

## **I. INTRODUCTION**

Smart Grid is defined as the modern infrastructure of the electric grid, whose objective is to improve efficiency, reliability and security. This is achieved through the control automation of the transmission and distribution lines, the enhancement of consumption metering technologies, the implementation of new renewable energy sources and new energy management techniques [1]. The growing demand of energy, changes in global weather, problems in the storing and distribution, and the need to implement more efficient consumption metering systems, are some of the factors that have led to transit towards a more complex and robust electric grid.

One of the main motivations for the transition towards a more automated, modern and efficient electric grid is the information exchange, in real time, between the Utility and the customer premises. At the same time, the improvement in the response time to network faults, natural disasters, interference problems and energetic resources loss, constitutes a strong reason to structure an electric grid with better energy transport, generation and distribution technologies.

On the other hand, due to the emerging energy crisis, caused by the depletion of fossil fuels and the corresponding reserves, global attention has been called to find alternative renewable energy sources, so that the industry can be sustained in the long term [2]. It is in this context that the concept of SG arises as a strategic solution to the energy optimization problem, since it is proposed that this new type of electric grid responds, in a dynamic and periodic way, to changes in the energy load that is being consumed. The new business model that now involves the client (who can be a consumer as well as a producer), would allow energy provision depending on climate changes, number of appliances switched on, and peak hours [3]. By these means, SG constitutes itself in the next generation of electric grid systems, that will incorporate different renewable energy resources, automatic and intelligent management of the energy and a more effective and interactive communication with the client.

To achieve the aforementioned features the integration of a bidirectional communication infrastructure is imperative. Through an advanced metering infrastructure (AMI), which results from the integration of advanced sensors, smart meters, monitoring systems, and energy management systems, a bidirectional communication between the Utility and the final users is enabled. This two-way data flow allows the sending of commands and information in real time to smart meters, as well as the reception of consumption information at the Utility's side [4]. Nevertheless, it is probable that in the future, the exchange of information between devices involved in the AMI might not be only related to client's consumption, or the control performed over the smart meters. Thus it is critical for the Utility to define the communication requirements and the more suitable technologies for implementing a suitable bidirectional communication system. In general, it is possible to distinguish two types of communication technologies based on the physical media used for the data transmission: wired and wireless. In each type, several advantages and drawbacks are identified, which are derived from the very nature of the physical media. In the case of wireless technologies, the deployment infrastructure is low cost. These technologies are especially useful to facilitate the connection in tough or unreachable areas. However, signal attenuation and functionality battery-dependent are their main drawback. On the other hand, as main advantage of wired technologies we can mention that they're less susceptible to interference problems (with the exception of PLC, a topic to which we shall return later). Lower flexibility to reach hard zones (for instance, rural zones) may be their most outstanding drawback.

The chosen technology should be adapted well to the kind of traffic that will be transported. For this purpose, two types of information infrastructure have been defined within the AMI: the first one is the dataflow from the sensors or electric devices to the smart meters; the second dataflow is between the smart meters and the data centers at the Utility side. Thus, on the basis of the type of dataflow that is being treated, the more suitable technology should be chosen. Concerning the communications between the electric appliances at the Client side and smart meters, ZigBee, Z-Wave and 6LoWPAN can be resorted to as

technological standards for its deployment. With regard to the second information flow, an alternative such as cellular networks (3G, GPRS, GSM), Wireless Mesh Networks (WMNs) and PLC have been considered as suitable technologies for this segment.

It is particularly important to identify in which environment the AMI is intended to be deployed, as well as advantages and drawbacks of the communication technologies, so that a choice according with the particular needs of each scenario and dataflows can be made. The choice of technology will be subject to diverse factors, such as the deployment's time and process, the nature of the environment (rural/urban) and the operational costs derived from the implementation.

In this article, we propose to outline the main features of the Advanced Metering Infrastructure (AMI), including communication technologies, topologies for deployment, and routing requirements. The overriding importance of the abovementioned subjects lies in the benefits that accrue for both Utilities and consumers, when enhancing the distribution system's efficiency. On the one hand, Utilities will benefit from an automated information gathering system, reducing thus operational costs, as the system will collect and process data from the smart meters to its collectors located in strategic points within the service territory. Not only will the Utility benefit from an automated system for information gathering. A better understanding of how AMI works will allow utility to have a reduction in costs arising from lines losses (thefts and other kinds). On the other hand, users will have a better service experience as the two-way communication scheme enables a more interactive communication with the service provider. A decrease in operative costs and a better knowledge of their consumption patterns and electricity price in real time will also lead to reduced bills for residential and industrial customers.

We will also discuss networking issues related to the implementation of AMI in different deployment scenarios. For this purpose, communication requirements for the IP-based AMI network (such as scalability, interoperability, and latency, among others), routing strategies for data packets forwarding (in particular the ones proposed by the IETF 6LoWPAN,

## **Evaluation of technologies and routing mechanisms in AMI networks**

Survey – Prepared by Diego Ramírez

Mesh-under and Route-over) and a full analysis of network performance in different scenarios are introduced.

## II. ADVANCED METERING INFRASTRUCTURE (AMI)

The Advanced Metering Infrastructure (AMI) is a component of the Smart Grid, which provides a two-way communication between the Utility and the HANs (Home Area Networks) at the customer side. The main purpose of this building block in the whole system is to measure, gather and analyze energy consumption as well as patterns of energy use. The main components of the AMI system include smart meters, a Meter Data Management System (MDMS), a communication network, access points and a head-end [7][8]. While utility companies use their own AMI backhaul communication networks on a general basis, it is now required for the new communications architecture to be IP-based in order to guarantee interoperability with standard applications. AMI communications network is usually categorized into three main types: Home Area Network (HAN), which serves as communication infrastructure for sensors and devices inside home; Neighborhood Area Network (NAN), which connects smart meters and data collectors; and Wide Area Network (WAN), which communicates data collectors with a utility control center. [9]. A view of a typical AMI deployment is depicted in Figure 1.

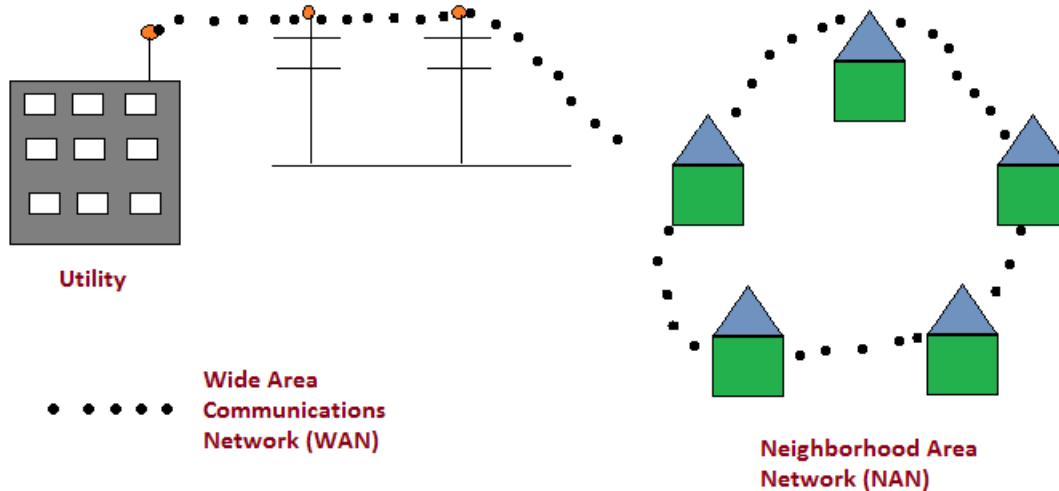


Figure 1. Basic AMI deployment

As stated before, the AMI break into one of three main systems: Wide Area Networks (WANs), Neighborhood Area Networks (NANs) and Home Area Networks (HANs). NAN handles the bulk of regional data, while the WAN connects the NAN to a control or data center. All messages are stored and analyzed in a MDMS (Meter Data Management System) at a head-end. NAN is, therefore, the core of the AMI communication, as it provides the two-way communication paths to the utilities' meters or endpoints. Although the two predominant technologies are PLC and Radio Frequency (RF), many other wireless technologies are being considered for the AMI NAN (e.g. ZigBee, Wi-Fi, Cellular networks etc.). With regard to wired technologies, two different sets of standards to power line networking can be identified: home users and industrial controls. In relation with this, NIST has included IEEE 1901, HomePlug AV and ITU-T G.hn as “Additional Standards Identified by NIST Subject to Further Review” for the Smart Grid in the U.S [9].

The AMI must support different types of traffic, coming from different sources (meters, data collectors, Utility). Therefore, the AMI network must fulfill specific requirements to meet the needs of different traffic nature and to face the constraints of limited bandwidth and comparatively low-capacity of some devices (in terms of memory, processing capacity, etc.). The main requirements for the IP-based communication network deployed in the AMI are as follows [7]:

- **Interoperability:** With the purpose of making possible the communication between segments using different technologies and networking protocols and with the aim of providing end-to-end services, the IP suite and protocols should be standards-based.
- **Scalability:** Supporting large and dense deployments is a must in the Smart Grid.
- **Security:** Given the fact that the meters transmit information on a regular basis, the network must provide security to the data transfer. Security services must be provided at both the network and the application layer, in order to cover different types of traffic [8]. Real time information about neighbor's energy consumption habit, for instance, would be a kind of data that must be protected (as the visibility of this information from third parties would constitute an invasion of privacy).

In this respect, the implementation of efficient routing strategies becomes paramount to guarantee that the information reaches its final destination. In order to face this problem, several protocols have been designed, each one of them according to routing requirements such as: interoperability, reliability, security, availability, scalability, quality of service and effective packets delivery [10]. Routing should be more or less robust, depending on the type of technology used for the AMI implementation. Given the fact that the AMI network is an initial approach to a SUN (Smart Utility Network), the main characteristics of these kinds of networks and the most important routing requirements are discussed in this article.

### ***Design Factors of the AMI Network***

Due to the evolution of the electrical grid, specifically electricity metering, a two-way communication network has been required. Applications such as smart metering, demand response (DR) and remote disconnect/reconnect require a communication network that supports them, as well as future application that will become prevalent, such as the sending of information about prices in real time from the Utility to the consumer's home or electrical vehicle charging stations.

Aspects regarding the choice of technology in which the AMI will be deployed, the constraints of the routing protocols and system capacity limits are some of the issues that must be addressed through a proper network planning. This plan requires the use of best practice guidelines for the design and deployment of the AMI. An outline for the main factors to consider when designing AMI networks is as follows:

- Understanding the networking needs and goals of the Utility
- Identifying the main design constraints of the AMI vendor's equipment (in terms of hardware and software capacity).
- Pilot installation, field testing, and site infrastructure exploration
- Model tuning within design software
- Design of the AMI network
- Deployment, Testing and Post-Design Adjustments

Given that each Utility will have different needs and expectations on the behavior of their network, and considering the varying constraints on performance requirements, a fully understanding of these goals and success criteria must be taken into account when designing the AMI. The design of the AMI Network should then consider factors such as: compatibility with the AMI communication protocols, production costs, network topology, and adaptability with wireless and wired communications, fault tolerance, hardware constraints, power consumption, environment, and transmission media. These requirements will affect the design process, as they will define the approach to meet the Utility's expectations.

In relation to the definition of the vendor's equipment, the creation of the link budgets for the various types of devices that will be used in the network deployment is the first step. This process includes accounting for transmit power, receive sensitivity, antenna gains, cable losses and meter location losses. In the case of a mesh approach, hopping limits, capacity limits, transmission requirements of radio and battery capacity are some of the issues that must be considered, as the influence of all these elements in the system affect the maintenance requirements and operation expenses for the Utility. Also, computer-aided design tools may be required for simulation, dimensioning and placement of infrastructure equipment purposes. Through this kind of tools, the model of the network is created and then the planning of the whole system's architecture can be deployed in the service area destined for that aim.

Another integral part in the design process is setting up a pilot system. In [25], a set-up of test transmitters in multiple locations within the service area is recommended. Execution of field measurements by testing the link configurations such as collector-to-meter, collector-to-repeater, and meter-to-meter is also proposed, in order to get a general view of the system performance.



### III. COMMUNICATION TECHNOLOGIES IN THE AMI

In this section, we intend to address the communication technologies used for the AMI deployment. A more detailed analysis is performed regarding the technologies in the NAN domain.

#### *ZigBee*

There are several technologies that are now under consideration for the communication network in the SG. Some of them have been established by consensus of the scientific community and the industry. Such is the case of ZigBee [5], wireless communication technology that is considered ideal for the real time monitoring of multiple targets, due to its low power consumption, low deployment cost, self-organization and self-configuration characteristics. Therefore, ZigBee is especially useful as deployment technology for HANs (Home Area Network) [6]. It's important to note that many providers of devices used in the AMI prefer smart meters on which the ZigBee protocol can be integrated, embracing the recommendation of the NIST (National Institute of Standards and Technology). This technology is defined by the IEEE 802.15.4 standard. Main technical specifications, advantages and drawbacks of this technology are described below:

1. *Technical specifications:* It has 16 channels in the 2.4GHz band, each with 5MHz bandwidth. The maximum power out of the radios with a transmission range between 1 and 100m is 0Dbm (1mW), with a data rate of 250 Kb/s, in OQPSK modulation [6].
2. *Advantages:* Due to its simplicity, mobility, robustness, low bandwidth requirements, low deployment cost, easy implementation and the fact that it operates over a non-licensed spectrum band, ZigBee is considered a good option for the metering and management of energy.
3. *Drawbacks:* Regarding the restrictions of this technology, we can cite its low processing capacity, a limited memory, low latency performance and the interference caused by other devices using the same transmission media. ZigBee is then vulnerable to noise.

## **IEEE 802.15.4**

This standard specifies PHY and MAC layer for LR-WPANs (Low Rate- Wireless Personal Area Networks). Physical layer is divided in two layers: PHY data service and PHY management, whose main function is to transmit and receive messages through the radio medium. On the other hand, MAC layer provides two main services: MAC data service and MAC management service. Both of them allow the transmission and reception of frames (MPDU), through the PHY data service. Functions such as channel switching, energy detection measurement, clear channel assessment, security functions (AES encryption) and QoS (Quality of Service) through a (GTS) Guaranteed Time Slot are some of other features of this standard.

### *Technical specifications:*

- Frequency band: 868 MHz/915 MHz and 2.4GHz
- Raw data rate: 868 MHz: 20kbps; 915 MHz: 40 kbps; 2.4GHz: 250 kbps
- Channels: 11 in the 868/915 MHz ; 16 in the 2.4 GHz
- Range: 10-20 m
- Latency: Down to 15ms
- Addressing: Short 8 bit or 64bit IEEE
- Channel access CSMA-CA and slotted CSMA-CA
- Modulation technique: DSSS (Direct Sequence Spread Spectrum)

## **IEEE. 802.15.4g**

It's an amendment to IEEE 802.15.4 whose objective is to provide a global standard that facilitates very large scale process control applications such as the ones found in Smart Utility Networks, capable of supporting large, geographically diverse networks with minimal infrastructure and millions of fixed endpoints. This standard was published in May 2012 and features the following technical specifications and operating modes:

- It accounts for the performance characteristics of SG networks, such as moderate bandwidth but very low latency
- It addresses SG geographic requirements by defining appropriate power levels
- It increases data rates formally to hundreds of kbps, and even Mbps, thus broadening the applicability of mesh systems beyond AMR and AMI to support the full sweep of smart grid applications.
- The standard defines technologies supporting up to 1 Mbps
- It establishes a global standard by explicitly including unlicensed and region-specific frequency ranges, or spectrum bands.
- It supports for Frequency Hopping Spread Spectrum (FHSS) transmission techniques.

Among the main advantages and drawbacks of this technology we can find:

- 1) *Advantages:* Because of the backward compatibility built into the standard, utilities hardware can be integrated with no changes, so their investment in the technology is protected. IEEE 802.15.4g addresses SG outdoor reliability, interference resiliency and high density operation by FHSS techniques, thus allowing a vast improvement over historical not so reliably wireless technologies.

### ***Wireless Mesh Networks (WMN)***

A WMN is a flexible network consisting of a group of nodes, in which every node acts as an independent router. In the case of the AMI network, every meter constitutes a router. The self-healing characteristic of this type of network, allows the communication signals to find alternative routes through the active nodes, in the event that some of the other nodes fail. Thus, each meter acts as a data forwarder until data reach the collector. Once the data have been collected, they are transferred to the Utility via a communications network. Some of the advantages and drawbacks of this technology are described below:

1. *Advantages:* This kind of technologies provides a cost-effective solution, as it improves the network performance, balances the load and extends the range of coverage by taking advantage of its self-organizing, self-healing and self-configuration characteristics. Due to each node acting as a repeater, the technology provides a good performance in the scalability and adaptability requirements.
2. *Drawbacks:* The most pressing issues of this kind of technology are identified in the urban environment. On the other hand, as sometimes a third company is required for the network management, security becomes a particularly important issue to face. Finally, possible problems of loops could generate excessive control information that, eventually, may result in bandwidth compression.

### ***Cellular Networks***

Cellular Networks may be a suitable option for the communication between the smart meters and the Utility, as they use the existing infrastructure, thus avoiding incurring in additional installation and deployment costs. Among the main cellular communication technologies employed for AMI are: 2G, 2.5G, 3G, LTE, GSM, GPRS and WIMAX. This kind of technologies has a high-capacity of bandwidth and, consequently, they can also support several QoS requirements.

1. *Advantages:* When outsourcing the communications network to a mobile operator, utilities can significantly reduce operative costs, as they don't have to bear the cost of deploying and maintaining the infrastructure. Data rates for cellular technologies-based AMI projects are now much more competitive. On the other hand, coverage provided by cellular networks is another outstanding advantage, which helps to improve network capabilities. Thus, because of the fact that the cellular network infrastructure already exists, the Utility does not have to incur in additional costs for building infrastructure. Due to the significant amount of information that is transported between the Utility and the Client, a large bandwidth capacity is sometimes required (such is the case of 3G, 4G and WIMAX), which is provided by

these cellular networks. In general terms, the low maintenance costs and fast installation are the main advantages of this technology.

2. *Drawbacks:* The main drawbacks of cellular networks are associated to information security. As the physical medium used for transmission is susceptible to interceptions, sensitive information (such as contractual data or bills) must be protected, to guarantee that it reaches its intended recipient with no understanding by other individuals or devices attempting to intercept it. On the other hand, particularly given that the communication channel in the SG is shared with users of the mobile telephony, the network performance may be impaired. Finally, in adverse situations such as wind storms, the service could not be guaranteed, neither the communication in the SG. Moreover, transmission through cellular networks still has a high cost, especially when SMS is used as communication media between smart meters and data collectors.

### ***GSM***

Global System for Mobile Communication (GSM) is an open digital cellular technology used for transmission of mobile voice and data services. It makes use of TDMA (Which stands for Time Division Multiple Access) as access method for signals transmission. Advantages and drawbacks of this technology are stated below:

1. *Advantages:* Among the reasons to choose GSM as communication technology are the improved spectrum efficiency, low-cost sets and base stations, compatibility with ISDN and a large population of subscribers.
2. *Drawbacks:* While GSM is intended to be a secure wireless system, it is completely vulnerable to several attacks, each of them aiming a part of the network [14]. Hereunder, security constitutes one of the main drawbacks of this technology, as user authentication and encryption do not seem to be enough for the robustness of the entire network, and several techniques must be addressed in order to face security threats.

### ***Power Line Communication (PLC)***

PLC is a technology that uses the existing electric grid to enable high-speed data transfer (2-3Mbps). This is why PLC is considered a natural solution for the communication aspect between the Utility and the Smart Meters, as the implementation investment is low, as long as the power lines are used as physical transmission media.

In a typical PLC network, the smart meters are connected to the data center through power lines and the data are transferred to the collectors via cellular networks like the ones stated above. The choice of technology is then based on the network part intended to be covered: for the Smart meters - Collectors PLC is realized to be a good candidate; for the Collectors – Utility's data centers cellular network communication such as GPRS or GSM may be suitable choices.

### ***Technical specifications***

Two main types of communication architectures based on PLC have been defined: NarrowBand PLC (NBPLC) and Broadband PLC (BPLC). The first type allows data transmission at lower rates than those provided by BPLC (from few dozens of kbps to 100 Mbps, respectively) [6]. Narrowband power line communication (N-PLC), systems generally use the CENELEC (Comité Européen de Normalisation Electrotechnique) bands (3-148.5 kHz). N-PLC generally operates in transmission frequencies of up to 500 kHz (as opposed to Broadband PLC that targets much higher bandwidth at shorter distances and operates over a much higher frequency band). Frequencies of 148.5 kHz and less have been recognized by CENELEC standards for use in N-PLC systems on a public utility's power wires.

Regarding the Broadband PLC (B-PLC), the operation bands go from 1.8 MHz up to 250 MHz. Some examples of BB-PLC technologies are described in IEEE 1901 and ITU-T G.hn (G.9960/G.9961) recommendations. B-PLC generally refers to PLC systems supporting data rates over 1 Mbps.

The main advantages and drawbacks of this technology are stated below:

1. *Advantages:* The main advantage of this technology is associated to the low implementation costs. Additionally, the coverage provided by PLC is exactly the one intended by the Utility, because of the fact that the existing infrastructure allows the implementation of services in the SG (smart metering, monitoring and control applications). On the other hand, as the power lines are owned by the Utility, there's more independence in relation to other operators or networks.
2. *Drawbacks:* The very nature of the physical transmission media generates some challenges. The main disadvantage of this technology is the high susceptibility to signal degradation, due to the harsh power lines. The technology is also limited by its low bandwidth (around 20 kbps), which is why it's not suitable for more robust applications that may require higher bandwidth capacity.

### ***Digital Subscriber Lines (DSL)***

DSL is a high speed digital data transmission technology which main feature is the use of the wires of the voice telephone network. As with PLC, this technology seems to be a suitable candidate for the implementation of network segments within the AMI, as it reuses the existing infrastructure, thus reducing installation cost of an implementation from scratch. As for the technical specifications, the network performance and perceived throughput will depend on how far away the subscriber is from the serving telephone [1]. Main advantages and drawbacks of this technology are listed below:

*Technical specifications:* Commonly, the frequencies on which this technology works are greater than 1MHz through an ADSL enabled telephone line.

- 1) *Advantages:* With a high data transmission rate, and given the low installation costs for the network deployment, DSL is a good option for the AMI implementation.
- 2) *Drawbacks:* Distance dependency and lack of standardizations are the primary constraints of this technology.

### ***ETHERNET***

It's a very common communication technology standard primarily used within the HAN, but can also be used on the WAN. A variety of speeds can be achieved, including 10Mbps, 100Mbps, 1000Mbps and 10000Mbps. While 100Mbps is the most common speed found in the HAN, 1000Mbps is becoming more extensive, since Video and Network Attached Storage are being more prevalent applications.

- 1) *Advantages:* Being standard-based, set up and configuration are easier.
- 2) *Drawbacks:* This technology may not be appropriate for connecting all devices in the HAN, due to the high cost and power requirements plus the need for separate cabling back to a central point.



## IV. ROUTING

As a first development phase of smart grid involves the implementation of an Advanced Metering Infrastructure (AMI), which is expected to provide a two-way communication path between utilities and consumers, a deployment of a network connecting a dense number of nodes (meters) with data collectors is needed. But most importantly, such mesh based AMI network should provide efficient and suitable routing functionalities, which guarantee a reliable and effective delivery of packets. Regarding the traffic involved in the two-way communication channel, two types of traffic can be identified: 1) inward unicast traffic, consisting of data containing the meter-reading, going from homes to Utilities' data collectors, and 2) outward unicast traffic, consisting of data containing data going from collectors to substation or the Utility itself.

The importance behind the implementation of efficient routing strategies and protocols lies in the need of an effective data packet delivery mechanism. It is required that data transmitted between nodes in the WMN reach the final destination (data collector), so that such information can be successfully received by the Utility, through the bidirectional communication channel outlined under the AMI concept. In [6] routing protocols have been classified, according to the AMI component in which they are used (HAN, NAN or N2N). As a consequence, several routing protocols and strategies are specified.

### ***RPL***

In this part of the AMI, the routing protocol must guarantee low energy consumption; assure privacy and information security, as well as supporting self-organization and self-configuration features. For this purpose, IETF has proposed RPL (Routing Protocols for Low Power and Lossy Networks) [11]. This protocol is of the distance-vector type, and is based on IPv6. It was designed considering the requirements specified in RFC 5826, RFC 5673, RFC 5548 and RFC 5867 [10].

In [29], a detailed RPL implementation for AMI networks is presented. The authors considered a static multi-hop wireless AMI network that consists of  $n$  meter node and one gateway node. In the proposed protocol, a DAG structure is maintained at the gateway

node. Once the information that must be stored and maintained by each node is defined, the data traffic forwarding rules are introduced. Then the authors provided a detailed characterization for the DAG construction and maintenance, as well as an ETX measurement scheme based on MAC layer mechanism. Finally a reverse path recording mechanism is proposed, in order to enable routing support for outward unicast traffic, which flows from the gateway to each meter.

D. Wang et al [29] also presented a practical implementation of RPL that aims at providing reliable and low-latency routing support for large-scale AMI networks, through the integration with CSMA-based MAC layer protocols. The authors adopted the Expected Transmission Time (ETX) as the link metric, and proposed a novel ETX-based rank computation method to provide high end-to-end reliability in AMI networks.

One of the main advantages of this protocol is that it does not define a unique routing metric, but gathers a set of metrics. This is a must in the AMI network, given its heterogeneous and diverse nature. Multiple devices involved in the AMI, as well as the different types of applications uploaded to the network, entails a need to define several types of metrics to ensure the protocol efficiency in all cases. For this purpose, an objective function (OF) is defined, in which a set of metrics are combined.

The main idea behind RPL is to maintain information about the network status using one or more directed acyclic graphs (DAGs). A DAG is a directed graph in which all edges are oriented in such way that no cycles exist. For each DAG created in RPL there's a root. The DAG's root is typically the Gateway in the AMI network. All edges in the DAG are contained in the routes oriented to the root node. Each node in the DAG is associated to a Rank or value. For the construction of the DAG, the Gateway will create control messages called DIOS (DAG Information Object). The main functions executed by the DIO messages are listed below [10]:

- a) To identify the DAG from which any root is originated
- b) To spread the Rank information of the starting node
- c) To define the objective function (OF) that specifies the metric or the combination of metrics used to compute the Rank in each node.

Once multiple DIO messages have been received, a node will compute its own Rank and will determine its position in the DAG. One way to compute the Rank is utilizing ETX as a metric. ETX will measure the quality of a route between two nodes, by estimating the average number of required transmissions to send data packets to a neighbor. As nodes in a wireless sensor network (like AMI) are susceptible to multiples faults, RPL builds a Destination Oriented DAG (DODAG) with several routes from each node. This contributes to enhance the performance and robustness of the network, as well as to guarantee quality of service and to handle traffic in real time [13].

### ***Geographic Routing***

In this routing principle paths can be discovered through the node coordinates. For this purpose, GPS receivers are required, as well as the use of hard coding. Among the drawbacks of this protocol, we can mention that the GPS devices have a high price, as well as the immediate consequence derived from the use of hard coding, in which the coordinates can't be changed. This may result in a problem, as consumer's locations may change. In general terms the determination of geographical location is a challenging task [6].

Gopalakrishnan [10] presented a performance analysis of Geographical routing in AMI networks, through a simulation set up. The author considered this protocol because of the fact that it has been widely used in smart utility networks and AMI deployments, currently running in over 2 million metering end-points. For analysis purposes, a 100 node derived from a rurally deployed real AMI network was set up. Several data such as the computed ratio of total transmitted packets to those received by each node, the packet success probability and latency were collected.

Geographic routing considers packet forwarding by means of position information instead of network addresses and routing tables. The destination location is utilized to route the packet. Through the neighbor's location, each node can select the next hop that is closer to the destination (specified by its location). One of the main advantages of this routing protocol is that routing tables maintenance and route discovery are unnecessary activities, as the packet forwarding function is only based on geographic information. Three

assumptions are required for geographic routing to be performed: i) A node can determine its own position; ii) A node is aware of its neighbor's positions; and iii) The position of the destination is known [15].

Regarding the determination of every node's position, GPS devices are the main tools utilized for making position information available. On the other hand, to enable the node's awareness of its neighbor's positions, a broadcasting of the position information to other nodes in the network is required. Finally, in order to determine the position of the destination, a location service mapping network addresses to geographic locations is needed (excepting in cases in which the destination inherently knows the location, like in some sensor network applications, where a node can collect some measurement information). Thus, if a positioning system already exists geographic routing provides a scalable solution for routing in wireless networks.

### ***AODV***

Ad Hoc On-Demand Vector routing protocol builds on the Destination-Sequenced Distance- Vector [DSDV] algorithm and is based on the RFC 3561[12]. AODV creates routes on demand basis by minimizing the number of required broadcasts unlike the DSDV algorithm which maintains a list of routes. This algorithm is an improvement to DSDV algorithm. AODV is also called as a pure on-demand routing acquisition system because only the nodes which are on the selected path maintain the routing information are involved in routing table exchange. When a source node wants to communicate with some destination node but does not have a valid route to that destination, the source node then initiates a path discovery process to discover the other node. To achieve this, source node broadcasts Route Request [RREQ] packet to its neighbors. This request is in turn sent to its neighbors and so on until either the destination route or an intermediate node route to the destination is traced. This protocol uses hop count as routing metric.

In [31] a test-bed implementation of AODV in an AMI small scale scenario is presented. In the simulation the nodes were placed at distances such that the transmitted signal was only

received by the neighboring nodes. As the number of hops increased, the throughput decreased, which is quite obvious due to the routing overheads increment. Regarding the scalability of AODV, it was tested in a large scale string scenario, showing an inverse relationship between the throughput and the number of nodes. A modification of the protocol, where some nodes are provided more intelligence than the others, contributes to lower latency than regular AODV, making it a useful protocol communication for certain current and future AMI applications.

### ***DSR***

Dynamic source routing protocol is an on-demand routing protocol and is based on the concept of source routing. It is based on the RFC 4728 [33]. In this protocol, a node maintains a route cache which contains source routes that is known by all other nodes. The route cache is continually updated as new routes to the source are learnt by the nodes. This protocol maintains two major phases: Route discovery and Route maintenance. Whenever a node has to send a packet to some destination, it initially checks the route cache to find out whether the route to the destination is already known. If the route to the destination is already present in the route cache, it uses the same route to transmit the packet. On the other hand, if the route to destination is not present in the route cache, then the node initiates route discovery by broadcasting a route request packet. This route request packet contains destination address, source node's address and a unique identification number. Each and every node checks if it has the destination route to the address sent in the route request packet. If the node does not find the destination route in its route cache, it adds its own address to the route record packet and forwards the packet to the nodes among its outgoing links. A route reply is generated only when the route request packet reaches the destination or an intermediate node containing the route to the destination in its route cache.

If the route reply is generated by the destination, then the destination places the route record contained in the route request into the route reply. If the route request is responded by an intermediate node, then it will append its cache route to the route record to generate the

route reply. The responding node must have a route to the initiator in order to send the route reply. If the responding node has the route to the initiator in its route cache, then it should use that route. Otherwise, if symmetric link is supported, then the node must send the route reply by using the reverse route in the route record.

### ***DADR***

Distributed Autonomous Depth-First Routing (DADR) [21] is a proactive distance vector protocol that uses a control mechanism to provide at most  $k$  (if available) paths for each destination. It also utilizes Depth First Search algorithm for path recovery in cases of link failure. As the data forwarding occurs, all the information learned is used to update the routing table. This happens during periodic Hello Messages exchanges among neighboring nodes, or when the nodes receive a route poisoning message. In order to control and detect loops, a unique FID (Frame ID) is added to a packet. Each time a node forwards a packet its FID is stored in the FID table, as well as the packet's sender and packet's next hop. Thus, if given a received packet, the node finds its FID in the FID table, it means that a loop is about to occur. When the loop is detected, a poisoning message is generated, so the other nodes in the topology are informed about the situation, making the route to be removed from their routing tables.

In [22] a simulation of scenarios of about 2107 smart meters was run, and an analysis of the routing protocol was tested in a 1500 node network topology. As for the reliability, the protocol shows the capability of learning new routes in both indoor and outdoor environments. On the other hand, the protocol doesn't need too much control overhead when updating routes, which is an advantage in a large-scale network. Finally, packet latency in a flat mesh network is affected by the several hops the data packet needs to travel forward to in order to reach the destination.

### ***HYDRO***

Hybrid Routing Protocol [23] is a link state routing protocol for Low Power and Lossy Networks (LLNs). It uses DAGs to provide multiple reliable paths to a border router. To

this end, each node builds its default route table by adding its neighboring nodes towards a border router. The entries in the route table will be ordered following an ETX metric. According to the top ranked entries of its default table, each node periodically creates a topology report. The nodes piggyback those topology reports on periodic collection traffic, allowing border routers to build and maintain a global view of the topology. The first primitive of HYDRO is the provision of a Default Route Table, which is made of a list of entries (each containing the link-layer address of a node in the direction of a border router). Thus, each node will have information about the link-layer packet success rates, so an evaluation of the quality of that link can be performed. This feature is especially crucial in the reliability requirement, as multiple routes are provided to a given destination. This is why HYDRO is both a centralized and distributed forward mechanism, as low-power nodes maintain a distributed DAG that provides them with a set of default routes for communicating with border routers, which will maintain a global view of the network topology (through the reports sent by each of the nodes).

In [23] a performance evaluation of HYDRO on different metrics was executed through the implementation of a set of testbeds and a real network deployment. In this last one, a 57 node network was set up with HYDRO as the running routing protocol, during six months. The workload consisted of each node transmitting every 1 minute to an external server. The statistics collected show that the PDR is an average 98.9%. As for the scalability, every node's state is bound by the number of destinations it communicates with.

### ***Hybrid Wireless Mesh Routing Protocol (HWMP)***

The Hybrid Wireless Mesh Protocol (HWMP) is the multihop default routing protocol for IEEE 802.11s WLAN mesh networking. With the purpose of allowing interoperability between devices from different vendors, HWMP serves a common path selection protocol for every IEEE 802.11s compliant device. The term hybrid is due to the use of both reactive and proactive approaches in the routing scheme. HWMP results from an adaptation of AODV called Radio-Metric AODV (RM-AODV), which, unlike AODV, works on layer 2 and uses a radio-aware as routing metric.

In [28] the route discovery process is explained, stating that when a node needs a path to a given destination broadcasts a route request message requesting a route to that destination. This route request message is processed and forwarded by all mesh points to the originator of the route discovery. The destination node or intermediate nodes with a path to the destination answer with a unicast reply message indicating the route requested. Finally the forward path to the destination is set up.

### ***Routing strategies in 6LoWPAN***

As IEEE 802.15.4 defines a standard that may support a potential technology for the deployment of the AMI, it becomes important to study the routing strategies stated by the IETF 6LoWPAN, which describes the way how packets of a larger size (as the ones of IPv6) can be transported through a wireless link that only accepts packets of a maximum 127 bytes size. 6LoWPAN introduces an adaptation layer between data link and network layers that enables the transition of IPv6 packets over LoWPANs. For this purpose, header compression and fragmentation of IPv6 packets is performed and mesh forwarding is also executed to deliver the packets from source to destination over a multihop scenario.

The importance of the study of these routing schemes lies on the fact that the wireless network thus formed is sensitive because capabilities of nodes are limited in terms of energy, processing, transmission range, etc. Depending on the layer in which the routing decision takes place, the data forwarding mechanisms can be classified as mesh-under or route-over. Following sections describe both schemes in more detail.

### ***Mesh-Under***

In this scheme, the network layer does not perform any IP routing. The forwarding decision is made at the adaptation layer which forwards the packet to the destination over multiple radio hops. In Mesh-Under scheme, routing and forwarding are performed at link layer based on 802.15.4 frame. To send a packet to a particular destination, 64 bit address or the 16 bit short address is used and sent it to a neighbor node to move the packet closer to the destination. Because multiple hops based on link layers are used to complete a single IP hop, it is called the mesh-under approach. An IP packet is fragmented by the adaptation



layer to a number of fragments. On the other hand, these fragments are delivered to the next hop by mesh routing to reach the destination. Different fragments of an IP packet can go through different paths and they are all gathered at the destination. If all fragments are reached successfully, then the reassembling of the IP packet takes place at the adaptation layer. In case of loss of any fragment, the entire IP packet (this is, all fragments for this IP packet) must be retransmitted to the destination for recovery.

### ***Route Over***

In route-over scheme all routing decisions are taken in the network layer where each node acts as an IP router. In route-over, each link layer hop is an IP hop. The IP routing supports the forwarding of packets between these links. In the forwarding process IP routing tables and IPv6 hop-by-hop options are used. For routing and forwarding processes the network layer takes decision using the additional encapsulated IP header. The adaptation layer of 6LoWPAN establishes a direct mapping between the frame and the IP headers. When an IP packet is fragmented by the adaptation layer, fragments are sent to the next hop based on the routing table information. The adaptation layer of the next hop checks received fragments. If all fragments are received successfully, the adaptation layer creates an IP packet from fragments and sends it to the network layer. If the packet is destined for itself, the network layer sends the IP packet to the transport layer, otherwise forwards the packet to the next hop based on the routing table information. If there are one or more fragments missing, then all fragments are retransmitted to one hop distance. After receiving all fragments successfully the adaptation layer creates an IP packet from these fragments and passes it to the network layer. The network layer then forwards or processes the IP packet based on the destination of the packet.

### **Metrics used for routing strategies comparison**

The communication infrastructure in smart grid undertakes important information exchange responsibilities, which are the foundations for the function diversified and location distributed electric power devices to work synergistically. Unsatisfactory communication

performance not only limits the AMI from achieving its full energy efficiency and service quality, but also poses potential damages to the grid system. To protect the AMI and ensure optimal operation, the communication infrastructure must meet a number of requirements.

### ***Latency***

The concept of latency refers to the maximum time in which a particular message should reach its destination through a communication network. It's important to state that the messages between various entities within the AMI may have different network latency requirements. Thus, while the protection information and commands exchanged between intelligent electronic devices (IEDs) in the distribution network will require a lower network latency, the information messages exchanged between electrical sensors and control centers may accept higher values of latency. Moreover, the messages exchanged can be event driven (e.g., protection and control related) or periodic (e.g., monitoring related) [11]. The network architecture and communication medium must support the diverse requirements. The network architecture will determine if the message sent from one communicating entity to the other will reach its destination in one or more hops. This will directly affect the latency. Similarly, the data rates supported by the communication medium also dictate how fast an entity can communicate an event observed or reply to a message received.

### ***Data delivery***

This refers to the criticality of arrival of packets throughout the network, and it will depend on the needs of the application. This need may be decided at the time of connection establishment between two applications. Different levels of data delivery criticality can be considered, as following: i) high, it is used where the confirmation of end-to-end data delivery is a must and a retry will be mandatory in case of absence of confirmation; ii) medium which is used where end-to-end confirmation is not required but the receiver is able to detect data loss; iii) non-critical, which will be used when data loss is acceptable to

the receiver. In this case reliability can be improved by repetitive messages. In this last case, the non-critical level can be used for periodic data for monitoring purposes.

### ***Reliability***

The grid stability will depend, to a great extent, on the reliability of the distribution network. Hence, it becomes extremely important for the communication backbone to be reliable, in order to enable successful and timely message exchanges. Different events may affect the communication backbone reliability. Some of these failures include time-out failures, network failures, and resource failures. A time-out failure occurs if the time spent in detecting, assembling, delivering and taking action in response to a control message exceeds the timing requirements [2]. On the other hand, a network failure occurs when there is a failure in one of the layers of the protocol suite used for communication (this is, the failure may be originated in a logical level, and prevent a packet to reach its destination in spite of the existence of a physical link). Other factors can affect the communication, such as noise and interference. Finally, a resource failure implies failure of the end node which initiates communications or receives messages. Hence, there is a need to assess the reliability of the system in its design phase and find ways to improve it.

### ***Security***

Taking into account that the AMI involves a distribution network that will be spread over large areas, and that the information that will transit throughout that network will be sensitive (as it can involve patterns of consumption from the customer, billing, etc.), the security of data becomes a great matter. Moreover, if a wireless communication medium (like WiFi or Zigbee) is used as part of the communication network, security concerns will be increased given the shared and accessible nature of the medium. Hence, to provide security protection for the AMI, it's important to identify different communication use cases (e.g., demand side management, advanced meter reading, among others.) and thus find appropriate security solutions for each case. As an example of that, we can cite the authorization of access to the real time data and control functions, but in order to prevent

spoofing in wide area communications, the use of encryption algorithms may be the right strategy to implement [6].

### *Time synchronization*

Some of the devices on the AMI need to be synchronized in time. The requirements for time synchronization of a device depend on different factors, such as the criticality of the application. For example, processes involving the measurement of phase units (PMUs) have the strictest need of time synchronization as they provide a real-time measurement of electrical quantities (voltage and current) from the Utility. This is why synchronization becomes an important issue as it involves control of different entities within the distribution network. Other examples of mechanisms that help to achieve time synchronization are the Precision time protocol (PTP), which is defined by the standard IEEE 1588 and provides time synchronization with up to nanosecond precision over Ethernet networks, as well as the Global positioning system (GPS).

### *Scalability*

This metric can be considered as the ability of a system to handle growing amounts of work in an efficient manner [19]. Most of the times the concern lies on the load scalability, which is the easiness for a system to increase its resources to accommodate the increasing load. For this purpose, it's necessary to define the specific requirements for scalability in this dimension. In our case, the way how we measure the scalability is regarding the ability of the routing table on a router (meter) scales with the number of nodes of the whole AMI network. It's also important to take into account that scalability is related to a more economically deployable system, and thus costs associated to the deployment of the network must be considered. Summarizing, the network of wireless nodes is expected to be quite large considering the scale of towers from the substation to residential units. The communication architecture must work equally well for a small network as for a large network.

### ***Ease of deployment***

This refers to the level of feasibility and easiness with which the network can be deployed utilizing a given routing protocol.

### ***Adaptability***

This refers to the ability of the routing protocol to adapt to different network topologies.

## **Performance Comparison**

In [10] a performance analysis of RPL and Geographic Routing in a Smart Grid context was executed, taking into account some of the metrics described above. In this analysis, OMNeT++ was used as the simulation tool to implement the routing algorithms in AMI scenarios, based on real topology networks. RPL was implemented to build the DODAG (Destination Oriented Directed Acyclic Graph) using ETX (Expected Transmission count) as the metric for rank computation. On the other hand, Geographical Routing was modeled using a combination of ETX and geographical proximity to compute routes. Links with a packet success probability of more than 60% were selected as potential neighbor nodes for each node. The distance between each neighbor node and the destination (collector) was computed using the Euclidean distance formula.

In the study mentioned above, simulations of RPL and Geographical routing algorithms were run for the 500 node real network with the application layer running a test case for gathering the statistics of hop count and end to end delay. The test case used for the performance analysis was constructed based on the scenario that each of the 500 nodes sends multi-point to point traffic directed towards the collector. The application packet rate was set at 1 packet/second. This was done sequentially to measure individual statistics. All other nodes in the network simply participated in the routing and were not allowed to transmit when one of the nodes was transmitting. Each node transmitted 100 packets with the collector as the destination. An average of 160ms and 173ms of delay were obtained for RPL and Geographical routing, respectively.

Regarding reliability, it was measured by computing the packet delivery ratio, defined as the total number of received packets at the collector over the total number of packets transmitted by each node. On this matter, RPL showed a constant packet delivery ratio between 98% and 100% for each packet and an average of 99.98% while Geographical routing showed similar performance with an average of 99.30% [10].

Other protocols such as DADR and HYDRO are also analyzed, considering their behavior in testbeds and real deployments, with respect to some of the metrics described before. Both protocols share a route-distribution approach. In [21] a study was conducted to determine how the protocol would work in a 1500 node network topology. The results showed that DADR doesn't need too much overhead when updating routes, which becomes an advantage in large-scale networks. On the other hand, the capability of learning new routes when link failures occur, as well as removing paths because of possible loops, make the protocol outstanding in the Reliability and Adaptability requirements. Finally, an average 97.8% PDR was obtained.

HYDRO, as a combination of both centralized and distributed forwarding mechanisms, shows in [23] a high reliability, as multiples routes are provided to a given destination. By constantly evaluating the qualities of the links, the protocol becomes robust in the Adaptability requirement, as any change in the topology is detected and the protocol reacts to it. A median PDR of 98,9% was obtained when examining the performance of the protocol in a 57 node real-world deployment.

A summary of the results explained results in this section can be observed in Table 1. A comparison of the six routing protocols described, considering the metrics explained in the previous section, is performed.

## Evaluation of technologies and routing mechanisms in AMI networks

Survey – Prepared by Diego Ramírez

	Similar performance for the given network size and traffic scenario. (500 Node Network)		Similar features: Discovery and Maintenance Mechanisms		Sharing distributed forwarding approaches		
	Geo Routing	RPL	AODV	DSR	DADR	HYDRO	HWMP
<b>Scalability</b>	High: >2Million metering end points	Implementation specific. (Factors such as trickled timer, operating mode, etc.)	Low. Transmission of hello messages in a large network can become flooding. High cost of processing	Low. Maintenance of routing tables in a large network have a high cost	High. 1500 Node network topology. The protocol doesn't need too much overhead when updating routes.	High. As the protocol is defined by both centralized and distributed mechanisms.	Low. When 25 or more nodes are in the network, congestions occur.
<b>Latency</b>	End-to-end delay: Avg 173ms	End-to-End Delay: Avg 160ms	High. Great amount of overhead generated (hello messages)	Better than that reached by AODV. Less Overhead	High. Data packets need to travel forward to several hops in order to reach the destination.	Better than the reached by DADR. The border router helps to forward packets faster.	End to end delay: 300ms for a 300 node network [6].
<b>Delivery Packets Rate</b>	High: PDR>99%	High: PDR>99.9%	To be Completed	To be Completed	High: PDR > 97,8%	HIGH: PDR> 98,9%	HIGH: PDR>96%
<b>Reliability</b>	High. Measured considering the PDR	High: Measured considering the PDR	To be Completed	To be Completed	High. Protocol shows capability of learning new routes when link failures.	High. Multiple routes are provided to a destination. Redundancy.	High. 95-98% reliability was obtained when 9 nodes were deployed, but the protocol outperform when the number of nodes increase to 25 or more.
<b>Adaptability</b>	Highly adaptable to different network topologies	High. routing paths from the nodes to the central points are constructed according to the deployed architecture	High. Expiration time feature helps to clean up table potential broken and out-of-date links information	High. Any change in the network is detected through the Maintenance Mechanism.	High. Routing paths are updated/removed/constructed according to the topology state.	High. As the protocol involves the evaluation of links qualities according to topologies changes.	Highly adaptable to different network topologies
<b>Routing scheme</b>	Mesh-Under	Route-Over	Mesh-Under	Mesh-Under/Route-Over	Mesh-Under	Mesh-Under/Route-Over	Mesh-Under

Table 1. Comparative analysis between Geo Routing, RPL, AODV, DSR, DADR, HYDRO and HWMP in AMI context.

As a primary conclusion, we could say that RPL is most likely to emerge as the imposing protocol as it is on its way to becoming a standard. In order to make this analysis more robust, several other factors such as home, industrial, in-building and outdoor routing conditions and metrics must be considered.

The choice of the routing protocol will then be considered taking into account the technology that is used for deployment purposes. Thus, a protocol might fit better than other, in a certain technology. For instance, in the case of a mesh technology, a protocol that involves end-to-end retransmission when a packet loss occurs wouldn't be too suitable, as the possibility of fragments loss is bigger in a multihop scheme.

## **V. FUTURE WORK**

It would be of a great value to test the coexistence of different traffic patterns, which is an important issue, as we mentioned before, given the very nature of the AMI concept. On the other hand the possibility to see tests and evaluations of simulated AMI deployments with real information regarding the energy usage of customers, would also be interesting, as this can have a great impact on the nature of the traffic and its intensity. It will also be an important research issue the determination of the applications that can be supported by each one of the routing strategies defined in this paper, for which different sets of metrics must be defined and evaluated. While meter readings are one of the main features of the AMI, it is also imperative the evaluation of other features and applications that will robust the AMI infrastructure in the near future. It can be concluded that new routing protocols must be designed with various applications in mind, and performance evaluation has to be more comprehensive. Finally, it is important to note that some projects for testing and deployment of SGs in real-world conditions are on the way. For example, Mitsubishi Electric has recently started full-scale tests in Japan on how to manage a large number of renewable energy resources in a power grid [16]. General Motors (GM) and OnStar have also launched projects, in both cases for managing the operation of electric vehicles [17].



## References

- [1] Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P., "Smart Grid Technologies: Communication Technologies and Standards," *Industrial Informatics, IEEE Transactions on* , vol.7, no.4, pp.529,539, Nov. 2011
- [2] Wang et al., 2011 W. Wang, Y. Xu, M. Khanna., "A survey on the communication architectures in smart grid", *Computer Networks*, 55 (2011).
- [3] Castellani, A.P.; Ministeri, G.; Rotoloni, M.; Vangelista, L.; Zorzi, M., "Interoperable and globally interconnected Smart Grid using IPv6 and 6LoWPAN," *Communications (ICC), 2012 IEEE International Conference on*, vol., no., pp.6473,6478, 10-15 June 2012
- [4] Deconinck, G., "An evaluation of two-way communication means for advanced metering in Flanders (Belgium)," *Instrumentation and Measurement Technology Conference Proceedings, 2008. IMTC 2008. IEEE* , vol., no., pp.900,905, 12-15 May 2008
- [5] ZigBee Alliance, "Understanding ZigBee gateway," *ZigBee Document 095465r13*, September 2010
- [6] Sabbah, A.; El-Mougy, A.; Ibnkahla, M., "A Survey of Networking Challenges and Routing Protocols in Smart Grids," *Industrial Informatics, IEEE Transactions on* , vol.PP, no.99, pp.1,1, 0
- [7] Jun Wang; Leung, V.C.M., "A survey of technical requirements and consumer application standards for IP-based smart grid AMI network," *Information Networking (ICOIN), 2011 International Conference on* , vol., no., pp.114,119, 26-28 Jan. 2011
- [8] Bennett, C.; Highfill, D., "Networking AMI Smart Meters," *Energy 2030 Conference, 2008. ENERGY 2008. IEEE* , vol., no., pp.1,8, 17-18 Nov. 2008 doi: 10.1109/ENERGY.2008.4781067
- [9] Cheng-Jen Tang; Miao-Ru Dai, "An Evaluation on Sensor Network Technologies for AMI Associated Mudslide Warning System," *Networking and Computing (ICNC), 2010 First International Conference on* , vol., no., pp.237,242, 17-19 Nov. 2010
- [10] Gopalakrishnan B. Iyer, M.S. Thesis, "Wireless Mesh Routing in Smart Utility Networks", Auburn University, December 2011
- [11] T. Winter and P. Thubert, RPL: IPv6 Routing Protocol for Low Power and Lossy Networks, draft-ietf-roll-rpl-04.txt, October 2009.
- [12] <https://www.ietf.org/rfc/rfc3561.txt>
- [13] Bogdan Pavković , Fabrice Theoleyre , Andrzej Duda, Multipath opportunistic RPL routing over IEEE 802.15.4, Proceedings of the 14th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, October 31-November 04, 2011, Miami, Florida, USA

- [14] Toorani, M.; Beheshti, A., "Solutions to the GSM Security Weaknesses," *Next Generation Mobile Applications, Services and Technologies*, 2008. NGMAST '08. *The Second International Conference on* , vol., no., pp.576,581, 16-19 Sept. 2008
- [15] S. Rü,hrup, &ldquo,Theory and Practice of Geographic Routing,&rdquo, Ad Hoc and Sensor Wireless Networks: Architectures, Algorithms and Protocols, Bentham Science, 2009.
- [16]<http://www.mitsubishielectric.com/company/environment/report/products/randd/smartgrid/index.html>
- [17] General Motors Smart Grid Pilot, [Online]. Available: [http://media.gm.com/content/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2011/Jul/0719\\_onstar.html](http://media.gm.com/content/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2011/Jul/0719_onstar.html)
- [18] J. Bergmann, C. Glomb, J. Götz, J. Heuer, R. Kuntschke, and M. Winter, "Scalability of smart grid protocols: Protocols and their simulative evaluation for massively distributed DERs," in First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, pp. 131-136.
- [19] J. Zhou , R. Q. Hu and Y. Qian "Scalable distributed communication architectures to support advanced metering infrastructure in smart grid", IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 9, pp.1632 -1642 2012
- [20] M. Arenas-Martinez, S. Herrero-Lopez, A. Sanchez, J. Williams, P. Roth, P. Hofmann, A. Zeier and A. &ldquo,A Comparative Study of Data Storage and Processing Architectures for the Smart Grid,&rdquo, Proc. IEEE First Int'l Conf. Smart Grid Comm., pp. 285-290, 2010.
- [21] <http://tools.ietf.org/html/draft-iwao-roll-dadr-00>
- [22] T. Iwao, K. Yamada, M. Yura, Y. Nakaya, A. Cardenas, S. Lee, R. Masuoka, Dynamic data forwarding in wireless mesh networks, in: First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, pp. 385–390.
- [23] S. Dawson-Haggerty, A. Tavakoli, D. Culler, Hydro: A hybrid routing protocol for low-power and lossy networks, in: First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010, pp. 268–273.
- [24] <http://www.ieee802.org/15/pub/TG4g.html>
- [25] B. Lichtensteiger et al, "RF Mesh Systems for Smart Metering: System Architecture and Performance," IEEE SmartGridComm 2010.
- [26] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks Specific

Requirements Part 15.4:Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)," IEEE Std 802.15.4-2003, pp. 0\_1-670, 2003.

**[27] N. Saputro, K. Akkaya, and S. Uludag, "A survey of routing protocols for smart grid communications," Computer Networks, vol. in press, 2012. (ppr)**

[28] M. Bahr, Proposed routing for IEEE 802.11s WLAN mesh networks, in Proc of ACM International Conference, The 2nd annual international workshop on Wireless internet, 2006.

[29] D. Wang et al., "RPL Based Routing for Advanced Metering Infrastructure in Smart Grid," 2010 IEEE Int'l. Conf. Commun. Wksps. (ICC), May 2010, pp. 1–6.

**[30] V. Skendzic, A. Guzma, Enhancing power system automation through the use of real-time ethernet, in: Proceedings of Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 2006. (ppr)**

[31] Md. Jahangir Toimoor, M.S. Thesis, "Study of the Scalability of Modified AODV-UU Routing Protocol for the Smart Grid Application", University of Windsor, January 2013

[32] Adithya Shreyas, "Analysis of Communication Protocols for Neighborhood Area Network for Smart Grid", The Oxford College of Engineering, 2006.

[33] <https://www.ietf.org/rfc/rfc4728.txt>