Software Defined Communication Network Reliability for Secondary Distribution Power Grid

Yona Andegelile*, Hellen Maziku*, Nerey Mvungi*, Mussa Kissaka**

*Department of Computer Science and Engineering, College of Information and Communication Systems, researcher at the department, P.O.Box 33335, Dar es Salaam, Tanzania

**Department of Telecommunications Engineering, College of Information and Communication Systems, researcher at the department, P.O.Box 33335, Dar es Salaam, Tanzania

(yona.andegelile@gmail.com, nahelna@gmail.com, nhmvungi@gmail.com, mkissaka@yahoo.com)

‡Corresponding Author; Yona Andegelile, Tel.: +255754-710-453; E-mail address: yona.andgelile@gmail.com

Received: 13.09.2020 Accepted:30.09.2020

Abstract- Operations automation of Secondary Distribution Electrical Power Grid (SDEPG) requires reliable communication network to facilitate end to end power grid visibility and control through various sensors and actuators deployed across the power grid network. Available solutions to enhance communication network reliability have addressed mostly requirements for transmission and primary distribution portions of the grid, which use wired communication network technologies. The nature of SDEPG demands reliability solutions to incorporate a combination of wired and wireless technologies.

In this research we propose a Software Defined Networking (SDN) based, cross layers resilient communication network for SDEPG. The solution segments the SDEPG into three parts, namely access, aggregation and core networks. Since aggregation and core comprise of wired network, we adopt the resilience approach proposed by previous researchers. As for access network that is largely comprised of wireless network, we propose a software defined algorithm that modifies the Radio Frequency (RF) parameters of failover Access Points (AP) to optimally cover abandoned clients when the serving AP fails.

Using a virtualized HP server, we deploy OPNET that contains NS3 and mininet to simulate the network topology and SDN controller algorithm respectively. We initiate traffic flow in a simulated network topology containing two access points and two stations. Simulating different failure scenarios reveals that in case of Access Point (AP) failure, the SDN controller seamlessly redirects users to a nearby AP while maintaining acceptable bandwidth, latency and availability.

Keywords Software defined networking, Resilience, Secondary Distribution Electrical Power Grid.

1. Introduction

Secondary Distribution Electrical Power Grid (SDEPG) is part of power system that connects consumers to the electrical power network [1]. SDEPG includes generation, transmission, primary and secondary distribution networks. SDEPG is ubiquitous, connected users are randomly distributed across towns and villages making it difficult to build a well-structured easily manageable network that is efficient and with optimal operational cost. Hence, to optimize operation cost and efficiency of management of power grid, automation such as fault detection and correction is required [2]. A highly reliable communication network is fundamental for automation of the electric power grid to send sensors information to actuators and receive commands from central control offices. Therefore, the SDEPG communication network must be reliably available and meet required bandwidth and latency [3], otherwise the power grid will be unmanageable and uncontrollable.

Software-Defined Networking (SDN), a new way of increasing communication resilience [4] is widely adopted [5, 6] since it provides superior network resilience (Rehmani, et al., 2019). However, SDEPG reliability requirements have not been addressed extensively. The existing solutions are based on wired technologies that is more suitable for transmission and primary distribution. The nature of SDEPG requires combination of both wireless and wired communication network technologies (ITU-Radio Communication, 2018) where failure cannot be tolerated.

Communication network failures can be caused by security attacks, natural disasters, system or telecommunication equipment malfunction, etc, but current studies concentrate on specific resilience challenges like security in [9]. Therefore, there is a need to come up with a solution that cuts across all power grid layers and meets SDEPG requirements.

In this paper, SDN based resilience communication network solution for SDEPG is proposed. The solution takes into consideration all communication network technologies and cuts across all layers to achieve reliable SDEPG automation. In order to achieve cross layer resilience, the proposed solution segregates the network to three layers namely core, aggregation and access. Redundancy capacity is used to address AP failure such that the Floodlight SDN controller detects and adjusts RF parameters of nearby APs to cover defective stations.

Using a virtualized HP server, we deploy OPNET that contains NS3 and mininet to simulate the network topology and SDN controller algorithm respectively. The proposed solution is simulated under different failure scenarios and the results are analysed to check if they meet SDEPG reliability requirements. The results show that the proposed solution achieves high communication network availability for SDEPG automation.

The study confirms that SDEPG requires combination of both wired and wireless technologies, and that a reliability solution should cater for this requirement. Moreover, this study explores characteristics of SDN and wireless network radio frequency parameters that could be linked together to obtain improved wireless communication network reliability.

2. Relevant Resilience Enhancement Approaches

2.1. SDN Based Resilience Solution Approaches

SDN is instrumental in all aspects of network reliability including availability, security and quality of service (QoS). Some studies focus in achieving reliability for specific type of failures, e.g. failures due to security attacks [10] and [9]. However, the power grid network is challenged by many types of failures. Some of the studies focus on a particular physical layer technology, e.g. [7] develop a reliability solution using IEC 61850 for wired technologies by monitoring physical interfaces on the switch. Similarly, [5] propose an SDN based reliability solution specifically for optical networks. Hence, there is a need to come up with a reliability solution that considers all failure scenarios and caters for SDEPG communication requirements.

2.2. Wired Vs Wireless Reliability Solutions

Automation of operations and management of SDEPG needs wired and wireless networks because of its ubiquitous nature, making it difficult to be served by a single technology. Therefore, SDEPG deploys millions of sensors across a power grid network which have to be connected hence needing backhauling of large traffic over long distance. While wired technologies are challenged by issues such as physical impact of the media and facilitating devises, wireless technologies face coverage, mobility and interference challenges.

Some researchers use handovers to improve network service resilience in wireless networks [11, 12]. However, the handover approach is challenged by AP overload or weak signals reception. For instance, [13] reveal that SDN handover schemes are challenged by interference. [14] address reliability concerns due to equipment failure cases in wired technologies. [15] proposed wireless network as a failover solution for wired technology, but not in architecture where all are work simultaneously. None of these solutions is comprehensive for multiple layers and technologies.

2.3. Reliability Strategies

The reliability framework by [16], defines ideologies based on resilience strategy, defined as D2R2 + DR: representing; Defend, Detect, Remediate, Recover, Diagnose, Refine. The strategy involves a real time control loop to dynamically enable networks to respond to challenges and a non-real time one to improve the network design [17].

One or a combination of these strategies have been used to realize reliability like authors [18] and [19] who only use defend strategy. The resilience strategy/approach cannot be very efficient because it is not practical to avoid all types of failures, hence useful for some types of failure scenarios. The reactive strategy by [20] and [21] detects failure and remediates it. However, efficiency of detection method in terms of time and accuracy is core to this approach. Most researchers focus on addressing current service interruption and not on recovering the network to the original state. This includes recovering, diagnosing and refining. The risk of this, when the chosen alternative is also interrupted, the network may fail to recover because of deployed redundancy paths limitations.

3. SDEPG Communication Network Reliability Requirements

SDEPG communication network reliability is the ability to facilitate SDEPG operations measured by its availability and QoS (e.g. bandwidth and latency), hence the capability of the communication network to meet its service functional and performance requirements [16, 22]. A reliable network will have good degree of resilience, providing and maintaining acceptable level of service even in challenging operational environment. There are several applications that need to work together to realize end to end automation of SDEPG. The applications cover all fundamental components of power grid operations including fault management [23], performance management and configuration management [24]. Each application has different reliability requirements that must be met to deliver intended functions. ITU standard [8] defines coverage, reliability, latency and security requirements for four application categories in SDEPG automation as summarized in Table 1. Similarly, Table 2 reflects SDEPG application based quantified minimum requirements for data size, latency and availability.

Table 1. Performance Requirements for SDEPG Application Categories

Smart network sub-system	**Coverage**	**Reliability**	**Latency Time**	**Security**
Meter reading - AMI	Medium	Medium	High	High
Field area network	High	High	Medium	High
Phase measurement	Medium	High	Low	Medium
Tele-protection	Medium	High	Low	Medium

Table 2. SDEPG Communication Network Reliability Requirements

Application	**System Requirement /Impact**		
	Typical data size	**Latency**	**Availability %**
Distribution automation – distribution system monitoring and maintenance data from field devices to DMS)	9.6-100 kbps	<5 s	>99.5
Distribution automation – Volt/VAR control (command from DMS to field devices)	9.6-100 kbps	<5 s	>99.5
Distribution automation – distribution system demand response (DSDR) (command from DMS to field devices)	9.6-100 kbps	<4 s	>99.5
Distribution automation – fault detection, clearing, isolation and restoration	9.6-100 kbps	<5 s	>99.5
(FCIR) (command from DMS to field devices)			
Outage and Restoration Management (ORM) (from meters to OMS)	9.6-100 kbps	<20 s	>98
Distribution customer storage (charge/discharge command from DAC to the storage)	9.6-100 kbps	<5 s	>99.5
Electric transportation (utility sends price info to PHEV)	9.6-100 kbps	<15 s	>98
Electric transportation (utility interrogates PHEV charge status)	9.6-100 kbps	<15 s	>98
Firmware updates (from utility to devices)	9.6-100 kbps	<2 min–7	>98

		days	
Program/configuration update (from utility to devices)	9.6-100 kbps	<5 min–3 days	>98
Customer information and messaging customers request account info from utility/utility responds to customers)	9.6-100 kbps	<15 s	>99

As seen in Table 2, any solution design intended to serve all SDEPG application categories must consider an availability of greater than 99.5%, a bandwidth of not less than 100Mbps and a latency of 4s.

4. Proposed SDN Based Reliability Solution Design

4.1. High-level architecture Design

As depicted in Fig. 1, an optimal resilience solution for a communication network segments it into three layers; Core, aggregation and access layer. The Core network backhauls traffic from aggregation layer to the central control office using optical network and IP networks. Core network is protected by rings of optical fiber around the aggregation points. Point to MultiPoint (P2MP) microwave links and optical fiber for some areas is used to aggregate traffic from clusters of wireless network base stations. Aggregation network is protected by 1+1 space diversity and protection rings of microwave link paths to reach various clusters of wireless networks. The survivability solution by [5] of core and aggregation portions of the network is promising and can be adopted. The access network is made of wireless network base stations and layer 2 switches. The SDN functions serving core and aggregation are extended to access network. SDN controller connects WLAN controller and Access Points (AP) through Representational State Transfer (REST), Application Programming Interface (API) with JavaScript Object Notation (JSON) format. The SDN controller connects with SDN capable switches which interconnect APs in clusters through OpenFlow protocol North Bound Interface (NBI). Fig. 1 depicts the access network architecture, detailing interfaces and protocols used between SDN controller and other network elements.

4.2. Proposed Access Network Availability Algorithm

Each AP is designed to have its own coverage footprint, and all corresponding Radio Frequency (RF) parameters are set to ensure no interference with other APs coverage areas. Since the APs are remote Media Access Control (MAC), all access points RF parameters are managed by a controller. The controller is responsible to managing health status of the APs. Uplink and Downlink traffic served by an AP pass through the controller which then forwards the traffic through switch and then router.

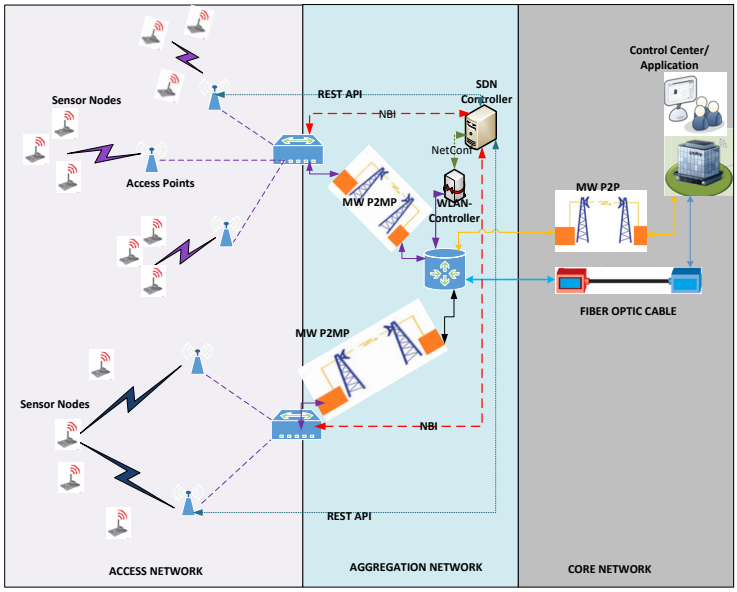

Fig. 1. SDN-based Communication Network Architecture Design for Reliability

With reference to Fig. 2, if the serving access point (AP1) fails, the WLAN controller detects abnormality on the health status of the AP through the CAPWAP protocol. The WLAN controller notifies the SDN controller of the status. The SDN controller tries a quick recovery, depending on the nature of the abnormality, if this doesn't work, the SDN controller adjusts the transmit power of the nearby APs (AP2) to ensure the abandoned coverage area is well covered. Then the STA connects to the AP2 with better signal strength. At the same time, SDN controller modifies flows on the open flow switch to accommodate the traffic flow change.

5. Simulation Setup and Results Discussion

5.1. Simulation Setup

To validate the design and to demonstrate the viability of proposed communication network resilience solution, the algorithm was simulated using OPNET, which contain NS3 for the network simulation and mininet for SDN.

The OPNET simulator was deployed on Virtual Machine (VM) that is hosted on linux machine using Virtual box as a hypervisor. The simulation comprised of two APs and four STAs. STAs are assigned IP addresses in the same network range. Fig. 4 depicts the mininet topology showing network elements arrangements.

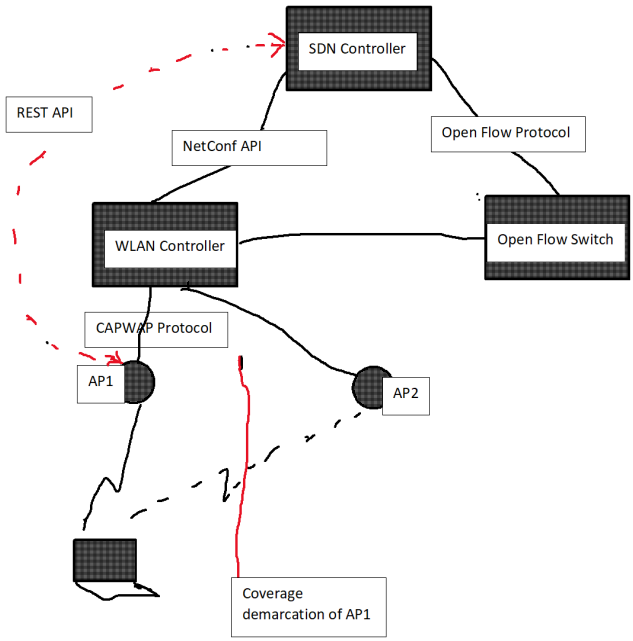

Fig. 2. Availability Design

Initially the STA1 with MAC address 00:00:00:00:00:02 is connected to AP2 with MAC address 02:00:00:00:05:00. Fig. 5 presents a wireshark print screen when the STA was in the process of registering in the network.

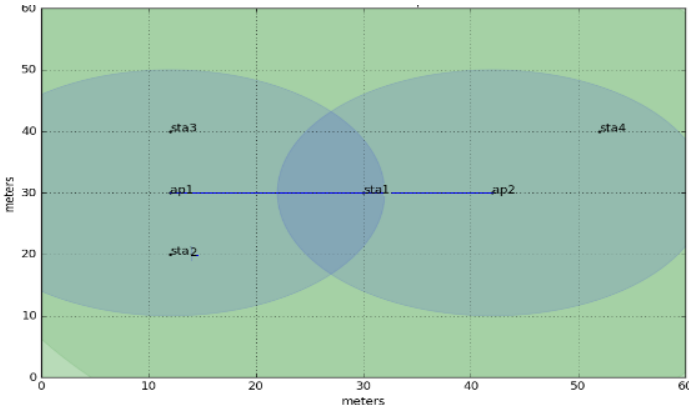

Fig. 4. Simulation Topology

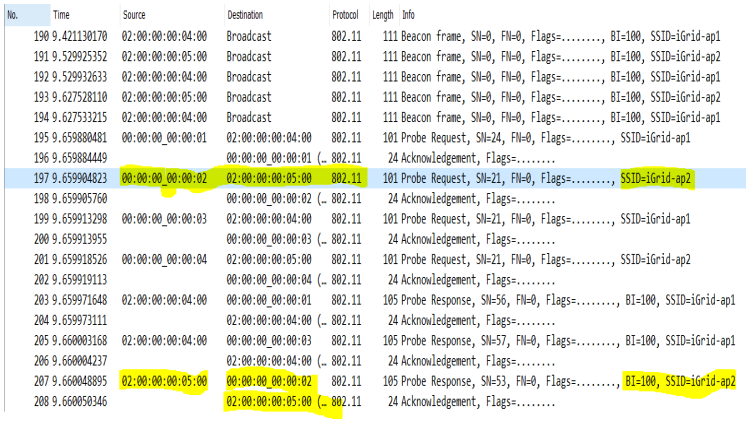

Fig 5. STA Association Wireshark Screen Shot

5.2. Simulation Results

By using the xterm terminal command 'iwconfig' to the station, it can be shown that STA1 is receiving a signal level of -49dBm, this is categorized in the range of excellent signal strength [25] from the AP2.

Various results were recorded when the STA1 was connected to the serving AP, then the serving AP was deliberate made to fail, and connected to fail over AP, with and without influence of SDN controller. Table 3 summarises results obtained from the failover tests.

Table 3. Simulation Results Summary

S/N	Access Points Event	Status at the Station			
		Received Signal Strength (dBm)	Link Quality	Bandwidth (Mbps)	Latency (ms)
1	Serving AP (AP 2) is up	-49	61/70	14.5	6.957
2	Serving AP (AP 2) is down Before Re-association	0	Nil	Nil	Nil
3	Failover to standby AP(AP1) without SDN	-80	30/70	9.59	16.185
4	Failover to standby AP(AP1) with SDN	-58	52/70	12.5	10.185

5.3. Results Discussion

According to [16], the availability is calculated using the following formula:-

$$Availability(\%) = \frac{Uptime}{Total\ Time} \times 100 \quad (1)$$

Whereby

$$Total\ Time = Downtime + Uptime \quad (2)$$

To collect data, we simulate two access points and one STA for 10 minutes whereby the serving AP is deliberately made to fail two times and the backup AP one time. Figure 6 is the availability trend for individual APs and service availability which is the actual experience from served station.

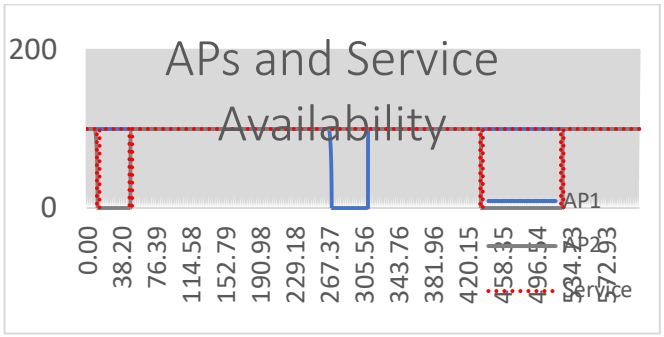

Fig. 6. Availability trend for APs and Service

Measured from the 10 minutes simulation time, the overall availability of AP1 is 93.44% while that of AP2 is 79.46%. The overall service level availability is 98.69% while the one for overall network availability is 86.45% as shown in Fig .7

.

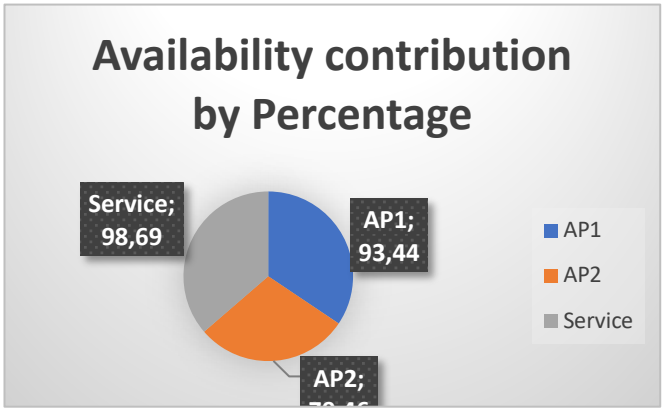

Fig. 7. Overall Availability for APs and Service

6. Conclusion and Recommendations

In this paper, we introduced an SDN based, communication network resilience enhancement solution for SDEPG. Unlike previous research work where end to end solution including the access network suitable for SDEPG was not taken into consideration in resilience solution, this work took into consideration cross layers resilience solution that will suit SDEPG. The study improved further the available wireless network handover schemes to suite SDEPG in which end stations are static by dynamically optimizing the coverage of the abandoned workstations. The proposed design guarantees reliable network regardless of the part of the network which is challenged, be it on the wireless or wired part of the network.

From the simulation results, we obtain a service level availability of 98.69% that is less than that of SDEPG reliability requirement, even though the network is fully redundant. This is attributed by the fact that, when STA loses connection, it takes about 2 sec to perform re-association to another AP and start sending traffic. The solution delivers a throughput of 12.5 Mbps and an average latency of 10.185 mSec which are far better as compared to SDEPG requirements.

Despite the practical implications, the present study also contributed to existing literature. This study contributed to the understanding of how SDEPG operations can be transformed for the purpose of saving operational costs and improving delivery efficiencies. The holistic analysis of this study added to existing research by identifying reliability requirements for SDEPG that should be considered when designing a reliability solution. The study confirmed that SDEPG requires combination of both wired and wireless technologies, and that a reliability solution should cater this requirement. The study emphasizes extension of existing studies results that also presented cross layers reliability solution but only focused on wired technologies like [5]. Moreover, the present study identified characteristics of SDN and wireless network radio frequency parameters that could be linked together to obtain improved wireless communication network reliability. Future work should focus on improving further communication network availability to suite the SDEPG requirements by finding optimal ways to reduce re association time.

Acknowledgements

This material contained in this paper is part of the on the work supported by iGrid-Project at the University of Dar es salaam (UDSM) under sponsorship of Swedish International Development Agency (Sida).

Acknowledgements

Authors may acknowledge to any person, institution or department that supported to any part of study.

References

[1] A. M. Costa, V. J. Garcia, P. M. França, and C. L. Filho, "A new method for planning secondary distribution networks," *Ser. Energy Power Syst.*, no. May 2014, pp. 437–442, 2014.

[2] A. Zidan *et al.*, "Fault Detection, Isolation, and Service Restoration in Distribution Systems," *IEEE Trans. Smart Grid*, pp. 1–16, 2016.

[3] V. Kounev, M. Lévesque, D. Tipper, and T. Gomes, "On smart grid communications reliability," in *2015 11th International Conference on the Design of Reliable Communication Networks, DRCN 2015*, 2015, pp. 33–40.

[4] N. Feamster, J. Rexford, and E. Zegura, "The Road to SDN: An Intellectual History of Programmable Networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, pp. 87–98, 2014.

[5] V. Lopez, J. P. F. Palacios, T. Szyrkowiec, M. Chamania, and D. Siracusa, "Multi-layer resilience schemes and their control plane support," *DRCN 2017 - 13th Int. Conf. Des. Reliab. Commun. Networks*, vol. 2017, pp. 86–92, 2017.

[6] J. Shamsi and M. Brockmeyer, "QoSMap: Achieving quality and resilience through overlay construction," in *Proceedings of the 2009 4th International Conference on Internet and Web Applications and Services, ICIW 2009*, 2009, no. ii, pp. 58–67.

[7] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software Defined Networks based Smart Grid Communication: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, pp. 1–1, 2019.

[8] ITU-RadioCommuncation, "Annex 9 to Working Party 5A Chairman ' s Report ELEMENTS FOR A WORKING DOCUMENT TOWARDS A POSSIBLE PRELIMINARY DRAFT NEW REPORT ON UTILITY COMMUNICATION NETWORKS REQUIREMENTS," 2018.

[9] H. Maziku and S. Shetty, "Software Defined Networking enabled resilience for IEC 61850-based substation communication systems," *2017 Int. Conf. Comput. Netw. Commun. ICNC 2017*, pp. 690–694, 2017.

[10] A. S. Active and P. Filter, "Transmission and Distribution Components," *Quadrenn. Technol. Rev. 2015*, no. January, pp. 1–22, 2015.

[11] E. Germano Da Silva, L. A. Dias Knob, J. A. Wickboldt, L. P. Gaspary, L. Z. Granville, and A. Schaeffer-Filho, "Capitalizing on SDN-based SCADA systems: An anti-eavesdropping case-study," *Proc. 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015*, pp. 165–173, 2015.

[12] V. Lopez, J. Pedro, F. Palacios, T. I. D. Gcto, and D. Siracusa, "Multi-layer resilience schemes and their control plane support," 2017, vol. 2017, pp. 86–92.

[13] K. Nahida *et al.*, "Handover Based on AP Load in Software Defined Wi-Fi Systems," vol. 19, no. 6, pp. 596–604, 2017.

[14] J. Q. Filho, N. Cunha, R. Lima, E. Anjos, and F. Matos, "A Software Defined Wireless Networking Approach for Managing Handoff in IEEE 802.11 Networks," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018.

[15] W. S. Kim, S. H. Chung, C. W. Ahn, and M. R. Do, "Seamless handoff and performance anomaly reduction schemes based on openflow access points," *Proc. - 2014 IEEE 28th Int. Conf. Adv. Inf. Netw. Appl. Work. IEEE WAINA 2014*, pp. 316–321, 2014.

[16] N. Dorsch, F. Kurtz, and C. Wietfeld, "Enabling hard service guarantees in Software-Defined Smart Grid infrastructures," *Comput. Networks*, vol. 147, pp. 112–131, 2018.

[17] 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," *2016 IEEE Int. Conf. Commun. ICC 2016*, 2016.

[18] J. P. G. Sterbenz *et al.*, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Comput. Networks*, vol. 54, no. 8, pp. 1245–1265, 2010.

[19] P. Smith *et al.*, "Network resilience: A

systematic approach," *IEEE Commun. Mag.*, vol. 49, no. 7, pp. 88–97, 2011.

[20] A. Modarresi, S. Gangadhar, and J. P. G. Sterbenz, "A framework for improving network resilience using SDN and fog nodes," *Proc. 2017 9th Int. Work. Resilient Networks Des. Model. RNDM 2017*, pp. 1–7, 2017.

[21] F. Kurtz and C. Wietfeld, "Advanced Controller Resiliency in Software-Defined Networking Enabled Critical Infrastructure Communications," in *Advanced controller resiliency in software-defined networking enabled critical infrastructure communications*, 2017, pp. 673–678.

[22] M. H. Rehmani, F. Akhtar, A. Davy, and B. Jennings, "Achieving Resilience in SDN-Based Smart Grid: A Multi-Armed Bandit Approach," *2018 4th IEEE Conf. Netw. Softwarization Work. NetSoft 2018*, pp. 105–113, 2018.

[23] L. Ren, "Resilient Microgrids through Software-Defined Networking Resilient Microgrids through Software-Defined," 2017.

[24] K. De Craemer and G. Deconinck, "Analysis of State-of-the-art Smart Metering Communication Standards," *Proc. 5th Young Res. Symp.*, pp. 1–6, 2010.

[25] C. J. Wallnerström, P. Hilber, and S. Stenberg, "Fault Management at a Distribution System Operator," 2012, no. June, pp. 350–355.

[26] M. Wang, X. Niu, L. An, and J. Li, "Research on performance evaluation method of effective assets of power grid based on value engineering," *E3S Web Conf.*, vol. 118, pp. 3–6, 2019.

[27] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," *Comput. Networks*, 2014.

[28] N. Gunantara, P. K. Sudiarta, A. A. N. A. I. Prasetya, A. Dharma, and I. N. Gde Antara, "Measurements of the Received Signal Level and Service Coverage Area at the IEEE 802.11 Access Point in the Building," *J. Phys. Conf. Ser.*, vol. 989, no. 1, 2018.