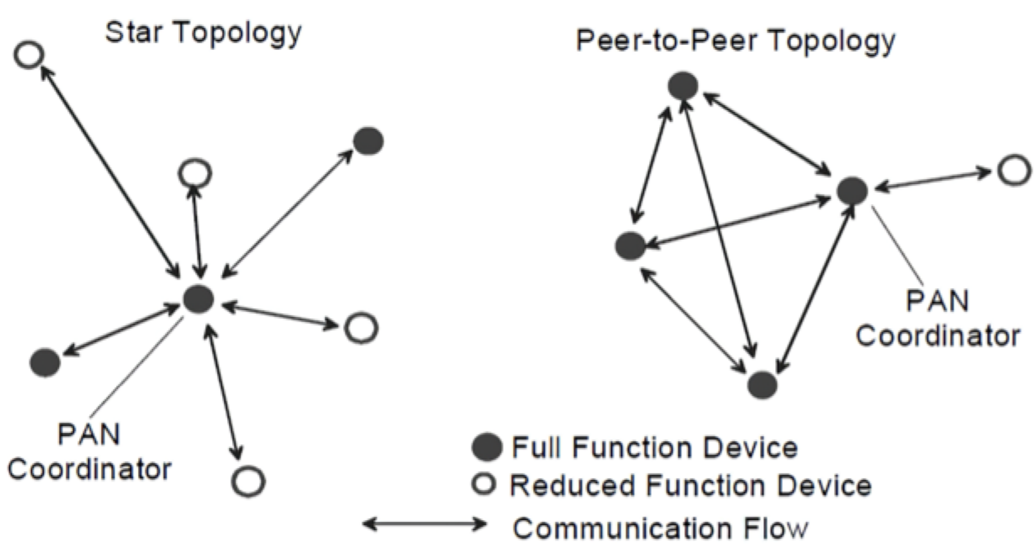

Figure 3-3: IEEE 802.15.4 proposed topologies [6]

.

This kind of networking configuration also allows multiple *hops* between nodes to route messages and ensure communication with the PAN coordinator, thus allowing more trustworthy connections, as no direct link between each node and the PAN coordinator is strictly needed. Nevertheless, it is important to consider that each one of the *hops* adds latency, which means that a compromise solution should be found between the maximum amount of allowed *hops* and the communication delays for data collection in a sensor *mesh* network infrastructure, for example.

3.3.2 Physical Layer (PHY) Specifications

As depicted before in section 3.1, layer 1 or physical handles the use if radio interfaces, thus being able to activate or deactivate the radio transceiver when needed. But also, it has other features such as measuring the amount of energy consumed in each data transfer operation, measuring the quality of the communication link thought measurements of receiving power and the channel selection within the desired communication frequency. Coexistence of IEEE 802.15.6 with other wireless standards is not considered in the scope of this work, but may be further analyzed as depicted in [30]. Frequencies available under the IEEE 802.15.4 standard are depicted in 3.2. Most important information is depicted as frequency bands being used in Europe, which are the 863MHz band and the 870MHz band. Each band is equally divided in *channels* with a fix width. For example, the European Band comprehended between 863MHz and 870MHz is divided in 35 communication channels when applied modulation is SUN [16] FSK under operating modes number #2 and #3, each one with a bandwidth equal to 200KHz. As channel width is reduced, more channels are available for communication, which increase the number of participants in a certain bandwidth, sharing the available frequency spectrum. Nevertheless, this also conditions the amount of data that can be transmitted. As a depicted example, channel spacing (in MHz), total amount of channels and the central frequency for each one of them are shown in Table 3.3 and Table 3.4. This frequency band has been chosen given its large application in the European area towards IoT developments. Normally, a data rate set as 50kbps is preferred, for 2-FSK modulation radio parameters [31].

Table 3.2: Frequency bands with geographic information, Europe is highlighted [6]
.

Band Designation	Frequency Band (MHz)	Country or Region
470 MHz	470 - 510	China
863 MHz	863 - 870	Europe
870 MHz	870 - 876	Europe
915 MHz	902 - 928	North America
915 MHz-a	902 - 928 (alternate)	North America and Mexico
915 MHz-d	915 - 921	Europe
920 MHz-a	920.5 - 924.5	China

Table 3.3: Channel numbering for SUN PHYs for the 863MHz Band [6] and [16]
.

Modulation	Channel Spacing (MHz)	Total Channels	Central Frequency
SUN FSK operating mode #1 and #1b	0.1	69	863.1
SUN FSK operating mode #2 and #3	0.2	35	863.1
SUN FSK operating mode #1a	0.05	137	863.1
SUN OFDM Option 4	0.2	35	863.1
SUN O-QPSK	0.2	35	863.1

Table 3.4: Channel numbering for SUN PHYs for the 870MHz Band [6] and [16]
.

Modulation	Channel Spacing (MHz)	Total Channels	Central Frequency
SUN FSK operating mode #1 and #1b	0.1	59	870.1
SUN FSK operating mode #2 and #3	0.2	30	870.2
SUN FSK operating mode #1a	0.05	117	870.1
SUN OFDM Option 4	0.2	30	870.2
SUN O-QPSK	0.2	30	870.2

3.3.3 Why Using Sub-1GHz Frequencies?

As it has been described before, the development of IEEE 802.15.4 standard focuses on low-power consumption devices, with acceptable bandwidth characteristics for the supported frequency bands, as depicted in Tables 3.2, 3.3 and 3.4. One interesting detail that should be highlighted is that mainly all support is done for frequencies which are below 1GHz. Although there are other proposals, like the use of Bluetooth Low Energy (BLE) for creating IoT networks like the one presented in Figure 3-4. BLE is specified for the ISM 2.4GHz band, with bandwidths that may reach up to 50 Mbit/s for Bluetooth version 5.2 developments in year 2020 [32]. Nevertheless, BLE applications are designed for IoT communication applied to narrow spaces and short distances, having an extremely good performance for little power consumption and excellent bandwidth [7].

As depicted in [33], for industrial and noisy environments applications, high levels of penetration constant and long range applications for low-power consumption devices are possible when using Sub-1GHZ frequency bands. Regarding *noisy* environments, these are not solely focused on industrial applications, given the fact that a smart city could also be considered as a challenge for reliable communication between end-nodes and LBRs. Being able to implement long range communications also improves the quality of the communication link, enhancing performance and reducing the amount of *hops* needed.

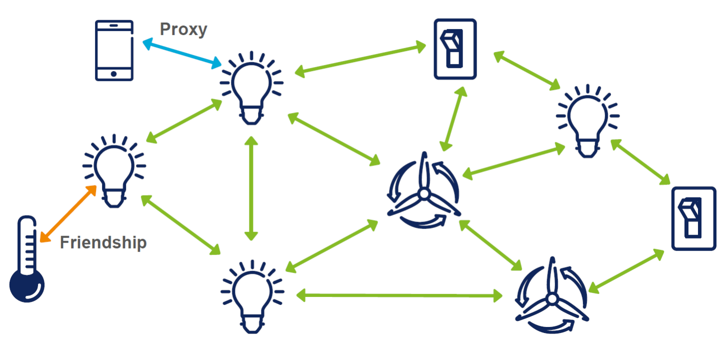

Figure 3-4: Example topology highlighting the friendship and proxy features [7]

.

3.4 LoRa® and LoRaWAN™: IoT's First Steps

As it can be extracted from 3-5, LoRa® was designed for long-time battery life sensor devices, which are designed for sending small amounts of data over long-range distances in noisy, challenging environments. Different from WiFi and BLE technology, which despite being globally accepted standards, they are only designed for short-range communication. On the other hand, traditional Machine-to-Machine (M2M) protocols over cellular network and GPRS infrastructure are designed for transmission of large amount of data but relying on mains power sources [8].

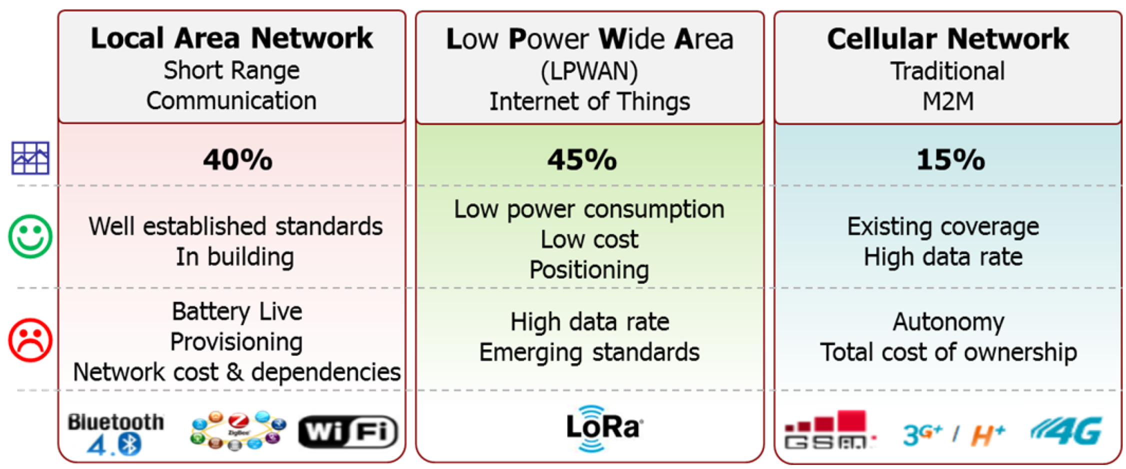

Figure 3-5: Differences between WiFi-BLE, LoRa® and cellular network [8]

.

LoRa® was designed to modify the PHY layer in order to achieve long-range communication with little power consumption. Considering that many designed systems use FSK modulation since its great efficiency regarding power consumption, LoRa was the first approach changing the rules of the game, thus proposing Chirp Spread Spectrum (CSS) in order to keep minimum power consumption, but enhancing communication range. On the other hand, LoRaWAN™ defines the communication protocol, up to the second layer from the OSI model, the MAC layer. One key difference that distinguish LoRaWAN™ is the *star*-topology network, depicted in 3-7, which can be achieved by having a large network composed of several LBR/DC instead of having only one DC device and several end-node devices.

This network configuration, compared with a *mesh*-topology network sacrifices range and radio-link redundancies but reduces the network complexity and increases battery lifetime as nodes are not receiving information from neighbor nodes. As carefully depicted in [8], a long star architecture makes the most sense for preserving battery lifetime when long-range connectivity can be achieved.

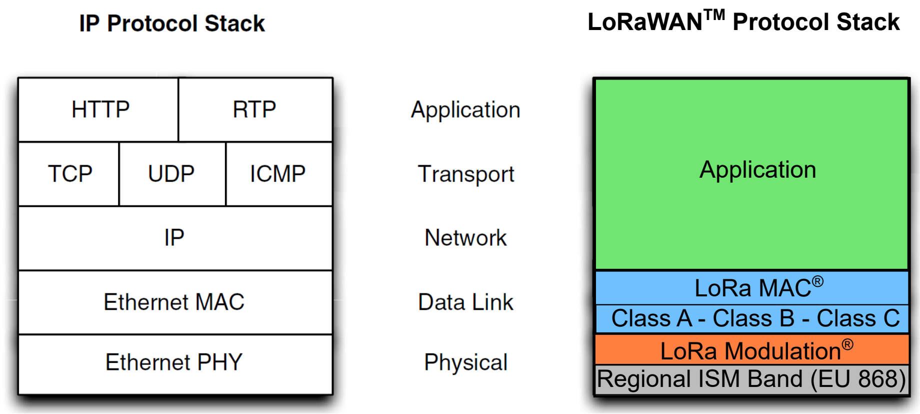

Figure 3-6: IP and LoRaWAN^{TM} protocols stack [8] and [5]

.

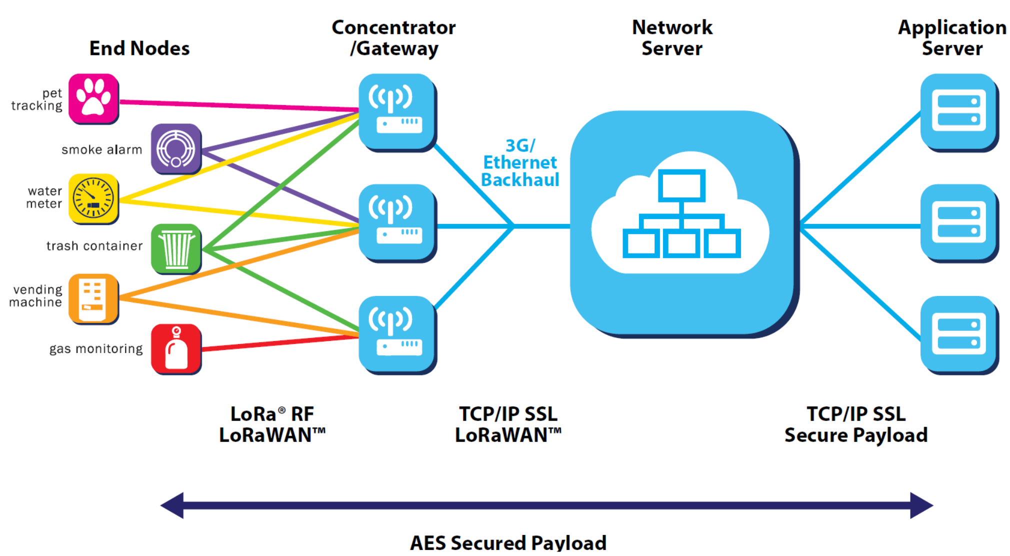

Figure 3-7: LoRaWAN^{TM} network structure proposed [8]

.

3.4.1 LoRaWAN™ for Europe: Parameters

LoRaWAN™ defines for Europe ten communication channels, with frequencies allocated in the Sub-1GHz band 867MHz-869MHz. A single FSK channel modulation is proposed at a data rate of 50kbps. Maximum power allowed is +14dbM or 25mW, specified by [34].

3.5 6LoWPAN: A new hope for IoT devices

IETF 6LoWPAN has been created to solve specific problems related with the large amount of resources needed to implement IP protocols on low-power constrained devices, as clearly explained in [21] and []:

- **Security Constrains:** For simple end-devices with limited processing capacities, IPv6 encryption methods defined as in [35] are too complex to be correctly processed.
- **Power Constrains:** As developed before, this is one of the most limiting constrains towards IoT in end-devices powered with batteries. Some devices allow working under *sleep mode* and reduced *duty cycle* operations. Nevertheless, traditionally IP devices were considered to be always connected, basically to mains power sources, grid direct connection or UPS sources.
- **Multicast Requirements:** As many IPv6 features substantially need the concept of *network flooding* with broadcast packets, IEEE 802.15.4 does not typically support this feature, as it is considered that broadcasting means having an inefficient use of power and bandwidth resources.
- **Mesh Network Topologies:** Multi-hop mesh infrastructures may be translated as more power consumption, as depicted before in section 3.4. Nevertheless, embedded radio technology for standalone operation could make use of the advantages of mesh networks, as a compromise solution between reaching the expected range and reducing cost.

- **Bandwidth and Frame Size:** IEEE 802.15.4 frames support a maximum size of 127 bytes, with OSI Model - Layer 2 payloads as low as 72 bytes. Since the minimum MTU of IPv6 protocol is 1280 bytes [36], part of the 6LoWPAN protocol is to provide data fragmentation, or reassembly mechanisms. In case one of the fragments get lost given the probability from LLNs networks, then the whole information has to be re-transmitted, therefore lowering the efficiency.

- **Reliability:** IP standard protocols are nor designed for LLNs, nor for noisy environments. Just to mention, the TCP protocol cannot differentiate between packets denied because of network congestion, or packets lost due to interference or low-quality communication links. 6LoWPAN makes use of UDP transport protocol specification, avoiding *handshakes* mechanisms, thus reducing the bandwidth requirements.

New features of IETF 6LoWPAN consider a simpler header structure and a hierarchical addressing mode, thus implementing a *lightweight* IPv6 version on IoT constrained end-devices. Another milestone development is the design of a Neighbor Discovery (ND) version specifically applied in 6LoWPAN, in order to develop low-power mesh-topology networks. Ideals of 6LoWPAN uses can be described as follows, based on [21]:

- **End-Devices:** Embedded, stand-alone end-devices which need to communicate between themselves and with Internet-based services (*cloud* storing for example). Network structure is depicted in Figure 3-8 and its network stack is presented in Figure 3-9.

- **Low-Power Consumption:** As devices are battery-powered, energy consumption must be minimal compared with Internet devices which are mains powered.

- **Flexible Network:** The proposed infrastructure must be open, easy to evolve and provide access to new standalone end-devices who wants to be part of it. The fact that the network is flexible, it also means it can be scaled under mobility issues, for example, E-Mobility or Smart Lighting applications.

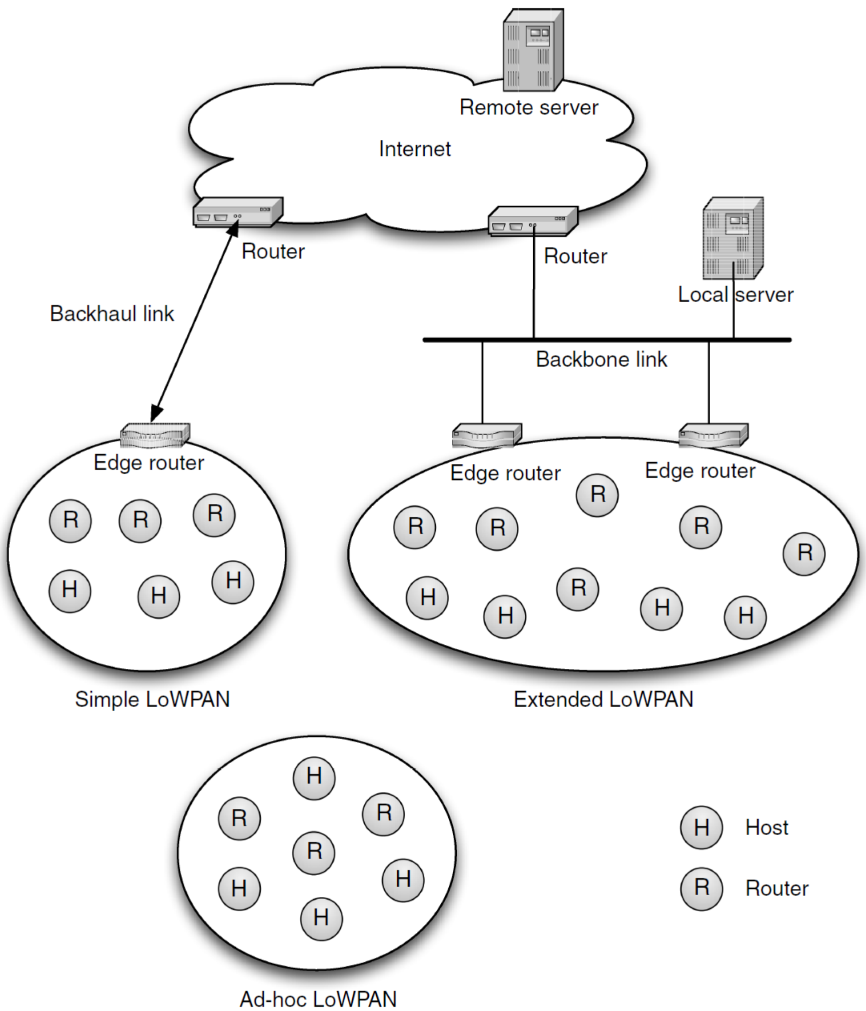

Figure 3-8: 6LoWPAN architecture [5]

.

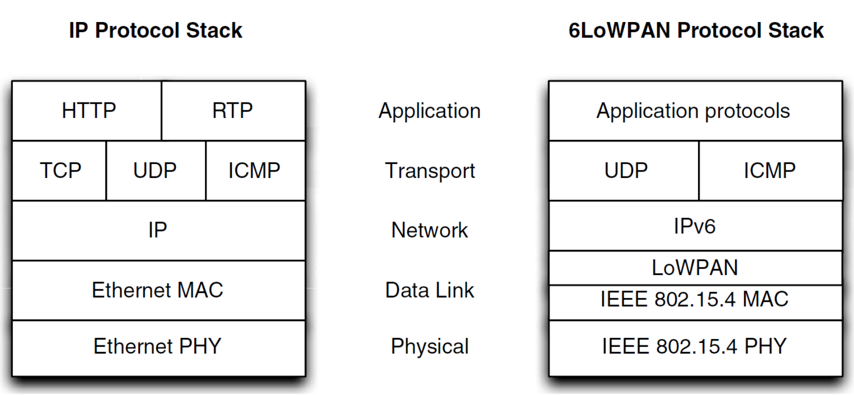

Figure 3-9: IP and 6LoWPAN protocols stack [5]

.

3.6 Routing Protocol for LLNs

A routing protocol describes how routers establish communication with each other, exchanging information that will allow them to select proper routes between any end-devices in a structured network. The algorithm will determine the routes that are going to be used. Knowing that each router knows only the networks directly *attached* to it, the routing protocol will share information firstly with its direct *neighbours*, and later propagate this information alongside the network [4]. Each IP datagram has two main components: *header* and *payload*. While the *header* contains enough information to be routed from source to end without relying on prior exchanges between two end-devices, the *payload* contains the data that needs to be transported. This process also receives the name of data *encapsulation*.

Routing protocol for low-power and lossy networks, also known as RPL, is described in RFC 6550 [37]. This routing protocol is based on *distance vectors* [9], based on routing metrics and building constrains imposed when configuring the network. As explained in 2.4 and in [37], Low-Power and Lossy Networks are characterized by high loss rates, low data rates, reduced bandwidth and communication links instability. Therefore, supported traffic flows should not only be from point-to-point, but also point-to-multipoint and vice-versa, allowing broadcasting and network flooding mechanisms.

3.6.1 Routes Formation

Formation of routes in RPL routing protocol are explained based on the information from [37], based on the *Distributed Algorithm Operation*. Radio networks, and therefore LLNs networks, do not have predefined topologies, as in a wired-connection network topology. RPL protocol has to discover the radio links available, and then choosing the best route accordingly. The routing protocol organizes the topology as a Directed Acyclic Graph (DAG), partitioned into one or more Destination Oriented DAGs (DODAGs), having one DODAG per sink or LBR/DC. Figure 3-10 depicts the formation of a network by RPL routing protocol, simulated in Cooja.

As a LBR/DC is configured to be a DODAG root, it advertises its presence, routing costs and related metrics by sending a multicast (broadcasting) DIO (DODAG Information Object) message to all RPL configured end-devices. Each node then listen for DIO messages and use the metric cost information to join a new DODAG root or maintaining the existing DODAG. By joining the network, each node provides routing tables entries, being promoted or degraded based on metric costs.

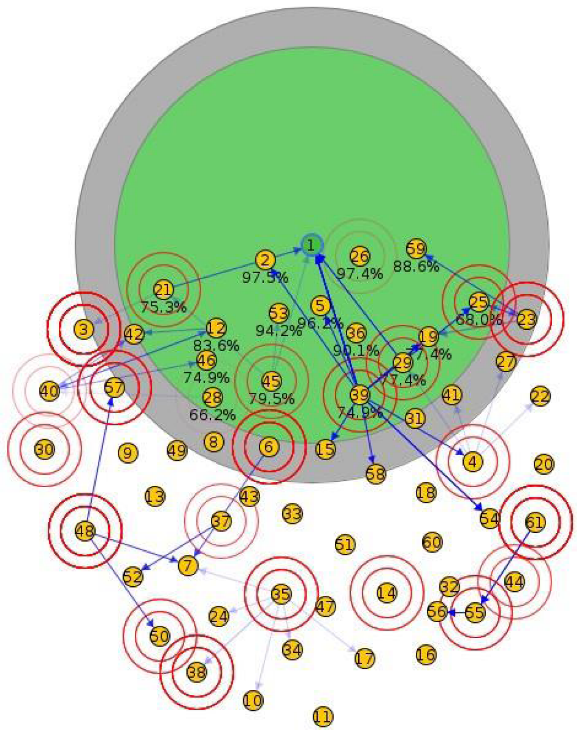

Figure 3-10: RPL random topology [9]

.

Destination Advertisement Objects (DAOs) messages are being used by RPL in order to establish downward routes. The rank of each node or end-device is a scalar representation of its own location within a DODAG. Constrains in order to calculate the right rank for each node is out of the scope of this work, and can be later analyzed in [37]. Nevertheless, it is important to mention that the rank does not represent the path cost, although the determination of a certain rank is deeply influenced by its metric costs. Next sections 4 will focus more on the hardware characteristics, analyzing candidate end-devices for energy measurement and smart lighting applications.

Chapter 4

IoT Devices: From Smart Meters to Lighting Sensors

As developed in previous sections and after reviewing the associated literature in 2, it came to a clear realisation that the amount of end-devices that can be interconnected in Internet applications are unimaginable. As correctly depicted in 1.3, IoT encompasses all devices and networks natively IP-enabled and Internet connected. The scope of this work is based on energy metering applications, using devices such as *smart meters*. Nevertheless, following the latest developments done by the City of Gijón regarding smart lighting reconfiguration using IEEE 802.15.4 and 6LoWPAN protocols [20], it is worth mentioning some characteristics regarding these kind of devices as well.

4.1 Smart Meters Technology

This specific part focuses on the analysis of different smart meters already available in the market. The main target is to analyse advantages and disadvantages of each one of them, exposing some basic characteristics such as connectivity, ease-of-use, basic features, types of variables that can be processed, among others. In the edge of the revolution of energy market, smart meters are becoming one of the key role players, shaping the new applications in interaction with web services and IoT technologies.

These kind of devices are not only able to measure and keep track of the electrical energy consumption, but also transmit this kind of information towards users and electricity companies, becoming a powerful device which should combine the amount of information they handle with real-time communication interfaces. Smart meters can be classified according to parameters such as the communication protocols used, voltage limitations or number of parameters that can be measured per sampling period. Different manufacturers and models can be considered, finding the ones that are more suitable for low-voltage distribution networks, with multiple prosumers and EV charging systems. Most of the compared devices are based on Phoenix Contact product catalog

4.1.1 Physical Communication Protocols

The main target is to analyze which are the different protocols used by smart meters, available in the market. An adaptation for wireless *mesh*-topology networks must be done, basically because there are no proof of smart meter hardware that can sustain IPv6 communication protocols over PLC or Low-Power, Lossy Networks (6LoPLC-6LoWPAN).

1. **Modbus Protocol:** Modbus is a serial protocol originally used in PLCs. Nowadays, it is widely used for connecting industrial electronic devices. Being open-source, Modbus has become a popular protocol among industrial environments, using serial RS485 as the physical layer. As it has been designed to be used with PLCs dating back to the end of the 70s', this protocol shows some limitations. One for example is the fact that large binary objects are not supported. Regarding cybersecurity, the protocol itself does not provide additional security against unauthorized commands or data interception, which can have large implications when it comes to ensure the safeness of data transmission and consumers' privacy.The protocol itself suffered several adaptations throughout its application in the industry. Most used varieties of the Modbus protocol can be shown, related with the communication adaptations done by Phoenix Contact.

- **Modbus RTU:** Mainly used in serial communication, uses a compact, binary representation of the data. It follows the commands with a cyclic redundancy check to ensure faultless data transmission. Messages are framed and separated by idle periods. No need for switch in a *star-topology* network, as one of the devices acts as a Gateway.

- **Modbus ASCII:** Used in serial communication, makes use of ASCII characters for protocol communication. ASCII messages are framed by a leading colon (:) and trailing newline (carrier return CR/LF).

- **Modbus TCP/IP:** Variant used for communications over TCP/IP networks, over port 502. Specifically, it is used for providing Ethernet connection to PLCs modules and smart meters. Does not require checksum, since lower layers already provide it.

- **PROFINET BUS:** Proprietary protocol from Phoenix Contact. Allows combination with Representational State Transfer (REST) and Application Programming Interface (API).

4.1.2 Phoenix Contact EMpro Product Line

As one of the leaders for the application of IoT technologies in the industry oriented to monitoring the quality of power installations, Phoenix Contact launches its EMpro product line [10], providing multi-function energy meter devices, already designed to be integrated into an specific network within minutes and in a flexible way. They provide historical recording error list for mandatory continuous energy monitoring in non-stoppable industrial activities. Under the premise that a reliable power supply is the key function for interruption-free operation of plants, idea is to build a network with trustworthy devices which allow industries to keep focus on main industries activities, automatizing the power quality measurement process. The company based in Blomberg, Germany, aims for an IoT based energy market, focusing on the future-oriented, upcoming energy market.

4.1.3 Industrial Energy Measurement with EMpro Devices

Versatility of smart meters allows several configurations, which can be applied for industrial environments as needed. Current measurements can be done using current transformers with a range up to 20.000A, or with Rogowski Coils with a maximum measurement range of 4.000A. The main difference lies in current transformers being recommended for new designs, because its bulky installation and the fact that de-energizing the installation is needed. On the other hand, Rogowski Coils are easier to install but need additional equipment, such as current-voltage transducers, before being able to extract the required data. Scheme is presented in Figure 4-1, where the Rogowski Coils and the voltage transducers are shown. It is important to mention the Ethernet connection between the smart meter and the PC device. This means, EMpro smart meters are already configured for providing Ethernet connection for monitoring applications, which can be an advantage when compared with other devices, which do not offer multiple communication protocols.

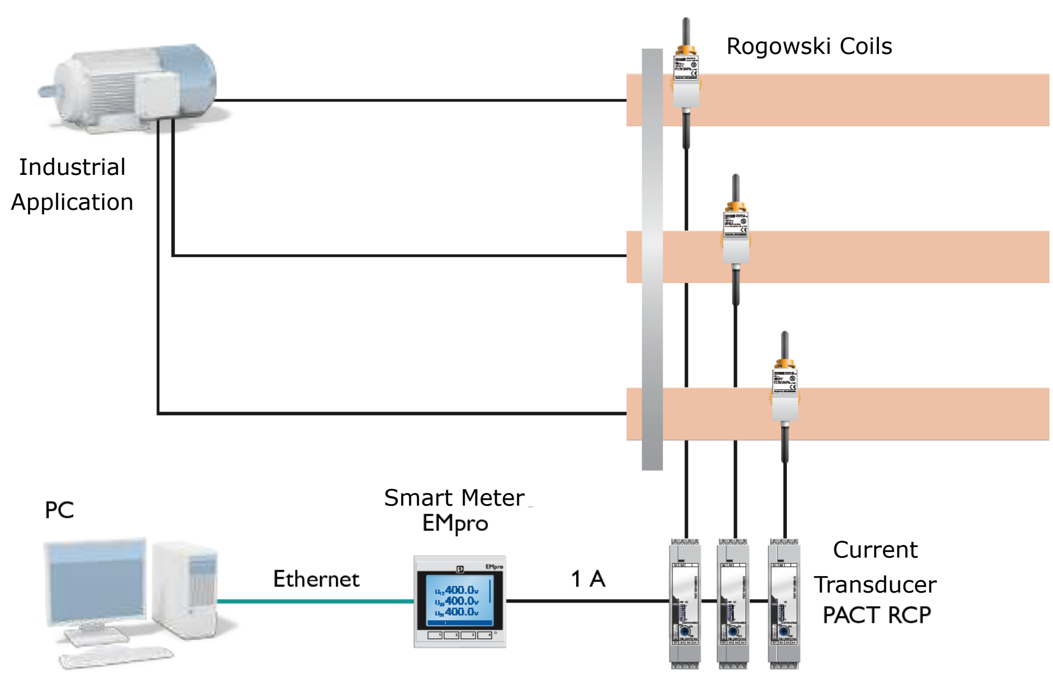

Figure 4-1: Using Rogowski Coils for indirect current measurements [10]

.

4.1.4 Modbus with REST/API Passive Network

Application case shown in Figure 4-2 presents the combination of an Ethernet network interface between the switch device and the energy monitoring and storage end-device. Modbus protocol, together with REST/API protocols is used for configuring the smart meter devices and data acquisition. Nevertheless, the use of REST/API commands is only destined for data acquisition and cannot control loads attached to each one of the smart meter devices, thus this configuration is designed as a *passive* application. Scheme presented can be useful for industrial applications acting as a monitoring infrastructure, offering logs entries for failures and determine the *health* status of the overall network. As depicted before, a healthy and reliable power supply is a key parameter for interruption-free operation of industrial applications.

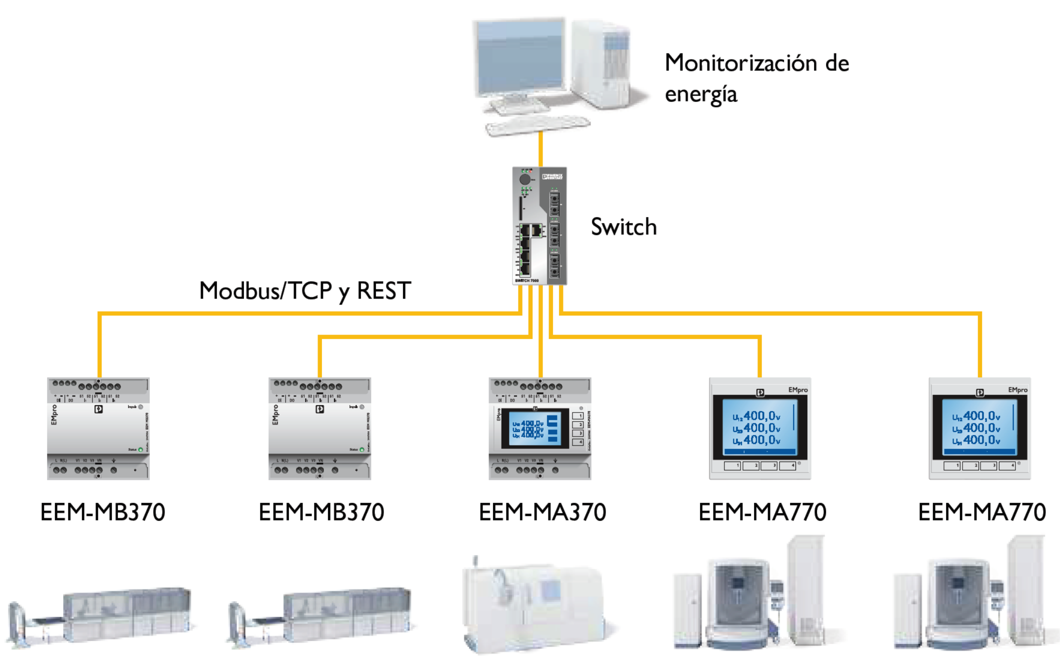

Figure 4-2: Energy monitoring on an Ethernet network using Modbus/TCP [10]

.

4.1.5 PROFINET BUS and PLC Interfacing

Application case shown in Figure 4-3 presents the use of a PROFINET BUS network. PROFINET BUS allows to easily configure the connection between energy smart meters and Programmable Logic Controllers (PLCs), which allows the ease of connecting and disconnecting loads at will, thus not only having a *passive* measuring network, but also a fully-controlled energy infrastructure. Moreover, PROFINET BUS is based on Ethernet as its communication layer. Compared with 4-2, PROFINET BUS allows devices to communicate with each other, different from the point-to-point communication proposed with Modbus. Nevertheless, the main disadvantage is the reliability on the PLC device, being this end-device the gateway for data acquisition, acting as a gateway between the AMI network and the DC. The lack of redundancy in the proposed scheme may be solved by considering additional communication interfaces, such as Modbus/TCP with REST-API protocols as the data transport infrastructure.

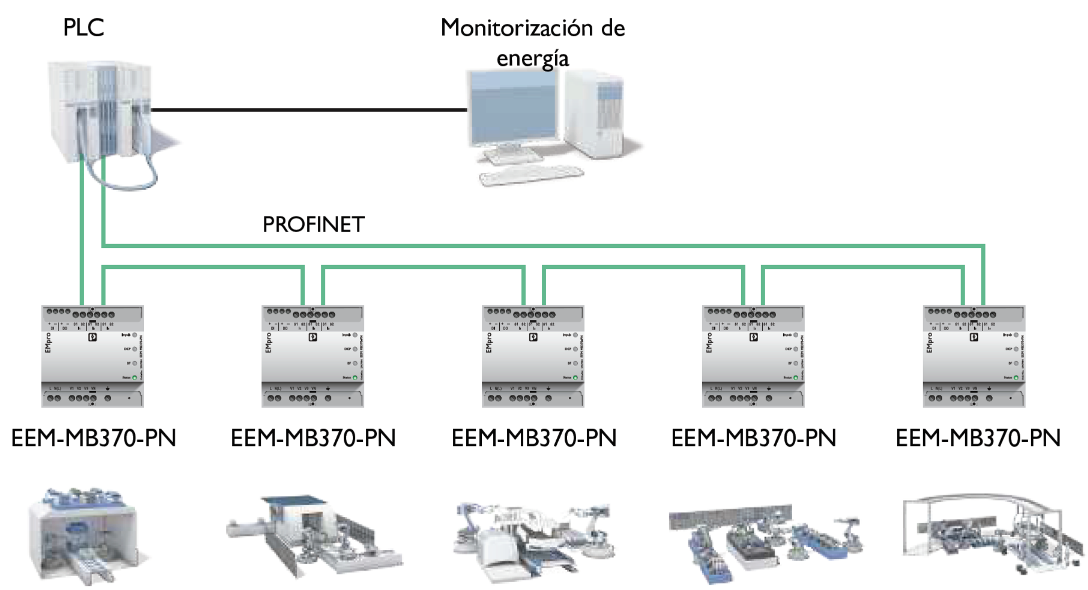

Figure 4-3: Energy monitoring on a PROFINET BUS network [10]

.

4.1.6 Modbus/TCP and PROFINET BUS Active Network

Application case shown in Figure 4-4 presents the combination between a Modbus/TCP or REST-API network and a PROFINET BUS network. Could be considered as one of the best solutions for load shedding and consumption control by using PLC applications, but also not depending solely on the PLC as a gateway device, thus enhancing the redundancy of the network against link failures. The Modbus infrastructure is proposed as the framework for data transport infrastructure, while the PROFINET BUS interface provides connection with the PLC for industrial applications. A SCADA control network could be also implemented, thus providing an interesting Graphic User Interface for data acquisition and processing. Ii is also important to notice that smart meters technology is not a restriction for interconnection. As long as the Modbus/PROFINET BUS interfaces are supported, smart meters can be as complex as the task they require to perform.

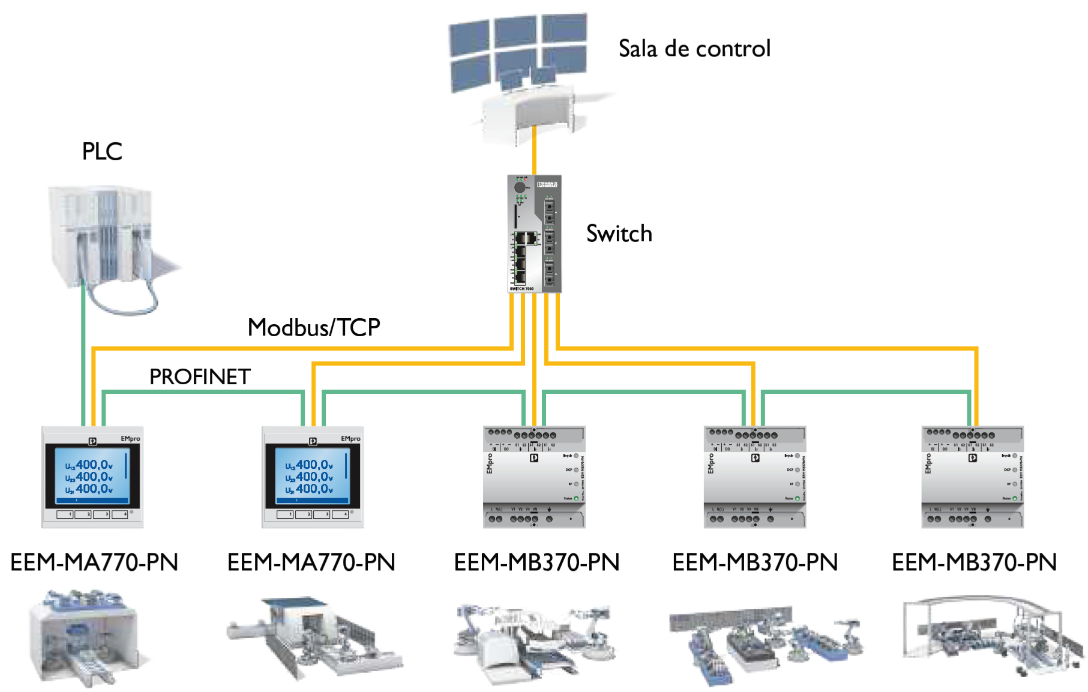

Figure 4-4: Monitoring on a Modbus/TCP with a PROFINET BUS network [10]

.

4.1.7 Ethernet and Proficloud Infrastructure

Application case shown in Figure 4-5 presents the use of MQ Telemetry Transport (MQTT) messaging protocol on Ethernet networks. Direct control over industrial loads is not strictly specified, so it is considered as a *passive* monitoring system. Nevertheless, main advantages consist on the possibility of using the Proficloud application for data storage and later processing, through HTTP request to the cloud server. Nevertheless, a physical wired structure is still needed, which implies the proximity between devices and lacks of the wireless advantages and a *mesh*-topology network infrastructure, as depicted before in section 3. Despite this, this infrastructure is useful to be considered in short-range applications, for example PEV charging stations in a cluster, or a residential building where measurement devices can be connected one after the other in a structured framework. Further analysis of this application case is made in 5.3.

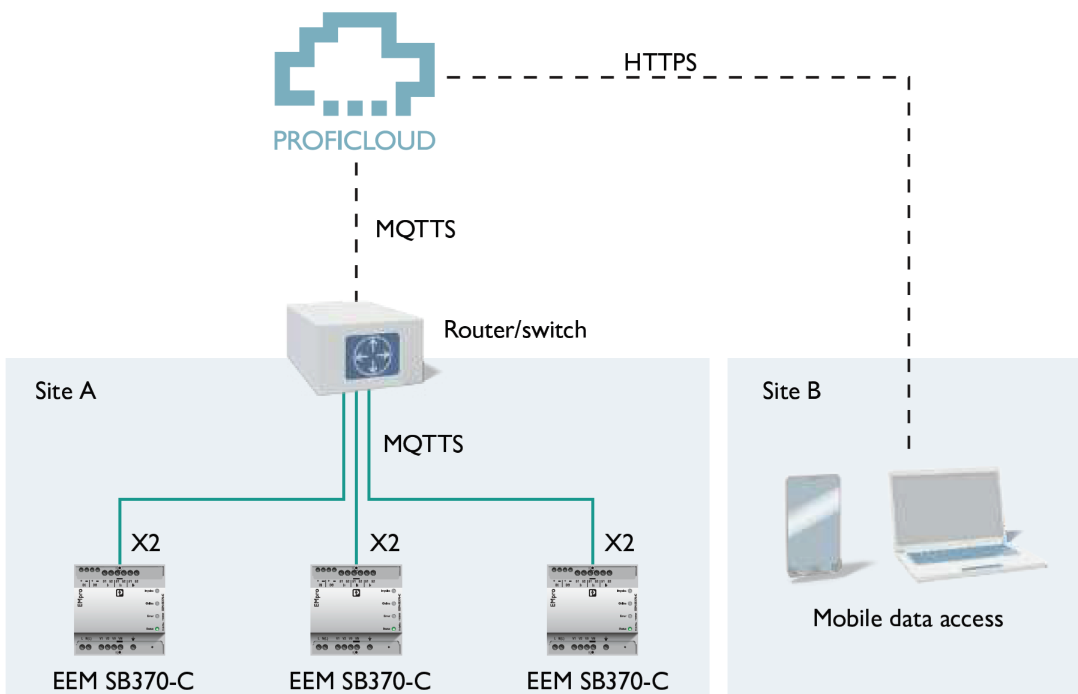

Figure 4-5: Using Ethernet and PROFICLOUD for data storing/processing [10]

.

Chapter 5

Project Implementation: From Excitement to Reality

After careful consideration, and based on the literary review done in section 2, analyzing communication protocols in section 3 and reviewing the hardware configurations as depicted in section 4, the following guidelines have been taken for a practical implementation of an advance metering infrastructure for smart grid real time energy management:

1. **Network structure:** Wireless network approach is proposed, given that the main goal of the project does not rely on the positioning of smart devices in a defined network. Moreover, wireless radio communication allows having a more flexible overall system, with more degrees of freedom.

2. **IoT topology:** *Mesh*-topology network is preferred over traditional *star*-topology networks, given the enhanced reliability of communication links, flexibility and ability of new nodes to easily join the network. Moreover, *mesh*-topology networks enhance range with little investments, given the fact that distributed LR with constrained processing characteristics are much more beneficial from the economics point of view, compared with distributed LBR/DC. Development launchpads working with Sub-1GHz frequencies are being used for the network building, aiming to implement IPv6 characteristics.

3. **Communication protocol:** As AMI is based on end-devices with enhanced capacities towards IoT connectivity, logically the first choice is to use IEEE 802.15.4 standard, moreover considering that application is done in noisy environments, where low-power, lossy networks are preponderant by default. Secondly, given that implementation is made with *mesh*-topology networks, 6LoWPAN is preferred over LoRa® and LoRaWAN™ applications.

End-devices in a mesh network have less processing abilities but also they are much cheaper than implementing a dedicated network of gateways in order to ensure a star-topology network. **This is the main advantage of 6LoWPAN standard over LoRa® and LoRaWAN™ solutions.** Although there are many example projects which took the risk and develop their own smart meters with grid-sensing devices, enhancing them with multiple-protocols gateways working in 6LoWPAN and IEEE.802.15.4 [12] [17], given time constrains this thesis takes a more *conservative* approach, based on the use of market available smart meters with serial RS232-RS435 interfaces, enhancing their communications properties by attaching network-capable development launchpads working with Sub-1GHz frequencies, and interfacing them with multi-protocol gateways for data up-links. As depicted in [17], sampling voltage using an interval of 10 seconds should be completely enough for diagnosing power quality disturbances, such as voltage deviations. Making a group of several smart meters in the same building could be considered as having an unique virtual smart meter behaviour. In case of an event in quality drop, higher sampling rates may be used for addressing the problem correctly and isolating it from the whole network.

5.1 Forming a *mesh*-topology network

As described previously in section 3.3, *mesh* networks are build around peer-to-peer networks. Based on the description given by the IEEE 802.15.4 standard [6], in a peer-to-peer network, one device is classified as the PAN coordinator, which is generally the LBR/DC device. After this, the network structure is constructed out of the peer-to-peer topology.

For a peer-to-peer network formation, the cluster tree example is being used. This is a special type of network, where all the devices are depicted as Full-Function Devices, or FFDs. As in a tree structure, there are also end-nodes that may be considered as *leaf devices*, since they do not allow other devices to associate with them. These type of end-devices are also called Reduce-Function Devices, or RFD. Which also means that any FFD device could start creating a network infrastructure, given the fact that it allows any other type of device to be associated to itself. Nevertheless, it is preferred for the LBR/DC to act as the PAN coordinator, given the fact that its computational and memory resources are larger, compared with LR acting as end-nodes. The first cluster is formed by chasing an unused PAN ID and broadcasting in order to detect and connect neighbor devices (also known as *neighbor discovery*). Once a device is detected at a reachable range, it can request to join the network. If accepted, the PAN coordinator is registered as the *parent* in the end-device's neighbor list, as the node starts to transmit periodic *beacons*, in order for other devices to join the network at that device.

5.2 Network Infrastructure Proposal

As it can be depicted from Figure 5-1, each single end-device enhances its network capabilities by attaching a Texas Instruments CC1310 Launchpad [11]. This communication board enables the application of an IPv6 over Low-Power and Lossy Networks infrastructure, or simply known as 6LoWPAN framework. Communication between the smart meter and the launchpad, which acts in fact as the Local Router (LR) is done by using RS232 or RS435 serial connections.

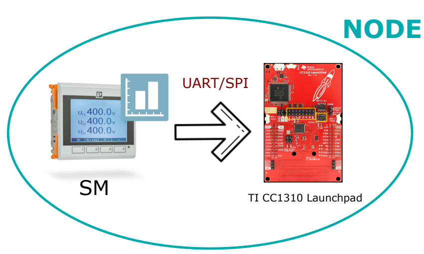

Figure 5-1: Node structure based on IPv6 6LoWPAN wireless connection.

The smallest unit that can be considered for building the network, which is basically the interfacing of a smart meter and a 6LoWPAN communication board is defined as a *node*. Therefore, the main idea is to create several nodes interfacing end-devices and LRs, and then start building a network from scratch. As presented in Figure 5-2, each node is able to intercommunicate with others, implementing the desired *mesh*-topology network. Moreover, each node is able to interface with a LBR/DC, with enhanced processing capabilities and which is able to interface with other long-range, large-bandwidth communication protocols for data up-link towards storing servers or cloud applications.

The proposed topology is made for long-range communication and considering application in industrial environments, normally overwhelmed by LLNs. Nevertheless, the scope of this thesis does not take into consideration the economic viability of the applied solution. Market price for an end-node 6LoWPAN-enhanced communication device, like the proposed TI CC1310, rounds €25.00 (taxes included) [38] without considering the final price of the smart meter end-device. Considering industrial applications, where communication devices are not only being used as end-nodes, but also as routing LR devices as depicted in section 2.4, amount of devices needed for a commercial-project implementation has to be compared with the expected costs.

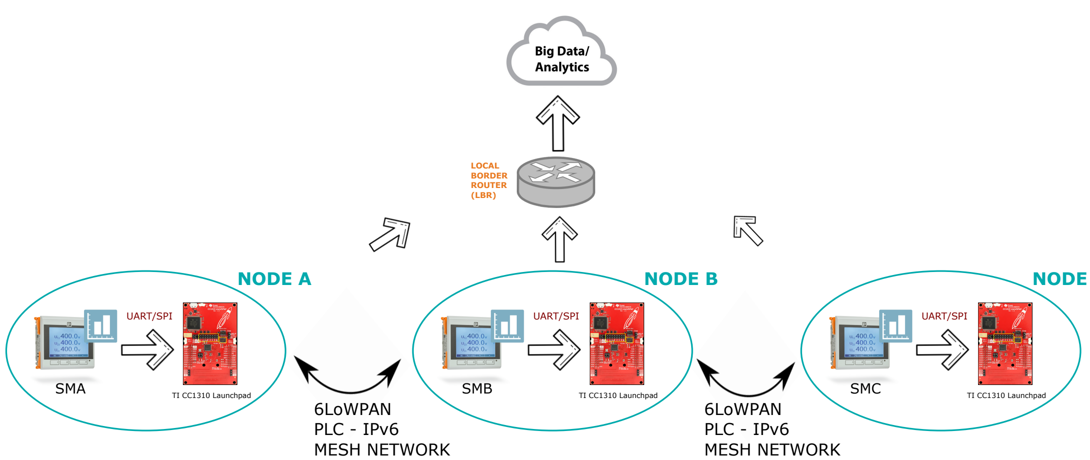

Figure 5-2: Long-range network structure based on IPv6 6LoWPAN network.

5.3 Buildings Energy Management

If it is possible to propose an scenario, where grid measurement devices are next to each other in a sort of structure distribution, then it is possible to reduce the costs by redefining the concept of *node* and using other type of communication interfaces to interconnect a small group of smart meter devices. For example, Figure 5-3 depicts this idea, while the distribution shown in Figure 5-4 represents the idea of using 6LoWPAN only focused on building a *mesh*-topology network between *nodes*. The conception of *node* starts to be a cluster of devices, instead of defining each end-device as a *node*. Routing protocols and data exchange between LR and LBR/DC is not substantially changed, which demonstrates that the network itself is flexible and easy to configure.

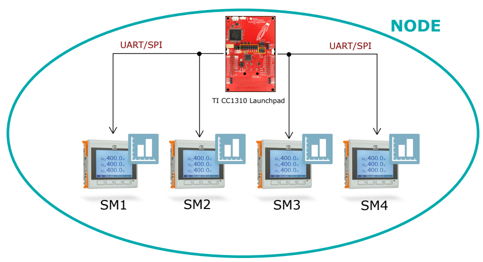

Figure 5-3: Node structure based on UART/SPI serial connection.

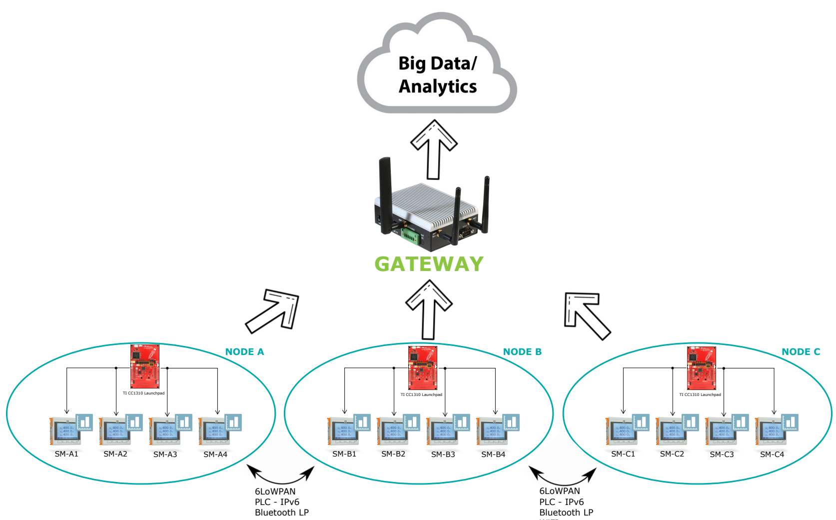

Figure 5-4: Long-range network structure based on UART/SPI serial connection.

Similar idea is presented in Figure 5-5 and its network implementation depicted in

Figure 5-6. The conception of *node* is similar to the previous definition, as a cluster of end-devices. Nevertheless, this also shows that communication protocols are not only limited to serial connections. Ethernet based protocols, and even more Profinet Bus application possibilities can be also explored in detail, as depicted in section 4.1. Nevertheless, this implies the use of additional hardware for OSI Model Layers 1 and 2, in essence, a switch device for each *node* structure, increasing the costs.

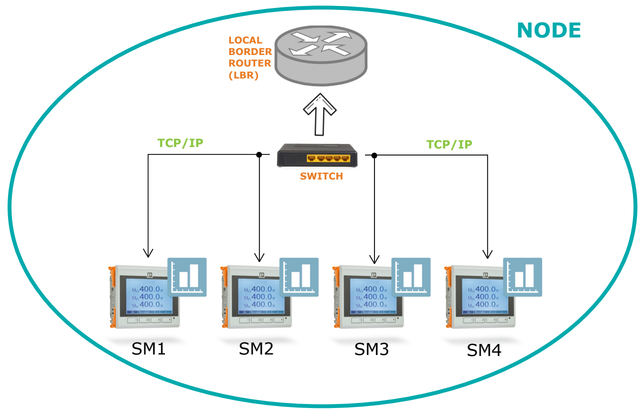

Figure 5-5: Node structure based on TCP/IP serial connection.

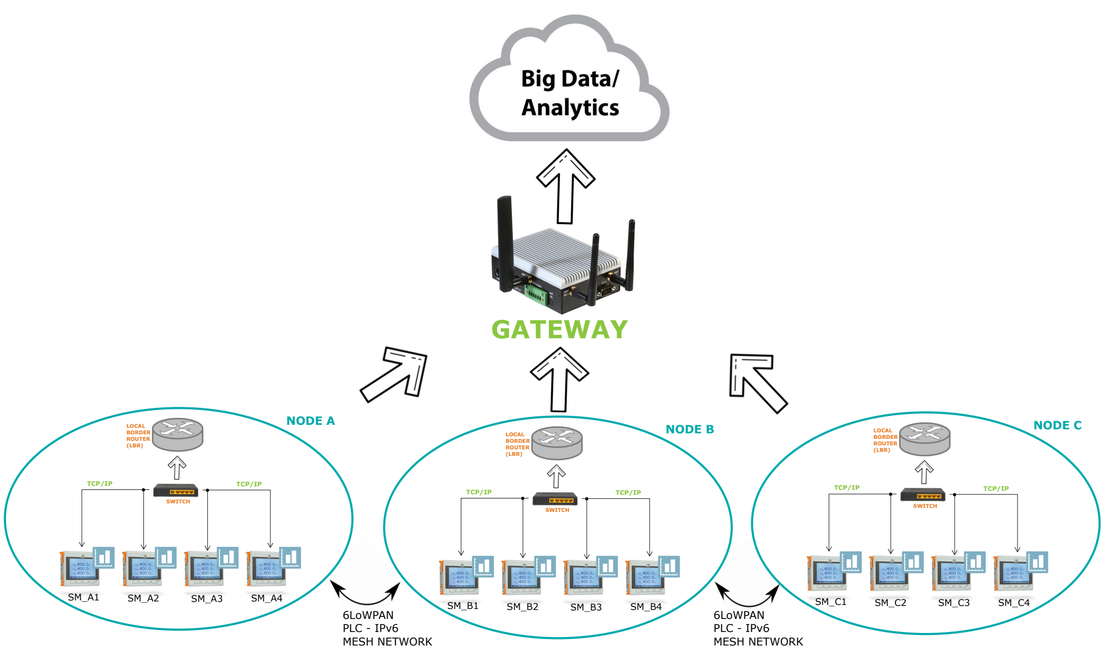

Figure 5-6: Long-range network structure based on TCP/IP serial connection.

5.4 Hardware Implementation and Results

After proposing the network structure in section 5.2, hardware application of a real system is implemented using four TI CC1310 Launchpads and a TI MSP430 Module for memory and processing resources enhancement. An extra LBR/DC has been placed, provided by Seneco, in order to debug the network implementation acting as a DAG/DODAG PAN coordinator. This device is also used for the Gijón DemoLAB initiative [20]. The configuration as shown in Figure 5-7 can be depicted as follows:

- **Local Routers (x2):** Two CC1310 are configured as **UDP-Clients** or LRs, which means that are the ones that provide the 6LoWPAN communication interface for the smart meters end-devices. Configured IPv6 addresses are **FD00::212:4B00:12CD:BEF8** and **FD00::212:4B00:12CD:C21D** respectively.

- **Local Border Router/Data Concentrator:** One CC1310 in series connection with a MSP430 is configured as a **UDP-Server** or LBR/DC, which means that are the ones that provide the 6LoWPAN communication interface between the *mesh*-topology network and the Internet, using a tunslip6 interface with Linux on a PC. Configured IPv6 address is **FD00::212:4B00:12CD:C062**.

- **Sniffer/Wireshark Interface:** The last CC1310 (from left to right) is configured as a 6LoWPAN, multiple channel **packet sniffer**, which means it can intercept IPv6 packets in order to monitor the communication performance. Interfacing with Wireshark, it can dissect communication packets and analyze protocols that are being used.

- **Seneco LBR/DC:** Interfaces with the network in order to provide the network with an already configured end-device, acting as a DAG/DODAG PAN coordinator. Configured IPv6 address is **FE80::212:4B00:12CD:C062**. This LBR/DC is used for debugging applications, sniffer appropriated configuration and network parameters implementation.

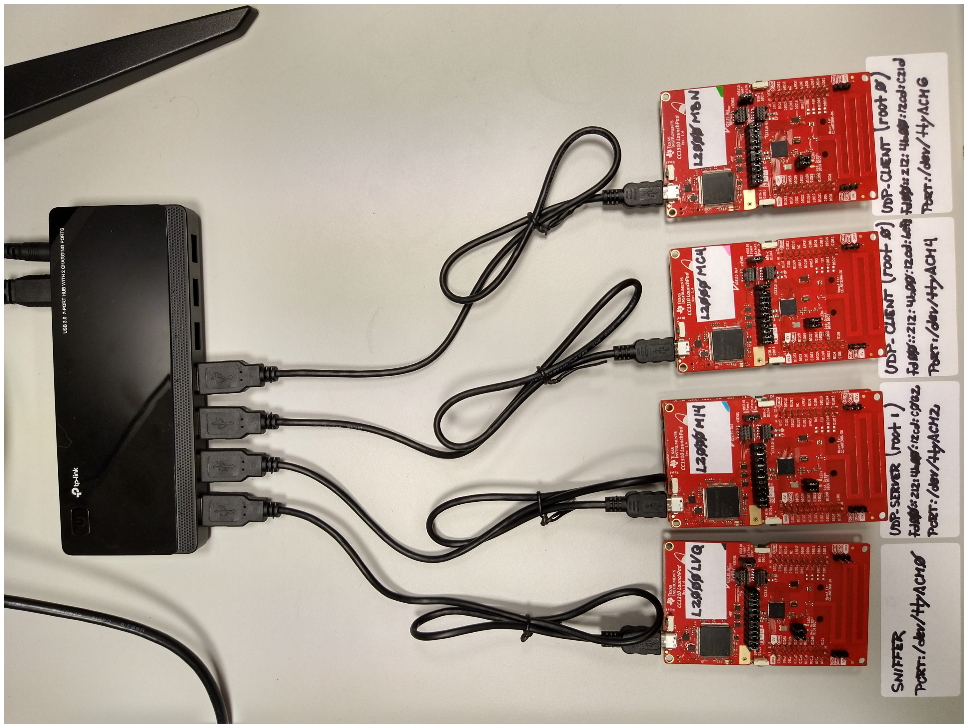

Figure 5-7: Hardware configuration with two UDP Clients and one UDP Server.

Figure 5-8: ZIV 5CTD-E2F smart meters, provided by EDP energy company.

Simulations done using the Cooja simulation environment from the Contiki-Ng programming suite shows the deployment for an UDP server, LBR/DC structure, and a UDP client are shown in Figure 5-9 and 5-10. Simulation environment demonstrates the successful deployment of a 6LoWPAN RPL network prior its physical implementation. Also, the deployment of an HTTP web server, embedded in the LBR/DC can be simulated using Cooja environment.

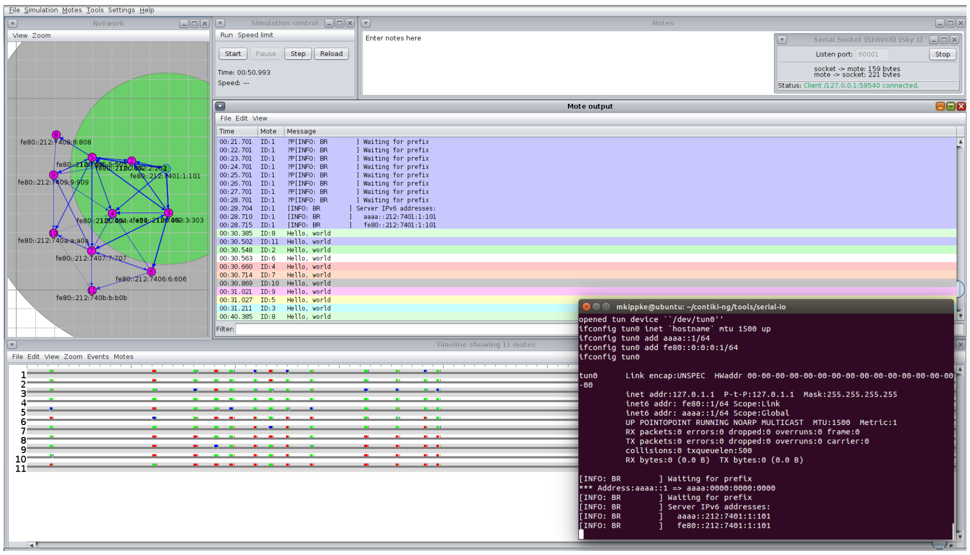

Figure 5-9: IPv6 network configuration using Cooja Simulator.

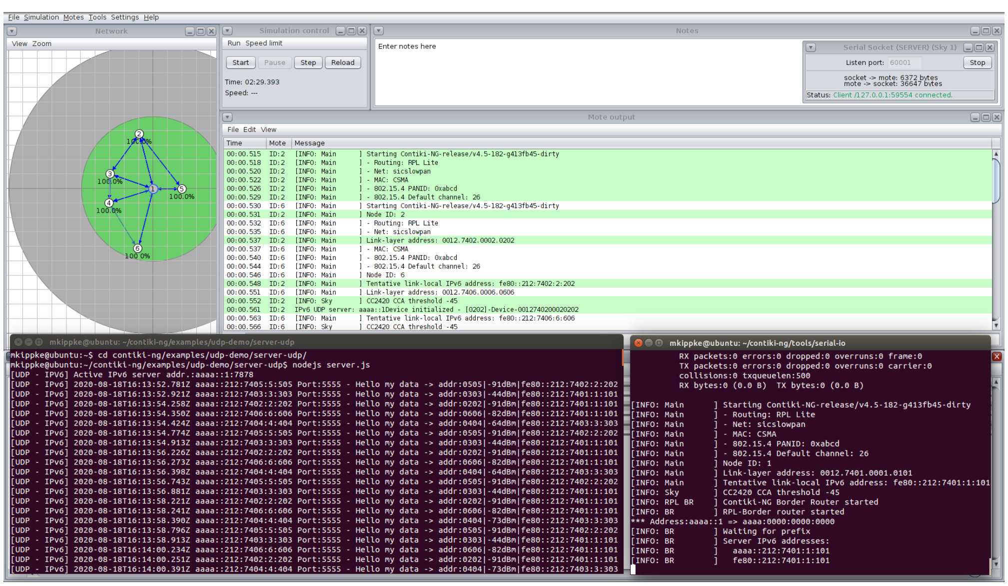

Figure 5-10: UDP server on the loop using Cooja Simulator.

Due to time constrains, it was not possible to implement testing on a real smart meter device interfacing with a Texas CC1310 Launchpad using a RS232 -RS435, as intended. Instead, the 6LoWPAN network was simulated and implemented, and the intended smart meters to be used for future applications are shown in Figure 5-8. Smart meters were provided by EDP energy company and correspond to version ZIV 5CTD-E2F smart meters for grid applications. Results shown are presented for *mesh*-topology network construction. Programming has been done using the Contiki-Ng development environment on a Linux 32-bits virtualization. Figure 5-11 shows the available ports for programming and data reading. Each one of the deployed TI CC1310 has two different `\dev\ttyACM` ports, one for the debugging interface and the other for the CC1310 micro-controller unit. Therefore, devices labeling is done as follows, from left to right following Figure 5-7:

- **Local Routers (x2):** `\dev\ttyACM6` and `\dev\ttyACM4` respectively.
- **Local Border Router/Data Concentrator:** `\dev\ttyACM2`.
- **Sniffer/Wireshark Interface:** `\dev\ttyACM0`.

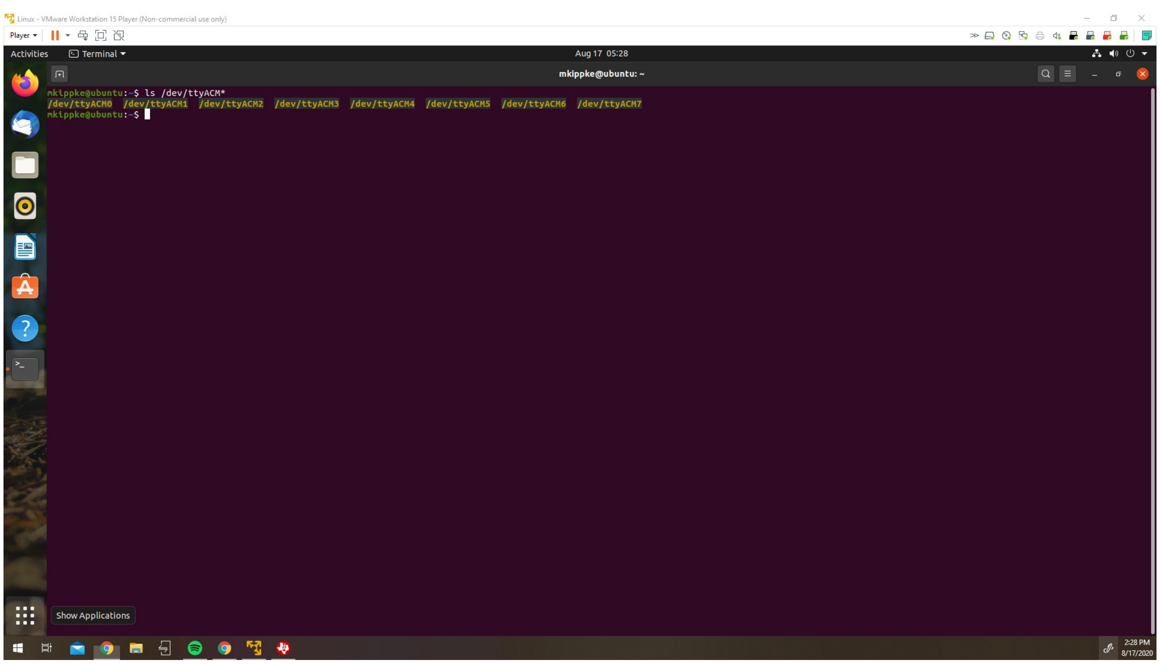

Figure 5-11: List of connected devices in the Linux environment.

After programming upload has been done on each device, it is possible to access each node by the emulated UART connection over USB protocol. Each node provides information about its own configuration, and it is possible to run a short script depicting its 6LoWPAN and RPL routing characteristics. As it can be obtained from Figure 5-12, following configuration has been done for the UDP server LBR/DC device.

- **Routing Protocol:** RPL Lite.
- **Net Type:** sicslowpan (6LoWPAN).
- **MAC Type:** CSMA (by default on Contiki-Ng environment).
- **IPv6 Local Address:** FD00::212:4B00:12CD:C062.
- **Transmission Channel N°:** 25 (200KHz channel spacing).
- **RPL Neighbours:** FE80::212:4B00:17BC:CDBA.

As it can be depicted from the data analysis, the node has been correctly configured and detected by the DAG/DODAG PAN coordinator. Sniffer in action, interfacing with Wireshark is shown in Figure 5-13, where the RPL routing commands packets (DIO and DAO objects) could be successfully dissected, demonstrating the feasibility of the node connection into an existing 6LoWPAN network.

Moreover, Figure 5-13 obtained by sniffing on channel 25, with a base frequency equal to 868.300MHz and a channel spacing of 200KHz following the SUN FSK operating mode #2 and #3 described in 3.3 in subsection 3.3.2, it is possible to analyze broadcasting messages done by the RPL DAG/DODAG PAN coordinator, as destination is announced as the FF02::1A broadcast address.

The second RPL neighbour that can be observed in Figure 5-13, with an IPv6 equal to FE80::212:4B00:1966:8088 belongs to one of the Seneco nodes which remained connected to an already existing 6LoWPAN network. The fact that the configured LBR/DC node could detect one existing node and interact with it demonstrates that any new included node may be able to communicate in the newly established network.

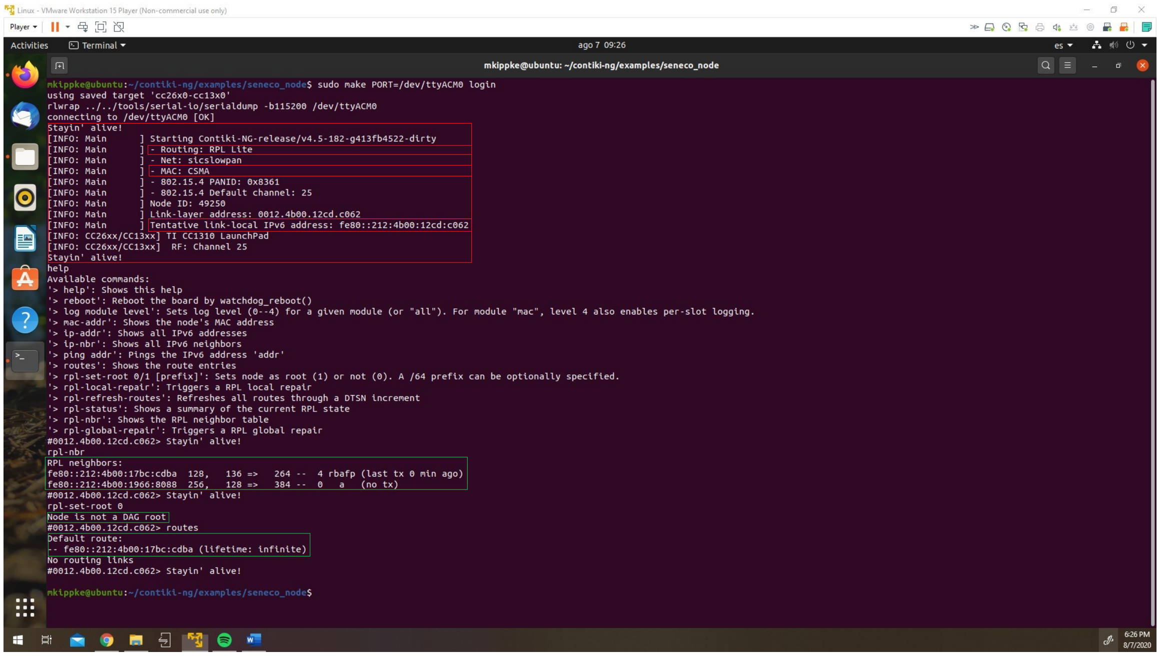

Figure 5-12: Accessing the node via UART emulation over USB for configuration.

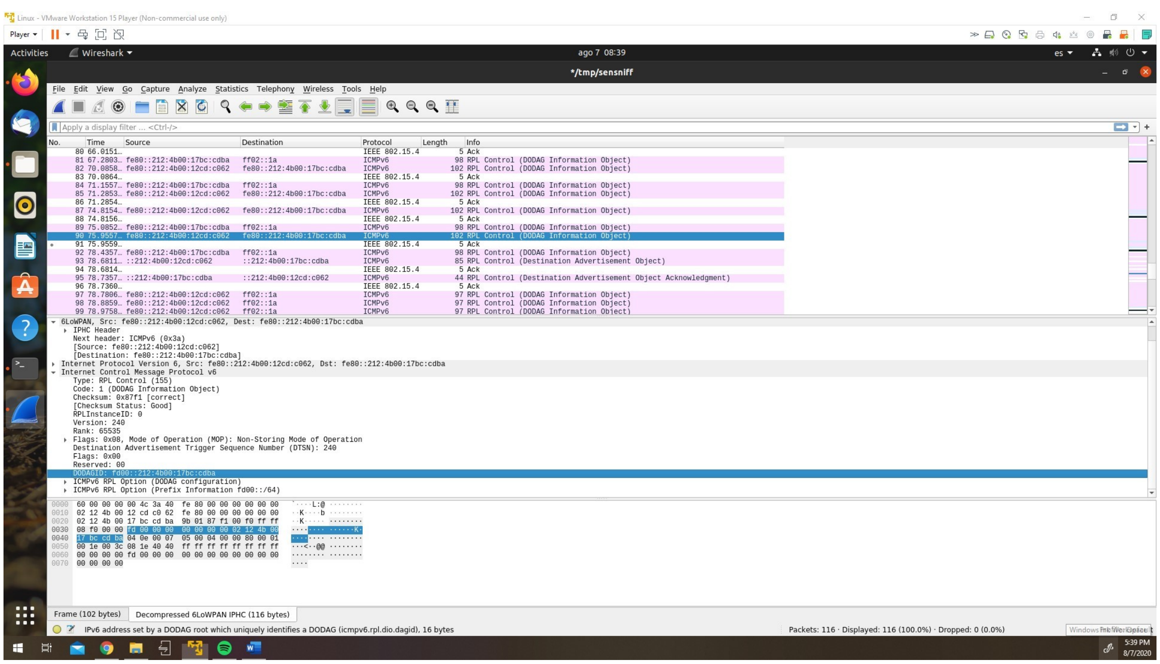

Figure 5-13: Sniffing and interfacing with Wireshark for RPL packets dissection.

One of the most important results can be obtained from Figure 5-14. Two UDP clients, LR end-node devices have been configured to be recognised by the RPL DAG/-DODAG PAN coordinator, in order to start sending data using the UDP transport protocol. As they are powered up, they initially exchange DIO and DAO RPL packets as part of the neighbor discovery routine, as shown in Figure 5-15. Once they are recognised and accepted into the new 6LoWPAN network, routes are defined. While one of the UDP clients is directly connected to the LBR/DC, the second one communicates to the LBR/DC using the first one as a *1-hop* connection towards data uploading. RPL protocol allows nodes to reconfigure their routes at any time, based on metrics and costs parameters. In this case, the fact that a *1-hop* structure has been deployed means that the routes are configuring themselves without any restriction. This network structure is depicted in Figure 5-16, where the communication links between the end-nodes and the LBR/DC are presented accordingly.

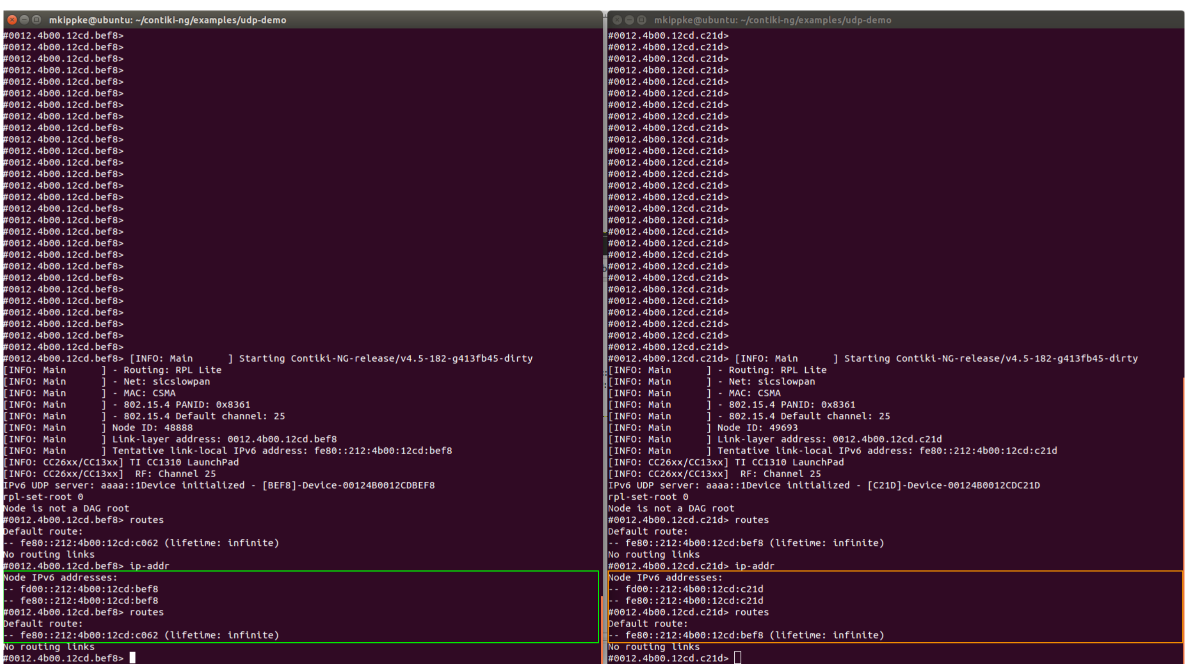

Figure 5-14: UDP Clients, LR end-nodes RPL routes configuration.

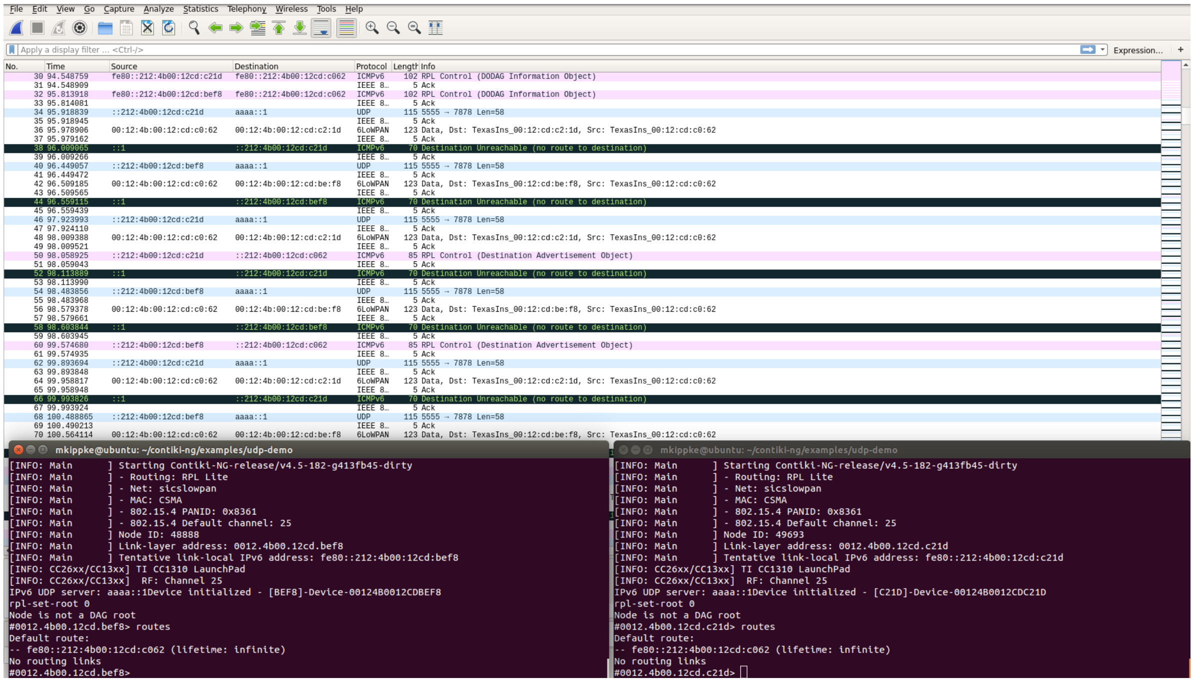

Figure 5-15: UDP Clients, end-nodes RPL routes and sniffing device with Wireshark.

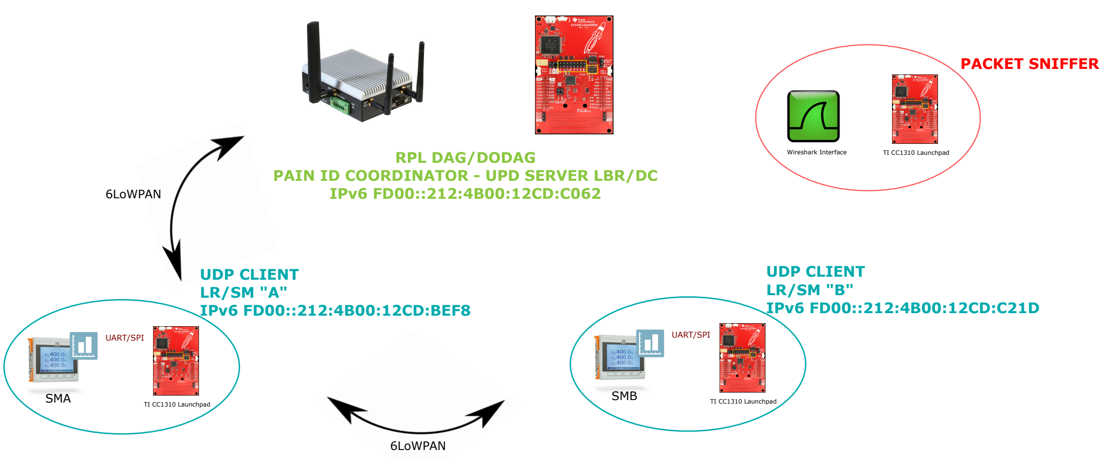

Figure 5-16: Final implementation scheme, depicting IPv6 addresses.

Chapter 6

Conclusions

After carefully analyzing the results obtained in previous section 5.4, it is possible to assume that deployment of a communication framework based on IEEE 802.15.4 and 6LoWPAN is possible, using low-cost, low-range communication end-devices in a *mesh*-topology network. This kind of topology aims to improve the range and quality of radio communication links, also being completely beneficial for industrial applications where devices are scattered in a non-structure topology and redesign or reallocation is often impossible. Results presented show the relatively flexibility of the system, since an already existing network is able to include new correctly configured devices without complications. Regarding AMI framework, it is expected that future smart meters will support IP connectivity directly, towards the creation of an IoT network and uploading measurements directly to metering platforms in the *cloud* without the need of other network infrastructures [17]. Moreover, considering the new digital highways that are being created in the newly deployed smart cities, like Gijón initiative towards applying 6LoWPAN for smart lighting operations [20], it is possible that AMIs structures based on smart meter nodes distributed in residential buildings may find a way to connect to the already deployed city 6LoWPAN network infrastructure. Therefore, the creation of digital infrastructures is not an isolated tasks: Once a network is created, expansion is easily achieved and multiple sensors can be interconnected towards reaching a real IoT framework. Transport protocols and media access control methods still need to be improved.

Results presented in Figure 5-15 show that the RPL routing protocol has been correctly applied for new nodes joining the network, after the DAG/DODAG PAN coordinator establishes the new routes towards the LBR/DC. Nevertheless, it is also possible to see some packets being unable to reach destination. Main cause of this is the lack of a proper UDP client/server interface, since the measurements acquisition protocol has nor been improved, nor develop in detail for data packets sending using the UDP protocol due to time constrains. Nevertheless, the main goal, depicting the creation of a flexible, security enhanced and low-power consumption network has been achieved. UDP routines for data acquisitions can be easily added, building a serial interface between the CC1310 and the smart meters presented in Figure 5-8. Another goal that has been reached is verifying if the proposed network structure is suitable for later implementing a Building Energy Management Systems protocols, as depicted in section 5.3. Structure presented in Figure 5-16 is suitable for industrial applications, but economic constrains may become an issue, given the fact that it is expensive to attach each smart meter with an specific 6LoWPAN module. Therefore, for new applications in industrial environments, or depicting BEMS future applications where smart meters can be connected in a structured matrix framework, other short-range, low-power consumption protocols can be analyzed, such as BLE or Wi-Fi, leaving the 6LoWPAN connection for data exports and changing the definition of a *node*. This conclusion is further analyzed in chapter 7.

Chapter 7

Future Works

In order to apply the proposed structure towards energy metering applied to residential buildings or newly deployed industrial installations, larger metering structures are needed. Texas Instruments proposed an IEEE 802.15.4 6LoWPAN AMI matrix formed by 100 devices in a *mesh*-topology network, as depicted in 7-1.

Figure 7-1: A 100-node *mesh* network used for data monitoring applications [11]

.

Results obtained from this thesis shows that although the system has proven to be useful for AMIs deployments, the associated cost per device might be over the required economic limits for a development like the one proposed. Buildings Energy Management Systems are designed with the idea that smart meters are connected one after the other, in a structured array.

This kind of arrangements allows the use of other types of protocols for short-range communications, like BLE or WiFi local networks, leaving the 6LoWPAN interfaces for longer-ranges in industrial or smart cities environments. The conception of what is defined as a *node* is therefore changed towards the integration of smart meters in a *clustered* structure. Many smart meters may share wired connections (such as Profinet Bus or Modbus) or wireless short range protocols, while data is being collected and transmitted to the overall 6LoWPAN network in a concatenated structure, as the depicted proposal presented in 5.3.

Further analysis also consider the use of Paradox IoT communication devices, which are designed around the Spirit One communication chip and allow further studies in other modulation schemes, not necessary towards SUN FSK, like Texas Instruments CC1310 launchpad applications. This enhances not only flexibility, but also would help to determine the intercommunication of devices from different manufacturers. A Paradox module, next to the mentioned TI CC1310, is presented in Figure 7-2.

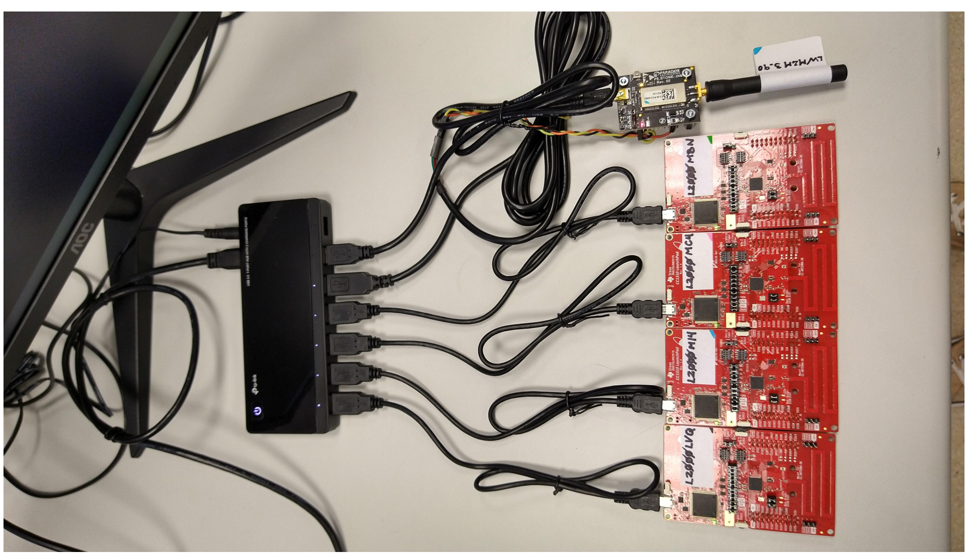

Figure 7-2: Paradox module based on Spirit One communication chip.

7.1 Blockchain and Cryptocurrencies in IoT

As mentioned before in section 1, security issues where out of the scope of this project. Nevertheless, it is important to consider the possibility of implementing a security layer based on Blockckain, for peer-to-peer energy trading platforms for devices workings in the same network, as the work depicted by [29]. AMIs structure in residential buildings or commercial installations, and later integrated into smart cities infrastructures may be the starting point towards a complete new conception of the energy market overall. As decentralized energy generation is on the rise, *prosumers* will also demand a more transparent way to access their own information. Moreover, this also proposes the idea that end-users may exchange amounts of energy building their own decentralized market, and therefore aiming to integrate the energy trading with cryptocurrencies and Blockchain-based security layers.

From smart lighting down to home automation technologies, and even considering citizens as *mobile sensors* or smart cities coming into reality, possibilities for IoT devices integrated into a communication structure are overwhelming, but there is one point that comes before any other development: Deploying the digital *highways* is vital for ensuring the correct processing of data, in ways were energy consumption is minimal but reliability is guaranteed. Energy management could be the foundation stone towards the awakening of new electric markets, with an infinite amount of players and overwhelming possibilities for artificial intelligence developments.

Appendix A

Contiki-Ng Example Codes

A.1 Packet Sniffer: Project Configuration Header

```
 * Copyright (c) 2016, George Oikonomou - http://www.spd.gr
 * All rights reserved.
#define PROJECT_CONF_H_
/*---------------------------------------------------------------------------*/
/* Configure the sensniff_mac_driver for netstack.h */
#define NETSTACK_CONF_MAC                    SENSNIFF_MAC_DRIVER
#define NETSTACK_CONF_RDC                    NULLRDC_DRIVER
/*---------------------------------------------------------------------------*/
/* Configure 6LoWPAN compression style */
#define SICSLOWPAN_CONF_COMPRESSION          SICSLOWPAN_COMPRESSION_HC06
/*---------------------------------------------------------------------------*/
/* Radio Configuration */
#define IEEE802154_CONF_PANID                0x8361
#define DOT_15_4G_CONF_FREQUENCY_BAND_ID     DOT_15_4G_FREQUENCY_BAND_CUSTOM
#define DOT_15_4G_CHAN0_FREQUENCY            863300
#define DOT_15_4G_CHANNEL_SPACING            200
#define DOT_15_4G_CHANNEL_MAX                32
#define PROP_MODE_CONF_LO_DIVIDER            0x05
#define IEEE802154_CONF_DEFAULT_CHANNEL      25
#define NETSTACK_CONF_FRAMER                 FRAMER_802154
#endif /* PROJECT_CONF_H_ */
```

A.2 UDP Client/Server: Project Configuration Header

```
 * Copyright (c) 2016, George Oikonomou - http://www.spd.gr
#define PROJECT_CONF_H_
/*---------------------------------------------------------------------------*/
/* Configure the contikimac_driver for netstack.h */
#define NETSTACK_CONF_RDC                        contikimac_driver
/*---------------------------------------------------------------------------*/
/* Configure the RPL Protocol */
#define RPL_CONF_MAX_DAG_PER_INSTANCE            1
#define REST_MAX_CHUNK_SIZE                      48
#define RPL_CONF_WITH_DAO_ACK                    0
#define RPL_CONF_OF                              rpl_of0
/*---------------------------------------------------------------------------*/
/* Disable TCP Services */
#define UIP_CONF_TCP                             0
/*---------------------------------------------------------------------------*/
/* Radio Configuration */
#define IEEE802154_CONF_PANID                    0x8361
#define DOT_15_4G_CONF_FREQUENCY_BAND_ID         DOT_15_4G_FREQUENCY_BAND_CUSTOM
#define DOT_15_4G_CHAN0_FREQUENCY                863300
#define DOT_15_4G_CHANNEL_SPACING                200
#define DOT_15_4G_CHANNEL_MAX                    32
#define PROP_MODE_CONF_LO_DIVIDER                0x05
#define IEEE802154_CONF_DEFAULT_CHANNEL          25
/*---------------------------------------------------------------------------*/
/* RPL Routing Defines */
#define NBR_TABLE_CONF_MAX_NEIGHBORS             32
#define NETSTACK_MAX_ROUTE_ENTRIES               64
/*---------------------------------------------------------------------------*/
/* Enable Neighbor Discovery */
#define UIP_CONF_ND6_SEND_NS                     1
/*---------------------------------------------------------------------------*/
#endif /* PROJECT_CONF_H_ */
```

A.3 Contiki-Ng Supported Frequencies

```
/*---------------------------------------------------------------------------*/
/* IEEE 802.15.4g frequency band identifiers (Table 68f) */
#define DOT_15_4G_FREQUENCY_BAND_169     0  /*  169.400  169.475 (Europe)
#define DOT_15_4G_FREQUENCY_BAND_450     1  /*  450.000  470.000 (US)
#define DOT_15_4G_FREQUENCY_BAND_470     2  /*  470.000  510.000 (China)
#define DOT_15_4G_FREQUENCY_BAND_780     3  /*  779.000  787.000 (China)
#define DOT_15_4G_FREQUENCY_BAND_863     4  /*  863.000  870.000 (Europe)
#define DOT_15_4G_FREQUENCY_BAND_896     5  /*  896.000  901.000 (US FCC Part 90)
#define DOT_15_4G_FREQUENCY_BAND_901     6  /*  901.000  902.000 (US FCC Part 24)
#define DOT_15_4G_FREQUENCY_BAND_915     7  /*  902.000  928.000 (US)
#define DOT_15_4G_FREQUENCY_BAND_917     8  /*  917.000  923.500 (Korea)
#define DOT_15_4G_FREQUENCY_BAND_920     9  /*  920.000  928.000 (Japan)
#define DOT_15_4G_FREQUENCY_BAND_928     10 /*  928.000  960.000 (US)
#define DOT_15_4G_FREQUENCY_BAND_950     11 /*  950.000  958.000 (Japan)
#define DOT_15_4G_FREQUENCY_BAND_1427    12 /* 1427.000 1518.000 (US and Canada)
#define DOT_15_4G_FREQUENCY_BAND_2450    13 /* 2400.000 2483.500
#define DOT_15_4G_FREQUENCY_BAND_CUSTOM  14 /* Custom frequency band settings */
/*---------------------------------------------------------------------------*/
/*
 * Channel count, spacing and other params relating to the selected band. We
 * currently only support some of the bands defined in .15.4g and for those
 * bands we only support operating mode #1 (Table 134).
 *
 *
 * DOT_15_4G_CHAN0_FREQUENCY is specified here in KHz
 *
 * Custom bands and configuration can be used with DOT_15_4G_FREQUENCY_BAND_CUSTOM.
 *
 *
 * Example of custom setup for the 868Mhz sub-band in Europe with 11 channels,
 * center frequency at 868.050MHz and channel spacing at 100KHz.
 * These should be put in project-config.h or similar.
 */
```

A.4 Contiki-Ng RF Core Module

```
 * Copyright (c) 2016, George Oikonomou - http://www.spd.gr
#define DOT_15_4G_H_
/*---------------------------------------------------------------------------*/
#if   DOT_15_4G_FREQUENCY_BAND_ID==DOT_15_4G_FREQUENCY_BAND_780
#define DOT_15_4G_CHANNEL_MAX             38
#define DOT_15_4G_CHANNEL_SPACING        200
#define DOT_15_4G_CHAN0_FREQUENCY     779200
#define PROP_MODE_CONF_LO_DIVIDER       0x06

#elif DOT_15_4G_FREQUENCY_BAND_ID==DOT_15_4G_FREQUENCY_BAND_863
#define DOT_15_4G_CHANNEL_MAX             33
#define DOT_15_4G_CHANNEL_SPACING        200
#define DOT_15_4G_CHAN0_FREQUENCY     863125
#define PROP_MODE_CONF_LO_DIVIDER       0x05

#elif DOT_15_4G_FREQUENCY_BAND_ID==DOT_15_4G_FREQUENCY_BAND_915
#define DOT_15_4G_CHANNEL_MAX            128
#define DOT_15_4G_CHANNEL_SPACING        200
#define DOT_15_4G_CHAN0_FREQUENCY     902200
#define PROP_MODE_CONF_LO_DIVIDER       0x05

#elif DOT_15_4G_FREQUENCY_BAND_ID==DOT_15_4G_FREQUENCY_BAND_920
#define DOT_15_4G_CHANNEL_MAX             37
#define DOT_15_4G_CHANNEL_SPACING        200
#define DOT_15_4G_CHAN0_FREQUENCY     920600
#define PROP_MODE_CONF_LO_DIVIDER       0x05

#elif DOT_15_4G_FREQUENCY_BAND_ID==DOT_15_4G_FREQUENCY_BAND_950
#define DOT_15_4G_CHANNEL_MAX             32
#define DOT_15_4G_CHANNEL_SPACING        200
#define DOT_15_4G_CHAN0_FREQUENCY     951000
#define PROP_MODE_CONF_LO_DIVIDER       0x05
/*---------------------------------------------------------------------------*/
#endif /* DOT_15_4G_H_ */
```

Nomenclature

Acronyms

PEV: Plug-in Electrical Vehicles

QoS: Quality of Service

MTU: Maximum Transmission Unit

DLMS: Device Language Message Specification

COSEM: Companion Specification for Energy Metering

LBR/DC: Local Border Router/Data Concentrator structure

RTT: Return Trip Time

DAG: Directed Acyclic Graph

BEMS: Building Energy Management System

LLN Low-Power, Lossy Network

OSI: Open System Interconnection

RPL: Routing Protocol for Low-Power, Lossy Networks

DNS: Domain Naming System

HTTP: Hypertext Transfer Protocol

FTP: File Transfer Protocol

PAN: Personal Area Network

WPAN: Wireless Personal Area Network

LR-WPAN: Low-Rate Wireless Personal Area Network

FFD: Full-Function Device

RDF: Reduced-Function Device

CSMA-CA: Carrier Sense Multiple Access With Collision Avoidance

SUN: Smart Utility Network

BLE: Bluetooth Low Energy

M2M: Machine-to-Machine

GPRS: General Packet Radio Service

FSK: Frequency Shift Keying

CSS: Chirp Spread Spectrum

UPS: Uninterrupted Power Supply

ND: Neighbor Discovery

WSN: Wireless Sensor Network

DODAG: Destination Oriented Directed Acyclic Graph

DIO: DODAG Information Object

DAO: Destination Advertisement Object

GUI: Graphic User Interface

SCADA: Supervisory Control and Data Acquisition

CDF: Cumulative Distribution Function

Definitions

ubiquitous: Distribution of comm. equipment to achieve continuous connectivity

DLMS/COSEM: Standard for smart energy metering, control and management

OSI Model: Standardized model for describing main communication functions

IP Datagram: Self-contained entity of data, routed from source to destination

Profinet: Industry technical standard for data communication over Ethernet

MQTT: Lightweight messaging protocol for mobile devices optimized for LLNs

tunslip6: Tool used to bridge IP traffic between a host and another network element

Wireshark: Former Ethereal, is a widely-used network protocol analyzer

Bibliography

[1] Red Electrica de España, "Electricity demand tracking in real time, associated generation mix and CO2 emissions," Aug. 2020.

[2] C. Sangumpai and C. Aswakul, "Development of Real-Time Interworking between IEEE1888 and ECHONET Lite Standards for Building Energy Management System," *Engineering Journal*, vol. 21, pp. 1–10, Oct. 2017.

[3] J. Dias, F. Ribeiro, R. Campos, M. Ricardo, L. Martins, F. Gomes, and A. Carrapatoso, "Evaluation of an RPL/6LoWPAN/IEEE 802.15.4g solution for smart metering in an industrial environment," in *2016 12th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, pp. 1–4, Institute of Electrical and Electronics Engineers (IEEE), Jan. 2016.

[4] A. Rayes and S. Salam, *Internet of Things From Hype to Reality: The Road to Digitization*. Springer International Publishing, 2 ed., 2019.

[5] M. Al-Ani, "IPv4/IPv6 Transition," Dec. 2012.

[6] Institute of Electrical and Electronics Engineers (IEEE), "IEEE Std 802.15.4™-2015, IEEE Standard for Low-Rate Wireless Networks," 2015.

[7] D. M. Pierguiseppe, P. Skillermark, A. Larmo, and P. Arvidson, "Bluetooth Mesh Networking," July 2017. Ericsson White Paper 284 23-3310 UEN.

[8] LoRa Alliance®, "What is LoRaWAN®," 2015.

[9] R. Ullah, Y. Faheem, and B.-S. Kim, "Energy and Congestion-Aware Routing Metric for Smart Grid AMI Networks in Smart City," *IEEE Access*, vol. 5, pp. 13799–13810, 2017.

[10] Phoenix Contact, "Productos y servicios para la gestión energética," Feb. 2020. IF 02-20.001.L3 MNR 110165/2020-03-02/02.

[11] Texas Instruments, "TIDA-010003 - Simple 6LoWPAN Mesh End-Node Improves Network Performance Reference Design," Apr. 2019.

[12] A. Ikpehai and B. Adebisi, "6LoPLC for smart grid applications," in *2015 IEEE International Symposium on Power Line Communications and Its Applications (ISPLC)*, pp. 211–215, Mar. 2015.

[13] E. N. Cam-Winget, J. Hui, and D. Popa, "Applicability Statement for the Routing Protocol for Low-Power and Lossy Networks (RPL) in Advanced Metering Infrastructure (AMI) Networks," 2017. Number: RFC 8036.

[14] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "A Survey on Smart Grid Potential Applications and Communication Requirements," *IEEE Transactions on Industrial Informatics*, vol. 9, pp. 28–42, Feb. 2013. Conference Name: IEEE Transactions on Industrial Informatics.

[15] U.S. Department of Energy, "Communications Requirements Of Smart Grid Technologies," Oct. 2010.

[16] B. Heile, "Wi-SUN FAN Overview," July 2017.

[17] J. Höglund, D. Ilic, S. Karnouskos, R. Sauter, and P. Goncalves da Silva, "Using a 6LoWPAN smart meter mesh network for event-driven monitoring of power quality," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, pp. 448–453, Nov. 2012.

[18] L. Scott, "Cisco Visual Networking Index (VNI) and VNI Service Adoption Global Forecast Update, 2015–2020," 2016.

[19] W. Boltz, "Chapter 8 - The Challenges of Electricity Market Regulation in the European Union," in *Evolution of Global Electricity Markets* (F. P. Sioshansi, ed.), pp. 199–224, Boston: Academic Press, Jan. 2013.

[20] Ayuntamiento de Gijón/Xixón, "Documentación Técnica Gijón City Lab," 2020.

[21] Z. Shelby and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*. John Wiley & Sons Ltd., 1 ed., 2009.

[22] D. H. Le and W. Pora, "Implementation of smart meter working as IEEE1888-6LoWPAN gateway for the building energy management systems," in *2014 11th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pp. 1–5, Institute of Electrical and Electronics Engineers (IEEE), May 2014.

[23] A. Zaballos, A. Vallejo, and J. M. Selga, "Heterogeneous communication architecture for the smart grid," *IEEE Network*, vol. 25, pp. 30–37, Sept. 2011. Conference Name: IEEE Network.

[24] B. Adebisi, A. Treytl, A. Haidine, A. Portnoy, R. U. Shan, D. Lund, H. Pille, and B. Honary, "IP-centric high rate narrowband PLC for smart grid applications," *IEEE Communications Magazine*, vol. 49, pp. 46–54, Dec. 2011. Conference Name: IEEE Communications Magazine.

[25] "GRID20/20 - Distribution Transformer Monitors."

[26] G. Z. Papadopoulos, R. A. Jadhav, P. Thubert, and N. Montavont, "Updates on RFC 4944: Fragment Forwarding and Recovery," *IEEE Communications Standards Magazine*, vol. 3, pp. 54–59, June 2019. Conference Name: IEEE Communications Standards Magazine.

[27] DLMS User Association, *DLMS/COSEM Architecture and Protocols*. DLMS User Association, green book ed. 9 ed., May 2019.

[28] R. M. Gardner and Y. Liu, "FNET: A Quickly Deployable and Economic System to Monitor the Electric Grid," in *2007 IEEE Conference on Technologies for Homeland Security*, pp. 209–214, May 2007.

[29] K. Khan, "Blockchain-Based Peer-to-Peer Energy Trading using IoT devices," Aug. 2019. Accepted: 2019-09-17T09:50:58Z.

[30] R. Natarajan, P. Zand, and M. Nabi, "Analysis of coexistence between IEEE 802.15.4, BLE and IEEE 802.11 in the 2.4 GHz ISM band," in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, pp. 6025–6032, Institute of Electrical and Electronics Engineers (IEEE), Oct. 2016.

[31] J. Muñoz, T. Chang, X. Vilajosana, and T. Watteyne, "Evaluation of IEEE802.15.4g for Environmental Observations," *Sensors (Basel, Switzerland)*, vol. 18, Oct. 2018.

[32] "The Bluetooth® Core Specification."

[33] Texas Instruments, "Infographic: Why Sub-1 GHz?," 2016.

[34] European Telecommunications Standards Institute (ETSI), "ETSI - TR 102 649-2 - Electromagnetic compatibility and Radio spectrum Matters (ERM); Technical characteristics of Short Range Devices (SRD) and RFID in the UHF Band; System Reference Document for Radio Frequency Identification (RFID) and SRD equipment; Part 2: Additional spectrum requirements for UHF RFID, non-specific SRDs and specific SRDs | Engineering360," 2008.

[35] K. Seo and S. Kent, "RFC 4301 - Security Architecture for the Internet Protocol," Dec. 2005.

[36] B. Hinden and S. E. Dr. Deering, "RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification," Dec. 1998.

[37] E. T. Winter, E. P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," 2012. Number: RFC 6550.

[38] Texas Instruments, "CC1310 SimpleLink™ Ultra-Low-Power Sub-1GHz Wireless MCU," July 2018.