Energy@home Leveraging ZigBee to Enable Smart Grid in Residential Environment

Andrea Ranalli and Claudio Borean

Telecom Italia S.p.A. - via g. Reiss Romoli, 274 - 10100 Turin, Italy
{andrea.ranalli,claudio.borean}@telecomitalia.it

Abstract. In this paper, the project called Energy@home is introduced. It is a new and innovative attempt to standardize the Smart Grid eco-system, providing use cases and standardization of the communication protocol within a Home Area Network (HAN). Energy@home has been started as an Italian collaborative project among different companies, founded by Electrolux, Enel, Indesit Company and Telecom Italia. The aim of the project was to develop a communication infrastructure that enables provision of "Value Added Services" based upon information exchange related to energy usage, energy consumption and energy tariffs in the HAN. Different technologies are supported, but the first integration among different devices has been developed using ZigBee: this technology offers green and global wireless standards connecting the widest range of devices to work together intelligently. After the release of Energy@home specification and the validation of it through a number of interoperability test events, the Energy@home project has moved from being a collaborative project into a non-profit association. The goal of the association is to promote technologies and services for the home energy efficiency and for the proactive participation of the end users. The Energy@home Association is open to any company and anyone who is wishing to contribute to its purposes and it is rapidly growing with the addition of new members.

The ZigBee Alliance is an open, non- profit association of more than 400 organizations driving development of innovative, reliable and easy-to-use ZigBee standards. The Alliance promotes worldwide adoption of ZigBee as the leading wirelessly networked, sensing and control standard for use in consumer, commercial and industrial areas.

Keywords: ZigBee, Energy@home, Customer Interfaces, Appliance Power Profile, Demand Side Management, HAN, HG, HN, Home Energy Monitor, Peak Demand, Smart Info, Smart Plug, Smart Appliance, Security, TrustCenter Link keys.

1 Introduction

The paper is structured into 6 core sections. In section 1 a general overview of the project is provided. In section 2 more details for the Energy@home are presented, giving a whole and generic overview of the system and the founding companies that started this project. Section 3 introduces the standard adopted by Energy@home, in

J. Cuellar (Ed.): SmartGridSec 2012, LNCS 7823, pp. 132–149, 2013.

particular the ZigBee technology and CENELEC, providing some useful insight about the benefits that those organizations can achieve by joining their forces. Section 4 enters into the details of the system architecture, defining all the devices, how they communicate and what kind of information they exchange. Section 5 introduces useful scenarios that are adopted by the Energy@home project (others can be defined in the future), with different level of functionalities (Customer Awareness and Appliance Regulation, which can be performed as a coordinated regulation or a self-regulation) and different aspects that concerns the maintenance of the devices within the house. Finally, section 6 introduces the ZigBee security model, showing the different level of security offered by the ZigBee Alliance[1] and which is the common model adopted.

2 Energy@home

The Energy@home project envisions a protocol that shall be used to build an integrated platform to allow cooperation between the main devices involved in residential energy management (please see section 4 for more details): the Electronic Meter, responsible for providing certified metering data; the Smart Appliances, able to cooperate in order to adjust power consumption by modifying their behavior, while preserving the quality of service and user experience; the Smart Plugs, able to collect metering data and to implement a simple on/off control on the plugged energy loads other than Smart Appliances; the Home Residential Gateway, which acts as the central coordinator of the entire home. This last component allows data exchange between the devices operating in the Home Network[2] (HN), in the Home Area Network[3] (HAN), and in the Internet.

These actors identify the main categories of devices in the Home Domain, without any limitation to the possibility for a device to implement functionalities from more than a category. As an example, an advanced Smart Appliance, provided with a rich user interface, could also implement functionalities typical of a Customer Interface. In the same way, a personal computer might be considered a Smart Appliance from the protocol point of view if it is able to behave like a white good within the HAN. To facilitate a whole vision about how those devices are interconnected, an overall scenario is presented in Figure 1. From a functional point of view, Energy@home envisions a system that can provide users with information on their household

[1] ZigBee Alliance website: `www.zigbee.org`

[2] A home network is a residential local area network, typically characterized by high throughput. It is used for communication between digital devices typically deployed in the home, usually personal computers, printers, gateways. The home network can be wireless (e.g. Wi-Fi) or wired (e.g. Ethernet).

[3] A home area/automation network is a residential local area network, usually characterized by low throughput. It is typically used for communication between devices within the home such as sensors, smart plugs, smart thermostats and household appliances. It can be a Wireless network (e.g. ZigBee) or wired (e.g. Power Line Communication). This is often referred to as PAN (Personal area network).

consumption directly on the display of the appliance itself, on the smart phone or on their computer. It is expected that, through easy access to information on consumption and through the possibility of downloading custom applications, consumers will be able to use their appliances in a "smart" way by enhancing the energy efficiency of the entire house system. For instance, Smart Appliances can start functioning at non-peak (and therefore less expensive) times of day as well as they can cooperate to avoid overloads by automatically balancing consumption without jeopardizing the proper execution of cycles.

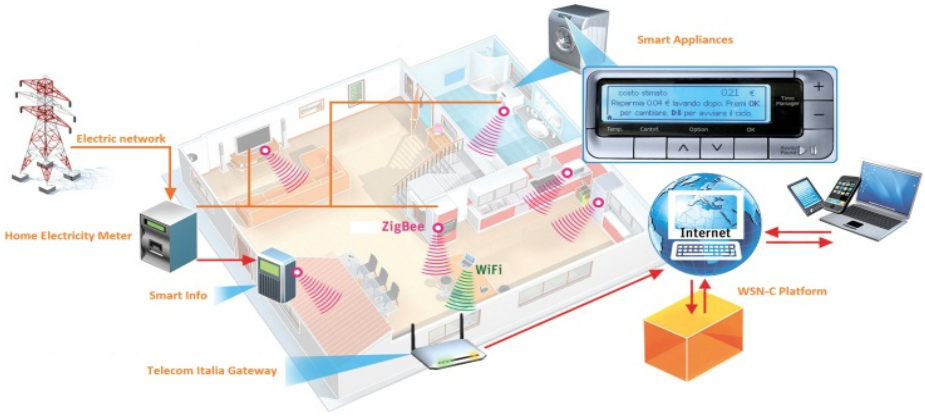

Fig. 1. Whole overall system

The project is a further step towards the development of a proper smart grid, that, in the future, will allow continuous real-time two-way information exchange between utilities and appliances in the houses to enable each customer to "self-manage" his/her energy behaviors depending on power supply and prices.

Energy@home aims to leverage existing standards, in particular the ZigBee wireless technology, the Smart Energy and Home Automation ZigBee Application Profiles (see section 3). If and where needed, these profiles will be extended and customized in order to fulfill the requirements of the project. The resulting protocol will be open to any stakeholder that will be free to define its own services and supporting business models, while being assured that the common communication platform will be able to ensure interoperability among platform of different vendors. Although the definition of services and business models is explicitly outside the scope of the project, partners have decided to perform a first assessment of the different categories of services that should be supported by the communication platform in order to ensure full support for a wide range of energy applications.

For this reason, this first deliverable provided by this project is the "Energy@home Use Cases" document (section 5), where the system architecture is presented together with reference application scenarios ([1]).

Samples of a real world deployment about this energy monitoring system will be provided in a future paper, once the current trial will be concluded and some data analysis can be done. In fact, there are currently 100 real homes spread around Italy using Energy@home, but the results can be shown only at the end of a fully year of usage, where we can collect and show consolidate numbers about energy efficiencies and reductions obtained using this system.

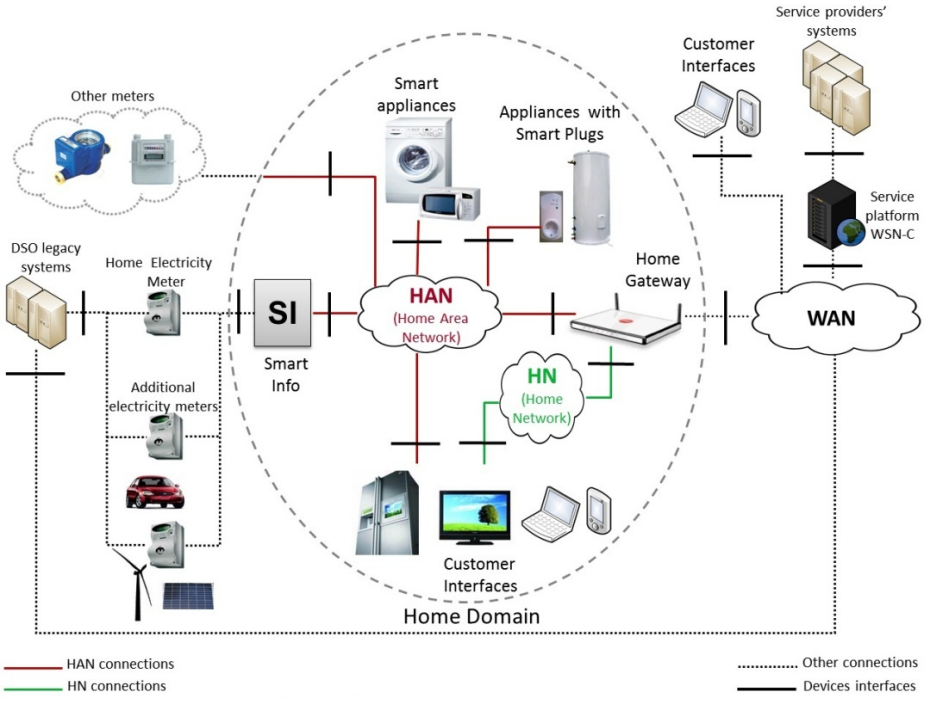

Fig. 2. E@H System architecture

3 ZigBee and CENELEC Standards

The Energy@home initiative started with a benchmark on existing standard technologies and solutions in order to leverage on existing tested and proven features. In case it has not been possible to find the proper features needed, new specifications have been provided to fill the gaps in the existing solutions. In particular, the technical specifications describe the specifications of the HAN communication, defines the wireless protocol to be adopted, the data model, the set of application messages, and the activity sequence diagrams showing the interactions among devices. The latest Energy@home specification is available at the website[4] (see [2]).

[4] Energy@home association web site: `www.energy-home.it`

ZigBee has been chosen since it is a very low-cost, very low-power-consumption, two-way, wireless communications standard. Solutions adopting the ZigBee standard are embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys and games. The ZigBee® Alliance and Energy@home have signed a liaison agreement to cooperate on the creation of an integrated residential energy value added services platform for Europe by leveraging four ZigBee standards. Under this agreement, the groups are focused on blending the strengths of ZigBee Home Automation™, ZigBee Smart Energy™, ZigBee Telecom Services™ and ZigBee Gateway™ to create a platform proposed by the Energy@home project. This platform offers control of consumer smart appliances, communication with broadband networks, and communication with Automatic Meter Management system. The platform creates value added services (please refer to section 5, where a list of use cased are introduced) designed to help European consumers better manage energy use in their homes. These energy services also give Europeans the ability to lead the way in the global energy efficiency challenge.

The collaboration between the two groups increases the scope and value of the ZigBee Home Automation profile, a core specification widely used in Energy@home, helping them to seize the numerous time-to-market advantages that ZigBee standards offer because improving the use of energy is recognized as a global issue. Also, the ZigBee Smart Energy profile, one of the world's leading standard for home area networks used by Smart Grid programs, together with the ZigBee Cluster library, will boost energy management and efficiency in homes around the world. Please refer to [3] for more information about each application profile.

The current collaboration between those two groups have been quite productive and successful, providing new clusters and devices as part of the next Home Automation specification (version 1.2), which is probably going to be released in Q1 2013. Different test events have been conducted in a joined site to strength the reliability of the whole architecture. Also, Energy@home relies on the security mechanisms offered by ZigBee (see section 6), avoiding to define another model that could have potentially bugs.

In order to define the interaction model with the Smart Appliances, Energy@home adopted the standard CENELEC EN50523 (see [6] and [7]) as specified by CECED[5], and mapped it into specific ZigBee clusters. Energy@home is also working with ZigBee Alliance, CECED and Home Gateway Initiative (HGI) to promote the requirements for home energy management and control and cover them by adopting a standard approach, since it is desirable to have the support of the features of power profiling of Smart Appliances, appliance control and scheduling.

4 System Architecture

An overall of the system architecture is presented in this chapter. The part inside the dotted area (that includes both the HAN and the HN) is the user's Home Domain,

[5] European Committee of Domestic Equipment Manufacturers.

where all the actors (Smart Appliances, Home Gateway, Smart Info and Customer Interfaces) can cooperate through some communication mechanism. All the depicted interfaces are logical ones and could be implemented through one or more communication technologies.

The following paragraphs reports in more details the main actors in the Home Domain (Figure 3 shows some examples of such devices). For more information please check also the technical document "A User-Centric Energy Management System" in [5].

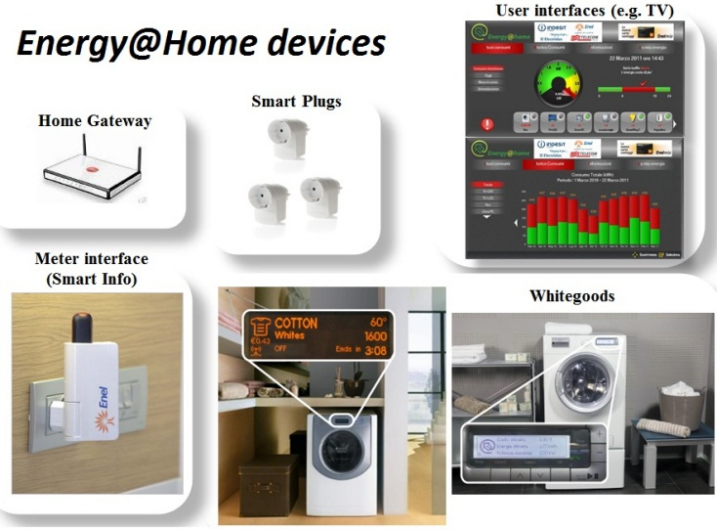

Fig. 3. Energy@home devices

4.1 Smart Appliances

This device can be seen as an evolution of the actual and standard white goods. See hereunder some of their possible new functionalities:

- Display to the customer information on their energy consumptions (e.g. used energy, instant power…)
- Dispatch in the HAN information on their energy consumptions (e.g. used energy, instant power…)
- Autonomously adapt their behavior according to information on energy consumptions coming from the house. (E.g. reduce their load when global house consumptions go beyond a threshold…)
- Cooperatively operate with other entities in order to optimize the energy usage through load shifting and load shedding.

In any case, the load control operations either performed autonomously or under an external supervision, shall be performed under the complete control of the appliance,

which assures the correct execution of its working procedure and its results and performances. For example, a smart washing machine, when requested to modify its consumption behavior, shall assure the result of the washing cycle. Smart plugs (able to provide remote metering and to be remotely controlled) could be somehow included in the Smart Appliances category although they can provide no direct control over the effect of remote control activities (Smart Appliances will not be controlled by Smart Plugs).

4.2 Customer Interfaces

This can be a generic user interface accessible through different type of devices (TV, laptop, table, smartphones, PDAs, ad hoc displays, entertainment systems and similar). Some typical functionalities are:

- Display information on energy usage like instant power, historical data, contractual information and similar, from the whole house (coming from the Smart Info) and from every single smart appliance. The level of details and graphical layout of their user interface is freely defined by every device.
- Transmit control message to Smart Appliances to request a modification of their behavior
- Configure Smart Appliances to modify their power consumption profile (e.g. a personal computer used to configure a thermostat to activate the controlled load only in certain time slots).

The Customer Interface, from this perspective, is connected in the HN/HAN; it is foreseen the possibility to have Customer Interfaces accessing the house from the WAN through a specific interface. The software application, which implements the user interface, could be local in the device or remotely hosted in another device and accessed through web-services (e.g. using a cloud-based service).

4.3 Home Gateway

It is the gateway between the HAN, the HN and the WAN (e.g. internet). It is able to interface Smart Appliances and other user's devices (e.g. laptop) through the communication protocol(s) used in the HAN (e.g. ZigBee) and in the HN (e.g. IP/HTTP) and to provide a broadband connection to internet (usually via a standard ADSL connection). Moreover, the gateway is able to collect energy data from the Smart Info and additional information from Smart Appliances, publish them in the HAN and in the HN and use all collected data to control Smart Appliances and optimize their behavior. Finally, the gateway can offer a web user interface and provide an Execution Environment (e.g. OSGi framework[6] for Java) to host third-party application (e.g. a software component implementing the algorithm to calculate the energy price at a given time, provided by the Energy Retailer).

[6] OSGi web site: `http://www.osgi.org/`

4.4 Smart Info

This is the element provided by the DSO[7], which dispatches energy related information into the HAN. Published data are a sub-set of those already available inside the Home Electricity Meter, and hence the Smart Info acts like a proxy of the meter. Additional data could be possibly generated by the Smart Info itself. Noticeably, near real-time instant power (sampled at of about 1 Hertz frequency or higher for overload prevention and load management, lower sampling can be performed for billing) should be acquired by another metering device, likely embedded inside the Smart Info. Additional elements (SI') can also be provided by third parties and used to dispatch data generated by other meters into the HAN.

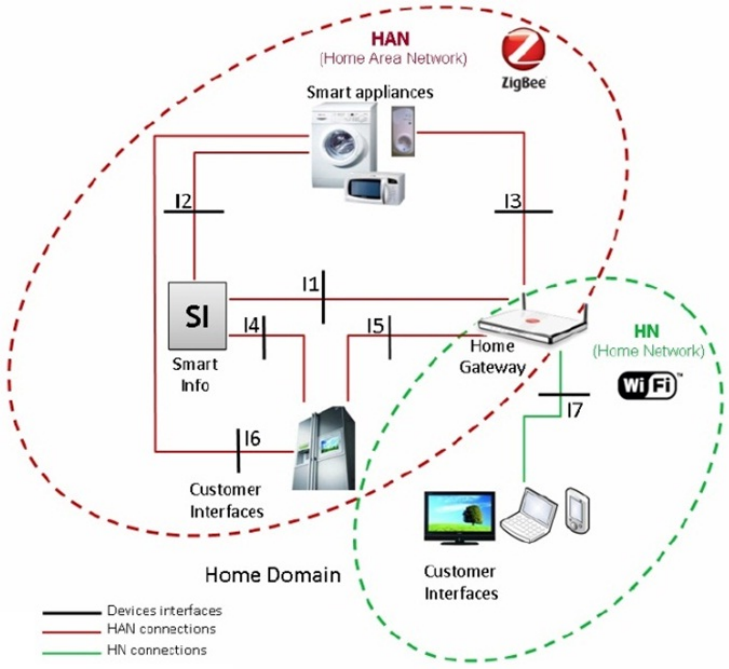

Fig. 4. In-Home domain and related logical interfaces

4.5 WSN-C

The Wireless Sensor Network Center is responsible to manage, together with the Home Gateway, the HAN devices and provides service oriented interfaces for the development of third-party applications. This component, as well as the Home Electricity Meter, are outside the Home Domain as shown in Figure 4: the in-home

[7] In electrical power business, a Distribution System Operator is an operator that carries and delivers electricity to the consumer from the TSO's distribution lines (Transmission System Operators).

domain and related logical interfaces are presented in more details, together with two network levels: HAN and HN, where ZigBee and Wi-Fi are mentioned just as an example of two possible communication technologies.

4.6 Home Electricity Meter

Another outstanding component outside the Home Domain is the electric meter, able to measure and record usage data in time differentiated registers, and capable of transmitting such data to central utilities system. Moreover, the meter should provide bi-directional communication to allow remote management of the meter.

Please note that all the above device's classification are intended to identify the main categories of devices in the Home Domain, without any limitation to the possibility for a device to implement functionalities from more than a category. As an example, an advanced Smart Appliance, provided with a rich user interface, could also implement functionalities typical of a Customer Interface. In the same way, while typical smart appliances are smart white goods, also a personal computer, able to perform such operations, should be considered an appliance from this perspective.

4.7 Smart Plug

The simplest but probably must important and used device is represented by the smart plug: connected to the plug of the appliance that the user wishes to monitor, this device is able to report the instant power consumption. This is particularly suitable for the migration path of existing appliances, avoiding replacing them all together when this system is installed. Enhanced versions of those devices are able to turn on/off the connected appliance, quite useful to control lights and standby consumptions.

5 Use Cases

In this section different type of services are introduced, taking into account incremental levels of interoperability in order to provide clients with different levels of service, starting from simple awareness, until the achievement of a fully integrated Energy Management system. The first release of the Use Cases has been identified taking into account the experience of the partners involved in the project and constitutes the initial set of functionalities that shall be addressed by Energy@home. However, new use cases will be introduced whenever partners shall identify the chance to implement supplementary categories of services for clients or taking into account additional experiences and points of view.

Use cases can be grouped into different incremental levels of functionalities of the Energy@home system:

- Customer Awareness
- Appliance Regulation

The next paragraphs are going to show them with more details. Moreover, some auxiliary use cases related to the set up and maintenance of the Network itself are defined, even if they are not strictly related to the Energy Management of the house.

5.1 Customer Awareness

The goal of this first level of functionalities is to enhance customer awareness about her/his energy consumption by displaying some useful energy related data. The appliance will not suggest directly to the customer any related action. Below are reported a number of scenario currently covered by Energy@home, while others, as the photovoltaic system cited in section 8, are currently considered as a future work that could be done to enhance the system's features.

Scenario 1: Visualization of Current Energy and Power Data
The aim of following this use cases is to provide customer with information on the current situation of her/his consumptions.

Scenario 2: Visualization of Historical Data
The aim of following this use cases is to provide customers historical and statistical information on their energy consumption, disaggregating the global energy time variations with the one coming from the Smart Appliances.

Scenario 3: Alarm
In case of a notification of Home Domain overload or black out, the customer is promptly informed: when the overall power drawn exceeds the maximum available power, the notification shall be done with local alarms (e.g. acoustic). The customer can also access to an historical view of any alarm. In case of a black out, only a Home Gateway equipped with an UPS is able to guarantee the correct activity for a minimum time.

Scenario 4: Other Energy Information
The Execution Environment, available in the Home Gateway, enables further applications dedicated to customer awareness. For example, the energy retailer could deploy an application able to provide clients with the energy sources mix used to supply his/her appliance, specifying the percentage of renewable sources, the CO2 footprint and similar information.

5.2 Appliance Regulation

The appliance regulation can be performed according to two increasing levels of performance and system complexity: a coordinated regulation among the devices of the HAN, or a self-regulation operated autonomously by the Smart Appliances. The goal of both approaches is to provide the customer automatically with suggestions and assistance on how to improve the energy management of the house (and thus to reduce the billing cost).

Coordinated Management Appliances Regulation
In this configuration, all the Smart Appliances in the house cooperate together to regulate their behavior according to global energy information of the house, their

current state and priority when the regulation is needed. The type of regulation performed by the appliance could vary according to the type of appliance. The regulation logic could be centralized or distributed but in any cases coordinated and harmonized. Only knowing the entire energy and power status of the Home Domain System, the full performance of the system could be guaranteed; on the other side, the involved algorithms will be the most complex, having to take into consideration the different and time variable energy states of the Smart Appliances and standard electrical loads in the house. In the future renewable energy could influence the energy tariffs by changing the cost even every 15 minutes, and thus whole overviews of the appliances in use are essential.

Self-management Appliances Regulation
In this configuration, the single Smart Appliance regulates its behavior according to global energy information of the house, such as current instant power and energy price. The type of regulation performed by the appliance could vary according to the type of appliance and its current state when the regulation is needed. The main difference here is that no cooperation with other appliances is involved.

Since in this level there is no coordination with other Smart Appliances, and thus knowledge of their power consumption (and of other independent electrical loads of the house), the full performance of the system could not be guaranteed; this is why the output of the use cases of this scenario should be considered as suggestions: the customer nevertheless will be in charge of coordinating the use of other Smart Appliances and independent electrical load of the house. The user will always decide if accepting or not the suggestions from the system. On the other hand, this configuration is much simpler to implement since it does not requires complicated algorithms.

Scenario 5: Home Domain Overload Management
In this scenario, the single appliance regulates its behavior upon home power availability. The aim is to foster the use the appliances when there is enough power in order to avoid overloading. The power peak management can leverage both on coordinated and self-management regulation as indicated before.

Scenario 6: Optimize Energy Cost in Case of Multi-tariff Contract
In this scenario the E@H system performs actions in order to reduce and optimize the energy cost. The optimization of energy cost can leverage both on coordinated and self-management regulation as indicated before.

Scenario 7: Demand Response
This scenario takes into account possible requirements to be provided by different ongoing projects aimed to define the future interactions between clients and electricity market. In the scope of those projects, the clients shall be presented with daily (or even hourly) offers coming from other actors and aimed to modify clients' behavior[8]. Offers shall be probably issued by a new player in the energy market called the

[8] As already said, this scenario could be imagined quite well in the presence of renewable energies.

Aggregator, which has the mission to aggregate many small clients and to operate into the energy market presenting them as a whole. The Aggregator shall reply to market needs offering services such as:

- Power limitation within a given geographical region and temporal slot
- Peak clipping
- Peak shifting

To assure clients' participation to the services, the Aggregator shall provide them with offers, for example providing them with remuneration for power reduction within the required temporal slots. To achieve this goal there should be a mechanism to provide the clients with the offer details (temporal slot, needed reduction, remuneration mechanism, etc.), which are generally indicated as price/volume signals. For example the Aggregator could require its clients to limit the power below 2 kWh between 14.00 and 16.00, granting remuneration for those who accept the offer. It is also possible that the same energy retailer could play the aggregation, hence offering discounts on energy price.

To guarantee a clients' acceptance of demand/response policies, price/volume signals have to contain information for the coming hours to allow the appliances' planning taking into account the client's needs and the appliances' cycles' characteristics. This requirement could be satisfied if price/volume signals are linked to daily energy market results (in place in most European Countries), hence containing indication for the next day. Short term advices could be originated by intra-day markets, balancing activities and similar mechanisms. The planning activity shall receive short-term signals as well. Nevertheless, those signals make more complex the decision on the best time to run. Moreover, very short-term signal (few minutes of notice) shall have bigger impact on client's needs and should be limited to unexpected conditions like critical grid Peak Demand conditions for an immediate reaction of the appliances.

From the Energy@home point of view, price/volume signals shall be collected by the Home Gateway and used as inputs for the cost-evaluation algorithms. Hence this scenario is an extension of scenario 6 (Optimize energy cost in case of multi-tariff contract).

5.3 Energy@home Provisioning and Maintenance

In order to enable the scenarios above described it is required to activate, remove and maintain the appliances in the HAN. Access to those three functionalities is required to guarantee the customer the desired level of security in order to prevent unauthorized control of the devices connected to the HAN. In case of a ZigBee network, the admission of any new device into the HAN is charged to the coordinator of this network. It is assumed that the Home Gateway could play the coordinator role.

In case of unavailability of the Home Gateway, another device in the HAN should provide a subset of its capabilities including the connection to the Internet. This device shall be, by instance, a smart meter, which provides the Smart Info data and some of the Home Gateway functionalities.

Add a New Device
When a user buys a Smart Appliance, he/she would generally like to start it up in the Energy@home HAN with the simplest human interaction possible. The admission procedure is required to guarantee the interconnection of the Smart Info, Smart Appliances and Home Gateway owned by the same customer.

If the HAN was previously activated by the Home Gateway, through a web interface, the user starts the admission procedure, identifies the new ZigBee device, checking manufacturer and model, and allows the new Smart Appliance to join the Energy@home solution. The same procedure could be activated for the Smart Info.

In case the Home Gateway is not available, the admission procedure should be managed by another device, which shall provide user with a user-friendly interface.

It is worth to notice at this point that the actual home user in the process of installing a new or changing an existing ZigBee device shall not be worried about security specific configuration issues (please see section 6) since those devices works as plug and play, and it is expected just a minimum level of interaction to setup logical aspects of the GUI (name of the device, where is it located, assign a logo to it, etc…).

Remove a Device
It can happen that a device is broken and thus it shall be replaced, or simply a device not desired joined the HAN and thus it shall be removed: for those scenarios the customer is provided with this procedure, where the user experience could be similar to the previous one (a simple button to remove the device should be enough).

Maintenance
If the customer experienced some problems with Energy@home, a web application on the Home Gateway could present the status of the HAN including the devices list, the devices status (i.e. a node joined to the HAN but it is not responding), etc. Also Warning and Alarm could be activated in case of communication problems. If the Home Gateway is not available, this functionality is critical to be provided.

6 Security Aspects

As already mentioned in section 3, Energy@home is currently based on ZigBee technology. This section will introduce the security model adopted by the ZigBee Alliance, avoiding to figure out how such model could be potentially attacked (this will be analyzed as future work). Please see [8] for more detailed information.

As already cited in 5.3, it is worth to remind that all those security aspects that we're going to introduce in this section are hidden to the final user, which shall just interact with a simple graphical interface to setup name and logo for each device.

Since most of the ZigBee modules can be seen as single-chip wireless microcontrollers executing the whole stack on a single CPU, a specification constraint assumes an 'open trust' model where the protocol stack layers trust each other. This implies that cryptographic protection only occurs between devices, and the same security suite level is used for all services.

The ZigBee Security Services provided in the specification are:

- Key establishment
- Key transport
- Frame protection
- Device authorization

To function securely in a network, a device must have a counterpart device which it can trust to obtain keys and which controls access. ZigBee therefore introduces the concept of the Trust Center, which stores the keys for the network, uses the security services to configure a device with its key(s), and uses the security services to authorize a device onto the network.

ZigBee security is based on symmetric keys, where both originator and recipient of a protected transaction need to share the same key. Clearly, there is a problem in how these keys get to both ends; three basic methods are supported:

- Pre-installation, where keys are placed into devices using out-of-band methods (e.g. commissioning tool)
- Transport, where the Trust Center sends the key (securely wherever possible) to the device.
- Establishment, where the device negotiates with the Trust Center and keys are established at either end without being transported. This can be done in different ways:
- SKKE (Symmetric-Key, Key-Establishment)
- CBKE (Certificate-based Key Establishment)
- ASKE (Alpha-secure Key Establishment)

In ZigBee there are three key types:

- Master key[9]
- Link key, which is uniquely shared between two and only two devices for protecting frames at the APS layer (one of those devices is normally the Trust Center), usually dynamically established using key establishment service. This key could be also being pre-installed or transported from the Trust Center.
- Network key, which is a global key which is used by all devices in the network. A set of network keys is held by the Trust Center and current network key is identified by a key sequence number. It is usually transported from the Trust Center and it can also be pre-installed (based on a two stage update mechanism):

  – Update new key and associated key sequence number.
  – Switch to new key sequence number

The common security model selected by the ZigBee Alliance for home automation applications relies on the usage of network key delivered with a pre-configured Trust Center link keys; the pre-configured TrustCenter-link key protects the transport of the

[9] Shared key for SKKE only.

network key. Eventually, additional link keys can be transported or established using higher-layer mechanism. In order to preserve compatibility among devices there are different approaches currently followed according to the different profiles:

1. Use of Default Trust center link key for Home Automation: in this case a default Pre-configured Trust center link key is used to deliver network key; the default trust center link key shall be used only during the joining phase (i.e. when permit joining on the network is enabled) and shall not be used for rejoining purposes;
2. Use of custom Trust center link key derived by install code: this procedure is used in Smart Energy profile 1.x and can be used in Home Automation profile for those devices requiring higher level of security; in this case the trust center link keys are derived from unique installation codes present on the devices and properly hashed to fir AES 128-bit key; this unique key shall be configured on the trust center out-of-band and then used to deliver the network key to the joining devices; this procedure increases the level of security of the network (and it is proposed as next step for the Energy@home control use cases) but make more complex for the user the procedure of adding a new device into the network (the installation codes shall be inserted in the trust center in some way, e.g. taking a picture on a QR-code on the product and sending it to a Home Gateway device acting as the trust center);
3. Use of certificate exchange to derive the unique TC link key: this procedure is used on the Smart Energy 1.x profile; after provisionally joining the network using installation code procedure described in the point 2) above, the SE 1.x devices use CBKE (certificates-base key exchange) to update the key. This procedure increases the level of security of the solution but introduce a dependency on a PKI (public key infrastructure).

It is worth noting that in case the approaches 2 and 3 are followed the security policy on the trust center shall not enable joining of devices following the approach 1); this allows a maximum flexibility to the owner of the network but it might create compatibility issues in case a home-user shall maintain the network, since it shall be aware on the security policy of the devices. In any case procedure 1) is recommended for simple home automation network, where there is a tradeoff between easy installation setup and security procedures, while procedures 2) and 3) are typically followed in utility-centric home area networks, where the user plays a minor role in configuring and owning the devices.

6.1 Frame Protection

The security suite used for frame protection is the AES-CCM[10], which guarantees low-cost implementation in terms of resources (some wireless microcontrollers may have hardware support for this algorithm). The protection is based on two main parts:

- Encryption
- Integrity protection

[10] Advanced Encryption Standard (AES) CCM Mode.

As shown in Figure 5, encryption scrambles the original data (called plaintext in 'security speaks') into cipher text, preventing an eavesdropper from being able to interpret frame payload. Integrity protection instead adds a Message Integrity Code (MIC, 4 octets length) to be transported along with the data to be protected: the MIC 'signs' the data and allows the recipient to verify that the data has not been tampered with, then provides origin authenticity since it is bound to the identity (IEEE address) of the originator. In fact, without integrity protection, a rogue device could modify a transmitted frame and the modification may not be detected by the recipient.

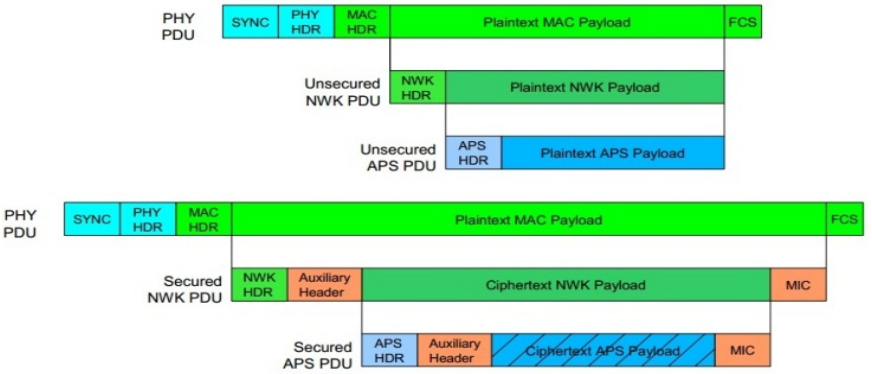

Fig. 5. Protecting at Network and APS layer

7 Conclusions

This paper provides an overview of the Energy@home project, an innovative smart grid project with the aim to allow continuous real-time and two-way information exchange between utilities and appliances in the houses, enabling customers to self-manage their energy behaviors depending on power supply and prices. Following the introduction of the Energy@home project, where information about the companies involved in the project and a first generic overview of the system architecture is provided, the paper moves on technical details, identifying in section 4 all the components involved in the project. This section is dedicated to introduce the benefits on merging the Energy@home specification in ZigBee Alliance and the current activities with CENELEC and HGI to standardize a home energy management and control device. Section 5 focuses on use cases and scenarios that are typically involved in a smart grid project, with the aim to generate new ideas to the user in how to integrate or expand different aspects of the smart grids. Finally, the last section is dedicated on security aspects: the ZigBee Alliance adopted a security model based on different levels of security (depending on the hardware resources that a ZigBee node support) and three different methods to transport the keys are presented (the common security models to guarantee frame protection and integrity are illustrated as well).

8 Future Works

In order to become a proper commercial solution, the Energy@home requires more focus on the privacy policies applied by each European Country and all the security aspects related to the transport and storage of those energy consumption data. Also, more sophisticated accesses to the maintenance area shall be considered, since this part is responsible to setup and guarantee the correct usage of the application. On the ZigBee side, the security model adopted is considered to be quite reliable, but some tests in how this model could be attacked could be a good and desirable work.

With the continuous development of the technologies, new kind of devices shall be considered, and this will probably turn into a new cluster or extension of the existing ones, providing extra work to be done in collaboration with the ZigBee Alliance.

However, ZigBee shall not be considered as the only and unique option for this project, and thus as a future work it could be considerable to replicate the whole protocol to other technologies as well (e.g. Wi-Fi and IP networks in general), in a way that the Energy@home project will become technology-independent.

On the certification side, so far the Energy@home project has been aligned to the ZigBee Certification Policies ([4]) due to the alignment with ZigBee Home Automation specification, but for other PHY layers, other options might be considered in the future.

Regarding the use cases, a future enhancement could be the integration of a photovoltaic system: if Energy@home will be able to move most of the electrodomestic consumptions during the absorption peaks, and thus maximize the rate of consumption when a renewable source is active, the user would gain important economic benefits.

Acknowledgements. The authors would like to thank the Energy@home members, active since 2009, with their periodically conference calls, test events, ad hoc meetings and lots of internal works. Thanks also to the ZigBee Alliance, which included the new Energy@home clusters and devices into the Home Automation 1.2 specification.

This work has been partly supported by the European Commission under the EU's Seventh Framework Program (FP7) within the context of the WP4 of the Finseny project (http://www.fi-ppp-finseny.eu/).

References

[1] Energy@home Use cases document, Energy@home association (2012), http://www.energy-home.it/Documents/EnergyHome%20Use%20Cases_v_1_2.pdf

[2] Energy@home Specification document, Energy@home association (2012), http://www.energy-home.it/SitePages/Download.aspx?url=/restricted/Restricted%20Documents/EH_specification_ver0.95.pdf

[3] ZigBee Alliance website, http://www.zigbee.org

[4] ZigBee Alliance, ZigBee Alliance Certification Policy document, doc # 07-4842. Available at ZigBee Website, member's area
[5] Borean, C., Ricci, A., Merlonghi, G.: Document "Energy@home: a "User-Centric" Energy Management System"
[6] BSI British Standards, document BS EN 50523-1:2009, Household appliances interworking - Part 1: Functional specification (July 2009)
[7] BSI British Standards, document BS EN 50523-2:2009, Household appliances interworking - Part 2: Data structures (July 2009)
[8] Robert Cragie, Jennic Ltd., ZigBee Alliance doc. numb 09-5378. Available at ZigBee Website, member's area