energies

MDPI

Article

Enabling Cyber-Resilient Smart Grid Communication Using 5G Network Slicing: A Comparative Analysis of LTE vs. 5G

Amritha Geetha [1,2,*], Fabrizio Granelli [1] and Manjula G. Nair [2]

[1] Department of Information Engineering and Computer Science (DISI), University of Trento, 38123 Trento, Italy
[2] Department of Electrical and Electronics Engineering, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam 690525, India
* Correspondence: amenr4eee23041@am.students.amrita.edu

Abstract

Communication networks are a crucial part of modern-day smart power grids. Delays in the communication network, caused by traffic congestion or cyberattacks, can affect effective grid operation. The research in this paper analyses how different smart grid communication frameworks (LTE and 5G) behave under similar traffic conditions. This study considers three major factors of evaluation: latency evaluation for 5G and LTE under traffic congestion, the advantages of network slicing in 5G, and smart grid cyber-resilience metrics for 5G and LTE. The traffic classification is established based on the IEEE Guide for Smart Grid Interoperability of Energy Technology and IT Operation, IEEE Standard 2030-2011. Based on this standard, the PMU traffic is allocated to the URLLC slice, the user traffic is allocated to the eMBB slice, and the distributed energy resources and energy storage traffic are allocated to the mMTC slice. The experimental design of both 5G and LTE smart grid communication architectures is realised through the co-simulation of MATLAB/Simulink (version R2026a) and Comnetsemu (version 1.0.0). The results of this study show that network slicing enables PMU traffic isolation under conditions of heavy traffic; therefore, the PMU traffic remains protected under congestion because of the slice-based resource allocation in 5G. In this study, 5G therefore provides better performance compared to the conventional LTE-based WAN architectures. The experimental results indicate that 5G provides better latency as compared to LTE in smart grid communication architecture. The average latency values for the 5G architecture range from 34 to 37 ms, whereas those of the LTE architecture are 46 to 47 ms. Both 5G and LTE architectures are also evaluated for cyber resilience under conditions of DoS attack. The 5G architecture recovers within an average of 9 s compared to LTE, which takes an average of 16 s. Our prior research has identified the advantages of network slicing in PMU traffic isolation in smart grid communication. The scope of this study indicates that the advantages of network slicing make 5G a comparatively better communication architecture in smart grid communication than LTE.

Keywords: smart grid; 5G; LTE; network slicing; PMU traffic; URLLC; eMBB; mMTC

Check for updates

Academic Editor: José Matas

Received: 6 October 2026
Revised: 19 October 2026
Accepted: 26 October 2026
Published: 2 November 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Modern-day smart power grids rely heavily on communication infrastructure for efficient operation. Intelligent Electronic Devices (IEDs), Phasor Measurement Units (PMUs), distributed energy resources (DERs), smart meters, and other smart grid devices generate and exchange data among themselves and the smart grid control centres. In fact, bidirectional exchange of data is a prominent feature of smart power grids. This data exchange

also plays a pivotal role in the effective functioning of the real-time monitoring systems in smart power grids. Delays in communication caused by traffic congestion or cyber threats in smart grids can often affect the stability of the grid, leading to power system instability and economic losses. There are several examples of real-world scenarios where cyberattacks have brought devastating effects on the grid as well as on the lives of consumers. The wide range of communication entities in smart grids presents different traffic requirements; that is, the smart grid devices create a heterogeneous traffic distribution across the communication network. This heterogeneous nature of the smart grid communication network poses a challenge, as it presents different requirements in terms of latency, availability, throughput, etc. To put it in terms of examples, measurement modules like PMUs require a very low-latency spectrum, as these have critical applications in the real-time monitoring and control of the smart power grids. Meanwhile, for user applications, throughput is considered to be more important than latency. Similarly, for modules like DERs and ESSs, which generate a relatively small amount of data, scalability is more important than latency-specific requirements. However, when different traffic classes are bound to share the same resources in the communication network, the network performance is affected, as the traffic from a less critical application might consume resources that are also required by a more critical application. This can often lead to increased latency, delays, and packet losses. Therefore, it is crucial for smart grid communication architectures to maintain application-based traffic class differentiation and resource allocation. It is also quite evident that modern-day smart power grid communication architecture is not just restricted to providing better connectivity, offering much more.

This study was implemented based on the Smart Grid Interoperability Reference Model (SGIRM) of the IEEE Standard 2030-2011 [1]. The latency requirements for the different smart grid applications and their corresponding traffic class allocations in the scope of this research were determined based on this reference. LTE (Long-Term Evolution) has been widely used in smart grid communication because of its reliability in connecting smart grid devices to the control centre. However, without traffic-class-based resource allocation, the traffic over shared resources often leads to resource contention. With the growing integration of ICT components into the smart grid environment, the load on the network is also increasing; this, in turn, leads to traffic congestion over shared resources. This presents an important challenge to be addressed while using conventional LTE networks in smart power grids. The 5G (Fifth-Generation) networks have a number of features that could address these challenges. Network slicing is one such feature, which creates multiple logical virtual networks within a shared infrastructure using Software-Defined Networking (SDN), thereby helping with traffic isolation and resource allocation. The broadly used traffic classes in 5G are URLLC (Ultra-Reliable Low-Latency Communication), eMBB (Enhanced Mobile Broadband), and mMTC (Massive Machine-Type Communication).

While both LTE and 5G can support smart grid communication, there are significant differences in their ability to handle heterogeneous traffic. The LTE communication architecture is based on the evolved packet system model with eNodeB and EPC, whereas 5G is established with a 5G core (5GC) and gNB architecture. This study is intended to help understand how both of these smart grid communication technologies behave under identical load conditions, and also to analyse the effect of these technologies on the latency and resilience of the smart power grid. The experimental analysis in this research is extended to understanding the performance of both LTE and 5G under normal conditions, load traffic, and high traffic loads. The cyber-resilience metrics are also considered in the performance evaluation by measuring the recovery time of the communication network with LTE and 5G technologies under the influence of a Denial-of-Service (DoS) attack. The cyber-resilience metric, the recovery time, is considered as the ability of the smart

grid communication network to return to its normal state of operation. The recovery time is measured using a moving-average-based sustained stability criterion. That is, the recovery time is measured as a moving average of latency measurements and is declared when this moving-average latency falls within a predefined tolerance range around the baseline derived from normal-operation values. The preliminary stages of this research were implemented for a conference publication, the scope of which evaluated experiments for PMU traffic isolation in smart power grids by utilising the network-slicing capabilities of the 5G communication model [2]. This research also explores the advantages of traffic class differentiation in the smart grid communication architecture and the role that 5G plays in achieving this. The present study broadens the research into understanding how 5G and LTE both work under similar stress conditions in smart grid communication, latency-wise analysis, network utilisation vs. latency analysis, and DoS cyber-resiliency metrics in terms of recovery time.

The present study was designed and developed as a co-simulation of different frameworks: MATLAB/Simulink to simulate the physical layer of the grid, and Comnetsemu as a network emulator. The Simulink platform simulates the physical layer properties of the smart grids and exchanges data pertaining to electrical quantities like the voltage and current values of the smart grid entities with the network emulator. Comnetsemu emulates the network behaviour of the smart grid communication model for both 5G and LTE in this case. The integration of the physical layer and the network layer of the smart grid architecture helps in simulating ideal smart grid behaviour for the experiments. Therefore, the experimental analysis is somewhat closer to real data exchange among the smart grid entities rather than simple communication network emulation. This could provide an ideal situation to assess the effects of changing network conditions on the performance of the smart grid system. The co-simulation also provides a better platform for the comparison of 5G and LTE communication technologies in the smart grid. The major contributions of this research can be underlined as follows:

i. A comprehensive comparative evaluation of 5G and LTE communication models to understand how different communication models perform under stressful traffic conditions in smart power grids.
ii. Evaluation of the LTE and 5G communication models under varying traffic load scenarios to experimentally analyse the relationship between percentage network utilisation and latencies in smart grid communication networks.
iii. PMU-specific latency analysis to understand the individual PMU traffic behaviour under conditions of both low and heavy traffic loads in smart grids.
iv. Evaluation of the cyber-resilience metrics of both LTE and 5G in smart grid communication using post-attack recovery time measurement and experimental analysis of latency degradation during a DoS attack.

2. Related Work

Modern-day smart grid operation is heavily dependent on communication networks. Wireless communication plays a pivotal role in smart power grids; however, it is associated with certain challenges with respect to functions like service isolation, bandwidth, and delay requirements [2]. This creates a necessity for adequate research in smart grid communication networks, analysing their latency requirements, reliability, and availability. Timely data exchange among the smart grid entities is crucial for real-time monitoring systems. Any delay in data exchange in the communication network could cause adverse effects on the stability and operational effectiveness of the smart power grids. Smart grid components like PMUs (Phasor Measurement Units) are critical in Wide-Area Monitoring Systems (WAMSs) to facilitate power system protection and control. Therefore, it is important to

study the latency requirements of the measurement units in the smart grid communication architecture. Studies suggest that there are potential technical and industrial communication technologies that could provide connectivity solutions to the grid [3]. Implementation of 5G in the smart grid has often been considered a solution to address the latency issues and delays in critical smart grid communication [4].

Several studies have investigated the performance of LTE in smart grid communication. The authors of [5] investigated the potential of delivering smart grid demand response traffic in loaded LTE networks; experiments were performed with different amounts of demand response traffic while the LTE network capacity was exceeded. The application of LTE communication systems in low-voltage grids is analysed in [6]; the delay and packet loss measurements are used to evaluate the state estimation accuracy. These studies highlight the importance of network loading and communication performance for specific smart grid applications. Smart grid communication systems rely on cost-effective, scalable, and flexible infrastructure; LTE Cat-M provides cost-effective infrastructure. LTE Cat-M technology shows a lot of potential in smart grid communication; with optimisation, it is possible to achieve a reduction in delay and reduce packet loss [7]. The results indicate that communication delays and packet losses could be reduced with optimisation. With the growing demand for PMUs in the smart grid infrastructure, combining low-power cellular solutions like LTE Cat-M has emerged as a popular option [8]. This approach has reported experimental results for reduced delays and jitter with better network performance. The recent trend shows increasing integration of distributed energy resources into smart power grids, affecting the communication system operation. Integration of LTE communication technology into utility applications like DERs and other smart grid devices seems to be a cost-effective solution that also guarantees network performance efficiency [9]. Delay sensitivity analysis of LTE network-enabled data exchange in microgrids in [10], using a Time-of-Use-aware unsupervised learning-backed microgrid data aggregation scheme, indicates that the microgrids could achieve larger time-sensitive data patterns in LTE networks. These studies demonstrate the implementation of LTE-based communication networks in smart grid applications like demand response, state estimation, PMU monitoring, DER integration, etc. However, the communication architectures and the applications across these studies vary, making a direct comparison across them difficult. Also, their respective contributions are different from a direct comparison between LTE and 5G networks under similar traffic conditions and cyber-resilience evaluations. Many studies have proposed LTE-based wireless network construction models [11]; studies that introduce co-simulation models are also gaining momentum. Platforms like Typhoon HIL and OMNeT++ have been co-simulated to understand the performance of LTE communication networks in smart power grids [12]. Such studies utilise co-simulation for integrating power system and communication network emulation to evaluate their interactions. The motivation for co-simulation comes from such studies, with the present study integrating two simulation platforms (Simulink and Comnetsemu) via co-simulation to compare the LTE and 5G networks in smart grids.

Present-day smart power grids need advanced communication technologies to facilitate efficient, reliable, and secure grid operation. The power grid now possesses the advantages of real-time monitoring and detection, self-healing, and predictive maintenance. Communication networks are the backbone for the efficient functionality of such smart grid entities; 5G and 6G networks are key enablers that support such technological advancements in the grid [13–15]. The evolving smart grid infrastructure also supports data-driven decision models and machine learning-integrated IoT systems—technologies backed by 5G connectivity. Power IoT (PIoT) offers great advancements in smart power grids in terms of generation, transmission, and distribution [16]; 5G networks are pivotal in

supporting these IoT technologies in the grid, playing key roles in reducing the latency of communication networks in grids and, therefore, improving equipment connectivity. This also protects the connection speed and response time of the smart grid entities. Research like [17] accurately depicts that 5G makes the microgrid systems more resilient. As several works contribute towards the deployment of 5G networks in smart power grids, ref. [18] proposes a 5G Field Area Network (FAN) that provides latency reduction and a self-healing mechanism in smart grids. In [19], 5G networks in smart grids also address the security issues arising from the increasing integration of IoT devices into smart grids. The impact of cyber threats in a 5G-enabled smart grid is investigated in [20], with the design of a commercial 5G smart grid testbed that is capable of simulating both the IT and OT layer operations of the grid. These studies demonstrate the effectiveness of 5G in smart grid applications like cybersecurity and cyber resilience. However, the findings of such studies in 5G-enabled smart grids address particular applications and evaluation methods. This motivates further experimental analysis of 5G network performance validation in smart grids under varying traffic loads and cyber-threat scenarios. Therefore, the present study is designed to analyse and compare LTE and 5G smart grid architectures in varying traffic conditions, PMU-specific performance, and cyber-resilience metrics under DoS attacks through recovery time computation.

Network slicing is one such feature that significantly improves the functionality of 5G technology. Network slicing divides the physical network into logical independent networks and, therefore, helps with resource sharing in heterogeneous networks [21,22]. Network slicing also plays a key role in IoT applications under heterogeneous network conditions in smart grids, by allotting dedicated slices for the IoT applications [23]. Trends also indicate the integration of machine learning and artificial intelligence in network slicing and IoT systems in smart power grids. Several studies have implemented 5G to explore its capabilities in delivering low-latency services using network-slicing technology. The authors of [24] illustrated a latency-as-a-service framework to achieve low-latency services in future 5G networks. A cost-optimal model for power grids needs to ensure the Quality-of-Service (QoS) metrics for the communication networks. QoS metrics such as latency, packet loss, reliability, and bandwidth requirements are essential characteristics in deriving a cost-optimal strategy for microgrids. Therefore, a smart grid communication architecture must be equipped to provide QoS and effective resource allocation [25,26]. These requirements motivate the differentiation of services such as Ultra-Reliable Low-Latency Communication (URLLC) and Enhanced Mobile Broadband (eMBB), which represent different service priorities and traffic classes. Recent research addresses different aspects of network slicing, low-latency service provision, resource allocation, and QoS policies. The present study complements the recent research by considering heterogeneous traffic classes, varying traffic loads, and investigating the PMU-specific communication performance for both LTE and 5G network configurations in smart power grids. Furthermore, PMU-specific latency degradation and post-attack recovery time under external DoS attacks extend the experimental evaluation of the present study beyond normal communication-oriented performance models. There are recent works on 5G network slicing that concentrate on guaranteeing service quality for differentiated traffic classes. The author of [27] proposes an interpretable slicing framework for advanced 5G slicing that works on slice admission and resource allocation under normal and degraded conditions for demand response and DER-coordination events. The authors of [28] evaluated the advantages of 5G network slicing with QoS measurement system validation on commercial 5G networks and Intelligent Electronic Devices (IEDs) for three specific smart grid applications: fault location, line differential, and intertrip protection. The results report that the traffic shaping in the slice improved the fault protection in congested conditions by 45.57%. Several works have also

characterised the 5G communication latency in the energy sector. The authors of [29] implemented an open-source 5G testbed that reported mean latencies of 19.2 ms and 10.3 ms for IEC 61850 on two devices, with the scheduling at the gNB being the main constraint. Recent projects have also deployed 5G networks in Wide-Area Monitoring Systems (WAMSs) to evaluate the network performance in terms of delay, reliability, and availability for Smart5Grid [30] and the PNNL 5G Energy FRAME programme [31], which provides a laboratory framework to evaluate 5G for grid use cases. Recent works present 5G as a promising communication technology for smart power grids; however, some of the gaps focus on resource-based scheduling rather than PMU latency under varying traffic loads. Most laboratory-based settings do not consider PMU data, the reporting rates do not consider LTE and 5G comparison under the same experimental conditions, and there is a lack of evidence on communication-level cyber-resilience capabilities.

5G technology has been implemented to ensure security mechanisms in smart grids. The authors of [32] studied 5G-enabled security for power-dispatching control systems in power grids. Such a system aims to ensure cyber resilience in power grids by securing the communication channels using 5G. The 5G security situational awareness system implemented in [33] helps in analysing network security and also in predicting potential security threats. With the integration of zero-trust principles and advanced encryption algorithms, this model enhances the recovery mechanism of smart power grids. Several works illustrate platforms to simulate experiments on 5G, especially with SDN (Software-Defined Networking). These platforms enable extensive research on resilience and cyber-threat mitigation in power grids, especially those with 5G networks [34–36]. Such studies also integrate models like federated learning and split learning into neighbourhood area networks (NANs). Such studies identify the importance of integrating the communication infrastructure with security monitoring, threat detection, and mitigation strategies. However, investigating threat detection capabilities and security mechanisms alone does not suffice to understand the communication performance of critical monitoring systems under cyberattacks in smart grids. It is essential to understand the smart grid cyber-resilience metrics by measuring the post-attack recovery times. The present study investigates the implications of cyberattacks on PMU communication and the time required for the communication architecture to return to its stable state of operation after a cyberattack—that is, post-attack recovery times. However, the evaluations on both LTE and 5G architectures integrating Simulink and Comnetsemu under a co-simulation framework only employ communication-network-level cyber-resilience characteristics under the defined experimental conditions, and they do not generalise to all attack types or security mechanisms.

The literature sheds light on three different aspects: studies on the implementation of LTE and 5G on smart grids, the advantages of network slicing in 5G networks, and experiments on using 5G to implement cyber resilience in power grids. Several studies in smart grids establish the importance of understanding PMU communication, communication latency, and delay. However, these studies do not consistently provide a direct comparative analysis of LTE and 5G in smart grid networks. Most studies on smart communication models are restricted to their behaviour under normal network conditions, while the effects of cyber threats on communication networks receive relatively less attention. Even though several studies investigate the detection and mitigation of cyber threats, degradation in communication latencies and post-recovery attack times are also important aspects that require further investigation and analysis. In particular, the post-attack recovery times are crucial in understanding how quickly the communication networks return to their normal state of operation after a cyberattack. Studies often implement co-simulation to emulate the 5G and LTE communication architecture of smart power grids. However, it is critical to also integrate the comparative analysis of LTE and 5G, 5G network slicing, PMU-specific

latency analysis, and recovery time analysis. The present work addresses these challenges through a co-simulation framework combining Simulink and Comnetsemu, designed with reference to the IEEE 2030 SGIRM. The framework generates smart grid traffic for both LTE and 5G architectures and experimentally evaluates the communication latency, PMU-specific latency, the advantages of network slicing, latency degradation under external DoS traffic flooding conditions, and the post-attack recovery time. By combining these aspects within the same experimental environment, this study provides a comparative analysis of the communication performance of both LTE and 5G and the communication-level cyber resilience under DoS attack conditions.

3. Materials and Methods

3.1. Research Problem

The performance of smart grid communication networks varies with factors like traffic load, network utilisation, and resource allocation, influencing the timely delivery of measurement data for critical grid services like monitoring and control systems. Cyber threats like DoS attacks also cause communication latency degradation and disrupt timely data delivery in critical traffic classes. Therefore, studying the communication network performance and investigating the cyberattack-induced network degradation and post-attack recovery mechanisms are essential to understand the reliability and cyber resilience of smart grid communication architectures. With this motivation, the present study is designed to address the research problem of a comparative evaluation of the LTE and 5G networks in smart grid communication under varying traffic load conditions and DoS attack scenarios. Therefore, the present experimental analysis evaluates the PMU-specific communication latency, the individual PMU traffic behaviour, and the corresponding network utilisation under varying traffic loads, along with latency degradation and post-attack recovery times during a DoS attack.

3.2. Research Objective

The primary objective of the present study is to investigate the performance of smart grid communication networks by experimentally evaluating the PMU-specific communication latencies and communication-level cyber-resilience metrics of both LTE and 5G network configurations, integrating a Simulink–Comnetsemu framework. The specific research objectives are as follows:

i. A comprehensive comparative evaluation of 5G and LTE communication models to understand how different communication models perform under stressful traffic conditions in smart power grids.
ii. Evaluation of the LTE and 5G communication models under varying traffic load scenarios to experimentally analyse the relationship between percentage network utilisation and latencies in smart grid communication networks.
iii. PMU-specific latency analysis to understand the individual PMU traffic behaviour under conditions of both low and heavy traffic loads in smart grids.
iv. Evaluation of the cyber-resilience metrics of both LTE and 5G in smart grid communication using post-attack recovery time measurement and experimental analysis of latency degradation during a DoS attack.

3.3. Research Methodology

This study implements an experimental methodology that integrates Simulink-based simulation and Comnetsemu-based communication network emulation to investigate smart grid communication architectures and the communication-level smart grid cyber resilience. The

scope of this study is to perform an experimental analysis of the PMU-specific communication latency under varying traffic loads, network utilisation, and post-attack recovery times during a DoS attack scenario for LTE and 5G network configurations. This achieves a comparative investigation of LTE and 5G network configurations for applications in smart grids.

The experimental framework in the present study was designed with Simulink and comnetsemu, where Simulink models the physical-layer power system environment and generates the electrical quantities for measurement-related traffic, while comnetsemu is used to emulate the communication network and its traffic-handling behaviour. Both LTE and 5G network configurations are evaluated under the bandwidth constraints, the varying traffic loads, and the network parameters defined in the model design. The 5G configuration in the present study implements OVS traffic classification and queue-based prioritisation to differentiate the traffic classes and analyse the effects of 5G network slicing. The present experimental framework employs a network emulation of the traffic differentiation; however, it does not represent a 3GPP-compliant 5G radio access and core network.

The experimental methodology consists of four distinct stages:

i. The generation of smart grid measurement data-based traffic using Simulink modelling and its transmission through the corresponding communication network emulation in comnetsemu. Both LTE and 5G networks are emulated in comnetsemu as separate experiments and are implemented based on their respective experimental design and network parameters.
ii. The traffic load in both LTE and 5G implementations is varied from low to high to investigate the PMU-specific communication latencies and the network utilisation. The reported results are used for the comparative analysis of LTE and 5G network configurations under varying traffic loads in smart grid communication.
iii. The PMU-specific latency measurements are also analysed for individual PMU streams for both low- and high-traffic-load conditions to understand the changes in the PMU-specific communication with increasing network loads.
iv. External DoS traffic flooding is induced in the experimental framework to evaluate the communication latency degradation during cyber threats for both LTE and 5G configurations. At the end of the DoS attack, the latency behaviour is analysed to report the post-attack recovery time, or the time required for the communication performance to return to its stable baseline operation. The post-attack recovery time is considered a metric to evaluate the cyber resilience of the smart grid under the investigated network configurations of LTE and 5G.

The major performance metrics considered for the present experimental evaluation are the communication latency, the PMU-specific communication latency, the network utilisation, the latency degradation during cyberattacks, and the post-attack recovery time. Both LTE and 5G configurations are analysed under different traffic loads from low to high; the corresponding latencies and the network utilisation are evaluated to study the relationship between the increasing traffic loads and the communication network performance. In order to achieve a fair comparison, the same experimental conditions were retained wherever applicable for both LTE and 5G. Individual PMU-specific latencies were also analysed to understand their behaviours under low-to-high traffic. An external DoS traffic flooding attack was induced on both LTE and 5G configurations; the latency measurements were obtained during the DoS attack scenario and were compared against the latency requirements of normal operating conditions to understand the implications of cyber threats for the communication network performance. These results constitute the attack-induced latency degradation and are compared for both LTE and 5G networks. The post-attack recovery time metrics are used to evaluate the communication-level cyber resilience of the LTE and 5G networks in smart grids. The end of the attack defines the start of the recovery analysis.

A 10-sample moving average was applied to the PMU-specific latencies, and the first point at which the moving average remained within ±5% of the stable baseline latency was recorded. The experimental analysis in its present form is limited to the network configurations, traffic conditions, defined metrics, and external DoS scenarios evaluated in this study.

4. Proposed System Architecture

The proposed system architecture provides a co-simulation framework that integrates the physical layer and communication network layer of the smart power grids to evaluate the heterogeneous smart grid traffic in both LTE and 5G networks. The co-simulation framework implements power grid physical-layer simulation in Simulink and communication-network emulation in Comnetsemu. This co-simulation framework generates realistic smart grid traffic for the experimental evaluation of smart grid cyber resilience. The proposed system consists of three distinct layers: the power system physical layer, communication layer, and a control layer. The physical-layer simulation in Simulink simulates the electrical infrastructure of the power system with a transformer, distributed energy resource (DER), Energy Storage System (ESS), consumer load, and the corresponding voltage and current measurement modules.

These smart grid entities simulate the grid behaviour and represent a smart power grid system. The voltage and current measurement modules in the simulation form the Phasor Measurement Units (PMUs), which extract the values of electrical quantities and send the corresponding data to the communication layer of the proposed framework. Comnetsemu emulates the smart grid communication network, which handles the network traffic. For the present study, two types of smart grid communication networks are emulated in comnetsemu: LTE and 5G, each with its own distinct architecture. Experimental evaluations are also made possible to understand the recovery time associated with the communication technologies by simulating normal and cyber-threat operating conditions. For the sake of this study, we have only evaluated the LTE and 5G networks under DoS attack; therefore, this study does not claim any generalisation to all threat types. For the slice allocation in the 5G networks, and for the latency requirement analysis of the smart grid communication models, the IEEE 2030 Smart Grid Interoperability Reference Model (SGIRM) is referenced. Figure 1 provides an overall block diagram representation of the proposed co-simulation model.

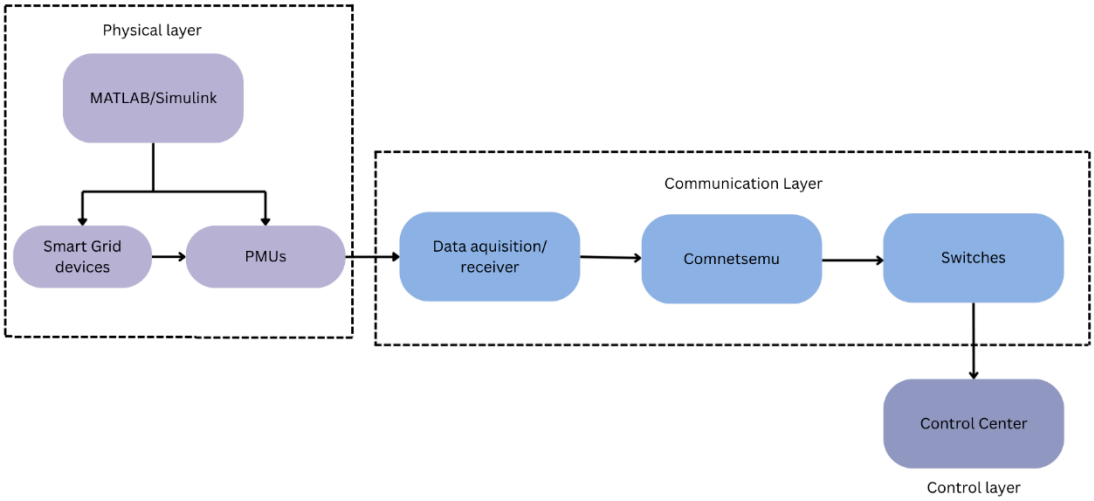


Figure 1. Block diagram representation of the proposed co-simulation framework.

4.1. Simulink-Based Physical Power System Layer Simulation Architecture

The physical power system layer models the electrical structure of the smart power grids in this particular study, and it was simulated in MATLAB/Simulink. This layer generates the electrical measurements of the corresponding smart grid modules and transfers this data to the communication network emulator as PMU traffic. As shown in Figure 2, the Simulink model consists of a transformer, consumer load, DERs (distributed energy resources), and ESSs (Energy Storage Systems). The voltage and current values are monitored and collected from the operating conditions of the consumer load, DERs, and ESSs. The electrical quantities (voltage and current) are measured by the voltage and current sensors, respectively. These sensors together represent the Phasor Measurement Units (PMUs) in the physical-layer simulation. The consumer load module in the simulation represents the conventional electricity demand in a smart grid system. The DERs in the proposed system are intended to introduce the behaviour of a distributed power generation system that contributes to the heterogeneous nature of the smart grid environment. In addition to the conventional consumer load and the distributed generation, the ESSs represent energy storage modules that act as a distributed energy resource. These smart grid entities help in simulating a conceptual power system physical layer. The integration of the DER and ESS components in the smart grid environment is crucial in introducing the effects of the penetration of heterogeneous devices into the smart grid traffic. The electrical quantities measured from all three modules are collected by independent PMUs: PMU1, PMU2, and PMU3 for the consumer load, DERs, and ESSs, respectively. For experiments on smart grid communication network performance and cyber resilience, the smart grid modules in the power system physical-layer simulation are represented by direct electrical components available in Simulink; therefore, we refrained from developing complex subsystems for these individual modules.

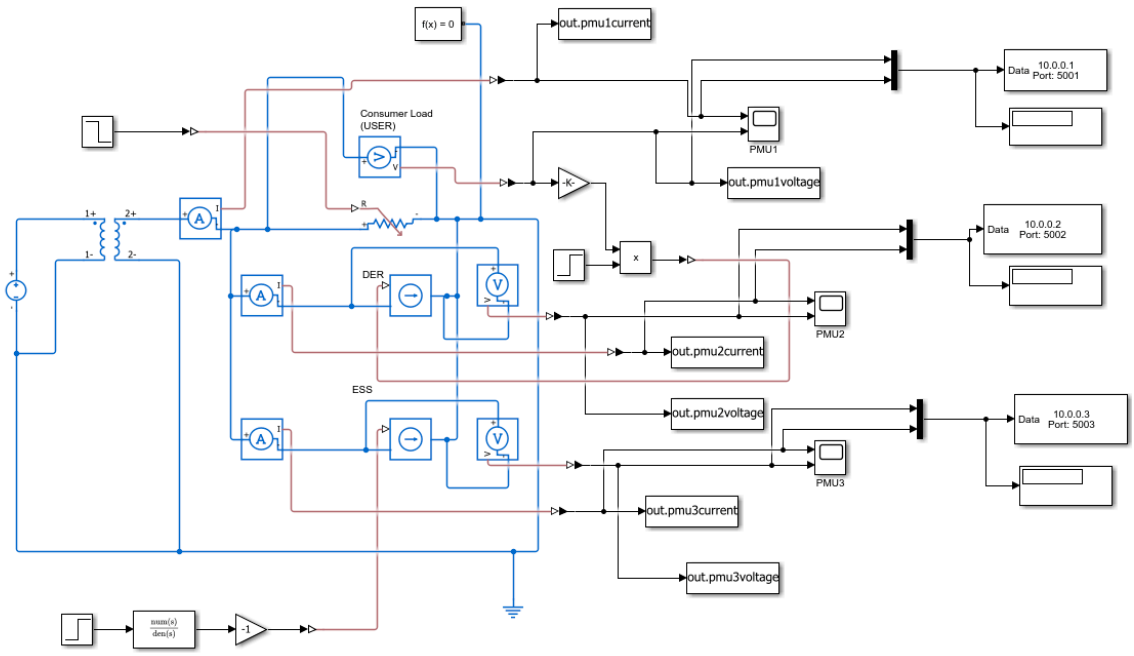


Figure 2. Simulink model for the physical power system layer of the proposed system.

4.2. Comnetsemu-Based Communication Architecture: LTE

The communication network of the proposed system was emulated in Comnetsemu. This emulation represents smart grid communication, making it possible to evaluate network performance. The overall architecture of the LTE-based communication network

implementation is shown in Figure 3. The LTE network is designed as an access network component representing the LTE eNodeB and a core network component representing the Evolved Packet Core (EPC), with a set of hosts corresponding to the smart grid entities in the physical-layer simulation and the control centre. The LTE communication architecture in comnetsemu consists of a centralised access switch, a core network switch, and seven host nodes. The control centre is indicated by the host h1, whereas the smart grid entities form hosts h2–h7, as described in Figure 2. The host connections in comnetsemu are implemented with TCLink, where components like PMU1, PMU2, PMU3, consumer load/user, DERs, and ESSs are connected to the LTE access network switch, s1. Each of these component nodes is connected to the access network switch with a bandwidth of 10 Mbps and a configured delay of 5 ms. The EPC, or the core network segment switch, s2, is connected to the access network switch s1 via TCLink, with a bandwidth of 10Mbps and a delay of 5 ms. This EPC segment is connected to the control centre host h1. Therefore, communication paths are established between the smart grid components and the control centre node. The control centre, h1, uses the IP address 10.0.0.100/24. Table 1 represents the relationships between the loads, PMUs, and the network nodes.

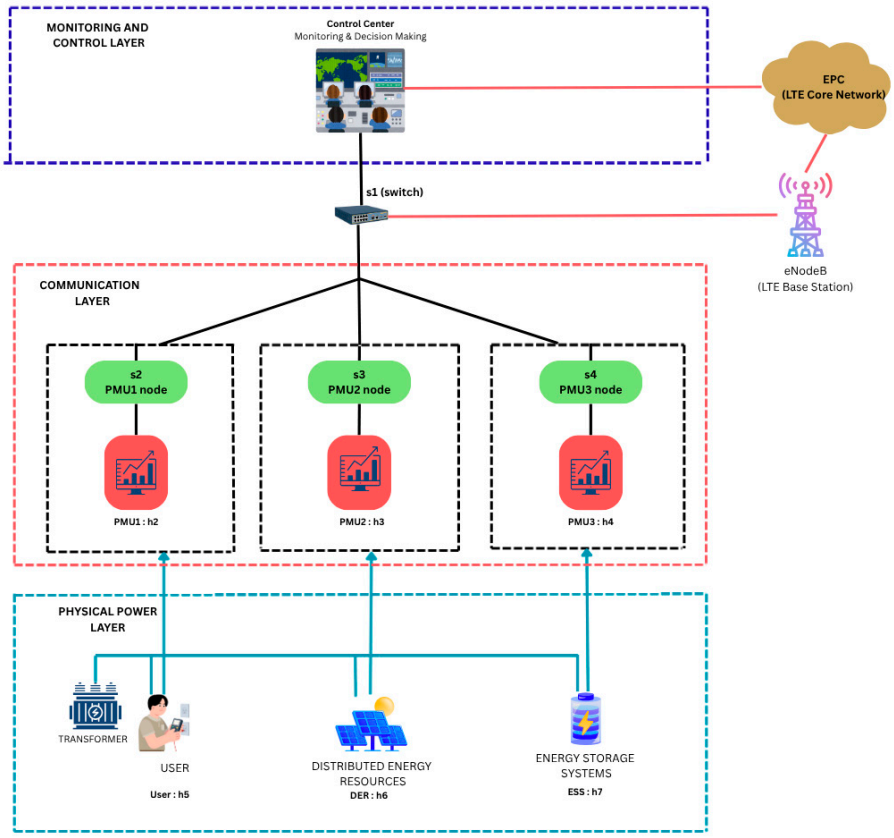


Figure 3. Proposed system architecture for LTE-based experiments.

Table 1. Relationships between the loads, PMUs, and network nodes.

Physical-Layer Component	Network Node	Corresponding PMU	PMU Network Node
Consumer Load/User	h 5	PMU1	h 2
DER	h 6	PMU2	h 3
ESS	h 7	PMU3	h 4

The PMUs (PMU1, PMU2, and PMU3) are represented by the hosts h2, h3, and h4, respectively. The PMU nodes are responsible for receiving the data generated by the physical-layer power system model in Simulink. The rest of the smart grid components are modelled as h5, h6, and h7 for consumer load/user, DERs, and ESSs, respectively. With this, the network topology is in direct concurrence with the physical-layer simulation and thereby allows the traffic generated by the physical layer to be directly mapped to its corresponding network node. The control centre in the proposed system is a representation of the monitoring and control layer, which is the backbone of decision-making in the smart power grids. The control centre is the final endpoint of the traffic generated by the smart grid modules, and this data is later utilised for the performance evaluation of the smart grid communication networks. The PMU traffic generation process is the same for the experiments on both LTE and 5G technologies; therefore, this evaluation gives a fair comparison.

4.3. Comnetsemu-Based Communication Architecture: 5G

The proposed 5G communication network was emulated in Comnetsemu using an Open vSwitch (OVS) as a virtual switch and an SDN (Software-Defined Networking) controller. The scope of this study emulates a 5G-based communication network that is capable of differentiating smart grid traffic, generated through the physical-layer simulation in Simulink. The overall architecture of the proposed 5G-based network emulation is shown in Figure 4. The 5G network design implements a main network switch for the gNB and three cluster switches that connect the PMUs and their corresponding smart grid components. The main switch, s1, is responsible for introducing traffic differentiation in the network using multiple QoS queues. The overall network design consists of one main switch (s1), three cluster switches (s2, s3, and s4), one control centre host, three PMU hosts, and three smart grid entity hosts. The overall architecture realises the network and traffic management behaviour of a gNB-side aggregation using the OVS-based topology rather than a complex physical or software-based 5G gNB protocol stack. The cluster switches are connected to the main switch s1, using links with a 1ms delay. The control centre h1 is also connected to the main switch s1 with a 1ms link. This network framework provides a controlled environment to evaluate traffic differentiation while using 5G in smart power grids.

The proposed 5G network architecture is realised over SDN to achieve a programmable and controlled communication network emulation. This 5G network performs traffic differentiation using network slicing; therefore, instead of creating physically independent networks, the smart grid traffic is differentiated into logical virtual networks. The QoS policies are implemented to separate the smart grid traffic into three different slices: Ultra-Reliable Low-Latency (URLLC) slices for the PMU measurements, Enhanced Mobile Broadband (eMBB) for the consumer load/user applications, and Massive Machine-Type Communication (mMTC) for the DER and ESS modules. That is, although the traffic classes in the proposed 5G-based smart grid network design share the same physical network, they are under different queueing and, therefore, have different resource allocations. A smart grid communication network produces vast amounts of heterogeneous traffic; without traffic differentiation, background traffic competes with the traffic of critical applications to share the same resources. The network-slicing technology in 5G networks addresses this problem by assigning a high-priority queue to the critical application traffic. In a smart grid communication network, measurement devices like PMUs are allocated the highest priority. This is fundamental, since the measurement devices play crucial roles in delivering timely data to real-time monitoring systems in smart grids. Therefore, real-time monitoring and threat-mitigation mechanisms are heavily dependent on measurement devices like PMUs for efficient grid operation. It is important that PMU traffic be considered the highest

priority and that PMU-specific latency analysis be conducted. The slice mapping with the corresponding queue allocation is as given in Table 2.

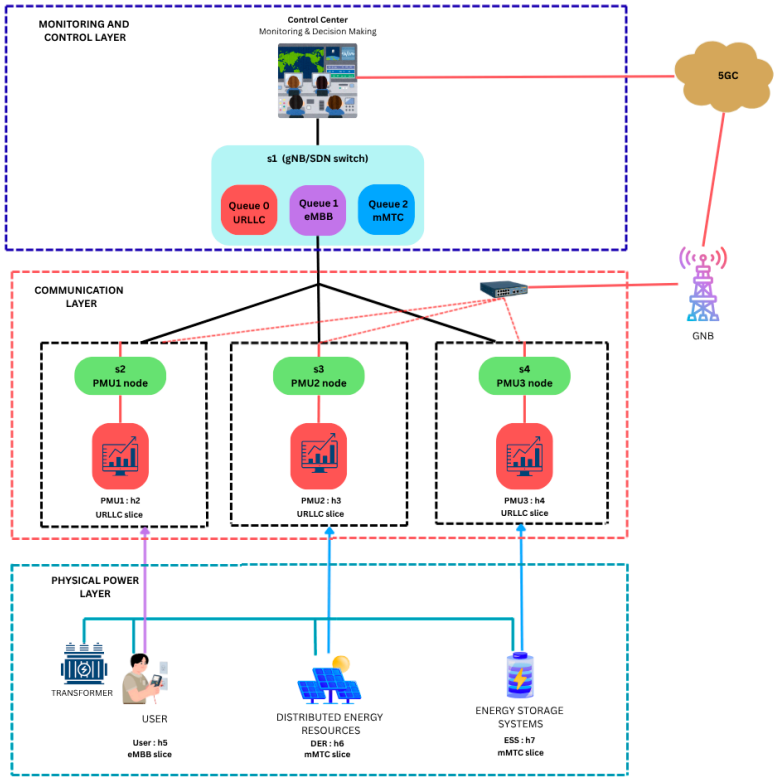


Figure 4. Proposed system architecture for 5G-based experiments.

Table 2. Slice mapping.

Smart Grid Entity	Slice Type	QoS Priority
PMU1	URLLC	Queue 0 (Highest)
PMU2	URLLC	Queue 0 (Highest)
PMU3	URLLC	Queue 0 (Highest)
User application/consumer load	eMBB	Queue 1 (Medium)
DER	mMTC	Queue 2 (Lowest)
ESS	mMTC	Queue 2 (Lowest)

The PMUs (PMU1, PMU2, and PMU3) are indicated by the hosts h2, h3, and h4, respectively. The PMU-to-corresponding physical-layer component mapping and the corresponding host mapping are the same for both LTE and 5G network architectures. As stated earlier, the traffic generation process for the PMUs was kept the same for experiments on both LTE and 5G to establish a baseline comparison. All three PMU traffic streams used URLLC slicing and were assigned to Queue 0, the highest-priority queue. The user application or the consumer load hosts broadband services and was therefore allocated the eMBB slice and Queue 1. Queue 1 provides an intermediate priority class and allows the user applications to exist alongside the PMU traffic without consuming the same network resources. The DER and ESS modules were allotted the mMTC slice with Queue 2; this lower-resource queue configuration assigns the lowest priority to distributed smart grid devices and background traffic. The flow rules were allocated by the switch s1 and were identified based on their UDP port numbers. The UDP port numbers assigned to the smart

grid modules are as follows: for PMUs, PMU1 is port 5001, PMU2 is port 5002, and PMU3 is port 5003; the DER and ESS modules are assigned to port 6000; and the user applications are allotted the default traffic. Queue 0 has the highest resource allocation, since it supports critical PMU measurements; Queue 1 is supported with intermediate resource allocation; and Queue 2 has the least amount of resources allocated to it. Therefore, the resource allocation is highest for URLLC, medium for eMBB, and lowest for mMTC. Without the traffic class differentiation and the corresponding resource allocation, the PMUs, DERs, ESSs, and user applications together compete for the same resources. This causes latency degradation and communication delay in smart grid communication, especially in cases of network congestion.

The IEEE 2030 SGIRM provides insights into the smart grid architecture, and the proposed framework references this standard for modelling the smart grid communication network and, later, for the latency requirement analysis. The proposed methodology has relied on this standard primarily for slice mapping and resource allocation. Therefore, the IEEE 2030 SGIRM provides a baseline architecture for the experiments in this research. The proposed smart grid communication model emulates the functionality of the 5G access network node and the core via OVS-based network components rather than a full 3GPP 5G protocol stack. This approach is preferred because the preliminary objective is to evaluate the network-level performance and cyber resilience of the 5G-based smart grid communication, rather than a complete 5G RAN or 5GC. This study also evaluates how network-slicing technology in 5G networks helps smart grids achieve shorter recovery times during cyber threats compared to LTE.

The communication bandwidth for both LTE and 5G was configured to 10 Mbps to understand the network performance within a common capacity constraint feasible for comparative evaluation. This bandwidth setting helps to validate the performance of the shared smart grid communication link carrying aggregated PMU measurements along with other traffic generated by the smart grid entities. In practice, the bandwidth requirements of smart grid communication infrastructure depend on the PMUs sharing the network, their reporting rates, message sizes, and protocol overhead, as well as the measurement streams sharing this communication interface. Previous studies on distribution system PMUs indicate that aggregating measurements from a large number of PMUs can produce an aggregate communication requirement close to 10 Mbps [37]. Therefore, this bandwidth provides a controlled operating condition where the effects of increasing traffic load, traffic prioritisation, and network slicing on the PMU communication in smart grids can be investigated. Both LTE and 5G were configured with the same bandwidth of 10 Mbps to provide a fair comparison by negating the influence of unequal link capacities. The bandwidth of 10 Mbps was considered an experimental constraint for the present study and not a generic bandwidth requirement for PMU applications.

The present study implemented the 5G communication network emulation using Comnetsemu with OVS (Open vSwitch)/SDN (Software-Defined Networking) mechanisms to provide the network topology, packet forwarding, and configurable traffic management. This implementation represents the communication links between the smart grid entities: Phasor Measurement Units (PMUs), distributed energy resources (DERs), Energy Storage Systems (ESSs), and the user application. The communication network was configured with bandwidth constraints, traffic classification rules, and OVS queues to manage the network traffic. These mechanisms also provide differentiated traffic classes for critical PMU traffic and other smart grid traffic classes linked to the Enhanced Mobile Broadband (eMBB) and Massive Machine-Type Communication (mMTC). Such a configuration allows a controlled evaluation of the traffic load, queue-based prioritisation, and differentiated traffic handling within the communication architecture. With that being the case, it is

important to understand that the present implementation does not configure a complete 3GPP-compliant system. In particular, the OVS/SDN mechanisms approximate the traffic management functions associated with network slicing and do not reproduce the entire 5G New Radio (NR) access network, gNodeB (gNB) functionality, 5G core network (5GC), or the end-to-end slice management procedures. Therefore, the experimental framework in its current state can only be interpreted as an SDN-based network emulation of communication and traffic differentiation behaviour rather than a complete implementation of 5G network slicing.

The experimental analysis evaluates the latency requirements in both LTE and 5G communication networks in smart grids. In the 5G communication network, since the traffic classes are divided into three slices based on network slicing, the total traffic at the core switch S1 is the sum of the traffic arrival rates of each of these traffic classes. Therefore, the PMU-specific latency calculation in 5G can be interpreted in two different ways: the latency for the network without network slicing, and the latency for the network with network slicing. These experiments have been performed and validated in a previous study and were reported in the authors' conference publication. The previous experiments were conducted in the context of understanding the role of network slicing in PMU communication latency in smart grids. The study was divided into two major experiments: with and without network slicing. That is, with network slicing, the 5G network provides traffic classes and a dedicated QoS queue; without network slicing, the same network resources are shared by all of the smart grid entities. These results are crucial in establishing a baseline for the present work; however, the focus of the present study is broader. The present work is focused on the comparative analysis of 5G and LTE technologies in smart grid communication. This work also performs the experimental evaluation of both LTE and 5G networks under DoS threat scenarios and analyses the recovery time for both architectures under the same network threat conditions. The previous study only reports the role of network slicing in 5G-based smart grid communication, whereas the present work is a substantial extension of the preliminary study. The latency analysis results with and without network slicing in 5G are reported in the previous study. The corresponding latency computation method is derived from the previous study. Therefore, the latency computation can be given as follows:

The latency T_{NS} without network slicing is

$$T_{NS} = T_{tx} + T_{queue}^{NS} + T_{proc} + Tprop \tag{1}$$

where

- T_{queue}^{NS} is the queueing delay;
- T_{tx} is the transimission delay;
- T_{proc} is the processing delay;
- $Tprop$ is the propoagation delay.

Meanwhile, the queue approximation is

$$T_{queue}^{NS} = \frac{1}{\mu - \lambda_{Total}} \tag{2}$$

where μ is the service rate of the switch and λ_{Total} is the total traffic arrival rate at the core switch.

The network latency T_S with slicing for the URLLC queue is

$$T_S = T_{tx} + T_{queue}^{S} + T_{proc} + T_{prop} \tag{3}$$

The queue approximation is

$$T_{queue}^{S} = \frac{1}{\mu_U - \lambda_U} \tag{4}$$

where μ_U is the service rate for the URLLC slice.

Therefore, the percentage improvement in the latency is calculated as follows:

$$I = \frac{T_{NS} - T_S}{T_{NS}} \times 100 \quad (5)$$

4.4. Experimental Framework for Cyber-Resilience Evaluation

The cyber-resilience experiments were designed to investigate the latency degradation and recovery time for both LTE and 5G. Therefore, we evaluated the normal operation, attack-induced latency degradation, and the recovery phase for the smart grid communication models. With the growing cyberattacks in modern-day smart power grids, it is essential to investigate which communication architectures can provide better network performance and lesser recovery time during a cyberattack instance. Therefore, the latency requirement analysis alone does not qualify as a suitable metric of evaluation for smart grid communication networks. The network performance may completely change when the resources are forced into congestion by malicious traffic. The present study only considers a DoS attack for the experimental evaluation; therefore, we do not claim any generalisation. The primary objective of this research is to understand how different smart grid communication models behave under a DoS attack or a cyber threat; therefore, the DoS attack was not designed with particular real-world attack tools or exploits. The DoS threat was introduced on a normal smart grid communication network, thereby ensuring that the network contained normal traffic as well as attack traffic at the same time. This enables the experimental analysis of normal operation, latency degradation during attack, and recovery time. The DoS attack was induced by congesting the network by generating additional traffic; this helps to investigate how the 5G architecture, especially with network slicing, would react to network congestion. Therefore, these experiments analyse whether network slicing in 5G networks can help reduce the impact of cyberattack-induced traffic congestion in smart grids, and they also determine which smart grid communication model (5G or LTE) performs better during cyber threats. The smart grid communication models emulate smart grid entities such as user applications, DERs, and ESSs, allocated to nodes h5, h6, and h7, respectively. These smart grid components from the physical-layer simulation are linked to their corresponding nodes in the communication network emulation. The experiments on DoS attacks were designed to analyse these individual network nodes rather than the network as a whole. This level of experimentation is also important because the degradation levels differ from component to component even though they belong to the same network. The network slicing and traffic differentiation are also different for these smart grid components; therefore, the underlying architecture treats each traffic class differently during congestion as well. Network node-wise experimentation helps in evaluating whether the degree of degradation is different for different traffic classes in the same backbone architecture. Both LTE and 5G architectures were subjected to the same experimental evaluation, and the results of both were compared. The major metric that evaluates the cyber resilience of the smart grid communication model is the recovery time. Once the DoS attack was terminated, the normal PMU traffic was analysed to understand when the system returns to stability. The recovery time was determined based on a moving average of the reduction in the latency value. The existing research on smart grid communication models only considers the latency requirements during normal grid operations; the proposed framework integrates an experimental evaluation of the latency requirements during both normal operating conditions and those of network congestion caused by a cyber threat. The co-simulation framework proposed in this study helps maintain the same normal operating conditions as a baseline for cyber-resilience experiments with both LTE and 5G. The proposed system architecture also aims to understand, through experiments,

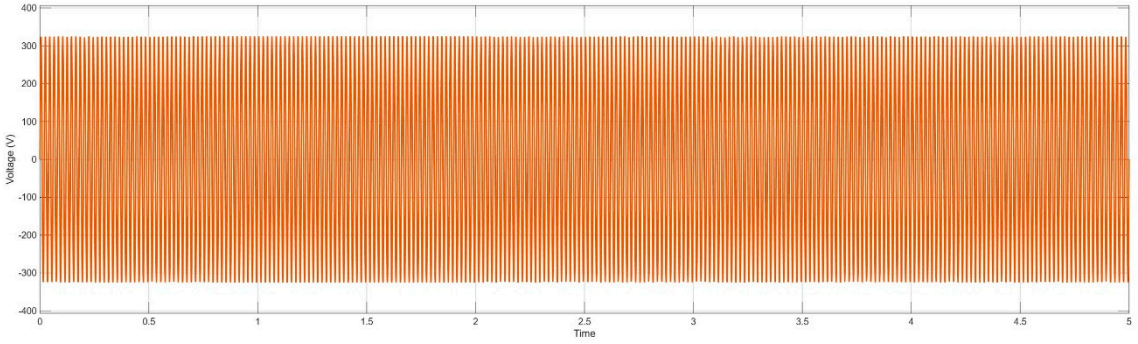
the advantages of network slicing in improving latency and network performance in 5G as compared to LTE in smart power grids.

5. Results and Discussion

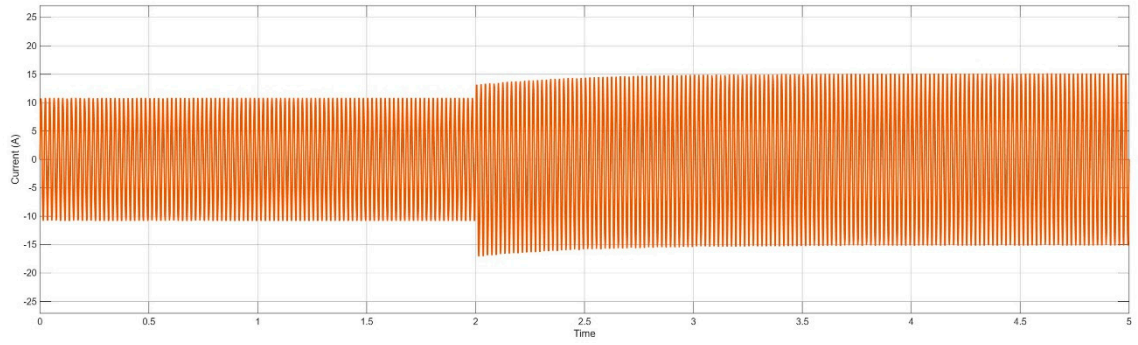
5.1. Validation of Physical Power System Layer

The physical power system layer of the proposed system was simulated in MATLAB/Simulink. The simulation, consisting of smart grid components such as the consumer load/user, DERs, and ESSs, was intended to validate that the physical layer generates stable, physically meaningful voltage and current values that are collected by the PMUs and transferred to the communication layer. The results in this section only validate the physical-layer power system simulation in Simulink, not the overall architecture of the proposed system. For the experimental evaluation, the smart grid components were simulated with direct electrical components from the Simulink library rather than developing complex subsystems.

The resulting waveforms of the consumer load/the user application simulation in the smart grid for a time period of 5 s are given in Figure 5. The voltage waveforms show a peak of 320–325 V and do not present any interesting variation throughout the 5 s simulation time. The 320 V peak voltage is consistent with the 230 V RMS voltage value, representative of a nominal low-voltage AC supply. The current waveform also presents stable operation, within the range of −11 A to +11 A with an 11 A peak current. The comparatively stable voltage and current waveforms indicate a relatively stable operating condition for the consumer load. The absence of any distortions in the resulting waveforms of the consumer load simulation provides consistency between the electrical supply and the consumer load in the proposed physical-layer smart grid simulation.



(**a**)



(**b**)

Figure 5. (**a**) The voltage waveform and (**b**) the current waveform of the consumer load.

Figure 6 represents the results of the validation of DERs in the proposed smart grid model. The voltage waveform is periodic throughout the simulation time of 5 s, with a peak of 320 V. The DER current waveform shows a dynamic response, with the current values between −11 A and +11 A until the transition at 2 s, beyond which the current amplitude is between −17 A and +15 A. This indicates that DERs are capable of supporting the changes in the operating conditions without losing synchronisation with the AC voltage. The DERs also do not induce any instability in the smart grid operation, as there is no significant stability loss during the transition at 2s. The DER current transition at 2s is the response to their power contribution to the overall smart grid system based on the control signal integrated in the Simulink model. However, the DER current and voltage waveforms confirm the component's ability to be a dynamic source rather than a steady-state generator.

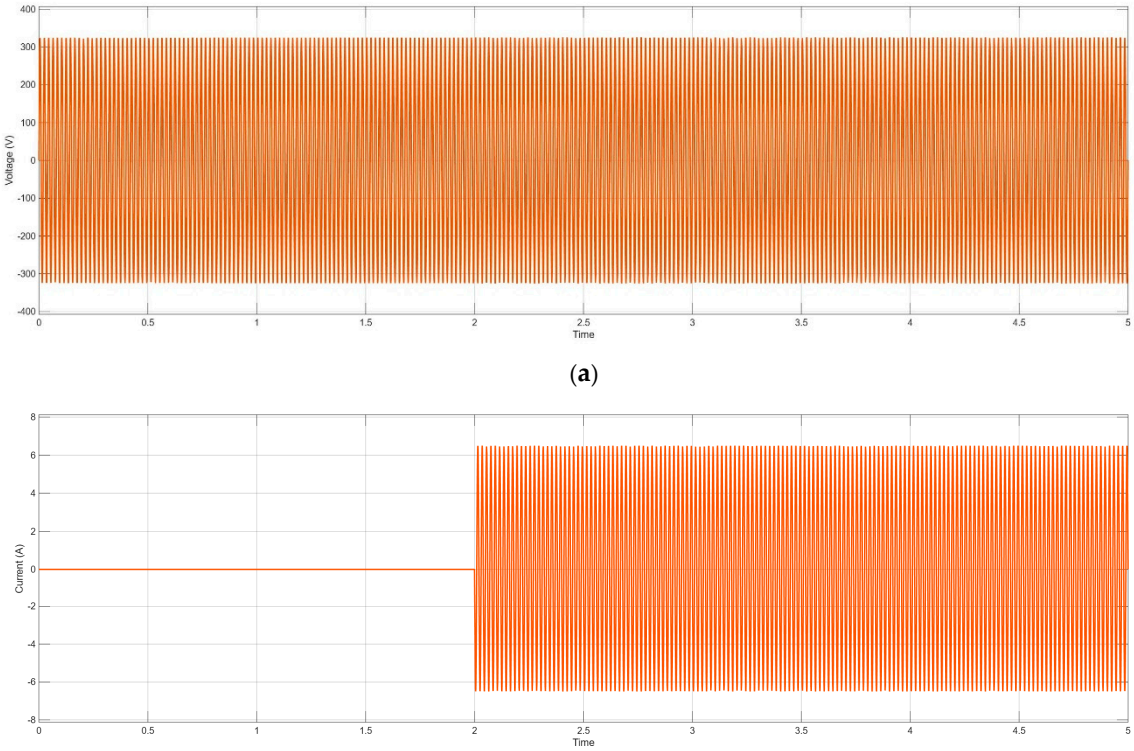
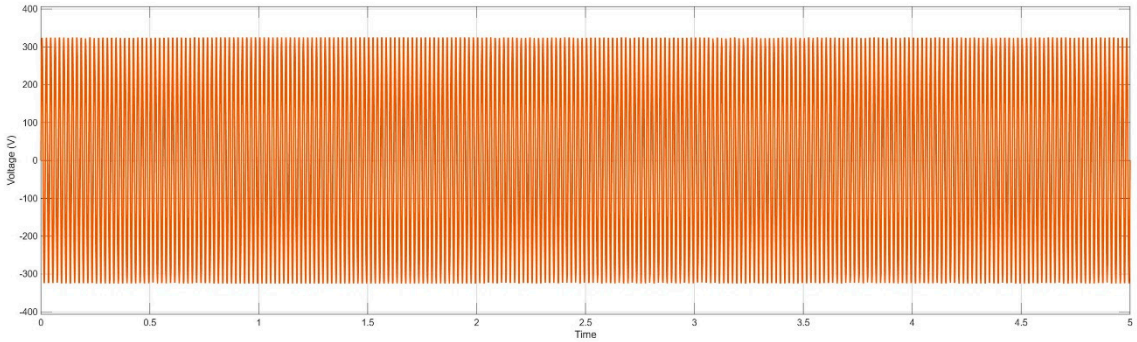
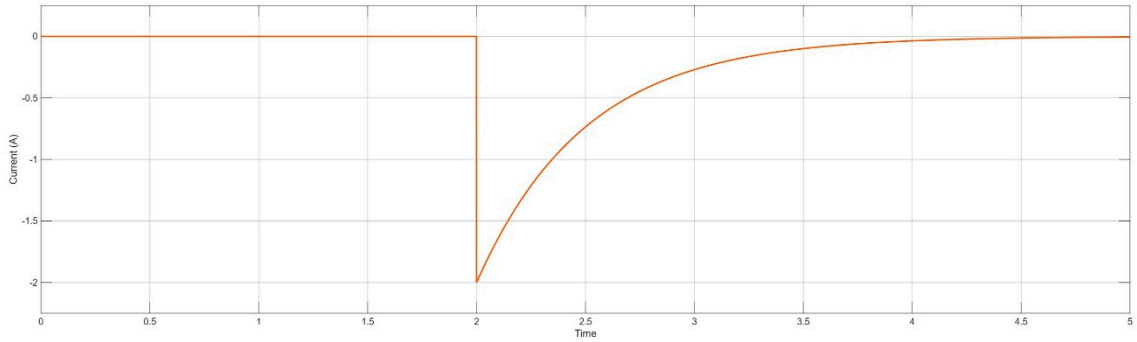


Figure 6. (**a**) The voltage waveform and (**b**) the current waveform of the DERs.

Figure 7 represents the voltage and current waveforms of the ESS module in the proposed smart grid system. The resulting voltage waveform from the ESS simulation retains a sinusoidal nature with a peak voltage of 320 V. The voltage waveform does not show any unstable operation during the transient change at 2 s and, therefore, remains electrically connected to the stable AC interface. The ESS current remains at 0 until switching at 2 s, indicating that the ESS module was not exchanging current with the AC network during the initial operating condition. At 2 s, the current reaches its initial magnitude of almost −2 A, and it returns to 0 by the end of the 5 s simulation time. These results confirm that the ESS module in this simulation replicates a controlled or transient interaction where it is activated by a switching instant and then returns to its steady operating condition. Although the current waveform shows transients, the voltage waveform remains stable and sinusoidal; that is, the ESS module does not cause any voltage disturbance for the simulated scenario.



(**a**)



(**b**)

Figure 7. (**a**) The voltage waveform and (**b**) the current waveform of the ESS module.

The results of the physical-layer simulation indicate that the physical layer is capable of representing both steady-state behaviour and dynamic operating conditions. The consumer load maintains stable waveforms for both current and voltage characteristics, indicating steady-state behaviour. The DERs present a controlled change in the magnitude of current after 2 s, and the ESS module shows an active transient nature at 2 s, followed by a gradual return towards zero. The voltage waveforms of all three smart grid components retain stability throughout the simulation. The peak voltage of 320 V is also the same throughout the simulation. For the DERs and ESS, the voltage waveforms remain stable during the current transients. These attributes confirm that the simulation does not produce unrealistic voltage fluctuations in the provided operating conditions. Therefore, the physical-layer power system simulation can simulate both the normal steady-state operation and the corresponding changes to the operating conditions.

5.2. Communication Latency Validation—LTE vs. 5G

The network performance of the proposed communication-layer architecture was validated under conditions of different traffic loads and network utilisation. The performance of both LTE and 5G technologies was compared via PMU-specific latency analysis and average latency analysis for smart grid communication. The latency analysis was performed under two distinct load conditions: low traffic load, and high traffic load. Both LTE and 5G architectures were configured for an overall bandwidth of 10 Mbps; therefore, traffic loads up to 10 Mbps were considered for low-load analysis, and loads of 15 Mbps to 60 Mbps were considered for high-traffic analysis. The overall results show that the 5G network performs better than LTE with lower latencies throughout the experimental scenarios.

1. Case 1: Low-Traffic Conditions

The low-traffic-load conditions were mapped to traffic loads from 1 Mbps to 10 Mbps for both LTE and 5G. Figure 8 gives the results of the average latency analysis of both

LTE and 5G networks in smart grid communication. The 5G network maintains lower latency values with increasing load as compared to LTE. At 10 Mbps, the LTE latency is 46.8 ms, whereas that of 5G is 32.5 ms. This indicates a latency reduction of almost 30% for 5G with respect to LTE. The increase in latency ranges is also gradual, and there is no sudden latency degradation. The PMU-wise latency analysis for low traffic loads is shown in Figure 9a. Under conditions of low traffic load, the results of LTE show relatively stable latency across all three PMUs. LTE also provides uniform latency across all of the PMUs, and there is a comparatively small difference among the PMU latencies under low-traffic conditions. In the case of 5G, PMU-wise latency analysis shows slight variation in the latencies; however, all three PMUs follow a similar trend overall. Therefore, the 5G latency remains considerably low for PMU-wise latency analysis as compared to that of LTE. The reduction in latency values under 5G as compared to LTE can be directly attributed to the traffic differentiation and isolation caused by network slicing in 5G. That is, in 5G, the PMU traffic is logically separated from the background traffic, with the allocation of a URLLC slice. The highest-priority queue allocation helps prevent resource contention for PMU communication. Therefore, network slicing in 5G helps reduce packet queuing and network congestion effects and prioritises the PMU traffic, leading to lower latency values. Table 3 shows the quantitative results of the latency analysis at low traffic for both LTE and 5G.

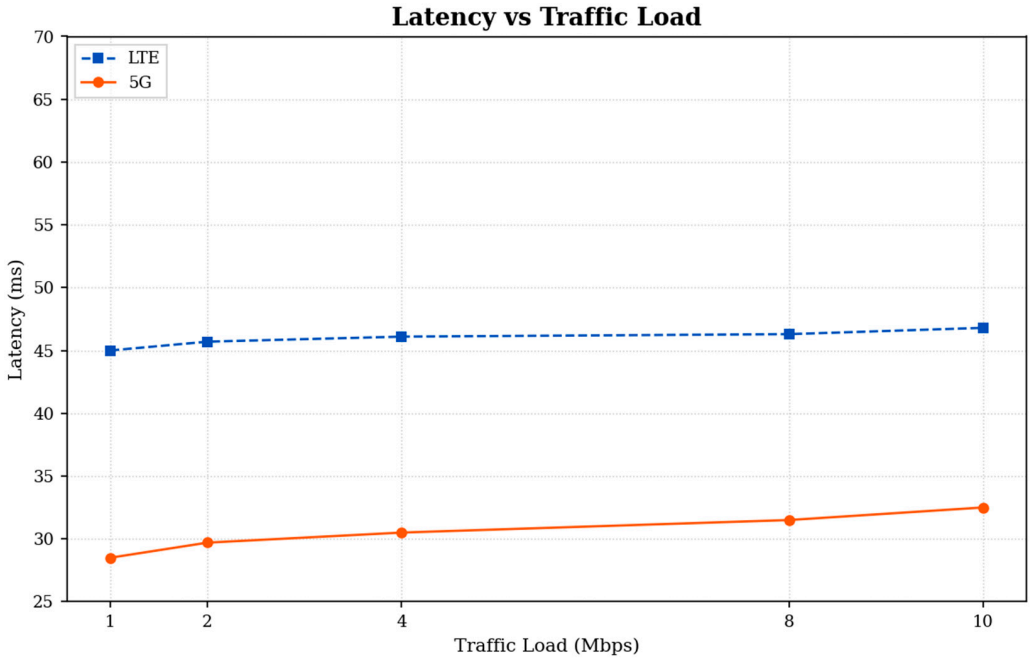
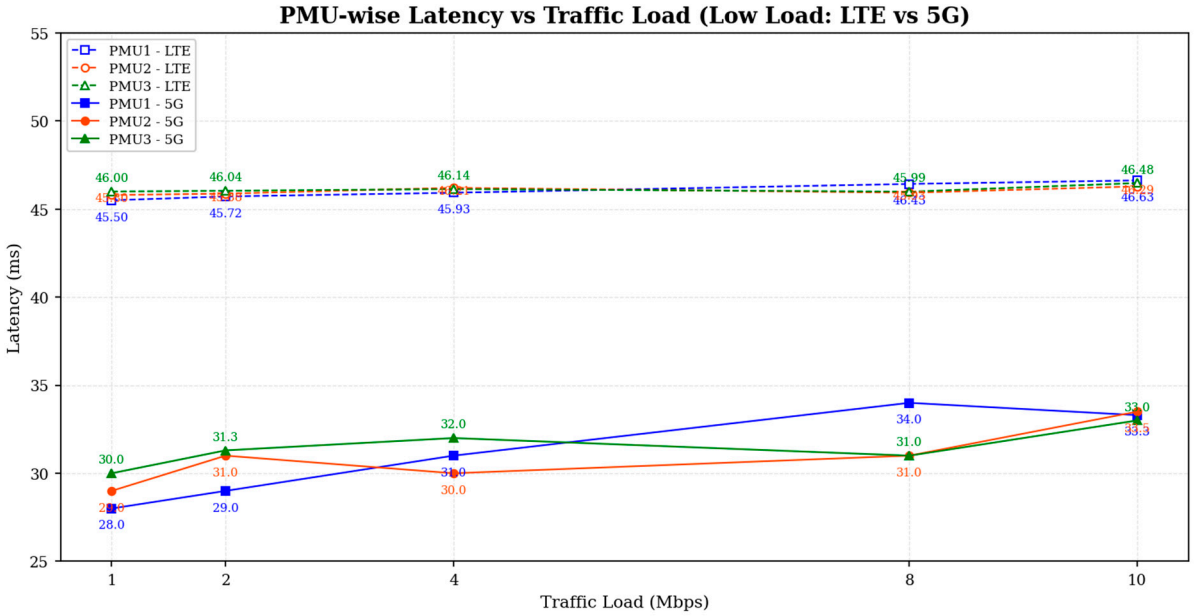


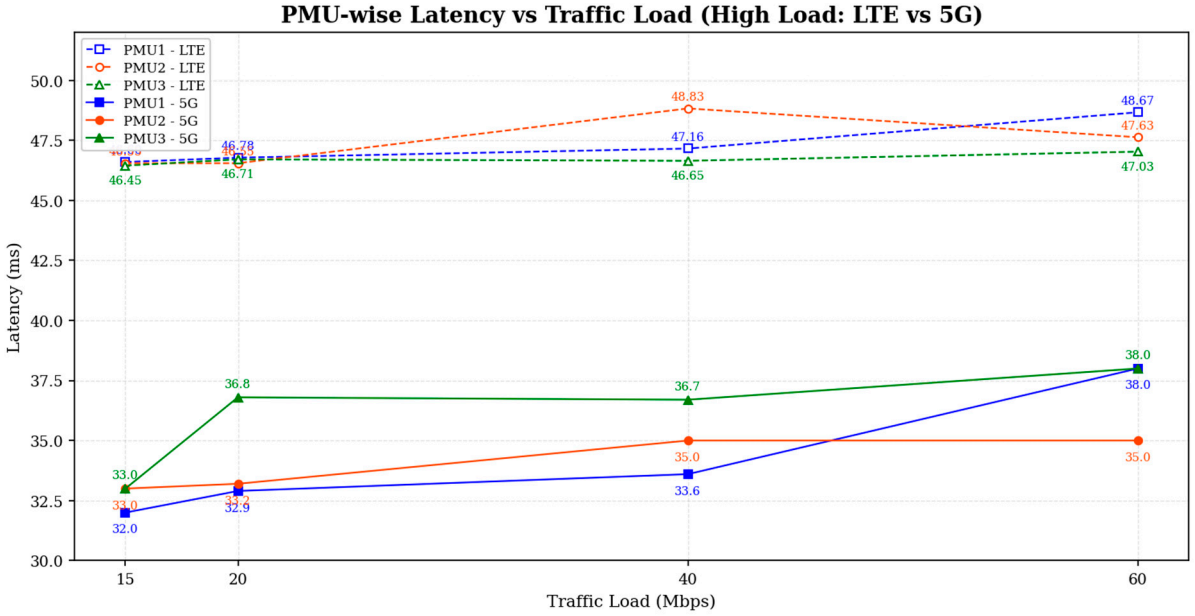
Figure 8. The latency vs. load characteristics under low-traffic conditions for LTE vs. 5G.

Table 3. Results of latency analysis for low traffic load.

Traffic Load (Mbps)	LTE Latency (ms)	5G Latency (ms)
1	45.77	29.00
2	45.88	30.43
4	46.09	31.00
8	46.12	32.00
10	46.47	33.00



(**a**)



(**b**)

Figure 9. PMU-wise latency analysis for (**a**) low traffic load and (**b**) high traffic load.

2. Case 2: High-Traffic Conditions

Under the high-traffic experiment loads, values of 15 Mbps to 60 Mbps were considered for both LTE and 5G latency analysis. The experiments on high traffic loads make the differences in LTE and 5G technology more evident in smart grid communication. In LTE, the average latency at the highest load (60 Mbps) is around 48.7 ms. The increase in latency with respect to the increase in load for LTE is consistent and gradual; however, the latency values are higher than those of 5G. For 5G, the latency at the highest load of 60 Mbps is around 37 ms; therefore, even though the latency values increase with the increase in load for 5G, they remain relatively lower compared to LTE. At the highest load, the difference in latency between LTE and 5G is therefore almost 11.7 ms, which is considerable. It is important to note that both the LTE and 5G models in these experiments were configured for

10 Mbps bandwidth; considering this baseline, it is safe to say that even under the highest loads, 5G maintains an advantage in latency. Figure 10 presents the latency analysis for both LTE and 5G under high traffic loads. Analysis for high traffic loads is critical for smart grid communication networks, as there are too many devices that transmit data at the same time in a smart grid network. Therefore, it is crucial that an experimental analysis of two smart grid communication models validates the models under scenarios of network congestion. The PMU-wise latency analysis for high traffic loads is shown in Figure 9b. For LTE, the PMU-wise latencies show a notable increase with the load; the results also indicate that the individual PMU nodes undergo different latency responses, even though the overall latency might remain stable. In the case of 5G, the PMU-wise latencies remain low and, even at the highest load of 60 Mbps, the PMUs maintain lower latencies compared to LTE. It is interesting to note that, in LTE, PMU2 generates the highest latency of 48.83 ms at 40 Mbps; however, PMU3 generates the highest latency in 5G, with a value of 36.8 ms at 20 Mbps. Therefore, the PMU-wise latency analysis sheds light on certain variations caused by the resource allocation among individual PMUs. Nevertheless, the overall latency for 5G remains considerably lower than for LTE. Table 4 consolidates the results of the latency analysis for 5G and LTE.

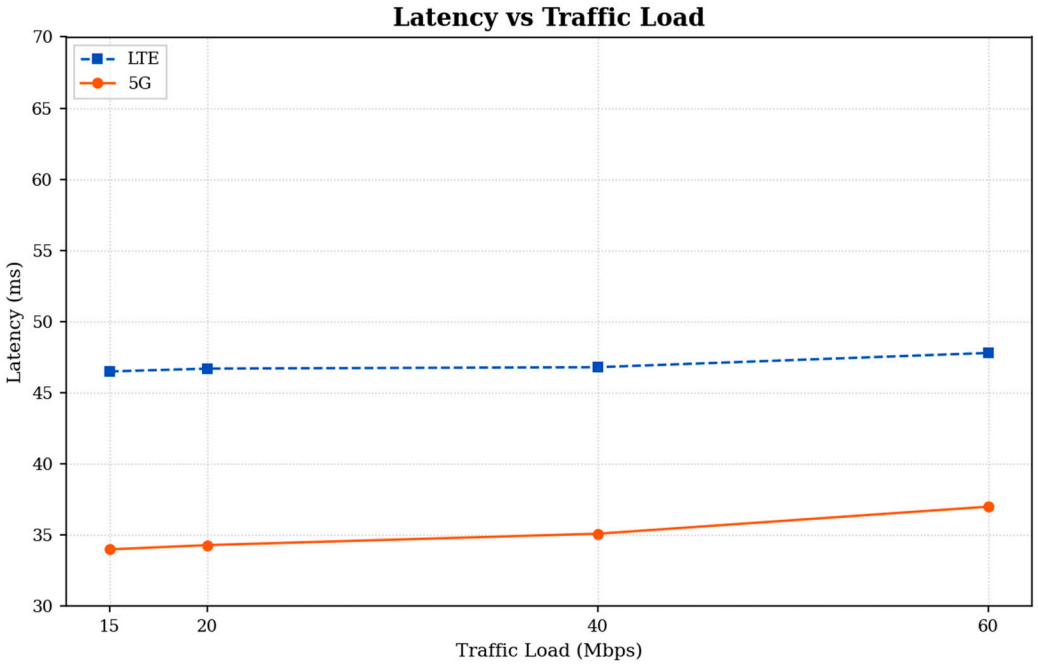


Figure 10. The latency vs. load characteristics under high-traffic conditions for LTE vs. 5G.

Table 4. Results of latency analysis for high traffic load.

Traffic Load (Mbps)	LTE Latency (ms)	5G Latency (ms)
15	46.53	34.00
20	46.68	34.30
40	47.55	35.10
60	47.77	37.00

The PMU-wise latency results under high-traffic load conditions are critical for the PMU communication scenario in smart grids, since 5G provides consistently lower latency than LTE under stressful network conditions. This advantage of 5G over LTE under network congestion can be especially linked to traffic differentiation, isolation, and network-slicing

technology. By logically separating the smart grid entities into different network slices, slicing isolates and prioritises PMU traffic over background traffic. The previous study provides more interesting observations into 5G networks with and without network slicing. Network slicing in 5G is successful in preventing resource contention for the priority traffic under high traffic loads and, therefore, provides lower PMU latencies during traffic congestion as compared to LTE. Therefore, the results of the experimental analysis on 5G vs. LTE demonstrate that 5G is a better option for providing lower-latency communication in smart grids than LTE, especially when the network conditions are stressful. This experimental analysis also indicates that the choice of communication technology in smart grids has a direct impact on the timely data exchange in PMUs. The advantages of 5G over LTE become important, especially when the network induces heterogeneous traffic. Therefore, in a smart grid system, it is crucial to adopt the best communication technologies to support latency-sensitive PMU modules so as to support efficient real-time monitoring and control.

3. Network Utilisation Analysis

The results of network utilisation analysis for LTE show a 45 ms latency at 10% network utilisation and 46.6 ms latency at 100% network utilisation. Meanwhile, for 5G, the latency is 28.7 ms at 10% network utilisation and 32.1 ms at 100% network utilisation. It is important to note that both LTE and 5G were configured for a bandwidth of 10 Mbps, and the percentage of network utilisation was computed based on this bandwidth. 5G networks continued to operate with lower latencies throughout the network utilisation range. This is crucial in PMU communication, as high network utilisation can lead to resource contention in the network and corresponding delays. The better performance of 5G under high network utilisation is therefore a direct result of traffic differentiation, isolation, and resource allocation. That is, 5G prioritises the latency-sensitive PMU traffic over background traffic. Figure 11 presents the results of network utilisation versus latencies for both LTE and 5G. The results of the network utilisation analysis indicate that 5G networks provide more resilience to increasing network utilisation than LTE networks. This is especially important in PMU-based data exchange and real-time monitoring and control applications in smart grid systems.

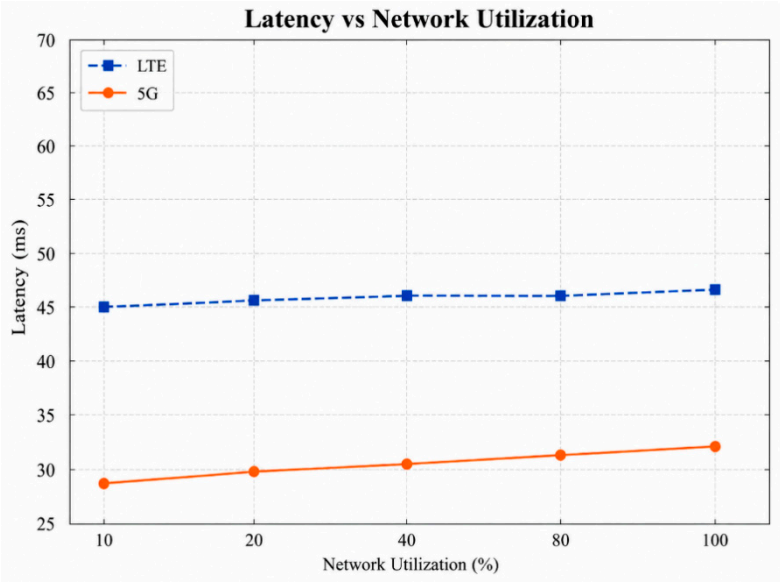


Figure 11. Latency vs. network utilisation for both LTE and 5G.

The results of the smart grid communication layer complement those of the physical-layer power system simulation validation. The physical-layer simulation validated the electrical measurements and transient responses of the smart power grid entities. The

communication-layer validation presents how the data generated at the physical-layer simulation end is transmitted through the communication network under different scenarios. This analysis is crucial for a smart grid cyber–physical system where the electrical counterpart and the communication counterpart are closely integrated and interdependent. Therefore, unlike traditional power grids, a modern smart grid infrastructure depends not only on the electrical behaviour of the power system components but also on the time-sensitive exchange of measurement and control data. The results of the comparative evaluation of LTE and 5G indicate that 5G performs better in latency-sensitive applications. Even at the highest traffic load of 60 Mbps, 5G maintains an average latency of 37 ms, whereas LTE has approximately 47 ms of average latency. These latency ranges differ for individual PMUs as well. However, these results should be interpreted specifically as a simulation-based validation of the latency behaviour, not as experimental measurements from a deployed LTE or 5G network. The results of the present research only demonstrate the relative communication performance of the emulated 5G and LTE networks under selected traffic conditions.

The comparative evaluation of LTE and 5G was achieved by varying the traffic loads from 1 to 60 Mbps. Each traffic load condition was evaluated for three independent experimental runs for both LTE and 5G. The results are presented in Tables 5 and 6 in terms of the mean latency ± standard deviation (SD) and 95% confidence intervals (CIs) calculated from the run-level measurements. Across all traffic loads from 1 to 60 Mbps, the mean latency of the 5G configuration is reported to be lower than that of LTE. At the lowest load of 1 Mbps, the mean latency of the 5G network is 29.00 ms, whereas that of LTE is 45.77 ms. At the highest load of 60 Mbps, in the present experimental framework, the mean latency for 5G is 37.00 ms, while that of LTE is 47.78 ms. Therefore, 5G networks reported lower latencies consistently over the measured traffic load range of 1 to 60 Mbps. The reported 95% CIs for both LTE and 5G did not overlap at any of the nine traffic load conditions. However, the 5G configuration shows varying levels of dispersion, as evident in its standard deviations and the width of the confidence intervals. The observed difference was also not constant across the varying traffic load conditions. Also, the mean latencies did not show a monotonous increase with the traffic loads in every condition. Therefore, these observations indicate that the reported performance depends on the configured communication architecture and the varying traffic conditions. It is important to consider that the results of the present comparative analysis between LTE and 5G can only be assessed under the specific experimental design rather than as a generic performance indicator for all LTE and 5G configurations.

Table 5. LTE latency results reported as means ± standard deviations and 95% confidence intervals.

Load (Mbps)	5G Latency (ms)	95% CI (ms)
1	29.00 ± 1.00	[26.52, 31.48]
2	30.43 ± 1.25	[27.33, 33.54]
4	31.00 ± 1.00	[28.52, 33.48]
8	32.00 ± 1.73	[27.70, 36.30]
10	33.27 ± 0.25	[32.64, 33.89]
15	34.00 ± 2.00	[29.03, 38.97]
20	34.30 ± 2.17	[28.91, 39.69]
40	35.10 ± 1.55	[31.24, 38.96]
60	37.00 ± 1.73	[32.70, 41.30]

Table 6. 5G latency results reported as means ± standard deviations and 95% confidence intervals.

Load (Mbps)	5G Latency (ms)	95% CI (ms)
1	45.77 ± 0.25	[45.14, 46.39]
2	45.88 ± 0.16	[45.48, 46.28]
4	46.09 ± 0.15	[45.73, 46.46]
8	46.12 ± 0.27	[45.44, 46.79]
10	46.47 ± 0.17	[46.04, 46.89]
15	46.53 ± 0.08	[46.34, 46.72]
20	46.68 ± 0.12	[46.39, 46.97]
40	47.55 ± 1.14	[44.71, 50.38]
60	47.78 ± 0.83	[45.72, 49.84]

5.3. Cyber-Resilience Validation

The proposed system was evaluated for its cyber resilience by instigating a DoS attack on the communication layer. This evaluation measured the latency of the communication network during a DoS attack and the corresponding recovery time. The experiments in the present study were designed to induce a DoS attack on different smart grid components, such as the consumer load/user application, DERs, and ESSs, and the corresponding average PMU latency was measured. The scope of these experiments was extended to evaluate both LTE and 5G networks. The substation components are represented by the nodes h5 for the user applications, h6 for DERs, and h7 for ESSs in the communication network.

Figure 12 represents the PMU latencies measured during DoS attacks at nodes h5, h6, and h7 for both LTE and 5G. The results of the cyber-resilience validation indicate that the latency values for the 5G network are considerably lower compared to those of LTE for the same experimental scenario: 5G achieves an approximate 20% to 41% reduction in PMU latencies compared to LTE. This directly supports the conclusion that 5G networks perform better than LTE during cyber threats in smart grid communication systems. In addition to latency requirements, the recovery time was also measured as a cyber-resilience metric in the present study. The recovery times for both 5G and LTE with respect to the attack node are given in Figure 11. The recovery times for LTE are 13s for an attack at h5, 16 s for an attack at h6, and 22 s for an attack at h7, whereas those of 5G are 8 s, 9 s, and 9 s, respectively. Therefore, there is a 38% to 59% reduction in recovery time for 5G when compared with LTE. During a DoS attack, the induced traffic congestion causes an increase in resource utilisation and delayed packets. Once the attack stops, the network is supposed to clear the accumulated traffic and restore the communication path to continue normal operation. However, in the case of an LTE network in the proposed smart grid environment, there is a large traffic backlog forcing the network to a high recovery time. Therefore, the increase in recovery time for the LTE networks is associated with the traffic backlog and persistent traffic congestion induced by the attack. Specifically for h7 (the ESS), the LTE network requires 22 s to recover—compared to 5G, which requires 9 s to recover—indicating that the 5G network can restore normal operation considerably faster than LTE under cyber-threat scenarios. The results of the cyber-resilience experiments are consolidated in Table 5. Figure 13 presents the recovery time for both LTE and 5G, as well as the cyber-resilience improvement with 5G networks.

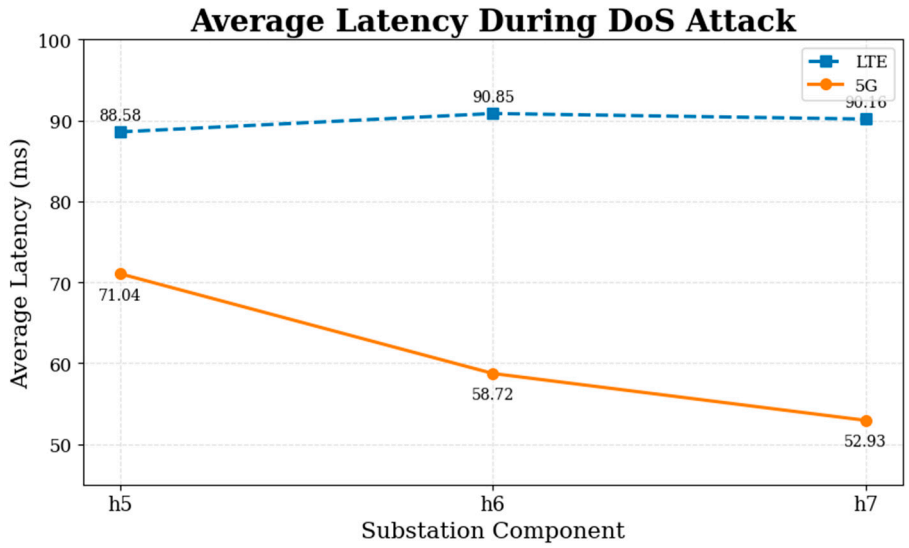
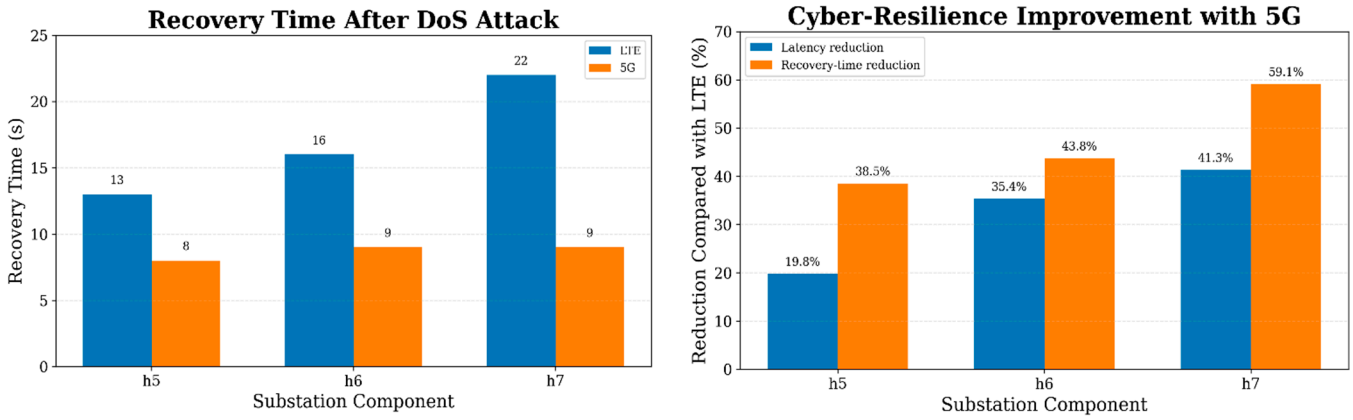


Figure 12. Average PMU latency during DoS attack for both LTE and 5G.



(**a**) (**b**)

Figure 13. (**a**) The recovery time after a DoS attack for both LTE and 5G. (**b**) The cyber-resilience improvement in latency and recovery time for 5G.

The results of the cyber-resilience evaluation indicate that the eMBB traffic or the h7 traffic is more susceptible to latency and recovery degradation during the DoS attack because of comparatively high traffic and resource demand. This is one of the reasons why the latency of such high-throughput traffic is higher compared to the mMTC traffic under the same conditions. Therefore, the results of this study are reliant on the traffic and attack scenarios of the proposed framework and are not a generalisation of the eMBB slice characteristics. The eMBB slices are designed to handle larger traffic volumes than the mMTC slices and, therefore, demand more network resources during a DoS attack, causing resource contention and network congestion. These cause packet delays and queue buildup, which, in turn, result in higher latency for eMBB traffic. The mMTC slices are designed to handle relatively small traffic and, therefore, require fewer network resources; therefore, the amount of traffic competing for the same resources is comparatively less, reducing packet delays and queue buildup. Even though there is higher traffic demand at the eMBB slice, the overall latency in 5G networks is considerably lower and the recovery times are shorter compared to LTE. This proves that the resilience metrics in smart grids are dependent not only on the traffic conditions but also on the fundamental architecture of the communication layer. Table 7 gives the results of cyber-resilience metrics for both

LTE and 5G. In the 5G architecture, network slicing provides traffic differentiation and resource separation, thereby reducing the network congestion caused by competing network resources. That is, an attack that affects a higher-traffic slice does not necessarily cause the same level of degradation throughout the entire communication architecture. This property of 5G helps in smart grid cyber resilience to reduce and contain the effect of a cyberattack and allows the critical modules to continue their operation.

Table 7. Results of cyber-resilience metrics for LTE and 5G.

Substation Component	Average Latency During DoS: LTE	Recovery Time for LTE	Average Latency During DoS: 5G	Recovery Time for 5G
h 5	88.58 ms	13 s	71.04 ms	8 s
h 6	90.85 ms	16 s	58.72 ms	9 s
h 7	90.16 ms	22 s	52.93 s	9 s

6. Limitations and Future Work

The current study presents a comparison of the LTE and 5G communication frameworks for smart grid communication architecture and evaluates their respective cyber-resilience metrics. The experimental analysis was based on the co-simulation of Simulink and Comnetsemu. The communication network was emulated through configured network links, transmission delays, bandwidth constraints, and queue-based traffic management. The 5G network was specifically modelled using OVS queues and SDN-based traffic management rather than a full 3GPP-compliant 5G radio access and gNB/5G core network stack; hence, the experimental evaluation does not possess all of the characteristics of operational LTE and 5G systems. Consequently, the configured queues represent an abstraction of selected network-slicing behaviours rather than complete 3GPP-defined network slices. Therefore, the reported results of latency and recovery times should only be interpreted as results obtained within the configured emulation environment, not as field measurements or evidence for absolute performance in the proposed networks. The primary objective of the comparative analysis was to understand the behaviour of the proposed LTE and 5G architectures within the controlled conditions of the experimental design in the scope of this study. Validation with a comprehensive 3GPP stack for 5G network architecture remains an important direction for future work. The cyber-resilience evaluation in the present study was primarily based on externally generated DoS attacks and their implications for the PMU-specific communication latency and recovery times on smart power grids for both LTE and 5G networks. The experimental analysis in its current state does not consider the full range of threats in smart grids, especially attacks originating from compromised internal devices, malicious traffic generated by legitimate network participants, or attacks that target the slice-management functions. Such threats could have effects on traffic classification and resource allocation that were not analysed in the scope of the present experiments. Future work will extend the threat model to include attacks originating from compromised internal devices and attacks that target the slice-management functions. Therefore, the reported results should be interpreted not as a comprehensive assessment of generalised smart grid cybersecurity but, rather, as a cyber-resilience evaluation within the specific external DoS traffic-flooding scenarios investigated. The evaluation metrics in the present experimental analysis focus on the PMU-specific communication latency and the post-attack recovery time to investigate the comparative communication performance and cyber resilience of the LTE and 5G configurations. However, these metrics alone are not sufficient to fully understand the communication network performance required by critical smart grid applications.

Specifically, metrics like packet loss and jitter help understand the missing or incomplete PMU measurements and the variations in packet delay, which may affect the delivery of time-sensitive measurement data. Such metrics are particularly relevant during high traffic loads and DoS attack scenarios, which cause communication degradation affecting the reliability of critical services like the monitoring and protection systems in smart power grids. Therefore, future work will extend the evaluation to integrate metrics like packet loss and jitter with communication latency and recovery times to give a more comprehensive analysis of the communication network performance and cyber resilience of LTE and 5G in smart grids. Even though the implemented 5G network-slicing architecture used traffic classification and a queue-based priority model, the scope of the present experiments does not consider the additional slicing orchestration overhead on low-latency traffic. In 5G communication networks, traffic classification, slice configuration, and resource allocation may introduce overhead on the network performance of low-latency traffic. Therefore, future work will investigate the overhead induced by slice orchestration on the performance of low-latency traffic. The present experimental study was deployed using a limited number of PMUs and smart grid communication nodes within a controlled environment integrating Simulink and comnetsemu. Although this experimental framework enables a controlled comparison of LTE and 5G networks, its scalability to larger real-world smart grid infrastructure has not been investigated. In practical scenarios, increasing the number of smart grid components like PMUs, DERs, ESSs, or other network-related entities may cause an increase in the communication traffic, processing requirements, queue contention, and the complexity of the traffic management. These factors may further affect the communication latency requirements, traffic congestion, and post-attack recovery times. Therefore, the reported results should only be interpreted within the scope of this particular experimental design, with the configured topologies, bandwidth constraints, and attack scenarios, rather than as predictions for larger real-world smart grid deployments. In the future, this study will be extended to investigate the scalability of the proposed configurations by increasing the number of smart grid nodes, varying the traffic conditions, and considering more cyber-attack scenarios to make the results more generalisable and deployable in real-world smart grid applications.

7. Conclusions

This paper presents a comparative evaluation of both LTE and 5G communication architectures in smart power grids to understand the network performance and communication resilience for PMU-specific applications. The proposed system evaluates the ability of both LTE and 5G to maintain PMU latencies under varying traffic conditions and cyber threats. The experimental analysis was designed through co-simulation of the physical-layer power system model in Simulink and the corresponding communication-layer emulation in comnetsemu. The traffic-load-based experiments analysed communication latencies under low- and high-traffic conditions. Low-traffic-load experiments were conducted with loads of 1 to 10 Mbps, and high-traffic-load experiments with loads of 15 to 60 Mbps. The latency value produced by LTE at the maximum traffic load of 60 Mbps was 47 ms, and that of 5G was 37 ms. Compared to LTE, 5G networks maintained lower latencies under both low-traffic and high-traffic load conditions. The PMU-wise latency was also evaluated for both LTE and 5G, demonstrating that traffic differentiation and priority queuing associated with the PMU traffic in 5G help mitigate the influence of background traffic on PMU communication in smart grids. Therefore, the better results reported by 5G for the latency requirements can be attributed to the network-slicing technology that makes it possible for 5G networks to adopt traffic differentiation, isolation, and resource allocation. Cyber-resilience experiments were also carried out to measure the latency of both LTE and 5G networks during a smart

grid cyber threat. Recovery times were also measured for both LTE and 5G under a DoS attack scenario on the proposed system architecture. The results of the cyber-resilience evaluation indicate that 5G provides better latency compared to LTE when a smart grid network is subjected to a DoS attack. The 5G networks prevent the additional traffic generated by DoS from competing for the network resources of the PMU traffic by using traffic isolation. 5G networks were also successful in retaining lower recovery times compared to LTE. Therefore, traffic differentiation can help the PMU traffic attain recovery of normal operation faster than conventional networks. Overall, the experiments indicate that the 5G sliced communication architecture provides more stable and cyber-resilient communication in smart power grids. The scope of the present study presents certain challenges that we hope to address in future work. The present study is just a simulation-based evaluation; therefore, we did not implement a fully commercial 5G network or utility-level communication infrastructure. The present experimental configuration also does not capture the potential capacity advantage of 5G under technology-specific radio conditions. Without such a bandwidth constraint, the latencies, relative performance, and congestion behaviour of the network configurations might change with respect to the capacity, resource allocation, and traffic prioritisation. Therefore, the conclusions are limited to the evaluated experimental configurations within the specific bandwidth of 10 Mbps and are subject to changes under different bandwidth configurations. Furthermore, future experiments will extend the experimental evaluation to packet loss, throughput analysis, service availability, etc. Evaluations on multiple attack scenarios are also intended as a future extension of the present work. Therefore, the results of the present work demonstrate the advantages of a 5G-slicing-based communication architecture in providing differentiated PMU traffic and thereby reducing the impact of traffic congestion and DoS attack-induced degradation in smart grid communication systems.

Author Contributions: Conceptualisation, F.G. and M.G.N.; methodology, A.G.; software, A.G.; validation, A.G., F.G., and M.G.N.; formal analysis, A.G.; investigation, A.G.; resources, F.G.; data curation, A.G.; writing—original draft preparation, A.G.; writing—review and editing, A.G.; visualisation, A.G.; supervision, F.G.; project administration, F.G.; funding acquisition, F.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available from the corresponding author upon reasonable request. Public access to the complete dataset is currently limited because further experiments and analyses using the data are ongoing.

Acknowledgments: The authors gratefully acknowledge the support of the Department of Electrical and Electronics Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, India, and the Department of Information Engineering and Computer Science, University of Trento, Italy, for their academic support, collaboration, and research facilities that enabled this work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. *IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads*; IEEE: New York, NY, USA, 2011. Available online: https://standards.ieee.org/ieee/2030/4593/.
2. Prajwal, K.S.; Amitasree, P.; Vamshi, G.R.; Kirthika Devi, V.S. Wireless Communication Network-Based Smart Grid System. In *Pervasive Computing and Social Networking: Proceedings of ICPCSN 2021*; Springer: Singapore, 2022; pp. 673–694.
3. Borenius, S.; Kekolahti, P.; Hämmäinen, H.; Lehtonen, M.; Mähönen, P. Novel Industry Architectures for Connectivity Solutions in the Smart Distribution Grids. *IEEE Access* **2023**, *11*, 68093–68112. [CrossRef]
4. Goswami, B.; Jurdak, R.; Nourbakhsh, G. Node Allocation Strategy for Low Latency Neighbourhood Area Networks in Smart Grid. *IEEE Trans. Netw. Sci. Eng.* **2024**, *11*, 5087–5098. [CrossRef]

5. Markkula, J.; Haapola, J. Shared LTE Network Performance on Smart Grid and Typical Traffic Schemes. *IEEE Access* **2020**, *8*, 39793–39808. [CrossRef]
6. Fisser, L.; Ipach, H.; Timm-Giel, A.; Becker, C. Evaluation of LTE-based Communication for Fast State Estimation in Low Voltage Grids. In Proceedings of the 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Tempe, AZ, USA, 11–13 November 2020; pp. 1–7. [CrossRef]
7. Dash, B.K.; Shah, S.; Malandra, F. Network Performance Analysis of Smart Grid Communications Over LTE cat-M. In Proceedings of the 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Glasgow, UK, 31 October–3 November 2023; pp. 1–6. [CrossRef]
8. Shah, S.; Koley, S.; Malandra, F. Experimental End-To-End Delay Analysis of LTE Cat-M With High-Rate Synchrophasor Communications. *IEEE Internet Things J.* **2023**, *10*, 19839–19848. [CrossRef]
9. Raszmann, E.; Prabakar, K.; Mather, B.; Li, J. Experimental Test Bed to Enable Realistic Evaluations for Direct Transfer Trip Relaying via Private Wireless LTE Communications. In Proceedings of the 2020 IEEE International Smart Cities Conference (ISC2), Piscataway, NJ, USA, 28 September–1 October 2020; pp. 1–6. [CrossRef]
10. Deniz, H.; Simsek, M.; Kantarci, B. On Delay Sensitivity Clusters of Microgrid Data Aggregation Under LTE-A Links. In Proceedings of the 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Bucharest, Romania, 24–28 May 2021; pp. 1–6. [CrossRef]
11. Lin, L.; Liu, B.; Tian, D.; Li, H.; Liu, Y. Research on the Construction of Power Wireless Private Network Based on LTE Technology. In Proceedings of the 2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 8–10 December 2023; pp. 1099–1103. [CrossRef]
12. Cakiroglu, D.; Geohar, H.; Sardoroud, B.A.M.A.; Jaseemuddin, M.; Arani, M.F.M.; Jahromi, A.A. A Co-Simulation Platform for Wireless LTE Networks in Smart Distribution Systems. In Proceedings of the 2024 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE), Dubrovnik, Croatia, 14–17 October 2024; pp. 1–5. [CrossRef]
13. Kumar, M.; Tripathi, N.D.; Reed, J.H. A Survey of Smart Grid Emerging Use Cases and Relevant 5G and 6G Capabilities and Features. *IEEE Access* **2026**, *14*, 30455–30475. [CrossRef]
14. Esenogho, E.; Djouani, K.; Kurien, A.M. Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect. *IEEE Access* **2022**, *10*, 4794–4831. [CrossRef]
15. Saleem, M.U.; Usman, M.R.; Yaqub, M.A.; Liotta, A.; Asim, A. Smarter Grid in the 5G Era: Integrating the Internet of Things With a Cyber-Physical System. *IEEE Access* **2024**, *12*, 34002–34018. [CrossRef]
16. Tao, J.; Umair, M.; Ali, M.; Zhou, J. The impact of Internet of Things supported by emerging 5G in power systems: A review. *CSEE J. Power Energy Syst.* **2020**, *6*, 344–352. [CrossRef]
17. Taveras Cruz, A.J.; Aybar-Mejía, M.; Díaz Roque, Y.; Coste Ramírez, K.; Durán, J.G.; Rosario Weeks, D.; Mariano-Hernández, D.; Hernández-Callejo, L. Implications of 5G Technology in the Management of Power Microgrids: A Review of the Literature. *Energies* **2023**, *16*, 2020. [CrossRef]
18. Singh, M.; Rallabandi, B.R.; Gattupalli, K.K.; Medarametla, M.S. Autonomous Private 5G Field Area Networks: Achieving Secure, Scalable, and Self-Healing Smart Grid Communications. In Proceedings of the 2025 2nd International Conference on Recent Trends in Electrical, Electronics and Computing Technologies (ICRTEECT), Warangal, India, 30–31 October 2025; pp. 1–6. [CrossRef]
19. Liu, P.; Zou, Y.; Guo, Q.; Ma, K.; Tian, N.; Zhang, Y. A Secure Transmission Strategy for Smart Grid Communications Assisted by 5G Base Station. *IEEE Trans. Ind. Appl.* **2025**, *61*, 1695–1703. [CrossRef]
20. Borgaonkar, R.; Burgos, D.; Zerihun, T.A.; Lange, S.; Zinner, T. Commercial Grade 5G Testbed for Cybersecurity Research in Smart Grid Systems: Design, Implementation, and DoS Evaluation. In Proceedings of the 2025 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), Valletta, Malta, 20–23 October 2025; pp. 1–5. [CrossRef]
21. Lekshmi, S.S.; Anjana, M.S.; Nair, B.B.; Raj, D.; Ponnekanti, S. Framework for Generic Design of Massive IoT Slice in 5G. In Proceedings of the 2019 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), Chennai, India, 20–21 March 2019; pp. 523–529. [CrossRef]
22. Rafique, W.; Barai, J.R.; Fapojuwo, A.O.; Krishnamurthy, D. A Survey on Beyond 5G Network Slicing for Smart Cities Applications. *IEEE Commun. Surv. Tutor.* **2025**, *27*, 595–628. [CrossRef]
23. Wijethilaka, S.; Liyanage, M. Survey on Network Slicing for Internet of Things Realization in 5G Networks. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 957–994. [CrossRef]
24. Das, R.M.; Sree, L.S.; Ponnekanti, S.; Paunovic, M. Key Enablers to Deliver Latency-as-a-Service in 5G Networks. In Proceedings of the 2019 27th Telecommunications Forum (TELFOR), Belgrade, Serbia, 26–27 November 2019; pp. 1–4. [CrossRef]
25. Devidas, A.R.; Ramesh, M.V. Cost Optimal Hybrid Communication Model for Smart Distribution Grid. *IEEE Trans. Smart Grid* **2022**, *13*, 4931–4942. [CrossRef]

26. Chen, J.; Xia, F.; Wei, X.; Zhao, Q.; Mei, Z.; Li, Y. Application of High Reliability 5G Slice in Smart Grid. In Proceedings of the 2024 International Conference on Power, Electrical Engineering, Electronics and Control (PEEEC), Athens, Greece, 14–16 August 2024; pp. 892–896. [CrossRef]
27. Zhang, X. 5G-Advanced Network Slicing for Smart Grid Communications. *J. ICT Stand.* **2026**, *14*, 461–506. [CrossRef]
28. Raussi, P.; Kokkoniemi-Tarkkanen, H.; Ahola, K.; Heikkinen, A.; Uitto, M. Prioritizing protection communication in a 5G slice. *J. Eng.* **2023**, *2023*, e12309. [CrossRef]
29. Boeding, M.; Scalise, P.; Hempel, M.; Sharif, H.; Lopez, J., Jr. Toward Wireless Smart Grid Communications: An Evaluation of Protocol Latencies in an Open-Source 5G Testbed. *Energies* **2024**, *17*, 373. [CrossRef]
30. Rantopoulos, M.; Chochliouros, I.P.; Brodima, D.; Tzani, N.; Ciornei, I.; Asprou, M.; Spiliopoulou, A.S.; Lazaridis, P. Testing Plan Description and Field Measurements for Real-Time Wide Area Monitoring of Interconnected Power Systems in the Smart5Grid Project. In *IFIP Advances in Information and Communication Technology*; Springer: Cham, Switzerland, 2024; Volume 715. [CrossRef]
31. Fan, X.; Chen, Y.; Wang, D.; Qin, C.; Liu, Y.; Guddanti, K.; Li, Y.; Wang, S.; Ogle, J.; Peterson, E.; et al. *5G Energy FRAME Report on 5G for Grid Use Case: Year 3 Final Report*; PNNL-36588; Pacific Northwest National Laboratory: Richland, WA, USA, 2024.
32. Zhang, X.; He, Y.; He, Y. Securing Distributed Power Dispatching Systems: A Framework for Cybersecurity and 5G Integration. In Proceedings of the 2025 IEEE 5th International Conference on Power, Electronics and Computer Applications (ICPECA), Shenyang, China, 17–19 January 2025; pp. 835–840. [CrossRef]
33. Sheng, Y.; Guanjie, Q.; Guozu, J.; Hao, D.; Liang, F.; Lingqi, L. Research on 5G-based Disaster-Resistant Security for Smart Power Grids. In Proceedings of the 2024 IEEE 7th International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), Shenyang, China, 27–29 December 2024; pp. 125–130. [CrossRef]
34. Chiu, S.C. SDN-Based Critical Infrastructure Resilience: A Smart Grid Perspective. In Proceedings of the 2023 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 13–15 December 2023; pp. 1054–1060. [CrossRef]
35. Chatzimiltis, S.; Shojafar, M.; Mashhadi, M.B.; Tafazolli, R. A Collaborative Software Defined Network-Based Smart Grid Intrusion Detection System. *IEEE Open J. Commun. Soc.* **2024**, *5*, 700–711. [CrossRef]
36. Lakhal, H.; Zegrari, M.; Bahnasse, A. Next-Generation Smart Grid Cybersecurity: A Systematic Review of OT Cyber Threats, AI-Driven Defense, Cyber Deception Techniques, and Emerging Security Strategies. *IEEE Access* **2025**, *13*, 181519–181552. [CrossRef]
37. Eto, J.H.; Stewart, E.M.; Smith, T.; Buckner, M.; Kirkham, H.; Tuffner, F.; Schoenwald, D. Scoping Study on Research and Development Priorities for Distribution-System Phasor Measurement Units. 2015. Available online: https://eta-publications.lbl.gov/publications/scoping-study-research-and-priorities (accessed on 10 October 2026).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.