Standardization and Security for Smart Grid Communications Based on Cognitive Radio Technologies – A Comprehensive Survey

Trong Nghia Le, *Student Member, IEEE*, Wen-Long Chin, *Senior Member, IEEE*, and Hsiao-Hwa Chen, *Fellow, IEEE*

Abstract – Today's electric power grids have been ageing and ill-suited to meet fast-growing demands for electricity energy generation, delivery, and supply. The global climate change and the greenhouse gas emissions on the Earth caused by power industries put a high pressure on the existing power grids. Consequently, smart grid (SG) has emerged to address these challenges. The SG can achieve improved load balancing through accessing instantaneous electricity demand information via two-way communication and power flows, which help power plants match their output to the demand precisely. To this end, SG works based on the exchanges of a large amount of information generated from metering, sensing, and monitoring. Hence, the choice of communication infrastructure for SG is critical to provide secure, reliable, and efficient data delivery between various SG components. Cognitive radio (CR) network has been recognized as a promising technology to address communication requirements, standardization, and security problems of SG. Moreover, possible solutions in CR-based SG communications are also identified. In particular, we identify the major challenges of communication architecture, standardization, and security issues to implement CR-based SG communications. The aim of this paper is to offer a comprehensive review on the state-of-the-art researches on CR-based SG communications, to highlight what have been investigated and what still remain to be addressed, particularly, in standardization and security aspects.

***Index Terms*—Cognitive radio; Smart grid; Communication network; Security; Standards**

I. Introduction

An electric power grid is a network of power generators, transmission lines, transformers, and distribution/relay systems to provide its consumers (residential, industrial, and commercial) with the power they need. Currently, electrical energy is generated in centralized utility plants and transported over long-distance transmission networks to distribution networks before reaching to the end consumers via communication and power flows in only one direction, i.e., from power plants to the customers, which are collectively called an electric grid. After many decades of development, it has been realized that various utilities can be interconnected to achieve a greater reliability of overall power systems, dealing with unexpected failures as well as disconnections from power devices, i.e., transmission lines and generators.

In an electric grid, generation, transmission, and distribution of power should be precisely coordinated. Fig. 1 depicts various sections in a today's electric grid, which consists of four segments including generation, transmission, distribution, and customers [1]. Power generation involves the production of electricity from energy sources such as wind farms, coal plants, and hydroelectric dams. Because generators cannot be located too close to population centers for safety, legal, and financial reasons, the electric grid needs transmission lines to carry the electricity over long distances (often more than hundreds of miles). Distribution segment includes taking the electricity from transmission lines and delivering it to the customers. Typically, an electricity distribution system includes medium voltage power lines (below 50 kV), substations, and transformers, starting at transmission substations and ending at the meters of customers. A substation consists of a bus to split up the power into different regions, step-down transformers, relays, and circuit breakers, which are designed to disconnect the substations from different distribution lines or from the power grid whenever necessary.

Due to the lack of situational awareness and automated analysis, today's electric power grid has been ageing and ill-suited to meet fast growing demands for electricity in the 21st century [2]. For example, in the US, the consumption and demand for electricity have increased by 2.5% annually over the last 20 years [3]. Besides, the global climate change and greenhouse gas emissions on the Earth caused by the electricity and transportation industries [4], [5] put a lot of stress on the existing power grids. Consequently, a new concept of next generation electric power systems is urgently needed to address these challenges, which motivates the proposal of smart grid (SG).

The SG can be viewed as a superposition of communication networks on electric grids. It aims to improve efficiency, reliability, safety, and security of electricity supply to the customers, with a seamless integration of renewable and alternative energy sources, such as photovoltaic systems, wind energy, biomass power generation, tidal power, small hydropower plants, and plug-in hybrid electric vehicles, through automated control and modern communication technologies [6]. In SG, various components in these four areas of the electric grid are

Trong Nghia Le (email: nghiahp79@gmail.com) is with Le Quy Don Technical University, Hanoi, Vietnam. Wen-Long Chin (email: wlchin@mail.ncku.edu.tw) and Hsiao-Hwa Chen (email: hshwchen@mail.ncku.edu.tw) are with the Department of Engineering Science, National Cheng Kung University, Tainan 70101, Taiwan.

This work was financially supported in part by the Ministry of Science and Technology, Taiwan, under the grants 104-2221-E-006-117, 105-2221-E-006-019-MY2, 102-2221-E-006-008-MY3, and 104-2221-E-006-081-MY2.

Manuscript was submitted on September 13, 2015, and revised on September 24, 2016.

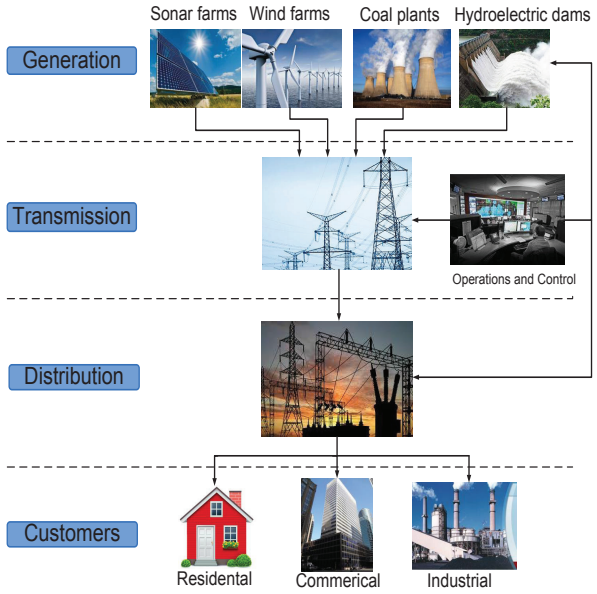

Fig. 1. A typical electric power grid.

linked together via two-way communication and power flows to provide interoperability among them [7]. Thus, consumers not only draw power but also supply surplus power to the grid using smart meters that enable monitoring and measuring of these bidirectional flows. This new infrastructure could potentially produce millions of alternate micro-energy sources and allow improved load balancing through instantaneous electricity demand information exchanges, which help power plants match their outputs to demands precisely with the help of information generated from metering, sensing, and monitoring.

Therefore, the choice of communication infrastructure in SG is critical to provide secure, reliable, and efficient data delivery between the components in both real-time and non-real-time manners. Most traditional communication technologies suffer from high costs for investment, maintenance, and operation [8]. The SG communication is a heterogeneous amalgamation of wired (e.g., fiber-optic and copper) and wireless (e.g., WiMAX, microwave, and satellite) technologies working in various standards [9] and different security requirements [10], [11]. The transmission over heterogeneous media is a major barrier to realize the SG. Moreover, a huge amount of data and information related to monitoring and control will be transmitted across SG using wireless communication infrastructures, increasing radio frequency (RF) interferences and competitions over limited and already very crowded radio spectrum, particularly when smart meters operate in 2.4 GHz industrial, scientific, and medical (ISM) unlicensed bands, shared with other existing wireless applications, such as WiFi, Bluetooth, and Zigbee. As a result, reliability of SG communications will be impaired. Since the current infrastructure is incapable of meeting the challenges in SG, a revolutionary communication infrastructure is urgently required.

A. Cognitive Radio Technology

Cognitive radio (CR) network is recognized as a promising technology to address the communication requirements, standardization, and security issues of SG communications [12]-[14]. According to a study on traditional policies of spectral assignment done by Federal Communications Commission (FCC), utilization of allocated spectrum varies in time and space between 15% and 85% [15]; whereas some portions of the unlicensed bands are so crowded by emerging wireless services overlaying the applications in SG [16]. Thus, dynamic spectrum access using CR is an important technology to improve the spectrum utilization of SG communications [17]. It is also critical to support various traffic types including multimedia, particularly for real-time traffic delivery with stringent quality of service (QoS) requirements in future SG systems [18]. In a traditional spectrum management paradigm, the spectrum is allocated to licensed users (i.e., primary users (PUs)) for their exclusive use. Recognizing the significance of the issue of spectrum shortage, FCC is considering to open up licensed bands to unlicensed operations as long as they do not interfere with the licensed users, meaning that unlicensed users (i.e., secondary users (SUs)) will be able to opportunistically operate in vacant licensed spectrum bands, increasing the efficiency of spectrum utilization. Mitola proposed the concept of CR to solve the problems of scarce spectrum and poor spectrum allocation based on traditional spectrum policies in [19]. To achieve this goal, the spectrum sensing [20]–[23] is the key technology of CR networks.

B. CR-based Smart Grid

A SU in CR must continuously monitor radio spectrum usage to give precedence to the PU. As such, if a PU starts to transmit signals, then SUs must switch to another spectral hole immediately, which may occur in a random fashion. For this reason, the random interruptions of SU traffic will unavoidably cause packet losses and delays for SU data delivery. The lost data packets can be real-time pricing information sent between utilities and customers, sensed data from remote terminal units (RTUs), and control commands from control centers to substations. The loss of data packets may have considerable effects on the control and management of the SG, particularly in urgent situations. The works in [24] and [25] emphasised that communication failures in communication channels can significantly degrade the reliability of the cooperative control of distributed energy resources (DERs) in distribution networks. Communication failures may cause very serious problems for both system operation and control in a power grid [26], and can interrupt the wide area damping control of power systems [27]. In [28], dynamic performance of automatic generation control (AGC) of a four-area power system was found to depend sensitively on communication topologies among local-area controllers. And communication topology changes among distributed damping controllers can jeopardise the power system performance [29]. Therefore, it is critical to address the aforementioned issues and to

TABLE I
MAJOR INTEGRATION ISSUES AND SOLUTIONS.

Integration model	Resource and interference management	PU activity measurement and prediction
[30], [31], [32]	[33]–[37]	[38]–[40]

understand the effects of random interruptions of SU traffic in CR networks on stability and performance of SG operation and control. Table I summarises the major integration problems of CR and SG systems and their relevant papers. They are briefly described as follows.

The authors in [30] addressed these problems and investigated modelling and stability issues of the AGC in a SG, for which CR networks are used as the infrastructure for aggregation and communication of both system-wide information and local measurement data. For this purpose, a randomly switched power system model was proposed for AGC of the SG under the conditions that the design of CR networks can ensure the stability of AGC. The authors in [31] investigated a combined system of electricity and CR technologies, considering their mutual interactions with enhanced reliability and efficiency of the overall SG system, including energy usage and power distribution associated with home/subscriber level multimedia applications. Collected information from smart meters and other grid elements is used to develop better load forecasting and power scheduling that will be interfaced with power distribution and transmission control centers via CR networks. The authors in [32] proposed a communication method through a CR link between sensors at a consumer site and a control center of the SG. To adjust this new communication link when it is affected by PUs, a state estimator was used. This link is governed by multiple semi-Markov processes, each of which can capture and model one channel of the CR system.

In [33], to improve energy efficiency in SG, cognitive heterogeneous mobile networks were proposed based on power allocation and interference management. Since the communications in a CR network are normally unreliable, it is a great challenge to support real-time applications, which have stringent delay requirements. To this end, the authors in [34] proposed to reroute real-time data traffic through neighbouring cells that work properly. However, the proposed scheduling algorithm did not consider the priority of data. To solve this problem, the authors in [35], [36] considered the heterogeneous characteristics of SG traffic including multimedia, and proposed a priority-based traffic scheduling approach for CR-based SG according to various traffic types such as control commands, multimedia sensing data, and meter readings. Specifically, they developed CR channel allocation and traffic scheduling schemes, taking into account channel switch and spectrum sensing errors, and solved a system utility optimization problem for SG communication systems. The work in [37] studied the code division multiple access technique using a kind of orthogonal chip sequences to increase the number of SUs.

The accurate inference of PU activities can facilitate the CR-based SG communications. In [38], geolocation databases, which are consulted before spectrum access, were designed to store information related to PUs. A radio environment map constructs a comprehensive map of the CR networks by utilizing multi-domain information from databases, characterised by spectrum usage, geographical terrain models, propagation environment, and regulations. Various spectrum occupancy models were reported in [39] and [40]. These models extract different statistical properties of the spectrum occupancy from the measured data. Autoregressive and/or moving-average models were used to predict the channel status.

In summary, CR is a critical technology to realize the SG. Nevertheless, a comprehensive survey on CR-based SG is not available in the literature. Therefore, the main purpose of this paper is to provide a thorough review on the works appeared in the literature, helping readers to understand what have been investigated and what still remain to be addressed in CR-based SG. In addition, this paper will discuss the architecture, standards, and security issues to implement CR-based SG, and major challenges and solutions for CR-based SG are also identified.

The reminder of this paper can be outlined as follows. In Section II, we review related survey articles and summarise our contributions in this survey. In Section III, we discuss SG communications infrastructure. A three-tier SG communication architecture based on CR and its applications are the subject of interest in Section IV. In Section V, the standards of SG based on CR are discussed, while their principal security problems will be addressed in Section VI. Sections VII and VIII identify enabling techniques and future challenges, respectively, followed by the conclusions given in Section IX. All the acronyms along with their definitions are provided in Table II.

II. RELATED SURVEY ARTICLES AND OUR CONTRIBUTIONS

Several works in the literature appeared to address the issues on CR supporting SG communications. However, there are still many issues pending to be investigated. Furthermore, some related survey papers were written without discussing specifically about the details of CR-based SG systems, especially on the standardization and security aspects. The authors in [41] gave a brief overview on the general principles of CR in SG communications to improve the performance in operation and control of SG. The survey in [42] focused on different cloud computing applications for SG architecture in three different areas, including energy management, information management, and security. The authors in [43] revealed the potentials of CR for supporting SG communications, in which its challenges and opportunities were identified. In [44], a survey was done on neighbourhood area networks (NANs), which is an important component of SG networks, suggesting

TABLE II
LIST OF ACRONYMS AND THEIR DEFINITIONS.

Acronym	Definition	Acronym	Definition
AGC	Automatic Generation Control	NIST	National Institute for Standards and Technology
AMI	Advanced Metering Infrastructure	PKI	Public Key Infrastructure
BDD	Bad Data Detection	PLCs	Power Line Communications
BSs	Base Stations	PUEA	Primary User Emulation Attack
CA	Certificate Authority	PUs	Primary Users
CPE	Customer-Premises Equipment	QKD	Quantum Key Distribution
CR	Cognitive Radio	QoS	Quality of Service
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance	RA	Registration Authority
CSN	Cognitive Sensor Network	RF	Radio Frequency
CSR	Certificate Signing Request	RTUs	Remote Terminal Units
DERs	Distributed Energy Resources	SDR	Software-Defined Radio
DoS	Denial-of-Service	SEP	Smart Energy Profile
FCC	Federal Communications Commission	SG	Smart Grid
FPGA	Field Programmable Gate Array	SIA	Seamless Integration Architecture
FSST	Fixed Sample Size Test	SPRT	Sequential Probability Ratio Test
HAN	Home Area Network	SUNs	Smart Utility Networks
HGW	Home Gateway	SUs	Secondary Users
IEC	International Electrotechnical Commission	T&D	Transmission and Distribution
IEDs	Intelligent Electronic Devices	TVWS	TV White Space
ISM	Industrial, Scientific, and Medical	UHF	Ultra High Frequency
IT	Information Technology	VA	Validation Authority
LocDef	Localization-based Defence	VHF	Very High Frequency
LQG	Linear Quadratic Gaussian	VPN	Virtual Private Network
MAC	Medium Access Control	WAMR	Wireless Automatic Meter Reading
MANETs	Mobile Ad Hoc Networks	WAN	Wide Area Network
NANs	Neighborhood Area Networks	WLANs	Wireless Local Area Networks
NGW	NAN Gateway	WRAN	Wireless Regional Area Network

to use CR in NANs. In [45], the works on CR-based SG were reviewed to propose a possible solution for implementing an effective SG communication network. Moreover, new methods were introduced to address the challenges in CR-based SG applications. In [46], the authors made an effort to combine wireless sensor networks with CR to build up CR-based wireless sensor networks in SG for a specific implementation case in Pakistan, where the sensor networks monitor physical parameters and then the measurement data are transmitted using CR. An overview on background, technology, regulation, and standardization in the course of deploying smart utility networks (SUNs), a specific form of an SG network operating in TV white space (TVWS), was presented in [47]. A comprehensive survey on SG characteristics, CR-based network architectures, spectrum management, and other major challenges was given in [17]. In contrast to [17], the authors in [48] offered an up-to-date review on CR-based SG communications, including spectrum sensing mechanisms, interference mitigation schemes, and routing/medium access control (MAC) protocols. However, standards and security issues on the subject were only mentioned briefly in [48]. For example, in the standardization of CR-based SG, the authors surveyed IEEE 802.22 only for cognitive wide area networks (WANs), without mentioning the standardization in home area networks (HANs) and NANs, which also play important roles in SG. In [48], the authors discussed security methods for SG without considering CR. In particular, the enabling techniques to tackle the challenges in CR-based SG are basically missing in [48]. In this connection, our survey paper can be viewed as a supplementary to [48], offering readers a more comprehensive survey on the state-of-the-art researches on CR-based SG communications.

The review articles of [46], [17], [48], and [45] have identified some selected topics on CR-based SG. In this survey paper, we aim to give a comprehensive survey, covering communication architectures, applications, standards, and security issues on CR-based SGs. Moreover, the possible solutions in CR-based SG communications are also suggested. In summary, the major contributions of this paper can be summarized as follows:

- We present a brief introduction on communication architectures for CR-based SG, including cognitive HANs, NANs, and WANs.
- We showcase several potential applications of CR-based SG.
- We provide a survey on the standardization works for CR-based SG.
- We focus very much on the security issues in the implementation of CR-based SG.
- We suggest the enabling techniques to tackle the challenges in CR-based SG.
- We point out the open issues and challenges for CR-based SG systems.

III. SMART GRID COMMUNICATIONS INFRASTRUCTURE

SG communications infrastructure is expected to incorporate a hybrid of diverse communication technologies to provide efficient and reliable access to various SG components in different environments. Similar to existing data and voice telecommunication networks, SG communications infrastructure is expected to be a multi-tier network that extends across multiple grid operation tiers. The SG communication networks

TABLE III
COMMUNICATION TECHNOLOGIES RELEVANT TO SG.

	Technology	Spectrum	Date rate	Coverage	Application	Limitation
Wireless	GSM	900-1800 MHz	Up to 14.4 Kbps	1-10 km	AMI, demand response, HANs, NANs, WANs	Low data rates
	GPRS	900-1800 MHz	Up to 170 Kbps	1-10 km	AMI, demand response, HANs, NANs, WANs	Low data rates
	3G	1.92-1.98 GHz 2.11-2.12 GHz (licensed)	384 Kbps-2 Mbps	1-10 km	AMI, demand response, HANs, NANs, WANs	Costly spectrum fees
	WiMAX	2.5 GHz, 3.5 GHz, 5.8 GHz	Up to 75 Mbps	10-50 km (LOS) 1-5 km (NLOS)	AMI, demand response, NANs, WANs	Not widespread
	CDMA	450-2100 MHz	Up to 153 kbps	49 km	WANs, NANs	Low data rates
	ZigBee	2.4 GHz, 868-915 MHz	250 Kbps	30-50 m	AMI, demand response, HANs	Low data rates, short range
	Cognitive Radio (IEEE 802.22 Standard in North America)	54-–862 MHz	18–24 Mbps	10—100 km	WANs, NANs, AMI, demand response, HANs	Passive operation (depending on PU)
	Wifi	2.4 and 5 GHz	2-600 Mbps	100-300 m	Automatic Meter Reading	Low data rates, short range
	4G	700-2500 MHz	3.3 Gbps for LTE-Advanced	10 km	DERs, AMI, EVs, ADR, NANs, WANs	
	Microwave	2-40 GHz	155 Mbps	60 km	AMI, demand response, HANs	Low data rates, short range
	Bluetooth	2.4 GHz GHz	1 Mbps	10-100 m	AMI, demand response, HANs	Low data rates, short range
	LTE	900 MHz	300 Mbps	30 km	WANs, NANs	
	Satellite Communications	1-40 GHz	1-15 Mbps	28100-36000 km	WANs, NANs, HANs	Low data rates
Wired	PLC	1-30 MHz	2-45 Mbps	1-3 km	AMI	Harsh noisy channels
	Fiber-optical	$3x10^8$ GHz	10 Gbps to 1600 Gbps	Unlimited (from 100 to 1000 km requires 1 repeater)	WANs, NANs	High investment cost
	Digital subscriber lines	240 kHz-1.5 MHz	256 Kbps to 10 Gbps	3 miles (requires 1 repeater)	WANs,NANs,HANs	Low data rates

need to spread over large geographical areas, including generation, transmission, and distribution to the consumer premises [49]. Fig. 2 shows an example of the SG with a three-tier communication architecture [12]. This communication architecture includes a WAN, a NAN, and a HAN. As shown in Fig. 2, the WAN provides communication links between the grid and core utility systems, and it connects geographically distant sites [12]. The NAN provides the connections between various devices such as intelligent electronic devices (IEDs), which control circuit breakers and transformers, and smart meters to local access points. The NAN connects several HANs. In the future, the NANs might be joined by various environmental sensor devices to perceive wide area situations. Finally, a HAN provides the access to in-home appliances and it connects the customer networks as well as utility networks within a home area [12]. In addition to the meters, it can include various energy-consuming home devices. The WAN, NAN, and HAN can be connected to the same core network or each of them (or a set of them) might have a separate core network.

To improve the efficiency, reliability, and sustainability of electricity services, SG uses communication technologies to exchange real-time data and information between the utilities and consumers [49], as well as to optimize the operation of interconnected power units. Various communication technologies are supported mainly by wired and wireless communications media. Table III shows an overview of various communication technologies in SG. The data and information exchange is critical in SG for system control and management. In a SG system, communication media are needed for delivering two-way information flows in HANs, NANs, and WANs. The first data flow is between electrical appliances, distributed sensors, and smart meters in HANs. This flow can utilize power line communications (PLCs) or wireless communications, such as ZigBee, 6LoWPAN, Z-wave, and others [50]. The second flow in NANs and WANs is from smart meters to the utility's data centers. The data flow delivery can be accomplished through cellular technologies or the Internet. However, the choice of communication technologies that suit one environment, e.g., rural or indoor environments, may not be appropriate to the others, e.g., urban or outdoor environments.

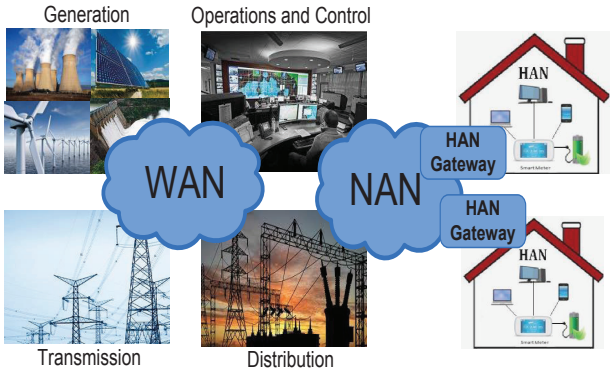

Fig. 2. SG with a three-tier communication architecture.

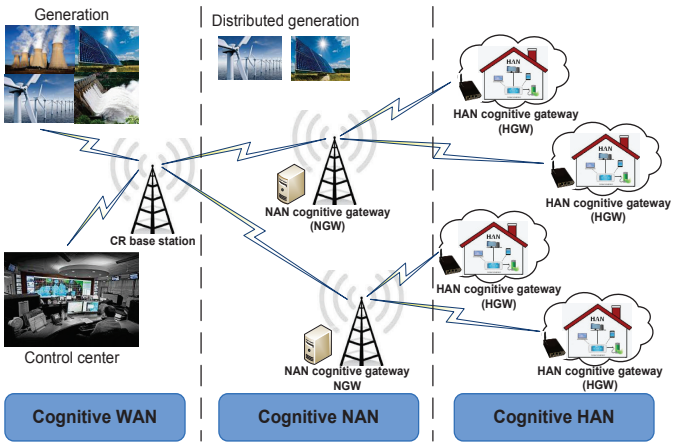

Fig. 3. CR-based SG communications.

IV. Overview on CR-based SG Architecture and Applications

A. CR-Based Smart Grid Architecture

Depending on the network characteristics of each tier, different wireless or wired communication technologies can be adopted, i.e., Zigbee, Bluetooth, or PLC for HANs in a small area, WiMAX, or WiFi for NANs with wireless mesh topology, and fiber optics or broadband cellular networks for WANs. However, these traditional communication technologies bear high costs for investment, operation, and maintenance [8], which are incapable to meet the requirements and challenges in SG. It has been recognised that CR is a promising technology to construct a more advanced communication infrastructure for SG [51]. The concept of applying CR technology to SG was first suggested by A. Ghassemi *et al.* in [12]. A comprehensive review on SG characteristics, architectures based on CR networks, and major challenges was presented in [14] and [17]. In [14], the authors proposed a CR-based communication architecture for SG as shown in Fig. 3. This architecture adopts a three-tiered hierarchical structure, which involves HANs, NANs, and WANs. It can support energy- and spectrum-efficient designs [52]–[55], also avoiding interference and adapting to data throughput requirements.

However, unlicensed operation suggests that reliability is a fundamental concern in SG communication infrastructure based on CR. To address this problem for communications between the three network tiers (i.e., HANs, NANs, and WANs), in [56], ISM frequency bands and leased bands were proposed to serve as backup spectra to ensure QoS requirements of data transmissions. Based on a rule that decides when to stop spectrum sensing and access to the ISM bands, the proposed scheme in [56] can reduce channel handoffs, thus guaranteeing reliability of communications for distributed generation systems. The QoS issues were discussed in [57], [58], [14], [17]. It is noted that machine to machine communication is a promising technology for CR-based SG. The work [59] designed a MAC protocol based on packet reservation multiple access scheme to support the coexistence of the cognitive and primary networks.

Table IV summarises the CR-based SG communication architectures, which are briefly described as follows.

1) Cognitive HANs

Fig. 4 shows the architecture of a HAN based on CR [14]. Typically, a HAN performs two necessary functions, namely commissioning and control. Commissioning is used to identify new appliances as they join or leave a HAN, and manage the joining or forming of a self-organizing network. The function of control is to guarantee interoperability and maintain the communication links between devices in a SG network. These communication links usually use ISM bands (such as IEEE 802.11 WLANs, WiFi, Bluetooth, and Microwave), and ZigBee is a default standard for HANs. Hence, ZigBee may cause interferences to other appliances also operating in ISM bands (see Section V-C). In order to solve the interference problem, cognitive HANs, which can incorporate CR with ZigBee standard (IEEE 802.15.4) to work on dynamic spectrum access, can be a good choice for this purpose. Besides, using dynamic spectrum access, cognitive devices in HANs can also use licensed bands when they are not occupied by their PUs. As a result, SG can effectively provide advanced services, such as peak-demand shaving, power cost reduction, customer satisfaction survey, power supply-demand match, and accurate power measurements. To ensure energy- and spectrum-efficient designs in cognitive HANs, the authors in [60] proposed to use wireless sensor networks with some key modifications in routing protocols for low power and lossy networks. To solve the reliability issues in [60], the authors in [61] designed an energy efficient and reliable MAC protocol for cognitive sensor networks using a receiver-based MAC protocol.

The HANs normally use a star topology with either wired communication technologies (e.g., PLCs) or wireless communication technologies (e.g., Zigbee, Bluetooth, and WiFi) to manage the communications within a HAN and the communications between different HANs in a NAN service coverage [62]. A HAN is composed of many smart devices. The center of a cognitive HAN is home gateway (HGW) [14]. Hence, a

TABLE IV
CR-BASED SMART GRID ARCHITECTURE.

Architecture	Technology	Bands
HAN	Zigbee, Bluetooth, WiFi, microwave, sensor networks	Licensed-free band [53] Hybrid licensed & unlicensed bands [57], [14] ISM & leased bands as backup [56] Sensor networks [60], [61]
NAN	Cellular, WiMAX, WiFi	Licensed band [53] Hybrid licensed & unlicensed bands [57], [14], [44] ISM & leased bands as backup [56]
WAN	Cellular, fiber optics	Licensed band [53] Hybrid licensed & unlicensed bands [57], [14], [12] ISM & leased bands as backup [56]

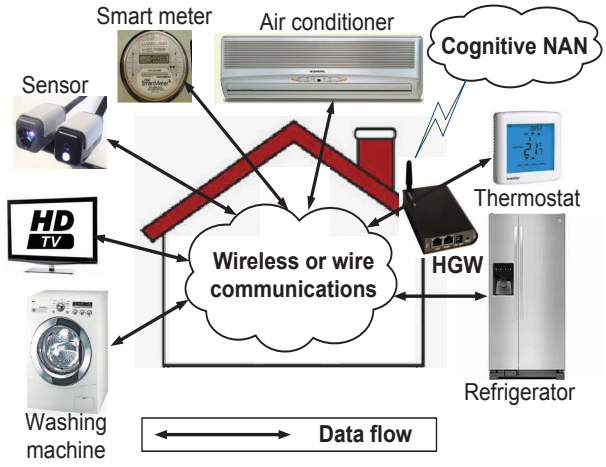

Fig. 4. Cognitive HAN architecture.

cognitive HGW is specially designed with self-configuration or advanced cognitive capability to autonomously adapt to various radio technologies via changing their transmitters' parameters. Besides, a HGW manages license-free spectrum bands, senses vacant frequencies of PUs in surroundings to utilize them, and provide optimal data rate subject to interference constraints. To improve the efficiency of spectrum usage in a cognitive HAN, an optimal solution to spectrum sharing among networked smart meters is necessary.

2) Cognitive NANs

As shown in Fig. 3, a NAN is on the next immediate tier of a HAN. A NAN will connect several HGWs from HANs through a cognitive NAN gateway (NGW), which acts as a cognitive access point to collect data from different HANs. A NGW is generally a utility pole-mounted device, a power substation, or a cognitive communication tower providing single-hop connection to the HGWs in a hybrid dynamic spectrum access manner [14], allowing HGWs to access both licensed and unlicensed spectrum bands. This novel access manner can improve the efficiency of spectrum usage in a cognitive NAN. Moreover, by using CR technology, the HGWs transmit data in licensed bands opportunistically to save the cost of leasing spectrum bands from a telecommunication operator. In SG applications, a NAN is responsible for collecting power consumption data from every customer in a neighbourhood and distributing the data to a control center of utility company through either open or private WANs. In the next subsection, we will discuss the issues on cognitive WANs.

3) Cognitive WANs

As shown in Fig. 5, several NANs constitute a WAN [14]. WAN is the upper tier of the SG communication architecture that provides broadband communications between NANs, SG substations, distributed grid devices, and electric utility companies. Using WAN, each NAN can exchange collected data and information with the utility control centers located far away [14]. Typically, a WAN consists of two interconnected networks, i.e., the core networks and backhaul networks [56]. The core networks provide connections to the control centers and commonly use fiber optics or cellular networks to guarantee high data rates and low latency. The backhaul networks handle the broadband connections to NANs and monitoring devices [12]. Applying CR technology in backhaul networks contributes to a reduction in investment costs and enhancement in the flexibility, capacity, and coverage. In the CR-based backhaul networks, each NGW is viewed as a cognitive node (SU) instead of an access point. A NGW has the capability of communicating with cognitive base stations (BSs) distributed over a wide area through licensed spectrum bands unused by PUs to enhance scalability. Fig. 5 shows a scenario, in which there are three NANs in a WAN with 11 licensed spectrum bands. According to different demands for data throughput, a spectrum broker may distribute five bands to NAN1 and six bands to NAN2. Since NAN1 and NAN3 are far away from each other, the spectrum broker will distribute five bands to NAN3, which is the same as those distributed to NAN1, provided that interference is not introduced.

B. Cognitive Radio Based SG Applications

Via integrating CR technology with power grid infrastructure, different types of data can be exchanged efficiently with varying security, reliability, and QoS requirements. They are critical to successful operation of the SG. In this section, several major applications in CR-based SG are summarized and discussed.

1) Distributed Generation Systems

Fast penetration of distributed renewable energy sources creates great challenges to the current power distribution infrastructure and operating procedures. The ways of controlling a conventional centralized generation facility may not be suitable for a distributed generation system. Moreover, power

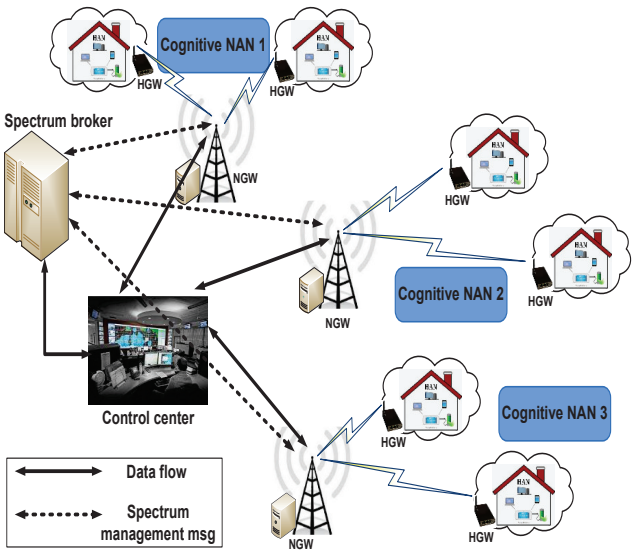

Fig. 5. Cognitive WAN architecture.

quality (reflected in voltage and frequency stability) is one of the system parameters that need to be measured for the continuity of power generation and storage operations. Due to a higher penetration level of distributed renewable energy sources, more advanced controls are required to maintain the stability and reliability of the whole power grid [63]. These controls include agile demand response, intelligent energy storage, and efficient data transmission, all of which rely on reliable and robust communication networks for distributed generation systems in SG.

A robust and reliable communication network is required for the overall distributed generation system integrity and safety. Wireless networks might be suitable for these kinds of applications because of their low cost and easy deployment features. However, several challenges exist for the integration of wireless nodes to a power grid, such as network contention, noise, obstructions, and interferences. CR networks can tackle these challenges and improve SG system performance through opportunistic spectrum access with maximizing spectrum utilization.

2) Automatic Generation Control

As mentioned earlier in Subsection I.C, communication failures may cause serious problems for both system operation and control in a power grid [26], and can interrupt the wide area damping control of power systems [27]. Consequently, the dynamic performance of AGC is also affected adversely. In a CR-based SG, when a SU is using a vacant channel of PU, if PU reclaims the channel, which may occur in a random fashion, the SU has to be squeezed out from the channel and it must immediately switch to another idle channel. Hence, the communications of SU will be interrupted if the idle channel is unavailable. The random interruptions of SU data traffic may cause packet losses and delays for SU data delivery, and it will in turn affect the stability of monitoring and control of a SG.

Therefore, it is critical to address the above problem and to understand the effects of random interruptions of SU traffic in CR networks on the stability performance of SG operation and control. In [32], state estimation of networked systems over CR networks and its applications in the SG were studied. By modelling a CR network as a semi-Markov process, the stability of a linear quadratic Gaussian (LQG) estimator was investigated. However, the effect of a CR network on AGC was not covered in this work. The authors in [56] addressed this problem and investigated the modelling and stability issues of the AGC in a SG, for which CR networks are used as the infrastructure for aggregation and communication of both system-wide information and local measurement data. For this purpose, a randomly switched power system model was proposed for the AGC in the SG in the design of CR networks to ensure the stability of the AGC.

3) Advanced Metering Infrastructure

Recently, advanced metering infrastructure (AMI) has gained a lot of attraction in both industry and academia due to its efficiency improvement in online meter reading and control. The AMI provides two-way communications between smart utility meters and utility companies [64]. The AMI includes smart meters, e.g., electric, gas, and heat meters, at customer premises, access points, communication backbone networks between customers and service providers, and data management systems to measure, collect, manage, and analyze the data for further processes. The smart meters can identify power consumption in a much more detail than conventional meters, and periodically send the collected information back to the utility company for load monitoring and billing purposes. In addition, the data from smart meter readings are also critical for the control centers to implement Demand Response mechanism. Using smart meters, customers can control their power consumption and manage how much power they are using, particularly managing the peak load. Hence, through customers' participation, the utility companies can likely provide electricity at a lower rate for all their customers, and the consequent carbon dioxide emission will be decreased effectively. Typically, the collected data from smart meters in AMI are huge and important, and it is estimated that a moderately sized city with 2 million homes could generate 22 GB of metering data every day [65], easily overwhelming the best planned data center capacity within a fairly short time. As a result, the communication backbone networks should be reliable, secure, scalable, and cost-effective enough to meet the requirements in terms of bandwidth and latency in data communications.

Several works investigated integrated communication technologies for the communication backbone of AMI. For example, mesh, Ethernet, and cellular AMI network topologies for SG were proposed in [66]-[70]. For the same reason, CR technology can be suitable for AMI communication systems [71]–[76]. The CR can contribute to AMI technology for self-configuration and easy deployment in coexisting wireless networks at different customer premises. With their spectrum-aware communication capabilities, AMI smart meters and equipment can be easily deployed at remote sites to achieve seamless and reliable communications between a utility con-

trol center and AMIs. The cognitive sensor network (CSN) nodes designed with a consideration of energy and price limitations in remote monitoring can be the main components for efficient realization of wireless AMI.

4) Real-time Pricing and Demand Response Management

CR and dynamic spectrum sharing are utilized to solve the spectrum scarcity problem and thus improve demand response performance and reliability of real-time pricing signals. Note that critical data such as monitoring and SCADA information will be transmitted over a dedicated network using licensed bands or wireline systems because of the strict real-time requirements. The dynamic spectrum sharing in CR is intended to be employed for relatively non-critical data, such as the information from smart meters. This frees up bandwidth in the dedicated networks for higher priority applications and thus avoids congestion there.

Based on real-time pricing signals from retailers to smart meters, the mobile service providers and customers can reduce power usage peaks by incorporating various communication technologies with intelligent control algorithms [77]–[84]. In [33], real-time pricing for demand-side management was considered in the SG, where multiple retailers provide real-time electricity prices to a heterogeneous mobile network based on CR technology. Based on a CR-based hierarchical communication architecture for SG as suggested in [14], G. Shah *et al.* utilized dynamic spectrum access to mitigate channel impairments, and proposed a distributed control algorithm for data transmission that maximizes the network utility under given QoS constraints [85]. The sensing performance tradeoff issue between control performance and communication cost was studied in [86] in a SG environment based on CR. However, the authors considered spectrum sharing only in time domain, i.e., the SG nodes opportunistically use the idle spectrum based on spectrum sensing. Thus, the spectrum utilization opportunities in spatial domain were ignored. In addition, SG nodes in different locations were assumed to have the same spectrum sensing capabilities, which is not the case in a real system. As an improvement, in [87], Q. Li *et al.* exploited the space-time spectrum utilization opportunities by using joint spatial and temporal spectrum sharing in order to better meet the spectrum resource and communication reliability requirements of real-time demand response management. To do this, a CR-based SG network was divided into two regions, namely a temporal spectrum sharing region and a free spatial spectrum sharing region. In the temporal spectrum sharing region, SG nodes can use the licensed spectrum when PUs are vacant; while in the free spatial spectrum sharing region they can simultaneously share this spectrum with the PUs without using power control.

5) Wide Area Situation Awareness

Wide area situational awareness is one of the most critical applications of the SG. There may exist many problems of communication networks, such as latency, interference, and overload, that will influence the safety, reliability, and security of a SG. Furthermore, distributed and large-scale nature of a wide area creates challenges for wireless sensors in terms of maintenance, difference in spectrum regulations, electromagnetic interferences, and fading. These will result in a need for advanced communications to ensure the reliability for accurately transmitting estimated state of the entire system. To this end, CR networks can improve the network performance in terms of wide area situational awareness and increase spectrum efficiency and capacity with advanced spectrum management functionalities, such as the ability of using different spectrum regulations, efficient spectrum utilization, and dynamic spectrum access.

6) Real-time Applications in CR-based SG Communications

To realize real-time applications, reliable and high-speed communication network is the key. Physical layer research works, such as advanced interference mitigation algorithms, advanced antenna techniques (e.g., MIMO), and advanced modulation and coding techniques, have paved a way to increase communication network capacity. Such research advancements have pushed the spectral efficiency of fifth-generation air interfaces (still under investigations) closer to system capacity limits [88]. To meet this high capacity demand for communication networks, CR technology is a promising paradigm for increasing spectral efficiency further. Moreover, to monitor and control SG in a real-time basis, we have to reduce vacant spectrum sensing time of SU using advanced algorithms, for example, real-time channel selection [89], and increase efficiency using licensed bands of PUs by scheduling adaptive transmissions for a large amount of data such as video streaming [90]. Such advancements in CR technology will help to meet the growing capacity demands of real-time applications in future SG.

V. Cognitive Radio Based SG Communication Standards

Generally, SG is a network of diverse systems, and it consists of a large number of components deployed in a wide area of the power systems via various communication networks. Hence, standardization of SG is an especially complex task, but it is extremely important to enable the integration of all the components in a seamless manner. For example, there are many industry sectors involved in SG standardization processes with different agendas, different levels of technical knowledge, and very different timelines for completion. In addition, because energy industry is highly regulated in most countries, the overlap or conflict between the standards and public policies means that politics will also be an important issue in the standardization processes. The implementation of SG should also be coordinated with governmental goals for national energy policies, national security, economic growth, and energy independence. As a result, they pose unique challenges to create a suite of standards for the SG.

Several review papers in the literature [9], [91], [92] discussed the standard issues in the context of emerging SG with CR. In [9], the authors described the standards for SG and provided a contemporary survey on the current state-of-the-art research in SG communications as well as the open issues in this field. Furthermore, in [91], a set of core

TABLE V
CR-BASED SG COMMUNICATION STANDARDS.

Cognitive WANs	Cognitive NANs	Cognitive HANs
[94], [12]	[95], [96]	[69], [70], [97]–[101]

standards were identified to suggest the most important topics for future research and development. Moreover, International Electrotechnical Commission (IEC) Technical Committee 57 Seamless Integration Architecture (SIA) was introduced and extended by the follow-up standards, which has become a SG standardization framework and has been included in several standards. IEC Technical Committee 57 SIA becomes the core standards for SG in terms of automation and power system management. In addition, the authors in [92] provided a survey on CR standardization activities, their past and present, and discussed the issues on future standardization efforts.

One of the key challenges is that a CR-based SG system does not have widely accepted standards, and this prevents the integration of advanced applications, including smart meters, smart devices, and renewable energy sources, and limits the interoperability between them [9]. Meanwhile, it is seen that CR techniques have been applied to many different communications systems because a lot of standardization works have been completed in recent years (i.e., IEEE 802.22 [93]), and more are in progress (i.e., IEEE 802.19, and IEEE 802.16). To successfully standardise CR-based SG systems, a critical prerequisite is the adoption of interoperability standards for the overall system. Seamless interoperability, robust information security, improved safety of SG products and systems, and a set of communication protocols are some of the objectives that can be achieved with SG standardization efforts using CR technology.

Table V summarises CR-based SG communication standards in three tiers of cognitive WANs, NANs, and HANs, which are elucidated as follows.

A. Standards for Cognitive WANs

Recently, IEEE 802.22 standard was proposed based on CR technology using available TV bands spectrum, which is called TVWS [94]. TV bands can provide a better broadband service for far-away users due to their superior propagation characteristics, which can improve the coverage and capability to penetrate buildings at a relatively low power level. The coverage area of an IEEE 802.22 network is far larger than other wireless broadband technologies, i.e., WiMAX, and thus it is a good solution for wireless broadband access in remote and rural areas. According to FCC regulations, cognitive devices (SUs) can utilize very high frequency (VHF) and ultra high frequency (UHF) channels to transmit data. The bandwidth of every channel is 6 MHz. The VHF channels occupy the frequency ranges from 54 MHz to 72 MHz, and 76 MHz to 88 MHz; while the UHF channels range from 174 MHz to 216 MHz, and 470 MHz to 806 MHz [94].

In SG, electric power transmission networks are generally far away from population centers, and as a result many of TV channels are expected to be vacant. The large coverage area of IEEE 802.22 cognitive WANs can be a great asset to provide connectivity in this environment. CR-based IEEE 802.22 is also appropriate for distribution networks. However, the channel characteristics in urban areas are substantially different from that in rural areas. Urban areas have a high density of customers. Hence, they have to accommodate high data rates in their wireless backhauls. The CR architecture has a unique advantage in this scenario due to its robustness and aforementioned performance enhancements. On the contrary, rural areas have widely distributed customers with a low density. Therefore, IEEE 802.22 CR system is also an optimal solution in this situation because it was designed for providing broadband connectivity in rural areas.

In [12], the authors proposed to use CR-based IEEE 802.22 standard in WANs for SG backhaul data flows. They suggested two different architectures for cognitive WANs, i.e., stand-alone radio and secondary radio, for SG communications according to specific circumstances and applications. They pointed out that a cognitive WAN works appropriately as a secondary radio, particularly in urban areas, and as a backup in disaster relief operations. When there exist higher capacity requirements hence with less available unused TV bands, cognitive WANs can opportunistically transmit non-critical SG data and work as a backup radio in case of a natural disaster or a security breach. In rural areas, there are more white spaces available in the TV bands, and they suggested that a stand-alone radio based on IEEE 802.22 can provide broadband access for utility backbone communications.

However, in both of their proposed architectures, transmission of SG time-critical data is still a big challenge because of inherent sensing delays and cognitive nature as specified in IEEE 802.22. Accordingly, the authors proposed a concept of dual-radio architecture for cognitive WAN transmissions, where one radio chain was used only for SG data transmission and reception, while the other chain was dedicated for spectrum sensing. The sensing radio constantly searches for new available channels, so that the transceiver chain does not have to postpone its data transmissions in order to seek for idle channels. By employing the proposed dual-radio architecture, a higher spectrum efficiency and sensing accuracy can be achieved, compared to a single-radio architecture, since spectrum sensing is performed all the time and thus a clear channel for SG data flow can be quickly allocated whenever required.

According to the discussions, it is convinced that their proposed CR-based WAN using IEEE 802.22 is well suited for SG backhaul networks and offers four benefits, which are listed and briefly discussed as follows.

- Soft capacity limit: The proposed CR-based WAN for SG communications has a soft capacity limit as it can opportunistically and dynamically use available TV channels to increase system capacity.
- Wide coverage area: The BS coverage area in the IEEE

802.22 standard is much larger than other 802 standards, which means that less BSs and hence less capital expenditure will be needed to implement CR-based SG communications.

- Fault tolerance and self-healing: The proposed architecture is inherently robust to failures because if one link is down due to natural disasters or security breach, a new connection can be established in a timely manner to maintain connectivity due to the fact that available channels are constantly sensed and found.
- Ease of upgradability: CR-based systems are implemented using software-defined radio (SDR) systems, which are usually implemented by means of software on a personal computer or embedded computing devices. Consequently, they are more flexible and can be easily modified through software upgrading.

B. Standards for Cognitive NANs

Cognitive NANs offer multiple advantages in terms of bandwidth requirements, deployment time duration, investment and operation costs, if compared to other wireline and wireless technologies. Currently, several standardization groups are working hard to merge CR technologies with NANs utilizing TVWS to support applications in SG, i.e., IEEE 802.22, IEEE 802.15, and IEEE 802.11af. IEEE 802.22 working group is in charge of the standards for wireless regional area networks based on TVWS with the coverage up to 10 km to 100 km. Hence, IEEE 802.22 could be used in both WANs and NANs. On the other hand, IEEE 802.15 study group was created to use TVWS for intermediate ranges. As a result, it is a good time to standardise cognitive NANs. In addition, IEEE 802.11af, which was approved in February 2014 [95], innovated IEEE 802.11 via amendments to allow wireless local area networks (WLANs) to operate in TVWS in UHF and VHF bands. The WLANs based on IEEE 802.11af standard were designed for the ranges up to 1 km, suitable for cognitive NANs and HANs.

Similar to other unlicensed devices, cognitive devices in NANs, e.g., AMIs, have to deal with interference or congestion issues, which may introduce new concerns on reliability and delay in SG communications. Therefore, they will limit the capability of unlicensed devices for real-time applications or time-sensitive control in SG. Cognitive NANs should go beyond dynamic spectrum access, develop self-coexistence mechanisms to coordinate spectrum usage, and may even prioritize spectrum usage according to the class of SG traffic, e.g., real-time versus non-real-time, emergency report versus demand response, etc. IEEE 802.19.1 working group is currently working on developing a standard for wireless coexistence in TVWS and can help mitigate interferences among cognitive NANs. Furthermore, cognitive NANs should also consider the ways to interoperate with other wireless technologies, such as wireless cellular networks, to make SG communications more resilient, scalable, and accessible. Especially, NAN devices in SG need to adopt a hybrid dynamic spectrum access scheme, which allows these devices to operate on both licensed and unlicensed spectrum bands as specified in IEEE 802.15.4g [96]. Such unlicensed bands may also be used by many other unlicensed systems. Thus, cognitive NANs should mitigate interferences from coexisting systems.

C. Standards for Cognitive HANs

Owing to versatile appliances in HANs, obviously, standardization is a subject of the utmost importance for communications among in-home devices. The market for smart appliances will be very limited if refrigerators and washing machines might one day lose their demand response capability due to different communication standards between utilities (e.g., WiFi vs. ZigBee). ZigBee (IEEE 802.15.4) [69], Wi-Fi (802.11a/b/n/ac) [97], and Bluetooth (IEEE 802.15.1) technologies use relatively low power with a relatively low cost deployment topology due to their use of ISM bands. ZigBee is ideal for energy monitoring, smart lighting, automatic meter reading, and local online monitoring applications as part of substation automation systems [98] and home automation. According to the works done in the US National Institute for Standards and Technology (NIST) [70], ZigBee and ZigBee smart energy profile (SEP) are the most suitable communication standards in SG residential network domain. Hence, these smart meters can communicate with ZigBee devices to control home appliances. The operation of ZigBee in unlicensed spectrum makes it easy to form a network based on a standardized protocol of IEEE 802.15.4 standard. Moreover, ZigBee SEP in intelligent home appliances can send messages to home owners, so that they can know the information of real-time energy consumption. ZigBee SEP supports advanced metering, load control/reduction, demand response, real-time pricing programs, real-time system monitoring for gas, water, and electricity utilities [70], [99]. Nevertheless, ZigBee has also its own shortcomings, i.e., its transmission distance is limited, the rate of data transmission is low, and its capacity to penetrate barriers is low due to its non-LOS transmissions. ZigBee may cause interferences to other appliances, which operate in identical 2.4 GHz ISM frequency band, such as IEEE 802.11 WLANs, WiFi, Bluetooth, and Microwave [70]. Hence, interference detection and avoidance schemes should be used to provide a reliable network performance. In order to solve the interference problems, an effective channel discovery algorithm based on carrier sense multiple access/collision avoidance (CSMA/CA) mechanism was proposed in [100]. Particularly, cognitive HANs, which can incorporate CR with standard ZigBee (IEEE 802.15.4) to work on dynamic spectrum access, can be a good choice for this purpose [101]. Besides, using dynamic spectrum access, cognitive devices in HANs can also use licensed bands when they are not occupied by their PUs.

VI. Security in CR-Based SG Communications

SG security is required to protect both communication networks and power grid, because these two systems need to ensure their availability of access as well as survivability in different scenarios. However, the security of communication networks and power grid differ in several ways. In

TABLE VI
SECURITY VULNERABILITIES IN FOUR DOMAINS OF SG COMMUNICATIONS [1], [102]–[104].

Common security objectives	Generation	Transmission	Distribution	Customer
Confidentiality [13], [107], [108] [117]	Confidentiality of utility proprietary information through the networks.	NA	NA	Breach of user privacy can lead to lawsuits.
Non repudiation [105]–[109]	NA	1) Unique keys for customers in AMI communications. 2) AMI transaction logging	NA	Mutual inspection with smart meters.
Availability [110], [118]–[120], [127]	Unavailability of information for demand response control.	1) Failure of the network to transmit fault/synchrophasor information. 2) Poor latency of synchrophasor information	Failure of the network to transmit fault information.	Failure of appliances through errors or malicious compromise of usage information.
Integrity [13], [111]–[115]	Poisoning of information for demand response.	1) Poisoning of synchrophasor data. 2) Byzantine failures of synchrophasor data. 3) Malicious propagation of false faults to disrupt system.	1) Poisoning of synchrophasor data. 2) Byzantine failures of synchrophasor data. 3) Malicious propagation of false faults to disrupt system. 4) Malicious tripping of relays and other nodes.	Billing fraud.
Authentication [107]–[109], [121]–[124]	Authentication to data storage and processing servers could be compromised.	1) Machine-to-machine authentication. 2) Repair person-to machine authentication.	1) Machine-to-machine authentication. 2) Repair person-to machine authentication.	Authentication built in smart meters could be stolen and/or compromised.
Authorization [105], [126]	Unauthorized access to critical systems.	Unauthorized access to synchrophasor/fault information (national security threat).	NA	Unauthorized access to user appliances through hacking of smart meters.

a communication network, latency needs to be limited and bandwidth needs to be guaranteed; while data manipulation (placement of false data), destruction of data, and unauthorized access should be prevented. On the other hand, security in a power grid needs to ensure reliability, power quality, and stability. Despite these differences, security between the two systems must be coordinated because the power grid and communication networks can be used to launch attacks against each other. For instance, because the power supply in SG will be controlled by instantaneous users information, manipulation of usage data could create a fictitious grid imbalance leading to voltage variations that can create large-scale failures. Similarly, if the state information of a grid is poisoned, the grid could be de-stablized with a potential for physical damage. Physical damage could occur through overheating of transformers and relays or through voltage fluctuations in appliances. In this section, we survey security objectives, and key security technologies for SG and CR-based SG.

A. Security Objectives of SG

In general, an electrical power system includes four domains, which include generation, transmission lines, distribution systems, and customers. To exchange information among the four domains, the SG utilizes various communication networks. The communications are the fundamental enabling technology that is ubiquitous in the SG, and it is expected to be a heterogeneous amalgamation of wired (e.g., fiber-optic, copper line, etc.) and wireless (e.g., WiMAX, microwave, satellite, etc.) media. There are several known threats to these media, such as jamming of wireless signals, damage to equipment (e.g., tampering or breakdown), spoofing of wireless routers via denial-of-service (DoS) or malicious data injection. While wired signals have additional security concerns, they can be affected due to the threats such as electrical storms, accidental damage, natural disasters, and sabotage. Historically, the major security objectives of an electric grid consist of availability, integrity, and confidentiality. However, the privacy of customers and utility companies is becoming an increasingly complex issue when the grid incorporates load management and smart metering. In [1], [102]–[104], SG security objectives were identified, including six common objectives as the most important issues for ensuring consistent SG operation, which include:

- Confidentiality: The data is transformed in such a way that it will be disclosed only to authorized individuals or systems, and it is un-accessible to any unauthorized entity.
- Non repudiation: Non-repudiation techniques prevent either senders or receivers from denying a transmitted message by ensuring that undeniable proof will exist to verify the truthfulness of any claim of an entity.
- Availability: The assurance that any network resources, such as data, bandwidth, and equipment, will always be available to any authorized entity and they are also protected against any incident that threatens their availability. One of the important functions of the availability is to

prevent DoS attacks, energy starvation, and selfishness.

- Integrity: The validation that the accuracy and consistency of distributed data in a network will be maintained and protected from malicious modification, insertion, deletion or replay. No unauthorized modifications, destruction or losses of data will go undetected. The integrity of data can be ensured by using cryptographic techniques.
- Authentication: The assurance that one user identifies another one or verifies the source of the origin of data in the network. With the help of authentication schemes, SG can prevent unauthorized users from gaining access to protected systems.
- Authorization: The validation that no entity in SG environment can access to the information or services beyond its authority. An access control will determine the access rights of every entity in the system.

Table VI summarises the major vulnerabilities in four different domains of SG. Among these security objectives, availability usually gets the highest priority in SG communications. Because the cyber infrastructure manages continuous power flows in a physical infrastructure, it must guarantee a high availability. Ensuring a high availability of power flows whenever needed is more important to most customers than ensuring that the information about power flows is confidential.

B. Key Security Technologies for SG

The authors in [105] discussed major security technologies for SG systems, including public key infrastructure (PKI) and trusted computing methodologies. Based on the security requirements of SG, the system structure, and required availability, the authors believed that utilizing PKI technologies together with trusted computing elements is the most desirable solution for SG security. The basic steps in utilizing a PKI are summarized as follows. First, in order to communicate with a secure resource (e.g., a relying node), the device (e.g., a certificate subject) sends a certificate signing request (CSR) to a registration authority (RA). The RA performs a validation function check to determine whether the requested bindings are correct or not. If the requested bindings are correct, RA signs the CSR and forwards it to the certificate authority (CA), which then issues a certificate. CA will issue the certificate and let the validation authority (VA) know the certificate information of the certificated subject at the same time. Later, when a device wants to access to a secure resource, it transmits a certificate to a reliable party, i.e., the secure resource. The reliable party validates the certificate, typically by requesting the certificate status from a VA. Eventually, VA will reply with a positive response if the certificate is valid. While PKI is known for being complex, the authors suggested that many of the items responsible for the complexity can be significantly simplified by including the following four major technical elements, namely PKI standards, automated trust anchor security, certificate attributes, and SG PKI tools. In [106], they suggested to use a novel technical element to reduce the complexity of PKI security, which is device attestation. The authors demonstrated that by including only these PKI elements into the overall security architecture, a comprehensive and cost-effective solution for SG security can be achieved.

A trusted computing platform is an comprehensive security plan that encompasses virtually all aspects of SG operations. The platforms and associated mechanisms in the trusted computing model are used to ensure that malware is not able to access to the software processing devices. The main functionality of trusted computing is to allow any devices, which want to join a grid network, to verify that authorized code runs on that system. The adoption of strict code signing standards by SG suppliers and operators was also suggested in [105]. Mechanisms for enforcing such standards have been put forward by the Trusted Computing Group and have been also well documented and available in the literature.

Several works in the literature pointed out that SG security solution requires a holistic approach including PKI technologies based on industry standards and trusted computing techniques. They also concluded that PKI technical elements, for examples, certificate lifecycle management tools, trust anchor security, and attribute certificates, are the existing technologies that can be tailored specifically for SG networks, resulting in an efficient and effective solution. To achieve their vision for the proposed secure SG networks, the authors in the works suggested that the primary step that should be taken is to develop a cohesive set of requirements and standards for SG security. For more works about the security issues in SG communications, please refer to [107] and [108].

The authors in [110] articulated the security threats to transmission and distribution (T&D) automation systems. They mentioned that vulnerabilities in power T&D automation systems exist at multiple levels, including components, protocols, and networks. An attack process involves three steps: access, discovery, and control [110]. First, the attacker gains access to a SCADA system through a connection with a corporate network or through a virtual private network (VPN). Subsequently, the attacker studies the behaviours of the system and finally launches an attack. The authors pointed out that the current security solutions are focused mainly on information technology (IT) but not control systems, and that there are different needs for them, making IT security solutions ineffective to control systems. They suggested to decouple the controls from security in order to make it accessible for legacy systems that do not have inherent security. Their work is mainly a conjecture without clear evidence or comparison with other approaches.

Other works suggested the use of a dynamical graph theoretical analysis for understanding the impact of cyber threats on a physical electrical grid [111]. They emphasized the importance of modelling the cause-effect relationships between cyber data and electrical grid state signals as they are related to the power delivery metrics. Such modelling allows a deeper understanding of the threats that manifest at the interfaces between the cyber and physical systems. Unfortunately, modelling such interactions even in the simplest system is extremely cumbersome, making this endeavour infeasible. If generic patterns of interactions can be abstracted, then this approach might become practical.

Because the stability and synchronization of the grid operation depend strongly on the data in the grid, data poisoning and false injection attacks remain to be the major concerns of SG security. Recent research works showed that carefully designed attacks with or without the knowledge of grid topology [112], [113] can bypass a bad data detection (BDD) system, which is used to ensure the integrity of state estimation to filter out fault measurements introduced by device malfunctions or malicious attacks. Besides, the authors in [112] showed how an attacker can exploit the configuration of a power system to introduce arbitrary errors in the state estimation, while bypassing the existing techniques for bad measurement data detection. They investigated two specific cases: 1) an attacker is constrained to a set of meters due to the physical protection of the meters, and 2) an attacker has limited resources to launch attacks against the meters. The authors' simulations showed that, despite the possible limitations, attackers will be able to compromise the state estimation in both scenarios. Other works investigated defence mechanisms against false data injection attacks via protecting a few carefully selected measurements [112], [114], [115]. They showcased both optimum and reduced-complexity sub-optimum algorithms for protecting data integrity and demonstrated them by physical experiments.

C. Key Security Technologies for CR-based SG

There are standard security techniques for dealing with each of these threats, as discussed earlier. However, an absolute security scheme does not exist in SG systems based on heterogeneous communications. CR-based SG can overcome the problems because the security technologies in CR networks are matured and standardized. Hence, CR-based SG provides improved grid stability and reliability. The key to achieve this is to securely share important measurements, such as synchrophasor measurements gathered by PMUs, among power grid entities over WANs with standard CR networks, i.e., IEEE 802.22 [116] and SCC41 [92]. Typically, such securely sharing follows entities' policies, which depend on consumer preferences, data generator, and time-sensitive contexts. For example, entities will more likely share the information during an emergency event. Working with the standards will be extremely important to ensure a highly secure, scalable, and consistent SG system in the future, as these standards will ensure the security requirements of SG based on CR. In [117], Sherman *et al.* suggested that the type of information to be accessed, QoS, and security requirements for data streams should be considered in CR scenarios according to IEEE standards. CR includes highly flexible devices that can self-configure many of their parameters to optimize communications in the network by optimizing spectrum usage.

Clearly, since CR technology has been introduced into SG communications, there come new forms of attacks, mostly on physical layer [118]. For more works about security issues and the countermeasures for various attacks on CR networks, please refer to [119] and [120]. In the literature, it is seen that the most common attack on the physical layer of CR networks is the primary user emulation attack (PUEA). The PUEA may masquerade as a PU by transmitting special signals in the licensed band, thus preventing other SUs from accessing that band. The PUEAs transmit only on the channels that are not used by PUs. Therefore, SUs regard these attackers as PUs and do not try to access the channels that are not used by PUs. The methods to defend against PEUA have been extensively investigated. In [121], the authors utilized a transmitter verification scheme called localization-based defence (LocDef) to detect the PUEAs. This scheme verifies whether a received signal at SU is that of an incumbent transmitter by estimating the location of this transmitter and observing its signal characteristics. In a practical case based on IEEE 802.22, the PUs can be TV signal transmitters (i.e., TV broadcast towers) and their receivers. Their locations are typically determined. If a malicious user wants to emulate the PU and its location is almost the same as the PU, SUs will not receive the signal of the malicious user since the transmit power of the malicious node is much lower than a TV tower. If a SU receives a high power signal from a malicious user, it means that the malicious user must be very close to the SU. Thus, the SU can determine whether a transmitter is a PU or PUEA, just by estimating the location of the transmitter.

However, as the users are moving nodes, the LocDef may not be able to identify PUEAs and PUs at PHY layer over multipath Rayleigh fading channels [122], [123]. Hence, the work in [124] proposed a solution to identify PUEAs via exploiting channel-specific features in mobile CR networks. To improve detection efficiency, it proposed to use Neyman-Pearson test and sequential probability ratio test (SPRT) to distinguish PUs from PUEAs over multipath Rayleigh fading channels at low signal-to-noise power ratios. The main contribution of this work is to combine the advantages of quick detection on PHY layer with those of the cooperative detection of PUEAs based on the proposed channel-tap power estimation. The change of channel-tap powers depends on the mobility of transmitter and receiver pairs, which are utilized as a radio frequency fingerprint to detect PUs and PUEAs in mobile CR networks. Additionally, by using the channel-tap powers, the proposed detection method is insensitive to the unknown phase of channel impulse response. Although the proposed scheme can quickly identify a PUEA by PHY layer detection mechanism, the result of detection for a single node may still be inevitably influenced by many other channel factors, such as shadowing and random fluctuations of small-scale fading. Therefore, the cooperative detection schemes were devised using fixed sample size test (FSST) and SPRT. Notably, this cooperative detection based on channel-tap power can mitigate the effects of wireless fading channels, enabling the use of low-complexity individual detectors to shorten the detection time. Moreover, cooperative detection increases the probability of detection in non-scattering-rich environments. However, cooperative sensing is vulnerable to sensing data falsification attacks. A two-stage scheme to overcome such an attack was proposed in [125].

The authors in [13] designed CR-based SG using hardware platforms, such as Virtex-5 and Virtex-6 field programmable gate array (FPGA) of Xilinx, and proposed a network testbed to evaluate security capability of the CR-based SG. The major concerns on hardware platforms for CR networks are

computing power and response latency. This work proposed a hardware architecture to address these two concerns based on detection and learning algorithms. The results showed that the CR-based SG requires a much higher computing power. Hence, increasing computing power and reducing response latency can help to enhance security. Besides, the authors in [126] proposed FPGA-based fuzzy logic intrusion detection to enhance the security for CR-based SG. In this method, different variables that influence the inference of an attack are analyzed and combined for the decision-making process of a security device.

From aforementioned discussions, based on the knowledge, solutions, and standards for CR technology, CR-based SG is very promising for future SG implementations because heterogeneous communications in SG are replaced by the CR technology, which has been standardized with the consideration of security issues. With the help of CR technology, the capacity of a network backbone can be increased up to 18 Mbps. Furthermore, electric systems can benefit from CR technology to improve the performance of their communication systems, since CR is characterized by its capability to cover a long distance. A large coverage as well as a sufficiently high data rate makes the CR-based SG particularly suitable for wireless automatic meter reading (WAMR) as part of utility automatic metering infrastructure [127]. CR can be used to provide real-time pricing information based on real-time energy consumption of the customers and provide different QoS requirements for electric systems in an economical manner. Major benefits of CR-based SG include improved communication reliability, lower installation costs, larger network coverage, and better network connectivity.

VII. Enabling Techniques for CR-Based SG Communications

In this section, we are engaged to identify the possible technologies that can tackle the challenges to implement CR-based SG communications.

A. Reliable Communications between Networks

1) Communications between cognitive HANs and NANs

In order to facilitate the communications between cognitive HANs and NANs, we suggest to use the following techniques.

- Hybrid spectrum access to extend the coverage of WANs: As spectrum holes of the licensed bands may not be enough to transmit a massive amount of data, the communications between HANs and NANs may temporarily operate in the license-free bands (i.e., ISM bands) at a lower bit rate. In this way, the performance could be maintained close to that of the existing infrastructures in the worst-case scenario. As a result, data transmissions between HGWs and NGWs can be conducted using a hybrid spectrum access scheme, so that the communications between HANs and NANs can be made more reliable. Here, the HGWs are considered to be cognitive nodes and responsible for spectrum sensing in the communication networks. The HGWs conduct spectrum sensing to find unoccupied spectrum bands. However, if sensing time is too long, data transmission time will be reduced, which will impair the throughput of the networks. Thus, there is a time instance, at which the HGWs should give up searching for an unoccupied licensed band and access to the ISM bands directly for data transmission. A policy to decide when to stop spectrum sensing and when to access ISM bands was proposed in [56] according to the expected throughput performance. In this case, ISM bands are introduced as backup bands for communications to improve service reliability of SG applications. If this situation happens frequently, more NGWs can be installed to utilize space diversity.
- Shorten delay for real-time applications: In cognitive HANs, neighbouring cells are combined to reroute real-time data traffic [34] with priority-based traffic scheduling for CR-based SG according to various traffic types [35], such as control commands, multimedia sensing data, and meter readings, to reduce delays of traffic and ensure real-time capability. Besides, in cognitive NANs, self-coexistence mechanisms should be developed to coordinate spectrum usage and priority spectrum access according to the class of SG traffic, e.g., real-time versus non-real-time, emergency report versus demand response, etc. Furthermore, cognitive NANs should also consider how to interoperate with other wireless technologies, such as wireless cellular networks, to make SG more resilient, scalable, and accessible.
- CR-based AMI self-configuration: As part of the end-user facilities, AMIs can also be efficiently realized with the help of CR technology. Using CR technology, AMI can self-configure in order to coexist with other wireless networks at different customer premises. With their spectrum-aware communication capability, AMI meters and equipment can be deployed easily at remote sites to achieve seamless and reliable communications between a utility control center and AMIs. This is a major opportunity for efficient implementation of wireless AMI in remote monitoring.

2) Communications between cognitive NANs and WANs

To ensure reliable and scalable communications between cognitive NANs and WANs, we identify the approaches as listed in the sequel.

- WAN coverage area extension to improve reliability: First, we can use hybrid access modes of licensed and leased bands to extend the coverage area of WANs and improve service reliability. The utilities can lease some radio bands, which are used as backup bands, at a low cost from a telecommunication operator. The hybrid access mode between the leased and licensed bands is intelligently scheduled and seamlessly switched, so that it can improve QoS of data communications, thus benefiting both utilities and users. In this sense, NGWs are considered to be cognitive nodes to conduct spectrum sensing in communication networks. The NGWs will choose leased bands to communicate with BS after a certain period of sensing time, while still searching for vacant spectrums to use them opportunistically. When

transmission rate of the leased bands is higher than that of cognitive licensed bands, SUs will stop spectrum sensing and access to the leased bands to transmit collected data. On the contrary, if transmission rate of the leased bands is lower than that of cognitive licensed bands, then SUs will find vacant spectrums and access to the licensed bands to transmit data for achieving a higher throughput. However, the number of the leased bands may be very limited and they also serve as backup bands for critical data transmissions in emergency situations. Thus, the NGWs should conduct spectrum sensing periodically and have to release the leased bands once a vacant spectrum band is found. In NANs, the available unoccupied spectrum bands are scarce in urban areas, while abundant in rural areas, because the amount of data traffic in urban areas is much larger than that in rural areas. Therefore, the number of leased bands, which are distributed to a NAN in urban areas, should be more than that distributed to a NAN in rural areas. Moreover, a leased spectrum band can be shared by several NANs without causing interference to each other if the service area of a WAN is very large. Similarly, the leased bands can be utilized as backup bands for communications to improve service reliability of SG applications.

Second, we can use cooperative communications to extend the coverage and improve service reliability. Other available wireless and wireline technologies, such as wireless cellular networks, the Internet, and fiber optics, could also interoperate with cognitive NANs and WANs to make SG more resilient, scalable, and reliable in an economical manner. For example, currently, the mobile communications have been implemented via both cellular networks and IPv6 mobile ad hoc networks (MANETs). We can utilize MANETs to transmit non-critical data. In [128], the authors proposed to use CR ad hoc networks as an infrastructure of SG communications to transfer dependable data simultaneously in SG and help disaster relief teams for making timely decisions based on SG data and other sensory information.

Recently, to meet the requirements for mobile multimedia communications in CR-based SG, small cells have been proposed and implemented to increase coverage with a higher data rate [81]. Due to their small coverage areas, BSs of small cells not only require much less transmission power than that of macrocells, but also are much more energy efficient in providing broadband services [129]. However, we have to use a large number of small-cell BSs to increase the coverage area. For this reason, the handoff frequency of mobile users going across cells also increases. As a result, performance of the whole CR-based SG could be degraded. Hence, we should consider to use some advanced handoff protocols with delay constraints to cover a large area reliably.

- Scalability: The CR technology creates an opportunity to increase scalability at a low cost. For example, a base station coverage area for IEEE 802.22 can be 33 km if power level of customer-premises equipment (CPE) is 4 W, and it can be extended to 100 km if higher power levels are allowed [12]. IEEE 802.22 standard was developed to bring broadband wireless access to wide-range rural areas operating in TVWSs from 54 MHz to 862 MHz, on a non-interfering basis with the PUs. It carries unique features, e.g., spectrum sensing, geo-location, and intra-system coexistence for CR-based operations.

B. Standards

First, the global community needs to agree on a single high-level architectural model to understand and develop the standards across different regions and standard groups. For instance, we cannot standardize the interface between an outage management system and a demand response management system if we do not agree on their technical specifications and interfaces.

Second, on PHY and MAC levels, we have to accept that we still see a necessary fragmentation in multiple technologies based upon reliability and cost constraints of the applications. We need further standardization works to reduce the number of unnecessary competing standards that share the same basic technologies and functions. Many SG applications, especially those located near to or in homes, cannot bear the cost of supporting multiple PHYs or gateway technologies to bridge them. We need to create common MAC/PHY standards that are widely accepted and that will remain stable for decades rather than months. Resolving this fundamental issue will make the design of demand-response systems a success.

Third, since different communication technologies and different standards for each of SG components will be used to exchange information independently from manufacturers or any type of physical device to meet the specific QoS requirements. These communication technologies may require to operate on different spectrum bands. Hence, CR technology should accomplish overall coordination between complex, different, and far-away SG components, which is a very difficult task and imposes a great challenge to CR technology for SG applications. Standard based and interoperable communication protocols can be good options to use CR technology to implement such a complex communication infrastructure. Moreover, message formats and rules (at a minimum around granularity, privacy, and usage) for interchange of information between utilities and consumers need to be standardized and made stable again for a long period of time, because many devices do not have upgrade capability. In addition, we need to develop the standards that define solutions for problems, and the standards that define the open platforms to deal with security problems and to ensure communications between multiple proprietary products.

Finally, user interface standards need to be agreed upon for in-home devices, and these interfaces need to be simple to operate. Otherwise, installations by consumers will not be easy if the installation of each device will need to read a big manual.

C. Security

1) Security analysis

It is important to develop a risk/security analysis process that can autonomously detect faults to limit the damages to the CR-based SG communications.

In addition to the analysis of causes and effects of different threats on the electric grid, we need to establish comprehensive failure scenarios that include the impacts of multiple threats simultaneously. The risks include those associated with interactions among cyberspace and physical systems. It will not be possible to consider all possible combinations of threats. Consequently, an automated test system taking into account different failures (attacks) in both cyberspace and physical systems will be an important additional source for mapping all of the threats and studying their behaviours. Contingency analysis is already performed for analyzing the stability of the grids. However, that will need to be extended to incorporate the risks due to threats coming from various communication networks. More precise detection techniques that use multiple factors for accurately predicting threats will need to be devised to reduce false-alarm probability. Based on the previous risk analysis, the algorithms can autonomously detect the faults in CR-based SG communication systems to limit the damages caused by degraded security performance.

2) Security standards

On the other hand, international security standards are also needed for CR-based SG communication. Currently, there are numerous independent efforts to develop security standards and legislations. Security standards being developed need to be future-proof, considering futuristic applications, operations, and energy markets. Standard test scenarios need to be developed for the people developing the algorithms, as well as for equipment manufacturers for detecting security attacks and failure scenarios at the interfaces between power grid and communication networks. Moreover, we should establish standardized testing requirements for the security in all applications and protocols for CR-based SG. It is also essential to create auditing systems to ensure compliance with security legislations for utilities, equipment manufacturers, and energy generators for local, national, and regional regulatory bodies.

3) Quantum key distribution in CR-based SG

The use of quantum key distribution (QKD) can help improve the security of communications in a CR-based SG. Quantum communication is an emerging technology with potential applications to the power grids. QKD has been proposed as an approach to improve the security of communications between the power grids, and it could be implemented over existing fiber-optic channels and free-space optical communication links, within generation systems and power distribution networks. Quantum communication employs a fundamentally different technique from most of traditional communication technologies, and it works based on the physics of entangled quantum states as a fundamental resource. The classical cyber security techniques depend on physical protection of communication channels, and they need complex computation techniques to encrypt transmitted data and protect its confidentiality. The observation of quantum communication measurements fundamentally disturbs the system, alerting the receiver for the changes in the channel. QKD has rapidly matured and is now providing commercial applications by several companies around the world. Researchers are exploring its applications in more challenging and interesting scenarios, including the SG. One potential usage in the SG is quantum location verification. As today's power system components tend to be stationary, quantum communication techniques could potentially be used to improve the security with regard to the identification of the location of a transmitter. This adds another level of security by ensuring that a transmitter placed at a fixed location in the power grid is truly at that location and is not being spoofed. There are many other potential applications of quantum communication techniques that might become useful to ensure the security in power grids [1].

4) Real-time control theory

Real-time control theory should be applied efficiently to the communication networks. Variations in latency have to be tolerated without making the control systems unstable. Also, control algorithms should become more distributed, and its focus should be put not only on traditional goal of stability, but also on cyber security and fault tolerance.

5) Cross-layer design for attack detection

Cross-layer design for attack detection in CR-based SG is another new research topic. To realize a secure CR-based SG communication system, security should prevail every other aspects of the whole system design, and be integrated into every system component. SG security includes the protection of both communication networks and power grids to ensure availability and survivability. The detection techniques based on higher-layer introduce an overhead in the network, which could potentially affect timely delivery of critical messages in the SG, resulting in instabilities. Thus, our earlier work proposed a cross-layer design for PUEA detection without burdening the networks with extra overhead [130]. In this work, to identify PUEAs and PUs definitely on PHY layer over multipath Rayleigh fading channels [122] in mobile CR networks, cross-layer intelligent learning capability of SU was exploited to establish RF fingerprint databases by combining the accuracy and capability of higher layer authentication [131] with a quick detection algorithm on PHY layer [124].

VIII. Open Issues and Challenges in CR-Based SG Communications

In this section, challenging issues in CR-based SG communications are identified in three areas, including communications between networks, standards, and security.

A. Communications between Networks

1) Communications between Cognitive HANs and NANs

The challenges to implement communications between CR-based HANs and NANs are identified as follows.

- The lack of spectrum holes of licensed bands for data transmissions from smart devices: In CR-based SG networks, the communications between HANs and NANs are realized by connecting HGWs and NGWs. A NGW connects many HGWs from various HANs using licensed

bands in an opportunistic manner. However, a SG system may generate vast amount of data coming from smart devices. Hence, it might happen that there are no enough spectrum holes of licensed bands to be used for the data transmissions, as there might be the times or locations where vacant bands are not available. Moreover, a great challenge in HANs is to interwork various customer equipments provided by different manufacturers using different standards such as WiFi, Zigbee, wireless regional area network (WRAN), and Bluetooth.

- Traffic delay and real-time capability: Bidirectional data transmissions between NANs and HANs must meet real-time requirements. The data transmissions in SG involve many types of data, which have different levels of time requirements. For example, the real-time data exchanges between IEDs and other power devices in a large distributed area should ensure that all decisions are made by the control centers in a timely manner, such as controlling or monitoring data, so that demand response can be realized in the customer ends; whereas some other data are transmitted in a periodic manner, such as power consumption data of households. The various types of data also bring in a major challenging issue due to low-speed transmission characteristics and inherent sensing delays of CR. Moreover, the SU in CR must continuously monitor radio spectrum usage to give the precedence to the PU. Therefore, the random interruptions in SU traffic will unavoidably cause packet losses and delays in sending SU data. As a result, the communications in a CR network are normally unreliable, and it is a major issue to support real-time applications.
- AMI self-configuration: HANs connect many smart devices to achieve optimum energy consumption and to implement demand response and AMIs. Smart meters, energy management systems, and smart devices installed in all customer premises are parts of the AMI. The AMI will enable these smart devices to communicate with the utility operation control centers to control their operations at a given time and thus implement demand-side management for the utility. However, the number and characteristics of the smart meters and devices may change randomly according to the preferences of customers, who can install new smart meters and devices or remove old smart appliances in an unpredictable manner. Hence, the AMI must have self-configuration ability to ensure online update and effectively monitor the random changes of these smart appliances.

2) Communications between NANs and WANs

The challenges to implement communications between CR-based NANs and WANs are identified in the sequel.

- Limited WAN coverage area due to the use of ISM bands: The communications between NANs and WANs are established based on cognitive BSs. Hence, there is also the problem of a possible licensed band shortage for opportunistic access. However, the ISM bands are not suitable for the communications between NANs and WANs because the coverage area of WAN is larger, while the ISM bands are suitable for short-range transmissions.
- Service reliability using TVWS to connect NANs and WANs: Another serious issue on using TVWS to connect NANs and WANs is service reliability. In spite of diversity algorithms, such as dynamic frequency switching and multi-channel utilization, which may provide the solutions to the reliability problems, the SU using TVWS is considered as a fundamental issue, in which the connections in TVWS must postpone its operations upon detecting the existence of an incoming PU. How to mitigate the unreliability caused by inherent cognitive characteristics of SG communications in the licensed bands remains to be an open issue.
- Scalability: The scalability feature of wired communication technologies for WAN connections in SG is limited because of high installation and maintenance costs. Hence, for wide area communications, wireless technologies are preferred because of its flexibility. However, scalability in wireless technologies is provided by adding more wireless access points and routers to the network, which will also increase the installation costs.

B. Standards

1) Requirement for a universal standard for secure CR-based SG communications

The success of CR-based SG depends largely on uninterrupted communications of its entities. With each sub-network in the SG having its own devices, its own capabilities, and its own requirements, ensuring the interoperability and uninterrupted communications between SG entities becomes a rather difficult task. Hence, a universal standard framework, whose functions include developing guidelines, protocols, and model standards for secure communications between the entities in different sub-networks of CR-based SG, is essential. Such a universal standard framework for secure communications in CR-based SG will contribute to meet the unique requirements proposed by specific SG subsystems.

2) Call for novel interoperability standards

To implement SG and ensure the interoperability among its entities, we need to take a novel approach. The traditional approach of developing standards individually first and then creating another standard to unify them will never give us the optimum results and may waste a lot of efforts. Certainly, in the US and Europe, the deadlines based upon politics, rather than engineers or project managers, have been mandated. This practice may not yield good solutions and will slow down the process and reduce the effectiveness of interoperability. Fortunately, at least some of those in the IEC process seems to work to meet the deadlines. It seems that globally harmonized standards will unlikely be created and adopted for CR-based SG within a short time. What is more realistic is to aim for establishing common models and common basic architectural rules that support interoperability, rather than theoretical interoperability.

3) Regional differences in electric grid topology

Because regions vary in their implemented topology of their grids, some technologies simply work better in some

regions than in others. For instance, power line communication technologies are much more efficient in low voltage-centric grids, which are popular in most countries of Europe but not in the U.S. The differences within a region, and even within a utility company, often mean that multiple technologies must be used to resolve interconnection issues.

4) Design of new protocols for SG

The stringent requirements of some of sub-networks in SG systems are partly the reason why the SG demands for redesigning the existing protocols. CR-based SG standards should be characterized by the flexibility needed for meeting their functional requirements. For example, IEC61850 standard for communications in a substation ensures that critical messages, such as an islanding command for fault isolation, will not experience delays of more than three ms. If this requirement is not satisfied, it will put the entire substation equipment at risk. In practice, any protocol used in a CR-based SG for data aggregation, secure communication, authentication and so on, has to be designed to meet SG's unique requirements.

5) Time-proof backwards compatibility

The members of world standard organizations believed that the SG should be backwards compatible with all existing technologies, including legacy systems, software, and interfaces, such as dial-up networks, MS-DOS, and serial ports. Clearly, this compatibility cannot be accomplished while allowing significant progress in the deployment of new technologies. The difference between setting up the standards that enable a future development path and establishing compatibility with all existing technologies seems not to be well understood by some parties of concern.

It is not a good option to deploy the technologies with critical functions to manage the grid, and then discontinue the manufacture of those devices because newer technology has been introduced. Technologies chosen to be the core of the SG need to have a long product life, and future versions need to be made backwards compatible. The questions of backwards compatibility with non-SG standards and the backwards compatibility of SG standards with its previous versions are very different and should not be confused.

6) Business and political barriers on the way to standardization

Utilities must make investment decisions on SG products with a very long life-cycle. Remember that SG is not an industry producing the products with their replacement life-cycles being only six months or two years, but the one with 20 or 30 years life span. Therefore, an evolutional path must be well planned, to avoid the trial-and-error approaches used in many telecommunications products.

As the members of world standard organizations have their different agendas, the people with skills in one area probably want the technologies they developed and know well how to make them survivable in the next years. Aside from the business barriers in the ways to develop standardizations, there are a lot of political issues in place, as different countries, states, consortiums, and other entities strive to be the leaders in the standardization processes of the new technologies, and gain competitive edge by adding their technologies into the standards.

C. Security

1) Difficulty to identify large-scale catastrophic failures

In CR-based SG security, the primary challenge stems from a high level dependence between grid components, such that seemingly independent random events can aggregate to yield large-scale catastrophic failures in the grid. High complexity in systems increases the probability of flaws, and unintended access points increase the possibility of attacks induced failures, especially in an adversary model, in which attacks are readily replicated, thus propagating the failures. In addition, new entities, such as electric vehicles and DER, are expected to be incorporated in the grids. However, researches on security raised up by the incorporations have received very limited attention. Hence, it is very difficult to identify and address the issues on new failure modes in such systems before they become large-scale problems.

2) Dependence between electric grids and communication networks

We understand the threats to the communication networks and power grids, and we understand to some extent how the threats associated with the SG communication infrastructure impact on the power grid. However, it is unclear how the threats in the power grids can affect the communication networks.

3) Difficulty to change the mindset of utilities about reliability

The mindset of utilities is still focused on reliability under natural disasters, instead of the security threads from a determined adversary. Additionally, the nature of services to the end customers is evolving under a mindset of functions (such functions are sometimes provided by the third parties, not the utilities). It is important to build up a set of regulations that define a clear line between which can be protected by the utilities and which cannot.

4) Challenges to detect network based threats

The most serious challenge comes from the ubiquitous connectivity in the equipment, software, and controls in the grids. Network based threats may propagate quickly to overwhelm the whole network. In addition, the universal connectivity and multiple access points make the system more vulnerable to attacks (such as DoS). We need to rely on automated detection schemes to respond to network based threats.

5) Intrusion detection, prevention, and recovery for CR-based SG

Typically, PUEA induced DoS and distributed DoS are two most dangerous attacks against a CR-based SG. If such attacks can not be detected and quarantined early enough, it will risk the failure of the functionality in most critical infrastructure and threaten the whole CR-based SG. Hence, we need new methods for risk assessment based on prior knowledge in order not to introduce further delays in the overall system. Besides, in case that an attack can not be identified and prevented, appropriate intrusion recovery techniques must be implemented to remedy the consequences of the attacks on the critical infrastructure.

6) Key management techniques for AMI and wide area measurement networks

Today, the majority of key management schemes were proposed only for secure communications within the SG, to address the issues on key establishment for the communicating entities within SCADA systems to protect critical messages, such as near-real time information, pricing signals, and feedback data regarding energy consumption of customers. In fact, very few studies have been carried out on key management schemes for the AMI and wide area measurement network entities. Hence, in the future, researchers should focus on the proposal of novel key management techniques specifically designed for the AMI and wide area measurement networks.

IX. Conclusions

In this paper, the CR technology for SG communications has been identified as an important technique for futuristic SG implementations, and the state-of-the-art research activities in this area have been reviewed. To implement CR-based SG in the years to come, the problems of security and standards for communications in CR-based SG have to be identified and solved first. Hence, the issues on standards, security, and communication architecture in CR-based SG have been discussed. To tackle these challenges, possible technologies to implement CR-based SG communications are surveyed and proposed. Future SG should use intelligent monitoring systems to keep a track of all electricity flows and collected data streams from a large number of smart devices. Hence, it must be flexible and resilient to accommodate newly emerging applications in an economic manner. To achieve this goal, CR technology will certainly play an important role in SG communication infrastructures. Moreover, with the help of CR technology, SG communications can support various types of traffic including multimedia, particularly real-time data delivery with stringent QoS requirements. With the CR technology, SG should preserve its interoperability and secured communications within a hybrid system, where both new and legacy grids coexist. Therefore, CR-based SG communications should be built upon open protocols and standards for compatible security requirements.

References

[1] *IEEE Vision for Smart Grid Communications: 2030 and Beyond*, IEEE Smart Grid Research, May 2013.

[2] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Trans. Ind. Electron.*, vol. 57, no. 10, Oct. 2010, pp. 3557-3564.

[3] (Aug. 4). *U.S. Department of Energy.* [Online]. Available: http://www.oe.energy.gov

[4] A. Y. Saber and G. K. Venayagamoorthy, "Plug-in vehicles and renewable energy sources for cost and emission reductions," *IEEE Trans. Indust. Electron.*, vol. 58, no. 4, Apr. 2011, pp. 1229-1238.

[5] M. Erol-Kantarci and H. T. Mouftah, "Wireless multimedia sensor and actor networks for the next generation power grid," *Ad Hoc Networks*, vol. 9, no. 5, Jun. 2011, pp. 542-551.

[6] P. Siano, C. Cecati, C. Citro, and P. Siano, "Smart operation of wind turbines and diesel generators according to economic criteria," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, Oct. 2011, pp. 4514-4525.

[7] J. Huang, H. Wang, and Yi Qian, "Smart grid communications in challenging environments," In Proc. *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, Tainan, Taiwan, 5-8 Nov. 2012, pp. 552-557.

[8] G. W. Arnold, "Challenges and opportunities in smart grid: A position article," *Proc. IEEE*, vol. 99, no. 6, Jun. 2011, pp. 922-927.

[9] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, Nov. 2011, pp. 529-539.

[10] 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, Fourthquarter 2014, pp. 1933-1954.

[11] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, Fourth Quarter 2012, pp. 998-1010.

[12] A. Ghassemi, S. Bavarian, and L. Lampe, "Cognitive radio for smart grid communications," In Proc. *First IEEE International Conference on Smart Grid Communications (SmartGridComm) 2010*, Gaithersburg, MD, USA, 4-6 Oct. 2010, pp. 297-302.

[13] R. C. Qiu, Z. Hu, Z. Chen, N. Guo, R. Ranganathan, S. Hou, and G. Zheng, "Cognitive radio network for the smart grid: Experimental system architecture, control algorithms, security, and microgrid testbed," *IEEE Trans. Smart Grid*, vol. 2, no. 4, Dec. 2011, pp. 724-740.

[14] R. Yu, Y. Zhang, S. Gjessing, C. Yuen, S. Xie, and M. Guizani, "Cognitive radio based hierarchical communications infrastructure for smart grid," *IEEE Network*, vol. 25, no. 5, Sep.-Oct. 2011, pp. 6-14.

[15] Federal Communications Commission, "Spectrum Policy Task Force Report, Technical Report 02-135," 2002.

[16] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. Netw. J.*, vol. 50, Sep. 2006, pp. 2127-2159.

[17] V. C. Gungor and D. Sahin, "Cognitive radio networks for smart grid applications: A promising technology to overcome spectrum inefficiency," *IEEE Veh. Technol. Mag.*, vol. 7, no. 2, Jun. 2012, pp. 41-46.

[18] K. Tan, K. Kim, Y. Xin, S. Rangarajan, and P. Mohapatra, "RECOG: A sensing-based cognitive radio system with real-time application support," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, Nov. 2013, pp. 2504-2516.

[19] J. Mitola III, Cognitive radio: An integrated agent architecture for software defined radio, Ph.D. dissertation, KTH, Stockholm, Sweden, May 2000.

[20] W. L. Chin, C. W. Kao, and Y. Qian, "Spectrum sensing of OFDM signals over multipath fading channels and practical considerations for cognitive radios," *IEEE Sensors J.*, vol. 31, no. 11, Apr. 2016, pp. 2349-2360.

[21] W. L. Chin, J. M. Li, and H. H. Chen, "Low complexity energy detection for spectrum sensing with random arrivals of primary users," *IEEE Trans. Veh. Technol.*, vol. 65, no. 2, Feb. 2016, pp. 947-952.

[22] W. L. Chin and J. M. Li, "Spectrum sensing scheme for overlay cognitive radio networks," *IET Electron. Lett.*, vol. 51, no. 19, Sep. 2015, pp. 1552-1554.

[23] W. L. Chin, C. W. Kao, H. H. Chen, and T. L. Liao, "Iterative synchronization assisted detection of OFDM signals in cognitive radio systems," *IEEE Trans. Veh. Technol.*, vol. 63, no. 4, May 2014, pp. 1633-1644.

[24] H. Xin, Z. Qu, J. Seuss, and A. Maknouninejad, "A self-organizing strategy for power flow control of photovoltaic generators in a distribution network," *IEEE Trans. Power Syst.*, vol. 36, no. 3, Aug. 2011, pp. 1462-1473.

[25] A. Dominguez-Garcia, C. Hadjicostis, and N. Vaidya, "Resilient networked control of distributed energy resources," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, Jul. 2012, pp. 1137-1148.

[26] M. Shahraeini, M. Javidi, and M. S. Ghazizadeh, "Comparison between communication infrastructures of centralized and decentralized wide area measurement systems," *IEEE Trans. Smart Grid*, vol. 2, no. 1, Mar. 2011, pp. 206-211.

[27] S. Zhang, and V. Vittal, "Design of wide-area power system damping controllers resilient to communication failures," *IEEE Trans. Power Syst.*, vol. 28, no. 4, Nov. 2013, pp. 4292-4300.

[28] S. Liu, X. P. Liu, and A. E. Saddik, "Modeling and distributed gain scheduling strategy for load frequency control in smart grids with communication topology changes," *ISA Trans.*, vol. 52, no. 2, Mar. 2014, pp. 454-461.

[29] J. Liu, A. Gusrialdi, S. Hirche, and A. Monti, "Joint controller-communication topology design for distributed wide area damping control of power system," in Proc. *18th IFAC World Congr.*, Milan, Italy, Aug. 2011, pp. 519-525.

[30] S. Liu, P. X. Liu, and A. ElSaddik, "Modeling and stability analysis of automatic generation control over cognitive radio networks in smart grids," *IEEE Trans. Syst., Man, and Cybern.*, vol. 45, no. 2, Feb. 2015, pp. 223-234.

[31] H. Wang, Y. Qian, and H. Sharif, "Multimedia communications over cognitive radio networks for smart grid applications," *IEEE Wireless Commun.*, vol. 20, no. 4, Aug. 2013, pp. 125-132.

[32] X. Ma, H. Li, and S. Djouadi, "Networked system state estimation in smart grid over cognitive radio infrastructures," In Proc. *45th Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, Maryland, USA, Mar. 2011, pp. 1-5.

[33] S. Bu, F. R. Yu, and Y. Qian, "Energy-efficient cognitive heterogeneous networks powered by the smart grid," In Proc. *IEEE INFOCOM 2013*, Turin, Italy, 14-19 Apr. 2013, pp. 980-988.

[34] J. Zhou, R. Q. Hu, and Y. Qian, "Traffic scheduling for smart grid in rural areas with cognitive radios," In Proc. *IEEE Global Communications Conference (GLOBECOM) 2012*, Anaheim, California, USA, 3-7 Dec. 2012, pp. 5172-5176.

[35] J. Huang, H. Wang, Y. Qian, and C. Wang, "Priority-based traffic scheduling and utility optimization for cognitive radio communication infrastructure-based smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 1, Mar. 2013, pp. 78-86.

[36] S. Xu, L. Wei, Z. Liu, S. Guo, X. Qiu, and L. Meng, "A QoS-aware packet scheduling mechanism in cognitive radio networks for smart grid applications," *China Commun.*, vol. 13, no. 2, Feb. 2016, pp. 68-78.

[37] A. Boustani, M. Jadliwala, H. M. Kwon, and N. Alamatsaz, "Optimal resource allocation in cognitive smart grid networks," In Proc. *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, USA, 9-12 Jan. 2015, pp.499-506.

[38] H. B. Yilmaz, T. Tugcu, F. Alagöz, and S. Bayhan, "Radio environment map as enabler for practical cognitive radio networks," *IEEE Commun. Mag.*, vol. 51, no. 12, Dec. 2013, pp. 162-169.

[39] Y. Chen and H.-S. Oh, "A survey of measurement-based spectrum occupancy modeling for cognitive radios," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, Firstquarter 2016, pp. 848-859.

[40] Y. Saleema and M. H. Rehmani, "Primary radio user activity models for cognitive radio networks: A Survey," *J. Network and Comput. Appl.*, vol. 43, no. 3, Aug. 2014, pp. 1-16.

[41] V. Dehalwar, M. Kolhe, and S. Kolhe, "Cognitive radio application for smart grid," *Int. J. Smart Grid and Clean Energy*, vol. 1, no. 1, September 2012, pp. 79–84.

[42] M. Yigit, V. C. Gungor, and S. Baktir, "Cloud computing for smart grid applications," *Comput. Networks*, vol. 70, Sep. 2014, pp. 312–329.

[43] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," *IEEE Trans. Smart Grid*, vol. 4, no. 1, Mar. 2013, pp. 36–46.

[44] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: A survey," *IEEE Network*, vol. 28, no. 1, Feb. 2014, pp. 24–32.

[45] V. Kouhdaragh, D. Tarchi, A. V. Coralli, and G. E. Corazza, "Cognitive radio based smart grid networks," in Proc. *Tyrrhenian Int. Workshop on Digital Communications - Green ICT (TIWDC)*, Genoa, Italy, 23-25 Sep. 2013, pp. 1–6.

[46] Z. A. Khan and Y. Faheem, "Cognitive radio sensor networks: Smart communication for smart grids-a case study of Pakistan," *Renewable and Sustainable Energy Rev.*, vol. 40, Dec. 2014, pp. 463–474.

[47] S. Chin-Sean, H. Harada, F. Kojima, L. Zhou, and R. Funada, "Smart utility networks in TV white space," *IEEE Commun. Mag.*, vol. 49, no. 7, Jul. 2011, pp. 132-139.

[48] A. A. Khan, M. H. 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, Firstquarter 2016, pp. 860-898.

[49] H. Farhangi, "The path of the smart grid," *IEEE Power Energy*, vol. 8, no. 1, Jan.-Feb. 2010, pp. 18-28.

[50] Office of the National Coordinator for Smart Grid Interoperability, "NIST framework and roadmap for smart grid interoperability standards, release 1.0." NIST Special Publication 1108, 2010.

[51] J. Wang, M. Ghosh, and K. Challapali, "Emerging cognitive radio applications:A survey," *IEEE Commun. Mag.*, vol. 49, no. 3, Mar. 2011, pp. 74-81.

[52] Vineeta and J. K. Thathagar, "Cognitive radio communication architecture in smart grid reconfigurability," in Proc. *Int. Conf. on Emerging Techn. Trends in Electr., Commun. and Netw. (ET2ECN)*, Gujarat, INDIA, Dec. 2012, pp. 1–6.

[53] Y. Han, J. Wang, Q. Zhao, and P. Han, "Cognitive information communication network for smart grid," in Proc. *Int. Conf. on Information Science and Technology (ICIST)*, Dalian, China, 23-25 Mar. 2012, pp. 847–850.

[54] J. Gao, J. Wang, B. Wang, and X. Song "Cognitive radio based communication network architecture for smart grid," in Proc. *IEEE International Conference on Information Science and Technology (ICIST)*, Mar. 2012, pp. 886-888.

[55] S. Kim, "Biform game based cognitive radio scheme for smart grid communications," *J. of Commun. and Networks*, vol. 14, no. 6, Dec. 2012, pp. 614-618.

[56] F. Liu, J. Wang, Y. Han, and P. Han, "Cognitive radio networks for smart grid communications," in Proc. *9th Asian Control Conference (ASCC) 2013*, Istanbul, Turkey, 23-26 Jun. 2013, pp. 1-5.

[57] 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, Jun. 2014, pp. 577-587.

[58] R. Yu, W. Zhong, S. Xie, Y. Zhang, 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, Feb. 2016, pp. 435-443.

[59] A. Aijaz and A.-H. Aghvami, "PRMA-based cognitive machine-to-machine communications in smart grid networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, Aug. 2015, pp. 3608-3623.

[60] A. A. Sreesha, S. Somal, and I. T. Lu, "Cognitive radio based wireless sensor network architecture for smart grid utility," in Proc. *2011 IEEE Systems, Applications and Technology Conference (LISAT)*, Long Island, Farmingdale, NY, Dec. 2011, pp. 1-7.

[61] A. Aijaz, S. Ping, M. R. Akhavan, and A. H. Aghvami, "CRB-MAC: A receiver-based MAC protocol for cognitive radio equipped smart grid sensor networks," *IEEE Sensors J.*, vol. 14, no. 12, Dec. 2014, pp. 4325-4333.

[62] K. Yang, J. Zhang, and H. Chen, "A flexible QoS-aware service gateway for heterogeneous wireless networks," *IEEE Network*, vol. 21, no. 2, Mar.-Apr. 2007, pp. 6-12.

[63] J. Kabouris and F. Kanellos, "Impacts of large-scale wind penetration on designing and operation of electric power systems," *IEEE Trans. Sustainable Energy*, vol. 1, no. 2, Jul. 2010, pp. 107-114.

[64] D. Backer, "Power quality and asset management the other two-thirds of AMI value," in Proc. *IEEE Rural Electric Power Conference*, Rapid City SD USA, 6-8 May 2007, pp. 6-8.

[65] S. Rusitschka, K. Eger, and C. Gerdes, "Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain," in Proc. *First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, USA, 4-6 Oct. 2010, pp. 483-488.

[66] S. W. Luan, J. H. Teng, S. Y. Chan, and L. C. Hwang, "Development of a smart power meter for AMI based on Zigbee communication," in Proc. *Int. Conf. Power Electron. Drive Syst.*, Taipei, Taiwan, 2-5 Nov. 2009, pp. 661-665.

[67] W. Luan, D. Sharp, and S. Lancashire, "Smart grid communication network capacity planning for power utilities," in Proc. *IEEE PES Transmission Distribution Conf. Expos.*, New Orleans, LA, USA, 19-22 Apr. 2010, pp. 1-4.

[68] B. Reid, "Oncor electric delivery smart grid initiative," in Proc. *62nd Annu. Conf. Protective Relay Engineers*, Austin, TX, Mar. 30-Apr. 2 2009, pp. 8-15.

[69] B. Lu, and V. C. Gungor, "Online and remote energy monitoring and fault diagnostics for industrial motor systems using wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 56, no. 11, Nov. 2009, pp. 4651-4659.

[70] Y. Peizhong, A. Iwayemi, and C. Zhou, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," *IEEE Trans. Smart Grid*, vol. 2, no. 1, Mar. 2011, pp. 110-120.

[71] A. Aijaz, H. Su, and A. H. Aghvami, "CORPL: A routing protocol for cognitive radio enabled AMI networks," *IEEE Trans. Smart Grid*, vol.6, no.1, Jan. 2015, pp. 477-485.

[72] T. Winter, "IPv6 routing protocol for low power and lossy networks," Internet Engineering Task Force, RFC 6550, Mar. 2012.

[73] K. Nagothu, B. Kelley, M. Jamshidi, and A. Rajaee, "Persistent Net-AMI for microgrid infrastructure using cognitive radio on cloud data centers," *IEEE Systems J.*, vol. 6, no. 1, Mar. 2012, pp. 4-15.

[74] S. Chang, K. Nagothu, B. Kelley, and M. M. Jamshidi, "A beamforming approach to smart grid systems based on cloud cognitive radio," *IEEE Systems J.*, vol. 8, no. 2, Jun. 2014, pp. 461-470.

[75] *Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands,* IEEE802.22, Jul. 2011.

[76] B. Li, B. Zhang, J. Guo, and J. Yao, "Study on cognitive radio based wireless access communication of power line and substation monitoring system of smart grid," in Proc. *International Conference on Computer Science and Service System (CSSS) 2012*, Nanjing, China, 11-13 Aug. 2012, pp. 1146-1149.

[77] H. Zhang, A. Gladisch, M. Pickavet, Z. Tao, and W. Mohr, "Energy efficiency in communications," *IEEE Commun. Mag.*, vol. 48, no. 11, Nov. 2010, pp. 48-49.

[78] G. Gur and F. Alagoz, "Green wireless communications via cognitive dimension: An overview," *IEEE Network*, vol. 25, no. 2, Mar. 2011, pp. 50-56.

[79] F. R. Yu, P. Zhang, W. Xiao, and P. Choudhury, "Communication systems for grid integration of renewable energy resources," *IEEE Network*, vol. 25, no. 5, Sep. 2011, pp. 22-29.

[80] X. Kang, R. Zhang, and M. Motani, "Price-based resource allocation for spectrum-sharing femtocell networks: A Stackelberg game approach," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 3, Apr. 2012, pp. 538-549.

[81] S. Bu and F. R. Yu, "Green cognitive mobile networks with small cells for multimedia communications in the smart grid environment," *IEEE Trans. Veh. Technol.*, vol. 63, no. 5, Jun. 2014, pp. 2115-2126.

[82] Y. Narahari, D. Garg, R. Narayanam, and H. Prakash, *Game Theoretic Problems in Network Economics and Mechanism Design Solutions.* London, U.K., Springer-Verlag, 2009.

[83] C. Shannon, "Communication in the presence of noise," *Proc. IRE*, vol. 37, no. 1, Jan. 1949, pp. 10-21.

[84] Q. D. Vo, J. P. Choi, H. M. Chang, and W. C. Lee, "Green perspective cognitive radio-based M2M communications for smart meters," in Proc. *International Conference on Information and Communication Technology Convergence (ICTC) 2010*, Jeju, 17-19 Nov. 2010, pp. 382-383.

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

[86] R. Deng, J. Chen, X. Cao, Y. Zhang, S. Maharjan, and S. Gjessing, "Sensing-performance tradeoff in cognitive radio enabled smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 1, Mar. 2013, pp. 302-310.

[87] Q. Li, Z. Feng, W. Li, T. A. Gulliver, and P. Zhang, "Joint spatial and temporal spectrum sharing for demand response management in cognitive radio enabled smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 4, Jul. 2014, pp. 1993-2001.

[88] S. P. Yeh, S. Talwar, G. Wu, N. Himayat, and K. Johnsson, "Capacity and coverage enhancement in heterogeneous networks," *IEEE Wireless Commun.*, vol. 18, no. 3, Jun. 2011, pp. 32-38.

[89] Y. Sun, C. Phillips, S. Wang, and B. Jingwen, "An improved QoS awareness scheduling scheme for CR mobile ad hoc networks," in Proc. *Wireless Telecommunications Symposium (WTS) 2013*, Phoenix, AZ, 17-19 April 2013, pp. 1-6.

[90] R. Yao, Y. Liu, J. Liu, P. Zhao, and S. Ci, "Perceptual experience oriented transmission scheduling for scalable video streaming over cognitive radio networks," in Proc. *IEEE Global Communications Conference (GLOBECOM) 2013*, Atlanta, GA, 9-13 Dec. 2013, pp. 1681-1686.

[91] S. Rohjans, M. Uslar, R. Bleiker, J. Gonzalez, M. Specht, T. Suding, and T. Weidelt, "Survey of smart grid standardization studies and recommendations," in Proc. *First IEEE International Conference on Smart Grid Communications (SmartGridComm) 2010*, Gaithersburg, MD, 4-6 Oct. 2010, pp. 583-588.

[92] A. N. Mody, M. J. Sherman, R. Martinez, R. Reddy, and T. Kiernan, "Survey of IEEE standards supporting cognitive radio and dynamic spectrum access," in Proc. *IEEE Military Communications Conference 2008 - MILCOM 2008*, San Diego, CA, USA, 16-19 Nov. 2008, pp. 1-7.

[93] C. Cordeiro, K. Challapali, D. Birru, S. Shankar, N. Res, and B.Manor, "IEEE 802.22: The first worldwide wireless standard based on cognitive radios," in Proc. *1st IEEE Int. Symp. New Frontiers in Dynamic Spectrum Access Netw. (DySPAN) 2005*, Baltimore, MD, USA, 8-11 Nov. 2005, pp. 328-337.

[94] IEEE802.22, "Working Group on Wireless Regional Area Networks (WRAN)," IEEE, Tech. Rep., 2009.

[95] (Agu. 5) *Official IEEE 802.11 Working Group Project Timelines,* [Online]. Available: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

[96] *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment 4: Physical Layer Specifications for Low Data Rate Wireless Smart Metering Utility Networks,* IEEE Std. P802.15.4g/D4 part 15.4, Apr. 2011.

[97] Ganesh, T. S., "Netgear R7500 Nighthawk X4 Integrates Quantenna 4x4 ac Radio and Qualcomm IPQ8064 SoC," AnandTech.

[98] H. Zhang, G. Guan, and X. Zang, "The design of insulation online monitoring system based on Bluetooth technology and IEEE1451.5," in Proc. *International conf. on Power Engineering*, Singapore, 3-6 Dec. 2007, pp. 1287-1291.

[99] C. Gezer, and C. Buratti, "A ZigBee smart energy implementation for energy efficient buildings," in Proc. *IEEE 73rd Veh. Technol. Conf. (VTC Spring)*, Yokohama, Japan, 15–18 May 2011, pp. 1–5.

[100] T. H. Wang and H. H. Chen, "Channel discovery algorithms for interference avoidance in smart grid communication networks – A survey," *Wiley Wirel. Commun. Mob. Comput.* vol. 16, no. 4, Oct. 2014, pp. 427–440.

[101] D. Cavalcanti, S. Das, W. Jianfeng, and K. Challapali, "Cognitive radio based wireless sensor networks," in Proc. *17th International Conference on Computer Communications and Networks 2008 (ICCCN '08)*, St. Thomas, US Virgin Islands, 3-7 Aug. 2008, pp. 1-6.

[102] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI application and security for controlled home area networks," in Proc. *IEEE Power Energy Soc. Gen. Meet.*, San Diego, CA, Jul. 24-29, 2011, pp. 1-8.

[103] A. Lazakidou, K. Siassiakos, and K. Ioannou, *Security in smart home environment,* Eds. Hershey, PA, USA: Medical Information Science, Jan. 2010, pp. 170-191.

[104] F. M. Cleveland, "Cyber security issues for Advanced Metering Infrastructure (AMI)," in Proc. *IEEE Power Energy Soc. Gen. Meet., Convers.Del.Elect. Energy 21st Century*, Pittsburgh, PA, Jul. 2008, pp. 1-5.

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

[106] A. R. Metke and R. L. Ekl, "Smart Grid security technology," *Innovative Smart Grid Technologies (ISGT) 2010*, Gaithersburg, MD, 19-21 Jan. 2010, pp. 1-7.

[107] Z. Fan, P. Kulkarni, S. Gormus, C. Efthymiou, G. Kalogridis, M. Sooriyabandara, Z. Zhu, S. Lambotharan, and W. Chin,"Smartgrid communications: Overview of research challenges, solutions, and standardization activities," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, Firstquarter 2013, pp. 21–38.

[108] M. Fouda, Z. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, Dec. 2011, pp. 675–685.

[109] W. L. Chin, Y. H. Lin, and H. H. Chen, "A framework of machine-to-machine authentication in smart grid: A two-layer approach," *IEEE Commun. Maga.*, Accepted, Aug. 2016.

[110] D. Wei, Y. Lu, P. Skare, M. Jafari, K. Rohde, and M. Muller, "Power infrastructure security: Fundamental insights of potential cyber attacks and their impacts on the power grid," DoE Office of Electricity Delivery and Energy Reliability, 2010, pp. 1–3.

[111] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Toward a framework for cyber attack impact analysis of the electric smart grid," in Proc. *First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, USA, 4–6 Oct. 2010, pp. 244–249.

[112] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, Nov. 2009, pp. 1–12.

[113] Z. H. Yu and W. L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, May 2015, pp. 1219-1226.

[114] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," in Proc. *2011 IEEE GLOBECOM Workshops*, Houston, TX, USA, 5–9 Dec, 2011, pp. 1162–1167.

[115] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 1, Jun. 2011, pp. 326–333.

[116] C. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. J. Shellhammer, and W. Caldwell, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag.*, vol. 47, no. 1, Jan. 2009, pp. 130-138.

[117] M. Sherman, A. Mody, R. Martinez, C. Rodriguez, and R. Reddy, "IEEE standards supporting cognitive radio and networks, dynamic spectrum access, and coexistence," *IEEE Commun. Mag.*, vol. 46, no. 7, Jul. 2008, pp. 72-79.

[118] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, May-June 2013, pp. 28-33.

[119] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey," *J. Network and Comput. Appl.*, vol. 35, no. 6, Nov. 2012, pp. 1691-1708.

[120] Z. Shu, Y. Yang, Y. Qian, and R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in Proc. *2011 IEEE Global Telecommunications Conference (GLOBECOM 2011)*, Houston, TX, USA, 5-9 Dec. 2011, pp.1-6.

[121] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, Jan. 2008, pp. 25–37.

[122] A. Goldsmith, *Wireless Communications*, Cambridge University Press, Cambridge, 2005.

[123] W. L. (William) Chin, T. N. Le, and C. L. Tseng, "Authentication scheme for mobile OFDM based on security information technology of physical layer over time-variant and multipath fading channels," *Elsevier Info. Sci.*, vol. 321, Feb. 2015, pp. 238-249.

[124] W. L. Chin, T. N. Le, C. L. Tseng, W. C. Kao, C. S. Tsai, and C. K. Kao, "Cooperative detection of primary user emulation attacks based on channel-tap power in mobile cognitive radio networks," *Int. J. Ad Hoc and Ubiquitous Computing*, vol. 15, no. 4, Apr. 2014, pp. 263-274.

[125] M. Basharat, W. Ejaz, and S. H. Ahmed, "Securing cognitive radio enabled smart grid systems against cyber attacks," in Proc. *2015 First International Conference on Anti-Cybercrime (ICACC)*, Riyadh, 10-12 Nov. 2015, pp. 1-6.

[126] R. Ranganathan, R. Qiu, Z. Hu, H. Hou, M. Pazos-Revilla, G. Zheng, Z. Chen, and N. Guo, "Cognitive radio for smart grid: Theory, algorithms, and security", *Int. J. Digit. Multimedia Broadcast.*, vol. 2011, Mar. 2011, pp. 1-14.

[127] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in Proc. *2010 IEEE Power Energy Soc. Gen. Meet.*, Minneapolis, MN, 25-29 Jul. 2010, pp. 1–7.

[128] H. Khayami, M. Ghassemi, K. Ardekani, B. Maham, and W. Saad, "Cognitive radio ad hoc networks for smart grid communications: A disaster management approach," in Proc. *International Conference on Communications in China (ICCC),* Xi'an, China, 12-14 Aug. 2013, pp. 716-721.

[129] J. Hoadley and P. Maveddat, "Enabling small cell deployment with HetNet," *IEEE Wireless Commun.*, vol. 19, no. 2, Apr. 2012, pp. 4–5.

[130] T. N. Le, W. L. Chin, and W. C. Kao, "Cross-layer design for primary user emulation attacks detection in mobile cognitive radio networks," *IEEE Commun. Lett.*, vol. 19, no. 5, May 2015, pp. 799-782.

[131] C. N. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in Proc. *First IEEE Workshop on Cognitive Radio Networks*, Las Vegas, NV, USA, Jan. 2007, pp. 1037-1041.