applied sciences

MDPI

Article

Assessment of Cyber-Physical Inverter-Based Microgrid Control Performance under Communication Delay and Cyber-Attacks

Ola Ali *, Tung-Lam Nguyen and Osama A. Mohammed

Energy Systems Research Laboratory, Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA; tunguyen@fiu.edu (T.-L.N.); mohammed@fiu.edu (O.A.M.)

* Correspondence: oali009@fiu.edu

Abstract: The integration of communication infrastructures into traditional power systems, transforming them into cyber-physical power systems (CPPS), accentuates the significance of communication in influencing system performance and sustainability. This paper presents a versatile, innovative cyber-physical co-simulation framework that integrates the physical power system and communication networks, uniting OPAL-RT, a network simulator (ns3), and Docker containers into a sophisticated platform, facilitating intensive studies into CPPS dynamics. The proposed experimental study provides an innovative way to assess the frequency control response of a cyber-physical inverter-based microgrid (MG), addressing the MG sustainability challenges. We consider diverse real-world scenarios, focusing on communication delays and distributed denial of service (DDoS) attacks within the communication channels. We propose a precise ns3-based communication model that bridges the MG's primary and secondary control layers, an aspect often overlooked in previous studies; this is a noteworthy contribution to elucidating the adverse impacts of communication latency on MG frequency performance. The experimental results demonstrate the effectiveness of the centralized secondary controller in eliminating the frequency deviations. Furthermore, the findings offer insights into stable and unstable regions, revealing how the communication delay value affects the frequency stability under different operating conditions. In addition, the developed real-time DDoS attacks model within the proposed communication surface unveils crucial insights into the MG's resilience to cyber threats. This work's revelations offer a foundational awareness of MG vulnerabilities, paving the way for designing robust and resilient communication networks and control strategies within the cyber-physical inverter-based microgrids.

Keywords: cyber-physical microgrid; co-simulation; communication networks; ns-3; cyber-attacks; vulnerability assessment

check for updates

Citation: Ali, O.; Nguyen, T.-L.; Mohammed, O.A. Assessment of Cyber-Physical Inverter-Based Microgrid Control Performance under Communication Delay and Cyber-Attacks. *Appl. Sci.* **2024**, *14*, 997. https://doi.org/10.3390/app14030997

Academic Editors: S. H. Shah Newaz, Nazmus Shaker Nafi, Yoon-Sik Yoo and Filipe Soares

Received: 26 October 2023
Revised: 17 January 2024
Accepted: 22 January 2024
Published: 24 January 2024

1. Introduction

With the increase in energy consumption and the growth in the penetration of distributed generators (DGs) in the power grid, there is a necessity for the transition from the conventional power grid to the smart grid [1]. Initiatives for smart grids aim to overlay the current electric grid with a more robust communication, processing, and sensing infrastructure, allowing the grid to accommodate a higher penetration of renewable energy sources besides contributing to sustainability by improving energy efficiency and the quality of service [2]. With the increase in the interaction between power grids and communication technologies, power systems have become cyber-physical power systems (CPPS) that include both power and communication networks. As a result, considering the interdependence between both networks is essential when studying the performance of the power or communication networks. Nevertheless, this integration intensifies vulnerability and cyber-attack threats [3]. With the increase in the dependency of CPPS on communication networks, several vulnerabilities can affect the system's performance in terms of communication interruptions, network congestion-induced delay, and packet loss [4], impacting the power system performance and leading to system failures.

Cyber attackers can adopt cyber-attacks to hack the communication network by manipulating or blocking the transmitted signals in the form of a false data injection (FDI) attack or distributed denial of service (DDoS) attack, causing system instability [5]. More details about FDI attacks are available in [6,7]; this paper focuses on modeling the DDoS attack behavior and studying its impact on power system performance. DDoS attacks can cause significant corruption in communication networks by overwhelming them with excessive traffic from diverse sources. Two types can define the categorization of DDoS attacks; the first is network/transport layer DDoS attacks, which overwhelm the network by flooding it with traffic. The second is application-layer DDoS attacks targeting higher-layer protocols [8]. Regarding network/transport layer DDoS attacks, TCP SYN flooding is an attack created by transmitting excessive TCP SYN connection requests to overwhelm the server [9]. To start the attack, the attacker sends packets with random source IP addresses, and each packet has a SYN flag set for creating a connection with the server. Then, the victim responds to the spoof IP address and stands for authorization, which never comes. After receiving them, the victim responds to spoof IP addresses and waits for confirmation, which never comes. Consequently, the TCP SYN packets overwhelm the server, fulfilling its table, and it cannot accept new connections. As a result, the authorized cannot reach the server. Turning to the UDP (User Datagram Protocol) flooding, it does not require a connection setup for transmitting data. Thus, the attacker sends random UDP packets to the targeted system's ports [10]. After that, the victim checks which application stands for the response's target port. If it does not find anyone, it will send an ICMP packet to the faked source address with the message of destination unreachability, leading to system collapse [9]. Thus, cyber-attacks on power systems affect the physical components, degrade the system's behavior, and interrupt the communication surface, leading to the system's instability. Therefore, while investigating the performance of power systems, it is necessary to consider the operation characteristics of the communication systems and the cyber threats [11].

Therefore, simulation is a proper solution for studying the performance of cyber-physical power systems, including the impact of communication and cyber-attacks on system performance. MATLAB/Simulink, Power World, and RT-LAB are the most popular simulation tools for the simulation of power systems. For communication network infrastructures, OMNET++, ns2, ns3, and OPNET are well-known communication simulators [12]. However, no simulator can simulate both power and communication networks because their simulation requires separate solvers, for there is a difference in the dynamic behavior of power and communication networks [13]. Therefore, there is a necessity for a single platform that combines power and communication networks (co-simulation). It provides a foundation for investigating various research studies, considering the impact of communication and cyber risks on the power system operation [14]. The authors in [15] implemented the integration between Open DSS and ns3 with Mosaik, highlighting its application for voltage regulation in distribution grids. In [16], based on high-level architecture (HLA), the work proposed a co-simulation platform called INSPIRE, where the DIgSILENT Power Factory simulates the power system and OPNET emulates the communication network. Furthermore, OPAL-RT and OPNET have formed a co-simulation platform [17] for controlling the load bus voltage in a simple distribution system by switching the capacitor bank ON/OFF. This study has simulated the percentage of occupancy in the communication channel using background traffic generators and its effect on the value of latency. On the contrary, they did not address the impact of changing communication delays on the performance of the power system.

Microgrids play a crucial role as an integral part of the smart grid, utilizing a variety of DGs to meet rising energy consumption at the distribution level. They can operate in grid-connected and islanded modes of operation; particularly, islanded inverter-based microgrids contribute to power system sustainability by providing a resilient power supply and minimizing the reliance on the utility grid [18]. A pivotal aspect of operating these systems is the control strategy, which is essential in managing the power-sharing between the DGs within the MG to meet the load requirements under different operating conditions. Hierarchical control is the current way of controlling MG operation, comprising three layers of control: primary control, secondary control, and tertiary control [18–23]. The primary control layer includes the local controllers for all the DGs within the microgrid for autonomous power-sharing during system operation. In comparison, the secondary control is responsible for restoring the system frequency/voltage to its rated values under different conditions. In this paper, we focus on the primary and secondary control layers. Droop control in the primary control layer controls and preserves the frequency stability of each inverter within the MG for generating the reference voltage and frequency at each operating condition [20–24]. It is a communication-less power-sharing control, as within this layer, each inverter-based distributed generator has its local droop control [22]. However, the frequency deviation caused by the droop control is the major drawback to using this way of control [23]; introducing a secondary control layer helps eliminate this deviation [19]. Nevertheless, while operating in real-world scenarios, the communication network infrastructure between the primary and secondary control layers directly affects the system response. The communication network characteristics regarding network topology, data rate, communication latency, and cyber-attack vulnerability impact the MG control system [25]. Therefore, a recommendation is to study the MGs as cyber-physical systems to evaluate their performance under various operating conditions, assessing the cyber vulnerability that affects the sustainability and security of the integrated power and communication system.

Numerous studies have proposed diverse control strategies for controlling the operation of microgrids; the authors in [20] developed a detailed work for managing voltage source converters under an islanding mode of operation based on droop control. In [24], the authors presented a centralized secondary control scheme for voltage and frequency in an islanded inverter-based MG. However, they did not mention any analysis regarding the impact of communication on the proposed scheme. An accurate simulation of frequency support through elaborate models was demonstrated in [26] by integrating the power adjustments of prosumers, besides offering an enhancement in MG frequency control, employing a fuzzy logic-based estimation method. The authors in [27] proposed a centralized secondary frequency control scheme based on the model predictive control (MPC) method for an inverter-based MG; however, they did not consider the impact of communication delay between the implemented MPC-based secondary control and the local controllers. A frequency restoration algorithm in an islanded MG based on an event-driven method was developed in [28]. The control mechanism generated the control action by sensing the change in the load demand and the power generation. In [29], the authors proposed a power control mechanism for MG, optimized through the combination of the genetic algorithm (GA) and particle swarm (PSO). The proposed scheme proved its effectiveness under different operating conditions, though they did not include the cyber aspect impact on the presented analysis. A cascade-forward neural networks-based droop control algorithm for the inverter-based MG was developed in [30]; the authors proposed real-time experimental tests. However, they did not introduce the impact of cyberattacks on the proposed system. Although the previously mentioned proposed control strategies successfully control the MG and enhance its performance, most research studies have not examined the inverter-based MG as a cyber-physical system. Furthermore, they have not considered the diverse impact of communication delays and cyber-attacks on the proposed control schemes.

Upon reviewing the studies mentioned above, there is a research gap, prompting more exploration in studying the inverter-based MG as a cyber-physical system, including the impact of communication networks and cyber-attacks on overall system performance. In addition, there is a need to develop a flexible tool that can be used for several cyber-physical power system studies, combining both the physical and cyber layers in a single platform. Considering the above discussion, this paper proposes an innovative approach for assessing the frequency performance of an islanded cyber-physical inverter-based microgrid in different real-world scenarios. The experimental study incorporates realistic and non-ideal cyber scenarios using the proposed sophisticated cyber-physical co-simulation platform. The integration of OPAL-RT and the network simulator ns3 in a single co-simulation framework offers a flexible platform that can be a basis for several power systems studies as a cyber-physical system, encompassing real-time simulation of power and communication systems. RT-LAB has different packages and models, enabling integration with MATLAB/Simulink and facilitating the simulation of various power system applications. Network simulator ns3 is an open-source tool that supports the simulation of IP-based communication network applications. Furthermore, using Docker containers as a virtual interface network enables seamless data exchange between the local measurements and the secondary controller through the ns3-based communication model, which is also freely accessible. Thus, the open-source accessibility nature of both ns3 and Docker containers notably minimizes the overall computational cost of the proposed approach. Within the proposed cyber-physical MG, we utilize a centralized secondary control strategy; it runs asynchronously in the secondary control layer with the primary control layer in the physical system. The central controller collects information from all the individual DGs' local controllers within the physical MG. After that, it sends the control signal back to the local controllers in the primary control layer via the proposed ns3-based communication network, effectively restoring the frequency value to its reference. The innovative communication model developed in this work mimics the communication infrastructure between the primary and secondary control layers; it enables the examination of MG performance as a cyber-physical system, including analyzing the impact of communication latency and DDoS attacks on frequency stability. To summarize, the main contributions of the proposed work are as follows:

- Implementing an innovative cyber-physical co-simulation platform that integrates OPAL-RT, the network simulator ns3, and Docker containers into a unified, sophisticated platform, providing a sustainable tool to pursue various research studies within cyber-physical power systems applications.
- Proposing an experimental study targeting the sustainability challenges in cyber-physical inverter-based microgrids through an innovative way of assessing the frequency stability in different real-world scenarios.
- Developing an innovative ns3-based communication model that adequately represents the communication infrastructure between the primary and secondary control layers within the islanded inverter-based microgrid.
- Proposing a distributed denial of service (DDoS) model in real-time operation within the ns3-based communication surface for assessing sustainable MG operation in different cyber scenarios regarding communication delays and DDoS attacks.

The remainder of the paper follows this organization: Section 2 presents the proposed architecture of the cyber-physical inverter-based microgrid, including the power system and communication network modeling. Section 3 demonstrates the modeling of Distributed Denial of Service (DDoS) attacks in real-time operation. Section 4 presents the implementation of the proposed cyber-physical co-simulation platform for assessing the operation of an inverter-based MG. Section 5 delineated four subsections to assess the MG performance under normal operation, communication delay, and DDoS attacks—the conclusion in Section 6.

2. The Proposed Architecture of the Cyber-Physical Co-Simulation Platform

The proposed architecture of the cyber-physical inverter-based MG, as Figure 1 illustrates, is the outcome of integrating the microgrid that represents the physical layer and the communication network as a cyber-physical power system. The inverter-based MG model was developed with an RT-LAB simulation platform fully integrated with MATLAB/Simulink, allowing real-time simulation within OPAL-RT.

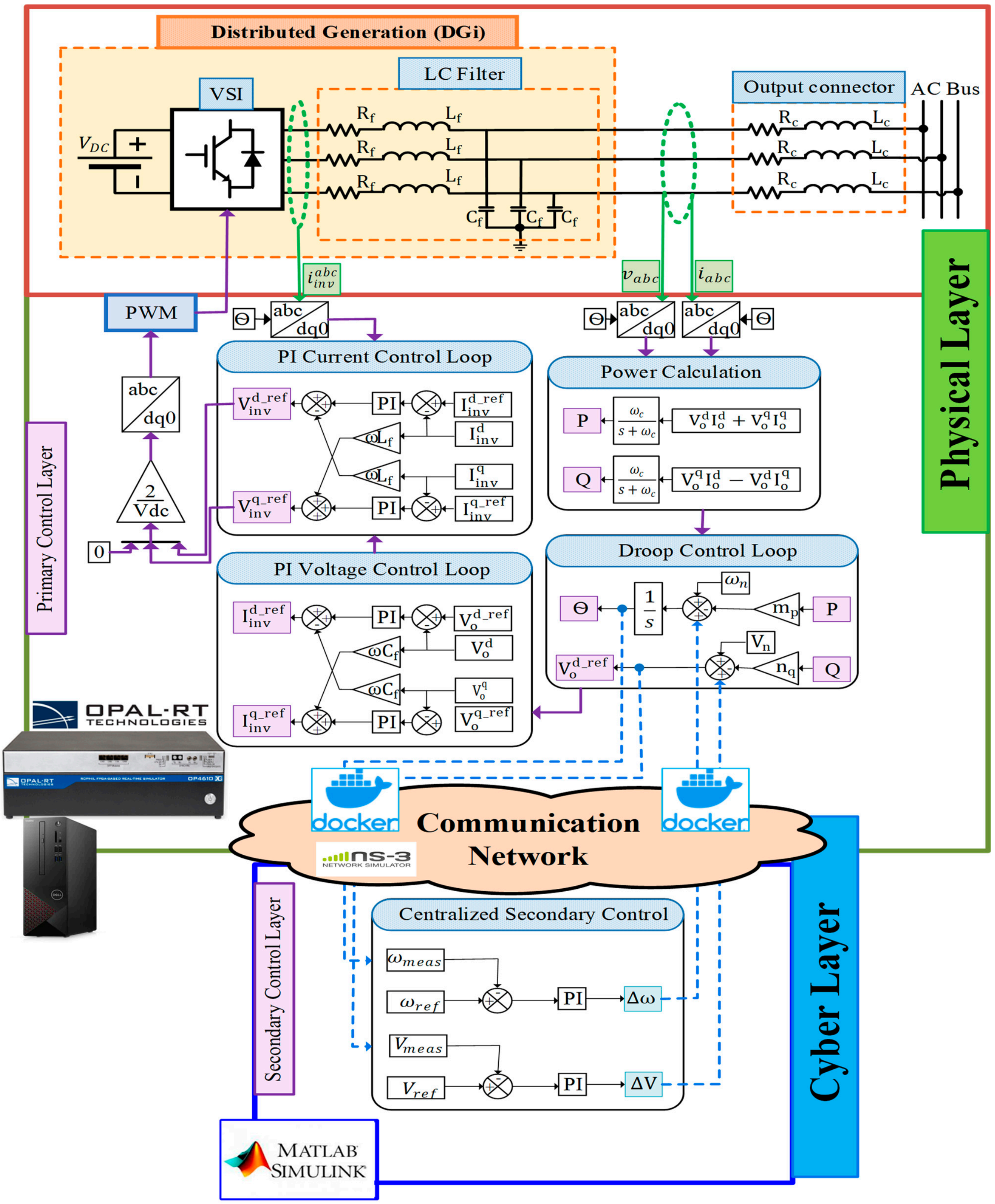


Figure 1. The proposed architecture of the cyber-physical inverter-based microgrid.

This work used the OPAL-RT real-time power systems simulator, the OP4610XG model, to simulate the inverter-based MG, including the MG model and its local controllers. In addition, we developed an innovative communication model using network simulator software (ns-3.35) to connect the centralized secondary controller, which runs on an external machine, to the MG model in OPAL-RT. The ns3 software provides a controlled environment for the experimental evaluation of different communication topologies. All the mentioned layers are in a single co-simulation platform that combines power and communication models. Docker containers facilitate the interfacing between the cyber and physical layers; these behave as proxies to transfer data between the real-time simulation in OPAL-RT and the communication network nodes in ns3 for information exchange.

2.1. Modeling and Control of an Inverter-Based Microgrid

Figure 2 describes the islanded inverter-based MG structure with its control loops considered in this study; it includes two parallel DGs equipped with their local controllers. Within the islanded inverter-based MG, each DG comprises a DC generation source, a voltage source inverter, an LC filter, and an RL output connector [31]. The modeling of the inverter-based MG, including the primary and secondary control layers, occurred using MATLAB/Simulink. In this work, focusing on the islanded inverter-based MG performance as a cyber-physical system, we simplified the input of the inverter as a DC source [32,33] to prioritize the investigations of real communication infrastructure impacts and cyber-attacks. This purposeful simplification omitted the intricate dynamics of renewable energy sources integrated into the DG system, such as solar variations and wind speed fluctuations, aligning with the proposed research goal and centering focus on the cyber-physical MG assessment. The inverters work under voltage control mode as the system works in an islanded mode, and the voltage and current control loops manage their operation; detailed equations governing these control loops are available in [30,34]. The two parallel-connected inverters operate under a droop control loop for power-sharing. The three mentioned control loops stand for the primary control layer of the MG, as described in Figures 1 and 2.

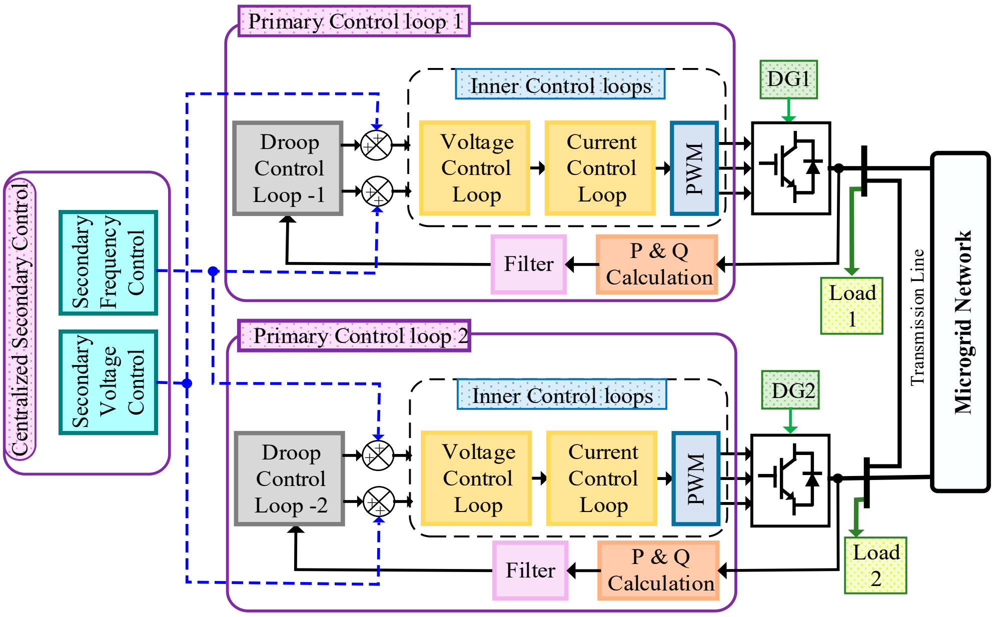


Figure 2. Schematic diagram of an islanded inverter-based microgrid with primary and secondary control loops.

The droop control regulates the system's frequency and voltage by controlling the active and reactive powers [31–34], standing as the primary level for frequency regulation within each inverter as per the present load conditions. It introduces synthetic droop to derive the reference frequency and voltage while computing the reactive and active output powers, as outlined in [33,34]. The instantaneous values of the active and reactive powers are p_{inst} and q_{inst}, respectively, as described in (1); v_o^{dq} and i_o^{dq} are the inverter output voltage and current after the dq-frame transformation. Subsequently, these instantaneous values pass through a low-pass filter to calculate the fundamental values of powers P and Q, as given in (2).

$$\begin{aligned} p_{inst} &= v_o^d i_o^d + v_o^q i_o^q \\ q_{inst} &= v_o^q i_o^d - v_o^d i_o^q \end{aligned} \tag{1}$$

$$P = \left(\frac{\omega_f}{s+\omega_f}\right) p_{inst} \qquad Q = \left(\frac{\omega_f}{s+\omega_f}\right) p_{inst} \tag{2}$$

Introducing an artificial droop in the frequency and output voltage of the inverter, as shown in (3), facilitates power-sharing among the sources; P_i and Q_i are the DG's active and reactive output power. ω_{ni} and V_{ni} are the reference signals for the system frequency and voltage, while the desired voltage and frequency are $v_{o,\ magi}$ and ω_i; m_{pi} and n_{qi} are the active and reactive power droop coefficients.

$$\begin{aligned} \omega_i &= \omega_{ni} - m_{pi} P_i \\ v_{o,magi} &= V_{ni} - n_{qi} Q_i \end{aligned} \tag{3}$$

We implement centralized secondary control to eliminate the deviations in the system's frequency and voltage from their nominal values during system operation. In this work, the centralized secondary control layer is based on a conventional PI control scheme that receives the frequency value from the primary control layer and restores the deviations in the frequency value, maintaining it at 60 Hz under different operating conditions. This method allows the restoration of voltage value deviation as well. The PI-based centralized secondary controller sends the control signals to restore the frequency and voltage deviations $\Delta\omega$ and Δv, respectively, as given in (4). For the implemented PI-based frequency secondary controller, ω_{ref} and ω_{meas} are the reference and measured frequency values; K_{pf_sec} and K_{if_sec} are the proportional and integral gains, respectively. V_{ref} and V_{meas} are the reference and measured voltage values, respectively, while K_{pv_sec} and K_{iv_sec} are the PI-based voltage controller gains. After that, the communication channels send the control signals to the primary control layer to eliminate the deviations, as introduced in (5).

$$\begin{aligned} \Delta\omega &= K_{pf\_sec}\,(\omega_{ref} - \omega_{meas}) + K_{if\_sec} \int (\omega_{ref} - \omega_{meas}) \\ \Delta v &= K_{pv\_sec}\,(V_{ref} - V_{meas}) + K_{iv\_sec} \int (V_{ref} - V_{meas}) \end{aligned} \tag{4}$$

$$\begin{aligned} \omega_i &= \omega_{ni} - m_{pi} P_i + \Delta\omega \\ v_{o,magi} &= V_{ni} - n_{qi} Q_i + \Delta v \end{aligned} \tag{5}$$

2.2. Modeling of the Communication Network Infrastructure

In this work, using the network simulator (ns3), we developed the emulation of the communication network for exchanging information between the local controllers in the physical system and the proposed centralized secondary controller. ns3 is an open-source network simulator with a highly flexible architecture, enabling users to implement different communication topologies. It also allows the application of various protocols. Figure 3 shows the basic architecture of ns3. This software offers a real-time simulation of actual communication devices, such as switches and routers, enabling the study of the communication issues impacting power systems, such as latency, package loss, and signal transmission errors [35].

The communication network model presented in this study comprises two local area networks (LANs), and the proposed architecture is based on the configuration of the power system application used in the testing [25,36]. In the ns3-based communication mode, a node represents each agent/controller in the power system. The first local area network (LAN-1) contains two nodes representing the local controllers for the two parallel inverters in the primary control layer. Meanwhile, a node in the second local area network (LAN-2) represents the centralized controller in the secondary control layer. Each node in the communication model has an IP address, as presented in Figure 4. Algorithm 1 demonstrates the development of the ns3-based communication network, mimicking the communication infrastructure between the central controller in the secondary control layer and each metering unit in the local controllers in the primary control layer. Based on this algorithm, we can emulate different communication models with different topologies depending on the power system application, considering the control algorithm, communication links, and the number of local measurement units in the physical layer.

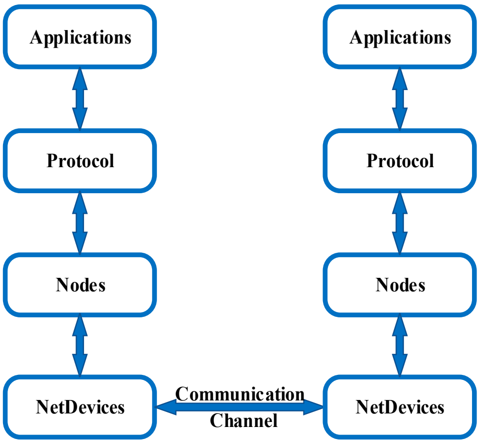


Figure 3. The basic architecture of ns3.

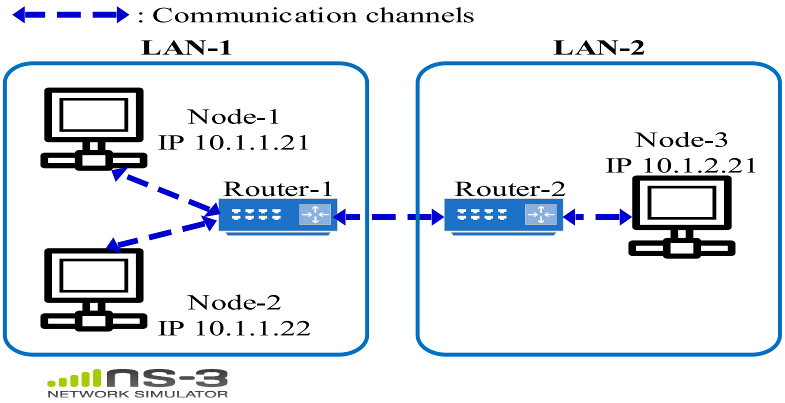


Figure 4. Schematic diagram of the developed communication network model in ns3.

Algorithm 1. Modeling of the ns3-based communication network.

```
1:  Include all the required headers based on the designed network topology.
2:  Enable logging in the developed model.
3:  Define the global configurations within the model.
4:  Identify the number of nodes based on the application; the number is five in this work.
5:  Create a node container for each zone:
      • LAN-1 container includes three nodes (node-1, node-2, and router-1).
      • LAN-2 container includes two nodes (node-3 and router-2).
      • The router's container includes two nodes (router-1 and router-2).
6:  Create a communication link between the nodes in the model based on the designed
    topology:
      • Point-to-point link between LAN-1 and LAN-2.
      • Carrier sense multiple access (CSMA) communication topology within each LAN.
7:  Assign IP addresses for the previously created nodes in each zone.
8:  Set a tab bridge at each node to interface with other devices outside the ns3-based
    communication model.
9:  Run the simulator.
```

2.3. The Interface between the Communication Network and the Physical System

The information exchange between each node in the communication model and the physical system devices occurs through docker containers. A docker container is a software package with the features needed to execute an application, as it is lightweight, standalone, and executable. The isolation of the software from its environment by containers guarantees that it runs consistently despite variances between development and staging environments [37]. This feature assesses security and allows different containers to run simultaneously on a single host. In this work, Docker containers in Linux OS act as proxies to transfer data between the local control agents in the physical system in OPAL-RT and in the communication network nodes in ns3. Figure 5 depicts the container's structure to set up virtual networks in Linux.

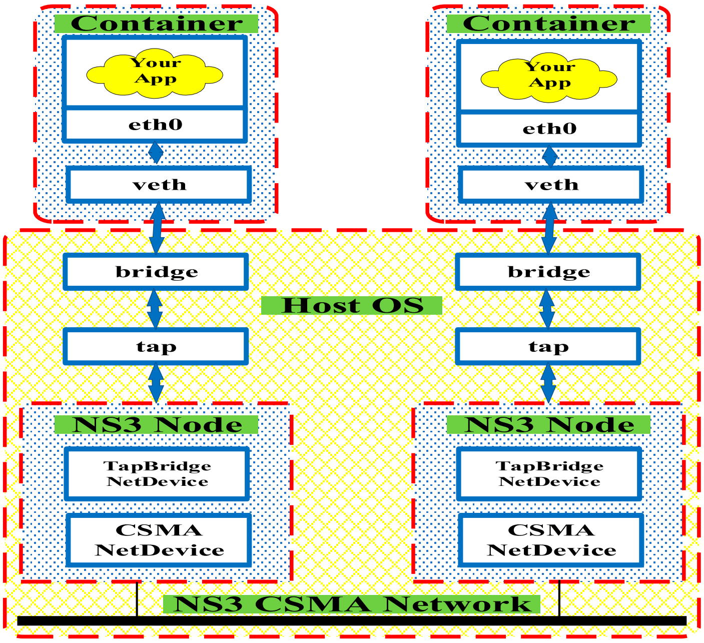


Figure 5. Construction of Linux containers to create virtual networks.

For interfacing between the two local control nodes in the physical layer and their corresponding nodes in the communication layer LAN-1, we created two docker containers. These containers eased access to each node in LAN-1 through the pre-configured tab bridges in the designed communication model. In addition, shared memory ran with the Linux operating system in the same machine with the docker containers to enable simultaneous access to the same memory by different actions. Thus, integrating the docker containers and the shared memory facilitated the bidirectional data flow between the physical system and the communication model.

3. Modeling of Distributed Denial of Service (DDoS) Attack

Distributed denial of service (DDoS) against the communication channels between the control center and the metering units can restrict the data flow from descending to their intended locations on time by way of distribution or forfeiting the connectivity, affecting the MG's performance [10]. The behavior of this attack involves flooding a target computer or network with traffic coming from multiple sources, seeking to prevent legitimate users from accessing the targeted system or network by consuming its resources. In the DDoS attack, using User Datagram Protocol (UDP) flooding represents one of the used techniques. The attacker conveys many packets to the victim's destination port. If the sent packets are large enough, the communication channels may become overburdened, and packets may not be able to reach their destination. Modeling UDP flooding attacks involves switching UDP traffic to the intended target point [38]. The attackers might utilize botnets to engage in illicit behaviors for hacking devices by sending UDP flooding attacks, causing the interruption of the targeted point, as Figure 6 depicts.

In this work, The DDoS attack can interrupt the communication channels between the MG's centralized secondary control and the local controllers in the primary control layer within the developed ns3-based communication model, affecting the MG's frequency stability. To mimic the DDoS attacks as a real-time simulation in ns3 that represents the cyber layer in this work, we emulated the UDP flooding behavior in ns3 to represent the DDoS attack that targeted the central control of the MG. Consequently, this overwhelms the centralized controller with many UDP packets sent from the attacker bots, increasing the contingency of the communication channels between the central and local controllers of the MG. This makes the controllers unable to send or receive any information and affects the system's performance. For emulating the DDoS in the developed communication model in ns3, it is necessary to identify the attack parameters and the application of the attack using UDP flooding within the communication network topology designed for communication between the secondary and primary control layers, as described in Algorithm 2.

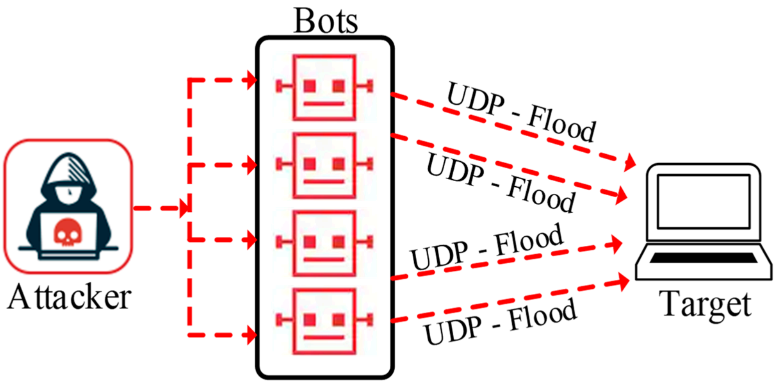


Figure 6. DDoS attack using UDP flooding.

Algorithm 2. DDoS attack using UDP flooding

```
1: Identify the DDoS attack experimental parameters (attack rate, max Bytes, number of bots).
2: Create nodes in the ns3-based communication model to identify the number of attackers' bots.
3: Create a link using point-to-point communication between the bot nodes and the target node (central controller node in LAN-2).
4: For each attacker bot node in the model:
       • Assign an IP address.
       • Define the behavior of the DDoS attack using UDP flooding and install the developed DDoS application in each created bot node.
       • Set the DDoS attack's start and stop times.
5: Run the simulation.
```

4. Implementation of a Cyber-Physical Co-Simulation Platform in the FIU Smart Grid Testbed

The proposed cyber-physical co-simulation platform was implemented on the FIU smart grid testbed, as demonstrated in Figure 7, with detailed IP addresses corresponding to each machine. This platform facilitates the assessment of different cyber-physical power systems with various control algorithms and their communication infrastructure.

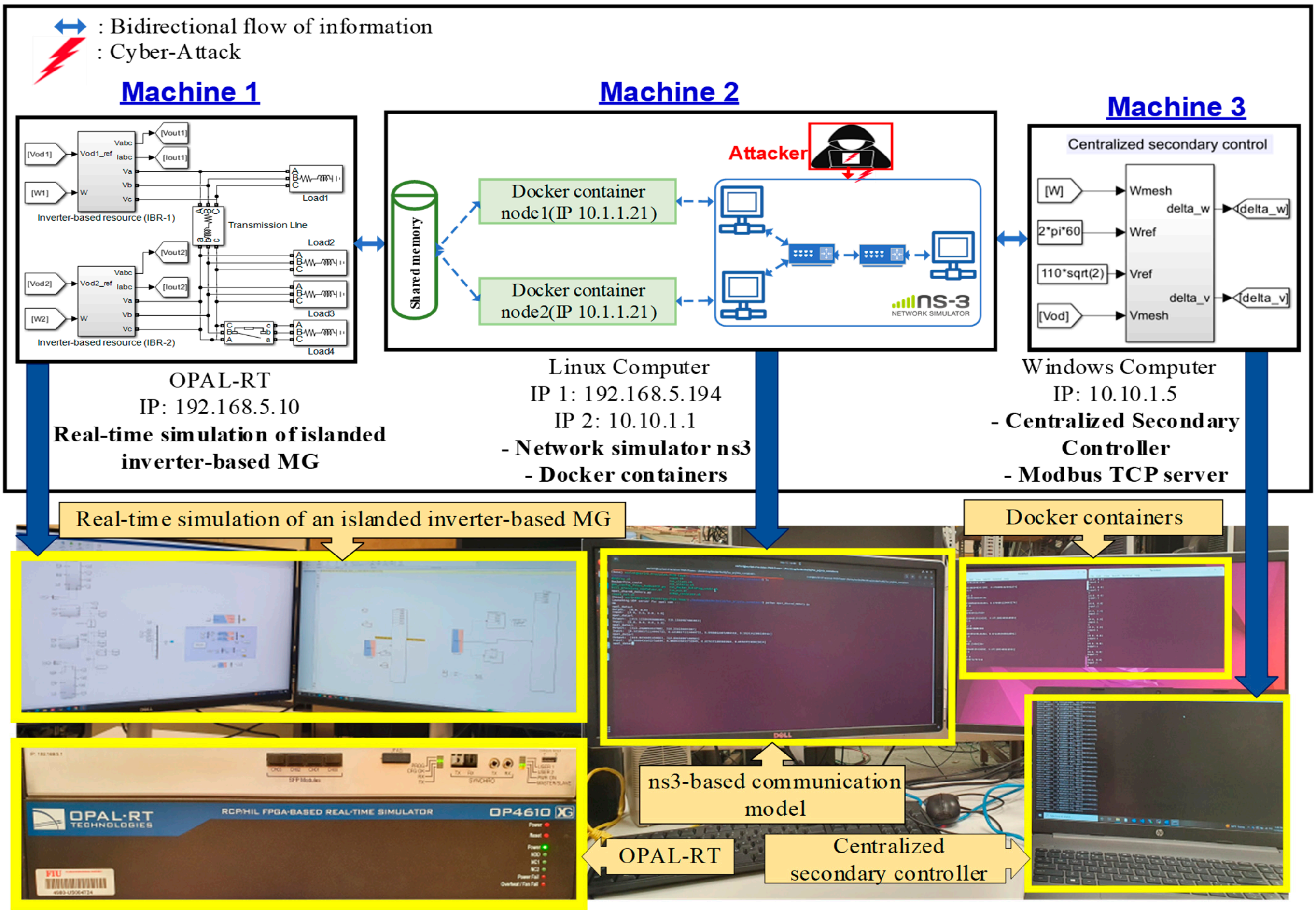
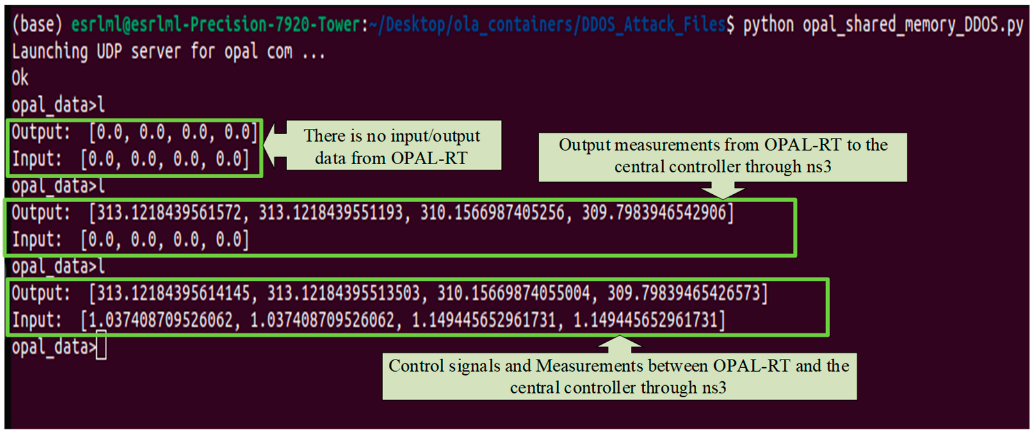

: Bidirectional flow of information
: Cyber-Attack
Machine 1
Machine 2
Machine 3
Inverter-based resource (IBR-1)
Inverter-based resource (IBR-2)
Transmission Line
Load1
Load2
Load3
Load4
Shared memory
Docker container node1(IP 10.1.1.21)
Docker container node2(IP 10.1.1.21)
Attacker
ns-3 NETWORK SIMULATOR
Centralized secondary control
[W]
2*pi*60
110*sqrt(2)
[Vod]
Wmesh
Wref
Vref
Vmesh
delta_w
delta_v
OPAL-RT
IP: 192.168.5.10
Real-time simulation of islanded inverter-based MG
Linux Computer
IP 1: 192.168.5.194
IP 2: 10.10.1.1
- Network simulator ns3
- Docker containers
Windows Computer
IP: 10.10.1.5
- Centralized Secondary Controller
- Modbus TCP server
Real-time simulation of an islanded inverter-based MG
Docker containers
ns3-based communication model
OPAL-RT
Centralized secondary controller

Figure 7. The proposed implementation of the cyber-physical co-simulation platform on the FIU smart grid testbed.

This paper examines the inverter-based MG's performance as a cyber-physical system using the proposed co-simulation platform, which integrates the following components:

- Machine 1: OPAL-RT, simulator for real-time simulation of the inverter-based MG, including all the local controllers of the physical system.
- Machine 2: Linux OS contains ns3 for communication network emulation, shared memory, and Docker containers to transfer data between OPAL-RT and network nodes in ns3. Two containers are created to connect to the two communication nodes of inverters. The UPD/IP protocol is used for interfacing between the communication model in machine 2 and the physical system that runs on OPAL-RT in machine 1.
- Machine 3: MATLAB/Simulink is used to implement the centralized secondary controller and a Modbus TCP server, then connect to the two developed containers in machine 2, representing the clients.

Figure 8 shows the data exchange through the proposed co-simulation platform. The flow of information can be checked throughout the shared memory designed between OPAL-RT and ns3; this process can be described as follows: in machine 2, we activated the communication model and established the docker containers. Following this, the power system model was executed in OPAL-RT (machine 1). Then, the proposed communication model facilitated the flow of local frequency and voltage measurement signals from OPAL-RT to the central controller (machine 3). Finally, communication between machine 3, containing the central controller (server), and machine 2 (clients) was implemented. After that, the data is exchanged between the controller and OPAL-RT through ns3; the data mapping is demonstrated in Table 1.



```
(base) esrlml@esrlml-Precision-7920-Tower:~/Desktop/ola_containers/DDOS_Attack_Files$ python opal_shared_memory_DDOS.py
Launching UDP server for opal com ...
Ok
opal_data>l
Output:  [0.0, 0.0, 0.0, 0.0]
Input:  [0.0, 0.0, 0.0, 0.0]
opal_data>l
Output:  [313.1218439561572, 313.1218439551193, 310.1566987405256, 309.7983946542906]
Input:  [0.0, 0.0, 0.0, 0.0]
opal_data>l
Output:  [313.12184395614145, 313.12184395513503, 310.15669874055004, 309.79839465426573]
Input:  [1.037408709526062, 1.037408709526062, 1.149445652961731, 1.149445652961731]
opal_data>
```

There is no input/output data from OPAL-RT

Output measurements from OPAL-RT to the central controller through ns3

Control signals and Measurements between OPAL-RT and the central controller through ns3

Figure 8. Data exchange between OPAL-RT and the central controller through ns3 (machine 2_ Linux OS).

Table 1. The mapping of data exchange.

Docker Container Name	IP Address	Device	Signals		Modbus Space on the Server	Position in Memory
			Name	**Data Type**		
Node 1	10.1.1.21	VSI-1	Meas f1	float	0–1	Output 0
			Meas v1	float	2–3	Output 1
			Ctrl f	float	4–5	Input 0
			Ctrl v	float	6–7	Input 1
Node 2	10.1.1.22	VSI-2	Meas f2	float	0–1	Output 2
			Meas v2	float	2–3	Output 3
			Ctrl f	float	4–5	Input 2
			Ctrl v	float	6–7	Input 3

5. Cyber-Physical Inverter-Based Microgrid Implementation and Experimental Results

In this part, we implement the real-time simulation of the islanded inverter-based MG in OPAL-RT to assess the MG's frequency control performance as a cyber-physical system. After that, it was integrated with the communication network emulation implemented in ns3 to obtain the control signals from the centralized secondary controller. Table 2 shows the tested MG and its control system parameters, considering that the two DGs have the same parameters.

Table 2. The MG parameters and the control system's gains.

Parameters	Symbol	Value
Filter inductance	L_f	3.5 mH
Filter capacitance	C_f	50 µf
Coupling inductance	L_c	0.35 mH
Coupling resistance	R_c	0.05 Ω
Inner voltage controller proportional gain	K_{pv}	0.285
The microgrid voltage	V_{rated}	110 V
The reference frequency	F_{ref}	60 Hz
Inner voltage controller integral gain	K_{iv}	590
Inner current controller proportional gain	K_{pc}	55
Inner current controller integral gain	K_{ic}	1570
Secondary controller proportional gain	K_{pf_sec}	0.08
Secondary controller integral gain	K_{if_sec}	7
The total connected load	P_{load_total}	13.9 kW

In this paper, we perform different experimental studies to investigate the MG's frequency control performance across various real-world scenarios. The experiments commenced with a real-time simulation of the proposed MG without the centralized secondary controller under different loading conditions. Subsequently, communication links were established between the secondary and primary control layers through the proposed ns3-based communication model. Finally, we assess the frequency stability of the MG under communication delays and the emulated DDoS attack that hacks the central controller.

5.1. Evaluating the MG Performance with the Primary Control Layer

In this section, the real-time examination of the islanded MG involves a connected load P_{load_total} shared across two parallel inverters. The MG experienced a step-change increase in the total connected load by P = 5.8 kW at t = 71 s and subsequently disconnected at t = 100 s, as shown in Figure 9. Figure 10 illustrates the MG's frequency response while operating with the droop control without the secondary control layer. The system exhibits stability, with the two parallel inverters sharing the load demand and coping with the load variations without oscillations. However, the droop control cannot eliminate the frequency deviation Δf. This deviation affects the connected load, especially when connecting sensitive loads. Furthermore, for prospective expansions, it is crucial to have a system with a constant frequency and voltage level without any deviations. This establishes connectivity with other DGs or MGs as a multi-MG system. Accordingly, appropriate control techniques and communication infrastructure design are essential to ensure the DGs' coordination without any voltage or frequency deviations from their reference values.

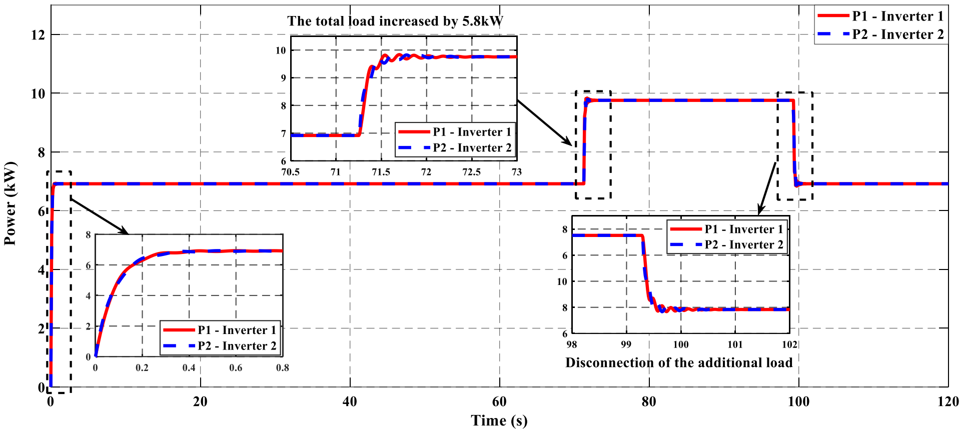


Figure 9. The generated power from the two parallel inverters.

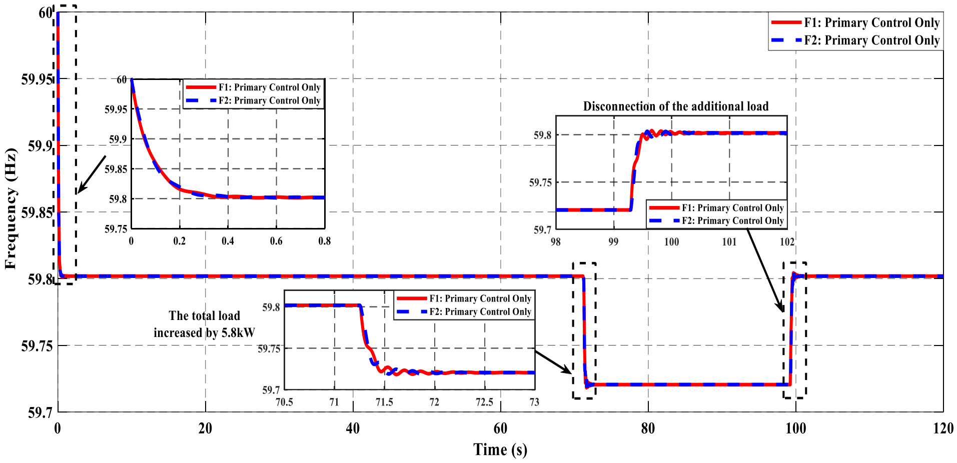


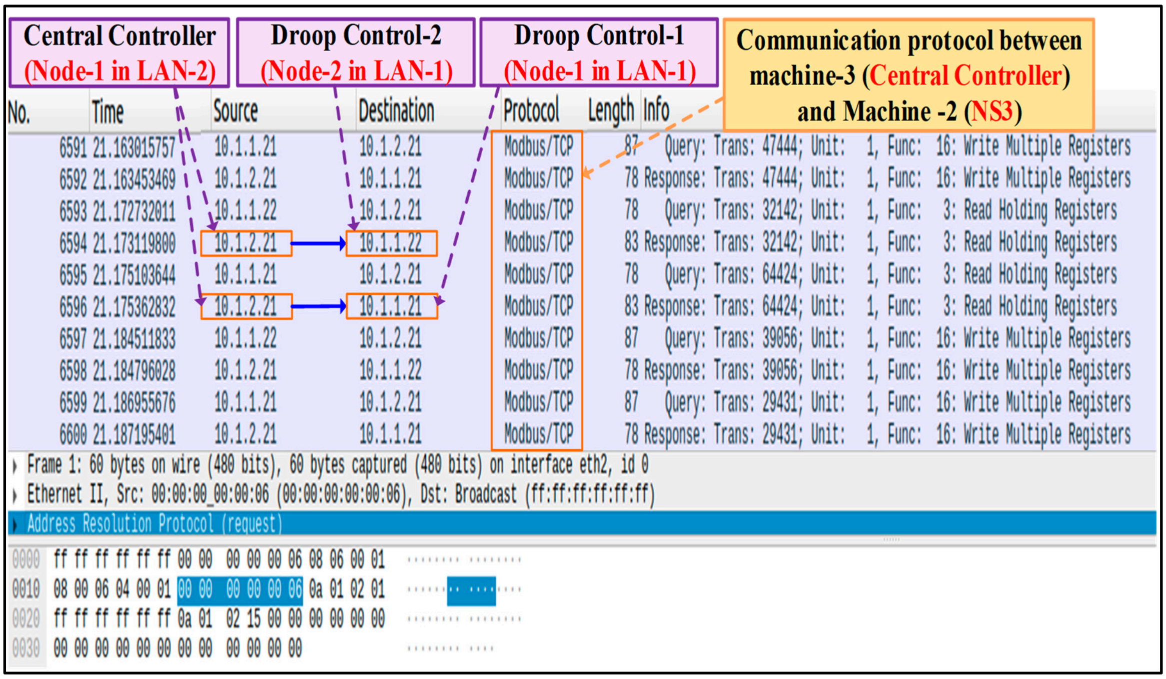
Figure 10. The frequency response with primary control only.

5.2. Assessing the MG's Stability with the Secondary Control

This section assesses the cyber-physical MG's operation with the centralized secondary controller that eliminates system frequency deviations. Beginning from this part forward, the developed ns3-based communication model establishes the communication links between the central controller and the physical system in OPAL-RT, encompassing the communication network features and the cyber vulnerability affecting the system operation. While operating solely with the primary control layer from t = 0 s, the activation of the communication model initiates to link the primary and secondary control layers at t = 36.5 s, assuming ideal communication channels (delay = 2 ms) between LAN-1 and LAN-2. The categorization of this experimental study includes the following four distinct phases:

- Phase 1 (0–36.5 s): The primary control only (based on droop control).
- Phase 2 (36.5–71 s): The activation of the ns3-based communication model and the secondary controller are working.
- Phase 3 (71–100 s): A step-up change in the total connected load with a value of 5.8 kW.
- Phase 4 (100–120 s): A step-down change with a value of 5.8 kW.

Figure 11 demonstrates the information flow, including bidirectional data transmission from the centralized controller node at LAN-2 (IP: 10.1.2.21) to the local controller nodes at LAN-1 (IP addresses: 10.1.1.21 and 10.1.1.22). As shown in Figure 12, during Phase 1, the droop control, a well-known method to control parallel inverters within the primary control layer, allows frequency synchronization at 59.8 Hz with deviations from the reference value. After activating the centralized secondary control in Phase 2 at t = 36.5 s, the frequency swiftly returns to the reference value of 60 Hz. Within Phase 3 and Phase 4, regardless of the additional load connection or disconnection from the MG, the steady-state frequency remains constant at 60 Hz. Accordingly, this implies that the designed centralized secondary control, based on the conventional PI controller, can eliminate the frequency deviations induced while operating with the primary control layer only.



```
No.   Time         Source      Destination  Protocol    Length Info
6591 21.163015757  10.1.1.21   10.1.2.21    Modbus/TCP  87    Query: Trans: 47444; Unit:  1, Func: 16: Write Multiple Registers
6592 21.163453469  10.1.2.21   10.1.1.21    Modbus/TCP  78 Response: Trans: 47444; Unit:  1, Func: 16: Write Multiple Registers
6593 21.172732011  10.1.1.22   10.1.2.21    Modbus/TCP  78    Query: Trans: 32142; Unit:  1, Func:  3: Read Holding Registers
6594 21.173119800  10.1.2.21   10.1.1.22    Modbus/TCP  83 Response: Trans: 32142; Unit:  1, Func:  3: Read Holding Registers
6595 21.175103644  10.1.1.21   10.1.2.21    Modbus/TCP  78    Query: Trans: 64424; Unit:  1, Func:  3: Read Holding Registers
6596 21.175362832  10.1.2.21   10.1.1.21    Modbus/TCP  83 Response: Trans: 64424; Unit:  1, Func:  3: Read Holding Registers
6597 21.184511833  10.1.1.22   10.1.2.21    Modbus/TCP  87    Query: Trans: 39056; Unit:  1, Func: 16: Write Multiple Registers
6598 21.184796028  10.1.2.21   10.1.1.22    Modbus/TCP  78 Response: Trans: 39056; Unit:  1, Func: 16: Write Multiple Registers
6599 21.186955676  10.1.1.21   10.1.2.21    Modbus/TCP  87    Query: Trans: 29431; Unit:  1, Func: 16: Write Multiple Registers
6600 21.187195401  10.1.2.21   10.1.1.21    Modbus/TCP  78 Response: Trans: 29431; Unit:  1, Func: 16: Write Multiple Registers
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth2, id 0
› Ethernet II, Src: 00:00:00_00:00:06 (00:00:00:00:00:06), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Address Resolution Protocol (request)
0000  ff ff ff ff ff ff 00 00  00 00 00 06 08 06 00 01   ········ ········
0010  08 00 06 04 00 01 00 00  00 00 00 06 0a 01 02 01   ········ ········
0020  ff ff ff ff ff ff 0a 01  02 15 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Figure 11. Wireshark capture of the data flows through the proposed ns3-based communication model (at the centralized controller node).

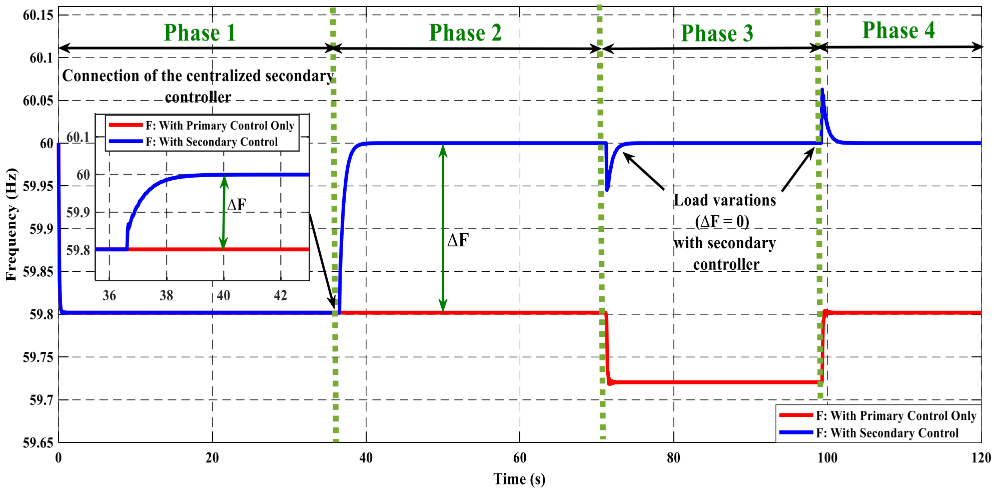


Figure 12. The frequency response with the proposed centralized secondary controller compared to the droop control only.

5.3. Scrutinizing the Impact of Communication Delay on Frequency Response

The communication infrastructure facilitates the control signals broadcasting from the secondary controller to the local controllers. However, these communication links may induce delays that can degrade the control performance and affect the system stability. In this experiment, to evaluate the impact of communication delay on the MG frequency performance, the assessment involved manipulating the communication delay value within the innovative communication model between LAN-2 (central controller) and LAN-1 (local controllers). Here, we assessed communication delays of 25 ms, 50 ms, 75 ms, and 100 ms while recording the frequency responses correlated to each value to illustrate how communication latency influences the MG's frequency stability, considering the same four phases of operation stated in the previous case study. Figure 13 depicts the impact of increasing communication latency between the central and local controllers under different operating conditions. In Phase 1, the frequency was stable at 59.8 Hz without oscillations; unfortunately, the MG encountered challenges in precisely tracking the reference frequency, revealing limitations in the droop control as one of the state-of-the-art control schemes in controlling multiple parallel inverter-based resources. Although it could effectively manage the power-sharing between the parallel inverters, it struggled to mitigate the steady-state deviation during operation.

Subsequently, at t = 36.5 s (Phase 2), the activation of the centralized secondary control, employing the PI-conventional controller, occurs and accesses the local frequency measurements from the primary control layer via the ns3-based communication channels. It compares the measured value with the reference frequency (60 Hz), leveraging the integral term in the PI controller to eliminate the steady-state error in frequency. The communication links relay the resultant control signal to the primary control layer, rectifying any frequency response inconsistencies within the parallel inverters. In this experiment, non-ideal communication channels between the primary and secondary control levels introduce delays, significantly impacting the transient frequency performance during the secondary control connection. These delays contribute to amplifying the maximum overshoot and longer settling times. Furthermore, the analysis of load variations in Phase 3 and Phase 4, as presented in Figure 14, depicts that elevating the delay value from 25 ms to 100 ms intensifies frequency oscillations and prolongs the system convergence to the steady state, especially at delay values of 75 ms and 100 ms during load changes compared to the ideal communication scenario.

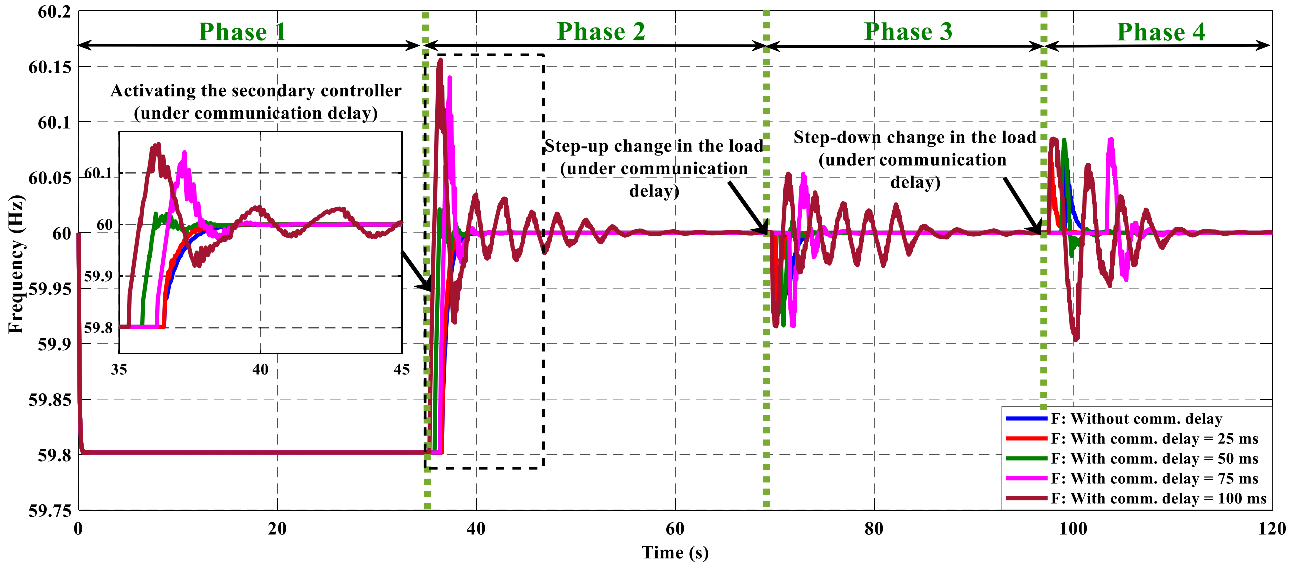


Figure 13. The impact of communication latency on the frequency response under different operating conditions.

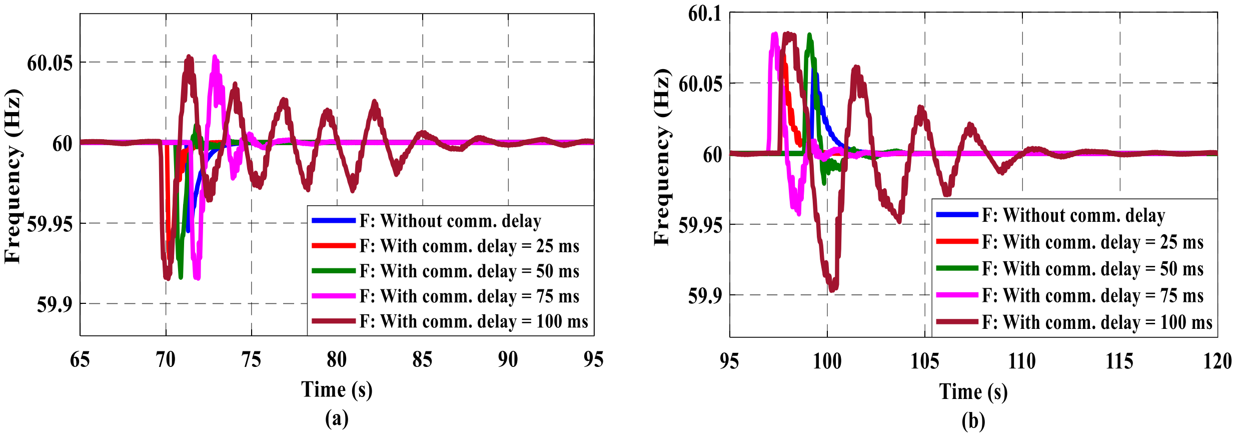


Figure 14. Enlarged view of the impact of communication latency on the frequency response under load changes: (**a**) step-up change in the load; (**b**) step-down change in the load.

The experimental results demonstrate that changing communication delay up to 100 ms affects the transient performance of frequency without compromising its stability. By contrast, instability issues arise when the communication delay exceeds 100 ms and the system cannot reach the reference value, as depicted in Figure 15, during step changes in the connected load under a delay of 120 ms. The frequency is critically stable and oscillates around the reference value. The observed fluctuations in frequency are due to a mismatch between the control signal transmitted to local controllers and the system's actual status. For instance, receiving delayed control signals with high values after the system has already reached a new state of operation makes the system critically stable. The system will be unstable if we increase the communication delays above 120 ms.

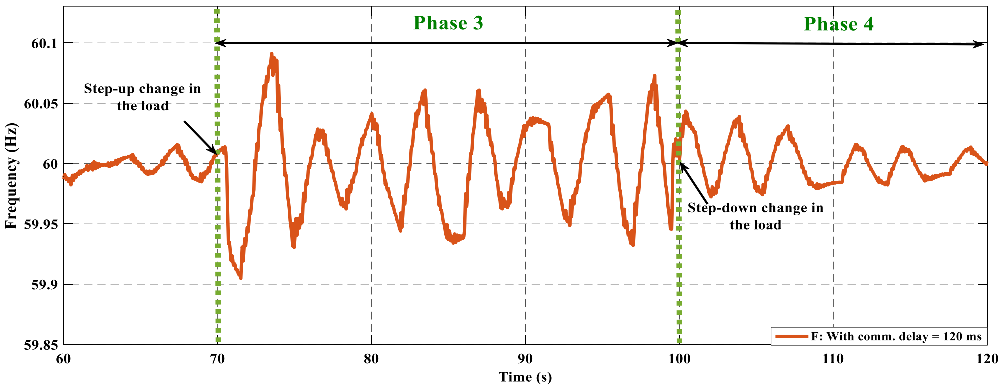


Figure 15. The frequency performance during load changes at a communication delay of 120 ms.

Figures 16 and 17 summarize the impact of increasing the communication delay on frequency transient stability in terms of the settling time and the percentage maximum peak (%MP) values, respectively. We can notably see that the increasing latency impacts the transient stability of the proposed system based on the value of the delay in communication between the secondary and primary levels within the MG. The classification of frequency stability regions for the system based on delay values involves classifying them into specific ranges as follows:

- Delay (0–100 ms): The frequency response is stable and can track the reference value effectively without steady-state errors.
- Delay (100–120 ms): The frequency is critically stable; it oscillates around the reference value and cannot reach a steady-state value.
- Delay (>120 ms): The frequency response is unstable.

Although the system can reach the reference value during this experimental study, the PI-based centralized secondary control works with limitations due to its operational characteristics employing constant gains values that cannot be adapted during the system operation. Thus, it cannot ensure the system's stability under different communication delays. This study proves the need to study the MG as a cyber-physical system through the proposed co-simulation platform, including the impact of real communication issues, such as delays, as these affect the overall performance. Furthermore, according to the assessment experiment's findings, we can specify this system's stability ranges. This is a research gap in MG control studies; they focus more on the control system design without considering how the communication links in real scenarios would influence the control system. As we present here, these communication issues must be considered, and the control design for MG will only be effective practically by considering the communication network.

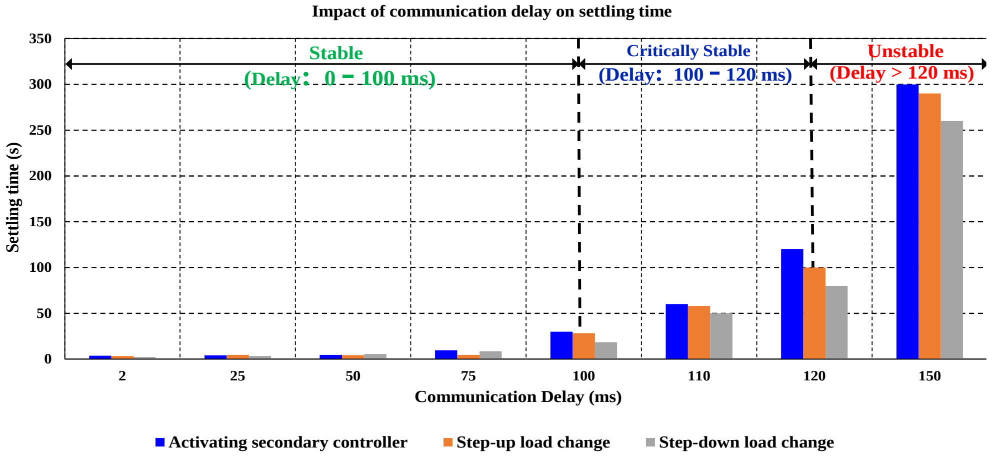


Figure 16. Impact of communication delay on settling time during different transient changes.

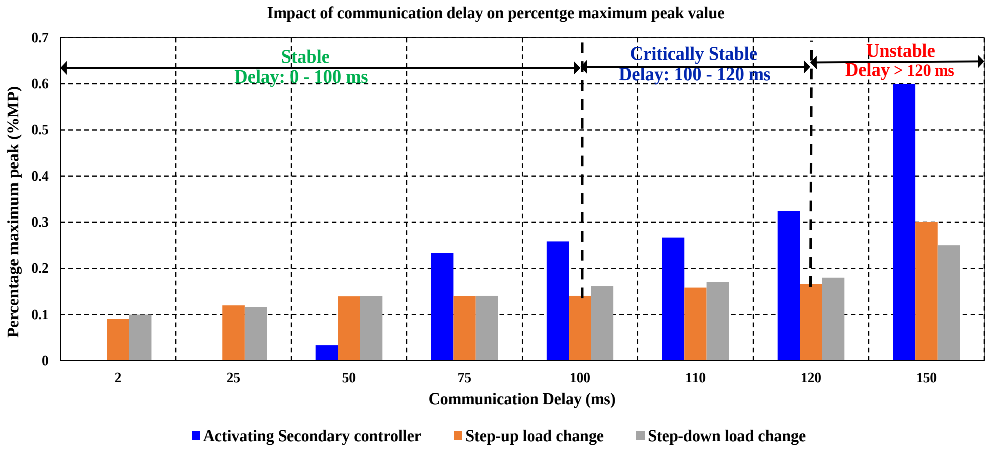
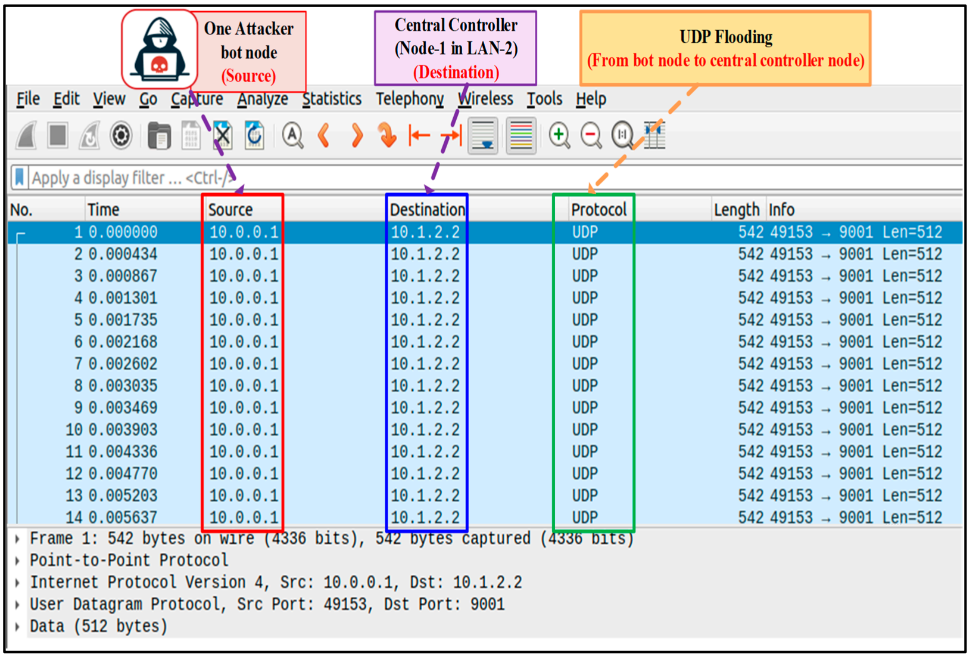


Figure 17. Impact of communication delay on percentage maximum peak value during different transient changes.

5.4. Examining the MG's Frequency Performance under the DDoS Attack

The communication surface between the central controller and the physical system is vulnerable to cyber risks. In this test, the communication surface represented by the ns3-based communication model was exposed to an emulated DDoS attack to assess the sustainable operation and stability of the MG. Based on Algorithm 2 in Section 3, the DDoS attack was modeled considering that the number of the attacker bots is ten, and the centralized secondary controller node is exposed to an emulated UDP flooding DDoS attack. The operation of the MG under the DDoS attack within the communication surface is as follows:

- At t = 0 s, the physical system typically starts in OPAL-RT without the secondary control.
- At t = 36.5 s, the centralized secondary controller connects to the physical system via the proposed communication model.
- At t = 40 s, the emulated attacker starts sending excessive UDP flooding messages, as presented in Figure 18, from the attacker's nodes to the centralized control node in LAN-2 within the ns3-based communication model, demonstrated graphically in Figure 19.


One Attacker bot node (Source)
Central Controller (Node-1 in LAN-2) (Destination)
UDP Flooding (From bot node to central controller node)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source     Destination  Protocol  Length Info
  1 0.000000   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
  2 0.000434   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
  3 0.000867   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
  4 0.001301   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
  5 0.001735   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
  6 0.002168   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
  7 0.002602   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
  8 0.003035   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
  9 0.003469   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
 10 0.003903   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
 11 0.004336   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
 12 0.004770   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
 13 0.005203   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
 14 0.005637   10.0.0.1   10.1.2.2     UDP        542 49153 → 9001 Len=512
› Frame 1: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits)
› Point-to-Point Protocol
› Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.1.2.2
› User Datagram Protocol, Src Port: 49153, Dst Port: 9001
› Data (512 bytes)
```

Figure 18. Wireshark capture at a bot node during the DDoS attack using UDP flooding.

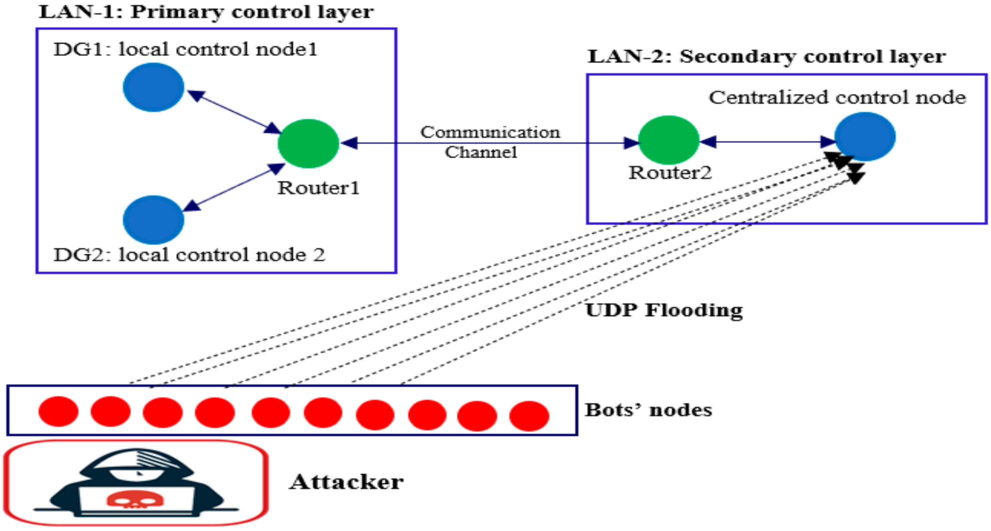
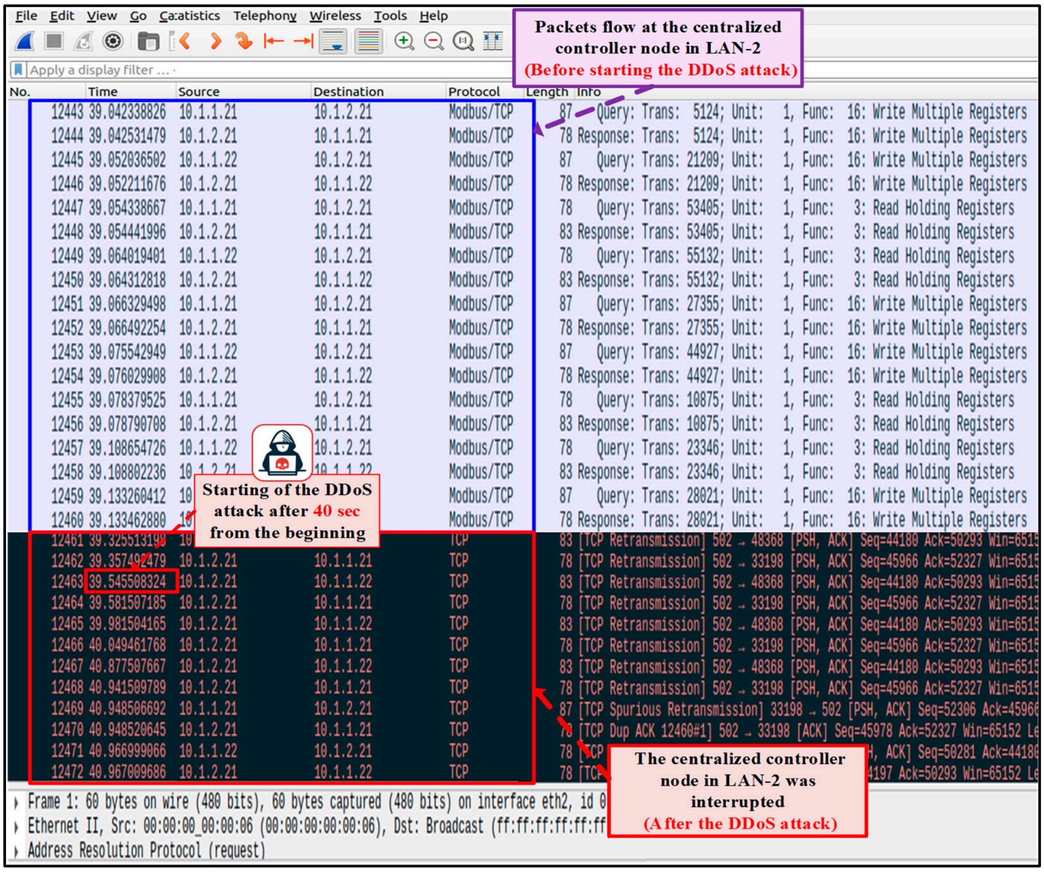


Figure 19. Graphical representation for DDoS attack within the ns3-based communication model.

While increasing the contingency resulting from UPD flooding through the communication channels, the centralized controller faces interruptions and cannot send or receive any packets. This results in a loss of connectivity between the primary and secondary control layers, as presented in Figure 20. Reducing the number of attacker bots in the proposed DDoS attack model results in the system acting similarly to its operation under communication delay, where the central controller can send delayed control signals to the local controllers. Figure 21 depicts the frequency performance during this test and divides it into the following four zones:

- Zone A (0–36.5 s): The MG worked based on primary control only; thus, the frequency was stable but deviated from its nominal value.
- Phase B (36.5–45 s): The established communication model connected the secondary control layer to the physical layer, eliminating the frequency deviation. At t_{attack} = 40 s, the DDoS attack commenced; however, it did not impact the system, as it was in a steady state.
- Zone C (45–70 s): The emulated attack hacked the communication surface, leading to central controller corruption, as described in Figure 20. However, the absence of secondary control signals within this zone did not affect the system, as no operating conditions change needed a control action.
- Zone D (70–100 s): A step-up change occurred at t = 70 s, while the central controller cannot sense this variation as it is under attack. Consequently, the frequency cannot remain constant at 60 Hz, and there is a frequency deviation. The system remains stable but with a frequency deviation value depending on the load change amount, the same as operation with droop control only.

It is pertinent to mention that the rate at which the DDoS attack affects the MG stability depends on the system's status when the attack occurs. Therefore, if the DDoS attack arises while the MG still has not reached its steady state, it may lead to severe conditions, jeopardizing the system's stability. Figure 22 depicts the MG under a DDoS attack at t = 37 s; meanwhile, the centralized secondary controller connection occurred at t = 36.5 s, meaning the MG did not reach its steady state. Accordingly, the system loses its stability due to the mismatch between the value of the control command from the secondary control layer and the current behavior of the MG's response in the physical layer.



```
No.    Time         Source      Destination   Protocol    Length Info
 12443 39.042338826 10.1.1.21   10.1.2.21     Modbus/TCP  87     Query: Trans:  5124; Unit:   1, Func:  16: Write Multiple Registers
 12444 39.042531479 10.1.2.21   10.1.1.21     Modbus/TCP  78 Response: Trans:  5124; Unit:   1, Func:  16: Write Multiple Registers
 12445 39.052036502 10.1.1.22   10.1.2.21     Modbus/TCP  87     Query: Trans: 21209; Unit:   1, Func:  16: Write Multiple Registers
 12446 39.052211676 10.1.2.21   10.1.1.22     Modbus/TCP  78 Response: Trans: 21209; Unit:   1, Func:  16: Write Multiple Registers
 12447 39.054338667 10.1.1.21   10.1.2.21     Modbus/TCP  78     Query: Trans: 53405; Unit:   1, Func:   3: Read Holding Registers
 12448 39.054441996 10.1.2.21   10.1.1.21     Modbus/TCP  83 Response: Trans: 53405; Unit:   1, Func:   3: Read Holding Registers
 12449 39.064019401 10.1.1.22   10.1.2.21     Modbus/TCP  78     Query: Trans: 55132; Unit:   1, Func:   3: Read Holding Registers
 12450 39.064312818 10.1.2.21   10.1.1.22     Modbus/TCP  83 Response: Trans: 55132; Unit:   1, Func:   3: Read Holding Registers
 12451 39.066329498 10.1.1.21   10.1.2.21     Modbus/TCP  87     Query: Trans: 27355; Unit:   1, Func:  16: Write Multiple Registers
 12452 39.066492254 10.1.2.21   10.1.1.21     Modbus/TCP  78 Response: Trans: 27355; Unit:   1, Func:  16: Write Multiple Registers
 12453 39.075542949 10.1.1.22   10.1.2.21     Modbus/TCP  87     Query: Trans: 44927; Unit:   1, Func:  16: Write Multiple Registers
 12454 39.076029908 10.1.2.21   10.1.1.22     Modbus/TCP  78 Response: Trans: 44927; Unit:   1, Func:  16: Write Multiple Registers
 12455 39.078379525 10.1.1.21   10.1.2.21     Modbus/TCP  78     Query: Trans: 10875; Unit:   1, Func:   3: Read Holding Registers
 12456 39.078790708 10.1.2.21   10.1.1.21     Modbus/TCP  83 Response: Trans: 10875; Unit:   1, Func:   3: Read Holding Registers
 12457 39.108654726 10.1.1.22   10.1.2.21     Modbus/TCP  78     Query: Trans: 23346; Unit:   1, Func:   3: Read Holding Registers
 12458 39.108802236 10.1.2.21   10.1.1.22     Modbus/TCP  83 Response: Trans: 23346; Unit:   1, Func:   3: Read Holding Registers
 12459 39.133260412 10                        Modbus/TCP  87     Query: Trans: 28021; Unit:   1, Func:  16: Write Multiple Registers
 12460 39.133462880 10                        Modbus/TCP  78 Response: Trans: 28021; Unit:   1, Func:  16: Write Multiple Registers
 12461 39.325513198 10                        TCP         83 [TCP Retransmission] 502 → 48368 [PSH, ACK] Seq=44180 Ack=50293 Win=6515
 12462 39.357492479 10.1.2.21   10.1.1.21     TCP         78 [TCP Retransmission] 502 → 33198 [PSH, ACK] Seq=45966 Ack=52327 Win=6515
 12463 39.545508324 10.1.2.21   10.1.1.22     TCP         83 [TCP Retransmission] 502 → 48368 [PSH, ACK] Seq=44180 Ack=50293 Win=6515
 12464 39.581507185 10.1.2.21   10.1.1.21     TCP         78 [TCP Retransmission] 502 → 33198 [PSH, ACK] Seq=45966 Ack=52327 Win=6515
 12465 39.981504165 10.1.2.21   10.1.1.22     TCP         83 [TCP Retransmission] 502 → 48368 [PSH, ACK] Seq=44180 Ack=50293 Win=6515
 12466 40.049461768 10.1.2.21   10.1.1.21     TCP         78 [TCP Retransmission] 502 → 33198 [PSH, ACK] Seq=45966 Ack=52327 Win=6515
 12467 40.877507667 10.1.2.21   10.1.1.22     TCP         83 [TCP Retransmission] 502 → 48368 [PSH, ACK] Seq=44180 Ack=50293 Win=6515
 12468 40.941509789 10.1.2.21   10.1.1.21     TCP         78 [TCP Retransmission] 502 → 33198 [PSH, ACK] Seq=45966 Ack=52327 Win=6515
 12469 40.948506692 10.1.1.21   10.1.2.21     TCP         87 [TCP Spurious Retransmission] 33198 → 502 [PSH, ACK] Seq=52306 Ack=45966
 12470 40.948520645 10.1.2.21   10.1.1.21     TCP         78 [TCP Dup ACK 12460#1] 502 → 33198 [ACK] Seq=45978 Ack=52327 Win=65152 Le
 12471 40.966999066 10.1.1.22   10.1.2.21     TCP         78 [TCP                      H, ACK] Seq=50281 Ack=44180
 12472 40.967009686 10.1.2.21   10.1.1.22     TCP         78 [TC                       4197 Ack=50293 Win=65152 Le
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth2, id 0
› Ethernet II, Src: 00:00:00_00:00:06 (00:00:00:00:00:06), Dst: Broadcast (ff:ff:ff:ff:ff:ff
› Address Resolution Protocol (request)
```

Packets flow at the centralized controller node in LAN-2 (Before starting the DDoS attack)

Starting of the DDoS attack after 40 sec from the beginning

The centralized controller node in LAN-2 was interrupted (After the DDoS attack)

Figure 20. Wireshark capture at the central controller node representing the controller collapse under the DDoS attack.

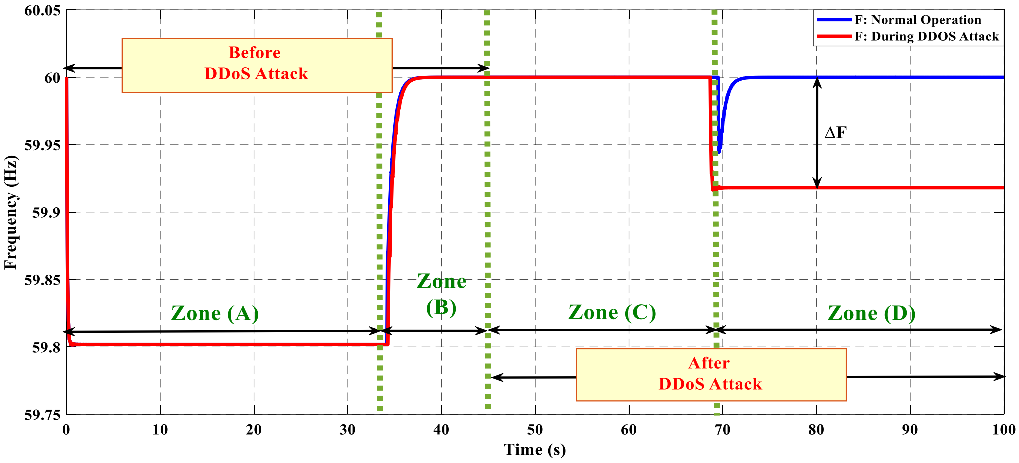


Figure 21. The MG's frequency response with/without the DDoS attack (t_{attack} = 40 s).

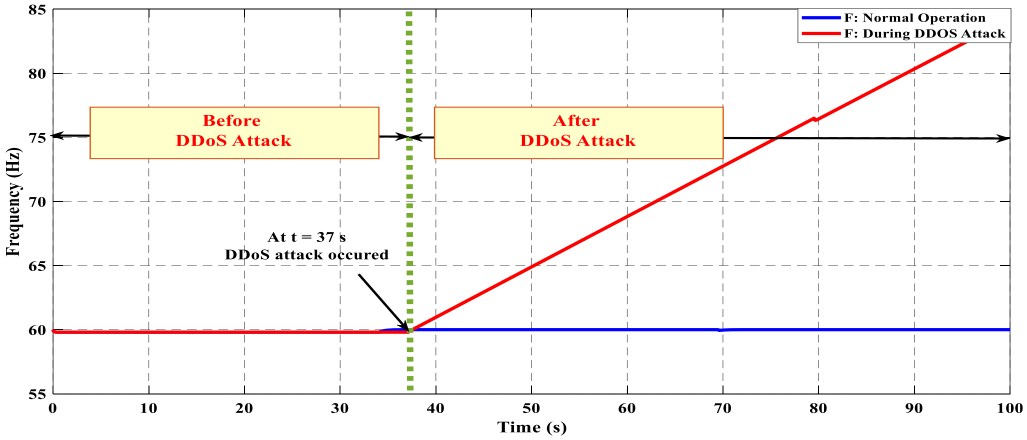


Figure 22. The MG's frequency response with/without the DDoS attack (t_{attack} = 37 s).

6. Conclusions

This study broadens our insights into the sustainability and security challenges intrinsic to inverter-based MGs, specifically in cyber-physical systems. Through the meticulous integration of OPAL-RT, ns3, and Docker containers, the developed innovative cyber-physical co-simulation framework uncovers the MG vulnerabilities, emphasizing the importance of exposing the MG control system to cyber threats for ensuring secure and sustainable operation. The experimental results depict the effectiveness of using the secondary controller, eliminating the steady-state error of the system's frequency and fortifying the MG's flexibility for scalable future expansions. Notably, the proposed ns3-based communication model emerges as a robust base for assessing the frequency stability of an islanded inverter-based MG under real-time communication delays and DDoS attacks. Real-time simulations demonstrate the impact of changing the communication delay on the frequency transient stability, offering insights into the stability and instability regions and highlighting the adverse effect of heightened delays, causing system destabilization.

Furthermore, the assessment of the MG's frequency response under the emulated DDoS attack highlights its impact on the MG's performance. It shows that the DDoS attack will impact the system based on the status of the physical system when the attack occurs. In addition, the proposed platform serves as a sustainable tool for examining communication effects on MG control and assessing vulnerability to cyber-attacks, forming a foundation for future studies of various cyber-physical power system applications. These findings offer insights into the vulnerability studies for inverter-based MGs, guiding the design of secure communication networks and resilient control strategies to enhance MG performance. In future work, we aim to develop an adaptive resilient control scheme to enhance the microgrid performance under communication delays and cyber-attacks. This addresses the adaptability limitations of the proposed PI-based conventional control scheme, which relies on fixed gains that cannot adjust under cyber-severe real-time conditions. Additionally, through the implemented cyber-physical platform, we can expand the proposed microgrid system into multi-microgrids with the proper design of their corresponding communication model, addressing the challenges in their operation as cyber-physical systems.

Author Contributions: Conceptualization, O.A., T.-L.N. and O.A.M.; methodology, O.A. and T.-L.N.; software, O.A. and T.-L.N.; validation, O.A.; formal analysis, O.A.; resources, O.A.M.; data curation, O.A.; writing—original draft preparation, O.A.; writing—review and editing, O.A. and O.A.M.; visualization, O.A.; supervision, O.A.M.; project administration, O.A.M.; funding acquisition, O.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by a grant from the US Department of Energy grant #DE-NA0004016 and the National Science Foundation grant #2113880.

Data Availability Statement: Data is contained within the article.

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

References

1. Lu, L.-Y.; Chu, C.-C. Consensus-Based Secondary Frequency and Voltage Droop Control of Virtual Synchronous Generators for Isolated AC Micro-Grids. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2015**, *5*, 443–455. [CrossRef]
2. Younesi, A.; Shayeghi, H.; Wang, Z.; Siano, P.; Mehrizi-Sani, A.; Safari, A. Trends in modern power systems resilience: State-of-the-art review. *Renew. Sustain. Energy Rev.* **2022**, *162*, 112397. [CrossRef]
3. Barbierato, L.; Estebsari, A.; Bottaccioli, L.; Macii, E.; Patti, E. A Distributed Multimodel Co-simulation Platform to Assess General Purpose Services in Smart Grids. *IEEE Trans. Ind. Appl.* **2020**, *56*, 5613–5624. [CrossRef]
4. Saleh, M.; Esa, Y.; Hariri, M.E.; Mohamed, A. Impact of Information and Communication Technology Limitations on Microgrid Operation. *Energies* **2019**, *12*, 2926. [CrossRef]
5. Nejabatkhah, F.; Li, Y.W.; Liang, H.; Ahrabi, R.R. Cyber-Security of Smart Microgrids: A Survey. *Energies* **2020**, *14*, 27. [CrossRef]
6. Zhang, H.; Meng, W.; Qi, J.; Wang, X.; Zheng, W.X. Distributed Load Sharing Under False Data Injection Attack in an Inverter-Based Microgrid. *IEEE Trans. Ind. Electron.* **2019**, *66*, 1543–1551. [CrossRef]
7. Reda, H.T.; Anwar, A.; Mahmood, A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts. *Renew. Sustain. Energy Rev.* **2022**, *163*, 112423. [CrossRef]
8. Hoque, N.; Bhattacharyya, D.K.; Kalita, J.K. Botnet in DDoS Attacks: Trends and Challenges. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2242–2270. [CrossRef]
9. Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. *IEEE Access* **2020**, *8*, 177447–177470. [CrossRef]
10. Ortega-Fernandez, I.; Liberati, F. A Review of Denial-of-Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning. *Energies* **2023**, *16*, 635. [CrossRef]
11. Tang, D.; Fang, Y.-P.; Zio, E. Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber-attacks and online detection methods. *Reliab. Eng. Syst. Saf.* **2023**, *235*, 109212. [CrossRef]
12. Li, W.; Zhang, X.; Li, H. Co-simulation platforms for co-design of networked control systems: An overview. *Control Eng. Pract.* **2014**, *23*, 44–56. [CrossRef]
13. Mets, K.; Ojea, J.A.; Develder, C. Combining Power and Communication Network Simulation for Cost-Effective Smart Grid Analysis. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1771–1796. [CrossRef]
14. Mihal, P.; Schvarcbacher, M.; Rossi, B.; Pitner, T. Smart grids co-simulations: Survey & research directions. *Sustain. Comput. Inform. Syst.* **2022**, *35*, 100726. [CrossRef]
15. De Souza, E.; Ardakanian, O.; Nikolaidis, I. A Co-simulation Platform for Evaluating Cyber Security and Control Applications in the Smart Grid. In Proceedings of the ICC 2020—2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–7. [CrossRef]
16. Georg, H.; Müller, S.C.; Rehtanz, C.; Wietfeld, C. Analyzing Cyber-Physical Energy Systems: The INSPIRE Cosimulation of Power and ICT Systems Using HLA. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2364–2373. [CrossRef]
17. Bian, D.; Kuzlu, M.; Pipattanasomporn, M.; Rahman, S.; Wu, Y. Real-time co-simulation platform using OPAL-RT and OPNET for analyzing smart grid performance. In Proceedings of the 2015 IEEE Power & Energy Society General Meeting, Denver, CO, USA, 26–30 July 2015; pp. 1–5. [CrossRef]
18. Nejabatkhah, F.; Li, Y.W. Overview of Power Management Strategies of Hybrid AC/DC Microgrid. *IEEE Trans. Power Electron.* **2015**, *30*, 7072–7089. [CrossRef]
19. Nguyen, T.-L.; Wang, Y.; Tran, Q.-T.; Caire, R.; Xu, Y.; Gavriluta, C. A Distributed Hierarchical Control Framework in Islanded Microgrids and Its Agent-Based Design for Cyber–Physical Implementations. *IEEE Trans. Ind. Electron.* **2021**, *68*, 9685–9695. [CrossRef]
20. Gurugubelli, V.; Ghosh, A.; Panda, A.K. Droop controlled voltage source converter with different classical controllers in the voltage control loop. In Proceedings of the IEEE International Conference on Power Electronics, Smart Grid, and Renewable Energy (PESGRE), Trivandrum, India, 2–5 January 2022; pp. 1–6. [CrossRef]
21. Tayab, U.B.; Roslan, M.A.B.; Hwan, L.J.; Kashif, M. A review of droop control techniques for microgrid. *Renew. Sustain. Energy Rev.* **2017**, *76*, 717–727. [CrossRef]
22. Sahoo, A.K.; Mahmud, K.; Crittenden, M.; Ravishankar, J.; Padmanaban, S.; Blaabjerg, F. Communication-Less Primary and Secondary Control in Inverter-Interfaced AC Microgrid: An Overview. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 5164–5182. [CrossRef]
23. Han, H.; Hou, X.; Yang, J.; Wu, J.; Su, M.; Guerrero, J.M. Review of Power Sharing Control Strategies for Islanding Operation of AC Microgrids. *IEEE Trans. Smart Grid* **2016**, *7*, 200–215. [CrossRef]
24. De Nadai Nascimento, B.; Zambroni de Souza, A.C.; Marujo, D.; Sarmiento, J.E.; Alvez, C.A.; Portelinha, F.M., Jr.; de Carvalho Costa, J.G. Centralised secondary control for islanded microgrids. *IET Renew. Power Gener.* **2020**, *14*, 1502–1511. [CrossRef]
25. Bhattarai, B.; Marinovici, L.; Touhiduzzaman, M.; Tuffner, F.K.; Schneider, K.P.; Xie, J.; Fisher, A. Studying impacts of communication system performance on dynamic stability of networked microgrid. *IET Smart Grid* **2020**, *3*, 667–676. [CrossRef]
26. Kyriakou, D.G.; Kanellos, F.D. Optimal frequency support method for urban microgrids of building prosumers. *Sustain. Cities Soc.* **2023**, *98*, 104776. [CrossRef]

27. Heins, T.; Joševski, M.; Gurumurthy, S.K.; Monti, A. Centralized Model Predictive Control for Transient Frequency Control in Islanded Inverter-Based Micrograids. *IEEE Trans. Power Syst.* **2023**, *38*, 2641–2652. [CrossRef]
28. Rey, J.M.; Rosero, C.X.; Velasco, M.; Martí, P.; Miret, J.; Castilla, M. Local Frequency Restoration for Droop-Controlled Parallel Inverters in Islanded Microgrids. *IEEE Trans. Energy Convers.* **2019**, *34*, 1232–1241. [CrossRef]
29. Dashtdar, M.; Flah, A.; Hosseinimoghadam, S.M.S.; Reddy, C.R.; Kotb, H.; AboRas, K.M.; Bortoni, E.C. Improving the Power Quality of Island Microgrid with Voltage and Frequency Control Based on a Hybrid Genetic Algorithm and PSO. *IEEE Access* **2022**, *10*, 105352–105365. [CrossRef]
30. Alzayed, M.; Lemaire, M.; Zarrabian, S.; Chaoui, H.; Massicotte, D. Droop-Controlled Bidirectional Inverter-Based Microgrid Using Cascade-Forward Neural Networks. *IEEE Open J. Circuits Syst.* **2022**, *3*, 298–308. [CrossRef]
31. Guerrero, J.M.; Vasquez, J.C.; Matas, J.; de Vicuna, L.G.; Castilla, M. Hierarchical Control of Droop-Controlled AC and DC Microgrids—A General Approach Toward Standardization. *IEEE Trans. Ind. Electron.* **2011**, *58*, 158–172. [CrossRef]
32. Guo, F.; Wen, C.; Mao, J.; Song, Y.-D. Distributed Secondary Voltage and Frequency Restoration Control of Droop-Controlled Inverter-Based Microgrids. *IEEE Trans. Ind. Electron.* **2015**, *62*, 4355–4364. [CrossRef]
33. Firdaus, A.; Mishra, S. Mitigation of Power and Frequency Instability to Improve Load Sharing Among Distributed Inverters in Microgrid Systems. *IEEE Syst. J.* **2020**, *14*, 1024–1033. [CrossRef]
34. Pogaku, N.; Prodanovic, M.; Green, T.C. Modeling, Analysis and Testing of Autonomous Operation of an Inverter-Based Microgrid. *IEEE Trans. Power Electron.* **2007**, *22*, 613–625. [CrossRef]
35. Ns-3 Tutorial Release ns-3-dev ns-3 Project. 2022. Available online: https://www.nsnam.org/docs/release/3.37/tutorial/ns-3-tutorial.pdf (accessed on 1 May 2023).
36. Tavassoli, B.; Fereidunian, A.; Mehdi, S. Communication system effects on the secondary control performance in microgrids. *IET Renew. Power Gener.* **2020**, *14*, 2047–2057. [CrossRef]
37. Docker Documentation Release 6.1.0. dev0. 2018. Available online: https://docker-sean.readthedocs.io/_/downloads/en/latest/pdf/ (accessed on 5 May 2023).
38. Aghmadi, A.; Hussein, H.; Polara, K.H.; Mohammed, O. A Comprehensive Review of Architecture, Communication, and Cybersecurity in Networked Microgrid Systems. *Inventions* **2023**, *8*, 84. [CrossRef]

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.