The role of communication systems in smart grids: Architectures, technical solutions and research challenges

Emilio Ancillotti, Raffaele Bruno *, Marco Conti

Italian National Research Council (CNR), Institute for Informatics and Telematics (IIT), Via G. Moruzzi 1, 56124 Pisa, Italy

1. Introduction

The term smart grid is commonly used to refer to a modernized electrical system, in which new and more sustainable models of energy production, distribution and usage will be made possible by incorporating in the power system: (a) pervasive communication and monitoring capabilities, and (b) more distributed and autonomous control and management functionalities [1,2]. As a matter of fact existing electric grids are a large-scale, unidirectional and centralized systems in which the electricity is delivered from remote power plants through a tree-based distribution system to local customers with pre-established load profiles [3]. However, a number of technological innovations, as well as environmental and economical concerns, have emerged in the last decade that have made traditional electric power systems outdated and not well suited to meet the reliability, efficiency and sustainability requirements posed by those changes [4].

Although there might be different views on what will be the definitive model of a smart grid, the following key capabilities are widely recognized as essential for the successful implementation of smart grids [5]:

- To enable the massive deployment and efficient use of distributed energy resources, including renewable energy sources and energy storage systems;
- To enhance the efficiency, resilience and sustainability of an electric grid by incorporating real-time distributed intelligence enabling automated protection, optimization and control functions;
- To allow the interaction of consumers with energy management systems to enable demand-response and load shaping functionalities;
- To enable real-time, scalable situational awareness of grid status and operations through the deployment of advanced metering and monitoring systems;
- To support the electrification of transportation systems by facilitating the deployment of plug-in electric vehicles and their use as mobile energy resources.

From a practical point of view the above vision requires the pervasive deployment of "intelligent" devices [6] (e.g., sensors, actuators, smart appliances, smart meters, embedded computers, etc.) that are capable of collecting real-time and fine-grained information about electricity usage patterns, as well as about the status of distributed energy resources and other components of the electric grid. This huge amount of heterogeneous information collected by the metering and monitoring infrastructures that will be incorporated in a smart grid must be shared in a reliable and secure...
manner to a multitude of distributed energy management systems. These systems are responsible for analyzing the received data, predicting and detecting possible issues (e.g., failures, energy shortages, disturbances), and making decisions to control and optimize the operations of the power system. Note that most of these management and control functions will be executed in response to local events but they may have an impact on the resiliency and efficiency of large portions of the electric grid.

To support information collection, distribution and analysis, as well as automated control and optimization of the power system, we argue that the smart grid communication system will rely on two major subsystems: a communication infrastructure and a middleware platform. The communication infrastructure consists of a set of communication technologies, networks and protocols that: (i) support communication connectivity amongst devices or grid sub-systems, and (ii) enable the distribution of information and commands within the power system. As better explained in the following, basic requirements for such communication infrastructure are scalability, reliability, timeliness and security. The middleware platform consists of a software layer, which is situated between the applications and the underlying communication infrastructure, providing the services needed to build efficient distributed functions and systems. Specifically, a middleware runs on the devices that are part of the smart grid communication infrastructure to support: (i) data management services (e.g., data sharing, storage, and processing), (ii) standard communication and programming interfaces for distributed applications, and (iii) computational intelligence and autonomic management capabilities. Furthermore, it is of paramount importance to ensure secure and reliable operations of the smart grid communication system to protect the entire smart grid. However, security solutions can not be confined to a single component of the smart grid communication system but security is a cross-layer issue because it is equally important to: (i) secure devices, information, and services, (ii) preserve data integrity, confidentiality and authenticity, and (iii) ensure very high availability of electricity provision. Then, the purpose of this survey is to provide a general reference architecture of the smart grid communication system and its major components. We utilize our reference model to identify basic system requirements and key technologies, with special focus on communication technologies and protocols, data management services, autonomic control functions and security mechanisms. Furthermore, this survey provides a comprehensive and up-to-date survey of state-of-the-art solutions and security mechanisms. Furthermore, this survey provides a comprehensive and up-to-date survey of state-of-the-art solutions and security mechanisms. Finally, we also identify main open issues and future research directions.

It is important to point out that other surveys exist targeting various aspects of smart grids. There are a number of positional papers that focus on explaining what makes an electric grid a smart grid. Those papers have the purpose of setting a common background and vision about smart grids, and to specify roadmaps and guidelines for the development of smart grids [1,2,7–10]. Other surveys have investigated the communication networks for smart grids in terms of requirements, enabling technologies and possible network architectures [11–18]. In [19] the research challenges for smart grid communications are analyzed from an industrial perspective in terms of interoperability, scalability and security. There are also surveys that focus exclusively on cybersecurity issues for smart grids [20–24]; smart grid standardization [25], and other aspects of smart grids, such as future utility control centers [26] or future technologies for the transmission grids [27]. The work in [28] provides a detailed overview of routing solutions for smart grid communications. The survey in [29] focuses on three major systems of smart grids, namely the smart infrastructure system, the smart management system, and the smart protection system. According to the view in [29] the smart infrastructure system is responsible for maintaining communication connectivity among systems, devices, and applications, which is similar to the role of the communication infrastructure described in this survey. In general, some of the cited surveys can be regarded as complementary to our work. However, our survey is distinct from those papers in the sense that it adopts a data-centric perspective and it tries to explain how communication networks will allow smart grid applications to collect, share and use information data in a timely, reliable and secure manner.

The rest of this paper, is organized as follows. In Section 2 we first outline key drivers for smart grids and we provide an outlook on the transition from existing power systems to future smart grids. We also describe the characteristics of the most innovative services and applications that smart grids can enable in Section 3. In Section 4 we introduce a conceptual framework of the main components of a smart grid communication system by following a bottom-up approach. Specifically, we will start by outlining the most popular communication technologies for smart grids. Then, we continue with describing in details the various proposals available in literature to implement communication infrastructures (Section 5), middleware platforms (Section 6) and and security mechanisms (Section 7) for smart grids, along with the most important open issues. Finally, in Section 8 we conclude our survey by summarizing lessons learned. In addition, refer to Table 1 for the abbreviations used in this survey.

2. The evolution path towards the smart grid

In this section we overview the infrastructure that underlies existing power systems to clarify its major shortcomings and the key drivers for smart grids. Furthermore, we discuss the most important new paradigms for electricity generation, delivery and consumption that are envisioned for smart grids.

2.1. Design principles and structure of traditional electricity grids

The essential purpose of an electric grid is to deliver electricity to customers, which are the termination points of the power distribution system. In the early days of electricity distribution, electric grids were isolated systems in which electric power was produced by small generators using direct current (DC). However, DC-based electricity could only be transmitted over short distances due to

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI</td>
<td>Advanced metering infrastructure</td>
</tr>
<tr>
<td>AMR</td>
<td>Automatic meter reading</td>
</tr>
<tr>
<td>BAN</td>
<td>Body area network</td>
</tr>
<tr>
<td>DER</td>
<td>Distribute Energy Resources</td>
</tr>
<tr>
<td>DG</td>
<td>Distributed generation</td>
</tr>
<tr>
<td>DR</td>
<td>Demand response</td>
</tr>
<tr>
<td>FAN</td>
<td>Field area networks</td>
</tr>
<tr>
<td>EMS</td>
<td>Energy management system</td>
</tr>
<tr>
<td>EV</td>
<td>Electric vehicle</td>
</tr>
<tr>
<td>HAN</td>
<td>Home area network</td>
</tr>
<tr>
<td>HMI</td>
<td>Human machine interface</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent electronic device</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-peer</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable logic controller/ Power line communication</td>
</tr>
<tr>
<td>PMU</td>
<td>Phasor measurement unit</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote telemetry unit</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory control and data acquisition</td>
</tr>
<tr>
<td>SDO</td>
<td>Standards developing organization</td>
</tr>
<tr>
<td>SMG</td>
<td>Smart micro-grid</td>
</tr>
<tr>
<td>V2G</td>
<td>Vehicle-to-grid</td>
</tr>
<tr>
<td>VPP</td>
<td>Virtual power plant</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide area network</td>
</tr>
<tr>
<td>WASA</td>
<td>Wide-area situational awareness</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless local area network</td>
</tr>
</tbody>
</table>
power line losses. With the advent of alternating current (AC) at the end of the 19th century it was possible to distribute electricity over long distances using high voltages more efficiently than with DC. Then, rapid industrialization, urbanization and economic development required the deployment of large-scale infrastructures for electricity delivery, which were operated through national monopolies. The structure of those national electric grids has remained (almost) unchanged till nowadays, and it consists of three main components: (1) generation, (2) transmission and (3) distribution [2].

In a traditional power grid, the generation sub-system relies on a small number of large power plants using conventional (coal, oil, natural gas, and nuclear) resources to produce electricity. Then, high-voltage transmission lines, which form the transmission network, are used to transfer electricity across long distances from power plants to electric substations. A substation includes transformers to change voltage levels from high transmission voltages to lower distribution voltages. Furthermore, substations perform several other important functions, such as grid protection and power control. Substations, medium- and low-voltage power lines, and electric meters form the distribution network. It is important to point out that a power system must be engineered such that electricity production always matches electricity demands. This implies that any change in power demands should be accommodated through an equal change in power supply. To deal with unexpected peak demands special power generators are deployed in existing power grids, which have very short start-up delays. Note that battery technologies are still expensive and inefficient, thus energy storage systems cannot be employed on a large scale to mitigate the impact of sudden load changes and fluctuations. Even if electric utilities keep generation capacity in reserves that can be accessed quickly, electricity imbalances are still possible for a number of reasons, and existing power systems may suffer from grid instabilities and power outages. Furthermore, as power grids are complex highly interconnected systems, a failure at one location can easily trigger a cascade effect that could result into regional blackouts, such as in the case of the Northeast US and Canada blackouts of 1965 and 2003 [30].

To improve the reliability of electricity provision and to support distribution automation, in the 1960s electric utilities started integrating Supervisory Control And Data Acquisition (SCADA) systems in their grid infrastructures. SCADA is not a specific technology but generally refers to computer-based centralized systems implementing control applications for industrial processes. As shown in Fig. 1, a SCADA system usually consists of the following components:

- Remote telemetry units (RTUs): microprocessor-controlled devices responsible for: (i) interacting with sensors, (ii) converting sensor readings to standard data formats, and (iii) delivering sensed data to monitoring stations;
- Programmable logic controller (PLCs): minicomputers that are used as field devices for process control and machine automation (e.g., to open or close circuit breakers at substations);
- A supervisory computer-based system that is composed of several remote units and a master station, and it is used to collect the data from RTUs, perform data analysis and send commands to PLCs;
- Databases for storing historical data, measuring trends and deriving forecasts;
- Human–Machine Interfaces (HMI) to present a simplified representation of the system and its status to a human operator, who can make supervisory decisions;
- A communication infrastructure connecting the supervisory system to the other SCADA components.

Early SCADA systems were installed in substations and transmission networks, and they were using dedicated point-to-point communication links (e.g. telephone lines or optical fibers) to connect the remote stations with the utility control center. Most vendors of SCADA products had developed simple proprietary communication protocols to connect the master stations with RTUs and PLCs [31]. However, as SCADA solutions were widely deployed by electrical utilities to control and protect the power grid, some of those protocols, such as Modbus [32], emerged as standard de facto recognized by all major SCADA vendors, while power engineering standardization bodies started to release public standard protocols, such as IEC 61850 [33]. Furthermore, the SCADA centralized architecture has also evolved over time, allowing more distributed processing and control, and the interconnection of different SCADA systems through wide-area networks [3,31]. However, as explained in following sections, SCADA systems do not appear suitable for implementing the fully decentralized and autonomous control functions demanded by future smart-grid applications.

2.2. Key challenges for existing electric grids

From the beginning of 1990s we are witnessing a rapid transformation of existing electric grids, which is driven not only by technological innovations but also by economical, regulatory and societal factors. Those changes impose new operational scenarios and technical challenges to power systems, which we outline in the following.

First of all, the soaring demand for new power supplies, and the increasing public awareness of the need of more sustainable sources of energy, are promoting the use of renewable energy resources (e.g., wind and solar technologies) for power generation [34]. According to various reports [35,36], half of the estimated 194 gigawatts (GW) of new electric capacity added globally during 2010 was derived by renewable resources. Although most of the electricity produced by renewable energy sources still comes from large-scale facilities (e.g. wind farms, solar parks, and biomass power plants), situation is rapidly changing with the proliferation of small-scale distributed generators using renewable resources. Many argue that there might be many advantages in the distributed generation (DG) model [37]. For instance, DG ensures that electricity generation is located near the place where energy is
used, reducing power losses and congestion on transmission lines [38–40]. However, as explained in Section 2.1, the existing distribution networks are not designed to handle power flowing from end users to substations, and this may negatively impact on distribution stability [41]. Most importantly, renewable energy resources are intermittent and highly variable, and the uncertainty in energy supply can cause reliability problems or power quality degradations (e.g., undesired voltage fluctuations) [42,43]. This necessarily requires more sophisticated coordination and control techniques than those supported in current electric grids [44]. Recently, utility companies have started introducing automated meter reading (AMR) systems in their distribution networks to remotely collect data from the meters (e.g., consumption records, alarms) at customers’ premises [45,46]. However, AMR systems are typically designed using simple one-way communication infrastructures that do not allow pervasive control of an electric grid [15].

Another factor that is contributing to the uptake of DG technologies is the deregulation of energy markets [47]. More specifically, power systems are no longer national monopolies, but there are independent power producers selling electricity to utility companies, and independent operators maintaining and controlling regional transmission and distribution networks. Then, electricity prices are determined in an electronic auction market according to demand and supply principles [48]. At least two types of electricity markets exist, which are regulated by different rules: (i) the wholesale electricity market for trading large amounts of energy between generators, system operators and retailers, and (ii) the retail electricity market, in which electricity retailers sell energy to end users [49]. Following the dynamics of those markets, energy costs fluctuate, and prices raise as demands increase. The first consequence of this competitive market structure is that current power systems have increasingly “meshed” topologies, emerging from the interconnection of several smaller grids. Furthermore, energy trading across regional power grids is causing uncertainties in energy delivery that current electric grids are not well suited to handle. Finally, in liberalized market environments, small electricity consumers can exploit DG technologies to become potential producers. However, this requires improved system flexibility to preserve the reliability and stability of the power system [42].

The desire of reducing the environmental impact of our lifestyle is also fostering the market penetration of electric vehicles (EVs). However, the mass adoption of EVs is not without challenges for electric grids [7,50]. On the one hand, EVs represent new mobile loads for the power system, which can significantly alter typical patterns of energy usage in households, while causing a dramatic soaring of electricity demands. For instance, the simultaneous charging of several EVs located in the same area can easily determine unexpected peak loads and rapid fluctuations of power demands in different parts of the electric grid [51]. Therefore, new management capabilities are needed to regulate the recharging process of EVs with the objective of flattening aggregated power demands and mitigating load imbalances in power systems [52,53].

2.3. The next-generation electric grid

As introduced in Section 1 next-generation electric grids are commonly denoted as smart grids. Although there are slightly different views about the ultimate model of a smart grid, a consensus is forming about the new technologies and paradigms that are essential for the successful deployment of a smart grid, namely: (1) advanced metering infrastructure, (2) distributed energy resources, (3) smart micro-grids, and (4) vehicle-to-grid technologies [1,2,7,9,10,54]. Fig. 2 provides a schematic view of the smart grid reference architecture used for the following discussion.

2.3.1. Advanced metering infrastructure (AMI)

As previously observed SCADA and AMR systems were the first attempts to introduce simple digital communication capabilities in power systems. However, smart grid applications will need pervasive and real-time control of each grid component and not only of smart meters and substations. For this reason, a smart grid should incorporate a pervasive and scalable two-way communication infrastructure to enable more distributed command-and-control functionalities. One of the most important components of this communication infrastructure is the advanced metering infrastructure (AMI) [55], which will be used to interconnect the smart meters (i.e., electricity meters that incorporate networking and data management functionalities) installed at end customers’ premises with other control systems and data aggregators (see Figs. 2 and 5 for illustrative examples). Then, AMI systems can contribute in several ways to the realization of the smart grid vision. First, electric utilities can use AMI as data acquisition networks to monitor: (i) power quality, (ii) how much electricity is produced/stored by DER (distributed energy resources) units, and (iii) power consumption of household appliances. This large amount of metering data can be exploited to proactively identify failure conditions and anomalies and to take appropriate countermeasures, or to implement sophisticated techniques to regulate electricity usage patterns (e.g., dynamic pricing or scheduling of residential loads). In a more general view, AMI networks can be foreseen to interconnect not only smart meters but also a variety of intelligent electronic devices (IEDs), which will be massively dispersed within smart grids. Communication architectures and technologies suitable for AMI will be analyzed in details in Section 5. It is also important to point out that AMI will allow smart grids to collect a huge volume of heterogeneous data from a large number of sources. How to efficiently aggregate, store and analyze this data is the subject of intensive research (see Section 6 for an overview on such body of work).

2.3.2. Distributed energy resources (DER)

As discussed in Section 2.2, in existing power systems it is becoming increasingly common a more distributed generation of electricity. This trend is rapidly gaining momentum as DG technologies improve, and utilities envision that a salient feature of smart grids could be the massive deployment of decentralized power storage and generation systems, also called distributed energy resources or DERs. We have already mentioned that smart grids will facilitate the integration of small-scale renewable energy sources (e.g., solar panels in residential applications), which will help to reduce demand for fossil-fuel power plants and to increase supply redundancy [34]. Distributed energy storage is widely recognized as a key enabler of smart grids for its role in complementing renewable generation by smoothing out power fluctuations [56,57]. For instance, surplus energy can be stored during conditions of low demand and supplied back during periods of heavy load. Moreover, energy storage systems generally have a quicker response than conventional power generators, and they can be used to increase system reliability [58,59]. However, how to coordinate diverse DER technologies, which have different capabilities and characteristics (e.g., energy capacity and time response functions), is not well understood yet.

2.3.3. Smart micro-grid (SMG)

As shown in Fig. 2, a smart micro-grid (or micro-grid for brevity) is a single, autonomous, self-sustainable power system formed by an interconnection of distributed energy resources, which serves various electricity customers (e.g., residential buildings, commercial buildings, etc.). DERs (e.g., solar panels) are connected to the micro-grid through AMI systems, which perform advanced monitoring and control functions for the micro-grid. AMI systems can also be used to monitor and control individual DERs, such as electric vehicles (EVs) or electric appliances. DERs can provide additional benefits, such as peak shaving, load management, and demand response.

IED is a term used to indicate microprocessor-based controllers of power system equipment that are provided with advanced monitoring and communication capabilities. IEDs are expected to replace RTUs and PLCs of SCADA systems [3].
commercial premises and small industries) located near one another [60,61]. A micro-grid should be able to either operate integrated with the utility grid or disconnected (i.e., islanded) from the distribution system. This also implies that a micro-grid should have its own management system to support the control functions needed to autonomously regulate electricity flows [62], as well as to participate into the energy market for electricity trading [63]. It is important to notice that the micro-grid concept is not totally new and there are already many practical examples of micro-grid applications, such as industrial micro-grids, which provide high-quality and reliable power to large industrial loads, or utility micro-grids, which serve loads in either densely populated urban areas or rural regions [64]. However, we can expect a proliferation of SMGs in future power systems, and in particular of customer-driven micro-grids, which will be established though contractual agreements among residential customers [57]. On the one hand, customer-driven (or community) micro-grids appear as the most suitable technology to optimize the deployment of DERs. On the other hand, micro-grids can also represent the best approach to tackle the complexity of pervasive deployment of intelligent and distributed control functions in electric grids. Indeed, each micro-grid can be seen as a smart grid at a much smaller scale. Thus, many experts believe that a smart grid can progressively emerge through the peer-to-peer interconnection of an increasing number of micro-grids [2,65,66].

2.3.4. Vehicle-to-grid (V2G)

As pointed out in Section 2.2, the increasing use of EVs pose new challenges to electric grids because electricity demands will rise significantly. Thus, a considerable body of work is concentrating on defining control strategies to distribute spatially and temporally EV charging in order to avoid peak loads and to optimally utilize grid capacity [52,67,53]. On the other hand, EVs can also offer many advantages to smart grids. Specifically, many studies have shown that during the day cars are parked most of the time, thus a large number of EVs can be assumed to be connected to a power socket at any given point in time [68]. Consequently, when EVs are plugged into the electric grid their batteries can be used as backup energy storage systems. For instance, EVs can supply back part of their stored electric power to stabilize the electricity produced by intermittent renewable energy sources. This new power-generation paradigm is generally known as vehicle-to-grid (V2G) technology [54,69]. To some extent V2G technologies can be seen as a special case of DERs with the additional complexity that power sources are mobile [9].

3. Smart grid applications

The smart grid vision entails innovative services and applications in addition to technological transformations. In the following we summarize the salient features of four major smart grid applications, which are also illustrated in Fig. 2. This is useful to identify the key requirements for smart grid communication systems.

3.1. Wide-area situational awareness (WASA)

One of the most important applications that smart grids should support is real-time wide-area situational awareness (WASA), which is defined as the ability to build a high-resolution description of the current state of the power grid over a wide area. Then, this information can be analyzed, for instance to predict the evolution of the power grid state under different operational conditions and energy control strategies [26,70–72].

Intuitively, WASA applications rely on a pervasive monitoring infrastructure to collect real-time data from widely dispersed sensors. The WASA monitoring system is expected to incorporate
diverse types of sensors, including sources of non-electrical data, such as weather information that is used to predict changes in wind and solar power generation. Specifically, synchronized measurement technologies are emerging as an essential enabler for WASA applications, especially for power control and protection [70]. The most advanced type of sensors based on this technology are the Phasor Measurement Units (PMUs), which provide synchronized, real-time and high-resolution (up to 60 samples per second) measures of voltage and frequency parameters for the transmission lines they are connected to [73]. Note that many system operators have already started deploying PMUs in their transmission networks [74,75]. It is also important to point out that WASA applications impose stringent latency requirements, and communication delays are the dominant component in the total system delays. Thus, special attention should be dedicated to the proper design of a communication infrastructure that is capable of ensuring delay guarantees.

Another key component of a WASA application is the set of tools that are used to analyze the huge amount of raw and heterogeneous data received from multiple sources that exist in the power grid. Specifically, simulation tools suitable for large-scale power systems are needed to identify trends, diagnose undesired behaviors and to detect in advance potential vulnerabilities [1]. How to combine simulation-based analysis of the power system with model-based analysis, with the objective of improving accuracy and convergence times of state estimation, is an important research topic [26]. Finally, visualization tools should be developed to present the output of data analysis in an effective and flexible manner, e.g. by combining geospatial information with electric information [76].

3.2. Energy management systems (EMS)

As observed in Section 2.1, in current electric grids, management functionalities are supported by utility control centers, which are typically implemented through distributed SCADA systems [3]. However, it is widely recognized that in smart grids it will be necessary to adopt a more decentralized control model in which multiple autonomous and independent energy management systems (EMSs) cooperate to achieve desired control objectives by exploiting the information collected by WASA applications. Furthermore, EMSs should be capable of operating on different parts of the grid and at different scales [9]. For instance, there will be home EMSs (HEMSs) to monitor and control the electricity usage in households, and building EMSs (BEMSs) coordinating multiple HEMSs to maximize the energy efficiency of entire buildings [77]. At a larger scale, there will be EMSs providing advanced management and control services for substations, micro-grids [63] or other subsystems of the power grid [44,78]. In general, several technologies beyond classical SCADA solutions can be considered to implement those EMSs, including service-oriented architectures (SOA), grid/cloud computing, multi-agent systems, etc. In particular, in Section 6.3 we will focus our attention on the large body of research work dedicated to the development of multi-agent control systems for smart grids.

3.3. Demand response (DR)

The term demand response (DR) is used to indicate a variety of mechanisms that smart grids will utilize to dynamically shape the electricity consumption of end users in response to energy supply conditions with the objective of improving the efficiency and reliability of electricity provision [49,79]. As an example, significant savings in power generation costs can be achieved by flattening out peak demands. Furthermore, approximately 20% of the total power generation capacity is deployed as backup reserve for coping with peak demands but it is in use only 5% of the time [66]. DR applications could help to obtain a more efficient utilization of the existing energy resources. The approach most commonly proposed for implementing DR applications is dynamic pricing. Basically, by adopting variable electricity tariffs the utility companies can incentivize customers to lower peak demands and smooth demand profiles by: (i) shifting some power-demanding household activities (e.g., dishwashers) to off-peak periods, (ii) temporarily changing the settings of energy-demanding appliances, such as heaters and air conditioners, or (iii) activating residential power generators to supplement the electricity provided by the distribution grid [49,80]. In the long term the expected potential benefits of DR would be to reduce overall electricity prices, and to significantly improve grid reliability and stability through a better spreading of electricity demands [79,81]. It is also useful to point out that different control approaches can be used to achieve DR objectives [77]. On the one end of the spectrum of proposed strategies there are pure customer-side techniques in which individual houses use real-time prices to make independent decisions about their energy usage profiles [82]. On the other hand of the spectrum there are utility-driven techniques, commonly known as direct load control (DLC) mechanisms, which allow electric utilities to schedule power consumption of residential appliances [83,84]. In general, the former approach requires more intelligent HEMSs, while the latter approach is easier to implement but it can suffer from scalability issues.

3.4. Virtual power plant (VPP)

It is expected that the proliferation of DG technologies in smart grids could lead to a new paradigm for power generation, called virtual power plant (VPP). More specifically, a VPP consists of a large cluster of distributed power generators co-located with each other in a single site, which are jointly managed and controlled. A VPP produces a total capacity similar to the one of a conventional power plant [85]. On the other hand, a VPP appears to the electricity markets and the grid system operators as a variable-size power plant ensuring more flexibility than conventional power plants [86–88]. For instance, a VPP is expected to be able to react to changes in customers’ load conditions much faster than traditional power plants [61]. In addition, the VPP approach could allow an easier integration of intermittent renewable resources into grid operations, because it implements the control functions needed to deal with power fluctuations. Finally, many studies argue that the VPP model provides an effective aggregation technique to control fleets of EVs as a single entity, thus facilitating the integration of V2G services into smart grids [69,89,90]. However, a VPP is also a complex system and the development of suitable energy management systems that can be used to implement the VPP model is still an open issue.

3.5. Smart grid standardization efforts

There is a general consensus that standardization is one of the key issues in the design of smart grids [25,5,91,92]. Indeed, the adoption of inter-operability standards for the overall system is a critical prerequisite for making the smart grid system a reality. However, a smart grid is a complex system that requires different layers of interoperability. For instance, standards for smart meters, smart devices, charging interfaces with electric vehicles are essential to facilitate market penetration of new smart grid products and services, as well as seamless interoperability between them. Similarly, all smart grid applications illustrated in previous sections require exchanges of information, for which interoperability standards are needed. Finally, a smart grid consists of many different domains and actors (i.e., generation, transmission, distribution,
markets, operations, service provider, and customer), and standard interfaces are needed among them.

There are many internationally recognized professional associations, e.g., Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF) or International Electrotechnical Commission (IEC), international standardization bodies, e.g., International Telecommunication Union (ITU), regional standardization organizations, e.g., National Institute for Standards and Technology (NIST), and industrial alliances, e.g., ZigBee, IPSO and HomePlug, working towards the development of standards for smart electricity systems. However, each entity typically targets a different market sector or application scenario. For example, IEEE focuses mainly on standards that cover media-related interoperability problems (i.e., message delivery over different communication technologies), while the activity of the IETF mainly covers interoperability issues related to transport and application areas. It is also evident that electrical industries can leverage many Internet-related standards to build a highly interoperable information and communication infrastructure for smart grids [91,92]. In Section 5 we will explain the details of some of the most important communication standards that can be applied to the smart grid domain, while in the following we focus on the most representative standards for smart grid applications.

Within the IEC there are many Technical Committees (TCs) that are working on standards for smart grid applications, such as TC 57, which prepares standards for equipment and systems used in the control, protection and automation of power systems, including EMS and SCADA [93], or TC 13, which prepares standards for smart metering systems, for electrical energy measurement, and customer information and payment [94]. Up to now, more than a hundred IEC standards can be identified relevant to the smart grid [95]. In these core standards, IEC/TR 62357 describes a SOA-based reference architecture for power system automation and provides a framework to illustrate the interdependencies between all the existing object models, services and protocols in TC 57 [96]. At the bottom level of this architecture there is the IEC 61850 family of standards, which specify communication networks and systems for power utility automation, with a special focus on substation automation [33]. Note that the abstract data models defined in IEC 61850 have been mapped to a number of protocols that can run over generic TCP/IP networks and/or switched Ethernet. Other series of core standards define a Common Information Model (CIM) to standardize the exchange of information between different classes of applications, such as Energy Management related applications (IEC 61970 family [97]) and electrical distribution systems (IEC 61968 family [98]). Data exchange for meter reading, tariff and load control is specifically addressed in the IEC 62056 series of standards [99]. Finally, security aspects for the TC57 series of protocols are handled in the standard IEC 62351.

IEEE is also very active in the smart grid sector and it has recently launched a new project called P2030 to establish a framework for achieving smart grid interoperability [100]. Up to now, nearly a hundred standards have been released or are under development, which cover different issues relevant to the smart grid, ranging from monitoring and control applications to communications over power lines [101]. Of particular importance is the IEEE 1815 standard, which has ratified the Distributed Network Protocol (DNP3) standard for communications in electric power systems [102]. DNPN3 plays a crucial role in modern SCADA systems, because it is primarily used for reliable and secure communications between control centers and RTUs or IEDs. In addition, interoperability standards are under development to support a transparent mapping between IEEE 1815 and IEC 61850. With regard to monitoring applications, it is also important to mention the IEEE C37 family of standards, which defines communication protocols for real-time PMU data exchange [103]. The series of standards IEEE 1547 provide guidelines criteria and requirements for interconnecting distributed energy resources to electric power systems, including standards for monitoring, information exchange and control [104]. Finally, IEEE is actively working towards standards for power line communications considering both broadband and narrowband technologies through the IEEE 1901 [105] and IEEE 1901.2 working groups, respectively.

4. Reference model of communication systems for smart grids

In the vision presented so far, and widely accepted by utility companies, regulators and academia, the smart grid architecture requires the integration of the energy infrastructure, which is responsible for electricity generation, delivery and consumption, with a communication system, which provides support for automated and distributed monitoring, management and optimization functions [5]. The communication system entails different technologies, components and services, and in this survey we analyze two of its major parts:

Communication infrastructure. The communication infrastructure (or network) is responsible for providing the connectivity service among individual electric devices or entire grid sub-systems. In the context of smart grids, the key priorities of this communication network are: (a) to ensure reliable and real-time data collection from an enormous number of widely dispersed data sources, and (b) to support the various communication services (e.g., multicast and group communications) that are needed by power control applications to distribute commands and configuration instructions in the power system. As explained in following sections, this communication infrastructure is envisioned as a collection of interconnected networks that will be structured into a hierarchy of at least three main tiers or domains: (1) local area networks for the access grid segment and the end customers, (2) field area networks for the distribution segment, and (3) wide area networks for the utility backbone. A variety of technologies, network topologies and communication protocols are considered for each of these categories [14,16].

Middleware platform. The middleware is a software layer running above the communication network, which provides communication and data management services for distributed applications, as well as standard interfaces between applications and smart grid devices. Different types of middleware solutions exist that differentiate from each other for the set of abstractions and programming interfaces they provide to applications, such as distributed objects, event notifications, distributed content management, synchronous/asynchronous communication functions, etc. [106]. Furthermore, middleware is increasingly used to create peer-to-peer (P2P) overlays, i.e., distributed systems in which devices (peers) self-organize into a network and cooperate with each other by contributing part of their (storage, computing, bandwidth) resources to offer useful services, such as data search, distributed storage, or computational intelligence [107,108]. Given the ability of P2P technologies to scale with increasing numbers of devices and services, several studies have proposed to use P2P-based middleware technologies to deal with the complexity of managing and controlling smart grids [109].

In the remaining of this survey we take a bottom-up approach to describe the main approaches proposed in the literature to build communication and middleware solutions suitable for smart grids. Fig. 3 provides a scheme to guide the following discussion. We start in Section 5.1 from the communication infrastructure by analyzing the requirements that this component must meet in order to support smart grid applications. For the sake of clarity we categorize these requirements into two classes: (i) quantitative requirements, which define target performance metrics for data
communications, and (ii) qualitative requirements, which define the functional characteristics that this communication infrastructure should exhibit [110,14,111]. Then, we continue in Section 5.2 by overviewing the wired and wireless communication technologies that are applicable in the smart grid context, and we identify major advantages and limitations of each solution. Furthermore, the full specification of a communication architecture requires to define: (a) which are the communicating entities and how they are organized in network topologies, and (b) which are the communication protocols used to exchange messages in standardized formats and to support various communication services. Section 5.3 deals with the first topic, while Section 5.4 deals with the second one.

In the second part of this survey we concentrate on middleware platforms for smart grids. In particular, in Section 6.1 we focus on middleware techniques specifically designed for supporting data management services that are able to meet the scalability, reliability and real-time requirements of applications that must process, store and share data from a large number of heterogeneous data sources. For instance, as explained in the following sections, most applications for grid protection require that monitored data is delivered immediately and automatically to appropriate control entities. To ensure data availability and timeliness in such large-scale and heterogeneous systems it is necessary to adopt more advanced data management models than classical client–server or polling techniques. Furthermore, in Section 6.3 we also explore the key role of middleware technologies in supporting intelligent systems, and in particular multi-agent systems, which are used to provide flexible, decentralized and autonomous management functions in smart grids.

To conclude this survey in Section 7 we analyze a cross-layer issue affecting both communication infrastructures and middleware platforms, that is security and privacy. Some challenges will not be dissimilar from those of other large-scale telecommunications networks, but new vulnerabilities are due to the fact that smart grids are complex systems that integrate physical infrastructures with information and communication technologies. It is also important to point out that electricity must always be available in power systems. Thus, continuous availability must be considered the most important security objective in smart grids. On the contrary, in most telecommunications networks confidentiality and integrity are often considered more critical than availability. As described in following sections, this implies that security mechanisms for smart grids must operate in a timely manner and without interrupting the grid services.

5. Communication infrastructures for smart grids

There are several important issues in communication network design, such as:

- Which communication technologies should be used to establish links between devices?
- Which network topologies are applicable in the context of electric grid infrastructures, and how communication technologies and grid geography affect the topology of the network?
- Which networking and transport protocols are the most appropriate for meeting the requirements of smart grid communications?

There is a general agreement that it is not possible to give a unique answer to the above questions because smart grids will operate in different environments and use cases. In the rest of this section we focus on discussing the main advantages and disadvantages of the different options that have been proposed in the literature, along with open issues and future research directions.

5.1. System requirements

To identify which communication technologies are suitable for smart grids first of all it is necessary to specify the basic requirements that smart grid communication infrastructures should satisfy. Therefore, utility companies, research organizations and governments have elaborated several reports on the communication needs of smart grid services [110,111,14,17]. In the following we list the most important requirements focusing on two categories: (i) quantitative requirements, which specify in a measurable manner the target communication performance demanded by the applications, and (ii) qualitatively requirements, which identify the capabilities that must be supported by the communication system.

5.1.1. Quantitative requirements

The key communication requirements for smart grid applications can be summarized as follows:
Latency: In general most control and protection functions in power systems have tight delay constraints and require prompt transmission of information. For instance, in the case of distribution automation the IEDs that are deployed in substations should send their measurements to data aggregators within 4 ms, while communications between data aggregators and utility control centers require a network latency ≤ 8–12 ms [112]. Other applications are less time-critical and can tolerate higher network delays (e.g., most smart meters today send their readings periodically every 15 min). It is also important to point out that network latencies depend on several factors. Therefore, communications with low and stable latencies require a communication network specifically designed to optimize delay performance [14].

Reliability: Critical functionalities in smart grid require very high levels of reliability (up to 99.9999% reliability which corresponds to a total outage period shorter than one second per year) [110], which cannot be obtained if the underlying communication infrastructure does not support very reliable communications [113]. Note that there is a number of possible causes for network failures, including link/node failures, routing inconsistencies, overloading, etc., which make necessary the use of different techniques to cope with them. However, redundancy (e.g., multiple copies of the same messages, multiple paths used for the same information flow, multiple servers to execute a task, etc.) will be of paramount importance to ensure reliability in large-scale networks. In addition, data may have different levels of criticality, and there are messages that can occasionally tolerate losses [114]. Thus, the communication network should provide applications with the ability to select between different priority levels for data transmissions.

Data rate: The bandwidth requirements of smart meters and other sensors that are used in electric grids are typically modest (each meter reading requires about 300 kbps). However, bandwidth demands are growing and the bandwidth used by smart meters, PMUs and other IEDs will probably be in the range between 10kbps and 100kbps [110]. Then, the data rate of the communication channel can become a serious concern, especially in the utility core backbone, due to the high number of IEDs that are expected to be connected to smart grids. It is also interesting to note that many studies argue that it will be necessary to over-provision the communication infrastructure in terms of channel bandwidth to ensure low transmission delays and reduce packet losses on transmission buffers [16].

5.1.2. Qualitative requirements

The key capabilities for smart grid communications can be summarized as follows:

- Scalability: A smart grid can involve millions of users and even more devices. Thus, scalability is probably one of the most intuitive requirements for the smart grid communication system. However, there are different types of scalability, like load scalability (i.e., the ability of the communication system to easily handle an increasing amount of data traffic or service requests) or geographic scalability (i.e., a network that is deployable in a wide range of sizes and configurations). Similarly, different measurements of scalability can be considered, such as the size of routing tables as the number of nodes increases, or the amount of communication resources used by each node [115,16]. Distributed communication architectures have emerged in the past to support Internet services in a scalable manner, such as peer-to-peer networks (P2P) [107], which could also be applied in the smart grid context. However, the scalability issue in smart grids is further exacerbated by the fact that most of the grid devices will be limited in terms of storage, computing and communication capabilities.

- Interoperability: As pointed out above, and better described in the following sections, many different devices, communication technologies and networking protocols will be used in smart grids. Therefore, it is essential to ensure the interoperability between those different communication networks. Standards and open network architectures (i.e., using non proprietary protocols like IP-based networks) will play a key role for interoperability at all the layers of the network architecture [5]. On the other hand, networking elements could be introduced to provide translation services between different standards (e.g., network gateways that route packets between different networks that use separate protocols). It is important to note that network interoperability is one face of the interoperability problem, but application interoperability is also essential. For instance, application interoperability requires standards to ensure that applications assign the same meaning to exchanged messages.

- Flexibility: Flexibility of the smart grid communication system is a multi-faceted concept. On the one hand, flexibility entails the ability to support heterogeneous smart grid services, which have different reliability and timeliness requirements. On the other hand, flexibility also implies the ability to provide different communication models. For instance, multipoint-to-point (MP2P) communications are important in monitoring applications, which require to periodically and simultaneously collect status information from a large number of sensors. Point-to-multipoint (P2MP) communications, or more in general group-based communications, are equally important because are used to distribute commands and configuration instructions to electric devices [116,14]. In summary, there is a need for networking technologies and protocols with a high degree of flexibility and (self-) adaptability because the same communication infrastructure must satisfy the requirements of different applications running on top of it.

- Security: A smart grid is a critical infrastructure that needs to be robust against failures and attacks. Thus, stringent security requirements are imposed on its communication infrastructure in terms of resilience to cyber attacks and protection of customers’ privacy [117]. For instance, the communication system must ensure that devices are well protected by physical attacks, unauthorized entities cannot have access to the metering information, or that sensitive data cannot be modified while in transit in the network. Similarly, the communication system must be robust against network attacks that aim at disrupting the communication services to damage electricity provision. Authentication, encryption, trust management, and intrusion detection are examples of important security mechanisms that must be supported in smart grids to prevent, detect and mitigate such network attacks [20].

5.2. Communication technologies and standards

Communication technologies can be classified into two broad categories: wired technologies and wireless technologies. Generally speaking wired technologies are considered superior to wireless technologies in terms of reliability, security and bandwidth because cables are easier to protect from interference and eavesdroppers. Furthermore, the equipment is generally cheaper
compared to wireless solutions, as well as the cost of maintenance. On the other hand, wireless networks ensures low installation costs and flexible deployments with minimal cabling, which are essential characteristics to rapidly provide network connectivity over wide areas or in areas where there is not a pre-existing communication infrastructure. Moreover, new approaches have been proposed to improve the energy efficiency of mobile-connected devices [118]. In addition, recent advances in broadband wireless technologies are providing data rates and network capacities comparable to those of popular wired networks. For these reasons, electric utilities are increasingly relying on wireless technologies to build their communication infrastructures [12].

The rest of this section is dedicated to analyze the most important wired and wireless technologies and standards that can be utilized in a smart grid. Furthermore, a summary of the main features of wired and wireless communication technologies are reported in Table 2 and Table 3, which compare those two classes of communication technologies in terms of: standardization activities, maximum data rates, transmission ranges, frequency bands, and applicability scope in the smart grid communication system. The tables also summarize the advantages and disadvantages of each technology.

5.2.1. Wired technologies

Traditionally, wired communication technologies were preferred by utility operators because were considered the most reliable option for a communication network. The most important wired technologies that are used in smart grids are:

- **Power line communications (PLC).** PLC technologies utilize existing power cables for information exchange [55]. This allows utility companies to use a single infrastructure for both power and data transmission. For this reason, PLC systems have been proposed as a cost-effective and straightforward solution to grid communication needs. As an example, the majority of AMR deployments around the world are using PLC technologies for transmitting metering data [46]. However, the use of power lines to provide reliable data transmissions has to face a number of technical challenges due to the signal propagation characteristics of typical power cables, such as high signal attenuation, disruptive interference from other power signals, including nearby electric appliances, or external electromagnetic sources [119,120]. It is also important to note that there are two major families of PLC technologies that operate in different bands and have different capabilities. More precisely, there are **narrowband** PLC (NB-PLC) technologies that operate in transmission frequencies of up to 500 kHz. Within this frequency range, the resulting data rates are modest, from 1 bps to ~10 Mbps up to ~500 Kbps. NB-PLC can be used on both high and low voltage lines, and trial deployments have demonstrated that it is possible to cover very large distances (150 km or more) [75]. The other category of PLC solutions includes **broadband** PLC (BB-PLC) technologies, which target significantly higher bandwidth performance than NB-PLC (up to 200 Mbps) by operating over much higher frequency bands (2–30 MHz). On the downside, the higher frequency bands that are used in BB-PLC reduce the maximum coverage and reliability of data communications. Thus, BB-PLC is mainly considered for in-home applications. Nevertheless, device manufacturers have recently announced new BB-PLC modems that can support data rates of about 10 Mbps up to distances of 8 km over transmission lines [55].

Many standards have been developed or are under specification for the PLC systems described above. The most important industrial association that provides widely-adopted technology specifications for in-home PLC systems is the HomePlug Powerline Alliance [121]. Over the past years this standardization group has released several standards, which have progressively enabled increasing channel rates, starting from 4 Mbps (HomePlug 1.0) to 85 Mbps (HomePlug Turbo), and, more recently, 200 Mbps (HomePlug AV and AV2). It is useful to note that HomePlug AV is a quite advanced technology that not only provides high-quality, multi-stream networking over power lines, but it also offers several co-existence operational modes. For instance, it is backward compatible with HomePlug 1.0, it enables inter-networking with devices using the IEEE 1901 standard (also known as Broadband over Powerline (BPL) technology) [119,105], and it is the first standard to allow hybrid home networks, combining wired and wireless devices [122]. Finally, the HomePlug Alliance has also designed the HomePlug Green PHY (GP) Specification, which is a lower data rate, lower power version of HomePlug AV, fully interoperable with HomePlug AV and IEEE 1901 products, which is expected to significantly reduce power consumptions and costs.

**Optical communications.** In the last decades optical communication technologies have been widely used by electric utilities to build the communication backbone interconnecting substations with control centers [3]. The major advantages of this communication technology are: (a) its ability to transmit data packets over distances in the order of several kilometers providing a total bandwidth of tens of Gbps (by aggregating multiple individual fibers), and (b) its robustness against electromagnetic and radio interference, making it suitable for high-voltage environments. For instance, several restoration and protection schemes have been devised for optical grids, which can overcome simple network failures by providing backup paths [123]. In addition, a special type of optical cables, called Optical Power Ground Wire (OPGW), combines the functions of grounding and optical communications, allowing long-distance transmissions at high data rates. Thus, OPGWs have been used in the construction of transmission and distribution lines [124]. It is reasonable to believe that fiber-optic communications will play a key role also in smart grids. Recent studies are also expanding the scope of optical communications by proposing the use of optical fibers to provide smart grid services directly to end customers [125,126], although the cost of fiber installation is recognized as an obstacle for the adoption of this technology. It is important to point out that the use of optical communications in access networks, also known as fiber-to-the-home (FTTH), is made possible by the advent of passive optical network (PON) technologies. Specifically, PONs do not require electrically powered switching equipment but they use only optical splitters to separate and collect optical signals as they move through the network. Furthermore, PONs enable a single optical fiber to serve multiple premises in a point-to-multipoint fashion, which permits to support network topologies suitable for access networks (e.g., tree-based topologies) [127]. Among the many variants of PON technologies, Ethernet PON (EPON) has been attracting much interest from grid operators because it enables the use of the standard Ethernet communication protocol over an optical network. This offers significant benefits over other PON solutions because it facilitates the interoperability with existing IP-based networks.

**Digital Subscriber Lines (DSL).** DSL generally refers to a suite of communication technologies that enable digital data transmissions over telephone lines. The main advantage of DSL technologies is that electric utilities can interconnect residential users to control centers avoiding the additional cost of deploying their own communication infrastructure. On the downside, a communication fee must be paid to the telecommunications operators maintain the network infrastructure. Note that there are a number of DSL variants, ranging from basic Asymmetric DSL (ADSL), which supports up to 8 Mbps in the downstream and up to 640 kbps in the upstream, to ADSL2+ with a maximum theoretical download and upload speed of 24 Mbps and 1 Mbps respectively. Very-high-bit-rate DSL (VDSL or VHDSL) provides faster data transmission over copper wires (up to 52 Mbps downstream and 16 Mbps/s
<table>
<thead>
<tr>
<th>Family</th>
<th>Standards</th>
<th>Data rate</th>
<th>Coverage</th>
<th>Scope</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| **PLC** | • NB-PLC: ISO/IEC 14908-3 (Lon-Works), ISO/IEC 14543-3-5 (KNX), CEA-600.31 (CEBus), IEC 61334-3-1, IEC 61334-5 (FSK and Spread-FSK)  
• BB-PLC: TIA-1113 (HomePlug 1.0), IEEE 1901, ITU-T G.hn (G.9960/G.9961)  
• non-SDO NB-PLC: Insteon, X10, G3-PLC, PRIME  
• non-SDO BB-PLC: HomePlug AV/Extended, HomePlug Green PHY, HD-PLC | • NB-PLC: 1–10 Kbps for low data-rate PHYs, 10–500 Kbps for high data-rate PHYs  
• BB-PLC: 1–10 Mbps (up to 200 Mbps on very short distance) | • NB-PLC: 150 km or more  
• BB-PLC: ~1.5 km | • NB-PLC: large-scale AMI, FAN, WAN  
• BB-PLC: HAN/small-scale AMI | • Large-scale communication infrastructure is already established  
• Physical separation from other telecommunications networks  
• Low operational costs | • Multiple non-interoperable technologies  
• High signal attenuation and channel distortion  
• Disruptive interference from electric appliances and other electromagnetic sources  
• Difficult to support high bit rates  
• Routing is complex  
• Standards evolve relatively slowly |
| **Optical Fibers** | • AON: IEEE 802.3ah  
• PON: ITU-T G.983 (BPON), ITU-T G.984 (GPON), IEEE 1901, IEEE 802.3ah (EPON) | • IEEE 802.3ah (AON): 100 Mbps up/down  
• BPON: 155–622 Mbps up/down  
• GPON: 155–2448 Mbps up, 1.244–2.448 Gbps down  
• EPON: 1 Gbps up/down | • IEEE 802.3ah (AON): up to 10 Km  
• BPON, GPON: up to 20–60 Km  
• EPON: up to 10–20 Km | • WAN  
• AMI (with FTTH systems) | • Long-distance communications (much longer than DSL)  
• Ultra-high bandwidth (suitable for supporting multimedia services to residential customers)  
• Robustness against electromagnetic and radio interference  
• Large-scale communication infrastructure is already established  
• Most commonly deployed broadband technology for residential customers | • High network deployment costs (lower with PONs than AONs)  
• High cost of terminal equipment  
• Difficult to upgrade  
• Not suitable for metering applications  
• Telco operators can charge utilities high prices to use their networks  
• Not suitable for network backhaul (long distances result into data rate degradation) |
| **DSL** | • ITU G.991.1 (HDSL)  
• ITU G.992.1 (ADSL), ITU G.992.3 (ADSL2), ITU G.992.5 (ADSL2+)  
• ITU G.993.1 (VDSL), ITU G.993.1 (VDSL2) | • ADSL: 8 Mbps down and 1.3 Mbps up  
• ADSL2: 12 Mbps down and up to 3.5 Mbps up  
• ADSL2+: 24 Mbps down and up to 3.3 Mbps up  
• VDSL: 52–85 Mbps down and 16–85 Mbps up  
• VDSL2: up to 200 Mbps down/up | • ADSL: up to 4 km  
• ADSL2: up to 7 km  
• ADSL2+: up to 7 km  
• VDSL: up to 1.2 km  
• VDSL2: 300 m (maximum rate) – 1 Km (50 Mbps) | • AMI  
• FAN | • Telco operators can charge utilities high prices to use their networks  
• Not suitable for network backhaul (long distances result into data rate degradation) |
<table>
<thead>
<tr>
<th>Family</th>
<th>Standards</th>
<th>Data rate</th>
<th>Coverage</th>
<th>Scope</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPAN</td>
<td>IEEE 802.15.4</td>
<td>IEEE 802.15.4: 256 Kbps</td>
<td>IEEE 802.15.4: Between 10 and 75 m</td>
<td>V2G</td>
<td>Very low power consumption</td>
<td>Low bandwidth</td>
</tr>
<tr>
<td></td>
<td>Non-SDO: ZigBee, WirelessHART, ISA 100.11a (all based on IEEE 802.15.4)</td>
<td></td>
<td></td>
<td>HAN</td>
<td>Cheap equipment</td>
<td>Do not scale to large networks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AMI</td>
<td>Suitable for devices with low memory and computing power</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>New standards provide full interoperability with IPv6-based networks</td>
<td></td>
</tr>
<tr>
<td>WiFi</td>
<td>IEEE 802.11e (QoS enhancements)</td>
<td>IEEE 802.11e/s: up to 54 Mbps</td>
<td>IEEE 802.11e/s/n: up to 300 m (outdoors)</td>
<td>V2G</td>
<td>Low-cost network deployments (unlicensed spectrum)</td>
<td>High interference since it operates in a very crowded unlicensed spectrum</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.11n (ultra-high network throughput)</td>
<td>IEEE 802.11n: up to 600 Mbps</td>
<td>IEEE 802.11n: up to 300 m</td>
<td>HAN</td>
<td>Cheap equipment</td>
<td>power consumption might be too high for many smart grid devices</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.11s (mesh networking)</td>
<td></td>
<td></td>
<td>AMI</td>
<td>High flexibility, suitable for different use cases</td>
<td>Simple QoS support (basically traffic prioritization)</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.11p (WAVE - wireless access in vehicular environments)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WiMAX</td>
<td>IEEE 802.16 (fixed and mobile broadband wireless access)</td>
<td>802.16: 128 Mbps down and 28 Mbps up</td>
<td>IEEE 802.16: 0–10 km</td>
<td>AMI</td>
<td>Suitable for thousands of simultaneous users</td>
<td>Network management is complex</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.16 (multihop relay)</td>
<td>802.16: m: 100 Mbps for mobile users, 1 Gbps for fixed users</td>
<td>IEEE 802.16 m: 0–5 (optimum), 5–30 (acceptable), 30–100 (reduced performance) km</td>
<td>FAN</td>
<td>Longer distances that WiFi</td>
<td>High cost of terminal equipment</td>
</tr>
<tr>
<td></td>
<td>IEEE 802.16 m (advanced air interface)</td>
<td></td>
<td></td>
<td>WAN</td>
<td>A connection-oriented control of the channel bandwidth</td>
<td>Use of licensed spectrum</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>More sophisticated QoS mechanisms than 802.11e.</td>
<td></td>
</tr>
<tr>
<td>3G/4G</td>
<td>3G: UMTS (HSPA, HSPA+)</td>
<td>HSPA: 14.4 Mbps down and 5.75 Mbps up</td>
<td>HSPA+: 0–5 km</td>
<td>V2G</td>
<td>Able to support tens of millions of devices</td>
<td>Cellular operators can charge utilities high prices to use their networks</td>
</tr>
<tr>
<td></td>
<td>4G: LTE, LTE-Advanced</td>
<td>HSPA+: 84 Mbps down and 22 Mbps up</td>
<td>LTE-Advanced: 0–5 (optimum), 5–30 (acceptable), 30–100 (reduced performance) km</td>
<td>HAN</td>
<td>Low power consumption of terminal equipment</td>
<td>Use of licensed spectrum increases cost</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LTE: 326 Mbps down and 86 Mbps up</td>
<td></td>
<td>AMI</td>
<td>Cellular operators are launching smart grid-specific service solutions</td>
<td>Difficult to ensure delay</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LTE-Advanced: 1 Gbps down and 500 Mbps up</td>
<td></td>
<td></td>
<td>High flexibility, suitable for different use cases</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>High interference reduced by QoS mechanisms</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Open industry standards</td>
<td></td>
</tr>
<tr>
<td>Satellite</td>
<td>LEO: Iridium, Globalstar,</td>
<td>Iridium: 2.4 to 28 Kbps</td>
<td>Depend on number of satellites and their beams</td>
<td>AMI</td>
<td>Long distance</td>
<td>High cost of terminal equipment</td>
</tr>
<tr>
<td></td>
<td>MEO: New ICO</td>
<td>Inmarsat-B: 9.6 up to 128 Kbps</td>
<td></td>
<td>WAN</td>
<td>Highly reliable</td>
<td>High latency</td>
</tr>
<tr>
<td></td>
<td>GEO: Inmarsat, BGAN, Swift, MPDS</td>
<td>BGAN: 384 up to 450 Kbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
upstream), and on coaxial cable (up to 85 Mbps down- and up-stream), but it can only operate over short distances (about 1.2 km). Second generation systems (VDSL2) promise to obtain data rates exceeding 100 Mbps in both upstream and downstream directions at a range of 300 m.

5.2.2. Wireless technologies

Nowadays, there are different technologies and standards for wireless communications, which can be easily classified based on their transmission ranges. In the following we overview the most important wireless technologies that are applicable to smart grids by going from the technology with the smallest coverage area to the technology with the largest one:

802.15.4-based networks. The IEEE 802.15.4 technology [128] is the reference standard that specifies the physical and MAC layers for low-rate, low-power and low-cost wireless personal area networks (LR-WPANs). Indeed, the basic IEEE 802.15.4 physical layer offers data rates of 250 Kbps over distances of about 10 m, although alternate physical layer standards have been proposed that allow higher communication throughput [129]. The supported network topologies are star (single-hop), cluster-tree, and mesh (multi-hop). In each type of topology there is a special node, called PAN coordinator, which is responsible for managing the entire network. Networks with tree or mesh topologies have also special nodes, called routers, that relay messages by establishing multi-hop connections between end devices and PAN coordinator. The standard also defines two different channel access methods that provide support for different power management mechanisms and channel sharing algorithms. Furthermore, within the 802.11 working group, a new task group, called 802.15.4 g, has been established to design PHY layer enhancements to legacy 802.15.4 suitable for smart utility networks (SUNs) [130]. However, it is also known that IEEE 802.15.4 power management mechanism can lead to very low packet delivery ratios if the MAC parameters setting is not appropriate [131]. A distributed algorithm is proposed in [132] to autonomously configure the 802.15.4 MAC layer to minimize the power consumption while meeting the reliability requirements of applications.

It is important to point out that the IEEE 802.15.4 standard is the basis for many other industrial standards for monitoring and control applications. Among these industrial efforts the most important ones are the ISA 100.11a standard [133], the WirelessHART standard [134], and the ZigBee standards [135]. More specifically, the first two standards are primarily designed for industrial automation and control systems. They both use 802.15.4-based radios but they replace the 802.15.4 MAC protocol with a collision-free TDMA-based scheme. Furthermore, they both include additional adaptation layers to support distributed command-and-control applications. Note that WirelessHART is not a completely new technology but it is a backward-compatible enhancement of the HART Communication Protocol, which is an open standard commonly used in the automation industry for the last 20 years. In addition, in 2010 WirelessHART has been approved by the International Electrotechnical Commission (IEC) as an international standard [IEC 62591 [134]]. Note that one of the main advantages of IEEE 802.15.4 over other short-range radio technologies is the very low power consumption [136]. However, ZigBee is certainly the most widely adopted technology for LR-WPANs in both industrial and commercial environments because it is considered simpler and less expensive than other solutions. Specifically, ZigBee is a specification for a suite of protocols that extend the IEEE 802.15.4 standard with additional network management capabilities, security functions and application support sublayers. One of the most important features of the ZigBee standard is the definition of application profiles that allow multiple vendors to create interoperable products. These profiles provide a description of: (a) the devices supported for a specific application, and (b) the data formats, message types and communication models to be used by those devices. Relevant to smart grid is the ZigBee Smart Energy Profile (SEP), which provides an interface for managing appliances that monitor, control, and automate the delivery and use of energy [137]. At the time of the writing two SEP versions exist, SEP 1.x and SEP 2.0. SEP 2.0 was developed in cooperation with other standardization groups, such as IPSO (IP for Smart Objects) [138] and HomePlug [121] industrial alliances. It offers new capabilities, such as control of plug-in hybrid electric vehicles and apartment buildings. In addition, it integrates some IETF standards, such as 6LoWPAN and ROLL [139], which will ensure full interoperability between ZigBee networks and IPv6-based networks (see Fig. 4). More details on those standards are reported in Section 5.4.1.

IEEE 802.11-based networks (WiFi). The family of IEEE 802.11 standards, also known as WiFi, is certainly the suite of wireless communication technologies mostly used for home and local area networking (i.e., WLANs). The main reasons of this success are: (i) WiFi operates in unlicensed 2.4 GHz and 5 GHz frequency bands, (ii) WiFi uses simple and flexible access schemes based on CSMA/CA principles, and (iii) low-cost radio interfaces exist. The original version of the IEEE 802.11 standard was released in 1999 and clarified in 1999, but since then several amendments have been approved adding new features and extended capabilities. Today the vast majority of WiFi radio interfaces are dual band and they have the capability to transmit on the 5 GHz band using 802.11a physical mode, and also in the 2.4 GHz band using 802.11b/g/n physical modes [140,141]. The highest data rates are supported by 802.11n, which integrates the OFDM-based transmission schemes used in 802.11a/g with multiple-input multiple-output (MIMO) antennas to boost the maximum data rate of 54 Mbps supported in 802.11a/g up to 150 Mbps. Given the large number of data rates that are available, several algorithms have been proposed for dynamic rate adaptation [142]. Note that the transmission ranges depend on a number of factors including transmission powers, antenna types, indoor or outdoor environments, and modulation schemes. Experimental studies indicate that reasonable outdoor ranges can be up to 300 m for 802.11n-based radio interfaces. Finally, the flexibility of 802.11 standard allow their use in various parts of the smart grid communication system, as better explained in Section 5.3. On the downside, CSMA/CA access schemes are less energy-efficient than TDMA-based schemes (e.g., 802.15.4 MAC). Thus, various techniques have been devised to minimize the energy consumption of the WLAN interface, including power saving modes, packet compression and aggregation, or duty cycling during contention periods [143].

Besides 802.11n, there are three other standards in the IEEE 802.11 family that are expected to be important for smart grid communications. The first one is the 802.11e standard [144] because it offers QoS features (e.g. traffic prioritization, scheduling and admission control) that are suitable for delay-sensitive applications. The second one is the 802.11s standard [145], which defines mechanisms to support multi-hop transmissions and to build wireless mesh networks on top of the 802.11 physical layer. Finally, the third one is the 802.11p standard [146], which defines enhancements to basic 802.11 standard to support wireless access in vehicular environments. Thus, the 802.11p standard will be one of the key enabling technologies for V2G systems.

IEEE 802.16-based networks (WiMAX). The IEEE 802.16 standard, commercialized under the name of WiMAX, was firstly released in 2001 to support long-distance (up to 7–10 km) broadband (up to 100 Mbps) wireless communications, especially in rural and suburban areas [147]. Conceptually, IEEE 802.16 is conceived as a complementary technology to IEEE 802.11 because it is designed to support: (i) thousands of simultaneous users over larger areas,
(ii) a connection-oriented control of the channel bandwidth, and (iii) more sophisticated QoS mechanisms than the traffic categories defined in 802.11e. On the downside, 802.16-based networks require a more complex network management and they operate on licensed frequency bands, which make 802.16 technology more suitable for network operators. As for 802.11, different versions of WiMAX technologies exist. The most recent version is the 2009 release [148], which includes many advanced features such as: (i) OFDMA, MIMO and various types of adaptive modulation and coding schemes, (ii) support for multicast and broadcast services, and (iii) seamless handover for nomadic users. In addition, different types of multi-hop relaying techniques are specified in the 802.16j standard [149] to enable larger coverage areas and more flexible deployments. Finally, an important evolution of the 802.16 standard family currently under development is the 802.16 m amendment [150], whose goal is to provide at least 100 Mbps data throughput at high mobility (350 km/h) and 1 Gbps at low mobility. Furthermore, 802.16 m will support handover with other radio access technologies, including 802.11 and cellular. Note that data rates and coverage ranges of 802.16 technologies make them suitable for connecting large facilities (e.g., power plants) to utility control centers, as well as to deploy AMI networks in scarcely populated areas.

3G/4G cellular networks. One of the main advantages of public cellular networks over other wireless communication technologies is the larger coverage area. For these reasons, in the past, utilities have extensively used cellular technologies, such as GSM, GPRS and EDGE, for data communications in SCADA and AMR systems [151,152,45]. A shortcoming of cellular data services is that they are relatively expensive. Furthermore, cellular networks generally provide variable throughput and latency performance, depending on the number of other users served by the same base station. On the other hand, cellular networks are witnessing a rapid evolution and new generations of cellular technologies supporting higher data rates and more sophisticated data communication services are being developed. Today, the most widely commercialized mobile cellular systems are based on the third generation (3G for short) of cellular technologies. 3G standards are developed and maintained by the 3GPP industrial organization, UMTS systems, first offered in 2001, are still the most popular 3G standards. Among the various radio interfaces used in UMTS systems, the highest speeds are provided by the Evolved High-Speed Packet Access standard (HSPA+) [15], which can support data rates up to 168 Mbps in the downlink and 22 Mbps in the uplink. The successors of 3G standards will be 4G systems, which are designed to enable mobile ultra-broadband Internet access. A candidate 4G system under development by 3GPP is the Long Term Evolution (LTE) – Advanced standard, a major enhancement of currently deployed LTE systems [153]. The main new capabilities introduced in LTE-Advanced with respect to previous 3G technologies include: (i) bandwidth and spectrum flexibility, (ii) an easier handoff between different networks, (iii) better support for heterogeneous network architectures ranging from macro-cells to femtocells, and (iv) more advanced mobile networking capabilities. Note that another candidate for 4G system is the 802.16 m technology, which was described in the previous section, although it is not targeting ubiquitous connectivity as LTE does.

Satellite. Satellite systems support communications with variable bandwidth and latency performance using satellites stationed on orbits at different altitudes, including Low Earth Orbits (LEO), Medium Earth Orbit (MEO), and Geostationary Earth Orbits (GEO) [154]. Satellite systems using high altitude orbits have the advantage of not requiring tracking antennas, which are expensive. The downside is that they are affected by higher transmission delays (up to one second if link-layer acknowledgments are used). On the other hand, LEO satellite systems are less expensive to deploy. Traditionally, electric utilities have considered satellite communications for SCADA systems and other services provided in rural or geographically remote locations, which are either beyond the coverage of terrestrial communication networks, or it is difficult (and costly) to reach with dedicated fibers. Recent advances in satellite systems, with the development of smaller and low-cost stations, can open up new opportunities for the use of satellite communications in smart grids. For instance, satellite systems can be used to provide backup communication services at critical substations or backhaul transport services for AMI networks.

5.3. Communication network architecture

In Section 4 we have anticipated that the smart grid communication infrastructure is commonly envisioned as a hierarchical network with a three-tier architecture, consisting of: (1) an access tier, (2) a distribution tier, and (3) a core tier. The purpose of this section is to further elaborate on this view and to present a detailed reference model for such communication infrastructure. This reference architecture describes the communication capabilities that should be provided to electric devices at different tiers. Furthermore, it explains how devices should be organized into network topologies. In addition, we discuss how small-scale networks could be interconnected to build a large-scale communication system providing end-to-end connectivity over a regional or national area. Finally, this reference network architecture allows us to easily map the communication technologies described in Section 5.2 onto the different components of the communication infrastructure (this mapping is also reported in Table 2 and Table 3). To guide the following discussion in Fig. 5 we illustrate our reference architectural model by giving an example of a possible smart grid communication network. This example has been obtained by considering the smart grid illustrated in Fig. 2 and substituting the energy flows with information flows.

Access tier. The communication networks deployed in the access tier of the smart grid communication infrastructure are responsible for: (i) enabling real-time information flows between end customers and energy management systems, and (ii) allowing a more active role of end customers in the electricity market and the power grid management. Therefore, home area networks (HANs) are very important for the access tier because they can provide low-cost solutions to support monitoring and control of electric devices that are deployed at customers’ premises. Both low-range wired and wireless technologies can be used to build such networks. However, WiFi is generally considered too expensive for most HAN devices and it consumes too much power, while ZigBee is the de facto standard used by many manufacturers to provide low-power wireless communication capabilities to a variety of tiny devices (e.g., sensors) [155]. Nevertheless, HAN gateways should be equipped with multiple radio interfaces to facilitate the integration of different classes of devices. It is also important to point out that similar concepts can be applied to networks with larger scales such as Building Area Networks (BANS) and Industrial Area Networks (IANs), which will be used in the access tier to monitor and control the electricity consumption in buildings and industrial facilities.

The access tier must also provide connectivity services suitable for electric vehicles, which will have the twofold roles of mobile consumers and mobile storage of electricity. In this case wireless communication technologies are the most natural choice for supporting V2G scenarios. However, different use cases can be envisaged that require different networking solutions. For instance, electric vehicles need to interact with HANs when parked at homes or offices, and WiFi-based LAN solutions appear the best option. On the other hand, electric vehicles can stay connected to the smart grid communication system when on the move by using public...
3G/4G cellular networks or a WiFi-enabled roadside communication infrastructure [156]. More generally, vertical handover techniques can be used by moving vehicles to switch from one wireless network to another while maintaining seamless connectivity. A survey of the main vertical and horizontal handover approaches in the literature can be found in [157,158].

**Distribution tier.** The communication networks deployed in the distribution tier of the smart grid communication infrastructure are responsible for: (i) enabling the state estimation and real-time control of the distribution grid, (ii) supporting the interconnection of local area networks (i.e., HANs, BANs and IANs) with the smart grid communication backbone, and (iii) providing the communication support for implementing the data management services that are needed to efficiently handle the large amount of data collected in the distribution grid. As observed in Section 2.3, AMI networks will be a key component of the distribution tier because they interconnect smart meters with data aggregators and control systems deployed in the distribution grid. It is important to point out that there is not a single communication technology that can meet the requirements of all AMI deployment scenarios, and utility companies are considering both wired and wireless communication technologies for building their AMI systems. Options include conventional PLC technologies, point-to-point communications using cellular or medium-range wireless (e.g., WiMax or WiFi) technologies; multi-hop wireless technologies, such as mesh networking solutions, which can provide a flexible and easy to deploy extension of the existing wired networks [159]. Given the heterogeneity of communication technologies, specific technologies are needed to support internetworking and to provide seamless service provisioning. The IP Multimedia Subsystem (IMS) is a promising solution to address this issue, since it offers the needed interworking environment and service flexibility for the integration of wireless access technologies [160]. The 802.21 standard is also supporting various mechanisms that can be used to enable the seamless interoperation between heterogeneous technologies [161].

In addition to AMI networks the distribution tier will include specialized networks to provide reliable communications to a large number of heterogeneous sensors and actuators that will be deployed in smart grids to monitor and control power system equipment (e.g., circuit breakers, feeders and substation transformers, DER units, etc.). These networks are commonly named Field Area Networks (FANs), or Neighborhood Area Networks (NANs) [14,16]. In some cases the communication technologies used in FANs will not be dissimilar from the ones that are considered for AMI networks. However, FANs can also be considered an evolution of existing SCADA-based networks that are used for power grid protection, and they will have more stringent real-time requirements than AMI networks. Furthermore, elements in a FAN can be physically distant from each other. Thus, 4G technologies (e.g., LTE) will have a key role in most FAN deployments, while they are less important in AMI networks [15].

**Core tier.** The core tier of the smart grid communication system consists of a Wide Area Network (WAN). Such high-capacity communication backbone is used to deliver the large amounts of data collected by the highly dispersed AMI systems and FANs to remote control centers over long distances. Various options have been considered for the deployment of a WAN meeting the requirements of smart grid communications, such as all-IP core networks or MPLS-based networks. However, the fundamental choice that electric utilities are facing is between the deployment of private WANs and the use of public data networks. Several factors are influencing the decision of grid operators and the need of high reliability, security and low latency are the most important ones, along with economical affordability. As a matter of fact, a growing number of utilities are choosing to deploy a private hybrid fiber/wireless network as the backbone for their electric grid [162].

So far we have presented a general reference model of the network topology for the smart grid communication system. To conclude this section we further elaborate on some specific areas that are worth exploring: (i) the applicability of Internet concepts and models to smart grid communications, (ii) AMI deployments,
and (iii) the applicability of multi-hop wireless technologies for smart grid communications.

5.3.1. Similarities between the Internet and the smart grid communication infrastructure

In this section we discuss the fundamental similarities that may exist between the architectural model of the Internet and the reference model of the smart grid communication network that we have described above [163,164]. To recognize those similarities is important because they motivate the adoption of Internet design principles when designing scalable, reliable and secure networking solutions for the smart grid [14,165,16]. For instance, both the Internet and the power grid have emerged from the incremental interconnection of an enormous number of (computing, sensing and electric) devices. Both the Internet and the power grid are highly heterogeneous and wide-area complex systems, which must support various degrees of autonomous control at different time scales. Finally, both the Internet and the power grid are witnessing a transition from a structure with a clear distinction between the core network and the access network (with almost all the system intelligence residing in the core) to a more federated system where the intelligence of the network (i.e., its ability to distribute, store, and modify information and energy, respectively) can be migrated to the periphery [166–168]. To cope with scalability, heterogeneity and decentralization requirements, the Internet architecture has relied on the interconnection of small-scale subnetworks, which were then organized into a hierarchy of networks covering larger geographic areas. As we have described earlier, such structure is also conceived as the most suitable for smart grids in which individual electric subsystems have the responsibility of controlling separate geographical regions (e.g. micro-grids). Then, such electric subsystems can be easily mapped into separated communication subsystems interconnected with each other so as to form a hierarchy of communication networks [169]. Furthermore, the IP stack has proven its interoperability and extensibility as the basis of the global Internet over the last 30 years. Thus, Internet technologies may be seen as a promising solution for the interoperability problem in the smart grid communication infrastructure [91]. On the downside, there are well-known Internet problems (like security) that may hinder a tighter integration between the smart grid communication infrastructure and the Internet.

5.3.2. Examples of communication networks for AMI systems

The network architecture model we have outlined above provides a unified conceptual framework to support end-to-end communication services in smart grids. However, in the literature there are also several examples of specialized communication networks that have been designed for specific components of the smart grid communication infrastructure. In particular, the design of communication networks for AMI systems has attracted much research interest. A full-fledged network architecture for AMI systems is described in [170]. In that architecture the smallest communication subsystem is the HAN, which corresponds to an individual apartment. Then, a number of HANs are aggregated into a BAN, while several BANs form a NAN. Distinguishing features of this network architecture are the use of: (i) low-power wireless communication technologies in the HANs, (ii) different types of gateways to control the communications of increasingly larger areas and to facilitate the interconnections of different subsystems, and (iii) cellular (3G) technologies to enable communications between multiple BAN gateways and a NAN gateway. Note that in [170] it is also envisaged that the 3G network interconnecting the gateways is a dedicated network separated from public cellular systems to ensure improved safety and reliability.

AMI networks similar to the one proposed in [170] have been also described in [171,83,45,172]. In particular, in [171] data management services are deployed within the NAN gateways, which are called concentrators, to support aggregation and storing of the information flows coming from multiple NANs. Furthermore, a base station is deployed to serve an area containing multiple NANs, which receives the data sent by NAN concentrators over dedicated WiMAX channels, and forwards this information to the regional control center over a wired network (e.g., using the Internet core backbone). In general, the trend is to prefer licensed wireless technologies, such as WiMAX [11,83] and GSM/GPRS [45,172], for the communications in the neighborhood area networks, because grid operators can establish their own private network infrastructure, which makes easier to guarantee the required communication reliability and QoS. On the other hand, unlicensed wireless technologies, such as ZigBee [173,174,172,175,176] and WiFi [177], are the main standards that are being considered for communications within houses or buildings, although they have also been proposed as less expensive options for supporting communications in NANs [178]. As observed in Section 5.2, some of those standards have been also recently extended to provide specific support for the interoperability of devices that will be used in smart grids, such as the ZigBee SEP [179,137].

5.3.3. Multi-hop wireless networking in smart grids

In this section we discuss the potential role that the multi-hop communication paradigm can have in a smart grid. Specifically, we focus our attention on two of the most mature and consolidated examples of networking technologies using multi-hop wireless communications: wireless mesh networks and wireless sensor networks. Interested readers can find an up-to-date overview of research and development in the broader area of networks based on the multi-hop ad hoc networking paradigm in [180].

Wireless mesh networks. A wireless mesh network (WMN) is a dynamically self-organized network in which nodes automatically establish and maintain network connectivity through multi-hop wireless paths. There is a general agreement that wireless mesh networking is a key enabling technology for most next-generation wireless networks [159]. WMNs have the potential to bring many advantages also to the smart grid communication system and many studies have advocated the use of WMNs in smart grids [11,16]. For instance, a multi-hop wireless communication system inherently provides multiple redundant paths between any pair of communicating nodes. This eliminates single point of failures and mitigates the occurrence of bottleneck links, increasing the communication reliability with respect to conventional infrastructure-based wireless networks [181,182]. Furthermore, multiple paths can be used to achieve a more balanced distribution of traffic over the network [183] or to minimize the energy used by the mesh backbone to route traffic [184]. Note that the use of self-organizing networking technologies allows to provide self-healing capabilities to the communication network, which is necessary to meet the reliability requirements of smart grid communications. At the same time, wireless multi-hop communications are a low-cost solution to increase the coverage of existing wired networks and to deal with the difficulties of deploying new cables in existing facilities. Finally, as observed in Section 5.2 most popular wireless technologies, including WiFi, ZigBee and WiMAX, are now including amendments to their standards to provide support for multi-hop communications (e.g. 802.11s and 802.16j). Thus, mesh networking capabilities are expected to be supported by most commodity products. Recently, millimeter-wave links that operate in the 71–86 GHz frequency band have also been proposed as a cost-effective high-speed alternative for fixed wireless mesh networks, with data rates up to 1 Gbps [185].

Wireless sensor networks. A wireless sensor network (WSN) consists of autonomous sensor devices monitoring physical or environmental phenomena, which employ multi-hop wireless
communication technologies to cooperatively transfer their readings to a common sink or gateway. Most advanced sensors can also perform simple actions (e.g., close a circuit). In this case the term wireless sensor and actuator network (WSAN) is generally preferred to denote a wireless network that is able to perform distributed sensing and acting tasks. As observed in Section 3.1, WSNs are expected to play a key role in enabling the pervasive monitoring of electric grids. It is important to point out that WSN is not a novel concept. There are more than two decades of intensive research in this field and several surveys exist in the literature that outline existing approaches for routing and data collection in WSNs [186–188]. In particular, energy awareness is a very important design consideration for protocols and algorithms in sensor networks, and the design of a WSN should consider the amount of energy each protocol can spend to perform its tasks [189]. In addition to energy efficiency, there are many other technical challenges to address before successfully applying WSN technologies in the smart grid domain. Specifically, the harsh environmental conditions of typical power systems, such as medium-voltage substations or power control rooms, pose significant issues to the reliability and latency of wireless communications, which also impact on the design of communication protocols for WSNs. Most importantly, in many classical applications for wireless sensor networks the goal is to detect the occurrence of an event (e.g., when the ambient temperature is above a given threshold), and it is sufficient that a small subset of the sensors that have observed the same event are able to report it to the application. This characteristic enables the use of mechanisms such as duty-cycling and data fusion to reduce spatially-correlated contention between nodes in the same neighborhood, as well as to improve energy efficiency and network lifetime [190]. On the contrary, in many smart grid applications the sensed data of each individual sensor might be needed. For instance, this is the case of smart metering applications, which must collect information from each smart meter. This means that existing data collection techniques for wireless sensor networks should be modified to meet this additional constraint. Furthermore, in wireless sensor and actor networks there is a need for suitable coordination mechanisms between sensing and control functions to ensure that correct actions can be taken within the strict time constraints of most power grid processes.

We conclude this section by pointing out that most WSNs for smart grids will be deployed in conditions that can make very difficult to replace batteries. Furthermore, maintenance costs due to the replacement of a large number of batteries may be excessive. To cope with these difficulties, many studies advocate the use of energy harvesting techniques to allow sensor nodes to take power from the surrounding environment. Energy harvesting covers a wide range of different technologies. Solar energy is the most obvious power source and photovoltaic cells can be used to obtain power from it. However, this solution is not applicable indoors. In smart grid environments electromagnetic induction seems the most feasible technology, but there are other approaches that can work as well. For instance, using the difference in temperature with thermal energy harvesting can be effective in sub-stations, where there is a significant temperature gradient. For sensors deployed in buildings, vibrational energy can also be used. The downside of energy harvesting technologies is that they are still unable to provide a sustained energy supply to support continuous operation. Therefore, new power management schemes, transmission techniques, data aggregation and link scheduling algorithms, and routing protocols are needed to exploit the sporadic availability of energy [191–193].

5.4. Communication protocols

To allow communications in a distributed network formed by devices from different vendors and using heterogeneous communication technologies, it is necessary to specify a suite of protocols to: (i) associate node identities to network devices (routing addressing functions), (ii) establish network paths between nodes (routing function); (iii) define message formats and rules to exchange those messages (transport function); and (iv) support advanced networking services such as broadcast, multicast, QoS and security. A comprehensive overview of all the network protocols and services that have been proposed in the literature for smart grid communications might require a separate survey per se. Thus, we focus on three important areas that we believe still entail major research challenges: (1) routing protocols, (2) QoS support, and (3) transport protocols.

5.4.1. Routing protocols

As observed above, routing protocols are responsible for establishing communication paths among nodes in a network. As discussed in Section 5.3, in a smart grid different classes of devices, communication technologies and network topologies will be used depending on applications and use cases. This implies that multiple routing protocols should be employed to enable smart grid communications in the different networks forming the smart grid communication infrastructure. It is important to point out that in the past electric utilities preferred to avoid using routing protocols to communicate with field devices due to potential (a) real-time violations and (b) security attacks. However, as motivated in Section 5.3 electrical grids are progressively migrating towards IP-based network architectures. Therefore, it is expected that routing protocols will be increasingly more important, especially in the access tier of the smart grid communication system.

It is out of the scope of this survey to outline all the different routing protocols that have been proposed so far for the various network categories described in Section 5.3. Interested readers can find a comprehensive survey of routing protocols for HAN and NANs in [28]. On the contrary, in the following we focus our attention on routing and data forwarding schemes for networks using wireless multi-hop communications (i.e., WMNs and WSNs) because we believe this is the area in which most research challenges are yet to be addressed, especially as far as QoS support is concerned. For the sake of clarity, in Fig. 6 we provide a

---

**Fig. 6.** Classification of research trends in the area of routing for WMNs and WSNs in the smart grid context.
classification of the research trends in the area of routing for smart grids, which we have analyzed in the following.

In the literature there exists a large amount of work on routing for ad hoc networks, as testified by the considerable number of different protocols that have been proposed, and the standardization of few of them by the IETF MANET working group. Furthermore, a number of surveys can be found on this area, which provide comprehensive classifications and comparisons of existing routing approaches [187,194–196]. Relevant to this survey are the studies that are dedicated to the development of a more solid understanding on the applicability of those routing approaches in the smart grid domain, and AMI systems in particular [197,177,198]. One of the main findings of those studies is that geographic routing strategies, which use geographical coordinates of networks nodes to optimize the path selection (e.g., selecting as intermediate relay the node that is geographically the closest one to the final destination), seem the best schemes for smart grid communications because they minimize routing overheads and they work particularly well in static networks. For instance, the authors in [197] consider an exemplifying PLC network used in low- and medium-voltage distribution grids, and show how different location-based routing strategies cope with variable link qualities and node failures.

Another research area related to routing in smart grid networks include the adaptation of routing schemes designed for general-purpose WMNs to the context of smart grid communications. In [199], the reliability of the AODV routing protocol is investigated in a distribution grid topology that spans many kilometers. A new multi-path routing protocol for multi-channel WMNs, called DMMR, is proposed in [200], which tends to choose paths that do not share network nodes to reduce the probability that multiple paths are broken at the same time when a single node fails. In this way, DMMR ensures stable end-to-end connections. Other works have explored the applicability of the Hybrid Wireless Mesh Protocol, or HWMP, specified in the IEEE 802.11s standard [145], for routing in WMNs that are used for the monitoring and management of electric grids. HWMP operates directly at the link layer and it uses MAC addresses for routing instead of IP addresses. Furthermore, it is an hybrid protocol that adopts a tree-based hierarchical routing scheme for data transfers from network nodes to mesh gateways, and an AODV-like routing scheme for data transfers between network nodes. A known issue of HWMP is route instability in case of link failures and the work in [201] proposes new routing metrics to reduce route fluctuations. A multi-path extension to the tree-based routing strategy used in HWMP is also described in [202]. Alternative tree-based routing schemes are proposed in [203,204] by employing data forwarding mechanisms inspired by distributed depth-first search algorithms. Furthermore, to reduce network control overheads those schemes use data packets to detect loops and to propagate the information on failed links. In this way, routing tables can be updated quickly and with little overhead.

Another considerable amount of work has been conducted on the design of routing protocols for WSNs that are able to cope with the limitation of computing power and memory size of embedded devices. Indeed, many of the devices installed in the last mile of an AMI network, such as home appliances, IEDs, and smart meters will be based on tiny micro controllers. Most of the above-described routing protocols for WSNs are not applicable to those devices because they perform complex computations and store a large amount of routing information. For these reasons, popular wireless standards for sensor and control systems, such as ZigBee and WirelessHART, have implemented much simpler routing schemes. Specifically, ZigBee specification include three routing protocols: (1) a tree-based routing scheme for data collection at the network sink, (2) a variant of the AODV algorithm that is used to establish on-demand multi-hop network paths, and (3) a source routing for communications between the sink node and the end devices. It is also important to point out that in the last few years there has been a growing interest from the research community in designing optimized networking protocols for WSNs, which could potentially match the requirements of the smart grid (interested readers are referred to [186,187,205] for detailed surveys). IETF had recently released a new standard specifying an IPv6-based routing protocol, called Routing Protocol for Low Power and Lossy Networks (RPL) [139], which is rapidly emerging as the most mature and commercially viable routing solution for large-scale AMI systems [206]. Specifically, RPL organizes the network topology into a tree-based structure (called Directed Acyclic Graph, DAG) and it adopts a gradient-based data forwarding scheme to minimize memory usage and protocol complexity. Given the importance of RPL applications, a few papers have addressed the performance evaluation of RPL in different use cases [207–210]. In particular, results shown in [209] for a medium-scale outdoor network deployment indicate that RPL ensures smaller routing tables and lower control overheads than conventional shortest-path routing algorithms. On the other hand, the study in [210] points out that RPL nodes may suffer from severe unreliability problems, mainly because RPL often selects sub-optimal paths with low quality links. Other studies have focused on proposing enhancements to the basic RPL standard. The work in [211] proposes to construct the DAG assigning to each link in the network a cost depending on the ETX metric, a popular routing metric initially proposed for wireless multi-hop routing protocols [212]. In [178] extensions to RPL are proposed to enable smart meters to automatically discover connectivity and recover from loss of connectivity. The effectiveness of the local repair mechanisms used in RPL is also investigated in [213]. However, RPL applicability in large-scale (thousands of nodes) networks with stringent reliability requirements is still an open issue. In addition, the stability of DAG structure with accurate PLC channel models and real-world traffic patterns needs to be examined.

5.4.2. QoS support

In Section 5.1 we have observed that reliability and timeliness are key requirements for smart grid communications. However, different smart grid applications may have different constraints for latencies and communication reliability. For instance, in basic metering applications a delay of few seconds when collecting metered data is tolerable, while applications monitoring transmission lines should operate on a time scale of few milliseconds. Similarly, most grid protection applications, which involve the remote control of critical grid components such as breakers and switches, require very high levels of communication reliability to avoid power grid instability. Consequently, the smart grid communication infrastructure should adopt suitable mechanisms to enforce different QoS guarantees to network flows depending on the application constraints. In telecommunications networks QoS differentiation is typically achieved through resource reservation and traffic prioritization. Specifically, various approaches can be employed to prioritize important and time-critical network flows over less critical data traffic. For instance, many MAC layers (e.g., 802.11e and 802.16) support the specification of different traffic categories and they use scheduling algorithms to provide bandwidth differentiation [214,215]. However, MAC-based solutions are generally limited to provide QoS guarantees on single communication links. For this reason, there is an increasing awareness that a full-fledged QoS-based architecture is needed to satisfy the different requirements of smart grid applications. Several QoS-based frameworks have been proposed for the Internet, such as Integrated Services (IntServ) [216], Differentiated Services (DiffServ) [217], and Multi-Protocol Label Switching (MPLS) [218], which could be applied
also in smart grid communication networks. It is out of the scope of this work to present a description of those solutions. However, we want to remark that it is still an open issue to decide which of those QoS-based architectures is the most appropriate for the smart grid domain. The study in [219] proposes to use MPLS technologies to handle fine-grained bandwidth management in smart grids communication systems, while the study in [220] discusses how to integrate MPLS with DiffServ. A multi-service routing architecture is described in [221], which uses the DiffServ model in the data plane, the RTCP protocol for performance monitoring and multi-service path calculation in the control plane [221]. A detailed and fair comparison of different QoS approaches, and their testing in real-world deployment are still missing. Note that recently most of the research efforts in this area have been focused on the development of optimization frameworks to compute network paths that satisfy multiple QoS constraints simultaneously (also known as constrained-based routing or QoS routing), because this is an essential feature for any communication infrastructure that aims at guaranteeing QoS. A comprehensive survey of existing algorithms for constrained-based routing can be found in [222]. Given the heterogeneity of the smart grid, traditional methodologies cannot be directly applied due to the requirements of high computing and storage capabilities. Thus, new schemes are needed that can be implemented by both powerful and resource-limited devices. Preliminary results on QoS routing solutions specific to smart grids have been developed in [223,224]. However, it is still an open problem to understand the impact of power system dynamics on the stability of QoS routing, or how to define QoS requirements in the context of smart grid.

5.4.3. Transport protocol

Transport protocols are responsible for delivering data among application processes running on separate hosts in a network [225]. Besides simple inter-process communications there are many other services that can be optionally provided by a transport protocol, such as data integrity, congestion avoidance and flow control. The simplest transport protocol in the Internet protocol suite is UDP, which is connection-less (i.e., it does not set up a dedicated end-to-end connection) and it does not provide any guarantee on packet delivery. However, UDP can be used tighter with the Real-time Transport Protocol (RTP), which provides specific mechanisms to improve the delivery of audio and video over IP networks [226]. For instance, RTP packets carry information (e.g., time stamp) that allows to implement jitter compensation at the receivers. Furthermore, RTP supports data transfer to multiple destinations through IP multicast. On the other hand, the most common alternative to UDP is the Transport Control Protocol (TCP). TCP is more sophisticated than UDP because: (i) it provides connection-oriented communications, (ii) it uses message numbering and retransmissions to recover packet losses and suppressed duplicate data, (iii) it supports reordering of out-of-order data, and (iv) it implements flow and congestion control techniques. Since the majority of smart grid applications require reliable communications, TCP seems the natural choice also for the smart grid communication system. However, TCP does not provide guarantees on network delays experienced by transmitted packets. In addition, the timeouts used to detect some packet losses can cause noticeably delay spikes. Thus, TCP cannot adequately meet the requirements of smart grid communications in terms of timely data delivery, especially for data traffic that is inherently periodic (e.g., metering readings, measurements from PMUs, etc.). Furthermore, data sources in most smart grid applications generate small-sized packets at a low rate. In this case, TCP congestion control can be ineffective and it can cause useless retransmissions of packets and throughput degradations. For these reasons, a few studies have been recently conducted to design either suitable modifications to TCP or totally new transport protocols in order to achieve lower latency while preserving reliability in data-collection applications. One example is the scalable and secure transport protocol that is proposed in [227], called SSTP, which is suitable for monitoring applications in which a large number of clients infrequently communicate with servers. More specifically, one of the main goals of SSTP is scalability, and this is achieved by assuming that the server does not continuously maintain state information for each session (i.e., sensor device) but it encrypts the session state and it transmits the encrypted information to the associated client, which temporarily stores it. Then, the client returns to the session the encrypted state with his next message. Furthermore, SSTP assumes that in-order delivery is not required as data is always time-stamped at the sender side. Finally, a SSTP client can immediately send a message without any delay unless its sending window, whose size is determined by the number of clients associated to the same server, is full. Results shown in [227] indicate that SSTP can provide much lower end-to-end delays than TCP. An alternative approach, called Split and Aggregated TCP (SA-TCP), is proposed in [228], which employs split and aggregation techniques. More specifically, in SA-TCP each client creates a TCP connection with a single intermediate node, called transport aggregator, which is deployed before a bottleneck link. Then, this node aggregates all received data and it creates another TCP connection with the final data collector. In this way, a bottleneck can be shared between many meters more fairly and the number of packet retransmissions is reduced. On the downside, TCP splitting approaches are more vulnerable to security attacks, and packets may suffer longer delays. An alternative congestion control technique is proposed in [229] by adapting the monitoring rate of smart meters to the available bandwidth. The basic idea is to formulate an optimization problem to determine which is the amount of traffic that can be reduced at different locations in the network without affecting the grid operations. It is also useful to point out that there is a large body of work focusing on reliable data collection protocols for WSNs (see [230,188] for survey papers on this area). However, those transport protocols can not be applied to smart grid monitoring applications without substantial modifications for a number of reasons: (i) in smart grid each packet conveys unique information associated to a specific meter at a given time instant, thus data aggregation techniques cannot significantly reduce the total volume of data traffic to be delivered, and (ii) redundant deployment is not a feasible solution for achieving reliability because smart meters identify specific end users.

6. Middleware platforms for smart grids

Many smart grid applications will require a precise estimation of the state of large portions of the power system in order to control and optimize the electricity delivery and usage. However, not all smart grid applications require the same sets of data, nor the same reporting frequency. For instance, off-line trend analysis does not impose tight delay constraints, while control and protection functions need real-time transmission of data (and commands). Therefore, scalable data management systems specialized for smart grids are needed to share this large amount of information, and to timely deliver relevant data to applications that really need it [231].

In Section 2.1 we have pointed out that SCADA systems already include solutions for storing and analyzing data collected from a large number of RTUs. However, those solutions rely primarily on centralized databases, which do not provide the level of scalability and flexibility needed to handle the huge increase in data storage and processing that will occur with smart grids. On the other hand, there is an increasing consensus among electric utilities that
Moreover, the publishers have the ability to inform the middle-allow subscribers to find particular status variables of interest. On the other hand, subscribers are application programs that use alarm conditions (status alerts) that require immediate attention. These variables and alerts. Then, the GridStat middleware provides sources of measurements and control settings (status variables), while the producers simply announce the availability of their data. Then, the middleware platform is responsible for delivering time-sensitive data between cooperatively controlling complex systems consisting of a large number of highly interconnected and interdependent components operating in dynamic environments. In particular, multi-agent middleware platforms are drawing much attention from researchers in the smart grid area because they appear the most suitable technology to provide self-adaptation and self-healing capabilities to smart grids [233].

In the following sections we will outline the most important middleware platforms proposed so far for smart grid control applications. Note that most middleware platforms are designed following a given model, or paradigm, which describes the approach used to manage communications and distribution of resources. Thus, to guide the following discussion in Fig. 7 we also provide a classification of the related work based on three main categories: (i) middleware services for data management; (ii) object-oriented middleware, and (iii) multi-agent systems.

6.1. Middleware services for data management

One of the earliest examples of a full-fledged middleware platform supporting data management for smart grid applications is known as GridStat [234–236]. More specifically, GridStat provides a publish/subscribe communication model in which a grid object can be either a producer or a consumer of data. The consumers can declare to the middleware system their interests in one or more types of data (e.g., a data aggregator may be interested in receiving at a higher frequency measurements from a set of smart meters), while the producers simply announce the availability of their data. Then, the middleware platform is responsible for distributing the relevant data to the subscribed consumers [237]. It is important to observe that the communication primitives provided by the middleware simplify the interactions between publishers and subscribers because subscribers do not need to know the identity nor the location of publishers, and vice versa. This decoupling is one of the main features that facilitate large-scale deployments. In the case of GridStat, the publishers are either sources of measurements and control settings (status variables), which are periodically updated by the middleware, or sources of alarm conditions (status alerts) that require immediate attention. On the other hand, subscribers are application programs that use these variables and alerts. Then, the GridStat middleware provides the services needed to control the way information is disseminated and accessed. For instance, a directory service is implemented to allow subscribers to find particular status variables of interest. Moreover, the publishers have the ability to inform the middleware infrastructure about the semantic of the status variables they monitor, such as type, availability frequency, and priority. Similarly, the applications can specify their QoS requirements for data access, such as the maximum delay for receiving status updates, the minimum update frequency, or the maximum number of updates that can be lost per unit time. In order to meet these QoS requirements directly at the middleware layer, the GridStat architecture requires the deployment of two classes of special devices within the smart grid:

- **status routers**, which establish redundant paths between the middleware peers to support QoS-aware multicast of periodic status updates;
- **brokers**, which are organized into a hierarchy of management entities that negotiate with the subscribers their initial QoS requirements in order to make them less stringent if necessary. In addition, brokers also handle the resource allocation in the communication network to ensure that the selected paths meet the QoS requirements of each subscription request.

A Java-based implementation of key mechanisms in the GridStat framework is described and experimentally evaluated in terms of delivery latency and throughput in [238]. Although GridStat offers a flexible and robust communication framework, it also suffers from a series of limitations. First of all, it only supports the publish/subscribe communication model, which is appropriate for delivering status updates or alerts, while alternative communication services (e.g., remote procedure calls for invoking commands) are needed in other use cases. In addition, GridStat relies on a rigid hierarchy of brokers that allocate resources at status routers and configure the network paths to meet the QoS application requirements. This scheme can generate significant signaling overheads. Therefore, other studies have considered alternative approaches based on self-organizing P2P technologies. For instance, a data-centric information infrastructure that uses a publish/subscribe communication model to deliver time-sensitive data between EMSs and distribution substations is designed in [109]. However, in this case the publish/subscribe system is not implemented using a centralized directory service as in [234], but through a distributed content overlay created over a networked pool of storage disks. In [109] it is assumed that these storage units are installed at substations but also sensors can be allowed to share part of their memory resources. Then, a distributed hash table (DHT) is employed for efficient and scalable data retrieval. More specifically, a hash function is used to generate a unique key per each data item, which is then stored and/or replicated among the peers in the network based on their identifiers. In this way, the overhead of both data storage and data search is evenly distributed among peers. This approach not only addresses the scalability issues caused by centralized storage repositories, but it also ensures improved reliability by avoiding single points of failures. In general, DHT-based overlay

---

**Fig. 7.** Classification of research trends in the area of middleware for smart grids.
networks can ensure a very efficient retrieval of single data items due to the use of key-based routing approaches [107]. Therefore, other papers have proposed to use DHTs for supporting large-scale data sharing and decentralized data repositories [231,239]. An alternative approach is proposed in [240], in which a middleware, called SeDAX, is developed to enable secure, large-scale data sharing to support both transaction and query-based communications. Specifically, SeDAX leverages on the properties of Delaunay Triangulation (DT) graphs to design efficient message forwarding schemes based on geometric hash functions. However, the creation and maintenance of a structured overlay network that maps each data key to a peer in the overlay is generally incurring high signaling overheads. Thus, other studies argue that unstructured P2P networks, which do not maintain a rigid overlay network, are more suitable for smart grid applications in which data must be distributed to a large number of interested parties at the same time [241].

6.2. Object-oriented middleware

The middleware solutions described in the previous section were primarily targeting the scalability of data dissemination and data sharing functions. However, as discussed in Section 5.1, interoperability between different devices, networks and communication technologies is another key requirement that smart grid communication systems must satisfy. The middleware paradigm that is commonly considered the most suitable for supporting interoperability between heterogeneous distributed systems is the object-oriented paradigm [106]. Specifically, in object-oriented middleware platforms, like CORBA [242] or Ice [243], resources, processes and components are abstract objects that implement standard interfaces, which hide all internal implementation details of the object. Furthermore, the object abstraction allows to invoke services or make calls to procedures on remote systems by also hiding the differences of underlying networking technologies. This distributed object-oriented paradigm is used in CoSGrid (Controlling the Smart Grid) [244], a middleware that provides support to specify special remote objects called embedding metering devices (EMDs). An EMD implements sensing and controlling capabilities, share information via remote method invocations, and it can be used to manage arbitrary smart grid components, from individual appliances to entire substations. EMD prototypes for different types of devices that work with CORBA and Ice are described in [232]. In addition, CoSGrid defines a set of interfaces for basic smart grid services, such as metering, notification, node and data aggregation, which can be used to ease the development of new distributed smart grid applications. A similar approach is followed by OHNet (Objected-based Middleware for Home Network) [245], an object-oriented middleware for supporting the interoperability between home devices and smart grid devices. In this system, home devices can be associated to state, function, control or streaming objects on the basis of their features, while discovery, connection and management objects are used to activate related functions on home devices. Then, OHNet ensures interoperability among devices, which may adopt different communication protocols and technologies, through the definition of the Virtual Network Adapte (VNA). Specifically, VNA is an abstraction layer that instantiates the invocations of abstract methods into protocol-dependent implementations. An alternative approach to build a Cyber-Physical Home Control System, i.e., a system that allows users to control appliances in the physical environment by intuitive operation through a virtual home on the network, is proposed in [246]. The key idea is to use an OSGi-based service architecture to support service-oriented remote control methods for home appliances. Note that the design of user-friendly and service-oriented HEMSs is a very active research area. For instance, the authors of [247] describe a system to control and manage home appliances in the framework of Universal Plug-and-Play (UPnP). Finally, the OSGi platform is also used in [248] to construct a general middleware for IoT applications involving RFID tagged objects, sensor networks and pervasive computing technologies.

Finally, it is worth noting that in the power engineering community there is an increasing consensus on the importance of the object-oriented paradigm, especially for the specification of interoperability standards. One example is the Common Information Model (CIM) [97], which is a series of open standards released by the International Electrotechnical Commission (IEC) to allow different applications to exchange information about the status of electric grid components. For instance, CIM-based models have been proposed to exchange power system data between: (i) energy management systems (IEC 61970 standards [97]), (ii) electrical distribution systems (IEC 61968 standards [98]), and (iii) intelligent electric devices within substations (IEC 61850 standards [249]). Then, CIM-based standards provide a common vocabulary to formally describe all the major components of a power system. Support is also provided to define multiple object classes and attributes, as well as the relationships between them [250,251]. Furthermore, the CIM architecture supports composition of different classes and attributes, which facilitates model flexibility and extensibility. However, it is important to note that CIM only facilitates the exchange of power system data in object-oriented communication systems, but how to extract useful information from an abstract representation of the power data is still an open issue.

6.3. Multi-agent intelligent systems

As observed at the beginning of this section, smart grids are complex systems consisting of a large number of heterogeneous and interdependent components operating in dynamic environments. Therefore, decentralized management is considered the only feasible approach to control the operations of electric grids over multiple time-scales [252,253]. However, with decentralized control it is difficult to achieve global optimization objectives, such as efficiency and stability of the entire grid. On the other hand, recently the emerging field of autonomic distributed computing has produced innovative middleware technologies to build intelligent distributed systems that are capable of managing, repairing, optimizing and protecting themselves without human intervention [253]. Among the various approaches that have been proposed so far to implement autonomic management capabilities in distributed environments, multi-agent systems (MAS in short) are the most popular in the smart grid research community [254,255,233]. This is also demonstrated by the large number of multi-agent systems that have been designed for a variety of smart grid applications, including power system restoration [256,257], fault diagnosis [258–261], management of distributed energy resources [262–264], demand-side management [265], management of energy storage systems [266,267], optimization of EV operations [268,269,270], substation automation [270], distribution control [271], network monitoring [272,273] and visualization [274,275], electricity market simulation [276,277], profiling of power generation and energy usage patterns [278], management of micro-grids and VPPs [279,280].

A MAS is a software system that is composed of multiple autonomous components – the intelligent agents – that interact with each other and react to environmental changes in order to accomplish a given task (e.g., to control a physical resource, or to solve a complex problem in a distributed manner) [280]. In the simplest case agents are reactive objects that can only respond to signals from the environment. In more advanced systems, agents can also be proactive in the sense that they are programmed to execute different actions in order to achieve a global goal. In addition, agents
can cooperate and coordinate with each other in order to find the best sequence of actions that could achieve that goal. To this end agents can employ various artificial intelligence techniques, including machine learning, fuzzy logic, neural networks or genetic algorithms for local decision making. Although an agent can show a high degree of flexibility and autonomy because it can dynamically change its behavior to achieve a given goal, it is also subject to an important limitation. Specifically, given the scale of the system to control the agent can only observe and measure small portions of the grid (i.e., the environment is only partially observable). This implies that an agent can not use global knowledge to make its decisions. Finally, it is useful to observe that the environment that is observable by a MAS can be either physical (e.g., transmission lines, generators of renewable energy, electrical appliances, etc.), and in this case it is observed through sensors; or virtual (e.g., databases, computing facilities, other agents), and in this case it is observable through programming interfaces [255].

From the above discussion we can observe that the main advantage of agent-based technologies in smart grids is to provide a decentralized management solution based on autonomous local decisions that can ensure a high level of flexibility and robustness. Although there are already many smart grid applications where MAS technologies have been investigated, there are also unsolved technical issues, which must be addressed in order to use this technology in real-world deployments. In the following we outline three of the most important technical challenges.

6.3.1. Functional architectures for MAS
A number of different functional architectures have been proposed in literature to build multi-agent systems [254], but there is not yet a consensus on which one of those approaches is the most suitable for smart grid applications. It is important to observe that flexible, extensible, and open architectures, where agents can be easily added or removed, should be preferred to closed architectures, where agent interactions are fixed at design time. The architectural model most commonly adopted in power systems is the multi-layered architecture. For instance, in [264] a three-layer architecture is proposed for managing distributed energy resources. In this model, the bottom layer consists of agents managing physical resources (e.g., energy generators and power storage systems). The middle layer includes agents that provide high-level management services (e.g., fault diagnosis, protection and restoration, optimization of power parameters, etc.) to the agents connected to the physical resources. Finally, the top layer contains the agents handling the user interfaces. To improve the scalability of MAS solutions many studies have proposed to group agents, especially those operating on physical resources, into clusters (e.g., a micro-grid cluster or a VPP cluster). Indeed, clustering and coalition formation are common techniques in multi-agent systems for reducing architecture complexity. For instance in [269] coalitions are used to integrate in a more efficient way electric vehicles into the electricity grid. In this case an aggregator agent, called coalition server, is used to hide the details about the individual vehicles, and to present a group of vehicles as a single resource to grid operators.

Alternative two-layer architecture models are considered in [257] for power system restoration, and in [272,281] for the management of the distribution grid. More precisely, in [257,272] two types of agents are considered: equipment agents and facilitator agents. The former are controlling physical resources, such as transmission lines, transformers and phase controllers, while the latter are used to promote the cooperation of the equipment agents that are associated to them. For instance, in [272] a facilitator agent is responsible for controlling an entire electric substation. A more elaborate architecture is described in [270], which defines multiple types of facilitators that perform different tasks such as: device control, data acquisition and transfer, data analysis and data querying. The use of facilitator agents is also proposed in [259]. However, in this case the facilitator agent is responsible for maintaining a list of services (or resources) that other agents in the system can offer (or control). With the support of a nameserver agent, which maintains the names and locations of each agent (e.g., IP addresses), a facilitator allows other agents to dynamically enter/leave the system and register/deregister their locations and capabilities.

6.3.2. Interoperability
When developing a multi-agent system it is essential to use standardized agent models to allow agents to easily cooperate, irrespective of their different capabilities and functions, or the platforms used to develop them. For these reasons in the MAS community there is a significant body of work focusing on the formalization of:

(a) agent specification languages, which are standards for defining messages types and agent interaction models. Today FIPA-ACL is used by MAS developers as the de facto standard for message exchange and interaction protocols [282];
(b) ontologies, which define a common "vocabulary" of terms and concepts that agents are able to exchange and interpret.

Currently, the trend in the community of MAS Developers is to implement application-specific ontologies. However, interoperability between multi-agent systems using different ontologies is difficult to obtain, even if they run on the same platform or they are based on similar concepts [283]. A solution to this problem is to employ a two-layer model for ontology specification. Specifically, the ontology in the top level, called "upper" ontology in [283], is responsible for defining the basic concepts that are in common to most smart grid applications (e.g., substation, switch, voltage, etc.), and it is used as a template for defining more specific ontologies for different applications. It is also useful to note that existing object-oriented standards for information exchange in power engineering applications, such as CIM [97] and IEC 61850 [249], can be easily used as reference models when developing an upper ontology for smart grid applications.

6.3.3. Implementation platforms
In recent years several tools and programming frameworks have been provided to develop multi-agent systems in the context of smart grid applications, and interested readers can refer to [284] for a complete survey. However, the open-source Java Agent Development Framework (JADE) [285] is probably the most common platform for developing MAS solutions for smart grid applications. Most of existing MAS implementations are prototypes used for lab-based experiments [286,277], which aim at demonstrating the feasibility of the MAS approach. Recently some multi-agent systems have been tested into operational electric grids. For instance, a multi-agent system, called Protection Engineering Diagnostic Agents (PEDA) [259], has been used by a transmission system operator in the U.K. to interpret SCADA-related data and to provide online diagnostic information and alarms [287]. In [269] a multi-agent system is implemented using JADE to integrate a group of electric vehicles into the electric grid and to support both demand response and V2G services. However, to demonstrate that MAS technologies meet the robustness and reliability requirements of typical power grid applications, large scale testing is still needed. A valuable option to avoid the costs and risks associated to test new technologies in real power grids is to employ realistic simulation tools that simultaneously model electric power scenarios and the behaviors of computer communication protocols. An example is provided by EPOCHS [288], which is a combined
7. Security mechanisms for smart grids

Electric utilities consider security, protection and reliability of the electric infrastructures one of their key priorities because failures or malfunctions in power systems not only would have an economical impact, but could also cause serious damages to people. Historically security in power systems was obtained by ensuring physical protection of power generators and distribution grids, as well as physical isolation of utility control centers. Furthermore, closed and dedicated communication networks running proprietary protocols were typically used in SCADA-based power control systems [3]. On the other hand, it is reasonable to expect that in smart grids the deployment of distributed and autonomous control functions, as well as the adoption of open network architectures, will bring new security vulnerabilities to smart grids and they will allow a variety of unforeseen security attacks. Different categories of security attacks specific to the smart grid domain have been discussed and identified in previous survey papers [117,21,295,296,24,297]. Based on those studies, the most important vulnerabilities of the smart grid communication system can be broadly classified as follows:

- **Device vulnerabilities**: IEDs will be widely deployed in smart grids to monitor and remotely control electricity production and distribution processes. However, malicious users or attackers can compromise these devices, e.g., to manipulate sensed data or to disrupt normal grid operations. Furthermore, many IEDs will support wireless communications to facilitate deployment and simplify the access to information. An intuitive downside of wireless communication technologies is that they rely on an inherently unprotected physical medium. This makes easier to capture private information (eavesdropping), disrupt communications with noise signals (jamming attack), or generate fake messages (injecting attack). Solutions of these attacks include encryption of messages for data integrity and confidentiality, authentication of network access, and various randomized transmission methods, such as spread spectrum techniques [23].

- **Network vulnerabilities**: The adoption of open network architectures, off-the-shelf network devices and publicly available communication standards is needed to meet the flexibility, scalability and interoperability requirements discussed in Section 5.1. However, this also causes various security problems observed in other telecommunications networks adopting open architectures (e.g., Internet), such as malicious modification of routing information, DNS hacking, and various types of denial of service (DoS) attacks. More specifically, in a typical DoS attack an attacker can control a set of nodes to overwhelm other nodes with data traffic, resulting in excessive network delays or even communication failures. For instance, compromised smart meters can be forced to flood an EMS with meaningless messages. In this way an EMS would consume all its computational and communication resources and it would not be able to timely react to legitimate requests. To prevent these network attacks, access control and intrusion detection are essential security mechanisms. Similarly, authentication and authorization schemes are also necessary to support secure remote configuration and control of geographically dispersed devices [298].

- **Data vulnerabilities**: Data manipulation is an important security issue because an attacker can modify data or control commands to compromise electric grid reliability. However, smart grids will also be increasingly vulnerable to data attacks designed to compromise the privacy of customers. For instance, the man-in-the-middle attack is a popular method used by malicious users to gain access to information without physically compromising the target. If an attacker is able to snoop the metering data transmitted from the consumer’s home it could infer consumer’s habits and activities. For instance, it would be possible to learn whether a home is occupied or not by detecting power consumption signatures of specific activities (e.g., watching television or using the microwave) [299]. As better explained in following sections, encryption, message authentication and intrusion detection schemes are needed to preserve data integrity and confidentiality in smart grids [21].

Finally, it is important to point out that security techniques developed for other telecommunications networks can fail to meet the security requirements of smart grid communication systems because [300]:

(i) Many security attacks envisioned for smart grid communication systems do not have a counterpart in other computer networks because they can target either the physical power system or the communication infrastructure or both [301]. For instance, in the power system there are several control loops used to control physical aspects of generation, transmission, and distribution processes, and an attack directed at the communication networks underlying these control loops can have a system-wide impact on power system stability.

(ii) Typical security objectives and priorities for smart grids are different from those of most telecommunications networks. Indeed, in most networks data confidentiality and integrity are more important than communication availability. On the contrary, in a power system electricity must always be available. Thus, availability is the most important security objective along with the protection of consumers’ privacy.

(iii) Most devices that are used in smart grids are expected to be heavily constrained in terms of computation capabilities and data storage. Thus, security techniques developed for high-capability Internet-enabled devices (e.g., servers, laptops, or smartphones) are not suitable for smart grid devices.

In the rest of this section we will present some fundamental security techniques that should be integrated in smart grids for improving the robustness of smart grids against various security attacks and privacy risks. Furthermore, we will also discuss a few representative solutions in each category to clarify interesting open problems. For the sake of clarity, in Fig. 8 we provide a classification of major research trends in the area of security for smart grids, which we have also outlined in following sections.

7.1. PKI management

A public key infrastructure (PKI) is a fundamental security tool in most telecommunications networks and distributed systems in
PKI-based security solutions have been extensively studied [302,303]. Basically, a PKI is a system of software and hardware components providing digital signatures, called certificates, which are used to identify a certain entity (e.g., a device, a program, an organization). These certificates are securely stored by a trusted certificate authority (CA), which also decides when and how to renew or revoke them. For instance, smart meters can register their serial numbers with a CA. Typically, a PKI employs public key cryptography techniques, which are based on the simultaneous creation of a pair of public and private keys, to securely store and exchange certificates. The public key is publicly available (as part of the digital certificates) in central repositories and it is used to encrypt messages, while the private key is known only to the recipient of the message and it is used for decryption. This is substantially different from symmetric key crypto-systems, where there is an initial exchange of a shared secret key, which would require to pre-establish a secure communication channel. Finally, PKI also supports message authentication because the sender can use its private key to encrypt a digital certificate, which is then utilized to sign transmitted messages.

Although PKI is the most popular key management scheme in the Internet there are some issues to apply existing PKI solutions to the smart grid domain [302,304]. First of all, there is a scalability problem because a PKI for smart grids should maintain certificates for millions of devices. Furthermore, differently from classical PKI systems, we cannot assume that identities are the only relevant properties that should be certified in smart grid devices. For instance, context information such as the installation location of the devices could also be included in the certificate. However, this information is known only after the installation and it may change dynamically. Hence, digital certificates associated to smart grid devices should also be dynamic. Finally, smart grids must support real-time and reliable operations. Therefore, PKI technologies should meet strict delay constraints and provide fault tolerance to ensure high availability. However, a PKI involves centralized authorities and complex certification policies and it might be quite challenging to satisfy latency requirements.

To address the above issues a number of research directions are currently being investigated. For instance, it is generally agreed that more automated configuration tools are needed for PKI systems in smart grids. These tools will be used to allow each organization to set its own security policies (how private keys are protected, which is the validity time of a certificate, how certificates are revoked, etc.) and to easily adapt these policies to the different requirements of smart grid devices and applications [302]. A large body of work is also dedicated to the design of PKI architectures that are able to meet the reliability, scalability and delay requirements of smart grids. For instance, a novel key management scheme is proposed in [305], which combines public-key and symmetric key approaches to achieve simplicity and to improve scalability. Basically, trust anchors are deployed in the PKI system, which employ robust public key methods to establish symmetric keys between data aggregators and data collectors. Then, trust delegation mechanisms are used to allow simple sensors nodes to access the grid and to communicate with data agents. However, the key distribution scheme proposed in [305] can suffer from the man-in-the-middle attack during the initial authentication phase. To solve this issue, in [306] it is proposed to use trusted third parties to distribute shared keys among the components of the smart grid. The focus of the work in [307] is the scalability and interoperability of the key management system. In particular, the key management scheme proposed in [307] uses existing standard protocols for network access authentication (i.e., EAP) to avoid that multiple authentication and key establishment processes are performed across different protocols and link-layer technologies. A simple PKI system is designed in [308], which assumes that a unique machine number is available at each device, which can be used by a central server holding a master key to generate unique private keys. The main advantage of this scheme is that it does not require to separately configure each device. On the other hand, unique machine identifiers are not always available. Finally, a public key crypto-system is proposed in [309], which exploits homomorphic encryption techniques to avoid that a pair of public and private keys is generated for each communication link between customers and utility control centers. In general, an aspect that needs much further investigation is the design of enhancements to existing PKI systems to support new use cases, in particular those due to the increasing adoption of mobile electric vehicles.

7.2. Authentication and access control

An essential security mechanism is the authentication method, which is used to verify device identities and data validity. As observed above PKI systems inherently provide device authentication through digital signatures. The authenticated device identity can be exploited to establish shared secret keys that are used for encrypting and authenticating data packets. It is important to note that symmetric key cryptography is generally preferred to public key cryptography for data authentication because it uses the same key for both decryption and encryption, and this results in faster cryptographic algorithms that requires less processing power. However, authentication schemes suitable for smart grids should take into account the limited resources (i.e., low memory and computational capacity) of most smart grid devices, as well as the stringent delay requirements of smart grid applications. A lightweight message authentication scheme is proposed in [310], which aims at minimizing the number of messages exchanged during authentication. This is achieved by combining the Diffie-Hellman
protocol for key establishment and an hash-based message authentication code (MAC) technique. An authentication protocol is proposed in [311] for multicast communications, which reduces storage and bandwidth overhead with respect to other schemes that use public-key signature over multiple messages. An alternative authentication approach is proposed in [312], which ensures both authentication and data integrity by jointly using digital signatures and timestamps. Finally, three authentication mechanisms are specified in [313] for devices typically used in HANs, such as smart meters, smart household appliances, and electric vehicles moving. Note that EVs pose the most complex authentication problems because they can move between different home area networks.

A data protection mechanism that it is closely related to device authentication is access control, which aims at ensuring that access to objects (i.e., any entity containing information or providing services) is permitted only to authorized users. The most common access control schemes in telecommunications networks are based on access control lists (ACLs), which specify the identities of users allowed to access shared objects and what privileges they have. However, ACL-based approaches may not scale with the huge number of customers and resources involved in smart grid services. Therefore, most of the research in this area is focusing on the formulation of role-based access control methods, in which permissions to perform certain operations are assigned to specific roles rather than user identities. A network access control model for power system with micro-grids is described in [314], in which each micro-grid is a separate network domain with an independent control center that maintains XML-based security policies and roles. In this scheme a role is defined as a collection of privileges that can be executed by authorized users in local and remote domains. Note that each user can be assigned with multiple roles. Furthermore, to improve scalability roles are structured into a hierarchy in which the “parent” role directly inherits all the privileges of its “children” roles. In [315] it is proposed to store data in an encrypted form that depends on the data attributes. Then, only users having the same attributes as the data can decrypt those messages. Finally, an alternative scheme is proposed in [316] to use smart meters as firewalls between home area networks and the utility core backbone.

7.3. Privacy protection and data integrity

The most intuitive method to ensure data privacy is to use a cryptographic protocol, which preserves data confidentiality by encrypting data messages between data originators (e.g., smart meters) and utility providers. The device authentication schemes described in the previous section can be used to create the shared secret keys that are needed for message encryption. However, the massive deployment of smart meters and smart appliances also raises new privacy concerns. Specifically, it becomes an important issue to avoid that malicious users can learn information about customers’ behaviors and habits. For these reasons several privacy protection methods specific for smart metering have been recently proposed [22]. These solutions can be categorized into two separated classes: anonymization techniques and randomization techniques.

Anonymization techniques achieve privacy protection for metering data by anonymizing energy usage measurements in order to make more difficult to associate metering information to a particular smart meter or customer. In [317] this is achieved by assuming that a trusted third party provides pseudonymous identities, which are then used to anonymize high-frequency metering data. Note that this metering data is the most critical to infer usage patterns of specific electrical appliances, while low-frequency metering readings used for billing purposes are rarely enough to offer adequate privacy. The use of a trusted third party is also proposed in [318], although this approach introduces additional complexities and requirements to the security framework. More efficient schemes can be designed by exploiting secure data aggregation techniques. For instance a privacy-preserving aggregation scheme, called EPPA, is designed in [319], which permits to perform data aggregation at intermediate proxies without decrypting the data received by individual smart meters. A new encryption mechanism is also proposed in [299], which allows a group of smart meters to encrypt their data in such a way that electric utilities can reconstruct aggregated energy usage information without decrypting them. Note that the main open issue in this class of privacy protection schemes is how to preserve the ability of electric utilities to know the instantaneous electricity consumption, which is needed to support demand response and direct load control.

Randomization techniques are used in particular to protect the confidentiality of usage patterns of household electric appliances. More specifically, this class of schemes achieve privacy protection by manipulating the metering data with some stochastic perturbation function so that it is difficult to infer patterns of energy consumption. For instance, a simple privacy scheme is developed in [318], which adds random Gaussian noises to each smart meter. This approach is simple but not very robust because it applies randomization on true readings and statistical methods could be used to extract load profiles. More sophisticated schemes are developed in [320], which mix actual smart meter readings with faked readings sampled from arbitrary distributions. However, further studies are needed to understand which is the level of uncertainty that is added by such randomization methods, and whether useful information about energy consumption can be maintained in the modified data. Finally, an alternative approach is proposed in [321,322] by assuming that smart homes will contain a variety of energy storage and generation systems, which can be used to obfuscate appliance load signatures by randomly mixing utility electricity with electricity from local generators.

7.4. Intrusion detection

Although several security mechanisms can be used to deal with security attacks, more sophisticated attackers can exploit unknown system vulnerabilities and succeed in compromising network components. In this case an intrusion detection system (IDS) is essential to identify the attack and trigger appropriate countermeasures. There are different approaches that can be applied to design intrusion detection techniques, but at least three major methodologies can be identified [323]:

- Anomaly detection: anomaly detection recognizes intrusive actions by looking for deviations from normal behaviors of protocols, programs or processes. This approach requires the specification of accurate statistical models of normal profiles, which can be quite difficult and costly to obtain. The main advantage of anomaly detection is its ability to detect unknown attacks. However, anomaly detection techniques also produce a high number of false alarms if the model is not sufficiently accurate. Furthermore, this approach is suitable for relatively stable systems, otherwise new models of normal operations should be developed after any configuration change.

- Signature detection: signature detection is complementary to anomaly detection because it uses deterministic patterns of known attacks to characterize malicious behaviors. The main advantage of signature-based methods is that they provide high accuracy and a low number of false alarms. However, there are also some drawbacks such as the inability of these schemes to detect novel attacks, whose
signatures are unknown. Furthermore, pattern matching techniques and classification algorithms typically used in signature detection methods can be quite costly in terms of computing and data storage.

- Specification-based approach: specification-based methods detect attacks by defining ordered sequence of events, called policies, which corresponds to correct protocol behaviors. A violation to this set of constraints and rules is considered a security violation. A specification-based IDS is able to detect unknown attacks as for anomaly detection. However, an obvious downside of this class of techniques is that the development of specifications is time consuming and protocol specific. Another issue is that specifications are difficult to verify on devices that have limited memory and computational power.

In the following we outline most representative solutions for intrusion detection in the smart grid domain based on the above categories.

A key design problem for both anomaly and signature detection methods is to collect empirical data from smart grids and to extract accurate models for normal and malicious behaviors, respectively. Note that many intrusion detection schemes use neural networks to learn normal profiles and detect deviations from these profiles [323,324]. However, those techniques do not seem suitable for smart grids because they are quite demanding in terms of computational and memory overheads. Furthermore, they do not guarantee deterministic response times. A variety of techniques have been proposed to address those issues. For instance, in [325] supervised learning models known as support vector machines (SVM) are used to extract features (e.g., connection duration and protocol type) and recognize patterns representing normal communications because of their high accuracy and scalability. In [326] it is shown that Decision Tree techniques can outperform other supervised machine learning techniques to implement real-time intrusion detection. A novel unsupervised network intrusion detection system based on clustering techniques is described in [327]. Alternatively, if service level agreements (SLAs) are established between the service provider and its customers then SLA monitoring can be used to detect service violations and to verify intrusion attempts [328]. In addition, [325] defines a hierarchical IDS solution, in which an IDS module is installed at each protocol layer. Then, individual IDS modules are trained using data that are relevant to their level, but they also cooperate to detect possible attacks. In [329] malicious events are modeled as random variables following a Gaussian process. For instance, a random variable may be used to represent the number of malfunctioning smart meters in a building, or the number of failed authentication attempts in a given time interval. Then, conventional stochastic tools are used to predict the occurrence of an attack. Distributed and low-complexity pattern recognition algorithms are also developed in [330,331]. Finally, many anomaly detection algorithms utilize a sensitivity threshold to detect violations of normal behaviors, and the proper selection of this threshold is essential to reduce the occurrence of false alarms. In [332] fuzzy-logic rules are developed for tuning this sensitivity threshold based on an estimate of the system knowledge obtained by the IDS module. However, an intelligent adversary could compromise the IDS and adapt its actions to reduce the probability to be detected. How to dynamically adjust the sensitivity threshold in response to more intelligent attacks is still an open issue.

An important challenge for both anomaly-based and signature-based IDSs is to identify which are the relevant events to monitor in the power system, and many studies exist that try to classify different types of attacks. Since a specification-based IDS do not require empirical data to detect intrusions, this class of intrusion detection schemes has been considered as a valid alternative to more sophisticated IDS solutions, at least in the early stage of smart grid development. For instance, in [333] a specification-based intrusion detection method is designed for the C12.22 standard protocol, which specifies an application-level messaging protocol to exchange power data over a network. In [334] a specification-based IDS is developed of the IEEE 802.15.4 standard applied in home area networks. However, there is still a high overhead associated to these schemes, and it might be impractical to run them on smart grid devices.

7.5. Security analysis

Utility companies need formal security analysis or simulation tools to quantify the robustness provided by adopted security mechanisms, as well as to predict the impact of attackers on smart grid operations and reliability. Obviously there are many tools to analyze vulnerabilities in traditional telecommunication networks [335] (e.g., to identify misconfiguration problems), and to rate and score known vulnerabilities [336]. However, new specific solutions are needed for smart grids due to the heterogeneity of devices, protocols and configurations. An automated tool for AMI configuration verification, called SmartAnalyzer, is developed in [337] using formal analysis based on Satisfiability Modulo Theories (SMT). Basically, this tool encodes AMI configuration templates, which describe device configurations, network topologies, monitoring schedules, into SMT logic. Then, an SMT solver is used to verify this configurations against a set of high-level constraints (e.g., reachability between devices, schedule and resource constraints) and user-driven constraints (e.g., data protection, data integrity, transmission reliability). The output of this verification process is a report that indicates reasons of constraint violations and possible remedies. An alternative approach to quantify the degree of damages that cyber attacks can cause to a power systems is designed in [338]. The key idea is that both physical components (i.e., electric grid elements) and cyber components (i.e., network devices and functionalities) can be modeled as objects to which state information is associated. Then, directed graphs are used to represent state dependencies amongst the various objects. Finally, a system of differential equations is utilized to specify the rules governing state evolution, and to model cause-effect relationships. However, identifying cause-effect relationships in large-scale power systems is a challenging task. Another class of methods for risk analysis in smart grids rely on computational intelligence approaches. A useful technique in this class is fuzzy logic because it supports probabilistic risk assessment by measuring uncertainties in the decision making processes and allowing for incomplete or ambiguous data (fuzzy data). An overview of the main algorithms in computation intelligence used in smart grid risk assessment is reported in [339]. A key open issue in the area of risk assessment is the design of toolkits that automatically generate models of the power system from specifications, operating procedures and network topologies to describe the vulnerabilities of devices, services and network connections. Note that power grid models are essential to identify system vulnerabilities, predict new attacks and evaluate potential service damages [340].

Related to risk assessment (as well as intrusion detection) is the design of mechanisms to evaluate the trustworthiness of smart grid objects (e.g., devices, service providers, entire subsystems). Specifically, a trust system allows an entity to assess the reliability of another entity before deciding to interact with it (e.g. to use a service provided by that entity) [341]. In this way, a trust model can be used to determine risks and to give a weight to those risks. Typically, trust models are associated to reputation systems, which enable peers to rate each other after the completion of a certain task. Then, a reputation system uses the aggregated ratings about
a given peer to derive its reputation score (or trustworthiness). As an example, power protection applications generally rely on the cooperation among grid components to cope with grid failures or grid instability. Thus, it will become very important to decide which is the best entity to collaborate with, and the reputation plays a key role in the decision process. For these reasons, various studies exist that have explored how to integrate reputation-based trust management systems in smart grids. For instance, in [342] a trust management methodology is developed to verify if individual smart meters generate selfish and malicious reports on energy usage. Furthermore, one of the advantages of a trust system is to provide an additional layer of protection in power systems implementing agent-based control functions as discussed in [343,344]. Specifically, those studies consider a backup protection scheme and propose trust metrics to improve the reliability of network communications. Similarly, in [345] an early warning system is designed for predicting and anticipating cascading failures in power systems, which uses a reputation mechanism for controlling network behaviors. Furthermore, nodes in a network can be assigned different roles and perform different functions depending on their trust levels [346]. Note that the design of suitable techniques for quantifying trust levels in dynamic environments while preserving data privacy is an open issue.

8. Summary and outlook on key research areas

In this survey we have advocated the view of a smart grid as the outcome of an evolutionary transformation of the existing electricity network towards an optimized and sustainable energy system. We have analyzed the several factors that are contributing to this evolution, ranging from technological developments (e.g., the introduction of electric vehicles, the deployment of renewable energy resources, the recent advancements in energy storage systems, time-synchronized measurement technologies of electricity quality) to economical and societal drivers (e.g., liberalization of energy markets with the advent of prosumers, new environmental concerns about climate changes and pollution, soaring growth of energy demands, need for higher operating efficiency, active participation of consumers in demand response, better resiliency against both physical and cyber attacks). The incorporation in the smart grid of a pervasive monitoring and communication infrastructure is essential to: (a) measure the system state, (b) collect the sensor information and propagate control signals, and (c) allow distributed smart applications to control power flows in the network. Thus, the goal of this survey was to present a complete model of this monitoring and communication infrastructure, covering all layers of its architecture, ranging from communication technologies at the physical layer, to communication topologies and protocols at the network layer, and concluding with middleware services needed to support the new applications in a distributed fashion.

We believe that this survey could provide the reader with a useful overview of the state-of-the-art solutions proposed at all layers of the smart grid communication infrastructure, as well as a guide of the open research issues. Hereafter, we aim at summarizing some of the novel research directions that are still worth exploring.

- Due to the massive number of data sets that will be collected in smart grids, classical database-management tools can be unable to process them within acceptable delays. In addition to data analysis, other critical issues are data storage, search and visualization. Nowadays there are many application domains that are already witnessing an explosion of collected data, such as healthcare, retail markets, online social sites, but smart grids have the potential to become one of the most demanding one [347]. However, since temporal and spatial variations of most electric processes are small, it is reasonable to expect that most measurements in this massive amount of data will be redundant. This creates many opportunities for the design of data mining techniques able to provide data compression. Furthermore, the design of novel knowledge-discovery methodologies that are specific for electric data is a very compelling research topic. Finally, cloud computing is considered an important data and computing model for data intensive smart grid applications.

- Energy routers indicate devices that allow units of energy (locally generated, stored, and forwarded) to be dispatched when and where it is needed [164]. The deployment of energy routers within the smart grid can enable innovative paradigms for energy distribution and control, in which energy is logically packetized, buffered and forwarded over the physical energy network. While energy routers guarantee more flexible and efficient power distribution and this facilitates an increased use of renewable energy sources, they also pose new challenges. As an example, an energy router should be able to dynamically redirect incoming energy flows towards outgoing energy flows. Thus, new power electronics are required in energy routers to implement automatic energy control. Similarly, energy routers should implement distributed intelligence to control the energy routing process. Furthermore, innovative ways of dispatching energy in a smart grid can be devised taking advantage of EVs. For instance, we can use the batteries of EVs as a mean of physically moving electrical energy. In this way EVs can support a delay-tolerant transfer of energy between homes. However, to quantify which are the potential gains of this approach a detailed cost-benefit analysis is necessary.

- The design of optimization strategies for the smart grid is a very active research area, and there is a rich set of methodologies and algorithms from different domains that have been considered for this purpose. For instance, there are several algorithms in the literature to determine the optimal load schedules of groups of domestic appliances. However, how to design management and control schemes able to provide real-time and wide-area control with limited computational costs is still an open problem. We believe that flow-based congestion control algorithms, which have been commonly applied in large-scale information networks, such as the Internet, may be a promising and attractive approach to mitigate power congestion by reducing peak loads. For instance, there are electric devices that can elastically adapt the amount of instantaneous power they need, such as many common household appliances. Then, those devices could intelligently increase/decrease their power demands depending on congestion feedback signals from the utilities.

- Due to the intrinsic differences between conventional power grids and smart grids, existing electric power simulation/analysis tools will not be able to accurately model and predict the behavior of new power grids. For instance, more precise models of renewable energy resources at increasingly lower time and spatial scales are needed to increase the reliability of protection and control systems. Similarly, the behaviors of power systems will be increasingly dependent on external factors, such as the reliability of the smart grid communication network. Thus, power simulators should integrate tools to model each component of a smart grid, as well as the possible interactions between components.
Security mechanisms are an essential part of a smart grid. Although a considerable amount of research has been conducted in this field many open issues still exist because the increased interconnection and integration, e.g., between electric grid, monitoring and communication network, data management systems and applications, also introduce new cyber-vulnerabilities into the smart grid. The most compelling research challenges are the design of suitable mechanisms to protect the confidentiality and integrity of metering data, as well as new mechanisms to control the access to smart-grid components and resources given that physical isolation of the power grid might not be feasible anymore.

References


National Institute of Standards and Technology (NIST), Guidelines for smart grid cyber security: smart grid cyber security strategy, architecture, and high-level requirements, NISTIR 7628, vol. 1, August 2010.


