Received: 29 Sep 2024 | Revised: 06 Jan 2025 | Accepted: 20 Jan 2025 | Published: 28 Feb 2025
Volume 3(1) Pages 1-11 DOI: https://doi.org/10.56279/jicts.v3i1.120

JICTS
Journal of ICT Systems

SDN Based WLAN Resilience Enhancement for Smart Grid

Yona Andegelile

Department of Computer Science and Engineering, University of Dar es Salaam, Dar es Salaam, Tanzania

[1]Corresponding author
Email: andegelile.yona@udsm.ac.tz

Funding information

This work was self-funded.

Keywords

Software-defined networking
Network resilience
Odin framework

Abstract

In smart grid operations, a resilient wireless network ensures continuous communication, sustains network availability, and meets the demanding quality of service (QoS) requirements. However, currently, Wireless Local Area Networks (WLANs) face substantial challenges in maintaining seamless handover between Access Points (APs) during disruptions, which can compromise smart grid steadiness. This study aims to enhance WLAN resilience by proposing a Software Defined Networking (SDN)-based WLAN that leverages the Odin framework to address these challenges, ensuring availability, acceptable bandwidth, and latency for smart grid communications. We implemented and tested our solution in a physical laboratory setup using off-the-shelf network components, including APs, routers, and switches. Outcomes show that the SDN-based WLAN achieves 100% network availability, with a throughput of 8.93 $Mbps$ and a latency of 20 ms, effectively meeting the resilience and performance requirements of smart grids. Outstandingly, the solution utilizes standard APs and requires no modifications to end stations, making it a cost-effective and scalable approach for enhancing smart grid communication resilience. This work contributes to the development of more robust WLANs for smart grids, ensuring reliable performance in the face of network challenges, which will eventually improve smart grid service reliability.

1. Introduction

Wireless Local Area Network (WLAN) resilience refers to the ability of a network to maintain an acceptable level of service in the face of faults and challenges, which is typically measured by metrics such as network availability, minimum required bandwidth, and acceptable latency [1]. In the context of smart grids, where reliable communication is paramount, these

resilience metrics take on even greater significance. The transition from traditional electric grids to smart grids involves the deployment of numerous sensors, actuators, and communication devices along the grid, greatly increasing the demand for continuous and reliable communication [2]. To ensure safe and efficient operations, smart grid communication networks must meet stringent requirements, including over 99.5% availability, bandwidth exceeding 100 kbps, and latency under 4 seconds [3].

One of the primary challenges in WLANs for smart grids is the seamless maintenance of connectivity when an Access Point (AP) fails or experiences issues. In conventional wireless networks, end devices are required to reassociate with a new AP whenever the serving AP becomes unavailable, leading to service disruptions and potential performance degradation [4]. Given the critical nature of smart grid communications, these disruptions can have serious consequences for grid reliability.

Software Defined Networking (SDN) offers a promising solution to this problem by providing a flexible and programmable network architecture that can dynamically manage network resources and improve resilience [5]. The Odin framework, built on SDN principles, enables the creation of Virtual Access Points (VAPs), which allow devices to stay connected even when the physical AP is no longer available, effectively eliminating service interruptions caused by AP failures [6].

This paper proposes an SDN-based approach to enhancing WLAN resilience in smart grids by utilizing the Odin framework. Unlike traditional WLANs, our solution eliminates the need for end stations to connect to specific physical APs, thus ensuring continuous connectivity without disruptions. We demonstrate that our solution meets the stringent resilience requirements of smart grids, achieving 100% availability, 8.93 Mbps throughput, and 20 ms latency—performance metrics that surpass those of previous studies. Moreover, the approach leverages off-the-shelf APs and requires no modifications to end stations, making it a practical, scalable, and cost-effective solution for enhancing WLAN resilience in smart grid applications.

2. Related work

Recently, there has been noticeable researcher's focus on exploiting SDN capabilities to improve WLAN performance. SDN has generally been influential in many aspects of WLAN performance, including station's mobility management, accessibility management, retainability and general quality of service (QoS) [1][2]. For example, Nahida et al. [3] introduced logical umbrella access point, which uses SDN to improve WLAN capacity management, in which stations were relocated to different APs to efficiently balance traffic between APs, thereby avoiding overloading. Filho et al. [4] proposed a Software Defined Wireless Networking (SDWN) approach, in which a controller decides when to initiate the handoff process and chooses the AP that the client's device must connect. Their solution requires modification on the end stations to ensure they support open flow. Vestin [5] proposed an improved connectivity stability that guarantees WLAN network resilience. The study came up with SDN-enabled traffic control algorithms to improve connection reliability. The study indicates that SDN can enhance the stability of Split-MAC WLAN networks. By utilizing the SDN controller to manage handovers between access points, the study has shown that connection stability significantly improves, even under heavy congestion conditions. However, the study considered only on load-triggered end device relocations, in which the primary link gets disturbed. This is a rare case for smart grid since the nature of traffic is predictable.

Da Silva et al. [6] proposed Quality of Service (QoS) enhancements to improve WLAN resilience. The study utilized SDN ability to allow for the implementation of QoS improvements through intelligent traffic management at the MAC layer. This capability is particularly beneficial in WLAN environments where maintaining service quality is critical during high-demand periods. The study guarantees service availability in a congestion scenario, which is a rare case for a smart grid with predictable traffic patterns.

Other studies mostly focus on improving mobility management, specifically handover improvement when the station (STA) is moving from one AP coverage to another. However, smart grid STAs are stationary, hence requiring a solution that ensures service availability for stationary STAs.

3. Fundamental Concepts

3.1 Wireless communication networking

Heterogeneous communication architecture design for the smart grid [7] and International Telecommunication Union (ITU) standards [8] recommend using both wired and wireless communication transport technologies to effectively manage smart grid communication networks.. While the former uses cables to connect communicating devices, the latter uses electromagnetic waves to transfer information between devices [9]. The two technologies have different capacities, coverage, mobility support, and hardware requirements [10]. The choice of wireless communication technologies for a large part of the smart grid is attributed to the fact that the well-hardened radios may offer the most effective and economical solution when compared to wired options, such as underground optic fiber cable.

If a buried cable is damaged and requires repair or replacement, the costs can be high. Wireless systems are relatively maintenance-free, and, if maintenance becomes necessary, they are easily installed and maintained. Once installed, top-class wireless systems rarely need servicing. Among many available wireless technologies, IEEE 802.11 based wireless LAN has been proven to provide more robust, high-speed point-to-point, and point-to-multipoint communication for smart grid [11]. Specifically, 802.11a/g offers data rates up to 54 Mbps and comparatively broad coverage suitable for smart grid [12]. For this reason, we adopt 802.11a/g in this study.

3.2 WLAN resilience

AWLAN is a computer network model that uses wireless data connections between network nodes [13]. WLAN is defined by IEEE 802.11 and implemented at the physical and data link layer of the Open System Interconnect (OSI) model. A wireless network comprises of a control plane that is responsible for routing management, admission control, mobility control, and authentication of devices [11]. These control functions enable the network to efficiently and securely service wireless devices. The control functions manage and influence the way STA performs AP discovery, authentication, and association as fundamental processes for STA to attach to the WLAN [14]. These processes significantly impact the resilience of WLAN since the STA is required to undergo these processes every time they connect to the network, making it difficult to realize reliable service availability. Also, the selection of AP for which the STA should be connected is only influenced by signal strength, making it difficult to manage loading on the APs. The time spent in association and authentication affects the time that the services get interrupted when a serving AP fails, which negatively impacts WLAN resilience [15]. The service interruption negatively affects the smart grid communication network resilience requirement, including over 99.5% availability, bandwidth exceeding 100 kbps, and latency under 4 seconds [16], which can potentially affect smart

grid network management and grid network reliability.

3.3 SDN and Odin framework

SDN is a computer network architecture that separates the control functions of the network (control plane) from the forwarding functions (data plane) (Figure 1) [17]. The SDN architecture is made up of three conceptual planes, namely application plane, control plane, and data plane [18]. The control plane is responsible for determining the network management logic, such as implementing routing protocols, while the data plane is responsible for forwarding data based on the logic implemented on the control plane. This SDN architecture allows the management of the whole network infrastructure with the use of application programming interfaces (API) available in the SDN controller [19].

The Odin framework takes advantage of API availability in the SDN. It was first developed by Suresh et al. [20], and further enhancement by Zhao et al. [21] and Koastal et al. [22]. This approach

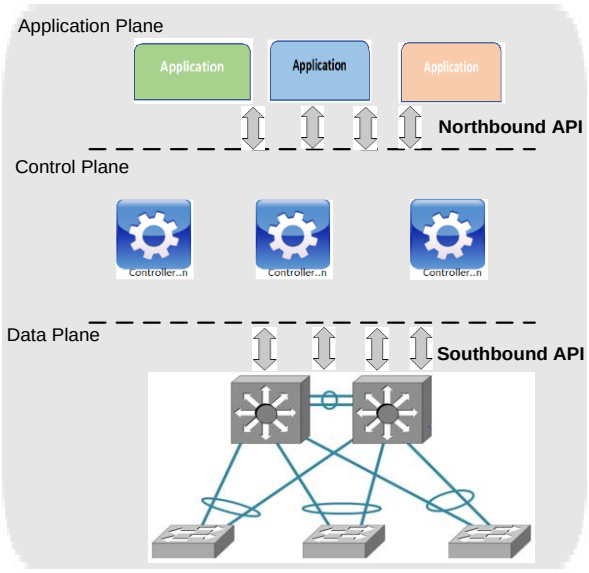

Figure 1. SDN architecture[17].

provides an optimized SDN based WLAN registration process. With the Odin framework, each STA has a unique Basic Service Set Identifier (BSSID) to connect to, creating the illusion of possessing its own AP. This client-specific AP is referred to as a Virtual Access Point (VAP). A physical AP thus hosts a VAP for each client connected through it. The VAP at minimum is comprised of STA's MAC address, IP address, VAP SSID, and BSSID [22]. The Odin Framework comprises Odin master that is attached with SDN controller and Odin client that is attached to each physical AP. The two components work together to realize virtual access points for each end station [22].

4. Proposed WLAN Resilience Algorithm

The proposed approach assumes that wireless network coverage and capacity planning in which all APs are provisioned with additional capacity to save extra traffic in an event when a nearby AP is challenged. The approach also assumes the failover APs availability is guaranteed when the serving AP has failed. The Odin master monitors the health of the Odin agent using PING (Packet Internet or Inter-Network Groper) messages. When the master does not receive four consecutive ping messages, it declares that the agent is down. It immediately triggers the mobility manager to relocate all VAP served under the agent to other APs. The selection logic of APs where abandoned VAPs get relocated depends on the utilisation of the APs and received signal quality levels by STA. The SDN controller changes flows on open flow switches in the physical switches and APs to reflect the new STAs relocation. The VAP migration is transparent to the STAs. The Odin Master keeps on monitoring the status of the failed agent. When the controller receives PING messages from the agent, it assumes that the failed AP is back, then it migrates back all STAs VAPs that were previously being served by the AP. Figure 2 is the flow chart summarizing the proposed approach algorithm.

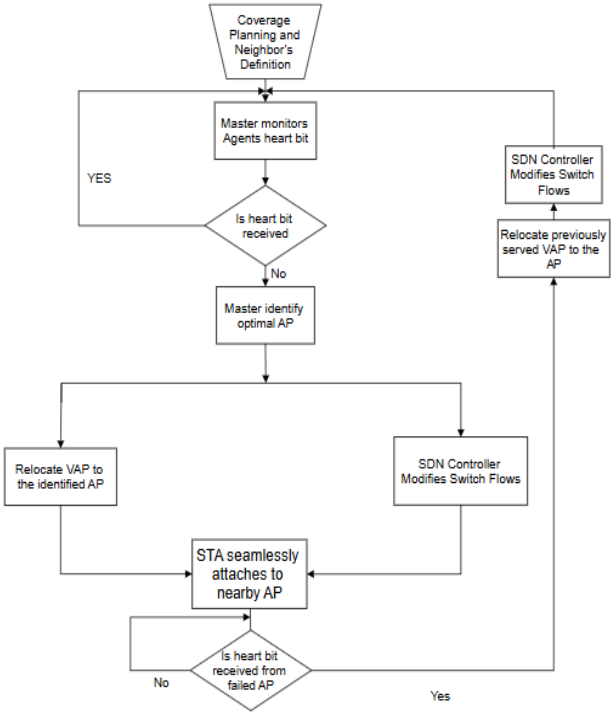

Figure 2. WLAN resilience algorithm.

The STA, Odin agent, and Odin master work together realize the overall WLAN resilience. Each component has its own function, captured in Figure 3 as STA use cases, in which the STA does two actions, one is making association with agents in the range and second send traffic when the association process is completed.

This Section presents the results obtained after data analysis or, for experimental research, after execution of the experiments. If this Section is presented alone the author is required to only show the results—and should not present and discuss the results simultaneously. When presenting results in Tables and Figures, JICTS recommends to highlight critical results.

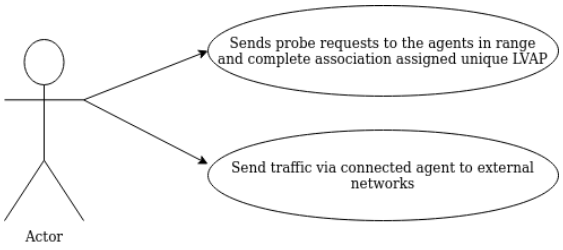

Figure 3. STA use case.

In essence, authors should not repeat or read contents of the Tables and Figures. We expect to see alarming results, such as those depicting trends or outperformance of a given method. Part of a typical results Section may read as follows:

Figure 4 is the Odin agent use cases, which implement the Wi-Fi split-MAC and VAP handling. They track client probe requests, inform the master, and communicate with the Odin Master over a control channel, also collecting statistics related to traffic and state of Aps.

The Odin Master, which act as OpenFlow application, uses information about the wireless network from the SDN Controller to manages the wireless part of the network as summarized in Figure 5. The logic to realize WLAN resilience was deployed in the Odin master and SDN controller.

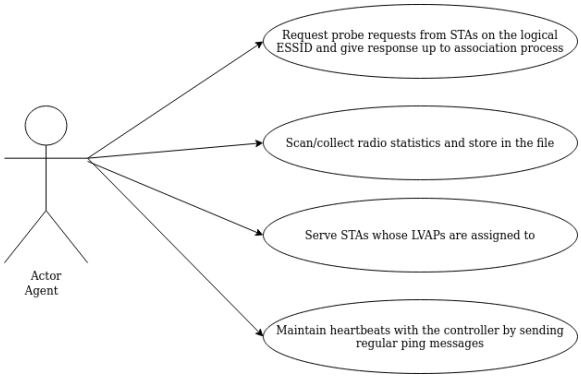

Figure 4. Odin agent use case.

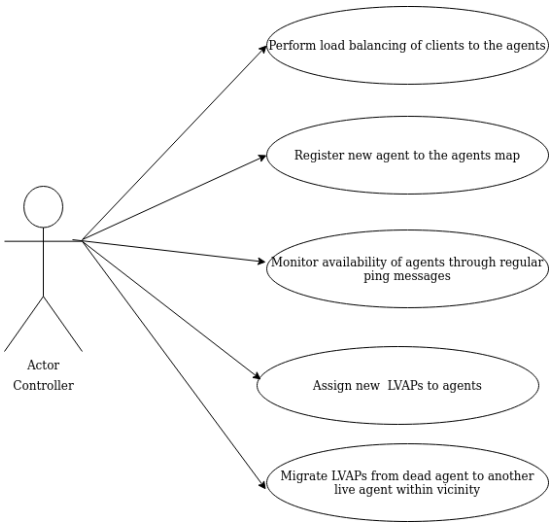

Figure 5: Odin master use case.

5. Experimental Setup

To validate the proposed resilience solution, the algorithm was deployed in a laboratory environment containing two APs, named AP5 and AP6, two STAs, three Cisco switches, and one Cisco router. Odin master and SDN controller were deployed in virtual machines that were hosted on a Linux computer, and virtualized using VirtualBox hypervisor. The physical AP used for the experiment was Netgear R6100. The detailed connectivity between the network elements is depicted in Figures 6, 7, and 8.

Packet loss or undelivered PING requests/responses can be managed by adjusting the threshold for the number of missed messages the ODIN master uses to determine that an agent is unreachable, prompting it to initiate a relocation action.

The two physical APs came up with a single logical ESSID. A web server was configured on a Windows computer configured in the same network as STA.

Figure 6. Prototype front view.

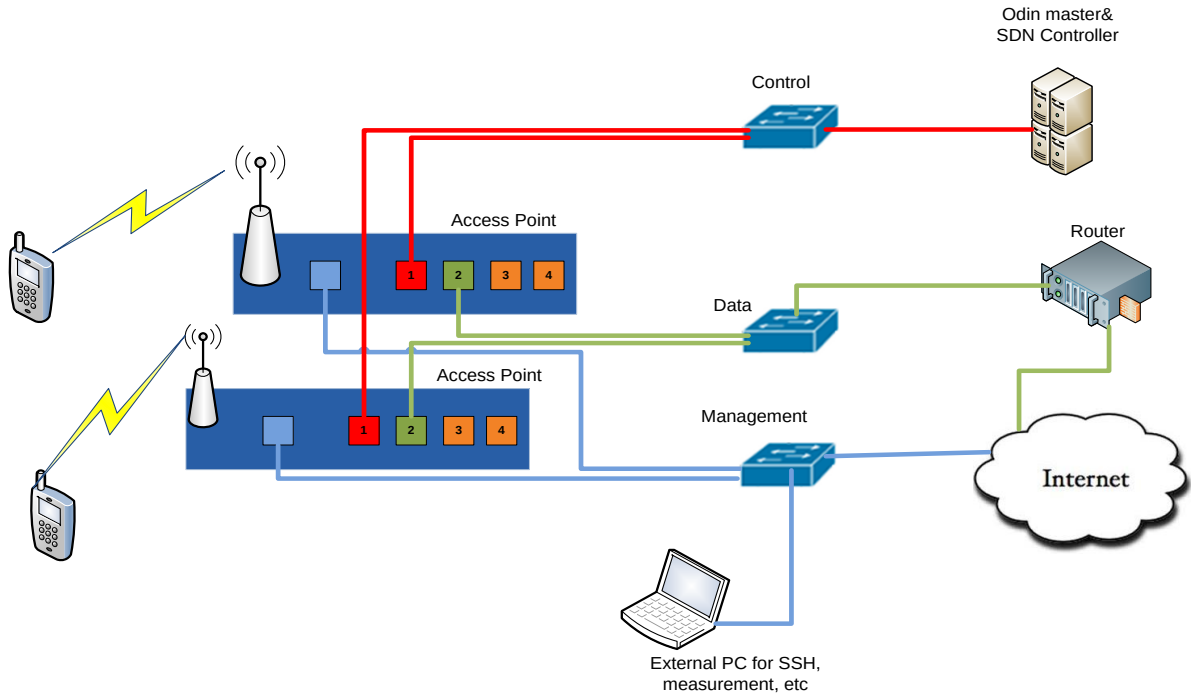

Figure 7. Laboratory experiment setup.

Figure 8. Prototype real view.

One physical access point (AP5) was configured with IP address 192.168.1.5 and another one (AP6) with 192.168.1.6. Odin agents were then recognized by these IPs. The STA was made to connect to the network and got allocated to AP with IP address 192.168.1.5, while its assigned IP address was 192.168.2.12. Figure 9 depicts the Odin master print events showing Odin agents registration, STA association, and VAP assignment.

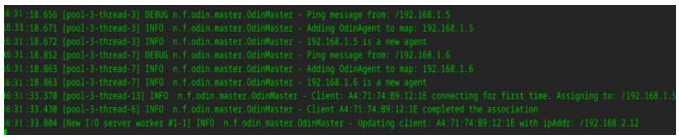

Figure 9. Agents STA registration.

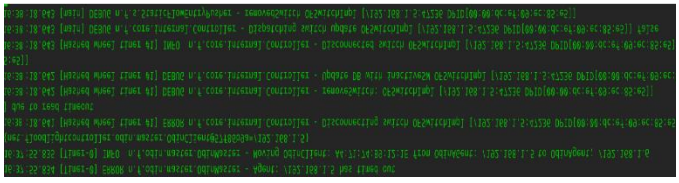

Figure 10. Serving AP failure scenario.

Figure 11. Throughput before relocation.

6. Results Discussion

The serving AP5 with IP address 192.168.1.5 was deliberately made to fail by switching off the power button of the AP. It was observed that the Odin master immediately detected the failure and relocated the client to a nearby, best-serving AP (AP6) (Figure 10).

It was observed that the throughput achieved by the STA was initially averaging at 8.93Mbps as (Figure 11). After relocating the STA to failover AP, the throughput did not degrade (Figure 12). These results were measured by the NetPerSec network performance measurement tool installed at the STAs.

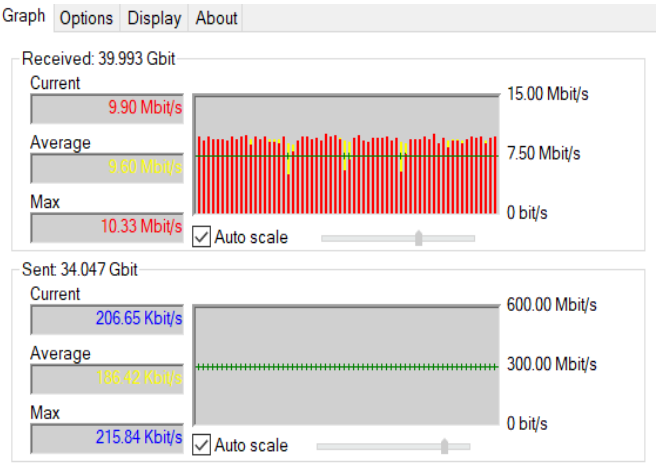

Figure 12. Throughput after relocation.

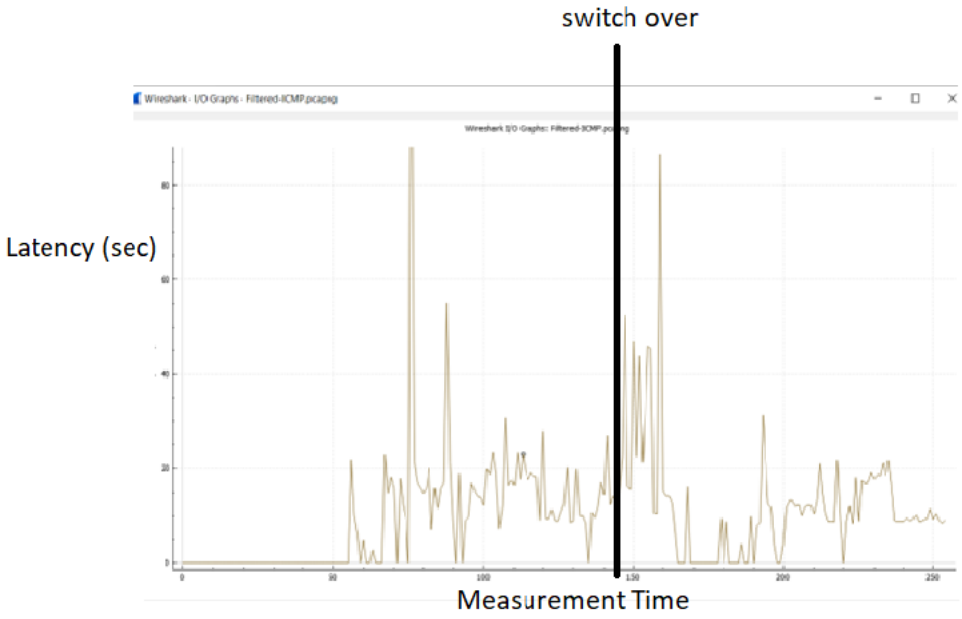

Figure 13. Latency trend during transition.

Furthermore, it was observed that, a latency averaged at 20ms could be obtained, with little flapping during switch over moment, but within smart grid requirements of 4 seconds (Figure 13).

Based on APs availability data as monitored by Odin master and service availability as measured from end STA, it was observed that one AP that did not fail, maintaining an availability of 100%, while the failed one obtained an average availability of 82.12% computed over the measurement duration.

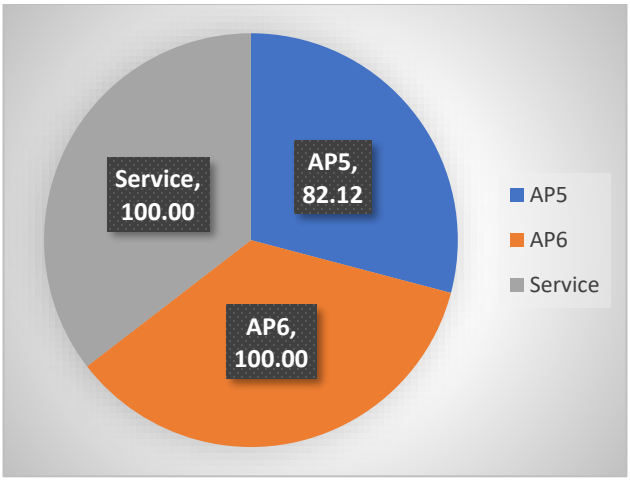

Figure 14. Overall availability for APs and Service.

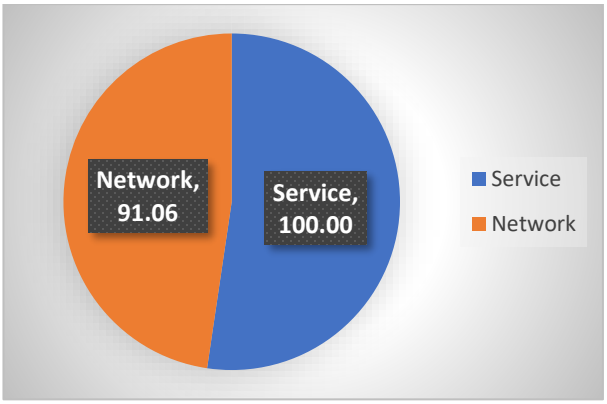

Figure 15. Overall availability for the Network and Service.

Since the STA was seamlessly relocated to working AP, the perceived service availability was 100% (Figures 14 and 15).

7. Conclusion

The study has demonstrated that the proposed SDN-based WLAN resilience solution can significantly improve wireless local area network service availability and maintain the key indicators without deterioration by seamlessly relocating abandoned stations when the serving access point is challenged. The solution is meant to satisfy smart

grid resilience demands in which corresponding devices are stationary in nature. The obtained availability of 100%, 8.93 Mbps of throughput and 20 ms of latency are superior results that satisfy smart grid requirements. The assurance of communication network reliability guarantees assured management of sensors and actuators deployed across the power grid, eventually ensuring reliable grid power services. Additionally, the study uses off-the-shelf APs, simplifying the efforts required to adopt the solution. Wireless communication network vendors can adopt the proposed architectural design and avail in the markets the products which are SDN and wireless network virtualization ready to simplify wireless network resilience deployment.

The proposed solution has been tested in a small-scale network with two Aps. But, since the logic to manage STA relocation is deployed in a centralized server, the solution can still apply regardless of the number of APs and STAs, so long as the connection to the centralized server is maintained, making the solution scalable and suitable for smart grid communication networks.

The adoption of this solution is key to the transformation of the power grid to the smart grid, which has several applications that are sensitive to specified communication network specifications.

ACKNOWLEDGEMENT

The author acknowledges members of the iGrid Research Team from the College of Information and Communication Technologies, University of Dar es Salaam, for their consistent moral support and constructive comments.

CONTRIBUTIONS OF CO-AUTHORS

Yona Andegelile	Conceived the idea and wrote the paper

REFERENCES

[1] S. Monin, A. Shalimov, and R. Smeliansky, "Chandelle: Smooth and Fast WiFi Roaming with SDN/OpenFlow," *A Poster Present. US Ignite*, pp. 31–32, 2014.

[2] H. Moura, G. V. C. Bessa, M. A. M. Vieira, and D. F. Macedo, "Ethanol: Software defined networking for 802.11 Wireless Networks," *Proc. 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manag. IM 2015*, pp. 388–396, 2015.

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

[4] 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, pp. 1–11, Nov. 2018.

[5] J. Vestin, A. Kassler, and J. Akerberg, "Resilient software defined networking for industrial control networks," in *10th International Conference on Information, Communications and Signal Processing (ICICS)*, pp. 1–5, 2015.

[6] A. S. Da Silva, P. Smith, A. Mauthe, and A. Schaeffer-Filho, "Resilience support in software-defined networking: A survey," *Comput. Networks*, vol. 92, pp. 189–207, 2015.

[7] A. Zaballos, A. Vallejo, and J. Selga, "Heterogeneous communication architecture for the smart grid," *IEEE Netw.*, vol. 25, no. 5, pp. 30–37, 2011.

[8] ITU-RadioCommuncation, "Annex 9 to Working Party 5A Chairman ' s report Elements for a working ducemnt towards a possible preliminary draft new report on utililty communication networks requirements," UTC América Latina, 2019.

[9] S. Kamble and B. R. Chandavarkar, "A Survey on Wired, Wireless, and Internet of Things Routing Protocols," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7, 2019.

[10] P. K. Ramalingam, Senthil P.; Shanmugam, "A Comprehensive Review on Wired and Wireless Communication Technologies and Challenges in Smart Residential Buildings," *Recent Adv. Comput. Sci. Commun.*, vol. 15, no. 9, pp. 1140–1167, 2022.

[11] IEEE, "IEEE Standard for Information technology--Telecommunications and information exchange between systems LAN and MAN--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2016," 2016.

[12] P. P. Parikh, M. G. Kanabar, and T. S. Sidhu, "Opportunities and challenges of wireless communication technologies for smart grid applications," in *IEEE PES General Meeting*, 2010, vol. 105, no. 4, pp. 1–7.

[13] M. M. Zanjireh, A. Shahrabi, and H. Larijani, "ANCH: A new clustering algorithm for wireless sensor networks," *Proc. - 27th Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2013*, pp. 450–455, 2013.

[14] Y. Andegelile, N. Mvungi, and M. Kissaka, "SDN Based High Availability Communication Network Architecture for Secondary Distribution Electric Power Grid," in *International Conference on Smart Grid (icSmartGrid)*, pp. 52–57, 2019.

[15] CISCO, “Ascertain Methods for 802 . 11 WLAN and Fast- Secure Roaming on CUWN,” 2024.

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

[17] 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.

[18] Y. Jarraya, T. Madi, and M. Debbabi, “A survey and a layered taxonomy of software-defined networking,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 4, pp. 1955–1980, 2014.

[19] P. Berde *et al.*, “ONOS,” in *Proceedings of the third workshop on Hot topics in software defined networking*, pp. 1–6, 2014.

[20] L. Suresh, J. Schulz-Zander, R. Merz, A. Feldmann, and T. Vazao, “Towards programmable enterprise WLANS with Odin,” *HotSDN’12 - Proc. 1st ACM Int. Work. Hot Top. Softw. Defin. Networks*, pp. 115–120, 2012.

[21] D. Zhao, M. Zhu, and M. Xu, “Supporting ‘One Big AP’ illusion in Enterprise WLAN: an SDN-based Solution,” in *2014 Sixth International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6, 2014.

[22] K. Košťál, R. Bencel, M. Ries, P. Trúchly, and I. Kotuliak, “High Performance SDN WLAN Architecture,” *Sensors*, vol. 19, no. 8, p. 1880, Apr. 2019.