International Journal of Smart Grid and Clean Energy

SDN-based cross layer resilience approach for secondary distribution power grid automation: Review and recommendation

Yona Andegelile[a], Hellen Maziku[a], Nerey Mvungia[a], Mussa Kissaka[b]*

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

Abstract

Secondary Distribution Electrical Power Grid (SDEPG) is the last mile of power grid connecting end users. Transforming a traditional SDEPG to a smart SDEPG demands for a need to have resilient communication in order to improve electrical power reliability. The ubiquitous nature of SDEPG requires combination of wired and wireless communication network technologies at all to facilitate the transformation, therefore communication network resilience solution must accommodate this requirement and use attributes at all communication network layers to effectively achieve optimally resilient network. Software Defined Networking (SDN) offers flexibility, making it superior in enhancing communication network resilience. This study present extensive survey on the SDN based communication network resilience solutions for SDEPG. The survey involved analysis of published materials from libraries and databases related to SDN based resilience solution by comparing different approaches adopted by researchers based on resilience discipline, target application, considered failure scenarios, target communication network technologies and communication network layer attributes used to deliver the suggested solution. The study is finalized by summarizing the current solutions challenges and proposes an approach that leverages SDN to deliver cross layers resilience solution to facilitate SDEPG transformation to smart grid.

Keywords: Cross layers, resilience, secondary distribution power grid, software defined networking

1. Introduction

SDEPG is the final stage in the delivery of electric power to end customers. This portion of the grid comprises of step-down distribution transformers, consumer services, and meters to measure the consumer energy consumption [1]. The secondary distribution power grid ranges between 0.4kV to 11kV voltage levels. The secondary distribution electricity infrastructure is complex characterized by distributed power generation points, manual power system management, and lack of interaction between end users and utility. Fig. 1 shows a sample SDEPG network from Mikocheni, Dar es Salaam. The network is over clouded with service lines and poles required to reach every house in the street. This leads to loss of energy, poor power quality, poor management of peak load. As a result, utility companies in developing countries suffer poor Net Promoter Score (NPS) and significant revenue loss from prolonged down time. [2].

* Manuscript received July 4, 2020; revised December 11, 2020.
Corresponding author. *E-mail address*: yona.andegelile@gmail.com.
doi: 10.12720/sgce.10.1.69-82

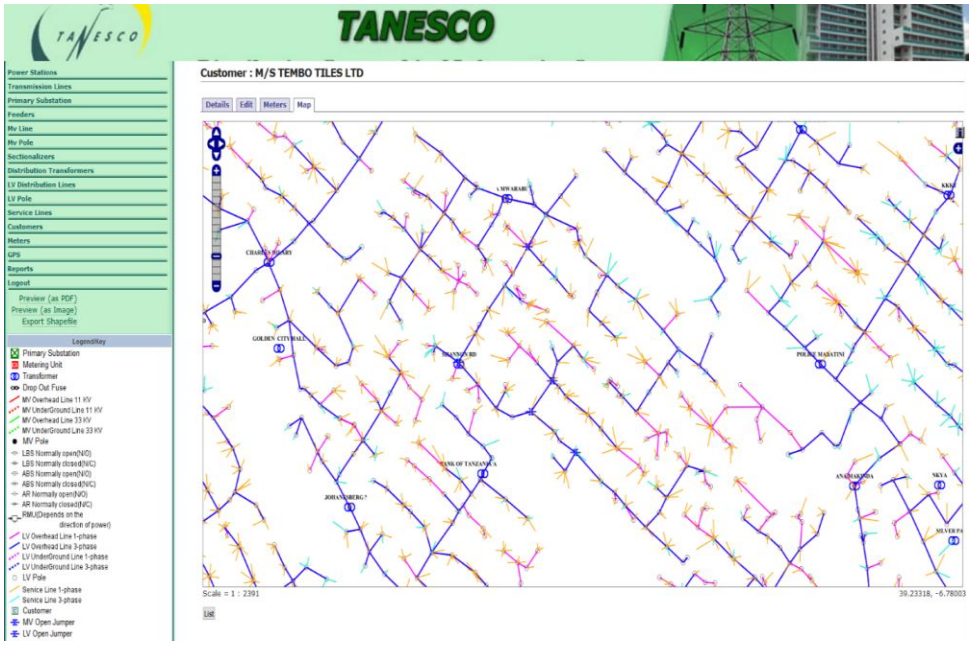

Fig. 1. SDEPG power network, source (Tanesco)

Current research efforts lean towards automating fault detection and clearance in traditional power grid networks[3], [4] as stepping stone towards transforming this portion of the grid to smart grid.

Communication network makes an essential part of power grids automation since it links all active devices across the network [5], and facilitate sending/receiving measurement and control commands from the control center [6]. Bearing its importance, communication network must be resilient enough for seamless and safe SDEPG automatic fault detection and clearance [7].

SDN is computer network architecture that separates the network's control and forwarding planes offering flexibility and programmability capabilities which allows easier management of the whole communication network infrastructure [9].

Considering the nature of SDEPGs, most of the sensors and Intelligent Electronic Devices (IEDs) spread across randomly, making the access network very complex, a combination of both wireless and wired communication technologies is required for efficient SDEPG automation. Therefore, a resilience solution which cuts across all technologies must be developed. There has been tremendous research addressing power grid communication network reliability using Software Defined Networking (SDN) technology including [8].

This study present extensive survey on the SDN based communication network resilience solutions for SDEPG. The survey involved analysis of published materials from libraries and databases related to SDN based resilience solution by comparing different approaches adopted by researchers based on resilience discipline, target application, considered failure scenarios, target communication network technologies and communication network layer attributes used to deliver the suggested solution.

The rest of the paper is organized as follows. It starts with a general overview of communication network resilience and SDN as an approach to efficiently achieve cross layers communication network resilience in section one. Section two provides highlights of methodology used in reviewing current resilience approaches. Section three presents some fundamental concepts related to resilience and SDN. Section four analyses different approaches that have been used to achieve communication network resilience, revealing their strengths and weaknesses.

Based on challenges identified, the study is finalized proposing an optimal resilient SDEPG communication network that leverages SDN, in achieving cross layers communication network resilience

for SDEPG in which wireless networks are proposed for the access network and wired for aggregation and core network. The proposed solution will address all challenges identified in the current studies.

2. Materials and Methods

The approach employed to produce this survey is systematic review method using scientific texts deep analysis of published materials and data searching in libraries and databases for relevant studies [10]. Examples of libraries and databases include IEEE Xplore, research gate, arxiv, Elsevier, ACM, and Wiley [11]. The search used over ten phrases based on the study of SDN, and Communication Network Resilience resulting in a total of 138 relevant research papers and technical reports. Following a study on the articles, 70 of them were removed from the list based on the degree of relevance to this study of addressing communication network resilience using SDN approach. Furthermore, when the year of publication, and relevance of a paper to power grid, IoT or industrial automation communication network resilience were considered, 19 more papers were removed. However, during deep review of the remaining papers, 11 relevant papers were identified and got added for the review. Hence, only 30 papers remained for deep qualitative analysis.

The papers were further scrutinized based on two resilience disciplines, tolerance and trustworthiness. Based on [7], tolerance is achieved by availability and reliability, while trustworthiness is achieved by dependability and performability.

Finally, the papers were analysed based on target application demands, failure types considered, technologies and target communication network layer to address resilience. The summary of the adopted research method is as it appears in Fig. 2.

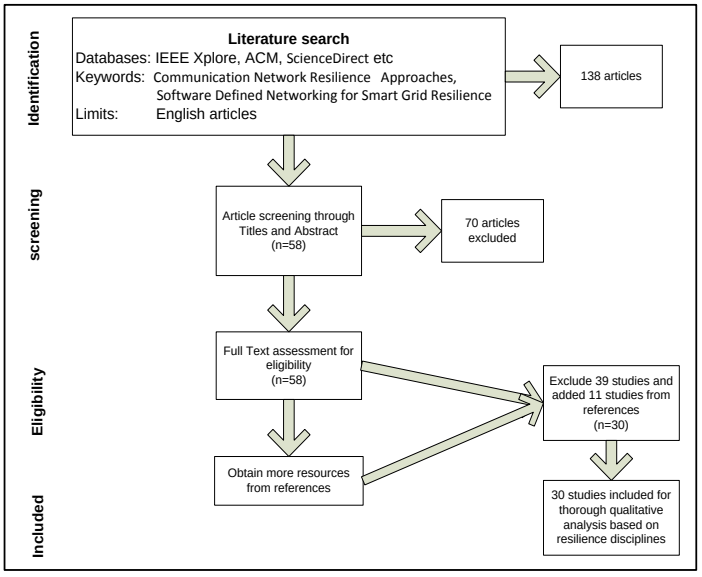

Fig. 2. Research methodology

3. Fundamental Concepts

3.1. Communication network resilience

Resilience can be an ability, capability or behavior, or a procedure. It can also relate to a certain discipline [12]. In general resilience means to coil back [13]. It is used in many disciplines, including psychology, physical sciences, ecology, and engineering, which relate it to the ability to recover from harmful events and catastrophes.

Communication network, Resilience is a quantitative property of a network that enable each level of hierarchy to maintain the same level of functionality when subjected to internal changes and external

disturbances. [14]. This can be weather related disruptions, technology-based disasters, and malicious human activities. The network is said to be resilient when it can maintain its capacity to allocate resources efficiently, and provide acceptable level of service [14].

3.2. Challenges to communication network resilience

Challenges are the events that can cause faults and/or misbehaviour, and eventually system failure. Network challenges are characterized based on the criteria as stipulated in [14] that includes:

Large-scale disasters that can be resulted from force majeure, for example the 2006 Taiwan earthquake, etc. Socio-political & economic challenges which are deliberate activities meant to disturb normal communication network operations. Dependent challenges that are resulted from cascade of failure. For example, power grid and internet dependent failures. Human-based challenges that are deliberate or non-deliberate activities. For example, malicious attacks. Unusual traffic which affects mostly the network traffic and may result in irresponsiveness of the end systems[15].

3.3. Software defined networking

SDN is computer network architecture that separates network control functions(control plane) from forwarding functions (data plane) [9]. The SDN architecture is an improvement of traditional networks which simplifies the introduction and deployment of newly developed control plane functions, for example routing strategies [16]. The SDN architecture is made up of three conceptual planes and couple of interfaces as shown in Fig. 3. The application plane which is accountable for performing applications that operate in the network infrastructure. These applications are responsible for manipulation of all networking features, for example network related policing and routing, such as visualization, path reservation and network provisioning [16].

The control plane implements control logic, such as routing schemes to orchestrate the behaviour of traffic [17]. The data plane is made up of the devices that are accountable for forwarding data, referred as switches [18]. Communication between the control and data planes is enabled through the Northbound API and the Southbound API interfaces [19]. The SDN flexibility to manage flows is largely enabled through these interfaces, bringing impact directly in areas such as security, traffic management and performance [20]. The SDN separation of control and forwarding plane has the potential to reduce the network deployment cost [21]. The separation of data and control plane has the potential to considerably simplify the implementation of resilience functionality through [22].

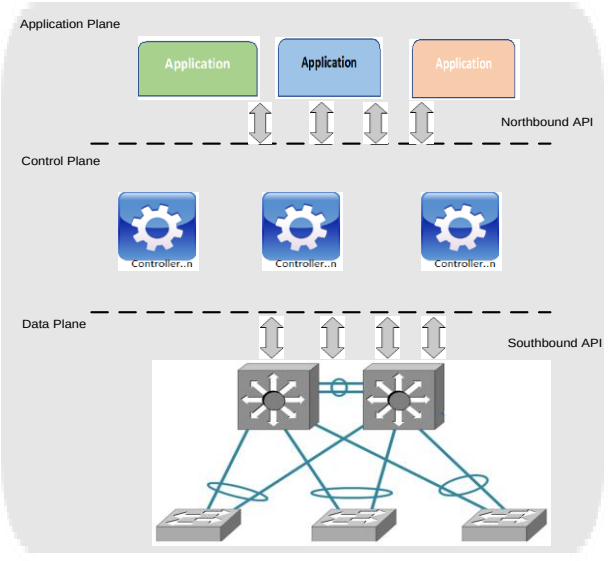

Fig. 3. SDN architecture

4. SDN Based Communication Network Resilience Approaches

In this survey, different studies are grouped into three disciplines of resilience as stipulated in [7]. First is discipline relating to resilience strategies and approaches, second is the discipline relating to challenges tolerance and third is the discipline relating to trustworthiness. The survey also analyses the studies from application point of view in which technologies, fault types and communication layer of interest were included in the review to make the survey relevant.

4.1. Resilience measures based on resilience strategies and approaches

Resilience framework built by [7], defined number of resilience ideologies, which are based on resilience strategy, defined as D2R2 + DR: The first 2 Ds represent Defend and Detect. The 2 Rs represent Remediate and Recover and last two DR stand for Diagnose and Refine.

The first part of this strategy explains a real time control loop that will dynamically enable the networks to respond to challenges, and a second part a non-real time control loop that focus on improving the network design [23].

- Defend

This refers protective mechanism that decreases the probability of a fault or failure occurrence [7]. The defence mechanism is built up by developing and analysing threat models and is made up of a passive and active component. Passive defences focuses on physical, example, redundancy and diversity paths [24]. Active defences are made up of survival mechanisms [25].

- Detect

Detect strategy is brought as a supplement for defend in which a network monitored with the purpose to observe its behaviour, then look for anomalies so as proper action can be taken to reduce service delivery impact when defence mechanism has failed. The network monitoring can be done in three ways; the first is vigilantly sensing deviations from normal operation, the second one applies a standard way to identify errors in the network by applying well know formulas or algorithms such as calculating Cyclic-Redundancy Checks (CRCs), the last one is kind of reactive as it is based on detecting service failures. Again, the strength of this relies on understanding of service requirements. [26].

- Remediate

This strategy focuses on finding a quick recovery mechanism to counter the effects of the network challenges. Remedial action examples include dynamic routing protocols to reroute traffic when there is a failure in a network path [27].

- Recover

Once the challenge is overcome, the network might fail to recover to normal state. Recovery strategies focuses on mechanism to bring back the network to normal operational behaviour.

- Diagnose

In some circumstances, it might not be possible to directly detect the challenges, in this case fault will need to be diagnosed based on observable error [7], manually or using automated way [28]. Analysis of packet traces to determine a protocol vulnerability is a good example of network-based fault diagnosis.

- Refine

The strategies mentioned above might not be efficient and effective enough due to dynamic behaviour of challenges, so improvement strategies must be employed after the challenge is over. The refine strategy focuses on learning and reflecting the way defence, detection, remediation, and recovery have worked so

they can be improved to continuously increase the resilience of the network.

Table 1. Review on resilience measures based on resilience strategies and approaches

Paper	Reliability	Availability	Dependability	Performability
(Modarresi, Gangadhar, & Sterbenz, 2017)[29]				
(Rehmani, Akhtar, Davy, & Jennings, 2018)[30]				
(Schaeffer-Filho et al., 2014)[22]				
(Lopez, Pedro, Palacios, Gcto, & Siracusa, 2017)[8]				
(Ren, 2017)[31]				
(Zhang, Wei, Guo, Hou, & Wu, 2016)[32]				
(Maziku & Shetty, 2017)[33]				
(Aydeger, Akkaya, Cintuglu, Uluagac, & Mohammed, 2016)[34]				
(Danzi, Angjelichinoski, Stefanovic, Dragicevic, & Popovski, 2018)[35]				
(Dong, Lin, Tan, Iyer, & Kalbarczyk, 2015)[36]				

Table 1 summaries different approaches proposed by researchers in the effort to develop resilience communication network. It is evident that, most of the researchers focused mostly on serving current service interruption but did not bother much on how to recover the network to the original setup. This includes recovering, diagnosing and refining the network back to its original design setup. The risk coming with this is, when the chosen alternative gets interrupted, there is large possibility that network will not be able to survive the failure. This is since, there is always a limit of redundant paths which can be deployed in the network, so recovering affected paths is paramount important. This is a big gap is communication network resilience as the resilience is limited to only first failure iteration. Resilience solution needs to be provided the network with future proof of availability despite the number of failures. Future researches need to focus on finding optimal scheme to recover the network back to its original state of operation after fault isolation.

There are also exist some challenges with most chosen approach like reactive methodology which about 90% of researchers suggested. In this a communication problem is detected, then a remedial action is taken to protect carried services. The strength of this methodology will largely depend of efficiency of detection method in terms time and accuracy. The longer the time it takes to detect the problem, the lesser the reliability of the network. Efficiency of remedial solution is also a key factor in determining the efficiency of the method. Considering the unstructured nature of failures, it's very challenging to have a detection method which can accommodate all types of failures. This is also an area of interest in the studies of communication resilience, i.e., finding an optimal scheme to detect all types of fault with corresponding remedial actions.

Some researchers proposed a proactive method, in which, the communication network is completely protected from failure. This is the best method if methods of prevention could be 100% efficient, however, it isn't practical to avoid all types of failures, this can be practical for some types of failures. This is open challenge for future researches to find an optimal scheme that can prevent all possible failure types. The better option could be combination of both approaches as proposed by some researchers. They proposed combination of proactive and reactive methods of ensuring the network is resilient. This it gives both options to defend the network and for failure types that could not be protected, detection and remedial solution to protect the services are in place.

4.2. Resilience measures based on tolerance and trustworthiness

Communication network ability to meet the resilience objectives are measured based on its ability to withstand challenges, which define its tolerance and trustworthiness. There have been several frameworks proposed for measuring resilience based on tolerance and trustworthiness. Some of the common measures are reliability, availability, dependability and performability. Many of the measures overlap with one another. [37][38].

Reliability: The probability that an entity (unit) will complete its intended mission as required over a specified period in its intended environment or stated conditions.

Table 2. Review on resilience measures based on tolerance and trustworthiness

Paper	Reliability	Availability	Dependability	Performability
(Modarresi, Gangadhar, & Sterbenz, 2017)				
(Rehmani, Akhtar, Davy, & Jennings, 2018)				
(Schaeffer-Filho et al., 2014)				
(Lopez, Pedro, Palacios, Gcto, & Siracusa, 2017)				
(Ren, 2017)				
(Zhang, Wei, Guo, Hou, & Wu, 2016)				
(Maziku & Shetty, 2017)				
(Aydeger, Akkaya, Cintuglu, Uluagac, & Mohammed, 2016)				
(Danzi, Angjelichinoski, Stefanovic, Dragicevic, & Popovski, 2018)				
(Dong, Lin, Tan, Iyer, & Kalbarczyk, 2015)				

Availability: The proportion of the operating time in which an entity meets its in-service functional and performance requirements in its intended environment [7] [39][40].

Dependability: Dependability is that property of a system such that reliance can justifiably be placed on the service it delivers [40]. There are different facets of dependability. The various attributes of dependability include availability (readiness for usage), reliability (continuity of service), correctness of service and maintainability [41]

Performability: Performability is the probability that the system will stay above a certain accomplishment level over a fixed period. It is often described by the QoS (quality of service) measures for a given set of operational conditions[38]. Performability can measure the degraded performance of a complex system such as the internet, etc.

Table 2 summaries different resilience targets as approached by various researchers. The resilience target will usually be guided by the service to be carried by the network. Some of the applications are very time sensitive, therefore network availability is the key factor in determining resilience network. Some applications have combination of requirements which define network reliability. These measures are sometimes used together interchangeably.

As can be seen, reliability and dependability are the key factors which have been a focus for all researchers. Since not all application are sensitive to tight Quality of Service (QoS) parameters, some researchers have been keen in ensuring performability is taken care when developing resilience solution. Since resilience targets are dependent on the services to be carried by the network, the studies suggest that it is important to explore target applications for before adopting a approach. This goes in hand with technologies which was considered and failure types. Further check on suitability of these studies reveals

that SDEPG application and technologies were not considered at all since these studies were mostly based on wired technologies with general grid application. Future studies need to focus on finding a resilience solution that can satisfy SDEPG, a solution that will cut across all layers.

4.3. Application view of a resilient communication network

Communication network resilience requirements depends much on applications meant to be served by the network, this will then determine technology to be deployed, resilience approach, potential fault types, communication layer where resilience algorithms need to be applied and later simulation tools to be used in the study. The type of simulation tools used determine trustworthiness and orientation of results obtained.

Table 3. Paper review based on application, technologies, fault types and communication network layer

Authors	Application	Technologies	Fault Types	Communication Layer	Simulation Tools	Weakness
(Modarresi, Gangadhar, & Sterbenz, 2017)	IoT	Neutral	IP Spoofing (security)	Network layer (Internet Protocol (IP))	Mininet	Single fault type, single Comm layer
(Rehmani, Akhtar, Davy, & Jennings, 2018)	Smart Grid (IEC 61850)	Neutral	Link/path failure	Physical /line protocol	Mininet	Wireless RF related problems not factored in
(Schaeffer-Filho et al., 2014)	Neutral	Neutral	IP Security challenges	Network layer (Internet Protocol (IP))	PReSET (OMNET++ & Ponder2)	Single fault type, single Comm layer
(Lopez, Pedro, Palacios, Gcto, & Siracusa, 2017)	Neutral	IP/MPLS & optical	Physical and IP layer failures.	Cross layers	No simulation, only design	No Security challenges consideration
(Ren, 2017)	Microgrids	Neutral	Physical & Application QoS failures.	Physical path change, Traffic prioritization	Hardware-in-the-Loop Testbed	Wireless RF related challenges not factored.
(Zhang, Wei, Guo, Hou, & Wu, 2016)	Smart grid	Neutral	Planned outage & Physical Link Failure	Physical /line protocol	NOX controller& OpenvSwitch	No Security challenges consideration, single Comm layer
(Maziku & Shetty, 2017)	IEC 61850	Neutral	IP based Security challenges	Network layer (Internet Protocol (IP))	GENI testbed	Single fault type, single Comm layer
(Aydeger, Akkaya, Cintuglu, Uluagac, & Mohammed, 2016)	Smart Grid (Smart Grid)	PLC (wired) & Wireless	Link/path failure	Physical path change, Traffic prioritization	Mininet & NS-3	Wireless as fall-back, Security challenges not considered.
(Danzi, Angjelichinoski, Stefanovic, Dragicevic, & Popovski, 2018)	Microgrids	Wireless & PLC	Cyber attack	Physical path change, Traffic prioritization	MATLAB /Simulink simulator	Only DDoS, Wireless RF challenges not considered
(Dong, Lin, Tan, Iyer, & Kalbarczyk, 2015)	Smart Grid	Neutral	IP Security challenges	Physical path change, IP traffic rerouting	Mininet & Powerworld Power Grid & Control Center Simulation Servers	Single failure type considered, comm technologies not specified

(Molina, Jacob, Matias, Moreira, & Astarloa, 2015)[42]	IEC 61850	Neutral	Physical & Application QoS failures.	Physical path change, Traffic prioritization	Mininet & open source rapid61850	Wireless RF related challenges not factored.
(Lee, Kwon, Shin, Lee, & Chung, 2016)[43]	Neutral	WLAN	AP system and RF failure	Physical path change	Not standard simulation tool, prototyped	IP recovery not considered, WLAN controller not considered
(Molina, Jacob, & Astarloa, 2016)[44]	Industrial automation	Wireless Networks	Wireless RF failure	Physical path change	OpenNet, PRP stack,OVS	IP recovery not considered, WLAN controller not considered
(Dorsch, Kurtz, & Wietfeld, 2018)[45]	Smart Grid (IEC 61850)	Neutral	Physical & Packet Loss & Hardware failures.	Physical path change	Nordic 32 test system & Mininet	Wireless RF related challenges and Security not factored.
(Aydeger, 2016) [46]	Smart Grid	PLC (wired) & Wireless	Link/path failure	Physical path change, Traffic prioritization	Mininet & NS-3	Wireless as fall-back, Security challenges not considered.
(Germano et al., 2015)[47]	SCADA Systems	Wired	Link/path failure	Security (Eavesdropping)	Mininet	Only Wired technology considered, Single failure type

Table 3 summarizes researchers view of the applications, technologies and communication resilience layer which were considered in developing resilience solution. As can be seen from the summary, large percent of the chosen papers were purely on smart grid, utilizing IEC 61850 as a standard protocol which define communication requirement for monitoring and control of power grid. Some of them were general industrial control, and few general IoT. Some studies did not specify target communication technology in the question. The downside of this is, some failures which specific for a technology, are not addressed. It is revealed that existing researches are focusing on addressing communication resilience for primary, and the rest of the grid which are mostly using wired technologies, with IEC 61850 which is centralized control. Considering the nature secondary distribution power grid, a combination of wired and wireless technologies is required to achieve its efficient monitoring and control [30]. Wireless networks suffer a lot of radio frequency problems like fading, interference etc, therefore, resilience solution for SDEPG must take into consideration all technologies while considering wireless network challenges.

5. Summary of Challenges and Current Solutions

The drive to automate the power grid and make it smart has largely been driven by advancement in electrical power systems, control engineering, and Information and Communication Technologies (ICT). The power grid needs to be equipped with advanced electrical power system components, sensing devices, control and actuation equipment, then get supplemented by ICT for it to be smart [48]. The dependability of the grid in ICT makes the communication part more sensitive, thus requiring high-level of availability.

Communication network failure can be caused by security attack, natural disaster, system or telecommunication equipment malfunction, hindering important information from being delivered to and from the smart grid entities like relays, Supervisory Control and Data Acquisition (SCADA) etc. This may result into, cascading failures which may include complete power blackout [49][50]. Identification of communication failure and finding alternative communication paths at run-time is very essential.

Based on recent studies done, SDN based solution has been proved to be superior [51]. The SDN superiority has largely been uplifted by it features like programmability, protocol independence, and availability of various APIs [52][53]. Additionally, SDN simplifies the management and control of the SDEPG communication networks.

However, SDEPG resilience requirements have not been addressed extensively. Resilience strategies and approaches need to be further exhausted to accommodate network recovery to its original state after fault isolation and service restoration. Researchers need to focus more on addressing resilience requirement that suits the SDEPG following its complexity. SDEPG requires combination of wired and wireless technologies, and there has not been a resilience solution that has addressed this need.

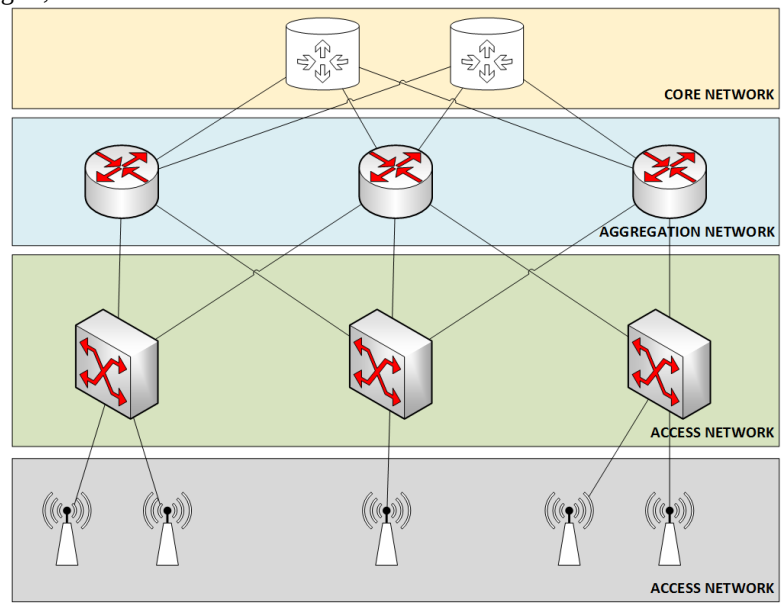

Fig. 4. Communication network segmentation

6. Future Research Directions

As for future research direction, focus should be more on solutions which cut across all communication network layers, including physical, data link and network layer. This should be possible considering programmability and flexible control of Software Defined Networking. The network architecture needs to be segmented into three layers, Core, aggregation and access layer. The Core network is mostly built up of optical network and IP networks. This connects power grid substations to the central control office. A multi-layer resilience schemes solution by [8], which focused only on optical fiber technology provides a breakthrough for this part of the network and can well be adopted. The aggregation network aggregates traffic from clusters of wireless network base stations, this will be access points for urban areas and long range (LoRa) network server for rular networks. The access network is made wireless network base stations and layer 2 switches. Fig. 4 shows communication network segmentation.

To achieve resilience on the access part of the network, which is purely layer 2, SDN controller is introduced to influence seamless failover of end stations to nearby base stations based on algorithm set on it. For urban networks, the controller is interfaced with WLAN controller and dynamically manipulate the Radio Frequency (RF) parameters of nearby Access Points (AP) when one AP is challenged, this is to ensure that end service reliability for stations in abandoned area is always guaranteed. For rural networks, LoRa [54] technology enables end stations to get served by multiple base stations. Algorithm implemented in SDN controller will influence the best packet duplication criteria and return path selection on the LoRa network server. Fig. 5 present the proposed future network to accommodate Cross Layers resilience network for SDPG.

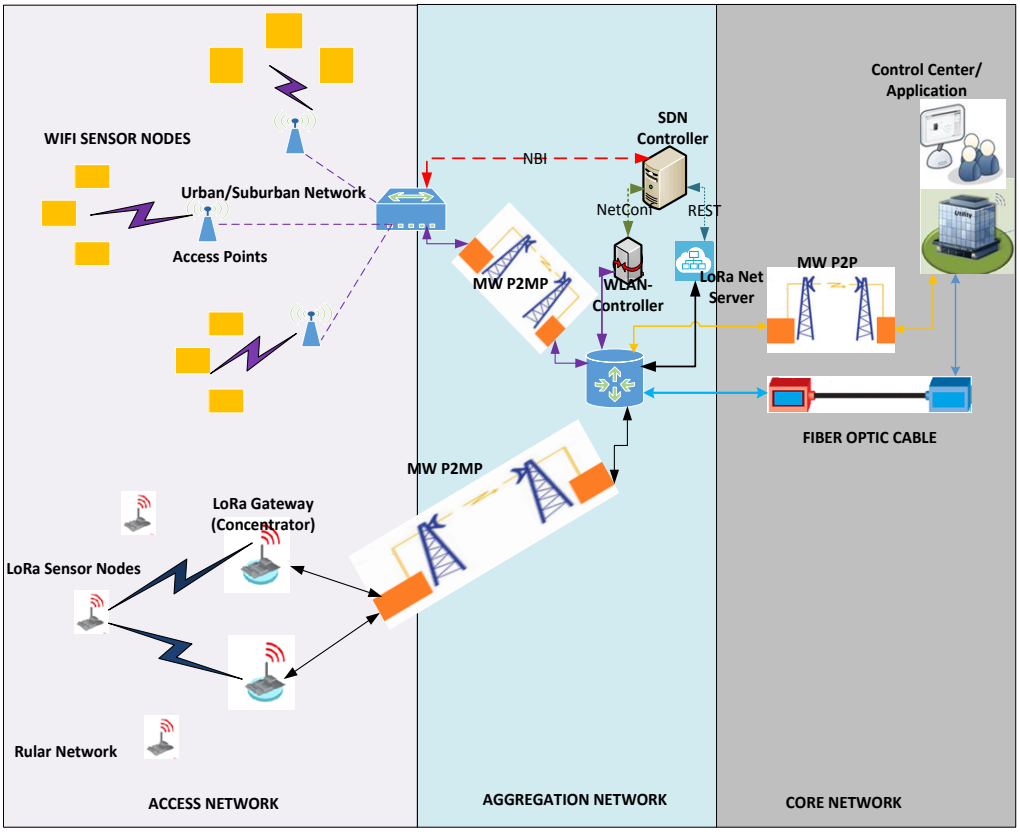

Fig. 5. Proposed cross layers resilience network solution

7. Conclusion

In this paper, SDN based communication network resilience techniques for secondary distribution power grid and general smart grid has been reviewed and scrutinized. Emphasis has been on the resilience solution which serves requirement of smart grid control and operation automation. Different resilience approaches and targets have been explored and discussed, with corresponding communication network technologies, and communication network layers considered when developing resilience solution.

It is clear from the discussion that, combination of proactive and reactive approaches in developing resilience solution works better as compared to individual methodologies, as it prevents some fault types from happening and reactively detect and apply remedial algorithms for the ones which could not be prevented. It is also clear that, most of the researchers did not consider developing means to bring the network back to original state after service restoration, which is exposing the network into a risk of not serving the purpose, if a second failure happens on the alternate path. Specifically, for secondary distribution power grid which depends largely on combination of wired and wireless communication technologies, very few works have been done considering wireless network radio environment challenges.

More researches should be conducted to explore the improvement of available resilience solution accommodate wireless network radio environment challenges and recovering the network back to original state ones the challenge is over.

Apart from that, the solutions should consider parameter and features available in all layers of communication network to achieve more efficient resilient communication network for secondary distribution power grid.

Conflict of Interest

The authors declare that they have no competing interest

Authors Contribution

YA designed, coordinated and drafted the manuscript. HM reviewed the format and contents, and English proofreading. MK participated in research coordination. NM participated in research coordination. Authors read and approved the final manuscript

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).

References

[1] Roshan Chhetri TL. Voltage profile in distribution system. In: *Proc. of 2nd International Conference on Renewable & Sustainable Energy Development 2017: A Step towards Achieving Gross National Happiness*, 2008, no. October 2016.

[2] Mohagheghi S, Stoupis J, Wang Z, and Li Z. Demand response architecture. *System*, 2010: 501–506.

[3] Isaac M and Van Vuuren DP. Modeling global residential sector energy demand for heating and air conditioning in the context of climate change. *Energy Policy*, 2009; 37(2): 507–521.

[4] Cecati C, Mokryani G, Piccolo A, and Siano P. An overview on the Smart Grid concept. in *IECON Proceedings (Industrial Electronics Conference)*, 2010: 3322–3327.

[5] Fang X, Misra S, Xue G, and Yang D. Smart grid - The new and improved power grid: A survey. *IEEE Commun. Surv. Tutorials*, 2012; 14(4): 944–980.

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

[7] Sterbenz JPG *et al.*, Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Comput. Networks*, 2010; 54(8): 1245–1265.

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

[9] Feamster N, Rexford J, and Zegura E. The road to SDN: An intellectual history of programmable networks. *ACM SIGCOMM Comput. Commun. Rev.*, 2014; 44: 87–98.

[10] Livoreil B. *et al.*, Systematic searching for environmental evidence using multiple tools and sources, *Environ. Evid.* 2017; 6(1): 1–14.

[11] Kiduk Y. and Meho LI. Citation analysis: A comparison of google scholar, scopus, and web of science. *Proc. ASIST Annu. Meet.*, 2006; 43.

[12] Windle G. "What is resilience? A review and concept analysis," *Rev. Clin. Gerontol.*, 2011; 21(2): 152–169.

[13] Marchese D, Reynolds E, Bates ME, Morgan H, Clark SS, and Linkov I. Resilience and sustainability: Similarities and differences in environmental management applications. *Sci. Total Environ.*, 2018; 613–614: 1275–1283.

[14] Mauthe A. *et al.*, Disaster-resilient communication networks: Principles and best practices. *Proc. 2016 8th Int. Work. Resilient Networks Des. Model. RNDM 2016*, 2016; 1–10,.

[15] Andegelile Y. and Mvungi N. SDN based high availability communication network architecture for secondary distribution electric power grid. in *2019 7th International Conference on Smart Grid (icSmartGrid)*, 2019; 52–57.

[16] Jarraya Y, Madi T, and Debbabi M. A survey and a layered taxonomy of software-defined networking. *IEEE Commun. Surv. Tutorials*, 2014; 16(4): 1955–1980.

[17] Berde P. et *al.*, "ONOS : Towards an open, distributed SDN OS," *HotSDN '14 Proc. third Work. Hot Top. Softw. Defin. Netw.*, 2014; 1–6.

[18] ONF, "OpenFlow Switch Specification Version 1.5.1 (Protocol version 0x06) for information on specification licensing through membership agreements," vol. 1, p. 283, 2015.

[19] Habib MF, Tornatore M, Dikbiyik F, and Mukherjee B. Disaster survivability in optical communication networks, *Comput. Commun.*, 2013; 36(6): 630–644.

[20] Nakayama H, Mori T, Ueno S, Watanabe Y, and Hayashi T. An implementation model and solutions for stepwise introduction

of SDN. *APNOMS 2014 - 16th Asia-Pacific Netw. Oper. Manag. Symp.*, 2014; 1: 2–5.
[21] Dai W. *et al.*, The cost of a cloud : Research problems in data center networks. *J. Inf. Technol.*, 2009; 27(3): 68–73.
[22] Schaeffer-Filho A, Smith P, Mauthe A, and Hutchison D. Network resilience with reusable management patterns. *IEEE Commun. Mag.*, 2014; 52(7): 108–115.
[23] Smith P. *et al.*, Network resilience: A systematic approach. *IEEE Commun. Mag.*, 2011; 49(7): 88–97.
[24] Guidoni DL, Mini RAF, and Loureiro AAF. On the design of resilient heterogeneous wireless sensor networks based on small world concepts. *Comput. Networks*, 2010; 54(8): 1266–1281.
[25] Bell D and LaPadula L. Network firewalls. *IEEE Commun. Mag.*, no. September, 1994; 50–57.
[26] Padmanabhan VN, Wang HJ, and Chou PA. Resilient peer-to-peer streaming, *Proc. - Int. Conf. Netw. Protoc. ICNP*, vol. 2003-Janua, 2003; 16–27.
[27] Kvalbein A and Hansen A. Fast IP network recovery using multiple routing configurations. in *2006. 25th IEEE* , 2006; 00(c):
[28] Steinder M and Sethi AS. A survey of fault localization techniques in computer networks. *Sci. Comput. Program.*, 2004; 53(2) SPEC. ISS., pp. 165–194,.
[29] Modarresi A, Gangadhar S, and Sterbenz JPG. A framework for improving network resilience using SDN and fog nodes. *Proc. 2017 9th Int. Work. Resilient Networks Des. Model. RNDM 2017*, 2017; 1–7.
[30] Rehmani MH, Akhtar F, Davy A, and Jennings B. Achieving resilience in SDN-based smart grid: A multi-armed bandit approach. *2018 4th IEEE Conf. Netw. Softwarization Work. NetSoft 2018*, 2018; 105–113.
[31] Ren L. Resilient microgrids through software-defined networking resilient microgrids through software-defined, 2017.
[32] Zhang X, Wei K, Guo L, Hou W, and Wu J. SDN-based resilience solutions for smart grids. *2016 1st Int. Conf. Softw. Networking, ICSN 2016*, 2016; 0–4.
[33] Maziku H and Shetty S. Software defined networking enabled resilience for IEC 61850-based substation communication systems. *2017 Int. Conf. Comput. Netw. Commun. ICNC 2017*, 2017; 690–694.
[34] Aydeger A, Akkaya K, Cintuglu MH, Uluagac AS, and Mohammed O. Software defined networking for resilient communications in Smart Grid active distribution networks. *2016 IEEE Int. Conf. Commun. ICC 2016*, 2016.
[35] Danzi P, Angjelichinoski M, Stefanovic C, Dragicevic T, and Popovski P. Software-defined microgrid control for resilience against denial-of-service attacks. *IEEE Trans. Smart Grid*, 2018; 1–9.
[36] Dong X, Lin H, Tan R, Iyer RK, and Kalbarczyk Z. Software-defined networking for smart grid resilience. 2015; 61–68.
[37] Jabbar A. A framework to quantify network resilience and survivability, 2010.
[38] Hagin AA. Performability, reliability, and survivability of communication networks: System of methods and models for evaluation. 2002; 562–573.
[39] De CK. and Deconinck G. Analysis of state-of-the-art smart metering communication standards. *Proc. 5th Young Res. Symp.*, 2010; 1–6.
[40] Satterlee JD. Fundamental concepts of NMR in paramagnetic systems. Part II : relaxation effects. *Concepts Magn. Reson.*, 1990; 2: 119–129.
[41] Algirdas A, Jean-Claude L, Brian R, and Carl L. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Secur. Comput.*, 2004; 1(1): 11–33.
[42] Molina E, Jacob E, Matias J, Moreira N, and Astarloa A. Using software defined networking to manage and control IEC 61850-based systems. *Comput. Electr. Eng.*, 2015; 43: 142–154.
[43] Lee HY, Kwon YM, Shin JW, Lee WJ, and Chung MY. High availability WLANs based on software-defined networking. *AICT 2016 Twelfth Adv. Int. Conf. Telecommun. High*, no. c, 2016; 24–28.
[44] Molina E, Jacob E, and Astarloa A. Using OpenFlow to control redundant paths in wireless networks. *Netw. Protoc. Algorithms*, 2016; 8(1): 90.
[45] Dorsch N, Kurtz F, and Wietfeld C. Enabling hard service guarantees in software-defined smart grid infrastructures. *Comput. Networks*, 2018; 147: 112–131.
[46] Aydeger A. Software Defined Networking for Smart Grid Communications. 2016.
[47] Germano E. *et al.*, Capitalizing on SDN-based SCADA systems , " *2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag.*, 2015; 165–173.
[48] Mouftah HT. *et al.*, Communication architectures and technologies for advanced smart grid services. *Transp. Power Grid Smart Cities*, 2018; 217–245.
[49] Humayed A, Lin J, Li F, and Luo B. Cyber-physical systems security - A survey. *IEEE Internet Things J.*, 2017; 4(6): 1802–1831.
[50] Komninos N, Philippou E, and Pitsillides A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Commun. Surv. Tutorials*, 2014; 16(4): 1933–1954.
[51] Rehmani MH, Davy A, Jennings B, and Assi C. Software defined networks based smart grid communication: A comprehensive survey. *IEEE Commun. Surv. Tutorials*, 2019; 1–1.

[52] Dorsch N, Kurtz F, Georg H, Hägerling C, and Wietfeld C. Software-defined networking for Smart Grid communications: Applications, challenges and advantages. in *2014 IEEE International Conference on Smart Grid Communications*, SmartGridComm *2014*, 2014: 422–427.

[53] Dong X, Lin H, Tan R, Iyer RK, and Kalbarczyk Z. Software-defined networking for smart grid resilience: Opportunities and challenges. *Proc. 1st ACM Work. Cyber-Physical Syst. Secur. - CPSS '15*, 2015; 61–68.

[54] Haxhibeqiri J, De Poorter E, Moerman I, and Hoebeke J. A survey of LoRaWAN for IoT: From technology to application. *Sensors (Switzerland)*, 2018: 18(11).

Copyright © 2021 by the authors. This is an open access article distributed under the Creative Commons Attribution License (CC BY-NC-ND 4.0), which permits use, distribution and reproduction in any medium, provided that the article is properly cited, the use is non-commercial and no modifications or adaptations are made.