A Survey on Energy Internet Communications for Sustainability

Kun Wang, *Member, IEEE*, Xiaoxuan Hu, Huining Li, Peng Li, *Member, IEEE*,
Deze Zeng, *Member, IEEE*, and Song Guo, *Senior Member, IEEE*

Abstract—Energy Internet (EI) is proposed as the evolution of smart grid, aiming to integrate various forms of energy into a highly flexible and efficient grid that provides energy packing and routing functions, similar to the Internet. As an essential part in EI system, a scalable and interoperable communication infrastructure is critical in system construction and operation. In this article, we survey the recent research efforts on EI communications. The motivation and key concepts of EI are first introduced, followed by the key technologies and standardizations enabling the EI communications as well as security issues. Open challenges in system complexity, efficiency, reliability are explored and recent achievements in these research topics are summarized as well.

Index Terms—Energy internet, survey, communications, security, smart grid

SG	Smart Grid
EI	Energy Internet
ICT	Information and Communication Technologies
DG	Digital Grid
DGR	Digital Grid Router
CR	Cognitive Radio
SDN	Software-defined Network
WSN	Wireless Sensor Network
HAN	Home Area Networks
NAN	Neighborhood Area Networks
WAN	Wide Area Networks
FREEDM	The Future Renewable Electric Energy Delivery and Management System
SST	Solid State Transformer
DRER	Distributed renewable energy resources
DER	Distributed energy resources
DESD	Distributed energy storage devices
MPC	Multiport converter
PLC	Power line communication
TDM	Time-division Multiplex
MAS	Multi-agent system
PVs	Photovoltaic cells
EV	Electric vehicle
WCNs	Wide Area Network Cloud Nodes
LCNs	Local Area Network Cloud Nodes
API	Application Program Interface
IEC	Intelligent Energy Controller
ADP	Adaptive Dynamic Programing
D2D	Device-to-Device
CoMP	Coordinated Multipoint
DSM	Demand-side management
AMI	Advanced Metering Infrastructure
EMS	Energy Management System
DMS	Distribution Management System
WAMS	Wide Area Measurement System
MDMS	Metering Data Management System
DCU	Data Concentrator Unit
SCADA	Supervisory Control and Data Acquisition
AGC	Automatic Gain Control
DAS	Distribution Automation System
GIS	Geographic Information System
PMUs	Phasor Measurement Units
ATO	Advanced Transmission Operation
AAM	Advanced Asset Management
PKG	Private Key Generator
IBE	Identity Based Encryption
SoS	System of System
DCCS	Distributed Computer Control System
DGI	Distributed Grid Intelligence
PSO	Particle Swarm Optimization
GCDC	Grand Cooperative Driving Challenge
DoS	Denial of Service
PHEV	Plug in Hybrid Electric Vehicle
NIST	National Institute of Standards and Technology
PCA	Principal Components Analysis

- *K. Wang is with the Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing University of Posts and Telecommunications, Nanjing 210003, China, and the Department of Computing, Hong Kong Polytechnic University, Hong Kong, China. E-mail: kwang@njupt.edu.cn.*
- *X. Hu and H. Li are with the Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing University of Posts and Telecommunications, Nanjing 210003, China. E-mail: hu_xiaoxuan@hotmail.com, huinli@outlook.com.*
- *P. Li is with the School of Computer Science and Engineering, University of Aizu, Aizu-Wakamatsu City, Fukushima 965-8580, Japan. E-mail: pengli@u-aizu.ac.jp.*
- *D. Zeng is with the School of Computer Science, China University of Geosciences, Wuhan 430074, China. E-mail: deze@cug.edu.cn.*
- *S. Guo is with the Department of Computing, Hong Kong Polytechnic University, Hong Kong, China. E-mail: song.guo@polyu.edu.hk.*

Manuscript received 3 Jan. 2017; revised 9 May 2017; accepted 17 May 2017. Date of publication 23 May 2017; date of current version 6 Sept. 2017.
(Corresponding author: Peng Li.)
Recommended for acceptance by V. Eramo.
For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TSUSC.2017.2707122

1 Introduction

According to the latest statistics [1], [2], [3], our existing computation and communication systems (e.g., data centers and cellular networks) have over-reliance on fossil fuel in current power system, and the imbalance between energy supply and demand is in continuous deterioration. Smart grid (SG) [4], [5], [6] has been proposed as the next-generation power grid, and attracts attention from both industry and acadamia. Different from traditional power grid with a tree-like hierarchical structure, smart grid enables two-way flows of electricity and information to create a widely distributed and automated energy delivery system.

Although smart grid is promising, recent studies and experiments show that it is still inadequate to address the challenges of growing complexity, variability, and high volume of the energy loads because of following reasons: (1) Smart grid accommodates and manages only a single-form energy, i.e., electricity. But in practice, energy can be generated, delivered and consumed in different forms, such as chemical, thermal and electromagnetic energy; (2) The electricity flows in smart grid are still delivered over existing power distribution grid. Although smart grid promises two-way electricity flows between consumers and power facilities, it has limited flexibility on energy flow scheduling and routing, leading to local energy sharing and suboptimal resource utilization.

Energy Internet (EI) [7], which is regarded as the evolution of smart grid, aims to sustainable computing by integrating various energy forms into a highly flexible grid similar to the Internet. It provides energy packing and routing functions in the global scale. The concept of EI has been proposed for more than a decade, but its definition has not reached a consensus. Huang et al. [8] treat the EI as an energy delivery and management system including existing power system and distributed energy sources. In the view of E-energy [9], EI is the combination of information and communication technologies (ICT) as well as the energy system. Digital Grid (DG) in Japan focuses on building an EI system by connecting microgrids using DG routers [10].

A typical EI system consists of three subsystems: energy subsystem, information subsystem, and network subsystem, which are connected by energy routers. As shown in Fig. 1, the energy router is the core of EI, and connects three subsystems by enabling both energy and data flow forwarding. Xu et al. [11] first introduced the concept of energy router with two major functions: dynamic scheduling of energy flows and real-time communications between power devices. Later, several visions on architectural design of energy router, such as energy hub [12], E-energy [13], digital grid router (DGR) [14], have been proposed by integrating information and communication technologies.

Communication technologies are critical to realize the promises of EI, and have melted into the information and network subsystems by connecting different components of EI to enable real-time monitoring, controlling and management. The information subsystem consists of intelligent sensing and computing infrastructure. It serves as an open platform for data gathering, analysis and management. The network subsystem connects all devices in the EI system by using wired and wireless technologies, such as ZigBee [15], WiMAX [16], cognitive radio (CR) [17], cellular communications [18], and software-defined network (SDN) [19]. These technologies are combined in EI to implement real-time monitoring of customers' demands and optimal energy allocation. For instance, SDN can be applied in EI to effectively support energy scheduling to satisfy the customized demands [20]. Although some technologies have been already applied in smart grid, there are many open challenges in integrating them into EI with multiple energy forms and flexible energy control. For example, the automatic and real-time communication between different users necessitates the information and communications systems with two-way communication capability, high transmission rate, and low latency that the smart grid cannot support.

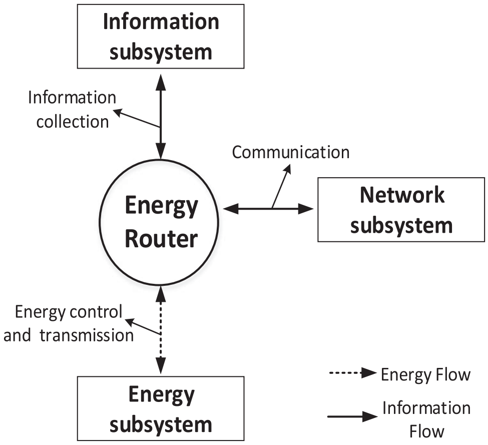


Fig. 1. Energy routers in EI.

With the help of communication technologies, EI system is constructed to realize the integration of information flow and energy flow [21]. Information subsystem has processing capability to predict and monitor the changes in extreme unstable power production, supply, and users' demands. Meanwhile, energy subsystem is responsible for energy transformation and scheduling. Features of distribution, openness and interconnectivity enable EI to intelligently manage both energy flow and information as well as promote operation efficiency. However, on the other hand, such features also make EI be a vulnerable system. Any malicious attack on a subsystem, either on the information flow or on the energy flow, may raise unprecedented disaster. For example, Stuxnet was a well-known malware program which intruded a large number of equipments in Iran nuclear power station and caused massive damages [22]. Similar malware program intrusion behaviors in energy system also happened in US and many other countries [23]. The interconnection of energy equipments, programs, applications, energy big data, power provides and terminal costumers shall raise more security threats. Exploit attack, malicious hack, eavesdropping and other serious bugs in either subsystem may incur unprecedented security problems to the whole system. In addition, privacy protection is another critical security issue as the customers' privacy information, without careful protection, are prone to be acquired by malicious attackers.

There are several articles [24], [25], [26], [146], [147], [148] that survey the recent work about smart grid, but the achievements in EI communication are seldom summarized. Wang et al. [27] introduce the concepts and characteristics of EI, and discuss EI infrastructure as well as related information technologies. They present the existing EI prototypes and compare them with traditional power grid and smart grid. Cao et al. [28] present an EI model where the energy router is regarded as the core switching devices. The existing supporting technologies and deployment issues are discussed. These two articles only give general descriptions about EI by introducing concepts and visions. Wang et al. [29] present a communication architecture for EI based on power electricity, and discuss several candidate information and communication technologies that can be applied in EI. Wang et al. [159] provided a survey on the basic concepts of EI and some technologies that could be used in EI. In addition, the differences among these surveys are discussed in Table 1. As can be seen from the table, these existing surveys have paid little attention to the communication technologies in EI.

This paper provides a comprehensive survey for the EI communication system and make the following contributions:

- We provide a detailed discussion of recent achievements in energy router, information, network aspects, standardizations, and security issues in EI communications.
- We discuss in detail the definitions and designs for the existing energy routers.
- We provide a review of communication technologies and give a comparison in the information and network aspects.
- We provide a survey of security issues from the aspects of requirements, potential solutions and remaining problems.

The rest of our paper is organized as follows. Section 2 describes the motivation and concepts of the EI system. In Section 3, we introduce major communication techniques in three aspects: energy router, information sensing and processing, and network technologies. Section 4 introduce the overview of EI communication security and potential solutions. Section 5 reviews the recent standardizations in EI communications. Section 6 discusses the challenges and future work. Conclusion is given in Section 7.

2 Motivations and Concepts

In this section, we first present the motivations of the EI by highlighting its differences from smart grid. Then, we introduce the EI communication infrastructure and its main functions.

2.1 Motivations

Our current electric grid was designed and built several decades ago when most homes has only small energy demands. The electricity is delivered from power plants to local communities, and consumers are billed once a month. It is difficult for the grid to respond to ever-changing and rising energy demands.

Smart grid aims to enhance the existing electric grid by enabling a two-way interaction between power plants and consumers. Smart meters and sensors are deployed to monitor the real-time power consumption and the health of power grid. Furthermore, renewable energy sources, such as solar and wind, are integrated into the power grid for cost saving. Fang et al. [30] studied the smart infrastructure system, the smart management system, and the smart protection system in smart grid, and investigate the future directions and challenges. Erol-Kantarci et al. [31] explored an energy-efficient communication architecture for smart grid, which includes Home Area Networks (HAN), Neighborhood Area Networks (NAN) and Wide Area Networks (WAN), based on wireless, wired and optical technologies. Bera et al. [32] discussed the cloud computing for energy management, information management, and security issues in smart grid.

Since the main components of smart grid are still built based on existing electric grid, it cannot address all weaknesses and the efficiency improvement is very limited. For an instance, in smart grid, the energy is distributed from generation sources to local electrical loads. The bi-directional energy transmission can only be conducted in a limited region due to the vehicle-to-grid technologies. The electric vehicles can charging their batteries from the grid and also can feedback the electricity to the grid. In a wide area, the energy flow can only be in a one-way transmission as the energy flow is transmitted from high voltage network to low voltage network. In addition, As the evolution of smart grid, the EI takes one giant step forward by introducing a novel power generation and distribution paradigm based on the energy router, a completely new design for energy and information exchange over longer distances. The main differences between smart grid and EI are listed as follows.

- The EI accommodates energy in multiple forms, such as chemical, thermal and electromagnetic energy, from distributed energy sources [33], while smart grid can deal with only electricity distribution.
- EI integrates energy and information exchange into a single infrastructure based on the energy router. In smart grid, energy is delivered over existing power grid, and information exchange is based on Internet.
- EI is constructed to achieve energy balance between supply and demand based on the Internet, distributed intelligence, and big data applications on a large-scale level. But in SG, the energy coordination is mainly enabled by a localized approach.

In order to widen the range of interconnection of power systems, multiple advanced communication technologies are in great need. An efficient and interoperable communication infrastructure is an essential part of EI system, which is responsible for effective and real-time energy management between interconnected equipment and systems. The EI communication infrastructure is constructed based on the communication structures of Internet and SG, but they are not the same. Compared with Internet communication and SG communication, EI communication is different in several aspects, as shown in Table 2. EI communication mainly utilizes energy router to implement the delivery and management of both distributed renewable energy and multi-source data, while Internet communication and SG communication are designed to transmit data and information. Generally, the energy transmission is the heart of the distinction.

2.2 The EI Communication Infrastructure

Fig. 2 illustrates the EI communication infrastructure consisting of distributed energy resources, management

TABLE 1
The Comparison with Related Survey Articles

Subject		Survey articles									
		Smart grid					EI				
		[24]	[25]	[26]	[146]	[147]	[27]	[28]	[29]	[148]	[159]
Communication	Requirement	✓	✓				✓	✓			✓
	Technologies	✓	✓	✓			✓		✓	✓	✓
	Security		✓	✓							✓
	Standards		✓	✓							
Energy router							✓	✓		✓	
Architecture					✓	✓	✓	✓	✓		✓
Application		✓			✓				✓		
Cyber security					✓	✓					

TABLE 2
The Distinctions Between Internet Communication, WSN Communication, SG Communication, and EI Communication

Categories	Internet communication [27]	WSN communication [149]	SG communication [24]	EI communication [29]
Characteristics	Data transmission	Data transmission	Information transmission	Energy and information transmission
Service objects	Multi-source heterogeneous data	Multi-source sensor data	Multi-source heterogeneous data	Multiple distributed renewable energy and Multi-source heterogeneous data
Routing equipment	Network routers and switches	Sensor nodes	Smart meters	Energy routers and smart routers
Functionality	Network interconnection Data processing (including firewall) Network management	Network interconnection Data acquisition and processing Data management	Grid interconnection Data processing Grid management	Grid interconnection Data and energy transmission processing (including isolation in power transmission) Grid management
Standards setting	Many international wired and wireless transmission standards are available	Many standards and protocols applicable to the particular scenario	Few national standards are available, more international standards are being set up	Not available

regions, and energy demands from residents, factories and electric vehicles. Distributed energy sources mainly include solar electricity, wind turbine, hydroelectricity, and energy storage [34]. Management regions contain data center, control center, and smart energy management system. Energy routers are deployed to provide energy and communication services [35], [144], [145]. For instance, a wide area grid is constructed to enable the energy and information exchange among different regions, where energy routers play vital roles in EI communication to realize intelligent energy management [36]. The energy routers in wide area network are responsible for the allocation of global energy and they can provide the bidirectional control of energy flows and the function of devices grouping. In addition, energy routers connecting distributed resources can achieve energy distribution and optimization. In management regions, both data center and control center help EI to conduct smart energy management in user side and power side. Meanwhile, electricity information acquisition control and monitoring of electricity quality can be implemented by smart meters.

In EI communication, the data volume could reach up to petabytes or even larger, causing energy network congestion. Many effective communication technologies such as fiber optical, power line communication, cellular communication, and CR, are proposed to increase throughput, prevent network congestion, and guarantee secure transmission in EI.

The main purpose of EI communication based on energy routers is to enable the information exchange to achieve real-time balance between energy generation and consumption. Thus, there are several functions equipped with the communication infrastructure in EI system as follows:

2.2.1 Energy Management

Unlike SG, the EI system needs to manage different types of energy in a large scale. To implement correct and efficient energy management, energy routers need to monitor energy generators, the quality of energy flows, and energy consumption in real-time. Meanwhile, energy routers can schedule energy flows for flexible and efficient energy management.

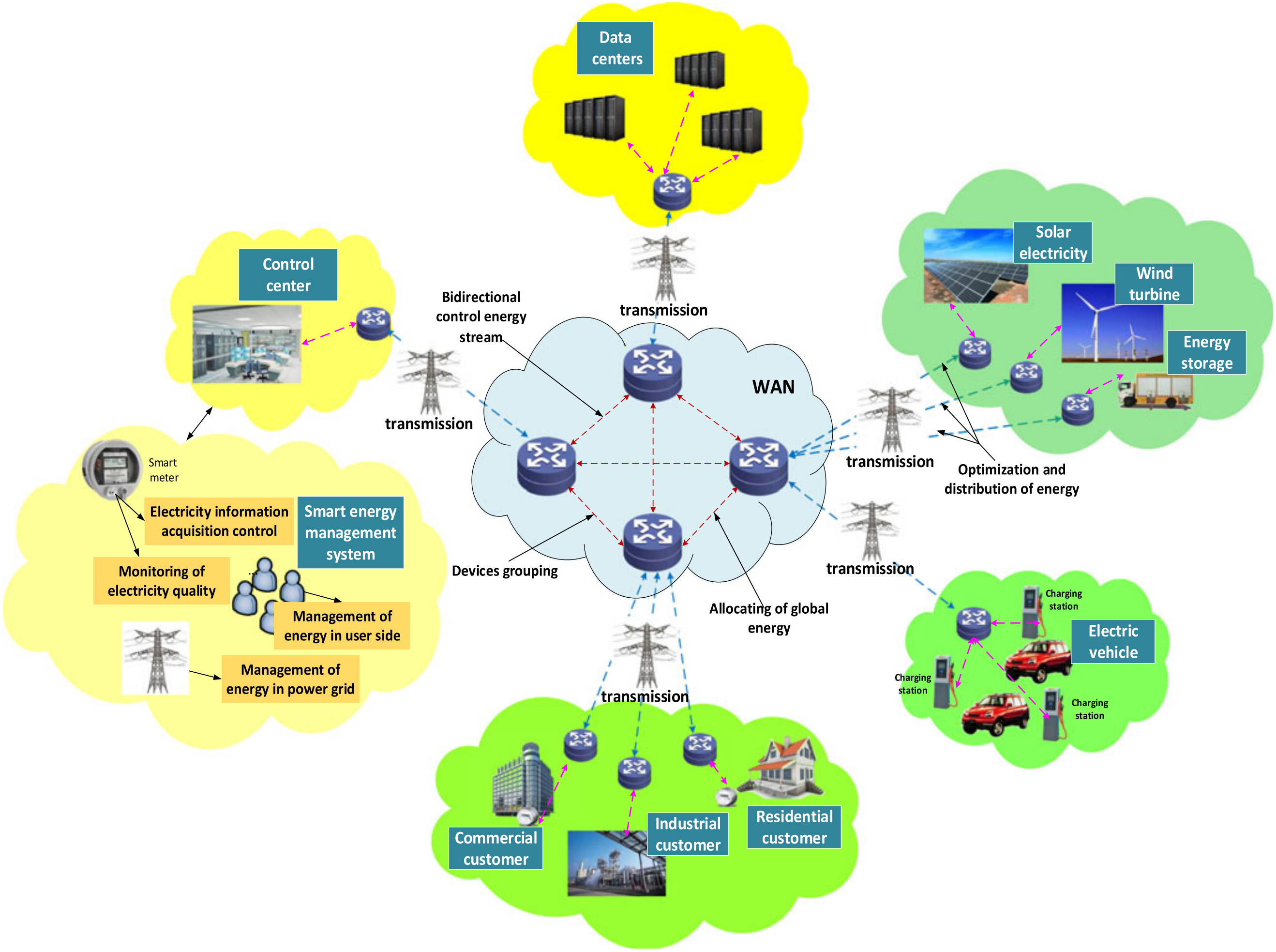


Fig. 2. Vision of EI communication infrastructures.

2.2.2 *Grid Operation Management*

Grid operation management is also important for EI. In SG, the grid management depends on the technologies in power transmission and distribution network. Energy routers in EI provide two modes: the grid-tie mode and the islanding mode for grid operation management [11]. In the grid-tie mode, energy routers are considered as energy flow regulators to balance energy supply and demand. In the islanding mode, the microgrid can be disconnected from the main grid by energy routers for protection.

2.2.3 *Real-Time Interaction with User Terminals*

EI is able to interact with user equipments and generate end behaviors through intelligent agent terminal. Based on real-time communication and measurement technologies. It can make accurate estimation on the power generation and consumption and provide customized energy using plans for users to choose.

2.2.4 *Plug-and-Play*

With the lower cost of distributed generation equipment, non-hardware cost (e.g., complicated installation and interconnection) has been accounted for an increasing proportion. Moreover, the fixed topology can also reduce the flexibility and security of the EI system. Therefore EI should support plug-and-play technology so that the grid can accommodate various power sources, especially distributed renewable energy sources and energy storage devices [37]. The advanced plug-and-play interface has the functions of power conversion and open-standard-based communication. The power conversion can be implemented via power electronic converters. The communication interface can instantly recognize the energy types of device connected to the grid and make response to the energy interaction based on users' requests. In order to fully exploit the plug-and-play functionalities, the inter-operability issues should be solved first in following three aspects: 1) Various energy equipment should be recognized each other; 2) An universal standards and protocols need to be developed; 3) The integration management of energy equipment should be implemented well.

3 Key Technologies

In order to achieve the realization of the EI systems, advanced communication technology is the significant part to implement the information exchange. In this section, we present key technologies for EI communication. The classification of the key communication technologies is presented in Fig. 3.

3.1 Energy Router

The energy router is the core of energy generation, distribution and storage. Different from the conventional electric

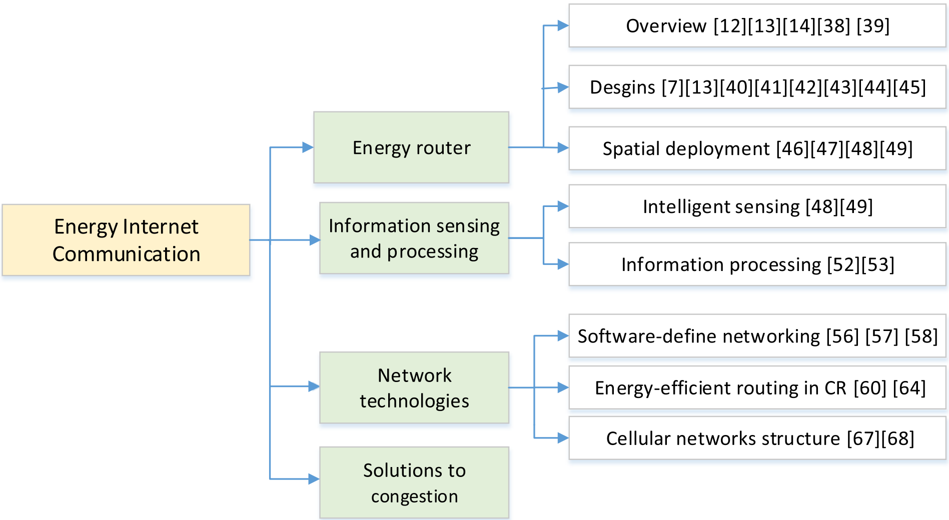

Energy Internet Communication
Energy router
Information sensing and processing
Network technologies
Solutions to congestion
Overview [12][13][14][38] [39]
Desgins [7][13][40][41][42][43][44][45]
Spatial deployment [46][47][48][49]
Intelligent sensing [48][49]
Information processing [52][53]
Software-define networking [56] [57] [58]
Energy-efficient routing in CR [60] [64]
Cellular networks structure [67][68]

Fig. 3. The classification of communication technologies in EI system.

devices, the energy routers are expected to be provided with the following features [150]. First, it could achieve a bidirectional high-quality power conversion among different kinds of terminals. Second it should equipped with plug-and-play interfaces to support the seamless connection between end users and electrical network. Third, it can achieve the optimal energy management in the local grid or the whole EI.

3.1.1 Overview of Energy Routers

EI has a fundamental view of the effective management of the energy flow and information flow. Energy router is considered as an intelligent energy transformer and management equipment. The overviews of energy router, energy hub, DGR, and E-router are as follows and the comparison between them is shown in Table 3.

- The energy router proposed by the FREEDM system [38] behaves as an intelligent energy management (IEM) node in EI, which consists of the solid state transformer (SST) device, distributed grid intelligence (DGI) software, and communication ports. The distributed renewable energy resources (DRER), distributed energy storage devices (DESD), and power loads are all connected to energy routers.
- The Swiss Federal Science Institute Research Team [12], [39] defined the energy hub, an unit for energy conversion and storage. Energy hubs themselves could be energy consumers that provides specific services. For example, many facilities such as industrial enterprises, commercial complexes, rural regions, and transportation vehicles can be regarded as energy hubs.
- The DGR is developed by the Japan federation of digital power grid, which is entirely based on information networks [14]. It connects existing power grid and EI by allocating IP addresses to various power grid equipments, such as generators, power converters, wind farms, storage systems, and rooftop solar cells. The base stations can be identified with IP address by DGR to implement the energy distribution.
- The E-router is defined by Shanghai Key Lab of Power Station Automation Technology [13]. It is an important equipment responsible for power dispatching and managing multiple distributed renewable energy sources in low-voltage delivery networks. The E-router can be classified into different types, according to the design structures and practical applications in terms of power transformation, energy administration and network communication.

TABLE 3
The Comparison Among Energy Router, Energy Hub, DGR, and E-Router

Types	Energy router	Energy hub	DGR	E-router
	[38]	[12], [39]	[14]	[13]
Energy flow	✓	✓	✓	✓
Information flow	✓		✓	✓
Two-way communication	✓		✓	✓
Plug and play	✓	✓		✓
Multiple renewable energy resources	✓	✓		✓

3.1.2 Designs of Energy Routers

Favre-Perrod et al. [40], [41] designed an energy router as an interface between various energy infrastructures and loads. It can be implemented as either an energy hub or an energy interconnector. An energy hub can conduct conversion, monitoring and storage of multiple energy sources to increase the reliability of power supply. As shown in Fig. 4, four energy sources, electricity, natural gas, district heat and wood chips, are connected to an energy hub that outputs electricity and energy for cooling and heating. In addition, the optimization of energy supply is enabled by characterizing the hub's inputs based on the cost, related emissions, availability and so on.

An energy interconnector supports the intergrated transmission of electricity, gas, and heat, as shown in Fig. 5. When the electricity and gas is transmitted through a single

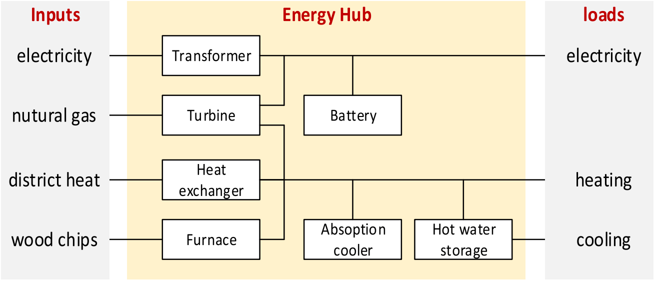


Fig. 4. The structure of energy hub [41].

energy interconnector, the gas temperature will increase because the heat losses are partially transferred to the gas. At the end of the connection, the heat losses will be recovered. As a result, electricity and gas transmission can be conducted simultaneously, greatly improving the efficiency of multiple energy transmission. However, the above researches take a greenfield approach into consideration without the concern of information transmission.

Xu et al. [7] suggested that the energy router should combine two technologies: power transmissions and information exchanges. The FREEDM project in the US uses the SST as a core component of the energy router in EI. Fig. 6 shows their proposed design of the energy router that integrates three core modules: power electronics module, communications module, and distributed grid intelligence module. Power electronics module supporting plug-and-play is able to convert the voltage. A series of sub-transformers can be used to provide different voltage ports for various electrical appliances. However, the energy in this energy router design is only in the form of electricity. There are two components in the communication module: the intra-communication component and the inter-communication component. The latter was designed as a communication board connected to the controlled SST. Several network access technologies can be adopted in the communication module, such as ZigBee, Ethernet, and wireless LAN. Meanwhile, a protocol for the communications between the communication module and SST was designed. The latency performance of this proposed module has been measured and the results cannot reach the required latency boundary. Therefore, there is still a large improvement on the communication delay. The grid intelligence module is incorporated into SST controller broad. The grid intelligence module uses the information collected from the communications module in every energy router to make the intelligent grid operation decisions on the management of optimized energy generation and distribution.

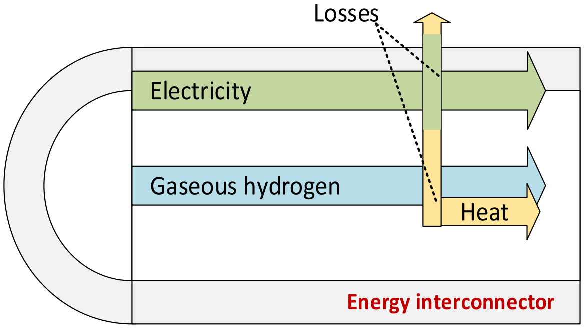


Fig. 5. The structure of energy interconnector [41].

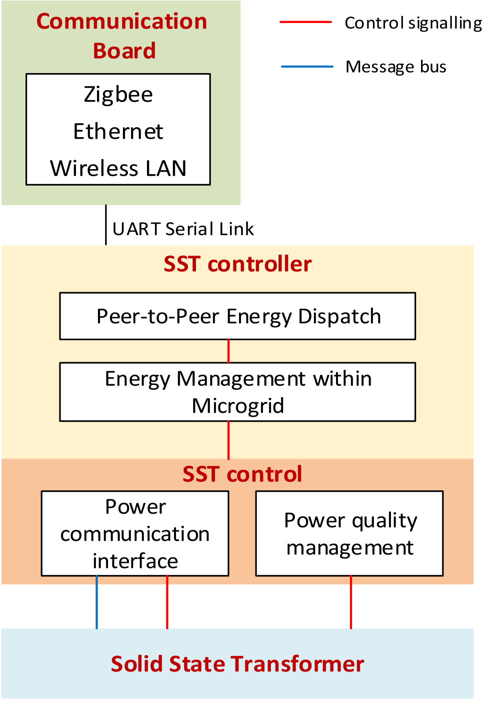


Fig. 6. The structure of energy router [7].

Guo et al. [13] divided E-router into three categories: SST-based E-router, multiport converter (MPC)-based E-router, and power line communication (PLC)-based E-router. SST-based E-router includes energy management module, power electronic conversion module and plug-and-ply interface, as same as the energy router in FREEDM project. Comparing to the SST-based E-router, MPC-based E-router achieves higher degree of reuse and integration [42], as shown in Fig. 7. In MPC-based distributed energy system, all kinds of subsystems can be contained, controlled by multiple port bidirectional converters to implement the energy supply balance. Each subsystem includes distributed energy sources, storage devices, and loads, connecting an independent DC bus system by their own DC ports.

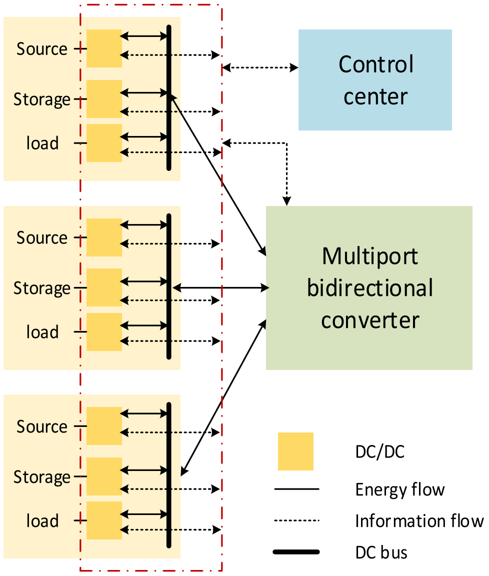


Fig. 7. The structure of MPC-based E-router [13].

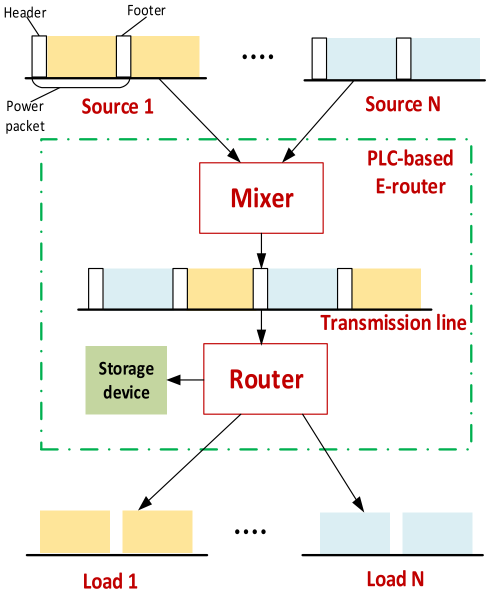


Fig. 8. The structure of PLC-based E-router [13].

Unlike SST-based E-router and MPC-based E-router, PLC-based E-router can achieve both energy and information transmission with low cost and low volume. PLC is not a new technique, dating back to the early 1900s [43]. In order to implement the information management and transmission in the aging power grid, PLC emerges again. The low cost of PLC deployment is the most obvious advantage compared to other wired communications. The existing distribution networks use transmission lines directly, greatly reducing the investment on networks. Meanwhile, the power line can form the most extensive networks and each family can be easily involved in. However, in order to achieve reliable long-distance communication with high capacity in EI, PLC still has the following shortages: low data transmission rates, limited bandwidth, signal attenuation, and high noise. When it applied into energy routers, the significant signal distortion and power loss cannot be ignored. Since distribution system voltage dispatching needs to realize the communication between substation and distribution feeder without high transmission rates, PLC technology becomes more challenging. Cheng et al. [44] proposed relay-aided (RA-) PLC to address these issues. A dual-hop amplify-and-forward (AF) based RA-PLC system was investigated, and a comparison between AF-based RA-PLC system capacity and direct link (DL)-PLC system capacity was conducted with the signal attenuation model. The proposed AF-based RA-PLC has the higher capacity and provides more branches and lower load impedances.

However, in order to implement both energy and information transmission simultaneously, conventional PLC technology still has some limitations, for example, the energy flow in EI cannot implenment the time-division and multi-path transmission. Therefore, Takuno et al. [45] proposed the time-division multiplex (TDM) technologies emloyed in the energy subsystem, as shown in Fig. 8. Each energy source is divided into a number of power packets, containing a header, a footer, and a piece of energy. Similar to the data packets in the Internet, each power packet is labeled with the information of senders and receivers. As a result, the energy package is quantized at the source side. Then, these power packets from different sources are multiplexed to the same transmission line through TDM technologies. Once the energy packages are received and decoupled at the load side, the energy is distributed by E-router to the given destination. Meanwhile, in considering of the intermittent and instability of the renewable energy, a energy storage device is deployed in the PLC-based E-router to improve the energy quality.

3.1.3 Spatial Deployment of Energy Routers

Based on above design, many research efforts focus on solving optimization problems in practical deployment. Hguyen et al. [46] designed a topology of energy routers in the active distribution network and studied the energy transmission strategy in energy routers. Meanwhile, the multi-agent system (MAS) is designed to enable the autonomous control of energy routers in the active distribution network. Deng et al. [47] studied the problem of optimal energy router allocation and designed a particle swarm algorithm to decide the installation locations of energy routers. Zhang et al. [48] designed a reliable energy router topology to realize the plug and play of photovoltaic cells (PVs) and circuit isolation for the access of residential solar energy. Yi et al. [49] proposed the concept of electric vehicle (EV) energy network and analyzed the deployment of energy routers in EV energy network to optimise the renewable energy usage.

3.2 Information Sensing and Processing

EI aims to provide flexible energy provision and sharing, which relies on the information technologies, including data sensing, gathering, transmission, processing, and service. We elaborate key technologies of intelligent sensing and information processing as follows.

3.2.1 Intelligent Sensing

Smart meters are installed at the customer side to obtain information of real-time electricity consumption [7]. Rech et al. [50] addressed that the smart meter works together with controllers for energy management in a decentralised hierarchical communication architecture in EI, consisting of multiple layers. The controllers at the bottom layer acts as gathering the energy requirements and production information via smart meters and other information collection facilities [51]. Electric energy are transferred from the bottom layer to the upper layer to keep balance between the provider and the consumer. When energy-using units cannot achieve the balance, the controller at bottom will send energy requesting information to the upper controller and cooperate with backbone bus structure to make adjustments.

Nowadays, smart meters become the mainstream of metering devices in the development of global power grid. Each smart meter has a unique and addressable identifier to enable the communication between users and power facilities [52]. Jignesh et al. [53] designed a multi-agent system with smart meters to manage the real-time power supply in a huge geographic region. The multi-agent system provides distributed analyses for fast restoration after failure by studying the types of agents and behaviours to exchange information.

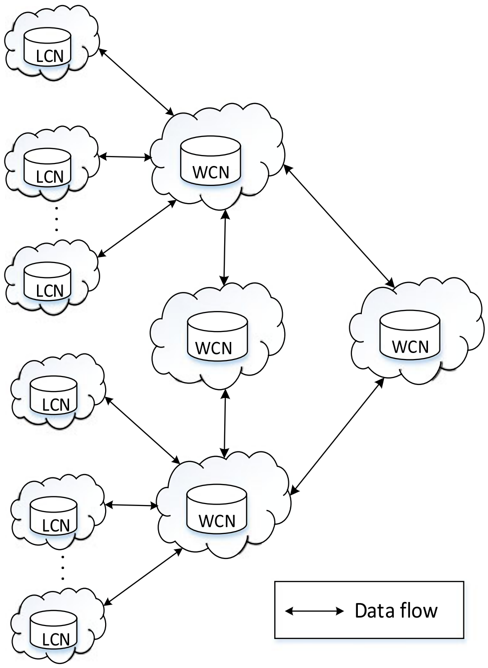


Fig. 9. The structure of cloud computing in EI [54].

3.2.2 Information Processing

Cloud computing technology can be used to process and storage information in the EI system. A cloud structure for information processing in EI has been proposed in [54]. As shown in Fig. 9, wide area network cloud nodes (WCNs) are deployed to offer cloud computing services (such as energy transaction and electricity charging) in wide area, while local area network cloud nodes (LCNs) are responsible for data processing (such as coordinating regional sources and forecasting community load) in microgrids. When power shortage or surplus happens in distributed and autonomous microgrids, they optimize power dispatching according to the information provided by WCNs and LCNs. Furthermore, the computational loads on WCNs and LCNs are different and change with time. The WCN in the root of Fig. 9 monitors real-time loads on LCNs as well as other WCNs, and rebalances the computation loads by migrating computing tasks among them.

A summingbird platform [55] has been proposed for real-time information management by enabling cloud-based data processing, flexible data sharing and robust system control. It can support both batch and stream processing based on Hadoop and Storm, respectively. The data mining jobs, such as power demand forecast and usage pattern discovery, are divided into small tasks that run multiple computing nodes in parallel.

3.3 Network Technologies

The EI system can be considered as a vast network that connect numerous devices and customers in an efficient and reliable manner. Table 4 summarizes the current achievements and limitations of the network technologies in EI.

3.3.1 Software-Defined Networking

An innovative software-defined network platform with three layers has been proposed in EI in [56]. The infrastructure layer at the bottom includes various wireless accessible devices like energy routers and virtual switches. The control layer in the middle is based on the OpenFlow protocol and effectively controls network traffic by separating the control plane and the data plane. The application layer in the top connects with control layer via application program interface (API). The application layer contains the service offered by the network operator, such as mobility management, traffic monitoring, and energy-efficient networking.

Zhang et al. [57] proposed a SDN-based network architecture, including intelligent energy controller (IEC), data center, and controller, for EI, as shown in Fig. 10. IEC monitors local distributed energy generation and energy storage devices and collects real-time information that are grouped into several categories, such as power generation information, electricity selling information and electricity purchase information. Then, such data are transmitted to data center via communication network for instant processing. Controllers communicate with IECs and data centers via the OpenFlow protocol to manage the energy flow and data analysis.

TABLE 4
Communication Technologies in Networks

Key Technologies	Related Works	Achievements	Limitations
Software-defined networking	G. Zhang et al. [57]	Propose a SDN based communication architecture in EI for energy interconnection.	-High latency in control networks
	M. Celenlioglu et al. [58]	Use SDN technology to set up an energy-aware routing model in communication networks.	-Security issues in controllers
	M. Vuppuluri et al. [59]	Design an optimized algorithm on controller to construct a SDN based energy efficient network.	-Many protocols are immature
Energy-efficient routing in CR	A. Khan et al. [61]	Show how to integrate CR based communication technology into EI system in different regions.	-Reliability threats
	R. Yu et al. [65]	Put forward ADP approach based on CR technology to optimize QoS.	-Maintenance of reliable link
Cellular networks structure	C. Kalalas et al. [68]	Propose a novel cellular technology called D2D communications in LTE standard.	-High monthly charges
	S. Bu et al. [69]	Design a system based on Stackelberg game model to descrease operational expense and green house emission.	-Delay for call establishment

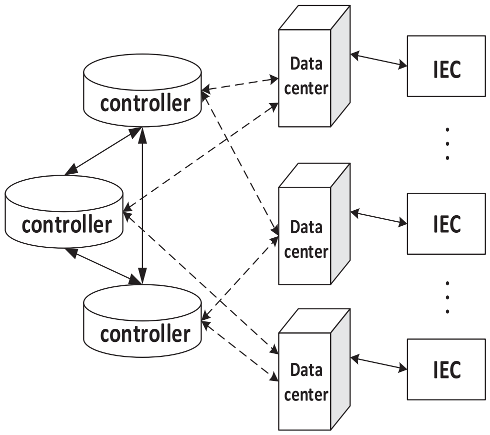


Fig. 10. The architecture of SDN based on EI [57].

To construct reliable communication network in EI, every data center need to connect two controllers at least so that one of the controllers can act as data backup controller to avoid data loss situations. Hence, the cluster technology is introduced to coordinate and build a special communication mechanism between multiple controllers in EI.

Celenlioglu et al. [58] used the SDN technology to bulid an energy-aware routing model for effective resource utilization in EI communication networks. The controller uses existing protocol to find paths between entry and exit energy routers in advance. These pre-built paths can be divided into operative ones and static ones. Operative paths carry communication traffic between energy routers, while static ones are in sleep. The controller can perform energyware routing control by first deciding which paths should be activated or deactivated for larger communication capacity with lower energy consumption. Second, the controller collects path information from energy routers and calculates network traffic in an iterative manner to balance network load according to path cost. Finally, a path resizing algorithm is applied to make adjustments on communication resource between under-used paths and over-used paths in time.

Vuppuluri et al. [59] designed an optimized algorithm to construct a SDN based energy efficient network. The controller is regarded as a pluggable programming module to manage network traffic and interact with other modules by writing code into it. In the algorithm, the controller needs to constantly monitor the whole energy network to check whether there exists network traffic changes. Once traffic changes, the controller records the change and prepare to update routing strategies. It adds a suitable traffic monitoring to avoid unnecessary alteration of severs in data center, which may result in more energy consumption in EI communication. This algorithm introduces a threshold in the amount of network traffic. If the traffic is more than the threshold, all servers in data center connected to the routers will be turned on to enable bidirectional communication between routers and controllers, where routers send information to the controllers, and the controllers transmit decisions to routers. Otherwise, only one server in data center needs to run. Such algorithm can provide an efficient and energy-saving environment in EI communication system.

3.3.2 Energy-Efficient Routing in CR

Various wireless communication technologies have been widely applied into EI communications, resulting in the spectrum scarcity issue. Therefore, CR technologies [151] are applied in EI communication network due to its advantages in efficient spectrum resource allocation [60]. The idea of using CR in different application scenarios has been appeared for many years, such as WSN [152], D2D communications [153], and smart grid [156]. Robert et al. [157] studied the architecture, algorithms, and hardware tested in the application of CR.

Khan et al. [61] presented several ways to integrate CR based communication technology into the EI according to different areas. In the user area, a cognitive energy router acts as a central node to establish links between various devices or terminals in EI, realizing a bi-directional communication [62]. In the grid area, energy consumption data is often transferred from users to the utility center. In this process, cognitive energy router acts as the access point (a central node) to make a single-hop connection with cognitive energy routers in the user area. In a larger geographic area, the cognitive energy router in grid area behaves as a cognitive node to make communication with the control center linked with CR base stations. This method can realize large communication coverage and real-time transmission [63], [64].

Yu et al. [65] proposed an adaptive dynamic programming (ADP) approach to optimize the quality of service (QoS) in EI communication network using the CR technology. Users are assigned with different priorities according to their roles and circumstances in EI communication network. If urgent information needs to be transferred, the corresponding user's priority will be upgraded. Then, the approach schedules spectrum resources and channels to complete data transmission according to users' priorities. The ADP approach can evaluate the transmission delay by studying the users' behaviors and adjust the scheduling mechanism to minimize transmission delay in EI communication network.

3.3.3 Cellular Networks Structure

Existing cellular network topology consists of multiple cells, allowing data flow transmission from cell to cell without interruption [66]. Based on different distributed energy resources, load regions, and management regions, cellular networks structures may formulate, consisting of many sub units for tight cooperation and high-quality communication. Cellular network technology can be employed to enable wide area communication in EI [67].

Kalalas et al. [68] proposed to enhance EI communication using device-to-device (D2D) communications that establish direct transmission links between end-devices in cellular networks. Intelligent device can take advantage of cellular resources and exchange information directly without passing cellular base stations in EI. Status information and control instructions approaching the grid area are able to acquire quicker response. he proposed LTE-D2D technology can be effectively applied in the grid area to manage realtime status of energy devices and acquire detailed pricing information with low latency and high reliability.

Bu et al. [69] designed a system based on Stackelberg game model to cut down operational expense and

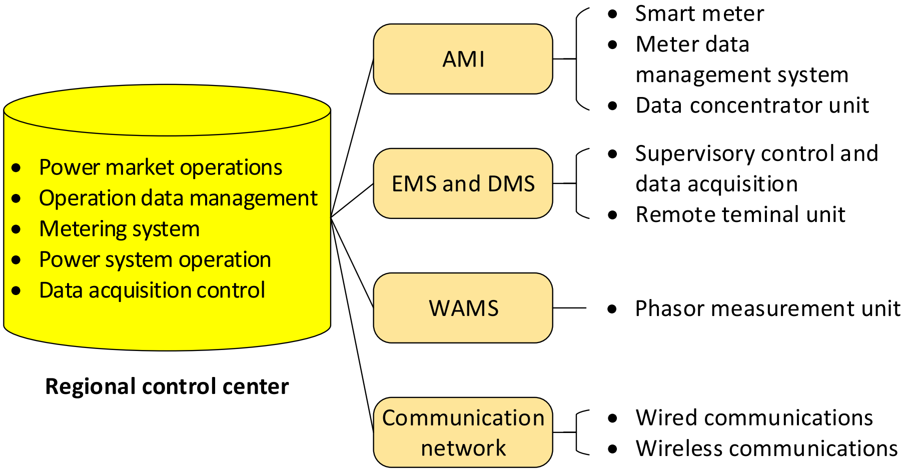


Fig. 11. EI security system.

greenhouse gas emission in green wireless cellular communication. This system contains coordinated multipoint (CoMP) communication, demand-side management (DSM) [155], and the electricity consumption model. CoMP coordinates the active base stations that decide how much electricity retailers can purchase in EI via concerning the pollutant level and the offered price of every retailer. It can also enlarge the coverage of dynamic base stations and guarantee acceptable QoS in cells whose base stations are closed during a low activity time in cellular communication. DSM is introduced to shift the electricity consumption and reflect demand response for users in cellular communication. Multiple DSM programs work together to reduce greenhouse gas emission and minimize the cost for electricity users.

3.4 Solutions to Congestion

Based on the various communication technologies, EI is a widely network and a large amount data will be generated in various loads, requiring the support from the advanced big data technology. EI communication system will face the challenge of congestion problem in data transmission and energy routers. For instance, with the expansion of the real-time monitoring system, a large number of multi-source heterogeneous data is transmitted simultaneously, thus forming huge data streams. Similarly for energy routers, limit capacity cannot be satisfied for the various advanced functions. Therefore, designing the distribution mechanism of EI data according to the requirement of reliability and effectiveness on EI communications is necessary. Wang et al. [158] discussed challenges of big data transmission in EI and discussed the scientific problems of the key technologies to be resolved.

In the designs of energy routers, there is also equipped with information processing module to realize the function of data computing. On the one hand, the received data can be filtered for redundant information. One the other hand, designing efficient information processing architecture is also necessary and the useful information can be sent to the appropriate control unit. In addition, design of information model also deserves some attention, responsible for the orderly and efficient mobility of various kinds of information. Cao et al. [28] provided a diversity scheme of information support layer, including interface diversification, multi-module parallel processing, and optimal selection of information. Through the diversity technology, various communication channels can be cooperative, improving the transmission efficiency and guaranteeing the data quality.

4 Cyber Security Threats and Defense Advances

In this section, we are motivated to investigate the security issues in EI. As the EI system consists of many subsystems, each of which has its specific communication security problems. We will discuss these security issues, mainly from the aspects of security requirements, existing potential solutions and open problems for future studies.

4.1 Overview of EI Security

The EI system consists of some regional control centers, which include data acquisition control, power system operations, power market operations, data management operations and metering systems [9], [91], [154]. It needs collection, transmission, analysis and decision on real-time dynamic information for distributed cooperation and control operations. Therefore, it contains several subsystems, namely advanced metering infrastructure (AMI) system, energy management system (EMS), distribution management system (DMS), wide area measurement system (WAMS) and network communication, as shown in Fig. 11.

4.1.1 AMI in EI

As a key factor in the EI system, AMI reflects the integration of power grids, communications and information infrastructure. AMI mainly consists of several components: smart meter, metering data management system (MDMS) and data concentrator unit (DCU) [92], [93].

- *Smart meter*: Smart meter is an intelligent measuring device which can record energy usage information in detail dynamically and provide consumers for references [94]. Consumers can make some adjustments according to the real-time energy consumption data. Smart meter can effectively improve energy sources utilization which is of great significance in AMI system [95], [96], [97]. However, some

TABLE 5
Solutions of EI Security

Key Technologies	Related Works	Solutions
Informatization	Y. Wang et al. [114]	Set up a information security standard architecture based on existing hierarchical system.
AMI Security	F. Steffen et al. [115]	Improve security algorithms and mechanisms in IEC62353 for AMI.
	B. Lu et al. [116]	Propose a Bloom key agreement mechanism to make security assessment.
	Y. Yu et al. [117], [118], [119]	Connect AMI with ADO, ATO, AAM for detection, location and monitoring.
Energy big data sucurity	F. Ye et al. [123]	Develop ICT framework based on a secure cloud computing, adding identity based encryption scheme.
Defense system	C. Ten et al. [124]	Create a novel anomaly detection model for substations in online network.
	Y. Mo et al. [126]	Summarize an algorithm to defense against replay attacks to ensure stability.

information about energy usage habits, such as energy consumption, the period of the electric appliances usage might be acquired by the unauthorized third parties. The data should be kept on the private devices in AMI system so that the actions of theft, smashing and physical harm could be prevented. The major issue is how to establish a completed protection system to protect the data confidentiality in smart meter. It is also important to update smart meter and record the changes instantly in case of damages in AMI system.

- *MDMS*: MDMS is a core part in AMI system which is responsible for deep processing, storage, and analysis of data. MDMS provides valid addresses for users to retrieve information according to data types [98]. MDMS ensures completeness of information system and accuracy of data flow. It shall be with high fault-tolerance such that the system can still work well even in some extreme circumstances where some EI links or the communication network is down.
- *DCU*: DCU collects the data from smart meter and then transfers them to MDMS. Cyber attacks on DCU have similar impacts to that on the smart meter in AMI system. If DCU is out of control, it will lead to power failure on millions of consumers. As a result, the security of DCU is also a non-ignorable issue [99].

4.1.2 EMS and DMS

EMS mainly includes supervisory control and data acquisition (SCADA), automatic gain control (AGC) and power estimation subsystem. DMS consists of distribution automation system (DAS), geographic information system (GIS), and demand side management (DSM) [100]. SCADA is regarded as a critical part to monitor and control substations in remote which can offer reliable supply and decrease operating expenditure. However, how to ensure the confidentiality and security of the data channels in EMS and DMS is still a problem to be solved.

4.1.3 WAMS

WAMS consists of phasor measurement units (PMUs), acting as real-time key data collector. SCADA cannot accurately make response to the running state of EI system while WAMS does well in real-time data collection and measurements in a wide area [101]. At present, many countries have gradually promoted WAMS to replace conventional SCADA. WAMS can be the basis of early warning analysis, which plays an important role in different kinds of emergencies [102]. Besides, with the capability of real-time information acquisition, it is also beneficial to the work efficiency promotion and consumption minimization [103]. With the development of WAMS, the industry has focused more on the security policy of WAMS to provide protection for substation communication network, wide area information and integrated network in EI system.

4.1.4 Communication Network

EI communication system is a heterogeneous and hybrid infrastructure containing various intelligent devices. EI communication network uses wired and wireless technologies. In wired communication, power line communication is mainly used for less deployment cost [104]. However, it also exists some hidden dangers. For example, PLC can not meet the increasing data rates, and PLC might become unavailable upon power failure. Wireless communication in EI system mainly contains: cellular communication network, cognitive radio network and wireless sensor network [64], [65]. Wireless communication is available during power failure. However, it will result in hack, forgery and destroy, once malicious terminal is connected to EI [105]. Currently, evaluating software and programs, which are designed for a single communication network and standard, faces great challenges in EI communication system. Therefore, it is urgently needed an effective security policy to reduce attacks on communication network.

4.2 Solutions

In this section, we provide several state-of-the-art solutions on EI security issues, as shown in Table 5.

4.2.1 Informatization

One of the notable features of EI is informatization that radically changes the manners of power generation, transmission and consumption in existing power grid. At the same time, EI system is therefore increasingly influenced by computer viruses, logic bombs and Trojan attacks from the Internet. We need to study effective information security in order to increase the system security level after informatization. Many issues should be carefully considered, including security management, security policy and security technology [26]. The significance of EI information security system lies in the full control of the running state of the entire network, requiring superior communication channels and comprehensive terminal acquisition applications. With the construction of EI information security system, it can greatly improve transmission efficiency and optimize resource allocation in the process of information security protection, providing a solid foundation for realizing the informatization of EI.

EI information security includes information acquisition security, transmission security and processing security. In information acquisition process, we often use short-distance wireless communication to protect information security, which provides key management, such as master key, link key and network key, for data encryption. It is mainly used to protect measurement data in EI system. During the transmission process, base station adopts responsive authentication protocols to certificate the identity of mobile users, in order to prevent information leakage caused by unauthorized use of communication resources. In information processing, we need to backup data periodically, so that data integrity and availability could still be guaranteed even when equipments are attacked or damaged.

Currently, in regard to cyber attacks, information integration platform has been built gradually based on the development of informatization technology in EI. At the same time, we have also built standardized management system and unified standards of information security protection system in EI. In addition, security management system and resource planning application system are designed to improve operation and management in EI. Wang et al. [114] set up an information security standard architecture. They argue that the new generation grid system is characterized by informatization, automatization and interactive. They also discussed information security threats and protection demands from different layers containing master station system layer, remote communication network layer, terminal layer and cross layer. Based on the existing hierarchical models and outlines, they carried out a more comprehensive and promising information security standard framework, mainly consisting of business information security standards and general information and communication security standards. It can greatly upgrade security in EI system from various dimensions, such as energy generation, energy transmission, energy distribution, utilization and many other aspects.

4.2.2 AMI Security

As a result of the existing various stakeholders, the interactive and relatively open environment, it is bound to increase the information security risks in AMI system [106], [107]. The international electrotechnical commission (IEC) emphasizes that corresponding solutions to the security risks in AMI system shall be studied [108]. Currently, the academic field, power operators and regulars are all involved in studying the security issues in AMI system, including safety risks analysis and assessment, intrusion detection system applications, and practical security scheme, etc [109], [110].

AMI collects and analyzes real-time electricity price, electricity load demand response and other energy using data. As a result, attacks to AMI system may result in the leakage of consumers' energy using habits and power enterprise management information. It gives chances to malicious users for tampering with energy using data, for industrial espionage to steal competitor's power consumption data to implement the hacker attacks [78]. Thus, it is urgent to prevent the data tampered, power theft and many other malicious attacks to guarantee the integrity, confidentiality and accuracy of smart metering data flow in AMI system.

In AMI, the information security standard IEC 62353 has been designed and improved [115]. This standard states the potential threats and demands for security in AMI system. The proposed security mechanisms mainly contain data encryption technology, digital signature technology, message digest technology, etc.

Lu et al. [116] proposed a Bloom key agreement mechanism, containing a trusted third party (key distribution centre) in AMI system. This mechanism is carried out not only to solve the limitation of computing and storage sources in smart meters, but also to make analysis and assessment on security. They introduced an anti-attack coefficient to examine the security level. Experiments showed that the password system may become invalid under the circumstance that more than 60 percent nodes were breached. Furthermore, they utilized symmetric encryption algorithm and grouping algorithm to protect the integrity and confidentiality of application data. This mechanism can effectively reduce network burden, prevent hacker attacks and avoid leakage of energy using habits, which is vital for both common users and power enterprises in AMI system.

In addition, AMI is also designed to connect to other system modules, such as advanced distribution operation (ADO), advanced transmission operation (ATO), advanced asset management (AAM), to realize tampering detection, fault location, power quality monitoring, demand response to guarantee the security [117], [118], [119].

4.2.3 Energy Big Data Security

With boost growing of data generation, big data has become more and more popular in research community universally. Many emerging and effective big data technologies, as well as the supporting technologies, are proposed and actually applied, such as cloud computing, data clustering, data deep mining, machine learning, stream data processing. It is an innovative and promising idea to utilize big data technologies in EI system. Exploring the power of big data, we can construct an energy big data management in EI system to pursue the goal of efficiency, scalability, economics and harmony. Energy big data intends to exploit universal data from different sources, such as metering data, energy using data, electricity price data, weather forecast data, business data, social media data, government data, health data [111]. The diversity in these data sources implies the huge potential of energy big data. However, at the same time, it may bring potential risks in EI system due to the untrusted or semi-trusted data. In addition, public cloud offers a highly active platform to process and store energy big data, but it is not good to the security and privacy because of its inherent multi-tenancy nature [112]. Thus, we are motivated to take some actions to guarantee a secure energy big data environment.

Big data technology recently has become a emerging research topic. Big data technology covers data acquisition, data processing, data analysis, data interpretation, data transmission, etc. As we have known, it is significant to introduce big data technology into EI system [120]. However, a secure energy big data environment shall always be pursued. To this end, energy big data encryption measures shall be taken into consideration [121], [122].

Ye et al. [123] developed an information and communication technology framework based on a secure cloud computing. It is designed to forecast energy and price which benefit both power generators and personal users to carry out energy generation arrangements or make consumption adjustments in advance. The proposed ICT framework works in private networks, local area networks and public Internet. At the user side, the smart meters monitor real-time energy consumption data from smart devices through local area network, then the metering data are transmitted to the provider side across private networks. At the provider side, as the result of the limited utilization resources and low computing capacity, the local control centers work at pre-processing the raw metering data, and then upload the pre-processing metering data to public cloud control center across public Internet. The public cloud control center has various large volume of data and information sources beneficial for the forecast, including metering data, business data, social network, weather forecast, stock markets forecast, etc. Using cloud computing and big data analytics, more credible energy forecast can be made. However, the public cloud control center may exist security risks due to its inherent untrusted characteristic. To prevent privacy leakage in public cloud control center, a trusted party named the private key generator (PKG) has been introduced. The authors proposed to add identity based encryption (IBE) methodology to the ICT framework for EI security. IBE defines arbitrary identities like IP address as user's public key. The data can be decrypted under the circumstance that the identities matched [120]. Local control center encrypts the pre-processed data into ciphertext, and then transfers to public cloud control center to decrypt by IBE. They also utilized identity based sign-cryption scheme to protect the energy forecast data which was offered to the power generators.

4.2.4 Trusted Active Defense System

Malicious attacks like eavesdropping and jamming often happen in EI system because some untrusted devices or equipments may pass the authentication. Once they have access to the system, they may eavesdrop on packets or signals being sent across EI system. Another type of eavesdropping is masquerading as legitimate nodes, which could receive private information from other legitimate nodes.

To strengthen the physical layer security in EI system, we shall ensure that malicious devices are not able to decode the packets. In addition, we need to study the behavioral pattern of malicious nodes to detect anomaly and eliminate the inside security attack behaviors timely. It is a challenging work and requires the tight cooperation of security monitoring system and real-time analysis system for intrusion detection.

Security monitoring system takes initiative supervision methods to implement monitoring across whole network operation in EI. At the same time, real-time analysis system makes dynamical analysis on the monitoring operational behavior and judges whether exists malicious intrusion. The above steps form a trusted defense system highly needed for security in EI [113].

Facing massive malicious attacks and intrusion, defense system is proposed widely to prevent substations failure, power outage and other electric catastrophes in EI system. Ten et al. [114] created a novel anomaly detection model for substations in existing on-line networks. This model can be applied in multiple substations environment and deal with massive intrusions simultaneously so as to build a powerful EI defense system. The anomaly detection algorithm focused on solving cyber-attacks like Night Dragon [115] greatly related to intelligent energy infrastructure control systems, attempting to investigate the malicious characteristics in temporal events, such as changes of file system, changes in status and setting of target system, and invading intentions. The malicious intrusion footprints were ultimately collected systematically based on temporal incidents in substation networks. In addition, an impact factor was introduced to evaluate how substation failure affects the whole EI system. This model contributes for setting up a new monitoring and defense mechanism for cyber security in EI system.

Mo et al. [116] introduced an algorithm to defense against replay attacks based on the combination of cyber security policies and system-theoretic security policies in EI system. Replay attacks record measurement data sequences and then maliciously repeat the sequences, and often happen in EI system. For instance, Stuxnet employed replay attacks to intrude large number of equipments in Iran nuclear power station and caused massive damages [21]. The proposed defense system based on the summarized algorithm introduces a controller, a detector and an estimator to analyze emergency and detect bad measurement data. It is designed to upgrade efficiency to detect replay attacks and ensure the stability in the circumstances where no attacks happen in EI system.

5 The Standards and Protocols of Energy Internet

In order to realize the vision of EI communications enabled by technologies mentioned above, it is essential that we have a whole set of integrated communications standards and protocols. In EI, many significant functions required the relevant protocols to support them, such as efficient energy transmission, accurate energy measurement, network optimization, and network operation management. In addition, for satisfying the customized demand, supporting the interactive real-time communication protocols is the key for guaranteeing the energy production and load balance. Thus, the standards and protocols of EI should be satisfied the following basic functions: two-way communications, interoperability for advanced energy applications, reliable and secure communications in end-to-end, and the capabilities against the potential cyber-attacks. This section summarizes the existing standards and protocols for constructing EI and then introduces the new standard for EI.

TABLE 6
Overviews on Communication Standards [164]

Standard	Description
EDIXL	Market communication for Germany
IEC TS 62351	data and communication security
ZigBee/HomePlug Smart Energy Profile	Home Area Network (HAN) Device Communications and Information Model
OpenHAN	Home Area Network device communication, measurement, and control
IEC 61850-7-410	Distributed Energy Communication, DMS, DER, EMS
IEEE C37.118	Phasor measurement unit (PMU) communications
IEC 62325	Market communications using common information model
IEC 60870	Communication protocol
IEC 61851	EV-Communication, Smart Home, e-Mobility
IEC 61400-25	Wind Power Communication, EMS, DMS, DER
IEC 60870-6/TASE.2	Inter-control center communications, TASE.2 Inter Control Center Communication, EMS,DMS
IEEE 1547	Physical and electrical interconnections between utility and distributed generation

5.1 Existing Standards and Protocols

- Smart Meters Communications in European: The European Commission released Mandate M/441 EN to development a comprehensive standard for smart meter communication [160]. In addition, the management of the standardization work of M/441 was set by smart meters coordination group. A number of significant standards include various aspects of smart meting. For instances, the interfaces and information content are specified by IEC 61968-9 for the reading and control of smart meters. The grid communication systems are built through CEN TC 294 for remote reading of smart meters.
- E-Energy Program in German: E-Energy Program consists of six model regions in German and identified a set of standards for eight topics. The ICT infrastructure was inserted into German electricity system and a number of existing standards were connected to decentralized energy generation, transport grids, energy quantity measurement and end consumption [161].
- Worldwide Standardization: The IEEE P2030 project focuses on interpretability of energy technology and ICT. There are three tasks: power systems, information systems, and communication systems. IEEE 1701 and IEEE 1702 have been introduced by IEEE Standards Association, creating a multi-source plug and play environment for various devices communications [162], [163].

Besides the standardization mentioned above, several studies are developed for the use of standards. Table 6 summarizes various standards with a short description.

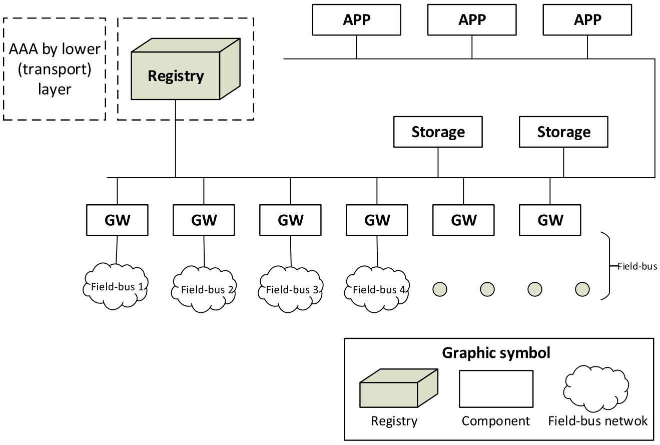


Fig. 12. The architecture of ISO/IEC/IEEE 18880 [141].

5.2 ISO/IEC/IEEE 18880

Already, there are a variety of protocols and standards in the recent power grid. However, each protocol or standard can only accomplish a certain functional side of EI. Therefore, an open extensible data exchange standard is now urgently required. ISO/IEC/IEEE 18880 is developed for this need [165]. The full name of ISO/IEC/IEEE 18880 is ISO/IEC/IEEE 18880-2015 Information technology. Ubiquitous green community control network protocol, which is used as the basic communication architectures and protocols for demand side in EI. It is developed for the effective solutions of consistency problem of terminal access, and the loose coupling and hierarchy of data acquisition, data access, data transmission, data storage, and data analysis. The connection among billions of meters and network can be implemented, while mass data produced by these equipment can be standardized.

ISO/IEC/IEEE 18880 uses standardized communication interfaces, data formats, and communication protocols to support remote information transmission in the wide area network based on TCP/IP. The various existing non-IP network is compatible through multi-protocol gateway and the scale of applications and deployments are guaranteed by the integration of heterogeneous networks [166].

ISO/IEC/IEEE 1880 defines the following entities: gateway, storage, application service element, and registrar, as shown in Fig. 12. One of the main goals of this standards is to achieve inter-operability between different network components. Hence, the gateway, storage, and application unit are abstracted as component, which has the same interface. To be specific, registrar is responsible for the management information query (similar to DNS). Gateway is responsible for the data acquisition. Storage is responsible for data storage, also named as real-time database and application is responsible for completing various end user applications.

Moreover, ISO/IEC/IEEE 1880 also defines two kinds of communication protocols, including the communication protocols between components and the communication protocols between component and registrar. The communication protocol of ISO/IEC/IEEE 1880 belongs to the application layer in the OSI protocol, thus many LAN technologies can be supported, such as Powerline, WiMAX, Bluetooth, UWB, 3G/4G/LTE, 802.11. As a result,

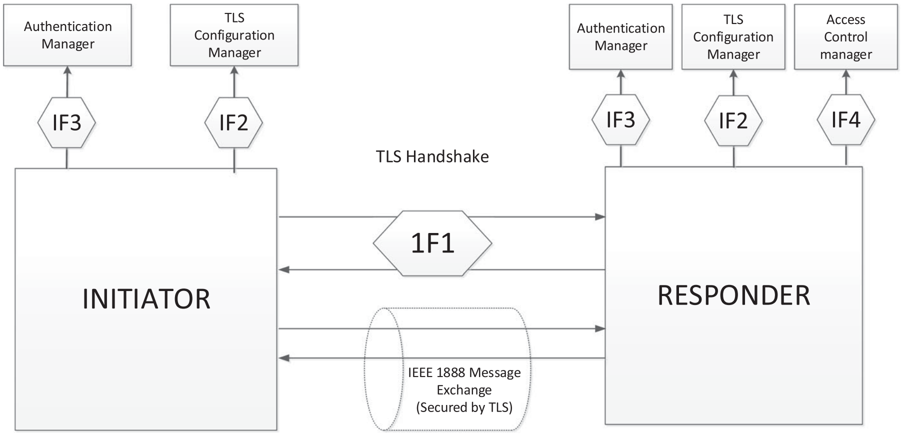


Fig. 13. Safety interface of ISO/IEC/IEEE 18883 [141].

ISO/IEC/IEEE 1880 focuses on the data transmission in EI, neglecting the security of data transmission.

Considering the limitations of ISO/IEC/IEEE 1880, ISO/IEC/IEEE 1881 [167] and ISO/IEC/IEEE 1883 [168] are developed for complement in the areas of network management and network security.

6 Challenges and Future Work

In this section, we present open challenges in the EI communications, from the aspects of complexity, efficiency, reliability, and security, which are summarized in Fig. 14.

6.1 Complexity

Power system is a complex physical system which consists of the real-time generation, transmission, distribution, and consumption of electrical power. The energy flow is characterized with many complex physical properties, such as high dimension, nonlinear, time-invariance, and multiple coupling. The communication systems consist of a large amount of packets and the optimization of communication networks remains to be a tough issue. Combing these two systems, the researches on reliability and safety will become more complex. Luo et al. [70] proposed a distributed EI communication system called systems of system (SoS), consisting of a group of large-scale, complex and concurrent communication systems, in which each member has unique ability and shoulders different missions. They can manage themselves and run independently, as well as change their characteristics under different circumstances. Prince et al. [71] proposed a distributed computer control system (DCCS) for distributed EI communication. It can control communication devices, monitor their performance and change their configurations. Due to its inherent complexity, Various challenges in modeling, analyzing and designing an efficient communication infrastructure need to be addressed.

- A new grid interface is needed to allow plug and play of energy supply and demand, anywhere and anytime.
- A communication infrastructure needs to be built that allows the real time management of energy supply and demand though distributed grid intelligence software [72], [73].
- Local grids can be completely isolated from the main grid and continue to operate autonomously based on renewable energy.
- Stable power supply needs to be provided and improve energy efficiency of the system, which requires a real-time information and communication system that can detect events like power failure in the EI system [74], [75].

6.2 Efficiency

Modern communication and information technology is proposed to construct a communication infrastructure that provides coordinated monitoring and controlling functions in EI system. Such a communication infrastructure needs to provide instant and efficient bidirectional communication among distributed renewable energy sources, energy storage devices, and individual energy loads. It requires quick responses to energy demands and efficient data processing ability. EI needs to collect and analyze all kinds of real time data, including static data, graphic interaction data, and business information integrated data, so as to improve the efficiency. The challenges are as follows:

1) *Optimization of Energy Scheduling*. Building an efficient network for resource optimal allocation is the key content in the EI communication. Miao et al. [76] addressed that complicated tradeoffs exist between every user's performance and the entire energy network as the result of limited communication resources. For example, various electrical components, domestic appliances, and radio systems all work in the 2.4 GHz band at the same time. They proposed a flexible cross-layer optimization methodology for energy savings, which considers time, frequency and circuit resources in energy scheduling. Pedrasa et al. [77] created a decision-support tool to optimize electrical energy service and schedule distributed energy resources for the maximization of net benefits. In this tool, improved particle swarm optimization(PSO) algorithm is used due to its capability to perform near-optimal schedules during controllable computation times.

In addition, both traditional communication networks and EI have to be confronted the network congestion problem. In EI, due to the congestion issue, the transmission efficiency of both information flow and energy flow will

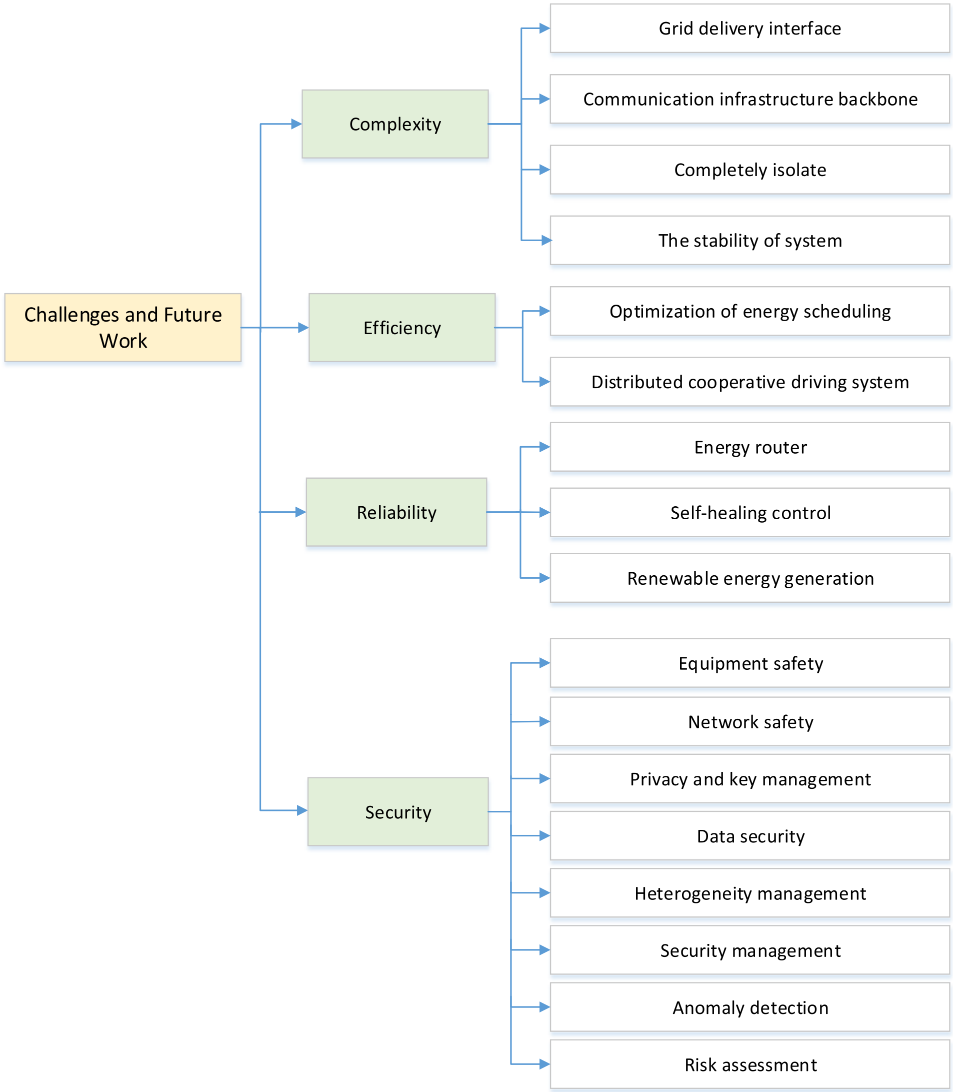


Fig. 14. Challenges of EI communication.

dropped sharply. Lin et al. [140] studied routing strategy in EI considering both energy transmission congestion and energy load balancing. However, this research is based on an ideal routing model of EI. The differences between individual energy routers cannot be completely ignored, resulting in increasing the complexity of this issue.

2) *Distributed Cooperative Driving System*. As the popularity of electric vehicles, new communication technologies emerge to handle challenges of distributed cooperative driving system. The Chalmers team [78] in the 2011 Grand Cooperative Driving Challenge (GCDC) developed a cooperative driving system integrated into a Volvo S60 for low-cost and efficient communication infrastructures. Kianfar et al. [79] investigated the proposed cooperative driving system in GCDC and provided simulation and experimental results. The proposed cooperative driving system gathered required measurements mainly from local built-in sensors, added external sensors and the communication node. The system's output information are often transferred to vehicle's low-level controller, communication node and human-machine interface. The system can enable real-time interaction between the vehicle and the external hardware modules as well as fuse information from different sensors for estimation of state parameters. Xu et al. [80] designed a flocking method based cooperative driving system for automomous electric vehicles, which takes driving constraints and dynamic features into consideration. Partially-linear kinematic model is applied in the proposed system for reducing the computational burden and enhancing control performance.

6.3 Reliability

In EI system, energy router, renewable energy resources, and self-healing control system should work in collaboration to improve the reliability. We might encounter many reliability challenges in EI system's construction and operation.

6.3.1 Reliability of Energy Routers

Energy router undertakes vital functions of energy dispatching and exchange to enforce the reliability in EI communication. Cao et al. [81] proposed an energy router as the core equipment in EI communication system that manages

TABLE 7
The Security Threats to EI System

Security threats	Examples	Results
Natural threats (like thunderstruck, snowstorm, windstorm, etc.)	Thunderstruck Snowstorm Windstorm	1. Causing electromagnetic interference. 2. Affecting the accuracy of information. 3. Damaging the EI, etc.
Man-made threats	Integrity damage Non-infringement Computer virus Communication outage Monitor Tampering Camouflage intrusion	1. Causing device misoperating, system parameter error, etc. 2. Damaging the integrity,Communication outage privacy, reliability of the information. 3. Affecting safe and stable operation. 4. Bringing economic losses, etc.

energy and information to satisfy the requirements of the system operation, which is similar to the router behaves in the Internet. Sanchez-Squella et al. [82] presented an energy router design that dynamically manages energy flows. The energy router should guarantee the quality of energy flow to satisfy demands, as well as ensure that energy flows are routed to the load properly. Furthermore, the energy router needs to monitor the quality of the energy flow in real-time, and make automatic adjustments safely and accurately to construct a reliable communication infrastructure.

6.3.2 Self-Healing Control

Since EI contains various resources and information, we need an intelligent and autonomous system to manage critical processes and assist people with their busy tasks. The next generation self-healing control system shall be taken into consideration because it can restore the system and return back to normal state instantly when facing power failure in EI communication [83], [84]. Jia et al. [85] studied the structure of self-healing control in EI system, consisting of base layer, support layer and application layer. They also defined normal mode, warning mode, critical mode, emergency mode and recovery mode in energy network operation according to self-healing capabilities. Zidan et al. [86] proposed a cooperative multiagent framework to apply in the self-healing control in EI, which is designed to detect failures and perform switching operations for the restoration of abnormal loads. Gao et al. [87] investigated the basic theory to support self-healing control of EI system, as well as discussed critical technologies including self-healing control process, device monitoring and network optimized reconstruction.

6.3.3 Renewable Energy Generation

EI generation equipment includes traditional energy generation and renewable energy generation. Yu et al. [88] stated that renewable energy generation are in great need, including wind power, hydroelectric power, solar thermal power, biomass power, tidal power generation, etc. By comparison, hydropower and biomass power are relatively more developed, while wind power, solar power, solar thermal power, geothermal and tidal power still have many problems to be solved. We mainly discuss the challenges in wind power generation and solar photovoltaic.

Wind power has the most large-scale commercial development prospects. When using wind power, we have to transform wind energy into electrical energy that means the output power is determined by the wind. Georgilakis et al. [89] discussed technical challenges in wind power, including the wind power impacts on system's operating expenditure, system dynamics, energy flow quality, energy imbalances, and transmission planning.

As people raise the awareness of renewable energy and solar photovoltaic systems, solar power technology prospects can be very broad. Solar photovoltaic technology uses semiconductor materials directly to convert solar energy into electricity in order to improve efficiency. Singh et al. [90] gave a comprehensive overview in the development the solar power generation and further highlighted the potential challenges in the power generation quality and reliable applications. They addressed that the cost of photovoltaic power has not been reduced to an economic level, and it required further improvement.

6.4 Security

Threats in EI can also be divided into two main categories: natural threats and man-made threats, as shown in Table 7. By analogously analyzing smart grid and EI, the challenges will be encountered in the following aspects, i.e., equipment safety, network security, privacy and key management, data security, heterogeneity management, security management, anomaly detection, and risk assessment.

6.4.1 Equipment Safety

In EI communication system, intelligent devices are utilized to replace human beings to do some complex and dangerous jobs. If they are deployed in the unmanned monitoring environment, information can easily be stolen and tampered by attackers. At the same time, due to the technology imperfection in new equipment, there also exists problems which may result in instability on the normal operations in EI communication system. The operating system adopted by EI communication system has undesirable natures such as false logic design, system vulnerabilities or programming errors [127]. When this operating system connects to the Internet, deliberate illegal attackers will be able to pass through these defects, bugs or errors to implant viruses that may steal the important energy using data, or even control and damage the whole EI communication system. Access to the control operation often stems from computer platform, USB disks, mobile hard disks, etc. As long as the information carriers have infectious virus, the hackers can launch malicious attacks on the whole EI communication system. Therefore, A more robust EI security defense system needs to be built to ensure the power equipment safety in EI communication system.

6.4.2 Network Security

Due to various types of EI users and the widespread of application scopes, energy network is at high risks in a sense. Main threats [128] come from eavesdropping, invasion, side channel attacks and denial of service (DoS) attacks. In EI communication, illegal users may go into the Internet information system and attack password system, leading to the leakage of customers' privacy. The behavior of intercepting the transmission of information in network will result in the chaos of the EI communication system. By delaying, blocking or destroying the transmission and exchanging of information between nodes in network, the malicious users can cause congestion to the EI system. What's worse, it will lead to the network collapse [129], [130]. During different research areas including the Internet, wireless networks, and sensor networks, many work has been investigated to deal with networking security issues. An effective solution is to design the security standards, such as the security capabilities in 802.11i, 802.16e, and 3GPP LTE to protect the routing security in wireless networks [142], the advanced encryption standard to protect the sensor data in sensor networks [143]. However, these solutions can only handle the security issues in a single side. ISO/IEC18883 named IEEE Standard for Ubiquitous Green Community Control Network: Security aims to deal with the networking security in several aspects: data transmission security, identity authentication, and some permissions problems.

6.4.3 Privacy and Key Management

Fraud cases always exist, especially in the case of different consumption energy sites (e.g., plug in hybrid electric vehicle (PHEV)). One example was analyzed in the national institute of standards and technology (NIST) report [131]. When both the landlord and the tenant have PHEVs, they should be charged separately. To protect the privacy of the tenant, communication between smart electric meter and the PHEV need be via a secure attachment, i.e., energy services communication interface. This interface is provided by the utility company. Smart electric meter cannot allow any third party to misuse or modify the collected using data. Utilizing key management for access permission is another good choice. Without the corresponding keys, it is impossible for unauthorized landlord to access and modify using data from the tenant.

6.4.4 Data Security

Data security includes the safety itself and the protective security. There is no standardized access permission mechanism and rigorous certification measures in EI communication system. Therefore, it is easy to cause confusion, private information leakage and data access mechanism modification. Besides, the lack of powerful intelligent data storage center and data backup measures can result in the data management chaos and data recovering failure in EI communication system after a disaster, etc [132], [133].

The innovation of EI communication technology is to integrate the information network into the traditional power grid. EI extends to every power supplier and every household. Therefore, EI access channels are varied, including user homes, buildings, residential space, wireless communication, etc. Each access channel exists potential attacking threats. The attacker may intercept data or illegal tampering in any position. In addition, the information network extension also makes network isolation becomes very difficult. This may bring a large number of illegal accesses and unauthorized external connections and cause more data security issues in EI communication system.

6.4.5 Heterogeneity Management

EI is a distributed network system, which has a large number of connected devices. It is impossible to implement both information and energy sharing via a unified platform and model [134]. In heterogeneous EI communication system, security for interoperability between different smart devices or systems is necessary.

Each part of EI communication system has its own communication technologies in order to satisfy the specific communication requirements. It is a huge challenge to make multiple heterogeneous communication technologies and standards coexist in every part. For example, 4G/5G heterogeneous systems which can be used in EI communication have the characteristics of complex network topology. Inevitably, various interference problems may occur between the protocols in EI system, and the systematic operation is more vulnerable to be attacked. In order to strengthen the EI system to avoid potential security risks, how to select the suitable information communication methodology that matches energy and information transfer requirements is still a emerging research. ISO/IEC18883 is designed based on three principles: the utilization of mature security solutions, the separation of certificate management and authorization management, the compatibility of ISO/IEC18880 architecture. In addition, the ISO/IEC18883 has also defined the function of secure communication interface, as shown in Fig. 13.

6.4.6 Security Management

The objects security management contains reasonable communication spectrum utilization, handling transaction request, providing auxiliary safety functions testing in EI communication system. How to deal with large numbers of intelligent devices and set up reliable and healthy cooperation between them bring challenges to the monitoring and maintenance for objects' security management in EI system. In addition, human beings have been actively involved in EI communication system as well. The goal of human beings security management is to monitor people's unsafe manners against illegal operations. However, how to better manage and control human beings' unrational behaviours for security can be a great challenge in EI communication. A more advanced safety management system targeting at both objects and human beings shall be constructed.

6.4.7 Anomaly Detection

In the traditional power grid, information and energy is delivered to users in a one-way manner, and there is no interaction between power grid and users. Since information networks adopt special communication technologies with strict physical isolation with external networks, security risks are mainly from the internal network and terminals, such as the spread of virus, abuse of terminal resources, unauthorized accesses, information leakage, and vandalism. However, in EI system, a digital network with two-way communication is enabled between the grid and the user, so that they are apt to be attacked since they are directly exposed to malicious users. Recently, many researches have studied anomaly detection in EI communication system. Chen et al. [135] found that traditional optical fiber wiretapping detection method based on exploration of light power changes is difficult to prevent eavesdropping effectively. They studied different approaches of optical fiber hacking and investigated a novel optical fiber eavesdropping detection technology to monitor real-time network operations and build fast recovery strategy. Ten et al. [136] designed an anomaly detection model to collect malicious intrusion footprints on-line at the same time for multiple substations, which is often employed in large-scale intrusions environment. Mo et al. [137] used an algorithm based on system-theoretic security strategies to investigate emergency and detect bad measurement data in order to deal with replay attacks in EI system. Wang et al. [138] developed a deep data fusion model to deal with the risk perception issues. Particularly, a machine learning method based on kernel principal components analysis (PCA) is proposed to explore possible risks from high-dimensional data space in EI communication system.

6.4.8 Risk Assessment

The security threats at the user side becomes more and more prominent, as the network boundary of EI communication system extends to the user side. Various types of business terminals are deployed in the unattended environment, resulting in high possibility of violent intrusion, information leakage, unauthorized access and illegal control. Thus, risk assessment shall be taken into consideration. Zhao et al. [139] presented an overall risk assessment framework in energy networks, including financial risk assessment and engineering risk assessment, especially under the circumstance of large-scale renewable power generation. Risk assessment, as an indispensable analytical method, should be paid more attention to at the early stage of EI construction. First, for the power generation, we need to collect the operation state of the equipment and release the risk information to help maintain the equipment. Then, the transmission network should establish a comprehensive risk assessment system based on a secure architecture to improve the automation level and enhance the ability to deal with the faults. Moreover, such assessment system shall interact with users actively, aiming at collecting the information and issuing risk warnings to users.

7 Conclusion

EI is a next generation grid formed by communication system, power generation system, intelligent system, and many green components. Among them, communication system plays a critical role for effective and real-time energy management between interconnected equipment and systems in EI. In this paper, we provide a complete overview of EI communication system. We present the motivations and communication infrastructure for EI. Energy routers, energy storage devices, distributed renewable energy sources, and the loads are all actively involved in the communication network. In the EI communication system, we regard energy router as a critical central coordinator to implement renewable energy sharing and achieve real-time balance between supplies and demands, differing from the communication in traditional power grid and SG. Then, we divide EI communication system into energy routers, information subsystem, and network subsystem. We investigate potential technologies to support in energy router, information sensing and processing, and network operations. In addition, recent standardizations and some existing potential security solutions based on the proposed requirements are discussed. Finally, various challenges in both system design and operations are paid active attention for constructing a more healthy EI communication architecture.

Acknowledgments

This work is supported by NSFC (61572262, 61533010, 61373135, 61571233, 61532013); National China 973 Project (2015CB352401); the NSF of Jiangsu Province (BK20141427); The Qinlan Project of Jiangsu Province; China Postdoctoral Science Foundation.

References

[1] K. Zhou, S. Yang, C. Shen, S. Ding, and C. Sun, “Energy conservation and emission reduction of China’s electric power industry,” *Renewable Sustainable Energy Rev.*, vol. 45, pp. 10–19, May 2015.

[2] Q. Zhang, K. He, and H. Huo, “Policy: Cleaning China’s air,” *Nature*, vol. 484, pp. 161–162, Apr. 2012.

[3] T. Hammons, “Impact of electric power generation on green house gas emissions in Europe: Russia, Greece, Italy and views of the EU power plant supply industry-a critical analysis,” *Int. J. Electric Power Energy Syst.*, vol. 28, no. 8, pp. 548–564, Oct. 2006.

[4] Q. Hu, Y. Qian, H. Chen, and H. Mouftah, “Cyber security for smart grid communications: Part I,” *IEEE J. Mag.*, vol. 50, no. 8, pp. 16–17, Aug. 2012.

[5] Q. Hu, Y. Qian, H. Chen, and H. Mouftah, “Cyber security for smart grid communications: Part II,” *IEEE J. Mag.*, vol. 51, no. 1, pp. 16–17, Jan. 2013.

[6] K. Wang, Z. Ouyang, R. Krishnan, L. Shu, and L. He, “A game theory based energy management system using price elasticity for smart grids,” *IEEE Trans. Ind. Inform.*, vol. 11, no. 6, pp. 1607–1616, Dec. 2015.

[7] L. Tsoukalas and R. Gao, “From smart grids to an energy internet: Assumptions, architectures and requirements,” in *Proc. 3rd Int. Conf. Electric Utility Deregulation Restruct. Power Technol.*, Apr. 2008, pp. 94–98.

[8] A. Huang, “FREEDM system-A vision for the future grid,” in *Proc. IEEE PES General Meeting*, Jul. 2010, pp. 1–4.

[9] H. Appelrath, O. Terzidis, and C. Weinhardt, “Internet of energy-ICT as a key technology for the energy system of the future,” *Bus. Inf. Syst. Eng.*, vol. 4, no. 1, pp. 1–2, Feb. 2012.

[10] R. Abe, H. Taoka, and D. McQuilkin, “Digital grid: Communicative electrical grids of the future,” *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 399–410, Jun. 2011.

[11] Y. Xu, J. Zhang, W. Wang, A. Juneja, and S. Bhattacharya, “Energy router: Architectures and functionalities toward energy internet,” in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2011, pp. 31–36.

[12] M. Geidl, G. Koeppel, P. Favre-Perrod, B. Klöckl, G. Andersson, and K. Fröhlich, "Energy hubs for the futures," *IEEE Power Energy Mag.*, vol. 5, no. 1, pp. 24–30, Jan./Feb. 2007.

[13] H. Guo, F. Wang, J. Luo, and L. Zhang, "Review of energy routers applied for the energy internet integrating renewable energy," in *Proc. IEEE 8th Int. Power Electron. Motion Control Conf.*, May 2016, pp. 1997–2003.

[14] X. Deng, "Japan digital power grid project," *World Sci.*, no. 7, pp. 8–9, 2013.

[15] Q. Zhang, Y. Sun, and Z. Cui, "Application and analysis of ZigBee technology for smart grid," in *Proc. Int. Conf. Comput. Inf. Appl.*, Dec. 2010, pp. 171–174.

[16] F. Aalamifar and L. Lampe, "Optimized WiMAX profile configuration for smart grid communications," *IEEE Trans. Smart Grid*, vol. PP, no. PP, pp. 1–10, Mar. 2016.

[17] R. Yu, C. Zhang, X. Zhang, L. Zhou, and K. Yang, "Hybrid spectrum access in cognitive-radio-based smart-grid communications systems," *IEEE Syst. J.*, vol. 8, no. 2, pp. 577–587, Jun. 2014.

[18] Y. Xu and C. Fischione, "Real-time scheduling in LTE for smart grids," in *Proc. 5th Int. Symp. Commun. Control Signal Process.*, May 2012, pp. 1–6.

[19] A. Aydeger, K. Akkaya, and A. Uluagac, "SDN-based resilience for smart grid communications," in *Proc. IEEE Conf. Netw. Function Virtualization Softw. Defined Netw.*, Nov. 2015, pp. 31–33.

[20] X. Zhang, K. Wei, L. Guo, W. Hou, and J. Wu, "SDN-based resilience solutions for smart grids," in *Proc. Int. Conf. Softw. Netw.*, May 2016, pp. 1–5.

[21] P. Favre-Perrod, "A vision of future energy networks," in *Proc. IEEE Power Eng. Soc. Inaugural Conf. Expo.*, Jul. 2005, pp. 13–17.

[22] Stuxnet renews power grid security concerns. (2010). [Online]. Available: http://www.computerworld.com/article/2519574/security0/stuxnet-renews-power-grid-security-concerns.html

[23] Electricity Grid in U.S. penetrated by spies. (2009). [Online]. Available: http://www.wsj.com/articles/SB123914805204099085

[24] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on smart grid communication infrastructures: Motivations, requirements and challenges," *IEEE Commun. Surveys Tut.*, vol. 15, no. 1, pp. 5–20, Jan.–Mar. 2013.

[25] V. Güngör, et al., "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Inform.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[26] Z. Fan, et al., "Smart grid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 21–38, Jan.–Mar. 2013.

[27] J. Wang, K. Meng, J. Cao, Z. Cheng, L. Gao, and C. Lin, "Information technology for energy internet: A survey," *J. Comput. Res. Develop.*, vol. 52, no. 5, pp. 1109–1126, May 2015.

[28] J. Cao, et al., "An energy internet and energy routers," *Scientia Sinica Informationis*, vol. 44, no. 6, pp. 714–727, Jun. 2014.

[29] J. Wang, et al., "Review on information and communication key technologies of energy internet," *Smart Grid*, vol. 3, no. 6, pp. 473–485, 2015.

[30] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid-the new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, Oct.–Dec. 2012.

[31] M. Erol-Kantarci and H. Mouftah, "Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 179–197, Jan.–Mar. 2015.

[32] S. Bera, S. Misra, and J. Rodrigues, "Cloud computing applications for smart grid: A survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1477–1494, May 2015.

[33] S. Gupta, T. Mukherjee, G. Varsamopoulos, and A. Banerjee, "Research directions in energy-sustainable cyber-physical systems," *Sustainable Comput. Inform. Syst.*, vol. 1, no. 1, pp. 57–74, Mar. 2011.

[34] W. Su and A. Huang, "The energy internet and electricity market in the United States," *Chin. Sci. Bulletin*, vol. 61, no. 11, pp. 1210–1221, 2016.

[35] L. Chen, Q. Sun, L. Zhao, and Q. Cheng, "Design of a novel energy router and it's application in energy internet," in *Proc. Chin. Autom. Congr.*, Nov. 2015, pp. 1462–1467.

[36] F. Wu, P. Varaiya, and R. Hui, "Smart grids with intelligent periphery: An architecture for the energy internet," *Eng.*, vol. 1, no. 4, pp. 436–446, Dec. 2015.

[37] R. Davies, "Hydro ones smart meter initiative paves way for defining the smart grid of the future," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2009, pp. 1–2.

[38] Q. Huang, M. Crow, G. Heydt, J. Zheng, and S. Dale, "The future renewable electric energy delivery and management (FREEDM) system: The energy internet," *Proc. IEEE*, vol. 99, no. 1, pp. 133–148, Jan. 2011.

[39] M. Schulze, L. Friedrich, and M. Gautschi, "Modeling and optimization of renewables: Applying the energy hub approach," in *Proc. Int. Conf. Sustainable Energy Technol.*, Nov. 2008, pp. 83–88.

[40] P. Favre-Perrod, "A vision of future energy networks," in *Proc. IEEE Power Eng. Soc. Inaugural Conf. Expo.*, Jul. 2005, pp. 13–17.

[41] M. Geidl, G. Koeppel, P. Favre-Perrod, B. Klockl, G. Andersson, and K. Frohlich, "The energy hub-a powerful concept for future energy systems," in *Proc. 3rd Annu. Carnegie Mellon Conf. Elect. Ind.*, Mar. 2007, pp. 13–14.

[42] H. Wu, J. Zhang, and Y. Xing, "A family of multiport buck-boost converters based on DC-link-inductors (DLIs)," *IEEE Trans. Power Electron.*, vol. 30, no. 2, pp. 735–746, Feb. 2015.

[43] M. Schwartz, "History of communications-carrier-wave telephony over power lines: Early history," *IEEE Commun. Mag.*, vol. 47, no. 1, pp. 14–18, Jan. 2009.

[44] X. Cheng, R. Cao, and L. Yang, "Relay-aided amplify-and-forward powerline communications," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 265–272, Mar. 2013.

[45] T. Takuno, M. Koyama, and T. Hikihara, "In-home power distribution systems by circuit switching and power packet dispatching," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 427–430.

[46] P. Nguyen, W. Kling, and P. Ribeiro, "Smart power router: A flexible agent-based converter interface in active distribution networks," *IEEE Trans. Smart Grid*, vol. 2, no. 3, pp. 487–495, Sep. 2011.

[47] Y. Deng, G. Venayagamoorthy, and R. Harley, "Optimal allocation of power routers in a STATCOM-installed electric grid with high penetration of wind energy," in *Proc. Clemson Univ. Power Syst. Conf.*, Mar. 2015, pp. 1–6.

[48] Y. Zhang, J. Umuhoza, Y. Liu, C. Farnell, H. Mantooth, and R. Dougal, "Optimized control of isolated residential power router for photovoltaic applications," in *Proc. IEEE Energy Convers. Congr. Expo.*, Sep. 2014, pp. 53–59.

[49] P. Yi, T. Zhu, B. Jiang, R. Jin, and B. Wang, "Deploying energy routers in an energy internet based on electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 4714–4725, Jun. 2016.

[50] D. Rech and A. Harth, "Towards a decentralised hierarchical architecture for smart grids," in *Proc. Joint EDBT/ICDT Workshops*, 2012, pp. 111–115.

[51] Y. Ji, Q. Ai, and D. Xie, "Research on co-development trend of distributed generation and smart grid," *Power Syst. Technol.*, vol. 34, no. 12, pp. 1000–3673, 2010.

[52] T. Zhu, Z. Huang, A. Sharma, and J. Su, "Sharing renewable energy in smart microgrids," in *Proc. ACM/IEEE 4th Int. Conf. Cyber-Phys. Syst.*, 2013, pp. 219–228.

[53] J. Solanki, S. Khushalani, and N. Schulz, "A multi-agent solution to distribution systems restoration," *IEEE Trans. Power Syst.*, vol. 22, no. 3, pp. 1026–1034, Aug. 2007.

[54] Z. Liu and M. Wang, "The application of summingbird cloud computing platform in energy internet," *Comput. Sci. Appl.*, vol. 5, no. 12, pp. 464–471, Dec. 2015.

[55] O. Boykin, S. Ritchie, I. O'Connell, and J. Lin, "Summingbird: A framework for integrating batch and online MapReduce computations," in *Proc. VLDB Endowment*, vol. 7, no. 13, pp. 1441–1451, Aug. 2014.

[56] B. Li, L. Kong, W. Cao, Z. Yang, and L. We, "A novel wireless distribution network application to support further internet of energy," in *Proc. 11th Int. Conf. Wireless Commun. Netw. Mobile Comput.*, Sep. 2015, pp. 1–6.

[57] G. Zhang, L. Su, and Y. Wang, "Research on communication network architecture of energy internet based on SDN," in *Proc. IEEE Workshop Adv. Res. Technol. Ind. Appl.*, Sep. 2014, pp. 316–319.

[58] M. Celenlioglu, S. Goger, and H. Mantar, "An SDN-based energy-aware routing model for intra-domain networks software," in *Proc. 22nd Int. Conf. Telecommun. Comput. Netw.*, Sep. 2014, pp. 61–66.

[59] M. Vuppuluri, N. Sunder, M. Hegde, and K. Sreelakshmi, "SDN based solutions for energy efficient networks," in *Proc. 1st Int. Conf. Next Generation Comput. Technol.*, Sep. 2015, pp. 143–148.

[60] A. Cacciapuoti, M. Caleffi, F. Marino, and L. Paura, "Sensing-time optimization in cognitive radio enabling smart grid," in *Proc. Euro Med Telco Conf.*, Nov. 2014, pp. 1–6.

[61] A. Khan, A. Ali, M. Rehmani, and M. Reisslein, "Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 860–898, Jan.-Mar. 2016.

[62] Vineeta and J. Thathagar, "Cognitive radio communication architecture in smart grid reconfigurability," in *Proc. Int. Conf. Emerging Technol. Trends Electron. Commun. Netw.*, Dec. 2012, pp. 1–6.

[63] F. Liu, J. Wang, Y. Han, and P. Han, "Cognitive radio networks for smart grid communications," in *Proc. Asian Control Conf.*, Jun. 2013, pp. 1–5.

[64] V. Kouhdaragh, D. Tarchi, A. Coralli, and G. Corazza, "Cognitive radio based smart grid networks," in *Proc. Tyrrhenian Int. Workshop Digit. Commun.-Green ICT*, Sep. 2013, pp. 1–6.

[65] R. Yu, W. Zhong, S. Xie, and Y. Zhang, "QoS differential scheduling in cognitive-radio-based smart grid networks: An adaptive dynamic programming approach," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 2, pp. 435–443, Feb. 2016.

[66] K. Wang, et al., "Wireless big data computing in smart grid," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 58–64, Apr. 2017.

[67] V. Gungor, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Inform.*, vol. 7, no. 4, pp. 529–539, Nov. 2011.

[68] C. Kalalas, L. Thrybom, and J. Alonso-Zarate, "Cellular communications for smart grid neighborhood area networks: A survey," *IEEE Access*, vol. 4, pp. 1469–1493, 2016.

[69] S. Bu, F. Yu, Y. Cai, and X. Liu, "When the smart grid meets energy-efficient communications: Green wireless cellular networks powered by the smart grid," *IEEE Trans. Wireless Commun.*, vol. 11, no. 8, pp. 3014–3024, Aug. 2012.

[70] Y. Luo, Y. Wang, A. Wang, L. Shi, and G. Tu, "A conceptual layered cooperative system of system model for smart grid," *Autom. Electric Power Syst.*, vol. 33, no. 17, pp. 1–5, 2009.

[71] S. Prince and M. Sloman, "Communication requirements of a distributed computer control system," *IEEE Proc.-Comput. Digit. Techn.*, vol. 128, no. 1, pp. 21–34, Jan. 1989.

[72] S. Woodruff, "Complexity in power systems and consequences for real-time computing," in *Proc. IEEE PES Power Syst. Conf. Expo.*, Oct. 2004, pp. 10–13.

[73] R. Rios-Zalapa, X. Wang, J. Wan, and K. Cheung, "Robust dispatch to manage uncertainty in real time electricity markets," in *Proc. Innovative Smart Grid Technol.*, Jan. 2010, pp. 1–5.

[74] A. Abdel-Khalik, A. Elserougi, A. Massoud, and S. Ahmed, "Fault current contribution of medium voltage inverter and doubly-fed induction-machine-based flywheel energy storage system," *IEEE Trans. Sustainable Energy*, vol. 4, no. 1, pp. 58–67, Jan. 2013.

[75] Q. Sun, Y. Zhang, H. He, D. Ma, and H. Zhang, "A novel energy function-based stability evaluation and nonlinear control approach for energy internet," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1195–1210, May 2015.

[76] G. Miao, N. Himayat, Y. Li, and A. Swami, "Cross-layer optimization for energy-efficient wireless communications: A survey," *Wireless Commun. Mobile Comput.*, vol. 9, no. 4, pp. 529–542, Apr. 2009.

[77] M. Pedrasa, T. Spooner, and I. MacGill, "Coordinated scheduling of residential distributed energy resources to optimize smart home energy services," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 134–143, Sep. 2010.

[78] Grand Cooperative Driving Challenge (GCDC). (2011). [Online]. Available: http://www.gcdc.net/

[79] R. Kianfar, et al., "Design and experimental validation of a cooperative driving system in the grand cooperative driving challenge," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 994–1007, Sep. 2012.

[80] L. Xu, G. Yin, and N. Zhang, "Flocking cooperative driving control of four-wheel independently driving electric autonomous vehicles considering vehicular dynamic processes," in *Proc. 35th Chin. Control Conf.*, Jul. 2016, pp. 4487–4492.

[81] J. Cao and M. Yang, "Energy internet-towards smart grid 2.0," in *Proc. 4th Int. Conf. Netw. Distrib. Comput.*, Dec. 2013, pp. 105–110.

[82] A. Sanchez-Squella, R. Ortega, R. Grino, and S. Malo, "Dynamic energy router," *IEEE Control Syst.*, vol. 30, no. 6, pp. 72–80, Dec. 2010.

[83] M. Amin, "Challenges in reliability, security, efficiency, and resilience of energy infrastructure: Toward smart self-healing electric power grid," in *Proc. Power Energy Soc. General Meeting-Convers. Del. Elect. Energy 21st Century*, Jul. 2008, pp. 1–5.

[84] T. Li and B. Xu, "The self-healing technologies of smart distribution grid electricity distribution," in *Proc. China Int. Conf.*, Sep. 2010, pp. 1–6.

[85] D. Jia, X. Meng, and X. Song, "Study on technology system of self-healing control in smart distribution grid," in *Proc. Int. Conf. Adv. Power Syst. Autom. Protection*, Oct. 2011, pp. 26–30.

[86] A. Zidan and E. El-Saadany, "A cooperative multiagent framework for self-healing mechanisms in distribution systems," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1525–1539, Sep. 2012.

[87] X. Gao and X. Ai, "The application of self-healing technology in smart grid," in *Proc. Power Energy Eng. Conf.*, Mar. 2011, pp. 1–4.

[88] S. Yu, Y. Sun, X. Niu, and C. Zhao, "Energy internet system based on distributed renewable energy generation," *Electric Power Autom. Equipment*, vol. 30, no. 5, pp. 104–108, 2010.

[89] P. Georgilakis, "Technical challenges associated with the integration of wind power into power systems," *Renewable Sustainable Energy Rev.*, vol. 12, no. 3, pp. 852–863, 2008.

[90] G. Singh, "Solar power generation by PV (photovoltaic) technology: A review," *Energy*, vol. 53, no. 1, pp. 1–13, 2013.

[91] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2474–2482, Sep. 2017.

[92] P. Balakrishna, K. Rajagopal, and K. Swarup, "Analysis on AMI system requirements for effective convergence of distribution automation and AMI systems," in *Proc. Power India Int. Conf.*, Dec. 2014, pp. 1–7.

[93] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang, and T. Sato, "A key management scheme for secure communications of information centric advanced metering infrastructure in smart grid," *IEEE Trans. Instrum. Meas.*, vol. 64, no. 8, pp. 2072–2085, Aug. 2015.

[94] S. Bera, S. Misra, and M. Obaidat, "Energy-efficient smart metering for green smart grid communication," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 2466–2471.

[95] D. Hart, "Using AMI to realize the smart grid," in *Proc. Power Energy Soc. General Meeting-Convers. Del. Elect. Energy 21st Century*, Jul. 2008, pp. 1–2.

[96] I. Joe, J. Jeong, and F. Zhang, "Design and implementation of AMI system using binary CDMA for smart grid," in *Proc. 3rd Int. Conf. Intell. Syst. Des. Eng. Appl.*, Jan. 2013, pp. 544–549.

[97] D. Xu, M. Lei, F. Zhou, and W. Luan, "Study on hybrid storage method of AMI mass data," in *Proc. China Int. Conf. Elect. Distrib.*, Sep. 2014, pp. 1288–1293.

[98] G. Barai and K. Raahemifar, "Optimization of distributed communication architectures in advanced metering infrastructure of smart grid," in *Proc. IEEE 27th Can. Conf. Elect. Comput. Eng.*, May 2014, pp. 1–6.

[99] C. Pirak, T. Sangsuwan, and S. Buayairaksa, "Recent advances in communication technologies for smart grid application: A review," in *Proc. Int. Elect. Eng. Congr.*, Mar. 2014, pp. 1–4.

[100] B. Zhang, H. Sun, and W. Wu, "A new generation of EMS implemented in chinese electric power control centers," in *Proc. Power Energy Soc. General Meeting-Convers. Del. Electr. Energy 21st Century*, Jul. 2008, pp. 1–3.

[101] E. Babovic and J. Velagic, "Lowering SCADA development and implementation costs using PtP concept," in *Proc. 22nd Int. Symp. Inf. Commun. Autom. Technol.*, Oct. 2009, pp. 1–7.

[102] J. De La Ree, V. Centeno, J. Thorp, and A. Phadke, "Synchronized phasor measurement applications in power systems," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 20–27, Jun. 2010.

[103] M. Qiu, W. Gao, M. Chen, J. Niu, and L. Zhang, "Energy efficient security algorithm for power grid wide area monitoring system," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 715–723, Dec. 2011.

[104] T. Papadopoulos, C. Kaloudas, A. Chrysochos, and G. Papagiannis, "Application of narrowband power-line communication in medium-voltage smart distribution grids," *IEEE Trans. Power Del.*, vol. 28, no. 2, pp. 981–988, Apr. 2013.

[105] Q. Ho, Y. Gao, and T. Le-Ngoc, "Challenges and research opportunities in wireless communication networks for smart grid," *IEEE Wireless Commun.*, vol. 20, no. 3, pp. 89–95, Jun. 2013.

[106] D. Ramïrez, S. Cëspedes, C. Becerra, and C. Lazo, “Performance evaluation of future AMI applications in smart grid neighborhood area networks,” in *Proc. IEEE Colombian Conf. Commun. Comput.*, May 2015, pp. 1–6.

[107] D. Bian, M. Kuzlu, M. Pipattanasomporn, and S. Rahman, “Analysis of communication schemes for advanced metering infrastructure (AMI),” in *Proc. IEEE PES General Meeting—Conf. Expo.*, Jul. 2014, pp. 1–5.

[108] N. Liu and J. Zhang, “Cyber security risks and requirements for customer interaction of smart grid,” *Autom. Electric Power Syst.*, vol. 35, no. 2, pp. 79–83, Feb. 2011.

[109] A. Mohman, P. Bera, and E. AI-Shaer, “Smart analyzer: A noninvasive security threat analyzer for AMI smart grid,” in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 2255–2263.

[110] F. Cleveland, “Cyber security issues for advanced metering infrastructure (AMI),” in *Proc. Power Energy Soc. General Meeting-Convers. Del. Energy Soc. 21st Century*, Jul. 2008, pp. 1–5.

[111] K. Wang, H. Li, Y. Feng, and G. Tian, “Big data analytics for system stability evaluation strategy in the energy internet,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1969–1978, Apr. 2017.

[112] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, “Protection of big data privacy,” *IEEE Access*, vol. 4, pp. 1821–1834, 2016.

[113] M. Ali, E. A-Shaer, and Q. Duan, “Randomizing AMI configuration for proactive defense in smart grid,” in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2013, pp. 618–623.

[114] Y. Wang, B. Zhang, W. Lin, and T. Zhang, “Smart grid information security-a research on standards,” in *Proc. Int. Conf. Adv. Power Syst. Autom. Protection*, Oct. 2011, pp. 1188–1194.

[115] S. Fries, H. Hof, and M. Seewald, “Enhancing IEC 62351 to improve security for energy automation in smart grid environments,” in *Proc. 5th Int. Conf. Internet Web Appl. Serv.*, May 2010, pp. 135–142.

[116] B. Lu and Y. Ma, “Research on communication system of advanced metering infrastructure for smart grid and it’s data security measures,” *Power Syst. Technol.*, vol. 37, no. 8, pp. 2244–2249, 2013.

[117] Y. Yu, “Technical composition of smart grid and it’s implementation sequence,” *Southern Power Syst. Technol.*, vol. 3, no. 2, pp. 1–5, 2009.

[118] W. Wang, Y. Xu, and M. Khanna, “A survey on the communication architectures in smart grid,” *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, Oct. 2011.

[119] H. Zhao, J. Zhou, and E. Yu, “Advanced metering infrastructure supporting effective demand response,” *Power Syst. Technol.*, vol. 34, no. 9, pp. 13–20, 2010.

[120] J. Baek, Q. Vu, J. Liu, X. Huang, and Y. Xiang, “A secure cloud computing based framework for big data information management of smart grid,” *IEEE Trans. Cloud Comput.*, vol. 3, no. 2, pp. 233–244, Apr.–Jun. 2015.

[121] W. Zhu and Q. Guo, “Data security and encryption technology research on smart grid communication system,” in *Proc. 8th Int. Conf. Meas. Technol. Mechatronics Autom.*, Mar. 2016, pp. 175–178.

[122] Z. Wang, F. Chen, and A. Xia, “Attribute-based online/offline encryption in smart grid,” in *Proc. 24th Int. Conf. Comput. Commun. Netw.*, Aug. 2015, pp. 1–5.

[123] F. Ye, Y. Qian, and R. Hu, “An identity-based security scheme for a big data driven cloud computing framework in smart grid,” in *Proc. IEEE Global Commun. Conf.*, Dec. 2015, pp. 1–6.

[124] C. Ten, J. Hong, and C. Liu, “Anomaly detection for cybersecurity of the substations,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.

[125] Night dragon. (2011). [Online]. Available: http://www.mcafee.com/us/about/night-dragon.aspx

[126] Y. Mo, T. Kim, and Brancik, “Cyber-physical security of a smart grid infrastructure,” *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[127] N. Rao, R. Narayanan, B. Vasudevamurthy, and S. Das, “Performance requirements of present-day distribution transformers for smart grid,” in *Proc. IEEE Innovative Smart Grid Technol.-Asia*, Nov. 2013, pp. 1–6.

[128] D. Rawat and C. Bajracharya, “Cyber security for smart grid systems: Status, challenges and perspectives,” in *Proc. IEEE SoutheastCon*, Apr. 2015, pp. 9–12.

[129] J. Dagle, “Cyber-physical system security of smart grids,” in *Proc. IEEE PES Innovative Smart Grid Technol.*, Jan. 2012, pp. 1–2.

[130] Z. Dong, “Smart grid cyber security,” in *Proc. 13th Int. Conf. Control Autom. Robot. Vis.*, Dec. 2014, pp. 1–2.

[131] J. Liu, Y. Xiao, S. Li, W. Liang, and C. Chen, “Cyber security and privacy issues in smart grids,” *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, Oct.–Dec. 2012.

[132] Y. Wang, X. Lin, and M. Pedram, “Coordination of the smart grid and distributed data centers: A nested game-based optimization framework,” in *Proc. Innovative Smart Grid Technol. Conf.*, Feb. 2014, pp. 1–5.

[133] J. Ansilla, N. Vasudevan, J. JayachandraBensam, and J. Anunciya, “Data security in smart grid with hardware implementation against DoS attacks,” in *Proc. Int. Conf. Circuit Power Comput. Technol.*, Mar. 2015, pp. 1–7.

[134] S. Ruj and A. Nayak, “A decentralized security framework for data aggregation and access control in smart grids,” *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 196–205, Mar. 2013.

[135] H. Chen and S. Zhu, “Exploration on optical fiber wiretapping and intrusion detection,” *Inf. Secur. Commun. Privacy*, vol. 34, no. 1, pp. 61–63, 2012.

[136] C. Ten, J. Hong, and C. Liu, “Anomaly detection for cybersecurity of the substations,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865–873, Dec. 2011.

[137] Y. Mo, T. Kim, and Brancik, “Cyber-physical security of a smart grid infrastructure,” *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[138] X. Wang, X. Bi, Z. Ge, and L. Li, “Deep data fusion model for risk perception and coordinated control of smart grid,” in *Proc. Int. Conf. Estimation Detection Inf. Fusion*, Jan. 2015, pp. 110–113.

[139] S. Zhao, D. Zhang, and Y. Yin, “Risk assessment of smart grid,” *Power Syst. Technol.*, vol. 33, no. 19, pp. 7–10, 2009.

[140] C. Lin, H. Zhao, X. Liu, H. Li, and J. Xu, “Research on routing strategy for intergrid,” *Trans. China Electrotechnical Soc.*, vol. 30, no. 11, pp. 37–44, 2015.

[141] ISO/IEC/IEEE 18880:2015-Information Technology-Ubiquitous Green Community Control Network Protocol. (2015). [Online]. Available: https://www.iso.org/standard/67485.html

[142] A. R. Metke and R. L. Ekl, “Security technology for smart grid networks,” *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[143] P. Zhang, O. Elkeelany, and L. McDaniel, “An implementation of secured smart grid ethernet communications using AES,” in *Proc. IEEE SoutheastCon*, Mar. 2010, pp. 394–397.

[144] C. Wu, T. Yoshinaga, Y. Ji, T. Murase, and Y. Zhang, “A reinforcement learning-based data storage scheme for vehicular Ad Hoc networks,” *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6336–6348, Jul. 2017.

[145] K. Wang, et al., “Distributed energy management for vehicle-to-grid networks,” *IEEE Netw.*, vol. 31, no. 2, pp. 22–28, Mar. 2017.

[146] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, Oct.–Dec. 2014.

[147] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber security and privacy issues in smart grids,” *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, Oct.–Dec. 2012.

[148] X. Zhou, F. Wang, and Y. Ma, “An overview on energy internet,” in *Proc. IEEE Int. Conf. Mechatronics Autom.*, 2015, pp. 126–131.

[149] F. Akhtar and M. Rehmani, “Energy replenishment using renewable and traditional energy resources for sustainable wireless sensor networks: A review,” *Elsevier Renewable Sustainable Energy Rev.*, vol. 45, pp. 769–784, May 2015.

[150] J. Zhang, W. Wang, and S. Bhattacharya, “Architecture of solid state transformer-based energy router and models of energy traffic,” in *Proc. IEEE PES Innovative Smart Grid Technol.*, 2012, pp. 1–8.

[151] F. Akhtar, M. Rehmani, M. Reisslein, “White space: Definitional perspectives and their role in exploiting spectrum opportunities,” *Telecommun. Policy*, vol. 40, no. 4, pp. 319–331, Apr. 2016.

[152] S. Hashim, R. Bukhari, M. Rehmani, and S. Siraj, “A survey of channel bonding for wireless networks and guidelines of channel bonding for futuristic cognitive radio sensor networks,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 924–948, Apr.–Jun. 2016.

[153] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, “Cognitive machine-to-machine communications: Visions and potentials for the smart grid,” in *Proc. IEEE PES Innovative Smart Grid Technol.*, 2012, pp. 1–8.

[154] H. Jiang, K. Wang, Y. Wang, M. Gao, and Y. Zhang, "Energy big data: A survey," *IEEE Access*, vol. 4, pp. 3844–3861, Aug. 2016.

[155] M. Rehmani, M. Kantarci, A. Rachedi, M. Radenkovic, and M. Reisslein, "Smart grids: A hub of interdisciplinary research," *IEEE Access Special Section Editorial*, vol. 3, pp. 3114–3118, 2015.

[156] G. Shah, V. Gungor, and O. Akan, "A cross-layer QoS-aware communication framework in cognitive radio sensor networks for smart grid applications," *IEEE Trans. Ind. Informat.*, vol. 9, no. 3, pp. 1477–1485, Aug. 2013.

[157] R. Qiu, et al., "Cognitive radio network for the smart grid: Experimental system architecture, control algorithms, security, and microgrid testbed," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 724–740, Dec. 2011.

[158] G. Wang, G. Zhou, H. Zhao, and H. Liu, "Real-time big data technologies of energy internet platform," in *Proc. IEEE Int. Conf. Power Syst. Technol.*, 2016, pp. 1–6.

[159] K. Wang, J. Yu, Y. Yu, Y. Qian, D. Zeng, S. Guo, Y. Xiang, and J. Wu, "A survey on energy internet: Architecture, approach, and emerging technologies," *IEEE Syst. J.*, to be pubished. doi: 10.1109/JSYST.2016.2639820.

[160] *Standardization Mandate to CEN, CENELEC and ETSI in the Field of Measuring Instruments for the Development of an Open Architecture for Utility Meters Involving Communication Protocols Enabling Interoperability*, European Standard M/441 EN, European Commission-Enterprise and Industry Directorate-General, 2009.

[161] Arch Rock, "Smart grid standards-meter reading and control using IEC 61968–9," 2010. [Online]. Available: http://www.archrock.com/blog/tag/iec/

[162] OFFIS, SCC. "Consulting, and MPC management coaching," Untersuchung des Normungsumfldes zum BMWi-Foerderschwerpunkt E-Energy-IKT-Basiertes Energiesystem der Zunkunft, vol. PP, no. PP, p. 1, 2009.

[163] BDI Initiativ, "Internet of energy-ICT for energy markets of the future," BDI publication, no. 439, pp. 1–52, 2008.

[164] S. Rohjans, et al., "Survey of smart grid standardization studies and recommendations," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, 2010, pp. 583–588.

[165] *ISO/IEC/IEEE Information Technology-Ubiquitous Green Community Control Network Protocol*, ISO/IEC/IEEE Standard 18880:2015, pp. 1–78, Apr. 2015.

[166] H. Takasaki, S. Mostafa, and S. Kusakabe, "Monitoring Hadoop by using IEEE1888 in implementing energy-aware thread scheduling," in *Proc. IEEE 11th Int. Conf Ubiquitous Intell. Comput. IEEE 11th Int. Conf. Autonomic Trusted Comput. IEEE 14th Int. Conf. Scalable Comput. Commun. Associated Workshops*, 2014, pp. 655–658.

[167] *ISO/IEC/IEEE International Standard-Information technology-Ubiquitous Green Community Control Network-Control and Management*, ISO/IEC/IEEE Standard 18881 First Edition 2016–04-15, pp. 1–65, Apr. 2016.

[168] *ISO/IEC/IEEE International Standard-Information Technology-Ubiquitous Green Community Control Network-Security*, ISO/IEC/IEEE Standard 18883 First Edition 2016–04-15, pp. 1–35, Apr. 2016.

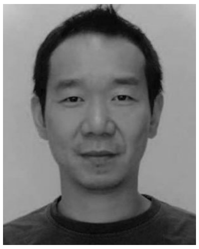
Kun Wang (M'13) received the BEng and PhD degrees from the School of Computer, Nanjing University of Posts and Telecommunications, Nanjing, China, in 2004 and 2009, respectively. From 2013 to 2015, he was a postdoc fellow in the Electrical Engineering Department, University of California, Los Angeles (UCLA), California. In 2016, he was a research fellow in the School of Computer Science and Engineering, University of Aizu, Aizu-Wakamatsu City, Fukushima, Japan. He is currently an associate professor in the School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing, China. He has published more than 50 papers in referred international conferences and journals. He has received Best Paper Award at IEEE GLOBECOM'2016. He serves as associate editor of the *IEEE Access*, the *Journal of Network and Computer Applications*, the *EAI Transactions on Industrial Networks and Intelligent Systems* and editor of the *Journal of Internet Technology*. He was the symposium chair/co-chair of IEEE IECON16, IEEE EEEIC16, IEEE WCSP16, IEEE CNCC17, etc. His current research interests are mainly in the area of big data, wireless communications and networking, smart grid, energy Internet, and information security technologies. He is a member of the IEEE and the ACM.

Xiaoxuan Hu received the BEng degree in automation from the Nanjing University of Posts and Telecommunications (NJUPT), Nanjing, China, in 2014, and is currently working toward the PhD degree in information acquisition and control at NJUPT. Her research interests include big data management and analysis, vehicle-2-grid networks, and communications networks in the smart grid.

Huining Li received the BEng degree in electronic science and technology from Nanjing University of Information Science and Technology (NUIST), Nanjing, China, in 2016, and is currently working toward the PhD degree in information acquisition and control at Nanjing University of Posts and Telecommunications (NJUPT). Her research interests include big data analysis, reinforcement learning, and communication networks in the Energy Internet.

Peng Li (M'12) received the BS degree from Huazhong University of Science and Technology, China, in 2007, the MS and PhD degrees from the University of Aizu, Japan, in 2009 and 2012, respectively. He is currently an associate professor with the University of Aizu, Japan. His research interests mainly focus on wireless communication and networking, specifically wireless sensor networks, green and energy-efficient mobile networks, and cross-layer optimization for wireless networks. He also has interests on cloud computing, big data processing, and smart grid. He is a member of the IEEE.

Deze Zeng (S'10-M'12) received the BS degree from the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China, in 2007, and the MS and PhD degrees in computer science from the University of Aizu, Aizuwakamatsu, Japan, in 2009 and 2013, respectively. He is currently an associate professor in the School of Computer Science, China University of Geosciences, Wuhan, China. He has authored one book and more than 70 papers in refereed journals and conferences in these areas. His current research interests include network function virtualization, cloud computing, software-defined networking, wireless sensor networks, data center networking, and networking protocol design and analysis. He is a member of the IEEE.



Song Guo is a Full Professor at Department of Computing, The Hong Kong Polytechnic University. He received his PhD in computer science from University of Ottawa and was a full professor with the University of Aizu, Japan. His research interests are mainly in the areas of big data, cloud computing, green communication and computing, wireless networks, and cyber-physical systems. He has published over 350 conference and journal papers in these areas and received 5 best paper awards from IEEE/ACM conferences. Dr. Guo has served in editorial boards of several prestigious journals, including IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Sustainable Computing, IEEE Transactions on Green Communications and Networking, and IEEE Communications. He an active volunteer as General/TPC Chair for 20+ international conferences and Chair/Vice-Chair for several IEEE Technical Committees and SIGs. He is a senior member of IEEE, a senior member of ACM, and an IEEE Communications Society Distinguished Lecturer.