Communication and Network Security Requirements for Smart Grid

Victor O. K. Li

Abstract To relieve the problems of climate change due to global warming, increased renewable energy generation based on wind and solar has been advocated in the power grid. Due to the intermittent nature of such generation, and the requirement of real-time power balance between generation and consumption, increased renewable energy generation may cause instability in the power grid. The smart grid is an attempt to deploy information and communication technologies (ICT) on the power grid to solve the instability problem due to renewable energy sources. The smart grid also enables customer participation in such applications as differential pricing and demand response and promises improved grid operating efficiencies, self-healing capabilities, and resiliencies against cyber attacks. In this chapter, we discuss the communication and network security requirements for smart grid.

1 Introduction

Concerns with the problems of climate change due to global warming prompted governments throughout the world to pursue policies aiming at the reduction of greenhouse gases, mostly carbon dioxide. One important government policy to achieve carbon reduction is to mandate increased renewable energy penetration in electricity generation. However, such increases may adversely impact power system operations. Due to the intermittent characteristics of renewable energy sources such as wind and solar, the outputs of wind farm and solar generators are difficult to forecast. Any change in wind conditions or a cloudy sky may result in very large changes in power outputs. Since a power system requires real-time

V. O. K. Li (✉)
Department of Electrical and Electronic Engineering, The University of Hong Kong,
Hong Kong, People's Republic of China
e-mail: vli@eee.hku.hk

D. Mah et al. (eds.), *Smart Grid Applications and Developments*,
Green Energy and Technology, DOI: 10.1007/978-1-4471-6281-0_6,

power balance between generation and consumption, increasing renewable energy penetration may cause instability in the power grid. The smart grid is an attempt to deploy information and communication technologies (ICT) on the electric grid to solve the instability problem due to renewable energy sources.

Another application of the smart grid is to allow active customer participation. This ranges from allowing customers to choose when to consume electricity (to take advantage of differential pricing) to allowing customers with small-scale renewable energy generators to sell electricity to the grid. To facilitate such participation, real-time two-way communications and smart meters are required.

The smart grid also promises improved operating efficiencies, self-healing capabilities, and resiliencies against cyber attacks.

To summarize, the objectives of the smart grid include (1) accommodating different types of electricity generation, including renewable resources, and storage options; (2) enabling active participation by consumers; (3) optimizing assets and operating efficiency; (4) providing good power quality for electricity supply; (5) providing self-healing capability from power disturbance events; (6) guaranteeing operating resiliency against physical and cyber attacks; and (7) enabling new products, services, and markets [1].

The European Union launched the smart grid project in 2003 [2]. The US Electric Power Research Institute started the IntelliGrid project (EPRI) [3]. The US Department of Energy initiated a Grid 2030 project [4]. Under the Energy Independence and Security Act of 2007, the US National Institute of Standards and Technology (NIST) is tasked with coordinating the development of a framework for information management to achieve interoperability of smart grid devices. The NIST report (Phase I) provides a conceptual reference model for the smart grid [5]. There is an urgent need to establish protocols and standards for the smart grid.

One may claim that the electric power grid with modern energy management system (EMS), consisting of large number of remote terminal units (RTU) sending real-time data every 2 s from substations in the power grid to the computer control center via the supervisory control and data acquisition (SCADA) system, and the advanced application software processing the data in the control center to ensure economic and reliable operation, is a smart grid already. For an introduction to SCADA and EMS, interested readers are referred to Wu et al. [6]. However, the computer and communication technologies employed by EMS and SCADA do not represent state-of-the-art ICT technologies. Moreover, most power systems do not support real-time monitoring and control in the lower-voltage distribution system from substation down. In addition, phasor measurement unit (PMU) [7], which provides global positioning system (GPS) time-stamped measurements in milliseconds, may be utilized to upgrade EMS to a smarter transmission grid. Therefore, it is now possible to have a unified smart grid which covers all parts of the power grid, including the centralized fossil-fuel generators, the distributed renewable energy generators, the transmission and distribution networks, and the smart meters and smart appliances at the consumer premises.

2 Smart Grid Enabling Technologies

According to the US National Energy Technology Laboratory (NETL) [8], we need the following technologies to deploy a smart grid: (1) sensing and measurement, (2) advanced control methods, (3) advanced components, (4) Improved interfaces and decision support (IIDS), and (5) integrated communications. These are summarized as follows:

(1) Sensing and measurement: The goal includes enhancing power management with frequent meter readings, preventing energy theft, enabling consumer choices and demand response, and supporting new control strategies. Two key sensor components will be deployed, including the PMU, and smart meters under the advanced metering infrastructure (AMI). PMUs acquire time-synchronized phasor measurement data for power system operations and have been proved capable of significantly improving the performance of power system monitoring, protection, and control. However, they are quite expensive, and one key problem is to minimize the required number of PMUs, while satisfying the requirement of wide-area monitoring with full coverage. This optimal PMU placement (OPP) problem has attracted much research, and integer linear programming approaches have been proposed. However, due to their computational complexity, such approaches may not scale and more recently, heuristic approaches, such as chemical reaction optimization [9], have been used [10]. Another important sensing infrastructure is the AMI, consisting of smart meters at consumer premises and the two-way communication system which connects the smart meters to the control centers of the service provider. AMI enables such applications as differential pricing and demand response.

(2) Advanced control methods: Traditional power dispatch attempts to always generate enough power to meet the demand. Due to start-up delays in traditional power plants, to guard against under-estimated demands, "spinning reserves" are deployed, i.e., the generator is kept running, so it can be put online at short notice. This does not help in our efforts to reduce carbon dioxide emission. With smart grid, and with an improved estimate of the system state due to advanced sensors such as PMUs, it is possible to have risk-limiting dispatch [11], in which the probability of not meeting the operating constraints is reduced to an acceptable level. Of course, the goal would be to eliminate this risk by making use of energy storage devices and such techniques as demand response. While battery storage is still relatively expensive, there are many studies on utilizing the batteries of electric vehicles hooked up to the grid to provide storage [12]. Demand response gives the utility company the flexibility to reduce the load of selected users, at relatively short notice, in return for reduced electricity rates.

(3) Advanced components: PMU is an important component of smart grid. Another recently developed component is the electric spring [13]. This power electronics device can be used to smooth the fluctuations in power generation

due to solar and wind sources. They may be distributed over the power grid to stabilize the system even when there is substantial wind and solar power generation.

(4) IIDS: This includes the " … essential technologies that must be implemented if grid operators and managers are to have the tools and training they will need to operate a modern grid. IIDS technologies will convert complex power system data into information that can be understood by human operators at a glance. Animation, color contouring, virtual reality, and other data display techniques will prevent 'data overload' and help operators identify, analyze, and act on emerging problems." [8, Appendix B5].

(5) Integrated communications: This is the "… infrastructure for real-time information and power exchange, allowing users to interact with various intelligent electronic devices …" [8, Appendix B1]. Since a typical power grid has an existing communication system, it is important for the new communication infrastructure to be compatible with the existing system. It is also important to consider security and privacy issues.

We note that to achieve the full functionalities of the smart grid enabling technologies, communication technology plays a fundamental role. Therefore, in the rest of this chapter, we will focus on the communication technology of smart grid. We shall first describe a communication-oriented smart grid framework, followed by communication requirements, and finally, security and privacy requirements.

3 Communication-Oriented Smart Grid Framework

To better understand the communication requirements for smart grid, it is necessary to develop a communication framework, on which all aspects of smart grid communication can be analyzed. Most existing work on smart grid communications addressed the communication specifications, but they only focused on some specific parts of the entire smart grid network. For example, Aggarwal et al. [14] presented a communication framework for the distribution network, while [15] focused on the home-area network. The US NIST proposed a framework for smart grids [16]. As shown in Fig. 1, this framework consists of seven domains or entities, namely markets, service providers, bulk generations, transmissions, distribution, operations, and customers. The role of each domain is summarized as follows:

(1) Markets: This domain consists of electricity market participants and operators. The goal is to match the energy production with consumption efficiently, through issuing real-time electricity pricing signals. This domain supports energy bidding, distributed energy resource (DER) aggregation, and energy retailing. In addition, ancillary operations, such as frequency regulation and voltage support, are carried out based on information received from this domain.

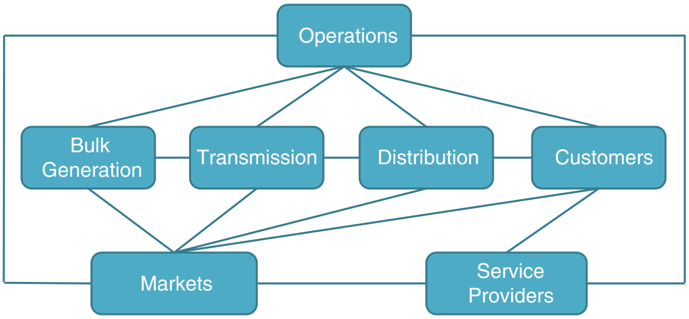

Fig. 1 NIST seven-domain smart grid framework

(2) Operations: This domain consists of electricity service operators. The goal is to ensure reliable and smooth power system operations. Various control and monitoring applications, such as SCADA and EMS, have their control centers in this domain. Moreover, many operational management applications, including fault management, asset maintenance, and operation planning, can be found here.

(3) Service providers: A service provider offers electricity services to customers. This domain acts as an intermediary among operations, markets, and customers. It provides customer management, billing, and other emerging services.

(4) Bulk generation: This domain consists of the electricity generation plants. Bulk generation is typically directly connected to transmission and interfaces with operations, markets, and transmission to support generation control, power flow measurement, plant protection, and other applications. One of the most important functions of bulk generation is to control greenhouse gas emissions, via increased renewable energy sources, and with the deployment of advanced storage devices for smoothing out the imbalance between energy generation and consumption.

(5) Transmission: This domain consists of transmission facilities, such as long-distance overhead lines and transformers. It connects bulk generation and distribution. The most important functions of this domain are transmission stability maintenance and energy loss reduction. This is achieved via voltage monitoring and control carried out at transmission substations. This domain interfaces with markets to procure ancillary services such as frequency regulation services, and with operations for transmission scheduling.

(6) Distribution: This domain consists of distribution facilities, including distribution transformers and underground cables. Distribution interfaces with transmission, customers, markets, and operations. It works with operations to provide real-time management of power flows, and with markets to provide real-time generation and consumption data. It also supports asset and line monitoring and control, distributed energy generation, and bi-directional power flows.

(7) Customers: A customer is an electricity end user, such as a household, a commercial business, or an industrial factory. Since it is increasingly common to have distributed electricity generation and storage facilities, such facilities are also included in this domain. This domain is electrically connected to distribution. It is supported by AMI, which enables communications with distribution, operations, markets, and service providers, facilitating such applications as demand response, building/industrial automation, and the ability by the end user to sell electricity back to the grid.

This high-level NIST framework is complete, but perhaps too complex for those focusing on the underlying communication networks.

In Wen et al. [17], a new communication-oriented framework for smart grid is introduced. This three-entity framework, shown in Fig. 2, is designed to be flexible to accommodate potential new smart grid technologies. It consists of three entities, namely operation network, business network, and consumer network. Operation network manages electricity generation, transmission, and distribution and typically includes automation technologies related to the legacy SCADA systems, wide-area measurement systems (WAMS), and large-scale EMS. Business network is used by the electricity market participants, including the metering service providers and government regulators, to coordinate the electricity market. Consumer network handles the communication for the electricity end users. It includes a home-area network as part of the AMI.

The design principles for this three-entity framework are summarized as follows:

- Simplicity: This framework is designed with only three entities and three types of inter-entity communications, for ease of analyses and further development.
- Completeness: Although simple, this framework represents a complete picture of smart grid communications and is flexible to accommodate all existing and future smart grid applications.
- Compatibility: The proposed framework is compatible with the seven-domain NIST framework. The mapping is as follows. Operation network in the three-entity framework includes the domains of operations, bulk generations, transmissions, and distribution in the NIST framework. Business network in the three-entity framework contains the domains of markets and service providers in the NIST framework. Consumer network in the three-entity framework corresponds to the domain of customers. Due to this compatibility, one can adopt this simple three-entity framework instead of the seven-domain NIST framework to study communication issues defined under the NIST framework.
- Ease of deployment: Three levels of communication requirements have been identified, and system components with the same level of communication requirements are grouped into the same entity. Components in operation network demand the most stringent requirements in terms of cyber security, data availability, and quality of service (QoS). Those components in business network have relatively less stringent requirements, and those components in consumer network have the least stringent requirements. Thus, they are divided

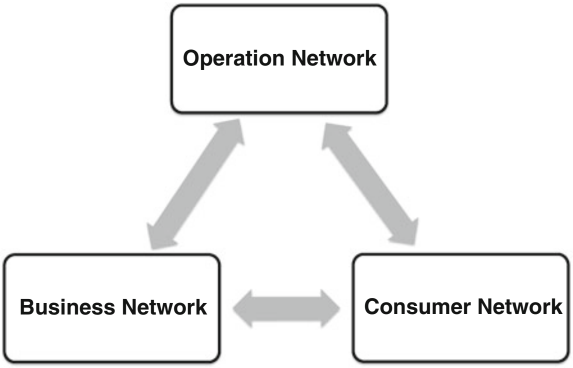

Fig. 2 Three-entity framework for smart grid communication

into three entities for ease of network deployment and inter-entity communication control.
- Ease of evolution: Operation network has been in existence for decades as the core of power system automation, and huge investments have been made by power companies. Due to such investments, future research and development efforts in this area will likely focus on the evolution of the existing network, as opposed to a fundamental change, to meet the requirements for smart grid. Internet technologies have been proposed for supporting business network [18]. Research and development efforts will likely focus on designing new applications and electricity market regulation schemes, such as in Jin and Mechehoul [18] and Rahimi and Ipakchi [16]. Consumer network is relatively new, and research and development on smart metering, demand response, and DER management will prove fruitful.
- Ease of collaboration: The future electricity system requires the expertise of electrical engineers, ICT professionals, business experts, and government officials. The communication-oriented framework must facilitate the collaboration of these experts from various fields.

We shall now describe these three entities in detail.

3.1 Operation Network

Operation network is responsible for electricity generation, transmission, and distribution, and for maintaining the stability and efficiency of the entire power system. As shown in Fig. 3, it consists of eight major components, described as follows:

- Business network gateway and consumer network gateway connect operation network and business network, and operation network and consumer network, respectively.

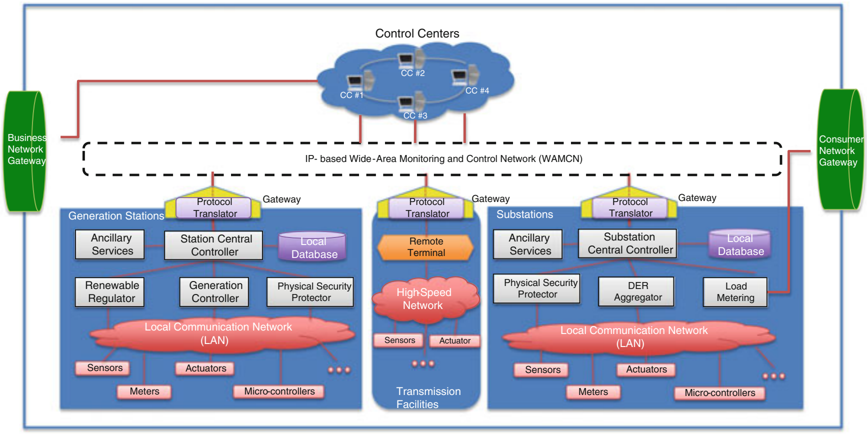

Fig. 3 Operation network [17]

- Control centers gather and process grid operation data. Different control centers communicate with each other to control the whole operation area via a dedicated, secure, high-speed network, managing the various facilities in a smart grid.
- A monitoring and control database is used to store the historical data of the system, including the status parameters of the grid during its operation, and event logs for operators.
- A wide-area monitoring and control network (WAMCN) acquires data from the remote stations or substations and issues control commands. These remote stations can communicate with each other to get a better picture of the system state.
- A generation station is a plant that generates electricity. Each generation station deploys a gateway with a built-in protocol translator to connect the station network to WAMCN.
- Transmission facilities include all the field devices remotely located from the power stations and substations. Most of these devices are monitoring devices (such as PMUs) and control devices (such as actuators). They communicate with the control centers or nearby substations to provide status report of the monitored facilities.
- A substation distributes electricity to the consumers. A gateway is deployed for a substation to access WAMCN.

3.2 *Business Network*

The business network consists of the components of electricity market regulator, smart meter service provider, demand responder, and electricity market participants. As shown in Fig. 4, they are connected via an IP-based virtual private

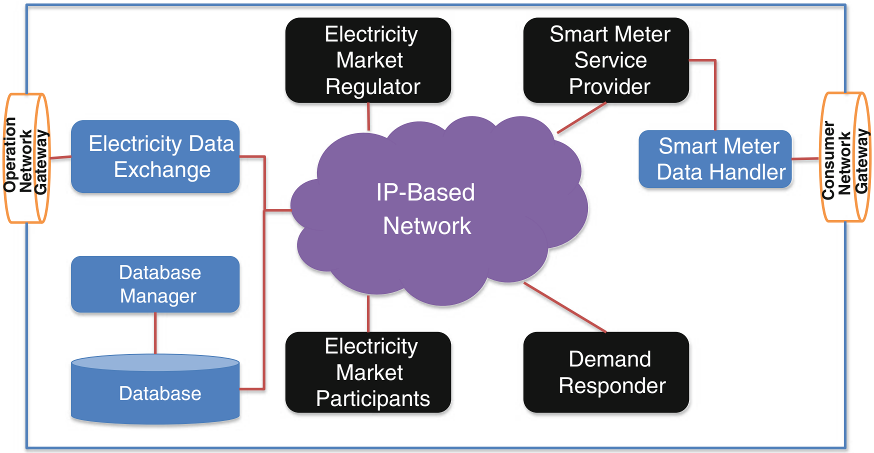
Electricity Market Regulator
Smart Meter Service Provider
Operation Network Gateway
Electricity Data Exchange
IP-Based Network
Smart Meter Data Handler
Consumer Network Gateway
Database Manager
Database
Electricity Market Participants
Demand Responder

Fig. 4 Business network [17]

network (VPN) and supported by a database manager that manages the electricity market information. They are described as follows.

- An electricity market regulator refers to the government or quasi-government organization which regulates the market.
- Smart meter service providers are the utilities that provide smart metering services to the end users.
- A demand responder refers to an electricity utility that attempts to alter the aggregate electricity consumption by the customers so as to match total consumption with the total power generation. To achieve this, the utility may provide incentives to the end users to either reduce consumption when the total demand is high, via differential pricing, or to agree to switch off some appliances on demand, via reduced utility rates.
- Electricity market participants are those that trade electricity.

3.3 Consumer Network

As shown in Fig. 5, consumer network is a local area network at a consumer premises. It may be located in one residential unit, or may connect multiple units. The major components are as follows:

- A smart controller coordinates the entire consumer network. It is responsible for switching on or off loads automatically according to the current grid operating status based on agreed contracts, analyzing smart meter data, and managing the local energy storage.

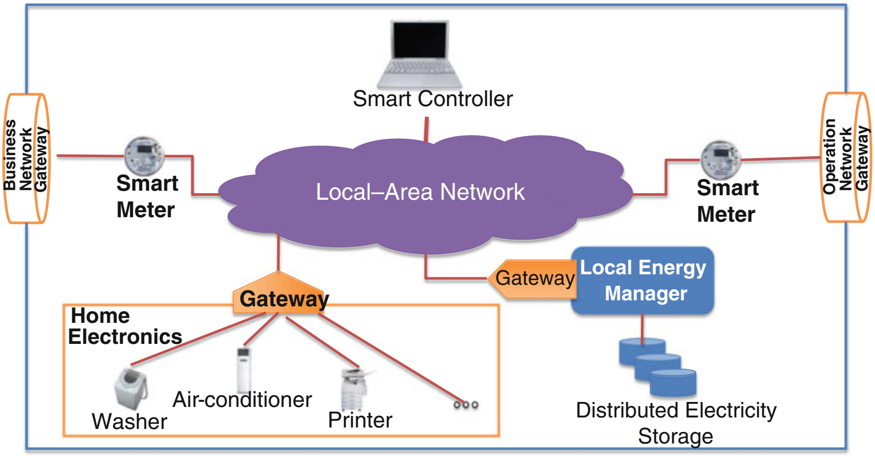

Fig. 5 Consumer network [17]

- A smart meter, which connects to operation network and business network, estimates the electricity usage schedule and sends it to operation network. It also receives real-time electricity rates from business network.
- Home electronics or appliances.
- A local energy manager handles the energy generation and storage at the consumer premises.

Communications among the three entities are required for an effective smart grid.

The communication between operation network and business network requires the highest level of reliability and security, as they form the backbone of the entire smart grid network. The communication between operation network and consumer network also requires high security, and since customer usage schedule will be transmitted to operation network, customer privacy must be ensured. The communication between business network and consumer network, on the other hand, requires high data availability and high reliability, but relatively less stringent security. As will be discussed later, there may be a trade-off between security and QoS requirements.

4 Communication Requirements

It has been advocated [19] that an electricity communication superhighway is required for supporting generation, transmission, substations, consumers, and distribution and delivery controllers. One major challenge is the development of a communication infrastructure to support universal connectivity and system-wide real-time monitoring. Multiple recipients must be able to receive up-to-date system status information, with various latency and rate requirements. In particular, the following communication requirements have been identified [17]:

(1) Capability to handle large volume of data: To enable real-time monitoring and control, deployment of such equipment as PMUs is required. The time resolution of PMU data is in milliseconds, and with a large number of PMUs deployed, the amount of such sensor data will be huge. There will also be large amount of data generated by the power generators, the consumers, and the distribution system. Therefore, the total amount of data generated will be many times the amount of data generated today. The brute force approach to solving these data deluge problem is to install additional transport capacity, probably at prohibitively high costs. But perhaps a more important question is whether we can process and effectively utilize all the data generated. In Li [20], three ways are proposed to handle the large volume of data. Firstly, data redundancy can be reduced by exploiting the spatial and temporal correlation of data. Secondly, adaptive messaging may be used. This calls for different QoS and different levels of security protection for different types of data, i.e., there will be a trade-off between QoS and security protection. Finally, it is desired to transform data to knowledge. After all, even if one can build a communication infrastructure to transmit all data to the operator, he will not be able to handle all of it. Instead, one may transform the deluge of data into specific events, and only send information of the occurrence of certain events to the operator. This will require domain-specific expertise and the development of data-to-knowledge transformation techniques, perhaps based on artificial intelligence.

(2) Extensive coverage: The network must cover the whole power system, including power generation, distribution, and consumption at the customer premises.

(3) QoS support: The system must be flexible to accommodate different reliability, delay, and throughput constraints. As mentioned earlier, there may be a trade-off between QoS and security requirements.

(4) Cyber security: The system must be secure from cyber attacks. This is such an important requirement that we will devote the next section to it.

5 Security and Privacy Requirements

The power grid is perhaps the most important national infrastructure in many countries. Secure and privacy-preserving communications are crucial to smart grid operations. Cyber security experts observed that some types of smart grid sensors can be easily hacked [21]. In addition, worms can spread easily among smart grid sensors [22]. Li et al. [23] has identified several potential attacks on smart grid:

(1) Distributed denial-of-service (DDoS) attack: In a DDoS attack, hacked sensors, which may be geographically distributed, are instructed by the hacker to simultaneously send a large volume of traffic to a victim sensor or to the control center. The victim sensor or control center will be overwhelmed by the huge volume of traffic, and normal data cannot be handled properly. Therefore, it is necessary to develop methodologies to enable a sensor or control center to differentiate between authentic and bogus traffic, and to identify malfunctioning equipment.

(2) Simultaneous shutdown attack: An attacker can pretend to be a control center and send fake control messages to command sensors and other system devices to shut down, thus rendering the smart grid ineffective. Therefore, one must ensure the confidentiality, integrity, and authenticity of control messages.

(3) Fake demand for power: An attacker can intercept and alter the estimated usage schedules from the smart meters to operation network, to dramatically increase or decrease the demand for power. This may lead to power imbalance in the system and cause power failures. Again, it is important to ensure the confidentiality, integrity, and authenticity of the data transmitted.

Other major security and privacy problems have also been identified and studied [24, 25]. For the communication between the control center and the smart meter, it can be proved that the statistical analysis approach cannot protect the system from false data injection attacks [26]. The statistical analysis approach will not work anyway since it requires the system to handle a large volume of data in real time, and the control center of the smart grid will not be able to give a timely response. In addition, the smart meter has been identified as the point of weakness of the AMI and of the smart grid communication system [27]. As the smart meter is located at the customer premises, it is difficult for the control center to protect it from potential attackers. Moreover, a smart meter is an inexpensive device and its memory and processing power are too limited to run complex protective measures. As a result, it is possible for attackers to hack its stored data [28] or even reverse engineer and modify its logic [29]. Therefore, smart meters can be considered as the most vulnerable components in smart grid. In Chim et al. [30], a three-layer architecture, as shown in Fig. 6, is proposed to study the security and privacy problems for the communication between the smart meter and the control center of a smart grid.

At the top layer resides the control center of the power operator. At the middle layer are the substations in the distribution network, and each substation is responsible for the power supply of a service area. The smart meters, placed at the customer premises, are located at the lowest layer. A smart meter communicates

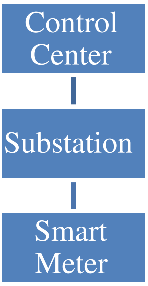

Fig. 6 Three-layer architecture for smart meter communications

with the control center via the substation in its service area. The control center may be a single server located inside the power plant or may be geographically distributed.

Under this three-layer model, the following security and privacy requirements have been identified:

(1) Message authentication: Each message sent by any smart meter should be checked to confirm that it is valid.
(2) Identity privacy preservation: The real identity of the customer should be confidential to everyone, including the power operator, to protect the privacy of customers.
(3) Message confidentiality: The content of the message sent by any smart meter to the control center should be unknown by any third party.
(4) Traceability: The total amount of power used by each customer in a certain service period should be known by the power operator (i.e., the control center), so a proper electricity bill can be prepared.

In Chim et al. [30], a privacy-preserving advance power request paradigm is proposed for smart grid. Presently, there is no need for a customer to inform the power utility how much electricity he/she will require. The power utility estimates the electricity demand (the load) based on historical and other factors and generates enough electricity to satisfy the load. Spinning reserves may be required to cover any shortfall due to load underestimation. Excess generation due to an overestimation of the load and the spinning reserves lead to waste. Under this proposed paradigm of advance power request, power is generated based on explicit customer demands. A customer is required to submit daily electricity usage plans, i.e., the required electricity required at hourly intervals throughout the day. These requests can be sent with different advance notices, such as 1 day ahead or 1 week ahead, but not in real time. This process may be automated by the smart meter, which communicates with all household appliances and stores the usage profile of the customer, and predicts the power usage for the day based on artificial intelligence or other techniques. Upon receiving all the electricity usage plans from all customers in its service area, the power operator schedules its power generation. A similar power request model was described in Li et al. [23]. Since the electricity usage plan includes the usage pattern of the customer, it is important to keep it private. In addition, one must ensure a customer does not make excessive power requests on purpose.

Following the three-layer model as shown in Fig. 6, and targeting the four security and privacy requirements identified, a privacy-preserving advance power request (PPAPR) scheme is proposed [31]. It consists of four modules, namely system start-up, credential request, power usage plan submission, and reconciliation. They are described as follows:

(1) System start-up: In a public key infrastructure (e.g., RSA), each party is assigned a public (known to everyone) and private (known only to itself) key pair. A key is just a string of "0" and "1" bits. When A wants to send a message to B, A encrypts the message using B's public key. B then uses its private key to decode the message. A also uses its private key to generate a digital signature on the message, and B can use A's public key to verify the signature. In the proposed PPAPR scheme, during system start-up, the control center assigns itself an RSA public and private key pair to sign credentials and for customers to encrypt messages to it. Before a new smart meter is put into service, it must be registered and assigned a unique identity.

(2) Credential request: At the beginning of each service period, say each month, customers request a certain number of credentials (or tickets) from the control center for the power usage for that service period. Customers are authenticated using their real identities. Each customer (via his/her smart meter) sends credential-signing requests to the control center. Each credential is of the format <CID, DOI>, where CID is a unique credential identity of each credential and DOI is the issue date that the credential. By presenting a credential, a customer can request V units of power. In PPAPR, all credentials are generated by customers. To make a credential anonymous, a customer first blinds it using a blinding factor (i.e., mixes it with some random components, so none can recognize its original content based on the blind version) and sends it to the control center. The control center signs the credential using its private key and sends it back to the customer. The customer performs some computation to remove the blinding factor in order to obtain the control center's signature on the credential. To prevent a customer from generating an invalid credential (e.g., CID already used or outdated DOI), a customer has to generate n times more credentials using different CIDs and blinding factors, where n is predetermined by the control center. For each n credentials, the control center randomly challenges the customer to open $(n - 1)$ of them and verify the details in them. If the information in all the opened credentials is valid, the control center signs the remaining one using its private key. Otherwise, the control center does not sign the credential and returns an error message to the customer. The control center computes and records the number of credentials N_{total} it has signed for that customer. Recall that the control center's public key is known by everyone, while its private key is only known to itself. Thus, its signature can be

verified by everyone, but can only be generated by it. Also note that although all credentials are known by the customers during generation, it will not cause any security problem because a credential is valid only if it contains the control center's signature.

(3) Power usage plan submission: The smart meter estimates and constructs a power usage schedule and attaches enough credentials of power units to it. The power usage schedule and credentials are encrypted using a randomly generated session key, and the session key is encrypted using the control center's public key, and the whole encrypted block is transmitted to the control center. Upon receiving the message, the control center obtains the session key using its private key and obtains the power usage schedule as well as the credentials using the decrypted session key. It then validates each credential by checking against its own signature and ensuring DOI is not outdated. It also records the credential identities CIDs into its local database so that the same set of credential identities cannot be reused. The control center then schedules appropriate control decisions to adjust the amount of power generated.

(4) Reconciliation: At the end of each service period, reconciliation will be performed and a bill will be generated. Customers need to be authenticated using their real identities. The smart meter of a customer sends all the credentials that it has not used to the control center. The control center then checks the credentials, counts the unused credentials N_{unused}, computes the total used credential Nused as $N_{\text{total}} - N_{\text{unused}}$, and charges the customer accordingly.

6 Conclusions

The smart grid is an attempt to utilize ICT on the power grid to solve the instability problem due to renewable energy sources. The smart grid also enables customer participation in such applications as differential pricing and demand response and promises improved grid operating efficiencies, self-healing capabilities, and resiliencies against cyber attacks. Deployment of smart grid requires technologies on sensing and measurement, advanced control methods, advanced components, improved interfaces and decision support, and integrated communications. To achieve the full functionalities of such smart grid enabling technologies, communication technology plays a fundamental role. In this chapter, we focus on the communication technology of smart grid. We describe a communication-oriented smart grid framework and identify the communication requirements, and the security and privacy requirements.

Acknowledgment This chapter republishes three figures from the paper "Communication-oriented smart grid framework" by Wen, M.H.F.; Ka-Cheong Leung; Li, V.O.K., Proc. IEEE International Conference on Smart Grid Communications, Brussels, Belgium, Oct 2011. Permission for reusing the figures has been granted by IEEE.

References

1. Myles P et al (2011) Electric power system asset optimization. DOE/NETL-430/061110, 7 Mar 2011
2. EC (2006) European smart grids technology platform: vision and strategy for Europe's electricity networks of the future. European Commission, Directorate-General for Research, Sustainable Energy Systems, EUR 22040
3. Electric Power Research Institute (2004). IntelliGrid: at a glance. Available at. http://intelligrid.info/
4. Department of Energy (2003) Grid 2030: a national vision for electricity's second 100 years, US
5. NIST (2010) NIST framework and roadmap for smart grid interoperability standards. Release 1.0, NIST Special Publication 1108
6. Wu FF, Moslehi K, Bose A (2005) Power system control centers: past, present and future. Proc IEEE 91(11):1890–1908
7. Ree JDL, Centeno V, Thorp JS, Phadke AG (2010) Synchronized Phasor Measurement Applications in Power Systems. IEEE Trans Smart Grid 1(1):20–27
8. National Energy Technology Laboratory (2007). U.S. Department of energy, modern grid initiative. https://www.smartgrid.gov/sites/default/files/pdfs/a_systems_view_of_the_modern_grid.pdf
9. Lam AYS, Li VOK (2010) Chemical-reaction-inspired metaheuristic for optimization. IEEE Trans Evol Comput 14(3):381–399
10. Xu J, Wen MHF, Li VOK, Leung KC (2013) Optimal PMU placement for wide-area monitoring using Chemical Reaction Optimization. In: Proceedings of IEEE PES innovative smart grid technologies conference, Washington DC, USA
11. Varaiya PP, Wu FF, Bialek JW (2011) Smart operation of smart grid: risk-limiting dispatch. Proc IEEE 99(1):40–57
12. Kempton W, Tomic J (2005) Vehicle-to-grid power fundamentals: calculating capacity and net revenue. J Power Sources 144(1):268–279
13. Hui SY, Lee CK, Wu FF (2012) Electric springs—a new smart grid technology. IEEE Trans Smart Grid 3(3):1552–1561
14. Aggarwal A, Kunta S, Verma PK (2010) A proposed communication infrastructure for the smart grid. Proc IEEE ISGT 2010:19–21
15. Chen KC, Yeh PC, Hsieh HY, Chang SC (2010) Communication infrastructure of smart grid. Proc IEEE ISCCSP 2010:3–5
16. Rahimi F, Ipakchi A (2010) Demand response as a market resource under the smart grid paradigm. IEEE Trans Smart Grid 1(1):82–88
17. Wen MHF, Leung KC, Li VOK (2011) Communication-oriented smart grid framework. In: Proceedings of IEEE international conference on smart grid communications, Brussels, Belgium
18. Jin T, Mechehoul M (2010) Ordering electricity via internet and its potentials for smart grid systems. IEEE Trans Smart Grid 1(3):302–310
19. Gellings C (2003) Smart power delivery: a vision for the future. EPRI J 9
20. Li VOK (2013) Smart sensing and adaptive messaging in smart grid. In: Workshop on clean energy and environment, University of Hong Kong initiative on clean energy and environment, Hong Kong. http://icee.hku.hk/activities/workshops/ICEEWorkshop_CleanEnergyEnvironment2013.html, 30 Apr 2013
21. Meserve J (2009) Smart grid may be vulnerable to hackers. CNN.com (Available online. http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html), 21 Mar 2009
22. Clemente J (2009) The security vulnerabilities of smart grid. J Energy Secur (Available online. http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96), 18 June 2009

23. Li VOK, Wu FF, Zhong J (2010) Communication requirements for risk-limiting dispatch in smart grid. In: Proceedings of IEEE workshop on smart grid communications, Cape Town, South Africa
24. Khurana H, Hadley M, Lu N, Frincke DA (2010) Smart-grid security issues. IEEE Secur Priv Mag 8(1):81–85
25. Security (2010) The smart grid interoperability panel cyber security working group second draft NISTIR 7628 smart grid cyber security strategy and requirements
26. Liu Y, Ning P, Reiter MK (2009) False data injection attacks against state estimation in electric power grids. In: Proceedings of the CCS'09, pp 21–32
27. Chan CB, Chim TW, Yiu SM, Li VOK, Hui LCK (2013) Smart meter obfuscation and attestation using non-deterministic execution sequence. Submitted for publication
28. Vigo R, Yüksel E, Ramli C (2012) Smart grid security: a smart meter-centric perspective. In: Telecommunications forum, pp 127–130
29. King C (2012) Smart meter security: the human element. Gigacom. http://gigaom.com/cleantech/smart-meter-security-the-human-element, 13 Apr 2012
30. Chim TW, Yiu SM, Hui LCK, Li VOK (2011) PASS: privacy-preserving authentication scheme for smart grid network. In: Proceedings of the IEEE SmartGridComm, Brussels, Belgium
31. Chim TW, Yiu SM, Hui LCK, Li VOK (2012) Privacy preserving advance power reservation. IEEE Commun 50(8):18–23