A Large-Scale Wireless Network Approach for Intelligent and Automated Meter Reading of Residential Electricity

Victor Custodio, Jose Ignacio Moreno, and Juan Pablo Viñuela

Telematic Engineering, Carlos III University of Madrid,
Av. Universidad, 30, E. Torres Quevedo. E-28911 Leganés (Madrid), España
{victor.custodio,joseignacio.moreno,juanpablo.vinuela}@uc3m.es

Abstract. Control of electrical energy consumption is a critical aspect when electric companies try to establish the correct balance between the supply and demand of energy. Current solutions are based on experience, historical demand behavior and global control of the electrical grid, but they lack of detailed information about users consumption behavior. In the future, electric companies will need to know, almost in real time, user needs on energy to avoid extra costs of an over provisioning infrastructure or a lack of service during peak times. In this paper we address network topology, capacity planning and security issues of an IT platform, based on wireless sensor networks, to meet the new market requirements. The resulting automated control system will be able to provide real-time control of user demands, as well as to open the market to future services in this area: differential billing schemes, remote control and others.

Keywords: Electricity Metering Platform, AMR, Security, ZigBee, WSN.

1 Introduction

Electricity meter reading is a common task that must be accomplished by every single electric company in the market. Why? This is a standard way they have to measure the effective amount of energy a certain user consumes over a period of time.

Until now, traditional methods for residential meter reading, involves the physical presence of companies' personnel at the user premises every one or two months to visually read the corresponding meters for every user or client of the service, a number big enough to reach hundreds of thousands or even millions of devices to be read. Although, many solutions have been developed to improve the time required to get manual readings from the meters through the use of wireless equipment, just a few of them, if any, introduces the possibility to do it remotely and automatically. Another big problem that electric companies have is that they face an uneven consumption curve during the day, forcing them to provision enough network infrastructure and operations to support periods of peak demand. This difference between the supply and demand of energy, introduces high operational costs and complex grid management.

Naturally, the described process leads to very high operational costs for the electric companies and also, complex logistics and management problems. But even more

S. Hailes, S. Sicari, and G. Roussos (Eds.): S-Cube 2009, LNICST 24, pp. 20–32, 2009.

important, this old-fashioned method does not allow these companies to be major players, and actively participate in one of today's world-most significant challenge which is energy efficiency, as stated by the European Union as one of the top important subjects in energy field for the next coming years [1].

In this work we present an IT platform to perform remote electricity-meter readings, which will enable companies to automate the process without the need of in-premises personnel, reducing operational expenditures and opening an unprecedented way for real-time energy metering, and consequently, the possibility of energy efficiency, not only saving money for electric companies and end-users, but also making big savings to the environment and the world. Moreover, companies will have the possibility to offer new services related to energy consumption. The proposed IT platform will make use of different communication technologies depending on the requirements and restrictions of each network segment of the design.

With the evolution of technology in recent years, new communications systems are coming into the markets. Wireless networks are no exception of this phenomenon, and these kinds of technologies are even more present in people's today's life, having outstanding advantages for a meter-reading platform such the one presented here. In the access network, there will be no need to deploy costly wired infrastructure around user premises, where wireless sensor networks (WSN) will be a good solutions due to its low cost and low power consumption. In the other hand, for a long range path, WSN won't provide the necessary range and processing power, where a different technology, wireless or not, will be more suitable (GPRS, WiMAX, ADSL, etc).

The main objective of this paper is to present an IT platform capable of reading every meter from the electric-service users at previously designated time-intervals of the day, or even on demand, and then send this information to the central servers of the electric company. This will enable them to develop differential billing schemes based on the energy demand during the day and the real-time knowledge of energy consumption, as well as to reduce the operational costs associated with the reading of the meters. It is important to mention that even thou this work have been done in an electricity meter context, it can also be applied to any other utility application.

The rest of this paper is organized as follows: Section 2 focuses on the analysis of requirements and the architecture for the meter reading platform. Section 3 explains the core aspects of network deployment and security for the platform. Section 4 shows a sample deployment and network dimensioning using typical values for an average electric company. Finally, we present some conclusions and future work.

2 Requirements and Architecture for Electricity Meter Reading

Until now, traditional methods of residential electricity metering has consisted in electric companies having to send dedicated employees to client premises (houses, buildings, etc) every one or two months to visually read the customer meter, and take note of the readings. Based on the reading made by the employee, the company is able to charge the user for the amount of energy consumed over the period of time being measured. Unfortunately, such method requires a big effort in terms of the number of employees needed to perform the task and many times involves having to get into users home to reach a meter, which could also represent a problem.

The purpose of Automated Meter Reading (AMR) technology is to enable electric companies to perform meter readings remotely, without sending employees to users home. Many technologies exist today for the automation of the process, but they generally involve sending an employee to the neighborhood or to a point of close vicinity of a group of users, or deploying wired infrastructures at user's premises.

With the introduction of WSN's, we can develop a distributed and automated process to perform the readings, where the edge is that we can avoid costly and/or complex situations such as the ones mentioned above. In this sense, the results obtained will turn into great improvements for electrical companies and end-users:

- Billing Schemes: Encourages energy use during low demand periods.
- Operational Expenditures Reduction: There is no longer need to send huge number of employees to customers' premises to perform readings.
- New Services: Companies can offer new services to their customers.

Automating the process through the use of WSN's, involves taking into account several aspects related to features, requirements and the specific scenario and architecture of applications, all of which we will describe in the rest of this section.

2.1 Features and Requirements

The proposed IT platform is based in a group of features and requirements for the technology to be used, as well as a series of features related to the specific applications to be implemented. Depending on these parameters, the proposed methodology tries to accommodate and solve the majority of the different scenarios.

2.1.1 Application Requirements

Nodes Identification. The EndPoints (devices attached to meters) have to be uniquely identifiable in the network and correctly associated to a specific customer.

Node Mobility. This is a very important feature of general WSN's, but in this case is not very relevant. Most of the time there will be no movement of the EndPoints.

Energy Consumption and Battery Lifetime. This is a very restrictive parameter for WSN's, especially if units are battery powered. For electricity meters, endpoints are expected to draw power from the corresponding electricity meter they are attached to.

Scalability. In the future, new endpoints will be joining the network. The design should consider the possibility of automatic growth of the network, without the need to perform specific and/or technical modifications to the design.

Reliability. This is one of the most important requirements for an AMR platform. Information cannot get lost, even considering that there could be connection dropouts in the network. Readings must be taken in a secure and timely manner.

2.1.2 Requirements Imposed by the Technology

Identification of Devices. Wireless endpoints will be based on ZigBee technology. There are two possibilities of addresses for the devices: 64 bits pre-encoded MAC addresses and 16 bits network addresses. The first of them are globally unique and usually used when a device is about to join a ZigBee network. The second of these two, is a much shorter address used for routing purposes inside the network.

Network Size. The size of a ZigBee network is theoretically determined by the limitation of the 16 bits addresses. Nevertheless, because of physical limitations, the maximum number of devices is 100 per ZigBee network, a much smaller amount.

Type of Sensors. Sensors connect to electricity meters through serial interfaces, so the wireless device will be inside the meter, thus reducing the range for the devices.

Maximum Number of Coordinators. There is a limit, by design, of 4 coordinators that can be directly attached to the interfaces of the concentrator.

2.2 Scenario Description

A typical scenario consists of a group of houses or buildings in dense urban areas, where the different buildings are in proximity one from another. We will find other situations too (small towns or isolated houses) but this scenario is a good start.

Every house has an electricity meter to be read. The location of the meter will depend on the type of edification: in houses, most of the time it will be just outside of the house; in buildings, it could be just outside of the apartment or sometimes in a special designated area to group a number of them. The meters connect through a wireless interface to a special device called concentrator, which aggregates all the readings of the meters in close proximity. The concentrator is responsible for sending all the information back to the management servers of the electric company, which in most cases will be several miles away from the customer's premises.

As we can see in Fig. 1, the scenario comprises a series of important elements, each of them having different roles. The combination of these elements in a network, make possible the automated meter reading process.

EndPoint. Network element integrated into the meter. It implements a physical and logical interface so it can interact with the meter to obtain the readings and manage the device.

Coordinator. Device responsible for the coordination of a ZigBee network. It allows nodes to join the network and assigns them network addresses, and it is in charge of routing, outside the network, the information from all the meters.

Concentrator. It's the network element responsible for collecting and aggregating all the information generated by a group of endpoints. It implements the logical interfaces to communicate with endpoints and the middleware platform

Management Servers. They represent the middleware platform that is responsible of making requests to nodes and storing the information of the readings from meters.

It is possible to identify two different network segments in the path that information has to travel from an endpoint all the way to the management servers: A *short range* which we will call "last mile" and correspond to the segment that goes from the endpoints to the concentrator; and a *long range* segment composed by the portion between the concentrators and the management servers.

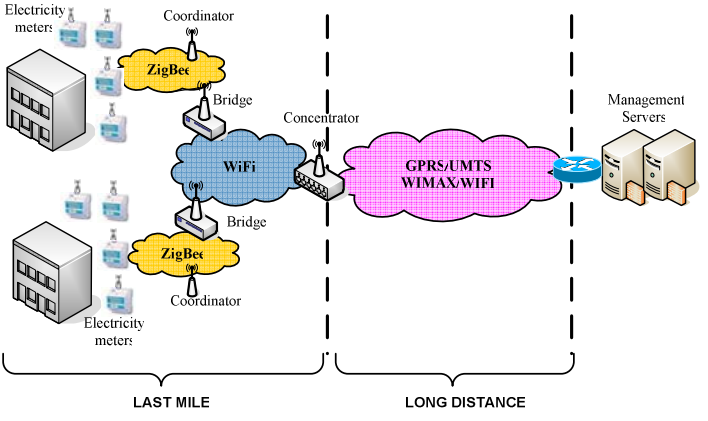

Fig. 1. Typical scenario for the meter reading platform

In order to make fast and economic deployments, which are a very important requirement in today's applications, we take advantage of wireless technologies as a base infrastructure for the network. The reading platform will sit on top of this infrastructure, regardless of the specific technologies used in each segment.

The last mile segment usually corresponds to one or several ZigBee networks, connected to a Concentrator directly through a serial connection or via a Wi-Fi Bridge. The Concentrator collects all the readings from the meters it serves in its area and is responsible of sending the information back to the management servers through the long range segment of the network. ZigBee is a low-cost and low-power wireless technology that perfectly suits the requirements for this part of the network, due to geographical disposition of meters and low traffic generated by them. Wi-Fi connections are needed when Concentrators are far away from the ZigBee networks.

The long range is used to connect the Concentrator to the middleware platform, and usually will be composed by one or a combination of GPRS/UMTS or Wi-Fi/WiMAX technologies. These technologies provide the necessary infrastructure to make possible for the aggregated meter information to reach the management servers.

It is important to mention that currently there are some alternatives to the one presented here, such as using PLC instead of ZigBee for the last-mile segment, or even using GPRS connections directly attached to each endpoint. Using GPRS directly on endpoints results in a very costly solutions, especially when it comes to get readings from million units. In the other hand, we use ZigBee instead of PLC because

has some bandwidth limitations (depending on the place of deployment) and also it is not as flexible as ZigBee. In the future, this platform could be used for other utilities, like gas or water, where a PLC connection could not be fully guaranteed.

3 Network Deployment Analysis

The main objective of the deployment analysis is to correctly identify problems and solutions related to the deployment of the network, to be able to successfully obtain the readings of all the electricity meters, subject to a series of constraints, such as reliability, costs, scalability and others. From this point of view, we have stated three fundamental tasks in the deployment activity: Sensor Identification, Network Security and Capacity Planning. The first one specifies how to univocally identify each and every node of the network, letting the management servers, or any other network element, to communicate with a specific endpoint; Network Security section explains the mechanisms to obtain authentication, data confidentiality and integrity, and high availability of the service; The third part, analyzes the different data size related to the meter, and uses this information to plan the capacity, in terms of needed bandwidth, to be supported in every section of the network.

3.1 Sensor Identification, Addressing and Naming Convention

Devices identification is one of the important and challenging parts of the deployment of the solution. As stated before, the number of meters for an electric company can easily reach hundreds of thousands or million units. Having a way to univocally identify them, involves the association of the meter with a specific customer.

Even if it was possible to use all the 16 bits addressing space given by ZigBee technology, it wouldn't be enough. Besides the number of addresses problem, there is a problem related to persistency. A ZigBee coordinator assigns networks addresses to devices dynamically, thus, the address of a specific device can change in time. This means that we cannot use only network addresses as a way to identify nodes. In a situation like this, it is convenient to use the long 64 bits MAC addresses as a way to uniquely identifying the nodes, although its use is not meant for routing purposes.

Now, provided that we are going to use 64 bits MAC addresses for identification, there is still a need to associate these addresses with specific customers. Taking into account that the meters will be grouped under concentrator devices, which will be operating on an IP network in the long-range segment, we will have the following tuple of information that has to be recorded into the management servers:

customer_id	node_mac_address	concentrator_id

The *customer_id* corresponds to a company-assigned identification for its customers, *node_mac_address* is the unique 64 bits addresses for ZigBee devices, and *concentrator_id* corresponds to an identifier for the concentrators of the network.

Using a scheme like this requires additional considerations and could introduce some potential problems. The row has to be repeated for each and every customer of the service, which can grow to a very large number and could lead to data-access

efficiency problems. Each time the management middleware has to contact a customer meter, it first has to consult the database to obtain the MAC address of the corresponding device, as well as the information regarding to the identification of the concentrator under which the meter operates. This way, the platform knows which concentrator to send a request to, in order to communicate with a certain meter. Once a concentrator receives a request, it passes the request, along with the MAC address to the coordinators it has attached to its interfaces, and the coordinators in turn, using the MAC address, search for the corresponding device inside the ZigBee network. Under a situation like this one, there is no chance for a good organization or hierarchy of the network, thus increasing complexity of the process.

As a workaround of the problems mentioned above, we propose the use of virtual networks and addresses. The main idea behind this is to build a complete IP-based network on top of the heterogeneous infrastructure of the different network technologies used. We have seen in the scenario description, that there will be an IP portion in the design, primarily corresponding to the long distance segment and maybe some portion in the short range part. The last mile, which considers the endpoints (electricity meter nodes), is based on ZigBee technology. The virtual network will sit just on top of this infrastructure.

ZigBee technology does not support the TCP/IP stack, mainly because of its size, but it is possible to implement a network address translation between IP and ZigBee addresses [2], without having to use the whole TCP/IP stack. This method is intended to be used for naming and addressing purposes but not for routing purposes. This means that the ZigBee network remains intact from the network-inside point of view. For the addresses translation to work, it is needed to add a gateway at the edge of the ZigBee network, which will be in charge of the translations. This way, from the outside, it will be possible to address endpoints through an IP address, simplifying the whole process of communicating with an endpoint. The main advantages will be:

- No need to send long MAC addresses through the network (end-to-end). Just the gateways need to know them.
- Network Hierarchy. It is possible to subdivide the network into subnets.
- The whole meter-reading process becomes more transparent to middleware.

Finally, to implement a solution like this one, it is needed to know what will be the size of the network, in terms of how many endpoints and concentrators there will be. This will lead to a correct address or naming convention and how to structure the network. The important things to take into account in this section are:

- Estimated number of endpoints
- Estimated number of concentrators
- Network planning: IP addresses to use and number of subnets

3.2 Network and Data Security

The AMR communication platform presented here is mainly based on wireless networks. These types of networks are generally exposed to a number of vulnerabilities that wired networks do not have, starting with the fact that possible

attackers have direct access to the network media. This way, anyone being in range and knowing the frequency of transmission could have access to the network, almost like any other device does. Among the most common and important types of attacks we have:

- Denial of Service: causing interference, taking advantage of the vulnerability of the CSMA-CA protocol. This is used in ZigBee and Wi-Fi.[3]
- Attack to the Confidentiality of the Data
- Replay Attacks
- Supplanting of endpoints

In the context of automated meter reading, the supplanting of endpoints will be the most likely attack to occur, therefore, authentication is one of the most important aspects to take into account, without leaving behind confidentiality and integrity of the data, and the availability of the service, which are of extreme importance too.

Now we describe possible solutions to provide security mechanisms for, at least, each of the five characteristics mentioned above, considering last mile and long-range segments.

3.2.1 Last Mile Segment

The communications in the last mile correspond to ZigBee and Wi-Fi networks.

The ZigBee Pro standards [4][5] provides two types of security: Standard Security and High Security. The standard mode is focused to avoid the access of external devices to the network, and it is based on a trust center that authenticates and distributes a network key that is used to encrypt all messages that flow through the network.

The high security mode is thought for networks where the security control is critical, and in order to satisfy the requirements of the system, it adds two more keys, master and link keys, besides the secure key exchange (handshake). In this mode all the messages are encrypted from point-to-point with a *link* key that is generated from a master key, after a handshake between both points. This way, the high security of ZigBee also avoids insider attacks. Because of its strength, this is the security standard that we are going to use for the meter reading platform.

In order to provide for the minimum security needed for the Wi-Fi network, we can make use of Wi-Fi security standard 802.11i (WPA/WPA2) with 802.1x authentication (EAP), which currently is considered to be safe. To strengthen its security even more, there are several mechanisms to consider:

- IPSEC (VPN tunnels): The information travels encrypted through the tunnel from the client to the VPN server.
- MAC Filtering: Only authorized devices are allowed access to the network.
- Hiding Access Point: Hiding the access point is possible (if available)

Given that we are working with mesh networks, hiding the access point is not supported, and the management of MAC filtering tables becomes very costly for large deployments. That's why both of these are not to be used.

On the other hand, due to high sensitivity of information against attacks and future potential vulnerabilities of the 802.11i standard, we introduce an extra level of security through the use of IPSec VPN tunneling.

3.2.2 Long Distance Segment

The communications in this segment consider any or a combination of GPRS/UMTS and/or Wi-Fi/WiMAX. In the latter case, the same safety mechanisms considered in the last mile apply here, because they are considered to be safe enough for now. The standards to be used consider 802.11i (WPA2) and 802.1x (EAP) authentication for Wi-Fi networks, 802.16g with EAP and PKMv2 for authentication in WiMAX networks [6]. Like in the last mile, we also increase security by using VPN tunneling based on IPSec.

Table 1. Security Mechanisms

Network	Link level	Network level	Application level
ZigBee	High Security		
Wifi	WPA2	VPN based in IPsec	-
GPRS	Security offered by telecomm operator		AES Encryption + PKI-based Authentication and key exchange
WIMAX	802.16g security with EAP and PKMv2	VPN based in IPsec	-

In situations where the information through the long range segment is sent over GPRS/UMTS, the telecomm operator that offers the service will be responsible for ensuring authentication, confidentiality, integrity, and service availability, in an end-to-end basis. As a safety measure, we again provide an extra level of security. In this case, all messages are encrypted using application-level AES. The exchange of symmetric keys for AES encryption and a second authentication is performed using a system public key (PKI). This information is summarized in Table 1.

3.3 Network Capacity Planning

Capacity planning is about estimating and knowing what are going to be the limitations and restrictions with respect to the different technologies involved in the design, making it possible to address and provision the necessary equipment for the system to work in optimal conditions, based on a set of requirements. This will lead to an estimation of the number of the different equipment needed for deployment and the bandwidth requirements over the different networks segments, among others.

The most important requirements and capacities limits for the design are:

- Number of Nodes
- Number of ZigBee Coordinators
- Number of Concentrators
- Size of summarized meter readings and firmware in each network segment.

To calculate the above restrictions, it is needed the following list of parameters:

- Number of customers to obtain energy consumption information from.
- Maximum number of nodes per ZigBee network
- Maximum number of coordinators supported per Concentrator
- Size of an electricity-meter reading
- Time interval between each reading.

These kind of considerations are well suited for a general purpose scenario, but in a real case deployment, it is necessary to take into account other parameters such as the types and level of isolation of buildings involved, communications technology availability and coverage in the specific area of deployment, among others.

The next section will show an example of a deployment and how the above information is useful to obtain gross estimations for infrastructure requirements.

4 Practical-Case Application of the Deployment

In this section we present an application of the deployment methodology presented in the previous section, covering the most relevant aspects of identification and capacity planning. Security parameters correspond to the ones presented in previous sections.

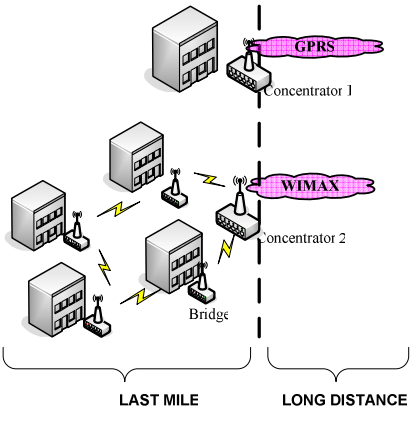

Fig. 2. Sample scenario for the application of the deployment methodology

The example is based on Fig. 2, where we assume the values presented in Table 2 for the different parameters involved the scenario. There are 5 buildings in the scenario. Four of them will connect to one concentrator through Wi-Fi bridges, and the fifth one will connect to another concentrator through its serial interface, because it is not close to the rest of the buildings. It has been stated that the reading of a meter consumes at most 60 bytes, including headers and security redundancy.

Table 2. Parameters for the example of the applications of the deployment methodology

Parameter	Value
Number of Buildings	5
Number of Floors per Building	8
Number of Apartments per Floor	6
Distance Between Buildings	< 30 mt
Distance from the Buildings To Management Servers	5 km
Maximum number of nodes per ZigBee network	50
Number of ZigBee interfaces per Concentrator	4
Size of an electricity-meter reading (including headers)	60 bytes
Size of a Firmware Update of a Meter	60 Kb
Meter-Reading Interval	15 min

Based on information from Table 2, it's possible to estimate the requirements on equipment and devices to be used for the solution. This is presented in Table 3.

Table 3. Estimation of number of needed devices based on parameters of the scenario

Parameter	Value
Number of Electricity-Meters/EndPoints	240
Number of Coordinators (ZigBee networks)	5
Number of Bridges (one per coordinator not connected directly)	4
Number of Concentrators	2

4.1 Identification and Addressing

In this scenario, we need to be able to uniquely identify 240 nodes, each of them corresponding to a customer. This is a very small number, so if we consider the use of Virtual IP, a Class C IPv4-network would be enough. Scalability is one of the requirements for the solution, so we have to consider the possibility of future growth of the network as new EndPoints are added under the management of an existing concentrator. Here is where we make use of the advantages of IP hierarchy characteristics, so we can assign a different Class C network to each of the concentrators. Table 4 shows the addressing scheme. For this purpose, we make use of private addresses. There is plenty of space for adding new endpoints.

Table 4. EndPoint identification and addressing scheme

Network Parameters	Concentrator 1	Concentrator 2
Network	192.168.1.0	192.168.2.0
IP Address	192.168.1.1	192.168.2.1
IP Range for Bridges	192.168.1.10-192.168.1.20	N/A
IP Range for End-Points	192.168.1.128-192.168.1.254	192.168.2.128-192.168.2.254

For Virtual IP to work, a special gateway is needed which is going to be in charge to do the translation between IP addresses and ZigBee address. That way, the coordinator will receive a request in a protocol it can understand. One gateway is needed per concentrator. Now, when the middleware platform makes a request to one of the EndPoints, it only need to know the IP address of the node, and the request automatically will arrive to the corresponding concentrator, where the gateway will make the address translation and then send it to the appropriate coordinator.

4.2 Capacity Planning

We already calculated, in Table 2, the requirements about number of nodes (endpoints), number of ZigBee coordinators and the number of needed concentrators. Now we are going to calculate what are going to be the amount of information to be handled by each device and, consequently, the capacity requirements on the communications links. This is calculated for meter readings and firmware updates.

Table 5. Total traffic to be managed by each element of the network

Network Element	Energy Reading	Firmware Update
Node (endpoint)	60 bytes	60 Kb
Coordinator	3 Kb	3 Mb
Bridge	3 Kb	60 Kb
Concentrator 1	2.88 Kb	60 Kb
Concentrator 2	11.5 Kb	240 Kb
Management Server	14.38 Kb	120 Kb

We assume mean values for coordinators and bridges, that is, they handle about the same amount of information regardless if they are alone or grouped under a concentrator. On the other hand, this design corresponds to a distributed network, so firmware updates only needs to be sent once to each concentrator, and this device is in charge to send the necessary copies to each endpoint.

The requirements on the amount of information are not so big, and this mainly reflects the fact that this is a small example. If we consider a complete deployment for a modern mid-size city, we can end up having about 2 millions electricity meters. For such condition, it would be needed around 10.000 concentrators, each having to manage 12 Kb. This implies a total of 120 Mb on the management server. Special care has to be taken, because some connections between a concentrator and the core could be over a GPRS connection, which has important restriction of bandwidth.

5 Conclusions and Future Work

Throughout this article we have presented an IT platform for remote management of electricity meters, covering deployment and security of the platform.

The implantation of this platform will enable electric companies to develop sophisticated billing schemes, helping to mange smartly and more efficiently the great differences that companies have to face between supply and demand of electric energy during a day. This energetic efficiency will make big savings for the companies, end-users and with no doubt, for energy resources in the world. The key

of the solution is the ability to do real-time and on demand electricity consumption readings. Another great advantage, besides the energy efficiency, is that electric companies will have the opportunity to offer new services, like differential billing, on-line service management and promotional offers with minimal operational costs.

ZigBee is a low-cost and low-power wireless technology that perfectly suits the requirements for the last mile segment, which are related to the geographical disposition of the meters and low traffic generated by them. Moreover, if we combine ZigBee with better-cover wireless technology such as Wi-Fi, WiMax, GPRS and/or UMTS, we obtain a complete solution for the remote AMR system. There is no need for expensive deployments of wired networks.

Unlike the standard and well-know data networks mentioned above which have better range, ZigBee does not support the TCP/IP stack, which generates problems for addressing and identification of the endpoints. Fortunately, these problems are resolved by the use of virtual IP addresses, which provide network hierarchy and transparency to middleware.

This platform could be extended for the use of other utilities companies, like gas and water. It is also possible to do remote readings of water or gas meters, as long as they can be integrated with sensor networks technologies. The communications system has been designed to be flexible and to be able to support the integration of other meter equipment. Nevertheless, it is quite important to take into account that these other purposes, most probably will have special requirements. Just to mention one, water or gas meters cannot draw electric power from the very service supply like electricity meters do, thus introducing new challenges worth a specific analysis before adopting this platform to the new scenario.

Acknowledgements

The presented work was mainly done within the research project IRIDIUM [7], which was partly funded by the Spanish Ministry of Industry, Tourism and Trade under the contract TSI-020400-2008-152. The authors would like to thank all the members of the project that contribute with fruitful discussion.

References

1. European Parliament: Action Plan for Energy Efficiency: Realising the Potential (2007/2106(INI))
2. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC4944, IETF
3. Raymond, D.R., Midkiff, S.F.: Virginia Tech:Denial-of-Service in Wireless sensor Networks: Attacks and Defenses (January-March 2008), http://www.ieee.org
4. ZigBee Alliance: ZigBee Specification (January 2008), http://www.zigbee.org
5. ZigBee-PRO Stack Profile: Platform restrictions for compliant platform testing and interoperability (January 2008), http://www.zigbee.org
6. 802.16g-2007 IEEE Standards for Local and metropolitan area networks, http://standards.ieee.org/getieee802/download/802.16g-2007.pdf
7. Project IRIDIUM, http://www.amr-iridium.com/