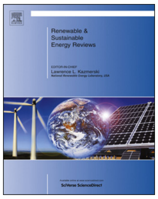
Renewable and Sustainable Energy Reviews 57 (2016) 302–318

Contents lists available at ScienceDirect

Renewable and Sustainable Energy Reviews

journal homepage: www.elsevier.com/locate/rser



# A survey on smart metering and smart grid communication

Yasin Kabalci*

*Department of Electrical and Electronics Engineering, Faculty of Engineering, Nigde University, 51240 Nigde, Turkey*

ARTICLE INFO

*Article history:*
Received 4 September 2015
Received in revised form
10 December 2015
Accepted 17 December 2015
Available online 5 January 2016

*Keywords:*
Smart grids
Microgrids
Advanced metering infrastructure
Automated meter reading
Communication
Smart grid security

ABSTRACT

The smart metering and communication methods used in smart grid are being extensively studied owing to widespread applications of smart grid. Although the monitoring and control processes are widely used in industrial systems, the energy management requirements at both service supplier and consumer side for individuals promoted the evolution of smart grid. In this paper, it is aimed to disclose in a clear and clean way that what smart grid is and what kind of communication methods are used. All components of a smart grid are introduced in a logical way to facilitate the understanding, and communication methods are presented regarding to their improvements, advantages, and lacking feature. The developing generation, transmission, distribution and customer appliances are surveyed in terms of smart grid integration. The communication technologies are introduced as wireline and wireless classification where the key features are also tabulated. The security requirements of hardware and software in a smart grid are presented according to their cyber and physical structures.

**Contents**

## 1. Introduction

The conventional grid is quite degraded from its first installation up to now and is not able to meet the actual requirements of information age. Although the smart grid (SG) that is based on its conventional ancestor, it supports to have an additional communication medium due to its capabilities. Owing to this popular technology, we can monitor the energy consumption and the actual indoor situations of our homes by using smart phones or other mobile devices. On the other hand, it provides to manage our energy consumption, having broadband internet, and converting homes to smart environments. Then, what are the components of this system?

* Tel.: +90 388 225 22 42; fax: +90 388 225 01 12.
*E-mail address:* yasinkabalci@nigde.edu.tr

http://dx.doi.org/10.1016/j.rser.2015.12.114
1364-0321/© 2015 Elsevier Ltd. All rights reserved.

**Nomenclature**

| | |
|---|---|
| ADSL | Asymmetric digital subscriber line |
| AGC | Automatic generation control |
| AMI | Advanced metering infrastructure |
| AMM | Automatic meter management |
| AMR | Automated meter reading |
| BAN | Building area network |
| BB-PLC | Broadband PLC |
| CHP | Combined heat plants |
| CIS | Consumer information systems |
| CR | Cognitive radio |
| DER | Distributed energy resources |
| DG | Distributed generation |
| DMS | Distribution management system |
| DoS | Denial-of-service |
| DSL | Digital subscriber line |
| EMS | Energy management system |
| EV | Electric vehicles |
| FAN | Field area network |
| G2V | Grid-to-vehicle |
| GEO | Geostationary earth orbits |
| GIS | Geographic information system |
| GPS | Global positioning system |
| GSM | Global System for Mobile Communications |
| HAN | Home area networks |
| HD-PLC | High Definition PLC Alliance |
| HomePlug | HomePlug Powerline Alliance |
| IAN | Industrial area network |
| LAN | Local area network |
| LEO | Low earth orbits |
| LTE | Long-term evolution |
| MAN | Metropolitan area network |
| MDMS | Metering data management system |
| MEO | Medium earth orbit |
| NAN | Neighborhood area network |
| NB-PLC | Narrowband PLC |
| NIST | National institute of standards and technology |
| OFDMA | Orthogonal frequency division multiple access |
| OMS | Outage management system |
| OSI | Open systems interconnection |
| PEV | Plug-in electric vehicle |
| PHEV | Plug-in hybrid electric vehicle |
| PHY | Physical layer |
| PKI | Public key infrastructure |
| PLC | Power line communication |
| PMU | Phasor measurement unit |
| QoS | Quality of service |
| RES | Renewable energy sources |
| SAE | Simultaneous authentication of equals |
| SCADA | Supervisory control and data acquisition |
| SFC | Secondary frequency control |
| SM | Smart meter |
| SSMP | Secure smart-metering protocol |
| SSP | Secure signal processing |
| T&D | Transmission and distribution |
| UMTS | Universal mobile telecommunications system |
| UPA | Universal Powerline Association |
| V2G | Vehicle-to-grid |
| VDSL | Very-high bit rate digital subscriber line |
| VHDSL | Very-high bit rate digital subscriber line |
| VoIP | Voice over internet protocol |
| VPN | Virtual private network |
| VPP | Virtual power plant |
| WAN | Wide area networks |
| WiMAX | Worldwide interoperability for microwave access |
| WPAN | Wireless personal area network |
| WRAN | Wireless regional area network |
| WSN | Wireless sensor network |

The SG is the most recent term that is used to describe the communication and control facilities integrated to the conventional grid in the 21st century. Although several appellations as intelli-grid, intelligent grid or inter-grid are used, the smart grid term is widely accepted for the grid including wireline and wireless communication infrastructures [1]. The main contribution of SG to conventional power grids is to provide bidirectional flow of energy and communication signals. The widespread control and communication substructure enables the SG to react to the changes that are occurred in any part of generation, transmission and distribution (T&D), and customer substations. This ability is inherited from sensor networks and agent based observation of entire grid where the integrated controllers instantly communicate with each substation and energy conversion units such as transformers, converters, inverters, and generators. Moreover, this kind of observation provides to detect source and load side demands to manage the energy flow in an extended decision circumstances [1,2]. On the other hand, the SG concept lists several problems in the conventional and centralized grid since the SG is based on distributed generation (DG), and to advance the conventional grid [3–5]. According to a report cited in [4], the fossil fuels that cause greenhouse gas effect, climate changes, and environmental impacts consist more than 80% of the globally generated energy. Another promoting factor of SG is centralization and degrading problems of conventional grid. These disadvantages cause harder restorations against peak load demands [4].

The preliminary researches on SG were the first steps of planning and designing the future energy networks that are fully interactive with generation plants and customers. The security, sustainability, efficiency, and reliability of SG should be taken into consideration besides its economic aspects [6,7]. In this point of view, the recent innovative SG researches include automatic voltage and frequency control, droop control, active and reactive power control, demand side management, microgrid integration, cyber-secure communication, and computational intelligence methods [8–10]. The SG environment can be analyzed in three technical perspectives as infrastructure, management, and protection. The infrastructure of SG involves the highest share of smart generation, T&D, metering, monitoring, and communication sections. High penetration of alternative energy sources, microgrids, and clean energy sources are listed in the infrastructure perspectives [1,9]. The advanced power electronics, sensing and measurement technologies are also related to infrastructural issues that improve the development of SG in terms of power management and demand control. The adaptive communication and smart control opportunities allow fast, accurate and real-time control owing to computational intelligence technologies [9,11]. Another lacking feature of the conventional grid is unidirectional communication and energy flow. It prevents the interaction between utilities and users in terms of bidirectional communication. It is not possible to detect how much energy is consumed or is wasted by the consumer in billing terms since there is not any monitoring or measuring infrastructure is located at the end-user side [4].

The smart infrastructure provides the bidirectional energy and data flow depending its energy, intelligence, and communication infrastructures. The conventional unidirectional grid is based on generating the energy and supplying to load sites over T&D lines. However, the SG allows load sites or customers to generate energy and supply to the utility grid by using micro-generation sources enabling bidirectional energy flow. The micro-generators can be either conventional or alternative sources that operate in the microgrid structure and assist the utility grid. The smart communication subsystem covers monitoring and metering objectives of entire generation and consumption parts of the SG [1,9]. The smart management systems require some purposes such as energy efficiency, demand profile, energy loss prevention, cost and pricing, several optimization processes, machine learning and control services. The smart communication and intelligence subsystems are related to management systems as well as infrastructural components. Therefore, the smart protection covering reliability, prediction, localization and security issues are the most recent research area of SG. The monitoring and measurement requirements are performed in this perspective. Smart metering systems measure the consumption and other related billing parameters in the predefined intervals. The measured data are modulated according to communication protocol and are transmitted to management system over wireline or wireless networks. The advanced metering infrastructure (AMI) could be assumed as the developed version of traditional automated meter reading (AMR) and automatic meter management (AMM) systems since it involves several enhanced technologies such as smart meters (SMs), home area networks (HANs), wide area networks (WANs) or neighbored networks [8,9].

The smart protection covering reliability, prediction, localization and security issued are the most recent research areas of SG. The failure detection, diagnosis, self-healing, and microgrid protection issues are also other aspects of smart protection system. The SG reliability depends on the sustainability of DG where the intermittent characteristics of renewable energy sources (RES) and fluctuations caused by load variations should be prevented to affect the SG. The measurement and monitoring systems become vital in order to pursue the reliability and quality of service at the required standards. Another important mission of SG protection is fault protection infrastructure that is based on prediction and prevention. In the next step of prediction mechanism, the fault detection, diagnosis, and fixing the fault should be rapidly performed by the system itself or by the operator. Consequently, the smart protection is handled in two points of view that are prevention before fault and recovering after fault. The prevention stage is performed by observing the amplitudes of voltage and currents, thermal variations, transient and steady state parameters continuously. This kind of monitoring prevents major faults. The fault detection and diagnosis rely on widespread measurement and communication network consisting phasor measurement units (PMUs), smart metering units as AMI and AMR, and other sensor networks [1]. Fig. 1 illustrates a detailed sketch of a smart grid that consists of DG sources, conventional generators such as combined heat plants (CHP), fossil fuel based power plants, RES, and loads namely electric vehicle (EV), intelligent buildings, smart homes, and data center that manages entire communication infrastructure. The communication system of an SG as shown in Fig. 1 should meet the system requirements such as quality of service (QoS), reliability, coverage and sustainability, and security and privacy [12]. The QoS of a communication infrastructure is important to perform the transmission securely. On the other hand, large number of nodes and systems are connected to communication system where several topologies and management substructures should be pursued in a reliable way.

The main purpose of this paper is to focus on smart grids and smart grid communication systems by taking into account the related technologies, applications and faced challenges. Hence, the outline of the paper is constituted in four main sections as SG and smart energy infrastructure, smart measurement and metering, communication technologies utilized in smart grid, and security issues on smart grid. The present states of each system are summarized and future research directions are presented in several subsections. The first of them, which is the SG and smart energy infrastructure, is considered in terms of power generation, transmission and distribution, and customer utilities. Later, the smart measurement and metering applications are examined by considering energy management and control systems, and reference standards. Hardware and software infrastructures of the smart metering systems that are directly related with communication and security issues are discussed in detail. The wireline and wireless communication systems frequently utilized in the SG are comprehensively investigated. In the last part of the paper, security issue of the smart grids is reviewed in terms of cyber and physical security requirements.

The organization of the paper is as follows. Section 2 describes SG and smart energy infrastructure in terms of power generation subsection, transmission and distribution, and customer utilities. Smart measurement and smart metering systems are presented in Section 3. While Section 4 includes wireline and wireless communication technologies utilized in SG, security issues on SG are comprehensively considered in Section 5. Finally, some concluding remarks are introduced in Section 6.

## 2. Smart grid and smart energy infrastructure

The smart infrastructure system includes smart energy system besides smart communication, and smart information systems. The smart energy system where the bidirectional energy and information flow is supported is constituted of three main sections as generation grid, transmission grid, and distribution grid. The conventional generation grid as its name implies produces the electricity by using centralized power plants of hydraulics, combined heat, nuclear, and fossil fuel based plants. The generated electricity is stepped up to desired values by using transformers, and then supplied to transmission grid where the generated electricity is delivered to distribution grids that are located several kilometers away. The distribution grid includes a number of substations to step down the transmitted voltage to distribution voltage ranges, and down to desired service voltage levels. Therefore, the transmission and distribution systems require several medium/high voltage (MV/HV) and low voltage (LV) transformers in order to construct the transmission and distribution lines where the entire system is named as power grid [1,4,13].

A sample power grid is shown in Fig. 2 where it is originally seen in [14]. While the conventional power grid is intended to generate and distribute the electricity, the SG infrastructure is much more flexible owing to communication features that are illustrated with blue lines in Fig. 2. Besides the communication, SG allows to integration of several DG sources such as RES and microgeneration plants that are usually small power generators ranging from a few kWs to 10 MW and improving the power reliability themselves [1,14]. The smart energy infrastructure and applications of the SG can be discussed in three subsections as power generation, transmission, and distribution referring to Fig. 2.

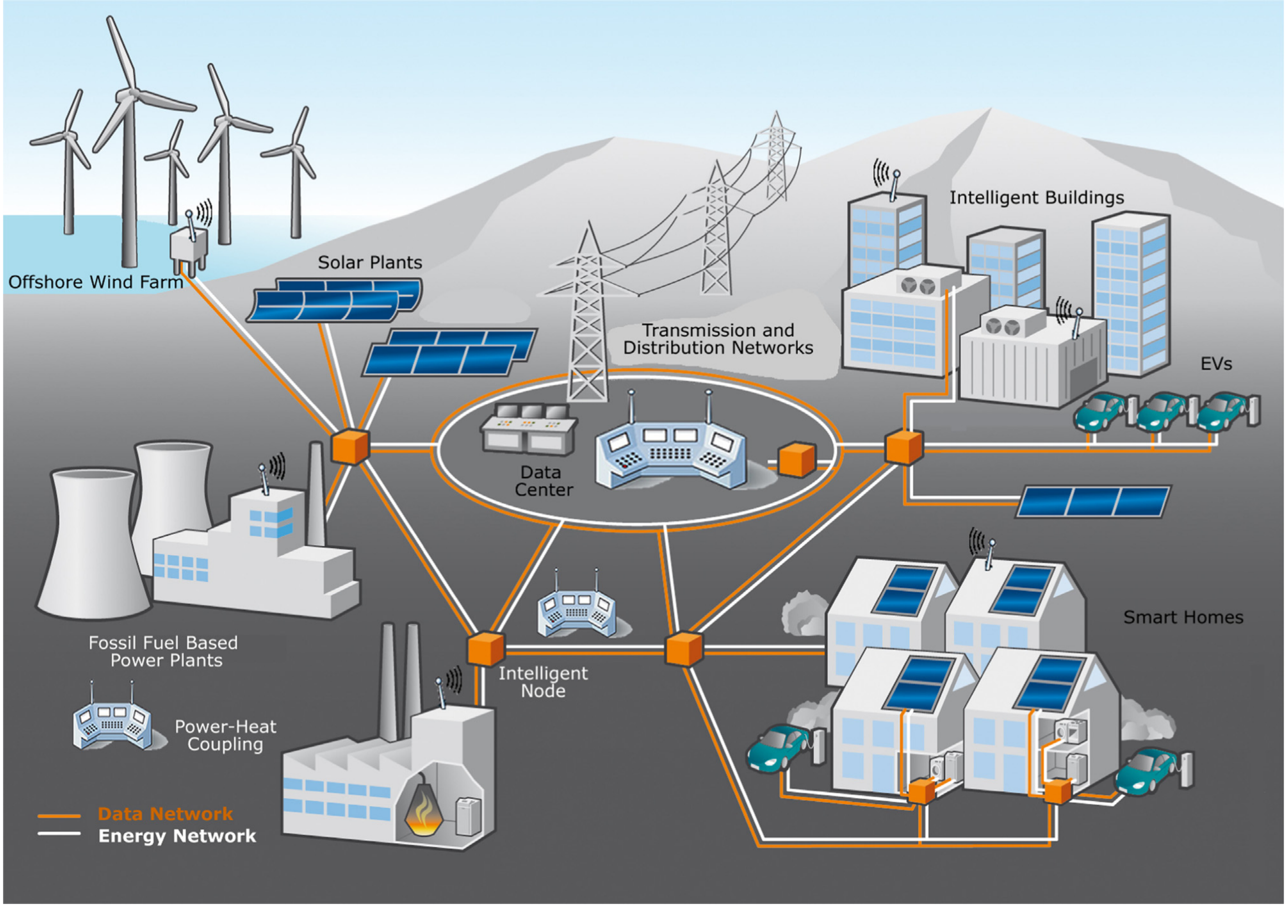


**Fig. 1.** A smart grid perspective with all components [12]. The communication components of a smart grid can include wireline and wireless methods such as power line communication, IEEE 802.15.4 protocol based technologies, and/or agent based control mechanisms.

### 2.1. Power generating subsection

The first improvements in power generation were occurred in the 18th and 19th centuries owing to discovery of cola and petroleum. Although the fossil fuel usage for electricity generation improved our civilization more than two centuries, their destructive effects on the environment and climate are being extensively discussed since a few decades. The increased costs and importing dependencies are other critic issues of conventional power generation process. The most recent approaches related to power generation are promoted by the developments realized in SG term where the DG is the key solution [1,15]. The next generation power grids are requested to be in a flexible, manageable, reliable, and innovative structure owing to information based infrastructures [16]. RES systems meet these aspects by decreasing the energy generation and conversion costs, safe integration to centralized generation plants, efficient storage options including batteries and flywheels, easily implementable communication and networking systems [15]. However, DG implementation requires comprehensive analyses before and after the installation since it involves large deployments achieved from RES such as photovoltaics, wind turbines, fuel cells, and micro-turbines. On the other hand, the generation costs of a unique DG source could be higher than a conventional large-scale power plant [1,15].

Therefore, the smart power generation should be related to demand forecasting and automatic generation control (AGC) to decrease generation costs while meeting the energy demand of consumers and load plants [16–18]. The forecasting methods and horizons that are generated according to involved periods are presented in [16]. The AGC has been used for long years to balance generation and load changes by distributing the required power among generators. The main objective is performed by controlling the system frequency since a small deviation in the system load causes to proportional changes in the frequency [17–20]. The AGC that is also known as secondary frequency control (SFC) ensures to meet the power demand owing to several methods such as area control [18], variable structure, adaptive control, optimal control, and computational methods as fuzzy or neural networks [20].

While the distributed energy resources (DER) promote capabilities of conventional grid, many of them cannot provide sufficient flexibility, efficiency, and controllability itself. The development of DGs requires a large number of DER operating together with a great capacity comparable to regular power generators that is defined with virtual power plant (VPP) concept [21–23]. A VPP can take the place of a conventional power plant owing to its efficiency and easily manageable structure [21]. Besides being a flexible representation of DER, VPP can create a single operation and communication node as an alternative to node-by-node monitoring. Moreover, a DER in the VPP can be connected to various nodes in a distribution network where the overall characteristics can be affected in terms of topology, impedance, and losses [16,22]. The energy management system improved by VPP controls the generation costs and avoids the possible loss of DER.

### 2.2. Transmission and distribution utilities

The future transmission and distribution systems are required to meet the needs of smart grid structure in terms of technical and economic aspects. The smart power generation enables several DER to integrate the entire system at transmission or distribution

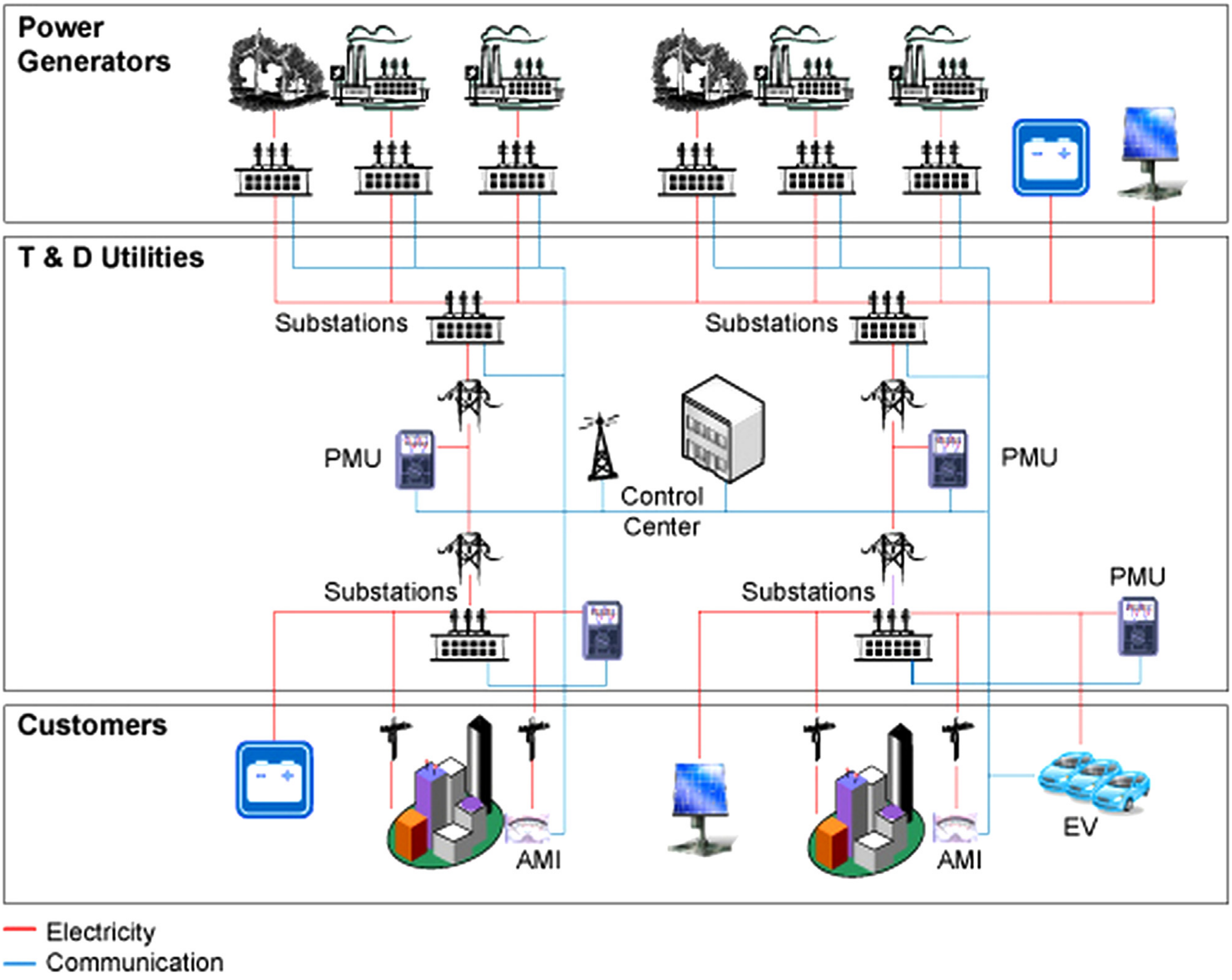


**Fig. 2.** Power generation, control, and measurement diagram across the distribution network and consumers [14].

layers. However, the conventional transmission and distribution systems were not implemented considering DGs where the intermittent profile of RES and DER affect the reliability without any control strategy. The unstable climate changes make RES based DGs quite dependent to the conditions and causes power, voltage, and frequency fluctuations [9,24,25].

Therefore, the transmission and distribution utilities are required to be adapted to ensure power reliability and efficiency against high penetration of DER to the conventional grid. The static VAR compensators are widely used systems in this topic. However, researchers proposed some energy management systems and methods for voltage regulations that are performed with step voltage regulators, and load controllable transformers [24]. In another study [26], reactive power management systems are introduced by referring to autotransformers and their compensating features as a line drop compensator. The agent based control approaches are intended to coordinate the voltage regulators in an efficient way by determining the optimum voltage and power rates [26,27].

The adaptation of current transmission and distribution utilities to the smart grid requirements involve some challenges. First of all, the digitalization should be dealt to convert the transmission grid to a digital platform in order to cope with communication protocols. The digital infrastructure provides increased controllability, flexibility, and data management opportunities. The flexibility enables the transmission utilities for easily adapting to intermittent structures of DER, provides various control strategies for centralized and deployed transmission and distribution, and decreases the ensures the compatibility of several types of communication and measurement systems that are interactively operating [9, 26]. On the other hand, the transmission grid must be capable to monitoring power flow by itself that is known as self-awareness includes voltage, frequency, and stability monitoring. The interactive control and protection mechanism supplied by system improve the security and sustainability of the entire transmission and distribution grid. Another important challenge of conventional transmission grid is sustainability that ensures the controllable growth of smart transmission grid. The sustainability of a smart transmission grid is achieved owing to three main smart system that are smart control centers, smart networks, and smart substations as shown in Fig. 2 [1].

The enhanced measurement, information, and control techniques are required in order to build a smarter and stronger transmission and distribution grid. PMU is one of the state of the art measurement techniques that is widely installed and is rapidly being deployed in increasing numbers. PMUs are intended for monitoring the phasor synchronizations, voltage stability, load sharing, power flows; detecting the faulty lines and islanding requirements, restoring the power systems, and estimating the efficient algorithms to recover lost power [28,29]. The PMU operates by extracting phasor of the line voltage and line current in power systems that all phase components are matched to period. Moreover, PMUs can also predict the frequency of the transmission line and manages the accurate detection of frequency security by rate of change of frequency methods [29–31]. The first application of PMUs started in 1980s in power systems [30]. However, standardizations of PMUs are performed regarding to first original synchro-phasor standard, IEEE Standard 1344-1995 [30], while its latest developments are arranged referring to IEEE Standard C37.118-2005 [29], that plays important role in steady-state characterization of phasor measurements. The updated version of this standard, IEEE C37.118.1-2011, is required to prevent the measurement errors in terms of total vector errors, and frequency errors [31].

The PMU can be a separate device or an operational section within a compact unit such as metering or protection devices. Many power generation and transmission utilities locate PMUs at the critical substations in order to install a dedicated monitoring system, and evaluate the information transmitted to load dispatch centers. A phasor data concentrator gathers the transmitted data at load dispatch centers to process and save the data [30].

### 2.3. *Customer section utilities*

The customer section covers numerous applications in terms of smart energy infrastructures such as microgrid with RES and hydrogen, electric vehicles interacting with grid as vehicle-to-grid (V2G) and grid-to-vehicle (G2V), energy storage systems, and smart home appliances. The individual customers are able to install low voltage generation plants by using fuel cells, CHP sources, RES, and several other DER in the distribution level. The microgrid model includes energy storage systems and loads besides customers' own generation plants [1,13,32,33].

The electrical loads are classified as static loads and electronic loads regarding to the most basic approach. The load models are assumed as residential, official and industrial where the official ones are defined as critical load belonging to military or hospitals that require highly reliable microgrids. Therefore, these loads involve some considerations such as priority management in load sharing, high power quality, and islanding control. The intermittent characteristics of RES are tolerated by battery storages as a backup model. The load/source operation strategy meets the net active and reactive power requirement in grid-connected mode, and stabilization of the voltage and frequency in island mode [33,34]. In addition to these advantages, the microgrid that is located near the load-sites decreases the transmission line losses owing to the distance between generation and consumption cycles. Moreover, the generated energy over the required can be supplied to utility grid regarding to regional regulations of transmission and distribution companies [33,34]. The smart home appliances are one of the most popular components of smart grid owing to their facilitating assistances to daily life. Smart home and microgrid integration is incorporated by energy monitoring devices, sensors that control the air conditioning and illumination, and smart meters that are capable to be remotely controlled for energy efficiency. Moreover, a master controller integrates the entire smart home appliances in a secure and reliable way owing to its wireline and wireless communication abilities [13,33].

The rising fuel costs and environmental legislations promote the usage of EVs, plug-in electric vehicles (PEVs), and plug-in hybrid electric vehicles (PHEVs) all over the world. Although the PEVs and PHEVs have not been widely spread, the EVs have attracted much more attention and usage by individuals, industries, and governments owing to their most effective contributions on reducing the fossil fuel consumptions. The most recent developments on EVs were related to electric machines, batteries, fuel cells, and several other components of a car up to 2000s. However, latest EV researches have been focused on energy exchange of EVs through the grid owing to the development of smart grid [35,36]. The batteries of EVs are not only assumed to provide propulsion but also are considered as an energy storage device that is capable to supply the grid during discharge modes. Besides, PEVs are quite advantageous comparing to PHEVs and internal combustion engine vehicles in terms of grid connection. This opportunity validates a bidirectional operation of EVs that are defined as V2G and G2V during the discharge and charge modes respectively [1,35,37,38].

In the V2G operation mode, EVs supply electrical energy to the grid by using their own energy storage devices such as batteries, fuel cells, or hydrogen tanks. Hence, intelligent charger systems should be used to integrate EVs to the grid while essential discharge and recharge operations were being held during parking periods. The capabilities and requirements of charger cannot be spared from G2V operation of EVs that involves bidirectional power flow for the SG applications [35,38,39].

In [1], a report is cited that remarks a car is driven around one hour a day in US that means cars are mostly parked in the left times. The EVs are classified to three major groups as hybrid or fuel cell vehicles, battery-powered or PHEVs, and solar vehicles that are used in small RES systems. A hybrid EV includes an internal combustion engine besides electric motor and a fuel tank where it generates electricity for its battery. These vehicles serve as DG systems generating electrical energy by using fossil fuels. The EVs are operated by their pure electricity system where there is not any fuel tank or fossil fuel is available, and these vehicles are assumed as distributed energy storage systems on the SG side [1,36]. The V2G operation of an EV requires connection control to grid, SFC, communication among vehicles and grid, instantaneous bidirectional smart metering, charging with frequency regulation, state of charge and battery state of charge controls, autonomous distributed control, and decentralized vehicle control where they are presented in detail [1,35,38,39].

## 3. Smart measurement and metering

The improvement of SG does not only promoted by smart energy infrastructure and power electronics, but also by the high-level information infrastructure, monitoring, measurement, and metering operations that provide a widespread communication substructure. Therefore, it should be noted that the bidirectional flow that the SG relies on is required for communication as well as energy. Hence, the SG is completely constructed with its distributed information systems incorporated to power generation, transmission, distribution, and consumption nodes. The smart measurement requirements such as sensors, networks, and PMUs, while smart metering solutions such as AMI, AMR, and AMM are investigated in this section.

### 3.1. *Smart measurement*

The intermittent structure of DER is widely known and considered in the context of SG applications where the measurement networks should be precisely organized to cope with this issue. Moreover, the interaction of nonlinear loads to the grid, legislations, and reliability issues inspire a vital role to pervasive monitoring and measurement infrastructures. The reliability and sustainability of the SG infrastructure is depended to a widespread management and measurement control that is integrated with the most recent communication systems [40]. The reliability of SG is quite important to prevent the faults causing outages that cost $25B–$180B annually to US economy. A robustly planned measurement system can decrease or prevent the faults and increase the sustainability ratio of the grid. In addition to prevention, measurement systems are essential for fault location in the long distance transmission lines decreasing the outage times and costs [41].

The measurement perspective handles the SG as a power network that is integrated to distributed measurement systems and requires to be operated by several control and protection feasibilities. In [40], a concept named distribution system operator is defined that is responsible of operating, maintaining, and improving the distribution system with its integration through several other systems. This control mechanism requires a distribution management system (DMS) that generates several substructures and control level including measurement, monitoring, and estimation duties [40]. The DMS should also consider the power quality measurements in order to ensure nominal voltage and current characteristics that are delivered to load sites.

On the other hand, the SG viewpoint of measurement side involves energy management system (EMS) with measurement subsystems. The EMS framework is classified into two types as centralized and decentralized where the centralized EMS includes intelligent algorithms and software while the decentralized system uses logical applications widespread on the entire system. The EMS should measure and estimate the active and reactive power supplied by DER, load demand, and overloading condition, losses, voltage drops, and overvoltage occurrences in the active network. However, numerous ambiguity affecting the accuracy and reliability of EMS operation occurs during measurement cycles. Therefore, the data stream with too high inaccuracy causes errors in the operation of EMS that yields unexpected costs [40,42]. The measurement errors may be caused by faults that are classified as permanent and temporary. Although the permanent faults are easily detected by traditional methods, temporary faults causes critical problems since they cannot be rapidly detected and are mostly originated from line-to-ground and line-to-line faults that are caused by physical and environmental effects [41].

It has been referred that the PMU measurements should meet the requirements of IEEE C37.118 standard [29,42]. The requirements that should be taken into account for other SG measurements are also defined by several standards such as IEC61000-4-30 for supply quality, IEEE Std. 1588 for precision time protocol in distributions systems, IEEE Std. 2030-2011 for the smart grid interoperability references. The IEEE 1547 series are defined with IEEE Std. 1547.4 that is for planned islands/micro-grids and IEEE Std. 1547.6 is for interconnection to distribution secondary networks, and the recently initiated P1547.8, which deals with extended use of IEEE Std. 1547. On the other hand, IEEE1588-PTP is available for precision time protocol while IEC 61850 standard series present regulations for communication networks and systems in substations [43–46].

### 3.2. Smart metering

The smart measurement is performed by using an SM that measures the energy consumption of any customer. Therefore, SMs should be capable to detect the energy consumption rates in real-time by capturing the voltage, phase angle, and frequency. A typical smart metering system illustrated in Fig. 3 consists of metering and communication infrastructures. The metering section of an SM includes time-of-use pricing control, data management system, and AMR framework. The communication components of a smart grid may include wireline methods such as power line communication (PLC) or wireless communications. The communication infrastructure should allow bidirectional data flow to enable the SM to acquire data about customer and utility grid [47–49]. Hence, the communication section of an SM includes network connection and control infrastructure that enables the meter to communicate with remote centers and to run the control commands. Besides the two main sections, the modules of an SM includes power supply module, control module, metering module, timing module, communication module, indicating module, encoding module, and timing module [50].

In addition to previously expressed features of SM, the logging module stores the consumer information including energy consumptions, date, power factor and so on. The metering module instantly acquires and measures voltage and current values by isolating the SM from utility grid. The billing module performs to generate electricity bill considering the timestamps, while the timing module provides reference points to this section. Two styles of the most widely used SM are shown in Fig. 4 where they can be programmed either to generate bills just depending to consumed energy from utility grid or billing by considering the contribution of user's DG sources that feeds the utility grid. Furthermore, the SMs can manage the energy demand of customer by limiting the consumption or remotely connecting and disconnecting other supplies [47]. It is believed that SM will hold vital roles in future smart grid application owing to their scalability, real time management, and security features. Access point architecture is also required to communicate with several hundreds of SMs in a region that is implemented similar to cell structures. Hence, the security issues to protect billing data and SMs should be considered [49,51]. There is an extensive interest on remote monitoring of SMs to increase the grid management and metering security. Moreover, the remote monitoring of SMs enables the utility companies to prevent illegal electricity usages that can be detected by statistical data acquired from SMs.

The AMI features of SM enable to manage bidirectional communication that makes the SM capable to operate control commands

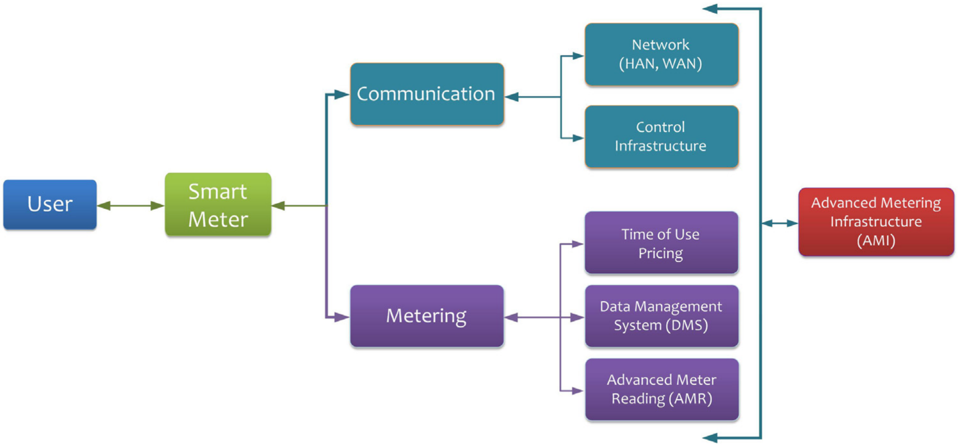


**Fig. 3.** A smart grid perspective with all components.

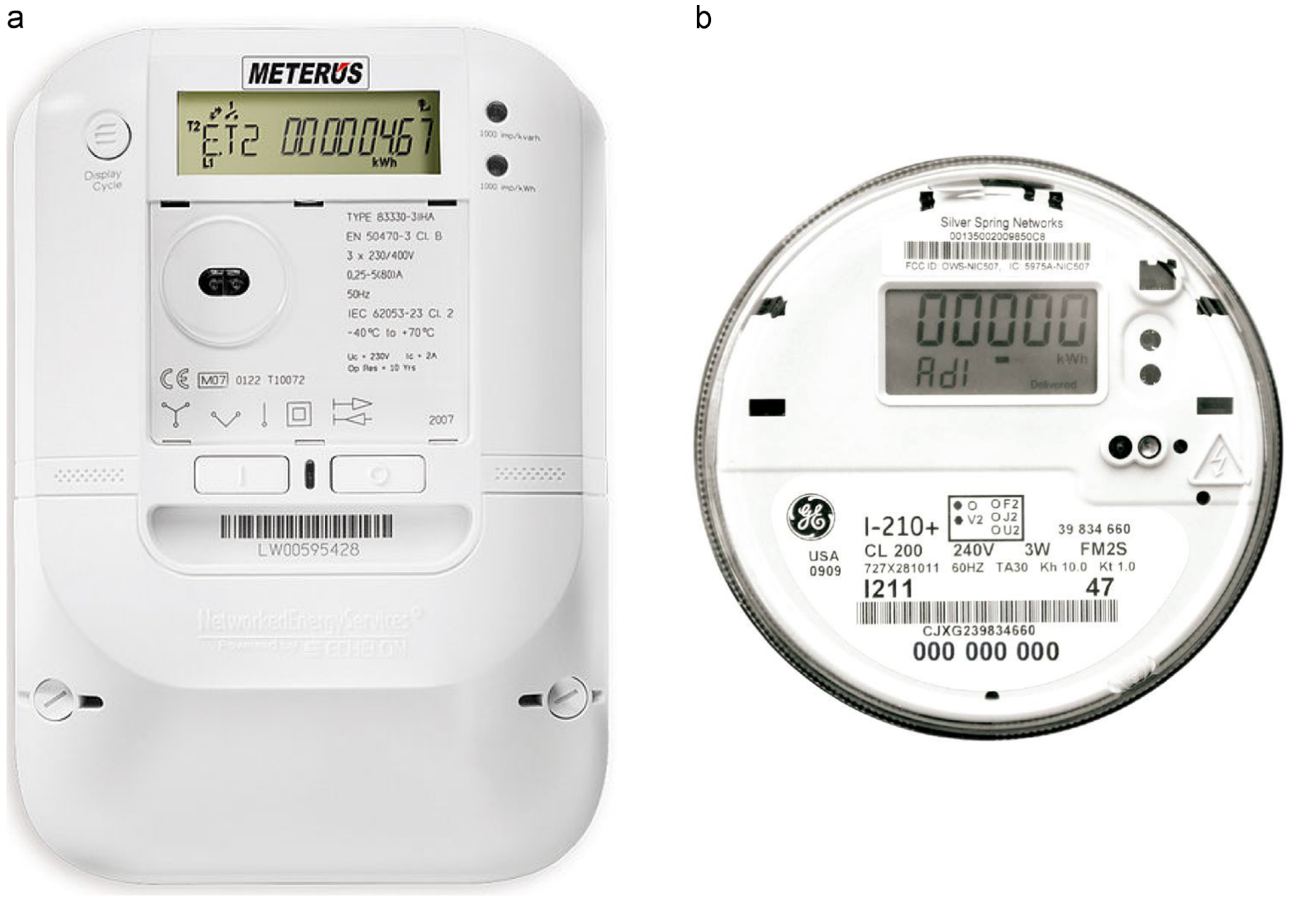


**Fig. 4.** Commercial smart meters (a) SM used by EVB Energie AG that uses two-way communication for SM ability to reduce load, connect/reconnect remotely, and interface to gas and water meters besides its AMR features, (b) high accurate and reliable in a solid-state kWh meter platform package of General Electric.

sent by utility company [52,53]. Against the control opportunity of SMs, they meet with several threats of unauthorized accesses on security, safety, and privacy issues. The unauthorized accesses and attacks make smart grid vulnerable against malicious applications. Numerous scenarios, protection researches, and cyber warfare practices are extensively investigated to prevent SMs to pose new risks in smart grids [54–58]. In addition to the security issues, unauthorized access to SM can cause to manipulations and billing losses. The SMs require refusing all these malicious accesses by using trusted software. This requirement is defined with secure signal processing (SSP) term [54] that protects the sensitive data by encrypting algorithms and properly addressing the SM security faults. The most recent researches propose privacy-preserving billing and secure data acquiring in smart grids [59–64]. The SSP is one of these powerful communication mechanisms that are based on preventing the unauthorized access to private data. The security mechanism is based on encryption that provides to process data in cryptographic forms instead of plain texts [59,60].

Some valuable studies about privacy of SM and secure billing are presented in the literature [60,62]. Smart metering meets several privacy interests from media, data experts, and consumers [60]. The privacy is related to various aspects such as measurement, transfer, and storing between the meters and operating service. In case of adequate privacy cannot equipped, anyone can intrude the system and obtain or change any stored data. This intrusion may cause to the undesired controls like abuses of heaters, coolers, and other households. Danezis et. al. [61] proposed a method called differential privacy to increase the security of SMs by hiding special data. The proposed method is based on simplifying the regular differential privacy protocol, and depends on fixed size databases for a fixed term billing period. The experimental study is tested by adding several defective data to the stored measurements, and correctness of the billed consumption is examined [61].

There are several studies performed to increase the security of SMs [62–64]. Rial et al [62] improved a privacy-preserving protocol that is based on user agents that comprises a secure communication channel in a wide area network. In the proposed study, there is not any additional channel requirement while the secure communication is installed. The agent and private key based security issues are intensively studied in order to improve the privacy-preserving methods for SMs [63,64].

## 4. Communication technologies used in smart grid

One of the most important achievements in smart grid is AMI system that is used to measure, acquire, and analyze the data about energy consumption and power quality of each consumer. Any SM with AMI infrastructure involves communication facility with metering devices on demand [56]. The bidirectional communication is performed between utility supplier and consumer to improve maintenance, demand management, and planning capability of supplier.

Fig. 5 illustrates a block diagram of wireline and wireless communication architecture used in smart grid. The data management is one of the quite important tasks in smart grid due to vital role of measured billing data. The central section of Fig. 5 is constituted by a metering data management system (MDMS) that performs data storage and processing tasks. The components of a

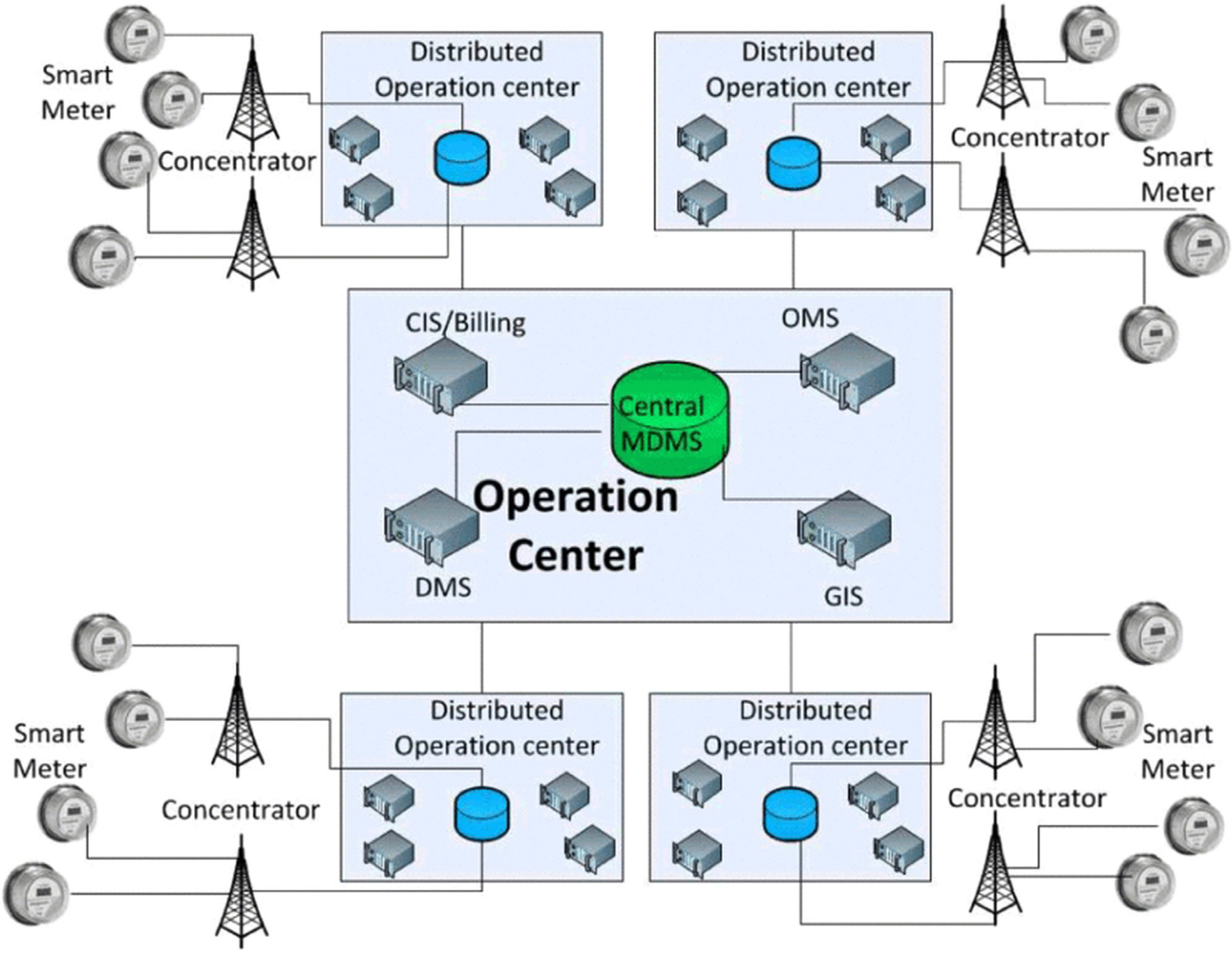


**Fig. 5.** A distributed communication and management architecture in smart grid [56].

MDMS are outage management system (OMS), geographic information system (GIS), consumer information systems (CIS), and DMS where each system are dedicated to cooperate the communication and management systems together [56].

The OMS system requires acquiring data when the power quality or related indicators are extraordinary for a customer. The regular measurements obtained at high frequencies are not related to operation features of the OMS and they are filtered at signal processing stages. This subsystem enables MDMS to detect any abnormal situation to interfere immediately. The GIS and CIS systems are required to collect data such as utility location, consumption rates, and billing information about SM and consumer. The DMS can be handled as a supervisor in the entire structure where it is in charge to observe power quality and load demand rates for management and forecasting. The central operation center can be extended to several distributed operation centers that are planned in the same MDMS structure [56].

The communication between operation center and SM can be applied in several protocols by using two ways such as wireline and/or wireless. The wireline communication is done by using transmission lines and widely known method is the PLC. The key idea is based on using the transmission and distribution lines as the communication medium where any additional communication channel requirement is tackled by this way. Although the losses of aged electrical lines are the most important handicap in this method, the transmission channel decrease total installing costs by eliminating additional system requirements [10,51]. On the other hand, PLC applications provide data transmission rates up to 200 Mbps for a single-phase system. It is also possible to use several wireless communication methods based on IEEE 802.22 protocol wireless regional area network (WRAN) or IEEE 802.15.4 protocol that is wireless personal area network (WPAN). There are numerous wireless smart grid studies that some of them are presented in the following section can be found in the literature [65–71]. The digital communication methods are substantially used to improve wireless networks including ZigBee, Wi-Fi, and Bluetooth to tackle the lack of PLC at higher frequency applications.

The communication architecture of the smart grid is defined by IEEE 2030-2011 standard that is important to understand applications and infrastructures at a hierarchical arrangement [70]. The standard is intended to create a consensus on the numerous confusing descriptions by clearly indicating a logical structure for the smart grid networks including of three sub-networks. The first network related to customer properties is called private networks including HAN, industrial area network (IAN) and building area network (BAN). The second network located at distribution layer is called WAN comprising neighborhood area network (NAN) and field area network (FAN). These networks are equipped with several control and monitoring systems such as remote terminal units, AMIs, and PMUs to manage out the various functions [69,70]. The last network type described by the standard is core network for the utility sections such as generation and transmission layers. The core network includes broadband communication architectures such as local area network (LAN), virtual private network (VPN), voice over internet protocol (VoIP), and GIS [71–75]. The communication technologies of smart grid are described

**Table 1**
Comprehensive list of communication technologies used in the smart grid.

| Tech. | Standards | Data rate | Distance | Network | Advantage | Disadvantage |
|---|---|---|---|---|---|---|
| **Wireline technologies** | | | | | | |
| **PLC** | • NB-PLC: ISO/IEC 14908-3,14543-3-5, CEA-600.31, IEC61334-3-1, IEC 61334-5 (FSK)<br>• BB-PLC: TIA-1113 (HomePlug 1.0), IEEE 1901, ITU-T G.hn (G.9960/G.9961)<br>• BB-PLC: HomePlug AV/Ext., PHY, HD-PLC | • NB-PLC: 1–10 kbps for low data rate PHYs, 10–500 kbps for high data-rate PHYs<br>• BB-PLC: 1–10 Mbps (up to 200 Mbps on very short distance) | • NB-PLC: 150 km or more<br>• BB-PLC: about 1.5 km | • NB-PLC: NAN, FAN, WAN, large scale<br>• BB-PLC: HAN, BAN, IAN, small scale AMI | • Already constructed wide communication infrastructure<br>• Physical disconnection opportunity according to other networks<br>• Lower operation and maintenance costs | • Higher signal losses and channel interference<br>• Disruptive effects caused by appliances and other electromagnetic interferences<br>• Hard to transmit higher bit rates<br>• Complex routing |
| **Fiber optic** | • AON (IEEE 802.3ah)<br>• BPON (ITU-T G.983)<br>• GPON (ITU-T G.984)<br>• EPON (IEEE 802.3ah) | • AON:100 Mbps up/down<br>• BPON:155–622 Mbps<br>• GPON: 155–2448 Mbps up, 1.244–2.448 Gbps down<br>• EPON: 1 Gpbs | • AON: up to 10 km<br>• BPON: up to 20–60 km<br>• EPON: up to 20 km | • WAN | • Long-distance communications<br>• Ultra-high bandwidth<br>• Robustness against electromagnetic and radio interference | • Higher installing costs (PONs are lower than AONs<br>• High cost of terminal equipment<br>• Not suitable for upgrading and metering applications |
| **DSL** | • ITU G.991.1 (HDSL)<br>• ITU G.992.1 (ADSL), ITU G.992.3 (ADSL2), ITU G.992.5 (ADSL2+)<br>• ITU G.993.1 (VDSL), ITU G.993.1 (VDSL2) | • ADSL: 8 Mbps down/1.3 Mbps up<br>• ADSL2: 12 Mbps down/3.5 Mbps up<br>• ADSL2+: 24 Mbps down/3.3 Mbps up<br>• VDSL: 52–85 Mbps down/16–85 Mbps up<br>• VDSL2: up to 200 Mbps down/up | • ADSL: up to 5 km<br>• ADSL2: up to 7 km<br>• ADSL2+: up to 7 km<br>• VDSL: up to 1.2 km<br>• VDSL2: 300 m–1.5 km | • AMI, NAN, FAN | • Already constructed wide communication infrastructure<br>• Most widely distributed broadband | • Communication operators can charge utilities high prices to use their networks<br>• Not suitable for network backhaul<br>(long distances) |
| **Wireless technologies** | | | | | | |
| **WPAN** | • IEEE 802.15.4<br>• ZigBee, ZigBee Pro, ISA 100.11a (IEEE 802.15.4) | • IEEE 802.15.4: 256 kbps | • ZigBee: Up to 100 m<br>• ZigBee Pro: Up to 1600 m | • HAN, BAN, IAN, NAN, FAN, AMI | • Very low power consumption, low cost deployment<br>• Fully compatible with IPv6-based networks | • Low bandwidth<br>• Limitations to build large networks |
| **Wi-Fi** | • IEEE 802.11e<br>• IEEE 802.11n<br>• IEEE 802.11s<br>• IEEE 802.11p (WAVE) | • IEEE 802.11e/s: up to 54 Mbps<br>• IEEE 802.11n: up to 600 Mbps | • IEEE 802.11e/s/n: up to 300 m<br>• IEEE 802.11p: up to 1 km | • HAN, BAN, IAN, NAN, FAN, AMI | • Low-cost network deployments<br>• Cheaper equipment<br>• High flexibility, suitable for different use cases | • High interference spectrum<br>• Too high power consumption for many smart grid devices<br>• Simple QoS support |
| **WiMAX** | • IEEE 802.16 (fixed and mobile broadband wireless access)<br>• IEEE 802.16j (multi-hop relay)<br>• IEEE 802.16 m (air interface) | • 802.16: 128 Mbps down/28 Mbps up<br>• 802.16 m: 100 Mbps for mobile, 1 Gbps for fixed users | • IEEE 802.16: 0–10 km<br>• IEEE 802.16 m: 0–5 (opt.), 5–30 acceptable, 30–100 km low | • NAN, FAN, WAN, AMI | • Supports huge groups of simultaneous users, longer distances than Wi-Fi<br>• A connection-oriented control of the channel bandwidth<br>• More sophisticated QoS than 802.11e. | • Complex network management is<br>• High cost of terminal equipment<br>• Licensed spectrum requirement |
| **GSM** | • 2G TDM, IS95<br>• 2.5G HSCSD, GPRS<br>• 3G UMTS (HSPA, HSPA+)<br>• 3.5G HSPA, CDMA EVDO<br>• 4G LTE, LTE-Advanced | • 2G: 14.4 kbps<br>• 2.5G: 144 kbps<br>• HSPA: 14.4 Mbps down/5.75 Mbps up<br>• HSPA+: 84 Mbps down/22 Mbps up<br>• LTE: 326 Mbps down/86 Mbps up<br>• LTE-Advanced: 1 Gbps /500 Mbps | • HSPA+: 0–5 km<br>• LTE-Advanced: optimum 0–5 km, acceptable 5–30, 30–100 km (reduced performance) | • HAN, BAN, IAN, NAN, FAN, AMI | • Supports millions of devices<br>• Low power consumption of terminal equipment<br>• High flexibility, suitable for different use cases,<br>• Open industry standards | • High prices to use service provider networks<br>• Increased costs since the licensed spectrum |
| **Satellite** | • LEO: Iridium, Globalstar,<br>• MEO: New ICO<br>• GEO: Inmarsat, BGAN, Swift, MPDS | • Iridium: 2.4–28 kbps<br>• Inmarsat-B: 9.6 up to 128 kbps<br>• BGAN: up to 1 Mbps | • 100–6000 km | • WAN, AMI | • Long distance<br>• Highly reliable | • High cost of terminal equipment<br>• High latency |

regarding to bandwidth features as narrowband and broadband. The following sections are dedicated to introduce these technologies in summary.

### 4.1. Wireline communication technologies

The wireline communication that is mostly preferred by service suppliers is used to perform data communication over power lines as its name implies [66,69,71]. The most important advantage of the wireline communication is reliability and insensitivity to interference. Although the PLC is most widely used wireline communication technology, others including fiber optic and digital subscriber line (DSL) are widely used over telephone lines. The digital communication methods can support high-speed data transmission between 10 Mbps and 10 Gbps in DSL medium, or between 155 Mbps and 160 Gbps in coaxial and fiber optic cables [66,71,76].

The PLC faces several technical challenges owing to unexpected propagation characteristics of transmission and distribution lines. These disruptive effects and interferences are usually concentrated at electromagnetic environments such as transformers [71,77,78]. Although there are numerous methods implemented in order to eliminate disruptive effects of wireline, there are two major PLC technologies operate in different bandwidths [71] that are narrowband PLC (NB-PLC) and broadband PLC (BB-PLC). The NB infrastructure was proposed for the transmissions ranging from few bps to a few kbps at its very early stages. The resulting bandwidths are later scaled from 1 bps to 10 kbps and up to 500 kbps precisely that operate at 500 kHz transmission frequencies. The NB-PLC can be used in both low voltage and high voltage lines that may cover up to 150 km or more transmission length. Another PLC infrastructure, BB-PLC, operates at significantly higher bandwidth up to 200 Mbps and higher frequency bands from 2 MHz to 30 MHz [71,73]. The success of NB-PLC promoted the progress of BB-PLC that is especially intended to be used for internet service and HAN applications. In 1997, the primary internet applications that are focused on internet access and service providing over PLC were seen in Europe. However, the results were upsetting the PLC based internet access idea. Hence, the interest is shifted to industrial communication and home applications in the early 2000s that is accelerated by several industry alliances such as the HomePlug Powerline Alliance (HomePlug), Universal Powerline Association (UPA), High Definition PLC (HD-PLC) Alliance, and The HomeGrid Forum [73]. In the last decade, there are several standardizations are described to arrange the implementations such as TIA-1113, ITU-T G.hn, IEEE 1901 FFT-OFDM, and IEEE 1901 Wavelet-OFDM [73,78–80]. Although the several products that enable to operate at physical layer (PHY) bandwidths of 14 Mbps (HomePlug 1.0), then 85 Mbps (HomePlug Turbo), and then 200 Mbps (HomePlug AV, HD-PLC, UPA) are improved, none of them are capable of working together. On the other hand, the BB-PLC that can be said the complementary of Wi-Fi at home networking has not yet capable to obtain considerable market share [73]. Other wireline communication systems besides the PLC are comprised of optical methods and DSL communications that provide higher data rates comparing to the PLC. The major advantages of optical communication are its capability of transmitting data packets of Gbps to several kilometers, and its strength against electromagnetic interference [71,73]. These features make it suitable for high voltage lines. Furthermore, a special cable type known as optical power ground wire allows to transmission of high data rates to long distances.

An another wireline communication technology used in smart grid is DSL that enables digital data transmission by using telephone lines. Hence, this infrastructure prevents additional setup cost for communication medium since the electric utilities are connected to control centers. The types of DSL technologies are Asymmetric DSL (ADSL) that provides 8 Mbps downstream of data, ADSL2+ with a maximum downstream of 24 Mbps, and Very-high bit rate DSL (VDSL or VHDSL) up to 52 Mbps downstream data transmission over copper wires [71]. The standards, data rates, advantages and disadvantages of wireline and wireless communication technologies are shown in Table 1.

### 4.2. Wireless communication technologies

National institute of standards and technology (NIST) has been proposed the wireless technologies as important networks to be utilized for SG. The demand management that is the key feature to provide efficiency and reliability of SG is based on selecting the most proper communication technologies to expedite the management. The main criteria to select the accurate technology are related to economic and technological feasibilities [81–83]. The wireless communication networks are one of the most extensively researched topics in power systems involved in SG concept. Although the wireless networks brought several advantages in terms of installation and coverage, the essential lacking is their sensitivity to limited bandwidth and interference [81].

The wireless network is comprised of hierarchical mesh networks using wireless LANs to interact with electrical devices. The most suitable AMI infrastructures are NANs and HANs for wireless deployment owing to their low cost installations [81,82]. The internet based communication infrastructures and data management points (DMPs) can be installed either wireline or wireless where the communication between NANs and DMPs can cover a range of kilometers. Any DMP can connect and manage hundreds of SMs where a wide coverage area can be installed with mesh networking or relaying the DMPs. The innovative studies in SG applications are rely on highly scalable and wide spreading communication networks that can be easily constituted by using wireless sensor networks (WSNs). Furthermore, the WSNs should provide a reliable infrastructure by decreasing the latency against demand requirements [82,83]. The latency requirements of OpenSG is less than 1 s for NANs that is more eased comparing to the commercial broadband communication. HANs that are constituted to perform energy management and demand planning involve a smaller coverage area comparing to NANs. HANs usually allows to latency less than 5 s that is also quite facilitated comparing to NANs [82].

The outstanding communication technologies used in NANs are based on worldwide interoperability for microwave access (WiMAX), universal mobile telecommunications system (UMTS)/ Long-term evolution (LTE), and IEEE 802.22 standards. Besides these, IEEE 802.11and IEEE 802.15 based Wi-Fi and WPAN technologies are also used in wireless SGs. The WiMAX, which is an execution of IEEE 802.16 standard for metropolitan area networks (MANs) is the principal technology to provide connectivity between DMPs and SMs. WiMAX uses orthogonal frequency division multiple access (OFDMA) that is the multi-user adaptation of regular OFDM digital modulation scheme. The multi-user structure is obtained in OFDMA by arranging the subsets of several subcarriers to unique consumers that allow simultaneous data transmission from a huge group of consumer in low data rates [82,84–86]. The subcarrier based multi-user structure of WiMAX prevents interference among the consumer data and increases the spectral efficiency of the entire system. Although the WiMAX structure is not much complicated comparing to cellular standards, it is not widely adopted as a wireless platform in SG applications. However, this situation does not limit its chance against rival platforms owing to its DMP interactions [82].

The IEEE 802.15.4 standard namely WPAN is the reference that defines the PHY layer for low data rate, low power consumption,

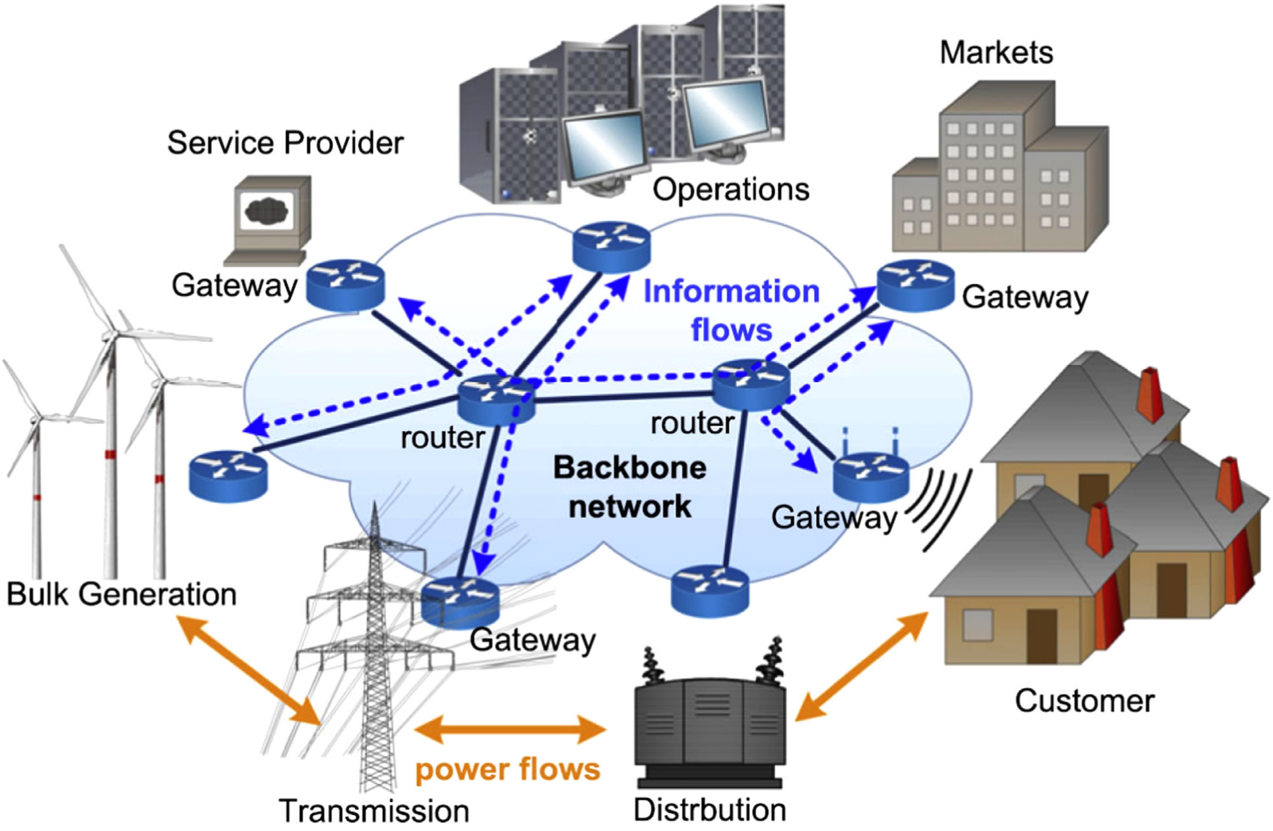


**Fig. 6.** A representation of backbone and local area network structure in smart grid [91].

and low-cost network. The basic PHY layer of WPAN provides 256 kbps data rate in the coverage area starting from 10 m to 1600 m in the star topology for single-hop, cluster-tree, and mesh topology for multi-hops. The PAN coordinator that manages the whole network is located in each type of topology. Furthermore, mesh and tree topologies include additional router nodes to interact between coordinator and devices to construct multi-hop connections. Several industrial standards are based on IEEE 802.15.4 standard to perform monitoring and control applications. The most widely known standards in this classification are ISA 100.11a, Wireless-HART, and the ZigBee that is the most outstanding one among others since they are used in industrial control processes. However, ZigBee is widely adopted in both industrial and commercial applications owing to its extended network management capabilities [71,82].

The cellular technologies such as UMTS and LTE that are based on Global System for Mobile Communications (GSM) provide several options for NAN coverage. The main advantage of GSM based technologies is larger coverage areas comparing other wireless networks. The evaluation of cellular networks is quite rapid and novel technologies support broader data bands. The UMTS that is the most widely known standard of 3G technology provides data communication up to 168 Mbps in the downlink and up to 22 Mbps in the uplink. The most recent cellular technology is 4G that is based on LTE and LTE Advanced standards improving the capabilities of UMTS.

It provides increased bandwidth and spectrum band, facilitated interaction among different networks, better network support that are ranging from macro-cells to femto-cells, and more improved mobile networking capabilities. Although the satellites allow wireless communication with variable bandwidth and latencies, it is a quite expensive technology itself.

The satellites are located at orbits known as low earth orbits (LEO), medium earth orbit (MEO), and geostationary earth orbits (GEO) to provide communication of networks that are installed in rural or large spanned locations where they are out of cellular coverage. It is expected that the decreased costs of smaller satellite stations can be a chance to integrate this technology to SG applications and AMI networks [71,82]. Wireless multimedia sensor and actor network that is introduced in [84] is intended to transmit image and voice data of several information about physical structure such as temperature, humidity, and similar telemetric data.

A novel wireless technology that is assumed to cope with inadequate spectrum is cognitive radio (CR). Users in smart grid are defined as primary and secondary in CR applications that allow dedicating the communication channel to any user, which requires at the exact time [87]. Since the CR can alleviate the licensed spectrum requirement, this issue created the most significant attention that is drawn to this technology. On the other hand, CR promoted the high radio bandwidths that are required to deliver large amount of multimedia data including monitoring and power control units [88]. The traffic management and security issues of SG are being extensively studied regarding to wireline and wireless networks. The cyber security threats of communication systems are analyzed into four types that are related to availability, protection, integrity, and authenticity [89,90]. The security concepts considered in SG applications are introduced in the following sections.

## 5. Security on smart grid

The SG framework that is planned to completely integrate to millions of high-speed, bidirectional information devices in order to establish an interactive energy metering, and management operations. A representation of backbone and LAN structure of SG is illustrated in Fig. 6. The power equipments are intended to manage demand responses, AMI, and AMR processes. Such a critical system requires a precisely established protection system against all possible threats and vulnerabilities of the system should be prevented accurately. However, the SG is vulnerable against several security risks since it is visualized to fully integrate to millions of power devices. This fact increases the awareness of reliable and secure operation requirements. There are numerous studies are performed to determine the security issues for improving the cyber resistance of SG in terms of requirements [91–97], cyber physical security operations [98–102], and precaution methods based on security agents, protocols and algorithms [103–109].

The outstanding high-level SG security objectives are listed as accessibility, integrity and privacy that require well-operated identification, authentication, and access control at physical level. Furthermore, NIST defines two additional security issues as cyber security and physical security. The cyber security issues are listed to sustain the privacy and protection of information and communication systems at the software level. On the other hand, the security of the other components of SG that are comprised of physical devices, smart meters, and power systems is ensured by physical security requirements [91]. The communication protocols that are located at the higher application levels should also be secure and efficient. Public key infrastructure (PKI) technologies are proposed to meet security requirements in terms of identification and authentication. Hence, users or power devices can authenticate each other by using digital certificates that enables its owner to encrypt and decrypt messaging [92,108]. The communication backbone includes wireline and wireless communication methods that are introduced in the previous section. The infrastructure is managed by gateways in LANs and by the routers in higher bandwidth requiring networks. The verified supervisory control and data acquisition (SCADA), as a PLC method, is widely used for management and monitoring applications of conventional transmission and distribution lines while the wireless methods such as ZigBee, Wi-Fi, GPRS, and GSM technologies are widely used for remote control and metering applications of consumer plants. The LAN is constituted by ad-hoc network of wireline and wireless communication technologies including sensor networks [91,96–99]. Some studies are especially focused on physical layer attacks that are most widely seen vulnerability issue of entire SG system [93–95]. Nordell reports that the communication protocols used in SG are same with the layered open systems interconnection (OSI) model where the lower three layers (physical, data link, and network) are complex and insecure comparing to upper four layers [94]. The denial-of-service (DoS) attacks are assumed as the malicious attacks against availability of SG. The main targets of DoS attacks are to delay, to block or to create interruption to make network unavailable by sending fake requests to servers and network. Maybe not all parts of SG but some uses IP-based communication protocols that are vulnerable to DoS attacks against TCP/IP protocols where it is widely studies [97–104].

The potential threats that are directed to SG are illustrated in Fig. 7 where they can be connection-based and device-based. The

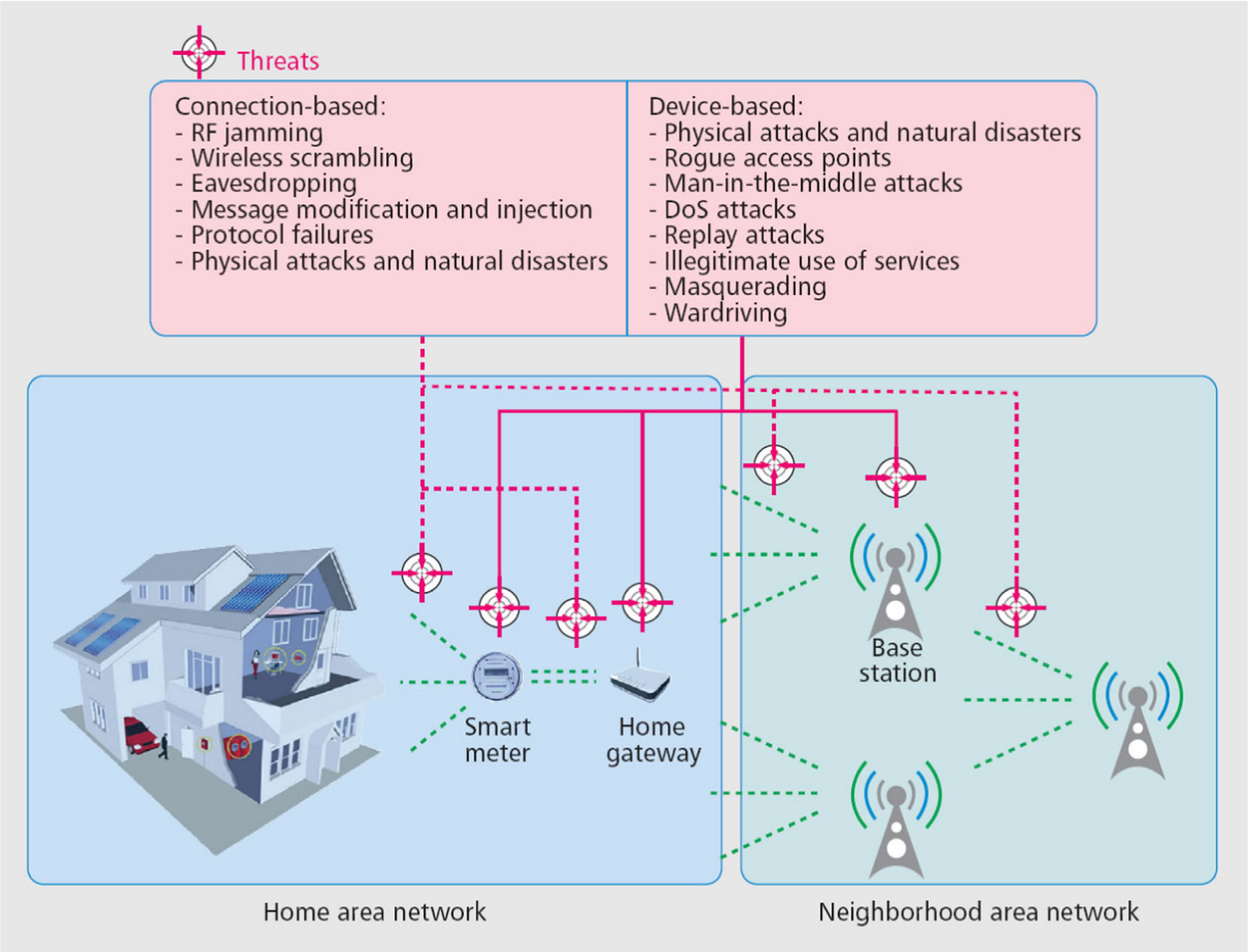


**Fig. 7.** Smart grid deployment and potential threats [98].

sensor networks based on distributed mesh topology provide SG communication infrastructures such as HANs and NANs with cost efficiency. However, the multi-hop mesh networks are more exposed to cyber attacks comparing to single-hop networks. Therefore, an important security issue in wireless SG applications is related to WSNs [105–107]. The security in a mesh network requires high capability to protect the message integrity against cyber attacks to guarantee the confidentiality and authenticity of the data transmissions. In order to manage security protocols, the IEEE 802.11s standard is released for IEEE 802.11 WLAN networks. This standard defines a default security protocol named simultaneous authentication of equals (SAE) that is based on a single password protection on all nodes. Since the unique password application makes the network vulnerable to attacks, efficient mesh security association is improved as an alternative method to SAE [105]. Although the cyber attack risk always exists for SG, there are numerous approaches are being improved and protection methods are being extensively studied. The cyber security requirements and physical security requirements are discussed in detail in the following subsections in order to provide further understanding.

### 5.1. *Cyber security requirements*

The industrial control systems are assumed as preliminary applications of SG owing to their network based hardware frameworks. Several cyber attacks disrupting and destroying the regular operations of the targeted systems are occurred in the last few years. Idaho National Laboratory performed an experimental study in 2007 to destroy the control mechanism of a diesel generator that was being operated remotely. In another event, it is believed that the Russian army destroyed the utility grid of Georgia by the cyber attacks during the Russian–Georgian war in 2008. According to a report of Wall Street Journal, cyber attacks are targeted the US grid and located numerous spies to the system for destroying the infrastructure. Certainly, the most significant and most famous attack was named Stuxnet that targeted programmable logic controllers of Siemens that is widely used in industrial control and communication systems such as SCADA. The operating system of controller was running on Windows, and Stuxnet exploited four different zero-day vulnerabilities resulting to destroy 60% of Iranian nuclear plant that is targeted [98–100]. These significant attacks prove that the cyber security of the SG plays a vital role in any case, and should be accurately taken into account.

The cyber security requirements are firstly related to awareness of the threat. Accordingly, the attacks should be detected and immediate resistance should be performed against the attack. However, since the SG that is deployed large areas with millions of nodes is almost an open communication network that makes impossible to secure each node against attacks. The communication network is required to test and compare the changes of the data stream, should regularly track the network traffic to detect abnormal activities occurred during the attacks [91–94]. The DoS attacks aim to exploit resources by sending unlimited fake requests to the system. Another type of DoS attacks, the distributed DoS attacks, is executed by using distributed resources such as SMs, power devices, and appliances. The smart meter attacks may cause to loss of pricing data that is critical to serious economic implications. Therefore, the integrity of billing information, meter data, commands, and running software is quite important. Although the integrity destruction of software is limited on income losses, it is a critical issue since intrusions or malwares can handle the control of any device, grid, and appliance [98–100]. Privacy of the measurements is required to ensure the identification and access control to prevent unauthorized accesses to devices. The uncontrolled intrusions threat the security of the resources, while personal security becomes vulnerable due to acquired usage information. The privacy is provided by using cryptographic functions on the entire grid to encrypt and decrypt data [91,98,99].

The PKI technologies are considered to meet attack detection, prevention, and privacy requirements owing to their interaction with trusted softwares. PKI includes several policies and procedures to identify customers depending to its digital certification framework that defines management, configuration, and operation strategies. The authorization process is performed by connecting data of registration authority and verification data called the certificate authority. The PKI certificate should be controlled and verified at each cycle referring to signing requests. Although the PKI technologies are thought quite complex, the main application includes four elements in a smart grid that are PKI standard, automated trust security, certificate, and PKI tools [92,95,96].

Besides the certificate applications such as PKI, the security can be achieved by using various communication protocols that enables efficient and reliable data stream on the grid. On the other hand, it is important to ensure real time performance and operations of the SG depending to the selected communication method. Including quite complex communication algorithms to the transmission and distribution infrastructure can cause to decrease the performance and increase the unexpected vulnerability issues [97]. Therefore, the trade-off between security and performance should ever be considered.

### 5.2. *Physical security requirements*

The most important physical equipments of SG are the SM and the PMU that consist of the sensor nodes. The SMs that are simply electrical meters are operated with bidirectional communication technologies to transmit consumption rates and pricing data in real time. On the other hand, PMUs are intended to measure the power quality of any system, and communication technologies are usually based on wireless equipments. The MDMSs communicates with sensor nodes and control centers through the measurement and control networks to analyze the actual data and make decisions.

Therefore, entire system is controlled even in the physical layer applications, and the security requirements as awareness, attack detection, prevention and privacy are met by this way. The SM gathers the instant consumption data and unauthorized intrusions are determined by the methods of AMI. One of the most important acquisitions of SMs is preventing the illegal usage that is especially seen in underdeveloped countries. An interesting subject of illegal electricity usage is noted in [110] referring to an electric service provider from Canada that is related to marijuana growing that is told that requires high amount of energy. Whatever causes to this, the framework including SM and AMI significantly prevents the illegal electricity usage. The framework notices the control center during the physical tampering, and the operation of SM can be locked remotely. On the other hand, other unauthorized access intrusions are immediately refused and are logged in the database of consumer. Electricity service supplier can monitor the modified consumer data at any time and can generate and save reports about the usage characteristic of SM [110–112].

The PMUs are utilized to measure the power flow direction and amount regarding to phasor measurements that are based on the amplitude and phase angle of voltage, current, and frequency. The higher phase angle of the first node means that the power is flowing form first node to second node that has lower phase angle. The magnitude of phase difference is depended to the amount of power flow from source to load where it can disrupt the stability of grid if it exceeds the permitted limits. Therefore, phasor measurement plays vital role to sustain the stability of power grid. The PMU includes timestamp and synchronized phasor measurements since the time synchronization of phasor nodes is required to analyze or monitor the grid at an exact time. Accordingly, the syncro-phasors that are synchronized by global positioning system (GPS) are used. Comparing to SCADA, PMUs perform more certain measurements owing to their sampling capacity that is increased up 60 measurements per second. The synchronization of measurements is considerably significant to pursue the real time control operations of power grid, and system planning. Furthermore, the syncro-phasor measurements allow to prevent illegal electricity usages particularly in large areas where the GPS assistance enables to detect the exact node [111].

Several additional precautions can be taken by assisting the SMs and PMUs in order to increase the physical security. The most recent ones of additional applications are performed with network synchronization supporting the periodical controls of SM. The additional equipment requirements include multi-hop networks using mesh topologies, and multiple link layers. These both requirement are based on multilayer authentication, and adapting the multiprotocol framework to advanced meters [113]. In this context, a sample application that proposes a secure smart-metering protocol (SSMP) is performed in [114] where it is designed for PLC applications. The procedures of SSMP targets four topics as generation of key materials and service supplying to the devices, authentication by using keys, secure communication between nodes, and withdrawing the management of disconnected devices. The protocol is based on several cryptosystems such as PKI, digital certificates, authentication keys, and share keys on the PLC network. In its proposed state, the protocol seems capable to prevent unauthorized accesses, DoS attacks, sustaining the privacy on a PLC network [114]. Since PLC does not require a dedicated communication infrastructure, it can be easily constructed and allows to connectivity. Moreover, it can be connected to several wireline and wireless networks through the backbone network.

## 6. Conclusion

This survey is comprehensively focused on smart metering and smart grid communication methods by considering the related technologies, applications, and challenges. Therefore, the survey is organized in four main sections that are SG and smart energy infrastructure, smart measurement and metering, communication technologies used in smart grid, and security on smart grid. The actual situations of each system are outlined and future research directions are introduced in several subsections. Moreover, the most recent topics such as microgrid, electric vehicles, and DG integrations are surveyed in terms of SG interactions. The SG and smart energy infrastructure is introduced in three aspects of the entire system that they are power generation, transmission and distribution, and customer utilities. The smart measurement and metering applications are surveyed referring to energy management and control systems, and reference standards. The smart metering system is reviewed according to hardware and software infrastructure that are directly related to communication and security issues. The communication methods used in SG framework are analyzed as wireline and wireless technologies where the management and control requirements are surveyed in detail. Therefore, a comprehensive table is presented including the standards, data rates, possible distances, network types, advantage, and disadvantages of each communication technology.

The security issues of the SG that is assumed as the transition of a traditional framework to a digital era of power flow and communication network are investigated in the fourth section. The outstanding high-level SG security objectives are surveyed in terms of cyber security requirements and physical security requirements. The smart protection methods, protocol based privacy, precautions against vulnerabilities are discussed in the security section. The evolution of SG shows that the security plays vital role in the reliability and sustainability of the entire system.

In case of the whole paper is considered, most of the current studies aim to increase the energy efficiency, demand management, utility planning, cost control and constructions. However, there some challenges and potential research issue can be remarked for metering application, SCADA networks, WAN measurements and control issues, and forensic sciences. For example, privacy of the personal usage and behavior of customers are one of the most important challenges in SM applications. On the other hand, security of data acquisition and storages, and operation cost predictions. It is believed that the most important challenges on SCADA applications are related to scalability issues that can be a worthy research issue in terms of scaling the networks and data collection in SCADA framework. The data processing, data security, and data storage issues are important challenges for WAN measurement that includes almost millions of nodes. Therefore, the storage problems of huge data amount can be coped with compression methods, sophisticated processing algorithms. The forensic sciences are also related to SG networks and application due to detecting and preventing the illegal usages. For this purpose, long-lasting data management and data storages are great challenges. In order to overcome these challenges, utilities need to expand data management systems into distributed data centers to handle huge data in a safe and reliable way. For this purpose, the most important candidate is cloud computing that is a developing computational model ensuring on-demand facilities and shared resources through the Internet. Energy management methods in smart grids can also be assessed by considering cloud computing applications. In addition, this structure provides more memory and storage ability for management systems. Moreover, this computing method can be utilized on the issue of communication management systems of SG. For instance, huge data obtained from SMs can be easily managed by cloud computing. Additionally, it offers the advantage of better security features. The event logging, instant access features, and critical intrusion management researchers could be considered to be studied.

## References

[1] Fang X, Misra S, Xue G, Yang D. Smart grid – the new and improved power grid: a survey. IEEE Commun Surv Tutor 2012;14:944–80.

[2] DeBlasio R, Tom C. Standards for the smart grid. In: Proceedings of the IEEE energy 2030 conference (ENERGY). Abu Dhabi; 4–5 November 2008, p. 1–7.

[3] Collier S. Ten steps to a smarter grid. IEEE Ind Appl Mag 2010;16(2):62–8.

[4] Lo CH, Ansari N. The progressive smart grid system from both power and communications aspects. IEEE Commun Surv Tutor 2012;14(3):799–821 Third Quarter.

[5] Kolhe M. Smart grid: charting a new energy future: research, development and demonstration. Electr J 2012;25:88–93.

[6] Ipakchi A, Albuyeh F. Grid of the future. IEEE Power and Energy Mag 2009;7:52–62.

[7] Goulden M, Bedwell B, Rennick-Egglestone S, Rodden T, Spence A. Smart grids, smart users? The role of the user in demand side management Energy Res Soc Sci 2014;2:21–9.

[8] Siano P. Demand response and smart grids – a survey. Renew Sustain Energy Rev 2014;30:461–78.

[9] Fangxing L, Wei Q, Hongbin S, Hui W, Jianhui W, et al. Smart transmission grid: vision and framework. IEEE Trans Smart Grid 2010;1:168–77.

[10] Kabalci E, Kabalci Y, Develi I. Modelling and analysis of a power line communication system with QPSK modem for renewable smart grids. Int J Electr Power Energy Syst 2012;34:19–28.

[11] Sechilariu M, Wang B, Locment F. Building-integrated microgrid: advanced local energy management for forthcoming smart power grid communication. Energy and Build 2013;59:236–43.

[12] Deutsche Telekom smart gridframework, ⟨http://powertown.no/wp-content/uploads/2011/11/SmartGrid_Ueberblick_ohneLegende.jpg⟩; 2015 [accessed 10.12.15].
[13] Farhangi H. The path of the smart grid. IEEE Power Energy Mag 2010;8(1):18–28.
[14] Wilson Ron, A network for the smart grid. Altera Inc., ⟨https://www.altera.co.jp/solutions/technology/system-design/articles/_2013/network-smart-grid.html⟩;2015 [accessed 10.12.15].
[15] Liserre M, Sauter T, Hung JY. Future energy systems: integrating renewable energy sources into the smart power grid through industrial electronics. IEEE Ind Electron Mag 2010;4(1):18–37.
[16] Hernandez L, Baladron C, Aguiar JM, Carro B, Sanchez-Esguevillas AJ, Lloret J, et al. A survey on electric power demand forecasting: future trends in smart grids, microgrids and smart buildings. IEEE Commun Surv Tutor 2014;16(3):1460–95 Third Quarter.
[17] Keyhani A, Chatterjee A. Automatic generation control structure for smart power grids. IEEE Trans Smart Grid 2012;3(3):1310–6.
[18] Variani MH, Tomsovic K. Distributed automatic generation control using flatness-based approach for high penetration of wind generation. IEEE Trans Power Syst 2013;28(3):3002–9.
[19] Sridhar S, Govindarasu M. Model-based attack detection and mitigation for automatic generation control. IEEE Trans Smart Grid 2014;5(2):580–91.
[20] Tyagi B, Srivastava SC. A decentralized automatic generation control scheme for competitive electricity markets. IEEE Trans Power Syst 2006;21(1):312–20.
[21] Molderink A, Bakker V, Bosman MGC, Hurink JL, Smit GJM. Management and control of domestic smart grid technology. IEEE Trans Smart Grid 2010;1(2):109–19.
[22] Pudjianto D, Ramsay C, Strbac G. Virtual power plant and system integration of distributed energy resources. IET Renew Power Gener 2007;1(1):10–6.
[23] Ruiz N, Cobelo I, Oyarzabal J. A direct load control model for virtual power plant management. IEEE Trans Power Syst 2009;24(2):959–66.
[24] Ziadi Z, Taira S, Oshiro M, Funabashi T. Optimal power scheduling for smart grids considering controllable loads and high penetration of photovoltaic generation. IEEE Trans Smart Grid 2014;5(5):2350–9.
[25] Mozina CJ. Impact of smart grids and green power generation on distribution systems. IEEE Trans Ind Appl 2013;49(3):1079–90.
[26] El Moursi MS, Zeineldin HH, Kirtley JL, Alobeidli K. A dynamic master/slave reactive power-management scheme for smart grids with distributed generation. IEEE Trans Power Deliv 2014;29(3):1157–67.
[27] Divenyi D, Dan AM. Agent-based modeling of distributed generation in power system control. IEEE Trans Sustain Energy 2013;4(4):886–93.
[28] Ma J, Zhang P, Fu H, Bo B, Dong Z. Application of phasor measurement unit on locating disturbance source for low-frequency oscillation. IEEE Trans Smart Grid 2010;1(3):340–6.
[29] Roscoe AJ, Abdulhadi IF, Burt GM. P and M class phasor measurement unit algorithms using adaptive cascaded filters. IEEE Trans Power Deliv 2013;28(3):1447–59.
[30] Gurusinghe DR, Rajapakse AD, Narendra K. Testing and enhancement of the dynamic performance of a phasor measurement unit. IEEE Trans Power Deliv 2014;29(4):1551–60.
[31] Tang Y, Stenbakken GN, Goldstein A. Calibration of phasor measurement unit at NIST. IEEE Trans Instrum Meas 2013;62(6):1417–22.
[32] Pan J, Jain R, Paul S. A survey of energy efficiency in buildings and microgrids using networking technologies. IEEE Commun Surv Tutor 2014;16(3):1709–31 Third Quarter.
[33] Hossain E, Kabalcı E, Bayındır R, Perez R. Microgrid testbeds around the world: state of art. Energy Convers Manag 2014;86:132–53.
[34] Hossain E, Kabalcı E, Bayındır R, Perez R. A comprehensive study on microgrid technology. Int J Renew Energy Res 2014;4(4):1094–107.
[35] Yilmaz M, Krein PT. Review of the impact of vehicle-to-grid technologies on distribution systems and utility interfaces. IEEE Trans Power Electron 2013;28(12):5673–89.
[36] Liu C, Chau KT, Wu D, Gao S. Opportunities and challenges of vehicle-to-home, vehicle-to-vehicle, and vehicle-to-grid technologies. Proc IEEE 2013;101(11):2409–27.
[37] Ortega-Vazquez MA. Optimal scheduling of electric vehicle charging and vehicle-to-grid services at household level including battery degradation and price uncertainty. IET Gener Transm Distrib 2014;8(6):1007–16.
[38] Liu H, Hu Z, Song Y, Lin J. Decentralized vehicle-to-grid control for primary frequency regulation considering charging demands. IEEE Trans Power Syst 2013;28(3):3480–9.
[39] Igualada L, Corchero C, Cruz-Zambrano M, Heredia F-J. Optimal energy management for a residential microgrid including a vehicle-to-grid system. IEEE Trans Smart Grid 2014;5(4):2163–72.
[40] Muscas C, Pau M, Pegoraro P, Sulis S. Smart electric energy measurements in power distribution grids. IEEE Instrum Meas Mag 2015;18(1):17–21.
[41] Peretto L. The role of measurements in the smart grid era. IEEE Instrum Meas Mag 2010;13(3):22–5.
[42] Moreno-Munoz A, Pallares-Lopez V, Gonzalez de la Rosa JJ, Real-Calvo R, Gonzalez-Redondo M, Moreno-Garcia IM. Embedding synchronized measurement technology for smart grid development. IEEE Trans Ind Inform 2013;9(1):52–61.
[43] Basso T, DeBlasio R. IEEE smart grid series of standards IEEE 2030 (Interoperability) and IEEE 1547 (Interconnection) status. In: Grid-Interop 2011, Arizona: Phoenix; 5–8 December 2011. p. 1–9.
[44] Ferrari P, Flammini A, Rinaldi S, Sisinni E. On the seamless interconnection of IEEE1588-based devices using a PROFINET IO infrastructure. IEEE Trans Ind Inform 2010;6(3):381–92.
[45] Lixia M, Benigni A, Flammini A, Muscas C, Ponci F, Monti A. A software-only PTP synchronization for power system state estimation with PMUs. IEEE Transn Instrum Meas 2012;61(5):1476–85.
[46] Bhatt J, Shah V, Jani O. An instrumentation engineer's review on smart grid: critical applications and parameters. Renew Sustain Energy Rev 2014;40:1217–39.
[47] Depuru SSSR, Wang L, Devabhaktuni V. Smart meters for power grid: challenges, issues, advantages and status. Renew Sustain Energy Rev 2011;15:2736–42.
[48] Sadinezhad I, Agelidis Vassilios G. Slow sampling on-line harmonics/interharmonics estimation technique for smart meters. Electr Power Syst Res 2011;81:1643–53.
[49] Li H, Mao R, Lai L, Qiu RC. Compressed meter reading for delay-sensitive and secure load report in smart grid. In: Proceedings of the IEEE SmartGridComm'10, Maryland, USA; 2010. p. 114–19.
[50] Yang Z, Chen YX, Li YF, Zio E, Kang R. Smart electricity meter reliability prediction based on accelerated degradation testing and modeling. Int J Electr Power Energy Syst 2014;56:209–19 March.
[51] Yaacoub E, Abu-Dayya A. Automatic meter reading in the smart grid using contention based random access over the free cellular spectrum. Comput Netw 2014;59:171–83.
[52] Bat-Erdene B, Lee B, Kim MY, Ahn TH, Kim D. Extended smart meters-based remote detection method for illegal electricity usage. IET Gener Transm Distrib 2013;7:1332–43.
[53] Cho HS, Yamazaki T, Hahn M. Determining location of appliances from multihop tree structures of power strip type smart meters. IEEE Trans Consum Electron 2009;55:2314–22.
[54] Erkin Z, Troncoso-Pastoriza JR, Lagendijk RL, Perez-Gonzalez F. Privacy-preserving data aggregation in smart metering systems: an overview. IEEE Signal Process Mag 2013;30:75–86.
[55] Tan O, Gunduz D, Poor HV. Increasing smart meter privacy through energy harvesting and storage devices. IEEE J Sel Areas Commun 2013;31:1331–41.
[56] Zhou J, Hu RQ, Qian Yi. Scalable distributed communication architectures to support advanced metering infrastructure. IEEE Trans Smart Grid Parallel and Distrib Syst 2012;23:1632–42.
[57] Wigan M. User issues for smart meter technology. IEEE Technol Soc Mag 2014;33:49–53 Spring.
[58] Kalogridis G, Sooriyabandara M, Fan Z, Mustafa MA. Toward unified security and privacy protection for smart meter networks. IEEE Syst J 2014;8:641–54.
[59] Lagendijk R, Erkin Z, Barni M. Encrypted signal processing for privacy protection. IEEE Signal Process Mag 2013;30:82–105.
[60] Jawurek M, Johns M, Kerschbaum F. Plug-in privacy for smart metering billing. In: Proceedings of the privacy enhanced technologies symposium. Waterloo, Canada; 2011. p. 192–210.
[61] Kohlweiss M, Danezis G. Differentially private billing with rebates. In: Proceedings of the information hiding conference (LNCS), Prague, Czech Republic; 2011. p. 148–62.
[62] Rial A, Danezis G. Privacy-preserving smart metering. In: Proceedings of the 10th Annu. ACM workshop on privacy in the electronic society (WPES'11), New York; 2011. p. 49–60.
[63] Garcia FD, Jacobs B. Privacy-friendly energy-metering via homomorphic encryption. In: Proceedings of the 6th workshop security and trust management (STM 2010), Athens, Greece; 2010. p. 226–38.
[64] Beye MRT, Erkin Z, Lagendijk RL. Efficient privacy preserving k-means clustering in a three-party setting. In: Proceedings of the IEEE workshop inform. Iguacu Falls, Brazil: Forensics Security; 2011. p. 1–6.
[65] Yan Y, Qian Y, Sharif H, Tipper D. A survey on smart grid communication infrastructures: motivations, requirements and challenges. IEEE Commun Surv Tutor 2013;15:5–20 First Quarter.
[66] Wang W, Xu Y, Khanna M. A survey on the communication architectures in smart grid. Comput Netw 2011;55:3604–29.
[67] Usman A, Shami S. Evolution of communication technologies for smart grid applications. Renew Sustain Energy Rev 2013;19:191–9.
[68] Lu X, Wang W, Ma J. An empirical study of communication infrastructures towards the smart grid: design, implementation, and evaluation. IEEE Trans Smart Grid 2013;4:170–83.
[69] Kuzlu M, Pipattanasomporn M, Rahman S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. Comput Netw 2014;67:74–88.
[70] Khan RH, Khan JY. A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network. Comput Netw 2013;57:825–45.
[71] Ancillotti E, Bruno R, Conti M. The role of communication systems in smart grids: architectures, technical solutions and research challenges. Comput Commun 2013;36:1665–97.
[72] Li W, Zhang X. Simulation of the smart grid communications: challenges, techniques, and future trends. Comput Electr Eng 2014;40:270–88.
[73] Galli S, Scaglione A, Wang Z. For the grid and through the grid: the role of power line communications in the smart grid. Proc IEEE 2011;99:998–1027.
[74] Khalifa T, Naik K, Nayak A. A survey of communication protocols for automatic meter reading applications. IEEE Commun Surv Tutor 2011;13(2):168–82 Second Quarter.

[75] Fan Z, Kulkarni P, Gormus S, Efthymiou C, Kalogridis G, Sooriyabandara M, et al. Smart grid communications: overview of research challenges, solutions, and standardization activities. IEEE Commun Surv Tutor 2013;15 (1):21–38 First Quarter.

[76] Liu S, Liu Xiaoping P, El Saddik A. Modeling and distributed gain scheduling strategy for load frequency control in smart grids with communication topology changes. ISA Trans 2014;53:454–61.

[77] Saputro N, Akkaya K, Uludag S. A survey of routing protocols for smart grid communications. Comput Netw 2012;56:2742–71.

[78] Lazarus BN. Smart grid enabled and enhanced by broadband powerline. In: Proceedings of ENERGY 2013, the third Int. Conf. on Smart Grids, Green Comm. and IT energy-aware technologies. Lisbon, Portugal; March 24–29, 2013. p. 77–83.

[79] Rahman MM, Hong C, Lee S, Lee J, Razzaque MA, Kim J. Medium access control for power line communications: an overview of the IEEE 1901 and ITU-T G.hn standards. IEEE Commun Mag 2011;49:183–91.

[80] Brown J, Khan JY. Key performance aspects of an LTE FDD based smart grid communications network. Comput Commun 2013;36:551–61.

[81] Xu Y, Wang W. Wireless mesh network in smart grid: modeling and analysis for time critical communications. IEEE Trans Wirel Commun 2013;12:3360–71.

[82] Zhu Z, Lambotharan S, Chin W, Fan Z. Overview of demand management in smart grid and enabling wireless communication technologies. IEEE Wirel Commun 2012;19:48–56.

[83] Ma R, Chen H, Huang Y, Meng W. Smart grid communication: its challenges and opportunities. IEEE Trans Smart Grid 2013;4:36–46.

[84] Wang H, Qian Y, Sharif H. Multimedia communications over cognitive radio networks for smart grid applications. IEEE Wirel Commun 2013;20:125–32.

[85] Niyato D, Wang P. Cooperative transmission for meter data collection in smart grid. IEEE Commun Mag 2012;50(4):90–7.

[86] Kulkarni P, Gormus S, Fan Z, Motz B. A mesh-radio-based solution for smart metering networks. IEEE Commun Mag 2012;50(7):86–95.

[87] Deng R, Chen J, Cao X, Zhang Y, Maharjan S, Gjessing S. Sensing-performance tradeoff in cognitive radio enabled. IEEE Trans Smart Grid 2013;4:302–10.

[88] Huang J, Wang H, Qian Y, Wang C. Priority-based traffic scheduling and utility optimization for cognitive radio communication infrastructure-based. IEEE Trans Smart Grid 2013;4:78–86.

[89] Gentile C, Griffith D, Souryal M. Wireless network deployment in the smart grid: design and evaluation issues. IEEE Netw 2012;26:48–53.

[90] Su H, Qiu M, Wang H. Secure wireless communication system for smart grid with rechargeable electric vehicles. IEEE Commun Mag 2012;50:62–8.

[91] Wang W, Lu Z. Cyber security in the smart grid: survey and challenges. Comput Netw 2013;57:1344–71.

[92] Metke AR, Ekl RL. Security technology for smart grid networks. IEEE Trans Smart Grid 2010;1:99–107.

[93] Eun-Kyu Lee, Gerla M, Oh SY. Physical layer security in wireless smart grid. IEEE Commun Mag 2012;50:46–52.

[94] Nordell DE. Terms of protection: the many faces of smart grid security. IEEE Power and Energy Mag 2012;10:18–23.

[95] Khurana H, Hadley M, Lu N, Frincke DA. Smart-grid security issues. IEEE Secur Priv 2010;8:81–5.

[96] McDaniel P, McLaughlin S. Security and privacy challenges in the smart grid. IEEE Secur Priv 2009;7:75–7.

[97] Yan Y, Qian Y, Sharif H, Tipper D. A survey on cyber security for smart grid communications. IEEE Commun Surv Tutor 2012;14:998–1010.

[98] Bou-Harb E, Fachkha C, Pourzandi M, Debbabi M, Assi C. Communication security for smart grid distribution networks. IEEE Commun Mag 2013;51:42–9.

[99] Yilin M, Kim TH-H, Brancik K, Dickinson D, Heejo L, et al. Cyber–physical security of a smart grid infrastructure. Proc IEEE 2012;100:195–209.

[100] Ericsson GN. Cyber security and power system communication – essential parts of a smart grid infrastructure. IEEE Trans Power Deliv 2010;25:1501–7.

[101] Hahn A, Ashok A, Sridhar S, Govindarasu M. Cyber–physical security testbeds: architecture, application, and evaluation for smart grid. IEEE Trans Grid 2013;4:847–55.

[102] Ross KJ, Hopkinson KM, Pachter M. Using a distributed agent-based communication enabled special protection system to enhance smart grid security. IEEE Trans Smart Grid 2013;4:1216–24.

[103] Yan Y, Hu RQ, Das SK, Sharif H, Qian Y. An efficient security protocol for advanced metering infrastructure in smart grid. IEEE Netw 2013;27:64–71.

[104] Qiu M, Su H, Chen M, Ming Z, Yang LT. Balance of security strength and energy for a PMU monitoring system in smart grid. IEEE Commun Mag 2012;50:142–9.

[105] Hu B, Gharavi H. Smart grid mesh network security using dynamic key distribution with merkle tree 4-way handshaking. IEEE Trans Smart Grid 2014;5:550–8.

[106] Liu J, Xiao Y, Li S, Liang W, Chen CLP. Cyber security and privacy issues in smart grids. IEEE Commun Surv Tutor 2012;14:981–97 Fourth Quarter.

[107] Li X, Liang X, Lu R, Shen X, Lin X, Zhu H. Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Commun Mag 2012;50:38–45.

[108] Xia J, Wang Y. Secure key distribution for the smart grid. IEEE Transon Smart Grid 2012;3:1437–43.

[109] Finster S, Baumgart I. Privacy-aware smart metering: a survey. IEEE Commun Surv Tutor 2014;16(3):1732–45.

[110] Erol-Kantarci M, Mouftah HT. Smart grid forensic science: applications, challenges, and open issues. IEEE Commun Mag 2013;51(1):68–74.

[111] Qiu M, Su H, Chen M, Ming Z, Yang LT. Balance of security strength and energy for a PMU monitoring system in smart grid. IEEE Commun Mag 2012;50(5):142–9.

[112] Fadlullah ZM, Fouda MM, Kato N, Takeuchi A, Iwasaki N, Nozaki Y. Toward intelligent machine-to-machine communications in smart grid. IEEE Commun Mag 2011;49(4):60–5.

[113] Das S, Ohba Y, Kanda M, Famolari D, Das SK. A key management framework for AMI networks in smart grid. IEEE Commun Mag 2012;50(8):30–7.

[114] Kim S, Kwon EY, Kim M, Cheon JH, Ju S, Lim J, et al. A secure smart-metering protocol over power-line communication. IEEE Trans Power Deliv 2011;26 (4):2370–9.