Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2012, Article ID 534512, 19 pages
doi:10.1155/2012/534512

Review Article

Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid

Sergio Saponara and Tony Bacchillone

Dipartimento Ingegneria dell'Informazione, University of Pisa, Via G. Caruso 16, 56122 Pisa, Italy

Correspondence should be addressed to Sergio Saponara, sergio.saponara@iet.unipi.it

Received 16 July 2012; Revised 13 November 2012; Accepted 18 November 2012

Academic Editor: Gildas Avoine

This paper discusses aims, architecture, and security issues of Smart Grid, taking care of the lesson learned at University of Pisa in research projects on smart energy and grid. A key element of Smart Grid is the energy home area network (HAN), for which an implementation is proposed, dealing with its security aspects and showing some solutions for realizing a wireless network based on ZigBee. Possible hardware-software architectures and implementations using COTS (Commercial Off The Shelf) components are presented for key building blocks of the energy HAN such as smart power meters and plugs and a home smart information box providing energy management policy and supporting user's energy awareness.

1. Introduction

Smart Grid is the evolution of the current power grid, into a new smarter network [1, 2]. It is a modernization, a reengineering of the electricity delivery system, through the exploitation of information and communication technologies (ICT) for power system engineering. The result should be an intelligent network that can monitor, protect, and optimize the operation of all its nodes, from the central and distributed generator layer to the end users [3–6]. The primary purpose of this innovation is to increase energy efficiency, reliability, and sustainability to address the growing electricity demand and to mitigate the climate changes reducing gas emissions. Thanks to continuous monitoring of all power grid nodes and the interconnection with classic ICT networks, Smart Grid may be used to increase the energy awareness of the society suggesting and stimulating "green behaviors."

This paper discusses aims, network architecture, and security/privacy problems of a Smart Grid in Section 2. Moreover some solutions are proposed in order to define a high-level architecture implementing privacy and security techniques in the grid.

From an ICT point of view a Smart Grid is a "network of networks" including wide area network (WAN), local area network (LAN), and home area network (HAN), going from the energy generation side to the customer's premises side. Particularly, a proper design of the HAN must ensure both customers' privacy and energy efficiency of the system. Sections 3 and 4 focus on a possible realization of an energy HAN, following the recommendations of the SEAS (Supporting Energy Aware Society) proposal by a team of Italian institutions. The aim of SEAS is the development of a high-level architecture to realize a HAN, that allows users to control their energy consumption remotely and to optimize the activities of the appliances within the network. After discussing a possible energy HAN topology, which exploits the ZigBee protocol for wireless node connectivity, the hardware architecture of the main building nodes is discussed (smart meters [7] and plugs plus a home smart information box providing energy management policy and supporting user's energy awareness). Possible implementations of such nodes, based on COTS (Commercial Off The Shelf) components, are also presented.

2. Smart Grid Aims, Architectures, and Security

2.1. Limits of Existing Power Grid and Challenges of Smart Grid. The typical structure of the existing power grid is

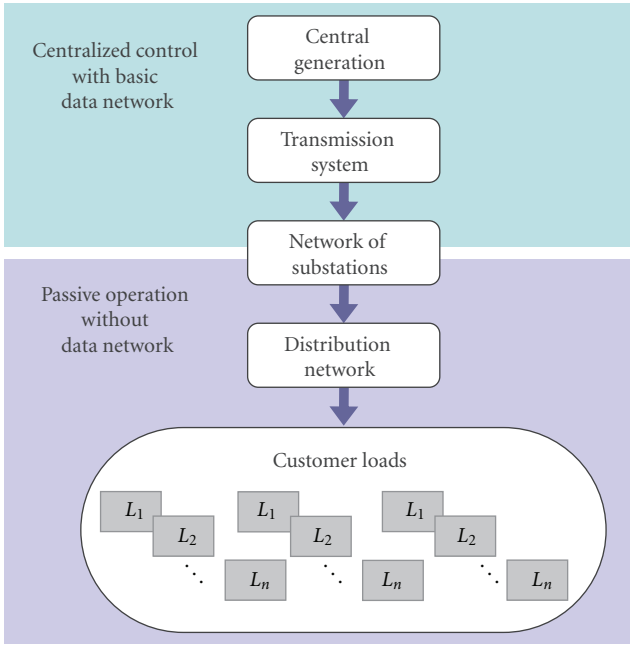


Figure 1: Structure of existing power grid.

shown in Figure 1. Utility companies all around the world designed their power grid imposing clear demarcation between its main subsystems: generation, transmission, and distribution systems. This approach has brought different levels of automation in the various subsystems, and each subsystem has separately experienced different evolutions and transformations. Moreover, the hierarchical structure of the grid can cause domino effect failures.

In term of efficiency, along the existing grid there is waste of energy in various forms: only one-third of fuel energy is converted into electricity (and waste heat is not recovered), 8% of the produced energy is lost along transmission lines, and 20% of the generation capacity exists only to support a potential peak demand [1]. This last point is very important. The existing grids are actually over-engineered to stand maximum peak demand, that are very infrequent, limiting therefore the whole system efficiency.

Moreover, present electricity grids are mainly unidirectional: generators produce energy and distribute it to the lower level, with very few information about grid status and end users energy consumption. Typically, the electric power source has no real-time information about service parameters of termination points and cannot control energy production according to the real request of the grid. The new challenges for present grids can be summarized in five main points.

(i) Introduction of new forms of power generation, in particular those using renewable energy sources such as wind, sun, and biomass. These type of generators have intermittent and small outputs and need therefore a different management from traditional generators.

Table 1: Smart Grid innovations versus existing power grid.

Existing grid	Smart Grid
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Hierarchical	Network of networks
Few sensors	Sensors throughout
Blind	Self-monitoring
Manual repairing	Self-healing
Failures and blackouts	Adaptive and islanding
Manual check/test	Remote check/test
Limited control	Pervasive control
Few customer choices	Many customer choices

(ii) Need of uninterrupted electricity supply.

(iii) Need to decrease peak demands during the day and to reduce energy waste to ensure adequate energy reserves.

(iv) Diffusion of new digitally controlled devices able to change the behavior of the electrical load (e.g., switching itself on or off), smart power meters, and energy control units implementing energy management strategy and improving energy awareness of users.

(v) Security threats, that involve not only the electricity supply but also cyber attacks [8, 9].

The evolution towards the Smart Grid begins with innovations in the existing grid by incorporating new ICT technologies in many point of the infrastructure. Table 1 shows the main differences between existing grids and Smart Grid. The starting point of this revolution is the bottom layer of the system, the electrical distribution subsystem. The first step is the insertion of distributed and networked monitoring and control systems in the electrical grid. Such systems can assist utility companies in grid monitoring and can identify potential risks, taking corrective actions in time. Secondly a complete overhaul of the ICT infrastructure is required. Communication and data management will provide a layer of intelligence over both the existing grid and the future infrastructure, allowing the introduction of new applications. This organic growth of the grid allows companies to gradually shift old grid's function into the new grid and consequently to improve their critical services.

The change of the unidirectional approach of the classic power grid with the bidirectional one introduced by the Smart Grid concept can favour the diffusion of distributed generators or cogenerators, along the existing grid. Indeed, Smart Grid can provide an easier integration of alternative sources of energy (i.e., sun, wind, etc.) characterized by time-varying energy production level with storage systems, in order to fill the gap between when/where the energy is produced and when/where the energy is required. Smart Grid can aid utility companies to make a more efficient use of the existing infrastructures, introducing step by step some

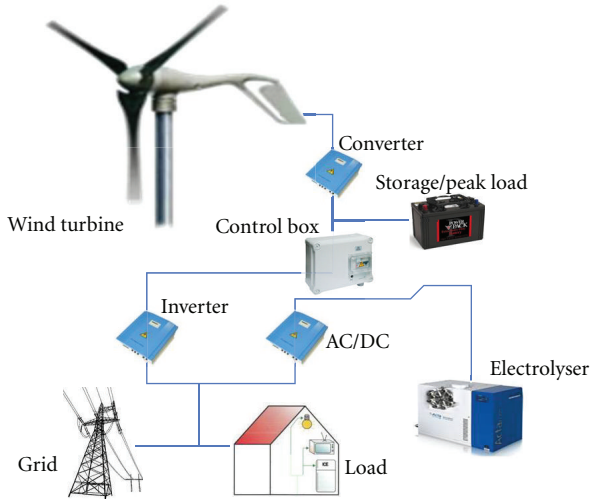


Figure 2: NanoCatGeo microgrid developed at University of Pisa.

key features as demand response, peak shaving, and service quality control [1].

The evolution of the grid requires the coexistence between Smart Grid and existing grid [10]. This permits the gradual growth of the grid, increasing step by step its capacity and adding new capabilities. A way to perform this evolution is the introduction of microgrids [11] which are networks of distributed energy systems, loads, and generators, that can work connected to the grid or not. They can be, for example, houses or factories, having their own local energy source, that want to optimize their energy consumption.

An example of a microgrid has been developed at University of Pisa in the framework of the NanoCatGeo project [12] in collaboration with industrial partners such as Acta Energy and Edi Progetti, see Figure 2. The idea was to develop a micro Smart Grid for wind-based energy autonomous homes located in windy zones. In the system a wind energy source (nonconstant energy production) plus an AC/DC converter provides energy on a DC bus wherein are also connected: (i) an inverter DC/AC system to power the home or sell any excess production to the energy utility company; (ii) an AC/DC converter to supply an hydrogen electrolyzer [13] to store in the form of hydrogen any excess when the wind electrical energy production is higher than the users' needs and to obtain energy back from hydrogen when the wind energy production is lower than users' consumption. All the subsystems of this Smart Grid are interconnected (wired) through a control box, implementing energy management strategies; the control box is based on a low-power microcontroller [14, 15], for example, an 8051-like core plus RS485 and CAN interfaces.

2.2. Smart Grid Network Architecture. Smart Grid can be viewed as a network of networks, see Figure 3. Starting from the customer side, the HAN is the network of communicating loads, sensors, and appliances within the customer's premises. Customers are connected to the energy distribution level through a LAN. LAN identifies the network of smart power meters, gateways, and elements in the distribution system. Last, we find the WAN. This is the network of upstream utility assets that include power plants, substations, distributed storage, and so on. Substation gateways interface WAN and LAN networks.

2.3. Security and Privacy Problems in Smart Grid. Since the existing grid is moving from a centralized network to a dynamic peer-to-peer network, with a growing complexity, it is also becoming more vulnerable to local and global disruptions. Smart endpoints introduced into the network become portals for intrusion and malicious attacks. Moreover, Smart Grid is growing over systems not designed with security criteria, thus with significant security holes [8, 16, 17]. Security problems do not involve only cyber security aspects, but it concern also failures in the grid and protection against natural disasters. The following is a list of potential risks for a Smart Grid:

(i) the complexity of the grid increases accidental errors and possible points of intrusion;

(ii) the deployment of new technologies can introduce new issues in the network;

(iii) the presence of many network links increases potential cascading failures and gives more opportunities to compromise the system;

(iv) smart nodes can be vulnerable entry points for denial of service (DOS) attacks.

Particularly, the focus of Smart Grid security is on the HAN: indeed WAN and LAN in Smart Grid are known computer networks whose security issues are widely discussed in literature. The HAN network is deployed into the customer domain, and its security is a critical point strictly related with customer's privacy.

A typical HAN is composed of four elements.

(i) A gateway that connects the HAN network to the outside information services, in the LAN or WAN network.

(ii) The access points or network nodes composing the HAN network.

(iii) A network operating system and a network management software.

(iv) Smart endpoints, such as smart meters, displays, refrigerators, appliances, and thermostats.

So far, many technologies have been considered in order to implement the HAN by different groups and organizations. The most significant standards are ZigBee [18], Z-Wave, Insteon, and Wavenis. They are all standards for wireless networks. The main features of these standards are presented in Table 2. Talking about security, if present, similar encryption algorithms are used by them: AES and in some cases 3DES. AES is the most reliable encryption algorithm between them [9], and its implementation (hardware and software) offers better performances than 3DES. Moreover, AES encryption can be performed using ad hoc

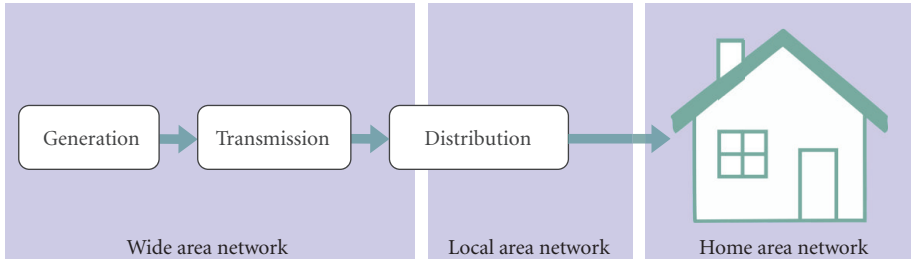


Figure 3: Smart Grid network hierarchy.

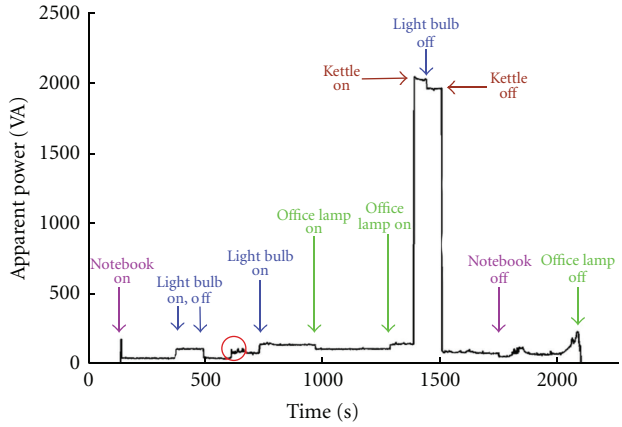


Figure 4: House electricity demand and information extracted: apparent power (Volt ∗ Ampere) for notebook, lighting sources, and a kettle [29].

Table 2: HAN standards and security algorithm, main characteristics.

	ZigBee	*Z*-Wave	Insteon	Wavenis
RF band, MHz	868/915/2400	868/908/2400	904	433/868/915/2400
Range, m	10–100	30–100	45	200–1000
Bit rate, kbps	20/40/250	9.6/40/200	38.4	4.8/19.2/100
Message size, bytes	127	64	14–28	NA
Security algorithm	128 b AES	128 b AES	NA	3DES/128 b AES

AES hardware, that is, an AES coprocessor, which is present in many of the solutions proposed for implementing HAN networks. In the example network proposed in this paper, and ZigBee standard will be used. ZigBee security issues will be discussed in detail in Section 4.

From the customer point of view, a fundamental requirement is the protection of the information exchanged between the utility company and the smart power meters installed at the customers' premises. Far from old electromechanical measuring systems, the new generation of power meters is fully electronic [19–24], and they provide advanced power measurement and management capabilities thanks to power Application Specific Integrated Circuits (ASIC) provided by semiconductor suppliers like STMicroelectronics [25]. The new generation of smart meters integrates a two-way communication system. In particular, power consumption data are transmitted over low-voltage power lines, using packet-switched digital power line communication standards [26], from the customer's premises towards data concentrators, based on Echelon technology [27]. On the other side, from each data concentrator point, information is sent to the servers of the utility company using the Internet network. Vice versa, the utility company can easily operate on remote smart meters by accessing through internet the data concentrators and from them, though power line communication over low-voltage residential power lines, the smart meters at the customers' premises. This way the utility operator can turn power on/off to customers, read usage information, change customer's billing plan, and also detect service outages or unauthorized electricity use.

Power line communication is based on the following idea. AC power is transmitted over high-voltage transmission wires at 50–60 Hz, so it is possible to impress a higher frequency signal carrying digital information in both directions (from customers' premises towards the utility company and vice versa). The carrier used for data transmission in power line communication has generally a frequency of about 100–200 kHz, for data rates of few Kbps, so that data signals can be easily separated from power ones. More details on power line communication in Smart Grid and the relevant packet formats and standards can be found in [27].

However, consumption records obtained through the smart meters can reveal a lot of information about customer's activities, thus it is important to satisfy some requirements in terms of *confidentiality*, *integrity*, and *availability*.

Confidentiality deals with information protection from unauthorized access. It is a customer side requirement. In Smart Grid, the focus is on data stored in the utility companies servers and transmitted from customer's smart meter. These data contain energy usage information and billing data. To protect them, it is important to properly implement the least privilege principle: a user has no more privileges than necessary to perform its function. A detailed guide for implementing security in the organization data server, that follows this principle, can be found in [28]. The protection of these confidential data assures customer's privacy. In fact, energy usage information reveals user

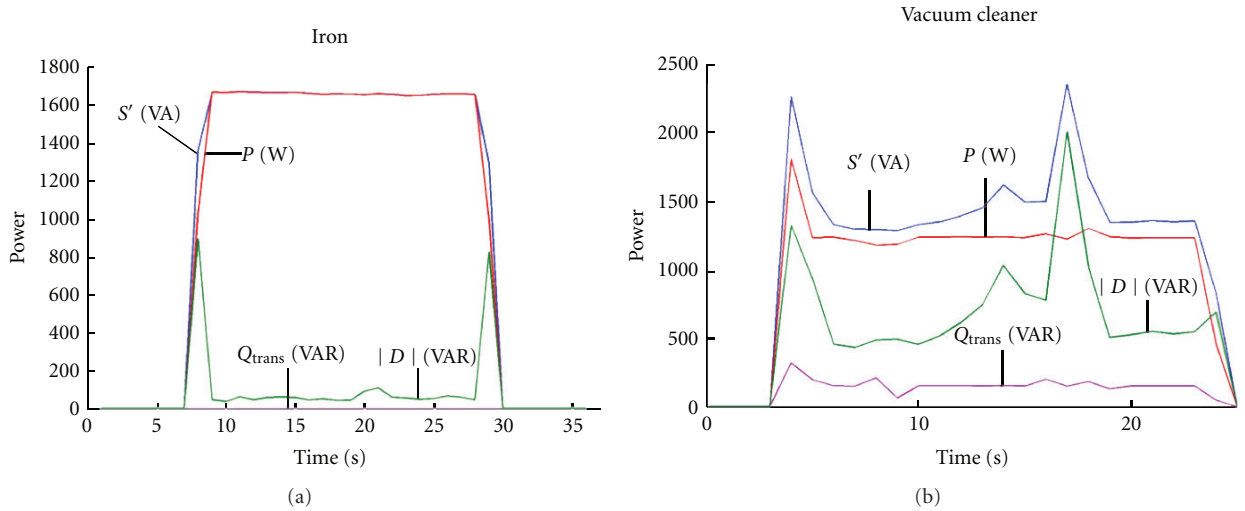


Figure 5: House electricity demand and information extracted: real power P, apparent power S, and reactive power D of an iron (a) and of a washing machine (b) [29].

activities during the day, allowing to deduce what kind of device or appliance was in use at a given time. In the literature there are a lot of load signature algorithms, results of NALM (Nonintrusive Appliance Load Monitoring) research branch [24, 29], that can extract detailed information from electricity usage records. An example of the results of these algorithms, over real consumption records, is shown in Figures 4 and 5. Signature of the usage of a specific power appliance can be extracted considering typical power consumption of the load, frequency of use, and transient response since different appliances have different load types: nonlinear resistors for heaters and bulb lamps, inductive for electric motors, reactive for microwave oven, and diode like for led lights.

Integrity ensures the correctness of information protecting data against modification attacks. A countermeasure to prevent this type of attack is based on the access control. With this, only authorized users can modify the information.

Availability ensures that services are always available to users. Security must prevent out-of-service due to human factor or DOS attack against utility companies that can compromise power distribution. Redundancy is a good practice to prevent environmental threats.

2.4. Practice to Secure the HAN in Smart Grid. In information technology, there are a lot of codes and rules in order to achieve the security requirements emphasized. An example is ISO/IEC 27000 series, a set of standards of certified best practices for information security [30–32]. Another security program, not certified, is the Information Security Forum (ISF) [33]. ISF is a nonprofit organization that distributes the Information Security Forum's Standard Of Good Practice free of charge.

These guides can be applied to ensure information security for every kind of systems, including Smart Grid and particularly for the HAN which is the main focus of this paper. A code of technical practice for security in the HAN of a Smart Grid can be summarized in the following twelve points.

(1) *Threat Modeling.* Possible threats must be identified, for preparing proper countermeasures. This study can be conducted analyzing use case versus abuse case.

(2) *Segmentation.* To minimize the impact of attacks, segmentation can be adopted limiting, for example, data traffic in specific area through a firewall: attack damage would be confined to such area.

(3) *Firewall Rules.* Proper rules must be used for firewall, proxy server, and content filtering.

(4) *Signing.* Software codes running in the grid have to implement digital signing. This allows the execution only of trusted applications and ensures integrity of the information exchanged within the Smart Grid.

(5) *Honeypots.* The deployment of honeypots, traps for hackers, permits identification of a new type of attack and alerts organizations in time. Thus, honeypots show weakness and security hole of the system. These elements can be placed in the Smart Grid environment and in its peripheral areas.

(6) *Encryption.* Through the encryption algorithm, sensitive information is protected from unauthorized disclosure. Encryption must be adopted on the transport layer, on the archived data and in the control network.

(7) *Vulnerability Analysis.* Utility companies have to create control centers to analyze network traffic and systems to identify any exposures that increase vulnerability to attacks.

(8) *Penetration Testing.* Beside vulnerability analysis, simulating an attack usually done by a malicious

Table 3: IEC 62351 core standards.

Core standard	Topics
IEC 62351-1	Communication network and system security introduction
IEC 62351-2	Glossary of terms
IEC 62351-3	Profiles including TCP/IP
IEC 62351-4	Profiles including manufacturing message specifications (MMS)
IEC 62351-5	Security for IEC 60870-5 and derivatives
IEC 62351-6	Security for IEC 61850
IEC 62351-7	Network and system management (NSM) data object models
IEC 62351-8	Role-based access control

hacker on the Smart Grid must be performed periodically; this way a snapshot of the effectiveness of the Smart Grid security can be obtained.

(9) *Source Code Review.* Smart Grid applications must present no vulnerabilities. Thus, their source code must be reviewed carefully in order to meet high-quality requirements. After the identification of vulnerabilities in the code, these can be fixed.

(10) *Configuration Hardening.* All the elements of the Smart Grid, especially smart endpoints, have to be tested before their deployment. This can be done with vulnerabilities scanners and benchmarking tests.

(11) *Strong Authentication.* There are three main types of authentication methods: something the user knows (e.g., password), something the user has (e.g., hardware key), and something the user is (e.g., biometric id). At least two of these methods must be used.

(12) *Logging and Monitoring.* They are powerful tools for providing information for attack identification and for reconstructing events in case of natural disasters. Starting from stored data, data-mining techniques and signal processing analysis give important information about attacks and grid behavior during certain events. However, if not correctly managed, data logging could represent a further backdoor into the system. For this reason it is important to define an accurate log planning process including log management planning, policies, and procedures taking into account security issues [34].

This set of practices can be also used as a backbone for the development of future Smart Grid standards.

2.5. Security Standards and Proposed Solutions for Smart Grid. Several associations and groups in different countries have developed many standards for security in Smart Grid. The IEC 62351 standard, developed by the International Electrotechnical Commission (IEC), is one of them. This standard concerns power system management and associated information exchanged and is divided in eight core standards, reported in Table 3. The scope of the IEC 62351 standard is information security for power system control operation [35]. In Table 3 other two IEC standards are mentioned: IEC 60870 and IEC 61850. The first one, the IEC 60870 standard defines system used for telecontrol. Part 5 of this standard deals with communication between nodes directly connected. IEC 61850 is an electrical substation automation standard for modelling data, reporting schemes, fast transfer of events, setting group, sample data transfer, commands, and data storage.

NIST interagency report 7628 for cyber security in Smart Grid is another important document [36]. This report contains a framework for cyber security risk management, a list of requirements for power meter security, and a discussion about privacy and Smart Grid. Moreover, this document contains power system use cases for security requirements and bottom up security analysis of Smart Grid.

Besides these standards, in literature there are some solutions and models proposed for implementing security in Smart Grid. One of the most interesting solution is based on public key infrastructure (PKI). This is based on the fact that security and privacy technologies use a key to encrypt and protect data, in order to meet the desired security requirements. The problem, in a large network as a Smart Grid, is the key management system. The PKI proposed is composed of five main elements:

(i) PKI standards;

(ii) Smart Grid PKI tools;

(iii) device attestation;

(iv) trust anchor security;

(v) certificate attributes.

PKI standards would be used to determine requirements on the PKI operations of energy service provider. PKI, however, is notoriously hard to deploy and to use, due to the fact that PKI standards provide only high-level framework, and leave to companies the detailed implementation. Smart Grid PKI tools give users an easy way to manage the infrastructure and enable the development of future applications, which meet PKI security requirements. An important feature of these tools is to eliminate the need of symmetric key configuration, which is an insecure and expensive process. In a secure system, each component must be a trusted component. Device attestation techniques are used to identify devices and to find out if the device has been tampered. Within a network based on PKI infrastructure, an important aspect is the management of devices' certificates. These certificates can be organized in trees, and the root is called Trust Anchor (TA). It is important to secure operations on TA: loading and storing, identification, management of local policy database (a set of rules defining how a device should use its certificates, and what type of certificates it should accept), and so forth. It is essential in Smart Grid that any device in the network can determine the authorization status of another device and authenticate it. This can be done using the attributes present into the certificate and contacting a security server. Therefore, it is important to distribute local security servers in various part of the network and not to rely only on a back-end server (single point of failure problem).

The solution proposed is only a high-level description of how security and privacy can be achieved in Smart Grid, and many problems may come out during the implementation of a PKI infrastructure. Some of these problems were discussed previously (i.e., need of distributed authentication servers, implementation of PKI standards, secure management of devices certificates, etc.).

Alternatively, the PAKE (password-authenticated key exchange) research [37, 38] explores an approach to protect passwords without relying on PKI at all. PAKE aims to achieve two goals. First, it allows zero-knowledge proof of the password. One can prove the knowledge of the password without revealing it to the other party. Second, it performs authenticated key exchange. If the password is correct, both parties will be able to establish a common session key that no one else can to compute.

As far as privacy of the customers is concerned, a possible solution is based on the anonymization of smart meters data. The idea is to distinguish smart meters data on the basis of their generation frequencies.

(i) High-frequency data sent by smart meters to utility data concentrators in order to control power generation and distribution network and to enable a real-time response to power quality. These data do not need to be attributable to a particular customer and are sent, for example, every minute.

(ii) Low-frequency data sent to utility company, for billing and account management. These data must be attributable to a customer or an account and are sent every day/week/month.

Only high-frequency data are "anonymized," because of their sending rate. A smart meter, using this technique, has two ID for its message: an HFID for high-frequency data, and a LFID for low-frequency data. The method proposed ensures the anonymity of the HFID, thus of high-frequency messages. The utility company and customers know only their LFID, and the HFID is known only by the manufacturer of the smart meter, that so it is the only one that has the correspondence between LFID and HFID. The HFID for example can be hardware encoded. This solution, however, considers only data sent from smart meters. The limits in terms of security of an approach similar to the proposed one (HFID and LFID correspondence is known by the smart meter manufactures and stored in its archives) are discussed in [39].

3. Home Energy Network Possible Implementation

3.1. Home Energy Network Architecture. This section presents a possible implementation of a home area network for smart energy management, discusses security issues, and analyzes some commercial hardware/software solutions for its implementation. The network proposed is derived from the experience gained in Smart Grid projects proposal in Italy such as the Energy@Home project [40], carried out by industrial partners such as Electrolux, Enel, Indesit and Telecom Italia, and the SEAS proposal, by Italian academic partners. The aim is to develop a communication infrastructure, for exchanging information related to energy usage, consumption, and tariffs in the home area network.

The general architecture of the smart energy HAN is presented in Figure 6. The HAN network contains a smart information box called Home Energy Angel, realized as an electronic control unit with on-board memory, computing capabilities (32-bit microprocessor with nonvolatile, SRAM, and SDRAM memories) and digital networking interfaces.

The Home Energy Angel box implements these main functions:

(i) collecting data from the power meters and from the smart endpoints in the home domain, monitoring the energy sources (from the electricity provider or from local renewable energy sources such as photovoltaic panels or wind-based systems), the energy loads (recharge point of electric vehicles if any, lighting, air conditioning, household appliances and infotainment devices), and the energy buffers (Li-ion batteries or H2-based energy storage [13]);

(ii) collecting data through the HAN from environmental sensors (temperature, light, and humidity);

(iii) forecasting of users' needs, based on data provided by sensors and by profiling methods;

(iv) sending commands to smart appliances according to preprogrammed strategies to implement power saving strategies (e.g., turn off/on lights adaptively on the environment conditions, proper time programming of washing machines or oven to avoid peak consumption,...),

(v) providing information to the users about their energy behavior through their tablet PC or smartphones.

Beyond the Home Energy Angel box, a home gateway is also connected to the HAN. This provides internet access for users through a Wi-Fi network. The home gateway is the interface between the HAN and the WAN network (internet in this architecture). Users can obtain information about home consumption contacting the Home Energy Angel information box through the home gateway, using a simple internet connection or locally using the connected interfaces on their tablet, laptop, or smartphone. The Home Energy Angel smart information box provides energy services to make customers aware about their energy consumption. These services are automatic load management, energy efficiency, active demand service, and networking with smart appliances.

A graphical user interface (GUI) will be developed for the Home Energy Angel, enabling a better user experience of the whole system. The GUI will be designed for two main purposes. Firstly, users will be able to easily provide information on their preferences in using the energy at home (i.e., on the appliance that they are willing to use, on the time window to start/stop each device). Secondly, it will be used to visualize the optimal energy plan calculated by the Home Energy Angel and to access additional information

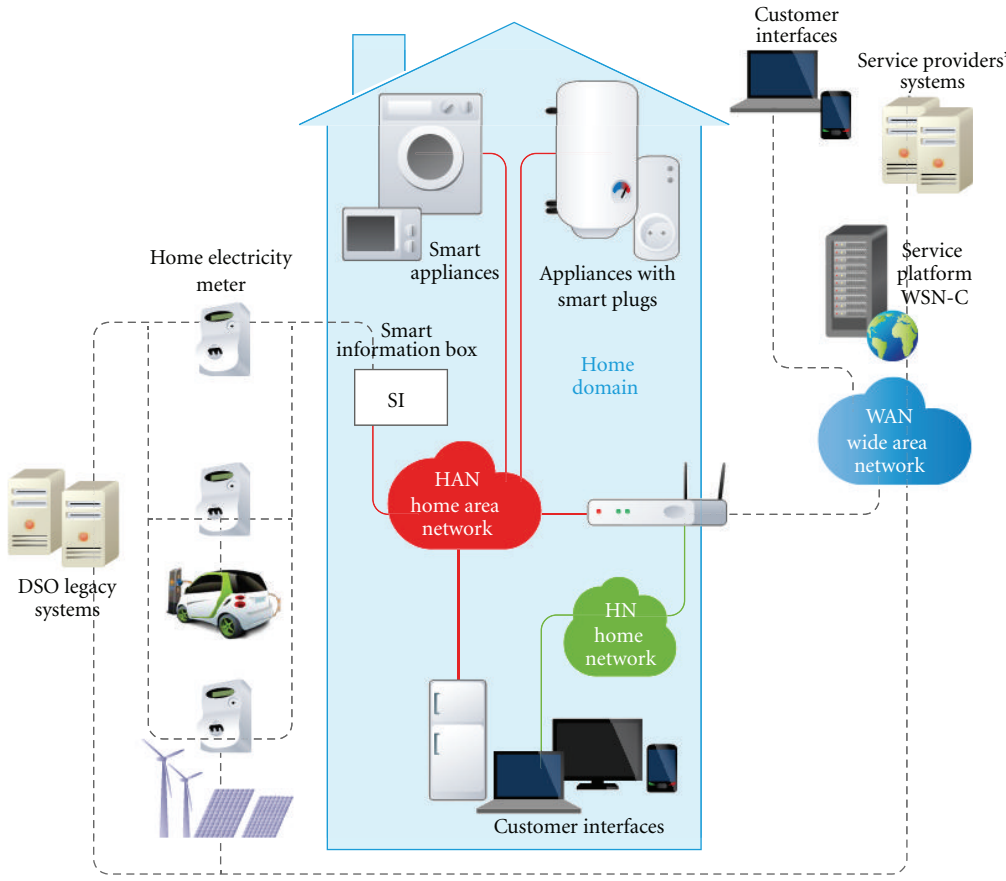


Figure 6: Smart energy HAN general architecture.

such as the load consumption profile, costs, or statistical data, thereby settling the general lack of awareness people have of their energy consumption.

The proposed Home Energy Architecture will provide benefits in terms of the following.

(i) Provide an easy-to-use support to optimize the production and consumption of electricity, reduce electricity cost, and minimize electricity waste.

(ii) Increase user awareness on energy consumption/saving.

(iii) Improve the grid efficiency by leveling peaks in the demand.

Energy consumption information, collected by meters, can be sent directly to the Distribution System Operator servers (DSO legacy systems in Figure 6) exploiting power line communication protocol instead of using the HAN connection.

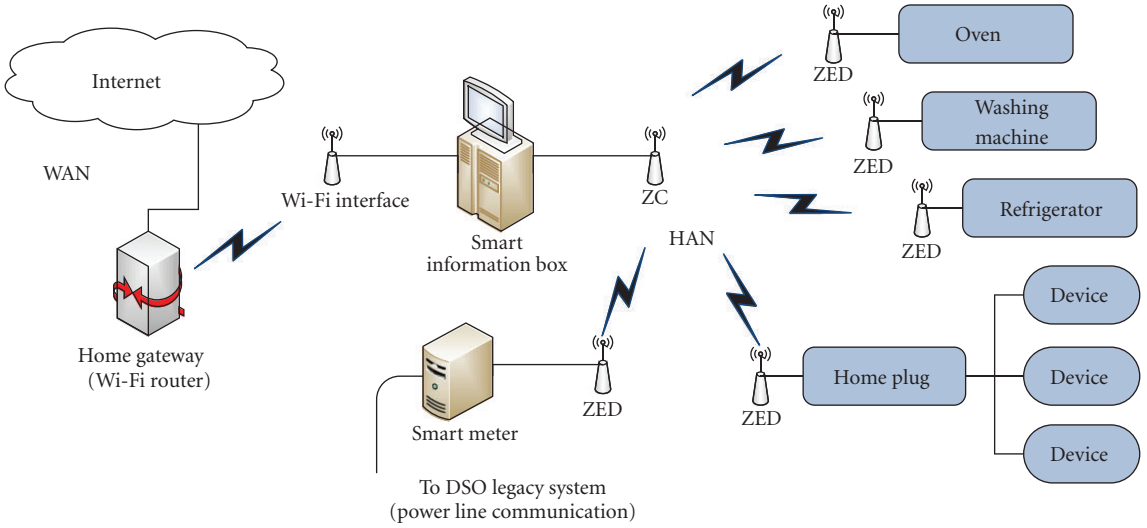
In the architecture detailed in Figure 6 there is another particular element: the smart plug. Smart plugs (or home plugs) are systems able to add intelligence to old generation devices. They are simple socket points with a wireless connection (e.g., ZigBee) providing consumption monitoring of the connected devices. Smart plugs can also control the status of the connected devices (powering them on/off, i.e., are intelligent power switch [41]) sharing the power among them.

The system architecture of the network is shown in Figure 7. A possible implementation of this system uses a ZigBee network for realizing the HAN. Within the network there is a smart information box, connected to the HAN through a ZigBee transceiver and equipped with a Wi-Fi interface for contacting the home gateway. The home gateway is a simple Wi-Fi router. The role of the smart information box is to collect data from the HAN to compute them using information coming from the internet network (customer's tariff, billing account information) and to present them by means of a user-friendly interface.

The home gateway acts as an interface between the WAN (internet) and the HAN. A Wi-Fi router can play this role: the smart information box can be accessed remotely from users and can easily contact the utility service servers. In the example of Figure 7 there are four smart appliances: an oven, a refrigerator, a washing machine, and a smart plug; together with the smart information box and the smart meter transceiver, they form the HAN.

ZigBee protocol assigns a role to each node into the network. There are three possible roles.

(i) ZigBee coordinator (ZC): it is the smartest device in the network. The coordinator node is the root of



ZED: ZigBee end device.
ZC: ZigBee coordinator.

Figure 7: Smart energy HAN architecture implementation example.

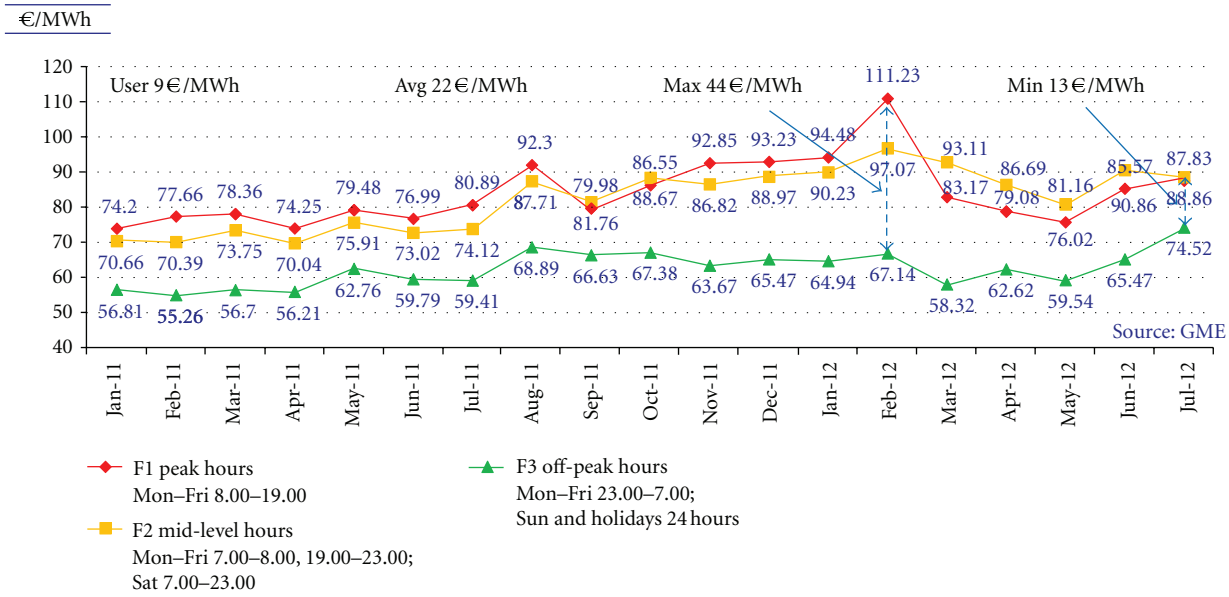


Figure 8: Cost of energy in different time ranges in Italy.

the network and can also act as a bridge between different networks. It can contain information about the network as well as store the security keys. In each ZigBee network there is only one coordinator. The smart information box is the ZC of the example network of Figure 7.

(ii) ZigBee router (ZR): it acts as router in the network, exchanging data between nodes (not present in the example network of Figure 7).

(iii) ZigBee end devices (ZEDs): they are the simplest nodes of the network, and they can communicate only with the coordinator or routers. ZEDs require little amount of memory. The devices in the network of Figure 7 are all ZEDs, and they communicate only with the smart information box.

It is worth noting that ZigBee is not a protocol for peer-to-peer networks (i.e., networks composed by nodes that have all the same role and where there is no distinction between them). ZigBee instead assigns a role to each node, and ZEDs cannot communicate directly, but only through a router or coordinator. Using routers within ZigBee network allows the deployment of a network architecture similar to mesh network.

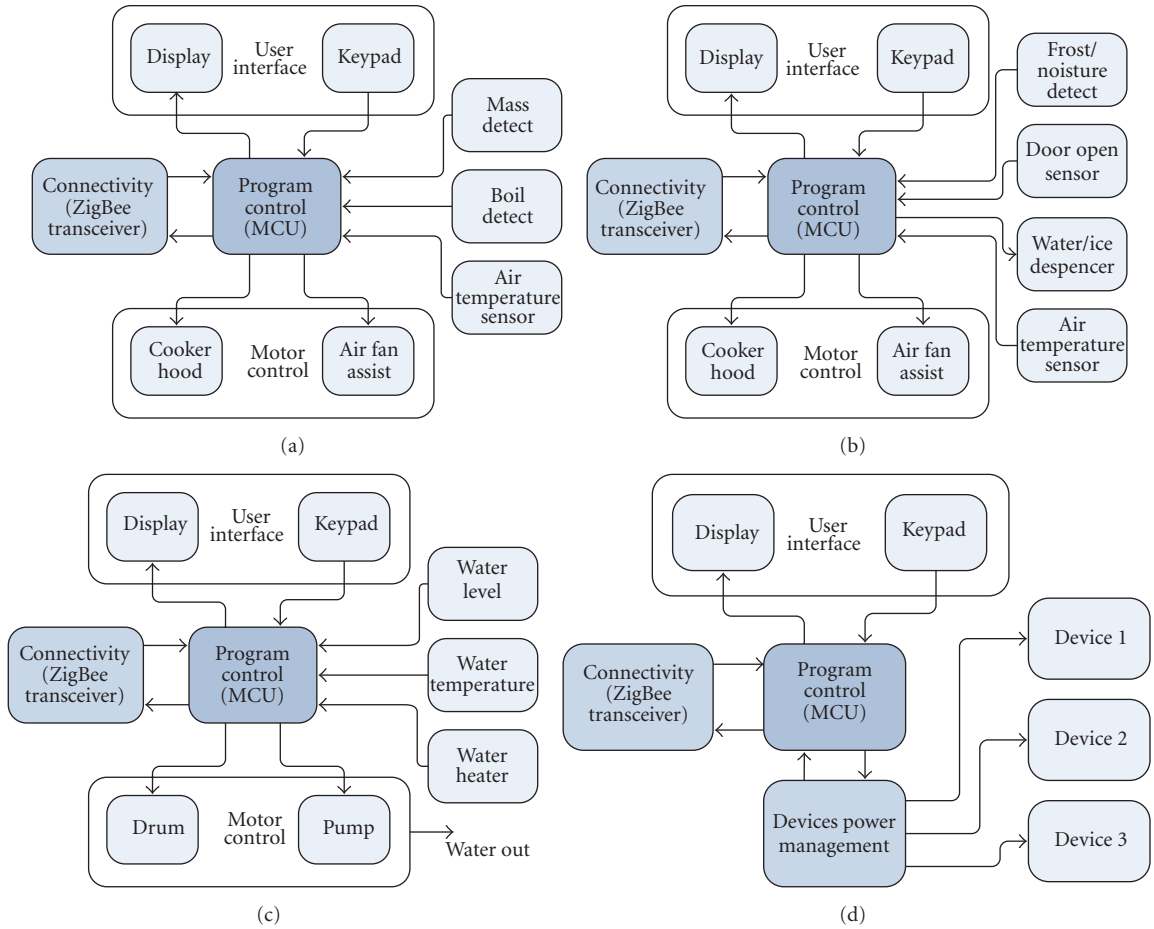


Figure 9: Oven (a), refrigerator (b), washing machine (c), and home plug (d) system diagram.

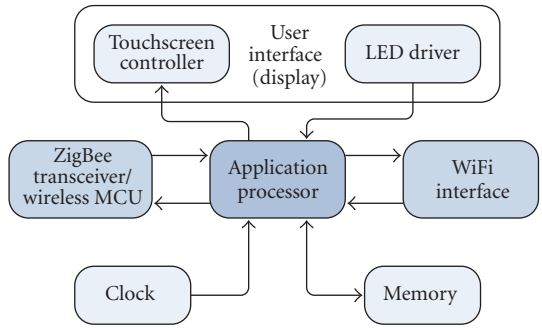


Figure 10: Architecture of the Home Energy Angel smart box.

Moreover the Home Energy Angel in our vision is a smart device that runs applications specific for energy management. It is a point of presence for every smart device within the home domain and for third party's domotic solutions. For our purpose, the Home Energy Angel smart information box can integrate also the Wi-Fi router to provide an internet access to users. In such a case all the applications for network and energy management run on the Home Energy Angel smart information box, that acts also as a gateway.

Implementing the proposed energy HAN will allow energy saving and cost saving benefits for the end users.

As discussed at the last SustainIT2012 conference in several papers [42–44] in Europe the household contribution to the overall electricity consumption is about 29% corresponding for a country like Italy [44] in 70 TWh per year, 12 billions of Euros of cost, 2.5 MWh/user per year. Simulations carried out considering the power cost of typical house appliances, and the consumption profiles of typical users allow the following estimation: the introduction of

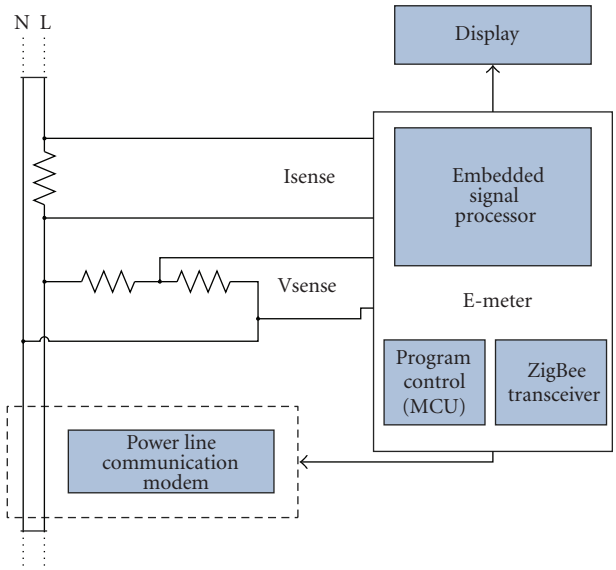


Figure 11: Architecture of the smart meter.

the energy HAN, supporting energy awareness of users, and implementing automatic energy management policy can reduce the user consumption per year by 20% from actual 2.5 MWh to 2 MWh.

A further cost saving can be achieved, thanks to the HAN, by enabling users to automatically exploit the high variability of energy cost which, as reported in Figure 8, can vary by a factor 3 from peak hours (F1 tariff in red in Figure 8) to off-peak hours (F3 tariff in green in Figure 8).

3.2. HW Architectures of Building Nodes: Smart Plugs, Home Energy Angel Box, and Smart Power Meters. Figure 9 shows the block diagrams of smart devices present in the example network. Every device has a microcontroller (MCU) core, for example, a 32-b RISC Cortex managing system activities, and an interactive user interface. The connectivity module enables them to join the network and to be remotely controlled. This subsystem can be a simple transceiver integrated with the MCU in the same PCB board, or a single-chip wireless microcontroller can be used.

An example of stand-alone ZigBee transceiver is the Texas Instruments CC2520. In the solution that integrates the wireless microcontroller and the transceiver in the same chip, the antenna can be directly printed on the PCB board achieving enough gain with a limited size, as demonstrated by recent works done at University of Pisa where multiloop multifrequency antennas have been realized as PCB-printed antenna for sub GHz applications [45, 46].

Both solutions can be used to upgrade the existing device's design enabling them to join home area networks. If we use a transceiver, the existing microcontroller could be connected to it using GPIO (general purpose input/output) and SPI (serial peripheral interface) lines. However, this introduces an overhead to the device MCU, that now has to control the system and to implement the communication protocol. On the other hand, using a wireless microcontroller avoids this problem. Actually, a wireless microcontroller can be used as coprocessor, placing it side by side with the device MCU in charge of the system control. The wireless microcontroller implements the communication protocol and manages the transmission and the reception of packets, while the other MCU continues implementing the control algorithm, and when it needs to communicate with other devices in the network it sends a request to the wireless microcontroller. The overhead introduced by this scenario is limited.

The architecture of the Home Energy Angel smart information box is shown in Figure 10. A touchscreen display (in-home display) provides an easy way for users to interact with the smart box. Through this display the user can manage the energy settings of the devices connected to the HAN network and can check the energy consumption records. An external permanent memory is needed to store past records, files for software running on the smart information box and any significant information about the network. The smart information box needs a connection to internet in order to retrieve information about customer energy account, that are used by energy management applications. For that reason there is a Wi-Fi interface connected to the device MCU.

Figure 11 presents the block diagram architecture for the smart meter to be installed by utility companies (e.g., ENEL in Italy). The core of the smart meter is represented by the electronic meter (E-meter), able to calculate the energy consumption by sensing current and voltage from the electric network through an analog front end. This information is digitized and elaborated by an MCU equipped with digital signal processing capabilities (e.g., a 32-bit Cortex processor), and then presented through a display. Also a power line communication modem is connected to the meter in order to send usage information to data concentrators. The extension required with respect to the current state of the art is the ZigBee transceiver. This component enables communication with the smart information box, so users can check their real-time consumption. The smart meter can also store consumption data into its memory for later use.

The described smart meter is the result of an evolution started from AMR (automated meter reading) systems. These meters allow utility companies to read consumption records, status, or alarms occurred. AMRs provide only one-way communication: utility companies cannot take corrective actions on the customer grid.

The evolution of AMR is the AMI (advanced metering information) meter whose hardware architecture has been detailed in Figure 11. AMI is characterized by a built-in two-way communication system, allowing the modification of customers' service level parameters. In this way customers can control energy cost choosing between different billing plans. However, as recognized in the state of the art, deploying a high number of smart meters in the environment is cumbersome. To reduce the number of deployed power metering devices without affecting the information reliability new approaches have been investigated, that is, load disaggregation for extracting individual appliance power consumption information from single-point circuit-level measures. Such approach is based on the observation that

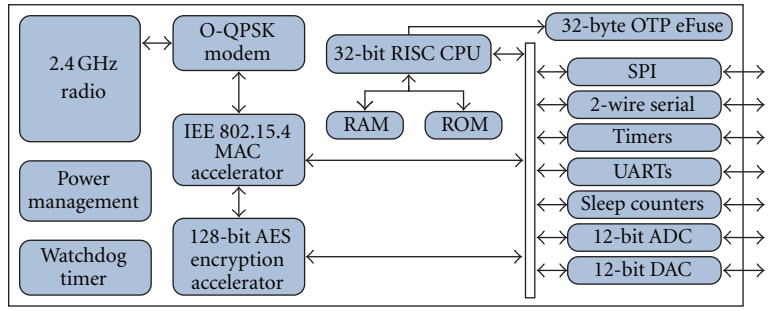


Figure 12: SoC architecture for wireless sensor networks in energy HAN.

each appliance has its own power consumption profile over time, as proved in Figures 4 and 5, which can be isolated from the single-point measure. Disaggregation aims to extract the signatures of the different appliances from the aggregate measures. With respect to the state of the art, where artificial neural networks [47] or a Bayesian approach [48] have been used to perform the appliance recognition, we aim at avoiding the training phase. To this aim we propose adopting a coarse description of the appliance "energy signatures" (i.e., how each type of appliance works and therefore its power consumption in any possible state) and recognize most of the appliance types used in a residential building by indentifying which unit is active, how long and how much is consuming. To this aim, the advanced hardware architecture proposed in Figure 11 is needed, since both a smart analog front end for the power meter measure (E-meter) and a powerful processing unit (the embedded signal processor) are required to implement the disaggregation DSP algorithms. Moreover the smart meter supports communication by wireless connection with the home area network and by power line communication with the main energy grid.

For antitapering reason a 3-axis tilt sensor is also integrated in the smart meter architecture and is connected to the Zigbee and the power line communication interfaces (i.e., if the smart meter is tampered, the end user and/or the utility is notified), see [49]. A detailed review of antitampering techniques for smart meters is reported in [50].

3.3. COTS Components Selection to Build the Energy HAN. Table 4 presents a selection of COTS components suitable for developing devices capable of forming a ZigBee network, according to the architectures presented in the previous sections. They are systems-on-chip (SoCs) integrating at least a ZigBee transceiver, on-chip nonvolatile memory, RAM memory, and a CPU with a security AES coprocessor (see on-chip architecture in Figure 12).

As far as the RF part is concerned all devices in Table 4 implement the ZigBee physical layer at 2.4 GHz with a transmitted power in the order of few mW (3–4.5 dBm being 0 dBm = 1 mW) and a sensitivity from −95 to −101 dBm. Hence considering a full TX-RX link the proposed devices can face path losses up to −100 dB which is enough to build reliable home area networks according to the topology discussed in Sections 3.1 and 3.2. Since 2.4 GHz is a worldwide unlicensed frequency, this allows the use of these transceivers in every country, without difficulties. By using an integrated MURATA antenna, printed on the PCB board, 3 dBm of TX power allows reaching 30 meters indoor/urban or 100 meters and more outdoor line of sight. As discussed in [51], several strategies are foreseen in ZigBee in order to solve frequency coexistence problems with other communication technologies (e.g., Wi-Fi, Bluetooth) in the crowded 2.4 GHz frequency spectrum.

As far as the power consumption is concerned it is in the order of several tens of mW in RX or TX active mode; by implementing power cycling strategies, the power consumption can be kept as low as few μW using the STM32W108C8 device which moreover has a short wake up time of 110 μs. To implement smart metering or energy management function devices with a 32-bit CPU have to be preferred and with both RAM and Flash (rather than ROM) on-chip capabilities. To this aim we have selected for the implementation the STM32W108C8 which has 8 kbytes and 64 kbytes or RAM and Flash, respectively, and a-32 bit Cortex M3 processor which has a computation efficiency of 1.25 Dhrystone MIPS/MHz, enhanced instructions such as Hardware Divide, Single-Cycle (32 × 32) Multiply, Saturated Math Support, and 149 μW/MHz when realized in 180 nm CMOS technology. Some of the typical MAC operations required during communication (such as ACK management, automatic back-off delay, and packet filtering) are implemented via hardware, in order to meet the strict timing requirements imposed by IEEE 802.15.4-2003 standard.

When optimizing the network, a specific customization can be done according to the specific device under control. For example, to control simple power appliances like oven, refrigerators, boiler, lights, or air conditioning, it is not needed a continuous control. They have to send their consumptions, alerts in case of troubles (oven overheat during cooking, failures in refrigerator's components, etc.), and the capability of turning on or off them remotely is needed. For these devices a simple transceiver can be added, and hence the overhead introduced is minimum. These devices have only to transmit and to receive messages at low rate: their status, including energy usage, is checked few times in a day (4/5 times in a day), and alerts do not occur frequently. So a RF transceiver can be added to the MCU already present in such machines, or their MCU can be replaced with a wireless SoC such as the STM32W108C8.

Table 4: COTS components to implement the energy HAN nodes.

Device	ATZB-24-A2/B0 [56]	JN5139	JN5148	STM32W108C8	CC2530
CPU	8 b RISC ATMega128	32 b RISC	32 b RISC	32 b RISC Cortex3	8 b RISC 8051
Radio freq.	2.4–2.485 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.394–2.507 GHz
Flash/ROM	128 kB Flash	192 kB ROM	128 kB ROM	64 kB Flash	32, 64, 128, and 356 kB Flash
RAM	8 kB	8 kB	128 kB	8 kB	8 kB
Data rate	250 kbps	250 kbps	250, 500, and 667 kbps	250 kbps	250 kbps
V supply	1.8 V–3.6 V	2.2 V–3.6 V	2 V–3.6 V	2.1 V–3.6 V	2 V–3.6 V
RX current	19 mA	34 mA	17.5 mA	27 mA	24 mA
Tx current	18 mA	34 mA	15 mA	31 mA	29 mA
Standby current	6 μA	1.3 μA	1.25 μA	0.8 μA	0.4 mA
Wakeup time	N.A.	N.A.	840 μs	110 μs	600 μs
RX sensitiv.	−101 dBm	−97 dBm	−95 dBm	−99 dBm	−97 dBm
TX power	3 dBm	3 dBm	3 dBm	3 dBm	4.5 dBm

In case of smart plug (e.g., turn on/off control of lights) where a microcontroller is not present (since no logic control is required) a simple transceiver is added without any CPU core.

When dealing with other appliances such as washing machines or rechargeable systems for electric vehicles, a continuous control can be useful to program their work and hence to find an optimal trade off between user needs, time-based energy tariff, and production peaks of renewable home energy generators (wind, photovoltaic), if any. A smart washing machine can be programmed to work during low cost time slots. To do this, once the device is programmed, it must be in standby mode until the job can be performed. Small standby consumption is required. The smart information box of Figure 10 can contact the washing machine when the low cost slot begins. Then the device can start its work. A good solution to implement the smart washing machine could be the STMicroelectronics STM32W108C8, mainly thanks to its low consumption of current during standby mode (0.8 μA). It could be envisaged the possibility to use this wireless microcontroller also to manage washing machine operations, for those models that are not too complex. Finally for the Home Energy Angel smart information box and for the smart meter with local processing capabilities (data disaggregation), powerful architectures are needed. As example in the smart meter, the STM32W108C8 SoC could just implement a part (the MCU and the wireless transceiver) of the architecture of Figure 11. The board of the smart meter should be equipped also with a display driver, an E-meter ASIC, a power line communication modem chipset, and a touchscreen/display controller. In the case of the Home Energy Angel also a Wi-Fi communication controller is needed. The ST7590 IC can be used as the power line communication modem. This device is able to operate at 28.8 kbps, and its architecture is reported in Figure 13.

For the E-meter, the ASIC reported in Figure 14 by STMicroelectronics can be used. It implements measures of active, reactive, and apparent energy by acquiring voltage or current value through dedicated acquisition channels. The accuracy is 0.1% of full scale value.

3.4. Security in the Proposed ZigBee/802.15.4 HAN. All the devices discussed in the previous section contain an AES dedicated processor to implement ZigBee/IEEE 802.15.4 secure communications. AES is the encryption algorithm used in the proposed network. On-chip one time programmable memory can be used to store 64-bit MAC ID and 128-bit AES security key. As reported in Figure 15, with respect to the ISO/OSI protocol stack, ZigBee implements the first three layers (application, transport, and network layer), while IEEE 802.15.4 provides protocols for data link layer (i.e., divided in logical link control and media access control). This standard has several versions, named by year. The most important are the 2003 and 2006 versions. IEEE 802.15.4 uses 27 channels divided in three main bands; the most interesting are the 16 channels available in the worldwide available 2.4 GHz unlicensed band. To avoid the simultaneous transmission of several nodes, the standard uses CSMA-CA (Carrier Sensing Multiple Access-Collision Avoidance) or GTS (Guarantee Time Slots) protocol. A node using the CSMA-CA protocol, before sending packets in the network, checks if the communication medium is free or not: if the medium is free the node will send its packets, otherwise the node will wait for a certain period of time, computed with specific back-off algorithms (e.g., exponential back-off algorithm). The GTS protocol, instead, uses a coordinator node which gives to the other nodes time slots, so that anyone knows when it has to transmit its data. An interesting feature of IEEE 802.15.4 is the channel energy scan. Before using a channel, network sees how much energy (other network activity, noise, and interference) there is.

This mechanism saves energy, choosing free channels when setting the network. IEEE 802.15.4 is a low consumption protocol. Nodes that use this protocol can keep their transceiver sleeping most of the time (up to 99%), and receiving and sending tasks can be set to take small part of the devices' energy. ZigBee [18] is a standard for high-level communication based on IEEE 802.15.4 [52–55] data link standard. ZigBee is widely used in short range wireless communications requiring low date rates, low energy consumption, and a secure channel. The standard offers four main services.

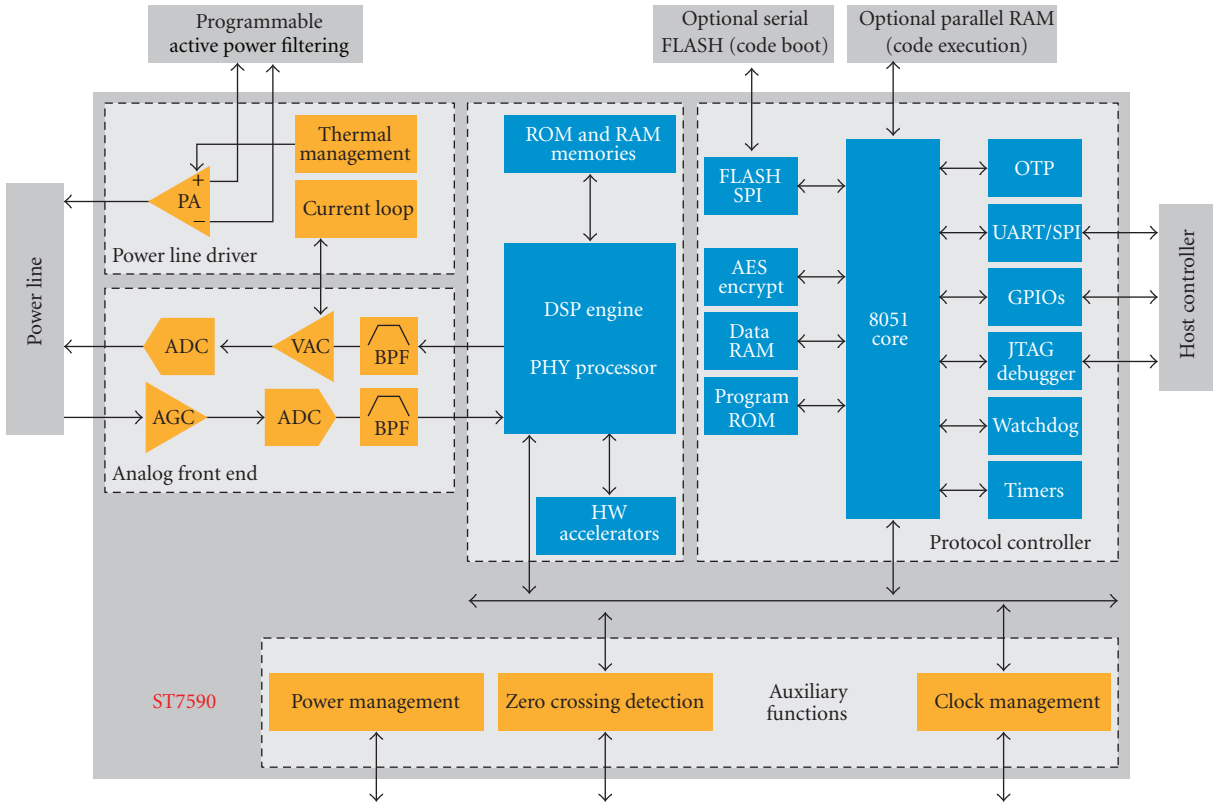


Figure 13: Architecture of the ST7590 PLC modem [25].

(i) *Extra encryption service*: the application and network layers use 128-bit AES encryption.

(ii) *Association and authentication*: only trusted nodes can join the network.

(iii) *Routing protocol*: the Ad hoc On-Demand Distance Vector (AODV) routing protocol specifies how nodes communicate with each other.

(iv) *Application service*: ZigBee introduces the concept of "cluster." Each node belongs to a cluster and can perform only actions allowed for the cluster. For example "house light system" cluster has only two possible actions: "turn lights on" and "turn lights off."

ZigBee nodes have a 16-bit network address, assigned by the coordinator during the association process. This address is used for routing information. Nodes within the network play different roles: coordinator, router, and end device. Coordinator and routers cannot sleep. They must be always awake in order to manage the network and to send packets along the network.

It is important to remind that the ZigBee network has not a peer-to-peer architecture, but a hierarchy one in which end devices can only communicate with routers and coordinators.

IEEE 802.15.4 supports only the encryption algorithm 128-bit AES. The reason is mainly due to the possibility to easily find on the market specific devices able to carry out encryption and decryption at the hardware level. The selected SoC has the AES processor embedded directly into transceivers and requires low resources. This standard does not specify how the keys have to be managed or the authentication policies to be applied. These details are leaved to the high-level standards. AES is used for data security (payload encryption) and for data integrity. In particular, the integrity is achieved using Message Integrity Code (MIC). MIC is obtained encrypting part of the MAC (Medium Access Control) frame, using the network key, and its length is usually 128 bits.

Figure 16 shows the IEEE 802.15.4 MAC frame. There are three important fields for security issues: frame control, auxiliary security header, and data payload.

Auxiliary security header field is meaningless if the security enable bit (within the frame control field) is unset. Otherwise, this field is divided into three subfields described hereafter.

Security Control. This field is used to select what kind of protection is used for the frame (i.e., security policies adopted): what is encrypted and how long is the key. The first 3 bits specify the security level, and related codes are listed in Table 5.

Frame Counter. To prevent replying attacks, every frame has an unique id.

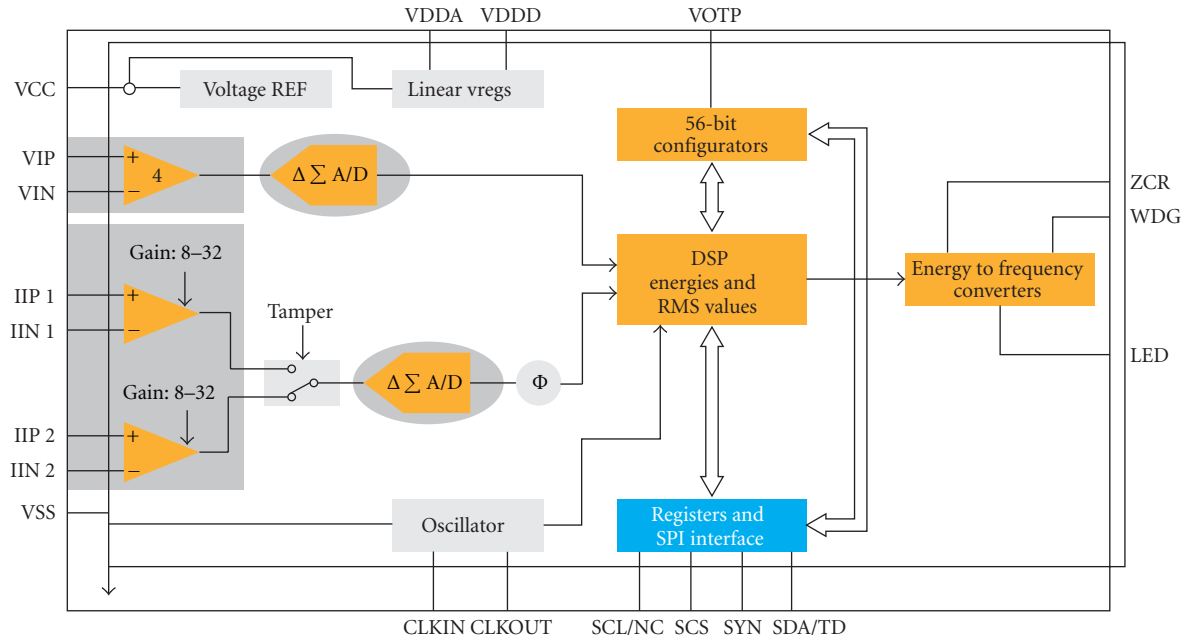


Figure 14: Architecture of the E-meter ASIC [25].

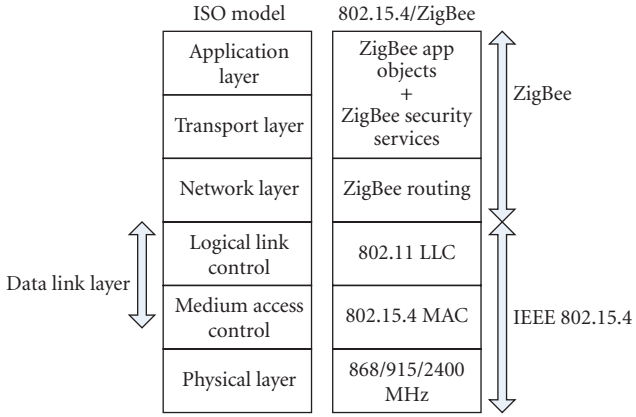


Figure 15: IEEE 802.15.4 and ZigBee role in the ISO/OSI stack.

Table 5: Security control codes.

Code	Security type	Authentication	Security services
0x00	No security	—	No security
0x01	AES-CBC-MAC-32	MIC-32	Data integrity
0x02	AES-CBC-MAC-64	MIC-64	
0x03	AES-CBC-MAC-128	MIC-128	
0x04	AES-CTR	—	Data security
0x05	AES-CCM-32	AES-CCM-32	Data integrity and security
0x06	AES-CCM-64	AES-CCM-64	
0x07	AES-CCM-128	AES-CCM-128	

Key Identifier. This field contains information about the type of key used in the communication with the other node. Keys can be implicit (known by nodes that are communicating) or explicit. In this last case, key index and key source subfields give indication about the key used.

Table 6: Access control list fields.

Field	Description
Address	Address of the destination node
Security suite	Security policy used
Key	128-bit key used in AES algorithm
Last initial vector (IV)	Used by the source to avoid reply attacks
Replay counter	Replay counter is equal to IV but is used by the destination node

Payload fields change according to security control field bits.

Every node within the network has an access control list (ACL), a list of "trusted brothers." Each node before sending data to another node checks if the receiver is a trusted brother using ACL table. If the receiver does not appear into the list, the node can take two possible actions, according to the security policy adopted for the network, reject the message or begin an authentication process. ACL fields are specified in Table 6.

With respect to the 802.15.4 layers, ZigBee adds two additional security layers: the network and the application layers. As all security mechanisms use 128-bit AES encryption, devices designed for IEEE 802.15.4 standard can be used without any modification. ZigBee standard uses three type of keys. These keys are actually used or not, according to the policy chosen for the network. ZigBee keys are:

(i) Master key: it is used for keeping link keys confidential and checking their correspondence.

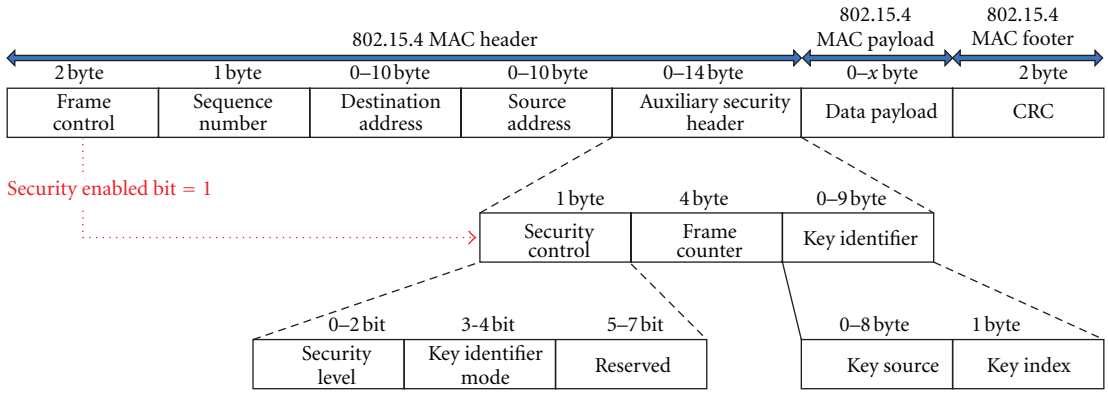


Figure 16: IEEE 802.15.4 MAC frame and security issues.

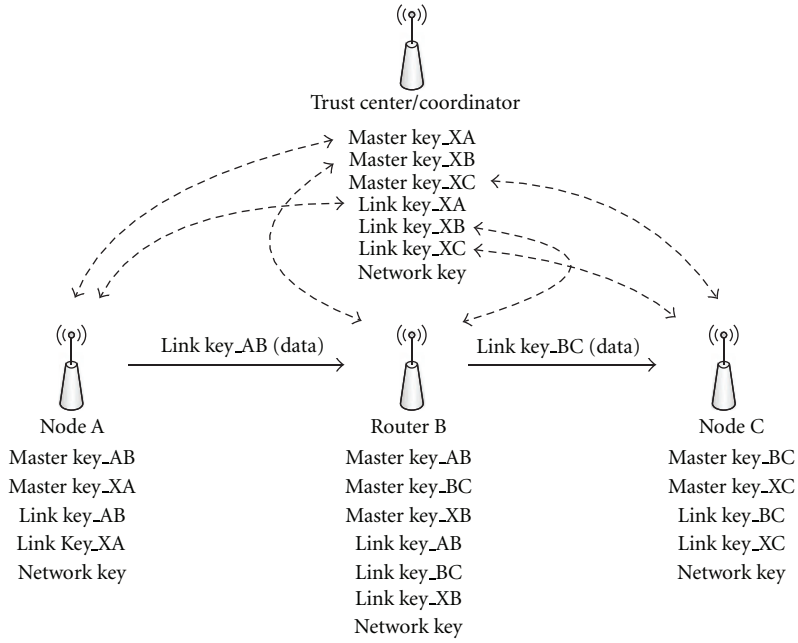


Figure 17: ZigBee commercial mode.

(ii) Link keys: these keys are unique between pair of nodes. The use of link keys introduces a significant overhead for the node, requesting more memory resources, due to the fact that all data exchanged between two nodes must be encrypted with this key. Link keys are used only in commercial mode policy.

(iii) Network key: it is an unique 128-bit key shared between the devices composing the network. Network key is generated by the trust center, and it is regenerated after specific time interval. The old key is used to encrypt the new key, that is sent to nodes.

Master and link keys are used by the application layer, and network key is used both by the ZigBee and the MAC layers. The trust center is a special device, that is trusted by the other nodes within the network. Generally, the coordinator is the trust center, even if this role can be played also by another node.

To ensure security, the ZigBee network can use both master and link keys, or if a simple connection is needed only the network key.

In the first case, ideally, every device has the trust center address and an initial master key preinstalled. Otherwise, master keys can be distributed by trust center, during initial network setup using an insecure channel. After all nodes have the master key, link key can be obtained using agreement or transport process. Link keys can be also preinstalled. An example of this use of keys is the commercial mode policy (shown in Figure 17).

When the ZigBee network uses only the network key there is an initial distribution of this key, that is done by the trust center through an insecure channel. Only after the network key is acquired by all nodes the communications between nodes become secure.

Security policies decide which keys are used to make safe the network.

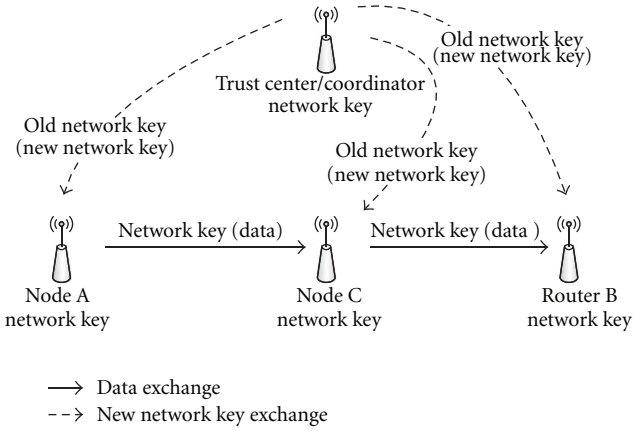


Figure 18: ZigBee residential mode.

(i) Commercial mode where both master key and link keys are used. In this case more memory resources are required.

(ii) Residential mode where data exchange within the network are encrypted using only network key. This mode is the easiest to implement but is less secure.

To ensure security and privacy protection in the example energy HAN, both residential and commercial modes (see Figures 17 and 18) can be used. In both modes, the trust center role can be played by the smart information box, that is also the coordinator of the network. This eliminates the need of a special node performing only security operations. Security parameters can be easily set using the interfaces of the smart information box, and information about network behavior (logs) can be stored and later accessed. Moreover, the Home Energy Angel smart information box is also accessible remotely, so users can control security status of the network also outdoor, using an internet connection.

To implement the residential mode the network will need only a network key. The Home Energy Angel smart information box can establish a first key and then distribute it through an insecure connection to other nodes. Otherwise users and operators can "write" it into the devices' memory; this operation is more secure. Actually any key is transmitted through an insecure channel. Summarizing, if residential mode is chosen security problems can occur during the initial setup of the network.

Commercial mode provides stronger security than residential mode but requires more resources (memory and CPU time). Actually each connection between two nodes uses different keys, and if security is broken in one link, this will not affect the whole network. Also in this mode, the initial key setting is a critical point. A secure method is to assign to each node a first master key "manually." Then, this will be changed by the trust center using a secure connection. If a first master key is not assigned, this task must be done by the trust center using an insecure channel. A successful conclusion of the initial setup of the network assures the confidentiality and the integrity of the network.

Information exchanged between nodes is always encrypted, and message integrity can always be checked, if the highest security level (AES-CCM-128) was selected. This choice does not affect devices performance since ZigBee transceivers have dedicated AES processors for encryption and decryption.

4. Conclusions

This paper has discussed and reviewed security problems in Smart Grid taking care of developed architectures and lesson learned at University of Pisa in some projects on the theme of smart energy. An energy home area network, a key element of Smart Grid, is presented, dealing with its security and privacy aspects and showing some solutions to realize a wireless network, based on ZigBee. Implementation challenges from the hardware and software point of view and possible architectures and implementation using COTS components are proposed for key nodes of the smart energy HAN: smart power meters, smart plugs, and a Home Energy Angel information box essential for energy management/saving policy and for energy awareness.

References

[1] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010.

[2] S. M. Amin and B. F. Wollenberg, "Toward a smart grid," *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, 2005.

[3] W. K. Park, C. S. Choi, I. W. Lee, and J. Jang, "Energy efficient multi-function home gateway in always-on home environment," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 1, pp. 106–111, 2010.

[4] M. Jahn, M. Jentsch, C. R. Prause, F. Pramudianto, A. Al-Akkad, and R. Reiners, "The energy aware smart home," in *Proceedings of the 5th International Conference on Future Information Technology (FutureTech '10)*, pp. 1–8, May 2010.

[5] D. Niyato, L. Xiao, and P. Wang, "Machine-to-machine communications for home energy management system in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 53–59, 2011.

[6] D. Y. Nagesh, J. V. Krishna, and S. S. Tulasiram, "A real-time architecture for smart energy management," in *Proceedings of the Innovative Smart Grid Technologies Conference (ISGT '10)*, pp. 1–4, January 2010.

[7] P. Kulkarni, S. Gormus, Z. Fan, and B. Motz, "A mesh-radio-based solution for smart metering networks," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 86–95, 2012.

[8] E. Pallotti and F. Mangiatordi, "Smart grid cyber security requirements," in *Proceedings of the 10th International Conference on Environment and Electrical Engineering (EEEIC '11)*, pp. 1–4, May 2011.

[9] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[10] EPRI, *Report to NIST on Smart Grid Interoperability Standards Roadmap*, EPRI, Gaithersburg, Md, USA, 2010.

[11] R. H. Lasseter and P. Paigi, "Microgrid: a conceptual solution," in *Proceedings of the IEEE 35th Annual Power Electronics Specialists Conference (PESC '04)*, pp. 4285–4290, June 2004.

[12] NanoCatGeo, "NanoCatGeo project," https://sites.google.com/site/nanocatgeo.

[13] Acta, "Hydrogen generators and fuel cells systems," http://www.actagroup.it.

[14] L. Fanucci, S. Saponara, and A. Morello, "Power optimization of an 8051-compliant IP microcontroller," *IEICE Transactions on Electronics C*, vol. E88, no. 4, pp. 597–600, 2005.

[15] S. Saponara, E. Petri, L. Fanucci, and P. Terreni, "Sensor modeling, low-complexity fusion algorithms, and mixed-signal IC prototyping for gas measures in low-emission vehicles," *IEEE Transactions on Instrumentation and Measurement*, vol. 60, no. 2, pp. 372–384, 2011.

[16] E. L. Quinn, *Privacy and the New Energy Infrastructure*, Social Science Research Network (SSRN), 2009.

[17] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*, Syngress, 2010.

[18] ZigBee, *The ZigBee Specification Version 1. 0*, ZigBee Alliance, San Ramon, Calof, USA, 2007.

[19] M. Zeifman and K. Roth, "Nonintrusive appliance load monitoring: review and outlook," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 1, pp. 76–84, 2011.

[20] T. S. Choi, K. R. Ko, S. C. Park, Y. S. Jang, Y. T. Yoon, and S. K. Im, "Analysis of energy savings using smart metering system and IHD (in-home display)," in *Proceedings of the Transmission and Distribution Conference and Exposition: Asia and Pacific*, pp. 1–4, October 2009.

[21] Z. Wang and G. Zheng, "Residential appliances identification and monitoring by a nonintrusive method," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 80–92, 2012.

[22] M. Venables, "Smart meters make smart consumers," *Engineering and Technology*, vol. 2, no. 4, p. 23, 2007.

[23] F. Benzi, N. Anglani, E. Bassi, and L. Frosini, "Electricity smart meters interfacing the households," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 10, pp. 4487–4494, 2011.

[24] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm '10)*, pp. 238–243, October 2010.

[25] Y. Gourdou, *Smart Grid/Metering Solution*, EMCU, 2011.

[26] M. Nassar, J. Lin, Y. Mortazavi, A. Dabak, I. H. Kim, and B. L. Evans, "Local utility power line communications in the 3–500 kHz band: channel impairments, noise, and standards," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 116–127, 2012.

[27] Echelon, *DCN, 1000 Series Data Concentrator*, Echelon, Memphis, Tenn, USA, 2012.

[28] IEEE, "IEEE guide for smart grid interoperability of energy technology and information technology operation with the Electric Power System (EPS), end-use applications, and loads," Tech. Rep. 2030-2011, IEEE, 2011.

[29] M. Weiss, A. Helfenstein, F. Mattern, and T. Staake, "Leveraging smart meter data to recognize home appliances," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom '12)*, pp. 190–197, 2012.

[30] ISO/IEC, *ISO/IEC, 27000:2009. Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, ISO/IEC, Geneva, Switzerland, 2009.

[31] ISO/IEC, *ISO/IEC, 27001:2005. Information Technology—Security Techniques—Information Security Management Systems—Requirements*, ISO/IEC, Geneva, Switzerland, 2005.

[32] ISO/IEC, *ISO/IEC, 27002:2005. Information Technology—Security Techniques—Code of Practice for Information Security Management*, ISO/IEC, Geneva, Switzerland, 2005.

[33] ISF, *Information Security Forum's Standard of Good Practice*, ISF.

[34] K. Kent and M. Souppaya, "Guide to computer security log management," Tech. Rep. 800-92, NIST Special Publication, 2006.

[35] IEC/TS, "IEC/TS, 62351. Power systems management and associated information exchange—data and communications security," IEC/TS.

[36] A. Lee and T. Brewer, "Smart grid cyber security strategy and requirements," NISTIR Draft 7628, 2009.

[37] F. Hao and P. Y. A. Ryan, "Password authenticated key exchange by juggling," in *Proceedings of the 16th International conference on Security protocols*, pp. 159–171, Springer, Berlin, Germany, 2008.

[38] F. Hao and P. Ryan, "J-PAKE: authenticated key exchange without PKI," in *Transactions on Computational Science XI*, M. Gavrilova, C. Tan, and E. Moreno, Eds., pp. 192–206, Springer, Berlin, Germany, 2010.

[39] M. Blaze, "Protocol failure in the escrowed encryption standard," in *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, pp. 59–67, ACM, Fairfax, Va, USA, November 1994.

[40] C. Borean, "Energy@home: a "user-centric" energy management system," in *Proceedings of the 5th European ZigBee Developers' Conference*, Munich, Germany, 2011.

[41] N. Costantino, R. Serventi, F. Tinfena et al., "Design and test of an HV-CMOS intelligent power switch with integrated protections and self-diagnostic for harsh automotive applications," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 7, pp. 2715–2727, 2011.

[42] T. Jakobi and T. Schwartz, "Putting the user in charge: end user development for eco-feedback technologies," in *Proceedings of the 2nd IFIP Conference on Sustainable Internet & ICT for Sustainability (SustainIT '12)*, Pisa, Italy, October 2012.

[43] N. Goddard, J. Moore, C. Sutton, J. Webb, and H. Lovell, "Machine learning and multimedia content generation for energy demand reduction," in *Proceedings of the 2nd IFIP Conference on Sustainable Internet & ICT for Sustainability (SustainIT '12)*, Pisa, Italy, October 2012.

[44] F. Bellifemine, "Smart consumption: the energy@home approach," in *Proceedings of the 2nd IFIP Conference on Sustainable Internet & ICT for Sustainability (SustainIT '12)*, Pisa, Italy, October 2012.

[45] S. Genovesi, S. Saponara, and A. Monorchio, "Parametric design of compact dual-frequency antennas for wireless sensor networks," *IEEE Transactions on Antennas and Propagation*, vol. 59, no. 7, pp. 2619–2627, 2011.

[46] S. Genovesi, S. Saponara, and A. Monorchio, "Compact Triple-Frequency Antenna for Sub-GHz Wireless Communications," *IEEE Antennas and Wireless Propagation Letters*, vol. 11, pp. 14–17, 2012.

[47] A. G. Ruzzelli, C. Nicolas, A. Schoofs, and G. M. P. O'Hare, "Real-time recognition and profiling of appliances through a single electricity sensor," in *Proceedings of the 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '10)*, pp. 1–9, June 2010.

[48] A. Marchiori, D. Hakkarinen, Q. Han, and L. Earle, "Circuit-level load monitoring for household energy management," *IEEE Pervasive Computing*, vol. 10, no. 1, pp. 40–48, 2011.

[49] Freescale, *Electronic Tamper Detection Smart Meter Reference Design*, Freescale, 2012.

[50] J. McCullough, *Deterrent and Detection of Smart Grid Meter Tampering and Theft of Electricity, Water, or Gas*, Elster, 2010.

[51] ZigBee, *ZigBee and Wireless Radio Frequency Coexistence*, ZigBee Alliance, San Ramon, Calof, USA, 2007.

[52] G. Anastasi, M. Conti, and M. di Francesco, "A comprehensive analysis of the MAC unreliability problem in IEEE 802.15.4 wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 1, pp. 52–65, 2011.

[53] C. Gomez and J. Paradells, "Wireless home automation networks: a survey of architectures and technologies," *IEEE Communications Magazine*, vol. 48, no. 6, pp. 92–101, 2010.

[54] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," in *Computer Networks*, vol. 38, pp. 393–422, Elsevier, New York, NY, USA, 2002.

[55] D. M. Han and J. H. Lim, "Smart home energy management system using IEEE 802.15.4 and zigbee," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1403–1410, 2010.

[56] Atmel, *ZigBit 2.4 GHz Wireless Modules—ATZB-24-A2/B0*, Atmel, 2009.