IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 29, 2021, accepted July 1, 2021, date of publication July 7, 2021, date of current version July 19, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3095317

Software-Defined Power Grids: A Survey on Opportunities and Taxonomy for Microgrids

MUSA NDIAYE[1], GERHARD P. HANCKE[2,4], (Life Fellow, IEEE), ADNAN M. ABU-MAHFOUZ[3,4], (Senior Member, IEEE), AND HUIFENG ZHANG[2], (Member, IEEE)

[1]Department of Electrical Engineering, Copperbelt University, Kitwe 10101, Zambia
[2]College of Automation and College of Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[3]Council for Scientific and Industrial Research, Pretoria 0083, South Africa
[4]Department of Electrical, Electronic, and Computer Engineering, University of Pretoria, Pretoria 0028, South Africa

Corresponding author: Gerhard P. Hancke (g.hancke@ieee.org)

ABSTRACT Future generation power grids will require the introduction and deployment of distributed energy resources to meet modern-day load requirements. Consequently, we expect to see a rise in microgrids (MGs) existing as part of the main grid (grid-connected) or independent (islanded). Contained in these microgrids are a combination of energy resources such as solar, wind and fossil fuels coupled with storage devices, electric vehicles and smart devices supporting the prosumer operation. However, the addition of renewable energy resources would mean fluctuations in energy supply which would cause power system instability if not managed effectively. Hence, to maximize the management flexibility of MGs, the concept of microgrid software definition is introduced. A concept that can be looked at as giving the microgrid an operating system to improve operation response and event detection by maintaining a global view of the network. This paper therefore critically analyses what this entails by presenting an architecture for Software-Defined Microgrids (SDMGs) and discussing the management opportunities that softwarization of the MG introduces. We also highlight the design requirements and associated challenges in implementing and deploying SDMGs.

INDEX TERMS Energy balancing, grid resiliency, microgrids, power grid management, software-defined networking, smart grids.

I. INTRODUCTION

Traditional power grids have long been faced with reluctance by power utility companies to adopt modern digital communication technologies for effective control of grid stability [1]. Implementation of control has been limited to monitoring blackouts, faults, and the management of load-shedding. Additionally, the push for renewable energy sources and the rise of prosumer households has received challenges taking into consideration that traditional power grids were not initially designed to support two-way power generation. The integration of microgrids in distributed power systems has long been considered a system stability risk as sudden fluctuations in power generation or consumption can lead to power system failures. While it is necessary to push for renewable power generation and integration, there is a need for greater system control if power system stability and efficiency are to be maintained.

Modern power distribution networks consist of a hybrid of power sources such as the main utility supply and a combination of solar, wind, thermal, etc. Some implementations require supply and distribution over a very vast area such as desert locations with very long distances between power sources and consumers. In Australia for example, such distribution needs have been encountered and mostly it is not feasible to run power lines across large desert distances. As such power utility companies have resorted to the development of microgrids in the required remote locations. Effectively what we get is a network of multiple power generators feeding into a common grid. How do we ensure greater system control to improve stability, efficiency and reduce cost?

The answer is fast becoming the need to softwarize traditional power grids as we know them. How about if the entire power grid was visualized as having an operating system similar to computers? This revolution has led to what is known as

The associate editor coordinating the review of this manuscript and approving it for publication was Mahdi Pourakbari Kasmaei.

Software-Defined Power Grid (SDPG), a paradigm that has long been implemented and utilized in computer networks. The concept of Software-Defined Networking (SDN) is based on the principle that the entire network control logic is moved to a logically centralized controller with a global view of the whole network and higher computational resources. SDN has been known to significantly improve network management and control while maintaining resource efficiency. A centralized power system controller can be used to control generation and loads in the grid based on collected system data at various points in the grid [2].

Katiraei *et al*. [3] mention that for microgrids to excel in implementation and acceptability there has to be extensive development in controller capabilities and microgrid operationality. Factors such as the depth of Distributed Energy Resource (DER) implementation, power quality constraints, load profile and market strategies affect the level of control required for a microgrid. The various levels of control required can be provided as algorithms implemented in the SDPG controller. In this light, this paper surveys the opportunities and derives the general taxonomy of SDPGs for microgrid management.

A. SUMMARY OF CONTRIBUTIONS

In recent years, the idea of software-defined power grids has been presented in several ways. Works from power grid network reprogrammability [4] to decoupling the cyber-physical layer of power grids [5]–[7] and also in form of a case study targeting a particular benefit microgrid softwarization [1]. The works present efforts and reviews on portions of this software-defined paradigm such as security concerns, resiliency, control. Thus we observed a gap especially concerning microgrids for a thorough and consolidated review and investigation of software-defined opportunities.

We aim in this work to look at multiple aspects of giving a microgrid an operating system including control, security, resiliency, energy management and general system design. All this while bringing together efforts by researchers in this particular microgrid area. In summary, this paper makes the following significant contributions to knowledge:

1) It brings together a critical analysis of what software definition can bring to the microgrid as we know it.
2) It presents an easy transition to Software-Defined Microgrid (SDMG) framework (based on Phasor Measurement Unit (PMU) data) both from the cyber/ physical standpoint and from the communication protocol standpoint.
3) It discusses in detail the design requirements of a taxonomy based on SDN for microgrid control and its associated challenges.

B. TAXONOMY OF THE PAPER

The rest of this paper is organized as follows: Section II presents a brief background to the concept of SDPGs in general. It also looks at some related works to this survey that attempt to discuss softwarization of microgrids. Section III discusses the existing technologies that support the easy transition from ordinary microgrids to SDMGs while Section IV highlights the various opportunities that software-defined control introduces to microgrids. In Section V, we discuss the various design requirements for developing and implementing a SDMG as well as the associated challenges. Section VI summarises some important lessons learnt thus far while highlighting future research opportunities. The paper is then concluded in Section VII.

The overall layout of this paper is shown in Fig. 1.

II. BACKGROUND

A. SOFTWARE-DEFINED POWER GRIDS

Software definition of a power grid has taken different stages and formats over the years. The idea of managing and controlling the grid from a centralized system (controller) has been approached since the era of Supervisory Control and Data Acquisition (SCADA). However, the management of power grids based on traditional SCADA was limited to minimal control functions and generally rigid [8]. The development of smart devices in the power grid and consequently SDN-based smart grids increased the level of management flexibility from a centralized controller.

Since then, there have been multiple proposals and test-beds for cyber-physical power grids (smart grids in particular), SDN-based power grids [9]–[12] and more recently SDMGs. The low inertia and intermittent nature of Renewable Energy Resources (RER) in microgrids have raised the need for more investigation into SDN-based control. In this work, we aim to bring together the works done in this particular microgrid area, leading up to what is known as the SDMG. First, we take a look at similar review papers in this SDMG area.

B. RELATED WORK

Network programmability featured in SDN has been highlighted to introduce management flexibility in microgrids [4]. SDN solutions to microgrid management were proposed to improve microgrid resiliency to cyber-attacks and physical disturbances.

Furthermore, a road map to secure and cyber-resilient microgrids based on SDN is presented in [13]. The authors presented opportunities and challenges that SDN introduces towards achieving improved security in microgrids. The work focused mainly on the cyber-security architecture of SDMGs based on the global controller visibility and programmability.

In their survey of SDN-based smart grid communications, Rehmani *et al.* [14] mentioned Networked Microgrid (NMG)s to be an essential requirement of smart cities. NMGs would take advantage of SDN in enabling flexible coordination and sharing of energy. This SDN-based approach would improve power deficiency problems in NMGs while accelerating system recovery.

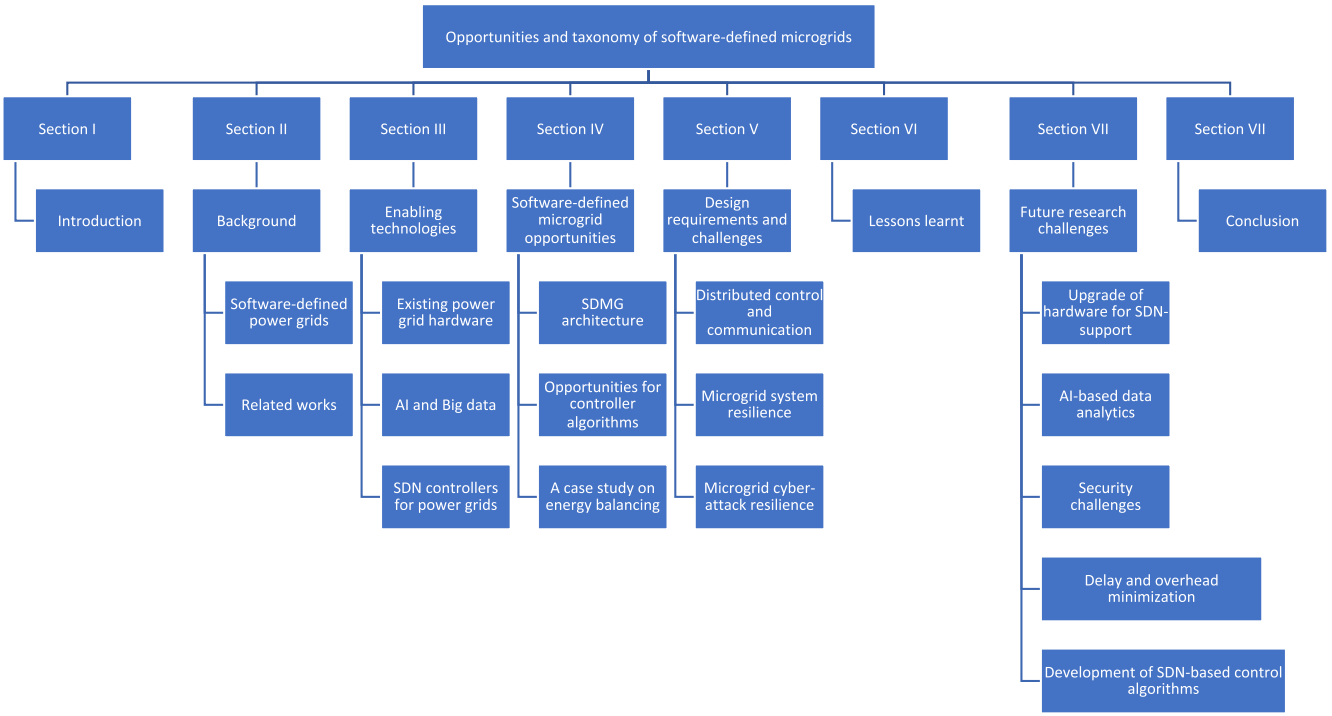

FIGURE 1. Taxonomy of paper.

Closely tied to SDMG operation are cyber-physical microgrids. Vu *et al.* [5] presented a comprehensive review on cyber-physical strategies for microgrid resiliency towards cyber-attacks. An SDN-based centralized controller had been highlighted to optimize management and control of the cyber-layer to improve the quality of service. The work presented here mostly focused on resiliency towards cyber-physical attacks in MGs mainly through network monitoring and control strategies.

In light of this, a review article further discussed new challenges in the cyber-physical architecture of microgrids [15]. Although the article did not solely focus on SDN control of MGs, it highlighted how separation of the physical layer and the cyber layer improved microgrid resiliency, particularly under cyber-attacks. Adequate definition and control of the communication framework in MGs is key to maximizing resilience. Similarly, this has been supported in [16] while hinting at investigating the potential benefits of SDN in MGs under future works. In our work, we marry this requirement of a robust cyber-physical framework with the opportunities featured in SDN-based MGs.

Table 1 presents a summary comparison of the related works discussed in this section against our work.

III. ENABLING TECHNOLOGIES AND APPLICATIONS

A. EXISTING POWER GRID HARDWARE

One of the deployment goals of SDPGs is the low cost of deployment. This entails minimal hardware requirements and modifications to the power grid as we know it. Therefore, the technology should use existing hardware as much as possible. Critical enabling hardware for software definition of a power grid comes from the already existing data acquisition framework. SCADA systems have long been implemented in power grids for low-level control of switches and fault monitoring. However, to achieve the rapid response time and higher-level control that SDPG promises, there is a need for a higher frequency, precision and resolution of the grid status data.

PMUs are grid-based sensor devices that provide real-time synchronous phase and voltage data known as synchrophasors. Syncrophasors measured by PMUs provide the backbone for effective monitoring and control of a potential software-defined grid. This phasor data has also formed a smart grid platform for control algorithms to make decisions [17] effectively. Integration with Global Positioning System (GPS) with PMUs has led to synchrophasor generation aligned to a common time base. GPS-based PMUs can be deployed as part of a Wide Area Management System (WAMS) for smart grids. Prototypes of GPS-based PMUs have been in development since the 1080s [17]. Synchrophasors allow PMU-based systems to make decisions within a 100th of a millisecond [18] providing essential support of smart grid applications and software-defined control.

In a distributed grid system, several PMUs can be deployed sending data to a Phasor Data Concentrator (PDC). For software-defined applications, the PDC can exist as part of a local controller implementation. The PDC collects PMU data and arranges it according to received time for use by the embedded control algorithms in the controller [18], [19]. For microgrid applications, PMUs can be used to measure

TABLE 1. A comparison of related review articles on aspects of SDN-based Microgrids (✓ indicates aspect has been covered, ✗ indicates aspect has not been covered, and ∗ indicates that the aspect is partially covered or not directly related to SDN.

Reference	Focus area	SDN-based microgrid control aspects				
		PMU-based	Energy Management (Balancing and storage)	Artificial Intelligence	Security	Architecture design and challenges
Ren *et al.* [4]	Microgrid resiliency	∗	∗	✗	✓	∗
Jin *et al.* [13]	Microgrid cyberattack resiliency	✓	✗	∗	✓	✓
Rehmani *et al.* [14]	Smart grid communications	✓	∗	✗	✓	∗
Vu *et al.* [5]	Microgrid cyber attack resiliency	✗	∗	∗	∗	✗
Tan *et al.* [15]	Microgrid communications, cyberattacks and resiliency	✗	✗	✗	∗	∗
This survey	Microgrid management	✓	✓	✓	✓	✓

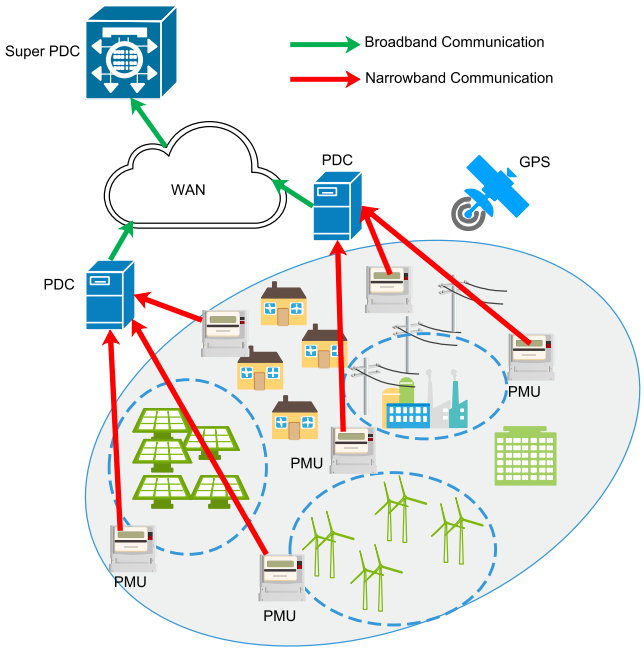

FIGURE 2. Synchrophasor data collection in a distributed power grid, adapted from [18], [19].

synchrophasors between renewable energy generation/ storage units and the grid bus and also in the main bus itself. The collected data from each PMU can be transmitted over a narrowband communication channel to the PDC, while communication between the local controller-based PDC and the super-PDC or global controller for software-defined applications can be made over wide bandwidth channels. Fig. 2 shows a typical distributed PMU deployment in a power grid [18], [19].

Apart from hardware supporting synchrophasor data collection, the use of smart switches and DER provides support for software-defined control. This existing hardware includes the use of power electronic coupling converters in a microgrid to provide software-defined system-level control.

B. ARTIFICIAL INTELLIGENCE AND BIG DATA

Software-defined control of power grids will result in large amounts of power system data being collected for purposes of control. The multiple PMUs deployed across the network will consequently generate big data. Therefore, existing Artificial Intelligence (AI) technologies would serve as an enabler for analyzing this big data and using it for prediction-based performance of the power grid. Machine learning and reinforcement learning can be used to increase the power grid resilience against sudden fluctuation in RER performance and cyber-attacks.

There have been several applications in the literature highlighting the use of AI techniques in managing power grids and smart grids in particular [20]–[23] and this provides promising importance in the control and management of SDPGs. The existence of these AI enabling technologies means there will be less effort and cost in implementing them for the benefit of SDPGs. The effort would mostly go into optimizing these techniques based on the requirement of grid network managers. Further in this work, we will look at the opportunities that AI-based technologies provide for the management of SDMGs.

C. SDN CONTROLLERS FOR POWER GRIDS

Softwarization of the grid based on SDN requires the use of controllers handling grid operations based on the maintained global view. There already exist controllers being used for ordinary SDN such as ONOS, Ryu, OpenDayLight, NOX, POX, etc [24]. As regards to whether these controllers can be used in their original state for management of SDMGs still remains an area of research interest.

However, in their efforts to provide a programmable microgrid network, Ren *et al.* [4] use a customized version of the Ryu controller. They mention that customization is necessary to meet the QoS requirements for emergency control of the microgrid. They again use the Ryu controller [4] to demonstrate distributed power-sharing in microgrids based on SDN with little mention of modification. The Ryu framework was mainly used to provide an API between the controller and the OpenFlow switch. In their SDN-based communications power grid network, Cahn *et al.* [11] use Ryu as it is based on their choice of programming language (Python) and open-sourceness of the controller.

On the other hand, the ONOS controller has been used in a testbed for cyber-physical microgrids as it is with little modification [13]. The generic feature of distributed SDN control in ONOS is used to monitor and manage the emulated communication network for the testbed. The NOX controller has been used in [12] without mention of much modification in demonstrating SDN-based smart grid resiliency.

The fact that researchers have successfully demonstrated the use of common SDN controllers such as ONOS and Ryu in deploying SDN-based control of microgrids shows further how cost-effective SDMGs can be. Re-usability of tools and devices is a feature that supports rapid, sustainable and cost-effective deployment of upcoming technologies such as SDMGs. It is however necessary to investigate the multiple SDN controllers available and identify their merits and demerits when it comes to managing SDMGs particularly.

Table 2 shows some of the SDN controllers used for power grid control applications.

IV. SDPG OPPORTUNITIES FOR MICROGRIDS

A. THE SOFTWARE-DEFINED MICROGRID ARCHITECTURE

MGs can be identified as local power stations that can be main-grid connected or distributed. Lasseter [27] defines a microgrid as a cluster of loads and micro-energy resources existing as a single controllable system servicing a local area. Increasing interest from industry and academia in renewable energy sources and advanced energy storage systems has led to a push in MG deployment. This is coupled with an increased variety of loads and smart grid infrastructure. Additionally, load distribution over vast areas existing in remote islanded areas requires local grids deployed as part of a network of microgrids.

Advances in communication technologies such as SDN have enabled the MG architecture to be more distributed and intelligent. Enabling technologies in the architecture allows for improvements in data communication and ensure power system stability. Tan *et al.* [15] state in their article that a distributed MG should be energy-efficient, connected, intelligent and flexible. SDN has been cited to provide management flexibility in these four key areas [14].

SDMGs should address the requirements of greater communication and control of MGs. A generic architecture of SDMGs should consider two modes of deployment:

- Neighbourhood area networks: This is tightly knit with home area networks consisting of home-based RER and consumer loads. An example is a gated community that has its loads supplied by energy sources such as solar within the community independent of the main grid. The community can be part of a grid-connected metropolitan city but can exist as a single controllable microgrid. In this mode power and communication flow can be bidirectional between the main grid and microgrid supported by smart metering and controllers respectively.
- Wide area networks: Remote locations that require microgrids to supply power to local loads due to very large distances from the main grid define this mode of deployment. A scenario may exist where a vast desert area separates the main grid and remote location making it economically not feasible to run long haul transmission lines across the desert area. In this case, the remote area should have a self-sustaining and independent microgrid for the various loads that exist therein. Power flow is between the loads, energy storage units and energy sources while communication flow can still be bidirectional between the microgrid and the main grid via a global controller and long-range communication protocols.

In general, a software-defined microgrid architecture should contain the following components:

- Consumer loads: The demand side of a power grid is made up of consumer loads such as home appliances, lighting and electric vehicles. Depending on the size of the microgrid energy supply, the demand side can also consist of small-scale industrial loads.
- Energy resources: Energy sources in a microgrid make up the supply side of the architecture and include home-based solar and wind power generators. Mini fossil fuel power plants can also be implemented to supply energy to a microgrid. Smart inverter technology needs to be included as part of the SDMG architecture. Controller algorithms can take advantage of smart inverters to control the power output to the microgrid based on grid status.
- Energy storage units: Renewable energy resources mostly require the addition of energy storage units to reserve power for use when renewable resource such as solar or wind are unavailable. Battery banks make up a significant portion of energy storage and for smart city applications, the use of electric vehicles as energy storage vessels is becoming popular. The concept of Vehicle to Grid (V2G) to dispatch energy at various locations in a grid has been proposed for smart grid implementations [14], [28], [29]. An electric vehicle can be dispatched via a controller to supply energy to the microgrid to smooth out a sudden dip in energy supply from renewable resources. Software-definition of a microgrid plays a key role in this application.
- Data collection units: Data forms the backbone of a SDMG control. Controllers can use data to issue and

TABLE 2. Some use-cases for potential SDMG controllers.

SDN Controller	Application	Targeted feature	Modification
Ryu	Provision of a programmable power grid network [4], Distributed power sharing in MGs [25], Power grid communication network [11]	Controller to OpenFlow API [4], [25], Python-based and open source [11]	YES [4], [25], NO [11]
ONOS	Monitoring and control of power grid communication network [13], SDN-based smart distribution grid resiliency [16]	Distributed SDN control [13], Pre-configured provisions for multiple virtual machine instances [16]	NO [13], [16]
NOX	SDN-based smart grid resiliency [12]	Ability to implement grid monitoring and control [12]	-
OpenDaylight	Threat analysis of industrial control system for MGs [26]	OpenFlow support mostly [26]	NO [26]

also predict system performance instructions. Grid status data for SDMGs extends more than blackout or fault data with PMUs providing a high resolution of voltage and phasor data at specific geolocations in the grid. The time-stamped synchrophasor data provided by PMUs increase the accuracy of detection and speed of control of at least two orders of magnitude than that provided by SCADA technology [30].

- Controllers: Functionality of a SDMG is executed in controllers. Therefore, controller hardware and software form an essential part of SDMGs. Control algorithms, monitoring and simulation tools usually PC-based provides the logical global control of the microgrid. Clusters of the microgrid can be assigned local controllers providing the resilience of a distributed controller framework [31], [32]. Distributed control allows for the assignment of control levels to each energy resource and storage units reducing the response time and improving the system efficiency. A global or master controller can coordinate grid operations between microgrids and the main power grid via long-haul communications protocols in wide area network setups.

Fig. 3 illustrates the generic architecture of a SDMG with the components discussed in this section.

B. OPPORTUNITIES FOR SDMG CONTROLLER ALGORITHMS

The operation and control of a microgrid can be significantly and conceptually different from ordinary power grids. Some of the reasons resulting in unique control requirements include [3]:

- Dynamic characteristics of DER units such as solar, wind and thermal can result in a significant imbalance in the microgrid. This is coupled with the effects of single-phase loads present in the microgrid.
- DERunits such as wind and solar can be classified as uncontrollable sources that may result in rapid power system performance fluctuations.
- Energy storage systems such as batteries and electric-vehicle present in the microgrid may require greater control to aid the operation of the power system.
- In some cases the microgrid may be required to provide a specific power quality level to some loads.
- Microgrid control should also take into account the economics and security of operation. Grid devices should accommodate the implementation of security, economic (billing) and isolation features all while still maintaining operation.

Controls of a microgrid can be divided into either interactive or non-interactive [3]. Non-interactive methods such as algorithms for achieving Maximum Point of Power Tracking (MPPT) can be implemented on DERs upon deployment and may not require frequent interaction post-deployment. Other algorithms such as voltage and frequency control may also be non-interactive depending on the application. However, with the unpredictable performance of DERs in a microgrid, there is a need for interactive control of voltages, frequencies, load sharing, power dispatch from storage devices, real and reactive power support.

The concept of software-defined control potentially provides extensive support mainly for interactive grid control. Controller-based algorithms can provide control both at the component level and system level. These control algorithms have also been demonstrated for implementation at the edge to further automate the MG and improve system resiliency [2]. We have therefore classified the opportunities for interactive SDMG control algorithms into the following categories:

1) ENERGY BALANCING

The distributed energy resources in a microgrid are composed of Distributed Generators (DG) and distributed storage (DS) units. If the energy source in a DG is renewable such as wind or solar which are non-controlled, the energy output cannot be controlled externally. The output is usually optimized based on MPPT algorithms and thus can result in fluctuations pushing the microgrid power system out of balance. In such a case energy balancing algorithms in the SDMG controller manages energy dispatches between DG and DS units. This effectively maintains a balance of both voltage and frequency in the MG system. Such a technique has been demonstrated in the PXiSE project [1] which will also be looked at as a case study further in this work.

Opportunities for algorithms to dispatch energy from DS units such as batteries existing as independent units or in electric vehicles are available. V2G control algorithms can further be enhanced to be part of the SDMG energy balance

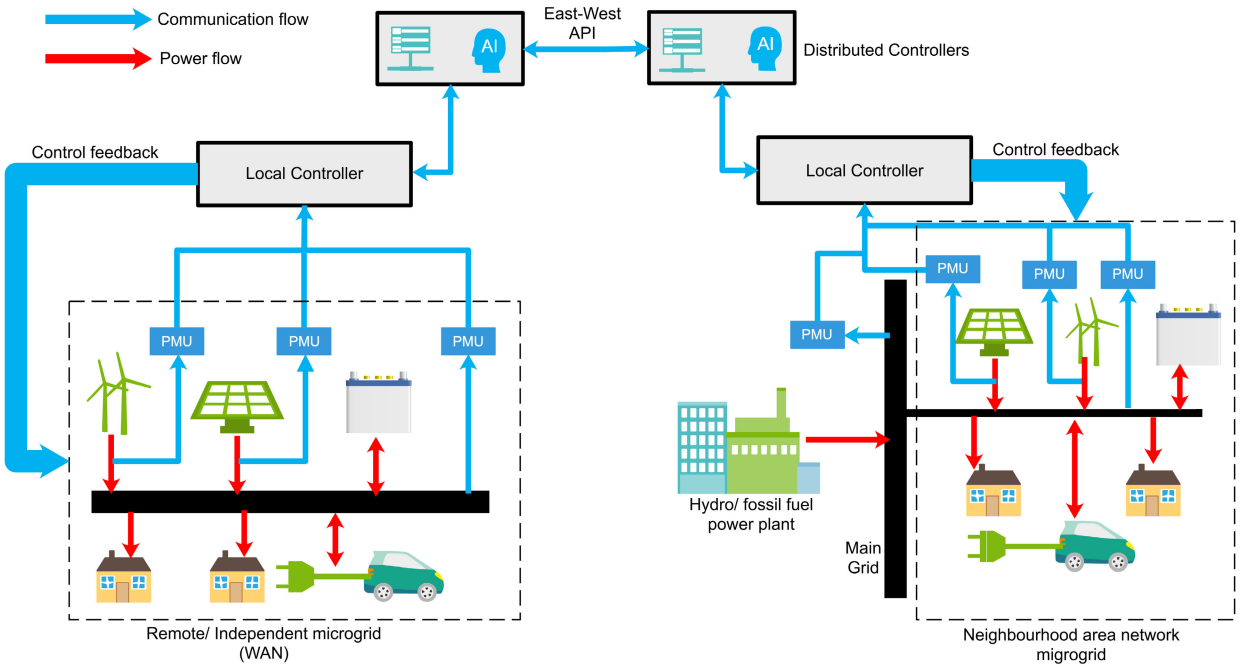

FIGURE 3. SDMG architecture.

management. In our scenario of SDMG energy management, energy balancing involves the regulation of both frequency and voltage levels in the microgrid system. The V2G concept has been highlighted to provide frequency regulation in a microgrid [33], [34].

Ahmed and Amrizal [33] demonstrate using MATLAB how the integration of Plug-in Hybrid Electric Vehicles (PHEV) affect the microgrid peak load and frequency. The findings of the work being V2G integration leading to improvements in microgrid system frequency. The percentage improvement in frequency increasing as the EV charger level increased. This aspect can be harnessed via software-defined control to optimize the system frequency improvement.

Iqbal *et al*. [34] propose a novel frequency control strategy in an industrial microgrid using V2G. The strategy is based on the effective coordination of three crucial V2G components: the charging operator, the EV operator and the aggregator. In this kind of application, the global view maintained by the SD controller can optimize and improve the coordination efficiency required for this kind of approach.

Furthermore, the global view maintained by the controller can allow the efficient dispatch of an EV to any point in the microgrid requiring regulation. This movement of EVs in the microgrid is further supported by the extensive communication network forming the backbone of SDMG control.

2) AI-BASED PERFORMANCE

Synchrophasor data accumulates at the local and global controllers after being generated by a distributed network of PMUs in the microgrid system. This buildup of voltage and phase information forms part of a big data framework. AI-based learning can use this data to predict microgrid supply and demand performance. Control algorithms can be implemented to regulate predicted system fluctuations as they happen. For instance, RERs such as solar power are intermittent and thus require some form of prediction to ensure effective power management [35].

There have been several contributions on how AI can improve energy performance in microgrid networks [35]–[39] however, this article focuses on the use of PMU data for AI-based prediction in a microgrid. We have established so far that synchrophasors are critical to the management of SDMGs. How are synchrophasors being used for AI-based management of MGs?

The intermittent nature of microgrids requires an up-to-date knowledge framework of the topology for efficient monitoring and control. Sychrophasors from distributed PMUs (D-PMUs) can be incorporated together with machine learning approaches to perform topology detection [40]. Liu *et al*. [40] also highlights the potential of ML techniques and synchrophasors in event detection and classification.

Hossain *et al*. [41] mention the possibility of using PMU and micro-PMU data in combination with machine learning to visualize the power grid system and provide monitoring support for frequency variations. Furthermore, the use of AI techniques such as reinforcement learning and Particle Swarm Optimization (PSO) has been demonstrated to provide load scheduling based on available RERs and enhancement of unplanned islanding stability in MGs respectively [41].

We see that core to this AI-based performance is big data analytics resulting from the massive build-up of PMU data. Big data analytics is key to effective microgrid energy

management as it can provide load and system stability prediction based on analysis. Analytical data can be fed into AI-based control algorithms for the optimized performance of the MG. Learning based on this analyzed data has also been mentioned to provide support for power system protection [42].

3) ENERGY STORAGE MANAGEMENT

Multiple RERs in a distributed microgrid network should always consider energy storage when the renewable resource is unavailable. A common storage mechanism consists of battery banks existing as independent units in the grid or as part of a network of electric vehicles in V2G applications. Control algorithms implemented in the SDMG controller can provide effective management of these energy storage devices.

Management of energy storage units in the microgrid includes energy storage commands when not in use or upon RER supply spikes and energy dispatch operations when energy deeps occur. Control algorithms can contribute to power system stability by optimizing the energy storage and dispatch operations during fluctuations in supply and demand.

Machine learning-based energy storage management is one such opportunity for SDMG control algorithms. Kolluri and Hoog [43] demonstrate how ML can be used for adaptive control of energy storage in a distributed MG. Their implementation demonstrates how ML can be used to achieve low overhead control of distributed storage units by allowing local control at storage units. This application promises the use of distributed controllers in a SDMG to minimize communication overhead costs. We envision sharing of control operations between the global controllers and MG energy units (local controllers).

Further AI-based battery management in MGs has been demonstrated by Mbuwir *et al*. [44] using batch reinforcement learning. Batch RL has been used to develop an optimized control policy for battery operations in the microgrid. The policy aims to minimize the buying and selling of power in a microgrid by smart scheduling of battery operations. To optimize the battery operations schedule, this technique makes heavy use of network-wide data and state-action value function [44]. An opportunity for a global controller would be to provide updated data on batteries distributed in the MG required by such an energy storage management strategy.

The flexibility and resilience of distributed control have introduced a further push for distributed energy storage management. This aspect of distributed energy storage coupled with SDMG distributed controllers can maximize the resiliency of microgrid systems. In [7], a cyber-physical implementation of distributed control for heterogeneous Energy Storage System (ESS) in microgrids is proposed. The proposed control scheme takes into account the distributed network of energy storage units as part of the physical layer and distributed control algorithms as part of the cyber layer. The control method provides the necessary voltage and frequency stability while maintaining a fair energy balance between energy storage systems. A distributed ESS requires an optimized and robust control coordination mechanism that can potentially be supported by tightly coordinated SDMG controllers.

Battery life which is essential for optimum MG ESSsupport has been linked to the level of control coordination in a distributed system [45]. Ali *et al*. [45] introduce a centralized and optimized control strategy for Battery Energy Storage System (BESS) to improve overall battery life. The global view maintained by the centralized controller selects energy dispatch only from storage units with the best health and capacity, therefore, extending overall BESS lifetime. In an SDMG crucial BESS data such as State of Charge (SOC), maximum capacity and the overall State of Health (SOH) can be stored in the global controller's dynamic memory units. Improvement of battery life through coordination of the V2G method for MGs has also been proposed in [46].

Additionally, a distributed control strategy for DC MGs for smoothening power outputs during RER fluctuations has been proposed [47]. A well-coordinated hybrid energy storage system composed of supercapacitors and accumulators is promised to stabilize intermittency and fluctuations of MG [47]. This drive towards optimized coordination of energy storage devices and demand response has also been supported by Wang *et al*. [48] and Muhamadjafari *et al*. [49]. Wang *et al*. [48] introduce a two-stage coordination approach involving a Price Based Demand Response (PBDR) and the BESS while in [49] the economic and power system advantages are studied based on an optimized Demand Response Program (DRP) and BESS.

Generally, a hybrid of energy storage devices for MGs has been proposed to balance the fluctuations inherent in RERs. A combination of battery units, supercapacitors, electric vehicles requiring effective and optimized control coordination using multiple techniques have been proposed [50]–[53]. The algorithms and techniques proposed in the works provide an opportunity for flexible and resilient implementation through the SDMG control approach.

These opportunities for energy storage in SDMGs are summarized in Table 3.

4) SECURITY MANAGEMENT

Microgrids especially ones integrating smart mechanisms to optimize efficiency have not been exempt from cyber-attacks. This could pose a risk to grid users regarding safety and also privacy if their usage data is compromised. Intrusion can cause forced blackouts in targeted areas or in software-defined scenarios a Distributed Denial of Service (DDoS). DDoS attacks are possible in an SDMG setup for example if the controller in charge of global operations is overwhelmed with intruder-induced control traffic thus affecting controller responsiveness.

Tan *et al*. [15] classify cyber-attacks on MGs into three main categories: Denial of Service (DoS), data replication by intruders and False Data Injection (FDI). Prevention of such

TABLE 3. Opportunities for SDMG energy storage management.

Storage mechanism	Supporting technology	Impact on storage management	Reference
Distributed battery banks	ML based adaptive storage control	Optimized battery storage control	[43]
Prosumer networked battery banks	Scheduled operations based on RL	Optimized power sharing	[44]
Heterogeneous storage systems	De-coupled cyber and physical planes	Balanced energy between multiple storage units	[7]
Battery storage systems	Logically centralized control based on storage properties	Extended battery life	[45]
V2G storage	Global controller based coordination of EVs	Extended battery life	[46]
Hybrid storage (batteries, supercaps, EVs)	Optimized and robust coordination based on decoupled cyber-physical planes	Stabilized and efficiency MG energy system	[47]–[53]

attacks has also been categorized into attack detection and mitigation both in the network layer and the physical layer of the MG network.

We will identify in this section, contributions towards preventing cyber-attacks in traditional microgrids that would benefit from software-defined deployment existing in SDMGs. The targeted benefits should address opportunities for improved system stability and efficiency of operation. Cybersecurity in microgrids is classified under two main schemes: protection and detection/mitigation schemes [54].

Before we address cyber-attack detection and mitigation in detail, it is crucial to discuss the critical situations under which attackers can target modern-day power grids. Malicious attackers can take advantage of data communications maintaining and controlling power grids to cause system disruption and also steal customer usage data [55]. Attackers can disrupt bulk electrical systems by remotely taking over system actuators such as breaks and output valves. This consequently results in economic loss for electric companies [56]; a key attack scenario for competition malpractice.

Furthermore, in [56] FDI attacks have been mentioned to take the form of manipulation of real-time measurement data obtained from grid devices. An attacker can intercept the real-time data transmission on its way to the station for purposes of FDI consequently disrupting grid operations. Additionally, an FDI hacker can take advantage of the Optimal Power Flow (OPF) problem to manipulate electric load data ultimately misleading service operators [57]. Such an attack can involve manipulation of the generation schedule leading to serious system economy losses.

Under protection, there have been contributions focused on the protection of microgrid smart devices such as sensors and energy meters. The smart microgrid framework is such it is composed of numerous smart meters and sensors, hence it is not economical to protect all of them. Only a few critical meters/ sensors can therefore be protected to reduce cost [54]. To optimize the number of protected smart devices for purposes of cybersecurity resiliency, there is a need to balance the cost of protection and the level of security required.

Taking this angle of protection into consideration, critical to SDMGs should be the protection of PMUs. There have been some proposals to offer PMU protection in microgrids and power systems alike using various schemes. Lin *et al*. [58] propose a self-healing and attack resilient PMU strategy for protection. The strategy takes advantage of the programming reconfigurability of SDN-based power system networks. During or after a cyber-attack, the SDN controller isolates and disconnects compromised PMUs and established new connections to secure PMUs for network continuity and resiliency purposes. This approach has been extended to other self-healing mechanisms based on the controller disconnecting compromised network paths and devices and connecting uncompromised devices autonomously [13].

Protection of microgrid smart devices from cyber-attacks can also be done through encryption strategies. An opportunity for this is the encryption of PMU data being transmitted through the various layers of the SDMG framework. There are already proposals to using encryption in microgrids like that proposed by Cruz-Duarte *et al.* [59]. Using raspberry pi 3 nodes, a security scheme for microgrids is proposed to introduce symmetric and asymmetric encryption algorithms. Other security mechanisms introduced to improved data authenticity in the microgrid include hash functions, Secure Socket Layer (SSL) certificates and digital signatures [59]. Named Data Networking (NDN) has also been mentioned to provide security for data communications in microgrids through encryption [60]. This is possible by demanding that the data publisher signs data packets with a cryptographic key.

Further on encryption of data communications, is the aspect of securing the standards and protocols coupling Internet of Things (IoT) devices and the MG. The software-defined architecture allows for the increased flexibility of IoT devices while allowing for energy management to increased device lifetime [61]. While this is an effective management opportunity for IoT devices in an SDMG, there is a need to discuss the methods of securing IoT protocols coupling the IoT integration in MGs. The properties of IoT security protocols and their impact on the security requirements of smart grids and MGs have been investigated [62]. Results showed that the required security protocols increased latency and traffic overhead by about three (3) times. However, solutions to similar latency and overhead traffic problems have been provided with the use of distributed controllers [63]–[65].

Keeping in with this distributed approach, microgrid attack resiliency has been achieved by using distributed adaptive observers [66]. This technique introduces an attack-resilient

secondary control approach that neutralizes cyber-attacks and promotes containment of power-sharing and synchronization of voltages. This approach is particularly important for situations of islanded single/three-phase (S/T) microgrids and can be classed under protection through attack neutralization.

A more proactive approach to cybersecurity in microgrids falls under the class of detection/mitigation [15], [54]. Here we will discuss the remedial action schemes towards cyber-threats. There has been continuous development of techniques and algorithms in the area of cyberattack detection and mitigation [67]–[71]. We ask how can these techniques benefit from the SDMG paradigm? Chlela *et al*. [67] for example, propose a testing platform for real-time FDI attacks. A Real-Time Digital Simulator (RTDS) is used to emulate the entire microgrid network and its critical components. This scheme can quantify the level of the cyberattack as well as test the effectiveness of the mitigation algorithm implemented. The flexibility for digital control support available in SDMGs would effectively benefit the integration of such a platform.

Detection schemes based on heuristic methods [70], algorithmic neural networks [69] and multi-layer approached [68], [71] show get potential for integration in SDMG controllers. Data collected at PDCs can be used to train the proposed neural networks. The ability to separate the control, network traffic and application data in software-defined networking would support the introduction of a multi-layered approach to detection and mitigation. Digital Twins (DTs) for detection of FDI attacks in the physical system introduced in [68] can take advantage of the distributed controllers available in the SDMG framework. Heuristic schemes used for attack detection in smart grids such that demonstrated by Xia *et al.* [70] can be adopted for use in SDN-based microgrids.

The use of heuristics in detecting cyber-attacks in microgrids can introduce the rapid response required to reduce economic losses. In a prosumer setup, such as that enabled by modern microgrids, amounts of energy generated and consumed regulate electricity bills. Therefore, a hacker can falsify consumption and generation data to achieve lower bills making the electric companies incur losses [70].

Table 4 shows a summary of opportunities for cybersecurity in SDMGs.

5) MANAGEMENT OF ECONOMICS AND BILLING

In modern microgrid configurations, smart prosumer meters are expected to handle the aspects of costing and billing. In software-defined MGs, data traffic from smart meters can be relayed through the already existing communication network of controllers and network devices. Controller-smart meter traffic can be classified as control traffic while smart meter-smart meter traffic can be data traffic traversing the data plane in an SDN scenario.

The controllers while maintaining a global view of the entire microgrid network, can keep an up-to-date database of production and consumption of electricity by prosumers identifiable by unique IDs. A similar mechanism of monitoring, control and billing management of microgrids has been demonstrated for a rural setup [72]. However, the proposed TDMA communication backbone linked up to a vendor-specific cloud platform can be generalized using the SDMG framework with the flexibility of vertical integration of applications. Furthermore, the potential for using smart metering data in centralized billing frameworks has been proposed in [73]. We envision that such systems can benefit from the generic and global nature of SDMGs.

Energy Sharing Management (ESM) has been highlighted to use a form of central control and coordination for photovoltaic (PV) prosumers [74]. In this particular application, a Microgrid Operator (MGO) is used to coordinate and control sharing of PV energy to ensure maximum profit. In an SDMG system, the role of the MGO can be integrated into local controllers alongside its many promised management benefits.

The multi-layer and decentralized approach to billing and monitoring management promised by blockchain [75]–[78] and dynamic pricing [79] can also be optimized by SDMGs. The potential for SDN-based communication in SDMGs, introduces flexible multi-layered traffic planes with a clear separation between control and data planes. This architecture fits well with distributed billing management approaches for MGs.

C. A CASE STUDY ON PXiSE: AN ENERGY BALANCING ALGORITHM

The PXiSE project carried out in Onslow, Western Australia highlights a use-case potential of SDPG [1]. The PXiSE energy team implemented a global controller to balance load and generator operations in grid-connected microgrids similar to a computer's operating system. Algorithms embedded in the controller manage resources in a microgrid containing multiple energy sources such as fossil fuels, solar, wind and energy storage systems. The controller balances the generation and load continuously ensuring a stable connection between the microgrid and the main grid as depicted in Fig. 4. The case in Onslow is such that small communities span a large desert area making the running of transmission lines not feasible. Therefore, local generation through microgrids is key and this is further supported by the push to reduce reliance on nonrenewable energy.

Consequently, we see an influx of solar and wind power systems being connected to the main grid. These multiple energy sources result in unbalanced loads and system instability due to the intermittency of renewable resources. This is further complicated by operator policies on the number of renewable resources to be connected and their outputs. In the Onslow project, the PXiSE team makes use of PMUs to provide a source of real-time phasor data to provide information on the grid status. This data together with machine learning algorithms enable the PXiSE controller to respond quickly to changes in generation and consumption with a provision of prediction on the future network status. Compensation algorithms and techniques are used to smooth out sudden

TABLE 4. Summary of SDMG opportunities for MG security management.

Cyber-security class	Proposed technique	Type of attack	Required resources	Reference
Protection	Protection of critical grid devices only to reduce cost	DoS/ FDI/ Data replication	Sensors and smart devices	[54]
	Self-healing and attack resilient PMUs	DoS/ FDI	SDN controllers, reconfigurable grids and PMU hardware	[13], [58]
	Network and data encryption	FDI/ snooping	Encryption support hardware (memory, processing, bandwidth)	[59], [60]
	Securing IoT protocols	FDI, DoS, snooping	Bandwidth, distributed controllers	[62]–[64]
	Distributed adaptive observers	FDI, DoS	Distributed S/T MGs	[66]
Detection and Mitigation	Monitoring and preparing via testbeds	FDI	Real-time simulators	[67]
	Detection based on heuristics and neural networks	FDI/ DoS	Computational resources	[69], [70]
	Multi-layered approach	FDI/ DoS	Cyber-physical decoupling hardware/software	[68], [71]
	Provision of digital twins	FDI	Replica computing and control hardware/software	[68]

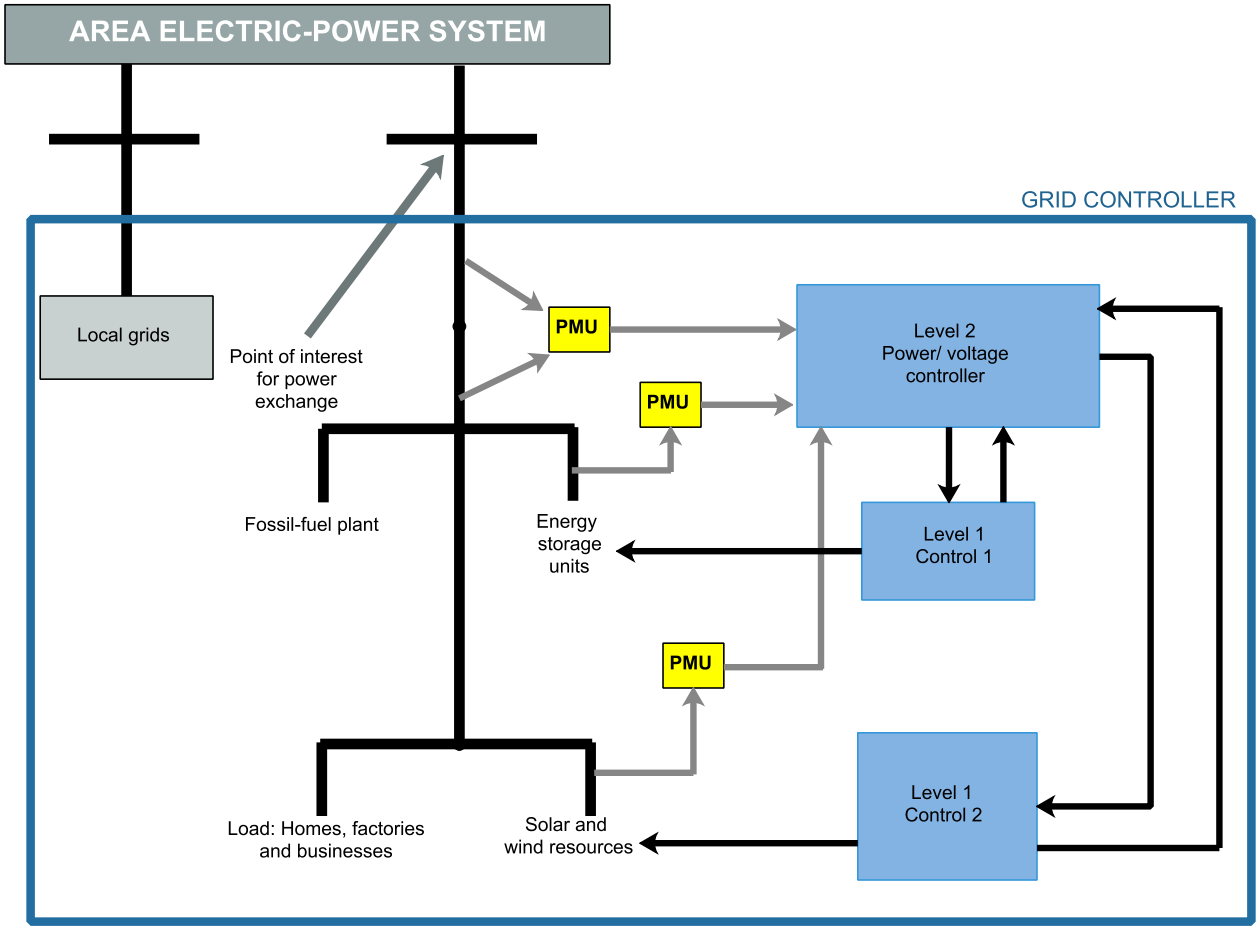

FIGURE 4. PXiSE Power Grid OS [1].

fluctuations in grid conditions which might otherwise cause system blackouts, equipment damage and general energy efficiency.

What we learn from the PXiSE pilot projects is that the use of PMUs allows for minimal changes to the hardware requirements for already existing traditional grid systems. Considering that most systems already use PMUs the only real hardware required for this type of grip control is a controller. The goal of this kind of approach is to shift control entirely to autonomous software, therefore, requiring minimal hardware implementation. The PXiSE team demonstrated through several projects how a sample controller

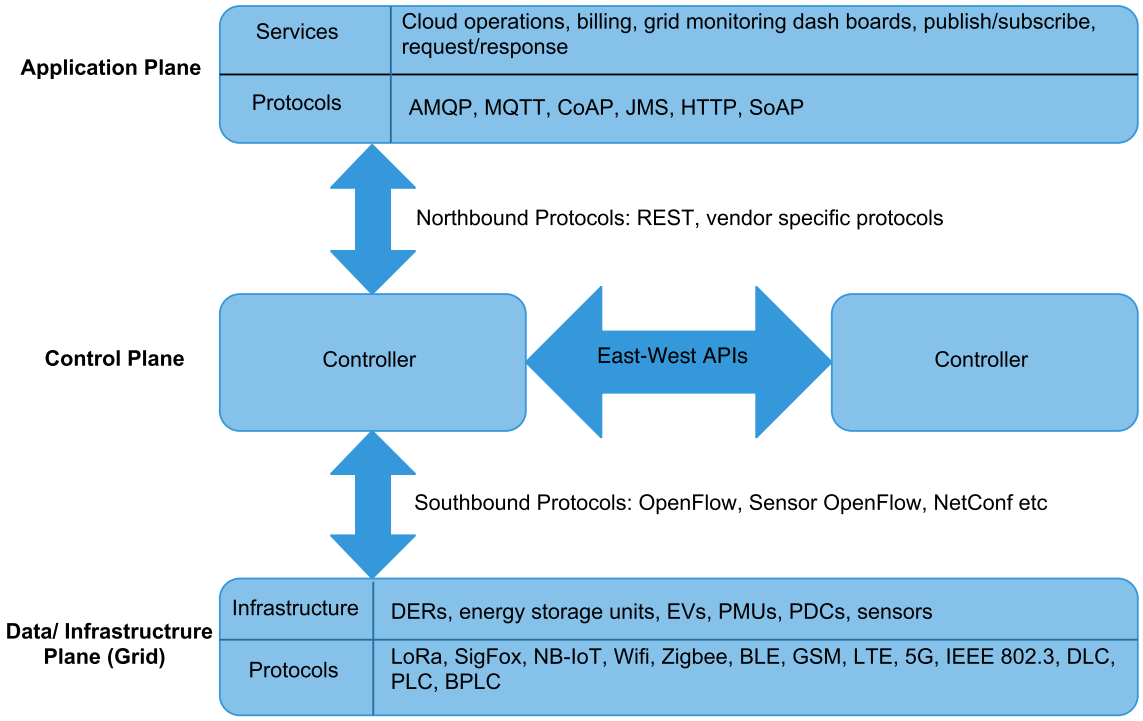

FIGURE 5. SDMG communication protocols.

setting can smooth our energy fluctuations either by remote dispatch of energy stored in batteries when generation suddenly reduces or by ramp control when energy generation increases suddenly. Artificial intelligence embedded in the PXiSE controller has also been demonstrated to forecast demand and generation ultimately optimizing grid stability and improving energy efficiency.

V. SDMG DESIGN REQUIREMENTS AND ASSOCIATED CHALLENGES

A. DISTRIBUTED CONTROL AND COMMUNICATION

Balanced energy distribution and efficient system response of a SDMG is heavily dependent on the communication network between the framework entities including controllers, switches, RER units, storage units, PMU and associated data concentrators. An efficient SDMG framework should consist of distributed controllers, energy generation and consumption units and IoT devices supported by a bi-directional communications network of heterogeneous devices. The resultant expectation is a hybrid communication network of energy and control devices. It is therefore, necessary to design a communication network to support this hybrid combination for use in SDMGs.

The software-defined MG requires the use of communication protocols available for east-west APIs in distributed controllers, north-south APIs for controller-device links. We will not dwell much on the already existing supply and demand-side communication protocols for traditional MGs highlighted in [15]. SDMGs bring in the addition of controllers and the principles of SDN to traditional MGs. Therefore, the design requires support for SDN protocols in addition to the available SCADA and TCP/IP protocols for traditional MGs.

We present an SDN-based framework of communication protocols in Figure 5.

To highlight the features and challenges of the communication and control system design requirements, there is a need to highlight the various modes of communications that exist in SDMGs. These include:

1) DER-to-DER: This communication model takes place in the infrastructure plane. Exchange of data packets between energy generation, consumption and storage devices is expected. Vehicle to vehicle communication in EVs for coordinated V2G functionality is one such example. Point-to-point communication protocols such as ZigBee, WiFi, Bluetooth, wired Ethernet and Power Line Communications (PLC) are common here. However, challenges exist here due to security vulnerabilities in the communication protocols being the use as well as the lack of OpenFlow support for traditional grid devices [80].
2) PMU-to-PDC: PMUs deployed across the SDMG network provide useful synchrophasor data for controller algorithms. Synchrophasor data is transmitted to phasor data concentrators which store unified data for controller reference at a local or global scale. PMU-PDC communication strategies can be short-range or long-range depending on the PMU cluster configuration. For long-range transmission of synchrophasors can use protocols such as LTE, Low-power Wide Area

TABLE 5. Summary of SDMG communication modes.

Communication mode	Properties	Protocols available	Challenges
DER-to-DER	Peer to peer communications between RERs, EVs, loads, fossil power plants, etc. Support for billing, V2G and blockchain. Exists mostly in the infrastructure plane and is bidirectional.	Ethernet, PLC, WiFi, Bluetooth, ZigBee	Prone to FDI attacks. Data privacy vulnerabilities. Lack of OpenFlow support
PMU-to-PDC	Unidirectional uplink of synchrophasors. Many to one approach to communications. Suitable for use with both short and long-range communication.	LoRa, SigFox, LTE, PLC, Ethernet.	Security concerns due to FDI attacks. Grid data privacy.
PDC-to-Controller	Based on SouthBound interface. High bandwidth requirement for data uplink. Requires support for controller requests and acknowledgments. Bidirectional flow of synchrophasor and control data.	BPLC, 5G, broadband Ethernet.	High overhead traffic concerns. Security and privacy of bulk synchrophasor data.
Controller-to-Controller	Distributed control, improved controller response, improved controller resilience. Requires East-West API support.	Ethernet, LTE, fiber optic links	Complexity in controller synchronization.
Controller-to-Cloud	Based on the NorthBound Interface. Bidirectional flow of control and policy data to support applications. Support for monitoring and billing.	5G, Ethernet, WiFi	Lack of standardization in the NBI, potential FDI attacks in the policy issuance from application plane.

Networks (LPWAN)s and PLC while short-range can make use of Bluetooth, ZigBee and WiFi. Security vulnerabilities are the main challenge in design here.

3) PDC-to-Controller: Concentrated synchrophasor data requires support for high bandwidth communications. Therefore communication between the PDC units and the controllers is expected to have high traffic overhead. Broadband protocols such as BPLC, ethernet and 5G are required to support this communication model. Traffic flow is usually one way expect for control packets requesting data from PDCs. PDCs can be configured to respond to requests from the controller. Security and privacy concerns of PDC data are critical here.
4) Controller-to-Controller: In a SDMG with distributed controllers to support resilience in control, controller-controller communication is necessary for synchronization. Adequate synchronization via east-west APIs ensures the reduction in latency and improved controller response time. Optimizing controller to controller synchronization can be a challenging task sometimes requiring vendor-specific techniques to minimize delays and errors. Common communication protocols such Ethernet, fiber optics and LTE can be used to link controllers together.
5) Controller-to-Cloud: This communication model exists between the control plane and the application plane. Cloud support services present in the application plane are updated by the global view of the grid maintained by controllers. Status reports and issuance of grid policies occur over this model supported by NBI. There is still a challenge regarding standardization of the NBI unlike with the SouthBound Interface (SBI) [80]. Several vendor-specific protocols supported by Ethernet, Wifi, LTE, 5G can be implemented to transfer data between the control plane and the application plane. Just like with other modern communication networks security of data is still a concern. An intruder can easily change policies administered in the application plane as they are transmitted for implementation in the control plane.

The communication modes discussed in this section are summarised in Table 5.

B. MICROGRID SYSTEM RESILIENCE

Microgrid system resiliency should incorporate the network's ability to quickly recover from faults, instability from emergency islanding and cyber-attacks. In cases of emergency islanding, the microgrid should have systems in place to ensure the smooth transition from the grid-connected mode to islanded mode. Design considerations for system resiliency prioritize fault mitigation and millisecond responses to grid anomaly detection and recovery.

MGs based on an SDN communications architecture have been proposed to enable system resilience [4]. The proposal highlights the need for an ultra-fast programmable network to improve response times on faults and cyberattacks in microgrids. Reliable and low latency communication are necessary to guarantee microgrid resilience. Unlike industrial control networks such as Profibus (Process Field Bus), SDN promises to introduce the required millisecond response time for MG communication networks. Proposed SDN techniques for MG resilience include millisecond network delay guarantee, fast recovery from failovers and data traffic prioritization. A key feature of SDMGs is network re-programmability based on the global knowledge in the controller however the deployment design should involve minimization of overall traffic delay if the resiliency is to be optimized.

In SDN-based MG applications, a critical contributing factor to controller response is increased overhead traffic from the multiple nodes in the grid distribution network.

TABLE 6. Cyber-attack resiliency of SDMGs and associated design strategies.

Cyber-attack challenge	Design strategies
Securing Communications stack	1) Network verification against security policies maintained by the controller global view [13] 2) Securing routing and transmission links via end-to-end encryption [2], [15] 3) Designing cyber-security protocols for integration in the communication stack [85] 4) Taking advantage of embedded security in wireless technologies [85] eg implementation of the secure by design concept [86] 5) Host authentication in data communications such as the implementation of a host-checker in the controller [87]
Early attack detection	1) Advancement in pattern, anomaly and third party detection [15] 2) Anomaly detection based on machine learning approaches [88] 3) Distributed detection scheme using multiple state observers to minimize localized attacks (anti-stealth strategy) [89], [90] 4) Software-defined active synchronous detection (SDASD) [87]
Early attack mitigation	1) Self-healing/ Self-recovery systems [4], [13], [91] 2) Increasing the signal to noise ratio to mitigate jamming [92] 3) Use of cryptographic signatures [93] 4) introduction of redundant communication link to be used during attacks [91] 5) introduction of ultra-fast network programmability [4]

The use of optimally synchronized distributed controllers has shown effectiveness in quenching control messages and minimizing overall delay [63], [64]. There is also potential for integrating edge computing in SDMG design to reduce the control traffic towards the controller as some decisions can be performed at the edge effectively improving response time to grid events [81]–[83].

AI techniques including machine learning and reinforcement learning at the edge promise to maximize system resiliency [84]. Training data can be used to predict and detect islanding, cyber-attacks, faults and general instability in the MG power system. AI can further improve the selection of control traffic that needs to go to the controller consequently decongesting the control traffic channel.

The integration of edge computing machines in traditional grid networks may pose a challenge of installing extra computing hardware and further configuration for fluid communication with grid controllers. Furthermore, cyber-attacks pose a critical challenge to using software definition for microgrid resiliency [12].

C. CYBER-ATTACK RESILIENCE

Dependency on a robust communication network has thus far being highlighted as a critical component of SDMG resiliency. However, the direct setback with this kind of approach to resiliency is the risk of cyber-attacks. This poses a challenge towards securely implementing SDMGs for grid stability and user data protection.

The design challenge should focus on securing the communication stack and early attack detection/mitigation. There have been several proposals for strategies to secure communication links in cyber-physical MGs similar to SDN-based MGs as well solutions to optimizing attack detection and mitigation.

Table 6 shows some of the design strategies available for resolving the above challenges in cyber-security for SDMGs.

VI. FUTURE RESEARCH CHALLENGES

As industry and academia gain interest in investigating and implementing SDMGs we observe a few things. We see the need to transfer traditional microgrids as we know them to a cyber-physical architecture that SDN can support. This includes the introduction of a multi-layered approach to grid control via algorithms in the controller and the application plane. All this while maintaining the least cost possible mostly by harnessing already existing infrastructure. A framework that requires minimal changes to existing hardware and software enables ease of transition and reduced cost. This aspect can be backed by the need to modify traditional microgrid hardware to enable support for the SDN concept.

However, the numerous management advantages that softwarization of the microgrid introduces come with associated challenges. Increased reliance on communications also creates opportunities for cyber-attacks in form of false data injection, denial of service and snooping. How do we approach the optimal balance between SDMG benefits and security concerns? We learn that it is possible to use some of the existing cyber-attack detection and mitigation techniques for the benefit of SDMGs. This also creates a culture of research and knowledge recycling and re-purposing to save on resources.

Another critical issue arising from the review is the issue of SDMG resiliency. Software-definition of the microgrid aims to maximize the grid resiliency against failure and attacks. Highlighted in this work is the aspect of energy balancing in the grid which is necessary for grid stability. Notwithstanding, a much more important observation is the need for defining what resiliency is and how much of it is sufficient. In support of this, Tan *et al.* [15] recommend the need to clarify and quantify microgrid resilience.

Finally, the nature of softwarization of the microgrid would result in large amounts of microgrid data being collected. We see this as an opportunity for increased management techniques based on machine learning, reinforcement learning and data science in general.

While discussing some important lessons on the architecture and management of SDMGs, we uncovered several opportunities for future research. Available future research challenges include:

A. UPGRADING OF HARDWARE TO SUPPORT SDN-BASED OPERATION

Current PMUs provide the necessary synchrophasors suitable for SDN-based management of the microgrid. However, there is a need to investigate more grid sensors with OpenFlow support. This will further optimize the SDN-based operation by enabling the sensor to sensor data forwarding and providing opportunities for data aggregation. Can PMUs be upgraded or updated to support SDN protocols? Such information can be useful as researchers consider further integration of SDN-enabled devices into the microgrid.

The DERs and associated loads in the microgrid can also be investigated for SDN control and support. Such support can enable close coupling between SDN controllers and the DERs/loads, ultimately increasing the management flexibility and efficiency. SDN support for microgrid hardware would also mean less required smart functionality in the grid. Most of the smart functionality can be moved to the control plane or edge computers.

B. EXTENDED AI-BASED DATA ANALYTICS FOR MICROGRID DATA

We expect more big data and AI application use cases for microgrid data such sychrophasors. Research beyond predicting DER fluctuations and MG faults is required. Machine learning for example can be used for anomaly detection in microgrids, a useful technique in the detection and mitigation of cyber-attacks.

Microgrid data on load profiles can be used to determine consumer behavior in the grid, therefore, optimizing power delivery where and when needed. Integration of AI in autonomous vehicles for purposes of V2G energy distribution is also expected. This will further improve the microgrid energy balance.

All forms of machine learning will play an important role in energy forecasting and control of MG DERs. This will mean an increase in effective planning and consequently cost reduction for utilities managing and controlling the MGs.

C. SECURITY CHALLENGES

Rising cyber-security concerns over the decoupled cyber-physical architecture of SDMGs, would mean increased demand for further research into MG security. The security of the governing communication protocols in MGs needs to be investigated with an option to add extra layers of protection for MG operations.

As mentioned before, smart and AI-based anomaly detection can be researched to ensure effective mitigation of cyber-attacks on the MG. Generally, we expect advancement in detection and mitigation techniques for attacks in the MG. The is space for developers to implement versatile security modules for the MG controller with vertical integration in mind. Provision for security updates and patches should be made available to the controller because of the agile nature of cyber-attacks.

Intruders always come up with clever ways to attack and hence flexibility in MG security management is critical. Proposed solutions should take advantage of the SDN paradigm to support multiple vendors and heterogeneous devices in the grid. A modular approach to security applications would be important for rapid prototyping.

D. DELAY AND OVERHEAD TRAFFIC MINIMIZATION

The need for a rapid response to microgrid events cannot be overemphasized. This promotes microgrid resiliency and makes the MG suitable for mission-critical applications. However, maintaining global control of multiple heterogeneous energy resources and loads may be faced with the challenge of congestion and delay. A suitable fix is the implementation of distributed controllers handling clusters of the microgrid with the latency of operation being dependent on controller synchronization and the amount of overhead traffic.

SDMG researchers are therefore faced with the challenge of optimizing the configuration of multiple distributed controllers to bring latency to a minimum. Controller fragmentation as demonstrated in [64] can be investigated for SDMGs and the improvement in operations response observed.

Another critical factor that affects controller responsiveness in software-defined configurations is the aspect of overhead messages bombarding the controller. Techniques such as data aggregation for synchrophasors can be investigated either in the physical MG plane or in phasor data concentrators. PMUs nearby may intelligently augment data and send it as a single message.

Edge computing is yet another open area of research in SDMGs aimed at improving system response and minimizing both delay and overhead traffic. The efficiency of placing dedicated computational devices within the microgrid to handle some of the local tasks can be analyzed using several metrics. The most important metric being the latency of operations in cases of MG events such as cyber-attacks, fluctuations and general system failures.

E. FURTHER DEVELOPMENT OF SDN-BASED CONTROLLER ALGORITHMS

While there have been several proposals and algorithms in literature for direct control of MG hardware such as power electronics converters, energy storage devices and energy resources there still exists several opportunities to investigate control from a logically centralized SDN-based controller.

TABLE 7. List of acronyms.

Acronym	Elaboration
AMQP	Advanced Message Queuing Protocol
BESS	Battery Energy Storage System
BPLC	Broadband Power Line Communications
CoAP	Constrained Application Protocol
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource
DG	Distributed Generators
DLC	Distributed Line Carrier
DoS	Denial of Service
DRP	Demand Response Program
DS	Distributed Storage
DT	Digital Twins
ESM	Energy Sharing Management
ESS	Energy Storage System
EV	Electric Vehicle
FDI	False Data Injection
G2V	Grid to Vehicle
GPS	Global Positioning System
IoT	Internet of Things
JMS	Java Message Service
LPWAN	Low-power Wide Area Networks
LTE	Long Term Evolution
MG	Microgrids
MPPT	Maximum Point of Power Tracking
MQTT	Message Queueing Telemetry Transport
NB-IoT	Narrowband IoT
NBI	NorthBound Interface
NDN	Named Data Networking
NMG	Networked Microgrid
OPF	Optimal Power Flow
PDC	Phasor Data Concentrator
PHEV	Plug-in Hybrid Electric Vehicle
PLC	Power Line Communications
PMU	Phasor Measurement Unit
ProFiBus	Process Field Bus
PSO	Particle Swarm Optimization
PV	Photovoltaic
RER	Renewable Energy Resource
RTDS	Real-Time Digital Simulator
SBI	SouthBound Interface
SCADA	Supervisory Control and Data Aquisition
SDMG	Software-Defined Microgrids
SDN	Software-Defined Networking
SDPG	Software-Defined Power Grids
SoAP	Simple Object Access Protocol
SOC	State of Charge
SOH	State of Health
SSL	Secure Socket Layer
V2G	Vehicle to Grid
WAMS	Wide Area Management System

What this opportunity entails is being able to develop and deploy control algorithms at the control plane without having to directly interact with the actual devices in the microgrid network. Researchers can investigate and recommend suitable SDN controllers for the proposed control algorithm or they can go further and develop their custom controller for optimal operation.

VII. CONCLUSION

This paper discussed in detail the concept of a SDMG. Microgrids are becoming a popular configuration for future generation power networks due to their support for multiple distributed energy resources and technologies. Hence, microgrids require flexibility and efficiency in the management of the distributed energy resources. In this regard, we presented an architecture that enables software definition of the grid while minimizing the changes required to the traditional microgrid as we know it. Controller operations were dependent on synchrophasors generated by PMUs already existing in microgrids.

As part of this work, we highlighted several opportunities for optimizing microgrid management based on the SDMG paradigm. Opportunities highlighted included energy storage and balancing, artificial intelligence and cyber-security. The design requirements and challenges of deploying an effective SDMG were also discussed while bringing to light the critical challenge of cyber-security arising from grid softwarization. The challenges led to a recommendation of several open research opportunities in the field of SDMGs.

APPENDIX

All the acronyms used in the paper are shown in Table 7.

REFERENCES

[1] (Jul. 2020). *The Software-Defined Power Grid is Here—IEEE Spectrum*. Accessed: Jul. 2020. [Online]. Available: https://spectrum.ieee.org/energy/the-smarter-grid/the-softwaredefined-power-grid-is-here

[2] L. Wang, Y. Qin, Z. Tang, and P. Zhang, "Software-defined microgrid control: The genesis of decoupled cyber-physical microgrids," *IEEE Open Access J. Power Energy*, vol. 7, pp. 173–182, 2020.

[3] F. Katiraei, R. Iravani, N. Hatziargyriou, and A. Dimeas, "Microgrids management," *IEEE Power Energy Mag.*, vol. 6, no. 3, pp. 54–65, May 2008.

[4] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh, and R. Jin, "Enabling resilient microgrid through programmable network," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2826–2836, Nov. 2017.

[5] T. V. Vu, B. L. H. Nguyen, Z. Cheng, M.-Y. Chow, and B. Zhang, "Cyber-physical microgrids: Toward future resilient communities," *IEEE Ind. Electron. Mag.*, vol. 14, no. 3, pp. 4–17, Sep. 2020.

[6] P. Buason, H. Choi, A. Valdes, and H. J. Liu, "Cyber-physical systems of microgrids for electrical grid resiliency," in *Proc. IEEE Int. Conf. Ind. Cyber Phys. Syst. (ICPS)*, May 2019, pp. 492–497.

[7] Y. Wang, T. L. Nguyen, Y. Xu, and D. Shi, "Distributed control of heterogeneous energy storage systems in islanded microgrids: Finite-time approach and cyber-physical implementation," *Int. J. Electr. Power Energy Syst.*, vol. 119, Jul. 2020, Art. no. 105898, doi: 10.1016/j.ijepes.2020.105898.

[8] A. H. M. Jakaria, M. A. Rahman, and A. Gokhale, "Resiliency-aware deployment of SDN in smart grid SCADA: A formal synthesis model," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 2, pp. 1430–1444, Jun. 2021.

[9] J. Zhang, B.-C. Seet, T.-T. Lie, and C. H. Foh, "Opportunities for software-defined networking in smart grid," in *Proc. 9th Int. Conf. Inf., Commun. Signal Process.*, Dec. 2013, pp. 1–5.

[10] M. You, X. Zhang, G. Zheng, J. Jiang, and H. Sun, "A versatile software defined smart grid testbed: Artificial intelligence enhanced real-time co-evaluation of ICT systems and power systems," *IEEE Access*, vol. 8, pp. 88651–88663, 2020.

[11] A. Cahn, J. Hoyos, M. Hulse, and E. Keller, "Software-defined energy communication networks: From substation automation to future smart grids," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2013, pp. 558–563.

[12] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in *Proc. 1st ACM Workshop Cyber-Phys. Syst. Secur.*, Apr. 2015, pp. 61–68.

[13] D. Jin, Z. Li, C. Hannon, C. Chen, J. Wang, M. Shahidehpour, and C. W. Lee, "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2494–2504, Sep. 2017.

[14] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2637–2670, 3rd Quart., 2019.

[15] S. Tan, Y. Wu, P. Xie, J. M. Guerrero, J. C. Vasquez, and A. Abusorrah, "New challenges in the design of microgrid systems: Communication networks, cyberattacks, and resilience," *IEEE Electrific. Mag.*, vol. 8, no. 4, pp. 98–106, Dec. 2020.

[16] G. Brown, N. Ventura, and J. Mwangama, "A software defined approach for improving resilience in smart distribution grids," in *Proc. Int. SAUPEC/RobMech/PRASA Conf.*, Jan. 2020, pp. 1–6.

[17] D. K. Mohanta, C. Murthy, and D. S. Roy, "A brief review of phasor measurement units as sensors for smart grid," *Electr. Power Compon. Syst.*, vol. 44, no. 4, pp. 411–425, Feb. 2016.

[18] M. Rihan, M. Ahmad, and M. S. Beg, "Phasor measurement units in the Indian smart grid," in *Proc. ISGT*, 2011, pp. 261–267.

[19] Cre. (Jan. 2020). *Phasor Measurement Unit for Monitoring Power Systems*. [Online]. Available: https://phoenix-h2020.eu/phasor-measurement-unit-for-monitoring-power-systems

[20] G. K. Venayagamoorthy, "Potentials and promises of computational intelligence for smart grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Jul. 2009, pp. 1–6.

[21] S. S. Ali and B. J. Choi, "State-of-the-art artificial intelligence techniques for distributed smart grids: A review," *Electronics*, vol. 9, no. 6, p. 1030, Jun. 2020, doi: 10.3390/electronics9061030.

[22] X. Chen, W. Cao, Q. Zhang, S. Hu, and J. Zhang, "Artificial intelligence-aided model predictive control for a grid-tied wind-hydrogen-fuel cell system," *IEEE Access*, vol. 8, pp. 92418–92430, 2020.

[23] A. C. Şerban and M. D. Lytras, "Artificial intelligence for smart renewable energy sector in Europe—Smart energy infrastructures for next generation smart cities," *IEEE Access*, vol. 8, pp. 77364–77377, 2020.

[24] O. Salman, I. H. Elhajj, A. Kayssi, and A. Chehab, "SDN controllers: A comparative study," in *Proc. 18th Medit. Electrotech. Conf. (MELECON)*, Apr. 2016, pp. 1–6.

[25] L. Ren, Y. Qin, Y. Li, P. Zhang, B. Wang, P. B. Luh, S. Han, T. Orekan, and T. Gong, "Enabling resilient distributed power sharing in networked microgrids through software defined networking," *Appl. Energy*, vol. 210, pp. 1251–1265, Jan. 2018.

[26] J. Brugman, M. Khan, S. Kasera, and M. Parvania, "Cloud based intrusion detection and prevention system for industrial control systems using software defined networking," in *Proc. Resilience Week (RWS)*, vol. 1, Nov. 2019, pp. 98–104.

[27] R. H. Lasseter, "MicroGrids," in *Proc. IEEE Power Eng. Soc. Winter Meeting*, vol. 1, Jan. 2002, pp. 305–308.

[28] I. A. Umoren, M. Z. Shakir, and H. Tabassum, "Resource efficient vehicle-to-grid (V2G) communication systems for electric vehicle enabled microgrids," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 23, 2020, doi: 10.1109/TITS.2020.3023899.

[29] H. Klaina, I. P. Guembe, P. Lopez-Iturri, J. J. Astrain, L. Azpilicueta, O. Aghzout, A. V. Alejos, and F. Falcone, "Aggregator to electric vehicle LoRaWAN based communication analysis in vehicle-to-grid systems in smart cities," *IEEE Access*, vol. 8, pp. 124688–124701, 2020, doi: 10.1109/ACCESS.2020.3007597.

[30] S. Cao, N. Lin, and V. Dinavahi, "Flexible time-stepping dynamic emulation of AC/DC grid for faster-than-SCADA applications," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 2674–2683, May 2021.

[31] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab, and A. Abusorrah, "Distributed control and communication strategies in networked microgrids," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2586–2633, Sep. 2020.

[32] S. Sahoo, Y. Yang, and F. Blaabjerg, "Resilient synchronization strategy for AC microgrids under cyber attacks," *IEEE Trans. Power Electron.*, vol. 36, no. 1, pp. 73–77, Jan. 2021.

[33] M. R. Ahmad and L. Q. Amrizal, "Vehicle-to-grid as frequency regulator in a microgrid system," in *Proc. ECCE*. Singapore: Springer, 2020, pp. 859–873.

[34] S. Iqbal, A. Xin, M. U. Jan, S. Salman, A. U. M. Zaki, H. U. Rehman, M. F. Shinwari, and M. A. Abdelbaky, "V2G strategy for primary frequency control of an industrial microgrid considering the charging station operator," *Electronics*, vol. 9, no. 4, p. 549, Mar. 2020, doi: 10.3390/electronics9040549.

[35] S. Aslam, H. Herodotou, N. Ayub, and S. M. Mohsin, "Deep learning based techniques to enhance the performance of microgrids: A review," in *Proc. Int. Conf. Frontiers Inf. Technol. (FIT)*, Dec. 2019, pp. 116–1165.

[36] M. Afrasiabi, M. Mohammadi, M. Rastegar, and A. Kargarian, "Multi-agent microgrid energy management based on deep learning forecaster," *Energy*, vol. 186, Nov. 2019, Art. no. 115873, doi: 10.1016/j.energy.2019.115873.

[37] M. Alhussein, S. I. Haider, and K. Aurangzeb, "Microgrid-level energy management approach based on short-term forecasting of wind speed and solar irradiance," *Energies*, vol. 12, no. 8, p. 1487, Apr. 2019, doi: 10.3390/en12081487.

[38] I. Mahendravarman, S. A. Elankurisil, M. Venkateshkumar, A. Ragavendiran, and N. Chin, "Artificial intelligent controller-based power quality improvement for microgrid integration of photovoltaic system using new cascade multilevel inverter," *Soft Comput.*, vol. 24, no. 24, pp. 18909–18926, Dec. 2020.

[39] J. Faraji, A. Ketabi, H. Hashemi-Dezaki, M. Shafie-Khah, and J. P. S. Catalao, "Optimal day-ahead self-scheduling and operation of prosumer microgrids using hybrid machine learning-based weather and load forecasting," *IEEE Access*, vol. 8, pp. 157284–157305, 2020, doi: 10.1109/ACCESS.2020.3019562.

[40] Y. Liu, L. Wu, and J. Li, "D-PMU based applications for emerging active distribution systems: A review," *Electr. Power Syst. Res.*, vol. 179, Feb. 2020, Art. no. 106063, doi: 10.1016/j.epsr.2019.106063.

[41] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, "Application of big data and machine learning in smart grid, and associated security concerns: A review," *IEEE Access*, vol. 7, pp. 13960–13988, 2019, doi: 10.1109/ACCESS.2019.2894819.

[42] F. Aminifar, S. Teimourzadeh, A. Shahsavari, M. Savaghebi, and M. S. Golsorkhi, "Machine learning for protection of distribution networks and power electronics-interfaced systems," *Electr. J.*, vol. 34, no. 1, Jan. 2021, Art. no. 106886, doi: 10.1016/j.tej.2020.106886.

[43] R. R. Kolluri and J. de Hoog, "Adaptive control using machine learning for distributed storage in microgrids," in *Proc. 11th ACM Int. Conf. Future Energy Syst.*, Jun. 2020, pp. 509–515.

[44] B. Mbuwir, F. Ruelens, F. Spiessens, and G. Deconinck, "Battery energy management in a microgrid using batch reinforcement learning," *Energies*, vol. 10, no. 11, p. 1846, Nov. 2017, doi: 10.3390/en10111846.

[45] A. Y. Ali, A. Basit, T. Ahmad, A. Qamar, and J. Iqbal, "Optimizing coordinated control of distributed energy storage system in microgrid to improve battery life," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106741, doi: 10.1016/j.compeleceng.2020.106741.

[46] Q. Yang, J. Li, W. Cao, S. Li, J. Lin, D. Huo, and H. He, "An improved vehicle to the grid method with battery longevity management in a microgrid application," *Energy*, vol. 198, May 2020, Art. no. 117374, doi: 10.1016/j.energy.2020.117374.

[47] T. Wu, F. Ye, Y. Su, Y. Wang, and S. Riffat, "Coordinated control strategy of DC microgrid with hybrid energy storage system to smooth power output fluctuation," *Int. J. Low-Carbon Technol.*, vol. 15, no. 1, pp. 46–54, Feb. 2020.

[48] B. Wang, C. Zhang, and Z. Y. Dong, "Interval optimization based coordination of demand response and battery energy storage system considering SOC management in a microgrid," *IEEE Trans. Sustain. Energy*, vol. 11, no. 4, pp. 2922–2931, Oct. 2020.

[49] M. Mohammadjafari, R. Ebrahimi, and V. P. Darabad, "Optimal energy management of a microgrid incorporating a novel efficient demand response and battery storage system," *J. Electr. Eng. Technol.*, vol. 15, no. 2, pp. 571–590, Mar. 2020, doi: 10.1007/s42835-020-00345-5.

[50] F. Tooryan, H. HassanzadehFard, E. R. Collins, S. Jin, and B. Ramezani, "Smart integration of renewable energy resources, electrical, and thermal energy storage in microgrid applications," *Energy*, vol. 212, Dec. 2020, Art. no. 118716, doi: 10.1016/j.energy.2020.118716.

[51] H. Afrakhte and P. Bayat, "A contingency based energy management strategy for multi-microgrids considering battery energy storage systems and electric vehicles," *J. Energy Storage*, vol. 27, Feb. 2020, Art. no. 101087, doi: 10.1016/j.est.2019.101087.

[52] S. Sinha and P. Bajpai, "Power management of hybrid energy storage system in a standalone DC microgrid," *J. Energy Storage*, vol. 30, Aug. 2020, Art. no. 101523, doi: 10.1016/j.est.2020.101523.

[53] I. R. S. da Silva, R. D. A. L. Rabêlo, J. J. P. C. Rodrigues, P. Solic, and A. Carvalho, "A preference-based demand response mechanism for energy management in a microgrid," *J. Cleaner Prod.*, vol. 255, May 2020, Art. no. 120034, doi: 10.1016/j.jclepro.2020.120034.

[54] F. Nejabatkhah, Y. W. Li, H. Liang, and R. R. Ahrabi, "Cyber-security of smart microgrids: A survey," *Energies*, vol. 14, no. 1, p. 27, Dec. 2020, doi: 10.3390/en14010027.
[55] X. Zhong, L. Yu, R. Brooks, and G. K. Venayagamoorthy, "Cyber security in smart DC microgrid operations," in *Proc. IEEE 1st Int. Conf. DC Microgrids (ICDCM)*, Jun. 2015, pp. 86–91.
[56] D.-J. Kang, H.-T. Kim, and S. Choi, "Methodology for quantifying the economic impact of cyberattacks on bulk electric systems," in *Proc. IEEE/IAS 55th Ind. Commercial Power Syst. Tech. Conf. (I&CPS)*, May 2019, pp. 1–5.
[57] E. Naderi and A. Asrari, "Approaching optimal power flow from attacker's standpoint to launch false data injection cyberattack," in *Proc. IEEE Green Energy Smart Syst. Conf. (IGESSC)*, Nov. 2020, pp. 1–6.
[58] H. Lin, C. Chen, J. Wang, J. Qi, D. Jin, Z. T. Kalbarczyk, and R. K. Iyer, "Self-healing attack-resilient PMU network for power system operation," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1551–1565, May 2018.
[59] S. Cruz-Duarte, P. A. Gaona-Garcia, and E. E. Gaona-Garcia, "Cybersecurity in microgrids," in *Proc. 6th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2018, pp. 7–12.
[60] K. Monteiro, M. Marot, and H. Ibn-Khedher, "Review on microgrid communications solutions: A named data networking-fog approach," in *Proc. 16th Annu. Medit. Ad Hoc Netw. Workshop (Med-Hoc-Net)*, 2017, pp. 1–8.
[61] M. Ndiaye, G. Hancke, and A. Abu-Mahfouz, "Software defined networking for improved wireless sensor network management: A survey," *Sensors*, vol. 17, no. 5, p. 1031, May 2017, doi: 10.3390/s17051031.
[62] A. Kondoro, I. B. Dhaou, H. Tenhunen, and N. Mvungi, "Real time performance analysis of secure IoT protocols for microgrid communication," *Future Gener. Comput. Syst.*, vol. 116, pp. 1–12, Mar. 2021, doi: 10.1016/j.future.2020.09.031.
[63] H. I. Kobo, G. P. Hancke, and A. M. Abu-Mahfouz, "Towards a distributed control system for software defined wireless sensor networks," in *Proc. 43rd Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2017, pp. 6125–6130.
[64] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "Fragmentation-based distributed control system for software-defined wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 2, pp. 901–910, Feb. 2019.
[65] M. Ndiaye, A. M. Abu-Mahfouz, G. P. Hancke, and B. Silva, "Exploring control-message quenching in SDN-based management of 6LoWPANs," in *Proc. IEEE 17th Int. Conf. Ind. Informat. (INDIN)*, Jul. 2019, pp. 890–983.
[66] J. Zhou, Y. Xu, L. Yang, and H. Sun, "Attack-resilient distributed control for islanded single-/three-phase microgrids based on distributed adaptive observers," *J. Mod. Power Syst. Clean Energy*, early access, Nov. 26, 2020, doi: 10.35833/MPCE.2020.000280.
[67] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2016, pp. 1–5.
[68] A. Saad, S. Faddel, T. Youssef, and O. A. Mohammed, "On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5138–5150, Nov. 2020.
[69] M. R. Habibi, H. R. Baghaee, T. Dragičević, and F. Blaabjerg, "Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks," *IEEE J. Emerg. Sel. Topics Power Electron.*, early access, Jan. 20, 2020, doi: 10.1109/JESTPE.2020.2968243.
[70] X. Xia, Y. Xiao, W. Liang, and M. Zheng, "GTHI: A heuristic algorithm to detect malicious users in smart grids," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 2, pp. 805–816, Apr. 2020.
[71] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in DC microgrids," *IEEE Trans. Power Electron.*, vol. 36, no. 3, pp. 2522–2532, Mar. 2021.
[72] M. Buevich, D. Schnitzer, T. Escalada, A. Jacquiau-Chamski, and A. Rowe, "Fine-grained remote monitoring, control and pre-paid electrical service in rural microgrids," in *Proc. 13th Int. Symp. Inf. Process. Sensor Netw. (IPSN)*, Apr. 2014, pp. 1–11.
[73] E. J. Palacios-Garcia, E. Rodriguez-Diaz, A. Anvari-Moghaddam, M. Savaghebi, J. C. Vasquez, J. M. Guerrero, and A. Moreno-Munoz, "Using smart meters data for energy management operations and power quality monitoring in a microgrid," in *Proc. IEEE 26th Int. Symp. Ind. Electron. (ISIE)*, Jun. 2017, pp. 1725–1731.
[74] N. Liu, X. Yu, C. Wang, and J. Wang, "Energy sharing management for microgrids with PV prosumers: A Stackelberg game approach," *IEEE Trans. Ind. Informat.*, vol. 13, no. 3, pp. 1088–1098, Jun. 2017.
[75] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets," *Appl. Energy*, vol. 210, pp. 870–880, Jan. 2018, doi: 10.1016/j.apenergy.2017.06.054.
[76] M. L. Di Silvestre, P. Gallo, M. G. Ippolito, R. Musca, E. R. Sanseverino, Q. T. T. Tran, and G. Zizzo, "Ancillary services in the energy blockchain for microgrids," *IEEE Trans. Ind. Appl.*, vol. 55, no. 6, pp. 7310–7319, Nov. 2019.
[77] R. Yaqub, S. Ahmad, H. Ali, and A. U. Asar, "AI and blockchain integrated billing architecture for charging the roaming electric vehicles," *IoT*, vol. 1, no. 2, pp. 382–397, Nov. 2020.
[78] M. O. Okoye, J. Yang, J. Cui, Z. Lei, J. Yuan, H. Wang, H. Ji, J. Feng, and C. Ezeh, "A blockchain-enhanced transaction model for microgrid energy trading," *IEEE Access*, vol. 8, pp. 143777–143786, 2020, doi: 10.1109/ACCESS.2020.3012389.
[79] T. Aljohani, A. Ebrahim, and O. Mohammed, "Dynamic real-time pricing structure for electric vehicle charging considering stochastic microgrids energy management system," in *Proc. IEEE Int. Conf. Environ. Electr. Eng., IEEE Ind. Commercial Power Syst. Eur. (EEEIC/I&CPS Europe)*, Jun. 2020, pp. 1–8.
[80] Z. Latif, K. Sharif, F. Li, M. M. Karim, S. Biswas, and Y. Wang, "A comprehensive survey of interface protocols for software defined networks," *J. Netw. Comput. Appl.*, vol. 156, Apr. 2020, Art. no. 102563, doi: 10.1016/j.jnca.2020.102563.
[81] N. Kiran, C. Pan, S. Wang, and C. Yin, "Joint resource allocation and computation offloading in mobile edge computing for SDN based wireless networks," *J. Commun. Netw.*, vol. 22, no. 1, pp. 1–11, Feb. 2020, doi: 10.1109/JCN.2019.000046.
[82] S. Chen, H. Wen, J. Wu, W. Lei, W. Hou, W. Liu, A. Xu, and Y. Jiang, "Internet of Things based smart grids supported by intelligent edge computing," *IEEE Access*, vol. 7, pp. 74089–74102, 2019, doi: 10.1109/ACCESS.2019.2920488.
[83] M. S. Munir, S. F. Abedin, N. H. Tran, and C. S. Hong, "When edge computing meets microgrid: A deep reinforcement learning approach," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7360–7374, Oct. 2019.
[84] M. A. Hasnat, M. J. Hossain, A. Adeniran, M. Rahnamay-Naeini, and H. Khamfroush, "Situational awareness using edge-computing enabled Internet of Things for smart grids," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6.
[85] S. Marzal, R. Salas, R. González-Medina, G. Garcerá, and E. Figueres, "Current challenges and future trends in the field of communication architectures for microgrids," *Renew. Sustain. Energy Rev.*, vol. 82, pp. 3610–3622, Feb. 2018, doi: 10.1016/j.rser.2017.10.101.
[86] R. C. A. Alves, D. A. G. Oliveira, G. C. C. F. Pereira, B. C. Albertini, and C. B. Margi, "WS3N: Wireless secure SDN-based communication for sensor networks," *Secur. Commun. Netw.*, vol. 2018, pp. 1–14, Aug. 2018, doi: 10.1155/2018/8734389.
[87] Y. Li, Y. Qin, P. Zhang, and A. Herzberg, "SDN-enabled cyber-physical security in networked microgrids," *IEEE Trans. Sustain. Energy*, vol. 10, no. 3, pp. 1613–1622, Jul. 2019.
[88] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Trans. Ind. Informat.*, vol. 17, no. 1, pp. 650–658, Jan. 2021.
[89] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3800–3815, Sep. 2020.
[90] S. Sahoo, S. Mishra, J. C.-H. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.
[91] A. Aydeger, K. Akkaya, M. H. Cintuglu, A. S. Uluagac, and O. Mohammed, "Software defined networking for resilient communications in smart grid active distribution networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.
[92] C. Stefanovic, M. Angjelichinoski, P. Danzi, and P. Popovski, "Resilient and secure low-rate connectivity for smart energy applications through power talk in DC microgrids," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 83–89, Oct. 2017.
[93] M. Abujubbeh, F. Al-Turjman, and M. Fahrioglu, "Software-defined wireless sensor networks in smart grids: An overview," *Sustain. Cities Soc.*, vol. 51, Nov. 2019, Art. no. 101754, doi: 10.1016/j.scs.2019.101754.

MUSA NDIAYE received the B.Eng. degree in electrical and electronics engineering from Copperbelt University, Zambia, in 2011, the M.Sc. degree in microelectronics and communications engineering from the University of Northumbria at Newcastle, U.K., in 2013, and the Ph.D. degree from the Advanced Sensor Networks Group, University of Pretoria, South Africa, in 2020.

He is currently a full-time Lecturer of electronics and computer engineering with Copperbelt University. His research interests include software-defined wireless sensor networks, network management, sensor node hardware development, and a wide range of the Internet of Things technologies.

GERHARD P. HANCKE (Life Fellow, IEEE) received the B.Sc. and B.Eng. degrees from the University of Stellenbosch, South Africa, in 1970, and the M.Eng. degree in electronic engineering from the University of Stellenbosch, in 1973, and the D.Eng. degree from the University of Pretoria, South Africa, in 1983.

He is currently a Professor with the College for Automation and the College for Artificial Intelligence, Nanjing University of Posts and Telecommunications, China, and the Department of Electrical, Electronic and Computer Engineering, University of Pretoria. He is recognized internationally as a Pioneer and a Leading Scholar at the Industrial Wireless Sensor Networks Research. He initiated and co-edited the first Special Section on Industrial Wireless Sensor Networks in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, in 2009 and the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, in 2013. He co-edited a textbook, *Industrial Wireless Sensor Networks: Applications, Protocols, and Standards* (2013), the first on the topic. He has been serving as an Associate Editor and a Guest Editor for the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE ACCESS, and the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS. He is a Co-Editor-in-Chief of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS and an Senior Editor of IEEE ACCESS.

ADNAN M. ABU-MAHFOUZ (Senior Member, IEEE) received the M.Eng. and Ph.D. degrees in computer engineering from the University of Pretoria.

He is currently the Center Manager of the Emerging Digital Technologies for 4IR (EDT4IR) Research Center, Council for Scientific and Industrial Research (CSIR), a Professor Extraordinaire with the Tshwane University of Technology, a Visiting Professor with the University of Johannesburg, and an Extraordinary Faculty Member with the University of Pretoria. He participated in the formulation of many large and multidisciplinary research and development successful proposals (as a Principal Investigator or a main author/a contributor). He is the founder of the smart networks collaboration initiative that aims to develop efficient and secure networks for future smart systems, such as smart cities, smart grids, and smart water grids. His research interests include wireless sensor and actuator networks, low-power wide area networks, software-defined wireless sensor networks, cognitive radio, network security, network management, and sensor/actuator node development. He is a member of many IEEE technical communities. He is an Associate Editor of IEEE ACCESS, IEEE INTERNET OF THINGS, and IEEE TRANSACTION ON INDUSTRIAL INFORMATICS.

HUIFENG ZHANG (Member, IEEE) received the Ph.D. degree from the Huazhong University of Science and Technology, Wuhan, China, in 2013.

From 2014 to 2016, he was a Postdoctoral Fellow with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China. From 2017 to 2018, he was granted as a Visiting Research Fellow by the China Scholarship Council to study at Queen's University Belfast and the University of Leeds, U.K. He is currently an Associate Professor with the Institute of Advanced Technology, Nanjing University of Posts and Telecommunications. His current research interests include energy management of microgrids, optimal operation of power systems, distributed optimization, and multi-objective optimization.