WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2014; **14**:1055–1087
Published online 23 July 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.2258

RESEARCH ARTICLE

Smart grid sensor data collection, communication, and networking: a tutorial

Nipendra Kayastha[1], Dusit Niyato[1]*, Ekram Hossain[2] and Zhu Han[3]

[1] School of Computer Engineering, Nanyang Technological University, 50 Nanyang Avenue, 639798, Singapore
[2] Department of Electrical and Computer Engineering, University of Manitoba, Canada
[3] Department of Electrical and Computer Engineering, University of Houston, USA

ABSTRACT

The smart grid is an innovative *energy network* that will improve the conventional electrical grid network to be more reliable, cooperative, responsive, and economical. Within the context of the new capabilities, advanced data sensing, communication, and networking technology will play a significant role in shaping the future of the smart grid. The smart grid will require a flexible and efficient framework to ensure the collection of timely and accurate information from various locations in power grid to provide continuous and reliable operation. This article presents a tutorial on the sensor data collection, communications, and networking issues for the smart grid. First, the applications of data sensing in the smart grid are reviewed. Then, the requirements for data sensing and collection, the corresponding sensors and actuators, and the communication and networking architecture are discussed. The communication technologies and the data communication network architecture and protocols for the smart grid are described. Next, different emerging techniques for data sensing, communications, and sensor data networking are reviewed. The issues related to security of data sensing and communications in the smart grid are then discussed. To this end, the standardization activities and use cases related to data sensing and communications in the smart grid are summarized. Finally, several open issues and challenges are outlined. Copyright © 2012 John Wiley & Sons, Ltd.

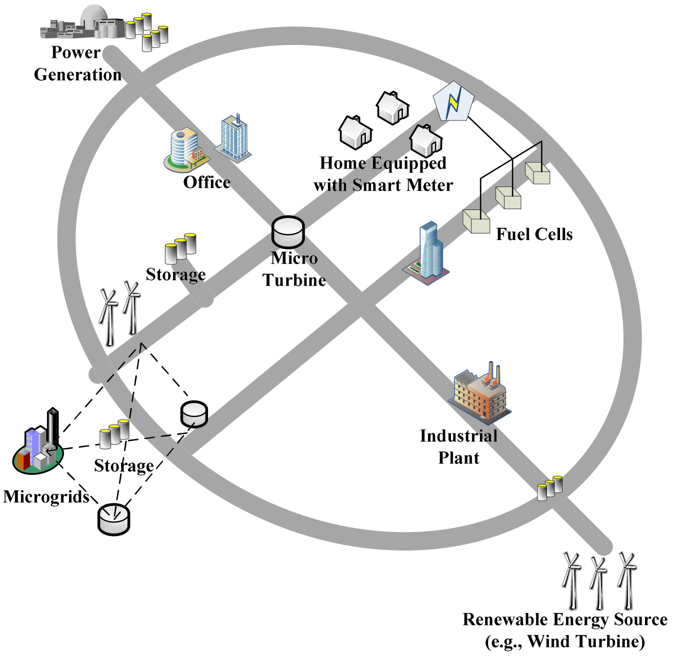
KEYWORDS
smart grid; sensor data collection and sensing

***Correspondence**
Dusit Niyato, School of Computer Engineering, Nanyang Technological University, 50 Nanyang Avenue, 639798, Singapore.
E-mail: dniyato@ntu.edu.sg

1. INTRODUCTION

The existing electrical power grid is by far the most sophisticated and significant engineering system of the 20th century [1]. The electrical power grid forms a very large network that is based on the centralized generation interconnected by numerous control systems and transmission lines. In many ways, the present power grid has served well in providing seamless unidirectional power supply of electricity to the consumers. However, it faces new challenges such as depletion of primary energy resources, generation diversification, climate changes, and reliability, which must be addressed in near future. Also, the conventional power grid lacks intelligence. Intelligence here refers to the capability of monitoring and controlling the various industrial appliances or functional components to provide optimal energy generation and usage. One example is the supervisory control and data acquisition (SCADA) technology, which provides communications infrastructure for the conventional electrical power grids. This system collects data from various sensors and then sends this data to a central computer for processing and storage. The SCADA system has limited control over their upstream function (from consumer premises towards the generation site) and lacks real-time control capability for the power distribution network. The existing electrical power grid is therefore evolving into a more intelligent, more responsive, more efficient, and more environmentally friendly system, known as the smart grid [2,3]. This evolution is driven by the increase in power demand, unreliable power flow, distributed system setting, and emergent renewal energy generation. To address these challenges, the smart grid requires a dynamic architecture, intelligent algorithms, and efficient mechanisms [2,4–8].

Figure 1 shows the landscape of the future smart grid with its promising characteristics. The components of the smart grid are connected by bidirectional electrical and data networks with the help of advanced metering infrastructure (AMI). One important requirement of AMI is to provide near real-time metering data including fault and



Smart Grid Characteristics

1. Self-healing:
Capability to rapidly detect, analyze, respond, and restore from the fault and failures.

2. Consumer friendly:
Ability to involve a consumer into the decision process of electrical power grid

3. High reliability and power quality:
Ability to provide continuous power to satisfy consumer needs.

4. Resistance to cyber attacks:
Ability to be immune and to protect the system from any cyber and physical attacks.

5. **Accommodates all generation and storage options:**
Ability to adapt to a large number of diverse distributed generation (e.g., wind energy and renewable energy) and storage devices deployed to complement the large power generating plants.

6. Optimization of asset and operation: Ability to monitor and optimize the capital assets by minimizing operation and maintenance expenses.

7. Enables markets:
Offers new consumer choices such as green power product and new generation of electric vehicle which leads to reduction in transmission congestion.

Figure 1. Smart grid landscape and its characteristics [2,8].

outage information to the utility control center. A node in the smart grid can behave as both information sink and source. The AMI provides a two-way communication architecture between the smart meter and a utility company. The smart meter is an advanced meter that provides more detailed and accurate power consumption information than that of a conventional meter that can be used for monitoring and billing purposes. Further, the AMI comprises of local data aggregator units (DAUs) to collect and relay the information from the meter side to meter data management systems (MDMS) and also an active user interface to provide information access to the consumers. The MDMS provides storage, management, and processing of collected data for proper usage by other power system applications and services. AMI will be comprised of many systems and subsystems, which can be grouped under a hierarchical structure on the basis of home area networks (HANs), neighborhood area networks (NANs), and wide area networks (WANs). Furthermore, the smart grid will incorporate some basic structures called intelligent microgrids. A microgrid can include interconnected distributed energy systems (loads and resources) with local storage devices and controllable load. The microgrids are not only generally connected to the electrical power grid, but they can also function independently (i.e., in islanded mode) and be resynchronized with the main grid in case of fault. Many communication aspects of the smart grid mostly related to the meter management and power consumption will be handled by the AMI to provide a user-centric approach for managing the electric power in the smart grid. By far, there is no standard document defining the AMI, and it is still open to new development and implementation.

A wide range of enabling technologies such as integrated communications, sensing and measurement, advanced component, advanced control, improved interface, and decision support will be adopted for the AMI in the smart grid [1]. Of these key technology areas, the implementation of integrated communications together with sensor data collection and networking will be the driving factor that will create a dynamic and interactive power grid infrastructure to integrate all upstream (toward generator) and downstream (toward consumers) components to work seamlessly [9]. The data communication network in the smart grid will provide the necessary functionality for connecting different sensors and actuators for sensing (e.g., meter reading, gathering real-time measurements from various locations of the power grid for fault detection, and security alarming) and controlling them to enable an optimal, reliable, and resilient operation of the grid. The sensors and actuators combined with advanced data communications techniques will help to meet the growing demand from consumers by integrating renewable energy resources, optimizing energy flow, isolating and restoring

DOI: 10.1002/wcm

power outage, providing power quality of electricity, and empowering the consumer with tools for optimizing their energy consumption. Sensor data collection and networking will be used in the smart grid to acquire and transform data into information for maintaining stability and integrity of the grid. For example, a smart meter can be used as a sensor node to measure, predict, and report power usage and demand to the public utility and to the consumers for providing demand–response information. Also, failure of a transformer can result in explosion that may hamper the grid stability and people safety. Sensors can be installed to detect the existence of internal discharge activity so that necessary maintenance action can be taken [10].

The smart grid will rely on several existing and future wired and wireless communication networking technologies such as power line communications (PLC), cellular and broadband wireless technologies (e.g., 3G, WiMAX, and 3GPP LTE), cooperative and cognitive communications networks, short-range wireless communications technologies (e.g., ZigBee) and Internet protocol (IP)-based networks. However, data sensing and networking in the smart grid still require to overcome a number of technical and procedural challenges. On the technical side, for instance, selection of communication and networking techniques is not straightforward because of different data requirements of the smart grid. A critical parameter would be to minimize the data packet loss, which can deteriorate the estimation accuracy for time-critical faults in the grid. The existing and future data communication protocols should be modified/designed taking into consideration the characteristics of the power systems. Another significant challenge is to ensure secure communication which is resilient to cyber and physical attacks. On the procedural side, regulating data sensing in the smart grid requires establishing a common and standard data output format because of numerous sensors deployed across the grid.

This article presents a tutorial on the data sensing and communication techniques in the smart grid. First, applications of data sensing in power generation, transmission, distribution, and consumption are reviewed (Section 2). The importance of effective data sensing and communications in the smart grid is also highlighted. Then, the requirements for data collection and communications and those related to the sensors and actuators to be used in the smart grid are discussed (Section 3). To support these requirements, a hierarchical network architecture is presented for the smart grid (Section 4). The related communication technologies are also discussed. Next, several emerging techniques for data sensing and communications are described (Section 5). Security-related issues for data sensing and communication in the smart grid and the approaches for providing security are then described (Section 6). Related standardization activities are reviewed (Section 7), and the use cases of sensor data collection and communication in the smart grid are discussed (Section 8). To this end, several open issues and challenges are outlined (Section 9). Note that because the focus here is on the sensing, communication, and networking technologies for the smart grid, a detailed exposition on the issues such as distributed energy resource (DER) management, demand-side management (DSM), architecture and protocol for power management in the smart grid are out of the scope of this article.

2. APPLICATIONS OF DATA SENSING IN THE SMART GRID

The applications of data sensing in the smart grid can be grouped into four general areas: (i) generation, (ii) storage, (iii) transmission and distribution, and (iv) consumption.

2.1. Power generation

Data-sensing techniques can be used to monitor the generation of electricity, power quality throughout the grid, equipment health and capacity, fault locations, meter tampering, vegetation intrusion, and also load balance between the grid and DER or renewal energy resources in the energy cycle [11]. Data sensing will be necessary as large wind and solar farms are being deployed to supply energy into transmission grid to balance the growing energy demand.

Distributed energy resource is gaining momentum in energy generation because of its potential to provide green energy that can significantly decrease the negative effect caused to the environment because of the usage of traditional fossil fuels. The U.S. Department of Energy envisions that wind power could supply 20% of all U.S. electricity by 2030 [12]. Because of its tremendous potential, it is necessary to provide conditional and structural monitoring of DER to prevent any future downtime because of component failures. Further, these DERs can be located in remote areas, thus creating challenges for efficient monitoring of various components such as status of battery cells in storage banks, load monitoring, and information about weather conditions [13]. Wireless sensor network (WSN) is an enabling technology for such monitoring applications because of its low cost and also ease of installation [14,15]. However, wireless communications are inherently limited by available transmission rates and bandwidth. Therefore, it is necessary to provide distributed processing in these wireless sensors, where the sensed data can be processed locally within the sensors. Consequently, only relatively small amount of processed data will need to be transmitted.

A WSN comprised of Stanford wireless sensors called WiMMS units [16] is deployed in the wind turbine structure to provide information about the dynamic behavior of wind turbine and response to loading [14]. This wireless sensor consists of a computational core for data processing and storage, a sensing interface for providing analog-to-digital conversion, and a communication interface for providing connection to the core network. The computational core consists of Atmel ATMegal128 microcontroller with an 8-bit integrated circuit architecture and 128 kB

DOI: 10.1002/wcm

of flash memory for providing any computational application. The sensing interface consists of Texas Instruments ADS8341, which is a four-channel, 16-bit analog-to-digital converter and interfaces with MEMS accelerometer sensor (i.e., Crossbow CXL01) and metal foil strain guage (i.e., Texas Measurements YFLA-5-5L). The communication interface consists of a MaxStream 24XStream wireless modem that operates at the 2.4 GHz (i.e., ISM) band. The WiMMS unit provides data rate up to 192 kbps with 5 km line-of-sight communication range. The sensed data are processed by the sensors and then transmitted to a laptop located at the base of the tower for further processing or forwarding to the control and monitoring stations.

2.2. Power storage

Energy storage will also be a critical part of the smart grid to store energy from renewable energy sources, whose output varies with weather conditions (e.g., solar panels generate energy only when the sun shines). For energy storage, lead-acid battery can be used, for which its temperature, voltage, and current need to be monitored [17]. Especially, the state-of-charge (SOC) is the most important parameter that needs to be measured and reported [18]. The SOC is measured from the acid level and acid density, where these parameters will change during charging and discharging processes. Small ion exchange material is used to build a sensor for measuring the concentration in a battery. Also, the temperature sensor is required in the liquid electrolyte, which monitors not only the operating point of concentration sensor but also the reliability of the battery. Also, the power storage can be used in the vehicle (e.g., plug-in hybrid vehicle). The SOC of the battery in a vehicle has to be monitored and reported for the optimization [19].

2.3. Power transmission and distribution

In the transmission and distribution part of the smart grid, data sensing can be used to monitor substations, transformers, underground lines, and overhead lines [10]. By using sensors to monitor real-time voltage, current, phase, and frequency information, the transmission capacity can be increased up to 10–15% compared with the capacity planning models that use static weather, wind, and temperature scenarios [17]. Moreover, sensors can be used to minimize the transmission loss by providing automatic operation of distribution capacitor on the basis of the needs of the transformer [13].

Sensors such as smart current/voltage sensors with communication capability can report real-time current/voltage data back to the feeder line so that it can distribute the current at a lower voltage, thus allowing more efficient use of the available electricity. For example, sensors by ZIV (one of the companies that provides protection, control, metering, and communication products for power systems) such as DRMT-1 and ACA-1/R sensors are resistive voltage sensors. They are constructed with high precision and are intended for fault detection applications for distribution power line, protective relaying, and distribution grid monitoring [20]. A new type of sensing system called three-dimensional heterogeneous sensor system on a chip for distributed power grid monitoring, fault detection, and control is also proposed in [21]. The heterogeneous sensor system on a chip uses noncontact sensors, analog and digital processing, and RF communications. The noncontact inductive sensor is used to detect the transmission line current, which will detect the changes in the power line amperage and notify of any fault in the distribution system.

The temperature of high-voltage (HV) power line also requires monitoring to track temperature changes because of the load variation in these lines. Any increase in electric current can increase temperature causing local oxidation to occur, which in turn increases the temperature even more. Surface acoustic wave (SAW) temperature sensors can be used to sense the variation in temperature [22]. The SAW sensor is based on piezoelectricity that uses an electrically induced acoustic wave on a piezoelectric substrate surface to measure the temperature. The acoustic wave is influenced by ambient temperature and can be used for temperature sensing. The temperature variation causes the surface wave velocity and the reflecting distance to change, which can be used to measure the temperature. The SAW sensor is a passive wireless sensor working at 433 MHz, which measures the temperature at adjustable interval from 10 seconds to 10 minutes. The effective sensing distance is 2.5 m, and the data transmission rate is 50 kbps [22]. The SAW system collects temperature data from sensors, packetizes, and transmits them to a processing unit where the data is digitized for further processing.

Because of the sensitivity of electronic equipments (e.g., computers and automated manufacturing devices) to the voltage fluctuations, maintaining power quality is of paramount importance. However, the power quality of the electricity varies considerably depending on factors such as lightning, inadequate or incorrect wiring, and grounding or short circuits caused by animals, branches, vehicular impact, and human accidents involving electric lines [23]. The fluctuation of voltage between 10% and 90% of nominal root mean square voltage lasting between 0.5 and 60 cycles is termed as voltage sag and causes a reliability problem in the grid. To maintain the power quality of electricity, in [23], a low-cost web-based sensor and alarm system termed as *PQ watch* is proposed. This PQ watch continuously monitors the energy consumption information and the data on power quality events including outages, blackouts, interruptions, and short-duration disturbances such as voltage sags. The PQ watch sensor is comprised of ADE7756 [24], the PIC 16F873 microcontroller, an EEPROM, and an RS-232 converter integrated circuit. The ADE7756 provides highly accurate electrical power measurement and a serial interface to the system. The microcontroller does the root mean square voltage calculation for control of the meter and communications. The EEPROM is used to store various calibration parameters of the meter and store the meter's data during a power down. The entire system can be accessed using the Internet.

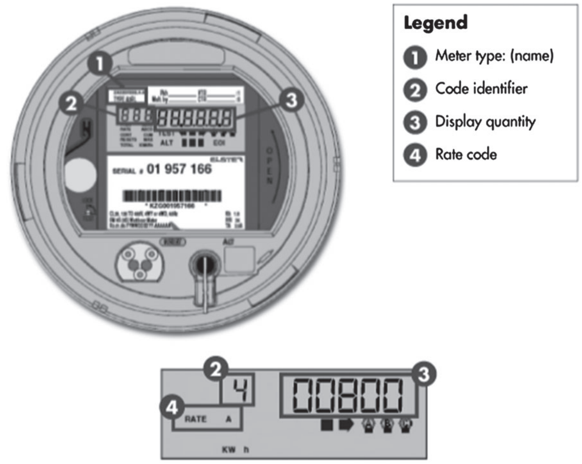
To monitor overhead transmission lines, various sensor networks (e.g., WSN and fiber-optic sensor networks) can be used [15,25]. Schneider Electric [26] introduces a wireless HV sensor that uses synchrophasor measurement solution (e.g., phasor measurement unit [PMU]) to provide highly accurate sensing of voltage for overhead transmission lines [27]. This HV sensor provides cost-effective, easy, clamp-on installation, and wireless integration for previously unmonitored points on the transmission grid. The HV sensor consists of a global positioning system (GPS) unit to provide accurate time synchronization which can transmit data via satellite, cellular, or licensed RF radio back to a control center. Also, this HV sensor can accurately verify and reclassify an existing instrument-class current transformer installed and operating in a field [27]. Alternatively, fiber-optic sensor technology such as fiber bragg grating (FBG) can also be used to form quasi-distributed sensor networks for providing overhead transmission line monitoring [28]. FBG can be used to detect various physical parameters such as strain, temperature, pressure, acceleration, and large magnetic field and tension [29]. The FBG sensors are deployed in series forming a network along the HV transmission lines, and wavelength-division multiplexing is used for data communication. The FBG sensors are clamped on the transmission lines for measurement, and it can be wrapped to contact the conductor for temperature measurement. An optical spectrum analyzer is used to detect the wavelength shifting, which can detect the change in strain and temperature. The FBG sensor has a transmission range of 100 km, which makes it more versatile for monitoring long transmission lines. The sensed data can be used to predict phenomena such as overheating, vibrations, galloping, ice accertion, and sag. Also, *smart capacitor control sensors* can be used to monitor or control capacitor banks, which helps to stabilize the voltage and power factors. The *smart continuity grid sensors*, on the other hand, help to identify the outage in transmission and distribution lines and automatically reroute power to maximize the electricity availability.

2.4. Power consumption

In the customer premises, data sensing presents a wide range of opportunities to both consumers and public utility for maintaining a good demand–response in the power grid even during peak hours. Data sensing in the consumer premises can be performed through smart meters, which provide information about real-time power usage and possibly control the power consumption automatically or on the basis of a predefined control mechanism. The smart meter acts as a sensor node and records the electricity consumption (kilo watt hour [kWh]) and time of use (TOU) [30]. TOU refers to consumer activity at a particular time that is generally measured on an hourly, daily, or weekly basis depending on the need. For each TOU, the public utility defines a TOU rate (i.e., price) on the basis of the local load pattern and generation cost. The energy management system (EMS) combines the energy consumption information with real-time electric prices to provide effective demand–response. For this, various home automation solutions can provide proper monitoring, prediction, and control over the fundamental function of heating, ventilation, and air conditioning. Whereas consumers will be able to reduce their cost through TOU rate information, a public utility will be able to use the real-time usage and outage information to improve efficiency of power generation and transmission [13], for example, by load prediction [31]. The real-time usage information will enable the public utility to understand the real-time demand and patterns, which can be used to increase the generation efficiency by allowing better load balancing or diverting the flow from nearby DERs.

As an example, the A3 ALPHA meter [32] from Elster Group [33] can be used in residential metering. The A3 ALPHA meter supports two-way communication to offer high accuracy, repeatability, and low ownership costs to the consumers. It also supports the American National Standards Institute (ANSI) C12 protocols for the AMI. The A3 ALPHA meter together with the EnergyAxis system [34] (i.e., IP-based two-way communication network designed for a harsh real-world utility environment) provides a unified solution for the smart grid. The A3 ALPHA meter is already in use in the Salt River Project [35], an agency of the state of Arizona in the U.S.A. that serves as an electrical utility for the Phoenix metropolitan area. Figure 2 shows the functionality of an A3 ALPHA meter. The A3 ALPHA meter can display both energy and demand values (5 digits). The code identifier will display the ID code on the left side, and the description of the code is shown in the right side of the display as shown in Figure 2. The meter also offers a power quality monitoring option. This feature helps isolate the cause of transients, harmonics, and sags.

Similarly, various temperature sensors, motion sensors, and light sensors can be used to monitor the environment inside a house to control different electrical appliances such as air conditioner, heating unit, and alarm systems for an effective home EMS (HEMS). The HEMS can be linked to the smart meter to control the usage of electrical appliance depending on the real-time pricing plans. For example, INSTEON Energy Display [36] can be used to track the energy consumption of an appliance connected to INSTEON power meter [37] (called iMeter Solo). The iMeter Solo is an adapter that uses PLC technology to measure, track, and monitor the energy usage of appliances (up to 15 Amps). The data can be analyzed, and a necessary control action can be initiated using INSTEON network called HouseLinc. The INSTEON Energy Display can link up to three iMeter Solo Power Meters, which can be used to view the amount of current energy consumption by the connected appliances, average amount of energy used per month, and power cost given a billing rate.



Code	Description of reading
88888	Display test
0	Time of day (Military time)
1	Day of Week
2	Date
3	Total kWh
4	On-Peak kWh (Rate A)
5	Off-Peak kWh (Rate C)
10	Maximum kWh

Figure 2. A3 ALPHA smart meter configuration [32,35].

3. REQUIREMENTS FOR DATA SENSING AND COMMUNICATION IN SMART GRID

The requirements for data sensing and communications for managing, controlling, and optimizing different devices and systems in the smart grid can be summarized as follows.

3.1. Requirements for sensors and actuators

Data sensing in the smart grid requires sensing of parameters such as voltage, current, temperature, moisture, continuity, and phase to calibrate and control various equipments on the basis of the fluctuations of these parameters. The sensors and actuators are the physical components that sense and initiate appropriate actions through the control algorithms to provide necessary corrective actions if any failure occurs [38]. Such a sensor generally includes sensor device, analog signal conditioning, analog-to-digital conversion, digital signal processing, and communication functionality in a single package [39]. The actuators, on the other hand, initiate actions such as setting the value of different parameters by converting the information collected by the sensors into physical phenomenon (e.g., displaying the sensor measurements or status of circuit breaker) [40]. The requirements for sensors and actuators are as follows:

- *Reliability and energy efficiency*: the sensors and actuators should be reliable to effectively support the smart grid applications. Also, they should not have any electromagnetic compatibility problem. In addition, the sensor and actuator devices should be energy efficient so that they can operate with low-power supply in case of emergency situations. Research and development activities are being carried out to develop sensors, which do not require external power supply, for example, by using technologies similar to passive frequency identification chips without battery or possibly by exploiting energy-harvesting techniques [40].
- *Cost-effective and secured operation*: the sensors and actuators should be low cost to make them economically attractive for the business and users [41]. The advancement of CMOS technologies has made the pervasive deployment of these smart sensors and actuators possible. Also, the sensors should be small in size and should be installed in a secured location so that the possibility of damage is minimized.
- *Longer life span*: this is important for sensors and actuators because a power grid has to be operated cost effectively over a long time horizon (e.g., 10–20 years).

3.2. Data collection requirements

The smart grid will consist of numerous systems and subsystems of diverse types that have their own data collection requirements. For example, the data collection requirements for power generation and transmission can be different from those for a smart meter in a consumer premise. Moreover, a large amount of data need to be gathered, verified, stored, and transformed in near real time for intelligent response and decision support in the smart grid. Data sensing in the smart grid has to scale accordingly to handle the required levels of data volume and complexity. For example, a PMU needs to send up to 30 reports every second to measure the quality of power delivery. Because the sensing nodes deployed in various locations of the power grid pose scalability challenges, there is a need for decentralized aggregation techniques for sensor measurement and distributed computation techniques for actuator parameters. The scalability of the network can be improved, for example, by organizing the sets of sensors and actuators into a hierarchical topology by forming groups or domains. These domains are controlled by a domain controller that is responsible for aggregating the sensed data and setting the actuator parameters within the domain. This domain controller also communicates with higher domains in the hierarchy. The overall operation of these sensors and actuators is optimized by the top level controller in the hierarchy.

Data collection mechanism from sensors should be able to support different applications (i.e., data should be reusable) [38]. As an example, to maintain effective demand–response in the generation side, information regarding the energy demand by consumers during peak hours (called *coincident peak demand*) is necessary. The same coincident peak demand information can be also used in the distribution network for load balancing. For this purpose, the same data should be tagged with location information such as substation name, bus and feeder number, and its voltage phase [38]. The location information helps to determine from which sector the peak demand is arising so that necessary flow of electricity supply can be maintained without tripping/overloading the transmission line. That means, even though the data collection requirements of smart grid applications vary in magnitude and time duration of monitoring, adding some network attributes to existing data output can change the use of the sensed data.

The sensed data should be encoded in a machine readable format so that it can be processed by the control centers automatically. Also, the sensed data should contain the temporal information including the timestamp (i.e., time that the data is collected from sensor) and duration with which the sensed data is valid. In addition, the identification of locations where the sensors are installed is important to determine the locations of the events (e.g., location of failure).

3.3. Requirements for communication networks

To transport the sensed data/control signal from/to the sensor and actuator, a communication infrastructure is required. The communication network will provide bidirectional flow of the sensed data (e.g., energy consumption, voltage sag, and current) from various devices (e.g., smart meter, voltage/current sensors, and transformers) to respective monitoring and controlling systems to provide continuous and reliable operation of the smart grid. Some of the requirements for the communication infrastructure for data sensing are summarized below [42].

- *Distributed operation*: because a large amount of data will be generated and processed in the smart grid, a traditional centralized communication architecture can create a bottleneck in the system. For instance, a PMU (i.e., a smart sensor that measures the electrical waves on an electricity grid) can generate up to 50/60 phasor measurements per second that can easily generate large amount of data within few minutes [43]. Transmitting all these phasor data in a centralized network can create a congestion easily, and a congestion control mechanism would be required [44]. Also, sensing nodes deployed in various locations of the power grid pose scalability challenges and present a need for decentralized aggregation techniques for sensor measurement and distributed computation techniques for actuator parameters [3,45,46]. Therefore, the communication network should be distributed with multiple processing and controlling units to avoid a single point of failure.
- *High bandwidth*: as new components are added into the network with the evolution of the smart grid, bandwidth requirement also becomes an important factor. Even for a power distribution system of moderate size, the bandwidth requirement is found to be very high (100 Mbps and above) [47]. This can be compensated by using optical fibers [47] or using Ethernet passive optical network [48] for data communication along the electrical transmission and distribution lines. However, using optical network is always costly in terms of initial installation.
- *Interoperability*: the communication network should be flexible such that it can communicate with different types of sensors and actuators seamlessly. Also, there should be a synergy between different communication technologies such as PLC, fiber-optic communications, and wireless communications.
- *Scalability*: the communication network should be scalable because of a large number of sensors and actuators in the network. It should have the plug-and-play capability to add or remove devices without the need for manual reconfiguration.
- *Security*: the communication network has to prevent the hackers' attacks such as false-data injection, network operation disruption, and denial-of-service attack. For example, in a meter-reading scenario, privacy and integrity of each load report should be protected, and it should not be eavesdropped or

revised by a third party. We will discuss the details of the security issues later in this article.

4. COMMUNICATION TECHNOLOGY, NETWORK ARCHITECTURE, PROTOCOLS, AND MIDDLEWARE FOR SMART GRID

In this section, we first describe the different technologies for sensor data communications in the smart grid. Then, we present a hierarchical network architecture and the networking protocols for the AMI. Last, we discuss the network middleware technologies for the smart grid.

4.1. Communication technologies

As has been mentioned before, for data communication, the smart grid will rely on different technologies such as PLC, fiber-optic communication, cellular wireless, IP-based communication, ZigBee, Wi-Fi, and WiMAX technologies. The choice among these technologies will depend on many factors such as cost, reliability, security, interoperability, geographic location, and availability. Because achieving all these requirements under a single communication technology is very unlikely, the smart grid will feature hybrid communication and access technologies.

Because of the ubiquitous presence of power distribution lines and associated advantage of low installation cost, PLC is likely to be widely adopted in the smart grid [49]. PLC is not only used in power distribution network but also used for short-haul communications of home automation, power network management, and last-mile communication in the smart grid [50]. The most common PLC technology uses single-carrier frequency-shift keying and binary phase-shift keying modulation techniques. Although this single-carrier technology is cheap and simple, it lacks the flexibility in selecting the carrier frequency and, hence, results in low throughput and poor reliability. Also, studies have shown that the characteristic of single-carrier PLC varies drastically with different geographical locations or number of network nodes. Also, its performance depends largely on system parameters (e.g., data packet size and response time [49,51]). Nevertheless, PLC can be improved using different approaches (e.g., single-frequency networking with flooding of message [49] and orthogonal frequency-division multiplexing [OFDM] modulation [51]).

In [49], the infrastructure requirements (e.g., network coverage and data flow, and quality-of-service [QoS] requirement) and transmission concepts (e.g., single-frequency network concept and flooding) are described for use in the smart grid. It is argued that to support large-scale control and automation of different switches, sensors, and meters in smart grid, PLC should fulfill the needs of adequate network coverage, *ad hoc* networking features, and QoS guarantee. New transmission mechanisms such as single-frequency network mechanism (i.e., using altruistic repeaters to transmit the same message simultaneously using the same frequency), flooding mechanism (i.e., using message flooding similar to the signal broadcasting in wireless communication), and hybrid medium access control (MAC) protocol are introduced. The hybrid MAC protocol is composed of random medium access (e.g., slotted ALOHA or carrier-sense multiple access [CSMA]) and deterministic medium access protocols (e.g., master–slave protocols and token ring protocol). By using a real field trial, it is shown that the combination of single-frequency networking with flooding embedded into a hybrid MAC protocol can improve the performance of PLC significantly [49].

Many other existing communication techniques such as code-division multiple access or OFDM-based access can be adopted in PLC to improve its performance. However, code-division multiple access is less robust to the frequency-selectivity problem. On the other hand, OFDM can provide better resistance to signal distortion and reliability to PLC [49,51,52]. In [51], it is shown that OFDM-based access can increase the reliability and throughput of the PLC.

Dispersed-tone PLC [53] is a type of PLC protocol that uses OFDM technology to transmit baseband data by selecting frequencies to avoid narrow band noise. Dispersed-tone PLC uses dispersed or plural tones to transmit data using differential binary phase-shift keying or differential quadrature phase-shift Keying modulation.

Further, recent research shows that combining different access technologies with broadband over power line (BPL) can improve the data transmission rate and QoS support for the smart grid communications. These access technologies could be either wireless (e.g., Wi-Fi or WiMAX) or wired (e.g., fiber or coaxial cable). This is referred to as the hybrid access technology. For example, a study shows that the integration of ubiquitous power distribution with Wi-Fi technology can enhance the reliability and reduce the cost of a broadband access network to be used for a power distribution network in the smart grid [52,54]. Specifically, BPL uses the medium voltage (MV) power line for signal transmission. BPL units are installed in various locations of the MV line to provide the functionality of a data aggregation point. Moreover, a BPL unit can act as the wireless interface gateway for converting the MV line signals to the Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g compatible signals. In this way, the BPL network can be transformed into a hybrid wireless-BPL network [52]. The field trial of this hybrid wireless-BPL network performed in [52] shows a considerable performance improvement on the 70-km MV power grid. Even though the PLC technology is still under development, the cost-effectiveness and ubiquitous presence of the power line infrastructure will make it one of the viable choices for providing distributed communications in the smart grid.

ZigBee is a low-cost, low-power, short-range wireless communications technology based on the IEEE

802.15.4-2003 standard for wireless personal area networks (WPANs). Because of its low cost, ZigBee is a viable technology to be widely deployed in wireless sensing, control, and monitoring applications for the smart grid. A ZigBee-based smart power meter is introduced in [55]. The proposed smart meter uses microcontroller (dsPIC30F series microchip) to perform necessary computations. The low-cost and low-power ZigBee system is integrated into the proposed smart meter that is used to transmit the power consumption information and outage statistics to a control center.

Long-range wireless communications technologies such as 3G cellular wireless, WiMAX, and 3GPP LTE technologies are also expected to be used for wide area networking and wireless backhauling for many smart grid applications. In addition, the evolving IEEE 802.22-based wireless regional area networking technology, which uses the cognitive radio (CR) concept, holds potential for long-range smart grid communications.

4.2. Communication network architecture

The data communication network infrastructures in the smart grid include AMI, wide area measurement systems (WAMSs), sensor and actuator networks (SANETs), HANs, NANs, and WANs.

- *Advanced metering infrastructure (AMI)*: AMI provides an automated communication system between a smart meter and a utility company (i.e., control center). All of the communications aspects of the smart grid will be handled by the AMI to provide a user-centric approach for managing the electricity usage in the smart grid. Various functions of smart grid can be implemented on AMI, for example, customer voltage measurement, consumer outage detection, hourly remote meter reading, remote meter programming, load control, and price signaling (e.g., TOU). The AMI will include a hierarchical network or a multitier architecture with star and mesh topologies and a variety of communication technologies such as PLC (e.g., BPL), cellular network (e.g., 3G, and 3GPP LTE), other wireless technologies (e.g., Wi-Fi, ZigBee, and WiMAX), and IP-based networking technologies. The AMI comprises of DAUs to collect and relay the information from the meter side to MDMS. The MDMS provides storage, management, and processing of meter data for proper usage by other power system applications and services [3]. A DAU connects a customer premise to a higher network entity in the smart grid such as the MDMS. The AMI will be comprised of many systems and subsystems such as WAMSs, SANETs that can be grouped under a hierarchical structure on the basis of HANs, NANs, and WANs as shown in Figure 3. The data control entity such as DAU and MDMS will act as a data sink to collect sensed data and also as a gateway to relay the data from one network hierarchy to another.

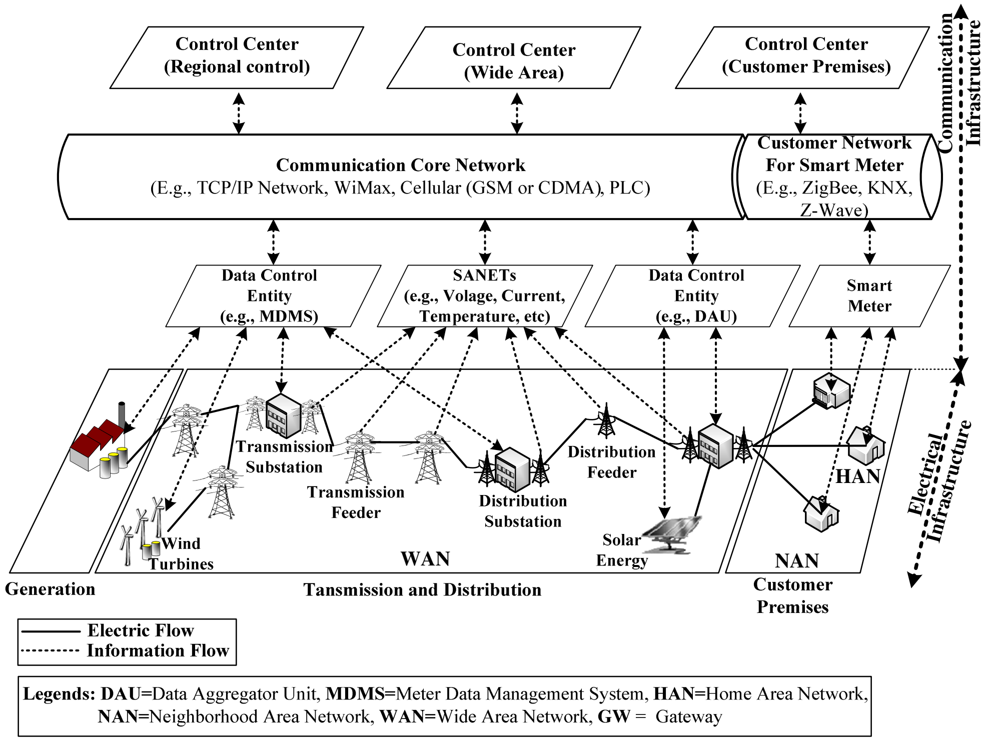

Control Center (Regional control)
Control Center (Wide Area)
Control Center (Customer Premises)
Communication Infrastructure
Communication Core Network
(E.g., TCP/IP Network, WiMax, Cellular (GSM or CDMA), PLC)
Customer Network For Smart Meter
(E.g., ZigBee, KNX, Z-Wave)
Data Control Entity (e.g., MDMS)
SANETs (e.g., Volage, Current, Temperature, etc)
Data Control Entity (e.g., DAU)
Smart Meter
Transmission Substation
Transmission Feeder
Distribution Feeder
Distribution Substation
Wind Turbines
Solar Energy
HAN
WAN
NAN
Electrical Infrastructure
Generation
Tansmission and Distribution
Customer Premises
Electric Flow
Information Flow
Legends: DAU=Data Aggregator Unit, MDMS=Meter Data Management System, HAN=Home Area Network, NAN=Neighborhood Area Network, WAN=Wide Area Network, GW = Gateway

Figure 3. Smart grid communication network architecture for data sensing and collection.

DOI: 10.1002/wcm

- *Wide area measurement systems (WAMSs)*: the key aspect of WAMS is to provide real-time (in order of milliseconds) monitoring and control of the electrical power grid to prevent any future contingency. The WAMS will be used to connect PMUs with wide area and dynamic coverage. The major advantage of WAMS over conventional SCADA and EMS that provide only local monitoring and control is the larger coverage. The WAMS can transfer sampled phasor data. This data is used to support various functions of the smart grid including state estimation, instability prediction, real-time monitoring, dynamic disturbance recording and data logging, analysis of power system dynamics, and analysis of damping/oscillation. In a typical WAMS architecture, multiple PMUs (i.e., sensors) are connected with a phasor data concentrator (PDC) through a regional network. This is referred to as the PMUs-PDC working group. A control center collects and aggregates phasor data from multiple PMUs-PDC working groups through a WAN (e.g., synchronous optical network/synchronous digital hierarchy) [56]. Because PMU performs continuous data sampling in real time (e.g., 16-bit resolution with 720 samples per second), congestion and delay are two critical issues in the WAMS [57]. Unlike SCADA, WAMS can monitor the power system state continuously and synchronously. WAMS support high sampling data rate, making WAMS suitable for the dynamic event management and failure recovery.
- *Sensor and actuator networks (SANETs)*: the various sensors and actuators installed in the grid can form SANETs [45] as shown in Figure 3. Through the SANET, the operational characteristic and behavior of the smart grid devices distributed along the grid can be monitored so that any outage or disturbance can be prevented and at the same time, effective DSM can be provided. The SANET can be formed using a hierarchical topology (e.g., cluster tree topology [58] or a linear topology [25]) or as a cooperative sensor network [59]. For example, an IEEE 802.15.4-compliant [60] sensor network can be used to implement wireless automatic meter reading, remote system monitoring, and equipment fault diagnosis [15]. The design and implementation of a cross-platform sensor network for transmission line monitoring are introduced in [61]. [62] introduces the sensor networks to monitor the conductor temperature and current of the overhead transmission line. The monitored parameters can be used to optimize the power transmission to maximize the ampere capacity (i.e., ampacity) of the overhead line meeting the reliability requirement under uncertain weather condition. In [63], the link scheduling algorithm is proposed for the WSN with tree topology, which is applicable for the transmission line monitoring. In particular, the multichannel assignment algorithm for the multimode hierarchical network is proposed. First, the network is formed in the hierarchical structure. Then, the channel assignment is performed for which the data forwarding is executed on the basis of the allocated channel. The objective is to improve the network throughput.

  Of particular importance in SANETs is the ability to set the actuator parameters depending on the values observed by the sensors so as to achieve a system-wide objective [45]. SANETs will also facilitate direct interaction between the public utility and the consumer [11]. Technologies such as the Internet, PLC, BPL, 3G/4G cellular, and WiMAX wireless communication technologies can accomplish this interaction. Note that the SANETs have to be optimized considering the unique communication characteristics (e.g., harsh environment of smart grid due to electromagnetic interference) and performance requirements (e.g., time-sensitive latency requirements, limited resources of memory, processing speed, and power supply, and the need of variable QoS).
- *Home area networks (HANs)*: a HAN is the smallest subsystem in the demand–response chain of the smart grid that provides dedicated DSM with the use of smart meters [5,64]. A typical HAN will consist of smart sensors and actuators to measure various parameters (e.g., light intensity and temperature), smart meter to sense and record electricity usage, in-home display for user interface, and a HEMS to optimize the energy usage based on real-time pricing information (Figure 4). Smart meter will also act as a gateway for public utility to access and retrieve electricity usage information for demand–response. Various wired technologies such as PLC, building automation and control network (BACnet), KNX protocol, and wireless technologies such as Wi-Fi, ZigBee, and Z-Wave can be used in HANs. The SANETs in the customer premises will constitute important solutions for HANs.
- *Neighborhood area networks (NANs)*: a NAN is a collection of multiple HANs to collect sensed data for aggregation. As shown in Figure 5, all the data from different HANs are collected at the data control entity (i.e., DAU in this case). The associated control center will monitor the amount of electricity distributed to a particular neighborhood to provide effective demand–response. The data control entity communicates with the smart meter by using network technologies such as PLC, fiber-optics, satellite, or WiMAX.
- *Wide area networks (WANs)*: a WAN connects multiple distribution systems together. A WAN will consist of variety of sensors (e.g., voltage sag sensors, PMU, and line temperature sensor) that will cover almost all the aspects of transmission and distribution lines to provide monitoring and control in the case of fault or outage. These distribution systems will also consist of data control entities (e.g., MDMS) that are used as hubs to collect all the sensory data. The collected data is then analyzed by respective distributed

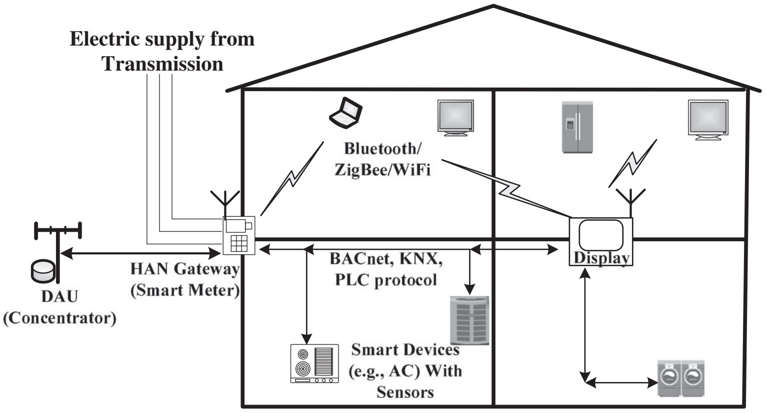

Electric supply from Transmission
Bluetooth/ ZigBee/WiFi
DAU (Concentrator)
HAN Gateway (Smart Meter)
BACnet, KNX, PLC protocol
Display
Smart Devices (e.g., AC) With Sensors

Figure 4. Home area network (HAN).

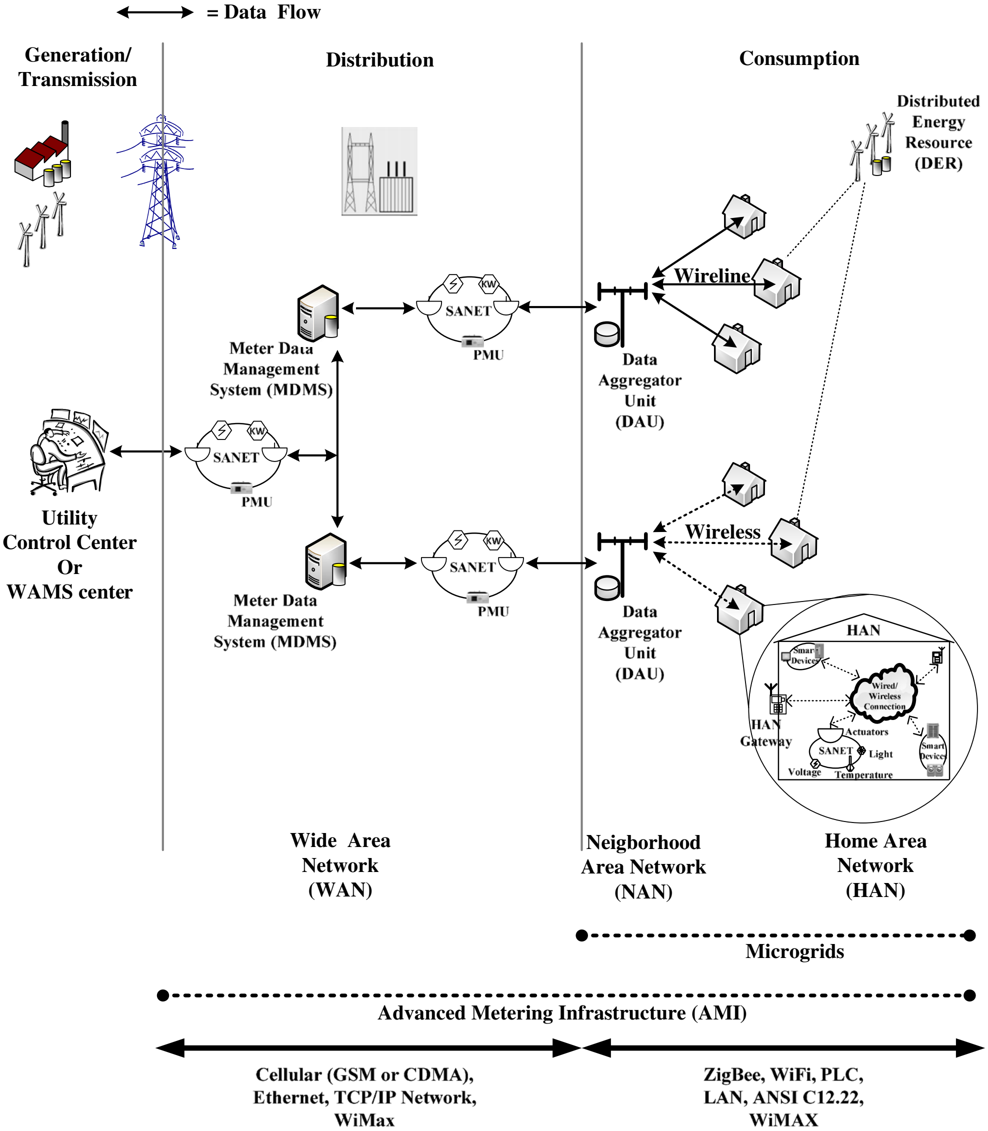

= Data Flow
Generation/ Transmission
Distribution
Consumption
Distributed Energy Resource (DER)
SANET
PMU
Meter Data Management System (MDMS)
Wireline
Data Aggregator Unit (DAU)
Utility Control Center Or WAMS center
SANET
PMU
Wireless
Meter Data Management System (MDMS)
SANET
PMU
Data Aggregator Unit (DAU)
HAN
Smart Devices
Wired/ Wireless Connection
HAN Gateway
Actuators
SANET
Light
Voltage
Temperature
Smart Devices
Wide Area Network (WAN)
Neigborhood Area Network (NAN)
Home Area Network (HAN)
Microgrids
Advanced Metering Infrastructure (AMI)
Cellular (GSM or CDMA), Ethernet, TCP/IP Network, WiMax
ZigBee, WiFi, PLC, LAN, ANSI C12.22, WiMAX

Figure 5. neighborhood area network (NAN) and wide area network (WAN).

control center for developing control algorithms. The WAN provides the backhaul communication infrastructure to connect all the entities within the smart grid. Various communication networking technologies such as PLC, fiber-optic, cellular wireless, the IEEE 802.22-based CR networks, and TCP/IP technologies can be used to connect all the functional subsystems in the smart grid WAN.

4.3. Networking protocols

The communication network for the smart grid should be self-healing, secured, efficient, interoperable, and scalable to handle a variety of applications. Also, it should support open standard with plug-and-play capability. An effective solution is to utilize IP-based network as the backbone communications infrastructure of the smart grid [65]. IP has many advantages over many other existing protocols as it is widely used in data networks, and also, many network technologies have a convergence layer for IP [66]. As discussed in [65], an IP-based network can ensure multicast traffic and reliable security within the smart grid. Almost every network technology can be integrated into an IP-based network. In this context, IPv6 protocol is identified to be a better choice than its predecessor IPv4 because of the new features (e.g., larger address space, mobility, and security services [66]). However, not all the existing network technologies have convergence with IPv6. A more flexible approach would be to use a mixed network of IPv4 and IPv6 as mentioned in [66]. However, this will require proper translation of network boundaries that could act as the initial transition for the shift to single IPv6 network (e.g., as implemented in Spanish GAD project [67]).

The traditional IP-based network is versatile but supports only best-effort packet delivery. That is, it does not ensure the QoS for data networking. However, the smart grid applications will require certain QoS guarantee in terms of latency, delay variation (jitter), bandwidth, and packet loss for efficient and reliable operation. Apart from the QoS, data networking in the smart grid should have proper security protection [42].

Different QoS-based services can be integrated into the IP networks to ensure the quality of data in smart grid. The Internet Engineering Task Force (IETF) has introduced many service models such as differentiated service (DiffServ), multiprotocol label switching (MPLS), and integrated services (InterServ) to meet IP QoS [68]. Among these, DiffServ and MPLS are used for providing IP QoS. DiffServ is a computer networking architecture that can be used to provide low-latency, QoS guarantee for critical network traffic, whereas providing simple best-effort service to noncritical applications such as web traffic or file transfer applications. DiffServ can be implemented in IPv4 as well as IPv6 to provide better QoS support. MPLS is also a standard technology for speeding up network traffic flow that integrates Layer 2 information about network links (bandwidth and latency) into Layer 3 (IP) within a particular autonomous system to simplify and improve QoS of IP packet exchange. Both these technologies are promising and can be used to provide necessary QoS support for smart grid. For instance, [68] introduces a way to provide QoS guarantee in International Electrotechnical Commission (IEC) 61850 substation automation protocol by using IPv6 DiffServ model. Also, the integration of MPLS and DiffServ can be used to meet the QoS requirements of data to be transmitted in the smart grid [69].

Over IP, the transmission control protocol (TCP) can be used as the transport layer protocol for wide area networking in the smart grid. However, TCP incurs considerable delay in data transmission and high network overhead [70] and also, because TCP lacks a mechanism to support real-time traffic, it might not be particularly suitable for services in the smart grid [70]. Moreover, it lacks of the multicast ability (to send a single packet to multiple destinations), which might be crucial for sending multiple control signals to many systems and devices in the smart grid in case of emergencies. For such applications, protocols such as real-time transport protocol running over the user datagram protocol (UDP) are usually recommended. UDP is a simple transmission protocol that is generally used for time-sensitive applications because it works without implicit acknowledgment and retransmission of messages. UDP has a smaller overhead in a message frame and also supports multicast but lacks a mechanism to support reliable packet delivery. Therefore, a combination of TCP and UDP can be used to provide reliable and ordered packet service in smart grid [70].

In a sensor networking environment (e.g., in a HAN), reliable data delivery is still an open research, and there has not been any standard transport layer protocol. An end-to-end transport protocol such as TCP may not be suitable for wireless SANETs in the smart grid because of its congestion control mechanism that was originally designed for wired networks and because of the very low data rate of the smart grid sensors, high header overhead, and energy efficiency reasons. For SANETs and HANs in the smart grid, transport protocols must be light-weight to support low-end sensors and actuators. The pump slowly fetch quickly (PSFQ) protocol [71] is designed for WSNs to provide reliable transmission under poor radio condition while using a light-weight signaling and a hop-by-hop error recovery mechanism. In PSFQ, a node requests retransmission from neighboring nodes once the packet loss is detected. Reliable multisegment transport [72] is another transport protocol for WSNs that uses both hop-by-hop and end-to-end error recovery for reliable data transmission. Unlike PSFQ and reliable multisegment transport, event-to-sink reliable transport [73] aims to achieve reliable *event detection* from each sensor nodes (not packets) and congestion control while minimizing energy consumption.

The performance of a transport layer protocol in the SANETs in the smart grid will depend on the underlying network and MAC layer protocols. There have been a plethora of data-centric routing protocols (instead of address-centric routing protocols such as IP) proposed for the WSNs in the literature that can be used to disseminate data from the sensor nodes to the sink node in energy-efficient manner, hence maximizing the lifetime of the network. The sensor routing protocols can be classified into the following major categories: flat routing (e.g., sensor Protocols for Information via negotiation (SPIN) [74]), hierarchical routing (e.g., Low-Energy Adaptive Clustering Hierarchy (LEACH) [75]), and location-based routing (e.g., geographic adaptive fidelity (GAF) [76]) protocols. Again, depending on the protocol operation, the protocols can be classified as follows: proactive, reactive, and hybrid protocols. On the basis of the channel access and collision resolution mechanisms, the MAC protocols for traditional WSNs can be classified into the following categories: contention-based (e.g., S-MAC [77]), contention-free (e.g., TRAMA [78]), and hybrid (e.g., Z-MAC [79]). Some of these routing and MAC protocols can be adopted for data sensing and communication in the smart grid environment. However, in general, besides the traditional design considerations (e.g., resource and energy constraints), issues such as harsh environmental conditions, stringent QoS requirements, scalability, and adaptability need to be taken into account for designing reliable and efficient routing and MAC protocols for the smart grid applications.

4.4. Networking middleware and application layer protocols

Networking middleware provides a higher level application interface that improves the interoperability, portability, and flexibility of data communication. It provides an interface between high level application QoS requirements and low level resource management such as bandwidth requirement and real-time data monitoring. Therefore, networking middlewares can be used to support interoperability of network protocols to meet the requirements of the smart grid.

GridStat [42] is a simple publish–subscribe middleware that can be used for acquiring the status variables and status alerts in the power grid. The status variables are the periodic measurements of status or control settings in the power grid. The middleware manages these measurements and ensures that it is up-to-date. The status alerts are used to inform applications of any failures or alarm condition with high priority. The QoS brokers are used to manage the resource allocation and to provide necessary path to deliver messages with proper QoS requirements. GridStat is being implemented by Avista Utilities in Washington on the basis of the SCADA system to acquire the necessary data directly from the sensors [42].

The Universal Plug and Play (UPnP) protocol$^{\mathrm{TM}}$ [80] is a device discovery protocol that supports zero configuration, transparent networking, and automatic discovery, and control of various kind of home network devices. The UPnP protocol provides data communication between any two or more devices under the command of UPnP control device or point in the network. The idea here is to shutdown the devices (or put to sleep state) when they are not in use for certain time and wake them up whenever necessary. Each device using the UPnP protocol advertises its power state, wake up status, and other general information periodically or as a response to UPnP control point search messages. The UPnP control point sends a multicast M-search message whenever it needs to access the particular device. The active devices are accessed directly and those in the sleep mode are waken up using the power management proxy. Using a test network, it is shown that by using the UPnP protocols, the average power consumption can be reduced drastically without compromising the usability.

5. EMERGING APPROACHES FOR DATA SENSING AND COMMUNICATIONS IN SMART GRID

In this section, we provide a survey on recent developments in data sensing and communications in smart grid. For sensing, we discuss three recent developments, namely, PMU, compressive sensing, and decentralized and cooperative sensing. Then, we discuss three main techniques used for data communications in the smart grid, namely, machine-to-machine (M2M) communications, relay-based cooperative communications, and cognitive radio (CR). To this end, we discuss the emerging MAC layer, network layer, and transport layer techniques for sensor data communications.

5.1. Techniques for sensing

5.1.1. Phasor measurement units.

Phasor measurement units (also referred as synchrophasors) measure the electrical waves, using a common time source for synchronization. A phasor is a complex number that represents both the magnitude and phase angle of the sine waves. Phasor measurements that occur at the same time are called *synchrophasors*, and the PMU devices can support these measurements. In typical applications, PMUs are sampled from widely dispersed locations in the power system network and synchronized using the common time source of a GPS radio clock. Synchrophasor technology provides a tool for system operators and planners to measure the state of the electrical system and manage power quality. Synchrophasors measure voltages and currents at diverse locations on a power grid and can output accurately timestamped voltage and current phasors. Because these phasors are truly synchronized, synchronized comparison of two quantities is possible in real time. These comparisons can be used to assess the system conditions.

A PMU can be a dedicated device, or the PMU functionality can be incorporated into a protective relay or other device. The IEEE Standard C37.118-2005 deals with issues concerning the use of PMUs in electric power systems. The specification describes standards for measurement, the method of quantifying the measurements, testing and certification requirements for verifying accuracy, and data transmission format and protocol for real-time data communication. Many applications of PMUs in power systems are given in the literature. A historical overview of synchronized phasor measurements is presented in [81]. The use of time synchronizing techniques, coupled with the computer-based measurement technique to measure phasors and phase angle differences in real-time, is reviewed in [82]. An important function of PMU is to observe voltage angle directly and independently of state estimation module. The analysis of power system observability using PMUs is conducted in [83–85].

5.1.2. Compressive sensing.

For the smart grid communication networks, the requirement of sampling and transmitting information from a huge number of sensors simultaneously would cast a significant challenge on the current state-of-the-art sensor networks. To overcome this challenge, a promising approach, named compressive sensing (CS), has been recently proposed [86–89], which combines the concepts of data acquisition, compression, dimensionality reduction, and optimization together. The fundamental principle of CS is that a K-sparse signal $\mathbf{x}$ of dimension N can be recovered from just a few incomplete measurements $\mathbf{y} = \mathbf{Ax}$ of dimension M via a L1-minimization optimization for certain types of random projection matrix $\mathbf{A}$. Surprisingly, the number of measurements M required when $\mathbf{A}$ is a Gaussian random matrix or Bernoulli matrix is just $M = O(K \log(N/K))$. It takes fewer measurements than traditional sensing and requires no additional compression. The cost is that the decoding process that reconstructs the original information from the *incomplete* measurements becomes a computational procedure. In other words, CS senses less and computes more. CS has attracted significant research attention and provides an effective approach to managing the high data bandwidth and information content. For many applications in the smart grid, such a shift of resource demands from pretransmission to posttransmission can be of great benefit [90].

5.1.3. Decentralized and cooperative sensing.

Electricity industry deregulation has led to the creation of many regional transmission organizations within a large interconnected power system [91]. Moreover, because a substantially large number of smart elements will be appearing in the grid, significantly more computational, processing, and communication resources will be needed. Consequently, increasingly more distributed information processing and control will be needed for power system operations [92]. For example, distributed state estimation methods have been considered for decades with the goal of reducing the computational burden at the central control center by distributing the tasks across the system. A simple but effective approach is decomposition-and-merge, which is essentially a two-level hierarchical method [93,94]. At the lower level, each local area independently runs its own estimator on the basis of its local measurements, whereas at the higher level, the central coordinator receives the state estimation results, with boundary measurements if necessary, from the individual areas and then combines them to obtain a system-wide solution. The *star-like* hierarchical methods have been also discussed in the recent literature [95,96]. More recently, a hybrid distributed state estimation method using the PMU measurements as well as the conventional measurements has been proposed [97–99].

5.2. Techniques for sensor communications

5.2.1. Machine-to-machine communications.

The concept of machine-to-machine communication has emerged to support pervasive communications among autonomous devices. M2M communication will be used to collect and transfer real-time data from various devices without human intervention. It can be used in the smart grid to achieve a hierarchical, robust, and efficient networking solution for different devices with presumably low processing capabilities. Wired, wireless, and hybrid communications technology can be used for M2M communication. IEEE 802.15.4 (ZigBee) and .15.4e/g/k, IEEE 802.11 (Wi-Fi), IETF 6LoWPAN (IPv6 over low-power WPANs), IETF ROLL, and IETF CoRE-based protocols will be typical for medium/short-range M2M communication networks. On the other hand, cellular wireless technology (e.g., 3G and 4G cellular and WiMAX) may be used for wide area M2M communications.

[100] provides a survey of different technologies to be adopted for M2M communications in the smart grid. These technologies are IEEE 802.15.3a-based ultra wideband, IEEE 802.11-based Wi-Fi, IEEE 802.15.1-based Bluetooth, and IEEE 802.15.4-based ZigBee technologies. Although ultra wideband and Wi-Fi consume more power for transmission and reception, they provide much higher transmission rates than Bluetooth and ZigBee.

In [101], the application of M2M communications in the HEMS is described. First, a network architecture is presented to collect the smart meter data. Meter data are transferred from houses to the concentrator and then relayed to the WAN base station. The base station transfers the collected meter data to the control center. The authors consider the problem of optimal traffic concentration. An optimal cluster formation algorithm is used to find the optimal location of traffic concentrator in a network.

A secure data aggregation protocol for a smart meter based on the M2M communications is proposed in [102]. The smart meter data is collected by the aggregator and then forwarded to the gateway. The end-to-end security in terms of confidentiality, integrity, and authentication is achieved by encryption carried out by smart meter using the same key as that of the gateway. The timestamp is embedded in a packet to provide the freshness information. Then, to improve the efficiency of meter data transmission, lossless aggregation based on a concatenation protocol is used to create a packet with optimal size while reducing unnecessary overhead. The performance of the protocol is evaluated based on the IEEE 802.15.4 ZigBee standard.

5.2.2. Cooperative communications.

Cooperative communications refer to the techniques in which multiple nodes help each other (e.g., in wireless mesh, *ad hoc*, and sensor networks) to relay or forward data packets to their destinations. In [103], a cooperative WSN is used to provide data transmission in urban-scale smart grid environment. The network is based on the IEEE 802.15.4 ZigBee standard. In this cooperative WSN, a number of ZigBee nodes work cooperatively to monitor electrical substations in an urban scenario. The network has one coordinator to control the data transmission of all nodes to the concentrator. In [104], a secure and reliable collaborative communication scheme for AMI is introduced. A multihop wireless network is used to connect smart meters with AMI to transfer meter data to a local collector. The trust services, data privacy, and integrity based on mutual authentication are developed with three processes, that is, initialization, meter-reading collection, and management message distribution. The initialization process is performed when a new smart meter requests to join the AMI. Once the smart meters join the AMI, a meter-reading collection process is performed. With the meter data, a management message distribution process is used for adjusting the electricity power generation, transmission, and distribution accordingly.

5.2.3. Cognitive radio (CR).

Cognitive radio techniques can increase the utilization and efficiency of radio frequency spectrum in wireless networks. With CR, the spectrum allocated to the licensed users (i.e., primary users) can be opportunistically and dynamically accessed by the unlicensed users (i.e., secondary users). To do so, intelligent algorithms will be implemented by the secondary users to avoid interference to the primary users, improve the transmission performance, and maximize the radio resource utilization. CR can be used for reliable smart grid communications in a cost-effective manner.

In [105], the application of the IEEE 802.22-based CR technology for the smart grid is explored. The IEEE 802.22 standard is designed to provide wireless access in the rural areas with a large coverage radius (up to 100 km). This can be achieved because of the use of the TV band that has favorable radio propagation characteristics. A dual-radio architecture for CR in smart grid applications is proposed for real-time data transmission. In this architecture, one radio interface is used for data transmission and reception, and the other radio interface is used for spectrum sensing. With a dedicated radio interface for sensing, the delay due to searching for available spectrum can be reduced. The performance enhancements in terms of flexibility due to soft capacity and system implementation, wide coverage area, fault tolerance, and self-healing due to the use of CR technique are highlighted.

For data sensing in the smart grid, a CR-based WSN using the 802.15.4 ZigBee standard is proposed in [106]. In this network, a coordinator is used to provide synchronization and control of data transmission, whereas a spectrum sensor is used to support frequency agility so that the transmission can be adapted on the basis of the wireless channel condition. In addition, the routing protocol for low-power and lossy network (LLN) [107] is modified to achieve highly reliable and low-latency data transmission. The protocol considers the asymmetric transmission capabilities and the limited battery power of the nodes. LLN is composed of many embedded devices with limited power, memory, and processing resources (e.g., sensors). These devices use wireless communications (e.g., IEEE 802.15.4, Bluetooth, low-power Wi-Fi, wired, or low-power powerline communication [PLC]) to transfer the application specific data.

A testbed and experimental system for using CR in the smart grid is developed in [105]. The testbed is developed on the basis of field-programmable gate array (FPGA), for example, Virtex-6 and Virtex-5 FX FPGA, to implement the physical and MAC layer functions. These functions include sensing a channel, transmitting and receiving data, and communicating with an external network via Ethernet. Independent component analysis (ICA) and robust principal component analysis (PCA) techniques are applied for data recovery in presence of interference. The proposed testbed is tested in a microgrid environment that requires near real-time data transmission to monitor the status of DERs and to collect smart meter data from houses and buildings.

5.3. Medium access control, routing, and transport protocols for sensor data communications

To support various smart grid applications with different traffic and QoS requirements, the MAC layer, network layer, and transport layer protocols in the smart grid network need to be optimized. For the MAC layer, the IEEE 802.14.5-based and 802.14.1-based protocols will be used widely in the smart grid sensor networks and HANs. In [108], these protocols are extended with QoS support (i.e., QoS-MAC) where the packet transmission is prioritized with different probability of channel access. In [109], the performance of the IEEE 802.15.4 MAC protocol for near real-time asset monitoring (i.e., condition monitoring in wind farms) in the smart grid is evaluated. A method to reduce the end-to-end delay and achieve service differentiation for the sensor nodes is introduced. This method is based on the assignment of different backoff parameters for different types of traffic and smart grid applications. However, because the IEEE 802.15.4 MAC is based on the CSMA with collision avoidance (CSMA/CA) mechanism, it could suffer from delay, loss, and high energy consumption because of packet collision. Alternatively, a tree-based time-division multiple access (TDMA) MAC protocol can be used for HANs in the smart grid [110].

For the network layer, the IP protocol (and in particular IPv6) will be adopted in the smart grid because of its openness, interoperability, scalability, and cost-effectiveness [111,112]. In [113], the technical requirements and consumer application standards for IP-based AMI network are reviewed. Then, different standards that could be integrated with IP-based AMI, including ANSI C12.22 (i.e., application layer messaging services) and session initiation protocol (SIP) (i.e., for maintaining data transfer sessions over multiple media stream), are listed. Because of the large address space of IPv6, every device in the smart grid can be assigned with a unique identification number, making the system deployment easier. In [111], an IPv6-based smart grid application is demonstrated. A particular smart home application is considered in which a smart meter can report meter reading to public utility over the IPv6 network. If there is an unexpected power shortage or surplus, the power price is adjusted, and the smart meter is notified so that the proper action can be taken at the consumer side. In [112], a QoS framework based on DiffServ model in IPv6 is developed for IEC 61850 (i.e., a set of united interfaces for substation automation system [SAS] in the smart grid). The IPv6 network is used to aggregate and transfer real-time data in SAS over TCP/UDP/IP protocol given the defined QoS service.

One major problem of using IPv6 over IEEE 802.15.4 MAC arises because of the small payload size in the MAC layer frame when compared with the minimum size of an IPv6 packet. This has led to the development of 6LoWPAN (IPv6 over low-power WPAN) protocol that basically provides a set of convergence (or adaptation) functionalities (e.g., fragmentation and IPv6 header compression) between IPv6 and the 802.15.4 MAC. 6LoWPAN will be adopted in data sensing and communications for the smart grid [107]. For example, 6LoWPAN is used along with PLC to provide a robust and reliable communication stack for smart metering, home control, or home area networking applications [114].

In [115], the implementation of a routing protocol, namely, the low-power and lossy network (LLN) protocol, for a large-scale AMI in the smart grid is presented. The LLN protocol is based on the directed acyclic graphs (DAG), which presents an abstraction of the network topology. [115] proposes to use the expected transmission time (ETX) as a routing metric, and a low-cost ETX measurement scheme is also introduced to accurately estimate the ETX metric. Then, an ETX-based rank computation method is used to construct DAG to support high reliability for unicast traffic in the AMI. In [116], a WSN based on LLN is implemented. In [117], the performance of LLN is evaluated in an outdoor smart grid substation network through simulations. With a local repair mechanism, LLN can recover from local link outage and achieve near optimal shortest path for data delivery. In [118], a mesh network architecture based on the LLN protocol is presented. The network is used to connect a smart meter with a radio so that the concentrator nodes in the vicinity can be discovered automatically for meter data transfer. This discovery is based on the connectivity detection and channel scanning procedures executed by a smart meter.

Note that there are some other routing protocols for the smart grid that are not directly based on LLN. For example, in [119], the distributed autonomous depth-first routing (DADR) protocol is proposed. This protocol is based on the distributed distance–vector routing that is able to adapt quickly to the link condition with minimum control overhead. In [120], a routing protocol for multichannel wireless mesh networks is introduced for multigate smart grid networks to improve the reliability, self-healing capability, and throughput performance. Such a routing protocol can be used in the home mesh network. The location information (i.e., from GPS) can be used to improve the routing performance [121].

[122] points out that a standard TCP protocol could suffer from excessive signaling messages and packet retransmissions. This is due to the fact that in the smart grid, each device may have one connection to the control center to transfer sensor and measurement data. Although the data rate of a device is low, a number of connections could result in a degraded network performance. To solve this problem, [122] introduces a traffic aggregation mechanism in the transport layer protocol. A TCP aggregator node is added into the network to split the connection between the device and control center. Then, the TCP aggregator collects and aggregates data from multiple devices and then forwards the data to the destination by using a fewer number of connections. It is shown that with this approach, the congestion and flow control can be performed effectively, improving the overall network performance. For the smart grid NANs, simplified application-cum-transport protocols based on the UDP, such as the constrained application protocol (CoAP) [123], can be also adopted. The advantages of CoAP are as follows: it includes light-weight web service functionalities and is interoperable with the HTTP protocol used in the Internet.

6. SECURITY FOR DATA SENSING AND COMMUNICATION IN SMART GRID

Security is a crucial issue to ensure the reliability and availability of smart grid applications [124]. Different attacks have been reported, which demonstrate the vulnerability of the smart grid. For example, [125] reports that the computer worm, called Stuxnet, has been spread into the SCADA system from Siemens, and as a result, the SCADA system performs suboptimally. This section summarizes the security vulnerabilities in sensor data communications and the impact of the vulnerability, and reviews the protection mechanisms.

6.1. Overview of vulnerability

The vulnerability of data sensing and communications arises at the different parts in the smart grid including the sensor nodes, the network devices, and the network protocols. The typical threats can be broadly categorized as follows.

- *Disclosure*: disclosure threat refers to an unauthorized access to the private and confidential data. For example, information about a smart meter (e.g., location and owner) can be stolen by an adversary (i.e., sensor vulnerability).
- *Deception*: deception threat refers to the injection of false data into the system. For example, false metering data can be transmitted by an adversary through a data aggregator to the public utility making wrong demand estimation and erroneous billing (i.e., network device vulnerability).
- *Disruption*: disruption threat refers to the interrupting the system from operating properly. For example, wireless transmission among appliance, smart meter, and HAN gateway can be interrupted by an adversary through jamming (i.e., protocol vulnerability).
- *Usurpation*: usurpation threat refers to the unauthorized control of the system. For example, a password of a smart meter can be extracted and the adversary can use this password to perform unauthorized access and modification to the smart meter firmware (i.e., sensor vulnerability).

Different threats will affect the confidentiality, integrity, authenticity, and availability of data sensing and communications in the smart grid. Disclosure threat will degrade the confidentiality of the system. Deception and usurpation threats lead to poorer system integrity and authenticity. Disruption threat degrades the availability of the system. [126] summarizes the importance of security requirements for different parts of the smart grid including data sensing and communication. For example, data acquisition (e.g., from PMU data for WAMS) has medium confidentiality requirement but high integrity, authenticity, and availability requirements.

The smart grid will rely on different data communication protocols for providing necessary bidirectional flow of information needed for reliable control and management of the entire grid. The security of these protocols against any cyber attack is a significant issue. The adversity of these cyber attacks can range from sending misleading data to the field device to sending tampered control and command messages to the device, which may result in overloading the grid. In particular, the use of standard communication networks such as TCP/IP networks poses security risk because they are prone to cyber threats. Security services such as IP Security (IPSec) can be used to minimize the vulnerability in these TCP/IP networks to some extent. IPSec helps to authenticate and encrypt each IP packet of a communication session.

6.2. Attacks to medium access control and wide area measurement system

Three major types of attacks to AMI can be summarized as follows.

- *Interrupting the measurement*: the aim of this type of attack is to make the smart meter inaccurately measure the demand. An adversary can stop the meter from measurement (i.e., disconnect meter). Alternatively, the meter can be forced to reserve the measurement (i.e., pretend that the consumer supplies power back to the grid).
- *Tampering stored data in smart meter*: a smart meter maintains a variety of data and information, for example, TOU pricing, log files, recorded power consumption, and estimated demand. Therefore, the storage is a target of attacks by adversaries. One of the approaches is to steal the password. As a result, adversaries can gain an access into the smart meter and change the data (e.g., recorded power consumption).
- *Modifying the network configuration and setting*: data transfer over a network is vulnerable to attacks. First, an adversary can reverse engineer the network protocol and intercept the communication. Then, on the basis of the knowledge of the protocol and network structure, the adversary can inject the modified traffic into the network between smart meter and public utility (e.g., modified power consumption data).

In [127], a test is performed on the aforementioned attacks (e.g., measurement interruption, password attraction, and communication interception), and it is demonstrated that the *energy theft* can be a serious threat to the AMI. In addition to energy theft, [128] analyzes the general attacks to the AMI and the consequences. For example, without proper authentication and authorization, an adversary can render the illegitimate network operation.

In [129], an assessment of the WAMS is presented from the security perspective. The risk and vulnerability of the WAMS can be summarized as follows.

- *Time source for synchronization*: because PMUs use GPS to provide time reference for each measurement, jamming can be used to alter the time reference, which could result in loss of data and unreliability.
- *Lack of authentication*: not all PMUs can support authentication for configuration. Therefore, the adversary can secretly install PMUs to inject false measurements into the WAMS.
- *Lack of security monitoring and defense*: both PMU and PDC do not have the ability to detect, prevent, and recover from cyber attack. An adversary can perform an attack to interrupt the measurement of PMU or data transfer of PDC.
- *Implicit trust*: the WAMS is assumed to be deployed and operated in a trusted environment. Therefore, there is no explicit authentication, authorization, and access control for data transmission (e.g., C37.118 or IEEE 1334 standards). The state estimation can be manipulated, which leads to the disruption of the power system.
- *Integration of different technologies*: because the WAMS will be an integration of different data

communication technologies (e.g., synchronous optical network, satellite, and wireless network), the integration point can be vulnerable to an attack. A unified protection across the entire WAMS would be required in this case.

[129] suggests some solutions to enhance the security of the WAMS. For example, the use of a virtual private network (VPN) is recommended, which can provide the authentication and encryption capabilities for WAMS devices and data (e.g., by using IP Security [IPSec]). An experimental study on the WAMS security particularly due to the attack on the PDC is performed in [130]. The vulnerability of PDC is due to the lack of encryption in the protocol and the verification of data from the PMU. The PDC used in the study is the OpenPDC platform developed by the TVA (Tennessee Valley Authority) [131]. OpenPDC is an open source PDC application and is able to manage timestamped streaming of phasor data. The study reveals that an SQL-based database injection attack can lead to false measurement and unstability of the power system.

6.3. Protection approaches

For secured data sensing and communication, a systematic mechanism for threat detection and prevention would be required. A number of works in the recent literature introduce different protection schemes, especially for the AMI and the WAMS.

For AMI security, an intrusion detection system (IDS) is proposed in [128]. A specification-based IDS is recommended because of high accuracy of detection and lack of historical attack data. In addition, specification-based IDS requires only small number of protocols and applications to monitor the AMI and hence results in lower cost of deployment, implementation, and maintenance. Then, a monitoring architecture is introduced for the AMI with the use of sensors reporting to the centralized management server. For scalability, a distributed architecture is also mentioned in which the sensors have the capability to perform some data processing. Accordingly, various types of sensors for different types of monitoring, including stateful specification-based, stateless specification-based, and anomaly-based monitoring, are introduced. However, the performance of the proposed AMI monitoring architecture is not evaluated.

In [104], an in-network collaborative scheme is proposed to improve the security and reliability of AMI. Data privacy and integrity through mutual authentication of a smart meter are the key features in this scheme. In addition, message authentication is used to meet data integrity and confidentiality requirements of AMI. The in-network collaborative scheme has three processes, that is, initialization, meter-reading collection, and message distribution processes. For meter-reading collection and message distribution processes, encryption and digital signature are used to achieve confidentiality and integrity.

In [132], the tradeoff between meter data confidentiality and integrity (achieved through redundant transmission) is investigated. Then, a scheme is introduced to encode the redundant meter data (i.e., measurement) at the bit rate lower than its entropy to avoid decoding from the encoded bit alone (i.e., using Slepian–Wolf codes). In this case, the reported measurement has to be used together with redundant measurement such that the compression rate is higher than the conditional entropy of the redundant measurement given the reported measurement. As a result, the confidentiality can be ensured. The advantage of this approach over the encryption is that the confidentiality can be guaranteed regardless of the capability of the eavesdropping adversary. In [133], an efficient message authentication scheme is proposed, which can provide the nonrepudiation (i.e., proof of the integrity and origin of data) services. The objective is to minimize the number of digital signature operations to reduce the power consumption of a device. In the scheme, a smart meter generates two secret keys for authentication with an AMI server. One of them is kept with a smart meter and it is referred to as the nonrepudiation key, which ensures that the server cannot refuse to send or receive meter data. Another key is sent to the AMI server. Similarly, an AMI server generates two keys and performs the key exchange. With this process, the adversary is unable to recognize the keys from both the smart meter and the AMI server, and therefore, cannot generate false data.

[134] presents an experimental study on energy consumption of different WAMS security algorithms (i.e., cryptography algorithms). The study is performed on the widely used CrossBow and Ember sensor nodes. The algorithms considered in the study are SHA-1, RC5, DES, and AES. Also, combinations of these algorithms under different key sizes are evaluated. The performance in terms of energy consumption (i.e., from CPU and RF module) is measured and compared. Then, a code optimization method is introduced to increase the energy efficiency. Specifically, the AES algorithm is optimized on the basis of the lookup table and loop unfolding operations. By analyzing the results, the guidelines for security algorithm selection and configuration are introduced on the basis of the balance of energy, security, and time. One of the proposed guidelines is that RC5 algorithm should be used because of low energy consumption.

[135] presents a design for the WAMS in a multimachine power system (i.e., four machines in two areas are considered) with an objective to improving reliability, integrity, and security. Reliability is achieved through sensor fault tolerance. Intrusion detection system and integrity check module are also employed at the communication nodes. The integrity check module compares inputs from different sensors. If there is a difference in their values, an intelligent algorithm will estimate and make a decision about the system state. If the discrepancy is significant, the error will be reported for further maintenance. [136] presents a game theoretic model to denial-of-service (DoS) attack in a remote state monitoring system of the smart grid. The jammer can jam the wireless data transmissions

from the sensors. To avoid jamming, a sensor node can switch among multiple channels. A zero-sum stochastic game is used to model such a situation and the Nash equilibrium is obtained. The existence of Nash equilibrium and its computation are also discussed.

A summary of the different security schemes for the AMI and the WAMS can be found in [128] and [134], respectively.

7. STANDARDIZATION ACTIVITIES

To address the smart grid sensor data collection and communication needs, an important aspect is to decompose the existing electrical grid and its underlying standards and technologies into logical parts such that the specific technology could be applied to fulfill the exact requirements of the sensing systems [137]. Many standard development organizations (SDOs) such as ANSI, IEC, IEEE, the International Organization for Standardization (ISO), and the International Telecommunication Union (ITU) are working toward developing the smart grid standards. Also, independent organizations (IOs) (e.g., National Institute of Standards and Technology [NIST] [138], Electric Power Research Institute [EPRI] [139], and U.S. Department of Energy [140]) and alliances (e.g., ZigBee Alliance [141], HomePlug Power Alliance [142], and Z-Wave Alliance [143]) are working with SDOs to promote the standard technologies for the smart grid. This standardization process will achieve interoperability, enabling information exchange and understanding between different components of the smart grid.

Among these SDOs, IOs, and alliances, NIST is comprehensively working on developing an interoperable framework among all the consumers, manufacturers, energy providers, and regulators with special attention to standards in the field of communication protocols and data models. NIST has already issued its first version of interoperability framework [5], which contains recommendation and guideline for 25 core standards and additional 50 standards (some are under review) that can be used for the smart grid development. The NIST framework of standards has been adopted by many other national and international smart grid initiatives as the foundation to build their own smart grid. In this section, we highlight some of the standards for smart grid data sensing and sensor networking, core communication network and customer premise network based on the NIST framework. However, these standards are neither exhaustive nor exclusionary and should not be treated as the final recommendation for the smart grid development. Instead, the NIST standard list provides a guideline to adopt the smart grid technologies.

7.1. Sensor network standards

Table I lists some of the standards that can be used for the smart grid sensor networks. For instance, the IEEE 1451 [144], a family of smart transducer interface standards for sensors and actuators, describes a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control networks. The key feature of these standards is the definition of transducer electronic data sheets. Transducer electronic data sheet is a memory device that stores information about transducer such as transducer identification, calibration, correction data, measurement range, and manufacture-related information. The IEEE 1451 provides a common interface to access a variety of data from transducers connected to

Table I. Smart grid sensor network standards.

Standards	Description
IEEE 1451	A family of smart transducer interface standards for sensors and actuators; describes a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control networks
IEEE 1588	Standard for time management and clock synchronization across the smart grid for equipment needing consistent time management
IEEE C37.118	Open and widely implemented standard that defines phasor measurement unit (PMU) performance specifications and communication requirements
IEEE 1547 Suite	This standard defines physical and electrical interconnections between utility and distributed generation (DG) and storage.
IEEE C37.2-2008	Standard for power system device function to protect circuit device modeling numbering scheme for various switchgear
IEEE C37.111-1999, Common Format for Transient Data Exchange (COMTRADE)	Open standard to facilitate monitoring of instabilities in the power grid using transient data from power system monitoring, including power system relays, power quality monitoring field, and workstation equipment
IEEE 1159.3	Recommended practice and applications for the transfer of power quality data in the electrical grid
IEEE 1379-2000	Substation automation for intelligent electronic devices (IEDs) and remote terminal units (RTUs) in electric utility substations

systems or networks via a wired or wireless means. Moreover, for data sensing and communication, the time requirements and synchronization for measuring and controlling the system parameters are becoming increasingly stringent and can range from 1 μs at critical sites to 1 ms at most loads. For this, NIST has recommended the IEEE 1588 standard [145], which defines a protocol enabling precise clock synchronization in measurement and control systems implemented with technologies such as network communication, local computing, and distributed objects. The IEEE 1588 protocol will help to enable system-wide synchronization among the heterogeneous systems by providing clock of various precision, resolution, and stability.

7.2. Standards for core communication networks

Table II provides a list of standards that can be used to provide all the necessary backbone and core networking functionalities for effective two-way communications in the smart grid. Among these, the IP suite has the most potential to be used in the core communication network of the smart grid becauase of its convergence layer for many wired and wireless networking technologies [5,66]. Many applications of IP-based networking are emerging such as those using digital routers with IP addressing for sending the packets over transmission line [146], using cloud computing concept that provides specific Internet-scale characteristics (e.g., interoperability, ease-of-use and extensibility, and distributed and parallel data management techniques) [147], using IPv6 framework for industrial monitoring and home automation system [148], and using Internet-based virtual private networks as the core network [149,150]. The European research project REMPLI [150] is an example, where the IP-based private network in conjunction with PLC has already been in use for providing core network functionalities for smart grid.

Similarly, the IEC 61850 standard can be used in automation system for transmission and distribution networks. The IEC 61850 standard is an open standard that is now being extended for communications between substations including DERs. Because of its flexible object modeling feature, IEC 61850 can provide high-speed, multicast, and peer-to-peer messaging functionalities required for communication backbones. Also, it is widely adopted and recommended by the IntelliGrid architecture [151].

Similarly, standards such as the common information model IEC 61970 [152] and its extension IEC 61968 [153] can be used for mapping and integration of smart grid systems. Both the IEC 61970 and the 61968 standards define guidelines and specifications of application program interface for EMS and for information exchange between electrical distribution systems. The IEC 61970 standard includes information associated with control center applications (e.g., EMS and SCADA), whereas the IEC 61968 standard extends common information model to include distributed management system functions such as asset management and outage management. The semantic model helps to understand the context of the data, which is beneficial for better system design and data processing [154]. This in turn helps to design a specialized protocol for a particular data type that is independent of underlying communication technologies and may eventually permit true plug-and-play capability of utility software applications.

Table II. Smart grid core communication standards.

Standards	Description
Internet Protocol Suite, (IPv4 and IPv6)	The foundation protocol for delivery of packets in the Internet network; IPv6 is a new version of the Internet protocol that provides enhancements to IPv4 and allows a larger address space.
IEC 61850 Suite	Widely adopted and recommended by IntelliGrid architecture, which defines communication structure within transmission and distribution substations for automation and protection
IEC 61968/61970 Suites, Common Information Model / Generic Interface Definition	These families of standards define information exchange among control center systems by using common information models. They define application-level energy management system interfaces and messaging for distribution grid management.
Distributed Network Protocol (DNP3)	Utility automation nonproprietary protocol that provides communication between consumer portals and distribution substations or operations centers using serial communications
IEC 60870-5-104 Telecontrol over TCP/IP	Provide SCADA type service for distribution automation by using telecontrol over IP for communication between consumer portals and distribution substations
IEC 60870-6 / TASE.2, Inter-Control Center Protocol (ICCP)	Provide data exchange over wide area networks (WANs) between utility control centers
IEEE P2030	Guide for smart grid interoperability of energy technology and information technology operation with electric power system (EPS) and end-use applications and loads

7.3. Standards for customer premises networks

Customer premises networks can be used to connect various sensors and actuators inside the customer premises (e.g., home, building, and industry) to provide effective DSM and energy management. Table III provides a list of standards that can be used inside a HAN for connecting various home appliances for providing effective energy management services. Technologies such as BACnet [155] and KNX [156] provide efficient and cost-effective home automation solutions that are based on PLC. Both BACnet and KNX standards combine a multitude of proprietary protocols that have been developed for home automation [6]. BACnet is published by ANSI and the American Society of Heating, Refrigerating and Air-Conditioning Engineers. KNX is the European standard equivalent to BACnet, which is administrated by Konnex Association [156]. Similarly, HomePlug [142] is specifically designed as a standard for supporting high-speed (i.e., ranging from 10 Mbps to 600 Mbps) home networking for broadband applications such as in-home distribution of TV, gaming, and connection to the Internet. HomePlug, with recent integration to IEEE 1901 standard [157] (i.e., standard for BPL networks defining medium access control and physical layer specifications). ZigBee/HomePlug Smart Energy initiative provides a common application layer enabling interoperability between HomePlug and ZigBee technologies.

Similarly, new and emerging protocols such as ZigBee [141] and Z-Wave [143] can provide alternative wireless communication solution for connecting various smart appliances within the HAN for EMS. ZigBee is a standard, whereas Z-Wave is a a proprietary wireless standard developed by Zensys A/S [158]. Both of these protocols can be used for connecting various sensors, monitors, and control devices with low power, low latency, and low cost. ZigBee (250 kbps) provides slightly higher data speed in contrast to Z-Wave protocol (9600 bits/second). However, Z-Wave uses sub-GHz band (900 MHz) instead of the overcrowded 2.4 GHz Wi-Fi band, thus making it immune to Wi-Fi interference with even higher propagation range up to 2.5 times of the 2.4 GHz signal. An important feature of ZigBee is that it offers a wide range of routing algorithms with explicit functions for automatic plug-and-play capability, whereas Z-Wave is based on source routing that does not support automatic entering and leaving a network.

Besides these communication protocol standards, there are guidelines, which define specific requirements for adopting any proposed standard. For example, the OpenHAN [159] task force has defined an OpenHAN system requirement specification containing the minimum system requirements that are necessary to facilitate a

Table III. Smart grid standards for home area networks.

Standards	Description
ANSI/ASHRAE 135-2008/ISO 16484-5 BACnet	Defines information model and messages for building system communications at a customer's site; BACnet incorporates a range of networking technologies for providing common language for different proprietary protocols.
ISO/IEC 14543-3 KNX	KNX is the European standard equivalent to BACnet, which ensures that all components within home area network (HAN) communicate via one common language for providing home monitoring and control.
HomePlug AV	Entertainment networking content distribution for consumer electronic equipment
HomePlug C&C	Control and management of residential equipment for whole-house control products: energy management, lighting, appliances, climate control, security, and other devices
IEEE 802.15.4 ZigBee	Short-range, low-power wireless network that is designed specifically for industrial and home automation for connecting sensors, monitors, and control devices
ZigBee/ HomePlug Smart Energy Profile	Strategic alliance of ZigBee and HomePlug to provide communication and information model in HAN
Z-Wave	A proprietary wireless standard designed for home control automation, specifically to remote control applications in residential homes
OpenHAN	A specification for HAN to connect to the utility-advanced metering system including device communication, measurement, and control.
OpenADR	The specification defines messages exchanged between utilities and commercial/ industrial customers for price-responsive and direct load control.
ISO/IEC 18012	Specifies requirements for product interoperability in the home and building automation systems
IEEE P1901	Broadband communications over powerline medium access control (MAC) and physical layer (PHY) p protocols for HAN and also access application
ITU-T G.hn/G.9960 Home Networking Standard	Defines in-home networking over power lines, phone lines, and coaxial cables

DOI: 10.1002/wcm

viable, robust, and competitive HAN market. Similarly, ISO/IEC 18012 also defines the guidelines and requirements for product interoperability used in HANs. On the commercial application side, a set of standards known as Open Automated Demand Response Communication Standard is published by the Lawrence Berkeley National Laboratory for specifying a low-cost communication infrastructure to improve the reliability, repeatability, robustness, and cost-effectiveness of demand–response in commercial buildings.

Despite these standardization initiatives, the interoperability issue among different standards still exists. As a result, the public utility is either being forced to commit to a particular technology or to provide a service only to those customers who already have a proper infrastructure to support these technologies. Therefore, it is necessary to include interoperability tests or guidelines while designing any standard for the smart grid. In this regard, besides SDOs, IOs, and alliances, the dedicated user groups are required, which identify interoperability challenges (requirements), write the tests to validate products, and certify those results. Also, there should be involvement from governments and governmental agencies to define certain rules, regulation, and incentives for adopting these new technologies.

EPRI's IntelliGrid initiative creates the IntelliGrid architecture, an open standard, requirement-based approach for integrating data networks and equipment that enables interoperability between products and systems. The main objective of this program is to provide the methodology, tools, and recommendations for standards and technologies when implementing systems such as advanced metering, distribution automation, demand–response, and wide area measurement. A brief summary of viable technologies for use in the smart grid is listed by IntelliGrid Consortium as IntelliGrid Consumer Portal Project [160], using the methodology developed in the original IntelliGrid architecture project. It evaluates the existing communication technologies on the basis of IntelliGrid evaluation criteria (e.g., level of standardization, openness, adoption, security, scalability, and manageability). These criteria are organized according to the core network, security, network management, data structuring and presentation, WAN, and local area network (LAN) technologies, power system operations, and consumer applications. However, this technological assessment is not a final recommendation and should be considered as a viable solution while designing the data communication infrastructure for the smart grid. Similarly, the GridWise Architecture Council (GWAC) [161], a team of industry leaders, operates to promote and enable interoperability among the many entities that interact with the electric power infrastructure. As a step in the direction of enabling interoperability, the GWAC proposes a context-setting framework to organize concepts and terminologies so that interoperability issue can be identified and debated and actions can be coordinated across the electric power community.

8. USE CASES OF SMART GRID SENSOR DATA COLLECTION AND COMMUNICATION

Efforts related to the implementation of data sensing and communications are summarized as the use cases. Here we describe two such use cases.

8.1. GridWise interoperability context-setting framework for residential demand–response

This use case is presented by the GWAC [161] to illustrate the use of GridWise interoperability context-setting framework [162] for possible future deployment of residential demand–response programs and AMI in California, U.S.A. This use case considers a fictional scenario where a customer wants to register in residential demand–response program to reduce the power bill [162]. For this, the California public utility office installs an EMS and also dispatches a package with instruction on how to set the energy manager controller so that the customer can register in a demand–response program to reduce the energy consumption. The package contains a kind of barcode that can enroll the customer in a demand–response program. This program not only helps the customer to manage the electricity usage more intelligently but also at the same time notifies the users of any occurrence of critical peak price or any emergency situation so that they can adjust their electric usage on the basis of the available options.

However, to provide all these functionalities, the public utility office requires stable communication infrastructure to transfer information to/from customer premises. The smart meter is equipped with ZigBee transceivers for providing wireless networks to communicate with the public utility office through a home communication gateway. The barcode on an installation package actually contains a radio frequency identification transmitter that contains all the detailed information of that particular customer. The controller transmits this information over to the smart meter using the ZigBee link. The simple object access protocol is used to provide syntactic interoperability among the format and structure for encoding information exchange between controller and throughout the AMI network. The AMI network is implemented using an IP-based network so that the same utility could use the same back-office systems to communicate over other networks.

8.2. The Electric Power Research Institute smart grid demonstration: integration of distributed energy resources

The EPRI Smart Grid Demonstration initiative is a 7-year international collaborative initiative demonstrating the integration of DER in almost 21 operational utility industries (e.g., American Electric Power, FirstEnergy, Salt River Project, and Southern California Edison) [163].

Communications and Standards	**American Electric Power**	**Con Edison**	**Duke Energy**	**Electricité de France**	**ESB Networks**	**First Energy**	**Exelon (ComEd /PECO)**
Customer Domain (e.g., SEP, BACnet, HomePlug, WiFi, etc.)	▨	▨	▨		▨		▨
Transmission & Distribution (e.g., IEC 61850, 60870, DNP3)	▨	▨	▨		▨	▨	▨
Operations Domain (e.g., IEC 61968/61970, MultiSpeak, OpenADR)	▨			▨	▨		▨
AMI or AMR	▨		▨		▨		▨
RF Mesh or Tower	▨				▨	▨	▨
Public or Private Internet		▨	▨	▨	▨		▨
Cellular Based (3G): (e.g., 1xRTT, GPRS, EVDO, CDMA)	▨		▨		▨		
WiMAX (4G): (e.g., WiMAX (IEEE 802.16), LTE)			▨				

Figure 6. Use of communication protocols and standards in Electric Power Research Institute's smart grid demonstration projects.

The initiative began in 2008 and focuses on integrating distributed and renewable energy generation, demand response, energy storage, and customer-side technologies into a *virtual power plant* for efficient and cost-effective deployment of the power transmission and distribution systems. The main objective of this initiative is to help the utility industries to understand the different procedural and technical requirements. These include standard development that will facilitate widespread deployment and integration of distributed resources [163]. EPRI's IntelliGrid methodology is used to define requirements for the technologies, communication, information, and control infrastructure that supports integration of DER. Currently, most of the projects are in the deployment phases, and the initial planning, deployment, data collection, and analysis are being used to understand the full range of standards and interoperability requirements needed to support the industry.

For specifying the requirements for communication and control of DERs, EPRI IntelliGrid architecture is used to develop the use cases. For each demonstration project implemented, interoperability assessments are conducted on the basis of the data collected through the deployment. Moreover, these demonstration projects include the design and demonstration of a unified communication infrastructure to link regional power transmission and distribution operations and customer premises to utility control centers. Figures 6 and 7 summarize[†] the communication protocols and standards considered to be used in EPRI's smart grid demonstration projects [163]. The grey shaded regions in these figures illustrate the communication standard used in that particular project. For instance, Con Edison project targets the development of interoperable protocols and software to leverage multiple types of customer-owned DER along with integration of renewal generation and commercial building demand response [163]. Thus, it is important to connect the public utility and the demand–response resources. For this, Con Edison deploys and tests a number of communication standards, protocols, and specification such as GridAgent framework, IEC 61850, IEEE P1547.3, IEEE 1451, and ZigBee. These standards are considered on the basis of the requirement and preliminary analysis of the use cases developed in conjunction with EPRI's IntelliGrid methodology. Similarly, the objective of Duke Energy Smart Grid Demonstration project is to optimize DERs to achieve efficient customer program for reliable grid operation [163]. To achieve this objective, Duke Energy plans to install 40 000 smart meters for customers and 8000 communication nodes at transformer, and distributed automation including line sensors. For connecting the smart meters, communication nodes, and sensors, the project plans to use commercial cellular networks. Also, the project will use Smart Energy Profile in wireless and PLC application for communication and also for HEMS. The choice of communication standards and protocols used in these demonstration projects will depend on the main objective of the project being implemented.

9. OPEN ISSUES AND CHALLENGES

In this section, we outline several open issues and challenges related to smart grid sensor data collection and networking.

[†] Note that AMR stands for automated meter reading.

Communications and Standards	**Hydro Québec**	**KCP&L**	**PNM Resources**	**Sacramento Municipal Utility District**	**Southern California Edison**	**Southern Company**
Customer Domain (e.g., SEP, BACnet, HomePlug, WiFi, etc.)	▨	▨	▨	▨	▨	▨
Transmission & Distribution (e.g., IEC 61850, 60870, DNP3)	▨	▨	▨	▨	▨	▨
Operations Domain (e.g., IEC 61968/61970, MultiSpeak, OpenADR)	▨	▨	▨	▨		▨
AMI or AMR	▨	▨	▨	▨		▨
RF Mesh or Tower	▨	▨		▨	▨	▨
Public or Private Internet	▨	▨	▨	▨	▨	▨
Cellular Based (3G): (e.g., 1xRTT, GPRS, EVDO, CDMA)		▨	▨	▨	▨	▨
WiMAX (4G): (e.g., WiMAX (IEEE 802.16), LTE)	▨				▨	

Figure 7. Use of communication protocols and standards in Electric Power Research Institute's smart grid demonstration projects (continuation).

- *Secure data sensing and communications*: data sensing and communications in the smart grid may become the point of intrusions, malicious attacks, and other cyber threats. Using public networks (e.g., cellular network and Internet) could result in vulnerability to many threats. Therefore, an alternative to secure the smart grid is to use private networks for communications [164]. Nevertheless, this approach may not always be economical and efficient. A hybrid approach may be considered in which some noncritical applications in the smart grid (e.g., meter data collection) are based on public networks, whereas critical and security sensitive applications (e.g., fault detection) are based on a private network.
- *Bad-data detection*: in power system state estimation, *bad data* resulting from large measurement bias, drifts, or wrong connections need to be detected and identified. Because of the importance of state estimation, it is also possible that bad measurement data are injected by the attackers, which can endanger the smart grid. Some strategies from the attackers' and defenders' perspectives have been studied in recent literature [165–168].
- *Cross-layer optimization of smart grid communication protocols*: to satisfy the reliability, availability, and scalability requirements of data transmission in a lossy and complex smart grid environment, robust communication protocols need to be designed (e.g., for SANETs and M2M communications) on the basis of cross-layer (e.g., MAC, routing, transport, and application layer) optimization.
- *Improved device technologies*: advanced technologies and mechanisms (e.g., for low-power consumption and power harvesting) for sensor and actuator devices will be required to improve the energy efficiency and hence the lifetime of these devices. The effect of these mechanisms on the communication and networking performance will then need to be analyzed.
- *Cost optimization of network design*: prior to deploying network infrastructure for data sensing and communications, a cost–benefit analysis should be performed to quantify the usefulness and risk of available technologies. Cost is due to not only the equipment installation and maintenance but also the performance such as latency, loss, and bandwidth. Therefore, for an optimal design of the data communication network, the performance metrics should be analyzed thoroughly to develop a cost-aware network infrastructure and data protocols. For example, using CR technique may save the cost for wireless bandwidth. However, it may incur packet loss because of interference and also result in delay. Therefore, the tradeoff of using CR and dedicated wireless channel must be investigated to minimize the total cost.
- *Quality-of-service (QoS) framework*: different smart grid data to be sensed and transferred can be sensitive to delay, error, and loss. For example, electric power supply may be suboptimal if the smart meter data is lost, or the power substation may fail if the notification of cooling system fault is not reported on time. Therefore, the QoS framework or QoS broker [42] for data sensing and communications for the smart grid has to be developed. The QoS metrics have to be defined for different smart grid applications. The service level agreement will need to be defined accordingly. Therefore, the QoS framework

or QoSservice level agreement in the sensing and communications infrastructure need to be developed. These mechanisms include multiple access, packet scheduling, congestion control, error detection, and recovery. Also, the analysis and optimization of the developed mechanisms need to be performed [169].

- *Reliability analysis*: reliability of the data sensing and communication infrastructure needs to be systematically analyzed. The dependability of components used in data sensing and communications has to be investigated. For this, fault tree analysis and dependability diagram can be applied [56]. In the reliability analysis, the impacts of different attacks performed by the adversaries have to be taken into account. To improve the reliability of the data sensing and communication infrastructure, fault-tolerant design and intrusion prevention methods need to be adopted. The tradeoff between reliability and cost needs to be analyzed to obtain the optimal decision on network design.
- *Networking middleware*: as stated in Section 7, interoperability is a significant issue for data communications in a heterogeneous smart grid communication environment. To deal with the interoperability problem, networking middleware can be developed to provide convergence among heterogeneous technologies [170]. With networking middleware, there will be an interface between applications and communications protocols, improving the flexibility of system and network integration.
- *Service-oriented networking*: data sensing and communications in the smart grid can be designed and implemented on the basis of a service-oriented architecture [171,172]. In this way, the resources (e.g., sensors, actuators, and protocols) will be treated as a unified service with a standard form of interface. This will help not only to reduce the complexity of the system integration but also to encapsulate the unnecessary detail to the external entities (e.g., a control center does not need to know the physical characteristics of a sensor). In this case, a service broker has to be developed as a point for the service supplier and the consumer to exchange their services.

10. CONCLUSION

The smart grid has been envisioned to be the future electrical power grid with enhanced flexibility, adaptability, and efficiency. By infusing digital intelligence, the smart grid will revolutionize the way electricity is produced, delivered, and consumed. Data sensing and communications will play one of the most important roles for the operation of the smart power grid. Data sensing has to be performed in different parts (i.e., power generation, storage, transmission, distribution, and consumption) of the smart grid, and the sensed data has to be transmitted to the control unit for the timely operation and maintenance of the smart grid. In this article, we have first summarized the different applications of data sensing in the smart grid. Then, the requirements for data sensing and communication methods for the smart grid have been discussed. A general network architecture has been discussed for the smart grid communications. Next, the emerging techniques for data sensing and communications have been reviewed. An overview of the security issues for data sensing and communication has been given. The standardization activities have been summarized together with the use cases of the smart grid sensor data collection and communication. Finally, some major open research issues and challenges have been outlined.

The scope and awareness of the smart grid are increasing, and as a result, many standard bodies (such as NIST, EPRI, IEEE, and European Commission) are working toward developing framework, communication standards, and security policies for the smart grid. With advancement in communications and information technology and active contributions from different research communities, it is a matter of time that smart grid will soon be a reality.

ACKNOWLEDGEMENT

This work was carried out in the Centre for Multimedia and Network Technology of the School of Computer Engineering, Nanyang Technological University, Singapore.

REFERENCES

1. Department of Energy, U.S.A. The smart grid: an introduction. Available from: http://www.oe.energy.gov/SmartGridIntroduction.htm [Accessed on April 2011].
2. European Commission Research. European smart grids technology platform vision and strategy for Europe’s electricity networks of the future. Available from: http://ec.europa.eu/research/energy/pdf/smartgrids_en.pdf [Accessed on April 2011].
3. Kim Y-J, Thottan M, Kolesnikov V, Lee W. A secure decentralized data-centric information infrastructure for smart grid. *IEEE Communications Magazine* 2010; **48**(11): 58–65.
4. Gharavi H, Ghafurian R. Smart grid: the electric energy system of the future. *Proceedings of the IEEE* 2011; **99**(6): 917–921.
5. National Institute of Standards and Technology (NIST), U.S.A. NIST framework and roadmap for smart grid interoperability standards, release 1.0. Available from: http://www.nist.gov/smartgrid/ [Accessed on April 2011].
6. Electric Power Research Institute (EPRI). IntelliGrid consumer portal telecommunications assessment and specification, technical update, 2006.

DOI: 10.1002/wcm

7. International Electrotechnical Commission. IEC smart grid standardization roadmap. Available from: http://www.iec.ch/smartgrid/ [Accessed on April 2011].
8. A & B National Energy Technological Laboratory (2007-07-27). A vision for the modern grid, United State Department of Energy. Available from: http://www.bpa.gov/energy/n/smart_grid/docs/Vision_for_theModernGrid_Final.pdf [Accessed on April 2011].
9. Vojdani A. Smart integration. *IEEE Power and Energy Magazine* 2008; **6**(6): 71–79.
10. Electric Power Research Institute (EPRI). Sensor technologies for a smart transmission system. *An EPRI White Paper*, December 2009.
11. National Energy Technology Laboratory (NETL). Sensing and measurement, March 2007. Available from: http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/Sensing%20and%20Measurement_Final_v2_0.pdf [Accessed on December 2011].
12. American Wind Energy Association (AWEA). 20% wind energy by 2030. *Fact Sheet*. Available from: http://www.awea.org/learnabout/ publications/factsheets/factsheets_windenergybasics.cfm [Accessed on July 2011].
13. Nano Markets. Smart grid: it's all about the sensors, October 2009. Available from: http://nanomarkets.net/articles/article/smart_grid_its_all_about_the_sensors [Accessed on December 2011].
14. Swartz RA, Lynch JP, Sweetman B, Rolfes R, Zerbst S. Structural monitoring of wind turbines using wireless sensor networks, In *Proceedings of the ESF-NSF Workshop on Sensor Network for Civil Infrastructure Systems*, 2008.
15. Gungor VC, Lu B, Hancke GP. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE Transactions on Industrial Electronics* 2010; **57**(10): 3557–3564.
16. Wang Y, Lynch JP, Law KH. A wireless structural health monitoring system with multithreaded sensing devices: design and validation. *Structure and Infrastructure Engineering* 2007; **3**(2): 103–120.
17. Nano Markets. Three types of smart grid sensors that will make money in next decade, May 2010. Available from:http://nanomarkets.net/articles/article/three_types_of_smart_grid_sensors_that_will_make_money_in_the_next_decade/ [Accessed on December 2011].
18. Morbel M, Kohnke H-J, Helmke J. Monitoring of lead acid batteries continuous measurement of the acid concentration, In *Proceedings of International Telecommunications Conference (INTELEC)*, September 2005; 263–268.
19. Juang LW, Kollmeyer PJ, Jahns TM, Lorenz RD. System identification-based lead-acid battery online monitoring system for electric vehicles, In *Proceedings of IEEE Energy Conversion Congress and Exposition (ECCE)*, September 2010; 3903–3910.
20. ZIV USA, Inc. Available from: http://www.zivusa.com/smartgrid/ZIV_Sensors_and_Couplers_for_Smart_Distribution_Grids.pdf [Accessed on July 2011].
21. Jain VK, Chapman GH. Massively deployable intelligent sensors for the smart power grid, In *IEEE 25th International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT)*, October 2010; 319–327.
22. Liu W, Tan B, Gong Y. SAW temperature sensors system for smart electric grid, In *IEEE Ultrasonics Symposium*, October 2010; 756–759.
23. Moreno-Munoz A, Sanchez JA, de la Rosa JJG, Luna JJ. Application of smart sensors to the measurement of power quality, In *IEEE Instrumentation and Measurement Technology Conference Proceedings (IMTC)*, May 2008; 218–222.
24. ADE7756 data sheets, active energy metering IC with serial interface. Available from: http://www.analog.com [Accessed on December 2011].
25. Hung KS, Lee WK, Li VOK, Lui KS, Pong PWT, Wong KKY, Yang GH, Zhong J. On wireless sensors communication for overhead transmission line monitoring in power delivery systems, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 309–314.
26. Schneider Electric. Available from: http://www.schneider-electric.com/site/home/index.cfm/ww/ [Accessed on August 2011].
27. Doig P. Smart sensors enable a smarter grid: improving high voltage grid reliability through the use of readily deployable, distributed, wireless intelligent sensors. *Schneider Electric White Paper*, 2006.
28. Huang Q, Zhang C, Liu Q, Ning Y, Cao Y. New type of fiber optic sensor network for smart grid interface of transmission system, In *IEEE Power and Energy Society General Meeting*, 25-29 July 2010; 1–5.
29. Rao YJ, Wang YP, Zhu T. *Principle and Application of Fiber Optic Gratings*. Science Press of China: Beijing, 2006.
30. Erol-Kantarci M, Mouftah HT. Wireless sensor networks for smart grid applications, In *Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, April 2011; 1–6.
31. Barbato A, Capone A, Rodolfi M, Tagliaferri D. Forecasting the usage of household appliances through power meter sensors for demand management in the smart grid, In *Proceedings*

of IEEE International Conference on Smart Grid Communications (SmartGridComm), October 2011; 422–427.

32. A3 ALPHA meter. Available from: http://www.elstermetering.com/en/921.html [Accessed on July 2011].
33. Elster Group. Available from: http://www.elster.com/ [Accessed on July 2011].
34. EnergyAxis, Elster. Available from: http://www.energyaxis.com/ea-home.asp [Accessed on July 2011].
35. Salt River Project (SRP), Arizona. Available from: http://www.srpnet.com/electric/home/ReadMeter.aspx [Accessed on July 2011].
36. INSTEON Energy Display. Available from: http://www.insteon.net/2448A2-Energy-Display.html [Accessed on July 2011].
37. iMeter Solo, INSTEON Power Meter. Available from: http://www.smarthome.com/manuals/2423a1.pdf [Accessed on July 2011].
38. Mak ST. Sensor data output requirements for smart grid applications, In *IEEE Power and Energy Society General Meeting*, September 2010; 1–3.
39. Wobschall D. Network sensors for the smart grid, In *Esensors White Paper on Sensors Expo*, 2010. Available from: http://www.eesensors.com/pdf/ESP24_Sgrid_Sen.pdf [Accessed on December 2011].
40. Organization for Economic Co-operation and Development (OECD). Smart sensor networks: technologies and applications for green growth, December 2009. Available from: http://www.oecd.org/dataoecd/39/62/44379113.pdf [Accessed on December 2011].
41. Slootweg JG, Veldman E, Morren J. Sensing and control challenges for smart grids, In *IEEE International Conference on Networking, Sensing and Control (ICNSC)*, April 2011; 1–7.
42. Hauser CH, Bakken DE, Bose A. A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid. *IEEE Power and Energy Magazine* 2005; **3**: 47–55.
43. Giri J, Sun D, Avila-Rosales R. Wanted: a more intelligent grid. *IEEE Power and Energy Magazine* 2009; **7**: 34–40.
44. Cherukuri N, Nahrstedt K. Cooperative congestion control in power grid communication networks, In *Proceedings of Smart Grid Communications Conference (SmartGridComm)*, October 2011; 605–610.
45. Pendarakis D, Shrivastava N, Liu Z, Ambrosio R. Information aggregation and optimized actuation in sensor networks: enabling smart electrical grids, In *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, May 2007; 2386-2390.
46. Farhangi H. The path of the smart grid. *IEEE Power and Energy Magazine* 2010; **8**(1): 18–28.
47. Aggarwal A, Kunta S, Verma PK. A proposed communications infrastructure for the smart grid, In *Innovative Smart Grid Technologies (ISGT)*, January 2010; 1–5.
48. Zhongwei S, Yaning M, Fengjie S, Yirong W. Access control for distribution automation using Ethernet passive optical network, In *Power and Energy Engineering Conference (APPEEC)*, March 2010; 1–4.
49. Bumiller G, Lampe L, Hrasnica H. Power line communication networks for large-scale control and automation systems. *IEEE Communications Magazine* 2010; **48**(4): 106–113.
50. Benato R, Caldon R. Application of PLC for the control and the protection of future distribution networks, In *IEEE International Symposium on Power Line Communications and Its Applications (ISPLC'07)*, March 2007; 499–504.
51. Bannister S, Beckett P. Enhancing power line communications in the smart grid using OFDMA, In *Proceedings of Power Engineering Conference, 2009 (AUPEC'09)*, Australian Universities, September 2009; 1–5.
52. Tsiropoulos GI, Sarafi AM, Cottis PG. Wireless-broadband over power lines networks: a promising broadband solution in rural areas, In *Proceedings of IEEE Bucharest PowerTech*, June-July 2009.
53. Inoue M, Higuma T, Ito Y, Kushiro N, Kubota H. Network architecture for home energy management system. *IEEE Transactions on Consumer Electronics* 2003; **49**(3): 606–613.
54. Gonzalez OA, Urminsky J, Calvo M, de Haro L. Performance analysis of hybrid broadband access technologies using PLC and Wi-Fi, In *Proceedings of International Conference on Wireless Networks, Communications and Mobile Computing*, Vol. 1, June 2005; 564–569.
55. Luan S-W, Teng J-H, Chan S-Y, Hwang L-C. Development of a smart power meter for AMI based on ZigBee communication, In *Proceedings of International Conference on Power Electronics and Drive Systems (PEDS)*, November 2009; 661-665.
56. Wang Y, Li W, Lu J. Reliability analysis of wide-area measurement system. *IEEE Transactions on Power Delivery* 2010; **25**(3): 1483–1491.
57. Naduvathuparambil B, Valenti MC, Feliachi A. Communication delays in wide area measurement systems, In *Proceedings of the Southeastern Symposium on System Theory (SSST)*, 2002; 118–122.

58. Yang Y, Lambert F, Divan D. A survey on technologies for implementing sensor networks for power delivery systems, In *Proceedings of IEEE Power Engineering Society General Meeting*, June 2007.
59. di Bisceglie M, Galdi C, Vaccaro A, Villacci D. Cooperative sensor networks for voltage quality monitoring in smart grids, In *Proceedings of IEEE Bucharest PowerTech*, June-July 2009.
60. IEEE 802.15.4 Standard. Wireless medium access control (MAC) and physical layer (phy) specifications for low-rate wireless personal area networks (LR-WPANs), October 2003.
61. Casey P, Jaber N, Tepe K. Design and implementation of a cross-platform sensor network for smart grid transmission line monitoring, In *Proceedings of Smart Grid Communications Conference (SmartGridComm)*, October 2011; 303–308.
62. Frolec J, Husak M. Wireless sensor system for overhead line ampacity monitoring, In *Proceedings of International Conference on Advanced Semiconductor Devices & Microsystems (ASDAM)*, October 2010; 211–214.
63. Li L, Zhu Y, Yu Y. Link scheduling and data forwarding in wireless sensor networks of long chains tree topology, In *Proceedings of IET International Conference on Wireless Sensor Network (IET-WSN)*, November 2010; 297–300.
64. Ota N. The home area network: architectural considerations for rapid innovation, White Paper for Trilliant Inc. Available from: http://www.trilliantinc.com/libraryfiles/white-papers/HAN_white-paper.pdf [Accessed on July 2011].
65. Lobo F, Cabello A, Lopez A, Mora D, Mora R. Distribution network as communication system, In *Proceedings of CIRED Seminar SmartGrids for Distribution (IET-CIRED)*, June 2008.
66. Lobo F, Lopez A, Cabello A, Mora D, Mora R, Carmona F, Moreno J, Roman D, Sendin A, Berganza I. How to design a communication network over distribution networks, In *Proceedings of International Conference and Exhibition on Electricity Distribution*, June 2009.
67. Active Demand Management (GAD) Project Under Technological Development Center of the Ministry of Industry, Tourism and Commerce of Spain (CDTI). Available from: http://www.gadproject.es/ [Accessed on June 2010].
68. Ting Y, Zhidong Z, Jiaowen W, Ang L. Research on transmission data system of smart grid based on IPv6 DiffServ model, In *Proceedings of Power and Energy Engineering Conference (APPEEC)*, March 2010; 1–4.
69. Ting Y, Zhidong Z, Jiaowen W, Ang L. Research on transmission data system of smart grid based on IPv6 DiffServ model, In *Proceedings of Asia-Pacific Power and Energy Engineering Conference (APPEEC)*, March 2010.
70. Sood VK, Fischer D, Eklund JM, Brown T. Developing a communication infrastructure for the smart grid, In *Proceedings of IEEE Electrical Power and Energy Conference (EPEC)*, October 2009; 1–7.
71. Wan CY, Campbell AT, Krishnamurthy L. PSFQ: a reliable transport protocol for wireless sensor networks, In *Proceedings of ACM International Workshop on Wireless Sensor Networks and Applications*, Atlanta, GA , USA, 2002; 1–11.
72. Stann F, Heidemann J. RMST: reliable data transport in sensor networks, In *Proceedings of First IEEE International Workshop on Sensor Network Protocols and Applications*, Anchorage, AK , USA, 2003; 102–112.
73. Sankarasubramaniam Y, Akan B, Akyildiz IF. ESRT: event to sink reliable transport in wireless sensor networks, In *Proceedings of ACM MobiHoc'03*, Annapolis, Maryland; June 2003.
74. Heinzelman WR, Kulik J, Balakrishnan H. Adaptive protocols for information dissemination in wireless sensor networks, In *Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, 1999; 174–185.
75. Heinzelman WR, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks, In *Proceedings of Annual Hawaii International Conference on System Sciences (HICSS)*, Vol. 18, 2000.
76. Xu Y, Heidemann J, Estrin D. Geography-informed energy conservation for ad-hoc routing, In *Proceedings of 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, 2001; 70–84.
77. Ye W, Heidemann J, Estrin D. Medium access control protocol with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on Networking* 2004; **12**(3): 493–506.
78. Rajendran V, Obraczka K, Aceves JJGL. Energy-efficient collision-free medium access control for wireless sensor networks, In *Proceedings of 1st ACM Conference on Embedded Networked Sensor Systems (SenSys)*, November 2003; 181–192.
79. Rhee I, Warrier A, Aia M, Min J. Z-MAC: a hybrid MAC for wireless sensor networks, In *Proceedings of 3rd ACM Conference on Embedded Networked Sensor Systems (SenSys)*, November 2005.
80. Universal Plug and Play Forum. UPnP^{TM} Device Architecture version 1.1. Available from: http://www.

upnp.org/resources/documents.asp [Accessed on May 2010].

81. Phadke AG. Synchronized phasor measurements-a historical overview, In *IEEE/PES, Transmission and Distribution Conference and Exhibition 2002: Asia Pacific*, Vol. 1, April 2002; 476–479.
82. Phadke AG. Synchronized phasor measurements in power systems. *IEEE Computer Applications in Power* 1993; **6**(2): 10–15.
83. Xu B, Abur A. Observability analysis and measurement placement for systems with PMUs, In *Power Systems Conference and Exposition*, April 2005; 943–946.
84. Chakrabarti S, Kyriakides E, Eliades DG. Placement of synchronized measurements for power system observability. *IEEE Transactions on Power Systems* 2009; **24**(1): 12–19.
85. Baldwin TL, Mili L, Boisen MB, Adapa R. Power system observability with minimal phasor measurement placement. *IEEE Transactions on Power Systems* 1993; **8**(2): 707–715.
86. Donoho D. Compressed sensing. *IEEE Transactions on Information Theory* 2006; **52**(4): 1289–1306.
87. Candes E, Romberg J, Tao T. Stable signal recovery from incomplete and inaccurate measurements. *Communications On Pure and Applied Mathematics* 2006; **59**(8): 1207–1223.
88. Candes E, Romberg J, Tao T. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *IEEE Transactions on Information Theory* 2006; **52**(2): 489–509.
89. Candes E, Tao T. Near optimal signal recovery from random projections: universal encoding strategies. *IEEE Transactions on Information Theory* 2006; **52**(12): 5406–5425.
90. Li H, Mao R, Lai L, Qiu RC. Compressed meter reading for delay-sensitive and secure load report in smart grid, In *IEEE Smart Grid Communications Conference*, 2010.
91. Wu FF, Moslehi K, Bose A. Power system control centers: past, present, and future. *Proceedings of the IEEE* 2005; **93**(11): 1890–1908.
92. Xie L. A framework for distributed decision making in electric energy systems with intermittent resources, *Ph.D. Dissertation*, Carnegie Mellon University, 2009.
93. Van Cutsem T, Horward JL, Ribbens-Pavella M. A two-level static state estimator for electric power systems. *IEEE Transactions on Power Apparatus and Systems* 1981; **PAS-100**(8): 3722–3732.
94. Van Cutsem T, Ribbens-Pavella M. Critical survey of hierarchical methods for state estimation of electric power systems. *IEEE Transactions on Power Apparatus and Systems* 1983; **PSA-102**(10): 247–256.
95. Bose A, Abur A, Poon KYK, Emami R. Implementation issues for hierarchical state estimators. *Final Project Report*, PSERC Document 10-11, August 2010.
96. Korres GN. A distributed multiarea state estimation. *IEEE Transactions on Power Apparatus and Systems* 2010; **41**(4): 550–558.
97. Zhao L, Abur A. Multiarea state estimation using synchronized phasor measurements. *IEEE Transactions on Power Systems* 2005; **20**(2): 611–617.
98. Jiang W, Vittal V, Heydt GT. A distributed state estimator utilizing synchronized phasor measurements. *IEEE Transactions on Power Systems* 2007; **22**(2): 563–571.
99. Valverde G, Chakrabarti S, Kyriakides E, Terzija V. A constrained formulation for hybrid state estimation. *IEEE Transactions on Power Systems* 2011; **26**(3): 1102–1109.
100. Fadlullah ZM, Fouda MM, Kato N, Takeuchi A, Iwasaki N, Nozaki Y. Toward intelligent machine-to-machine communications in smart grid. *IEEE Communications Magazine* 2011; **49**(4): 60–65.
101. Niyato D, Xiao L, Wang P. Machine-to-machine communications for home energy management system in smart grid. *IEEE Communications Magazine* 2011; **49**(4): 53–59.
102. Bartoli A, Hernandez-Serrano J, Soriano M, Dohler M, Kountouris A, Barthel D. Secure lossless aggregation for smart grid M2M networks, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 333–338.
103. Ullo S, Vaccaro A, Velotto G. The role of pervasive and cooperative sensor networks in smart grids communication, In *Proceedings of IEEE Mediterranean Electrotechnical Conference (MELECON)*, April 2010; 443–447.
104. Yan Y, Qian Y, Sharif H. A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid, In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, March 2011; 909–914.
105. Qiu RC, Hu Z, Chen Z, Guo N, Ranganathan R, Hou S, Zheng G. Cognitive radio network for the smart grid: experimental system architecture, control algorithms, security, and microgrid testbed. *IEEE Transactions on Smart Grid,* 2011; **2**(4): 724–740.
106. Sreesha AA, Somal S, Lu I-T. Cognitive radio based wireless sensor network architecture for smart grid utility, In *Proceedings of IEEE Long Island Systems,*

Applications and Technology Conference (LISAT), May 2011.

107. Ko J, Terzis A, Dawson-Haggerty S, Culler DE, Hui JW, Levis P. Connecting low-power and lossy networks to the internet. *IEEE Communications Magazine* 2011; **49**(4): 96–101.
108. Sun W, Yuan X, Wang J, Han D, Zhang C. Quality of service networking for smart grid distribution monitoring, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 373–378.
109. Al-Anbagi IS, Mouftah HT, Erol-Kantarci M. Design of a delay-sensitive WSN for wind generation monitoring in the smart grid, In *Proceedings of Canadian Conference on Electrical and Computer Engineering (CCECE)*, May 2011; 1370–1373.
110. Kim M, Kim S, Kim J, Yoo Y. Design and implementation of MAC protocol for SmartGrid HAN environment, In *Proceedings of IEEE International Conference on Computer and Information Technology (CIT)*, August-September 2011; 212–217.
111. Hoglund J, Eriksson J, Finne N, Sauter R, Karnouskos S. Event-driven IPv6 communication for the smart grid infrastructure, In *Proceedings of International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, June 2011.
112. Ting Y, Zhidong Z, Angm L, Jiaowen W, Ming W. New IP QoS algorithm applying for communication sub-networks in smart grid, In *Proceedings of Asia-Pacific Power and Energy Engineering Conference, (APPEEC)*, March 2010; 1–4.
113. Wang J, Leung VCM. A survey of technical requirements and consumer application standards for IP-based smart grid AMI network, In *Proceedings of International Conference on Information Networking (ICOIN)*, January 2011; 114–119.
114. Chauvenet C, Tourancheau B, Genon-Catalot D, Goudet P-E, Pouillot M. A communication stack over PLC for multi physical layer IPv6 networking, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 250–255.
115. Wang D, Tao Z, Zhang J, Abouzeid AA. RPL based routing for advanced metering infrastructure in smart grid, In *Proceedings of IEEE International Conference on Communications Workshops (ICC)*, May 2010.
116. Bressan N, Bazzaco L, Bui N, Casari P, Vangelista L, Zorzi M. The deployment of a smart monitoring system using wireless sensor and actuator networks, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 49–54.
117. Tripathi J, de Oliveira JC, Vasseur JP. Applicability study of RPL with local repair in smart grid substation networks, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 262–267.
118. Kulkarni P, Gormus S, Fan Z, Motz B. A self-organising mesh networking solution based on enhanced RPL for smart metering communications, In *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, June 2011.
119. Iwao T, Yamada K, Yura M, Nakaya Y, Cardenas AA, Lee S, Masuoka R. Dynamic data forwarding in wireless mesh networks, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 385–390.
120. Gharavi H, Hu B. Multigate communication network for smart grid. *Proceedings of the IEEE* 2011; **99**(6): 1028–1045.
121. Biagi M, Lampe L. Location assisted routing techniques for power line communication in smart grids, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 274–278.
122. Khalifa T, Naik K, Alsabaan M, Nayak A, Goel N. Transport protocol for smart grid infrastructure, In *Proceedings of International Conference on Ubiquitous and Future Networks (ICUFN)*, June 2010; 320–325.
123. Shelby Z, Frank B, Sturek D. Constrained Application Protocol (CoAP). IETF Internet Draft, draft-ietf-core-coap-06, 2010. Available from: http://datatracker.ietf.org/doc/draft-ietf-core-coap/ [Accessed on December 2011].
124. Wang Y, Lin W, Zhang T. Study on security of wireless sensor networks in smart grid, In *Proceedings of International Conference on Power System Technology (POWERCON)*, October 2010; 1–7.
125. McMillan R. Siemens: Stuxnet worm hit industrial systems. Computerworld, September 2010. Available from: http://www.computerworld.com/s/article/print/9185419 [Accessed on 16 September 2010].
126. Dan G, Sandberg H, Bjorkman G, Ekstedt M. Challenges in power system information security. *IEEE Security & Privacy,* to appear.
127. McLaughlin S, Podkuiko D, McDaniel P. Energy theft in the advanced metering infrastructure, In *Proceedings of International Conference on Critical Information Infrastructures Security (CRITIS)*, 2009; 176–187.

128. Berthier R, Sanders WH, Khurana H. Intrusion detection for advanced metering infrastructures: requirements and architectural directions, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 350–355.

129. Department of Energy. Securing Wide Area Measurement Systems. Available from: http://energy.gov/oe/downloads/securing-wide-area-m easurement-systems [Accessed on November 2011].

130. D'Antonio S, Coppolino L, Elia IA, Formicola V. Security issues of a phasor data concentrator for smart grid infrastructure, In *Proceedings of European Workshop on Dependable Computing (EWDC)*, no. 6, May 2011; 3–8.

131. Tennessee Valley Authority (TVA). Available from: www.tva.gov [Accessed on November 2011].

132. Varodayan DP, Gao GX. Redundant metering for integrity with information-theoretic confidentiality, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 345–349.

133. Choi J, Shin I, Seo J, Lee C. An efficient message authentication for non-repudiation of the smart metering service, In *Proceedings of ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI)*, May 2011; 331–333.

134. Qiu M, Gao W, Chen M, Niu J-W, Zhang L. Energy efficient security algorithm for power grid wide area monitoring system. *IEEE Transactions on Smart Grid,* 2011; **2**(4): 715–723.

135. Luitel B, Venayagamoorthy GK, Johnson CE. Enhanced wide area monitoring system, In *Proceedings of Innovative Smart Grid Technologies (ISGT)*, January 2010.

136. Li H, Lai L, Qiu RC. A denial-of-service jamming game for remote state monitoring in smart grid, In *Proceedings of Conference on Information Sciences and Systems (CISS)*, March 2011.

137. EnerNex Corporation. Smart grid standards assessment and recommendations for adoption and development. Available from: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/H2G/Smart_Grid_Standards_Landscape_White_Paper_v0_8.doc [Accessed on April 2011].

138. National Institute of Standards and Technology (NIST), U.S.A. Available from: http://www.nist.gov/smartgrid/ [Accessed on July 2011].

139. Electrical Power Research Institute. Available from: http://smartgrid.epri.com/ [Accessed on July 2011].

140. Department of Energy, USA. Available from: http://www.oe.energy.gov/smartgrid.htm [Accessed on July 2011].

141. ZigBee Alliance. Available from: http://www.zigbee.org/ [Accessed on July 2011].

142. HomePlug Powerline Alliance. Available from: http://www.homeplug.org [Accessed on July 2011].

143. Z-Wave Alliance. Available from: http://www.z-wavealliance.org/modules/AllianceStart/ [Accessed on July 2011].

144. IEEE Standard 1451.1 6. IEEE standard for a smart transducer interface for sensors and actuators. Available from: http://www.nist.gov/el/isd/ieee/1451intro.cfm [Accessed on July 2011].

145. IEEE Std. 1588-2002. IEEE Standard for a Precision clock synchronization protocol for networked measurement and control systems.

146. Abe R, Taoka H, McQuilkin D. Digital grid: communicative electrical grids of the future. *IEEE Transactions on Smart Grid* 2011; **2**(2): 399–410.

147. Rusitschka S, Eger K, Gerdes C. Smart grid data cloud: a model for utilizing cloud computing in the smart grid domain, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 483–488.

148. Wang D, Tao Z, Zhang J, Abouzeid AA. RPL based routing for advanced metering infrastructure in smart grid, In *IEEE International Conference on Communications Workshops (ICC)*, May 2010; 1–6, 23–27.

149. Gungor VC, Lambert FC. A survey on communication networks for electric system automation. *Computer Networks Journal (Elsevier)* 2006; **50**: 877–897.

150. Sauter T, Pratl G, Treytl A, Bumiller G. Secure and reliable widearea power-line communication for soft-real-time applications within REMPLI, In *International Symposium on Power Line Communications and Its Applications*, April 2005; 57–60.

151. IntelliGrid Consortium. Available from: http://intelligrid.epri.com/default.asp [Accessed on July 2011].

152. Energy management system application program interface (EMS-API) part 301: common information model (CIM) Base, Int. Electrotech. Comm. Std. IEC 61970-301 Ed. 2, IEC, April 7 2009.

153. IEC Syst. interfaces for distribution management part 11: common information model (CIM) extensions for distribution, Int. Electrotech. Comm. Std. IEC 61968-11 Draft CDV, 2009.

154. Haynes DD. A case for optimized protocols in the creation of a smarter grid. *IEEE Transactions on Power Delivery* 2010; **25**(3): 1476–1482.

155. BACnet. A data communication protocol for building automation and control networks. Available from: http://www.bacnet.org/ [Accessed on July 2011].

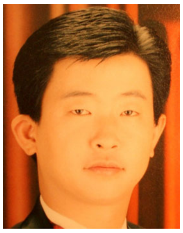
156. Konnex Association. Available from: http://www.knx.org/knx/whatisknx/ [Accessed on July 2010].
157. IEEE 1901. IEEE 1901 draft standard for broadband over power line networks: medium access control and physical layer specifications, February 2010.
158. Zensys A/S. Available from: http://www.zen-sys.com/modules/Zensys/ [Accessed on June 2011].
159. OpenAMI task force under the UCA International Users Group (UCAIUG). UtilityAMI 2008 HAN SRS. Available from: http://www.utilityami.org/ [Accessed on March 7, 2008].
160. IntelliGrid Consortium. IntelliGrid consumer portal telecommunications assessment and specification, December 2005. Available from: http://intelligrid.epri.com/technical_results.html [Accessed on December 2011].
161. GridWise Architecture Council (GWAC). Available from: http://www.gridwiseac.org/ [Accessed on July 2011].
162. The GridWise Architecture Council. GridWise interoperability contextsetting framework. Available from: http://www.gridwiseac.org/about/publications.aspx [Accessed on July 2011].
163. Electrical Power Research Institute's Smart Grid Demonstration. Available from: http://smartgrid.epri.com/Demo.aspx [Accessed on August 2011].
164. Metke AR, Ekl RL. Security technology for smart grid networks. *IEEE Transactions on Smart Grid* 2010; **1**(1): 99–107.
165. Kosut O, Jia L, Thomas RJ, Tong L. Malicious data attacks on smart grid state estimation: attack strategies and countermeasures, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 220–225.
166. Kosut O, Jia L, Thomas RJ, Tong L. Limiting false data attacks on power system state estimation, In *44th Annual Conference on Information Sciences and Systems (CISS)*, May 2010; 1–6.
167. Xie L, Mo Y, Sinopoli B. False data injection attacks in electricity markets, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 226–231.
168. Liu Y, Reiter MK, Ning P. False data injection attacks against state estimation in electric power grids, In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, November 2009; 21–30.
169. Levorato M, Mitra U. Optimal allocation of heterogeneous smartgrid traffic to heterogeneous networks, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2011; 144–149.
170. Garcia AP, Oliver J, Gosch D. An intelligent agent-based distributed architecture for smart-grid integrated network management, In *Proceedings of IEEE Conference on Local Computer Networks (LCN)*, October 2010; 1013–1018.
171. Postina M, Rohjans S, Steffens U, Uslar M. Views on service oriented architectures in the context of smart grids, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2010; 25–30.
172. Sucic S, Martinic A, Francesconi D. Utilizing SOA-ready devices for virtual power plant control in semantic-enabled smart grid analyzing IEC 61850 and OPC UA integration methodology, In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2011; 43–48.

AUTHORS' BIOGRAPHIES

Nipendra Kayastha received his B.E. (with distinction) in Electronics and Communication Engineering from Nepal Engineering College, Nepal in 2004 and his M.E. in Information and Communication Technologies from Asian Institute of Technology, Thailand in 2008. His research interests are in data communication and protocol design for new and emerging areas such as mobile social networks, smart grid, and femtocell. He has worked as a project officer with the Center for Multimedia and Network Technology, Nanyang Technological University, Singapore.

Dusit Niyato is currently an assistant professor in the School of Computer Engineering, at the Nanyang Technological University, Singapore. He obtained his Bachelor of Engineering in Computer Engineering from the King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok, Thailand. He received his Ph.D. in Electrical and Computer Engineering from the University of Manitoba, Canada. His research interests are in the area of radio resource management in cognitive radio networks and broadband wireless access networks.

Ekram Hossain is a full professor in the Department of Electrical and Computer Engineering at the University of Manitoba, Winnipeg, Canada. He received his Ph.D. in Electrical Engineering from the University of Victoria, Canada, in 2001. Hossain's current research interests include design, analysis, and optimization of wireless/mobile communications networks, smart grid communications and networking, and cognitive radio systems. He has authored/edited several books in these areas (http://www.ee.umanitoba.ca/ ekram). He served as the area editor for the IEEE Transactions on Wireless Communications in the area of "Resource Management and Multiple Access" from 2009–2011. Currently, he serves as an editor for the IEEE Transactions on Mobile Computing, IEEE Wireless Communications, and the editor-in-chief for the IEEE Communications Surveys and Tutorials (for the term 2012-2013). He has won several research awards including the University of Manitoba Merit Award in 2010 (for Research and Scholarly Activities), the 2011 IEEE Communications Society Fred Ellersick Prize Paper Award, and the IEEE Wireless Communications and Networking Conference 2012 (WCNC'12) Best Paper Award. He is a registered professional engineer in the province of Manitoba, Canada.



Zhu Han received his B.S. degree in electronic engineering from Tsinghua University, in 1997, and his M.S. and Ph.D. degrees in Electrical Engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was an R&D engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a research associate at the University of Maryland. From 2006 to 2008, he was an assistant professor in Boise State University, Idaho. Currently, he is an assistant professor in Electrical and Computer Engineering Department at the University of Houston, Texas. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, wireless multimedia, security, and smart grid communication.

Han is an associate editor of IEEE Transactions on Wireless Communications since 2010. He is the winner of IEEE Fred W. Ellersick Prize 2011, an NSF CAREER award recipient 2010, and the coauthor for the papers that won the best paper awards in IEEE International Conference on Communications 2009, 7th International Symposium on Modeling and Optimization in Mobile, *Ad Hoc*, and Wireless Networks (WiOpt09), and IEEE Wireless Communication and Networking Conference, 2012.

DOI: 10.1002/wcm