Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency

Saba Al-Rubaye, *Senior Member, IEEE*, Ekhlas Kadhum, Qiang Ni, *Senior Member, IEEE*, and Alagan Anpalagan, *Senior Member, IEEE*

***Abstract*—Software-defined networking (SDN) is a key enabling technology of industrial Internet of Things (IIoT) that provides dynamic reconfiguration to improve data network robustness. In the context of smart grid infrastructure, the strong demand of seamless data transmission during critical events (e.g., failures or natural disturbances) seems to be fundamentally shifting energy attitude toward emerging technology. Therefore, SDN will play a vital role on energy revolution to enable flexible interfacing between smart utility domains and facilitate the integration of mix renewable energy resources to deliver efficient power of sustainable grid. In this regard, we propose a new SDN platform based on IIoT technology to support resiliency by reacting immediately whenever a failure occurs to recover smart grid networks using real-time monitoring techniques. We employ SDN controller to achieve multifunctionality control and optimization challenge by providing operators with real-time data monitoring to manage demand, resources, and increasing system reliability. Data processing will be used to manage resources at local network level by employing SDN switch segment, which is connected to SDN controller through IIoT aggregation node. Furthermore, we address different scenarios to control packet flows between switches on hub-to-hub basis using traffic indicators of the infrastructure layer, in addition to any other data from the application layer. Extensive experimental simulation is conducted to demonstrate the validation of the proposed platform model. The experimental results prove the innovative SDN-based IIoT solutions can improve grid reliability for enhancing smart grid resilience.**

***Index Terms*—Industrial Internet of Things (IIoT), platform, resilience, service functions and management, smart grid, software-defined networking (SDN).**

I. INTRODUCTION

INDUSTRIAL Internet of Things (IIoT) is a new communication paradigm that combines information and technologies to enable real-time monitoring and provide controlling for industrial domains [1]. In the context of smart grids, the vision of deploying IIoT relies on using low-power communication technologies by employing standard Internet protocols (IPs) [2] in order to enable end-to-end communication between data center and remote access devices. Utility industry required certain functionalities (e.g., routing) to enable a universal monitoring and resiliency for distributed energy generation [3]. However, there are still two main challenges of IIoT to become in reality. First of all, the current low-power wireless technologies are not meeting energy consumption requirement with high reliability in industrial applications. The main requirements are already meting legacy deployments using wired technologies, but still undergoing development for wireless technologies. Second, IP stack can support end-to-end communications, but it is not flexible enough to interface remote devices that are regularly deployed or removed at industry locations. Considering the aforementioned challenges, there is a strong demand to support adaptive network architecture that can handle real-time changes in the smart grid data. These data process may include system monitoring, failure events, and network expansion requests. In context of smart deployment, operators have to manually reconfigure devices whenever an update request is received. This can be performed by separately configuring devices (e.g., router or switch). On the other hand, the features of ubiquitous data sensing (e.g., interaction, aggregating, and analysis) is important to be considered as a promising solution for industrial revolution.

A comprehensive communication profile with compliant services and topologies are normally managed according to IEC61850 standard [5], [6] in the smart grid. IEC61850 originally specified for substation automation and extended later to cover most aspects of smart grid communication. The provision of communication factor to perform the required functions based on this standard is important to create suitable smart grid communication infrastructure [7]. However, communications infrastructure needs to deal with different levels of requirements such as controlling data flows and managing voltage levels between various grid layers. Integrated software-defined networking (SDN) with IEC61850-based substation automation in power systems can facilitate the data forwarding of intelligent electric devices (IEDs) in a substation to control traffic congestion. Despite the fact that IEC61850 is a forward-based standard, but not all the features were dynamic and adaptive networking. The need of modern technology and extensive standardization process causes a huge gap in the smart grid requirements. For example, IEC61850 standard was originally produced for local area network that is used for intrasubstation

Manuscript received April 17, 2017; revised June 30, 2017; accepted July 21, 2017. Date of publication August 2, 2017; date of current version February 25, 2019. *(Corresponding author: Saba Al-Rubaye.)*

S. Al-Rubaye was with Quanta Technology, Toronto, ON L3R 5G3, Canada (e-mail: saba.alrubaye@ieee.org).

E. Kadhum is with the Department of Control and System Engineering, University of Technology, Baghdad, Iraq.

Q. Ni is with the School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, U.K.

A. Anpalagan is with the Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON M5B 2K3, Canada.

Digital Object Identifier 10.1109/JIOT.2017.2734903

communications. The requirement of this standard was accepted for IEDs to achieve communication between substations level [8]. However, later on such modification has been made in this standard to release IEC 61850-90-1; this modified standard can support intersubstation communications [9].

The ultradense deployments [10] of Internet connected devices motivate the leverage of SDN deployment within the context of fifth-generation (5G) smart applications. This will become reality by connecting various machines to allow hybrid automation between resources and industrial process requests [11], [12]. These new emerging technologies are expected to reshape the future of industries by using new concepts to handle IIoT applications for smart manufacturing, utility, and factory of things [13]. In the context of SDN paradigm, a key advantage of SDN is the potential ability to improve flexibility, scalability, and interoperability of smart grid using infrastructure/data forwarding devices [14] to prevent failures and attacks. Therefore, SDN [15] is considered as a promising solution for addressing the challenge and leveraging IIoT platform in the modern utility. The tremendous growth in the amount of electric data generated by utility providers and customer needs to be monitored, analyzed, and controlled especially in the modern smart grid technologies that require adaptive network bandwidth. Using SDN can enhance the smart grid networks by decoupling of infrastructure and control plane to increase the flexibility, interoperability, and reliability of the system, and reduces the cost incurred during any network upgraded due to simplified hardware operation [16]. In software-based networks, SDN [17] controller is able to extract the data using control function from data forwarding/infrastructure plane to reschedule and reconfigure the available resources. The network switches are forwarding the data, by received commands from central controller. This can be performed through open programmable interfaces, which are responsible for network virtualization, flow monitoring, centralized control, and fast fault detection, as shown in Fig. 1. Abstraction of SDN platform for wireless networking still undergoing development, and this can be seen as a key technology enabler for 5G networks [18], [19].

Although SDN requirements are not defined well for wireless domains [20], existing research on IIoT enabled by SDN controller in smart grid networks are not sufficient to cover the real-time monitoring and traffic problems. References [21]–[23] studied SDN and real-time monitoring in smart utility paradigm. An aggregation technique to hide the sensitive information in smart grid is presented in [24] that does not involve real-time monitoring system. Another sight of SDN platform capability to manage the data flow in the power system networks is given in [25], the authors propose an effective SDN platform to deliver high data rate of phasor measurement units (PMUs) and consumers with multicast data rate requirements.

The use cases of SDN controller has been addressed to prove the ability of SDN of provides underlying technology to manage the traffic engineering for PMUs in smart grid networks. However, the authors presented only a specific case that is not necessarily applicable to all other use cases of SDN in smart grid networks. Thus, reliable and sustainable electrical service is a contemporary issue challenging the smart grid networks [26]. The systems proposed in [27] cannot satisfy the ideal data scheduling and reconfiguration of power grid in group of smart grid networks, since the authors suggested a centralized SDN controller without any consideration of real-time monitoring system. Deprived of realistic approach of the resilience support that SDN can bring to the modern utility and methods to control the smart grid industry is uncertain to adopt SDN technologies. Key challenge in sympathetic these problems is important to respect smart utility requirements and data monitoring-based sensor and control in smart grids

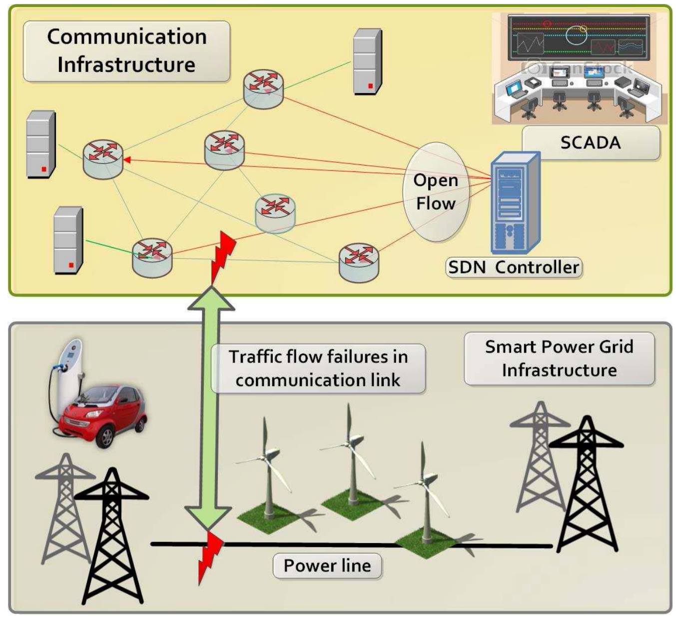

Fig. 1. SDN platform enabling fault detection in smart grid [4].

To the best of our knowledge, there is a limited work of IIoT in smart grid-based SDN platform to monitor, natural disaster, electric outage, and fault events. Unlike existing approaches, our model comprehensively captures the traffic flow of a typical smart grid in 5G networks employing SDN platform. Thus, we tackle the above problems by presenting a new vision of SDN platform for smart utilities to provide real-time data monitoring by performing control functionality that can give support to IIoT objects in case of fault and outage scenarios. The flexibility and capabilities of each entity in SDN to manage the data flow can make it a great fit under IIoT scenarios. In comparison to this paper, several works have elaborated on monitoring systems and fault recovery in grid network-based SDN architecture. Different from existing methodologies, our system model comprehensively considers both smart grid networks and SDN platform for the traffic flow scenarios. For example, function management on SDN switches are assumed in smart grid environment [28] by considering a centralized SDN controller employed communication protocol messages to detect the fault or outage link and trigger re-establishment activities. A similar idea of local outage in the smart grid network to be re-established has been presented in [29] by applying flow table admissions to support the fault link for recovery.

The novel contributions of this paper are summarized as follows.

1) SDN platform is proposed to enable IIoT technology and manage real-time data energy profiles by establishing dynamic routes for grid control commands in smart grid paradigm.
2) SDN platform within the context of smart grid is presented in order to identify the knowledge gap and bring together the information resources through SDN controller to reduce the traffic flow at the network core and end-to-end latency between smart utility devices.
3) Developed algorithm is proposed to adopt dynamic change in real-time smart grid system. The monitoring algorithm is developed to manage the traffic route and outage link, where SDN can reset switches or re-establish new routing of control application upon the discovery of negotiated switches, to maintain the system quality. Thus, any fault event can be handled by SDN in real time without any interruption.
4) Different topology scenarios are considered to demonstrate rerouting data among SDN switches (e.g., during network disturbance events). Simulation results provide evidence for the features and functionality in the SDN controller to achieve more than 80% accuracy during failure conditions.

The remaining parts of this paper are organized as follows. Section II proposes SDN platform and IIoT technology scheme is discussed in detail. In Section III, developed algorithm for system monitoring process and IIoT connectivity are presented. In Section IV, different use case scenarios is considered for real-time monitoring. Experimental results and validation are presented in Section V. Finally, this paper is concluded in Section VI.

II. SDN Platform Empowered by IIoT Technology

SDN platform provide necessary features of virtual resources and interfaces to support IIoT platform in smart grids [30]. To provide application oriented services and system interoperability, we propose SDN platform empowered by IIoT using three layers of SDN controller model, as shown in Fig. 2. Infrastructure layer consists of all hardware and physical equipments to perform route switching between network clusters and normally include SDN switches. Whenever new traffic flows are received by SDN switches, the routing requirements will be sent to the above control layer for evaluating data path allocation procedures. Typically, control layer will process the requested path and assign new routing rules and policies in agreement with application layer. Application layer at the back-end system can manage services for utility authentication contains of IIoT server to deliver and exchange the information of each service request and data storage based on policy, standards, events, and controls. The interoperability between these layers allows to process any application using the underlying network infrastructure. However, in order to achieve this an open communication protocol is employed to support the required functionality and resource allocation.

A. Infrastructure Layer

This layer is responsible for data forwarding between network clusters. Infrastructure layer consists of different devices such as (e.g., smart sensor and actuators), PMU, fieldbus control, advance metering infrastructure, demand response system, and core smart grid networks (e.g., gateway, switches, access point, base stations, and routers). In addition to data forwarding, this layer can perform monitoring of local information and conducting data gathering statistics. The data path management can be estimated locally at this layer using node-to-node negotiations in real-time statues. On the other hand, requests for more resource or bandwidth might be hard to meet real-time system requirement as this is unpredictable information subject to traffic profiles and application types. Once a change request in the path is computed by high layers, infrastructure layer will allocate supporting resources to perform data forwarding request. SDN data path consists of device interface agent and set of engines for data forwarding and processing functions. These engine and functions may contain data forwarding technique for external interfacing possibility or controlling internal traffic or exchanging the information with network edge functions.

B. Control Layer

In our proposed SDN platform, control layer consists of two main mechanisms: one of them is network operating system to manage, operate, and secure the data. Network operating system entity needs special interface for internal interaction and communication to enable multidomain interoperability [31]. The other one is advance distribution management system that includes supervisory control and data acquisition, distribution management system, and distributed energy resource management system. Control layer is appreciated for the ability of interfacing between application layer and physical infrastructure. Normally, the interaction with other layers is defined by application program interfaces (APIs), this can be either northbound or southbound. Control layer is responsible for programming and managing physical elements using southbound interfaces (SIs) and it has the ability to change their functionality according to network requirements. To this end, control layer can provide necessary information to infrastructure layer and define network operation and routing requirements. It can deliver relevant information on the new data paths to application layer using the northbound APIs. However, the whole data path may be upgraded if the application layer requested changing based on the data aggregation, communication link availability and processing scheme.

C. Application Layer

Application layer is the top layer of SDN platform, and it includes data center, servers, storage, analysis, processing, and

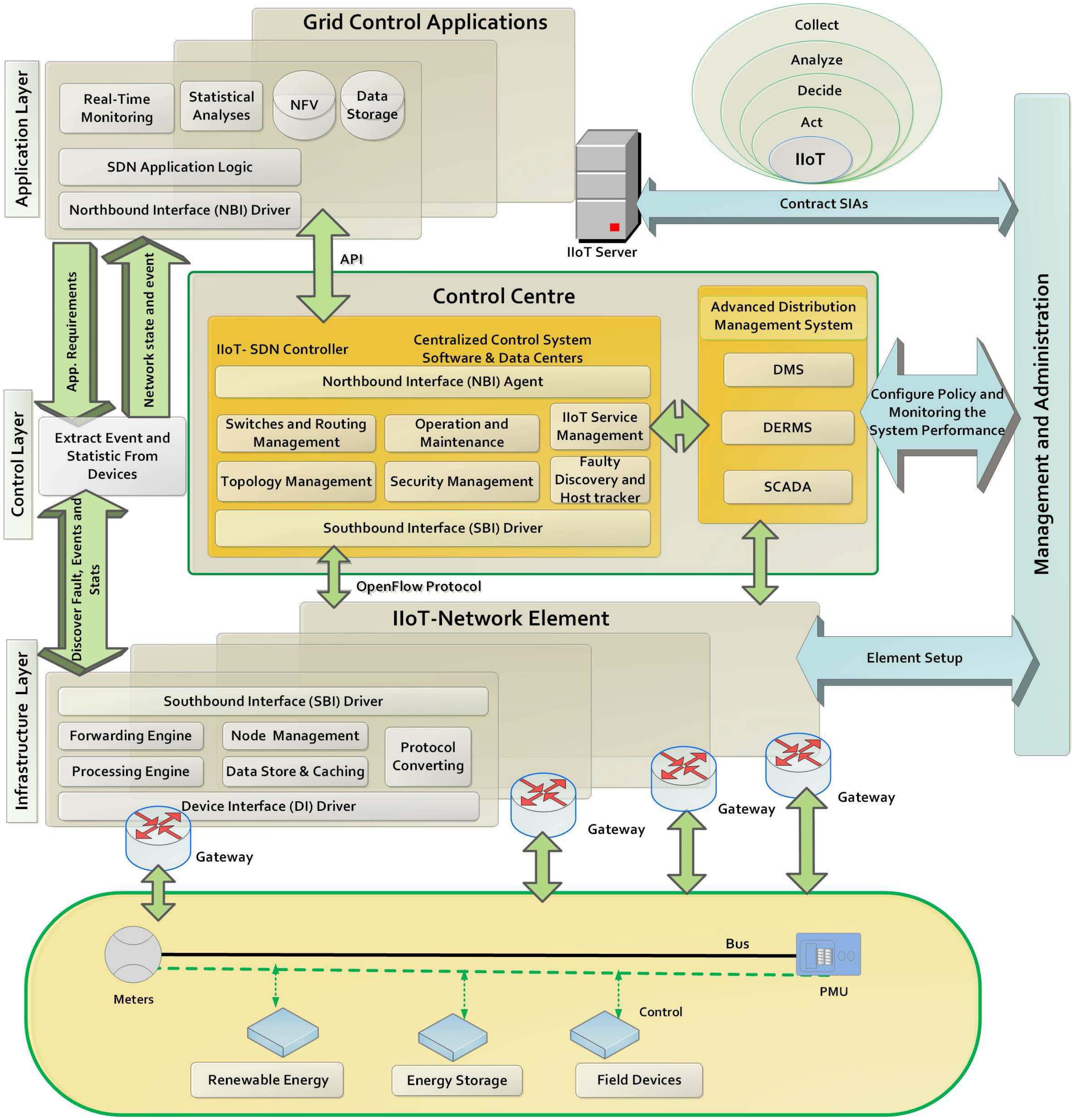

Fig. 2. SDN architecture-based IIoT for grid resilience.

applications. This layer can facilitate overall current status of any data path to compute the necessary end-to-end configurations to be performed by lower layers. In this layer, APIs can be used to design various innovative applications (e.g., equipment fault monitoring, utilization rate monitoring, and product processing status monitoring). Therefore, developers can accelerate the design of new applications by customizing the data collection, transmission and processing. To this end, application layer can collect an abstracted view of data network from SDN controllers by applying this information to deliver a suitable instructions for control layer. In this proposed framework, the application layer consists of IIoT servers for different smart grid applications, the interaction with control layer through APIs is known as northbound interface (NI).

D. Northbound APIs for Network Applications

NI is denoted from SDN controller viewpoint as APIs. Usually, NI APIs extract low-level guidance and critical information form control layer to use it for further processing. In general, SDN controller offers APIs to allow for meaning of interaction requirements in intellectual terms. Application layer is using NI to reconfigure SDN controller with the corresponding information as regulated by northbound protocol. To date, NI APIs is not well standardized, often allows to monitor the orchestrate of network behavior through SDN controller. Therefore, application layer is not directly involved with details information of SI. Additionally, application layer is not required to recognize all information about network real-time status. For example, certain application associated with SDN controller may carry the information about a certain path layout. But SDN controller is the only entity responsible for generating an appropriate instructions to adapt forwarding tables between involved SDN switches. To conclude, orchestration layer needs to facilitate new APIs in order to monitor and manage smart grid networks.

E. Protocol Options for Southbound Interface

SI is well-defined from SDN controller perspective to interconnect particular smart grid network element commands. This SIs perform adjustments to resources and data path between switches using shared infrastructure with variable parameters. The SIs have the functionality to be interfaced to any device in a flexible manner to exchange the necessary control information without any compatibility concerns. This wide interoperability between various vendor devices allows the controller to collect the requested key performance indicators dynamically in real-time. The new routing requests from the infrastructure layer and the SDN switch configurations are communicated to control layer through the SI. Similarly, corresponding control information is transferred back from SDN controller to SDN switches using the same southbound protocol. The control messages transmitted from SDN controller to corresponding SDN switches is defined as OpenFlow protocol. This protocol can be used to manage the data forwarding and synchronous operations along data path [32]. Moreover, the synchronous communications messages are used by OpenFlow protocol to enable SDN switches informing the SDN controller about real-time network events such as flow arrival and fault and flow termination.

F. IIoT Connectivity Adapter

IIoT connectivity adapter or software element is responsible for interconnection between smart sensor or actuators and future smart application mechanisms. This adapter employs special protocol agents to support connectivity interface to the IIoT protocol. The adapter can support front/back end transmissions to allow collected data for delivering to the above layers for further processing.

G. Gateways

Gateways are located at IIoT edge to interface field smart grid devices with wide area network. In other words, gateway elements can act as mediator for data exchange between unconstrained technologies, which is required in the core of IIoT network, and constrained technologies to provide connectivity via smart grid remote nodes. Therefore, gateway facilitates seamless connectivity to wide range of devices employing different protocols such as hypertext transfer protocol, IPv4/v6, efficient XML interchange, constrained application protocol, and 6LoWPAN, which are suitable even for very constrained devices. Sometime all these kind of protocols are required for conversion to enable interoperability with IIoT remote devices and SDN controller [1].

H. Management and Administration

This segment handles customer authentication and access authorization. Management system is required necessary to maintain and increase confidentiality, integrity, and availability of signaling exchanged between different layers to communication bus.

I. Data Services

Successful data delivery can be obtained in the smart grid domain based on SDN by integrating data context within communication protocol and orchestrated control across IIoT chain. SDN can provide necessary underlying layer services to perform data aggregation, communications, and data processing as follows.

1) *Data Aggregation:* This functionality enables multidevice interfaces to perform single or multisessions by providing API. The goal is to allow processing of various types of data within different attributes. Any session may be managed by a single user to customize the data profile and orchestrate a special format using the appropriate APIs. These different types of data are aggregated using this functionality to enable them to be transferred using the common networking infrastructure.
2) *Data Communication:* Transferring the data between industrial nodes are performed using combination of wireless and wired connections. The interaction among these devices is the foundation of new intelligent approach, which allows, for example, to design interactive mechanisms for avoiding deadlocks, or deploying system resources according to real-time requirements of different applications. These problems can be reported through orchestration layer to reconfigure data path and avoid service interruptions.
3) *Data Management:* In software defined data processing, this data should be categorized according to application types and path requirements. The determination of such categories is performed centrally based on processing requirements. For example, an industrial robot requires a certain path planning to support large amount of data processing. Therefore, large amount of virtual resources with multigigabyte interface is allocated to connect such data to the cloud. Processing the path information will require to allocate considerable computing resources in cloud and subsequently automated management of the robot using IIoT protocol. Therefore, software-defined data processing can provide more flexibility for remote control and centralized data storage.

III. Resilient Virtual Network Layer for IIoT Connectivity

SDN platform is integrated with network function virtualization (NFV) to provide virtual resources and applications on top of physical commercial off-the-shelf. The virtual network unleashes new era of central management that can meet the requirements of utility service providers to process large amounts of data over wireless links. By influence control plane functionality, SDN virtual entity can enable smart grid network status monitoring. For example, SDN virtual entity can be employed dynamic estimation of QoS metrics (e.g., data latency and packet loss rate) based on the dynamic development of the underlying infrastructure network. Based on the long monitoring, SDN controller can rapidly re-establish a virtual network for a smart grid control application to isolate uncertain switches. Therefore, monitoring system is integrated with SDN/NFV in order to support automation of data delivery, negotiation of IIoT service parameters for resource allocate, policy administration, and quality assurance.

The key application of this real-time monitoring is to adapt network infrastructure and associate operations using virtual interfaces. Integration of SDN and NFV allows for immediate reacting to critical or fault events and unpredictable behavior of IIoT platform. For example, once the system observes overload or failure events an automated forwarding behavior will be triggered by SDN/NFV in order to stabilize the utility grid. NFV may create additional virtual machines that hosts certain applications to handle data sensor processing requirements during overload conditions or heavy IIoT services. Time stamping of packets is provided by SDN controller for orchestrator to synchronize the clocks of involved nodes. However, one or several SDN controllers may be required in a particular utility network subject to distribution scheme and clustering model. This requires to change the hierarchical model of association between different network entities and the authentication to handle IIoT services. Smart sensors/actuators are dynamically sending information on traffic pattern changes to SDN controller. Therefore, SDN controller can discover the appropriate routes to nearest data center in a reliable and secure manner in order to enhance the overall performance of IIoT services.

In smart networks, edge devices are required to update the flow database located at the SDN controllers. Database entity comprises traffic patterns for each data flow to map IIoT platform services to the smart grids. The database entity may also include additional information such as utility identification, types of application, data priority, and critical data required [33]. To dynamically control traffic flows in SDN platform, we design a simple framework, as shown in Fig. 3. Any time the data flow arrives the application layer in the SDN will send a request to SDN controller in order to update the database entity. SDN controller will start to evaluate the network status such as throughput and packet loss rates of the traffic pattern. These evaluations are used to predict any congestion or failure occurrence in the services. Later, SDN controller will evaluate the QoS to resolve any bottlenecks based on adopted polices and make decide if there is any other

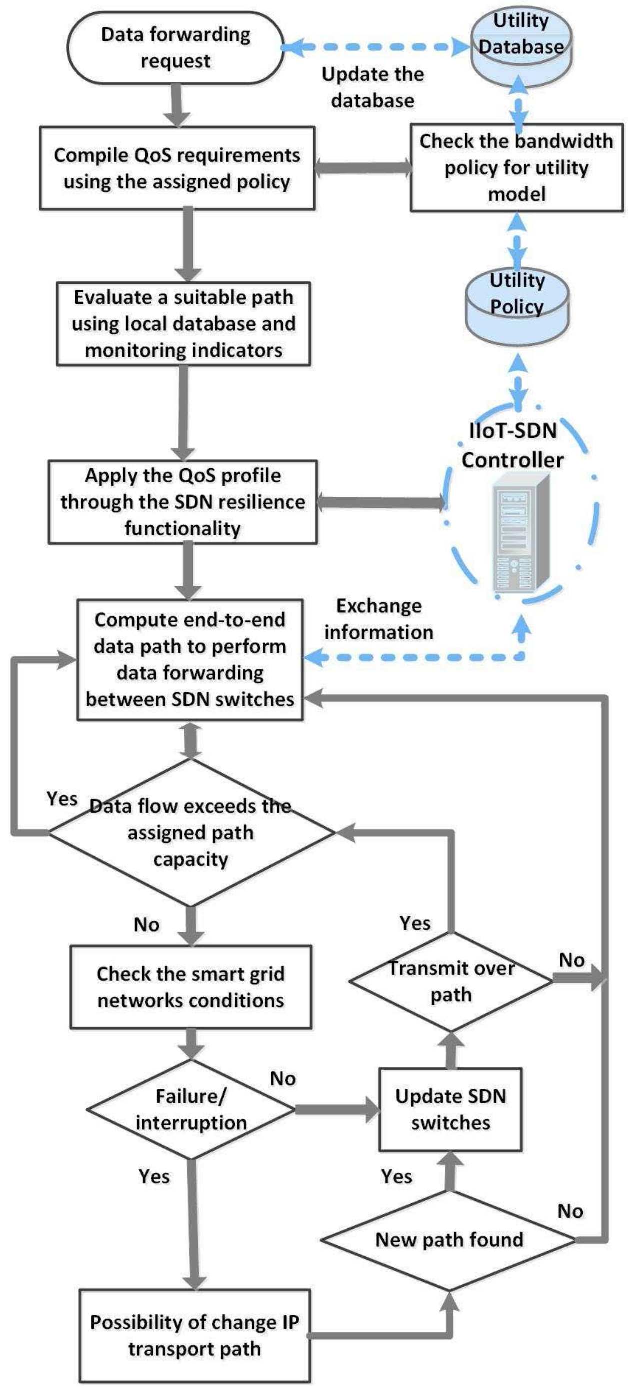

Fig. 3. Algorithm of SDN-based network configuration.

better route for data path. If the QoS is not guaranteed, SDN controller will evaluate the traffic profiles of the smart grid network and decide the possibility of changing data forwarding path. SDN switches can be reprogrammed periodically to reconnect different network sites using various requirements and resources. All SDN switches are connected with data centers to combine databases for a centralized control and monitoring of network performance. In this proposed algorithm, status data are collected by SDN switches to predict the necessary statistics required for managing the traffic route based on required QoS. It is necessary to inform the SDN controller dynamically on any changes of data monitoring. In the second stage, the obtained dataset will be analyzed by extraction of data features and structure in a procedure that may be apply as an input value for the estimation algorithm. Additionally, single SDN system can be a adapted subject to its own protocol parameters and cooperates with associated resources without interfering with any provision providers. Each SDN switch has a common control interface protocols (e.g., OpenFlow) to deal with different forwarding machineries supported by different equipment.

A. *Data Flow Path Recovery for QoS Preservation*

SDN controller is the entity that performs regular monitoring and evaluations of traffic flow status in smart grid networks. Therefore, when the traffic flows are affected by certain failure, SDN will identify the impacted data flow and will reschedule that flow subject to requested QoS. On the other hand, traffic flow will be reprocessed by common routing module. Data flows with highest priority will be assigned and guaranteed for alternative route first, while dropping further data redirection efforts. Consequently, traffic flows with low priority need to be eliminated to allow high priority data traffic to be served. Overloaded paths should not be supported as this will cause congestions and will most likely to cause a failure that triggers a new series of unnecessary actions for route changes. The alternative path configuration is published to SDN switches causing intermediary retrieval route configurations to be removed and another protection routes are recognized.

IV. Grid Resiliency-Based Different Topology Scenarios

Smart grid networks have critical infrastructures to support reliable communications between different entities. Therefore, end-to-end path connectivity needs to be guaranteed under any environment conditions. There is a strong need to develop a recovery mechanism that restores network balance as soon as a failure occurs. This will help to avoid link outages that may escalate the power imbalance between smart grid sites. In this paper, we consider different use cases scenarios for real-time monitoring, one of them assumes the system under fault scenario with dynamic flow path restoration, as well as we considered smart grid traffic conditions under expansion scheme. In this paper, we develop new resilience schemes that identifying alternative data routes for SDN-based networks beyond literature such as [34]. In our proposal, the faulty flow will be removed from the database list for the considered alternatives until the end of flow list. Once a flow is chosen, an acknowledgment messages will be exchanged between SDN controller and switches to reroute the data path. However, in order to reduce time of failure detection, we employ an independent discovery of failure by employing bidirectional forwarding detection (BFD) [35]. BFD is a type of protocol responsible for monitoring the status of communication link between two SDN switches.

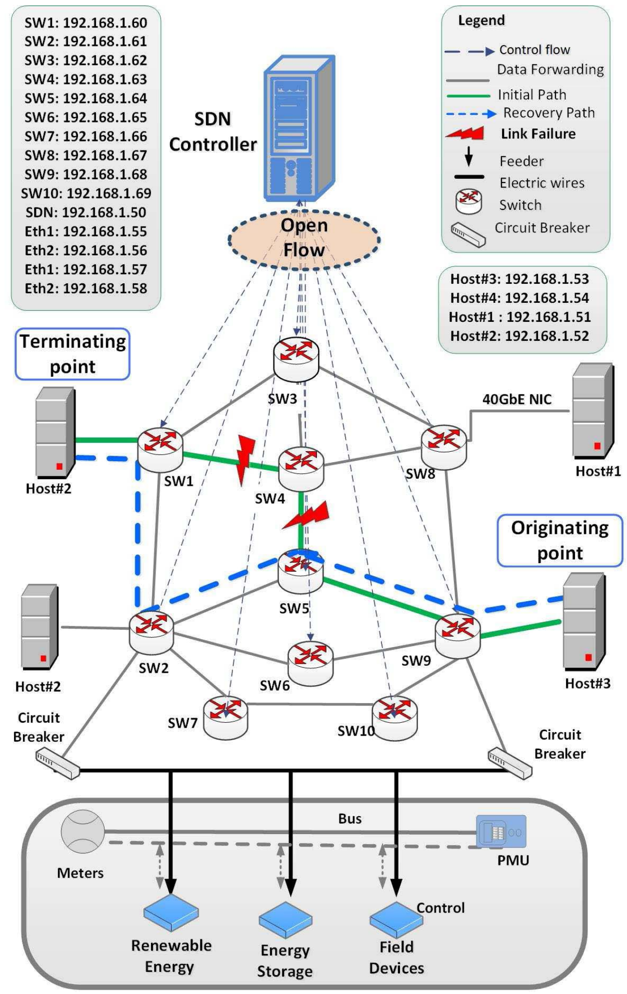

Fig. 4. Network fault detection scenario.

A. *Network Fault Detection Scenario*

Any failures or disturbance in the power system can cause dissatisfaction on large number of energy consumers. These failures have negative impact on power grid system, especially in delivering the critical information. As stated earlier, SDN controller can define a new route in case of discover any occurrence of network fault or communication failure. The switches will start to request for alternative routing, once another route is identified by control layer, the necessary redirecting instructions will be sent to associate SDN switches. In this regard, a developed algorithm as mentioned in the previous section is considered to manage the grid failures including failure activities that can be triggered by SDN functionality and protocols in order to mitigate expected failures. Once the calculation methods anticipate a failure, detective actions to mitigate this issues will be scheduled and activated. To analyze the restoration of link behavior in smart grid, we assume that an outage happen between SDN switches #1 and #4 of the power network infrastructure. The disrupted data is exchanged between hosts #2 and #3, as shown in Fig. 4. Following the disruption between SDN switches, the links between other switches (SW1), (SW4), (SW5), and (SW9) are also impacted and became invalid. Hence, SDN controller will receive an updated message about

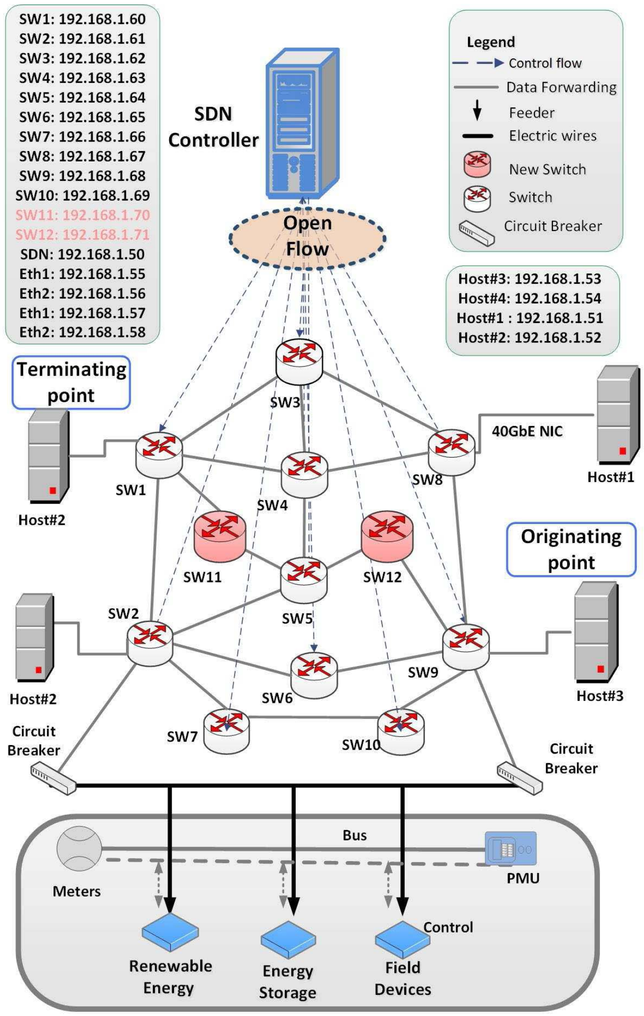

Fig. 5. Network upgrading scenario.

path changes and resilience functionality starting to track permissions and connectivity permutations. As soon as the connection failure occurs between SDN switches and the primary path disconnected, the resilience functionality in the SDN controller will perform topology scanning to evaluate the restoration path of (SW1, SW2, SW5, and SW9) to be able for reconnecting the utility provider with IIoT server. Finally, SDN controller updates the flow table with new predictions and inform the associated switches to change data path considering the requested QoS.

B. Network Upgrading Scenario

In modern grid design trends, there is a huge demand to install additional SDN switches in order to further slice the power grid area and interface the electric data at grid edges. In this way, we deploy additional SDN switches to our smart grid network scenario to meet the data communication requirements with multialternative paths, as shown in Fig. 5. This expansion enables SDN controller to choose among short/long paths to improve the services provided to smart grid applications. As soon as new SDN switches are deployed in the smart

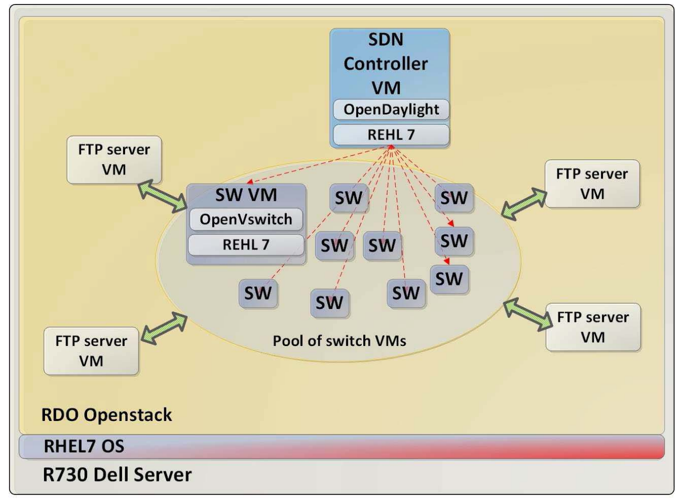

Fig. 6. Experimental setup.

grid network, SDN controller will receive corresponding message for new paths and starts to update the resilience function automatically.

V. Experimental Evaluation

In this section, extensive experimental simulations are conducted to validate the proposed SDN platform enabling resilience features for smart grid applications. To conduct our experiments, we use a Dell Server R730 that has Intel Xeon E5-2600 CPU and 32-GB RAM to operate Red Hat Linux 7. To create multiple entities in VMs, we use RDO Openstack Mitaka that runs on top of RHEL7. The SDN and switches are cerated in the form of VMs with four VMs that provide originating/terminating points for messages exchanged across the switches pool. The SDN VM has RHEL7 as the operating system and Open vSwitch to provide the functionality of SDN. Moreover, the SW VM has RHEL7 as the operating system and Open vSwitch to provide the functionality of software switch, as shown in Fig. 6. Data communications frailer are configured by sending error message flow during a normal session. To demonstrate the time accuracy of the proposed SDN platform for data monitoring to perform resiliency in smart grid networks, we present different use cases to handle a traffic flow in real-time monitoring. The first scenario created with consideration of conventional topology network to provide communication connectivity between SDN switches. The second scenario is the failure topology when fault event happens between SDN switches. Finally, upgraded topology was involved deployment of new SDN switches in the smart grid domain. In such smart grid network, we assume that SDN controller exchanges updating messages with associated SDN switches using openflow protocol. Our goal is to differentiate the conventional data flow, failure event, and network upgrade flow by calculating the traffic flow efficiency of SDN base switches. The time of message exchanges in the same SDN switches and time required to reroute end-to-end path connectivity is assessed to be 6 ms, as shown in Fig. 7. The latency performances of the network conventional are slightly high

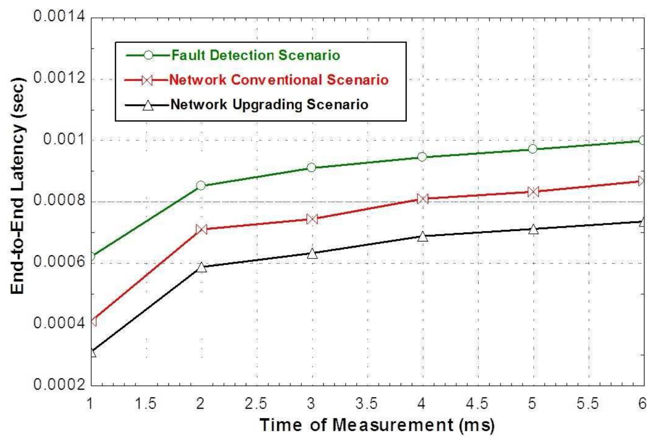

Fig. 7. End-to-end latency for different networks topology.

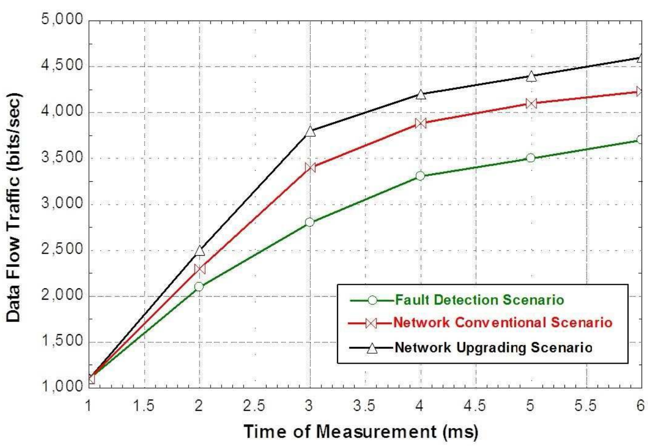

Fig. 8. Traffic flow for different networks topology.

due to the congested traffic load at the control center. For example, in case of failure event, the latency of data delivered to the control center under real-time monitoring system is higher than upgrade scenario due to the traffic overflowing effect.

The assignment of any SDN switch to a specific flow path is determined by SDN controller. Such decision is made based on data obtained from monitoring algorithm running at SDN controller. The proposed SDN controller can identify failures using interruption messages obtained from originating point, as we assume the starting point may need to receive acknowledgment messages for data forwarding. It is obvious the latency increases during the period of distribution or communication failure between SW1 and SW4. This is expected since time required for SDN controller to detect failure and recover the system is consumed to update the flow table of SW1. The latency time of data transmission is less in the upgraded system approach, which mean the transmission time contributes to overall system can perform well in the proposed scheme.

Fig. 8 shows the data traffic flow times at receiver side. In the scenario, SDN switches are set to frequently transfer their active status to SDN controller with data gathering traffic rate at 1500 kb/s. During the event of fault supervisions, SDN controller will identify any abnormal status after receiving report from the switches. In order to make sure the time of monitoring in the control center is accurate the SDN controller required to deliver real-time data measurements to the control center at the rate of 4800 messages per second [6]. Each message contains an instantaneous sample of power signals (e.g., voltage and current) readings. It is obvious, how system performance declines significantly when failure occurs. For conventional flow in infrastructure layer the monitoring features set-up at 6 ms time measurement.

VI. Conclusion

In this paper, we presented an efficient use of emerging SDN platform powered by IIoT platform for smart grid paradigm, which is currently considered as one of modernization challenges to utility providers. To overlay the path toward SDN employed IIoT integrated smart grid, there are still challenges ahead such as the use of OpenFlow protocol to integrate all the layers and development of efficient control algorithms with low complexity. In this regard, new SDN platform along with developed algorithm are proposed to adopt dynamic change in real-time smart grid system, and reliable and flexible operations to enable control layer in providing real-time monitoring. To verify the feasibility of the developed system different use cases are presented (e.g., expansion and fault scenarios) in smart grid paradigm to evaluate the data traffic flow and forwarding behavior. According to the demonstrative scenarios, this paper shows the potential of SDN controller for supporting resilience of smart grids, even under fault circumstances. The performance results indicated that the dynamic end-to-end reroute could be realized within tens of milliseconds and confirmed the effectiveness of the control scheme. However, smart grid fault detection required big data of information exchanges to reduce the latency performance of message transfer, particularly in upgraded smart grid networks. In this way, further analyses need to be considered using industrial protocol to allocate resources for various amount of data with different delay requirements.

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for smart cities,” *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.
[2] S. Mumtaz *et al.*, “Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation,” *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 28–33, Mar. 2017.
[3] S. Al-Rubaye, A. Al-Dulaimi, and J. Cosmas, “Spectrum allocation techniques for industrial smart grid infrastructure,” in *Proc. IEEE 14th Int. Conf. Ind. Informat. (INDIN)*, Poitiers, France, Jul. 2016, pp. 1036–1039.
[4] N. Dorsch, F. Kurtz, F. Girke, and C. Wietfeld, “Enhanced fast failover for software-defined smart grid communication networks,” in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–6.
[5] *IEC TC57: Communication Networks and Systems for Power Utility Automation*, IEC Standard 61850, 2014.

[6] X. Lu, W. Wang, and J. Ma, "An empirical study of communication infrastructures towards the smart grid: Design, implementation, and evaluation," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 170–183, Mar. 2013.

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

[8] A. Cahn, J. Hoyos, M. Hulse, and E. Keller, "Software-defined energy communication networks: From substation automation to future smart grids," in *Proc. IEEE SmartGridComm*, Vancouver, BC, Canada, Oct. 2013, pp. 558–563.

[9] J. Wen, C. Hammond, and E. A. Udren, "Wide-area Ethernet network configuration for system protection messaging," in *Proc. 65th Annu. Conf. Protect. Relay Eng.*, College Station, TX, USA, Apr. 2012, pp. 52–72.

[10] A. Al-Dulaimi, S. Al-Rubaye, J. Cosmas, and A. Anpalagan, "Planning of ultra-dense wireless networks," *IEEE Netw.*, vol. 31, no. 2, pp. 90–96, Mar./Apr. 2017.

[11] Z. Meng, Z. Wu, C. Muvianto, and J. Gray, "A data-oriented M2M messaging mechanism for industrial IoT applications," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 236–246, Feb. 2017.

[12] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[13] S. Savazzi, V. Rampa, and U. Spagnolini, "Wireless cloud networks for the factory of things: Connectivity modeling and layout design," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 180–195, Apr. 2014.

[14] D. Kreutz *et al.*, "Software-defined networking: A comprehensive survey," *Proc. IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[15] W. Zhong, R. Yu, S. Xie, Y. Zhang, and D. H. K. Tsang, "Software defined networking for flexible and green energy Internet," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 68–75, Dec. 2016.

[16] A. Al-Dulaimi, S. Al-Rubaye, and Q. Ni, "Energy efficiency using cloud management of LTE networks employing fronthaul and virtualized baseband processing pool," *IEEE Trans. Cloud Comput.*, to be published.

[17] S. E. Collier, "The emerging Enernet: Convergence of the smart grid with the Internet of Things," *IEEE Ind. Appl. Mag.*, vol. 23, no. 2, pp. 12–16, Mar./Apr. 2017.

[18] A. M. Akhtar, X. Wang, and L. Hanzo, "Synergistic spectrum sharing in 5G HetNets: A harmonized SDN-enabled approach," *IEEE Commun. Mag.*, vol. 54, no. 1, pp. 40–47, Jan. 2016.

[19] F. Granelli *et al.*, "Software defined and virtualized wireless access in future wireless networks: Scenarios and standards," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 26–34, Jun. 2015.

[20] H.-H. Cho, C.-F. Lai, T. K. Shih, and H.-C. Chao, "Integration of SDR and SDN for 5G," *IEEE Access*, vol. 2, pp. 1196–1204, 2014.

[21] F. G. Brundu *et al.*, "IoT software infrastructure for energy management and simulation in smart cities," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 832–840, Apr. 2017.

[22] B. Ahlgren, M. Hidell, and E. C.-H. Ngai, "Internet of Things for smart cities: Interoperability and open data," *IEEE Internet Comput.*, vol. 20, no. 6, pp. 52–56, Nov./Dec. 2016.

[23] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: A survey," *IEEE Commun. Mag.*, vol. 51, no. 11, pp. 24–31, Nov. 2013.

[24] M. Mahmoud, N. Saputro, P. Akula, and K. Akkaya, "Privacy-preserving power injection over a hybrid AMI/LTE smart grid network," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 870–880, Aug. 2017.

[25] A. Goodney, S. Kumar, A. Ravi, and Y. H. Cho, "Efficient PMU Networking with Software Defined Networks," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Vancouver, BC, Canada, Oct. 2013, pp. 378–383.

[26] G. Xu, W. Yu, D. Griffith, N. Golmie, and P. Moulema, "Toward integrating distributed energy resources and storage devices in smart grid," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 192–204, Feb. 2017.

[27] J. Lin, K.-C. Leung, and V. O. K. Li, "Optimal scheduling with vehicle-to-grid regulation service," *IEEE Internet Things J.*, vol. 1, no. 6, pp. 556–569, Dec. 2014.

[28] J. Kempf *et al.*, "Scalable fault management for OpenFlow," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 6606–6610.

[29] A. Sgambelluri, A. Giorgetti, F. Cugini, F. Paolucci, and P. Castoldi, "OpenFlow-based segment protection in Ethernet networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 5, no. 9, pp. 1066–1075, Sep. 2013.

[30] T. Xu *et al.*, "Defending against new-flow attack in SDN-based Internet of Things," *IEEE Access*, vol. 5, pp. 3431–3443, 2017.

[31] S. Al-Rubaye *et al.*, "Development of heterogeneous cognitive radio and wireless access network," in *Proc. 24th Wireless World Res. Forum (WWRF)*, Apr. 2010, pp. 1–5.

[32] N. Foster *et al.*, "Languages for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 128–134, Feb. 2013.

[33] S. Al-Rubaye and B. J. Choi, "Energy load management for residential consumers in smart grid networks," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Las Vegas, NV, USA, Jan. 2016, pp. 579–582.

[34] X. Zhang, K. Wei, L. Guo, W. Hou, and J. Wu, "SDN," in *Proc. Int. Conf. Softw. Netw. (ICSN)*, May 2016, pp. 1–5.

[35] P. R. Srivastava and S. Saurav, "Networking agent for overlay L2 routing and overlay to underlay external networks L3 routing using OpenFlow and Open vSwitch," in *Proc. 17th (APNOMS)*, Busan, South Korea, Aug. 2015, pp. 291–296.

Saba Al-Rubaye (M'10–SM'17) received the Ph.D. degree in electrical and electronic engineering from Brunel University London, London, U.K.

She was a Postdoctoral Fellow in smart grids with Stony Brook University. She was working with the advisory service of renewable energy and emerging technology with Quanta Technology, Toronto, ON, Canada. Her current research interests include smart grids, grid modernization, IIoT, microgrids, SDN platform, system integration, networking, and telecommunications. She has authored or co-authored many papers in IEEE publications and conferences in the area of energy and telecommunications system. She authored three book chapters focusing on green communications.

Dr. Al-Rubaye is a Registered Chartered Engineer (CEng) of the British Engineering Council. She was recognized as an Associate Fellow of the British Higher Education Academy in the U.K. She is a member of the IET, IEEE1932.1 Standard. She was a two-time recipient of the Best Technical Paper Award from the Wireless World Research Forum (WWRF)/*IEEE Vehicular Technology Magazine* in 2011 and 2015, respectively.

Ekhlas Kadhum received the Ph.D. degree in electrical and electronic engineering from the University of Science, Malaysia, in 2011.

She is currently a Senior Lecturer with the Control and Systems Engineering Department, University of Technology, Baghdad, Iraq. Her current research interests include communications and networking, covering LTE system communications and networking, software-defined networking platforms, and wireless sensors.

Qiang Ni (M'04–SM'08) received the B.Sc., M.Sc., and Ph.D. degrees from the Huazhong University of Science and Technology, Wuhan, China, all in engineering.

He is a Professor and the Head of the Communication Systems Group, School of Computing and Communications, Lancaster University, Lancaster, U.K. He has authored or co-authored over 180 papers. His current research interests include future generation communications and networking, covering green communications and networking, heterogeneous networks, small cell and ultradense networks, 5G, software-defined networking, cloud networks, energy harvesting, smart grids, wireless information and power transfer, Internet of Things, and vehicular networks.

Dr. Ni was an IEEE 802.11 Wireless Standard Working Group voting member, and a contributor to IEEE Wireless Standards.

Alagan Anpalagan (S'98–M'01–SM'04) received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical engineering from the University of Toronto, Toronto, ON, Canada.

He is a Professor with the Department of Electrical and Computer Engineering, Ryerson University, Toronto, where he directs a research group working on radio resource management and radio access and networking areas within the WINCORE Laboratory. He co-authored *Design and Deployment of Small Cell Networks* (Cambridge Univ. Press, 2014), *Routing in Opportunistic Networks* (Springer, 2013), and *Handbook on Green Information and Communication Systems* (Academic, 2012).

Dr. Anpalagan is a Registered Professional Engineer in the Province of Ontario, Canada. He is a Fellow of the Institution of Engineering and Technology. He served as an Editor for IEEE COMMUNICATIONS SURVEYS AND TUTORIALS from 2012 to 2014, IEEE COMMUNICATIONS LETTERS from 2010 to 2013, *Springer Wireless Personal Communications* from 2011 to 2013, and the *EURASIP Journal of Wireless Communications and Networking* from 2004 to 2009. He currently serves as the TPC Vice Chair for IEEE VTC Fall-2017 and served as the TPC Co-Chair for IEEE Globecom 2015: SAC Green Communication and Computing, IEEE WPMC 2012 Wireless Networks, IEEE PIMRC 2011 Cognitive Radio and Spectrum Management, and IEEE CCECE 2004/2008. He has served as the Vice Chair for IEEE SIG on Green and Sustainable Networking and Computing with Cognition and Cooperation since 2015, the IEEE Canada Central Area Chair from 2012 to 2014, the IEEE Toronto Section Chair from 2006 to 2007, the ComSoc Toronto Chapter Chair from 2004 to 2005, and the IEEE Canada Professional Activities Committee Chair from 2009 to 2011. He was a recipient of the Deans Teaching Award in 2011, the Faculty Scholastic, Research and Creativity Award in 2010, 2014, and 2017, the Faculty Service Award from Ryerson University in 2011 and 2013, the Exemplary Editor Award from the IEEE ComSoc in 2013, and the Editor-in-Chief Top10 Choice Award in the IEEE TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGY in 2012.