Received: 01 Oct 2024 | Revised: 02 Dec 2024 | Accepted: 10 Dec 2024 | Published: 29 Dec 2024
Volume 2(2) Pages 81-106
DOI: https://doi.org/ 10.56279/jicts.v2i2.122

JICTS
Journal of ICT Systems

Hybrid Communication Architecture Based on Hierarchical Computing for Low Voltage Power Network Automation: A Case of Tanzania Electric Grid

Godfrey William Chugulu

Department of Electronics and Telecommunications Engineering, University of Dar es Salaam, Dar es Salaam, Tanzania

Corresponding author
Email: chugulu.godfrey@udsm.ac.tz

Funding information

This work is self-funded.

Keywords

Distribution Automation
Communication Architecture
End Devices
Low Voltage Power Network
Hierarchical Computing

Abstract

Utility companies in developing countries, such as Tanzania, have made significant strides in automating the generation, transmission, and primary distribution segments of their electrical grids. However, automation in the Low Voltage Power Network (LVPN) remains limited, primarily due to the absence of sensors, actuators, and a communication infrastructure needed for real-time data transfer. This lack of automation leads to inefficiencies and service disruptions for both utilities and consumers. The Smart Grid Focus Group (SGFG) identifies critical applications such as Advanced Metering Infrastructure (AMI), Distributed Energy Resource (DER) coordination, and Distribution Automation (DA) that are essential for LVPN automation, each with specific latency requirements. Existing communication architectures fail to meet these latency limits due to the unique challenges faced in developing countries. This paper proposes a hybrid communication architecture built on a three-level hierarchical computing model tailored for Tanzania Electric Supply Company Limited (TANESCO) and the LVPN environment. Implemented in a laboratory testbed with actual deployment devices, the system achieved an average latency of 7.059 ms, well below the 20 ms threshold necessary for AMI, DER, and DA. This promising result demonstrates the architecture's ability to effectively support LVPN automation, enhancing service delivery and operational efficiency in Tanzania's electrical grid.

1. Introduction

The economic growth of developing countries, including Tanzania, heavily depends on the reliability of their electric power supply. Many of these nations still rely on outdated, one-way legacy grids, which only facilitate power flow from generation points to consumers [1, 2, 3] . A fully functioning legacy power grid consists of three main components: generation, transmission, and distribution, both primary and secondary (Figure 1). The red-highlighted area in Figure 1 represents the Low Voltage Power Network (LVPN), which spans from the 400V distribution transformer to the final consumer. The LVPN is sometimes referred to as the secondary distribution network [2, 4].

Studies show that legacy power grids in developing countries typically include systems to monitor and control the generation, transmission, and primary distribution components of the grid. However, LVPNs often remain unmonitored, primarily due to the lack of Remote Terminal Units (RTUs) and field sensors that provide necessary protection and visibility [5, 6, 7]. While Supervisory Control and Data Acquisition (SCADA) systems are commonly installed to oversee the primary distribution network, the LVPNs are frequently excluded from such monitoring infrastructure. This absence of visibility and control in the LVPNs presents a significant challenge to effective grid management and undermines the reliability of the power supply in these regions [5, 8, 9].

Legacy power grids face several critical challenges, including lack of automated analysis, inadequate communication systems, limited control, and poor coordination between energy generation and consumption. These deficiencies lead to frequent power disruptions and blackouts, which undermine the ability of utility companies to provide reliable and consistent power supply [10, 11]. Furthermore, the absence of robust communication infrastructure in the LVPN increases the grid's vulnerability to outages and system failures [12, 13]. These challenges can be addressed through the transition to a smart grid (SG), which introduces advanced capabilities for monitoring, control, and optimization of power systems [1, 14, 15, 16].

SG leverages advanced communication infrastructure to monitor, coordinate, and optimize all components of the power system, improving reliability and efficiency [16, 17, 18]. Central to the SG's operation is a robust communication network that ensures stable, uninterrupted, and high-quality electricity service. This network integrates sensors, actuators along service lines, and smart meters at consumer sites to monitor energy usage, detect faults and perform service restoration [8, 19]. Two-way communication allows utility control centers to collect real-time data on power consumption while simultaneously transmitting operational information and control commands to the appropriate nodes [2, 20]. The existing literature lacks detailed insights into the design aspects of the communication architecture required to automate LVPNs in developing countries, a key factor in modernizing these electrical grids.

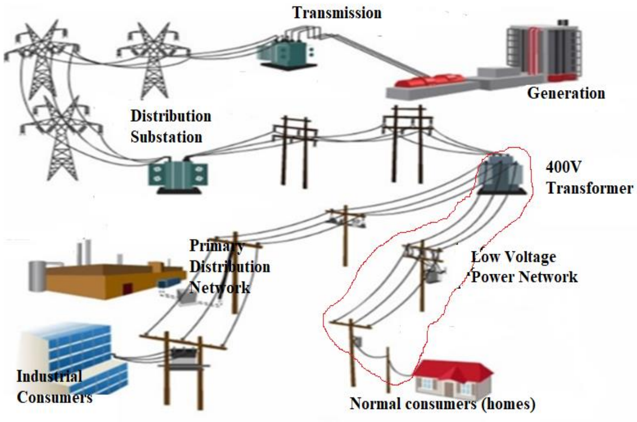


Figure 1. Parts of legacy power grid.

.

To enhance the efficiency of legacy grids, researchers have categorized the SG communication architecture into three key networks: Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN) (Figure 2). The NAN is sometimes referred to as the Field Area Network (FAN) when it connects field devices [21, 22, 23]. While most existing research has focused on monitoring and control at the WAN and HAN levels, it often treats the NAN merely as an Advanced Metering Infrastructure (AMI) network, neglecting its integration with field devices [24]. As a result, FAN remains the least explored [25]. These research setups are more suitable for developed countries, where LVPNs are well-structured and urban planning is more organized. In contrast, in developing countries, unplanned urbanization and poorly structured settlements complicate LVPN automation. This study aims to address this gap by designing an appropriate communication architecture for automating LVPNs in developing countries, an area currently lacking in the literature.

The Smart Grid Focus Group (SGFG) was established by the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) to address the communication and standardization needs of SG. The focus group’s primary functions are related to the development of global standards, guidelines, and frameworks to support the integration of Information and Communication Technologies (ICT) into power grids, ultimately enabling the transformation of legacy electrical systems into more efficient, reliable, and sustainable SGs [26].

SGFG emphasizes the need for installing end nodes for sensing and actuation within the low-voltage network, as well as a secure communication architecture to enable the transfer of data and control information for LVPN Automation [2, 13, 27]. Additionally, the SGFG outlines several critical smart grid (SG) applications essential for LVPN automation, including Advanced Metering Infrastructure (AMI), Distribution Automation (DA), Feeder Automation (FA), and the coordination of Distributed Energy Resources (DER) [28, 29, 30]. These applications, such as AMI, Distributed Feeder Automation (DFA), and DER coordination, must meet strict latency requirements as set by SGFG to ensure effective SG implementation. Any SG deployment must adhere to these latency standards to be considered successful. For LVPN automation, the required latencies for each application are summarized in Table 1. These latency values represent the maximum time allowed from the initial signal sent by a sensor or smart meter to the control node, and from the control node back to the actuator or responsible end node.

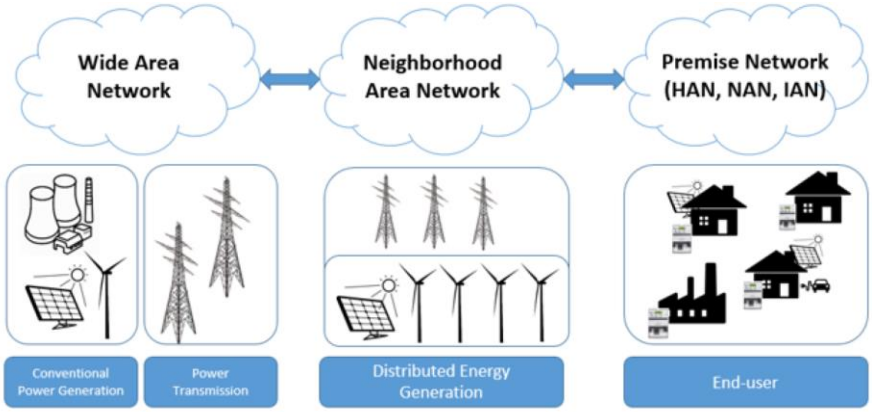

Wide Area Network
Neighborhood Area Network
Premise Network (HAN, NAN, IAN)
Conventional Power Generation
Power Transmission
Distributed Energy Generation
End-user

Figure 2. Communication networks in SG [12].

Table 1. Key applications for LVPN automation [13].

Application	Bandwidth	Latency
AMI	10 – 100 kbps	< 2s
DER	56 – 96 kbps	< 20ms
DFA	9.6 – 100kbps	< 100ms

Deploying an effective communication infrastructure for these SG applications in the LVPN is challenging due to the stringent latency requirements outlined in Table 1. However, this infrastructure is crucial for enabling automation within the LVPN. Automating processes in the LVPN will significantly accelerate faults detection and resolution, reducing the time required to address electrical faults compared to the current manual methods [13, 31].

Researchers have proposed different communication architectures utilizing a range of technologies. Some studies have suggested either centralized communication architectures based on SCADA systems [18, 32, 33] or employed communication technologies that are not well-suited for practical applications in developing countries power utilities (e.g., PLC, GSM and Bluetooth) [24, 34].

The proposed centralized architectures may be suitable for environments with fewer field devices; however, they are impractical for real utility companies that manage numerous field devices in the distribution network. The choice of Power Line Communication (PLC) does not adequately meet the specific needs of utilities aiming to automate LVPN, including fault detection and clearance. Moreover, when the power supply is interrupted, the PLC network also fails. Utility companies prefer to maintain control over the network components related to fault detection and clearance, making third-party technologies, such as GSM, WCDMA, and WiMAX, less desirable.

Other researchers have proposed decentralized or hierarchical architectures [35-37]Click or tap here to enter text. Click or tap here to enter text.. However, these designs did not fully address automation in the LVPN, particularly fault detection and clearance. They also overlooked the complexities introduced by numerous sensors and Intelligent Electronic Devices (IEDs) involved. While previous work utilized a two-level hierarchy, this study introduces a third level that enables end nodes to perform basic computing functions. Furthermore, it incorporates Software Defined Networking (SDN) into the architectural design, allowing for seamless configuration of numerous end nodes during faults and ensuring the maintenance of service level parameters, such as bandwidth and latency [38, 39].

This study builds on the work by Chugulu et al. [13], who proposed a practical communication architecture for automating LVPNs. The key distinction in this study is the specification of critical communication design criteria that enable the architecture to handle large volumes of data within the LVPN. To overcome the challenges posed by communication technologies discussed in the literature, this study employs a hybrid approach, integrating both wired and wireless technologies. Additionally, to prevent network overloads from transmitting raw data, the proposed architecture incorporates hierarchical computing, leveraging edge, fog, and cloud computing to efficiently process and manage data

This paper presents key communication architecture design requirements and features that enable the proposed architecture to facilitate LVPN automation within latency limits. It introduces a novel hybrid communication architecture for LVPN automation, specifically designed for developing countries. It integrates hierarchical computing to optimize data flow and decision-making across different levels of the network, ensuring efficient operation even in resource-constrained environments. The proposed architecture combines both centralized and decentralized communication approaches, enhancing reliability and scalability for LVPN automation. By focusing on the unique challenges of developing countries, such as limited infrastructure and network complexity, the paper offers practical solutions that can improve the resilience and performance of LVPN contributing to more reliable and sustainable energy systems.

2. Materials and Methods

2.1 Communication Architecture Requirements Specifications

The current study employed a mixed-methods approach. One method included conducting feasibility studies and gathering requirements through interviews and investigative questions. Another method focused on technical design and analysis. Throughout the research process, a Challenge Driven Education (CDE) approach was applied, ensuring that every stage from problem identification to solution validation actively involved key stakeholders from the electrical power grid sector and academia.

The requirements and data collected for the architecture development in this study were analyzed using a variety of methods and tools tailored to the specific characteristics of the data. Qualitative data were gathered from the Tanzania power utility company (TANESCO) through interviews, questionnaires, focus group discussions, and site visits, with an emphasis on capturing expert opinions. To analyze this qualitative data, a deductive codebook thematic analysis was employed, which is well-suited for extracting subjective information, such as participants’ experiences, views, and opinions. The use of interviews, questionnaires, focus group discussions, and site visits was essential to the data collection process, as these methods facilitated the acquisition of in-depth insights from experts. This approach was particularly important given the study's focus on obtaining detailed, qualitative perspectives regarding the LVPN, where expert knowledge plays a critical role in understanding the challenges and opportunities for automation. Appendix A shows questionnaire/guided interview document that experts from TANESCO responded to.

Simultaneously, a comprehensive and systematic document review was conducted to analyze qualitative data from secondary sources relevant to this study. The reviewed materials included published research, technical manuals from the utility company, technology standardization documents, white papers from technical forums, and official publications from globally recognized organizations. This review provided valuable insights into existing global solutions and helped identify gaps in the literature, which were crucial for informing the design of the proposed communication architecture.

As is well known, any research involving data collection and analysis is susceptible to various potential sources of bias and error, which can impact the quality and accuracy of the results. In this study, since most of the data for architecture design was sourced from TANESCO, several measures were implemented to ensure the accuracy and reliability of data collection and analysis processes. These measures included random sampling of engineers for interviews, comprehensive data cleaning procedures to ensure proper scrutiny and accountability, and the use of cross-validation techniques to assess the robustness of the analysis. These methods helped mitigate potential biases and errors, enhancing the credibility of the findings.

The quantitative data collected were analyzed using a range of methods and key analysis tools. Microsoft Excel was utilized to clean and format the Advanced Metering Reading (AMR) data and the tabular LVPN transformer data obtained from TANESCO, both of which were essential for modeling the LVPN data network. As a versatile tool, Microsoft Excel facilitated the cleaning and preprocessing of tabular data, which included tasks such as removing duplicates, correcting errors, standardizing formats, addressing missing values, and transforming the data into a more structured and usable format for analysis.

Quantum Geographic Information System (QGIS) was employed to analyze raw shapefile data from TANESCO, extracting critical information for the design of the communication architecture, including customer locations and the reconfiguration of the LVPN wiring within the study area. QGIS is an open-source software platform widely used for geospatial data analysis, mapping, and cartography. It enables users to create, edit, visualize, analyze, and interpret geographic data, providing valuable tools for spatial analysis and decision-making in the context of infrastructure planning.

InSSIDer was used to assess the existing Wi-Fi networks, providing essential data for access network design and validating WLAN band allocation information from the Tanzania Communications Regulatory Authority (TCRA). InSSIDer is a powerful network scanning and Wi-Fi analysis tool that enables users to monitor, troubleshoot, and optimize wireless networks. It offers comprehensive insights into nearby Wi-Fi networks, including signal strength, channel usage, security protocols, and network congestion, making it invaluable for ensuring efficient and reliable wireless network performance.

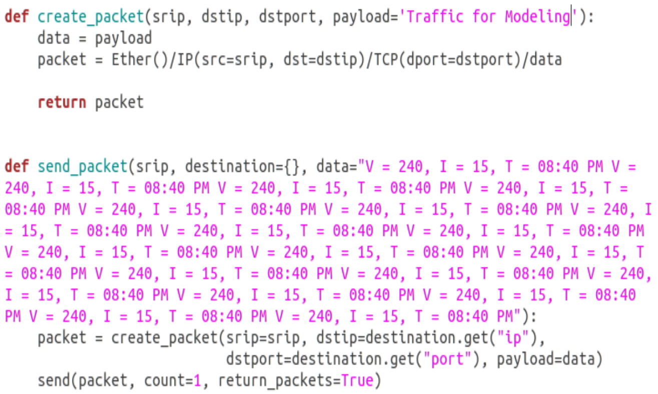
Furthermore, Mininet-WiFi through Python programming was employed to model the text-based smart meter data (AMR data) from TANESCO into IP packets/frames, with packet size details vital for dimensioning and bandwidth considerations in the design phase of the architecture. Mininet-WiFi is an extension of Mininet, a popular network emulator that allows the creation and testing of virtual networks to model and experiment with wireless communication protocols, network topologies, and performance evaluations in a simulated environment.

Table 2 presents sample text-based historical AMR meter reading data collected from TANESCO after being cleaned and formatted by Excel. Meter readings were taken every 20 minutes and transmitted to the utility's AMR central system. This data was subsequently analysed and modelled using Python programming within the Mininet-WiFi emulator to determine the IP packet size, which was critical for network capacity planning.

In the communication architecture, all transmitted data are in an IP-based format, requiring the conversion of text-based data into IP packets for accurate size assessment. An algorithm was developed to transform the text-based AMR data into IP packets, enabling analysis of their actual size. This conversion was essential for precise network dimensioning. Figure 3 illustrates the process of modeling text-based AMR data into IP packets using the Mininet-WiFi tool through Python programming. Since the text-based data consist of routine historical information, the modeling was designed to ensure efficient packet transmission via the Transmission Control Protocol within the network.

Table 2. Real TANESCO AMR meter data.

Date/Time	Phase A	Phase B	Phase C
1/1/2022 0:00	173.31 A	129.02 A	165.98 A
1/1/2022 0:20	173.61 A	126.52 A	161.82 A
1/1/2022 0:40	173.84 A	116.62 A	168.70 A
1/1/2022 1:00	162.95 A	116.17 A	173.84 A
1/1/2022 1:20	157.59 A	113.37 A	160.16 A
1/1/2022 1:40	164.77 A	119.04 A	152.83 A
1/1/2022 2:00	169.30 A	110.73 A	142.85 A
1/1/2022 2:20	162.12 A	110.73 A	141.49 A
1/1/2022 0:00	241.40 V	242.82 V	241.67 V
1/1/2022 0:20	240.28 V	241.81 V	240.66 V
1/1/2022 0:40	240.69 V	242.27 V	240.88 V
1/1/2022 1:00	240.73 V	242.15 V	240.99 V
1/1/2022 1:20	240.42 V	241.76 V	240.88 V
1/1/2022 1:40	240.87 V	242.36 V	241.42 V
1/1/2022 2:00	241.81 V	243.32 V	242.33 V
1/1/2022 2:20	242.60 V	244.03 V	243.06 V

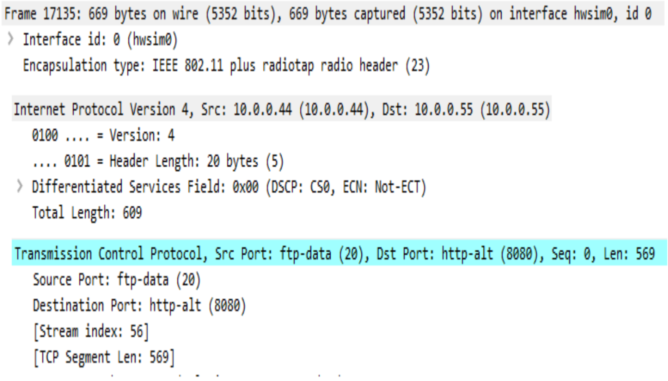


```
def create_packet(srip, dstip, dstport, payload='Traffic for Modeling'):
    data = payload
    packet = Ether()/IP(src=srip, dst=dstip)/TCP(dport=dstport)/data

    return packet


def send_packet(srip, destination={}, data="V = 240, I = 15, T = 08:40 PM V =
240, I = 15, T = 08:40 PM V = 240, I = 15, T = 08:40 PM V = 240, I = 15, T =
08:40 PM V = 240, I = 15, T = 08:40 PM V = 240, I = 15, T = 08:40 PM V = 240, I
= 15, T = 08:40 PM V = 240, I = 15, T = 08:40 PM V = 240, I = 15, T = 08:40 PM
V = 240, I = 15, T = 08:40 PM V = 240, I = 15, T = 08:40 PM V = 240, I = 15, T
= 08:40 PM V = 240, I = 15, T = 08:40 PM V = 240, I = 15, T = 08:40 PM V = 240,
I = 15, T = 08:40 PM V = 240, I = 15, T = 08:40 PM V = 240, I = 15, T = 08:40
PM V = 240, I = 15, T = 08:40 PM V = 240, I = 15, T = 08:40 PM"):
    packet = create_packet(srip=srip, dstip=destination.get("ip"),
                           dstport=destination.get("port"), payload=data)
    send(packet, count=1, return_packets=True)
```

Figure 3. Text-based AMR data modeling to IP packets in mininet-WiFi.

The output IP packet/frame with AMR reading data from the algorithm was captured and analyzed in Wireshark tool. Wireshark is a popular open-source network protocol analyzer used for monitoring and analyzing network traffic in real-time. Figure 4 displays a screenshot of the Wireshark analysis window, highlighting that the total length of the frame is 669 bytes. It offers a detailed view of the frame as captured and analyzed within the software. This frame size was a crucial part in network capacity design.

To design an effective and practical architecture for LVPN automation, this study analyzed the actual TANESCO LVPN. TANESCO provided raw shapefile data, including customer locations and LVPN wiring details, such as distribution service lines and transformer placements. Using QGIS, these data were reconstructed to extract meaningful insights. Figure 5 showcases the redrawn LVPN in QGIS, highlighting customers and end node locations to optimize coverage and capacity planning.



```
Frame 17135: 669 bytes on wire (5352 bits), 669 bytes captured (5352 bits) on interface hwsim0, id 0
› Interface id: 0 (hwsim0)
  Encapsulation type: IEEE 802.11 plus radiotap radio header (23)

 Internet Protocol Version 4, Src: 10.0.0.44 (10.0.0.44), Dst: 10.0.0.55 (10.0.0.55)
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 609

 Transmission Control Protocol, Src Port: ftp-data (20), Dst Port: http-alt (8080), Seq: 0, Len: 569
   Source Port: ftp-data (20)
   Destination Port: http-alt (8080)
   [Stream index: 56]
   [TCP Segment Len: 569]
```

Figure 4: Payload size of routine historical data containing 20 readings.

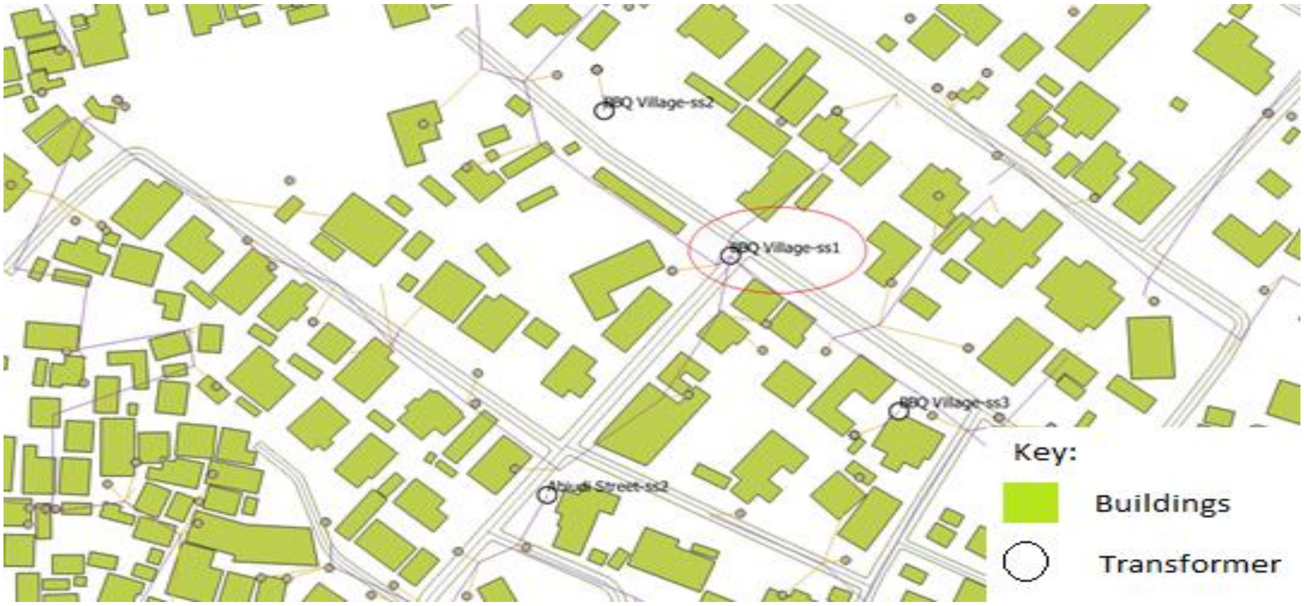


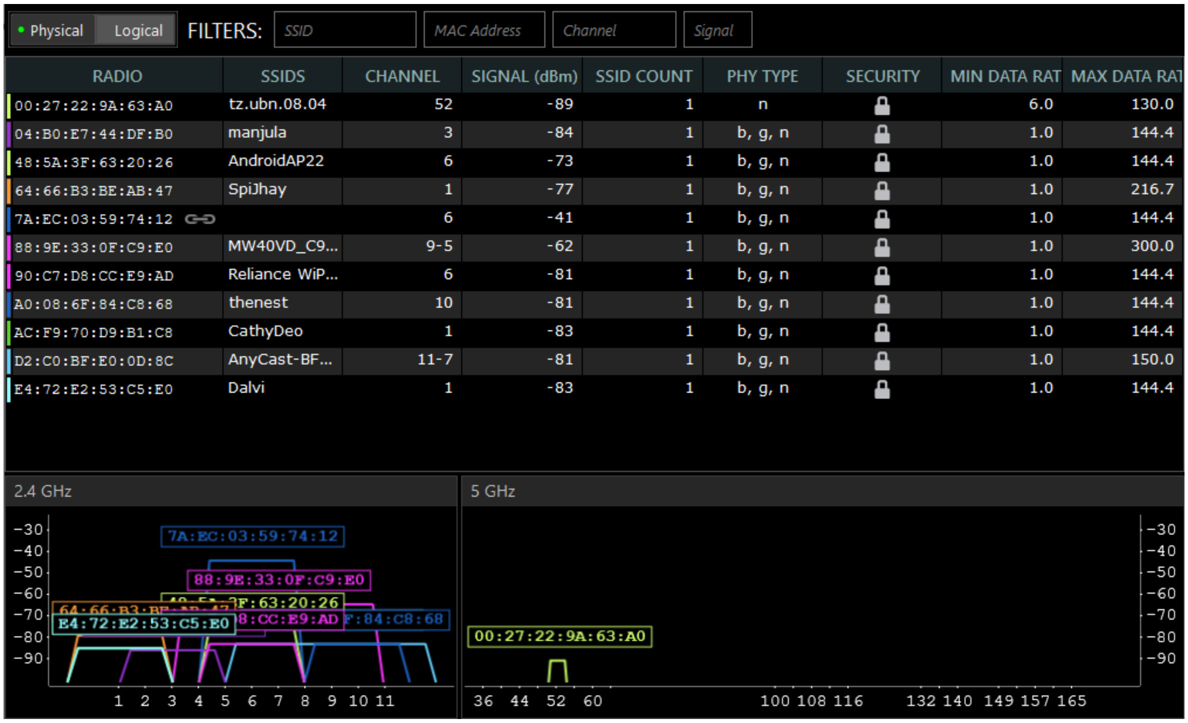
Figure 5: Study area LVPN analysis in QGIS.

Reconstructing the service area was crucial for effective design of the network and also validation of the shapefile data collected. It is essential to accurately identify the locations of customers, which indicate where smart meters are situated, as well as the locations of sensors, actuators, transformers, reclosers, and other devices. Ensuring that all these components receive adequate coverage is vital for seamless communication.

To effectively design a WiFi-based access network, it is essential to understand the existing WiFi networks and other technologies operating on the same channels to avoid interference and ensure reliable communication. Figure 6 illustrates the analysis of these existing WiFi networks in the study area, a critical step in planning channel allocations for the access network.

The key findings from the analysis with inSSIDer revealed that the 5 GHz band was largely underutilized, with only one location in the entire study area using a single channel. In contrast, the 2.4 GHz band exhibited moderate utilization, but the signal strength of existing networks was generally average, with most signals falling below -80 dBm. The primary channels in use for the 2.4 GHz band were channels 1, 3, 6, and 11. Furthermore, nearly all existing networks operated on the PHY type IEEE 802.11b/g/n. This information was crucial for effective planning to identify channels which minimize interference.

The 802.11 standard specifies 14 channels, each with a width of 20 MHz, within the 2.4 GHz industrial, scientific, and medical (ISM) band. Devices compliant with 802.11b/g/n can operate in this ISM band, but the availability of channels varies across the countries as dictated by local authorities. In Tanzania, the TCRA permits channels 1 through 14 in the 2400–2500 MHz range. This configuration provides three non-overlapping channels: 1, 6, and 11. Additionally, channels 2, 8, and 14 form another set of non-overlapping channels. However, due to the overlapping nature of most channels in the 2.4 GHz band, these channels were not deployed in areas with a high density of 802.11 users and devices.



RADIO	SSIDS	CHANNEL	SIGNAL (dBm)	SSID COUNT	PHY TYPE	SECURITY	MIN DATA RAT	MAX DATA RAT
00:27:22:9A:63:A0	tz.ubn.08.04	52	-89	1	n	🔒	6.0	130.0
04:B0:E7:44:DF:B0	manjula	3	-84	1	b, g, n	🔒	1.0	144.4
48:5A:3F:63:20:26	AndroidAP22	6	-73	1	b, g, n	🔒	1.0	144.4
64:66:B3:BE:AB:47	SpiJhay	1	-77	1	b, g, n	🔒	1.0	216.7
7A:EC:03:59:74:12		6	-41	1	b, g, n	🔒	1.0	144.4
88:9E:33:0F:C9:E0	MW40VD_C9...	9-5	-62	1	b, g, n	🔒	1.0	300.0
90:C7:D8:CC:E9:AD	Reliance WiP...	6	-81	1	b, g, n	🔒	1.0	144.4
A0:08:6F:84:C8:68	thenest	10	-81	1	b, g, n	🔒	1.0	144.4
AC:F9:70:D9:B1:C8	CathyDeo	1	-83	1	b, g, n	🔒	1.0	144.4
D2:C0:BF:E0:0D:8C	AnyCast-BF...	11-7	-81	1	b, g, n	🔒	1.0	150.0
E4:72:E2:53:C5:E0	Dalvi	1	-83	1	b, g, n	🔒	1.0	144.4

Figure 6: WiFi networks analysis by in SSIDer strengths.

Appendix B presents the final specifications for the communication architecture. These specifications serve as essential guidelines for designing and implementing the LVPN automation architecture, with a focus on efficient faults detection and service restoration. The key contribution of the current study is the outlined practical requirements that a power utility company can readily deploy.

2.2 Communication Architecture Design Features

To enable efficient automation in LVPN, the communication architecture incorporates several fundamental properties. It is designed to optimize network bandwidth utilization through a hierarchical processing model (edge, fog, and cloud), which allows for segmentation and clustering. Data from end nodes, such as sensors, smart meters, and IEDs, must first undergo local pre-processing before being transmitted to the designated part of the architecture. This approach prevents the architecture from becoming overwhelmed with raw data, which can lead to excessive network bandwidth and high computing resource usage. The initial processing at the end node is known as edge computing.

The cluster controlling unit is responsible for fog computing, managing all automation within a cluster. It also enables inter-cluster communication through neighboring fog devices. The top layer of the architecture, known as cloud computing, oversees the entire network and is equipped with high-performance computing resources and substantial storage capacity. In this study, fog computing is implemented at the transformer level, while cloud computing is hosted at the utility's data and control center. Figure 7 illustrates how hierarchical computing and clustering are implemented in the designed architecture.

Each cluster encompasses all sensors, smart meters, and actuators/IEDs within the electrical network served by LVPN distribution transformer in the area. All devices in the access network are installed at the transformer, ensuring reliable power availability and providing a centralized point for security.

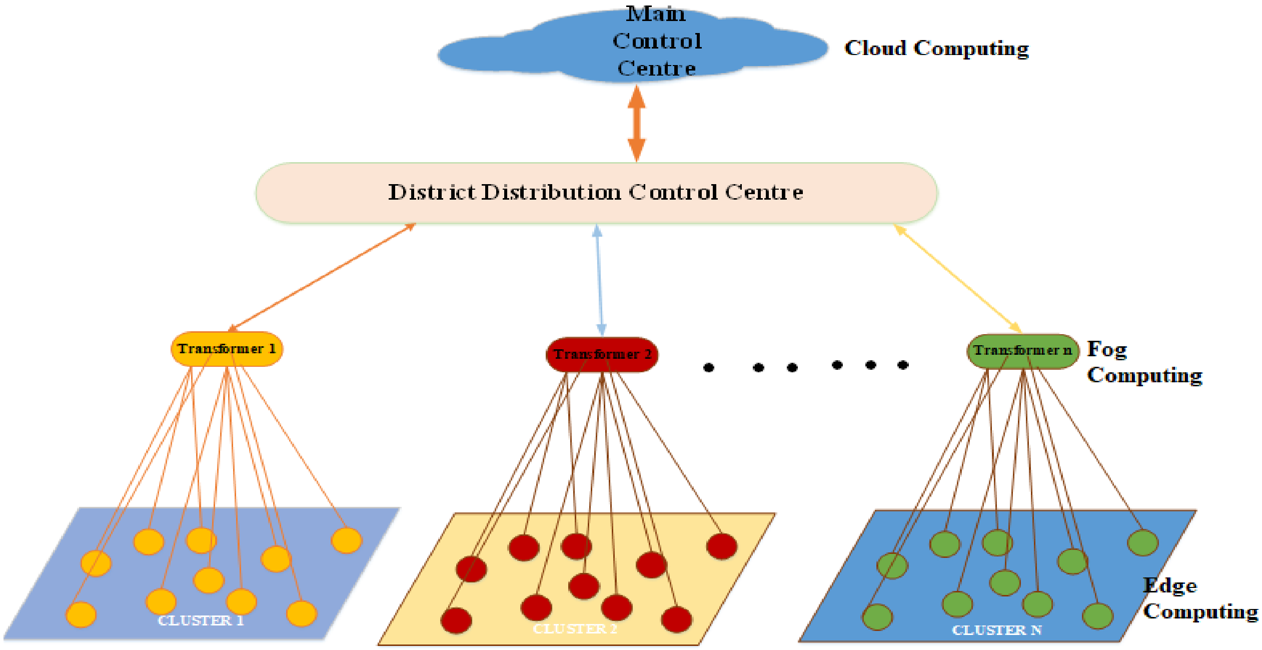


Figure 7. Architecture design based on Clustering and Hierarchical Computing.

The communication architecture is divided into two main components: the access network and the core network. The access network hosts end nodes, such as smart meters, sensors, and actuators that perform edge computing, along with cluster controlling nodes that execute fog computing. In contrast, cloud computing occurs within the core network, where extensive data processing takes place. This core network houses large servers, databases, and devices equipped with high computing capabilities. In most utility companies even in developing countries, core network is already properly designed and implemented.

Hybrid communication technologies have been integrated into the communication architecture. WLAN (WiFi) provides wireless network coverage for end nodes in the access network, while Un-Twisted Pair (UTP) cables, terrestrial microwave point-to-point (P2P) links, and fiber optics facilitate data transmission within the architecture. Whenever possible, the architecture leverages existing infrastructure deployed by the utility company to minimize implementation costs. In this context, the existing fiber optic cable network serves as the preferred backbone technology for data transmission.

Figure 8 illustrates the communication technologies implemented across various layers of the architecture, showcasing its hybrid nature through the integration of both wireless and wired communication methods. Smart meters, sensors, and actuators transmit historical data to the fog node at the transformer in a timely manner, preventing network congestion and ensuring efficient processing by the fog processor. During faults, all end nodes immediately relay data, necessitating that they be equipped with small processing units capable of analyzing the sensed data and identifying faults. The fog node features a database for temporarily storing this data from the end nodes, which is then analyzed and aggregated into larger batches before being sent to the control center. Each data entry is source-identified and time-stamped for accurate tracking.

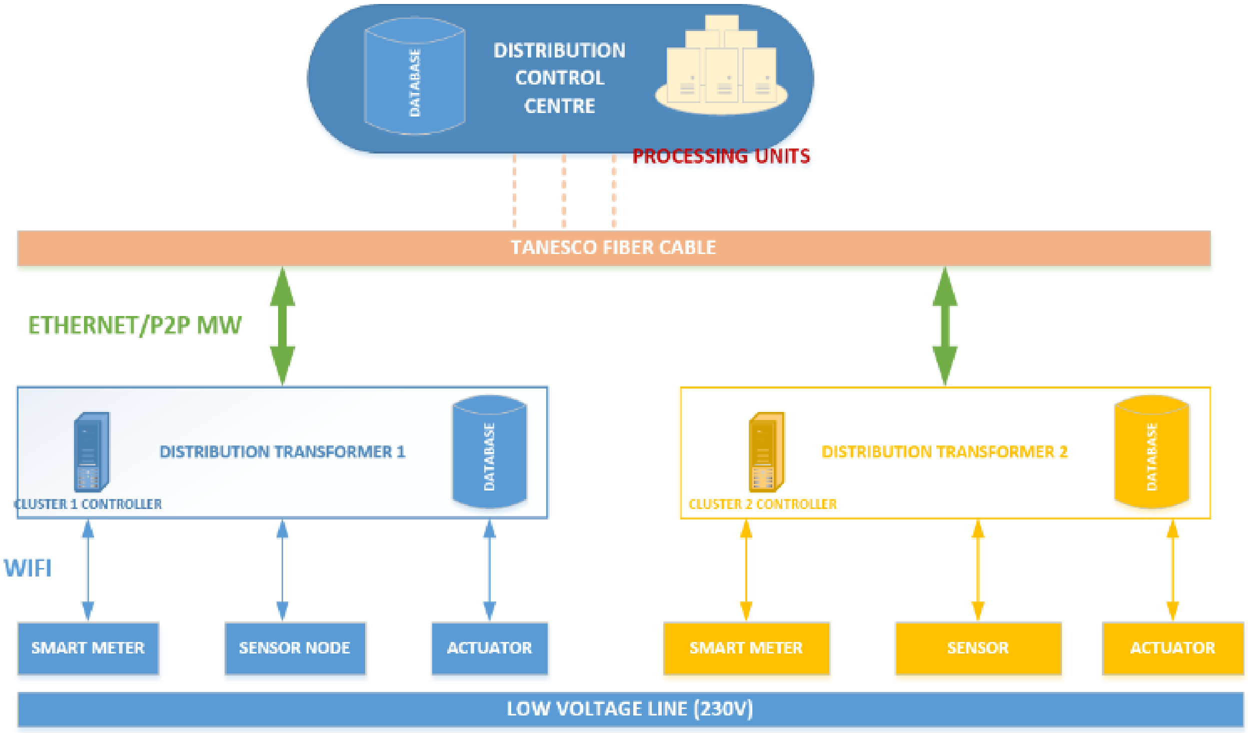


Figure 8: Hybrid communication technologies deployed in the architecture.

Figure 9 illustrates the flowchart outlining the preferred transport technology choices from the transformer to the control center (CC). This preference is determined by the location of the CC and the points of presence for fiber optic cables.

The access network coverage area was designed following principles from cellular network design to ensure continuous and reliable coverage. The area is divided into hexagonal cells for optimal distribution. WLANs operate using the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. As the number of concurrent access nodes increases, the likelihood of wireless packet collisions also rises, which can slow down network performance. To mitigate this issue, this study deployed three directional outdoor access points (APs) to serve end nodes, effectively reducing the potential for packet collisions. Figure 10 illustrates how the LVPN is segmented into clusters, specifically highlighting Cluster 1, which is further divided into three sectors served by powerful access points AP1, AP2, and AP3. Different non-overlapping channels are assigned for APs in both 2.4 GHz and 5 GHz bands so as to achieve interference-free communication. To extend coverage, these APs are directional and equipped with powerful external antenna.

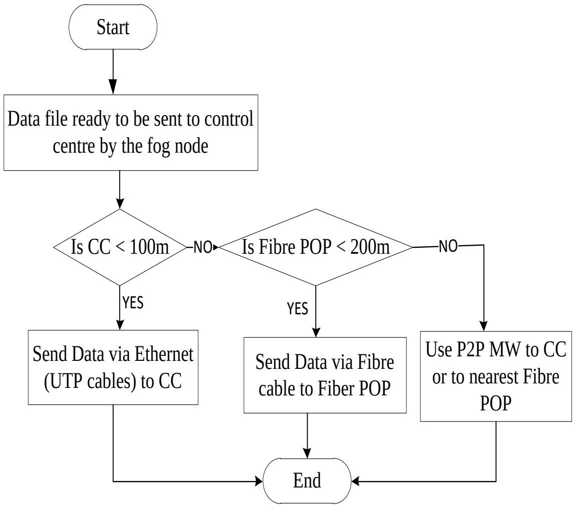

Start
Data file ready to be sent to control centre by the fog node
Is CC < 100m
NO
Is Fibre POP < 200m
NO
YES
YES
Send Data via Ethernet (UTP cables) to CC
Send Data via Fibre cable to Fiber POP
Use P2P MW to CC or to nearest Fibre POP
End

Figure 9: Communication technology choice based on control center and Fibre points of presence locations.

To strengthen the robustness of the access network and support a large number of end nodes, SDN features have been integrated into the WLAN-based access network. Within the ODIN framework, the SDN controller communicates with WLAN controller and access points (APs). Additionally, the SDN controller connects to SDN-capable switches, which interconnect the APs in clusters through the OpenFlow protocol's North Bound Interface (NBI). This setup is essential for effective traffic management during failures and faults. Figure 11 illustrates the integration of SDN into the legacy networking framework within the access network.

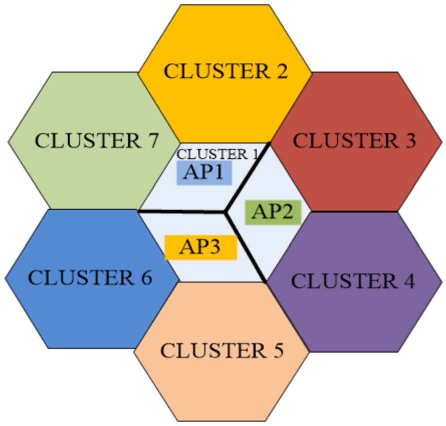


Figure 10: Access network coverage area based on cellular design.

This section has outlined the proposed communication architecture for Low Voltage Power Network (LVPN) automation, highlighting the integration of edge, fog, and cloud computing to enhance network efficiency and reliability. The hierarchical model optimizes bandwidth utilization and manages data flow from end nodes such as smart meters and sensors through local edge pre-processing to reduce congestion. The cluster controlling unit facilitates real-time fault management via fog computing, while the cloud layer at the utility's control center enables extensive data processing and storage. By utilizing hybrid communication technologies, such as WLAN, UTP

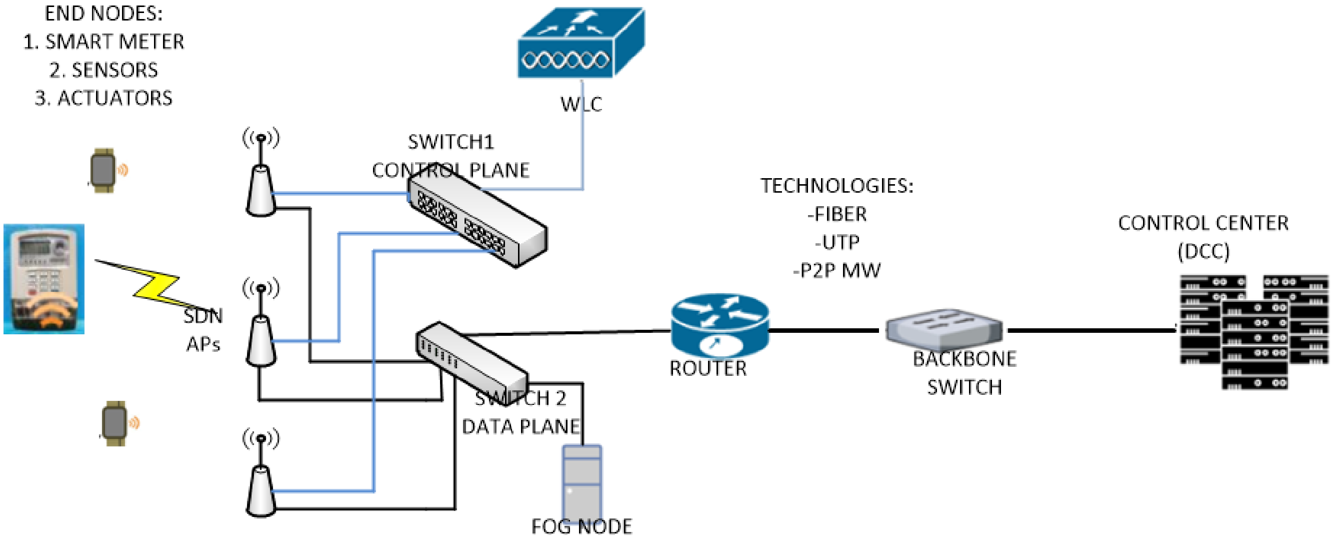


Figure 11. SDN based access network.

cables, microwave links, and fiber optics, the architecture maximizes existing infrastructure, reduces costs, and ensures reliable connectivity. Additionally, the incorporation of Software Defined Networking (SDN) improves traffic management during faults, supported by the ODIN framework for seamless communication among network components, addressing current challenges and paving the way for future advancements in LVPN automation.

3. Architecture Laboratory Deployment

To validate and evaluate the performance of the proposed design, a laboratory testbed was established based on the specifications and features outlined in Section 2.

3.1 Testbed Requirements

The communication architecture testbed for the LVPN automation comprises SDN capable wireless routers (APs), legacy 802.11 APs, Raspberry Pi (fog node), SDN Controller, Data Switch, Control Switch and a PC which act as data center receiving cluster updates regularly. The testbed hardware requirement are as follows:

i. The setup utilizes wireless routers (APs) equipped with the Atheros chipset, specifically employing the Ath9k wireless driver. While any router with the Ath9k driver can be used, the Netgear 6100 is selected for this demo. The Ath9k driver is advantageous because it can be patched to modify the mask of received 802.11 frames, enabling the access point to send layer-2 ACKs. The ODIN framework employs debugging tools to create a file at /sys/kernel/debug/ieee802.11/phy0/ath9k/bssid_extra, where this mask is stored. The driver uses this information to determine if a frame is directed at it, thereby facilitating the appropriate layer-2 ACK response. Additionally, another Atheros-compatible interface is set to monitor mode to collect external radio states; for this purpose, the TP-Link WL722N wireless adapter is used as the secondary interface, ensuring both interfaces are from the Atheros family.

ii. The communication setup includes two OSI Layer 2 switches, one designated for data plane traffic and the other for control plane traffic. It also features a legacy wireless router that supports dual bands (2.4 GHz and 5 GHz) to facilitate connectivity. A computer with a minimum of 2 GB RAM, a 1.5 GHz processor, and x86-64 AMD architecture is utilized to run the ODIN SDN Controller. Additionally, a Raspberry Pi 4 serves as the fog node, while various wireless client devices, such as smartphones, computers, and Node MCUs, connect to the network to send traffic as end nodes.

The testbed utilizes several key software components, including the Odin Controller, an extension of the Floodlight SDN Controller, which receives heartbeat messages from agents (APs) and makes decisions, such as initiating failover or changing the transmitting channel of an AP. It also features a custom-built OpenWRT wireless router operating system with Ath9k patches for enhanced performance. Additionally, Open vSwitch is deployed within the SDN-capable routers to manage OpenFlow protocol traffic. The setup includes the Odin Agent, which is integrated with a Click router and a patch that collects 802.11 frames, providing the data necessary for the controller to make informed decisions.

3.2 Testbed Implementation Setup

Figure 12 presents the architecture connectivity diagram for the lab implementation. Node microcontroller units (MCUs) and mobile phones serve as end nodes, while two SDN access points (APs) and one legacy AP provide WiFi coverage. A computer acts as the SDN controller, which also incorporates the functions of a Wireless LAN Controller (WLC), and is connected to the control switch. The SDN APs feature two ports: one connected to the data switch and the other to the control switch. A router directs traffic along optimal routes and assigns dynamic IP addresses to end nodes that do not have static IPs. A backbone switch connects data networks from different clusters, while Un-Twisted Pair (UTP) cables serve as the backhauling technology. Additionally, a high-performance desktop computer is utilized as the computing machine at the control center.

The actual deployment is depicted in Figure 13. Four MCUs were deployed: three configured as sensors/smart meters and one as an actuator. Additionally, three mobile phones were used as sensors specifically to emulate fault scenarios.

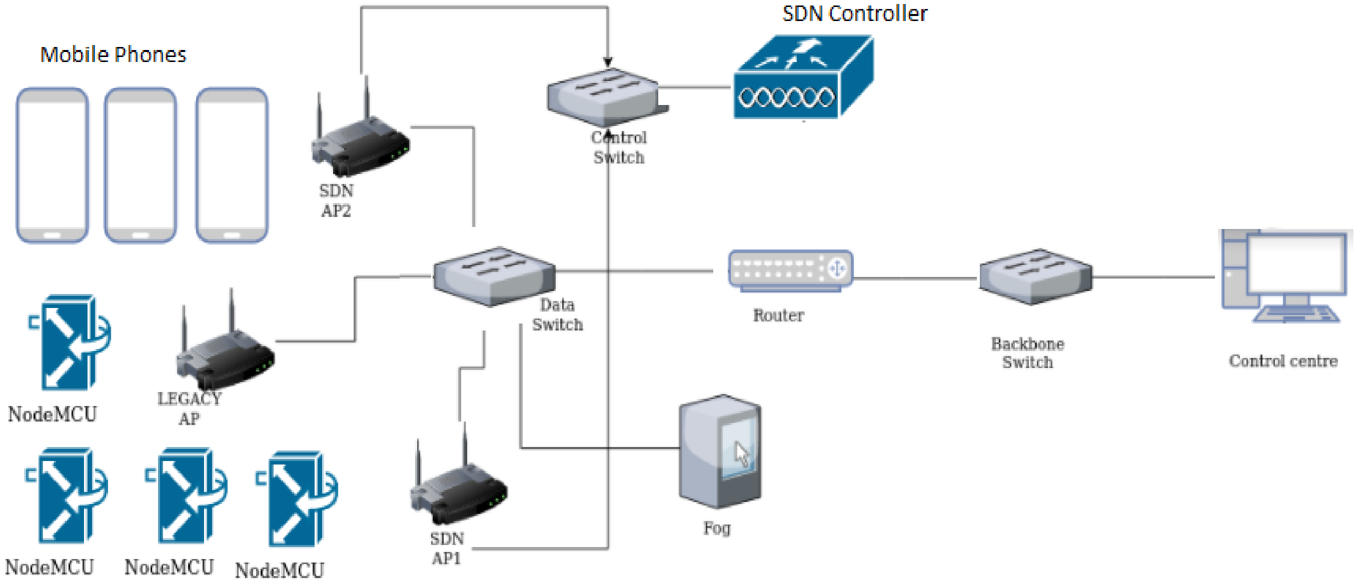


Figure 12. Lab architecture design.

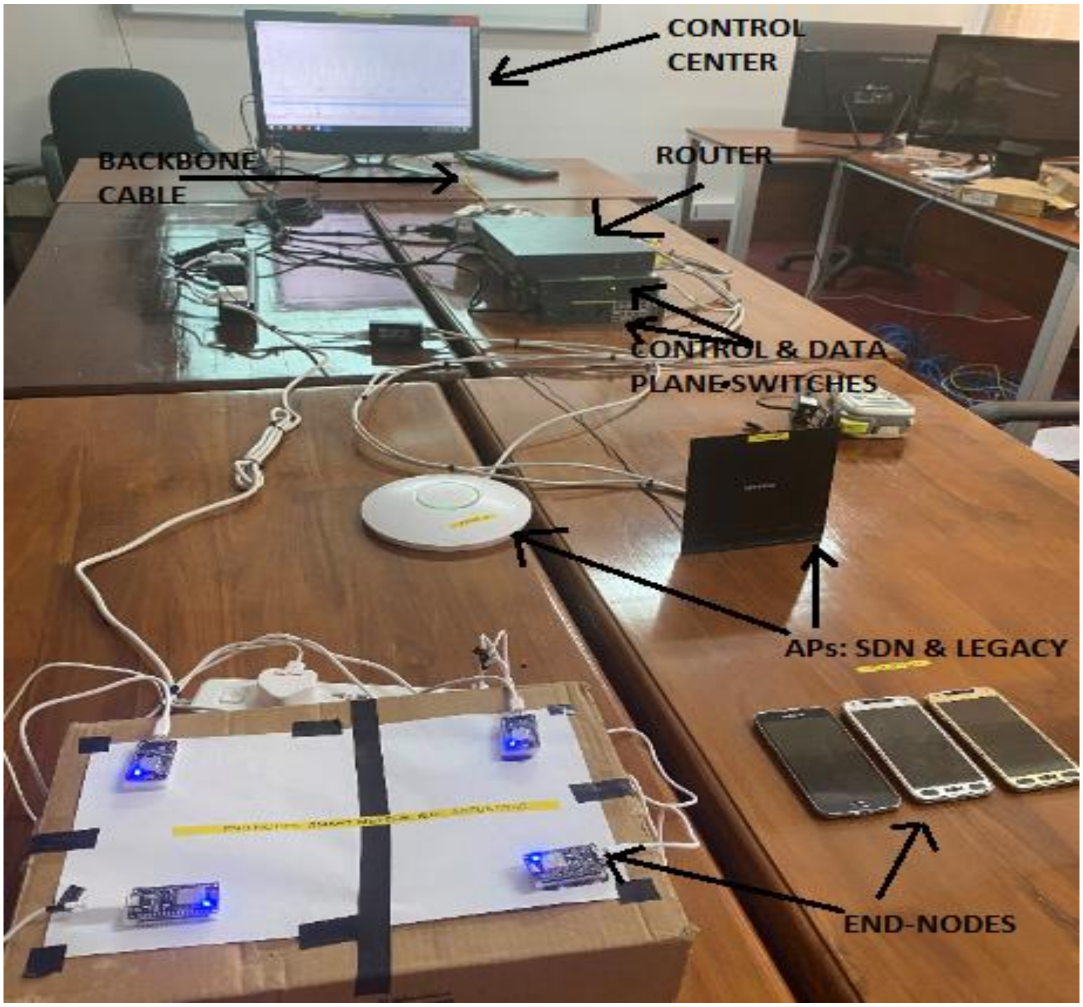


Figure 13. Actual Lab deployment of a hybrid architecture based on hierarchical computing.

Both a legacy AP and an SDN AP were implemented to evaluate interoperability and dual connectivity. The access network included two switches (for the data plane and control plane), one router, and one fog node (Raspberry Pi 4). The backbone/core network consisted of a backbone switch, UTP cables, and a desktop computer.

In the laboratory implementation, when an end node scans for nearby WiFi and requests a connection via probe requests, the Access Point (AP) notifies the SDN controller, which then assigns a light virtual access point (LVAP) containing the end node's IP and MAC addresses, as well as the virtual AP's MAC and SSID. Once assigned, the end node connects to the network through the AP's data plane interface. Sensors transmit data to the fog node using the MQTT protocol, while actuators subscribe to topics for commands sent by the fog node during faults.

The Raspberry Pi fog node, equipped with an EMQ X broker, aggregates data from edge devices, bundles and forwards them to the control center. The fog node also matches incoming data against predefined conditions to detect faults. The physical SDN AP's Eth1 interface connects to the control plane switch with the SDN controller, facilitating southbound OpenFlow communications. The SDN controller manages LVAP assignments, monitors AP heartbeats, migrates LVAPs if an AP fails, and adjusts channels to mitigate interference based on collected statistics.

Figure 14 illustrates the end nodes' traffic flow graph displayed on the control center's screen in the laboratory. This graph confirms that the design was successfully implemented and that all devices were able to communicate effectively.

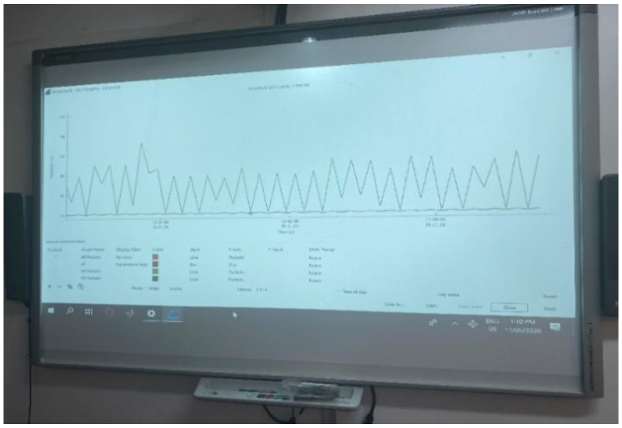


Figure 14. Traffic flow in control centre computer in the lab.

4. Results and Discussions

Firstly, it was important to verify that the proposed architecture was properly designed and implemented. The architecture was tested for its responsiveness to changes in the network environment. Initially, the system was started, and once all nodes were associated and authenticated, they were programmed to transmit routine data for thirty minutes. Subsequently, the nodes were paused for another thirty minutes before being instructed to resume data transmission. The results, illustrated in Figure 15, reveal that when the nodes stopped sending data, the TCP traffic dropped to zero. Upon resumption, TCP traffic increased accordingly. This behavior confirms that the architecture is well-designed and effectively responds to the nodes' activity levels. Figure 15 is from screenshot of Wireshark, which was used to monitor the network parameters.

Secondly, it was vital to demonstrate that the designed architecture could carry actual traffic generated by utility companies, such as TANESCO, from developing countries, The developed architecture was evaluated to determine its capability to support the transmission of various traffic types across multiple protocols, with a particular focus on its ability to handle TCP data for routine historical information and UDP for fault and emergency communications. Figure 16 presents a live capture of the network traffic, reinforcing the practicality of the architecture. The results clearly demonstrate the simultaneous transmission of both TCP routine data and UDP fault-related data, all while the access points continue to broadcast their beacons. Figure 16 also shows that end nodes could hook to all three APs in a cluster. Clearly, we see different beacon messages from APs and different end nodes IP addresses.

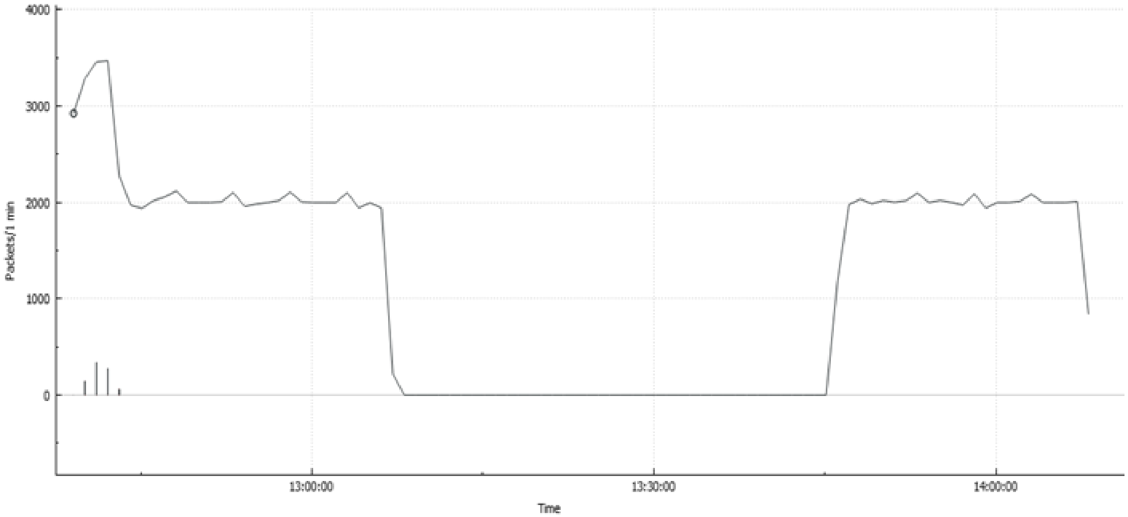
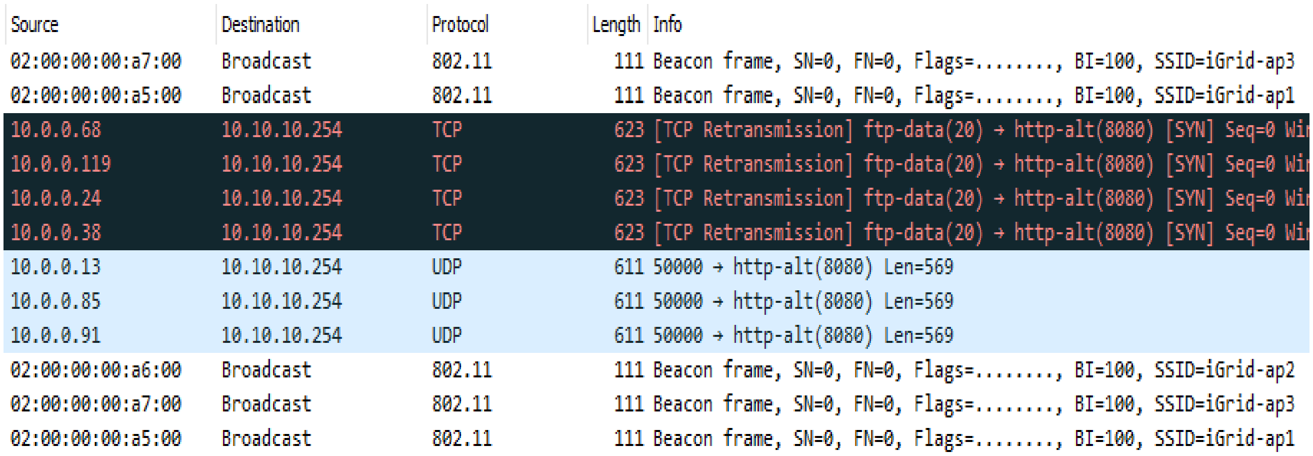


Figure 15. Architecture’s response when nodes send/stop sending data.



Source	Destination	Protocol	Length	Info
02:00:00:00:a7:00	Broadcast	802.11	111	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=iGrid-ap3
02:00:00:00:a5:00	Broadcast	802.11	111	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=iGrid-ap1
10.0.0.68	10.10.10.254	TCP	623	[TCP Retransmission] ftp-data(20) → http-alt(8080) [SYN] Seq=0 Wi
10.0.0.119	10.10.10.254	TCP	623	[TCP Retransmission] ftp-data(20) → http-alt(8080) [SYN] Seq=0 Wi
10.0.0.24	10.10.10.254	TCP	623	[TCP Retransmission] ftp-data(20) → http-alt(8080) [SYN] Seq=0 Wi
10.0.0.38	10.10.10.254	TCP	623	[TCP Retransmission] ftp-data(20) → http-alt(8080) [SYN] Seq=0 Wi
10.0.0.13	10.10.10.254	UDP	611	50000 → http-alt(8080) Len=569
10.0.0.85	10.10.10.254	UDP	611	50000 → http-alt(8080) Len=569
10.0.0.91	10.10.10.254	UDP	611	50000 → http-alt(8080) Len=569
02:00:00:00:a6:00	Broadcast	802.11	111	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=iGrid-ap2
02:00:00:00:a7:00	Broadcast	802.11	111	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=iGrid-ap3
02:00:00:00:a5:00	Broadcast	802.11	111	Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=iGrid-ap1

Figure 16. Live capture of various protocols in the architecture.

In this study, key evaluation criterion was Round Trip Time (RTT), which is the total time it takes for a data packet to go from the sender to the receiver and then back to the sender. It includes the time spent in transmission, propagation delays, queuing delays, and any delays caused by processing at the sender or receiver. RTT is commonly used to measure the latency of data transfer between two endpoints. RTT is typically measured in milliseconds (ms), and is a critical metric for understanding the responsiveness of a network. Lower RTT values generally indicate a faster, more responsive network, while higher values often point to delays or congestion.

The Lab architecture implementation was evaluated to check if the end nodes' data can reach the fog node successfully and timely. When the architecture was operational, meaning all end nodes were sending data and actuators responding to commands from the cluster fog node, then another laptop was connected and configured as an end node to connect to the WiFi network provided by the installed SDN AP. After the laptop end node had already acquired IP (192.168.2.20), fifteen (15) pings were directed to the fog node (192.168.2.9) with data of size 669 Bytes each. 669 Bytes was the calculated size from the collected AMR data containing twenty current and voltage readings. The Pings results are summarized by Figure 17, where it is shown that the average RTT was 7.059 ms.

The obtained RTT value in Figure 17 means the communication architecture can be used to detect and clear faults at LVPN efficiently as it imposed average delay, which is less than the latency limits of AMI, DER and DA (Table 1). Several other pings were done at different times, and all of them had lower RTT than the AMI, DER and DA limits.

This study proposes a clustered hierarchical architecture with three layers of processing, essential for meeting the stringent latency requirements of LVPN automation. End nodes within a specific cluster, managed by a fog node, can be promptly controlled to address faults originating in that cluster, rather than relying on a central control node. Figure 18 illustrates this concept, showing that various commands issued from the fog node to the end nodes (actuators) in the cluster were successfully delivered within the acceptable latency thresholds for DA in LVPN. Only one command experienced slightly higher latency than the acceptable limit for DER integration; however, this is not concerning as the overall success rate was over 93.3% (14 out of 15 commands). Notably, actual LVPN actuating commands are only 50 bytes in size, significantly smaller than the 669 bytes used in this experiment. Moreover, since DER integration is not currently implemented in LVPNs in developing countries, the delayed command does not pose a threat to the architecture's automation capabilities.

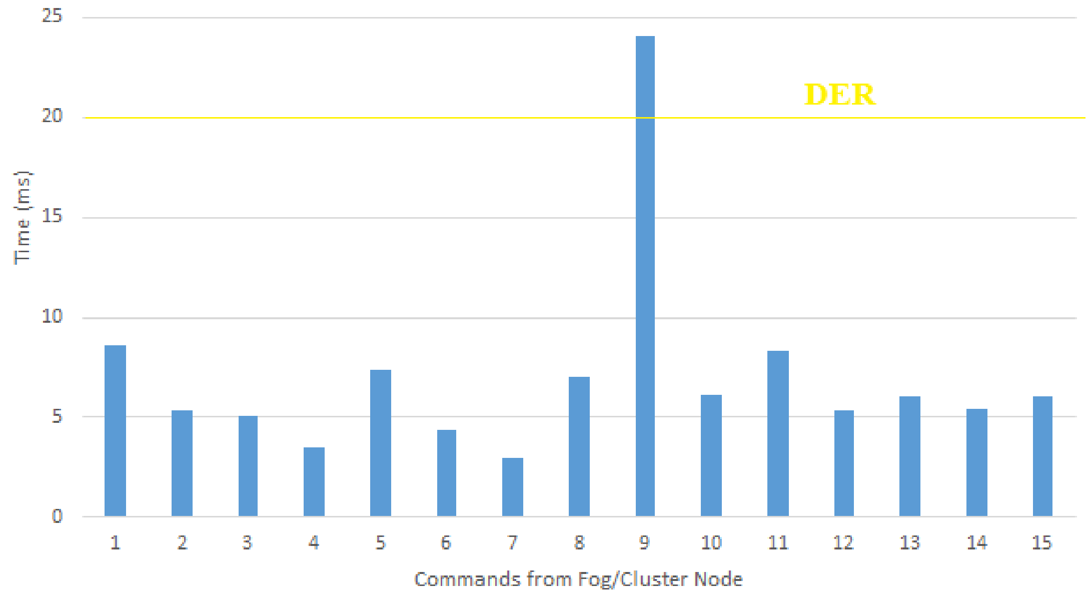
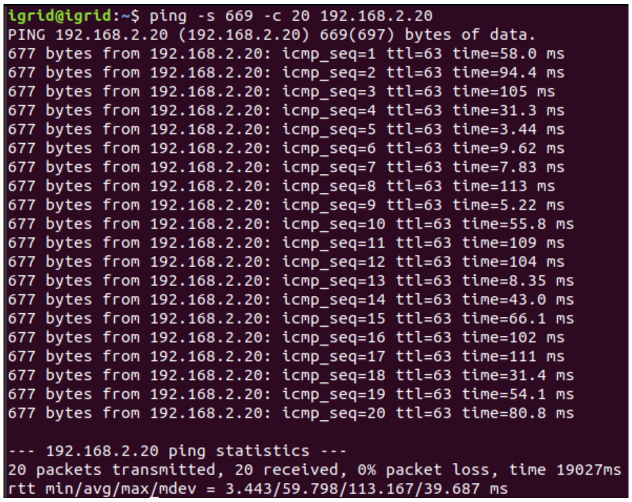


Figure 17. Latency values for Fog/Cluster node commands to End Nodes.

The architecture was then tested to evaluate if the control center computer's data directly to the end node can arrive timely within latency limits. The laptop was again used as the end node; the control center computer (10.10.10.10) pinged 20 times the end node (192.168.2.20), and the results were summarized in Figure 19. The average RTT was 59.798 ms, which is higher than the maximum latency limit for DER applications. Six (6) out of 20 pings (30%) had RTT above 100 ms, which means they could be used for neither DER nor DA.



```
igrid@igrid:~$ ping -s 669 -c 20 192.168.2.20
PING 192.168.2.20 (192.168.2.20) 669(697) bytes of data.
677 bytes from 192.168.2.20: icmp_seq=1 ttl=63 time=58.0 ms
677 bytes from 192.168.2.20: icmp_seq=2 ttl=63 time=94.4 ms
677 bytes from 192.168.2.20: icmp_seq=3 ttl=63 time=105 ms
677 bytes from 192.168.2.20: icmp_seq=4 ttl=63 time=31.3 ms
677 bytes from 192.168.2.20: icmp_seq=5 ttl=63 time=3.44 ms
677 bytes from 192.168.2.20: icmp_seq=6 ttl=63 time=9.62 ms
677 bytes from 192.168.2.20: icmp_seq=7 ttl=63 time=7.83 ms
677 bytes from 192.168.2.20: icmp_seq=8 ttl=63 time=113 ms
677 bytes from 192.168.2.20: icmp_seq=9 ttl=63 time=5.22 ms
677 bytes from 192.168.2.20: icmp_seq=10 ttl=63 time=55.8 ms
677 bytes from 192.168.2.20: icmp_seq=11 ttl=63 time=109 ms
677 bytes from 192.168.2.20: icmp_seq=12 ttl=63 time=104 ms
677 bytes from 192.168.2.20: icmp_seq=13 ttl=63 time=8.35 ms
677 bytes from 192.168.2.20: icmp_seq=14 ttl=63 time=43.0 ms
677 bytes from 192.168.2.20: icmp_seq=15 ttl=63 time=66.1 ms
677 bytes from 192.168.2.20: icmp_seq=16 ttl=63 time=102 ms
677 bytes from 192.168.2.20: icmp_seq=17 ttl=63 time=111 ms
677 bytes from 192.168.2.20: icmp_seq=18 ttl=63 time=31.4 ms
677 bytes from 192.168.2.20: icmp_seq=19 ttl=63 time=54.1 ms
677 bytes from 192.168.2.20: icmp_seq=20 ttl=63 time=80.8 ms

--- 192.168.2.20 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19027ms
rtt min/avg/max/mdev = 3.443/59.798/113.167/39.687 ms
```

Figure 18. End node – Control Center node RTT ping results.

The results presented in Figure 19 demonstrate that DER and DA applications within LVPN cannot be effectively managed by a centralized architecture. This is why the communication architecture proposed in this study employs a multilayered, hierarchical clustered approach. By positioning the cluster handling node (fog) physically closer to the end nodes, we can better meet the stringent latency requirements. While AMI primarily transmits historical data and informs grid operators for future predictive actions, its latency requirement is relatively lenient at 2 seconds. This flexibility allows even current centralized and two-layered architectures to function adequately, despite their limitations.

Figure 20 illustrates that a centralized infrastructure is limited to managing AMI applications and struggles to support LVPN automation tasks, such as opening and closing switchgears and reclosers along service lines. Notably, only 75% of commands from the CC achieve acknowledgment within the 20 ms threshold required for DER integration, and 70% meet the acceptable latency for DA within LVPN. These results would have been worse if all nodes transmitted data directly to the control center rather than leveraging the fog node during the tests.

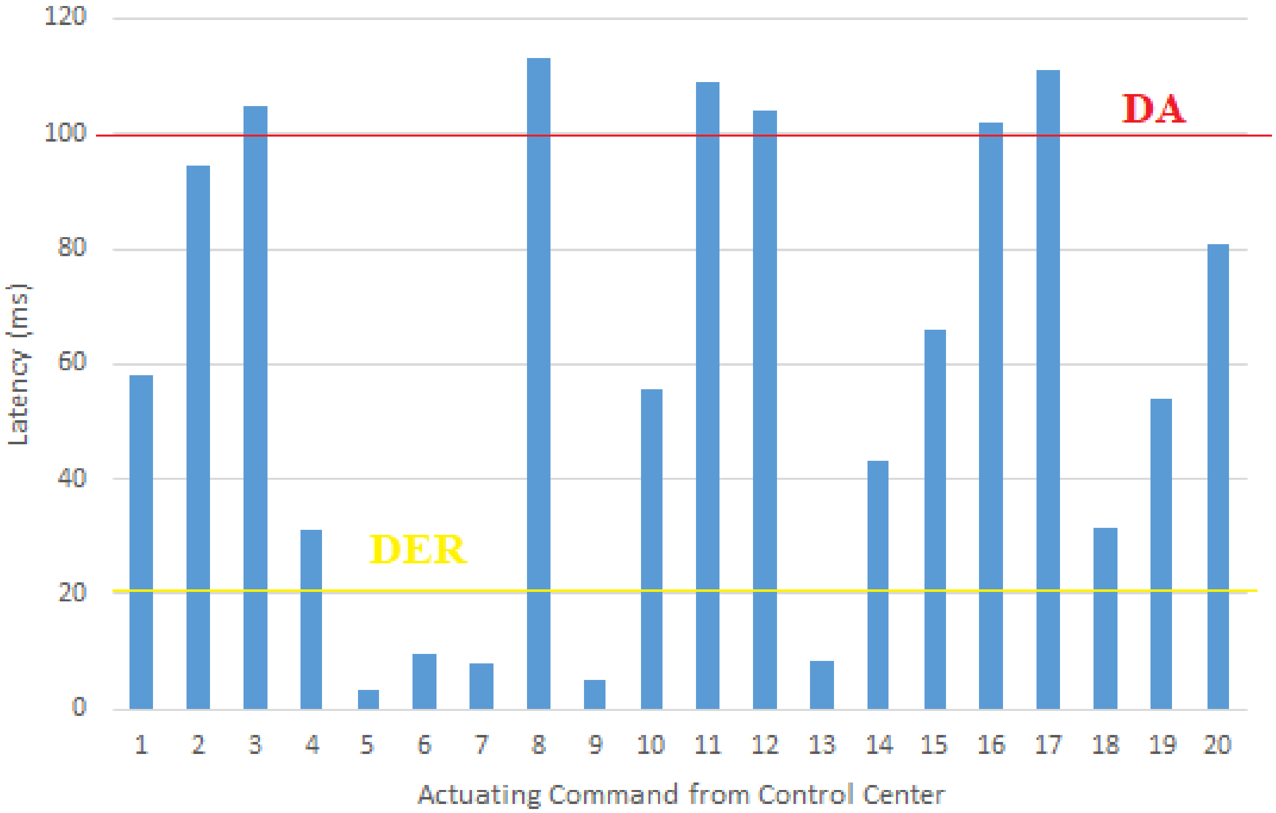


Figure 19. Latency values for CC commands straight to end nodes (centralized approach).

The latency values observed in this study (7.059 ms) were slightly higher than the maximum RTT values reported (3.68ms) in Chugulu et al. [13] for several reasons. First, in their study, the network conditions were ideal and did not account for equipment or node response time after receiving a signal or command. Second, their results were based on simulations in a virtual environment, while this study involved actual devices in a live environment. Finally, this study incorporated SDN capabilities to sense and hand over wireless nodes to nearby access points with stronger signals, which introduced some delay in the network and contributed to the higher latency values.

In summary, the proposed clustered hierarchical architecture effectively meets stringent latency requirements for LVPN automation. Initial tests show that it efficiently manages data and responds quickly to faults, supporting both TCP for historical data and UDP for critical communications. Unlike centralized systems, it ensures high success rates and reduces latency by delivering commands from the fog node. By positioning the fog node closer to end nodes, it enhances real-time responsiveness and supports future advancements in LVPN automation.

5. Conclusion

In this paper, a communication architecture tailored to the unique design specifications of automation in developing countries was proposed. Unlike previous studies, our work was grounded in the actual requirements of TANESCO, and was modeled, tested, and implemented using real-world grid data, actual devices, and protocols in a live environment. The proposed architecture integrates hierarchical computing with SDN capabilities to optimize the automation of LVPN systems. Specifically designed to meet the needs of power utilities in developing countries, this architecture enhances fault detection and service restoration by leveraging practical communication technologies.

Through the integration of edge, fog, and cloud computing, the architecture significantly improves system efficiency and reliability. Local pre-processing at the edge reduces congestion by optimizing bandwidth and data flow from end nodes. The cluster controlling unit supports real-time fault management, while the cloud layer provides scalable data processing and storage solutions. By utilizing existing fiber optic backhaul infrastructure, the design minimizes implementation costs while ensuring reliable connectivity. Additionally, the SDN capabilities enhance traffic management, particularly during fault conditions, ensuring network resilience.

When tested in a laboratory environment, the architecture demonstrated its ability to meet stringent latency requirements, effectively supporting LVPN automation tasks and ensuring timely responses. The results highlight the feasibility of this communication architecture for automating LVPN systems in developing countries, offering a cost-effective, scalable, and reliable solution for power utilities.

In our future work, the access network of the communication architecture will be deployed in an environment featuring thousands of end nodes within a cluster. This phase will involve analyzing the challenges posed by such a large number of end nodes, particularly in relation to meeting latency criteria for LVPN automations.

ACKNOWLEDGEMENT

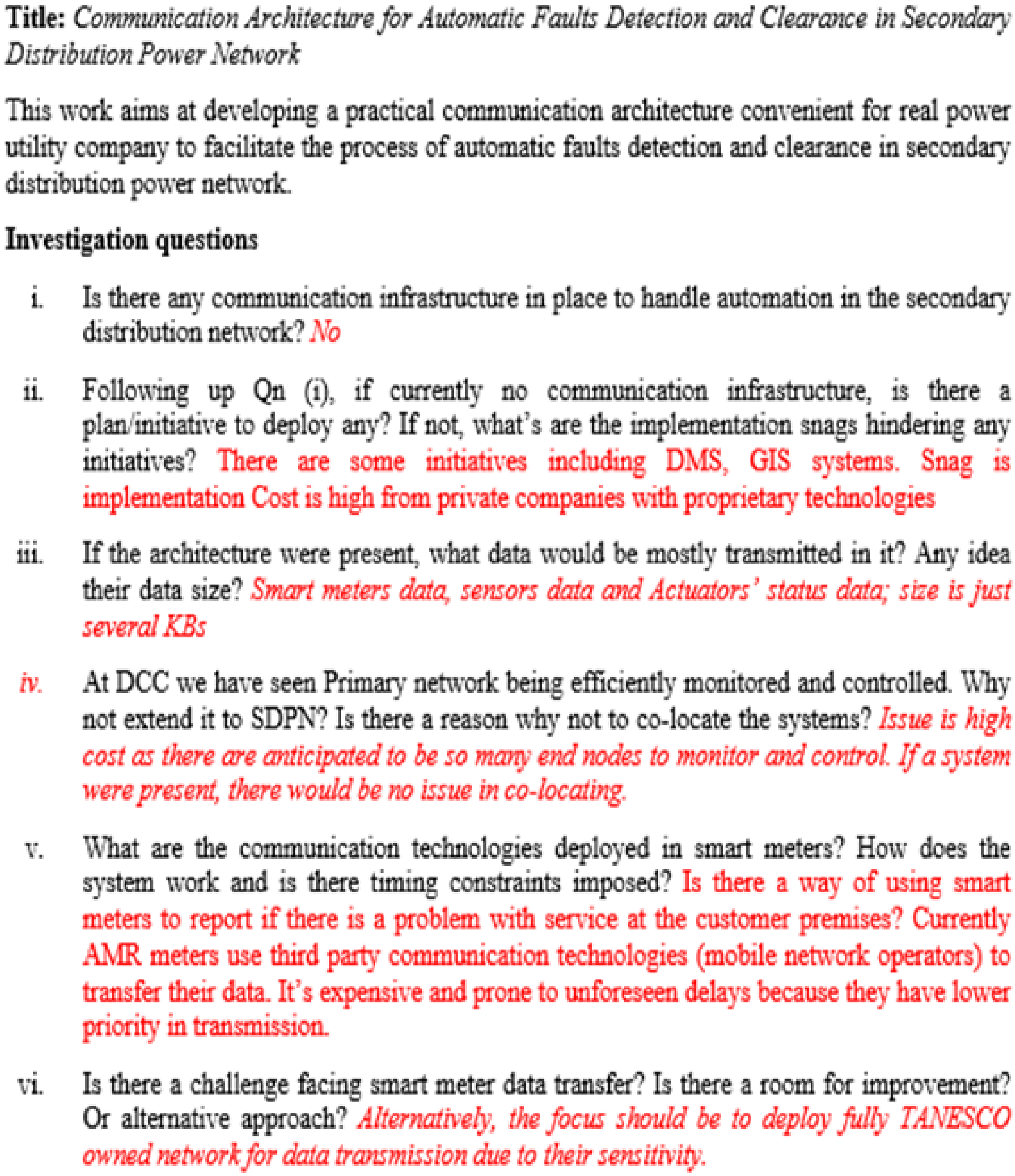
The author expresses gratitude to the experts at TANESCO for their willingness to participate in the requirements gathering and data collection process. Special thanks are also extended to the iGrid research group at the University of Dar es Salaam, where the author is a member. The insights and technical advice provided by iGrid researchers were invaluable to the success of this work.

CONTRIBUTION

Godfrey W. Chugulu	[ORCID: 0000-0001-7660-8643]	Conceived the idea and wrote the paper

APPENDICES

APPENDIX A: Guided Questions for LVPN Data Collection



Title: *Communication Architecture for Automatic Faults Detection and Clearance in Secondary Distribution Power Network*

This work aims at developing a practical communication architecture convenient for real power utility company to facilitate the process of automatic faults detection and clearance in secondary distribution power network.

Investigation questions

i. Is there any communication infrastructure in place to handle automation in the secondary distribution network? *No*

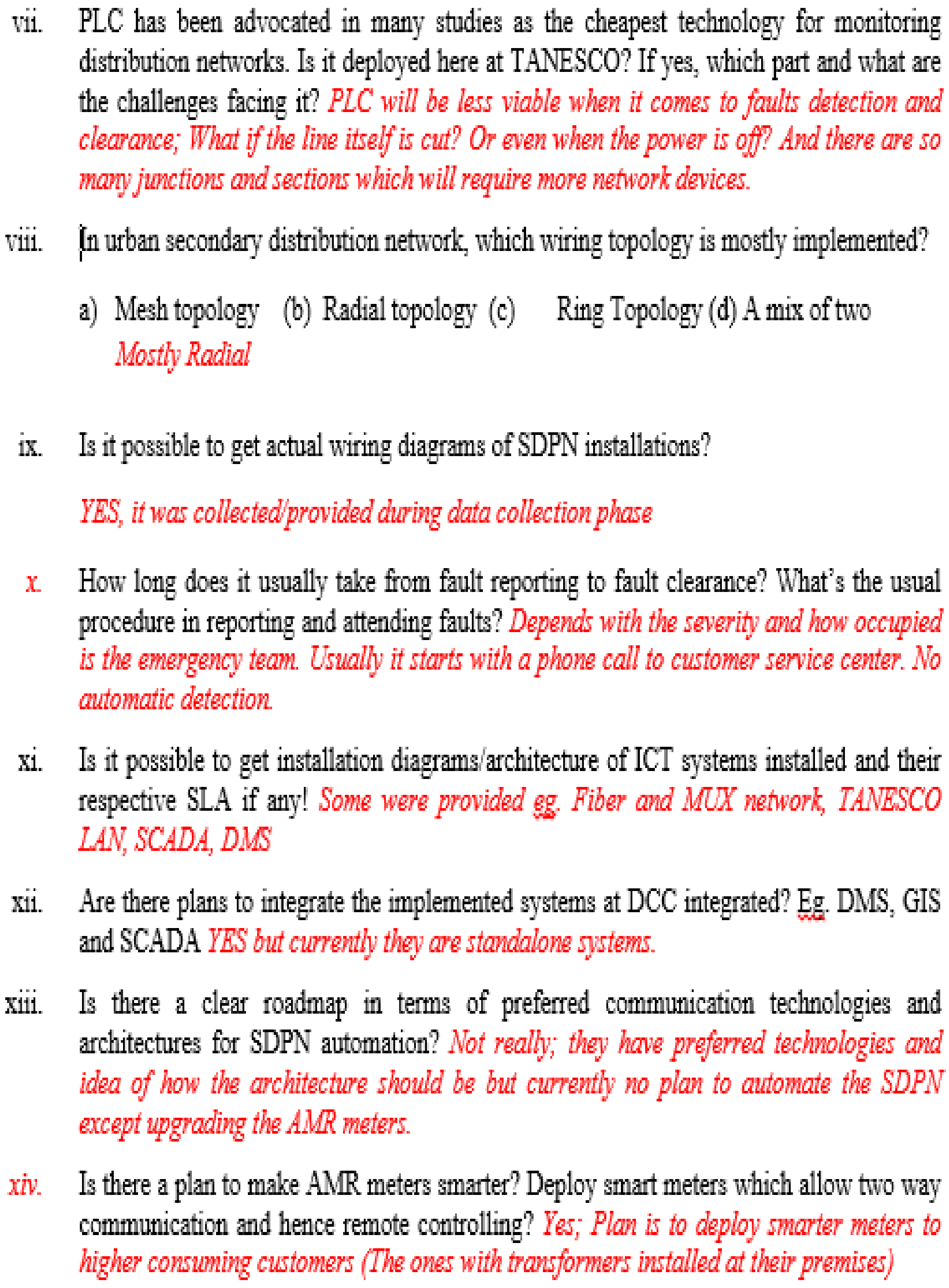
ii. Following up Qn (i), if currently no communication infrastructure, is there a plan/initiative to deploy any? If not, what's are the implementation snags hindering any initiatives? There are some initiatives including DMS, GIS systems. Snag is implementation Cost is high from private companies with proprietary technologies

iii. If the architecture were present, what data would be mostly transmitted in it? Any idea their data size? *Smart meters data, sensors data and Actuators' status data; size is just several KBs*

iv. At DCC we have seen Primary network being efficiently monitored and controlled. Why not extend it to SDPN? Is there a reason why not to co-locate the systems? *Issue is high cost as there are anticipated to be so many end nodes to monitor and control. If a system were present, there would be no issue in co-locating.*

v. What are the communication technologies deployed in smart meters? How does the system work and is there timing constraints imposed? Is there a way of using smart meters to report if there is a problem with service at the customer premises? Currently AMR meters use third party communication technologies (mobile network operators) to transfer their data. It's expensive and prone to unforeseen delays because they have lower priority in transmission.

vi. Is there a challenge facing smart meter data transfer? Is there a room for improvement? Or alternative approach? *Alternatively, the focus should be to deploy fully TANESCO owned network for data transmission due to their sensitivity.*



vii. PLC has been advocated in many studies as the cheapest technology for monitoring distribution networks. Is it deployed here at TANESCO? If yes, which part and what are the challenges facing it? *PLC will be less viable when it comes to faults detection and clearance; What if the line itself is cut? Or even when the power is off? And there are so many junctions and sections which will require more network devices.*

viii. In urban secondary distribution network, which wiring topology is mostly implemented?

a) Mesh topology (b) Radial topology (c) Ring Topology (d) A mix of two

Mostly Radial

ix. Is it possible to get actual wiring diagrams of SDPN installations?

YES, it was collected/provided during data collection phase

x. How long does it usually take from fault reporting to fault clearance? What's the usual procedure in reporting and attending faults? *Depends with the severity and how occupied is the emergency team. Usually it starts with a phone call to customer service center. No automatic detection.*

xi. Is it possible to get installation diagrams/architecture of ICT systems installed and their respective SLA if any! *Some were provided eg. Fiber and MUX network, TANESCO LAN, SCADA, DMS*

xii. Are there plans to integrate the implemented systems at DCC integrated? Eg. DMS, GIS and SCADA *YES but currently they are standalone systems.*

xiii. Is there a clear roadmap in terms of preferred communication technologies and architectures for SDPN automation? *Not really; they have preferred technologies and idea of how the architecture should be but currently no plan to automate the SDPN except upgrading the AMR meters.*

xiv. Is there a plan to make AMR meters smarter? Deploy smart meters which allow two way communication and hence remote controlling? *Yes; Plan is to deploy smarter meters to higher consuming customers (The ones with transformers installed at their premises)*

APPENDIX B: Communication Architecture Requirements Specification

S/N	SPECIFICATIONS	KEY DETAILS
1	Ownership and Security	i. The communication architecture must be fully owned and managed by the utility company, with no involvement of third-party providers. ii. For security reasons, the architecture should be entirely offline and disconnected from the Internet.
2	Distributed Processing Architecture	The architecture must be based on distributed processing, allowing hierarchical processing at three levels: Edge, Fog, and Cloud
3	Network Communication Technologies	i. Access Network: WLAN/WiFi (IEEE 802.11x) will be used for communication at the access network level. ii. Backbone Network: Fiber optic will serve as the backbone for high-speed data transport. iii. Supporting Transport Technologies: Outdoor UTP cables and Point-to-Point (P2P) free-to-air terrestrial microwave will be used for additional connectivity.
4	End Node Specifications	i. Each end node will be equipped with a Wi-Fi communication module (IEEE 802.11x) and a simple processor for basic computations. ii. End nodes should have some computational capability to support edge computing, such as running simple algorithms locally.
5	Data Aggregation and Cluster Architecture	i. Aggregation will be performed at the transformer, which provides easy access to power and hosts other network devices. This central location will channel all measurement and control data for further processing. ii. The architecture must be clustered to enable local processing of faults within each cluster, thereby meeting strict latency requirements.
6	IP-Based Communication	All communications within the architecture will be IP-based, regardless of the underlying protocols used by applications running on the nodes
7	Wireless Access Points and Coverage	i. Powerful directional outdoor wireless access points will be installed at transformers and select locations to ensure adequate coverage and capacity for end nodes. ii. For ease of maintenance and to reduce communication overhead, static IPs will be assigned to end nodes.

S/N	SPECIFICATIONS	KEY DETAILS
8	Cost Efficiency and Data Transmission	For cost-effective implementation, data from the aggregation switch should be transmitted to the nearest fiber Point of Presence (POP), ensuring efficient data routing to the control center.
9	Pre-Processing and Bandwidth Optimization	To optimize CPU usage and bandwidth utilization, data from end nodes must be pre-processed before being sent to the designated part of the architecture for further handling.
10	Scalability and Dynamic Programmability	The architecture must support Software Defined Networking (SDN) on the access network, enabling dynamic programmability, scalability, and "on-the-fly" configuration adjustments

REFERENCES

[1] G. Chugulu and F. Simba, “Communication Architecture for Automatic Faults Detection and Clearance in Secondary Distribution Power Grid: The Case of TANESCO,” *Proceedings of 2019 the 7th International Conference on Smart Energy Grid Engineering, SEGE 2019*, pp. 223–229, 2019, doi: 10.1109/SEGE.2019.8859909.

[2] D. Mnyanghwalo, S. Kawambwa, R. Mwifunyi, G. M. Gilbert, D. Makota, and N. Mvungi, “Fault Detection and Monitoring in Secondary Electric Distribution Network Based on Distributed Processing,” *2018 20th International Middle East Power Systems Conference, MEPCON 2018 - Proceedings*, pp. 84–89, 2019, doi: 10.1109/MEPCON.2018.8635141.

[3] A. R. Devidas, M. V. Ramesh, and V. P. Rangan, “High performance communication architecture for smart distribution power grid in developing nations,” *Wireless Networks*, vol. 24, no. 5, pp. 1621–1638, 2018, doi: 10.1007/s11276-016-1400-2.

[4] H. Mbembati and H. A. Bakiri, “Transformer faults in tanzanian electrical distribution networks: indicators, types, and causes,” *Journal of Electrical Systems and Information Technology*, vol. 10, no. 1, Jul. 2023, doi: 10.1186/s43067-023-00103-3.

[5] A. Zidan *et al.*, “Fault Detection, Isolation, and Service Restoration in Distribution Systems: State-of-the-Art and Future Trends,” *IEEE Trans Smart Grid*, pp. 1–16, 2016, doi: 10.1109/TSG.2016.2517620.

[6] M. Emmanuel and R. Rayudu, “Communication technologies for smart grid applications: A survey,” *Journal of Network and Computer Applications*, vol. 74, pp. 133–148, 2016, doi: 10.1016/j.jnca.2016.08.012.

[7] A. Abdrabou, “A Wireless Communication Architecture for Smart Grid Distribution Networks,” *IEEE Syst J*, vol. 10, no. 1, pp. 251–261, 2016, doi: 10.1109/JSYST.2014.2304291.

[8] R. J. Mwifunyi, D. C. Mnyanghwalo, and S. J. Kawambwa, “Enhancing Service Restoration in Tanzanian Power Grid using Internet of Things Sensors and Renewable Energy Sources,” *Tanzania Journal of Science*, vol. 49, no. 3, pp. 664–676, Sep. 2023, doi: 10.4314/tjs.v49i3.10.

[9] D. Mnyanghwalo and S. Kawambwa, “Deployment of an IoT based sensor node for faults detection and classification in electrical secondary distribution networks,” *Cogent Eng*, vol. 11, no. 1, 2024, doi: 10.1080/23311916.2024.2404679.

[10] M. Emmanuel, W. K. G. Seah, and R. Rayudu, “Communication Architecture for Smart Grid Applications,” *Proc IEEE Symp Comput Commun*, vol. 2018-June, pp. 746–751, 2018, doi: 10.1109/ISCC.2018.8538472.

[11] D. Baimel, S. Tapuchi, and N. Baimel, “Smart grid communication technologies- overview, research challenges and opportunities,” *2016 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, pp. 116–120, 2016, doi: 10.1109/SPEEDAM.2016.7526014.

[12] N. Suhaimy, N. A. M. Radzi, W. S. H. M. W. Ahmad, K. H. M. Azmi, and M. A. Hannan, “Current and Future Communication Solutions for Smart Grids: A Review,” 2022, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2022.3168740.

[13] G. Chugulu, F. Simba, and S. Lujara, “Proposed Practical Communication Architecture for Automatic Fault Detection and Clearance in Secondary Distribution Power Network,” *International Journal of Smart Grid - ijSmartGrid*, vol. 4, no. 4, 2020.

[14] Y. Andegelile, G. Chugulu, H. Mbembati, A. Bitebo, and H. Kundaeli, “Enhancing Faults Monitoring in Secondary Electrical Distribution Network,” in *I5th IFIP WG 9.4 International Conference on Social Implications of Computers in Developing Countries*, Springer International Publishing, 2019, pp. 1–804. doi: 10.1007/978-3-030-18400-1_58.

[15] A. R. Devidas, M. V. Ramesh, and V. P. Rangan, “High performance communication architecture for smart distribution power grid in developing nations,” *Wireless Networks*, vol. 24, no. 5, pp. 1621–1638, 2018, doi: 10.1007/s11276-016-1400-2.

[16] A. Abdalla and K. Ibwe, “Smart Grid in Tanzania: Research Opportunities,” *Tanzania Journal of Engineering and Technology*, vol. 42, no. 2, pp. 170–183, Jun. 2023, doi: 10.52339/tjet.v42i2.838.

[17] I. Colak, R. Bayindir, and S. Sagiroglu, “The Effects of the Smart Grid System on the National Grids,” *8th International Conference on Smart Grid, icSmartGrid 2020*, pp. 122–126, 2020, doi: 10.1109/icSmartGrid49881.2020.9144891.

[18] F. Khan, A. ur Rehman, M. Arif, M. Aftab, and B. K. Jadoon, “A survey of communication technologies for smart grid connectivity,” *2016 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube)*, pp. 256–261, 2016, doi: 10.1109/ICECUBE.2016.7495234.

[19] R. J. Mwifunyi, M. M. Kissaka, and N. H. Mvungi, “Distributed approach in fault localisation and service restoration: State-of-the-Art and future direction,” *Cogent Eng*, vol. 6, no. 1, 2019, doi: 10.1080/23311916.2019.1628424.

[20] F. E. Abrahamsen, Y. Ai, and M. Cheffena, “Communication Technologies for Smart Grid: A Comprehensive Survey.”

[21] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, “Communication network requirements for major smart grid applications in HAN, NAN and WAN,” *Computer Networks*, vol. 67, pp. 74–88, 2014, doi: 10.1016/j.comnet.2014.03.029.

[22] H. Farooq and L. T. Jung, “Choices available for implementing smart grid communication network,” *2014 International Conference on Computer and Information Sciences, ICCOINS 2014 - A Conference of World Engineering, Science and Technology Congress, ESTCON 2014 - Proceedings*, pp. 1–5, 2014, doi: 10.1109/ICCOINS.2014.6868383.

[23] Z. Soufiane, B. Slimane, and E. N. Abdeslam, “A synthesis of communication architectures and services of smart grid systems,” *Proceedings - 2016 3rd International Conference on Systems of Collaboration, SysCo 2016*, 2017, doi: 10.1109/SYSCO.2016.7831334.

[24] Z. Pourmirza and J. M. Brooke, “A Realistic ICT Network Design and Implementation in the Neighborhood Area of the Smart Grid,” *Smart Grid and Renewable Energy*, vol. 4, no. 6, pp. 436–448, 2013.

[25] N. S. Nafi, K. Ahmed, M. A. Gregory, and M. Datta, “A survey of smart grid architectures, applications, benefits and standardization,” *Journal of Network and Computer Applications*, vol. 76, pp. 23–36, 2016, doi: 10.1016/j.jnca.2016.10.003.

[26] G. M. Lee and D. H. Su, "Standarization of smart grid in ITU-T," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 90–97, 2013, doi: 10.1109/MCOM.2013.6400444.

[27] S. Ahmed, T. M. Gondal, M. Adil, S. A. Malik, and R. Qureshi, "A Survey on Communication Technologies in Smart Grid," *2019 IEEE PES GTD Grand International Conference and Exposition Asia, GTD Asia 2019*, pp. 7–12, 2019, doi: 10.1109/GTDAsia.2019.8715993.

[28] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart Grid Communication: Its Challenges and Opportunities," *IEEE Trans Smart Grid*, vol. 4, no. 1, pp. 36–46, 2013, doi: 10.1109/TSG.2012.2225851.

[29] K. C. Budka, J. G. Deshpande, T. L. Doumi, M. Madden, and T. Mew, "Communication Network Architecture and Design Principles for Smart Grids," *Bell Labs Tech J*, vol. 18, no. 4, pp. 3–17, 2014, doi: 10.1002/bltj.

[30] V. C. Gungor *et al.*, "A Survey on smart grid potential applications and communication requirements," *IEEE Trans Industr Inform*, vol. 9, no. 1, pp. 28–42, 2013, doi: 10.1109/TII.2012.2218253.

[31] A. T. Bitebo, H. Maziku, N., Hamisi, C. N. Tarimo, K. S. Ibwe, and A. T. Abdalla, "Design and Implementation of Distributed Identity and Access Management Framework for Internet of Things (IoT) Enabled Distribution Automation," *Tanzania Journal of Science*, vol. 48, no. 1, pp. 34–46, Mar. 2022, doi: 10.4314/tjs.v48i1.4.

[32] V. Dehalwar, A. Kalam, M. L. Kolhe, and A. Zayegh, "Review of IEEE 802.22 and IEC 61850 for real-time communication in Smart Grid," *2015 International Conference on Computing and Network Communications, CoCoNet 2015*, pp. 571–575, 2016, doi: 10.1109/CoCoNet.2015.7411245.

[33] V. Dehalwar, A. Kalam, and A. Zayegh, "Infrastructure for real-time communication in smart grid," *2014 Saudi Arabia Smart Grid Conference, SASG 2014*, pp. 2–5, 2014, doi: 10.1109/SASG.2014.7274281.

[34] F. Aalamifar, H. S. Hassanein, and G. Takahara, "Viability of powerline communication for the smart grid," in *2012 26th Biennial Symposium on Communications, QBSC 2012*, 2012. doi: 10.1109/QBSC.2012.6221343.

[35] J. Jiang and Y. Qian, "Distributed Communication Architecture for Smart Grid Applications," no. December, pp. 60–67, 2016.

[36] Y. Wang, P. Yemula, and A. Bose, "Decentralized communication and control systems for power system operation," *IEEE Trans Smart Grid*, vol. 6, no. 2, pp. 885–893, 2015, doi: 10.1109/TSG.2014.2363192.

[37] K. Ahuja and A. Khosla, "Network selection criterion for ubiquitous communication provisioning in smart cities for smart energy system," *Journal of Network and Computer Applications*, vol. 127, pp. 82–91, 2019, doi: 10.1016/j.jnca.2018.11.011.

[38] Y. Andegelile, H. Maziku, N. Mvungi, and M. Kissaka, "Software Defined Communication Network Reliability for Secondary Distribution Power Grid," *International Journal of Smart Grid - ijSmartGrid*, vol. 4, no. 3, 2020.

[39] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges," *1st ACM Workshop on Cyber-Physical System Security*, pp. 61–68, 2015.