IEEE Network, Volume 33, Issue 5, 2019, pp. 219-225
DOI: 10.1109/MNET.2019.1800312

Enabling Digital Grid for Industrial Revolution: Self-Healing Cyber Resilient Platform

Saba Al-Rubaye, *Senior Member, IEEE*, Jonathan Rodriguez, *Senior Member, IEEE*, Anwer Al-Dulaimi, *Senior Member, IEEE*, Shahid Mumtaz, *Senior Member, IEEE*, and Joel J. P. C. Rodrigues, *Senior Member, IEEE*

***Abstract*—The key market objectives driving digital grid development are to provide sustainable, reliable and secure network systems that can support variety of applications against any potential cyber attacks. Therefore, there is an urgent demand to accelerate the development of intelligent Software-Defined Networking (SDN) platform that can address the tremendous challenges of data protection for digital resiliency. Modern grid technology tends to adopt distributed SDN controllers for further slicing power grid domain and protect the boundaries of electric data at network edges. To accommodate these issues, this article proposes an intelligent secure SDN controller for supporting digital grid resiliency, considering management coordination capability, to enable self-healing features and recovery of network traffic forwarding during service interruptions. A set of advanced features are employed in grid controllers to configure the network elements in response to possible disasters or link failures. In addition, various SDN topology scenarios are introduced for efficient coordination and configurations of network domains. Finally, to justify the potential advantages of intelligent secure SDN system, a case study is presented to evaluate the requirements of secure digital modern grid networks and pave the path towards the next phase of industry revolution.**

INTRODUCTION

THE tremendous growth in the amount of electric data traffic caused by energy generation need to be secured and controlled efficiently to maintain network stability. In this way, developing an intelligent and secure communications system with capabilities to exchange the data status immediately is a critical criteria to operate and mange the digital grid [1]. The utility industry require certain functionalities (e.g. adaptive routing, security management) to facilitate a universal monitoring and resiliency of Distributed Energy Resources (DERs). For the current power grid, operating systems need to handle these functions manually, especially when acknowledge an updated request. This can be performed by separately configuring conventional communication devices (e.g., router or switch). As the security and management requirements cannot be satisfied by the regular networks, the requirements for ubiquitous access has triggered a dramatic expansion of communication infrastructures. Concurrently, the ubiquitous data obtained from sensors or actuators (e.g. interaction, aggregating, and analysis) are collected and analyzed to restructure the communication networks as a key aspect of industrial revolution [2]. In order to enhance the digital grid resiliency [3], the aging communication infrastructure need to be upgraded with secure systems that allow instant data traffic monitoring through advanced connectivity interfaces. Employing SDN technology enables smooth interaction cross the digital grid network elements (e.g. switches) to improve data forwarding between various network segments. In digital grid, deploying SDN helps to transfer proprietary hardware networks into software based systems to maintain higher resiliency against failures and also to prevent unpredictable cyber attacks in early stage. In such intelligent systems, the SDN [4] controller has the ability to extract the electric data from infrastructure layer using new features to reschedule and reconfigure the available resources subject to proceed requests. The adoption of this kind of intelligent systems allows to efficiently manage urgent quires of various application services by separating data control signaling from voltage transactions between various grid DERs.

An intelligent SDN controller can act as bridge between digital grid infrastructure network and grid services (e.g. self-healing, emergency demand, and islanding). Particularly, employing an intelligent SDN can provide central automated management for the whole digital grid system without the need to access individual devices for manual configuration [5]. In addition, each DER managed by digital grid controller should meet the criteria for interconnection standard as specified by IEEE Standard 1547-2003. The interconnection standard can offer a set of direction for voltage, frequency control, protection, and synchronization functionality to maintain the digital grid performance during the integration phase with the main utility grid. The SDN technology can be a good candidate [6], [7] to enrich functionality, improve self-healing, and resiliency of the modern digital grid by leveraging these configurations at control level. The correspondence between multi-SDN controllers that manage multiple power grid domains has tremendous challenges because of the behavior of power system operation, especially in disasters, which can impact real time services. Therefore, it is necessary to devise an developed cooperative control system that can offer reliable and secure communications with low-latency transmission between various domains to support rapid actions during unpredictable situations (e.g., link failure). In addition, a developed digital grid control may provide coordination features in real-time manner within a wide area of power grid systems to protect the utility sector against any cyber physical attacks. Since multi-cooperative digital grid controllers can support many applications that improve power system response during disturbance events, the digital grid interconnected with SDN system can leverage a fast self-healing capability using programmable control though communication

techniques [8]. In this article, we extend our previous work in [3], to recovering critical services at reasonable performance during cyber attacks and accidental failures. An intelligent SDN controllers based coordination is presented to support digital grid applications, which is beyond the literature, such as [9] and [10]. The advantage of cooperative controllers are to enable fast self-healing in the digital grid resilient networks by leveraging SDN platform. The intelligent SDN controller can provide secure communications for data routes through determining the problem cause at the source host or destination host, considering the digital grid service requirements. Finally, the intelligent SDN control system emulated using virtual switches for seamless data recovery during any failure or disturbance events and provide system validation.

This article is organized as follows. In the next section, we present the main challenges for enabling digital grid followed by requirements. Then, we elaborate on highlights the intelligent SDN system, distributed/cooperative digital grid controller and network topology with respect to the secure data management. Finally, we demonstrate the analysis of testbed platform for digital grid network traffic control.

Challenges and Enabling of Digital Grid

Modernization provides the network with the necessary features to incorporate more services and support new functionalities compared with current networks. The transformation is driven by the continuous evolution in technology and cost of operating current networks. Nowadays, the trend of technology is to employ generic platforms and software provided by open source. The key technologies that support vendor-agnostic approach are: Network Function Virtualization (NFV) and software-defined networking. Considering NFV, virtualizing proprietary hardware into software elements that can be deployed over cloud allows to the network to be vendor-agnostic for any type of virtual application provided with the necessary interfaces to other components. The SDN enables electing best overlaid route for traffic forwarding between virtual and physical. The SDN controllers are deployed in a hierarchy to control various domains and data centers. However, the SDN is blended more into hardware to provide new generation of adaptive data centers namely software-defined data center. This new generation of programmatic network control improves control over resources and improve network Key Performance Indicators (KPIs) (e.g. delay, jitter, etc.). For utility providers, this expansion in network control and monitoring help to increase resiliency, self-healing, and maintain efficient provision of conventional technologies (e.g. SCADA).

Digital Grid Requirements

In the digital grid paradigm, controllers are anticipated to play a key role for handling any protect actions of the substation system, especially, where DERs communicate with local control through digital grid domains. The intelligent SDN approach will provide great tools to tackle the security management of digital grid applications in order to reduce the probability of cyber attacks, while guaranteeing high level of services. These tools will dynamically accelerate the data

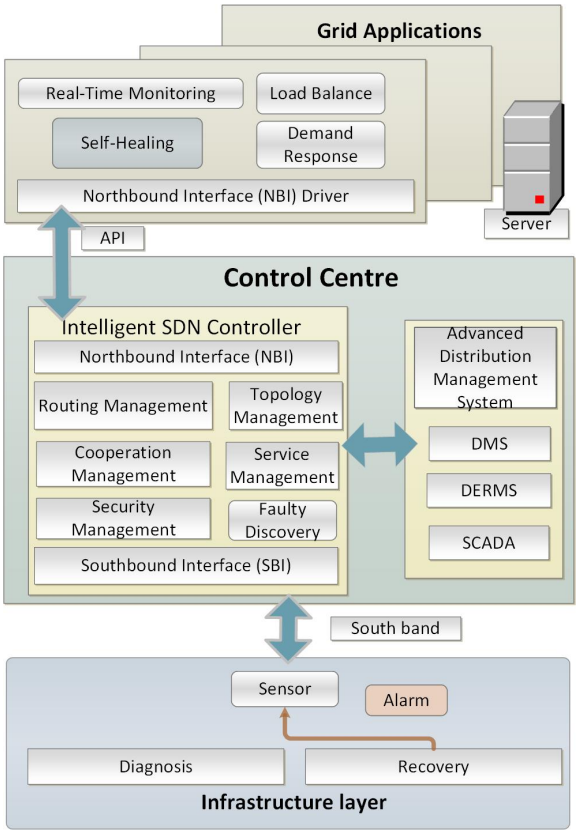

Fig. 1. Digital grid self-healing using intelligent SDN technology.

forwarding processes while enforcing certain security features on relevant SDN platform. In case of multi-controller, the requirements are more demanding for better robustness of the digital grid system and extend the abilities of real-time monitoring to have reconfiguration features of virtualized digital grid entities. Using intelligent programmable technology can enable control center to be more efficient in real-time interactions with Distribution Management Systems (DMSs) for management issues. Especially, when DMS need to adapt service requirement including bandwidth and latency to deliver an urgent services throughout the system with high-priority flows. Today, most of standardization activities sponsored by power industry are focusing on cyber physical attacks. Particularly, utility providers are focusing on using open-flow protocols in the communication infrastructure to facilitate the information exchange with the field elements [11]. The main key requirements for SDN controller from utility perspectives can be summarized as follow:

1) *Scalability*: Utility control system needs to be more adaptive to accommodate a variety of applications in digital grid segments to reflect on changes in network load.
2) *Management*: The management unit needs to be able to interact easily with other entities to facilitate an immediate reaction for any physical risk or cyber attack.
3) *Monitoring*: The consideration of real-time monitoring should meet the utility requirements for the system security and data traffic networks upon intelligent system control. Therefore, the control center needs to be more

fixable to deal periodically with the cyber attack and traffic flow condition.

4) *Robustness*: Throughout the service process the utility system should be more robust to avoid any type of failure or disaster.
5) *Service provision*: The control center must be intelligent enough to deal with the data flow dynamically by regular adjustment of service.
6) *Connectivity*: Communications need to be more secure and in high quality to meet the digital grid application requirements (e.g. self-healing).
7) *Service provision and Support*: Services must be provisioned carefully to provide a high quality of services (QoS) and service support over the digital grid network infrastructure.

In summery, a modernized digital grid requires developing an efficient control system that can accommodate sudden changes in data due to failure or attack, besides other changes in functionality cross the power grid.

DIGITAL GRID SELF-HEALING

Digital grid networks need to deploy critical communication infrastructures that support reliable connections between different entities/segments. In this regard, end-to-end path connectivity should to be guaranteed under any disaster or fault conditions to avoid link outages that may escalate into power imbalance between digital grid domains. Therefore, different use cases scenarios for self-healing and real-time monitoring can be considered, one of them assumes the system under fault scenario with automated path restoration. A control center employing SDN can provide enforces a predefined self-healing policy at the distributed local controller. Then, interoperability procedures are triggered to adjust the data paths to bypass interrupted links. This may cause more frequent fluctuations in digital grid configurations that require authentication to assure that a new selected path comply with the data forwarding strategies.

An intelligent SDN has new technical features that support self-healing schemes in microgrids through optimized network application layer that interconnects various network segments. When overload or faults occurs, the SDN controller reconfigure network switches to isolate the impacted segment using the cooperated relays. Then, SDN controller quickly will react to establish new paths for the affected uncooperative relays to maintain the power system observability. More specifically, the outage line will be determined and reconfigured in the SDN switches. The regular route can accommodate a data transmitting path table, which has the information of destination network. Therefore, the switches calculates the available path without having an overview of the network status. Historical measurements representing previous network dynamics collected by the SDN switches allow us to take a data-driven approach for predicting the traffic volume and processing time on each switch. Therefore, the key development aspects for a control system should be motivated by data ontology that reflects on utility sector.

INTELLIGENT SDN CONTROLLER

The employment of SDN technology within digital grid system is meant to support the strict requirement to deliver an amount of power that can meet the load demand during disturbance times. The intelligent SDN controller can interact directly with the supervisory control and data acquisition (SCADA), distributed energy resource management system (DERMS), and DMS. As a result, the digital grid entity including DERs, smart meters, and control system can be handled as individual elements using openflow protocol to enable interoperability throughout the utility grid [12]. To get enormous advantages from this intelligent system, we expand our previous work on SDN platform [3] to mitigate network failure with respect to the utility grid requirements including self-healing and fast reconfiguration. By employing an intelligent SDN controller, the vision of global visibility will be activated for empowering several services such as demand response, real-time monitoring, and self-healing functionality, as shown in Fig. 1. This new modeling of fast-healing will becomes an important scheme of future digital grid controller.

The detection unit will provide the necessary data about system health indicators through continuous monitoring. Once a cyber attack is detected, the alarm system will send notification messages through the communication network. The critical information will be sent to the SDN controller including a list of connected devices and service status. On another side, cyber physical system alarms are triggered when a disaster or any physical failures occurs in the equipment. The intelligent SDN controller has several functionality that can help to avoid any failures without requiring additional generated power. In addition, SDN making the routing path more flexible for the data traffic by considering management function, which helps the signal commands accessing relevant local switches. Similarly, the service management function helps coordinating the traffic at the micogrid domain level and interact directly with the utility units (e.g. DERMS). As a result, the digital grid control system can provide critical information to define grid operation, servicing and routing requirements. It help to deliver appropriate information to the application layer using the northbound application program interfaces (APIs). Some time the network traffic need to be diverted, if the application layer requested some changes according to the critical factors such as collected data, communication link availability and processing scheme. In this way, the digital grid control center facilitates inter-connectivity between various elements throughout network infrastructure. From SDN perspective, the interaction with other layers is defined by APIs that can be either northbound or southbound. For application layer, APIs can define various innovative services and applications (e.g., equipment fault monitoring, utilization, and processing status). Therefore, application layer collects selected data from local controllers and make such data available to the control center. Once the intelligent system recognized an emergency condition, the controller will send signal commands to local circuit breakers and switches to trigger islanding mode. Meanwhile, the load balancer immediately acts to recover the load demand needed. Power flows will reallocate the load to achieve a new

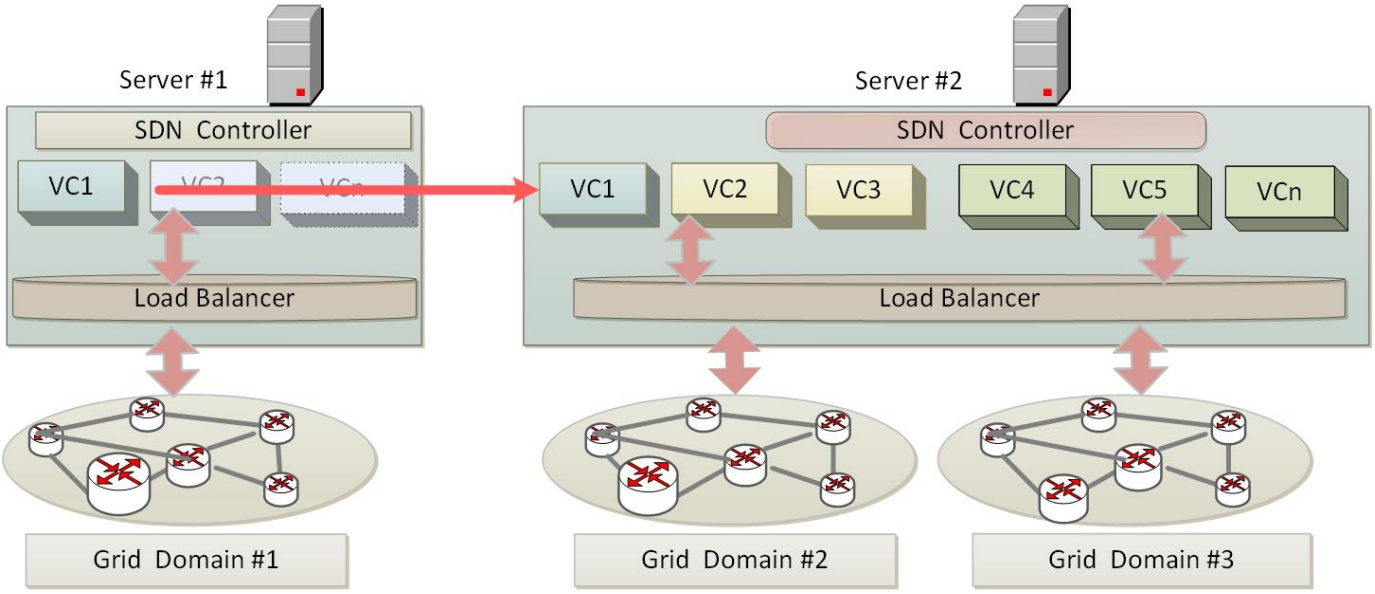

Fig. 2. Load balance and resource distribution between various grid domains.

balance, according to the level of load and available capacity of generation sources.

The API interfaces are used to deliver commands on data aggregation policy including statistics analysis and fault status from the infrastructure level. These APIs can also used to adjust the operational profiles of the digital grid system. The information about available resources are collected regularly by resource discovery entity and such information are used to explore if the available energy resources are in use or not. If the available resource are not assigned at the end of any detection interval, the local control will update resource function in the main control center to expose such resources as available. If a digital grid domain has enough energy resources available to meet an incoming request demanding electricity, the resource assignment function in the local SDN controller will assign resources locally to that request and acknowledge such action via APIs. To this end, digital grid resiliency can be obtained through: A communication infrastructure that is reliable enough with low-latency data transmission, and a dynamic network adaptation in response to changes in surrounding conditions (e.g., link failure, disaster events. etc.). Moreover, a resilient digital grid needs to meet diverse QoS requirements for different types of services being transmitted over the communication infrastructure. The QoS variance could change from small and periodic control data with milliseconds of delay to large energy management data that can tolerate minutes of latency.

Distributed Controller

The anticipated SDN platform has the ability to configure and manage the utility grid domain, while providing advanced connectivity services, resiliency, and reliability. Distributed local SDN controllers can enable ”Islanding” to separate certain digital grid domains aiming to reduce the problem of failure. However, islanded digital grid clusters can still be maintained individually using networking layers. The distributed local controllers determine the risk in advance using connected sensors and make necessary decisions prior to informing other digital grid controllers. As stated earlier, any disconnection in the communication infrastructure of the power grid (e.g. failure or natural disturbance) can led to interruptions in energy delivered to consumers. The SDN controller can direct the switches equipment in the data level by sending new route information and instructions, whenever a failure occurs. The local controller start analyzing possible actions, if discover any link failure, by mitigating this matter either by reschedule flows and deactivate the affected route. A distributed control system method aims to deliver a maximum support to the DER within its digital grid domain. The local SDN control system is smart enough to coordinate actions between different controllers to restore operations and maintain the digital grid performance. Local controllers collect the information from various sensors/actuators to monitor KPIs (including current/voltage values and energy level) to perform various determinations (e.g. decision making of local controls). However, some of these information can be invoked by the control center for decision making at digital grid application layer. The local control system has the ability to make independent decisions for managing its corresponding actuators. A distributed SDN control will use different interfaces to customize local consumption at different domains to use their local energy resources.

Multi-Controller Cooperative Strategy

Modern grid architecture is most likely to adopt a distributed topology that employs multiple neighbored zones or domains of power grid. This segregation into small grids requires to increase system reliability through enormous local sharing of information on power generation and demand. Therefore, it is necessary to monitor various digital grid components including

power generators, energy storage, consumer appliances, etc. The obtained KPIs refers to power status at different digital grid sites to enable efficient control of multi-stages of power production process. Considering a large distributed grid, each digital grid will employ a local SDN controller that balance load generation with consumption to maintain operational system with minimum need for additional resources from other grid domains. The digital grid controller will employ certain functionalities and enforce selected policies considering the digital grid resources and connectivity framework within the grid zone. During disturbances, the controller functionality allows to island the digital grid from the main grid to prevent scaling system interruptions and protect facilities from being damaged by power fluctuations. A local controller is also the facilitator of various interactions with the main grid to provide two-way access for energy resources during overloading conditions and emergencies.

The local controllers cooperate to prevent any sequential collapse of service by isolating any digital grid that appears to be losing control of power balance or eventually becomes unstable. This requires all controllers to provide grid controlling system a fair access to local digital grid energy indicators and state transitions. Considering grid hierarchy, local controllers are the lower layer of the control plane, while SDN controllers forms the higher layer of that domain. Since all the controllers are provided in the form of virtual machines that run on Commercial-Off-The-Shelf (COTS) hardware, they can all be connected and administrated on cloud [13]. Therefore, controllers can be accessed through management commands to edit virtual switches rules and define the flows directions between various sites. This system allow to share and control information flows that used to make decisions on energy allocations throughout the grid sites. To improve system control, an intelligent system control is employed to obtain instant resource availability of digital grid components using southbound interfaces. This improves information accuracy and provide timely status of the system that leads to efficient control and utilization of various resources. The grid main controller is the entity that coordinate local controllers operations and synchronize services between various sites. It is also responsible to manage self-healing during service interruptions considering accessibility rights to all microgrids information and enhanced decision-making features [14]. A well maintained communication system is the key component to provide all connectivity for all cloud controllers and to provide the underlying infrastructure for sharing information.

Load Balancing

Once, the control system obtains information about routing path, the SDN controller can determine all the available alternative routes between the source host node and the destination host node. By exploiting this ability of global routing sight at intelligent SDN controller, the load demand can be calculated easily at each path in the network topology. To emphasize the load balance at the intelligent SDN controller, the presented scenario (seen Fig. 2) implemented an advance load balancer server for enabling the load balance between potential destinations. To calculate the best self-healing path in real-time environment, the load balance function can act immediately to estimate the load condition of multiple cooperative routes, as soon as receiving a request from control center to establish new path [15]. Therefore, the digital grid controller periodically delivers information to the load balance server about the load status for each data path. Whenever, the SDN controller processing the load stability requirement, the load balance will start to collect the data path of network traffic and deliver it back to the control center. To this end, implementation of intelligent SDN controller can enable and strength the interior monitoring system regarding to the associated switches, combining with communicate policies for data forwarding.

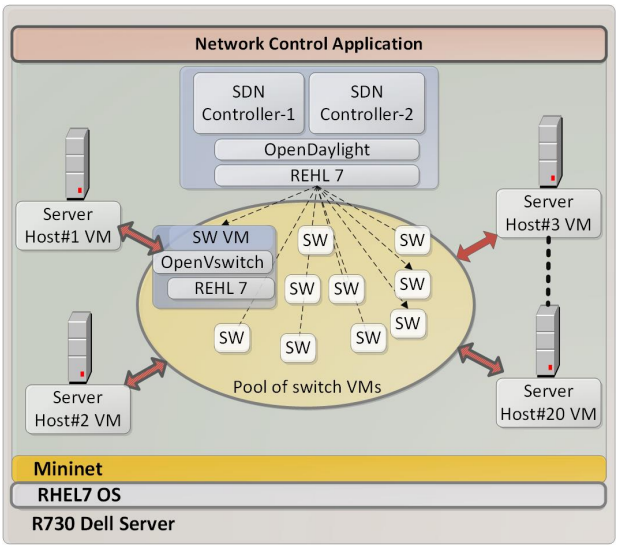

Fig. 3. Experimental platform.

Experimental Setup

In the modern digital grid design, the distributed local SDN controller can associate any extra available resources to another digital grid domains to meet the traffic demand. This process can be handled by SDN resource functionality that is responsible for prioritizing demands by reflecting the required coordination service policy. Later, an acknowledgment messages will be delivered from the host domain to the originating resource unit along with time stamps for immediate provision updates. Each message may approve the status of recognized services, whether it is in active mode or not. In this article, multiple intelligent SDN controllers are considered and deployed in a hierarchical order in the form of virtual machines (VMs) to be able to handle the data forwarding in correspondence with appropriate developments in digital grid domain. To be able to evaluate the prospective benefit of establishing multiple intelligent controller, OpenDayLight software is consider to generate the SDN platform. The OpenDaylight controller has the ability to support multi-digital grid domains. A group of virtual instances of controllers act as a single logical control that diverts the load between distributed entities by monitoring global status of the network. For this purpose, the Hydrogen release of OpenDaylight employed in different modules to related applications for network traffic control model.

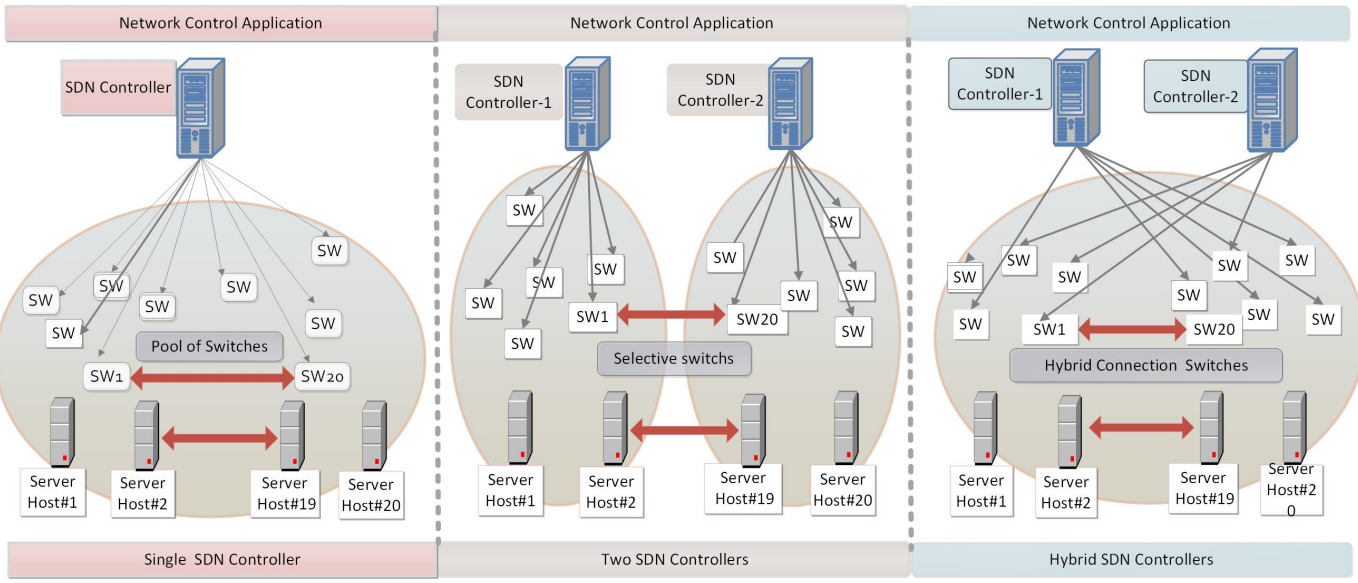

Fig. 4. Intelligent SDN control topologies.

Some additional layers of networks are generated and attached to the VMs to overly traffic routing between digital grid servers. From the northbound side the digital grid domain is connected via RESTful API and each request can send to local controllers in the same domain. From southbound, Openflow switches ae integrated with the virtual controllers in the digital grid domain via IP address. To conduct our experiments, we use a Dell Server R730 that has 18 physical cores and 128G RAM with multiple Ethernet ports. The software layers include Red Hat Linux 7 and Openstack (Mitaka Release). The SDN controller instances are created using OpenDaylight Hydrogen in the form of VMs. The traffic is exchanged across network using four servers that provide originating and terminating points across the switches pool. Each of those traffic servers has Red hat 7 and Openstack with multiple numbers of VM that has a descriptor to generate messages. Those VMs are also connected through OpenVswitch to virtual network system. Each elements of the overlay digital grid network topology (switch, server, and SDN controller) are mapped on a different VM to be run in one of the virtualization servers, as shown in Fig. 3.

Network Topology

Different topology scenarios and new features can be set in decentralized fashion of SDN system to address the desired data forwarding behaviour in particular applications, as shown in Fig. 4. A signal SDN is associated with 20 VMs where generated using OpenvSwitch. Each VM is intgarated with the host server to be able to simulate the data traffic generator. The data traffic is generated by in each switch, as long as there is no data flow in the entry port for the incoming data packet that the host may desire to deliver. After that, the VM will captures the electric data packet to deliver it to the SDN control system. Hence, signal controller will handle the data traffic and dealing with request message. The other scenario when we have two controllers are associated with switches. One of them

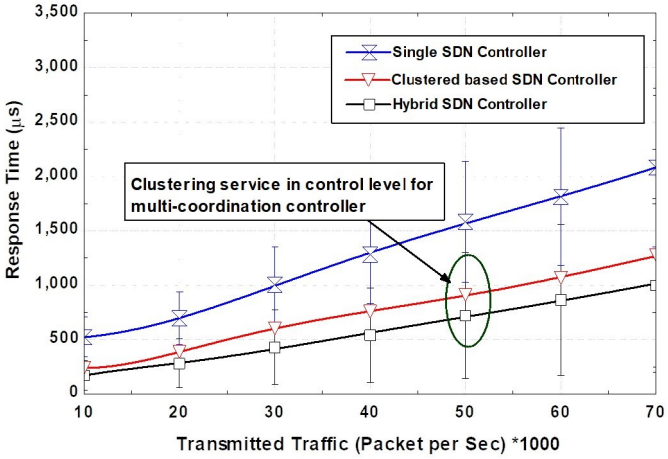

Fig. 5. Comparison of different digital grid network traffic topologies.

are associated with selective 10 VMs, while the rest of the VMs are associated to the another SDN. The hybrid mode has the capability of sharing the links cross the digital grid network by electric data traffic and SDN traffic. All communication links are assumed to be bi-directional with the ability of 1Gbps for each direction. SDN controllers and data sourcing points are randomly selected from the generated networking of 20 switches. For single and hybrid controls the data initiated randomly and the traffic demands from 512kbps to 3Mbps in uniform pattern with a step size of 128kbps. SDN control traffic load is controlled by the factor traffic density, which denotes the average number of desired data traffic collected from SDN controllers in each cycle. Comparing results of the multi-topology scenarios can deliver an indication that the amount of time required for the system to make an action is growth with increase the number of SDN controller in each digital grid domain. Nevertheless, still there is a significant variance for the time requirement between the single SDN

scenario and hybrid SDN controller scenario, which means that the resource availability in the hybrid controller has a huge impact for the obtained results, as illustrated in Fig. 5.

CONCLUSION

Intelligent SDN technology is still in its early stages considering market adoption. This article focused on the main requirements and functionalities of digital grid network to facilitate grid services that deploy control and operational concepts. The proposed intelligent SDN controller improves digital grid resiliency as a vital part of future modern power grid strategies. By employing intelligent SDN system, end-to-end path connectivity will be guaranteed during cyber, disaster, and fault conditions. This matter will motivate utility investments to obtain operational objectives, enhanced reliability, and modify energy production process. Finally, integrated SDN controller with digital grid can play a key role into the next phase of industry development.

FUTURE WORK

Employing SDN in industrial applications opens new opportunities to leverage current SDN technical features for efficient control of production lines. Firstly, it is important to integrate the virtual SDN at control centers with local production equipment (e.g. actuators, switches, robots, etc.). This means that all these equipment need to be attached to local and external networks and provided with the necessary API interfaces. This is a new form of transformation to computational based equipment rater than current model of task based equipment. This raise new challenges of defining the most efficient topology for each use case. In addition, the SDN features of automation need to be employed for self-healing using predefined business models for highly adapted grids that restructure connectivity based on pre-estimated and measured power consumption rates.

AUTHOR INFORMATION

Saba Al-Rubaye received her Ph.D. in Electrical and Electronic Engineering from Brunel University London, United Kingdom. Currently, she is a Senior Lecturer in the School of Aerospace, Transport and Manufacturing at Cranfield University, United Kingdom. She has more than 17 years of industrial and academic experience, she has led and managed several industrial projects in Canada and US in the area of Cyber-physical systems, automation systems, IIoT and communication networks. Dr. Al-Rubaye registered as a Chartered Engineer (CEng) and a Senior Member of IEEE.

Jonathan Rodriguez received his Masters degree in Electronic and Electrical Engineering and Ph.D from the University of Surrey (UK), in 1998 and 2004 respectively. In 2005, he became a researcher at the Instituto de Telecomunicacoes (Portugal), and in 2017, he became Professor of Mobile Communications at the University of South Wales (UK). He is author of more than 450 scientific works. Professional affiliations: Senior Member of the IEEE and Chartered Engineer (CEng) since 2013, and Fellow of the IET (2015).

Anwer Al-Dulaimi received the Ph.D. degree in electronic and computer engineering from Brunel University, London, UK in 2012. Currently, he is a Technical Product Owner in Center of Excellence at EXFO, Toronto, Canada. His research interests include 5G networks, cloud networks, V2X and Internet of Things. He is the chair of IEEE 1932.1 Working Group "Standard for Licensed/Unlicensed Spectrum Interoperability in Wireless Mobile Network" and IEEE Distinguished Lecturer.

Shahid Mumtaz has more than 10 years of wireless industry experience and is currently working as Senior Research Scientist Instituto de Telecomunicaes Portugal. He received his MSc and Ph.D. degrees in Electrical and Electronic Engineering from Blekinge Institute of Technology (BTH) Karlskrona, Sweden and University of Aveiro, Portugal in 2006 and 2011, respectively. Dr. Mumtaz has more than 150 publications in international conferences, journal papers, and book chapters. Dr. Mumtaz is a senior member of IEEE. He was nominated as Vice Chair for IEEE new standardization on P1932.1. He is ACM Distinguished speaker.

Joel J. P. C. Rodrigues is professor at the National Institute of Telecommunications (Inatel), Brazil and senior researcher at IT, Portugal. He is the leader of the Internet of Things Research Group (CNPq), Director for Conference Development - IEEE ComSoc Board of Governors, IEEE Distinguished Lecturer, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the Past-Chair of the IEEE ComSoc TCs on eHealth and on Communications Software. He is the editor-in-chief of an international journal and editorial board member of several journals. He has authored or coauthored over 650 papers in refereed international journals and conferences, 3 books, and 2 patents.

REFERENCES

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

[2] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, "Industrial Internet of Things Driven by SDN Platform for Smart Grid Resiliency," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–11, July 2017.

[3] S. Al-Rubaye and J. Aulin, "Grid Modernization Enabled by SDN Controllers: Leveraging Interoperability for Accessing Unlicensed Band," *IEEE Wireless Communications*, vol. PP, no. 3, pp. 1–7, Oct 2017.

[4] S. E. Collier, "The Emerging Enernet: Convergence of the Smart Grid with the Internet of Things," *IEEE Industry Applications Magazine*, vol. 23, no. 2, pp. 12–16, March 2017.

[5] K. Akkaya, A. S. Uluagac, and A. Aydeger, "Software Defined Networking for Wireless Local Networks in Smart Grid," in *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, Oct 2015, pp. 826–831.

[6] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh, and R., "Enabling Resilient Microgrid through Programmable Network," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[7] B. Galloway and G. P. Hancke, "Introduction to Industrial Control Networks," *IEEE Communications Surveys Tutorials*, vol. 15, no. 2, pp. 860–880, Second 2013.

[8] H. Ma, K. W. Chan, and M. Liu, "An Intelligent Control Scheme to Support Voltage of Smart Power Systems," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1405–1414, Aug 2013.

[9] X. Zhang, K. Wei, L. Guo, W. Hou, and J. Wu, "SDN-based Resilience Solutions for Smart Grids," in *2016 International Conference on Software Networking (ICSN)*, May 2016, pp. 1–5.

[10] 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 Transactions on Smart Grid*, vol. 8, no. 5, pp. 2494–2504, Sept 2017.

[11] A. Maitra, A. Pratt, T. Hubert, D. Wang, K. Prabakar, R. Handa, M. Baggu, and M. McGranaghan, "Microgrid Controllers: Expanding their Role and Evaluating their Performance," *IEEE Power and Energy Magazine*, vol. 15, no. 4, pp. 41–49, July 2017.

[12] G. S. Aujla, R. Chaudhary, S. Garg, N. Kumar, and J. J. Rodrigues, "SDN-enabled Multi-Attribute-based Secure Communication for Smart Grid in IIoT Environment," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2018.

[13] M. H. Yaghmaee, M. Moghaddassian, and A. Leon-Garcia, "Autonomous Two-Tier Cloud-Based Demand Side Management Approach with Microgrid," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1109–1120, June 2017.

[14] F. Shahnia, S. Bourbour, and A. Ghosh, "Coupling Neighboring Microgrids for Overload Management Based on Dynamic Multicriteria Decision-Making," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 969–983, March 2017.

[15] S. Park, J. Lee, G. Hwang, and J. K. Choi, "Event-Driven Energy Trading System in Microgrids: Aperiodic Market Model Analysis with a Game Theoretic Approach," *IEEE Access*, vol. 5, pp. 26 291–26 302, 2017.

Enabling digital grid for industrial revolution: self-healing cyber resilient platform

Al-Rubaye, Saba

2019-05-15

Al-Rubaye S, Rodriguez J, Al-Dulaimi A, et al., (2019) Enabling digital grid for industrial revolution: self-healing cyber resilient platform. IEEE Network, Volume 33, Issue 5, September 2019, pp. 219-225

https://doi.org/10.1109/MNET.2019.1800312