SIP (2015), vol. 4, e5, page 1 of 20 © The Authors, 2015.

doi:10.1017/ATSIP.2015.9

OVERVIEW PAPER

A survey on smart grid communication system

MILES H.F. WEN[1], KA-CHEONG LEUNG[1], VICTOR O.K. LI[1], XINGZE HE[2] AND C.-C. JAY KUO[2]

Concerns with global warming prompted many governments to mandate increased proportion of electricity generation from renewable sources. This, together with the desire to have more efficient and secure power generation and distribution, has driven research in the next-generation power grid, namely, the smart grid. Through integrating advanced information and communication technologies with power electronic and electric power technologies, smart grid will be highly reliable, efficient, and environmental-friendly. A key component of smart grid is the communication system. This paper explores the design goals and functions of the smart grid communication system, followed by an in-depth investigation on the communication requirements. Discussions on some of the recent developments related to smart grid communication systems are also introduced.

Keywords: Communication system, Cyber security, Smart grid

Received 29 November 2014; Revised 28 June 2015; Accepted 28 June 2015

I. INTRODUCTION

The growing concerns about the emission of greenhouse gases such as carbon dioxide and the desire for more reliable and efficient electricity transmission and distribution are driving the development of a highly secure, reliable, and environmental-friendly power grid system, namely, the smart grid [1].

The Energy Information Administration projected a total increase of about 1.8% in energy-related carbon dioxide emissions, from 5498 million metric tons in 2011 to 5599 million metric tons in 2040 [2]. Concerns with global warming prompt the adoption of renewable energy sources in the grid. A report by the Renewable Energy Policy Network for the 21st Century (REN21) shows that there is a stable rapid growth in utilizing renewable energy during the period from 2007 to 2013. The wind power capacity has grown an average of 25% annually, solar photovoltaics by 60%, concentrated solar thermal power by 20%, and biodiesel production by 17%. Moreover, the report also indicates that over 100 countries around the world have enacted some policies relating to the adoption of renewable energy [3]. Unfortunately, due to the intermittent nature of renewable sources, many existing power grids will experience severe stability problems when a large fraction of the energy generated comes from renewables. This further stimulates the needs in developing smart grid.

In addition to the environmental concerns, security, especially cyber security, has received much attention lately. In 2009, a report showed that some cyber-spies had penetrated the U.S. electricity grid control system and laid some spyware in the system. These malwares could be extremely dangerous because, once activated by the attackers, the electricity service could be disrupted or even totally paralyzed [4]. Since 2010, the US Department of Energy has invested more than $100 million in numerous R&D projects in industry, universities, and national laboratories to protect the nation's power grid from potential cyber attacks [5, 6].

Besides the environmental and security factors mentioned above, there is the traditional reliability issue. People have been discussing the reliability issue of an electricity network ever since its birth. However, the big blackout in the USA in 2003 has demonstrated that reliability is lacking in the traditional electricity grid. Another report has indicated that the US electrical grid is getting less reliable over the recent years [7, 8]. With smart grid, reliability is expected to be greatly enhanced.

In designing smart grid, we have identified the ultimate goals as follows:

(i) Adopt orderly renewable energy penetrations to protect the environment;
(ii) Make the grid highly resilient against disturbances caused by operation errors, malicious attacks, and natural disasters;
(iii) Provide reliable, secure, and high-quality electricity services to consumers; and
(iv) Get consumers to actively participate in the energy market and smooth the electricity demand or

[1]Department of Electrical and Electronic Engineering, Chow Yei Ching Building, The University of Hong Kong, Pokfulam Road, HKSAR, China
[2]Department of Electrical Engineering, Hughes Aircraft Electrical Engineering Building, 3740 McClintock Avenue, Los Angeles, CA 90089-2564, USA

Corresponding author:
M. H. F. Wen
Email: mileswen@eee.hku.hk

consumption curve for effective power generation-consumption balancing.

The communication infrastructure is key to achieving the aforementioned goals. For instance, one of the biggest challenges in increasing renewable energy sources in the grid is due to their stochastic nature, rendering stable grid operation very difficult. However, if a robust communication network is available, enabling better renewable predictions and real-time automated regulations, we may be able to overcome this challenge.

The objective of this paper is to survey the communication system of smart grid, identifying the key issues and directions for future research. Unlike other related work such as [9–13], our work intends to give readers an overview of the entire smart grid communication system, together with details on its requirements. To be specific [9], discusses the background and recent development on using the electric power line as a medium to support last mile communications in smart grid. Gharavi and Hu propose a backpressure-based packet scheduling algorithm for load balancing on communication traffic in a mesh network for last mile communication in smart grid in [10]. Fan *et al.* focus on communication challenges to achieve interoperability and future smart metering networks in [11], Fang *et al.* explore smart infrastructure system, smart management system, and smart protection system in [12], and Lo and Ansari summarized the progressive integration of different communication technologies into the old power system in [13]. Our work concentrates on and gives an in-depth survey on the communication systems for smart grid by discussing the communication requirements. We will facilitate the design and development of the proper communication systems for smart grid.

The paper is organized as follows. After a brief introduction, we will introduce the general concepts of smart grid, including its design goals, architecture, and functions, in Section II. This will familiarize readers with the general ideas about smart grid. Then, we will investigate in details the communication requirements imposed on smart grid in Section III. Some recent developments in smart grid communication systems will be discussed in Section IV, followed by an introduction to some open research issues in Section V and the conclusion in Section VI.

II. OVERVIEW OF SMART GRID

In this section, we will explore how smart grid differs from the traditional one through studying its design goals. Afterwards, we shall introduce its architecture and major functions.

A) Design goals

According to [14–23], the design goals of smart grid are environmental friendliness, reliability, flexibility, security, quality, and efficiency, as shown in Fig. 1.

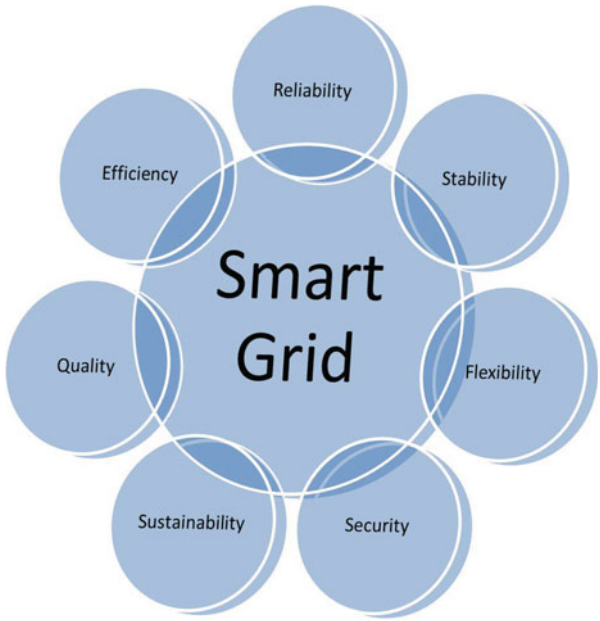

Fig. 1. Design goals of smart grid.

(i) *Sustainability*: In order to reduce the emissions of green house gases as well as other wastes during traditional power generation, high penetration of renewable energy resources, such as wind and solar, is expected in smart grid. Due to the stochastic nature of renewables, maintaining the grid's operational stability becomes one of the key challenges in smart grid development.

(ii) *Reliability*: As with the traditional grid, smart grid needs to provide reliable services, despite the intermittent nature of renewable sources. The reliability of the grid system primarily refers to the probability of the grid to function properly without any failures [24, 25]. This further involves a feature of smart grid, named as *self-healing*. Self-healing refers to smart grid's capability to anticipate disturbances and carry self-restoration rapidly. Reliability has always been the focal area of study when designing the electricity grid. It affects the quality of power delivered to consumers [26].

(iii) *Stability*: According to [25, 27], the stability of an electric grid indicates its capability to continue intact operation following disturbances. This is a classic topic that many people have been working on. However, as more renewable energy penetration and less kinetic energy reserve are present in smart grid, the stability issues are yet to be properly addressed.

(iv) *Flexibility*: According to [28], smart grid needs to be evolvable and adaptable so as to accommodate the various challenges imposed on it due to the rapid changes of technologies, policies, and consumer demands on the electricity system. To achieve this, smart grid must be:

- able to accommodate a large number of communication technologies so as to allow the grid to integrate easily with different platforms as well as interoperate among different software and hardware; and

http://dx.doi.org/10.1017/ATSIP.2015.9

- flexible to accommodate both regional and organizational differences across its service areas, especially those relating to the energy consumption habits and availability of primary energy resources, such as wind, solar, and so on.

(v) *Security*: Unlike legacy power system, smart grid has placed much emphasis on security issues. The reason is straightforward. First, it is well known that the more complex a system is, the more vulnerable it is. Envisioned as an integration of power system, information system, and communication system, smart grid is an extraordinarily complex system with potentially numerous security vulnerabilities and threats. Due to the unique features of power grid, these vulnerabilities and threats are fairly easy to monetize. For example, manipulation of energy costs is quite common in legacy power systems, with an estimated loss of $6 billion in USA [29]. Moreover, a recent report has shown that the electric grid has been the target of many daily cyber-attacks and many utilities have not spent enough efforts in protecting their system [30]. Undoubtedly, this situation will get worse in smart grid, since people do not only save money but can also earn money easily by trading stolen electricity. More seriously, malicious adversaries or terrorists may be interested in launching large-scale attacks to smart grid with potentially unpredictable consequences. In view of these concerns, security has been regarded as one of the most important issues in the current development and the future deployment of smart grid. Simply put, the goal of security in smart grid is to maintain confidentiality, integrity, and availability as well as to protect user privacy. More specifically, envisioned smart grid system must be capable of preventing sensitive data from being exposed to unauthorized parties, or from being tampered with by others. Timely access to and use of data by authorized parties must be guaranteed as well. For privacy, future smart grid system must ensure that the use of data will not compromise individual's privacy. To achieve this goal, the unified efforts from different stakeholders, including government, consumers, industry, and academia are required.

(vi) *Quality*: The quality requirements of smart grid are twofold, namely, the power quality in a power system and quality of service (QoS) in a communication system. Power quality refers to the deviations of voltage or frequency from the expected values, which determine the capability of a power system to operate its loads properly [31, 32]. On the other hand, QoS refers to the capability of a communication system to provide different service levels, say, priorities, to different applications according to their requirements, including transmission latency, jitter, bandwidth, and so on [33].

(vii) *Efficiency*: Optimization is a key operation procedure for smart grid. By allowing active customer participation, the market becomes more efficient in resource allocation. By optimizing the electricity assets through an advanced distributed storage (DS) and a better control and monitoring system, energy utilities operate more efficiently.

B) The National Institute of Standards and Technology (NIST) architecture

In 2007, the NIST was assigned the task to design a smart grid architecture that "includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems" [34]. The Smart Grid Interoperability Standards Project of NIST was completed in 2012, aiming to bring in a very robust, flexible, uniform, and technology-neutral interoperable framework for smart grid [21]. The framework consists of seven entities, namely, Markets, Operations, Service Providers, Bulk Generation, Transmission, Distribution, and Customers, as shown in Fig. 2. Each of the entities, known as "domains", further encompasses its own actors, applications, and set of networks. These interconnected entities cooperate to support the smart grid functions. The role of each domain is summarized as follows:

(i) *Markets*: The market domain consists of electricity market participants and operators. This domain contributes to efficiently matching the energy production with consumption, through issuing real-time electricity

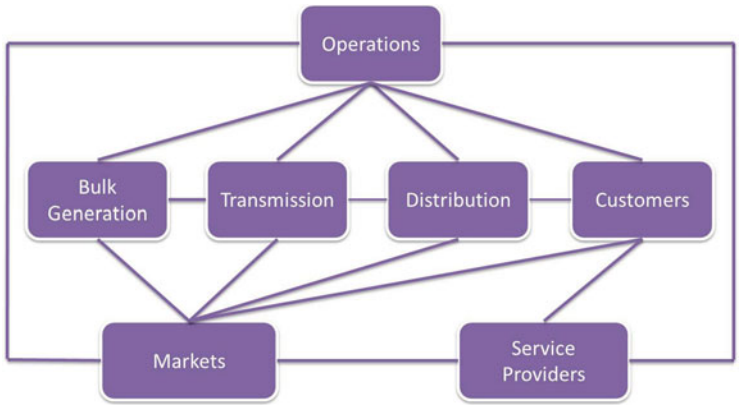

Fig. 2. NIST smart grid framework.

http://dx.doi.org/10.1017/ATSIP.2015.9

pricing signals. Markets support energy bidding, distributed energy resources (DER) aggregation, energy retailing, and so on. In addition, ancillary operations, such as frequency regulation and voltage support, are carried out based on information received from this domain.

(ii) *Operations*: Electricity service operators are in this domain. This domain aims to provide reliable and smooth operations in a power system. It is either physically connected or can communicate with all other domains. Various control and monitoring applications, such as supervisory control and data acquisition (SCADA) and energy management system (EMS), have their control centers in this domain. Moreover, many operational management applications, including fault management, asset maintenance, and operation planning, can also be found here.

(iii) *Service Providers*: A service provider is an organization that offers various electrical services to customers and utilities. This domain acts as a business intermediary among Operations, Markets, and Customers. It shares some communication interfaces and provides services to these three domains, and plays a critical role in the functionalities of these domains. Here, service support includes customer management, billing, and other emerging services.

(iv) *Bulk Generation*: Electricity generation plants are the primary actors in this domain. Bulk generation initiates the process of electricity provision and is typically directly connected to transmission. Such direct connection represents the most critical communications in smart grid. It interfaces with Operations, Markets, and Transmission to support generation control, power flow measurement, plant protection, and other applications. Most importantly, this domain aims to control greenhouse gas emission, and increase renewable energy penetrations with advanced storage devices for smoothing out the variability in energy generation.

(v) *Transmission*: Transmission facilities, such as long-distance overhead lines and transformers, reside in this domain. This domain works as the intermediary between Bulk Generation and Distribution. In this domain, efforts are spent primarily on two aspects, namely, transmission stability maintenance and energy loss reduction. It interfaces with Markets and Operations. Ancillary services are procured from the former, and then scheduled and operated by the latter, and finally delivered to Transmission. Most of the functions supported by this domain, such as line voltage monitoring and control, are carried out at transmission substations.

(vi) *Distribution*: Distribution facilities, including distribution transformers and underground cables, are the key entities in this domain. Distribution interconnects with Transmission, Customers, Markets, and Operations. It works closely with Operations to provide real-time management of power flows. It also works with Markets to provide real-time generation and consumption data. In addition to asset and line monitoring and control, this domain supports bi-directional power flows and distributed energy generation management, say, for photovoltaic cells placed at customer premises.

(vii) *Customers*: A customer generally refers to an electricity end user. Distributed electricity generation and storage facilities are also found in this domain. This domain can be further divided into three sub-domains, namely, household, commercial, and industrial. This domain is electrically connected to Distribution. It is activated mostly with the help of advanced metering infrastructure (AMI), which enables the communications with Distribution, Operations, Markets, and Service Providers. In this domain, applications, such as building/industrial automation and micro-generation, are supported.

C) Functions

Four general functions are provided in smart grid, namely, *advanced monitoring and control (AMC)*, *demand-side management (DSM)*, *generation and storage management (GSM)*, and *system protection (SP)*. These four functions play the most important role in smart grid operation and support various applications in smart grid.

(i) *AMC* refers to the function that continuously monitors and efficiently controls the entire electricity system. It is the most critical function in smart grid since its failure contributes to a very high proportion of the occurrences of disturbances in the past decades [35]. The traditional system serving this function is the several-decade-old SCADA system, which adopts a hierarchical architecture with remote terminal units (RTUs) collecting system data and master terminal units (MTUs) processing them and issuing control commands. Recently, two types of new systems, namely, wide-area measurement system (WAMS) and wide-area stability and voltage control system (WACS), have been developed to serve the AMC function for smart grid. These two systems aim to provide fast and reliable operations for smart grid, which in return contribute to the self-healing feature of smart grid. In the NIST smart grid architecture, this function primarily works in the Operations, Bulk Generation, Transmission, and Distribution domains.

(ii) DSM refers to the load management function that decides when to switch on or switch off loads to reduce the grid operation costs as well as the electricity charges of the consumers. The general idea of DSM is still very similar to the traditional paradigm, which involves either directly controlling the "interruptible loads", or stimulating consumers to shift their electricity usage via changing the electricity rates [36]. However, this function in smart grid involves the participation of more advanced technologies. For instance, the real-time control of the charging and discharging processes of electric vehicles (EVs), which is one of

http://dx.doi.org/10.1017/ATSIP.2015.9

the major interruptible loads in smart grid, will play a very important role in direct load control (DLC) in smart grid. Besides, with the help of advanced metering infrastructure, consumers will be stimulated to adjust their consumption behaviors by the adoption of dynamic pricing. This function works primarily in the Customers domain, being regulated according to information from the Service Providers, Markets, and Operations domains.

(iii) *GSM* is the function to manage various generation and storage devices, either distributed or centralized. It is an extension to the traditional generation dispatch function. That is, in addition to deciding which generators in a centralized power plant to switch in or off at any time in order to minimize the generation costs or protect particular generation plants, GSM extends to a highly distributed system and decides where and how much the excess energy generated should be stored. Moreover, environmental effects will also be the major factors that affect how GSM makes its decision. This function primarily works in the Operations and Bulk Generation domains, and may involve contributions from the Markets, Service Providers, and Customers domains, too.

(iv) *SP* refers to the function that carries out both preventive and corrective actions so as to make the entire system highly resilient against faults and disturbances, ultimately enabling the self-healing feature of smart grid. It is sometimes embedded in the system that provides the AMC function. In the existing power grid, the scheme that serves SP is known as special protection scheme (SPS) or remedial action scheme (RAS). The functionality of SP needs contributions from all seven domains of smart grid.

III. COMMUNICATION REQUIREMENTS

To develop the communication system for smart grid, the key is to understand its requirements. In this section, we investigate the requirements for the smart grid communication system to function properly. We carry out the investigation by classifying all requirements into four categories, namely, data transmission, cyber security, data privacy, and interoperability.

A) Data transmission

The data transmission requirements of the smart grid communication system primarily include *transmission rate*, *latency*, and *reliability*. Transmission rate determines the volume of data that can be sent to a destination through the communication network within a certain time. Latency refers to the time it takes a piece of data to reach a destination correctly. Reliability measures how likely a certain piece of data is received correctly. Since different functions of smart grid have very distinct requirements on data transmission, we are going to discuss the requirements for each of the four smart grid functions as follows.

For AMC, SCADA is the most widely used automation system in the traditional electricity grid. It consists of RTUs that collect system status data and actuate control commands and MTUs that process data received from RTUs and issue commands to them. These RTUs and MTUs communicate with each other via various communication technologies [37, 38]. However, SCADA was found lacking in fulfilling those specified transmission requirements and it provides inadequate situational awareness to operators, making them unaware of disturbances in neighboring control areas and eventually unable to limit the spread of disturbances [28, 39–41]. In order to alleviate the problem, a new system or an upgraded SCADA system for AMC must be developed, which must provide:

- High data acquisition rate so that a relatively large amount of data could be gathered for the system to make a better decision. For instance, when more advanced measurements, such as transmission line vibration [42] and substation transformer temperature [43], are needed for advanced control, considerable amount of data will be generated and transmitted through the network within a certain time limit.
- Low latency (<1 s) so that by the time the monitoring data reach the control center, they could give operators a better estimation of the current situation. It is worth noting that this low-latency requirement is just a general function-level specification. In March 2005, a standard specifying the detailed transmission time requirements for the automation system was released by IEEE, which brings the latency requirements to application levels [44]. However, this standard was published almost a decade ago, when the concept of smart grid had not been developed. Therefore, there is an urgent need to develop a new specification for smart grid latency requirements.
- High data reliability so that data gathered for real-time decision making can be correctly received by control centers (Fig. 3).

Working tightly with AMC, SP has very similar requirements, except that it will require extremely low transmission latency (usually not exceeding a few milliseconds [37]) and higher reliability, due to the fact that SP usually handles very severe emergencies that, if not solved within a short period, could cause disastrous or cascading failures of the entire system. In the traditional grid, SPS/RAS has been working with SCADA to serve SP for decades. SPS/RAS consists of a set of programs and devices that will protect against blackouts or brownouts when there are no faulty equipment in the power system [45, 46]. The architecture of SPS/RAS is almost identical to that of SCADA, except for some special devices (mostly protection relays) installed at necessary positions. However, it has been found that the traditional SPS/RAS works only for *pre-defined* emergency disturbances but responds extremely slowly to *arbitrary*

http://dx.doi.org/10.1017/ATSIP.2015.9

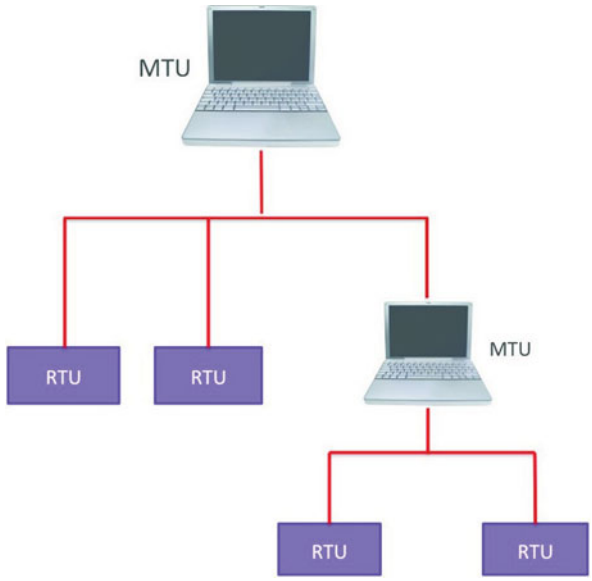

Fig. 3. An illustration of a simplified, hierarchical SCADA system.

contingencies. Hence, some changes must be made to alleviate the problem [47, 48].

Hence, due to the inadequacy of SCADA to support AMC and SPS/RAS for SP, two new systems, namely, WAMS [49] and WACS [47], have been developed in recent years. Both systems are designed to satisfy the requirements stated above.

- WAMS provides power operators with advanced monitoring capabilities. It utilizes phasor measurement units (PMUs) to collect GPS-synchronized dynamic power system data (with synchronization error <1 ms) at a very high sampling rate (up to 60 samples/s) and phasor data concentrators (PDCs) to concentrate PMU data and deliver them to control centers. This can thus help improve the security, stability, and reliability of the power system. Interested readers can refer to [49–55] for details. A simple illustration of the WAMS architecture is exhibited in Fig. 4.
- WACS is the modern grid wide-area control system. It primarily utilizes data gathered by WAMS and carries out real-time stability and voltage control (e.g. boosting the exciter on a synchronous generator) on the power grid. WACS is also sometimes called wide-area protection system (WAPS) since it also serves the SP function by responding to arbitrary emergency disturbances in the system. Hence, it is considered as a supplement and a partial substitution of SPS/RAS [47, 56–58].

Although WAMS and WACS are newly developed systems for supporting AMC in smart grid, it is desirable for them to be compatible with SCADA since electricity companies have made huge investments on SCADA during the past decades [57]. Efforts have been made by employing some alternative techniques to utilize phasor measurements obtained by WAMS as additional data to carry out state estimation in the modern EMS [59, 60].

In December 2011, PMU data format has been standardized in IEEE STD. C37.118.1 and IEEE STD. C37.118.2 [61, 62].

IEEE STD. C37.118.1 introduces the fundamentals of PMU data, including synchrophasor representations and synchrophasor measurement requirements. IEEE STD. C37.118.2 focuses on the PMU data transmissions by introducing the WAMS network and defining the transmission protocol and data format. Moreover, an experimental scheme for PMU data communications over IP network is also introduced in this document. A more recent standard published by IEEE in 2013, IEEE STD. C.37.242-2013, has provided a guideline for calibration, testing, and installation of PMUs [63]. However, the functionality of PDC is not

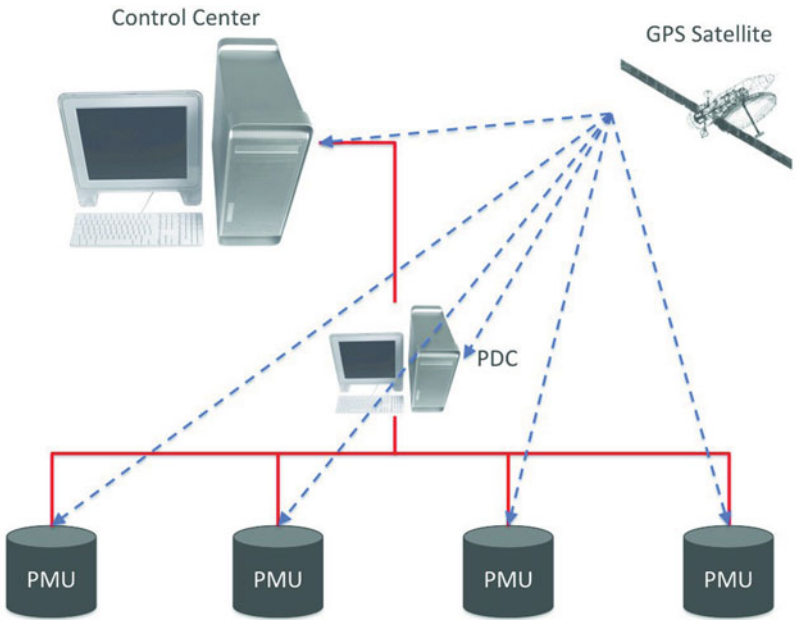

Fig. 4. An illustration of a WAMS system.

http://dx.doi.org/10.1017/ATSIP.2015.9

standardized yet, though two PDC designs have been proposed in [64, 65]. A recent study by Wen et al. investigated the possibility of installing extra PDC in a WAMS network to reduce the total traffic [55].

Since the functionality of GSM partly relies on AMC, the data transmission requirements for GSM are similar to those for AMC. However, GSM will have to handle numerous distributed generation (DG) and storage units, some of which are intermittent renewable generation units. It will require considerable amount of data to be generated and transmitted through the network for real-time management.

As discussed in Section II-C, the functionalities of GSM are twofold, namely, more advanced generation dispatch function on the centralized generation plants, and efficient management of DERs. Recent developments of the former include new generation dispatch schemes, such as risk-limiting dispatch [66–69], while those for the latter include the introduction of a new concept, called *microgrid*.

Microgrid, as illustrated in Fig. 5, is a subsystem of a power grid consisting of DG and DS units that can disconnect themselves from the grid in order to isolate the microgrid's loads from disturbances automatically. In other words, microgrid is a subsystem of the power grid that can operate when it is: (1) connected to the grid, (2) islanded from the grid, or (3) transitioning between these two modes. Besides, microgrid has a nice plug-and-play functionality that allows DG units and loads to come and go smoothly and rapidly in real time, thus accommodating the stochastic nature of renewables [70–76]. Promising as microgrids are, they requires carefully designed distributed monitoring and control mechanisms to operate optimally. This will put additional loads to the smart grid communication system and, therefore, additional communication bandwidth should be reserved when one designs communication systems for a microgrid-enabled smart grid [77].

DSM generally refers to two different techniques. The first technique is demand response (DR) that requires customer participation by responding to changes in electricity prices [78]. The other function is DLC that directly manages some of the interruptible loads, such as air conditioners and heaters, to minimize both the system operation costs and consumer consumption costs [36, 79, 80].

As compared to the other three functions, DSM has relatively looser requirements on data transmission. Except for the requirement of a highly reliable communication link, it has the following requirements:

- Lower average but bursty transmission rate compared to that of AMC. Although DSM involves the participation of a large number of nodes, the transmission load for messages at each node is moderate. Take AMI as an example. Typically, price update signals are transmitted to smart meters at the consumer end once per hour or per half an hour.
- Relatively higher transmission latency (although still within a few seconds) could be tolerated by DSM.

DR in smart grid is primarily achieved with the help of AMI. A network of smart meters that allows consumers to respond actively to grid operation status signals by means of real-time pricing [81–83]. In order to allow consumers to respond in an optimal manner, some automated DR systems are to be developed [84–86].

Besides DR, plug-in electric vehicles (PEVs) can play an important role in DLC for smart grid. As exhibited in Fig. 6, PEVs can play three different roles, namely, storage, source, and load, interchangeably. Properly managed, they will have a great potential for improving the performances of smart grid operations. For instance, the aggregated PEVs could help regulate the voltage profile, reduce costs and emissions, improve frequency regulations, and so on [87–91].

Combining the results from [92, 93], the data transmission requirements of each of the four functions are summarized in Table 1.

B) Cyber security

In Fig. 2, each domain is composed of a certain number of actors which may be sub-systems, applications, devices, or

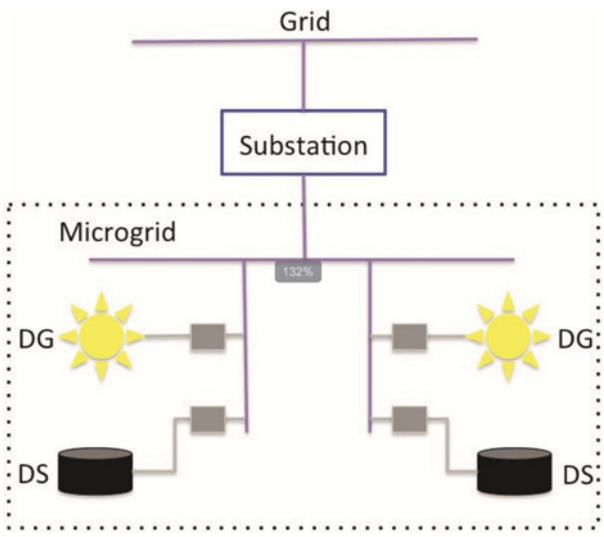

Fig. 5. A typical microgrid.

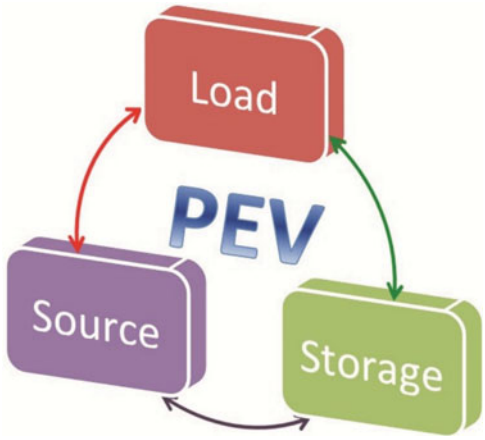

Fig. 6. The role of a PEV in smart grid.

http://dx.doi.org/10.1017/ATSIP.2015.9

Table 1. Data transmission requirements for the four smart grid functions.

	Rate (kbps)	Latency	Reliability (%)
AMC	56–128	15–200 ms	99.0–99.99
DSM	9.6–56	500 ms–5 min	99.0–99.99
GSM	56–256	200 ms–1 s	99.0–99.99
SP	56–128	10–200 ms	99.9–99.999

other participants in smart grid. Each actor may exchange data with other actors within the same domain or in other domains. In such a large and highly interconnected complex system, cyber security is a critical issue for the reliability of the whole system as mentioned in Section I, especially when the public communication network (e.g. Internet) is introduced and adopted.

Compared with physical attacks, cyber attacks, which are not constrained by distance, are generally less risky, cheaper, and much easier to coordinate and replicate. With a little basic knowledge about the structure and operation of the network, adversaries are able to launch various attacks wherever they are through a set of interconnected computers or even just smart phones. Many incidents indicate the seriousness of cyber security. In March 2007, researchers at the Department of Energy's Idaho lab launched an experimental cyber attack causing a generator to self-destruct [94]. In 2008, evidence showed that hackers had penetrated power systems and caused a power outage affecting multiple cities [95]. Besides, virus, worms, and other malwares raise other cyber security issues in smart grid. In 2009, for example, a security consulting firm showed a simulation in which more than 15 000 out of 22 000 homes had their smart meters hijacked by a worm within 24 h [96]. More recently, researchers have already created a worm that spread among smart meters [29].

In order to mitigate these concerns, cyber security in smart grid aims at maintaining availability, integrity, and confidentiality of the entire system. It is worth noting that, different from an information and communication system, a power system is concerned more about availability than integrity and confidentiality. However, with the increasingly complex interactions among different components in smart grid, massive sensitive data are produced and propagated. Confidentiality is becoming an increasingly important issue in the development of smart grid.

(i) *Availability*: Simply put, availability requires a system to provide the right information to the right people within the right time period. Take the well-known blackout in 2003 as an example. Although the incident was initially caused by an equipment problem, the ongoing and cascading failures were primarily due to the unavailability of information at the control center about what had happened in the system. In smart grid, many events may cause traffic congestion and hence increased message delay, thereby causing the availability problem. Typical examples include denial-of-service (DoS) attacks, malwares, and equipment malfunction.

(ii) *Integrity*: Message integrity is another critical factor for the reliable operation of smart grid. Without effective protection, it is not difficult for a user to modify his/her power consumption data recorded by a smart meter so as to reduce his/her electricity charge. If some malicious hackers take advantage of this by modifying a power demand message, the utility may generate and deliver more than enough electricity to the system. This may either cause the wastage of electricity, or compromise many digital sensitive devices. More seriously, a large scale attack might be mounted through fabricating control data and controlling smart meters. All controlled smart meters would be switched off simultaneously.

(iii) *Confidentiality*: Confidentiality in smart grid prevents the transmitted data from being exposed to unauthorized parties and has the following two major benefits. First, it is difficult for adversaries to intercept and analyze the network data. For example, with an effective encryption scheme, an adversary who does not have access to the secret key is unable to decrypt any intercepted ciphertext for the corresponding plaintext. Second, it is critical to protect user privacy, which is to be discussed.

For the availability issues, a variety of monitoring tools and techniques can be adopted in smart grid system to detect attacks and abnormal activities or conditions, such as intrusion detection system, intrusion prevention system, malicious code protection system, and network monitoring system. Compared to enterprise systems, a control system has a relatively stable number of users, a limited number of protocols as well as a regular set of communication patterns. All these features may simplify the design and implementation of the above monitoring tools and techniques.

Cryptography-based schemes are usually used to cope with the integrity and confidentiality issues. Due to the scale and limited resources (e.g. central processing units, memory, and communication bandwidth) of devices, the conventional techniques in computer networks may not perform well in smart grid. Many challenges and issues have to be addressed. Specific adaptations or novel algorithms have to be designed for smart grid. In [97], several smart grid security issues were discussed, including the management problems of a large-scale public key infrastructure (PKI) system and the updating problems of cryptographic keys due to the limited capabilities of processors. The PKI implementation issues in smart grid were investigated in [98]. Besides, a series of trial standards and guidelines are now available [21, 99–102], some of which will be discussed in later sections.

C) Data privacy

To achieve high intelligence and automation in a smart grid system, smart meters are required to provide some fine-grained details in the power consumption data of a user within a much shorter time interval (say, 15 min) than before. This transformation from aggregate data to

http://dx.doi.org/10.1017/ATSIP.2015.9

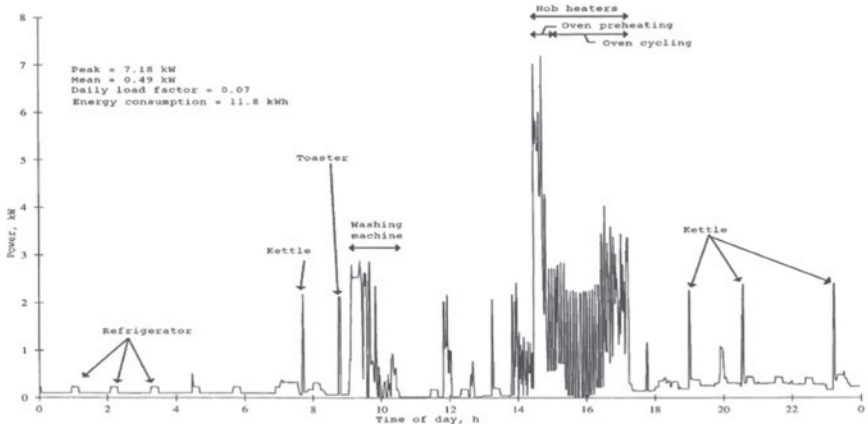

Fig. 7. Power usage to personal activity mapping [103].

granular data inevitably brings in the privacy issues. Using some technologies like non-intrusive load monitoring, daily activities of individuals are recorded as shown in Fig. 7. Due to the interoperability requirement of smart grid, many parties besides the utilities have access to such records. More seriously, it is not difficult for data analysts to derive further information that may invade user privacy. For example, the number of daily heating cycles of a water heater may indicate the number of people living in the house. The electricity consumption of a home may show whether it is occupied or not. The daily usage of electricity may reflect when the home owner wakes up, leaves for work, and so on. Besides, the charging data of a PEV may be used to track the traveling schedule of an individual and his/her location. Many third-party companies may be interested in these sensitive private data to exploit their commercial benefits. This will undoubtedly give rise to the privacy concerns during various data processing phases, like monitoring, collection, aggregation, and analysis. [104] has proposed a privacy-preserving scheme to allow communication between smart meters and the utilities.

For data privacy, some relevant laws and regulations have to be enacted first. They must be clear on who owns and controls the data, who has the right to access the user data, how do utilities or other parties share the user data without compromising privacy, and how to manage the huge amount of sensitive data. Secondly, information and communication technologies are potential alternatives to cope with the data privacy issues, such as homomorphic encryption [105, 106]. An ideal lattice-based fully homomorphic encryption scheme proposed by Gentry in 2009 is well-known as a great breakthrough in this field [107]. Although the current fully homomorphic encryption schemes are still too inefficient to be practical, it indeed brings hopes and motivations for research in this area. For smart grid, privacy and interoperability concerns would be largely mitigated with efficient, fully homomorphic encryption schemes.

D) Interoperability

As a system of systems, smart grid has to ensure interoperability among the power systems, information systems, and communication systems. A good design of one particular system without proper consideration of other systems will not achieve the best result for the whole system. Information, like the user data and control message, which is produced and transmitted in one particular system, may also be used in other systems. Importantly, data are generated in vast quantities in smart grid. How to manage, store, and effectively use these data become a critical issue.

The interoperability of smart grid allows utilities, consumers, and other stakeholders to communicate securely and effectively, even though there are a variety of different information systems over geographically dispersed regions. In September 2011, IEEE published IEEE STD. 2030 as a guideline of the interoperability issues in smart grid, and this will be discussed in Section IV-E.

Last but not least, since building smart grids from the existing power systems is an incremental process, the interoperability of new functionalities/systems with the existing ones must be properly addressed, too. For instance, although WAMS and WACS will eventually replace SCADA in the future smart grid, the change will not happen unless WAMS, WACS, and SCADA are interoperable with each other during the upgrade process [108–110].

IV. THE SMART GRID COMMUNICATION NETWORK STRUCTURES AND TECHNOLOGIES

Since smart grid will have monitoring and controlling capability throughout the system from generation to end user sites, the communication network of smart grid is proposed in a similar hierarchy of wide area network (WAN), neighborhood area network (NAN), and home area network (HAN), accordingly [111]. HAN connects to smart grid via smart meters and provides communications and energy management among appliances at the user premises. NAN connects multiple HANs to WAN. Apart from being part of AMI, NAN may also support DG and the automation of the distribution network. WAN connects NANs, distribution substations, automation, and monitoring devices/systems (such as SCADA,

http://dx.doi.org/10.1017/ATSIP.2015.9

RTU, and PMU) to the transmission substations and utility enterprise computer networks, and further to the public Internet. Note that HAN, NAN, and WAN have different maximum transmission distances in the order of 100 m, 10 and 100 km, respectively. The required transmission bandwidths of HAN, NAN, and WAN are in million, hundred millions, and 10 gbps, respectively. Different communication media and transmission technologies are therefore used in HAN, NAN, and WAN to ensure cost-effective performance.

In HAN and NAN, communication cost is a major factor for consideration because of the large number of connecting devices [23]. Wireless and power line communications (PLCs) will be the appropriate communication technologies. Wireless communications have the advantages of no wiring cost, flexible deployment, and easily connecting large number of devices. However, they also have the shortcomings of lower communication bandwidth, shorter transmission distance, and security concerns. Hence, wireless communications are mainly used in HAN, and sometimes in NAN if the required transmission distance is short. Among the wireless communication schemes, Zipbee and WiFi are the two attractive wireless solutions. Zigbee is an IEEE 802.15.4-based, low power, low-cost, and two-way wireless communication standard. It normally has transmission range up to 75 m, and supports up to 65 000 networked devices, and transmission bandwidths of 20–250 kbps depending on the applied industrial, scientific, and medical (ISM) frequency band, i.e. 864, 915 MHz, and 2.4 GHz. On the other hand, WiFi is an IEEE 802.11 wireless local area network (WLAN) standard, also on the ISM frequency band (e.g., 2.4 GHz). It provides coverage range from 30 to 100 m, up to 255 connections to an access point (AP), and physical transmission throughput from 11 to 600 mbps depending on the applied standard/technology. At the moment, the main advantage of Zipbee over WiFi is the power consumption. However, this advantage is diminishing as power consumption of WiFi chipsets has been undergoing significant improvements.

PLCs use power lines as media for data communications to eliminate the requirement of additional physical infrastructure. Standards such as IEEE 1901 and ITU-T G9960/61 have been developed recently to promote the applications of PLCs. The deployment cost for PLCs is therefore low similar to that of wireless communications. However, the transmission distance and bandwidth of PLCs are rather limited since power grids are designed for electricity transmission. Data transmissions are sent on carrier frequencies (3–500 KHz for narrowband PLCs (NB-PLCs) and 1–30 MHz for broadband PLCs (BB-PLCs)) far higher than the utility frequency, i.e., 50 or 60 Hz. The quality of PLC signals is often degraded by path attenuation, electricity noise, and the interference from wireless communication signals. Hence, PLCs may serve the applications in HAN and even NAN but it may not be suitable for WAN. For example, NB-PLCs can have 100 km transmission distance but only with hundred bits per second transmission rate. BB-PLCs with millions bits per second transmission rate can only have the transmission distance of a 100 m.

Owing to the distance and bandwidth requirements of smart grid WAN communication network, optical fiber communications is one of the appropriate media/technologies. Note that single mode optical fibers can have less than 0.2 dB attenuation per kilometer for optical signals. Thousand kilometers transmission distance can be easily achieved with optical fibers using commercially available optical amplifiers, e.g., erbium-doped fiber amplifier (EDFA). A single fiber can provide more than 80 wavelength division multiplexing (WDM) channels, each with 100 GHz bandwidth and immune to electrical noise. At the moment, no other technologies can have similar advantages of distance and bandwidth as that of optical fibers. Surely, cost is the main concern with the deployment of optical networks. Recently, passive optical networks (PONs) technologies such as Ethernet PON (EPON) and Gigabit PON (GPON) have become popular. This reduces the cost slightly for optical network deployment. To have further cost reduction, one may share the optical network bandwidth with other applications and traffic.

A mechanism is needed to unify the mixed communications from different networking technologies in the smart grid communication network. As suggested by NIST, the Internet Protocol (IP) is the practical approach for solving the problem. IP has the flexibility of exchanging information between applications independent of the underlying physical communications technologies. Using IP for smart grid communication networks, however, brings new challenges beyond those in traditional communication networks. We believe IPv6 (IP version 6) will be a key enabler of smart grid communications. The communications of sensing/monitoring devices in smart grid will need a huge number of network addresses that cannot be provided by the current IPv4 since its 32-bit address space has been almost exhausted. Smart grid applications such as real time monitoring will need special QoS (e.g., guaranteed latency and loss) and security that have not been well supported in IPv4. Moreover, the battery-powered smart sensors/devices in smart grid for distributed monitoring and control will only have low processing capability and transmit packets over unreliable/noisy media such as wireless and PLC links. Note that IPv6 has 128-bit address space and better built-in QoS/security control. The new IPv6 associated standards such as Routing Protocol for Low-power and lossy links (RPL) and IPv6 over Low power WPAN (6LoWPAN) are going to solve the problems of low processing capability, and packet routing over unreliable links. Though the smart grid communication network is evolving, IPv6 has demonstrated the potential capability and flexibility to solve the potential problems.

To learn more, readers are encouraged to attend IEEE SmartGridComm [112], IEEE ICC [113], IEEE ISGT [114], IEEE PES-GM [115], and other related conferences where people discuss the most recent research development in smart grid communications.

http://dx.doi.org/10.1017/ATSIP.2015.9

V. RECENT DEVELOPMENTS IN SMART GRID COMMUNICATIONS

A) Communication framework

Due to the concern that the conceptual smart grid framework proposed by NIST, as shown in Fig. 2, could be a bit too complicated for researchers in data communication to deal with, a much simpler three-entity smart grid framework has been proposed [116, 117]. As shown in Fig. 8, this simplified, communication-oriented framework consists of Operation Network, Business Network, and Consumer Network.

Operation Network contains all the communication systems needed by a power system that manages the power flow from the generation side to the consumption side. In other words, it contains Bulk Generation, Transmission, Distribution, and Operations of the NIST framework.

Business Network refers to the communication system that enables the advanced smart grid electricity market as well as various new services provided by different smart grid companies. In other words, it contains Service Providers and Markets of the NIST framework.

Consumer Network covers all the communication technologies to be used at a consumer's premise, primarily a local area network (LAN) connecting various smart devices, such as smart meters, smart controllers, and PEVs, altogether. It is equivalent to the Customers domain in the NIST framework.

In addition to this framework, the conceptual architecture of the lower-level subnetwork for each of the three entities, and the communication requirements needed for interconnecting these three entities have also been presented. This three-entity framework not only gives researchers a much simpler option for a high-level view of the smart grid communication system, but also encourages researchers from different fields to collaborate with each other.

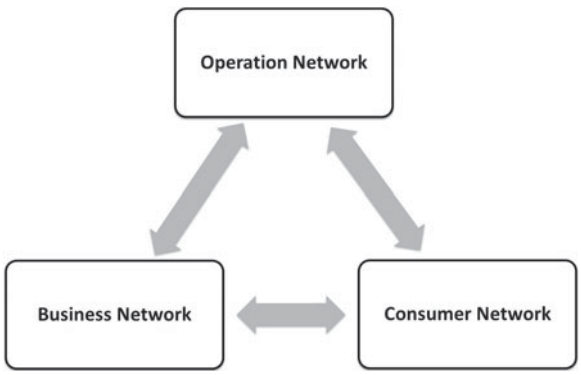

Fig. 8. Three-entity communication-oriented smart grid framework.

B) IEEE STD. 1815-2012

IEEE STD. 1815-2012, also known as Distributed Network Protocol (DNP3), is a popular communication protocol for SCADA since 1990s. The latest version of DNP3 [118] has been standardized by IEEE in 2012, which aims to:

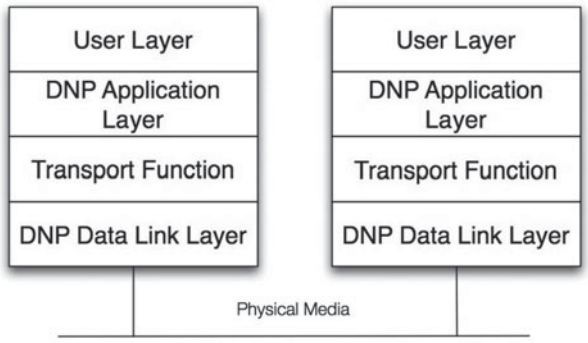

Fig. 9. DNP3 master-outstation model.

(i) Use the minimal bandwidth;
(ii) Make remote devices intelligent;
(iii) Share the best features of all other existing protocols;
(iv) Be compatible with other existing standards; and
(v) Be highly reliable.

As illustrated in Fig. 9, the general DNP3 protocol follows a three-layer model, termed Enhanced Performance Architecture (EPA). The three layers include the application layer (AL), the data link layer (DLL), and the physical layer (PL). AL is the top layer in the model, interfacing with the user software and the lower layers. It provides functions, data formats, and procedures for efficient data transmission. DLL provides error detection and station addressing for transmitting the AL data across the communication channel. PL, which goes beyond the DNP3 standard descriptions, provides bitwise data transmission through the physical communication media. There is no dedicated transport layer (TL) in the DNP3 protocol stack, unlike the one in a typical Open Systems Interconnection (OSI) reference model. The transport function (TF) is implemented within AL to divide AL data into some smaller segments so that they could be transmitted over noisy links more easily. The existence of TF instead of TL is primarily because of the concerns of compatibility, reliability, and execution speed.

Due to the increasing user demands for implementing DNP3 over high-speed digital networks, IEEE STD. 1815-2012 defines how to transport DNP3 data over the IP suite. The solution provided is to implement a connection management layer (CML) below DNP3 DLL. CML is on top of the transport layer, network layer, link layer, and physical layer of the IP network. CML thus interfaces between DNP3 and IP.

Although SCADA is a legacy system and may not adequately satisfy the requirements of AMC in smart grid, it is not economical to merely abandon SCADA in smart grid. Therefore, we believe that DNP3 may provide a reasonable option for enhancing the performance of SCADA.

C) NISTIR 7628

NISTIR 7628, namely, Guidlines for Smart Grid Cyber Security, is a three-volume report which presents a framework to help organizations make effective cyber security strategies [99–101]. The guideline was developed in 2010 by

http://dx.doi.org/10.1017/ATSIP.2015.9

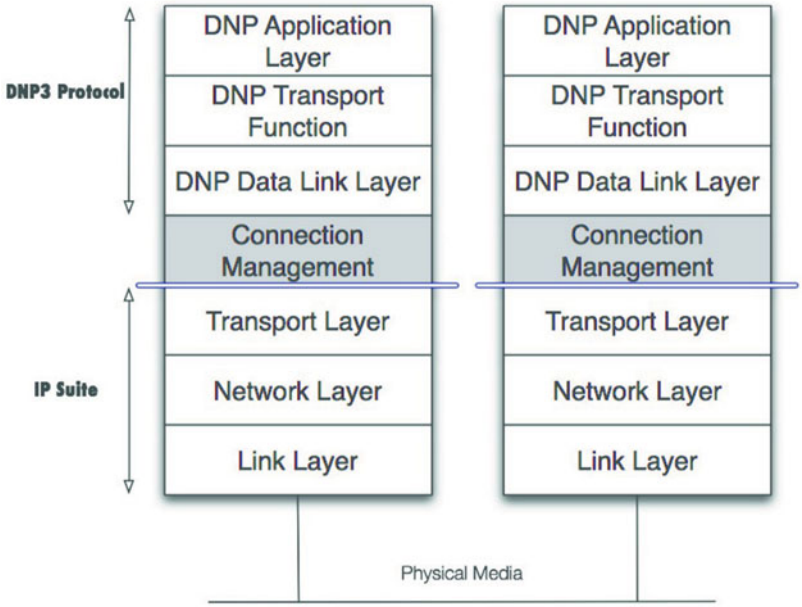

Fig. 10. DNP3 over the IP suite.

NIST Cyber Security Working Group (CSWG) of the Smart Grid Interoperability Panel (SGIP), which consists of more than 400 participants including federal agencies, regulatory organizations, standard organizations, vendors, service providers, manufacturers, and academia.

The first volume of the guideline begins with a discussion of the cyber security strategies used by SGIP–CSWG for the development of this guideline. It examines both domain-specific and common requirements of the cyber security issues for a series of tasks in smart grid, such as risk assessment, and requirement identification and modification. The analytical approach described in this part could serve as a guidance for organizations to identify high-level cyber security requirements for their own systems. The first volume then proposes a smart grid conceptual model followed by a detailed logistic reference model. Each interface in the logistic reference model is analyzed and assigned an appropriate impact level (high, moderate, or low) with regard to security. The high-level security requirements are thoroughly analyzed and discussed. Cryptographic and key management issues are carefully addressed along with potential alternatives. The second volume, focusing on the privacy issues, first discusses the privacy impact assessment and mitigating factors in smart grid. Besides the potential privacy issues, this volume also gives some high-level recommendations for privacy solutions. The third volume has abundant supportive analysis and references and the potential vulnerabilities in smart grid are discussed in details. Moreover, a number of security problems, but without specific solutions, are identified. Research and development themes for cyber security of smart grid are carefully discussed as well.

For the information and communication system, some high-level cyber security requirements are listed below:

(i) Separation of communication and control: This requires the control of communication to be physically or logically separated from the telemetry/data acquisition service.
(ii) DoS protection: This requires smart grid to mitigate or limit the impacts of all kinds of DoS attacks.
(iii) Communication integrity and confidentiality: This requires organizations to employ some cryptographic mechanisms to ensure data integrity and prevent the unauthorized disclosure of information during transmission.
(iv) Message authenticity: This provides authenticity of message and devices in communication. It is used to protect from malformed traffic, misconfigured devices, and malicious entities. It is suggested to be implemented inside the protocol.
(v) Honeypot: It is designed to be a target of various attacks, which are detected, tracked, and analyzed by collecting the attack data.

D) IEEE STD. 1711-2010

IEEE STD. 1711, i.e. IEEE Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links, has developed a trial standard for a cryptographic protocol used for serial communication among SCADA substations [119]. The standardized protocol, known as the serial SCADA protection protocol (SSPP), provides integrity and optional confidentiality for cyber security of serial links connecting substations. With the minimal overheads, SSPP encapsulates each SCADA or application messages in a cryptographic envelope before sending it to the underlying communication protocols (e.g. DNP3 and Modbus) for efficient authentication and encryption. SSPP is not limited to serial SCADA communication, but is also applicable to other types of serial communication (e.g. data concentrator and load management links). However, applications or systems are required to tolerate message losses

http://dx.doi.org/10.1017/ATSIP.2015.9

Table 2. Cipher suites in SSPP.

Cipher suite number	Cipher suite	Comments
0x0004	AES + CTR mode + HMAC-SHA256	Used for dynamic sessions
0x0005	AES + PE mode + HMAC-SHA256	Used for dynamic sessions with a session clock
0x0006	Plaintext + SHA256	No security provided
0x0008	Plaintext + HMAC-SHA256	Used for dynamic sessions
0x000A	AES + CBC mode + HMAC-SHA256	Used for dynamic sessions

since SSPP is designed to discard susceptible messages. The cipher suites adopted in SSPP are shown in Table 2.

SSPP is designed to support three kinds of communication links, namely, point-to-point, multi-drop, and broadcast. In addition, the mixed mode operation, in which some of the substations use SSPP to protect communication among each other, whereas others communicate in plaintext, is introduced to support both multi-drop and broadcast links. This is motivated by considering the flexibility of the SSPP deployment in the future smart grid system. By using the mixed mode, SSPP can be implemented in an incremental fashion so that there is no need for all substations to implement SSPP at the same time. Besides, SSPP can be implemented as standalone security devices, integrated in communication modems, or embedded in applications or systems. The standalone bump-in-the-wire security device approach, as shown in Fig. 11, needs little or no modification of the existing systems and equipment for legal serial system updates.

However, it is worth noting that the standard does not address the key management issue for SSPP.

E) IEEE STD. 2010-2011

Sponsored by the IEEE Standards Coordinating Committee 21 on Fuel Cells, Photovoltaics, Dispersed Generation, and Energy Storage, IEEE STD. 2030, i.e. IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads, has recently been developed as a guideline for supporting interoperability in smart grid [120]. The guideline introduces smart grid as "a complex system of systems" and lists the 12 architectural principles for smart grid, including openness, extensibility, scalability, interoperability, security, and privacy. Particularly, it discusses in details interoperability and interoperability-related security, privacy, and reliability requirements in smart grid. For extensibility, scalability, and upgradability, the smart grid interoperability reference model (SGIRM) is proposed through three different perspectives, namely, power system, communication system, and information system. Specifically, the power system interoperability (PS-IAP) puts an emphasis on power generation, transmission, distribution, and consumption. The communication technology interoperability (IT-IAP) represents a view of the control of processes and data management flow. The communication technology interoperability (CT-IAP) emphasizes the interconnectivity and communication among systems, applications, and devices. Each of the above reference models divides the whole system into domains with respect to different perspectives. Constraints, issues, and impacts on interoperability are considered for each domain. The relationship on the characteristics of data exchanged among domains is carefully examined. This detailed reference model provides stakeholders basic understanding of the interoperability criteria and help them identify and define the optimal design criteria for the interoperability of future smart grid implementations.

F) Smart grid demonstration projects

Over the past few years, there have been numerous smart grid demonstration projects that provide invaluable insights into the development of smart grid. In this subsection, we will briefly introduce three of the most prominent demonstration projects and their significance in building smart grids.

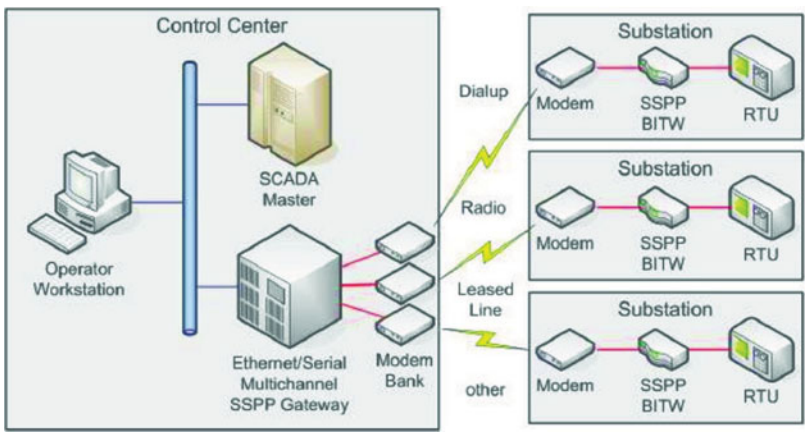

Fig. 11. Retrofit bump-in-the-wire SSPP deployment [119].

http://dx.doi.org/10.1017/ATSIP.2015.9

In late 2010, National Rural Electric Cooperative Association (NRECA) has initiated a $68 million Smart Grid Demonstration Project (SGDP) to "examine various smart grid technologies for their technical effectiveness, suitability to the cooperative business model, and return on investment (ROI)" [121]. Co-funded by the U.S Department of Energy (DOE) under the American Recovery and Reinvestment Act of 2009 (ARRA), SGDP involves 23 electric cooperative that serve over 750 000 consumers across 12 states in the U.S. In particular, SGDP investigated AMI technologies, communication systems, conservation voltage reduction, consumer acceptance of smart grid technologies, DR, energy storage, and meter data management technologies [122].

The Electric Power Research Institute (EPRI) Smart Grid Demonstration Initiative (SGDI) is a seven-year collaborative research that investigates the integration of DER into the grid and the electricity market. This multi-million dollar project involves 24 contributing utilities from Australia, Canada, France, Ireland, Japan, and the USA. By the year 2015, EPRI SGDI has tested various technologies including remote dispatch of customer-owned resources, reliability enhancement with DER, self-healing technologies for smart grid, use of storage for voltage smoothing and peak shifting [123].

Costing a a total of €53 million, GRID4EU is the biggest smart grid project funded by the European Union [124]. By 2015, GRID4EU has initiated six demonstration projects in Germany, Sweden, Spain, Italy, Czech Republic, and France, respectively, mostly focusing on grid automations and renewable energy integration. This 51-month project is expected to be completed by Jan. 2016.

VI. OPEN RESEARCH ISSUES

Since smart grid is relatively new, numerous problems remain to be solved. In this section, we will give a brief discussion on some of these problems.

A) Communication support for vehicle-to-grid (V2G) system

It is well-known that PEVs, with the ability to play roles including loads, sources, and storages, have a significant potential to improve the effectiveness of smart grid operations. However, since the capacity of a battery inside a PEV is too small to have a significant impact on the entire grid while unregulated charging of too many PEVs may lead to electricity shortage in the grid, researchers need to study how to effectively and efficiently manage and regulate the charging and discharging processes of PEVs in smart grid. This is called the V2G problem. Researchers are now developing an optimal charging strategy that can meet numerous objectives in smart grid. Although how communication systems affect the performances of V2G systems has been discussed in the literature [103, 125–130], how to build an optimal communication system to support V2G is yet to be addressed. Moreover, user privacy issues have not been fully investigated in the literature.

B) WAMS communication network

Despite the numerous advantages that WAMS could bring to smart grid operation, as discussed in Section III-A, its high transmission rate, low latency, and high reliability requirements make it very challenging to design an appropriate communication network for WAMS. In this design process, one of the most critical issues is to decide the protocol(s) to be used. The TCP/IP suite would not be a likely solution to WAMS due to its best-effort design and high unpredictability. Traditional industry protocols used in SCADA might not be a feasible solution, because they were not designed for high-speed WAMS [131–135]. This important topic should be more thoroughly explored by the research community.

C) Cryptographic schemes

As discussed in Section III-B, cryptography is indispensable in smart grids for the sake of security and data privacy. However, existing cryptographic schemes do not meet specific requirements of smart grid systems. For example, the limited computational and communication power of smart meters demand low-complexity cryptographic schemes. Furthermore, real-time power quality monitoring imposes a strict constraint on the complexity of cryptographic algorithms. Although some existing symmetric key encryption schemes can be efficiently used for secure data transmission, the distribution of the initial secret key is still a challenging problem due to the large scale of the smart grid system. Conventional public-key-based secret sharing schemes need to address the problems of scalability, efficiency, and connectivity in smart grids. For data privacy, advanced cryptographic schemes (e.g. homomorphic encryption) are widely considered as a potential solution to data sharing and data aggregation [136–139]. However, no practical solutions have been found yet, especially for data sharing. Thus, the design of efficient cryptographic schemes that satisfy the security, privacy, and reliability requirements of smart grids is an open research topic.

D) Key management

Key management is another critical issue in smart grid research. A smart grid system typically has tens of millions of users. The conventional key management system (e.g. PKI) often fails to support key generation, distribution, and revocation in such a large system, and a highly scalable key management system is needed. Identity-based encryption (IBE) is known to provide a possible solution, where the device identity is automatically bound to its public keys. As a result, there is no need for key generation and revocation. A key management scheme also has to be computationally efficient because of the limited computational and communication power of smart meters. In addition, due to the large geographical coverage of a power system, some distant

http://dx.doi.org/10.1017/ATSIP.2015.9

devices may only have intermittent connection with central key management servers. Under this context, a distributed key management scheme is needed to solve this problem. For example, key management can be accomplished locally with proxy re-encryption and proxy re-signature techniques [140–144]. The development of more scalable, secure, robust, and efficient key management systems is an important research topic to be further explored in the near future.

VII. CONCLUSIONS

Smart grid is considered the next generation electricity grid, providing reliable and efficient electricity generation and distribution, and accommodating high penetration of clean, renewable energy. In this paper, we have studied the design goals and architecture of smart grid and identified its four major functions, namely, AMC, DSM, GSM, and SP. We have also investigated the communication requirements, namely, data transmission, cyber security, data privacy, and interoperability requirements, of the smart grid communication systems, followed by some of the recent developments in such systems, including a communication framework as well as some newly developed communication standards for smart grid. Since each smart grid function has very distinct communication requirements, it is very unlikely that any single existing communication technology will serve all. Therefore, we should design new communication systems that take advantage of the existing communication technologies and satisfy the specific requirements of smart grid.

The paper concludes with some future research directions, including communication supports for the V2G system and WAMS, cryptographic schemes, and key management.

ACKNOWLEDGEMENTS

The authors would express sincere gratitude to our colleague from the University of Hong Kong, Dr. Chun-Yin Li, for contributing to the discussion of smart grid communication network structures and technologies. This research is supported in part by the Collaborative Research Fund and the Theme-based Research Scheme of the Research Grants Council, Hong Kong Special Administrative Region, China, under Grant No. HKU10/CRF/10 and T23-701/14N, respectively.

VIII. LIST OF ACRONYMS

A

AL	Application Layer
AMC	Advanced Monitoring and Control
AMI	Advanced Metering Infrastructure
AP	Access Point
ARRA	American Recovery and Reinvestment Act of 2009

B

BB-PLC	Broadband Power Line Communications

C

CIA	Confidentiality, Integrity, and Availability
CML	Connection Management Layer
CSWG	Cyber Security Working Group
CT-IAP	Communication Technology Interoperability

D

DG	Distributed Generation
DER	Distributed Energy Resources
DLC	Direct Load Control
DLL	Data Link Layer
DNP3	Distributed Network Protocol
DOE	U.S. Department of Energy
DR	Demand Response
DS	Distributed Storage
DSM	Demand-Side Management
DoS	Denial-of-Service

E

EDFA	Erbium Doped Fiber Amplifier
EIA	Energy Information Administration
EMS	Energy Management System
EPA	Enhanced Performance Architecture
EOPN	Ethernet Passive Optical Network
EPRI	Electric Power Research Institute
EPS	Electric Power System
EV	Electric Vehicle

G

GPON	Gigabit Passive Optical Network
GPS	Global Positioning System
GSM	Generation and Storage Management

H

HAN	Home Area Network

I

IBE	Identity-Based Encryption
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv6	IP version 6
ISM	Industrial, Scientific, and Medical
IT-IAP	Communication Technology Interoperability

L

LAN	Local Area Network

M

MTU	Master Terminal Unit

N

NALM	Non-intrusive Load Monitoring
NAN	Neighborhood Area Network
NB-PLC	Narrowband Power Line Communications
NIST	National Institute of Standards and Technology

http://dx.doi.org/10.1017/ATSIP.2015.9

NRECA	National Rural Electric Cooperative Association
O	
OSI	Open Systems Interconnection
P	
PDC	Phasor Data Concentrator
PEV	Plug-in Electric Vehicle
PKI	Public Key Infrastructure
PL	Physical Layer
PLC	Power Line Communications
PMU	Phasor Measurement Unit
PON	Passive Optical Network
PS-IAP	Power System Interoperability
Q	
QoS	Quality of Service
R	
RAS	Remedial Action Scheme
REN21	Renewable Energy Policy Network for the 21st Century
ROI	Return on Investment
RPL	Routing Protocol for Low-power and Lossy Links
RTU	Remote Terminal Unit
S	
SCADA	Supervisory Control and Data Acquisition
SGDI	Smart Grid Demonstration Initiative
SGDP	Smart Grid Demonstration Project
SGIP	Smart Grid Interoperability Panel
SGIRM	Smart Grid Interoperability Reference Model
SP	System Protection
SPS	Special Protection Scheme
SSPP	Serial SCADA Protection Protocol
T	
TF	Transport Function
TL	Transport Layer
V	
V2G	Vehicle-to-Grid
W	
WACS	Wide-Area Stability and Voltage Control System
WAMS	Wide-Area Measurement System
WAN	Wide Area Network
WAPS	Wide-Area Protection System
WDM	Wavelength Division Multiplexing
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
#	
6LoWPAN	IPv6 over Lower Power WPAN

REFERENCES

[1] IEEE smart grid. [Online]. Available: http://smartgrid.ieee.org/

[2] U.S. Energy Information Administration (EIA): Annual energy outlook 2014 with projections to 2040, April 2014. [Online]. Available: http://www.eia.gov/forecasts/archive/aeo14/pdf/0383(2014).pdf

[3] Renewable Energy Policy Network for the 21st Century: Renewables 2013 global status report, paris: REN21 secretariat, October 2013. [Online]. Available: http://www.ren21.net/wp-content/uploads/2015/06/REN12-GSR2015_Onlinebook_low1.pdf

[4] Gorman, S.: Electricity grid in us penetrated by spies. Wall Street J., 8 (2009).

[5] Department of energy launces initiative with industry to better protect the nation's electric grid from cyber threats. *DOE News Release*, January 2012. [Online]. Available: http://www.energy.gov/articles/department-energy-launches-initiative-industry-better-protectnation-s-electric-grid-cyber

[6] Innovating to meet the evolving cyber challenge. *DOE News*, September 2013. [Online]. Available: http://www.energy.gov/articles/innovating-meet-evolving-cyber-challenge

[7] Amin, S.M.: U.S. electrical grid get less reliable. IEEE Spectr., **48** (1) (2011), 80.

[8] Amin, S.M.: Living in the dark: why the U.S. needs to upgrade the grid. *Forbes Technology*, November 2012. [Online]. Available: http://www.forbes.com/sites/ciocentral/2012/07/11/living-in-the-dark-why-the-u-s-needs-to-upgrade-the-grid/

[9] Galli, S.; Scaglione, A.; Wang, Z.: For the grid and through the grid: the role of power line communications in the smart grid. Proc. IEEE, **99** (6) (2011), 998–1027.

[10] Gharavi, H.; Hu, B.: Multigate communication network for smart grid. Proc. IEEE, **99** (6) (2011), 1028–1045.

[11] Fan, Z. *et al.*: Smart grid communications: overview of research challenges, solutions, and standardization activities.' IEEE Commun. Surv. Tutor., **15** (1) (2013), 21–38.

[12] Fang, X.; Misra, S.; Xue, G.; Yang, D.: Smart grid the new and improved power grid: a survey. IEEE Commun. Surv. Tutor., **14** (4) (2012), 944–980.

[13] Lo, C.-H.; Ansari, N.; The progressive smart grid system from both power and communications aspects. IEEE Commun. Surv. Tutor., **14** (3) (2012), 799–821.

[14] Amin, S.M.; Wollenberg, B.F.: Toward a smart grid: power delivery for the 21st century. IEEE Power Energy Mag., **3** (5) (2005), 34–41.

[15] Smart grid primer (smart grid books). Department of Energy. [Online]. Available: http://energy.gov/oe/technology-development/smart-grid/smart-grid-primer-smart-grid-books

[16] Farhangi, H.: The path of the smart grid. IEEE Power Energy Mag., **8** (1) (2010), 18–28.

[17] Gellings, C.W.; Samotyj, M.; Howe, B.: The future's smart delivery system [electric power supply]. IEEE Power Energy Mag., IEEE, **2** (5) (2004), 40–48.

[18] Kezunovic, M.; Vittal, V.; Meliopoulos, S.; Mount, T.: The big picture. IEEE Power Energy Mag., **10** (4) (2012), 22.

[19] Li, F. *et al.*: Smart transmission grid: vision and framework. IEEE Trans. Smart Grid, **1** (2) (2010), 168–177.

[20] Miller, J.: Understanding the smart grid: features, benefits, and costs, in *Illinois Smart Grid Initiative – Workshop*, 2008. [Online]. Available: https://www.smartgrid.gov/files/understanding_the_smart_grid_07-2008.pdf

[21] Bryson, J.; Gallagher, P.: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, National Institute of Standards and Technology (NIST), Technical Report, NIST Special Publication 1108R2, 2012, 2.0.

[22] Wang, W.; Xu, Y.; Khanna, M.: A survey on the communication architectures in smart grid. Comput. Netw., **55** (15) (2011), 3604–3629.

[23] Hossain, E.; Han, Z.; Poor, H.V.: Smart Grid Communications and Networking, *Cambridge University Press*, New York, 2012.

[24] Glover, J.D.; Sarma, M.; Overbye, T.: Power System Analysis & Design, SI Version. *Cengage Learning*, Stamford, CT, 2011.

[25] Kundur, P. *et al.*: Definition and classification of power system stability IEEE/cigre joint task force on stability terms and definitions. IEEE Trans. Power Syst., **19** (3) (2004), 1387–1401.

[26] Moslehi, K.; Kumar, R.: A reliability perspective of the smart grid. IEEE Trans. Smart Grid, **1** (1) (2010), 57–64.

[27] Kundur, P.; Balu, N.J.; Lauby, M.G.: Power System Stability and Control, vol. **7**, *McGraw-Hill*, New York, 1994.

[28] Hauser, C.; Bakken, D.; Bose, A.: A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid. IEEE Power Energy Mag., **3** (2) (2005), 47–55.

[29] McDaniel, P.; McLaughlin, S.: Security and privacy challenges in the smart grid. IEEE Sec. Priv., **7** (3) (2009), 75–77.

[30] Markey, E.J.; Waxman, H.A.: Electric Grid Vulnerability: industry Response Reveal Security Gaps. *US House of Representatives*, 2013. [Online]. Available: http://democrats.energycommerce.house.gov/sites/default/files/documents/Report-Electric-Grid-Vulnerability-2013-5-21.pdf

[31] Arrillaga, J.; Bollen, M.H.; Watson, N.R.: Power quality following deregulation. Proc. IEEE, **88** (2) (2000), 246–261.

[32] Bollen, M.H.F.: Understanding the Power Quality Problems. Vol. 3. *IEEE Press*, New York, 2000.

[33] Kurose, J.; Ross, K.: Computer Networks: a Top-Down Approach. *Addison-Wesley*, Boston, 2009.

[34] Independence, E.: Security Act of 2007. Public Law, **110** (140) (2007), 19.

[35] Xie, Z.; Manimaran, G.; Vittal, V.; Phadke, A.; Centeno, V.: An information architecture for future power systems and its reliability analysis. IEEE Trans. Power Syst. , **17** (3) (2002), 857–863.

[36] Gellings, C.W.; Chamberlin, J.H.: Demand-Side Management: Concepts and Methods. *The Fairmont Press Inc.*, Lilburn, GA, 1987.

[37] McDonald, J.D.: Electric Power Substations Engineering. *CRC Press*, Boca Raton, FL, 2012.

[38] Shahidehpour, M.; Wang, Y.: Communication and Control in Electric Power Systems: Applications of Parallel and Distributed Processing. *John Wiley & Sons Inc*, Hoboken, NJ, 2004.

[39] Anjia, M.; Jiaxi, Y.; Zhizhong, G.: Pmu placement and data processing in WAMS that complements SCADA, in *IEEE Power Engineering Society General Meeting, 2005.*, 2005, 780–783.

[40] Group, N.S. *et al.*: Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What did We Learn, Report to the NERC Board of Trustees, 2004.

[41] Liscouski, B.; Elliot, W.: Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, A Report to US Department of Energy, vol. **40**, 2004.

[42] García, B.; Burgos, J.C.; Alonso, Á. M.: Transformer tank vibration modeling as a method of detecting winding deformations-Part i: Theoretical foundation. IEEE Trans. Power Deliv., **21** (1) (2006), 157–163.

[43] Pradhan, M.: Assessment of the status of insulation during thermal stress accelerated experiments on transformer prototypes. IEEE Trans. Dielectr. Electr. Insul., **13** (1) (2006), 227–237.

[44] IEEE standard communication delivery time performance requirements for electric power substation automation, IEEE Std 1646–2004, 2005, 1–24.

[45] Bertsch, J.; Carnal, C.; Karlson, D.; McDaniel, J.; Vu, K.: Wide-area protection and power system utilization. Proc. IEEE, **93** (5) (2005), 997–1003.

[46] Bose, A.: Smart transmission grid applications and their supporting infrastructure. IEEE Trans. Smart Grid, **1** (1) (2010), 11–19.

[47] Taylor, C.W.; Erickson, D.C.; Martin, K.E.; Wilson, R.E.; Venkatasubramanian, V.: Wacs-wide-area stability and voltage control system: R&D and online demonstration. Proc. IEEE, **93** (5) (2005), 892–906.

[48] Horowitz, S.; Phadke, A.G.; Renz, B.: The future of power transmission. IEEE Power Energy Mag., **8** (2) (2010), 34–40.

[49] Chakrabortty, A.; Chow, J.H.; Salazar, A.: A measurement-based framework for dynamic equivalencing of large power systems using wide-area phasor measurements. IEEE Trans. Smart Grid, **2** (1) (2011), 68–81.

[50] Phadke, A.; Thorp, J.; Adamiak, M.: A new measurement technique for tracking voltage phasors, local system frequency, and rate of change of frequency. IEEE Trans. Power Appar. Syst., **PAS-102** (5) (1983), 1025–1038.

[51] Phadke, A.: Synchronized phasor measurements in power systems. IEEE Comput. Appl. Power, **6** (2) (1993), 10–15.

[52] De La Ree, J.; Centeno, V.; Thorp, J.S.; Phadke, A.G.: Synchronized phasor measurement applications in power systems. IEEE Trans. Smart Grid, **1** (1) (2010), 20–27.

[53] Wang, Y.; Li, W.; Lu, J.: Reliability analysis of wide-area measurement system. IEEE Trans. Power Deliv., **25** (3) (2010), 1483–1491.

[54] Zhang, Y. *et al.*: Wide-area frequency monitoring network (fnet) architecture and applications. IEEE Trans. Smart Grid, **1** (2) (2010), 159–167.

[55] Wen, M.H.; Li, V.O.: Optimal phasor data concentrator installation for traffic reduction in smart grid wide-area monitoring systems, in *2013 IEEE Global Communications Conf. (GLOBECOM)*, 2013, 2622–2627.

[56] La Scala, M. *et al.*: Development of applications in WAMS and wacs: an international cooperation experience, in *IEEE Power Engineering Society General Meeting, 2006.*, 2006, 10 pp.

[57] Terzija, V. *et al.*: Wide-area monitoring, protection, and control of future electric power networks. Proc. IEEE, **99**, (1) (2011), 80–93.

[58] Wilson, R.E.; Taylor, C.W.: Using dynamic simulations to design the wide-area stability and voltage control system (wacs), in *Power Systems Conf. and Exposition, 2004. IEEE PES*, IEEE, 2004, pp. 100–107.

[59] Kekatos, V.; Giannakis, G.B.: Distributed robust power system state estimation. IEEE Trans. on Power Syst., **28** (2) (2013), 1617–1626.

[60] Zhou, M.; Centeno, V.A.; Thorp, J.S.; Phadke, A.G.: An alternative for including phasor measurements in state estimators. IEEE Trans. Power Syst., **21** (4) (2006), 1930–1937.

[61] IEEE standard for synchrophasor measurements for power systems. IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005), December 2011, 1–61.

[62] IEEE standard for synchrophasor data transfer for power systems. IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005), December 2011, 1–53.

[63] IEEE guide for synchronization, calibration, testing, and installation of phasor measurement units (PMUS) for power system protection and control. IEEE Std C37.242-2013, March 2013, 1–107.

[64] Armenia, A.; Chow, J.H.: A flexible phasor data concentrator design leveraging existing software technologies. IEEE Trans. Smart Grid, **1** (1) (2010), 73–81.

[65] Skok, S.; Matica, R.; Šturlić, I.: Enhanced open architecture of phasor data concentrator. Eur. Trans. Electr. Power, **21** (4) (2011), 1531–1540.

[66] Bialek, J.W.; Varaiya, P.; Wu, F.; Zhong, J.: Risk-limiting dispatch of smart grid, in *Power and Energy Society General Meeting, 2010 IEEE*, 2010, 1–2.

[67] Li, V.O.; Wu, F.F.; Zhong, J.: Communication requirements for risk-limiting dispatch in smart grid, in *2010 IEEE Int. Conf. on Communications Workshops (ICC),* IEEE, 2010, 1–5.

[68] Rajagopal, R.; Bitar, E.; Varaiya, P.; Wu, F.: Risk-limiting dispatch for integrating renewable power. Int. J. Electr. Power Energy Syst., **44** (1) (2013), 615–628, 2013.

[69] Varaiya, P.P.; Wu, F.F.; Bialek, J.W.: Smart operation of smart grid: risk-limiting dispatch. Proc. IEEE, **99** (1) (2011), 40–57.

[70] Chaouachi, A.; Kamel, R.M.; Andoulsi, R.; Nagasaka, K.: Multiobjective intelligent energy management for a microgrid. IEEE Trans. Ind. Electr., **60** (4) (2013), 1688–1699.

[71] Huang, A.Q.; Crow, M.L.; Heydt, G.T.; Zheng, J.P.; Dale, S.J.: The future renewable electric energy delivery and management (freedm) system: the energy internet. Proc. IEEE, **99** (1) (2011), 133–148.

[72] Katiraei, F.; Iravani, M.R.: Power management strategies for a microgrid with multiple distributed generation units. IEEE Trans. Power Syst., **21** (4) (2006), 1821–1831.

[73] Katiraei, F.; Iravani, R.; Hatziargyriou, N.; Dimeas, A.: Microgrids management. IEEE Power Energy Mag., **6** (3) (2008), 54–65.

[74] Lasseter, R.H.; Paigi, P.: Microgrid: a conceptual solution, in *IEEE 35th Annual Power Electronics Specialists Conf., 2004. (PESC 04) 2004*, vol. **6**. IEEE, 2004, 4285–4290.

[75] Savaghebi, M.; Jalilian, A.; Vasquez, J.C.; Guerrero, J.M.: Autonomous voltage unbalance compensation in an islanded droop-controlled microgrid. IEEE Trans. Ind. Electron., **60** (4) (2013), 1390–1402.

[76] Vaccaro, A.; Popov, M.; Villacci, D.; Terzija, V.: An integrated framework for smart microgrids modeling, monitoring, control, communication, and verification. Proc. IEEE, **99** (1) (2011), 119–132.

[77] McMillin, B.; Akella, R.; Ditch, D.; Heydt, G.; Zhang, Z.; Chow, M.: Architecture of a smart microgrid distributed operating system, in *Power Systems Conf. and Exposition (PSCE)*, 2011, 1–5.

[78] U. D. of Energy: Benefits of demand response in electricity markets and recommendations for achieving them, 2006.

[79] Ruiz, N.; Cobelo, I.; Oyarzabal, J.: A direct load control model for virtual power plant management. IEEE Trans. Power Syst., **24** (2) (2009), 959–966.

[80] Sullivan, M.; Bode, J.; Kellow, B.; Woehleke, S.; Eto, J.: Using residential AC load control in grid operations: PG&E's ancillary service pilot. IEEE Trans. Smart Grid, **4** (2) (2013), 1162–1170.

[81] Baker, F.; Meyer, D.: Internet protocols for the smart grid, in *Request for Comments RFC*, vol. **6272**, 2011.

[82] Benzi, F.; Anglani, N.; Bassi, E.; Frosini, L.: Electricity smart meters interfacing the households. IEEE Trans. Ind. Electron., **58** (10) (2011), 4487–4494.

[83] Lui, T.J.; Stirling, W.; Marcy, H.O.: Get smart. IEEE Power Energy Mag., **8** (3) (2010), 66–78.

[84] Piette, M.A.; Ghatikar, G.; Kiliccote, S.; Watson, D.; Koch, E.; Hennage, D.: Design and operation of an open, interoperable automated demand response infrastructure for commercial buildings. J. Comput. Inf. Sci, Eng., **9** (2) (2009), 021004.

[85] Gans, W.; Alberini, A.; Longo, A.: Smart meter devices and the effect of feedback on residential electricity consumption: evidence from a natural experiment in northern ireland. Energy Econ., **36** (2013), 729–743.

[86] Mohsenian-Rad, A.-H.; Leon-Garcia, A.: Optimal residential load control with price prediction in electricity pricing environments. IEEE Trans. Smart Grid, **1** (2) (2010), 120–133.

[87] Dallinger, D.; Krampe, D.; Wietschel, M.: Vehicle-to-grid regulation reserves based on a dynamic simulation of mobility behavior. IEEE Trans. Smart Grid, **2** (2) (2011), 302–313.

[88] Deilami, S.; Masoum, A.S.; Moses, P.S.; Masoum, M.A.: Real-time coordination of plug-in electric vehicle charging in smart grids to minimize power losses and improve voltage profile. IEEE Trans. Smart Grid, **2** (3) (2011), 456–467.

[89] Han, S.; Han, S.H.; Sezaki, K.: Development of an optimal vehicle-to-grid aggregator for frequency regulation. IEEE Trans. Smart Grid, **1** (1) (2010), 65–72.

[90] Ortega-Vazquez, M.A.; Bouffard, F.; Silva, V.: Electric vehicle aggregator/system operator coordination for charging scheduling and services procurement. IEEE Trans. Power Syst., **28** (2) (2013), 1806–1815.

[91] Saber, A.Y.; Venayagamoorthy, G.K.: Plug-in vehicles and renewable energy sources for cost and emission reductions. IEEE Trans. Ind. Electron., **58** (4) (2011), 1229–1238.

[92] Communication Requirements of Smart Grid Technologies, Department of Energy, Tech. Rep., 2010. [Online]. Available: http://energy.gov/sites/prod/files/gcprod/documents/Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf

[93] Gungor, V.C. *et al.*: A survey on smart grid potential applications and communication requirements. IEEE Trans. Ind. Inf., **9** (1) (2013), 28–42, 2013.

[94] Meserve, J.: Sources: staged cyber attack reveals vulnerability in power grid, in *CNN. Com*, 26 September 2007.

[95] Greenberg, A.: Hackers cut cities power, *Forbes, Jaunuary*, 2008.

[96] Fehrenbacher, K.: Smart meter worm could spread like a virus, 2009.

[97] Khurana, H.; Hadley, M.; Lu, N.; Frincke, D.A.: Smart-grid security issues. IEEE Sec. Priv., **8** (1), 81–85, 2010.

[98] Metke, A.R.; Ekl, R.L.: Security technology for smart grid networks. IEEE Trans. Smart Grid, **1** (1) (2010), 99–107.

[99] NISTIR 7628 guidelines for smart grid cyber security v1.0: vol. 1, smart grid cyber security strategy, architecture, and high-level requirements, Smart Grid Interoperability Panel Cyber Security Working Group, 2010.

[100] NISTIR 7628 guidelines for smart grid cyber security v1.0: vol. 2, privacy and smart grid, Smart Grid Interoperability Panel Cyber Security Working Group, 2010.

[101] NISTIR 7628 guidelines for smart grid cyber security v1.0: vol. 3, supportive analysis and references, Smart Grid Interoperability Panel Cyber Security Working Group, 2010.

[102] Boyer, W.F.; McBride, S.A.: Study of Security Attributes of Smart Grid Systems-current Cyber Security Issues, Idaho National Laboratory, USDOE, Under Contract DE-AC07-05ID14517, 2009.

[103] Quinn, C.; Zimmerle, D.; Bradley, T.H.: The effect of communication architecture on the availability, reliability, and economics of plug-in hybrid electric vehicle-to-grid ancillary services. J. Power Sources, **195** (5) (2010), 1500–1509.

[104] Chim, T.W.; Yiu, S.-M.; Hui, L.C.; Li, V.O.: Privacy-preserving advance power reservation. IEEE Commun. Mag., **50** (8) (2012), 18–23.

[105] Li, F.; Luo, B.; Liu, P.: Secure information aggregation for smart grids using homomorphic encryption, in *2010 First IEEE Int. Conf. on Smart Grid Communications (SmartGridComm)*, 2010, 327–332.

[106] He, X.; Pun, M.-O.; Kuo, C.-C.: Secure and efficient cryptosystem for smart grid using homomorphic encryption, in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, 2012, 1–8.

[107] Gentry, C.: A Fully Homomorphic Encryption Scheme. Ph.D. dissertation, Stanford University, Palo Alto, CA, 2009.

[108] Huang, Y.-F.; Werner, S.; Huang, J.; Kashyap, N.; Gupta, V.: State estimation in electric power grids: meeting new challenges presented by the requirements of the future grid. IEEE Signal Process. Mag., **29** (5) (2012), 33–43.

[109] Kashyap, N.; Werner, S.; Riihonen, T.; Huang, Y.-F.: Reduced-order synchrophasor-assisted state estimation for smart grids, in *2012 IEEE Third Int. Conf. on Smart Grid Communications (SmartGridComm)*, IEEE, 2012, 605–610.

[110] Kashyap, N.; Werner, S.; Huang, Y.-F.; Riihonen, T.: Power system state estimation under incomplete PMU observability – a reduced-order approach. IEEE J. Sel. Topics Signal Process., **8** (6) (2014), 1051–1062.

[111] Berger, L.T.; Iniewski, K.: Smart Grid: Applications, Communications and Security, *Wiley*, Hoboken, NJ, 2012.

[112] IEEE international conference on smart grid communications. [Online]. Available: http://ieee- smartgridcomm.org/

[113] IEEE Int. Conf. on Communications. [Online]. Available: http://ieee-icc.org/

[114] IEEE PES Conf. on Innovative Smart Grid Technologies. [Online]. Available: http://ieee-isgt.org/

[115] IEEE PES General Meeting. [Online]. Available: http://pes-gm.org/

[116] Wen, M.H.; Leung, K.-C.; Li, V.O.: Communication-oriented smart grid framework, in *2011 IEEE Int. Conf. on Smart Grid Communications (SmartGridComm)*. 2011, 61–66.

[117] Wen, M.H.; Li, V.O.: Form follows function: designing smart grid communication systems using a framework approach. IEEE Power Energy Mag., **12** (3) (2014), 37–43.

[118] IEEE standard for electric power systems communications-distributed network protocol (DNP3), IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010), October 2012, 1–821.

[119] IEEE trial-use standard for a cryptographic protocol for cyber security of substation serial links, IEEE Std 1711-2010, February 2011, 1–49.

[120] IEEE guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS), end-use applications, and loads, IEEE Std 2030-2011, 10 September 2011, 1–126.

[121] CODY, E.P.: Brave New World: Electric Cooperatives Pilot a Wide Array of Smart Grid Technologies, CRN TechSurveillance, June 2014.

[122] NRECA smart grid demonstration project. [Online]. Available: http://www.nreca.coop/what-we-do/bts/smart-grid-demonstration-project/

[123] Smart grid demonstration – integration of distributed energy resources. [Online]. Available: http://smartgrid.epri.com/Demo.aspx

[124] Grid4eu: a large-scale demonstration project of advanced smart grids solutions with wide replication and scalability potential for Europe. [Online]. Available: http://www.grid4eu.eu/

[125] Parsons, G.R.; Hidrue, M.K.; Kempton, W.; Gardner, M.P.: Willingness to pay for vehicle-to-grid (v2g) electric vehicles and their contract terms. Energy Econ., **42** (2014), 313–324.

[126] Schuller, A.; Dietz, B.; Flath, C.M.; Weinhardt, C.: Charging strategies for battery electric vehicles: economic benchmark and v2g potential. IEEE Trans. Power Syst., **29** (5) (2014), 2014–2022.

[127] Vachirasricirikul, S.; Ngamroo, I.: Robust LFC in a smart grid with wind power penetration by coordinated V2G control and frequency controller. IEEE Trans. Smart Grid, **5** (1) (2014), 371–380.

[128] Kumar, K.N.; Sivaneasan, B.; Cheah, P.; So, P.; Wang, D.: V2G capacity estimation using dynamic EV scheduling. IEEE Trans. Smart Grid, **5** (2) (2014), 1051–1060.

[129] Chukwu, U.C.; Mahajan, S.M.: V2G parking lot with PV rooftop for capacity enhancement of a distribution system. IEEE Trans. Sust. Energy, **5** (1) (2014), 119–127.

[130] Chukwu, U.C.; Mahajan, S.M.: Real-time management of power systems with V2G facility for smart-grid applications. IEEE Trans. Sust. Energy, **5** (2) (2014), 558–566.

[131] Fesharaki, F.H.; Hooshmand, R.-A.; Khodabakhshian, A.: Simultaneous optimal design of measurement and communication infrastructures in hierarchical structured WAMS. IEEE Trans. Smart Grid, **5** (1) (2014), 312–319.

[132] Das, S.; Singh Sidhu, T.: Application of compressive sampling in synchrophasor data communication in WAMS. IEEE Trans. Ind. Inf., **10** (1) (2014), 450–460.

[133] Cheng, X.; Wang, Y.: The risk assessment quantitative research of WAMS communications network, in *Proc. 2012 Int. Conf. Cybernetics and Informatics*, *Springer*, 2014, 1639–1647.

[134] Golshani, M. *et al.*: Performance analysis of wide area network communications using discrete event simulation tools, in *IEEE 2014 Int. Conf. Power System Technology (POWERCON)*, 2014, 1098–1105.

[135] Amarasekara, B.; Nirmalathas, A.; Evans, R.J.: Analysis of JP-based communication backbone over shared wide area-network for smart grid applications, in *IEEE 2014 Int. Symp. on Wireless Personal Multimedia Communications (WPMC)*, 2014, 601–606.

[136] Li, H.; Lu, R.; Zhou, L.; Yang, B.; Shen, X.: An efficient merkle-tree-based authentication scheme for smart grid. IEEE Syst. J., **8**, (2) (2014), 655–663.

[137] Wen, M.; Lu, R.; Lei, J.; H. Li, Liang, X.; Shen, X.S.: Sesa: an efficient searchable encryption scheme for auction in emerging smart grid marketing. Sec. Commun. Netw., **7** (1) (2014), 234–244.

[138] Fan, C.-I.; Huang, S.-Y.; Lai, Y.-L.: Privacy-enhanced data aggregation scheme against internal attackers in smart grid. IEEE Trans. Ind. Inf., **10** (1) (2014), 666–675.

[139] Birman, K.; Jelasity, M.; Kleinberg, R.; Tremel, E.: Building a secure and privacy-preserving smart grid. ACM SIGOPS Oper. Syst. Rev., **49** (1) (2015), 131–136.

[140] Xiao, S.; Gong, W.; Towsley, D.: Dynamic key management in a smart grid, in *Dynamic Secrets in Communication Security*, *Springer*, 2014, 55–68.

[141] Jiang, R.; Lu, R.; Luo, J.; Lai, C.; Shen, X.S.: Efficient self-healing group key management with dynamic revocation and collusion resistance for SCADA in smart grid. Sec. Commun. Netw., **8** (6) (2014), 1026–1039.

[142] Yu, K.; Zhang, D.; Mohammad, A.; Nguyen, N.H.; Sato, T.: A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid, in *IEEE 2014 Int. Conf. on Power System Technology (POWERCON)*, 2014, 2019–2024.

[143] Liu, T. *et al.*: A dynamic secret-based encryption scheme for smart grid wireless communication. IEEE Trans. Smart Grid, **5** (3) (2014), 1175–1182.

[144] Badra, M.; Zeadally, S.: Design and performance analysis of a virtual ring architecture for smart grid privacy. IEEE Trans. Inf. Forensics Sec., **9** (2) (2014), 321–329.

Miles H.F. Wen received the B.Eng. degree in computer engineering and Ph.D. degree in Electrical and Electronic Engineering from the University of Hong Kong, Hong Kong, in the 2011 and 2015, respectively. His research interests include smart grid technologies and Internet technologies.

Ka-Cheong Leung received the B.Eng. degree in Computer Science from the Hong Kong University of Science and Technology, Hong Kong, in 1994, the M.Sc. degree in Electrical Engineering (Computer Networks) and the Ph.D. degree in Computer Engineering from the University of Southern California, Los Angeles, California, USA, in 1997 and 2000, respectively. He was Senior Research Engineer at Nokia Research Center, Nokia Inc., Irving, Texas, USA from 2001 to 2002. He was Assistant Professor at the Department of Computer Science at Texas Tech University, Lubbock, Texas, USA, between 2002 and 2005. Since June 2005, he has been with the University of Hong Kong, Hong Kong, where he is currently Assistant Professor at the Department of Electrical and Electronic Engineering. His research interests include transport layer protocol design, vehicle-to-grid (V2G), and wireless packet scheduling.

Victor O.K. Li received S.B., S.M., E.E. and Sc.D. degrees in Electrical Engineering and Computer Science from MIT in 1977, 1979, 1980, and 1981, respectively. He is Chair Professor of Information Engineering and Head of the Department of Electrical and Electronic Engineering at the University of Hong Kong (HKU). He has also served as Assoc. Dean of Engineering and Managing Director of Versitech Ltd., the technology transfer and commercial arm of HKU. He served on the board of China.com Ltd., and now serves on the board of Sunevision Holdings Ltd. and Anxin-China Holdings Ltd., listed on the Hong Kong Stock Exchange. Previously, he was Professor of Electrical Engineering at the University of Southern California (USC), Los Angeles, California, USA, and Director of the USC Communication Sciences Institute. His research is in the technologies and applications of information technology, including clean energy and environment, social networks, wireless networks, and optimization techniques. Sought by government, industry, and academic organizations, he has lectured and consulted extensively around the world. He has received numerous awards, including the PRC Ministry of Education Changjiang Chair Professorship at Tsinghua University, the UK Royal Academy of Engineering Senior Visiting Fellowship in Communications, the Croucher Foundation Senior Research Fellowship, and the Order of the Bronze Bauhinia Star, Government of the Hong Kong Special Administrative Region, China. He is a Registered Professional Engineer and a Fellow of the Hong Kong Academy of Engineering Sciences, the IEEE, the IAE, and the HKIE.

Xingze He received the B.S. and M.S. degrees in the Department of Communication and Information System at Xi'an Jiaotong University, Xi'an, China, in 2007 and 2009 respectively, and the Ph.D degree from the Ming Hsieh Department of Electrical Engineering at University of Southern California, Los Angeles, USA, in 2013. His current research interest is in the area of Smart Grids including power quality problem detection, public key cryptography and homomorphic encryption.

Chung-Chieh Jay Kuo received the B.S. degree from National Taiwan University, Taipei, Taiwan, in 1980, and the M.S. and Ph.D. degrees from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 1985 and 1987, respectively, all in electrical engineering. He is currently the Director of the Multimedia Communications Laboratory and DeanŠs Professor of Electrical Engineering at the University of Southern California, Los Angeles, CA, USA. His research interests include digital image/video analysis and modeling, multimedia data compression, communication and networking, computer vision and machine learning. He has co-authored about 230 journal papers, 870 conference papers, and 13 books. He is a fellow of the Institute of Electrical and Electronics Engineers (IEEE), the American Association for the Advancement of Science (AAAS) and the International Society for Optical Engineers (SPIE).