



Article

Controller Hardware-in-the-Loop Testbed of a Distributed Consensus Multi-Agent System Control under Deception and Disruption Cyber-Attacks

Ibtissam Kharchouf *  and Osama A. Mohammed * 

Energy Systems Research Laboratory, Department of Electrical and Computer Engineering, Florida International University, Miami, FL 33174, USA

* Correspondence: ikhar002@fiu.edu (I.K.); mohammed@fiu.edu (O.A.M.); Tel.: +1-305-348-3040 (O.A.M.)

Abstract: The impact of communication disturbances on microgrids (MGs) needs robust and scalable Information Communication Technology (ICT) infrastructure for efficient MG control. This work builds on advances in the Internet of Things (IoT) to provide a practical platform for testing the impact of various cyber-attacks on a distributed control scheme for a Multi-Agent System (MAS). This paper presents a Controller Hardware-in-the-Loop (CHIL) testbed to investigate the impact of various cyber-attacks and communication disruptions on MGs. A distributed consensus secondary control scheme for a MAS within an MG cyber-physical system (CPS) is proposed. The proposed cyber-physical testbed integrates a real-time islanded AC microgrid on RT-Lab, secondary controllers implemented on single-board computers, and an attacker agent on another single-board computer. Communication occurs via a UDP/IP network between OPAL-RT and controller agents, as well as between the agents. Through meticulous experimentation, the efficacy of the proposed control strategy using the developed platform is validated. Various attacks were modeled and launched including deception attacks on sensors, actuators, and their combinations, as well as disruption attacks. The ramifications of both deception and disruption cyber-attacks on system performance are analyzed.



Citation: Kharchouf, I.; Mohammed, O.A. Controller Hardware-in-the-Loop Testbed of a Distributed Consensus Multi-Agent System Control under Deception and Disruption Cyber-Attacks. *Energies* **2024**, *17*, 1669. <https://doi.org/10.3390/en17071669>

Academic Editors: Quynh Thi Tu Tran and Saeed Sepasi

Received: 8 February 2024

Revised: 24 March 2024

Accepted: 28 March 2024

Published: 31 March 2024



Copyright: © 2024 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 (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: microgrids; consensus algorithm; distributed secondary control; real-time simulation; deception attack; denial-of-service attack (DoS); cyber-physical system (CPS); multi-agent system (MAS); OPAL-RT; controller hardware-in-the-loop (CHIL)

1. Introduction

In the face of increasing concerns about the environmental impact of fossil fuel-based power plants and the commitment of many countries to achieving net zero carbon emissions by 2050, microgrids have emerged as a practical solution to integrate renewable energy and ensure energy security. The term microgrids refers to a group of distributed generators (DGs), loads, and energy storage systems capable of seamlessly transitioning between islanded and grid-connected modes. The control architecture of microgrids is hierarchically structured, involving primary, secondary, and tertiary control levels [1]. The primary control (PC) often has a droop-based design to stabilize the frequency and voltage and to achieve active/reactive power-sharing using local measurements. The secondary control (SC) is implemented as centralized or distributed [2]. It addresses deviations caused by primary control by restoring frequency and voltage. At the top level, tertiary control (TC) is used to manage the power flow and for optimal dispatch operation. Communication networks become vital as secondary controllers exchange critical information such as voltage, frequency, and active and reactive power among DGs [3]. Some standard communication protocols used in microgrids are DNP3, Modbus, TCP/IP, XML, CAN Bus, IEC 61850 [4], etc. The complex interdependency between cyber and physical systems makes them vulnerable to cyber threats. Therefore, a Controller

Hardware-In-the-Loop (CHIL) testbed is developed in the real-time environment using OPAL-RT to analyze the impact of different cyber-attacks on the AC microgrid [5–7].

Cyber-physical systems simulation techniques can be classified into three types, i.e., co-simulation, semi-physical simulation, and embedded simulation. The embedded simulation technique aims to design the communication modules in the power system simulation software. However, the difficulty of this technique lies in the communication module design. In the semi-physical simulation method, one of the systems is simulated using simulation software while a real hardware object replaces the other system. This technique presents an increased simulation authenticity and high simulation accuracy. However, real physical devices make it expensive. Finally, the co-simulation technique aims to build a joint simulation platform by using power system and communication network simulation software, and to realize information exchange between both systems. It is divided into real-time co-simulation and non-real-time co-simulation. The physical and communication simulators have different time management mechanisms in the non-real-time co-simulation. Therefore, a time synchronization method should be designed to achieve collaborative simulation between the two simulators. Even though a collaborative study of a CPS can be achieved through non-real-time co-simulation with a good time synchronization method, real-time co-simulation is given more attention. Real-time co-simulation means that the simulation software runs in real time and that the system can be divided into various sub-models for parallel computation purposes. Hardware-based real-time power system simulation platforms are required for real-time co-simulation, such as OPAL-RT and RTDS [8]. CHIL is a specific co-simulation type involving a hardware controller interacting with a simulation [9]. In our study, we built a CHIL testbed using OPAL-RT and implemented multiple secondary controllers using single-board computers. The developed platform is suitable for studying the impact of communication network disturbances, such as time delays, packet loss, limited bandwidth, and cyber-attacks on cyber-physical systems.

Cyber threats present a serious risk to CPS-based microgrids [10]. For instance, a breach in the communication link may result in miscommunication among DERs, deteriorating the power-sharing objectives and MG stability. Compared to conventional cyber security; attacks on CPSs manipulate data transmission and the physical entities within the system. These attacks can be categorized into replay attacks, DoS, and deception attacks. Replay attacks disrupt authentication by intercepting and retransmitting valid messages [11,12], while DoS attackers jam the communication links among agents to prevent data from reaching their destination. DoS attacks are widely discussed in the literature. Deception attacks compromise sensors' and actuators' data integrity through injection or modification. These attacks do not necessarily require deep knowledge of system dynamics and may result in catastrophic consequences [13]. Recent cyber-attacks on industrial infrastructure, such as the Stuxnet worm's attack on Iran's nuclear power plant and coordinated attacks on power grids in Ukraine and Venezuela, underline the urgent need for robust defensive strategies in CPS security. For instance, the cyber-attack on Ukraine's power grid in 2015 began with an initial compromise as early as eight months before. Initially, the attacker managed to compromise the information technology (IT) network through spear fishing emails. Once inside the network, variants of BlackEnergy 3 malware were remotely controlled to penetrate the industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) systems responsible for managing the power grid. With control over these systems, the hacker remotely took control and executed commands to manipulate the operation of electrical substations and power distribution equipment. At the same time, the operator was prevented from regaining control of the network using a modified KillDisk firmware attack and customers were prevented from reporting the outages by launching a distributed denial of service (DDoS) attack on call centers. The prolonged impact of the attack underscored the vulnerability of critical infrastructure to cyber-physical threats and highlighted the need for robust defense mechanisms to mitigate such risks effectively [14]. Similarly, Venezuela experienced blackouts caused by cyber-attacks.

Hence, the motivation for this paper arises from the critical need to analyze the impact of different cyber-attacks on microgrids and further develop robust defensive strategies to protect microgrids' cyber-physical systems.

The contributions of this research paper can be summarized as follows:

- Development of a novel cyber-physical platform integrating a real-time islanded AC microgrid model running on OPAL-RT, distributed consensus secondary control on Raspberry Pis, and an attacker agent for disruption and deception attacks;
- Development of a distributed consensus secondary controller for frequency and voltage restoration and accurate power sharing;
- Implementation of a communication network using graph theory and the Laplacian matrix to enable information exchange among agents and assess network vulnerabilities;
- Modeling and implementation of disruption and deception attacks on the microgrid communication network using an attacker agent deployed on a Raspberry Pi;
- Assessment of multi-agent system operation under various scenarios of disruption and deception cyber-attacks.

Figure 1 shows a multilayered MAS framework, where each agent receives and shares information with neighboring agents through a communication network. The hardware setup includes an OPAL-RT real-time simulator and independent hardware agents running on Raspberry Pis. The communication between the OPAL-RT and the agents, as well as the communication between the agents, is all through the UDP/IP protocol.

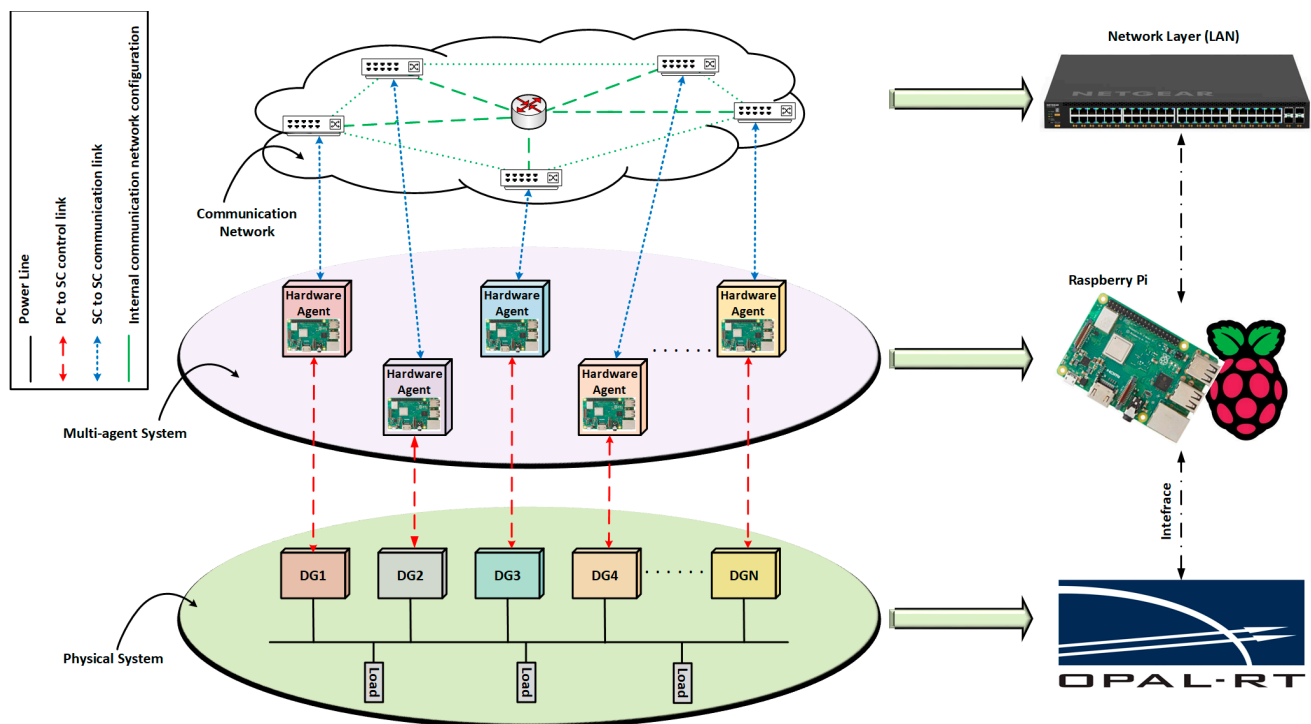


Figure 1. Multilayered framework of a multi-agent system.

The rest of the paper is organized as follows. Section 2 introduces preliminaries on the primary control, secondary control, and communication network. The cyber-attacks model is explained in Section 3. The testbed setup is presented in Section 4. Section 5 presents experimental results and discussion to validate the testbed setup and show the impact of deception and disruption attacks on the proposed consensus control strategy. Section 6 concludes the research paper.

2. Preliminaries

Voltage Source Inverters (VSIs) are usually used to connect DGs to the network. Figure 2 depicts the block diagram of a VSI, its components, the primary and secondary control loops, and the communication network. The primary and secondary control loops are presented in the following.

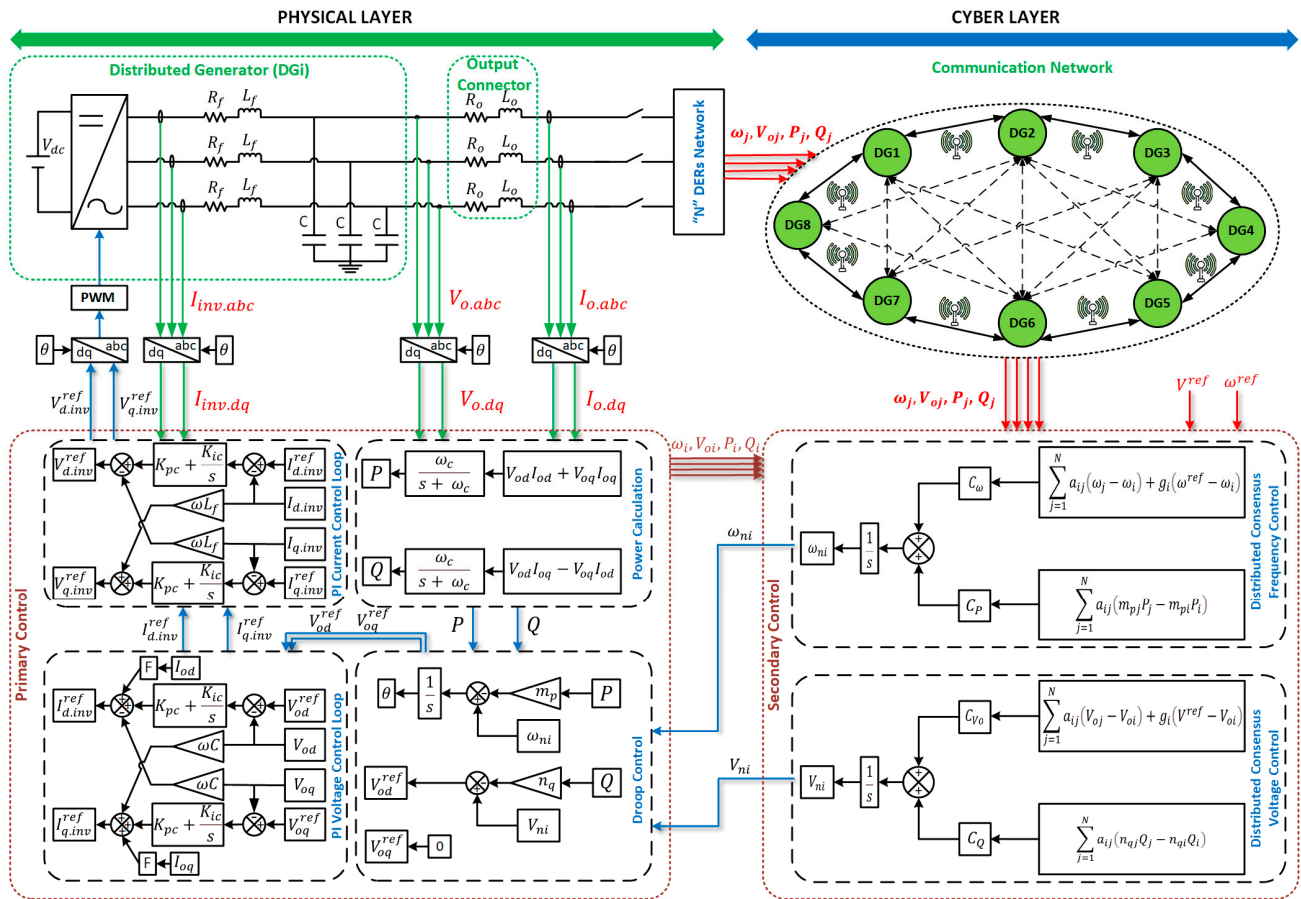


Figure 2. Diagram of cyber-physical AC microgrid controlled by a distributed consensus secondary control scheme.

2.1. Primary Control

The primary control aims to stabilize the microgrid and ensure power sharing. The proportional control loops are employed locally at each inverter to enable plug-and-play functionality and enhance redundancy. While this decentralized control strategy enables power sharing, it also impacts voltage and frequency regulation.

It consists of three control loops: power control loop, voltage control loop, and current control loop.

2.1.1. Power Control Loop

It is widely employed to adjust the frequency and voltage magnitude in the case of inverter-based DGs in islanded MGs. This adjustment is based on droop characteristics associated with both real and reactive power. The concept of droop control is derived from emulating the behavior of synchronous generators in conventional power systems. Rotating machines respond to an increase in demand by decreasing the system frequency, governed by their droop characteristics. Similarly, inverters implement this principle by reducing the reference frequency as the load increases. The reactive power sharing is managed through the implementation of a droop characteristic in the voltage magnitude [15–17]. The block diagram of the power control loop is shown in Figure 2.

The active (P) and reactive (Q) power can be calculated from the measured output voltage and current and then passed through low-pass filters as given in Equation (1), where ω_c is the cut-off frequency and s is the Laplace variable.

$$\begin{cases} P = \frac{\omega_c}{s+\omega_c} (V_{od}I_{od} + V_{oq}I_{oq}) \\ Q = \frac{\omega_c}{s+\omega_c} (V_{od}I_{oq} - V_{oq}I_{od}) \end{cases} \quad (1)$$

The active and reactive power sharing between VSIs is achieved by using an artificial droop, introduced, respectively, in the frequency and the voltage magnitude as given in Equation (2), where ω_n and V_n are the nominal frequency and voltage amplitude, respectively. ω and V_o are the reference frequency and voltage, respectively [18,19].

$$\begin{cases} \omega = \omega_n - m_p P \\ V_o = V_n - n_q Q \end{cases} \quad (2)$$

The droop coefficients (m_p and n_q) are calculated in Equation (3) based on the output power rating. The power control loop provides the voltage reference for the voltage control loop (V_o^{ref}). Note that the output voltage reference is chosen to be aligned to the direct axis of the inverter reference frame (d-axis), and the quadrature axis (q-axis) reference is set to zero.

$$m_p = \frac{\Delta\omega}{P_{max}}, \quad n_q = \frac{\Delta V_o}{Q_{max}} \quad (3)$$

2.1.2. Voltage and Current Control Loops

Voltage and current control loops provide the output current and input voltage references (I_{inv}^{ref} and V_{inv}^{ref}). The block diagram of the internal voltage and current control loops is shown in Figure 2.

2.2. Preliminaries and Communication Network

This section briefly describes graph theory properties. The microgrid is essentially envisioned as a MAS, where the DGs take on the roles of communicating agents or nodes, while the communication links are seen as edges forming a sparse communication network. Each DG can exchange information with its neighboring DGs through this sparse communication network. In our case, the studied system is an islanded microgrid consisting of N DGs, where the communication among them is visually represented by a directed (one-way) or undirected (two-way) communication graph [20,21]. This graph is mathematically represented as $\mathcal{G} = (\mathcal{V}, E, A)$ where $\mathcal{V} = \{v_1, v_2, \dots, v_N\}$ is a set of N nodes, $E \subseteq \mathcal{V} \times \mathcal{V}$ is a set of edges, $A \triangleq [a_{ij}] \in \mathbb{R}^{N \times N}$ is the Adjacency matrix, and it is defined as follows:

$$A \triangleq [a_{ij}] \quad \text{where} \quad a_{ij} \triangleq \begin{cases} 0 & \forall i = j \\ > 0 & \forall i \neq j \end{cases} \quad (4)$$

The edge (v_j, v_i) means that node j transmits information to node i . The weight of edge $a_{ij} > 0$ if $(v_j, v_i) \in E$, otherwise $a_{ij} = 0$. $N_i = \{j | (v_j, v_i) \in E\}$ is the set of neighbors of the i th node where j is called the neighbor of i if $(v_j, v_i) \in E$. Every node in a graph has an in-degree matrix $D \triangleq \text{diag}\{d_i\}$, defined as follows:

$$D \triangleq \text{diag}\{d_i\} \quad \text{where} \quad d_i \triangleq \sum_{j \in N_i} a_{ij} \quad \forall i = j \quad (5)$$

where the Laplacian matrix $L \triangleq D - A$ is defined as follows:

$$L \triangleq [l_{ij}] \quad \text{where} \quad l_{ij} \triangleq \begin{cases} d_i = \sum_{j \in N_i} a_{ij} & \forall i = j \\ -a_{ij} & \forall i \neq j \end{cases} \quad (6)$$

A weighted graph is called balanced if and only if all the included nodes are balanced such that $\sum_{j=1}^{\mathcal{N}_i} a_{ij} = \sum_{j=1}^{\mathcal{N}_i} a_{ji}$. A graph \mathcal{G} is said to be strongly connected (SC) if there is a connection path of edges between each two separate nodes with accurate direction. The graph is said to have a spanning tree if there is a directed path from a root node i_r to every other node in the graph [22].

The adjacency, in-degree and, Laplacian matrices, as well as other parameters, can effectively improve the control algorithm [23]. Equation (7) is always used in control algorithms based on graph theory where any scalar x_i satisfies the consensus principle in continuous time.

$$\dot{x}_i = u_i = \sum_{j \in \mathcal{N}_i} a_{ij} (x_j - x_i) \quad (7)$$

The microgrid model is shown in Figure 3a, its equivalent weighted graph is shown in Figure 3b, and its corresponding adjacency matrix is shown in Figure 3c.

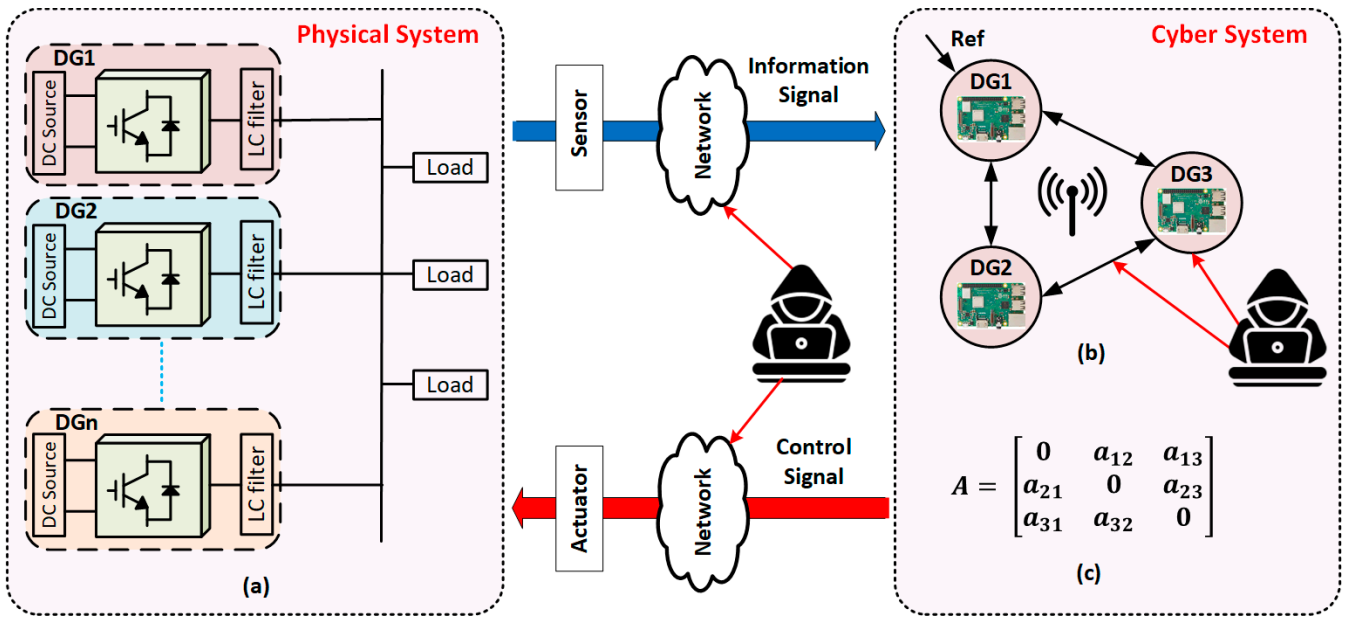


Figure 3. (a) MG model, (b) Weighted graph, (c) Adjacency matrix.

2.3. Distributed Secondary Control

The secondary control objectives include frequency and voltage restoration and contributing to the power sharing. Each DG communicates with its neighboring DGs to exchange information. Differentiating both terms in Equation (2) gives:

$$\begin{cases} \dot{\omega}_i = \dot{\omega}_{ni} - m_{pi} \dot{P}_i \equiv u_{\omega i} \\ \dot{V}_{oi} = \dot{V}_{ni} - n_{qi} \dot{Q}_i \equiv u_{Voi} \end{cases} \quad (8)$$

The SC sets the nominal set-points ω_{ni} and V_{ni} as follows:

$$\omega_{ni} = \int (\dot{\omega}_i + m_{pi} \dot{P}_i) dt = \int (u_{\omega i} + u_{Pi}) dt \quad (9)$$

$$V_{ni} = \int (\dot{V}_{oi} + n_{qi} \dot{Q}_i) dt = \int (u_{Voi} + u_{Qi}) dt \quad (10)$$

The accurate power sharing problem can be expressed as follows: $u_{Pi} = m_{pi} \dot{P}_i$ and $u_{Qi} = n_{qi} \dot{Q}_i$.

ω_{ni} has $u_{\omega i}$ and u_{Pi} as secondary control inputs and V_{ni} has u_{Voi} and u_{Qi} as secondary control inputs, where $u_{\omega i}$ and u_{Voi} are the auxiliary controls.

The proposed distributed SC control objectives are as follows:

1. Frequency and voltage restoration:

$$\lim_{t \rightarrow \infty} |\omega_i(t) - \omega_{ref}| = 0 \quad \forall i = 1, 2, \dots, N. \quad (11)$$

$$\lim_{t \rightarrow \infty} |V_{oi}(t) - V_{ref}| = 0 \quad \forall i = 1, 2, \dots, N. \quad (12)$$

2. Accurate Power Sharing:

$$\lim_{t \rightarrow \infty} |m_{pi}P_i(t) - m_{pj}P_j(t)| = 0 \quad \forall i \neq j. \quad (13)$$

$$\lim_{t \rightarrow \infty} |n_{qi}Q_i(t) - n_{qj}Q_j(t)| = 0 \quad \forall i \neq j. \quad (14)$$

Achieving these control objectives involves adjusting the control inputs for each agent: $u_{\omega i}$, $u_{V_{oi}}$, u_{P_i} , and u_{Q_i} .

2.3.1. Frequency and Voltage Control

For a microgrid composed of N DGs, the secondary voltage and frequency control for a first order and linear MAS are transformed into the tracking synchronization problem.

$$\left\{ \begin{array}{l} \dot{V}_{o1} = u_{V_{o1}} \\ \dot{V}_{o2} = u_{V_{o2}} \\ \vdots \\ \dot{V}_{oN} = u_{V_{oN}} \end{array} \right. \quad (15)$$

$$\left\{ \begin{array}{l} \dot{\omega}_1 = u_{\omega 1} \\ \dot{\omega}_2 = u_{\omega 2} \\ \vdots \\ \dot{\omega}_N = u_{\omega N} \end{array} \right. \quad (16)$$

As mentioned earlier, DGs communication is achieved through the designed communication graph shown in Figure 3b. The control signals $u_{\omega i}$ and $u_{V_{oi}}$ are calculated using the DGs' own information and the neighbors' information as follows:

$$u_{\omega i} = C_{\omega} \left[\sum_{j=1}^N a_{ij} (\omega_j - \omega_i) + g_i (\omega^{ref} - \omega_i) \right] \quad (17)$$

$$u_{V_{oi}} = C_{V_o} \left[\sum_{j=1}^N a_{ij} (V_{oj} - V_{oi}) + g_i (V^{ref} - V_{oi}) \right] \quad (18)$$

C_{ω} and C_{V_o} represent the control gains; both are greater than zero. The pinning gain g_i is set to 1 if a DG can directly receive set points, otherwise g_i is set to 0.

In a global form, Equations (17) and (18) can be written as:

$$u_{\omega} = C_{\omega} \left[-L\omega + G(\omega^{ref} \mathbf{1}_{n \times 1} - \omega) \right] \quad (19)$$

$$u_{V_o} = C_{V_o} \left[-LV_o + G(V^{ref} \mathbf{1}_{n \times 1} - V_o) \right] \quad (20)$$

where $u_{V_o} = [u_{V_{o1}}, \dots, u_{V_{oN}}]^T$, $u_{\omega} = [u_{\omega 1}, \dots, u_{\omega N}]^T$, $V_o = [V_{o1}, \dots, V_{oN}]^T$, $\omega = [\omega_1, \dots, \omega_N]^T$, $C_{\omega} = \text{diag}(C_{\omega 1}, \dots, C_{\omega N})$, $C_{V_o} = \text{diag}(C_{V_{o1}}, \dots, C_{V_{oN}})$, and $\mathbf{1}_N$ is an all-ones vector of length N.

2.3.2. Active and Reactive Power Sharing

According to the power sharing objective in Equations (13) and (14), the power ratio among DGs will be equalized in steady state.

$$m_{pi}P_i(t) = m_{pj}P_j(t) \quad (21)$$

$$n_{qi}Q_i(t) = n_{qj}Q_j(t) \quad (22)$$

Substituting the droop coefficient equations in Equation (3), the real and reactive power among DGs is shared as in Equations (23) and (24).

$$\frac{P_i}{P_j} = \frac{m_{pj}}{m_{pi}} = \frac{\frac{\Delta\omega}{P_{jmax}}}{\frac{\Delta\omega}{P_{imax}}} = \frac{P_{imax}}{P_{jmax}} \quad (23)$$

$$\frac{Q_i}{Q_j} = \frac{n_{qj}}{n_{qi}} = \frac{\frac{\Delta V_o}{Q_{jmax}}}{\frac{\Delta V_o}{Q_{imax}}} = \frac{Q_{imax}}{Q_{jmax}} \quad (24)$$

The auxiliary controls u_{pi} and u_{qi} are chosen based on the DGs' own information and their neighbors' information as follows:

$$u_{pi} = C_P \left[\sum_{j=1}^N a_{ij} (m_{pj}P_j - m_{pi}P_i) \right] \quad (25)$$

$$u_{qi} = C_Q \left[\sum_{j=1}^N a_{ij} (n_{qj}Q_j - n_{qi}Q_i) \right] \quad (26)$$

In a global form, Equations (25) and (26) can be written as:

$$u_P = -C_P L(m_p P) \quad (27)$$

$$u_Q = -C_Q L(n_q Q) \quad (28)$$

where $u_P = [u_{p1}, \dots, u_{pN}]^T$, $u_Q = [u_{q1}, \dots, u_{qN}]^T$, $m_p P = [m_{p1}P_1, \dots, m_{pN}P_N]^T$, $n_q Q = [n_{q1}Q_1, \dots, n_{qN}Q_N]^T$, $C_P = \text{diag}(C_{P1}, \dots, C_{PN})$, and $C_Q = \text{diag}(C_{Q1}, \dots, C_{QN})$. Note that L and a_{ij} , the Laplacian matrix and the elements of the adjacent matrix A , are defined in the Preliminaries section.

3. Cyber-Attacks Model

3.1. Deception and Disruption Cyber-Attacks

Deception and disruption attacks have been widely discussed in the networked control literature. Disruption attacks, known as DoS or jamming attacks, primarily target data availability, whereas deception attacks target the integrity of packets [24,25]. In deception attacks, intruders may manipulate sensor measurements and control commands within networked agents by accessing physical agents, sensors, controllers, actuators, and/or communication channels. This latter proves challenging to detect and handle especially if the attack sequences are strategically launched. Deception attacks can be classified based on attack types and attack points [26].

3.1.1. Attack Types

- Linear additive deception attack:

- Characteristics: The attacker injects false data $\mathfrak{A}_{ij}(t)$ into the normal data $\mathfrak{d}_{ij}(t)$ sent by agent i ;
- Effect: The corrupted data $\tilde{\mathfrak{d}}_{ij}(t)$ received by agent j are the addition of the original data and the injected false data.

$$\tilde{\mathfrak{d}}_{ij}(t) = \mathfrak{d}_{ij}(t) + \mathfrak{A}_{ij}(t) \quad (29)$$

- Multiplicative deception attack:
 - Characteristics: This attack involves scaling up or down the original data $\mathfrak{d}_{ij}(t)$ by a scaling factor $\mathfrak{s}_{ij}(t)$;
 - Effect: The received data $\tilde{\mathfrak{d}}_{ij}(t)$ are a scaled version of the original data, potentially altered in magnitude.

$$\tilde{\mathfrak{d}}_{ij}(t) = \mathfrak{d}_{ij}(t)\mathfrak{s}_{ij}(t) \quad (30)$$

- Combined additive and multiplicative deception attack:
 - Characteristics: This type of attack combines both additive and multiplicative deception. It scales the original data and adds injected false data;
 - Effect: The received data $\tilde{\mathfrak{d}}_{ij}(t)$ are a combination of the scaled original data and the injected false data.

$$\tilde{\mathfrak{d}}_{ij}(t) = \mathfrak{d}_{ij}(t)\mathfrak{s}_{ij}(t) + \mathfrak{a}_{ij}(t) \quad (31)$$

- Replacement attack:
 - Characteristics: In a replacement attack, the attacker completely replaces the normal data $\mathfrak{d}_{ij}(t)$ with an arbitrary signal $\mathfrak{r}_{ij}(t)$;
 - Effect: The received data $\tilde{\mathfrak{d}}_{ij}(t)$ are entirely replaced by the arbitrary signal, disregarding the original data.

$$\tilde{\mathfrak{d}}_{ij}(t) = \mathfrak{r}_{ij}(t) \quad (32)$$

- Impulsive false data attack:
 - Characteristics: This attack involves injecting impulsive false data using Dirac impulses $\delta(\cdot)$ at designated time instances $\{t_k\}_{k=1}^{\infty}$, with destabilizing impulse parameters \mathfrak{T}_k ;
 - Effect: The received data $\tilde{\mathfrak{d}}_{ij}(t)$ include the normal data $\mathfrak{d}_{ij}(t)$ along with impulsive false data at designated time instances.

$$\tilde{\mathfrak{d}}_{ij}(t) = \mathfrak{d}_{ij}(t) + \sum_{k=1}^{\infty} \mathfrak{T}_k \mathfrak{d}_{ij}(t) \delta(t - t_k) \quad (33)$$

3.1.2. Attack Points

Deception attacks can be classified based on the attack points. Intruders may launch attacks on sensors, actuators, or both. Equations (34) and (35) model attacks on actuators and sensors, respectively [27].

$$\tilde{\mathfrak{x}}_i(t) = \mathfrak{x}_i(t) + \alpha_i(t)\mathfrak{x}_i^a(t) \quad (34)$$

$$\tilde{\mathfrak{u}}_i(t) = \mathfrak{u}_i(t) + \beta_i(t)\mathfrak{u}_i^a(t) \quad (35)$$

where, $\mathfrak{x}_i^a(t)$ and $\mathfrak{u}_i^a(t)$ denote the attack signals injected into the sensor and the actuator of agent i , respectively. $\tilde{\mathfrak{x}}_i(t)$ and $\tilde{\mathfrak{u}}_i(t)$ are the corrupted state and control protocol of agent i . $\alpha_i(t) = 1$ when agent i is under sensor attack, otherwise $\alpha_i(t) = 0$. Similarly, $\beta_i(t) = 1$ when agent i is under actuator attack, otherwise $\beta_i(t) = 0$.

3.2. Attacks Model

3.2.1. Disruption Attack Model

Various strategies can be employed to conduct a DoS attack such as data packet loss, network flooding, zero input, etc. Let us consider the communication channel between DG_i and DG_j during $[t_1, t_2] \subset [0, \infty]$. The states communicated from the OPAL-RT simulation to the agents as well as between the agents are $x_i \in [\omega_i, V_{oi}, m_{pi}P_i, n_{qi}Q_i]$ and from the

agents to the OPAL-RT simulation are $y_i \in [u_{\omega i}, u_{V_{oi}}, u_{P_i}, u_{Q_i}]$. Let m_μ be the number of DoS attacks that might occur during $[t_1, t_2] \subset [0, \infty]$ and $I_k = [t_a, t_a + \tau_a]$ is the k th interval in which a DoS attack take place, where t_a , $t_a + \tau_a$, and τ_a are, respectively, the start, end, and length of DoS attack [7]. The total DoS time intervals of DoS between two DGs can be given as:

$$\Gamma_{DoS}^{(i,j)} = (t_1, t_2) \cap \left(\bigcup_{a=1}^{m_\mu} I_k^{(i,j)} \right) \quad (36)$$

In order to achieve stealthiness, which is a property under which attacks are not detected, intruders may impose some additional constraints, for instance on τ_a .

3.2.2. Deception Attack Model

Let δ_i^S denotes the potential attacks applied by the adversary on the i th agent sensors. The consensus control in Equations (17) and (18) in the presence of such an attack can be written as follows:

$$\tilde{u}_{\omega i} = C_\omega \left[\sum_{j=1}^N a_{ij} \left((\omega_j + \delta_{\omega i}^S) - \omega_i \right) + g_i \left(\omega^{ref} - \omega_i \right) \right] \quad (37)$$

$$\tilde{u}_{V_{oi}} = C_{V_o} \left[\sum_{j=1}^N a_{ij} \left((V_{oj} + \delta_{V_i}^S) - V_{oi} \right) + g_i \left(V^{ref} - V_{oi} \right) \right] \quad (38)$$

Similarly let δ_i^a denote the potential attacks applied by the adversary on the i th agent actuators. The consensus control in Equations (17) and (18) in the presence of such attack can be written as follows:

$$\tilde{u}_{\omega i} = C_\omega \left[\sum_{j=1}^N a_{ij} (\omega_j - \omega_i) + g_i \left(\omega^{ref} - \omega_i \right) \right] + \delta_{\omega i}^a \quad (39)$$

$$\tilde{u}_{V_{oi}} = C_{V_o} \left[\sum_{j=1}^N a_{ij} (V_{oj} - V_{oi}) + g_i \left(V^{ref} - V_{oi} \right) \right] + \delta_{V_i}^a \quad (40)$$

The attack signals δ_ω^a and δ_V^a can be designed to cause the microgrid instability while remaining stealthy to adversary-detection systems.

4. Testbed Setup

This section introduces an evaluation framework for the implemented agents featuring the proposed distributed secondary control. It outlines the components of the examined three-bus islanded Microgrid (MG), providing insights into various aspects such as real-time simulation, Multi-Agent System (MAS) control platform, communication network design, and protocols.

As depicted in Figure 4, the Controller Hardware-in-the-Loop (CHIL) experimental testbed comprises two main interconnected parts: (i) the proposed physical system, encompassing AC microgrid elements and local controllers, implemented in the OPAL-RT real-time simulator; (ii) the distributed consensus secondary controller, where hardware agents operate independently on Raspberry Pi devices. Initially, real-time measurements are transmitted from the OPAL-RT simulation to the corresponding external control hardware (Raspberry Pi agents) through the UDP/IP protocol and transmitted to neighboring agents via UDP/IP.

4.1. Real-Time Simulation

The simulated AC microgrid is modeled using MATLAB/Simulink and implemented in OPAL-RT. The developed model for this experiment contains the power system model along with all primary controllers and is implemented in RT-Lab version 2023.1. The primary controllers consist of inner and outer loops for current and voltage control. During each control iteration, the local data packets $[\omega_i, V_{oi}, m_{pi}P_i, n_{qi}Q_i]$ from the primary controllers are transmitted to the corresponding Raspberry Pis via UDP. The control input packets $[u_{\omega i}, u_{V_{oi}}, u_{P_i}, u_{Q_i}]$ from the secondary controllers are sent back to OPAL-RT via UDP to calculate ω_{ni} and V_{ni} setpoints. The exchange of data between external secondary controllers, the real-time simulator, and neighboring agents occurs through the LAN net-

work. This interconnected system enables the essential communication and coordination for the functioning of the AC microgrid model.

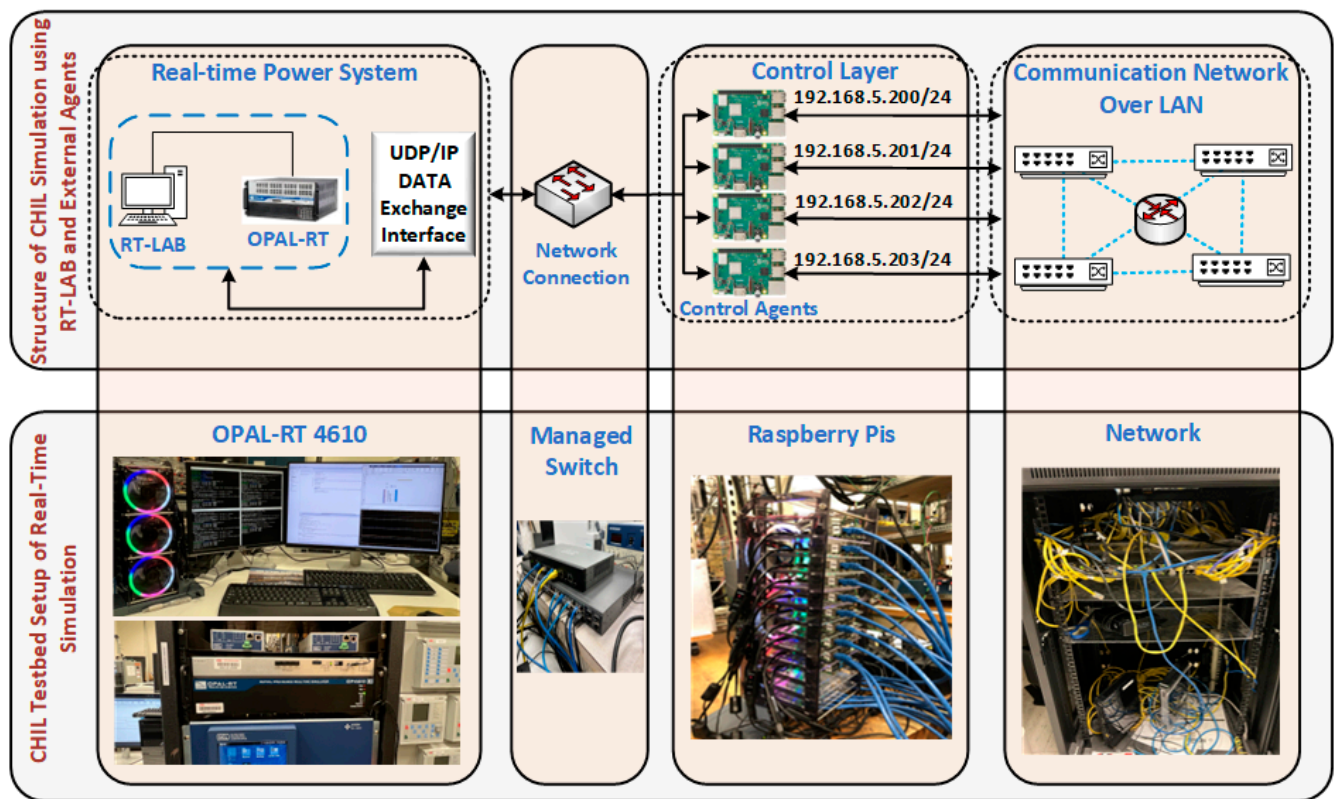


Figure 4. CHIL testbed setup.

4.2. Cyber Layer-Based Raspberry Pi Agents

The agents designed with the proposed distributed consensus secondary control can update the power network state, perform calculations, and provide control decisions. Each DG is represented by an agent responsible for managing the distributed secondary control algorithm based on predefined control objectives. The secondary agent collects voltage, frequency, active, and reactive power data from local measurements and sends control signals to the primary controller (PC). The communication topology among the Raspberry Pi agents is depicted in Figure 2.

For this implementation, the Raspberry Pi 3 Model B+ is utilized. The control action is programmed within each agent (Rpi) using a Python script, with all agents assigned static IP addresses. Communication ports are established when running the Python script. Each Raspberry Pi opens a communication channel for each device to facilitate data exchange with neighboring agents and establishes a client socket with OPAL-RT. Once the connection is established, the client sends commands to the runtime. The flow of the consensus algorithm implemented in every agent is shown in Figure 5.

4.3. Attack Agent

The attack agents were programmed using Python scripts and implemented in a separate agent. The objective of DoS depends on the targeted agent's IP address and port. An agent can be flooded with many packets to consume its resources and, therefore, make it out of service. Also, the communication links between DGs or between a DG and the real-time simulator can be attacked, which results in modifying the communication topology.

The result of deception and disruption attacks and their impact on the physical system are demonstrated using the CHIL testbed setup. The network traffic during a sequence of

DoS attacks with varying packet rates and attack lengths targeting one of the DGs can be shown in Figure 6.

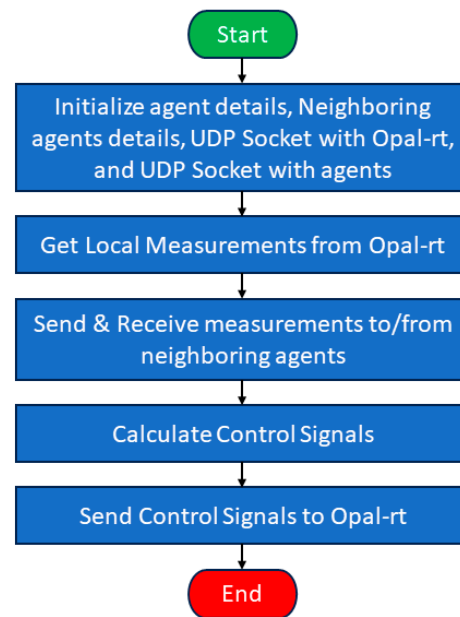


Figure 5. The flow of the consensus algorithm.

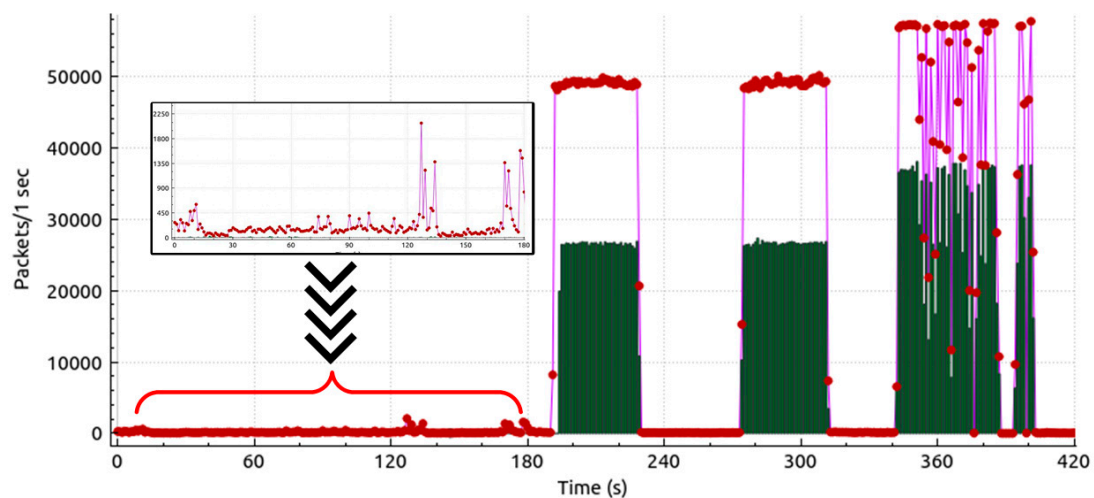


Figure 6. Network traffic during a sequence of DoS attacks (Purple line and red dots: All Packets, Green Impulse: UDP Packets).

5. Results and Discussion

Extensive real-time digital simulations on OPAL-RT are performed to evaluate the effect of various cyber-attacks on the proposed distributed consensus secondary control of islanded AC MG. Using MATLAB/Simulink, an AC microgrid, structured by three parallel inverters with power ratings of 500 KW, 300 KW, and 200 KW connected to the PCC bus, is modeled. The parameters of distributed secondary controllers are all set to $C_\omega = 0.2$, $C_{VO} = 0.1$, $C_P = 4$, and $C_Q = 100$. The droop coefficients are all set to $m_p = 0.01$ and $n_q = 0.04$.

In this section there are three study cases conducted, including:

- Performance Under Normal Operation;
- Performance Under Linear Additive Deception Attacks on Sensor, Actuator, and Combined;
- Performance Under Disruption Attack.

5.1. Performance under Normal Operation

Under normal operation, the performance of the proposed distributed consensus secondary control strategy in case of load variations is presented in Figure 7. At $t = 20$ s, droop activation initiated proportional power sharing among the three DGs, maintaining the frequency and voltage around 60.15 Hz and 598 V, respectively. Following a load increase at $t = 40$ s, the DGs adjusted their power outputs, resulting in a frequency and voltage drop to 59.98 Hz and 694 V, respectively. The activation of the distributed consensus secondary controller at $t = 60$ s restored frequency and voltage to reference values (60 Hz and 600 V) without disrupting proportional power sharing, indicating stable microgrid operation. Further load variations at $t = 80$ s, $t = 100$ s, and $t = 120$ s prompted additional power output adjustments by the DGs, ensuring continued stability with restored frequency and voltage levels.

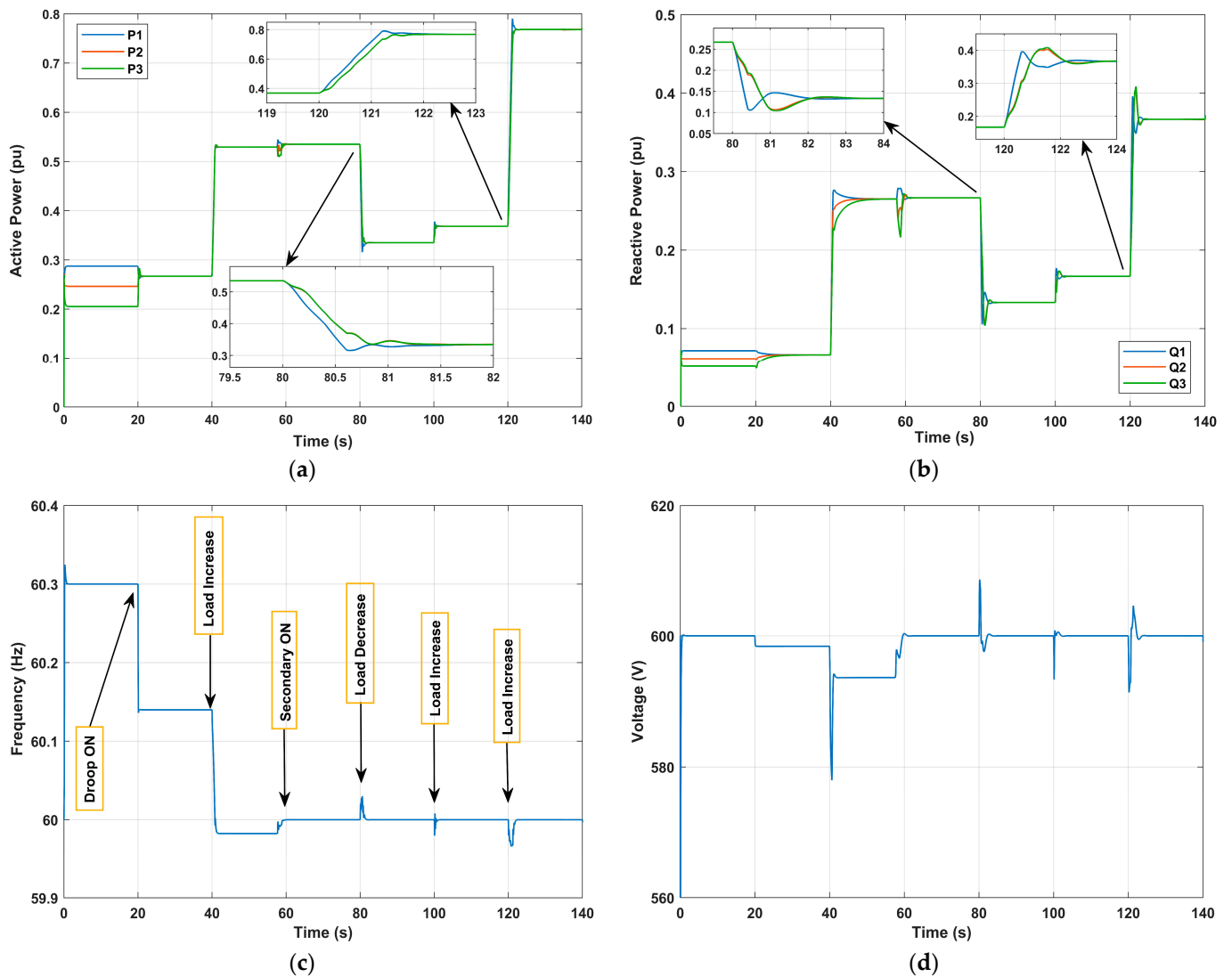


Figure 7. Performance of the proposed distributed consensus secondary control under normal operation: (a) Active power, (b) Reactive power, (c) Frequency, (d) Voltage.

5.2. Performance under Deception Attacks

This section evaluates the effect of linear additive deception attacks on sensors, actuators, and both.

5.2.1. Deception Attack on Actuators' Frequency

In this study case, $\delta_1^{a,\omega}$ denotes the actuator attack injections to the frequency control loop of DG #1. The attack signal is $\delta_1^{a,\omega} = \delta_1^{a,\omega1}$ for $59.8 < t(s) < 109.8$ and $\delta_1^{a,\omega} = \delta_1^{a,\omega2}$ for $109.8 < t(s) < 160$ where $\delta_1^{a,\omega1} > \delta_1^{a,\omega2}$.

The simulation scenario for this case is as follows:

- At $t = 20$ s, the Droop control is activated;
- At $t = 40$ s, the distributed consensus secondary control is activated;
- At $t = 59.8$ s, the first actuator attack is launched;
- At $t = 90$ s, the load is increased;
- At $t = 109.8$ s, the second actuator attack is launched;
- At $t = 140$ s, the load is decreased.

The results are shown in Figure 8. At $t = 40$ s, when there is no cyber-attack, the frequency and voltage of the islanded microgrid restore to their reference values while the active and reactive power of DGs are accurately sharing. The cyber-attack is initiated at approximately $t = 59.8$ s, resulting in a notable transient impact on the system. However, both voltage and frequency stabilize, maintaining alignment with the consensus power sharing objectives. Remarkably, despite the ongoing attack, the system recovered. By $t = 90$ s, even with an increase in load, the microgrid operates as if it were under normal conditions. At $t = 109.8$ s, the attack signal is slightly reduced. As a result, the system shows behavior similar to that observed during the initial attack. The performed real-time tests demonstrated that the control objectives were achieved successfully with bounded attack signals. However, with unbounded attack signals, the system became unstable. This underscores the vital role of cybersecurity measures in keeping the microgrid stable and dependable.

5.2.2. Deception Attack on Actuators' Voltage

In this study case, $\delta_1^{a,V}$ denotes the actuator attack injections to the voltage control loop of DG #1. The attack signal is $\delta_1^{a,V} = \delta_1^{a,V1}$ for $59.8 < t(s) < 109.8$ and $\delta_1^{a,V} = \delta_1^{a,V2}$ for $109.8 < t(s) < 160$ where $\delta_1^{a,V1} > \delta_1^{a,V2}$. The simulation scenario is as follows:

- At $t = 20$ s, the droop control is activated;
- At $t = 40$ s, the distributed consensus secondary control is activated;
- At $t = 59.2$ s, the first actuator attack is launched;
- At $t = 90$ s, the load is increased;
- At $t = 109.2$ s, the second actuator attack is launched;
- At $t = 140$ s, the load is decreased.

In this experiment, we focused on the vulnerability of the actuator voltage control loop to cyber-attacks within the islanded AC microgrid system. The setup mirrored the first experiment with adjustments made to the voltage control loop instead of the frequency control loop. As depicted in Figure 9, the results showed a similar pattern to the previous experiment.

5.2.3. Deception Attack on Sensors' Frequency

In this study case, $\delta_1^{S,\omega}$ denotes the sensor attack injections to the frequency measurements of DG #1. The attack signal is $\delta_1^{S,\omega} = \delta_1^{S,\omega1}$ between $60 < t(s) < 80$ and $\delta_1^{S,\omega} = \delta_1^{S,\omega2}$ between $120 < t(s) < 140$ where $\delta_1^{S,\omega1} > \delta_1^{S,\omega2}$. The simulation scenario for this case is as follows:

- At $t = 20$ s, the droop control is activated;
- At $t = 40$ s, the distributed consensus secondary control is activated;
- At $t = 60$ s, the first frequency sensor attack is launched;
- At $t = 80$ s, the first attack is removed;
- At $t = 100$ s, the total load is increased;
- At $t = 120$ s, the second frequency sensor attack is launched;

- At $t = 140$ s, the second attack is removed;
- At $t = 160$ s, the load is decreased.

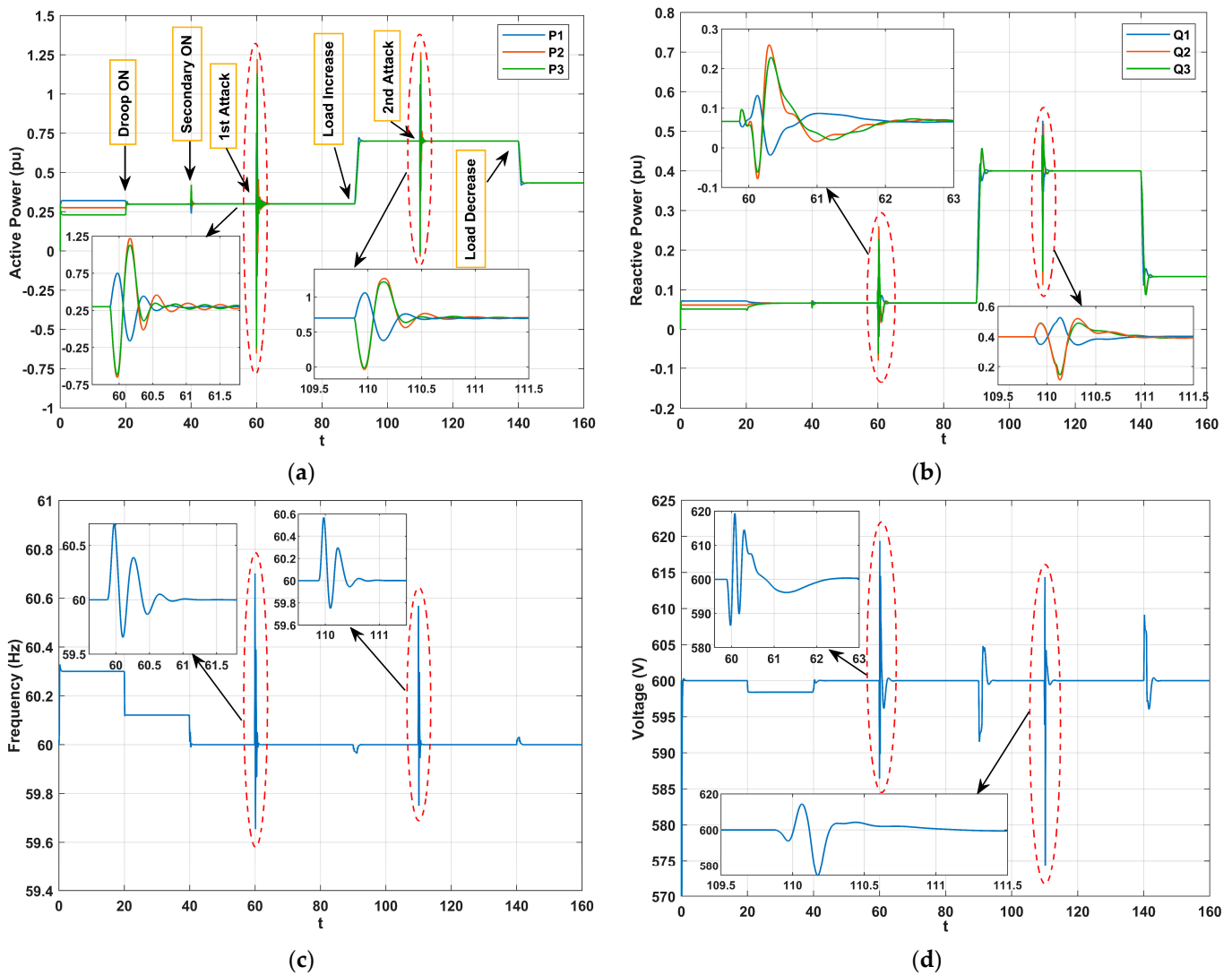


Figure 8. Performance of the proposed distributed consensus secondary control under deception attack on actuators' frequency: (a) Active power, (b) Reactive power, (c) Frequency, (d) Voltage.

The experiment conducted using the test setup demonstrates results when subject to deception attacks on sensor frequency, as shown in Figure 10. Following the activation of droop and secondary controllers, the first attack is launched at $t = 60$ s. The attack induced a notable impact on the system dynamics; it caused a frequency drop from its rated value. Upon initiation of the attack, the frequency dropped, and the equitable distribution of active power among DGs was impacted. Notably, the attacked DG1's active power output was minimal while DG2 and DG3 maintained their active power sharing and even increased compared to pre-attack levels. Simultaneously, transient voltage and reactive power disturbances were observed, though quickly mitigated. Upon the removal of the attack at $t = 80$ s, an instantaneous restoration of the frequency to its nominal value was observed alongside the restoration of active power sharing objectives. Afterwards, a similar behavior was noticed during the second attack at $t = 120$ s, though with a smaller amplitude, yet still impacting the frequency and active power sharing. These results underscore the importance of understanding the effects of attacks on MG systems and highlight the need for robust defense mechanisms to protect against potential disruptions.

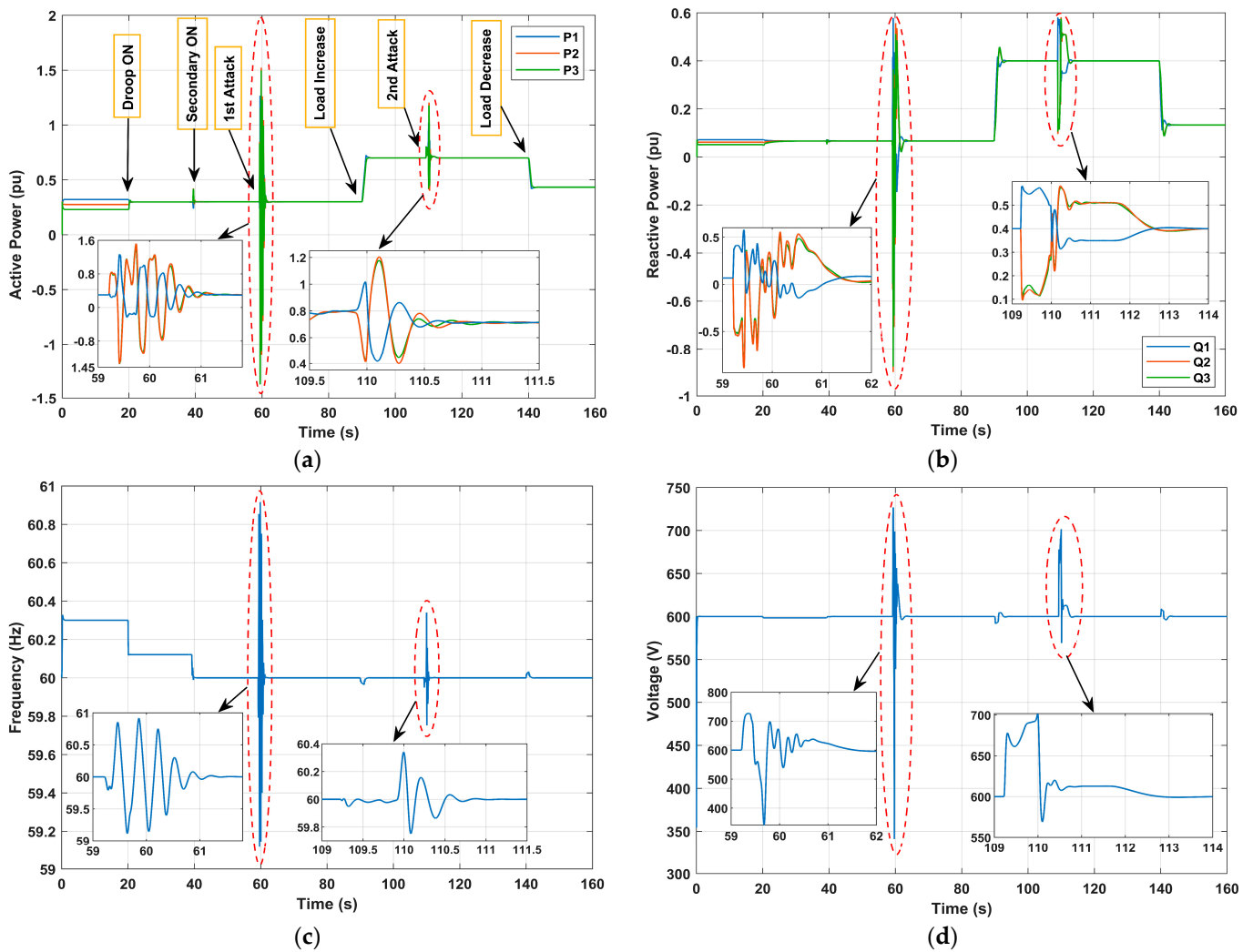


Figure 9. Performance of the proposed distributed consensus secondary control under deception attack on actuators' voltage: (a) Active power, (b) Reactive power, (c) Frequency, (d) Voltage.

5.2.4. Deception Attack on Sensors' Voltage

In this study case, $\delta_1^{S,V}$ denotes the sensor attack injections to the voltage measurements of DG #1. The attack signal is $\delta_1^{S,V} = \delta_1^{S,V1}$ between $60 < t(s) < 80$ and $\delta_1^{S,V} = \delta_1^{S,V2}$ between $120 < t(s) < 140$ where $\delta_1^{S,V1} > \delta_1^{S,V2}$.

The simulation scenario for this case is as follows:

- At $t = 20$ s, the droop control is activated;
- At $t = 40$ s, the distributed consensus secondary control is activated;
- At $t = 59$ s, the first voltage sensor attack is launched;
- At $t = 79$ s, the first attack is removed;
- At $t = 100$ s, the total load is increased;
- At $t = 119$ s, the second voltage sensor attack is launched;
- At $t = 139$ s, the second attack is removed;
- At $t = 160$ s, the load is decreased.

The conducted experiment shows the effects of deception attacks on sensor's voltage measurement within the distributed control framework. Notable consequences were observed upon launching the attack at $t = 59$ s, where the voltage dropped significantly from its rated value of 600 V to 530 V as shown in Figure 11. The consensus reactive power sharing deteriorated, and there was a decrease in active power sharing compared to pre-attack conditions. However, an unexpected behavior was observed upon ceasing the attack

at $t = 79$ s. Instead of a smooth recovery of the control objectives as seen in the previous experiment, the voltage surged beyond its rated value, accompanied by an increase in both active and reactive power as shown in Figure 11. While the control objectives were eventually restored after approximately 14 s, this deviation highlights the sensitivity of the system to this kind of attack, even with small injected values. After a load increase and the launch of a second attack at $t = 119$ s, a similar situation was observed, yet with a crucial difference. Despite the attack being stopped at $t = 139$ s, the system took a longer time to respond. It was not until $t = 180$ s that the control objectives were eventually restored. This suggests that the severity and duration of the attack directly influence the system’s ability to recover and maintain stability.

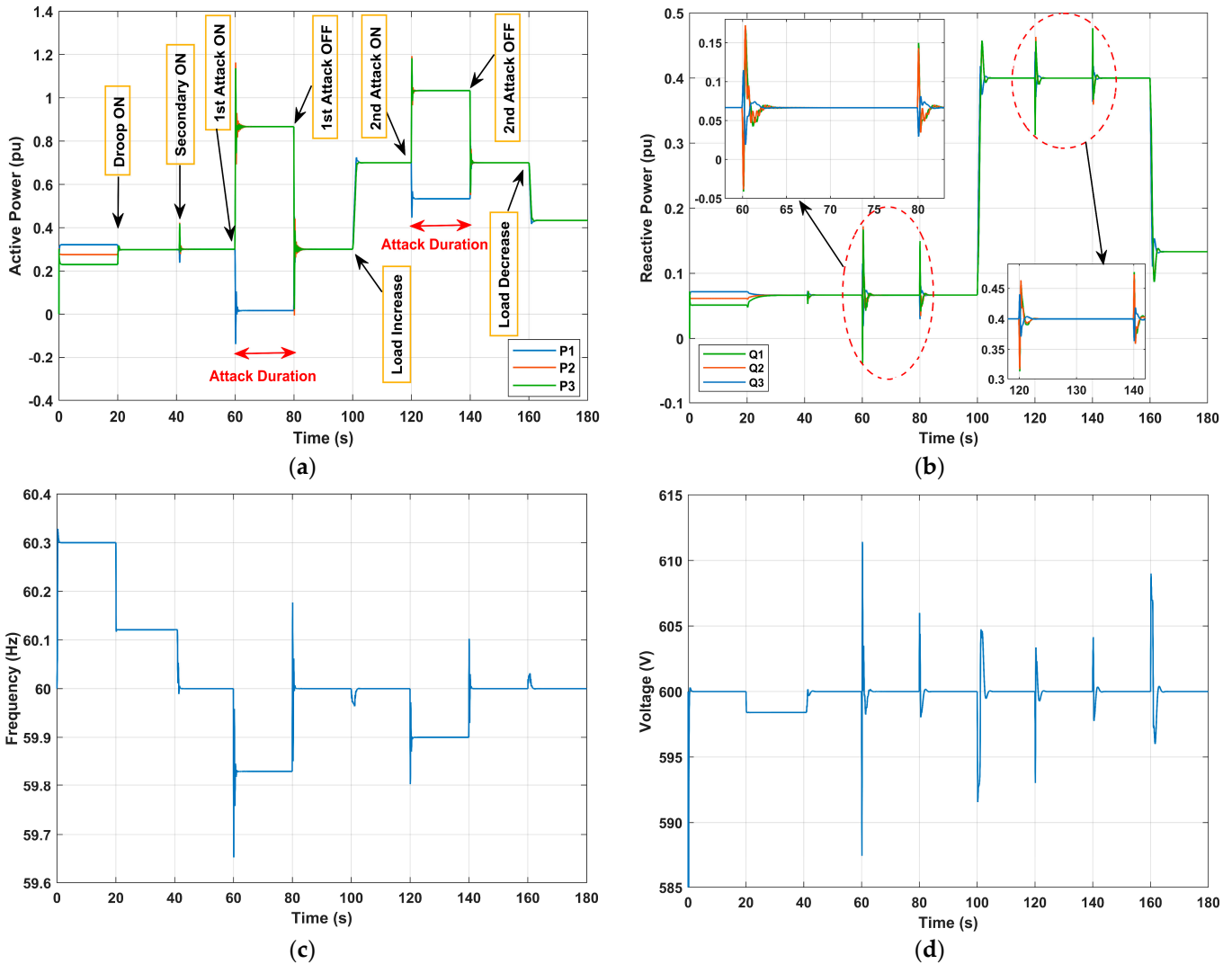


Figure 10. Performance of the proposed distributed consensus secondary control under deception attack on sensor’s frequency: (a) Active power, (b) Reactive power, (c) Frequency, (d) Voltage.

5.2.5. Combined Deception Attack on Frequency

In this study case, $\delta_1^{a,\omega}$ denotes the actuator attack injections to the frequency control loop of DG #1. The attack signal is $\delta_1^{a,\omega} = \delta_1^{a,\omega1}$ between $51.6 < t(s) < 71.6$ and $\delta_1^{a,\omega} = \delta_1^{a,\omega2}$ between $111.6 < t(s) < 131.6$ where $\delta_1^{a,\omega1} > \delta_1^{a,\omega2}$, and $\delta_1^{S,\omega}$ denotes the sensor attack injections to the frequency measurements of DG #1. The attack signal is $\delta_1^{S,\omega} = \delta_1^{S,\omega1}$ between $57.6 < t(s) < 77.6$ and $\delta_1^{S,\omega} = \delta_1^{S,\omega2}$ between $117.6 < t(s) < 137.6$ where $\delta_1^{S,\omega1} > \delta_1^{S,\omega2}$.

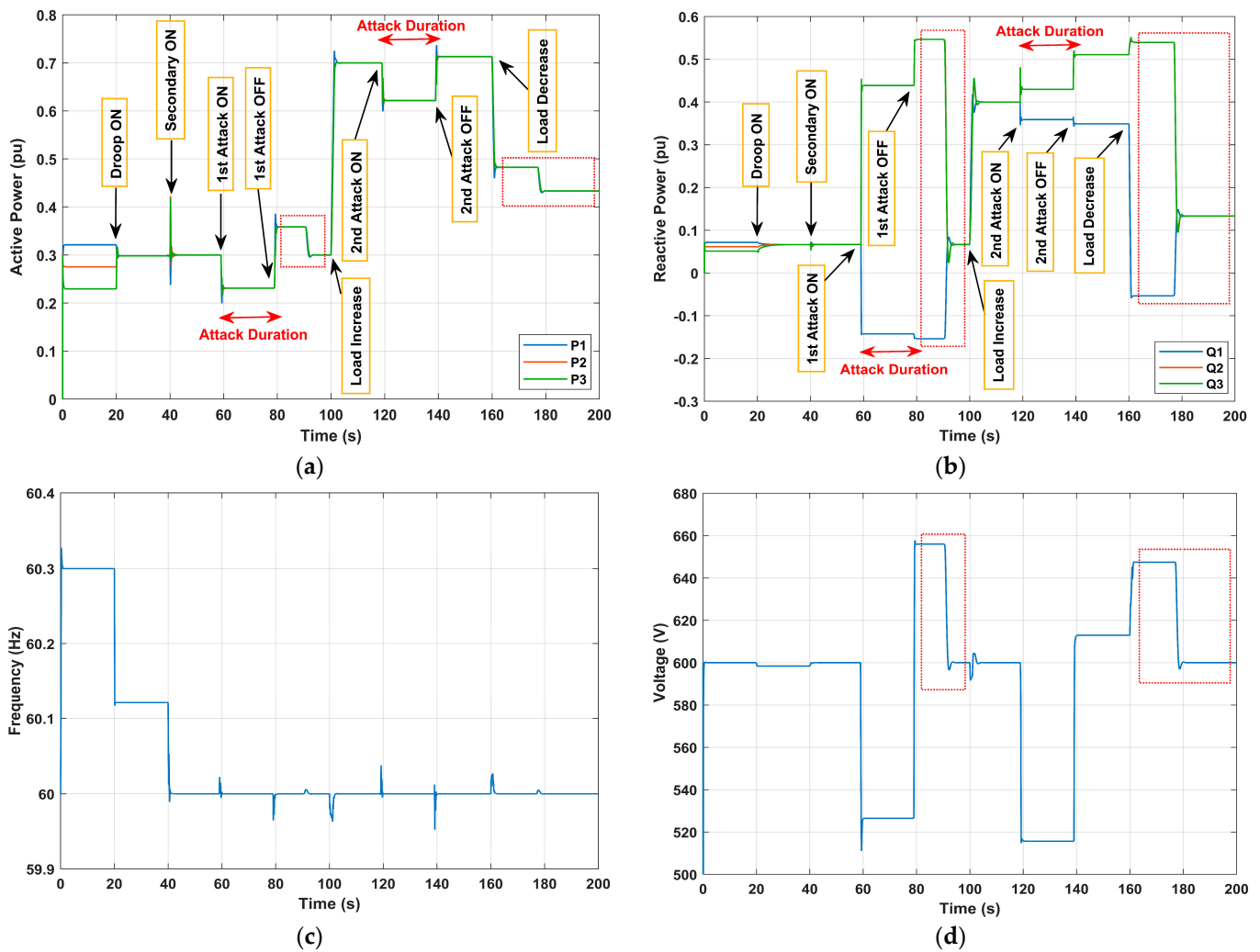


Figure 11. Performance of the proposed distributed consensus secondary control under deception attack on voltage: (a) Active power, (b) Reactive power, (c) Frequency, (d) Voltage.

The simulation scenario for this case is as follows:

- At $t = 20$ s, the droop control is activated;
- At $t = 30.6$ s, the distributed consensus secondary control is activated;
- At $t = 51.6$ s, the first frequency actuator attack is launched;
- At $t = 57.6$ s, the first frequency sensor attack is launched;
- At $t = 71.6$ s, the first frequency actuator attack is removed;
- At $t = 77.6$ s, the first frequency sensor attack is removed;
- At $t = 100$ s, the total load is increased;
- At $t = 111.6$ s, the second frequency actuator attack is launched;
- At $t = 117.6$ s, the second frequency sensor attack is launched;
- At $t = 131.6$ s, the second frequency actuator attack is removed;
- At $t = 137.6$ s, the second frequency sensor attack is removed.
- At $t = 160$ s, the load is decreased.

This experiment involves both actuator and sensor deception attacks on the frequency control loop of DG #1. It demonstrates a sequence of events where actuator attacks are initiated first, followed by sensor attacks as depicted in Figure 12. The attack signals for both actuator and sensor attacks vary in time intervals and magnitudes. During the attack periods, the system exhibited similar behavior to that observed in experiments 5.2.1 and 5.2.3. Upon removal of the attacks, the system restores to its nominal operating conditions.

However, the restoration may not be instantaneous and may depend on the attack's severity and duration as shown in the next experiment.

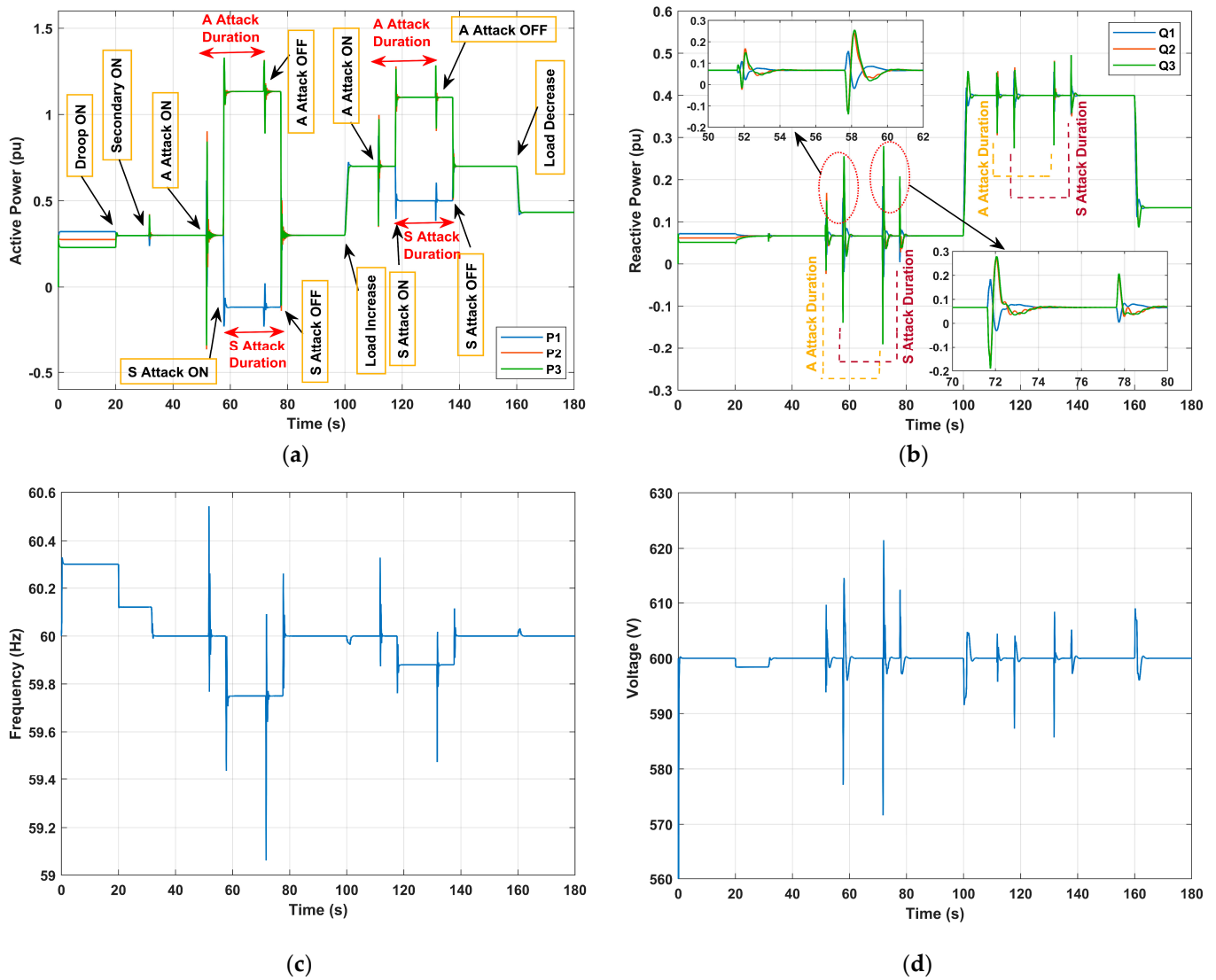


Figure 12. Performance of the proposed distributed consensus secondary control under combined deception attack on frequency: (a) Active power, (b) Reactive power, (c) Frequency, (d) Voltage.

5.2.6. Combined Deception Attack on Voltage

In this study case, $\delta_1^{a,V}$ denotes the actuator attack injections to the voltage control loop of DG #1. The attack signal is $\delta_1^{a,V} = \delta_1^{a,V1}$ between $62.7 < t(s) < 82.7$ and $\delta_1^{a,V} = \delta_1^{a,V2}$ between $122.7 < t(s) < 142.7$ where $\delta_1^{a,V1} > \delta_1^{a,V2}$, and $\delta_1^{S,V}$ denotes the sensor attack injections to the voltage measurements of DG #1. The attack signal is $\delta_1^{S,V} = \delta_1^{S,V1}$ between $68.7 < t(s) < 88.7$ and $\delta_1^{S,V} = \delta_1^{S,V2}$ between $128.7 < t(s) < 148.7$ where $\delta_1^{S,V1} > \delta_1^{S,V2}$.

The simulation scenario for this case is as follows:

- At $t = 20$ s, the droop control is activated;
- At $t = 41.7$ s, the distributed consensus secondary control is activated;
- At $t = 62.7$ s, the first voltage actuator attack is launched;
- At $t = 68.7$ s, the first voltage sensor attack is launched;
- At $t = 82.7$ s, the first voltage actuator attack is removed;
- At $t = 88.7$ s, the first voltage sensor attack is removed;
- At $t = 100$ s, the total load is increased;

- At $t = 122.7$ s, the second voltage actuator attack is launched;
- At $t = 128.7$ s, the second voltage sensor attack is launched;
- At $t = 142.7$ s, the second voltage actuator attack is removed;
- At $t = 148.7$ s, the second voltage sensor attack is removed;
- At $t = 160$ s, the load is decreased.

This experiment combines scenarios of both experiments 5.2.2 and 5.2.4. Actuator attacks on the voltage control loop are initiated first, followed by sensor attacks. During the attack periods and similar to the individual experiments, deviations from nominal voltage levels occur, impacting the consensus power sharing among DGs. As shown in Figure 13, the recovery of the system after the removal of the attacks at $t = 148.7$ s depends on severity of the attack.

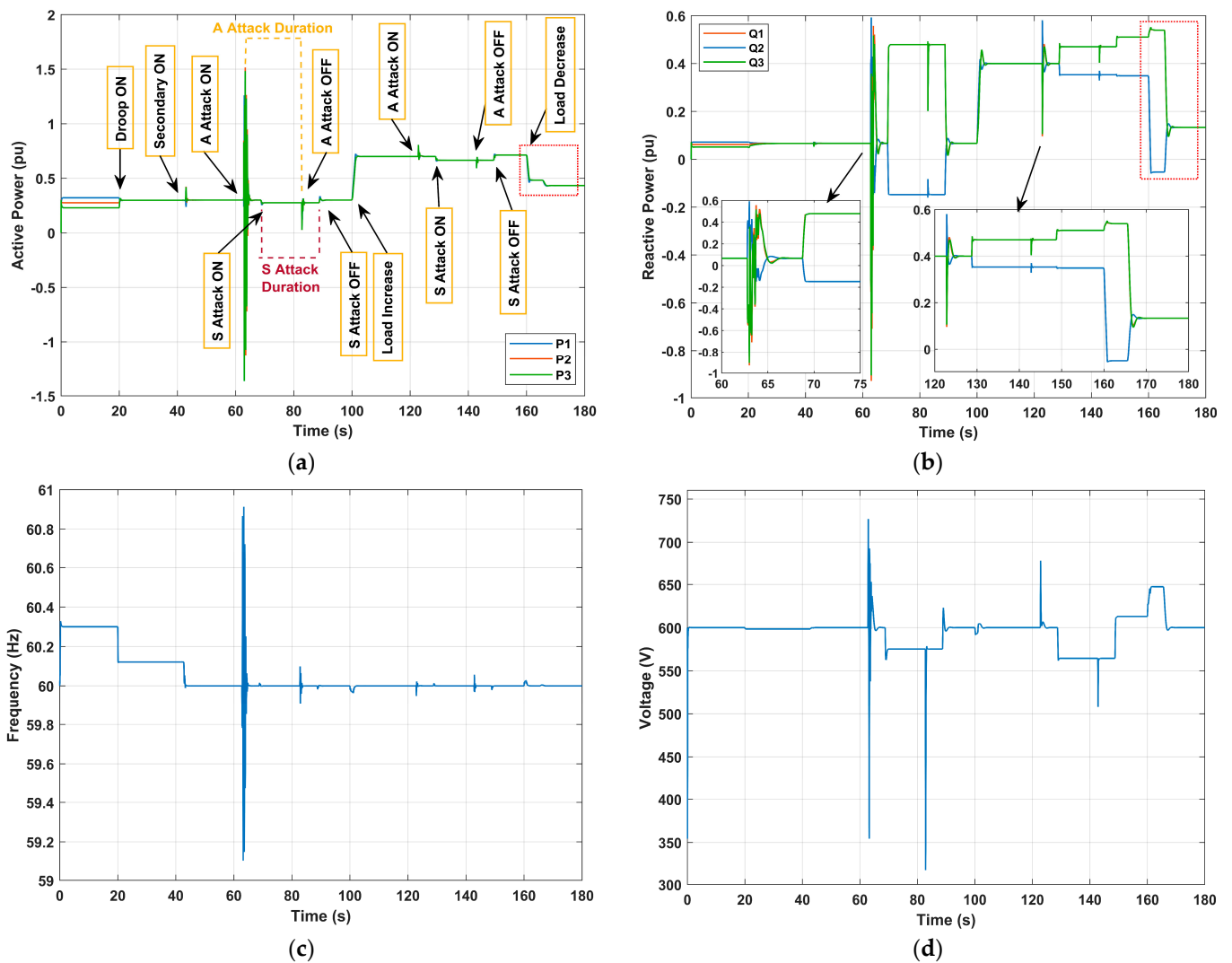


Figure 13. Performance of the proposed distributed consensus secondary control under combined deception attack on frequency: (a) Active power, (b) Reactive power, (c) Frequency, (d) Voltage.

5.3. Performance under Disruption Attacks

The simulation scenario for this case is as follows:

- At $t = 20$ s, the droop control is activated;
- At $t = 40$ s, the total load is increased;
- At $t = 60$ s, the distributed consensus secondary control is activated;
- At $t = 80$ s, the total load is decreased;
- At $t = 100$ s and $t = 120$ s, the total load is increased.

The DoS attack occurs at $t = 20$ s, $t = 65$ s, $t = 80$ s, and $t = 100$ s. The attack targeted agent #2 with short lengths (around $\tau_a = 5$ s) except the last one ($\tau_a > 10$ s). Due to local droop control and DG1 reference signal, system frequency and voltage can still be restored to 60 Hz and 600 V as shown in Figure 14. However, it can be noticed that when $\tau_a > 5$ s the DoS attack has a direct impact on the MG stability.

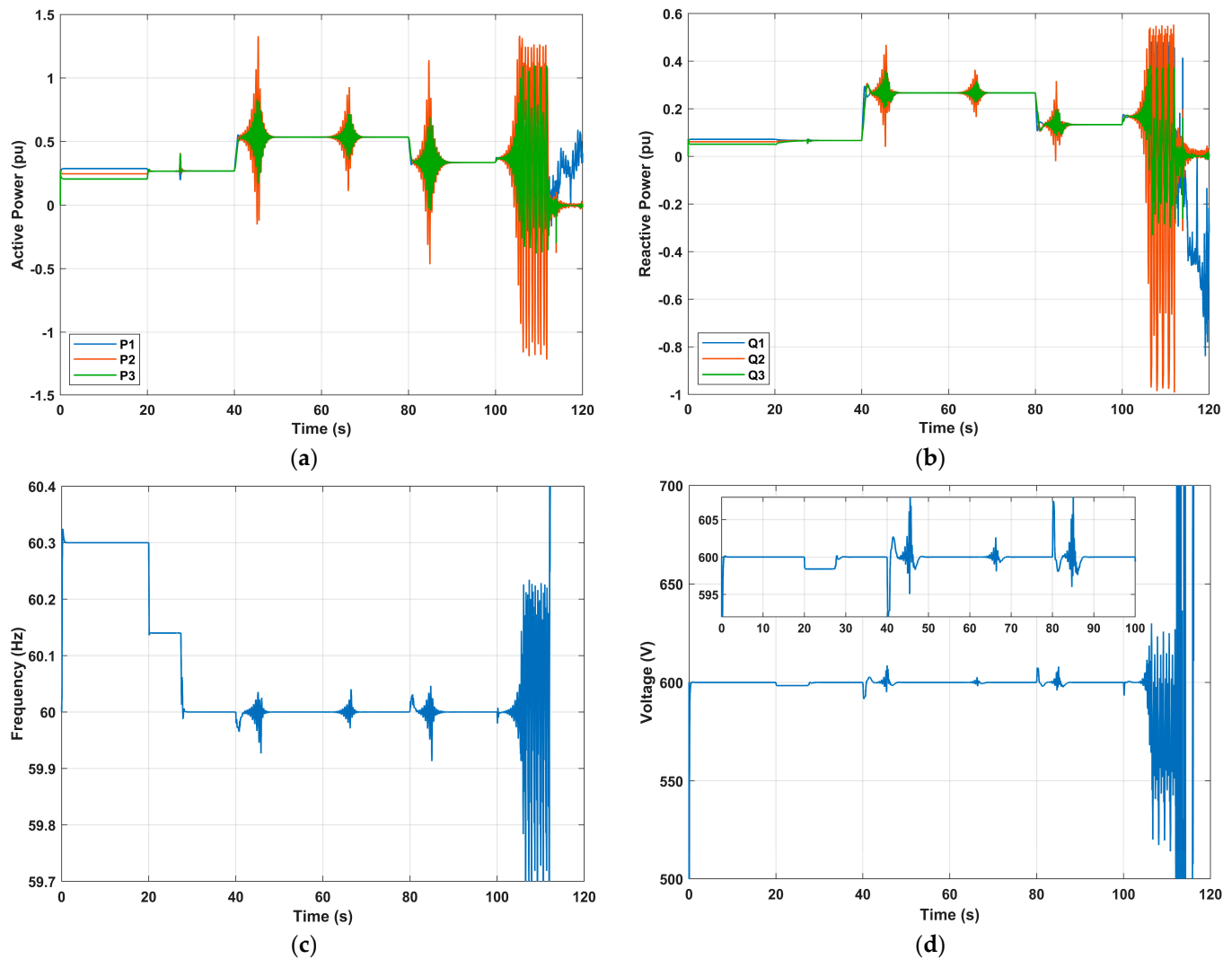


Figure 14. Performance of the proposed distributed consensus secondary control under combined deception attack on frequency: (a) Active power, (b) Reactive power, (c) Frequency, (d) Voltage.

It is worth mentioning that the effectiveness of DoS attacks often depends on the volume of traffic generated and the capacity of the target system to handle it. Attackers may adjust the packet rate based on their own resources and the target capabilities.

6. Conclusions

Considering the growing reliance on interconnected systems, the vulnerabilities of microgrid cyber-physical systems need careful attention. Through the development of a CHIL testbed and the implementation of distributed consensus secondary control strategy, this research not only highlights the potential risks posed by cyber threats but also is a building block for developing concrete solutions to bolster the resilience of microgrids. The proposed platform includes, a real-time islanded AC MG implemented on OPAL-RT, controllers implemented on Raspberry Pis, and a separate Raspberry Pi to launch the attacks. Extensive real-time digital simulations on OPAL-RT are performed to evaluate the

effect of various cyber-attacks on the proposed distributed consensus secondary control of the islanded AC MG. The experiments include modeling and launching linear additive deception attacks on sensors, actuators, and their combinations, as well as disruption attacks. The outcomes of our real-time tests vividly illustrated the effects of both bounded and unbounded cyber-attacks on control objectives and system stability. These findings underscore the critical importance of implementing robust cybersecurity measures to uphold the stability and reliability of microgrid cyber-physical systems.

Author Contributions: Conceptualization, I.K. and O.A.M.; methodology, I.K.; software, I.K.; validation, I.K. and O.A.M.; formal analysis, I.K.; investigation, O.A.M.; resources, O.A.M.; writing—original draft preparation, I.K.; writing—review and editing, O.A.M.; visualization, I.K.; supervision, O.A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by grants from the Office of Naval Research, National Science Foundation, and the US Department of Energy. The authors are with the Energy Systems Research Laboratory, Department of Electrical and Computer Engineering, Florida International University, Miami, FL, USA.

Data Availability Statement: Data are contained within the article.

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

References

- Abianeh, A.J.; Mardani, M.M.; Ferdowsi, F.; Gottumukkala, R.; Dragicevic, T. Cyber-Resilient Sliding-Mode Consensus Secondary Control Scheme for Islanded AC Microgrids. *IEEE Trans. Power Electron.* **2022**, *37*, 6074–6089. [\[CrossRef\]](#)
- Yang, T.; He, Y.; Liu, G.-P. Distributed Voltage Restoration of AC Microgrids Under Communication Delays: A Predictive Control Perspective. *IEEE Trans. Circuits Syst. Regul. Pap.* **2022**, *69*, 2614–2624. [\[CrossRef\]](#)
- Liu, Y.; Li, Y.; Wang, Y.; Zhang, X.; Gooi, H.B.; Xin, H. Robust and Resilient Distributed Optimal Frequency Control for Microgrids Against Cyber Attacks. *IEEE Trans. Ind. Inform.* **2022**, *18*, 375–386. [\[CrossRef\]](#)
- Chlela, M.; Joos, G.; Kassouf, M.; Brissette, Y. Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–5. [\[CrossRef\]](#)
- Rath, S.; Pal, D.; Sharma, P.S.; Panigrahi, B.K. A Cyber-Secure Distributed Control Architecture for Autonomous AC Microgrid. *IEEE Syst. J.* **2021**, *15*, 3324–3335. [\[CrossRef\]](#)
- Yao, W.; Wang, Y.; Xu, Y.; Deng, C. Cyber-Resilient Control of an Islanded Microgrid Under Latency Attacks and Random DoS Attacks. *IEEE Trans. Ind. Inform.* **2023**, *19*, 5858–5869. [\[CrossRef\]](#)
- Tadepalli, P.S.; Pullaguram, D. Distributed Control Microgrids: Cyber-Attack Models, Impacts and Remedial Strategies. *IEEE Trans. Signal Inf. Process. Netw.* **2022**, *8*, 1008–1023. [\[CrossRef\]](#)
- Fan, H.; Wang, H.; Xia, S.; Li, X.; Xu, P.; Gao, Y. Review of Modeling and Simulation Methods for Cyber Physical Power System. *Front. Energy Res.* **2021**, *9*, 642997. [\[CrossRef\]](#)
- Li, Y.; Fan, L.; Bao, L.; Miao, Z. CHIL Testbed of Consensus Control-Based Battery Energy Storage Systems. In Proceedings of the 2020 52nd North American Power Symposium (NAPS), Tempe, AZ, USA, 11–13 April 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6. [\[CrossRef\]](#)
- Naderi, E.; Asrari, A. Hardware-in-the-Loop Experimental Validation for a Lab-Scale Microgrid Targeted by Cyberattacks. In Proceedings of the 2021 9th International Conference on Smart Grid (icSmartGrid), Setubal, Portugal, 29 June–1 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 57–62. [\[CrossRef\]](#)
- Ren, X.; Liang, J.; Liu, Q. A Defensive Strategy for Integrity Detection in Cyber-Physical Systems Subject to Deception Attacks. In Proceedings of the 2020 10th International Conference on Information Science and Technology (ICIST), Bath, London, and Plymouth, UK, 9–15 September 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 241–246. [\[CrossRef\]](#)
- Shabad, P.K.R.; Alrashide, A.; Mohammed, O. Anomaly Detection in Smart Grids using Machine Learning. In Proceedings of the IECON 2021—47th Annual Conference of the IEEE Industrial Electronics Society, Toronto, ON, Canada, 13–16 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–8. [\[CrossRef\]](#)
- Afshari, A.; Karrari, M.; Baghaee, H.R.; Gharehpetian, G.B. Resilient Synchronization of Voltage/Frequency in AC Microgrids Under Deception Attacks. *IEEE Syst. J.* **2021**, *15*, 2125–2136. [\[CrossRef\]](#)
- Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 3317–3318. [\[CrossRef\]](#)
- Lai, J.; Zhou, H.; Lu, X.; Yu, X.; Hu, W. Droop-Based Distributed Cooperative Control for Microgrids with Time-Varying Delays. *IEEE Trans. Smart Grid* **2016**, *7*, 1775–1789. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)

17. Mohammadi, F.D.; Vanashi, H.K.; Feliachi, A. State-Space Modeling, Analysis, and Distributed Secondary Frequency Control of Isolated Microgrids. *IEEE Trans. Energy Convers.* **2018**, *33*, 155–165. [[CrossRef](#)]
18. Jamali, M.; Sadabadi, M.S.; Davari, M.; Sahoo, S.; Blaabjerg, F. Resilient Cooperative Secondary Control of Islanded AC Microgrids Utilizing Inverter-Based Resources Against State-Dependent False Data Injection Attacks. *IEEE Trans. Ind. Electron.* **2024**, *71*, 4719–4730. [[CrossRef](#)]
19. Kharchouf, I.; Abdelrahman, M.S.; Mohammed, O.A. ANN-Based Secure Control of Islanded Microgrid Under False Data Injection Cyber-Attack. In Proceedings of the 2023 IEEE Industry Applications Society Annual Meeting (IAS), Nashville, TN, USA, 29 October–2 November 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–6. [[CrossRef](#)]
20. Raman, G.; Liao, K.; Peng, J.C.-H. Improving AC Microgrid Stability Under Cyberattacks Through Timescale Separation. *IEEE Trans. Circuits Syst. II Express Briefs* **2023**, *70*, 2191–2195. [[CrossRef](#)]
21. Mi, Y.; Deng, J.; Wang, X.; Lin, S.; Su, X.; Fu, Y. Multiagent Distributed Secondary Control for Energy Storage Systems with Lossy Communication Networks in DC Microgrid. *IEEE Trans. Smart Grid* **2013**, *14*, 1736–1749. [[CrossRef](#)]
22. Bidram, A.; Davoudi, A.; Lewis, F.L. A Multiobjective Distributed Control Framework for Islanded AC Microgrids. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1785–1798. [[CrossRef](#)]
23. Han, Y.; Li, H.; Shen, P.; Coelho, E.A.A.; Guerrero, J.M. Review of Active and Reactive Power Sharing Strategies in Hierarchical Controlled Microgrids. *IEEE Trans. Power Electron.* **2017**, *32*, 2427–2451. [[CrossRef](#)]
24. Zhuang, J.; Peng, S.; Wang, Y. Secure Consensus of Stochastic Multi-agent Systems Subject to Deception Attacks via Impulsive Control. In Proceedings of the 2022 4th International Conference on Control and Robotics (ICCR), Guangzhou, China, 2–4 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–6. [[CrossRef](#)]
25. Lu, L.-Y.; Liu, J.-H.; Lin, S.-W.; Chu, C.-C. Concurrent Cyber Deception Attack Detection of Consensus Control in Isolated AC Microgrids. *IEEE Trans. Ind. Appl.* **2023**, *59*, 7584–7596. [[CrossRef](#)]
26. He, W.; Xu, W.; Ge, X.; Han, Q.-L.; Du, W.; Qian, F. Secure Control of Multiagent Systems Against Malicious Attacks: A Brief Survey. *IEEE Trans. Ind. Inform.* **2022**, *18*, 3595–3608. [[CrossRef](#)]
27. Mustafa, A.; Moghadam, R.; Modares, H. Resilient Synchronization of Distributed Multi-agent Systems under Attacks. *arXiv* **2019**, arXiv:1807.02856. [[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.