

Article

Trends and Potentials of the Smart Grid Infrastructure: From ICT Sub-System to SDN-Enabled Smart Grid Architecture

Jaebeom Kim ^{1,2,†}, Fethi Filali ^{1,†} and Young-Bae Ko ^{2,*}

¹ Qatar Mobility Innovations Center, Qatar Science and Technology Park, Doha 210531, Qatar; E-Mails: jaebeomk@qmic.com or kimjaebum@ajou.ac.kr (J.K.); filali@qmic.com (F.F.)

² Graduate School of Computer Engineering, Ajou University, 206 World Cup-ro, Suwon 16499, Korea

[†] These authors contributed equally to this work.

* Author to whom correspondence should be addressed; E-Mail: youngko@ajou.ac.kr; Tel.: +82-031-219-1841.

Academic Editor: Minhho Shin

Received: 12 July 2015 / Accepted: 29 September 2015 / Published: 10 October 2015

Abstract: Context and situational awareness are key features and trends of the smart grid and enable adaptable, flexible and extendable smart grid services. However, the traditional hardware-dependent communication infrastructure is not designed to identify the flow and context of data, and it focuses only on packet forwarding using a pre-defined network configuration profile. Thus, the current network infrastructure may not dynamically adapt the various business models and services of the smart grid system. To solve this problem, software-defined networking (SDN) is being considered in the smart grid, but the design, architecture and system model need to be optimized for the smart grid environment. In this paper, we investigate the state-of-the-art smart grid information subsystem, communication infrastructure and its emerging trends and potentials, called an SDN-enabled smart grid. We present an abstract business model, candidate SDN applications and common architecture of the SDN-enabled smart grid. Further, we compare recent studies into the SDN-enabled smart grid depending on its service functionalities, and we describe further challenges of the SDN-enabled smart grid network infrastructure.

Keywords: software-defined networking; smart grid network; Advanced Metering Infrastructure (AMI); context awareness

1. Introduction

A smart grid is an extensive combination of power grids, communication networks and information management systems, which contributes to green and cost-effective energy generation. Generally, a smart grid comprises a data communications infrastructure integrated with an electrical grid that collects and analyzes data captured in near real time about power transmission, distribution and consumption [1]. Thus, the key to enabling a smart grid system is the seamless convergence of existing electronic grid systems and information-communication technologies (ICTs).

The electrical power grid system can be divided into four elements: electricity generation plants, transmission substations, distribution substations and end users [2]. First, power plants generate power from a variety of sources, including solar, wind and nuclear sources, for distribution. As the power approaches the customers' homes, it is again stepped down to the voltage required for residential use. Finally, home appliances access power through their electric smart meters [2–4]. Even though the primary goal of these elements differs, time-critical information that is generated by each element needs to be robustly shared between all elements in a smart grid system. For example, power generation can be dynamically controlled by using the real-time energy consumption of the end users. Meanwhile, the end user can visualize the real-time power usage of the home and can obtain the real-time cost of the power supplied from the power provider. In a smart grid, electricity can also be returned to the grid by users. For example, home users may be able to generate electricity using photovoltaic (PV) systems and return it to the grid or electric vehicles may provide power to help balance loads by “peak shaving”, *i.e.*, sending power back to the grid when the demand is high. This backward flow is important. For example, it can be extremely useful in a microgrid that has been “isolated” because of power failures. With the help of the energy feedback from the customers, the microgrid can continue to function, albeit at a reduced level.

By exchanging information between different elements, the smart grid provides predictive information and recommendations to utilities, their suppliers and their customers on how to manage power in an optimal manner [4]. In addition, this information can be collected at the data server and reproduced by the service provider in order to develop new services and business models. Potential smart grid services focus not only on power-related services, but they also aim to enable the development of utility services and business models, such as water, gas, facility monitoring and unmanned surveillance [5,6]. Further, all electric grid elements must share the common understanding that the smart grid needs to be integrated with a data-networking infrastructure in order to be categorized them as “smart things” [7].

In this paper, we revisit the current smart grid system architecture, and we investigate a new paradigm called SDN-enabled smart grid. In addition, we compare recent studies of the SDN-enabled smart grid based on its service functionalities, and we present further research issues regarding the SDN-enabled smart grid. To the best of our knowledge, this is the first work that deals with the identification and comparison of SDN-enabled smart grid architectures.

The rest of this paper is organized as follows. In Section 2, we describe the essentials of the smart grid technologies. In Section 3, we describe the isolated subsystems of the current smart grid that are based on information management and communication layers, namely the information characteristics, communication architecture and its requirements. We present the survey and common design of the

SDN-enabled smart grid in Sections 4 and 5, as well as its challenges and guidelines for the smart grid. In Section 6, we conclude the paper.

2. Smart Grid Technology Essentials

The smart grid is a large-scale and complex networking system, and the National Institute of Standards and Technology (NIST) has therefore developed a conceptual hierarchical smart grid network infrastructure [1]. This conceptual architectural reference model enables us to analyze use cases, to identify interfaces for which interoperability standards are required and to facilitate the development of a cyber-security strategy [1,9]. Figure 1a shows an example of a three-tier hierarchical smart grid network that is organized by wide area networks (WANs), neighbor area networks (NANs) and home area networks (HANs). The HAN is an end-user network that is constructed by the connection between smart household electric appliances. The NAN is a capillary of the smart grid that provides large-scale data communication and connectivity between each household and a WAN. The WAN is a high capacity data network between NAN gateways and the head-end system (HES). In this smart grid network, all devices need to use the same communication policies, such as the routing strategy and quality of service (QoS) properties of the application, in order to provide the 3S autonomous network functions, namely self-configuration, self-healing and self-optimization. Figure 1b shows the layer-based information and power-flow model of the smart grid. In this figure, all objectives between the power facility and end-user system, such as the power generator, substation and AMI, are connected to the wired power grid infrastructure. The information data from each objective is exchanged via the data-communication infrastructure, which can be established using both wired and wireless communication protocols, such as powerline communication (PLC), Ethernet, IEEE 802.11 wireless local area network (WLAN) and the IEEE 802.15.4 family of protocols [8–10].

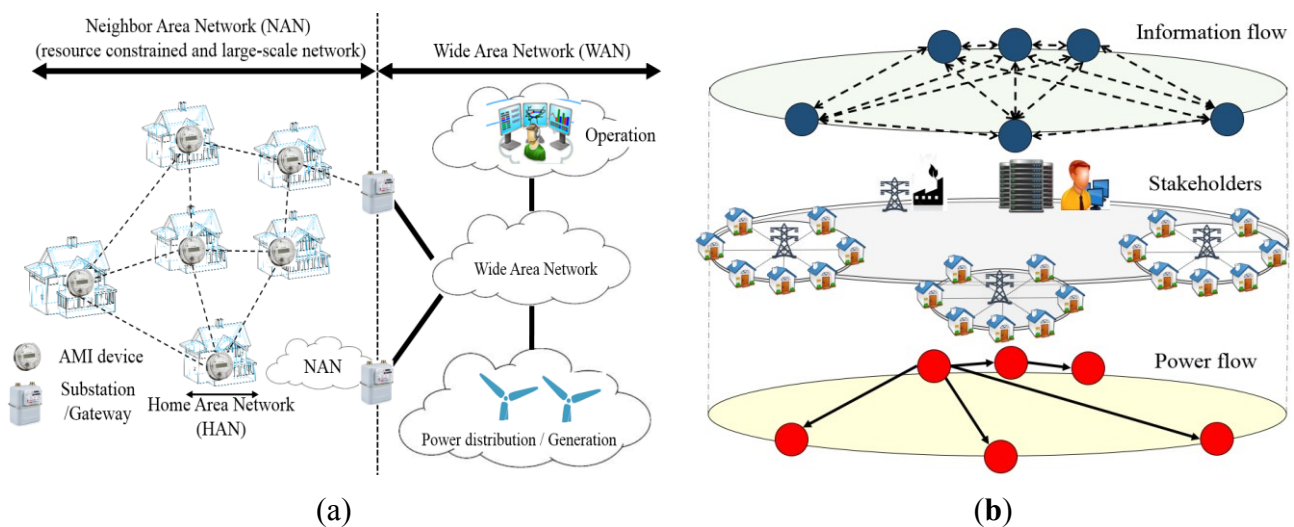


Figure 1. (a) multi-tier-based smart grid network architecture. (b) Abstraction of the information and power flow view of the smart grid infrastructure;

In this layered smart grid model, the electric and communication infrastructure support the two-way flow of electricity and information. Note that it is straightforward to understand the concept of the

“two-way flow of information”. “Two-way flow of electricity” implies that the electric energy delivery is no longer unidirectional. The synthesized requirements of the desired smart grid are as follows:

- The smart information subsystem is responsible for advanced information metering, monitoring and management in the context of the smart grid.
- The smart communication subsystem is responsible for communication connectivity and information transmission between systems, devices and applications in the context of the smart grid.

The smart grid technologies employed for industrial and mission-critical environments require new network-management technologies to provide simple system management between smart grid sub-layers from the application and information sub-systems to the communication infrastructure. Currently, the smart grid concept is a relevant critical-use case, which includes the protection, automation and control of electric power systems and which is supported by ICT facilities that must meet the real-time requirements of these applications with high dependability and security [11].

However, the current communication infrastructure may not be able to dynamically adapt to the new business model of the smart grid because of hardware dependencies. According to some smart grid researchers [12–15], communication technologies first need to be further developed, and they predict that software-defined networking (SDN) will allow information exchange in different network platforms, different layers and provide the adaption of new business models of the smart grid without hardware replacement. In addition, they argue that the SDN-based smart grid will improve the system robustness by enhancing the reliability and optimization of the transmission asset utilization [13,15]. In the SDN architecture, the control plane of the network is controlled by using a centralized SDN controller, and a service provider can identify not only the network status, but can also flexibly make a network plan for services and business models. This separate control and data plane model of the SDN enables us to find a suitable solution, even if there are potential problems, such as route disconnection, bottlenecks, collisions and application errors without special network devices [16]. However, current SDN is designed for highly capable network environments and needs to solve various challenges to enable the SDN-enabled smart grid in terms of the control message overhead, route construction between devices and interoperability between smart grid protocols.

3. ICT Sub-Systems of the Smart Grid

The smart grid is a complex and interoperable system that needs to process meaningful and actionable information between different subsystems. The exchanged information will be shared by the systems, and this information will elicit agreed-upon types of responses. The reliability, fidelity and security of the information exchanges between smart grid systems must achieve the required performance levels [17]. The ICT technologies are basic building blocks for the underlying data-centric smart grid system. The combined requirements of the desired smart grid ICT are as follows:

- Integrity: The smart grid scopes (generation, transmission, distribution, consumption and control center [1]) and sub-scopes will use a variety of communication networks that are integrated with the IT networks.

- Interoperability: The smart grid will have the capability of two or more networks, systems, devices, applications or components with respect to the ability to exchange and readily use information securely, effectively and with little or no inconvenience to the user [17].
- Interactivity: Utilities and customers will reduce their usage during peak hours. Mechanisms will also be incorporated for consumers to smartly use their power devices to lower their cost.

3.1. Smart Grid applications

From an application perspective, there are three major domains for ICT integration into the power grid [4], as shown in Figure 2. Supervisory control and data acquisition (SCADA) is already widely used for remote monitoring and controlling of higher levels of the distribution grid [5]. This area is also well covered by advanced standards, such as IEC 61850 for substation automation. The active distribution grids are the core of modern smart grids and enable the integration of distributed energy sources mainly into the mid-level voltage grid. The primary task of communication in this respect is to collect critical network parameters and to actively influence the distributed energy generation, so as to maintain the overall power quality. On the lower grid levels, smart metering is the most relevant use case for ICT. Originally intended to enable the remote retrieval of meter values, smart metering also includes load profiling, local power-quality monitoring and the remote switching of loads [23]. This requires a permanent connection to a communication network, even though real-time requirements are not as stringent as in SCADA control applications, e.g., the overall load balancing on the grid.

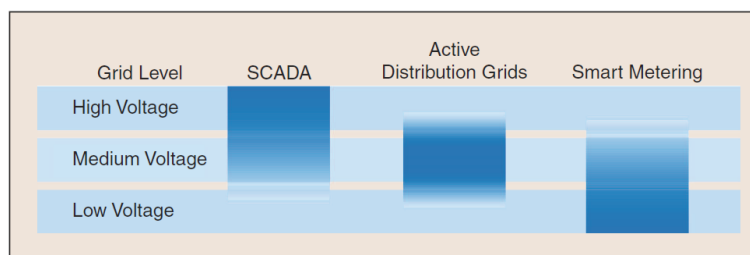


Figure 2. Major ICT application domains in smart grids and their correlation with the grid levels. SCADA, supervisory control and data acquisition.

3.2. Information Management

The traffic volume of smart grid systems has grown rapidly because of extended business models and service domains, such as gas, water and facility surveillance [6]. Although it was an offshoot of recent power grid systems, the smart grid is required to meet more requirements and has to attain new features. This is because the volume of the generated and consumed data traffic is extremely high when compared to the traditional power grid network.

Smart grid needs to use real-time analytic engines that enable the analysis of the power network, determine the current state and condition of the power system, predict what may happen and develop an action plan [24,25]. These engines receive data from the utility and external entities, such as weather services, through an advanced metering infrastructure (AMI). AMI is usually a combination of smart meters, data management modules, communication network modules and applications that are specific

to metering and plays a key role in smart grid technology, enabling the enhancement of energy efficiency. Utilities, regulators and policymakers should focus on the consumer-centric architectures for appliance control, the public architecture on which AMI communication is based and the collaborative architecture for content. However, it is evident that choices made by utilities as part of their smart grid deployment strategy and network architecture, which are guided by the policies dictated by state and federal regulatory authorities, may significantly affect the outcome of the smart grid initiatives.

- Control and management: This is intended to monitor and manage all of the components of the electric power system. For example, their behaviors and performances can be modified and predicted to avoid or address potential emergencies [16,18–20,33]. In the smart grid system, the HES needs to provide dynamic pricing and end-user device management. Meanwhile, the HES needs to find the optimal configuration parameters of the smart grid system, such as the monitoring pattern, business model, network monitoring and network system configuration [6].
- Neighbor area optimization: This is designed to help customers know the real-time prices of power, enabling them to optimize the power usage accordingly [9,17,21,22]. In addition, consumers then become informed participants and can choose different purchasing patterns based on their needs and the Grid's demand, which can ensure the reliability of the electricity supply [5]. Meanwhile, the communication protocol needs to be optimized to provide stable data delivery services in the resource-constrained environment of the NAN [6].

To realize a stable smart grid, there is a need for information analysis, management and different architectural directions for the smart grid that compares utility-controlled and consumer-controlled energy networks. For instance, with utility control, the intelligence of devices is derived from a central control point via a private utility network. However, with consumer control, these devices use a control system that is located in the home, business or on the Internet, but is ultimately managed by the needs of the consumer [26]. For both of these extremes, in addition to intermediate possibilities, it is important to consider how choices affect the combined efficiency and demand-response application (*i.e.*, energy monitoring), as well as support/limit innovation in supporting a responsive energy future. Many utilities have begun smart grid implementation with AMI.

3.3. Communication Infrastructure

The smart grid is a combination of ICTs and the electrical power grid. It is expected to affect all segments of the current electrical grid system, including generation, transmission and distribution. However, these segments will not function well without an effective data communication networking system. In other words, designing a communication architecture that meets the requirements of the power grid is key to the successful implementation of the smart grid, because power grid implementation has long been established. Based on the requirements of smart grid, it initially implies a need for bidirectional, real-time communication networks for data collection and processing [17]. From a communication technology point of view, information exchange in the upper grid levels for SCADA applications is usually covered by existing communication networks belonging to utilities or grid operation [3].

A smart grid communication infrastructure also includes HANs, building area networks (BANs), industrial area networks (IANs) and a WAN. A HAN is a communication network comprising appliances and devices within a home. A NAN is a network of multiple HANs that delivers the metering data to data concentrators and delivers control data to HANs. A WAN is the largest network for communications to/from data control centers. In a HAN, appliances (such as meters for electricity, gas, water, heat and solar panels) can be equipped with smart meters; these meters also connect smart appliances (*i.e.*, appliances with communications and remote control functions, such as smart dishwashers, dryers and ovens). In addition, these meters connect to a metering gateway. In a NAN, many metering gateways of HANs are connected to each other to form a wireless mesh network [6]. A WAN connects smart metering gateways with utilities and the distribution control system.

These networks are often based on fiber-optic links that are installed in parallel to the high-voltage grid and connect primary substations, large power plants and control rooms. Furthermore, they are mostly based on Internet technologies. Today, the challenge regarding interconnection lies in the medium- and low-voltage levels required, which are usually not reachable (or only to a small extent) by utility-owned communication infrastructures. To bridge this gap, several communication protocols are provided. PLC systems overcome traditional electronic communication technologies. The PLC channel is problematic, because it is time varying and depends greatly on the actual network topology and the connected electrical loads. To ensure connectivity from a communication viewpoint, network elements, such as transformers, need to be bridged with phases coupled, which requires additional equipment that is expensive at the higher voltage levels. Furthermore, regulation of the frequency bands used for data transmission is fragmented worldwide and remains unclear. The implementation of PLC is considered to be both economically and technically challenging and is still in its infancy compared to other communication technologies. However, it is a promising possibility that is currently being investigated.

The use of wireless networks is an alternate option, because they are flexible and can be used to build utility-owned networks. However, typical broadband computer network technologies, such as worldwide interoperability for microwave access (WiMAX) and WLANs, are problematic with respect to their limited transmission range and reachability, especially in urban areas. Hence, they may serve only as communication subsystems for small clusters of devices, such as meters. For long-distance transmission, trunked radio systems, such as terrestrial trunked radio (TTR) or trans-European trunked radio (TETRA), are becoming popular in some countries. Installation costs are moderate, even though the frequencies used are not license free. As TETRA is limited in bandwidth (7.2 kb/s per time slot), it can be considered as a substitute for services that are currently run over GSM/ General Packet Radio Service. Typical applications are metering (load profile meters and households), supervision of transformer stations and safety-related applications [3].

4. Evolution of the Smart Grid Infrastructure: SDN-Enabled Smart Grid

The smart grid technologies employed for industrial and mission-critical environments require new network management technologies to provide simple system management between smart grid sub-layers from applications, information sub-systems and communication infrastructure. Currently, the smart grid concept is a relevant critical use case that includes the protection, automation and control of electric power systems and which is supported by ICT facilities that must meet the real-time

requirements of these applications with high dependability and security. However, the current communication infrastructure may not dynamically adapt to the new business model of the smart grid due to its hardware dependability. For example, in the traditional network paradigm, each network device, such as switches (AMI meter), individually manages its routing table by using a pre-defined routing protocol. In this architecture, the pre-defined routing protocol of the network device cannot be flexibly changed or configured to adapt network dynamicity. From a service (application) perspective, the system administrator cannot dynamically manage the network system because the network and service layer are isolated from each other. Thus, the service administrator would not be able to directly identify a network problem even when the application service is down due to network instability. Further, a new application profile of the utility service or network function needs to be added to legacy AMI infrastructure, and all AMI devices need to be replaced or upgraded with service interruption. According to smart grid researchers, smart grid communication technologies are required to evolve in order to solve these various complexity problems affecting the large-scale smart grid system. In addition, they predict that SDN will allow information exchange across different network platforms and different layers and will enable the adaption of a new business model of the smart grid system [27,28]. Meanwhile, SDN-enabled smart grid architecture has been considered for various companies, such as Fujitsu and Cisco [46].

SDN is a next-generation network architecture that provides simplified and flexible network-management services through the abstraction of lower-level functionality, such as packet filtering, switching and monitoring. In SDN, to isolate the control and data plane of the network, a centralized network controller manages the control plane of the network instead of individual network switches. The incoming packet information (flow) of each switch is reported to the SDN controller when a packet is not listed in its flow table. The SDN controller decides and publishes the flow entry of the requested flow from the network switches using an SDN application that can be directly programmed by the system administrator. This separated control is implemented in the application layer through an application-network interconnection interface, such as OpenFlow API [29]. Thus, the service administrator manages and monitors not only the service (business) application status, but also the communication system without the need for an additional network management system. Moreover, each resource-constrained AMI device does not need to maintain its routing strategy, which is maintained using the SDN controller. The network design and potential advantages of the SDN-enabled smart grid are discussed below.

4.1. Network Design of the SDN-Enabled Smart Grid System

The SDN-enabled smart grid system can be simply installed over a legacy IP network infrastructure without the need for any additional wired or network installation. This is because the SDN functions are implemented by application software with a general operating system, such as Linux, instead of traditional hardware-dependable network systems. Figure 3 shows an example of an SDN-enabled smart grid. In this example case study, the message exchange between HES and the edge AMI meter is realized using a switch and gateway intelligent electronic device (IED). This communication architecture is the same as the traditional smart grid communication infrastructure, and it can be simply enhanced to become an SDN-enabled smart grid infrastructure by using centralized SDN controllers [4]. In addition, the resource and service capability of the SDN controller is determined depending on its service domain (tier) as a

smart grid WAN and HAN. The service function as a communication policy and smart grid (power system) application can be realized within the SDN controller. Meanwhile, the service functions between communication infrastructure and the power grid system application can share the information to optimize the smart grid system.

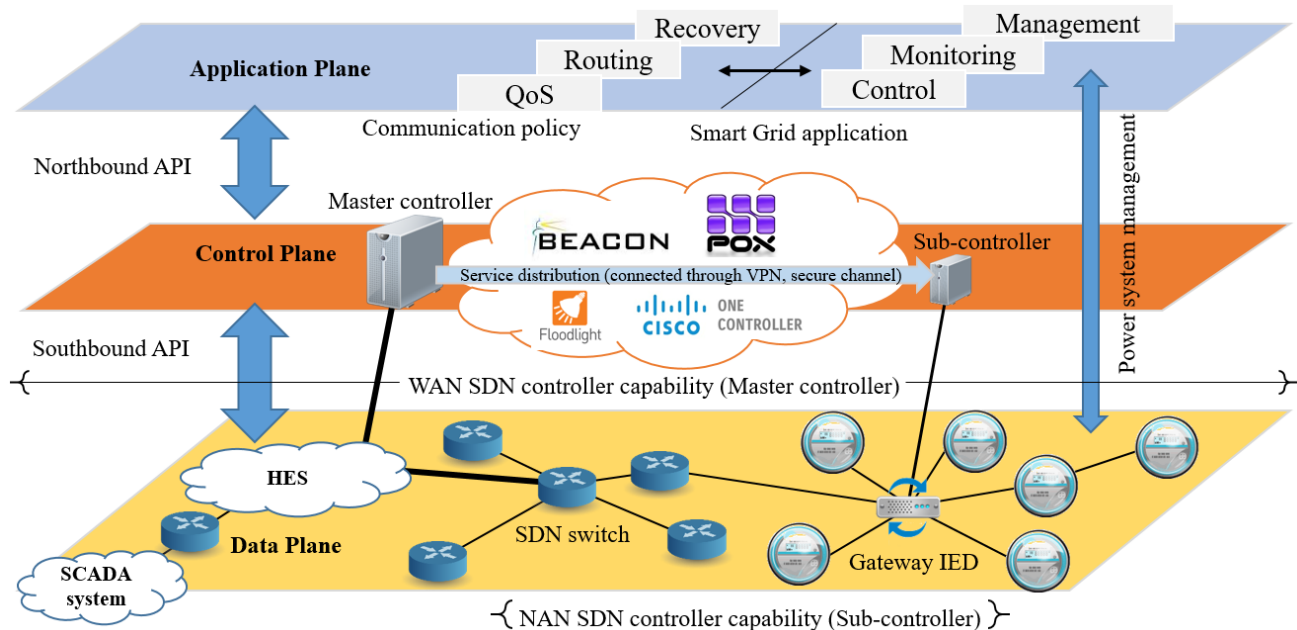


Figure 3. Illustration of the multi-controller-based SDN-enabled smart grid infrastructure.

- **WAN SDN case study:** The WAN SDN controller needs to be designed to enforce the communication policy and smart grid application of the smart grid system. The WAN SDN controller is generally called a master controller and handles the back-end HES service applications, such as SCADA and intrusion detection system (IDS) control. In addition, its service capability can be extended to micro-grid service applications, such as AMI monitoring systems, depending on the network scale and system resources. Dong, X. et al. proposed a WAN SDN controller architecture that is designed for the back-end SCADA management infrastructure of the smart grid [18,44]. In this system, the master SCADA controller is implemented for one of the SDN applications and controls slave SCADA systems in the power grid network. This WAN SDN controller system handles the global optimization of the smart grid system, such as end-to-end routing, network capacity planning and back-end network management, but it also needs to consider the system resources, such as storage, link capacity and computational power.
- **NAN case study:** The NAN SDN controller (sub-controller) provides local optimization of the resource-constrained smart grid network. The service capability of the sub-controller is generally limited to a single subnet of the smart grid network. In Figure 4, the gateway IED is directly connected to the sub-controller, and its service capability is migrated from the master SDN controller. The sub-controller framework can be installed in the gateway IED of the smart grid system to achieve resource-constrained AMI network management.

4.2. Potential Benefits of the SDN-Enabled Smart Grid

- **Simplified system management:** The main purpose of SDN is to realize simplified network management that allows an extension of the scale and flexibility of a network. To reduce the management complexity of the network system, SDN isolates the control and data forwarding planes [15]. The control plane of the network is implemented using an SDN controller that constructs the network topology, and the data forwarding plane of the network is implemented using feedback information from the SDN devices on the network. The feedback information between the SDN controller and the device is exchanged using a secure control channel that is established using network tunneling [29]. Service providers can deploy application and network functionalities, such as the routing strategy, topology and QoS policy, using a secure control channel. In the SDN-enabled smart grid HAN, resource-constrained AMI devices do not need to decide their own routing path, QoS or transmission strategies. Instead, the centralized SDN controller architecture determines the optimal configuration of the network, reducing the resource usage of the AMI devices in terms of power consumption and the number of control messages required [30].

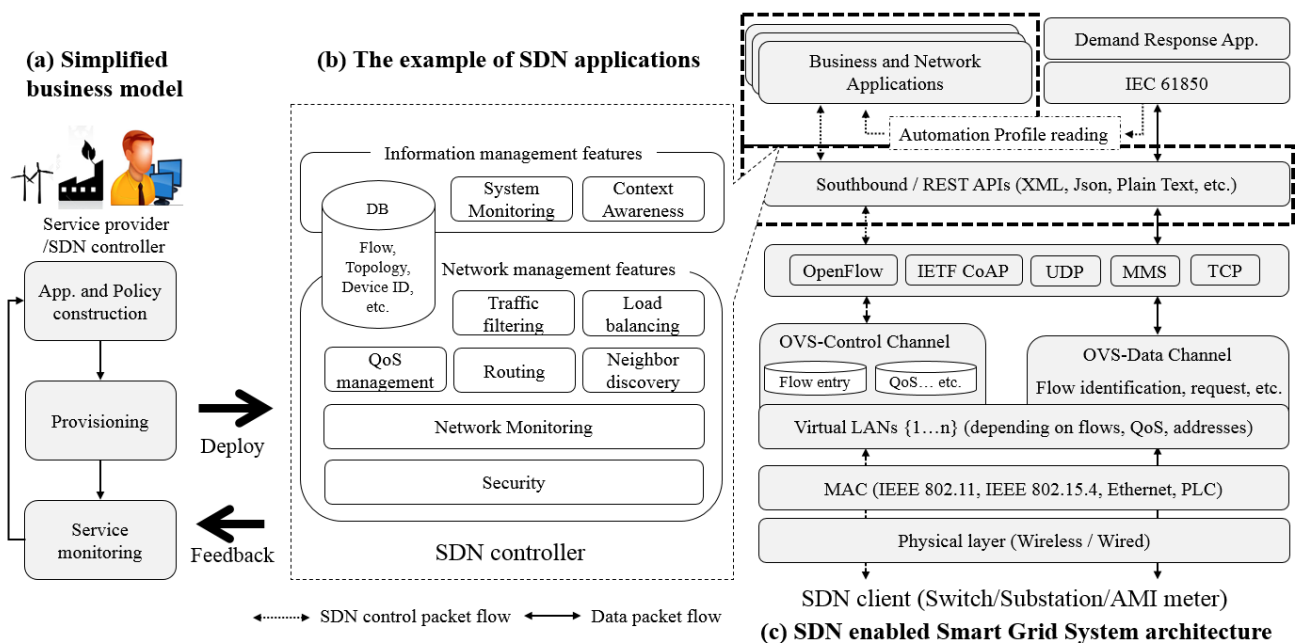


Figure 4. Abstraction of the SDN-enabled smart grid: business model process, categorized SDN application and system architecture. OVS, Open vSwitch; PLC, powerline communication. (a) Simplified business model. (b) The example of SDN applications. (c) SDN enabled Smart Grid System architecture.

The management software for the SDN controller can be categorized into two types, namely open-source-based and commercial systems. Nox [39] and Floodlight [12] are the most famous SDN control software frameworks that can handle the request and response messages that are sent between the application layer and network layer [39]. The SDN controller determines the network policy using an SDN application, and it maintains the flow information, route, forwarding strategy, topology and

network status. Figure 4c shows an example of the SDN-enabled smart grid architecture. In this figure, SDN applications, such as network configuration, IEC 61850 configuration and system monitoring, are connected to the SDN controller using Southbound and REST APIs. Southbound is a connection application program interface (API) between the application and communication interface. When the AMI device receives a new flow, such as AMI metering data, it requests the forwarding policy from the SDN controller using the secure control channel. The forwarding policy of the requested flow is generated using the SDN application and is transmitted to the AMI meter. This process, which is carried out by the SDN-enabled smart grid, provides not only simplified network management, but also reduces the computational overhead of the AMI meter. Further, service providers simply add, remove or update network policies without the need for any hardware replacement or upgrade.

- **Interoperability:** SDN provides data and control message exchange between different types of communication infrastructure by using tunneling and Open vSwitch (OVS) and OpenFlow standards [29]. Figure 4c shows an example of the SDN system architecture. In this figure, the IEC 61850 utility protocol of the application and OVS is connected through the REST APIs of the OpenFlow interfaces. OpenFlow is the de facto SDN standard software that provides an interface between the control and forwarding layers of the SDN. OpenFlow allows direct access to and manipulation of the forwarding plane of network devices, such as switches, routers, whether they are physical or virtual (hypervisor based) [28]. OVS is an alternative to the bridge module that has been part of the kernel since the 2.4 series. OVS enables communication interface virtualization and port mapping for SDN router construction. All of the information received from each module can be monitored using SDN applications, and the service provider can access and control the system without the isolated stack regulations of the device.
- **Situational awareness and flexibility:** In SDN, the service provider can monitor the real-time network situation by using feedback information obtained from each SDN device. For example, in a traditional smart grid system, a service provider may not understand the need to upgrade the reception stability of the metering data without the need for additional network analyzers, such as firewalls, packet inspection routers and systems, when new standard protocols are utilized. However, in SDN, the network analysis system can be provisioned by employing an Open Systems Interconnection Reference Model Layer 2–3 network-monitoring SDN application [29]. Meanwhile, the service provider can simply identify network-wide network situations, such as congestion, collisions, bottlenecks and the flow status of the data packet, without additional hardware installation. In addition, network functionalities, such as routing, load balancing and the QoS management function, can be dynamically optimized and provisioned using network-wide situation information.
- **Simplified service deployment:** In the SDN-enabled smart grid, the application and network control plane can be removed from devices, such as routers, switches and AMI devices. Figure 4a–c shows an example of the SDN-enabled smart grid business model, SDN applications and system architecture. Generally, the SDN controller is directly managed by the service provider, and it is located in the HES. The service application is embedded within the application layer, which ensures hardware-independent system programming, and the new services and network

policies can be dynamically deployed to the SDN devices without the need for new hardware installation and configuration.

- **Simplified business model:** The SDN-enabled smart grid business model can be simplified to include policy development, service provisioning and service monitoring, as shown in Figure 4a. In this model, the system administrator develops an SDN application, such as topology construction, routing, QoS and traffic-filtering program. The implemented SDN application and policy need to be provisioned to the SDN controller, which is a part of the HES of the SDN-enabled smart grid system. In the application provisioning step, the service provider deploys an SDN application or policy to the SDN controller. The service monitoring is a key to developing a new application and profile. In this step, the service provider analyzes the network event history by using diagnostic SDN applications.

4.3. Candidate SDN Application for the Smart Grid

Figure 4b shows an example of the SDN applications. The SDN application is directly connected to the SDN stack using Northbound APIs [31]. Thus, the service providers do not need to consider hardware dependability, which allows interoperable data exchange between different network devices. The policy applies to the configuration profile of the SDN application, which enables the situational awareness of the smart grid infrastructure without the need for a replacement SDN application or hardware reconfiguration. The related studies about the information and network management SDN-enabled smart grid applications are categorized and shown in Table 1.

Table 1. Comparison between candidate SDN smart grid architectures.

| Architecture | Evaluated Features | Context Awareness | System and Network Monitoring | Neighbor Discovery and Routing | Load Balancing | QoS | Security | SDN Controller Program | Network Interface(s) | Target Network |
|-------------------------------|--------------------|-------------------|-------------------------------|--------------------------------|----------------|-----|----------|------------------------|----------------------|----------------|
| Molina, E. <i>et al.</i> [12] | | √ | √ | - | √ | - | √ | Floodlight | Ethernet | WAN/NAN |
| Sydney, A. <i>et al.</i> [36] | | - | √ | - | √ | √ | - | Nox | Ethernet | WAN/NAN |
| Byun, J. <i>et al.</i> [33] | | √ | √ | - | √ | √ | - | Custom | ZigBee/PLC | HAN |
| Andrew, <i>et al.</i> [13] | | - | - | √ | - | - | - | Nox | Ethernet | WAN |
| Cahn, A. <i>et al.</i> [14] | | - | √ | - | √ | | √ | Custom | Ethernet | NAN |
| Qin, Z. <i>et al.</i> [38] | | √ | √ | - | - | √ | - | Qualnet, Sim | IEEE 802.11 | HAN |
| Dorsch, N. <i>et al.</i> [34] | | √ | √ | √ | - | √ | - | Custom | Ethernet | WAN/NAN |
| Dong, X. <i>et al.</i> [44] | | - | √ | - | - | - | √ | ns-2, Sim | Ethernet | WAN/NAN |

√: Supported; -: Not supported.

- **Context awareness:** Context awareness is an important feature for intelligent information management and provides situation-based interaction between a service provider and various IEDs. For example, the context awareness system can automatically identify and configure a new device's installation depending on its location and equipment type. In addition, this information can be utilized to anticipate an end-user's immediate needs, in the process offering more sophisticated, situational-aware, and usable functions. Magoutas, B. proposed a situational-aware demand-response algorithm for a smart meter that can be ported to the SDN controller [32]. In

this algorithm, the system (controller) predicts the demand request patterns of the customer and automatically sends related information. Thus, the number of request messages and, thus, network congestion can be reduced. Byun, J. et al. proposed a smart energy distribution and management system (SEDMS). In this scheme, monitoring data from each household are reported to the centralized demand management system (DMS), which categorizes and optimizes the monitoring pattern for each household. The SEDMS application system is implemented using a software program without any specialized device, and its functions, such as the knowledge repository, context analyzer and monitoring-pattern generation module, can be dynamically updated or replaced by a new system without the need for any hardware replacement. These optimized traffic controls using the context-awareness function of the SDN can help to improve the network and service reliability of the resource-constrained smart grid infrastructure as an AMI system [36]. The experimental result of the SEMDS shows that the number of request messages and response delay time of the situational-awareness system are reduced compared to the traditional pre-defined profile-based demand response smart grid system [33].

- **System and network monitoring:** In traditional smart grid communication infrastructure, the service provider cannot monitor the network status without an additional packet inspection device. IEC 61850 focuses on device monitoring automation and not on network-wide monitoring. Thus, the service provider cannot determine the accruable reason for the instability of the communication infrastructure without using a network-monitoring device. Further, it may be difficult for the network system administrator to determine the actual problem leading to the loss of application packets, because the network stack cannot open the application packet itself. Thus, the system administrator can only identify the end-to-end perspective problem, even if the packet-loss problem occurred during packet transmission in the link layer (hop-by-hop). However, in the SDN-enabled smart grid, the service provider can not only monitor the device, but can also monitor the network status, such as the real-time throughput, dropped packets, topology and link-connection stability between devices. To realize application and network monitoring in SDN, the smart grid application characteristics and network parameters should be handled by an SDN controller. In 2014, Molina, E. et al. proposed a smart grid SDN management application for an IEC 61850-based smart grid system [12]. In this system, they presented a substation configuration description (SCD) information-mapping algorithm for SDN. In traditional smart grid infrastructure, the communication system cannot utilize these types of information for network optimization and monitoring. The SCD is an application profile of the IEC 61850 system and indicates various metering application profiles, such as monitoring intervals, attributes and types. However, in this scheme, the SCD profile is converted to the OpenFlow flow structure. The converted flow structure from the SCD is inserted into the OpenFlow entry table, and the SDN controller maintains the smart grid data flow using its monitoring application. Thus, the system administrator can simplify the access and management of both the application (service) and network using a single SDN controller. The experimental result of the IEC 61850 and OpenFlow achieves automated network monitoring as a real-time topology view, link bandwidth, traffic flow and address information of the substation network. Further, the authors can easily detect service denial attacks using the application and network

monitoring SDN application without the need for additional network monitoring devices, such as firewalls [44].

- Neighbor discovery and routing: Optimal network configurations, such as routing and network topologies, are key to providing stable smart grid data communication links between HES and IEDs, but they cannot be dynamically configured by service providers in traditional networks. For example, the neighbor-discovery message interval cannot be dynamically configured in a traditional smart grid, even if the communication environment is very stable. Therefore, the service application may suffer from excessive control message overheads. In addition to the topology construction overhead, excessive routing-control message overheads may lead to a low QoS in resource-constrained AMI network environments [45]. SDN provides a flow-based forwarding strategy that employs combined neighbor discovery and routing SDN applications. Nils et al. proposed a multi-layered SDN4 smart grid architecture in 2014 [34]. In this architecture, the routing path between the central server and devices was constructed using a centralized SDN controller instead of the distributed routing protocol of the devices in the network. The SDN controller periodically monitors the network device, and constructs the network topology and route information between devices in the network. In addition, a SDN4 smart grid controller can maintain multiple routing paths between source and destination devices to provide DiffServ QoS routing between flows. If an AMI device, which has no route for incoming flow packets, requests the forwarding direction of the packet to the SDN controller, the SDN controller responds with the forwarding direction (next hop) to the requester. The experimental result of the end-to-end smart grid traffic delay shows that SDN4 smart grid routing outperforms open shortest path first (OSPF).
- Load balancing: SDN load balancing applications are flow information-based stateless control service applications that allow systems to bypass the limitations of traditional stateful hardware appliances, such as load balancers and firewalls [35]. In particular, load-balancing features must be considered for use in resource-constrained substation automation domains, such as wireless smart grid AMI networks. For example, if the emergency power-quality alert message from the AMI device is transmitted to the HES, end-to-end transmission needs to be guaranteed, but traditional network systems cannot detect specific flow priorities, because application profile information is not shared between application network layers. Therefore, the network cannot suspend low-priority flow transmission, even if the network capacity is overloaded. While traditional per packet-based admission control algorithms can be utilized to process network control message exchange, they need to be extended for application-flow identification. Sydney A. et al. proposed flow-based admission control for SDN [36]. In this algorithm, the SDN application creates two virtual network interfaces to isolate high-priority and best-effort flow transmission. The data rate of the developed virtual interfaces can be dynamically configured using queue-size management, which enables us to control the volume of the flow traffic in each network. This algorithm can be effectively utilized to protect the minimum bandwidth requirements of the high-priority data flow as emergency power quality traffic when a large volume of the best-effort data traffic, such as firmware and diagnostics flows, coexists on the

network. The experimental result shows that the SDN controller can provide per flow-based service differentiation using a smart grid service profile.

- **QoS management:** The smart grid communication infrastructure must simultaneously support a wide range of QoS requirements for numerous smart grid and legacy applications. To satisfy the delay requirement of the smart grid traffic, the SDN controller uses both the context-awareness and load-balancing SDN applications. In the traditional network infrastructure, cross-layer-based QoS algorithms are widely utilized, but their use increases the network-system complexity [37]. However, in SDN, cross-layer information is easily shared using OpenFlow and OVS, which are operated without any direct information exchange between different network layers [29]. Qin, Z. et al. proposed a heuristic flow scheduling-based QoS algorithm for smart grid devices [38]. In this algorithm, the authors assumed that SDN can detect the flow information and real-time flow status using an SDN flow monitoring application. The SDN controller assigns flow priority depending on a calculus-based queue model that considers the flow-traffic arrival rate, delay requirement of the flow and the available network bandwidth of the device. Each application flow of the AMI device can be assigned a different virtual interface depending on the smart grid service profile. The interface configuration can also be dynamically changed using the calculated flow priority of the SDN controller to optimize the network capacity and service QoS. The performance result shows that SDN APP can provide not only the DiffServ QoS of the smart grid flows, but also the dynamic QoS configuration of the flows in the network.
- **Security:** The smart grid system autonomously collects massive amounts of data and transfers them to utility companies, consumers and service providers [35]. These data include the private information of customers, such as activities, devices being used and times at which the home is vacant. Abnormal user access and control packets of the SDN are protected by secure socket layer (SSL) and digital mark-based packet-inspection algorithms. The traditional packet-inspection system that is used as a firewall may be degraded because of the large network scale of the smart grid. In addition, the network installation cost will increase when the number of firewalls in the network is increased. However, SDN can provide packet inspection without specialized hardware, which allows dynamic protection rule updates by a system administrator. The ForNox is a role-based access control system for SDN [39]. In this scheme, the SDN controller inserts the validated digital sign to all control packets, and it is encapsulated by using a pre-shared key. Further, the SDN control channels are protected by the SSL protocol [29]. Rowan et al. presented an SDN security analysis model for information disclosure, denial of service and tampering attack detection [40]. In this algorithm, the SDN controller randomly chooses the sample packets and data flow table from the network devices. The collected sample data are analyzed using Microsoft STRIDE [40] and attack tree modeling methods, and experimental results show that the SDN effectively isolates and detects the abnormal flows without the need for an additional network monitoring system.

5. Further Research Opportunities of the SDN-Enabled Smart Grid

SDN is an emerging and promising future networking solution, but it needs to be optimized for use in a smart grid environment. Traditional SDN is designed for rich resource systems that are generally considered for backhaul IP networks. From a network design perspective, SDN-enabled smart grid systems require an additional network processing server, which must consider the end-to-end route between the SDN controller and each smart grid device in the region. Therefore, the communication overhead between the SDN controller and devices needs to be optimized in order to reduce network congestion, bottlenecks and computational delay problems. Challenging issues pertaining to the SDN-enabled smart grid system are as below:

- Reducing SDN control message overhead: In spite of the different benefits, such as simplified network and system management, SDN may not be directly utilized in resource-constrained AMI networks because of the control message and end-to-end session-management overhead. Generally, the SDN controller and all clients periodically exchange control messages for service provisioning and monitoring via a secure path. These control messages use secure control paths that are logically isolated from the data path using SSL or virtual private networks (VPNs). However, the MAC and physical perspective of the communication interface control and data packet use the same physical interface. Further, SSL-based data communication requires end-to-end session management control packets that are periodically exchanged between the SDN controller and all devices in the network. From a security perspective, control and data channel isolation are acceptable methods, but the end-to-end transmission reliability of the data packet can suffer from network congestion due to the SDN control traffic. In addition, when the control message between the controller and device is not stably delivered, metering traffic cannot be transmitted, even if the network capacity is sufficient. In particular, resource-constrained smart grid networks, such as wireless HANs, need to consider low-overhead message exchange protocols, such as Internet Engineering Task Force (IETF)-Constrained Application Protocol (CoAP), to reduce congestion and realize a reliable SDN-enabled smart grid [41,45].
- Route construction between SDN controller and clients: SDN enables flow-based data forwarding that can replace the traditional distributed routing protocols. This centralized routing is a key feature of SDN, but during the network initialization stage, each client needs to find a default route path to the SDN controller [42]. To solve this problem, a distributed routing protocol, such as OSPF, is considered for simultaneous use with SDN in wired SDN, but it is not suitable for use in resource-constrained wireless and PLC-based HANs. To solve this problem, the SDN-enabled smart grid must use the default routing function, which provides a dynamic configuration to legacy routing protocols, or discover the routing path by using an SDN routing application. In HANs, the routes between the SDN controller and a device are constructed using a link discovery procedure. Generally, the SDN controller uses a link discovery application that enables it to find the adjacent one-hop neighbor SDN controller of the device. Meanwhile, the device that is connected to the SDN controller can respond to the link discovery request with SDN connection flags. This connection information can be sequentially flooded to the entire

network, and the default routes between the SDN controller and the devices are established without additional routing protocols.

- **SDN controller and function distribution:** In a large-scale smart grid network, the flow information request messages from all clients are concentrated at an SDN controller. There is the potential problem of network congestion, queue overflow, large processing delay and service instability of the SDN. To solve this problem, multiple SDN controllers need to be distributed to the network and HES. In the case of multiple SDN controllers, all of them need to share the common management policy of the network. For example, the elastic SDN controller distribution (ElastiCon) algorithm can be utilized for a large-scale smart grid network [43]. In this algorithm, the SDN controllers are classified as a master and slaves. The master SDN controller can be located in the HES, and slaves are inserted at the substations. The master SDN controller assigns and distributes the slave SDN controllers to the network depending on the link capacity of the switch or router. Further, the SDN network functions (application) are distributed to the multiple slaves. During the migration process between the master and sub-controllers, at least one controller is activated to avoid a service suspension problem. The experimental results show that the network congestion, end-to-end control message delay, flow request-response time problem can be solved by using an elastic controller distribution system.
- **Interoperable design between IEC 61850 and SDN protocols:** In traditional layered networking architecture, communication strategies, such as routing policy, QoS policy and MAC parameters, may not dynamically adapt to applications and services. However, an SDN-enabled smart grid network can be optimized for specific smart grid services by using IEC 61850 standard profiles. The IEC 61850 protocol is the de facto application standard of the smart grid [12]. The information model of the smart grid substation is defined in IEC 61850-7, and the configuration language is also defined in IEC 61850-6. The IEC 61850 application defines the power-monitoring interval, transmission type (IEC 61850 Manufacturing Message Specification or multicast) and service priorities. The IEC 61850 uses the XML (or JSON) data format, which can be decoded using SDN applications because the SDN API basically uses the XML and JSON formats to exchange control messages between the SDN controller and clients. Thus, the service profile of the IEC 61850 can be simply identified and utilized for the network configuration. By using an interoperable management architecture between IEC 61850 and SDN, the service capability of the SDN-enabled smart grid can be extended from the network to smart grid application management.
- **Interoperable controller system:** Interoperability among different SDN architectures needs to be considered for SDN-enabled smart grid systems [45]. This is because SDN is implemented by a vendor-neutral strategy, depending on the capability and business goal of the service domain, without the need for any international agreement. In particular, northbound API and SDN controller systems need to be standardized to realize simplified communication and the development of smart grid SDN applications.

6. Conclusions

The complexity and heterogeneity of smart grid services are rapidly increasing because of the increased usage of IEDs, automation and service integration between utility domains. However, traditional networks that focus on distributed packet-forwarding strategies may not dynamically adapt to different business models, because the context and situation status of the application cannot be directly utilized for network configuration. Instead of the legacy networking system, in recent years, the SDN paradigm has been considered for the smart grid network infrastructure. However, traditional SDN architectures need to be optimized for the smart grid environment, and this process is still at the initial stages.

In this paper, we investigated the current information subsystem, communication infrastructure of the smart grid and an emerging communication infrastructure called the SDN-enabled smart grid. In particular, we described the SDN-enabled smart grid architecture in detail, as well as the abstracted business model process of the service provider, a candidate SDN-enabled smart grid application and system architecture. Finally, we presented a comparison of current SDN-enabled smart grid systems and categorized the examined network services and applications that have been developed based on the SDN paradigm. To the best of our knowledge, this is the first such comparison of studies into SDN-enabled smart grid communication infrastructures. Finally, we identified challenging issues affecting the current SDN-enabled smart grid and proposed possible solutions.

Acknowledgments

This publication was made possible by the National Priorities Research Programme (NPRP) award (NPRP 6-244-2-103) from the Qatar National Research Fund (a member of The Qatar Foundation). The statements made herein are solely the responsibility of the author(s).

Author Contributions

Jaebeom Kim and Fethi Filali conceived of the principle reported in this work for the current smart grid architecture and its trends. Young-Bae Ko categorized the current ICT subsystems of the smart grid and its sub-technologies from communication infrastructure and services. Jaebeom Kim and Fethi Filali jointly developed an abstract SDN-enabled smart grid architecture model and its related work. Jaebeom Kim wrote the paper.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Locke, G.; Gallagher, P.D. *Nist Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*; National Institute of Standards and Technology: Gaithersburg, MD, USA, January 2010.

2. Güngör, V.C.; Sahin, D.; Kocak, T.; Ergüt, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart Grid technologies: Communication technologies and standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539.
3. Liserre, M.; Sauter, T.; Hung, J.Y. Future energy systems: Integrating renewable energy sources into the smart power grid through industrial electronics. *IEEE Ind. Electron. Mag.* **2010**, *4*, 18–37.
4. Hauser, C.H.; Bakken, D.E.; Bose, A. A failure to communicate: Next generation communication requirements, technologies, and architecture for the electric power grid. *IEEE Power Energy Mag.* **2005**, *3*, 47–55.
5. Fang, X.; Misra, S.; Xue, G.; Yang, D. Smart Grid—The new and improved power grid: A survey. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 944–980.
6. Kim, J.; Kim, D.; Lim, K.-W.; Ko, Y.-B.; Lee, S.-Y. Improving the reliability of IEEE 802.11 s based wireless mesh networks for Smart Grid systems. *J. Commun. Netw.* **2012**, *14*, 629–639.
7. Niyato, D.; Xiao, L.; Wang, P. Machine-to-machine communications for home energy management system in Smart Grid. *IEEE Commun. Mag.* **2011**, *49*, 53–59.
8. Bauer, M.; Plappert, W.; Wang, C.; Dostert, K. Packet-oriented communication protocols for Smart Grid services over low-speed PLC. In Proceedings of the IEEE International Symposium on Power Line Communications and Its Applications, ISPLC 2009, Dresden, Germany, 29 March–1 April 2009; pp. 89–94.
9. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major Smart Grid applications in han, nan and wan. *Comput. Netw.* **2014**, *67*, 74–88.
10. Yi, P.; Iwayemi, A.; Zhou, C. Frequency agility in a zigbee network for Smart Grid application. In Proceedings of the Innovative Smart Grid Technologies (ISGT), Gaithersburg, MD, USA, 19–21 January 2010; pp. 1–6.
11. Bumiller, G.; Sauter, T.; Pratl, G.; Treytl, A. Secure and reliable wide-area power-line communication for soft-real-time applications within REMPLI. In Proceedings of the 2005 International Symposium on Power Line Communications and Its Applications, Vancouver, Canada 6–8 April 2005; pp. 57–60.
12. Molina, E.; Jacob, E.; Matias, J.; Moreira, N.; Astarloa, A. Using software defined networking to manage and control IEC 61850-based systems. *Comput. Electr. Eng.* **2015**, *43*, 142–154.
13. Goodney, A.; Kumar, S.; Ravi, A.; Cho, Y.H. Efficient PMU networking with software defined networks. In Proceedings of the 2013 IEEE International Conference on Smart Grid Communications (Smart GridComm), Vancouver, BC, Canada, 21–24 October 2013; pp. 378–383.
14. Cahn, A.; Hoyos, J.; Hulse, M.; Keller, E. Software-defined energy communication networks: From substation automation to future Smart Grids. In Proceedings of the 2013 IEEE International Conference on Smart Grid Communications (Smart GridComm), Vancouver, BC, Canada, 21–24 October 2013; pp. 558–563.
15. Zhang, J.; Seet, B.-C.; Lie, T.-T.; Foh, C.H. Opportunities for software-defined networking in Smart Grid. In Proceedings of the 2013 9th International Conference on Information, Communications and Signal Processing (ICICS), Tainan, Taiwan, 10–13 December 2013; pp. 1–5.
16. Parniewicz, D.; Doriguzzi Corin, R.; Ogradowczyk, L.; Rashidi Fard, M.; Matias, J.; Gerola, M.; Fuentes, V.; Toseef, U.; Zaalouk, A.; Belter, B. Design and implementation of an openflow hardware abstraction layer. In Proceedings of the 2014 ACM SIGCOMM workshop on Distributed cloud computing, Chicago, IL, USA, 17–22 August 2014; pp. 71–76.

17. Pullins, S. *West Virginia Smart Grid Implementation Plan*; Technical Report DOE/NETL-2009/1386; West Virginia Division of Energy, National Energy Technology Laboratory, US Department of Energy, Morgantown, WV, USA, November 2009.
18. Logenthiran, T.; Srinivasan, D.; Shun, T.Z. Demand side management in Smart Grid using heuristic optimization. *IEEE Trans. Smart Grid* **2012**, *3*, 1244–1252.
19. Pendarakis, D.; Shrivastava, N.; Liu, Z.; Ambrosio, R. Information aggregation and optimized actuation in sensor networks: Enabling smart electrical grids. In Proceedings of the 26th IEEE International Conference on Computer Communications, INFOCOM 2007, Anchorage, AK, USA, 6–12 May 2007; pp. 2386–2390.
20. Luan, W.; Sharp, D.; Lancashire, S. Smart Grid communication network capacity planning for power utilities. In Proceedings of the 2010 IEEE PES Transmission and Distribution Conference and Exposition, New Orleans, LA, USA, 19–22 April 2010; pp. 1–4.
21. Vytelingum, P.; Voice, T.D.; Ramchurn, S.D.; Rogers, A.; Jennings, N.R. Agent-based micro-storage management for the Smart Grid. In Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems, Toronto, ON, Canada, 9–14 May 2010; Volume 1, pp. 39–46.
22. Momoh, J. Smart Grid design for efficient and flexible power networks operation and control. In Proceedings of the PSCE 2009 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, USA, 15–18 March 2009; pp. 1–8.
23. Moreno-Munoz, A.; de La Rosa, J.G. Integrating power quality to automated meter reading. *IEEE Ind. Electron. Mag.* **2008**, *2*, 10–18.
24. Meehan, B. *Enterprise Gis and the Smart Electric Grid*; Electric Power White Paper, ESRI, 2008.
25. Jeremy, P. *Optimizing the Performance of Smart Grid Technologies*; Business Insights White Paper, Pitney Bowse, 2010.
26. Bari, A.; Jiang, J.; Saad, W.; Jaekel, A. Challenges in the smart grid applications: An overview. *International Journal of Distributed Sensor Networks*, **2014**, *2014*, 1–11.
27. Giordano, V.; Fulli, G. A business case for Smart Grid technologies: A systemic perspective. *Energy Policy* **2012**, *40*, 252–259.
28. Hashmi, M.; Hänninen, S.; Mäki, K. Survey of Smart Grid concepts, architectures, and technological demonstrations worldwide. In Proceedings of the 2011 IEEE PES Conference on Innovative Smart Grid Technologies (ISGT Latin America), Medellin, Colombia, 19–21 October 2011; pp. 1–7.
29. Shirazipour, M.; John, W.; Kempf, J.; Green, H.; Tatipamula, M. Realizing packet-optical integration with sdn and openflow 1.1 extensions. In Proceedings of the 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 10–15 June 2012; pp. 6633–6637.
30. Jarschel, M.; Wamser, F.; Hohn, T.; Zinner, T.; Tran-Gia, P. Sdn-based application-aware networking on the example of youtube video streaming. In Proceedings of the 2013 Second European Workshop on Software Defined Networks (EWSDN), Berlin, Germany, 10–11 October 2013; pp. 87–92.
31. Salsano, S.; Blefari-Melazzi, N.; Detti, A.; Morabito, G.; Veltri, L. Information centric networking over sdn and openflow: Architectural aspects and experiments on the ofelia testbed. *Comput. Netw.* **2013**, *57*, 3207–3221.

32. Magoutas, B.; Apostolou, D.; Mentzas, G. Situation-aware demand response in the Smart Grid. In Proceedings of the 2011 16th International Conference on Intelligent System Application to Power Systems (ISAP), Hersonissos, Greece, 25–28 September 2011; pp. 1–6.
33. Byun, J.; Hong, I.; Kang, B.; Park, S. A smart energy distribution and management system for renewable energy distribution and context-aware services based on user patterns and load forecasting. *IEEE Trans. Consum. Electron.* **2011**, *57*, 436–444.
34. Dorsch, N.; Kurtz, F.; Georg, H.; Hagerling, C.; Wietfeld, C. Software-defined networking for Smart Grid communications: Applications, challenges and advantages. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (Smart GridComm), Venice, Italy, 3–6 November 2014; pp. 422–427.
35. Wang, X.; Yi, P. Security framework for wireless communications in smart distribution grid. *IEEE Trans. Smart Grid* **2011**, *2*, 809–818.
36. Sydney, A.; Ochs, D.S.; Scoglio, C.; Gruenbacher, D.; Miller, R. Using geni for experimental evaluation of software defined networking in Smart Grids. *Comput. Netw.* **2014**, *63*, 5–16.
37. Cuomo, F.; Abbagnale, A.; Cipollone, E. Cross-layer network formation for energy-efficient IEEE 802.15.4/zigbee wireless sensor networks. *Ad Hoc Netw.* **2013**, *11*, 672–686.
38. Qin, Z.; Denker, G.; Giannelli, C.; Bellavista, P.; Venkatasubramanian, N. A software defined networking architecture for the internet-of-things. In Proceedings of the 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 5–9 May 2014; pp. 1–9.
39. Pfeifferberger, T.; Du, J.L. Evaluation of software-defined networking for power systems. In Proceedings of the 2014 IEEE International Conference on Intelligent Energy and Power Systems (IEPS), Kyiv, Ukraine, 2–6 June 2014; pp. 181–185.
40. Kloti, R.; Kotronis, V.; Smith, P. Openflow: A security analysis. In Proceedings of the 2013 21st IEEE International Conference on Network Protocols (ICNP), Goettingen, Germany, 7–10 October 2013; pp. 1–6.
41. Castellani, A.P.; Gheda, M.; Bui, N.; Rossi, M.; Zorzi, M. Web services for the internet of things through CoAP and EXI. In Proceedings of the 2011 IEEE International Conference on Communications Workshops (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–6.
42. Das, S.; Parulkar, G.; McKeown, N. Why Openflow/SDN can succeed where GMPLS failed. In Proceedings of the 2012 38th European Conference and Exhibition on Optical Communication, Amsterdam, The Netherlands, 16–20 September 2012; pp. 1–3.
43. Dixit, A.; Hao, F.; Mukherjee, S.; Lakshman, T.; Kompella, R. Towards an Elastic Distributed SDN Controller; In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking, Hong Kong, China, 12–16 August 2013; pp. 7–12.
44. Dong, X.; Lin, H.; Tan, R.; Iyer, R.K.; Kalbarczyk, Z. Software-defined networking for Smart Grid resilience: Opportunities and challenges. In Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Singapore, 14–17 April 2015; ACM: New York, NY, USA; pp. 61–68.
45. Kim, J.; Y.-B., K.; Fethi, F. A Lightweight CoAP-based Software Defined Networking for Resource Constrained AMI Devices. In Proceedings of the IEEE International Conference on Smart Grid Communications (Smart GridComm), Miami, FL, USA, 2–5 November 2015; pp 1–6

46. Fusitus. *Software-Defined Networking for the Utilities and Energy Sector*; Fujitus White Paper, Fusitus, 2014.

© 2015 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>).