UNIVERSIDAD NACIONAL DE COLOMBIA

Cyber-Attack Resilient Control for Microgrids

Estéfany Osorio Arroyave

Universidad Nacional de Colombia
Facultad de Ingeniería Eléctrica Departamento
Bogotá, Colombia
2020

Cyber-Attack Resilient Control for Microgrids

Estéfany Osorio Arroyave

Master Thesis, as partial requirement for the degree in:
Magister en Ingeniería - Automatización Industrial

Advisor:
Eduardo Alirio Mojica Nava Ph.D.

Research program:
Redes Eléctricas Inteligentes
Research Group
PAAS-UN

Universidad Nacional de Colombia
Facultad de Ingeniería Eléctrica
Bogotá, Colombia
2020

To my granny, who is no longer here, but who would be proud of this my new step.

To my parents, my sister, and my niece, my lovely family, who supported me in every decision that brought me here.

Acknowledgments

I am thankful to my advisor Dr. Eduardo Mojica Nava, associate professor of the engineering faculty of the Universidad Nacional de Colombia, for his direction during the development of this project. I thank Wladimir Toro Tovar, Ph.D. student in engineering at the Universidad Nacional de Colombia, who provided the first bases for the subsequent development of the primary control of this work. Finally, I express my appreciation to the PAAS-UN research group for the valuable welcome they gave me during my stay on the UN campus.

Abstract

This document presents a secondary resilient control on an islanded inverter-based microgrid. The studies of the system are done in a microgrid with six inverters under four scenarios of cyber-attacks either in the controller or in the communication links. The control architecture is presented in a hierarchical framework with decentralized primary control and a distributed secondary control based on a cooperative scheme, including two observer designs to withstand the attacks in the system. The synchronization of frequency and voltage is reached despite an attack event under the adequate selection of the control strategy. The effectiveness of the proposed control architectures is probed through simulations in Simulink, Matlab®.

Keywords: resilient, control, microgrid, inverter, cyber-attack, communication-link, cooperative, observer.

Resumen

Este documento presenta un control secundario resiliente para una microrred aislada basada en inversores. Los estudios del sistema se realizan en una microrred con seis inversores en cuatro escenarios de ciber-ataque, ya sea en el controlador o en los enlaces de comunicación. La arquitectura de control se presenta en un marco jerárquico con control primario descentralizado y control secundario distribuido basado en un esquema cooperativo, que incluye dos diseños de observadores para resistir los ataques en el sistema. La sincronización de frecuencia y voltaje se alcanza a pesar de un evento de ataque bajo la adecuada selección de la estrategia de control. La efectividad de las arquitecturas de control propuestas se prueba mediante simulaciones en Simulink, Matlab®.

Palabras clave: control, resiliente, microrred, inversor, ciber-ataque, cooperativo, observador.

Content

Acknowledgments **vii**

Abstract **ix**

List of figures **xiii**

List of tables **xvii**

1 Introduction **21**

1.1 Context of the Microgrids . . . 21

1.2 Benefits and Components of the Microgrids . . . 22

1.3 Cyber-Physical Risk and Limitations . . . 22

1.4 Scope of this Work . . . 23

2 Models of AC Islanded Microgrids **25**

2.1 The Generator Model . . . 26

2.1.1 The Inverter Bridge . . . 27

2.1.2 The Power Controller . . . 29

2.1.3 The Voltage Controller . . . 30

2.1.4 The Current Controller . . . 31

2.1.5 Compact Model of the Controller . . . 32

2.2 The Branch Connection Model . . . 34

2.2.1 The Output Connector . . . 34

2.2.2 Power Equations . . . 35

3 Control Strategies for Microgrids **39**

3.1 Primary Control . . . 40

3.1.1 Zero Control . . . 41

3.1.2 Primary Frequency Control . . . 41

3.1.3 Primary Voltage Control . . . 42

3.2 Secondary Control 43
3.3 Tertiary Control 48
3.4 Islanded vs Connected - grid Microgrids 48

4 Models of Sophisticated Attacks on Islanded Microgrids 51
4.1 Controller Attacks 52
4.1.1 Offsetting the Controller Set-points 52
4.1.2 Hijacking the Entire Controller 53
4.1.3 Sensor/Actuator Compromised 54
4.2 Communication Links Attacks 55
4.2.1 Offsetting the Communication Data 55
4.2.2 Hijacking the Entire Communication Link 56

5 Resilient Secondary Cooperative Control 57
5.1 Graph Basics and Connectivity 58
5.1.1 Matrix Representation 61
5.1.2 Spectral Properties and Connectivity 63
5.2 Agents' Dynamics and Consensus Protocols 64
5.2.1 First-order Dynamics 65
5.2.2 Second-order Dynamics 66
5.3 Distributed Cooperative Control 67
5.3.1 Secondary Frequency Control 69
5.3.2 Secondary Voltage Control 70
5.4 Observer-based Cooperative Control 71
5.4.1 Observer Design 1 72
5.4.2 Observer Design 2 73
5.5 Case Studies 76
5.5.1 System Configuration 76
5.5.2 Communication Layer 76
5.5.3 Scenarios Description 80
5.5.4 Results 83

6 Conclusions and Recommendations 103
6.1 Conclusions 103
6.2 Recommendations 104

References 104

List of Figures

2-1 General scheme of a microgrid 25
2-2 VCVSI generator. From [9]. 26
2-3 Simplified topology of a three phase inverter bridge. From [16]. 27
2-4 Power estimation process. From [9] 29
2-5 Voltage controller. From [9] 31
2-6 Current controller. From [9] 32
2-7 Inverter connected to the AC common bus. 35

3-1 Primary control functions. 40
3-2 Primary control and zero Control. 41
3-3 Secondary control variations. 44
3-4 Primary and secondary control synergy for the cooperative control approach. . . 48
3-5 Reference values of frequency and voltage for both islanded and connected mode. 49

5-1 General graph illustration: (a) Graph components; (b) Digraph. 58
5-2 Example of graph notation. From [36] 60
5-3 Example of digraph notation. From [36] 60
5-4 Agents' dynamics and some consensus protocols. 68
5-5 Observer design 1. 73
5-6 Observer design 2. 75
5-7 Original IEEE 34 node test feeder. 76
5-8 IEEE 34 node test feeder modified with six inverters. 77
5-9 Inverters connection to the AC bus. 78
5-10 IEEE 34 bus modified with the communication layer. 79
5-11 Communication network topology of the microgrid with 6 inverters. (a) General graph. (b) Graph with the references pinned to the leader node. 79
5-12 Constant disturbance attack to communication link of inverter 2. 82
5-13 Hijacking attack to communication link of inverter 2. 82
5-14 Communication graph topology of Figure **5-11** with the edge $v_2 v_3$ disconnected. . 83

5-15 Physical disconnection of DG2 from the common bus. 83

5-16 Frequency response of the system with the conventional cooperative control under a constant disturbance attack of 0.2 Hz in the controller of inverter 2 in $t = 1$ s. 85

5-17 Voltage response of the system with the conventional cooperative control under a constant disturbance attack of 0.2 Hz in the controller of inverter 2 in $t = 1$ s. . 86

5-18 Frequency response of the system with the conventional cooperative control under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. 87

5-19 Voltage response of the system with the conventional cooperative control under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. 87

5-20 Frequency response of the system using the conventional cooperative control under a constant disturbance attack of 0.2 Hz in the communication link of inverter 2 in $t = 1$ s. (a) Frequency response before the attack deployment (measured value). (b) Frequency signal received by the secondary control 88

5-21 Voltage response of the system using the conventional cooperative control under a constant disturbance attack of 0.2 Hz in the communication link of inverter 2 in $t = 1$ s. 89

5-22 Frequency response of the system using a frequency observer-based cooperative control (design 1) under a a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. 90

5-23 Voltage response of the system using a frequency observer-based cooperative control (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s for two different values of coupling gain: (a) $c_v = 120$ and (b) $c_v = 200$. 91

5-24 Frequency response of the system using a frequency observer-based cooperative control (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. Disconnection of node 2 from the graph in $t = 6$ s. 91

5-25 Voltage response of the system with a frequency observer-based cooperative control (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. Disconnection of node 2 from the graph in $t = 6$ s. 92

5-26 Voltage response of the system with a cooperative control using observers for frequency and voltage (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. 93

5-27 Voltage response of the system with a cooperative control using observers for frequency and voltage (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. Disconnection of node 2 from the graph in $t = 6$ s. 93

5-28 Voltage response of the system with a cooperative control using observers for frequency and voltage (design 1) under a constant disturbance attack of 0.2 Hz in the communication link of inverter 2 in $t = 1$ s. 94

5-29 Frequency response of the system using the design 2 of the observer based-cooperative control under a constant disturbance attack of 0.2 Hz in the controller of inverter 2 in $t = 1$ s. 95

5-30 Voltage response of the system using the design 2 of the observer based-cooperative control under a constant disturbance attack of 0.2 Hz in the controller of inverter 2 at $t = 1$ s. 96

5-31 Frequency response of the system using the design 2 of the observer-based cooperative control under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. 97

5-32 Voltage response of the system using the design 2 of the observer-based cooperative control under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. 97

5-33 Frequency response of the system with the design 2 of the observer-based cooperative control under a constant disturbance attack of 0.2 in the communication link of inverter 2 in $t = 1$ s. (a) Frequency response before the attack deployment (measured value). (b) Frequency signal received by the secondary control. 98

5-34 Voltage response of the system with the design 2 of the observer-based cooperative control under a constant disturbance attack of 0.2 Hz in the communication link of inverter 2 in $t = 1$ s. 99

5-35 Frequency response of the system with the design 2 of the observer-based cooperative control under a hijacking attack of 60.2 Hz in the communication link of inverter 2 in $t = 1$ s. (a) Frequency response before the attack deployment (measured value). (b) Frequency signal received by the secondary control. 100

5-36 Voltage response of the system with the design 2 of the observer-based cooperative control under a hijacking attack of 60.2 Hz in the communication link of inverter 2 in $t = 1$ s. 100

List of Tables

5-1 Transformer specifications. 77
5-2 Parameters of the inverters. 77
5-3 Implemented cyber-attack experiments. 84
5-4 Performance response of the control schemes under different attack scenarios. . . . 101

1 Introduction

1.1. Context of the Microgrids

Even though renewable energies have been a topic in discussion for more than twenty years, it is only recently that it has gained strength as a research interest [14]. The introduction of new technologies in the control and monitoring of electrical power grids, such as smart metering and the concept of distributed generation, has changed the paradigm of control in power grids. Smart grids appear as a proper solution to the new necessities, including new structures and approaches such as *the microgrids* [38]. A microgrid is a small local network performing a similar task to the main power grid, but its generation sources are usually renewable. Microgrids can work either connected to the main grid or as an autonomous system, i.e., connected-mode or islanded mode. Microgrids provide high-quality power as well as proper coordination through their distributed generators (DGs) [58, 37].

Communication networks became an essential component in these new systems, which increasingly operate on open networks with many benefits, but also with cyber-security challenges [53, 27]. The electric power system is a cyber-physical infrastructure, and as such, it is prone to cyber-threats throughout all their components and levels, including generation, distribution, and consumption [4]. Microgrids have similar elements to the main power grid. Their structure is complex, and designing their control and protection systems is difficult [9]. Nevertheless, microgrids also have many benefits such as excellent system reliability, the inclusion of plug-and-play storage systems, auto-restoration (also known as an autogenous start-up, or black start, after an event of partial or total network failure), and an active load control [39].

Despite the associated cybernetic risk and their intrinsic complexities, microgrids offer a plethora of benefits that outweigh those perils, and therefore their use will only increase and will become ubiquitous. For governments, developing strategies to protect these infrastructures become an essential task since system failures and system hijackings mainly would be catastrophic endangering lives, as well as the entire economy of a country [5].

1.2. Benefits and Components of the Microgrids

One of the most representative benefits, among the multiple, that microgrids have to offer is their Plug-and-play (PnP) capability. PnP enables the devices to be connected or disconnected without having to change the system configuration; examples are inverters and electric vehicles. PnP also allows the microgrid to be connected to or disconnected from the main power grid without having to modify its structure or its control parameters. When connected, the microgrid is said to be in grid-connected mode. When disconnected, the microgrid is said to be in an islanded mode. The selection of operation mode implies differences in how the control strategy works.

Most control architectures used for microgrids are hierarchical and include three basic control levels. The first level (the primary control) works autonomously and in a decentralized way; this level is in charge of providing the adequate exchange of power among the inverters through the regulation of the values of frequency and voltage. The second level (the secondary control) must guarantee the synchronization of voltage and frequency values in the DGs. Finally, the third level (the tertiary control) is in charge of operational and economic aspects, such as optimal dispatch, which refers to the flow of active and reactive power between the main network and the microgrid [58]. *In grid-connected mode*, the main grid performs the tasks of the secondary control. In other words, the set-points for frequency and voltage in the microgrid are imposed externally from the main grid [9]. In this mode of operation, both the microgrid and the main grid work together to supply the loads requirements. *In islanded mode*, the microgrid itself must perform the tasks of the secondary control [58].

As in the main grid, microgrids need to be also “smart”. They require mechanisms to switch between modes, and sensors and actuators to monitor and command each component in the system for each level of the control hierarchy [9].

1.3. Cyber-Physical Risk and Limitations

In the hierarchy of the microgrid, the physical risk appears in the first level of control. Here, the attacks are performed locally in any of the components of the inverter bridge, e.g., the sensors, or the actuators, extensively studied in the literature [18, 41, 15]. On the other hand, cyber-risk appears in the second level, which includes the critical communication layer through which a large volume of information is exchanged. Accordingly, the attacks may occur in 1) the communication links of the DGs or 2) in the controller of an inverter [28]. Examples of cyber-attacks are the alteration of the signal or the hijacking of the signal. For the particular case of a microgrid, the altered signal could be either the frequency or the voltage values.

Traditional control architectures can be used to mitigate noise disturbances, or to estimate latent variables (those variables that can not be measured directly). Most conventional filters aim to mitigate random noise and are not suitable for the case of attacks where the disturbance in the variables has been deliberately designed [2]. In an attack, measurements can be completely false, albeit within an available range of values. Methods to recover from an attack are philosophically different from those to ameliorate noise [6, 5]. For example, in a signal hijacking, variable readings could be false and controlled by the adversary, who attempts to produce a break down in the system [27].

In some electric power dispatch centers, the strategies used to deal with cyber-threats are based on disconnecting affected equipment, once an incoming threat is detected, e.g., the case in the Colombian National Center of Dispatch manged by XM, as stated by an Intercolombia engineer during the Fifth Colombian Seminar in Power Systems SASE 2019 [48]. Although it could be an effective solution, it is not viable in distributed generation systems, like in a microgrid, which must supply the demand reliably and continuously.

The National Association of Regulatory Utility Commissioners (NARUC) in the USA, has developed detailed guidelines for an integrated cyber-security risk management specifically for the electrical power sector [12, 32, 17]. Just in 2018, big oil companies invested more than 1.87 billion dollars in the development of their cyber-security infrastructure [22], which is an indication of the size of the problem.

1.4. Scope of this Work

The focus of this work is to establish a methodology for the resilient control strategy of a microgrid, operating in islanded mode, under cyber-attack in its communication links. The scope of the work includes: 1) modeling the microgrid as a cyber-physical system, 2) modeling a different kind of attacks that could occur in the communication links, 3) developing a control strategy to keep the microgrid operational during attacks, and 4) validating the proposed control strategies in a simulation tested using the IEEE 34-bus in Matlab® and Simulink® with Simscape Electrical®.

The rest of this document is set up as follows: Chapter 2 introduces the basic concepts of the microgrid, its main components, and the job of each component into the system. Also, it introduces the building elements of the DG, such as the inverter and its controllers. Chapter 3 presents the control strategies for all the levels in the hierarchy, including frequency and voltage controllers. Chapter 4 describes the mathematical models and methods used to represent attacks on a microgrid. Chapter 5 presents a proposal for a resilient control strategy to attacks on the communication links, as well as the case studies and results. Finally, Chapter 6 presents the conclusions of this work and proposes future work on how to expand this research further.

2 Models of AC Islanded Microgrids

Even though a microgrid is a local electrical network, its modeling can be as complex as the one for the wide area electrical system. This local network is composed of coupled electrical systems, sensors and actuators, and communication networks. Therefore, a microgrid is a cyber-physical system, and its modeling must take into account all the complexities of such systems.

The microgrid could be seen as an electrical interconnected multi-agent system, where each of the agents has a specific behavior or model, and all of them are coupled with buses, branches, and nodes. A general scheme of a microgrid could be seen in Figure **2-1**.

In Figure **2-1**, the bus is an electric transmission system that supports the power flow in the microgrid. The branches are the connections between the bus and any node, and finally, a node could be either a generator or a power load.

The microgrid is properly modeled by a coupled model of the generators, the branches, and loads connected to the bus. The following sections focus on describing the individual models of each component and the interaction among them.

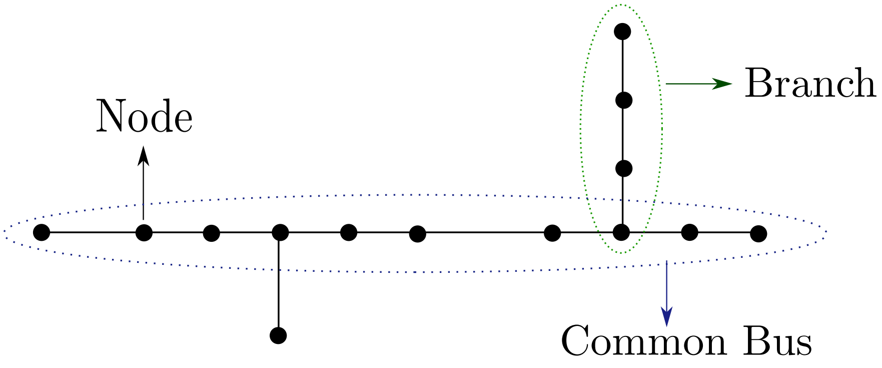

Figure 2-1: General scheme of a microgrid

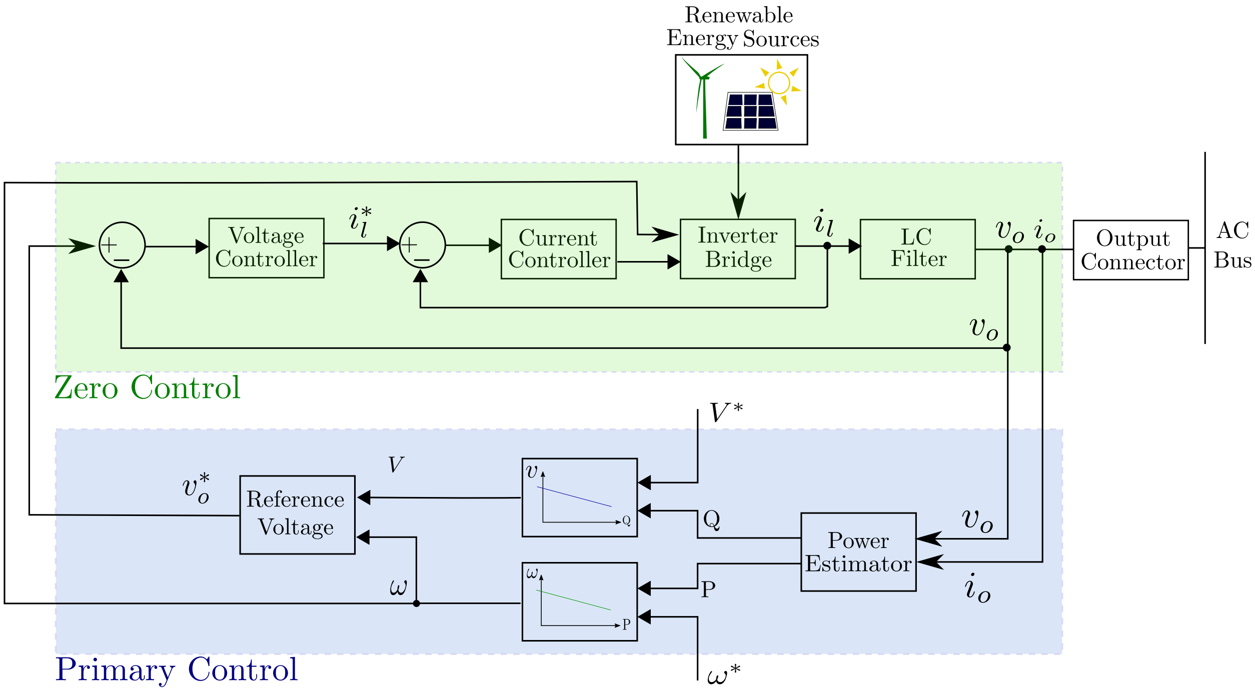

Figure 2-2: VCVSI generator. From [9].

2.1. The Generator Model

The generator is a pivotal component of the microgrid model, especially in islanded mode, given that it provides power to the system and keeps the network operation. The most energy sources in islanded microgrids are renewable, whose energy is usually produced in direct current (DC) and stored in battery banks. Then, a three-phase inverter bridge is needed to transform the generated DC energy into alternating current (AC), to make possible the interaction with the connected loads and the eventual connection with the main power grid. Figure **2-2** illustrates a general diagram of the internal structure of a generator; in this case, a VCVSI (Voltage-Controlled Voltage Source Inverter), which is mainly adopted from [9].

In general, the output of the inverter is a set of three-phase near-sinusoidal waves. The LC filter helps to decrease the distortion caused by switching effects and provides a generator output with lower total harmonic distortion. The internal computations require measurements of output voltages and currents in all controllers. These terms belong to a three-phase system, abc. However, in order to simplify computations, these 3-phase quantities can be transformed into direct-quadrature components (dq) using the *Dq0 Transform*. The Dq0 transformation is a tensor that

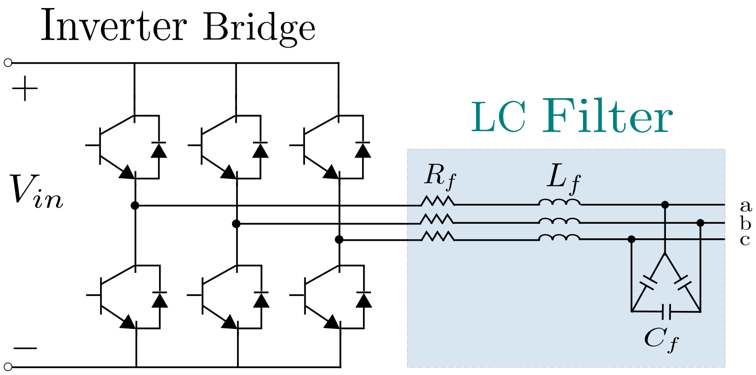

Figure 2-3: Simplified topology of a three phase inverter bridge. From [16].

maps a 3-phase quantity into two components (in the case of balanced systems) named d and q. Figure **2-2** exhibits a typical configuration for the interconnection of the zero and primary controllers.

2.1.1. The Inverter Bridge

A 3-phase inverter bridge is a standard interconnection of power transistors that converts DC voltages into a sinusoidal AC signal. The transistors are activated using a PWM scheduling, which effectively divides the signal into time slots where specific transistors should be conducting. The size of such time slots will limit the resolution of the sinusoidal output. Hence, an LC low-pass filter is required to reduce the total harmonic distortion of the output signal. Figure **2-3** shows the topology of a typical inverter bridge, including its output filter.

The design of inverter bridges is a topic of itself [16, 34, 57], and a state-of-the-art review on the matter can be found in [25] and [59].

The inverter's output line current i_l (as seen in Figure **2-2**), can be represented by its dq components, from the Dq0 transformation, and using average value modeling techniques as [9]. Equation (2-1) represents a dynamic model for the inverter, where R_f, C_f, and L_f are the resistance, the capacitance, and the inductance of the LC filter as shown in Figure **2-3**.

$$\begin{aligned}
\dot{i}_{ld} &= -\frac{R_f}{L_f} i_{ld} + \omega i_{lq} + \frac{1}{L_f} v_{id} - \frac{1}{L_f} v_{od} \\
\dot{i}_{lq} &= -\frac{R_f}{L_f} i_{lq} - \omega i_{ld} + \frac{1}{L_f} v_{iq} - \frac{1}{L_f} v_{oq}
\end{aligned} \tag{2-1}$$

Furthermore, ω is the inverter's frequency, whose estimation will be detailed later in Section 2.2.2. Currents i_{lq} and i_{ld} are the dq components of the i_l current. v_{od} and v_{oq} are the dq components of voltage v_o at the LC filter's output. v_{id} and v_{iq} are the dq components of voltage v_i in the LC filter input.

Similarly, generator's voltage and current outputs, v_o and i_o as seen in Figure **2-2**, are represented by their dq components as shown in Equations (2-2) and (2-3), respectively

$$\begin{aligned}
\dot{v}_{od} &= \omega v_{oq} + \frac{1}{C_f} i_{ld} - \frac{1}{C_f} i_{od} \\
\dot{v}_{oq} &= -\omega v_{od} + \frac{1}{C_f} i_{lq} - \frac{1}{C_f} i_{oq}
\end{aligned} \tag{2-2}$$

$$\begin{aligned}
\dot{i}_{od} &= -\frac{R_c}{L_c} i_{od} + \omega i_{oq} + \frac{1}{L_c} v_{od} - \frac{1}{L_c} v_{bd} \\
\dot{i}_{oq} &= -\frac{R_c}{L_c} i_{Lq} - \omega i_{od} + \frac{1}{L_c} v_{oq} - \frac{1}{L_c} v_{bq}
\end{aligned} \tag{2-3}$$

here, R_c and L_c are elements of the output connector shown in Figure **2-2** and explained in detail in Section 2.2.1.

Representing voltages and currents using their dq components, allows to manipulate 3-phase signals as two DC quantities, and hence making its processing much more manageable. Furthermore, the $Dq0$ transformation allows removing the time dependency of inductances as required by the performed analyses.

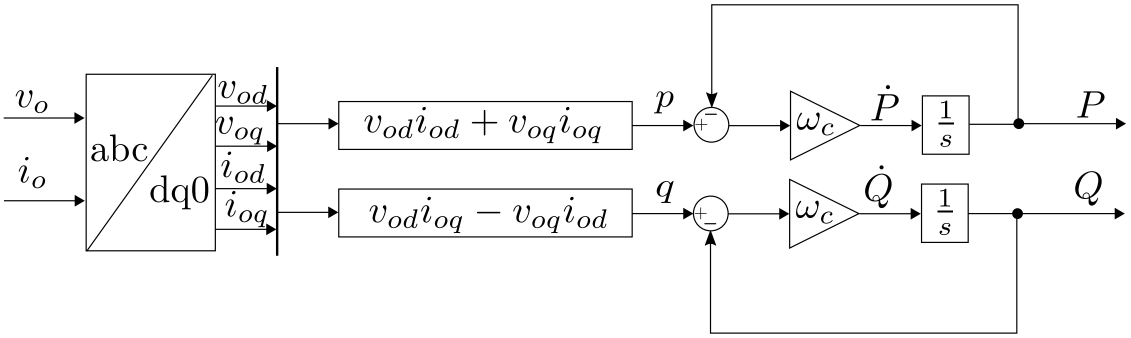

Figure 2-4: Power estimation process. From [9]

2.1.2. The Power Controller

Instantaneous measurements for active p and reactive q power, provided by Equation (2-4), are corrupted by random noise and, therefore, are not directly suitable for stable and smooth inverter's performance.

$$\begin{aligned} p &= v_{od}i_{od} + v_{oq}i_{oq} \\ q &= v_{od}i_{oq} - v_{oq}i_{od} \end{aligned} \tag{2-4}$$

Consequently, a low-pass filter with a cut-off frequency ω_c is required. Power controller's dynamics is described by Equation (2-5) in terms of the dq components,

$$\begin{aligned} \dot{P} &= \omega_c \left(-P + v_{od}i_{od} + v_{oq}i_{oq}\right) \\ \dot{Q} &= \omega_c \left(-Q + v_{od}i_{oq} - v_{oq}i_{od}\right) \end{aligned} \tag{2-5}$$

where $\dot{P}$ and $\dot{Q}$ are the first-order derivatives of P and Q, the inverter's estimated active and reactive power, respectively. Figure **2-4** illustrates the power estimation process for P and Q.

As seen in Figure **2-2**, the voltage reference v_o^* can be estimated from the voltage V and the frequency ω, as in Equation (2-6),

$$v_o^* = \sqrt{2}\,V \sin \omega t \tag{2-6}$$

where ω and V are set to be linearly proportional to the estimated P and Q respectively, with proportionality constants K_p and K_q. This strategy is known as **droop control**. Equation (2-7) shows the dq components of v_o^*

$$\begin{aligned} v_{od}^* &= \quad V^* - K_q Q \\ v_{oq}^* &= \quad 0 \end{aligned} \tag{2-7}$$

where V^* is the external reference for the inverter output voltage, i.e., the voltage at which the microgrid is intended to operate. Equation (2-8) shows the estimated frequency

$$\omega = \omega^* - K_p P \tag{2-8}$$

where ω^* is the external reference for the inverter output frequency, i.e., the frequency at which the microgrid is intended to operate.

The power controller is also known as the **Primary Control**. Its main task is to provide voltage and frequency references to the **Zero Controller**, which is the low-level controller in charge of regulating output voltage and output current. Figure **2-2** shows sections corresponding to each controller. The components of the zero controller will be detailed in Sections 2.1.3 and 2.1.4.

2.1.3. The Voltage Controller

The voltage controller has the goal of tracking the reference voltage defined by the power controller, which is generally a decoupled PI (Proportional Integral) controller, as shown in Figure **2-5**. PI controllers are based on error measurements and their integrals, as defined in Equation (2-9).

$$\begin{aligned} \dot{\epsilon}_{vd} &= v_{od}^* - v_{od} \\ \dot{\epsilon}_{vq} &= v_{oq}^* - v_{oq} \end{aligned} \tag{2-9}$$

The voltage controller defines the current set-point for the inverter bridge, and its behavior is given by Equation (2-10)

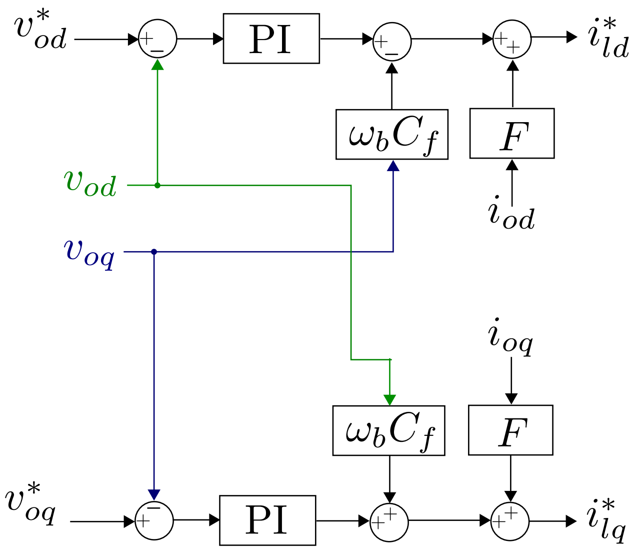

Figure 2-5: Voltage controller. From [9]

$$\begin{aligned} i_{ld}^* &= F i_{od} - \omega_b C_f v_{oq} + K_{PV}(v_{od}^* - v_{od}) + K_{IV}\epsilon_{vd} \\ i_{lq}^* &= F i_{oq} + \omega_b C_f v_{od} + K_{PV}(v_{oq}^* - v_{oq}) + K_{IV}\epsilon_{vq} \end{aligned} \quad (2\text{-}10)$$

where F is the transition matrix in the dynamic model, ω_b is the nominal angular frequency, and C_f is the capacitance value of the LC filter from Figure **2-3**. K_{PV} and K_{IV} are the proportional and integrative gains of the voltage PI controller, respectively. ϵ_{vd} and ϵ_{vq} are the auxiliary state variables of the PI controller.

2.1.4. The Current Controller

Finally, the structure of the current control is similar to the voltage controller. Figure **2-6** shows the scheme, and Equation (2-11) defines the error measurements and its integrals.

$$\begin{aligned} \dot{\epsilon}_{id} &= i_{od}^* - i_{od} \\ \dot{\epsilon}_{iq} &= i_{oq}^* - i_{oq} \end{aligned} \quad (2\text{-}11)$$

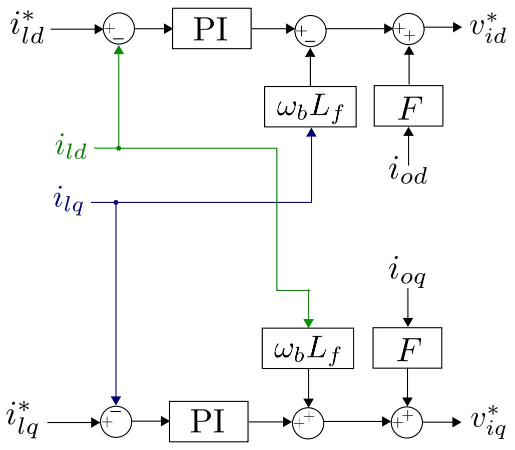

Figure 2-6: Current controller. From [9]

The current controller defines the sinusoidal wave for the inverter bridge v_i^*, and its behavior is given by Equation (2-12)

$$\begin{aligned} v^*_{id} &= -\omega_b C_f i_{lq} + K_{PI}(i^*_{od} - i_{od}) + K_{II}\epsilon_{id} \\ v^*_{iq} &= \omega_b C_f i_{ld} + K_{PI}(i^*_{oq} - i_{oq}) + K_{II}\epsilon_{iq} \end{aligned} \tag{2-12}$$

where K_{PI} and K_{II} are the proportional and integrative gains of the current PI controller, respectively. ϵ_{id} and ϵ_{iq} are the auxiliary state variables of the PI controller.

2.1.5. Compact Model of the Controller

The compact, non-linear model of an inverter can be seen in Equation (2-13)

$$\dot{\mathbf{x}} = \mathbf{f_i}\left(x_i\right) + \mathbf{k_i}\left(x_i\right)\mathbf{D_i} + \mathbf{g_i}\left(x_i\right)u_i \tag{2-13}$$

where the state vector x_i is defined as

$$x_i = [\delta, P_i, Q_i, \epsilon_{vdi}, \epsilon_{vqi}, \epsilon_{iqi}, \epsilon_{iqi}, i_{ldi}, i_{lqi}, v_{odi}, v_{oqi}, i_{odi}, i_{oqi}] \tag{2-14}$$

and D_i is defined as

$$D_i = [\omega_{com}, V_{bdi}, V_{bqi}] \tag{2-15}$$

where, V_{bdi} and V_{bqi} are the dq components of V_b, the voltage value in the AC bus as illustrated in Figure **2-7**(b). ω_{com} is the common reference frequency.

The input vector u_i is defined as $u_i = [\omega^*, V^*]$, where ω^* and V^* are the frequency and voltage references, respectively.

Therefore, the vector $\dot{\mathbf{x}}$ is simply the first derivative of x_i given by Equation (2-14). The transition matrix $\mathbf{f_i}$ has the non-linear form of Equation (2-16) and can be derived from Equations (2-3), (2-5), (2-7), (2-10), (2-11), and (2-12).

$$\begin{bmatrix}
-K_{pi} & & & & & & & & & \\
-\omega_{ci} & & & & & & & & \omega_{ci}v_{odi} & \omega_{ci}v_{oqi} \\
 & -\omega_{ci} & & & & & & & \omega_{ci}v_{oqi} & -\omega_{ci}v_{odi} \\
 & -K_{qi} & & & & & -1 & & & \\
 & & & & & & & -1 & & \\
 & & & & & & & & -1 & \\
 & & & & & & & & & -1 \\
 & -K_{pvi}K_{qi} & K_{ivi} & & & & -K_{pvi} & -\omega_b C_{fi} & F_i & \\
 & & & K_{ivi} & & & \omega_b C_{fi} & -K_{pvi} & & F_i \\
 & & & & \frac{1}{C_{fi}} & & & \omega_i & -\frac{1}{C_{fi}} & \\
 & & & & & \frac{1}{C_{fi}} & -\omega_i & & & -\frac{1}{C_{fi}} \\
 & & & & & & \frac{1}{L_{ci}} & & -\frac{R_{ci}}{L_{ci}} & \omega_i \\
 & & & & & -\frac{R_{ci}}{L_{ci}} & & \frac{1}{L_{ci}} & -\omega_i &
\end{bmatrix} \tag{2-16}$$

and the rest of the equation: $+\mathbf{k_i}\,(x_i)\,\mathbf{D_i}\,+\,\mathbf{g_i}\,(x_i)\,u_i$ is given by:

$$
+\begin{bmatrix} -1 & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & & \\ & \frac{-1}{L_{ci}} & \\ & & \frac{-1}{L_{ci}} \end{bmatrix}\begin{bmatrix} \omega_{com} \\ V_{bdi} \\ V_{bqi} \end{bmatrix}+\begin{bmatrix} 1 & \\ & \\ & \\ & \\ & \\ & \\ & \\ & K_{pvi} \\ & 0 \\ & 0 \\ & 0 \\ & 0 \\ & 0 \end{bmatrix}\begin{bmatrix} \omega_i^* \\ V_i^* \end{bmatrix} \tag{2-17}
$$

2.2. The Branch Connection Model

The branch connection refers to the coupling elements between the nodes and the bus. Given the deviations between the generator parameters (voltage and frequency) and the bus parameters, these elements behave as a damping interface between the generator and the central bus (network).

2.2.1. The Output Connector

The output connector is a series connection of a resistor and an inductor connected between the output of the generator whose voltage is v_o and the bus whose voltage is v_{bus}, it couples these components properly and mitigates the effects of voltage and frequency deviations. Figure **2-2** shows a detailed representation of the output connector, and Figure **2-7** shows a diagram for modeling effect, here, the generator is connected to the common bus through a coupling impedance Z. The purpose is to illustrate how the power flows from the generator to the bus.

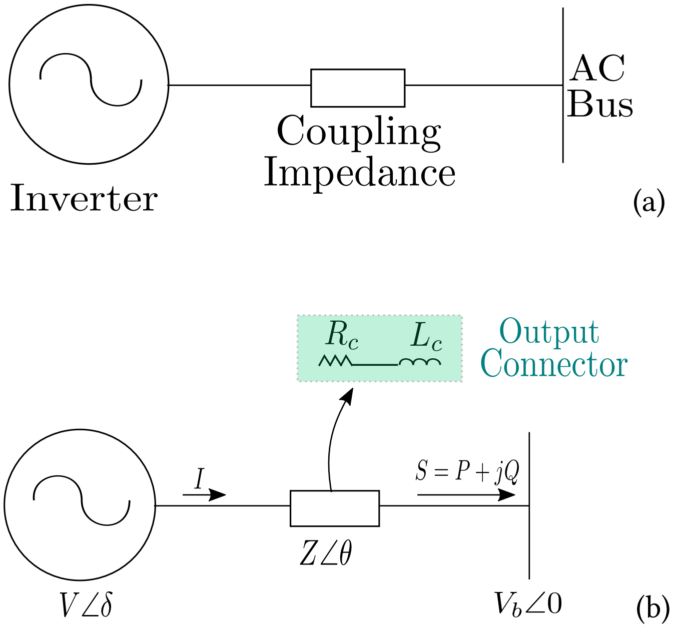

Figure 2-7: Inverter connected to the AC common bus.

2.2.2. Power Equations

The power $\mathbf{S}$ provided from the generator to the common bus is shown in Equation (2-20).

From the definition of apparent power

$$\mathbf{S} = \mathbf{V}\mathbf{I}^* \tag{2-18}$$

where $\mathbf{V}$ is the voltage at the common bus ($V_{bus}\angle 0$), and $\mathbf{I}$ is defined by Equation (2-19)

$$\mathbf{I} = \mathbf{I_z} = \frac{\mathbf{V_z}}{\mathbf{Z}} \tag{2-19}$$

where;

$$
\begin{aligned}
\mathbf{V_z} = &\ V\angle\delta - V_{bus}\angle 0 \\
\mathbf{I} = &\ \frac{V\angle\delta - V_{bus}\angle 0}{Z\angle\theta} \\
\mathbf{I} = &\ \frac{V\angle\delta}{Z\angle\theta} - \frac{V_{bus}\angle 0}{Z\angle\theta} = \left(\frac{V}{Z}\angle\delta - \theta\right) - \left(\frac{V_{bus}}{Z}\angle - \theta\right) \\
\mathbf{I}^{*} = &\ \left(\frac{V}{Z}\angle\theta - \delta\right) - \left(\frac{V_{bus}}{Z}\angle\theta\right) \\
\mathbf{S} = &\ V_{bus}\angle 0\left(\left(\frac{V}{Z}\angle\theta - \delta\right) - \left(\frac{V_{bus}}{Z}\angle\theta\right)\right) \\
\mathbf{S} = &\ \left(\frac{V_{bus}V}{Z}\angle\theta - \delta\right) - \left(\frac{V_{bus}^2}{Z}\angle\theta\right)
\end{aligned}
$$

finally,

$$\mathbf{S} = \frac{V_{bus}V\angle\theta - \delta}{Z} - \frac{V_{bus}^2\angle\theta}{Z}. \tag{2-20}$$

From Equation (2-20) is possible to find the expressions for active and reactive power P and Q as it is shown below in Equation (2-21)

$$
\begin{aligned}
P &= \tfrac{V_{bus}V\cos(\theta-\delta)}{Z} - \tfrac{V_{bus}^2\cos(\theta)}{Z} \\
Q &= \tfrac{V_{bus}V\sin(\theta-\delta)}{Z} - \tfrac{V_{bus}^2\sin(\theta)}{Z}.
\end{aligned} \tag{2-21}
$$

Now, taking for example an output connector predominantly inductive $\theta \approx 90^{\circ}$, and taking into account that

$$
\begin{aligned}
\cos(\alpha) &= \sin(90^{\circ} - \alpha) \\
\sin(\beta) &= \cos(90^{\circ} - \beta)
\end{aligned} \tag{2-22}
$$

expressions in Equation (2-21) can be reduced to

$$\begin{aligned} P &= \frac{V(V_{bus})}{Z}\sin(\delta) \\ Q &= \frac{V(V_{bus})\cos(\delta)-(V_{bus})^2}{Z}. \end{aligned} \tag{2-23}$$

According to Equation (2-23) the active power has a strong connection with the generator output phase, while reactive power depends on its voltage. Equation (2-24) shows these relationships, which are known as the droop model, and they are specially used to design controllers, like the one shown in Figure **2-2** [39].

$$\begin{aligned} \omega &= \omega^* - K_p P \\ V &= V^* - K_q Q \end{aligned} \tag{2-24}$$

3 Control Strategies for Microgrids

In a distributed power grid, the control system's main task is to guarantee the stable operation of the network. Also, in the case of microgrids, the control system protects the network from overloads in the generators and inverters [14]. The most common control schemes for microgrids consist of a hierarchical structure, usually composed of three levels: primary, secondary, and tertiary control [11].

Primary control schemes do not require communication among the agents of the network; thus, they can work seamlessly in a decentralized, centralized, or distributed way. However, it is more usual to find decentralized schemes at this level [14].

Regarding the secondary and tertiary control, a specific exchange of information among the agents, all over the network, becomes essential. Some implemented architectures include both centralized and distributed control. The centralized control is a conventional topology used in both secondary and tertiary levels. This topology is usually fully-connected and bidirectional, which makes it robust, but not scalable, and might introduce a single point of failure [43, 45]. Cooperative and distributed control emerge as important communication topologies - the latter with sparse networks and some significant advantages such as scalability and flexibility, but without global knowledge of the system. The lack of a comprehensive understanding of the system leads to a proper environment for cyber-attacks [1].

This chapter describes each control level in detail, and it is organized as follows. Section 3.1 provides general concepts of the primary control, the equations for stable levels of voltage and frequency, and the power-sharing equations. Section 3.2 describes secondary control schemes and the equations to compensate deviations of frequency and voltage. Finally, Section 3.2 provides a general description of tertiary control objectives, although not in deep since this is not the focus of this work.

3.1. Primary Control

The primary control performs five basic tasks: 1) To mitigate undesired circulating currents in the inverter. 2) To stabilize voltage and current values after the islanding process. 3) To guarantee the plug and play capability of the inverters during voltage and current changes due to variations in generated and demanded power. 4) To regulate voltage and current values at the inverter output. Finally, 5) To ensure proper power-sharing among the Distributed Generators (DGs).

Furthermore, the primary control also embeds the *Zero Control*, which is responsible for the internal control of voltage and current of the inverter, and it is performed in two possible modes; *PQ Control Mode* or *Voltage Control Mode*. Figure **3-1** summarizes the primary control tasks aforementioned.

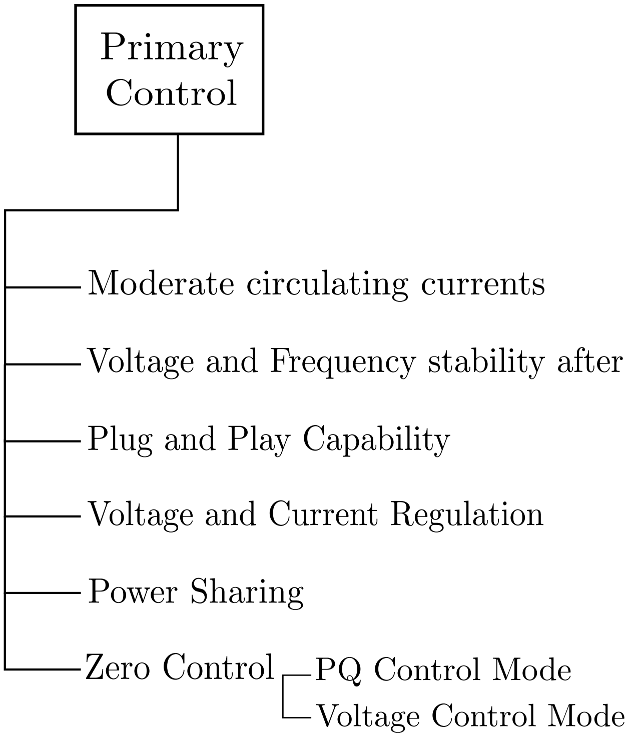
Primary Control
Moderate circulating currents
Voltage and Frequency stability after islanding process
Plug and Play Capability
Voltage and Current Regulation
Power Sharing
Zero Control
PQ Control Mode
Voltage Control Mode

Figure 3-1: Primary control functions.

In this section, the *Droop Control* is introduced, which is a specific and typical scheme of primary control. The droop control is widely used due to its autonomy and independence features. As in other primary control strategies, communication among the inverters is not required for droop control [11]. Particular to droop control, the variables locally measured are the active power P,

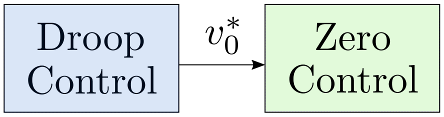

Figure 3-2: Primary control and zero Control.

and the reactive power Q, whose control must guarantee a satisfactory operation of the system and a proper power-sharing among the inverters.

3.1.1. Zero Control

As mentioned in Section 3.1, the zero control is in charge of regulating the internal levels of voltage and current in the inverter. There are two basic control modes, the PQ mode, and the Voltage Control mode.

The **PQ control mode**, uses a current-controlled voltage source (CCVSI), in order to reach the set-points for active and reactive power. In other words, the inverter can be seen as a voltage source controlled by currents. These currents are the active and reactive current, i.e., i_p and i_q, respectively [33, 11]. The active power in the inverter varies, causing voltage deviations. A *PI* control is used to correct this deviation adjusting the active current i_q.

The **Voltage control mode** uses a voltage-controlled voltage source inverter (VCVSI). The inverter can be seen as an AC source. P and Q are controlled through the frequency and voltage droop characteristics, respectively. This control mode requires an input voltage reference v_0^*, provided through droop characteristics, as illustrated in Figure **3-2**. The scheme of this control mode will be used in this work to model the inverter operation and is also the scheme used in Figure **2-2**.

3.1.2. Primary Frequency Control

One of the variables to control is the active power, P, whose behavior directly affects the power angle, and this, in turn, affects the performance of the system frequency [14, 11]. This relationship is described through frequency droop characteristics, as shown in Equation (3-1)

$$\omega = \omega^* - K_p P. \tag{3-1}$$

A decrease in the frequency value indicates that there is an increase in the load. In consequence, the active power, P, must increase through the adjustment of the generator torque.

For n inverters, the angular frequency of the inverter i is defined in Equation (3-2)

$$\omega_i = \omega_i^* - K_{pi}P_i \tag{3-2}$$

where ω_i^* is the reference angular frequency of inverter i in $[rad/s]$ provided by the secondary control. K_{pi} is the active power droop coefficient, given by design through algorithms or any heuristic technique. Droop control uses a criterion known as power-sharing, detailed in Equation (3-3), which allows for some accepted frequency fluctuation. P_i is the average active power (RMS) in the inverter i [11].

The primary control ensures that each inverter supplies energy according to their active power maximum value. This task is called power-sharing, and Equation (3-3) describes this relationship

$$Kp_1P_1 = Kp_2P_2 = Kp_iP_i = \cdots = Kp_jP_j = \Delta\omega_{max} \tag{3-3}$$

where $\Delta\omega_{max}$ is the maximum allowed frequency variation in the microgrid. Equation (3-3) is equivalent to have

$$\frac{P_1}{P_{max1}} = \frac{P_2}{P_{max2}} = \frac{P_i}{P_{maxi}} = \cdots = \frac{P_j}{P_{maxj}} = \Delta\omega_{max}. \tag{3-4}$$

3.1.3. Primary Voltage Control

Since the voltage is not a global value in the system, the reactive power Q affects its behavior. Equation (3-5) shows this relationship [9].

$$V = V^* - K_qQ \tag{3-5}$$

For n inverters, the droop characteristic of the inverter i voltage is defined as

$$V_i = V_i^* - K_{qi}Q_i \tag{3-6}$$

where V_i^* is the reference voltage of the inverter i in $[Volts]$ provided by the secondary control. K_q is the reactive power droop coefficient, given by design, through algorithms or any heuristic technique, as in the frequency control. In this case, power-sharing will allow for some accepted voltage fluctuation detailed in Equation (3-7). Q_i is the average reactive power (RMS) in the inverter i [11]

$$Kq_1 Q_1 = Kq_2 Q_2 = Kq_i Q_i = \cdots = Kq_j Q_j = \Delta V_{max} \tag{3-7}$$

where ΔV_{max} is the maximum allowed variation of voltage in the microgrid. Equation 3-7 is equivalent to have

$$\frac{Q_1}{Q_{max1}} = \frac{Q_2}{Q_{max2}} = \frac{Q_i}{Q_{maxi}} = \cdots = \frac{Q_j}{Q_{maxj}} = \Delta V_{max}. \tag{3-8}$$

When the voltage value is different from the reference, the excitation magnetic field of the synchronous generator changes. In consequence, the reactive power changes making the voltage reach the reference value.

3.2. Secondary Control

The secondary control level in the hierarchy possesses a slower response (in the order of minutes) than the primary control. This situation allows for the restoring of voltage and frequency drifts caused by the primary control (droop method in this case) [35, 39]. Equations (3-2) and (3-6) from the primary control are modified for a secondary term as follows

$$\omega_i = \omega_i^* - K_{pi} P_i + \delta_\omega \tag{3-9}$$

$$V_i = V_i^* - K_{qi} Q_i + \delta_V. \tag{3-10}$$

The secondary terms δ_ω and δ_V represent the error signals for frequency and voltage, respectively.

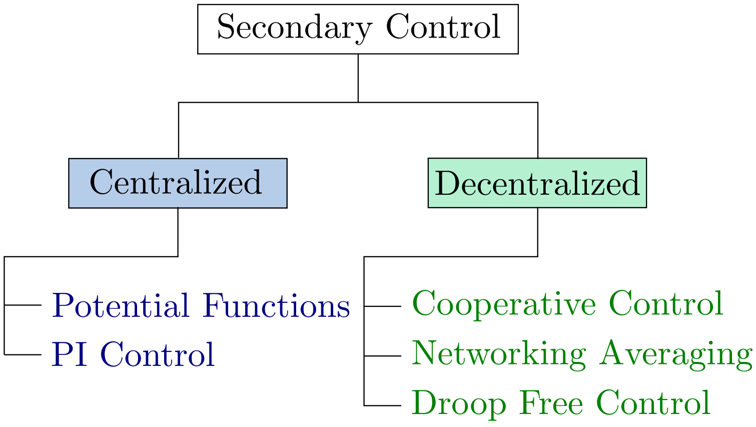

Figure 3-3: Secondary control variations.

Secondary control is performed through different strategies, either centralized as in [33, 23, 7, 35] or decentralized as in [11, 52]. Conventionally, it has been used centralized strategies, some of them are: (1) one based on a proportional-integrative (PI) control [23], and (2) an optimization-based control with potential functions [35]. On the other hand, some decentralized strategies are: (1) the networking averaging based on a PI control [52], (2) the droop free control [42], and (3) the consensus-based cooperative control [10]. These variations of secondary control are summarized in Figure **3-3**.

Centralized Control Strategies

The centralized strategy based on a **PI control** to determine the frequency error and the voltage magnitude error, $\delta\omega$, and δV, is described through Equations (3-11) and (3-12), respectively [23]

$$\delta\omega_i = K_{P_\omega}\left(\omega_{ref} - \omega\right) + K_{I_\omega}\int\left(\omega_{ref} - \omega\right)\mathrm{dt} + \Delta\omega_s \tag{3-11}$$

$$\delta V_i = K_{P_V}\left(V_{ref} - V\right) + K_{I_V}\int\left(V_{ref} - V\right)\mathrm{dt} \tag{3-12}$$

where, K_{P_ω}, K_{I_ω}, are the proportional and integrative constants of the PI frequency control. K_{PV}, and K_{I_V} are the proportional and integrative constants of the PI voltage control. ω_{ref} and V_{ref} are the reference values for frequency and voltage, respectively. These reference values are provided from different sources according to the connection mode of the microgrid, as explained later in Section 3.4. $\Delta\omega_s$ is a term that allows the synchronization frequency of the microgrid, also explained in Section 3.4.

The other centralized strategy based on optimization techniques uses **potential functions**, $\phi\left(.\right)$, providing information about the microgrid state and how far is the actual state from the desired. $\phi\left(.\right)$ as an optimization function, presents information about the measurements of the inverter i (provided by the state vector x_i), the control goals, and constraints, denoted with the superscripts u, g, and c, respectively. The potential function of the inverter i is defined in Equation (3-13), [35]

$$\phi_i(x_i) = w^u \sum_{i=1}^{n_u} p_i^u(x_i) + w^c \sum_{i=1}^{n_c} p_i^c(x_i) + w^g p_i^g(x_i) \tag{3-13}$$

where the term p denotes a potential function and w denotes the weight of the corresponding potential function.

The state vector x_i is given by

$$x_i = [P_i, Q_i, V_i, i_i]$$

where P_i, Q_i, V_i, and i_i are the measurements values of the active power, the reactive power, the voltage and the current of the secondary control, respectively.

However, centralized structures of control exhibit some significant disadvantages, such as the possibility of a total system destabilization as a consequence of a failure in the central controller (single-point of failure). Furthermore, centralized schemes are not flexible, have limited scalability, and require a very robust communication system [1, 52].

Decentralized Control Strategies

Distributed secondary control strategies appear as an outstanding alternative to alleviate most of the centralized structure's problems. These schemes have individual controls in each DG, so in order to reach an instability that breaks down the entire system, all the nodes would have to fail or be simultaneously attacked, which is highly improbable. That is why distributed strategies result in a superior alternative to the centralized ones. However, distributed schemes suffer from other significant weaknesses. Most of these weaknesses are related to cyber-vulnerabilities, which have been subject to several studies [1]. Some of these weaknesses are approached in this work.

The decentralized strategy of **networking averaging** use a PI control to update the error signals for frequency, voltage magnitude, and reactive power, as described in Equations (3-14), (3-15), and (3-16), respectively [52]

$$\delta\omega_i = K_{P_\omega}\left(\omega_{ref} - \overline{\omega}_i\right) + K_{I_\omega}\int\left(\omega_{ref} - \overline{\omega}_i\right)\mathrm{dt} \tag{3-14}$$

$$\delta V_i = K_{P_V}\left(V_{ref} - \overline{V}_i\right) + K_{I_V}\int\left(V_{ref} - \overline{V}_i\right)\mathrm{dt} \tag{3-15}$$

$$\delta Q_i = K_{P_Q}\left(Q_i - \overline{Q}_i\right) + K_{I_Q}\int\left(Q_i - \overline{Q}_i\right)\mathrm{dt} \tag{3-16}$$

where ω_{ref} (V_{ref}) is the reference frequency (voltage) value in the microgrid (see Section 3.4 for more detail), Q_i is the reactive power of the inverter i. $\overline{\omega}_i$ ($\overline{V}_i$, $\overline{Q}_i$), is the averaging term, that in every sample time, gathers the received measurements of frequency (voltage, reactive power) from all the inverters and averages them, as defined in Equation (3-17) ((3-18), (3-19)). Then the secondary control signal $\delta\omega$ (δV, δQ) is updated for every inverter.

$$\overline{\omega}_i = \frac{\sum_{k=1}^{n}\omega_k}{k} \tag{3-17}$$

$$\overline{V}_i = \frac{\sum_{k=1}^{n}V_k}{k} \tag{3-18}$$

$$\overline{Q}_i = \frac{\sum_{k=1}^{n}Q_k}{k} \tag{3-19}$$

where, $i = 1, 2, ..., N$ with N the total number of inverters. $k = 1, 2, ..., n$ with n the total number of measurements in a sample-time.

The other decentralized strategy known as **distributed cooperative control** emerges as a method based on consensus algorithms that makes the secondary control more reliable. The concept of “distributed”, means that each agent works with its own, and neighbors’ information. Unlike distributed strategies, the “cooperative” term, introduce the concept of making every agent works for a collective purpose [11, 8]. This secondary control approach is used in this work and is explained detailed in Chapter 5. The cooperative control laws for frequency and voltage are defined as follows in Equations (3-20) and (3-21), respectively [9]

$$e_{\omega_i}\left(t\right) = \sum_{j\in N_i} a_{ij}\left(\omega_i\left(t\right) - \omega_j\left(t\right)\right) + g_i\left(\omega_i\left(t\right) - \omega_{ref}\right) \tag{3-20}$$

$$e_{v_i}\left(t\right) = \sum_{j\epsilon N_i} a_{ij}\left(V_i\left(t\right) - V_j\left(t\right)\right) + g_i\left(V_i\left(t\right) - V_{ref}\right) \tag{3-21}$$

from where it is defined an additional control input $u_{\omega i}$ and u_{vi} for (3-20) and (3-21), respectively

$$u_{\omega_i}\left(t\right) = -c_\omega e_{\omega_i}\left(t\right) \tag{3-22}$$

$$u_{v_i}\left(t\right) = -c_v e_{v_i}\left(t\right) \tag{3-23}$$

finally the frequency and voltage set-points provided to the primary control are defined as follows [8]

$$\omega_i^* = \int \left(u_{\omega_i}\left(t\right) + K_{pi}\dot{P}_i\right) \mathrm{dt} \tag{3-24}$$

$$V_i^* = \int \left(u_{v_i}\left(t\right) + K_{qi}\dot{Q}_i\right) \mathrm{dt} \tag{3-25}$$

where $\dot{P}_i$ and $\dot{Q}_i$ is find with Equation 2-5.

Equations (3-1) and (3-6) in the primary control are updated with the term ω_i^* and V_i^*. Equations (3-9) and (3-10) are not considered in this control approach.

To summarize the interaction between primary and secondary control in this strategy, Figure **3-4** illustrates this synergy.

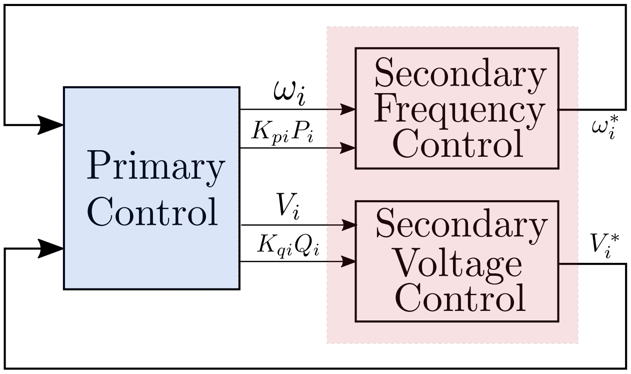

Figure 3-4: Primary and secondary control synergy for the cooperative control approach.

3.3. Tertiary Control

Tertiary Control is mainly meant to perform optimal economic dispatch of the DGs, the other tasks such as the control of the power flow are mostly required for the grid-connected mode [7, 9, 39]. For example, in Equations (3-2) and (3-6), the terms ω_i and V_i are provided for the tertiary control in grid-connected mode. In islanded mode, these values are set as $2\pi \times 60$ rad/s and V_i is set as the nominal voltage of the microgrid [9].

Tertiary control leads the system to optimize the generated power according to demand and the energy availability criteria, which usually involves monetary cost [24].

For more information about tertiary control, go to [7, 58, 55, 60].

3.4. Islanded vs Connected - grid Microgrids

In the *islanded mode*, primary and secondary levels of control receive the feedback signals from the microgrid. In the *grid-connected mode* the set-point signal for the tertiary control is provided from the main grid [11].

As was explained in Section 3.3, in *connected mode*, references for voltage and angular frequency are externally imposed from the main grid. Hence, ω_{ref} in Equations (3-11), (3-14), and (3-20); and V_{ref} in Equations (3-12), (3-15), and (3-21) are either imposed for the main grid or set internally for the same microgrid. Those variations depend on the connection mode, as is illustrated in

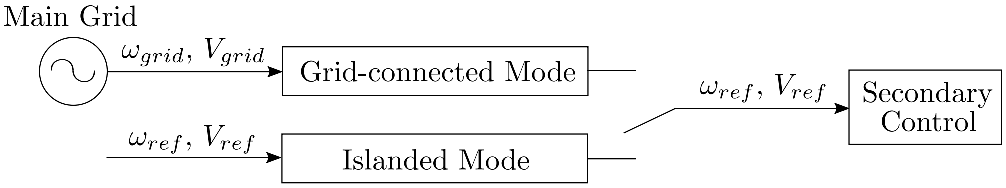
Main Grid
ω_{grid}, V_{grid}
Grid-connected Mode
ω_{ref}, V_{ref}
Islanded Mode
ω_{ref}, V_{ref}
Secondary Control

Figure 3-5: Reference values of frequency and voltage for both islanded and connected mode.

Figure **3-5**.

Similarly, Equations (3-2) and (3-6) for the secondary control are modified as follows [33].

$$\omega_i^* = \omega_{grid} + K_{pi}P_i \tag{3-26}$$

$$V_i^* = V_{grid} + K_{qi}Q_i \tag{3-27}$$

where P_i and Q_i are the desired outputs, which are reached adjusting ω_{0i} and V_{0i} through Equations (3-26) and (3-27), respectively.

From Equation (3-11) the term $\Delta_{\omega s}$ is set as zero in *islanded mode.* In *grid connected mode* this term allows the synchronization of the microgrid with the main grid, and is provided through a PLL (phase-locked loop) [9].

4 Models of Sophisticated Attacks on Islanded Microgrids

Distributed control systems used in microgrids have incorporated power electronic devices with an important component of information technology (IT). This fact makes smarter systems (such as microgrids) possible, but at the same time, make them systems prone to cyber-attacks, and software failures [3, 1]. For an attacker, it is almost impossible to compromise the entire data from the metering devices. However, partial information knowledge is enough to cause desynchronization on inverters, and in some cases, the partial or total breakdown of the system [31].

Cyber-attacks subject is not a new topic of interest. Systems with critical cyber-layer such as PLCs-based systems (e.g., SCADA systems), and computer-based systems, have been attacked with devastating consequences [54]. SCADA systems are used in an extensive amount of utilities, such as electric, water, gas, oil, and other systems. Hence, the study of its vulnerability is a topic of high interest. In particular, power grids are susceptible to attacks since these are communication and computer-based multi-agent systems. Frequent attacks are performed like actions that can destabilize the system. Some basic techniques based on noise filtering and disturbances attenuation methods are used to mitigate the effects of these attacks. However, strategically designed attacks such as data corruption and hijacking actions cannot be treated with these basic techniques to hold normal operation of the system under attack.

In case an agent presents a non-adequate behavior, it is possible to identify it and remove it [46, 47]. However, it is required the knowledge of the whole communication network, which makes it a non-scalable solution.

Current studies of attacks in microgrids are focused on the alteration of exchanged information through; 1) the communication links, and 2) the controllers. In 2), the attack can be performed either on their sensors/actuators, which is a physical attack; or in a real set-point. Techniques used to solvent these disturbances are designed to verify the veracity of data in centralized structures. Therefore, for the case of distributed control systems, these techniques are not adequate [3, 46, 47].

Among the techniques applied in distributed control systems, are the game-theoretic approaches, such as non-cooperative strategies, see [3, 20] for more details. Other approaches like the used in [31] model an attack of local load redistribution based on incomplete information, which demonstrates that an attacker can inject false data in smart meters with the knowledge of local information without being detected for the state estimator.

The distributed controllers for islanded AC microgrids have usually limited communication among inverters, as described in Section 3.2. This fact makes them prone to malicious attacks with corrupt constant signals. Therefore, the study of distributed resilient protocols for the cooperative secondary control of islanded AC microgrids, become essential for the scientific community.

4.1. Controller Attacks

Controller attacks could be both cybernetic or physical, according to the specific element disturbed. If the attack is carried out over a sensor/actuator, then it is a physical attack. However, if the affected components are loops like communication links considered in Section 4.2 or the set-points computed with information received from the communication links, it is considered a cybernetic attack.

Another controller attack consists of sending a shutdown command to the controllers. In the area of control, this type of attack is not considered, given that it is not possible to compute or apply any control signal to extinguish the effects of the attack.

4.1.1. Offsetting the Controller Set-points

The offsetting attack consists of applying an offset to certain signals, i.e., the addition of a constant value to these signals. Equation (4-1) defines a mathematical model for the **voltage set-point offsetting attack**

$$V_s = V_c + \mu_{aV} V_a \tag{4-1}$$

where V_a is the offset value, usually a small quantity of corrupt voltage, μ_{aV} is a binary factor that indicates the presence or absence of an attack, whose value is '1' in presence of an attack and ‘0’ in normal operation. V_c is the voltage set-point, computed with the consensus control law, introduced in Chapter 3, from the information received of the communication links. Finally, V_s is the inner controller set-point for voltage.

Similarly, Equation (4-2) defines a mathematical model for the **frequency set-point offsetting attack**

$$\omega_s = \omega_c + \mu_{a\omega}\omega_a \tag{4-2}$$

where ω_a is a small value of offset, that represents the corrupt frequency value added to the original signal. $\mu_{a\omega}$ is a binary factor that indicates the presence or absence of an attack, whose value is ‘1’ in presence of an attack and ‘0’ in normal operation. ω_c is the reference value provided by the secondary control to the primary. Finally, ω_s is the frequency at the inverter that can be corrupted or not according to the $\mu_{a\omega}$ indicator.

4.1.2. Hijacking the Entire Controller

The hijacking attack is more drastic than the attack described in Subsection 4.1.1. This attack consists of changing the entire set-point in the controller. Equation (4-3) defines a mathematical model of **voltage set-point hijacking attack**

$$V_s = V_c^{(1-\mu_{hV})} V_h^{\mu_{hV}} \tag{4-3}$$

where V_h is the corrupt voltage value, it is assumed that the attacker defines it. μ_{hV} is a binary factor that indicates the presence or absence of an attack, whose value is ‘1’ in presence of an attack and ‘0’ in normal operation. V_c is the reference voltage in the primary control provided by the secondary control with the information received from the communication links (see Chapter 3). Finally, V_s is the inverter voltage, which can be corrupted or not according to the μ_{hV} indicator, i.e., V_s equals V_c when $\mu_{hV} = 0$, and equals V_h when $\mu_{hV} = 1$.

Similarly, Equation (4-4) defines a mathematical model of **frequency set-point hijacking attack**

$$\omega_s = \omega_c^{(1-\mu_{h\omega})} \omega_h^{\mu_{h\omega}} \tag{4-4}$$

where ω_h is the corrupt frequency value, it is assumed that the attacker defines it. $\mu_{h\omega}$ is a binary factor that indicates the presence or absence of an attack, whose value is '1' in presence of an attack and '0' in normal operation. ω_c is the reference voltage in the primary control provided by the secondary control with the information received from the communication links (see Chapter 3). Finally, ω_s is the frequency at the inverter that can be corrupted or not according to the $\mu_{h\omega}$ indicator. ω_s equals ω_c when $\mu_{h\omega} = 0$, and equals ω_h when $\mu_{h\omega} = 1$.

4.1.3. Sensor/Actuator Compromised

The sensor/actuator attacks are related to disturbances that affect the physical elements directly. These disturbances can be modeled of two forms; additive altering (offsetting) attacks and hijacking attacks.

Equation (4-5) defines a model for the **offsetting attack** [46, 47]

$$u = u_c + \mu_{asa} u_a \tag{4-5}$$

where u_a is the injected disturbance to the physical variable. μ_{asa} is a binary factor that indicates the presence or absence of an attack, whose value is '1' in presence of an attack and '0' in normal operation. u_c is the control signal in the actuator computed by the controller, i.e., the real sensor value. Finally, u is the primary control signal, i.e., the measured value.

Equation (4-6) describes a model for a **hijacking attack**

$$u = u_c^{(1-\mu_{hsa})} u_h^{\mu_{hsa}} \tag{4-6}$$

where u_h is the injected disturbance to the physical variable. μ_{hsa} is a binary factor that indicates the presence or absence of an attack, whose value is '1' in presence of an attack and '0' in normal operation. u_c is the control signal in the actuator computed by the controller, i.e., the real sensor value. Finally, u is the primary control signal, i.e., the measured value.

4.2. Communication Links Attacks

The attacks performed over communication links are considered cybernetics, which can be carried out remotely. An example of this type of attack consists of degenerating the information through the communication links.

Another controller attack consists of breaking the entire communication link. In the area of control, this type of attack is not considered, given that it is not possible to compute or apply any control signal to extinguish the effects of the attack.

Communication links attacks can be classified, too, as offsetting or hijacking attacks.

4.2.1. Offsetting the Communication Data

The communication data offsetting attack consists of modifying the signals sent across the communication links. This action is performed applying an offset, i.e., the addition of a constant value to these signals. Equation (4-7) defines a model for the **frequency set-point offsetting attack in the communication link**

$$\omega_r = \omega_t + \lambda_{a\omega}\omega_a \tag{4-7}$$

where ω_r is the frequency value read from the communication link. ω_t is the measured frequency communicated by the inverter. $\lambda_{a\omega}$ is a binary factor that indicates the presence or absence of an attack, whose value is '1' in the presence of an attack and '0' in normal operation. Finally, ω_a is a corrupt frequency offset defined by the attacker.

Similarly, Equation (4-8) describes a model for the **voltage set-point offsetting attack in the communication link**

$$V_r = V_t + \lambda_{aV}V_a \tag{4-8}$$

where V_r is the voltage value read from the communication link. V_t is the measured voltage communicated by the inverter. $\lambda_{aV}$is a binary factor that indicates the presence or absence of an attack, whose value is ‘1’ in presence of an attack and ‘0’ in normal operation. Finally, V_a is a corrupt voltage offset defined by the attacker.

4.2.2. Hijacking the Entire Communication Link

The hijacking attack of a communication link consists of changing completely the signals sent across the communication channels. In this attack, the attacker takes the original signal value, discards it, defines a different one and send it to the neighbors through the network. Equation (4-9) defines a model for the **frequency hijacking attack in the communication link**.

$$\omega_r = \omega_t^{(1-\lambda_{h\omega})} + \omega_h^{\lambda_{h\omega}} \tag{4-9}$$

where ω_r is the frequency value read from the communication link. ω_t is the measured frequency communicated by the inverter. $\lambda_{h\omega}$ is a binary factor that indicates the presence or absence of an attack, whose value is ‘1’ in presence of an attack and ‘0’ in normal operation. Finally, ω_h is a corrupt frequency defined and re-transmitted by the attacker.

Similarly, Equation (4-10) defines a model for the **voltage hijacking attack in the communication link**

$$V_r = V_t^{1-\lambda_{hV}} + V_h^{\lambda_{hV}} \tag{4-10}$$

where V_r is the value read from the communication link. V_t is is the measured voltage communicated by the inverter. λ_{hV} is a binary factor that indicates the presence or absence of an attack, whose value is ‘1’ in presence of an attack and ‘0’ in normal operation. Finally, V_h is a corrupt voltage defined and re-transmitted by the attacker.

5 Resilient Secondary Cooperative Control

As described extensively throughout the document, in the hierarchy of an islanded microgrid, the secondary level of control includes an essential communication component through which the inverters exchanged information. It is at this level where the attacks take place and, consequently, where it becomes needful to incorporate a resilient control strategy. In consequence, it is a prerequisite finding an adequate representation to model the microgrid and its elements. Given the structure and synergy between all the components in a microgrid, multi-agent systems are suitable to model it. In a multi-agent system, each agent works autonomously but collectively for a common purpose; hence this approach is also known as cooperative control or control of distributed dynamic systems in graphs. The agents are interconnected through a communication network, wherein each of them sends/receives information to/from its neighbors. Under this concept, the agents (or nodes) in the network represent the inverter-based DGs in the microgrid. Finally, the common goal is to synchronize the frequency and voltage values from each inverter with the reference [30, 63].

The interaction of a multi-agent system with the communication network can be represented with a graph. The nodes in the graph represent the agents in the system, as well as, the edges represent the links in the communication network. The way of how the information flows between the network agents determines the topology of the graph, bringing the concept of graph connectivity explained later in Section 5.1. The agents' behavior can be modeled through different dynamic's orders, and the implementations of consensus algorithms must respond to those agents' dynamics, whether first-order [26, 56], second-order [49, 62, 64], or higher order [51, 19]. When the network cannot reach the agreement, i.e., the network does not synchronize; it is needed to apply a controlling law. Multi-agent systems require distributed control schemes, in which every agent's action is determined by its information and the received from its neighbors, where the set of neighboring nodes must be a subset of the total network nodes. However, in the case of *connected graphs* (see Section 5.1), in the end, the information will reach every single node. This control approach is extensively explained in [30, 63]. On the other hand, the desired response

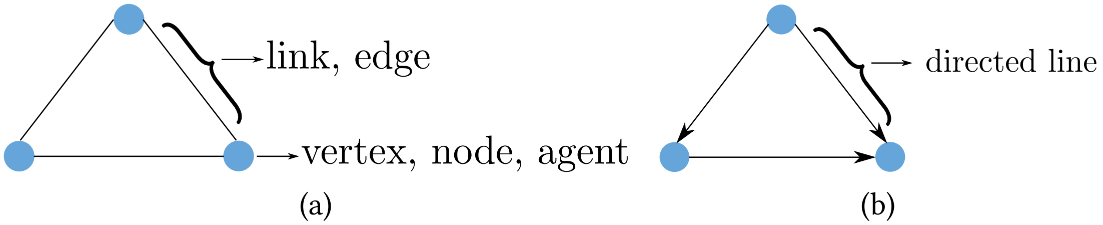

Figure 5-1: General graph illustration: (a) Graph components; (b) Digraph.

in every agent of the network is not sufficient to guarantee a stable performance in the whole system. This final performance is also related to the connectivity of the graph.

Section 5.1 introduces some relevant fundamentals of graphs, as well as their properties and configurations. It also presents matrix representations of graphs and their properties in terms of the Laplacian and spectral theory. Section 5.2 presents some relevant concepts of agent dynamics, their consensus protocols, and their corresponding equations. Section 5.3 describes the cooperative control strategy extensively, and its synchronization performance on some case studies. Section 5.4 describes two proposed observers for the cooperative control. Finally, Section 5.5 describes the case studies, including the system description, some cyber-attack scenarios, and the performance of the proposed control strategies in these scenarios through the implementation of some experiments.

5.1. Graph Basics and Connectivity

In a graph, the information can flow in different possible ways; hence, the analysis and properties can vary. If a simple line represents the link without arrows, it is assumed that the information flows bidirectionally. These graphs are named undirected graphs. The other possibility is the flow of information in a specific direction, stated by the arrow in the line that represents the edge. These graphs are named directed graphs or simply, *digraphs*. The above means that an undirected graph is a particular case of the digraphs. A network with sensors as agents is an application example of directed graphs. Other considerations to take into account for the analysis of the graphs include time-variant topologies and mobile agents. Into the networks' variations to consider are the dynamic and random networks, whose analysis requires tools like models of hybrid systems, Lyapunov theory, and stochastic stability [36].

In this sense, the most simple case to analyze is a time-invariant static network with undirected links, not self-cycles in the nodes, and not more than one edge in every pair of nodes, like the graph in Figure **5-1**. Under these considerations lets define a graph G, with a set of nodes (vertices) V and a set of edges (links) E, as $G = (V, E)$. V with n nodes is defined as

$$V = \{v_1, v_2, ..., v_n\} \tag{5-1}$$

and E with m vertex is defined as

$$E = \{e_1, e_2, ..., e_m\}. \tag{5-2}$$

However, the edges of a graph are expressed in terms of its vertices $\{v_i, v_j\}$, or $\{v_i v_j\}$ for simplicity. The subscripts i, j refer to the vertex i from which the link leaves and reaches the node j, in other words, node i receives information from the node j. In fact, under the premise of undirected graphs, it is true that $v_i v_j = v_j v_i$. On the other hand, for directed graphs, the subscripts i, j, are the tail and the head of the edge, respectively. This is illustrated in Figure **5-1** (b). Finally, the set of edges in the graph can be expressed as

$$\{v_i, v_j\} \in E. \tag{5-3}$$

where $i, j = 1, ..., n$ and given the assumption that there not exist self-cycles in the nodes $i \neq j$. Regarding to the set of nodes and links, it follows the nomenclature, $V(G)$ and $E(G)$, respectively.

Lets name the graph from Figure **5-1** (a) as G. It could be defined the set of vertex as $V(G) = \{v_1, v_2, v_3\}$. And the set of edges as $E(G) = \{e_1, e_2, e_3\}$, where $e_1 = v_1 v_2 = v_2 v_1$, $e_2 = v_1 v_3 = v_3 v_1$, and $e_3 = v_2 v_3 = v_3 v_2$. This formulation can be represented as shown in Figure **5-2**.

Analogously, for the digraph from Figure **5-1** (b) named as D. It could be defined the set of vertex as $V(D) = \{v_1, v_2, v_3\}$. And the set of edges as $E(D) = \{e_1, e_2, e_3\}$, where $e_1 = v_1 v_2$, $e_2 = v_1 v_3$, and $e_3 = v_2 v_3$. This formulation can be represented as shown in Figure **5-3**.

Another possibility in the graph features is the assignation of weight in the edges. As seen so far, the graphs posses edges with weights of 1 in all of them. However, the weight can be different from 1, as well as different on every edge. For general purposes, the weight associated with

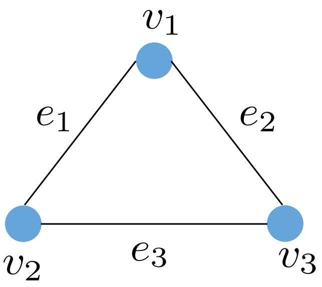

Figure 5-2: Example of graph notation. From [36]

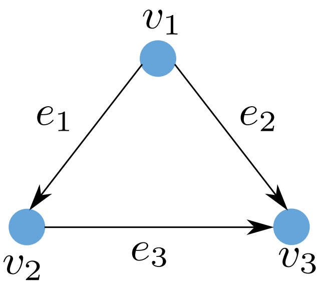

Figure 5-3: Example of digraph notation. From [36]

each edge will be denoted as w_{ij}. The graphs with the previous features are known as **weighted graphs**.

The neighborhood of the vertex v_i, denoted as $N(v_i)$ or only $N(i)$, is a subset of nodes, specifically, the adjacent nodes of i, as is expressed below

$$N\left(i\right) = \{v_j \in V \,|\, v_i v_j \ \in \ E\}. \tag{5-4}$$

For undirected graphs, it is true that if $v_j \in \ N(i)$, then $v_i \in \ N(j)$.

From the previous definitions, let us define some important concepts, such as *path*, *cycle*, *forest*, and *tree*.

A **Path** is a route that exist for every pair of vertices v_i, v_j, where the route is a sequence of vertices $v_0, v_1, ..., v_p$ such that v_0 and v_p correspond to the end vertices v_i, v_j, respectively. $v_1, ..., v_{p-1}$ are the inner vertices. Additionally, for undirected graphs v_i and v_{i+1} are adjacent with $i = 0, 1, ..., p-1$. For digraphs, it is used the term of **directed path** and $v_i, v_{i+1} \in E$ with $i = 0, 1, ..., p-1$.

In this sense, it is said that a graph is **connected** if for every pair of vertices $v_i,\ v_j$, there is a path between them. For digraphs, it is said this is **strongly connected** if $(v_i,\ v_j)$ are connected for all the nodes in the graph.

A **cycle** is a path whose sequence has the end vertices repeated, i.e., $v_0 = v_p$.

A graph is a **forest** if there are no cycles in it. In this sense, a **tree** is a particular case of a forest of one component. In the case of a digraph, if it is connected and all the nodes, except one called the root, have a single incoming arrow, then this is a **directed tree**. In other words, all the nodes, except the root, have one node as the only source of information.

A **Spanning Tree** is a minimum structure of tree that contains every vertex of the graph and guarantees that the graph is connected. In a spanning tree, all the nodes can be accessed from the root node. This structure is essential for further studies related to spectral theory and analysis of consensus dynamics [13, 36, 30].

5.1.1. Matrix Representation

A graph allows its representation in a matrix, from where it follows a series of properties and analysis. The adjacency and Laplacian matrices are some of the most representatives for the spectral theory described further in Section 5.1.2.

The **Adjacency** matrix is a representation of the adjacency relations of the agents in a graph. The dimension of this matrix is $n \times n$ and is denoted as $[A\,(G)]_{ij} = A\,(G) = a_{ij}$ for undirected graphs, and $[A\,(D)]_{ij} = A\,(D)$ for digraphs. For simplicity, it can be named just as A. The definition of A for undirected graphs is shown in Equation(5-5)

$$[A\,(G)]_{ij} = \begin{cases} 1 & \text{if } v_i v_j \ \in\ E\,(G) \\ 0 & \quad \text{otherwise} \end{cases} \tag{5-5}$$

where A is symmetric, thus $A = A^T$. On the other hand, the graph is balanced.

For digraphs A is defined in Equation (5-6)

$$[A\left(D\right)]_{ij} = \begin{cases} w_{ij} & \text{if } v_i v_j \in E\left(D\right) \\ 0 & \text{otherwise.} \end{cases} \tag{5-6}$$

Finally

$$a_{ii} = 0$$

for both directed and undirected graphs.

The **Laplacian** matrix, also known as the Kirchhoff matrix, is an element of high importance for the study of spectral theory and the analysis of dynamical multi-agent systems. This matrix is defined in terms of the adjacency matrix A and the degree matrix Δ, as shown in Equation (5-7). This definition is valid for both directed and undirected graphs. The Laplacian is denoted as $L(G)$ for graphs in general, or $L(D)$ for the specific case of digraphs, whose each case specifications come from A and Δ [13].

$$L = \Delta - A \tag{5-7}$$

where, for undirected graphs case we have

$$L\left(G\right) = \Delta\left(G\right) - A\left(G\right), \tag{5-8}$$

and for digraphs we have

$$L\left(D\right) = \Delta\left(D\right) - A\left(D\right). \tag{5-9}$$

$A\left(G\right)$ and $A\left(D\right)$ are defined in Equations (5-5) and (5-6), respectively. Likewise, for undirected graphs the degree matrix Δ is defined through Equation (5-10)

$$\Delta = \text{diag}\{d_i\} \tag{5-10}$$

where d_i is the degree of vertex v_i, i.e., the number of elements contained in the neighborhood of v_i. Thus d_i express the sum of the i-th row elements of A as in (5-11)

$$d_i = \sum_{j=1}^{N} a_{ij}. \tag{5-11}$$

Analogously, for directed graphs we have,

$$\Delta = diag\{d_{i(in)}\} \tag{5-12}$$

similarly, $d_{i(in)}$ is the in-degree of vertex v_i, but here $d_{i(in)}$ express the sum of the weighted i-th row values of A as detailed in Equation (5-13)

$$d_{i(in)} = \sum_{j \,|\, v_j v_i \in E(D)} w_{ij}. \tag{5-13}$$

Under the assumption of undirected graphs, the Laplacian has some significant properties. This matrix is symmetric, independent of orientation, and positive semi-definite. Additionally, the sum of elements in each row is equal to zero, as well as in each column. These mentioned properties and the other missing, are related to the spectral theory explained later in Section 5.1.2. The information of graphs Laplacian is also useful for formation tasks in networks with linear dynamics as those described in Section 5.2, even with non-linear systems linearizable by feedback [44, 21, 61].

5.1.2. Spectral Properties and Connectivity

As was mentioned in the previous section, spectral properties are strongly related to the eigenvalues of the different matrix associated with a graph. The most relevant analysis comes from the Laplacian matrix. Hence the following properties are mostly around this matrix.

The Laplacian matrix $L(G)$ brings information about the graph topology and, consequently, of its connectivity. $L(G)$ also provides information about the convergence of agents' agreement. Undirected graphs, are balanced, i.e., $\mathbf{1}^T L = \mathbf{0}$. Then, $L(G)$ for these graphs is symmetric and positive semidefinite. Accordingly, the eigenvalues are real and can be organized sequentially. The first eigenvalue λ_1 is the smallest value, and the n-th eigenvalue λ_n is the largest value, being n the number of nodes in the graph. Then, we have

$$\lambda_1 \leq \lambda_2 \leq ... \leq \lambda_n \tag{5-14}$$

here, λ_1 is equal to zero. The second eigenvalue λ_2 is truly important for the analysis of many agreement protocols convergence, which is directly associated with the graph connectivity. Specifically, if $\lambda_2 > 0$, the graph is said to be connected, and then it will eventually reach the agreement. λ_2 is also known as the Fiedler eigenvalue, or the algebraic connectivity eigenvalue. For dense graphs topologies, λ_2 tends to be large, as well as, small for sparse graphs. In other words, a dense graph solves the agreement faster than a connected but sparse graph. As larger λ_2 is, as faster the agreement is reached [44].

Besides of spectral analysis of λ_2, in the introduction of Section 5.1 was mentioned the existence of a spanning tree to guarantee the convergence. For a consensus protocol of first-order described later in Section 5.2, the presence of a spanning tree guarantees the convergence of the agreement [62]. However, the convergence of a first-order protocol applied in a multi-agent system with second-order dynamics can not be guaranteed even in the presence of a spanning tree [63, 50].

The Laplacian matrix for digraphs is not necessarily symmetric, positive, and semi-definite. In order to extend the connectivity theory in the context of digraphs, it is used the concept of graph mirror. Graph mirroring process allows obtaining from the original Laplacian matrix one symmetric equivalent, positive semi-definite. This way, the last spectral properties can be applied [44].

5.2. Agents' Dynamics and Consensus Protocols

The goal in a multi-agent system is to achieve the synchronization, i.e., every agent in the network must eventually reach the same state or the consensus value. In this sense, the final state of agent i; x_i, must be equal to the final state of its neighbor; x_j, it is, $x_i = x_j$, $\forall\, i, j$. A distributed cooperative control is applied in the system when agents can not reach the consensus value by themselves, as seen further in Section 5.3. As was mentioned, this control strategy is based on local and neighbors' information. However, it would be impractical to apply the control in every single node. Hence, the control law is applied in some nodes, known as *pinned nodes* or leader agents, who later exchange the information with those remaining. To establish an adequate control strategy in the system requires a proper definition of the dynamics' order that better fits the behavior of the agents [30, 63].

The concept of dynamic is related to the individual agent behavior and the equations to model it. Hence, there are first, second, and higher-order dynamics to describe different behaviors. As an example, in the context of electrical circuits, the order of the system is given by the number of energy storage elements contained in there (e.g., inductors and capacitors). In this sense, those circuits with a single energy storage element are first-order circuits, those with two energy storage elements are second-order circuits and so on [36]. In another context, the order of the dynamic is related, for example, to variables like position, velocity, and acceleration, being of first, second, and third-order, respectively.

On the other hand, consensus or agreement protocols are related to the tools used to communicate the agents in a network and how they interact, i.e., graph topologies, information flow direction, communication protocols, and others. Some topologies can be either fixed or variable, as well as; some communication channels that can present time-delays or not. Those configurations determine the selection of an adequate consensus protocol to make the network agents reach the agreement or the desired synchronization. Hence, for the same dynamic, there may be different consensus protocols. Moreover, even if a topology of a second-order networked system possesses a spanning tree, a first-order protocol is not guaranteed to work correctly in it to meet the agreement. Some relevant dynamics are described below, as well as some consensus protocols.

5.2.1. First-order Dynamics

A system with a **first-order dynamics** own a single-integrator, as described in Equation (5-15) [30]

$$\dot{x_i}\left(t\right) = u_i\left(t\right) \tag{5-15}$$

where $u_i\left(t\right)$ represents the control input and is defined in function of the states of the i-th node $x_i\left(t\right)$, as shown in Equation (5-16)

$$u_i\left(t\right) = k_i\left(x_{i_1}, x_{i_2}, ..., x_{i_{mi}}\right) \tag{5-16}$$

where N the total number of nodes and $m < N$ to guarantee a distributed control protocol. $x_i\left(t\right) \in \mathbf{R}$, represents a physical quantity.

Some consensus protocols for the dynamics of Equation (5-15) are:

For a **fixed or variable topology with no communication delay**, the local protocol in the agent i can be defined by an average consensus, as expressed in Equation (5-17)

$$u_i\left(t\right) = \sum_{j \in N_i} a_{ij}\left(x_j\left(t\right) - x_i\left(t\right)\right) \tag{5-17}$$

where a_{ij} is the element ij from the adjacency matrix A. N_i is the neighborhood of the node i and is variable for non-fixed topologies.

For **fixed topologies with time delays in the communication channel**, a consensus protocol is expressed in Equation (5-18)

$$u_i\left(t\right) = \sum_{j \in N_i} a_{ij}\left[x_j\left(t-\tau_{ij}\right) - x_i\left(t-\tau_{ij}\right)\right] \tag{5-18}$$

where $\tau_{ij} > 0$ is a constant time delay.

Another protocol for the first-order dynamics is the **non-linear** presented in Equation (5-19), which requires Lyapunov analysis to meet the convergence [44]

$$u_i\left(t\right) = \sum_{j \in N_i} \Phi_i\left(x_j\left(t\right) - x_i\left(t\right)\right). \tag{5-19}$$

5.2.2. Second-order Dynamics

A system with a **second-order dynamics** owns a double-integrator. This system is described by Equation (5-20)

$$\ddot{x}_i\left(t\right) = u_i\left(t\right) \tag{5-20}$$

where

$$\dot{x}_i\left(t\right) = v_i\left(t\right) \tag{5-21}$$

and

$$\dot{v}_i\left(t\right) = u_i\left(t\right). \tag{5-22}$$

A protocol consensus for the dynamic of Equation (5-20) in a local neighborhood is defined in Equation (5-23)

$$u_i\left(t\right) = \alpha \sum_{j \in N_i} a_{ij}\left(x_j\left(t\right) - x_i\left(t\right)\right) + \beta \sum_{j \in N_i} a_{ij}\left(v_j\left(t\right) - v_i\left(t\right)\right) \tag{5-23}$$

where $\alpha,\ \beta\ > 0$, are the stiffness and damping gains, respectively. This last equation is a variation of a Proportional-Derivative (PD) Control.

Analogously to Equation (5-18), the protocol consensus for a second order dynamic in **delayed directed networks** is described in Equation (5-24)

$$u_i\left(t\right) = \alpha \sum_{j \in N_i} a_{ij}\left[x_j\left(t - \tau_{ij}\right) - x_i\left(t - \tau_{ij}\right)\right] + \beta \sum_{j \in N_i} a_{ij}\left[v_j\left(t - \tau_{ij}\right) - v_i\left(t - \tau_{ij}\right)\right]. \tag{5-24}$$

A summarized description of the above relationships between the agent dynamics and some of their consensus protocols is shown in Figure **5-4**.

For more detailed information on the dynamics, their consensus protocols, and their convergence analysis, go to [30, 36, 44, 63].

5.3. Distributed Cooperative Control

On an isolated microgrid, one of the main objectives is to achieve the synchronization of frequency and voltage values from each inverter and bring them to the reference value. The primary

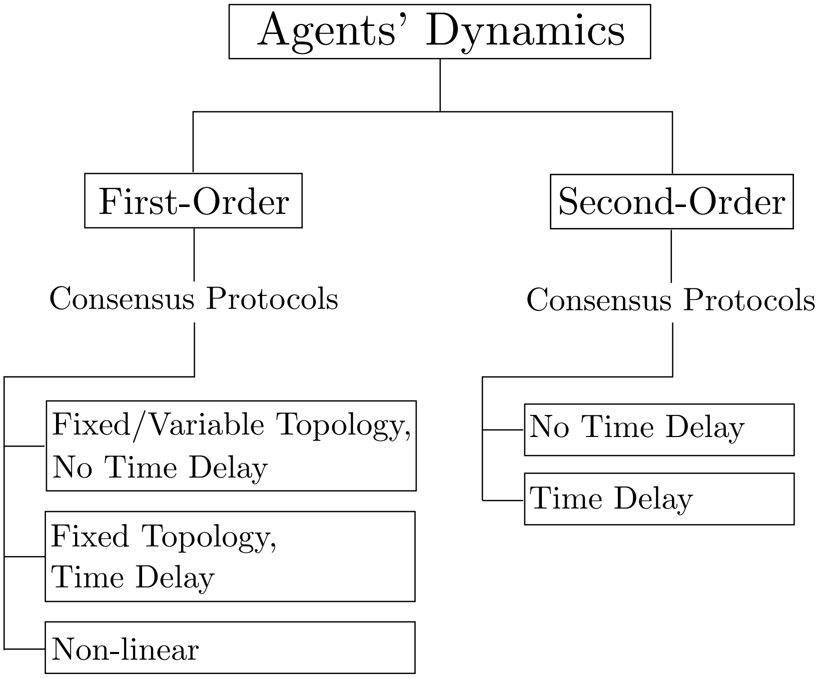

Figure 5-4: Agents' dynamics and some consensus protocols.

control described in Section 3.1 is applied locally to each inverter of the microgrid to accomplish this task. However, synchronization is not entirely achieved, as some deviations from the reference value occur when such control is applied. The secondary control allows us to adjust the frequency and voltage values and synchronize them with the reference. In the cooperative approach, the control provides the appropriate frequency and voltage reference set points, ω_i^* and V_i^*, for the primary control Equations (3-2) and (3-6). This way, it leads the frequency and voltage values to reach the reference ω_i and V_i, respectively [1, 8].

The multi-agent system considered in this work has one node as the leader, and its followers belong to a subset of the total number of nodes. The leader node provides the reference setpoint; then, all the agents' states must synchronize to the leader's state. Additionally, the control approach considered guarantees the synchronization when the graph contains a spanning tree, independent of its topology [65].

5.3.1. Secondary Frequency Control

Let's be the angular frequency of inverter i, ω_i, and of its neighbor j, ω_j. The objective is that eventually $\omega_i = \omega_j, \ \forall i, j$. According to the definitions in Section 5.2, the cooperative control law can be defined based on a first-order's dynamic. Applying the derivative to Equation (3-2) the dynamics of the angular frequency of inverter i can be obtained as [1]

$$\dot{\omega_i} = \dot{\omega_i^*} - K_{pi}\dot{P_i} \tag{5-25}$$

then, the first-order control protocol for the inverter i, $u_{\omega_i}(t)$ can be defined as follows

$$u_{\omega i}(t) = \dot{\omega_i}. \tag{5-26}$$

Under the assumption of non-time-delay in the communication system, the agreement protocol can be defined through the average consensus of Equation (5-17). Consequently, the distributed cooperative control law based on local neighboring information can be established for the agent i as [29]

$$e_{\omega_i}(t) = \sum_{j \in N_i} a_{ij}\left(\omega_j(t) - \omega_i(t)\right) + g_i\left(\omega_{ref} - \omega_i(t)\right) \tag{5-27}$$

where ω_i and ω_j are the measured frequencies at inverter i and its neighbor j, respectively. ω_{ref} is the reference frequency in the microgrid. a_{ij} is the element ij from the adjacency matrix A. g_i is the pinning gain, defined as follows

$$g_i = \begin{cases} 1, & \text{pinned nodes to the leader} \\ 0, & \text{non-pinned nodes.} \end{cases} \tag{5-28}$$

The control input, u_ω, can also be defined in terms of the tracking error (cooperative control law); e_{ω_i}, as

$$u_{\omega_i}(t) = c_\omega e_{\omega_i}(t). \tag{5-29}$$

where $c_\omega > 0$ is the coupling gain, defined as the convergence speed. Then, Equation 5-29 is expressed as

$$u_{\omega_i}(t) = c_\omega \left(\sum_{j \in N_i} a_{ij} \left(\omega_j(t) - \omega_i(t) \right) + g_i \left(\omega_{ref} - \omega_i(t) \right) \right). \tag{5-30}$$

Finally, the frequency set-point provided for the primary control is

$$\omega_i^* = \int \left(u_{\omega_i}(t) + K_{pi} \dot{P}_i \right) \mathrm{dt} \tag{5-31}$$

where $\dot{P}_i$ is found with Equation (2-5).

5.3.2. Secondary Voltage Control

Similar to previous subsection, we have for the voltage's dynamics of inverter i

$$\dot{V}_i = \dot{V}_i^* - K_{qi} \dot{Q}_i \tag{5-32}$$

where the first-order input $u_{vi}(t)$ is

$$u_{v_i}(t) = \dot{V}_i = c_v e_{v_i}(t) \tag{5-33}$$

and $c_v > 0$ is the coupling gain, defined as the convergence speed. The distributed cooperative control law based on local neighboring information for agent i is [9]

$$e_{v_i}(t) = \sum_{j \epsilon N_i} a_{ij} \left(V_j(t) - V_i(t) \right) + g_i \left(V_{ref} - V_i(t) \right). \tag{5-34}$$

where V_i and V_j are the measured voltages at inverter i and its neighbor j, respectively. V_{ref} is the reference voltage in the microgrid. a_{ij} is the element ij from the adjacency matrix A. g_i is the pinning gain, defined in Equation (5-28). Then, Equation 5-33 is expressed as [11]

$$u_{vi}\left(t\right)=c_v\left(\sum_{j\epsilon N_i}a_{ij}\left(V_j\left(t\right)-V_i\left(t\right)\right)+g_i\left(V_{ref}-V_i\left(t\right)\right)\right). \tag{5-35}$$

Finally, the voltage set-point provided for the primary control is [8]

$$V_i^*=\int\left(u_{v_i}+K_{qi}\dot{Q}_i\right)\mathrm{dt} \tag{5-36}$$

where $\dot{Q}_i$ is found with Equation 2-5.

5.4. Observer-based Cooperative Control

In practice, it is not always possible to get all the measurements' information from inverters. Also, in some cases, the reliability of such information is affected either for an attack on an inverter or a random failure in the system. One of the main purposes of the network controls is avoiding the propagation of the effect of an inverter's attack through the entire network. In this sense, it is necessary to use a methodology that allows the use of estimated values in the design of control protocols instead of measured values, i.e., estimate the states and the outputs in the inverter. The incorporation of an observer in the control design is a possibility to address the scenario just described.

The controller design that incorporates an observer can be performed with complete information of the neighborhood for both observer and control input. However, as was explained so far, there is not always access to such information. On the other hand, in multi-agent systems, synchronization can be reached even if just one of them (observer or controller) has complete access to neighbors' information. Accordingly, two architectures possibilities can be 1) a controller with neighbors' information and an observer that uses only local information, 2) a controller with local information and an observer that uses neighbor's information [65]. The following Subsections 5.4.1 and 5.4.2 show the development of two designs for an observer based on the second architecture, i.e., local information controller with an observer with neighbors' information.

5.4.1. Observer Design 1

The scheme proposed is based on a controller with local information and an observer that uses neighbor's information. So for inverter i, the observer's design includes either the measured values or the estimated values of the states and the outputs. On the other hand, the controller contains information about the estimated values from the neighbors of i [65]. This approach works effectively for an attack in the sensor actuator, like the one described in Subsection 4.1.3; its design avoids the spreading across the network of this attack's effect. Additionally, a hijacking attack in the controller, like the one described in Subsection 4.1.2, can also be avoided from spreading through the network; it will just affect the attacked node given that the communicated information is the estimated.

Frequency Observer

The new model for the local control input of frequency, $u_{\omega_i}(t)$, is set as follows

$$u_{\omega_i}(t) = c_{\hat{\omega}}\left(\hat{\omega}_i(t) - \omega_i(t)\right) \tag{5-37}$$

where $\hat{\omega}_i(t)$, is the observed angular frequency and is defined with the neighbors' information as follows

$$\dot{\hat{\omega}}_i(t) = \sum_{j \epsilon N_i} a_{ij}\left(\hat{\omega}_j(t) - \hat{\omega}_i(t)\right) + g_i\left(\omega_{ref} - \hat{\omega}_i(t)\right) \tag{5-38}$$

where $\hat{\omega}_j$, is the observer frequency of the neighbor j. Accordingly, the error neighborhood tracking is defined as

$$e_{\hat{\omega}_i}(t) = \dot{\hat{\omega}}_i(t)\,. \tag{5-39}$$

The frequency set-point provided for the primary control is the same defined in Equation (5-31). The diagram that illustrates the complete interaction of the observer and the control protocol is shown in Figure **5-5**.

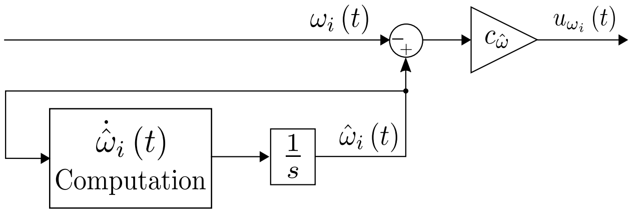

Figure 5-5: Observer design 1.

Voltage Observer

Similar to the model used for frequency, the local control input for voltage, $u_{v_i}(t)$, is set as follows

$$u_{v_i}(t) = c_{\hat{v}}\left(\hat{V}_i(t) - V_i(t)\right) \tag{5-40}$$

where $\hat{V}_i(t)$, is the observed voltage and is defined with the neighbors' information as follows

$$\dot{\hat{V}}_i(t) = \sum_{j \epsilon N_i} a_{ij}\left(\hat{V}_j(t) - \hat{V}_i(t)\right) + g_i\left(V_{ref} - \hat{V}_i(t)\right) \tag{5-41}$$

where $\hat{V}_j$, is the observer frequency of the neighbor j. Accordingly, the error neighborhood tracking is defined as

$$e_{v_i}(t) = \dot{\hat{V}}_i(t)\,. \tag{5-42}$$

The voltage set-point provided for the primary control is the same defined in Equation (5-36).

5.4.2. Observer Design 2

The scheme proposed is based on a controller with local information and an observer that uses neighbor's information. So for inverter i, the observer's design includes either the measured values or the estimated values of the states and the outputs. On the other hand, the controller contains information about the estimated values from the neighbors of i [65].

This approach makes two estimation levels of the frequency and voltage values, i.e., ω_i and V_i. The possible deviations produced in the measured values due to a cyber-attack are corrected in the first level of estimation. Then, in the second level of estimation, it is computed a refined value. Finally, in the control input, this refined value is compared with the measured one. Attacks in the communication links like the described in Subsections 4.2.1 and 4.2.2 are effectively corrected through this control design.

Frequency Observer

The new model for the local control input of frequency, $u_{\omega_i}\left(t\right)$, is set as follows

$$u_{\omega_i} = c_{\hat{\omega}}\left(\tilde{\omega}_i - \omega_i\right) \tag{5-43}$$

where $\tilde{\omega}_i$, is the refined observed frequency of inverter i, defined as follows

$$\tilde{\omega}_i\left(t\right) = \omega_i + \sum_{j\epsilon N_i} a_{ij}\left(\hat{\omega}_j\left(t\right) - \hat{\omega}_i\left(t\right)\right) + g_i\left(\omega_{ref} - \hat{\omega}_i\left(t\right)\right) \tag{5-44}$$

where $\hat{\omega}_i\left(t\right)$, $\hat{\omega}_j\left(t\right)$ are the observed voltages of inverter i and its neighbor j, respectively. The definition of the observed frequency is given by Equation (5-38) in Subsection 5.4.1. Then, the neighborhood tracking error can be defined as follows.

$$e_{\hat{\omega}_i}\left(t\right) = \tilde{\omega}_i\left(t\right). \tag{5-45}$$

The frequency set-point provided for the primary control is the same defined in Equation (5-31). The diagram that illustrates the complete interaction of the observer and the control protocol is shown in Figure **5-6**.

Voltage Observer

Similar to the model used for frequency, the local control input for voltage, $u_{v_i}\left(t\right)$, is set as follows

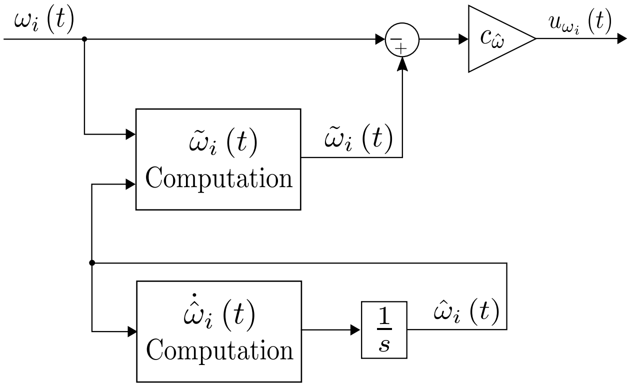

Figure 5-6: Observer design 2.

$$u_{v_i} = c_{\hat{v}} \left(\tilde{V}_i - V_i \right) \tag{5-46}$$

where $\tilde{V}_i$, is the refined observed voltage of inverter i, defined as follows

$$\tilde{V}_i(t) = V_i + \sum_{j \epsilon N_i} a_{ij} \left(\hat{V}_j(t) - \hat{V}_i(t) \right) + g_i \left(V_{ref} - \hat{V}_i(t) \right) \tag{5-47}$$

where $\hat{V}_i(t)$, $\hat{V}_j(t)$ are the observed voltages of inverter i and its neighbor j, respectively. The definition of the observed voltage is given by Equation (5-41) in Subsection 5.4.1. Then, the neighborhood tracking error can be defined as follows

$$e_{\hat{v}_i}(t) = \tilde{V}_i(t) \, . \tag{5-48}$$

The voltage set-point provided for the primary control is the same defined in Equation (5-36).

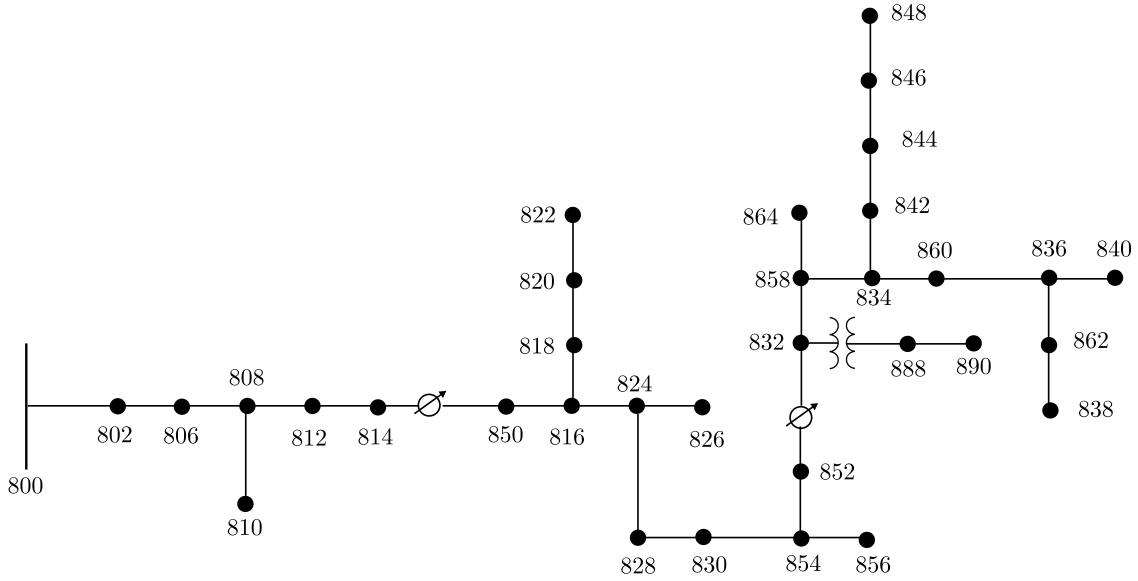

Figure 5-7: Original IEEE 34 node test feeder.

5.5. Case Studies

5.5.1. System Configuration

The proposed control schemes are probed in the IEEE 34 node test feeder illustrated in Figure **5-7** [40]. This system is modified with six inverter-based DGs making up the microgrid studied in this work, as shown in Figure **5-8**. These inverters are connected to the feeder through a transformer with the configuration shown in Table **5-1**. Some considerations of the system includes; no losses, inductive transmission lines, enough capacity to meet the demand, and no time-delays in the communication channels. The inverters of the microgrid have the droop control gains specified in Table **5-2**, where K_p and K_q are the active and reactive power gains, respectively. The DGs are connected in parallel to the common bus through the output connector, as shown in Figure **5-9**. Additionally, to the common bus are connected three RLC loads of 10 kW each.

5.5.2. Communication Layer

The communication layer through which the inverters exchange information is illustrated with green striped lines in Figure **5-10**. The topology of this communication system can be represented

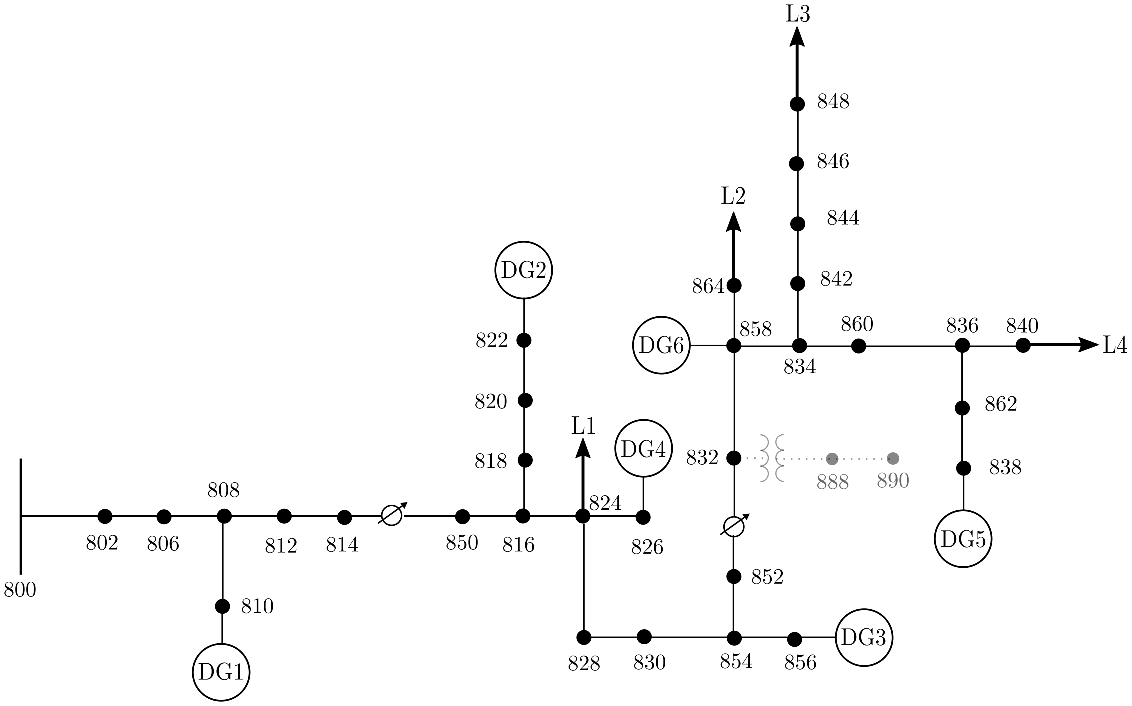

Figure 5-8: IEEE 34 node test feeder modified with six inverters.

Frequency	60Hz
Connection	Y-Y
Series Impedance	$(0.03 + j0.12)$p.u
Power	400kVA
Primary Voltage	480V
Secondary Voltage	24.9kV

Table 5-1: Transformer specifications.

		Inverters 1, 2, 4, 5	Inverters 3, 6
Droop Gains	K_p	9.4×10^{-5}	12.5×10^{-5}
	K_q	1.3×10^{-5}	1.5×10^{-5}
Output Connector	R_c	0.03Ω	
	L_c	$0.35mH$	
LC Filter	R_f	0.1Ω	
	L_f	$1.35mH$	
	C_f	$50\mu F$	

Table 5-2: Parameters of the inverters.

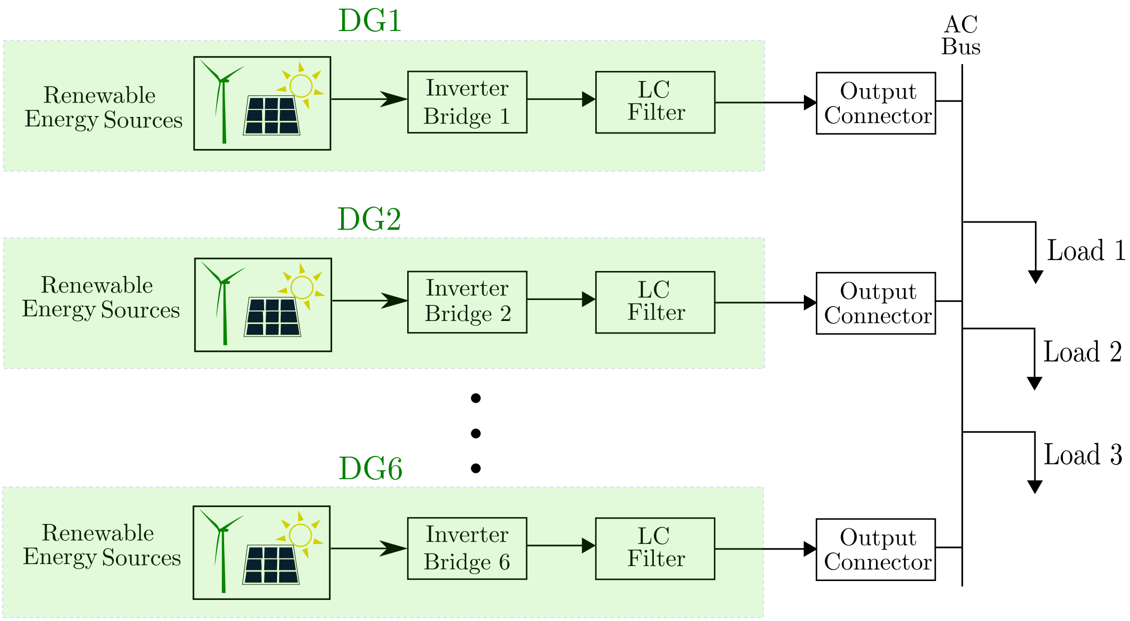

Figure 5-9: Inverters connection to the AC bus.

through the digraph of Figure **5-11**. Given that the multi-agent system considered in this work is made up of one leader node and n identical followers, the reference signal of frequency and voltage are received by the leader, i.e., the *DG1*, as illustrated in Figure **5-11** (b). Accordingly, the pinning gain vector g is set as

$$g = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

and the adjacency matrix that describes the interaction of the agents is given by Equation 5-49

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{5-49}$$

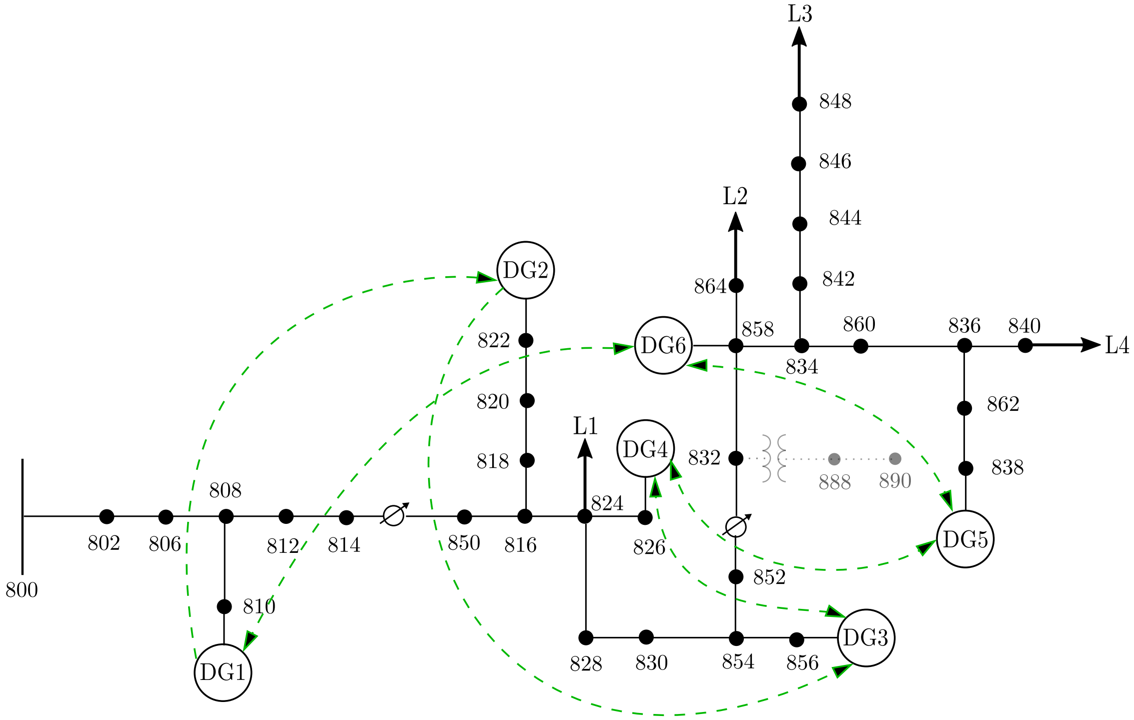

Figure 5-10: IEEE 34 bus modified with the communication layer.

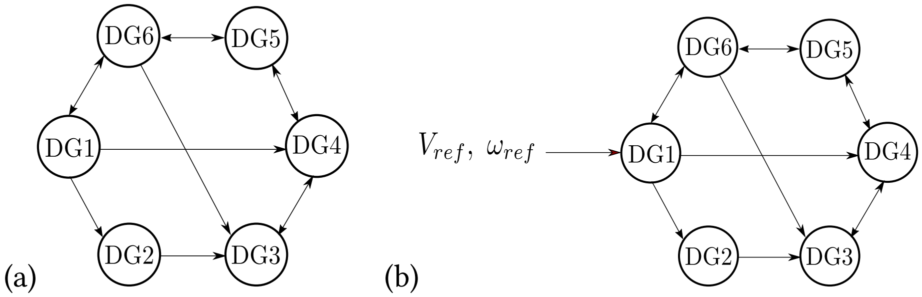

Figure 5-11: Communication network topology of the microgrid with 6 inverters. (a) General graph. (b) Graph with the references pinned to the leader node.

5.5.3. Scenarios Description

The performance of the different control schemes are analyzed under two main cyber-attack scenarios, i.e., A) controller attacks and B) communication link attacks. Additionally, these two scenarios are studied with two attack models each, i.e., 1) constant disturbance and 2) hijacking. Below is a summary of the different attack scenarios

Cyber Attack Scenarios

- A. Controller
  - 1. Constant Disturbance
  - 2. Hijacking
- B. Communication Link
  - 1. Constant Disturbance
  - 2. Hijacking.

Case A: Controller Attack

The conceptual description of this attack is comprehended in Section 4.1, where three different types of attacks are modeled. The subsequent analysis shows the two first models, i.e., the explained in Subsections 4.1.1 and 4.1.2, which are considered cybernetic. These two attacks are both deployed at the primary level of control.

Case A - 1: Constant Disturbance

In $t = 1$ s, a constant signal of 0.2 Hz is added to the primary reference frequency of inverter 2. Then, from Equation 3-2 and in terms of hertz we have the following equivalent expression

$$f_i = f_i^* - \frac{K_{pi} P_i}{2\pi} \tag{5-50}$$

accordingly, the frequency for inverter 2 under this attack scenario is defined as follows

$$f_2 = \begin{cases} f_2, \quad t = 0\,\text{s} \\ \\ f_2 + 0.2\,\text{Hz}, \quad t = 1\,\text{s} \end{cases}$$

Case A - 2: Hijacking

In $t = 1$ s, the primary reference frequency, f_2, stops from being received for the inverter 2, and it gets a constant signal of 60.2 Hz instead. Then, from Equation 5-50 we have for the inverter 2

$$f_2 = \begin{cases} f_2, \quad t = 0\,\text{s} \\ \\ 60.2\,\text{Hz}, \quad t = 1\,\text{s}. \end{cases}$$

Case B: Communication Link Attack

The conceptual description of this attack is comprehended in Section 4.2, where is modeled two different types of attacks. The subsequent analysis shows those models, i.e., the explained in Subsections 4.2.1 and 4.2.2, which are considered cybernetic. These two attacks are both deployed in the communication between the primary and secondary levels of control.

Case B - 1: Constant Disturbance

In $t = 1$ s, a constant signal of 0.2 Hz is added to the f_2 signal communicated between the primary and secondary levels of control. This action is illustrated in Figure **5-12**.

Case B - 2: Hijacking

In $t = 1$ s, the f_2 signal stops from being communicated between the primary and secondary levels of control and it is communicated a constant signal of 60.2 Hz instead. This action is illustrated

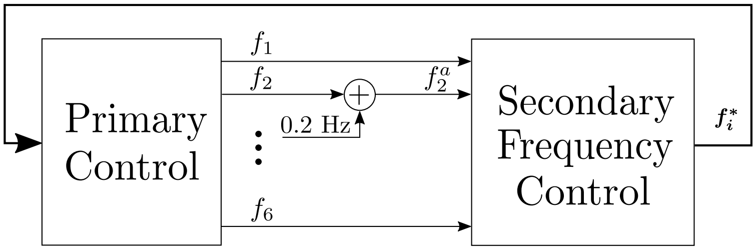

Figure 5-12: Constant disturbance attack to communication link of inverter 2.

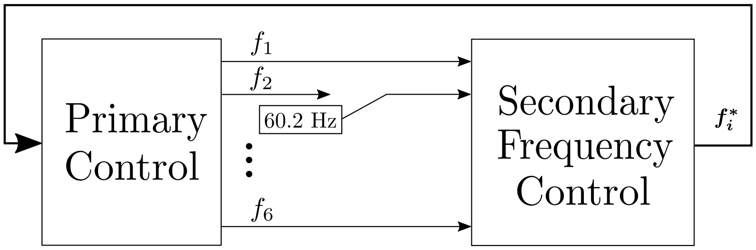

Figure 5-13: Hijacking attack to communication link of inverter 2.

in Figure **5-13**.

Disconnection of the Affected Node

When the control strategy used in the system does not present a desirable performance for the frequency and voltage responses, it can be adopted as an action, the disconnection of the affected node to improve the performance. In the following case studies, all the attack scenarios are performed on inverter 2. Then, *DG2* can be disconnected from communication topology to correct the performance. Accordingly, the outgoing link of *DG2* is disconnected, and the new topology is illustrated in Figure **5-14**, with the corresponding adjacency matrix given by Equation (5-51). On the other hand, *DG2* is also physically disconnected from the common bus, as illustrated in Figure **5-15**.

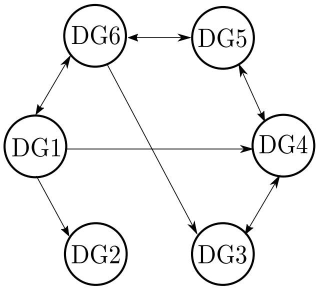

Figure 5-14: Communication graph topology of Figure **5-11** with the edge v_2v_3 disconnected.

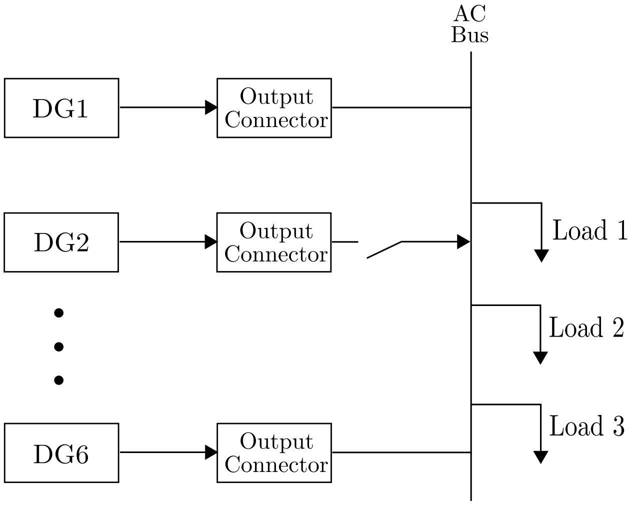

Figure 5-15: Physical disconnection of DG2 from the common bus.

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{0} & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \tag{5-51}$$

5.5.4. Results

This section shows the results of the control approaches under the different cyber-attack scenarios from Table **5-3**, i.e., 1) the conventional cooperative control, described in Subsection 5.3, 2) the

			ATTACK			
			A. Controller		B. Communication Link	
			1. Constant Disturbance	2. Hijacking	1. Constant Disturbance	2. Hijacking
CONTROL	Cooperative Control		✓	✓	✓	✓
	Observer Design 1	F	✓	✓		
		F & V	✓	✓	✓	✓
		Disconnection		✓		
	Observer Design 2	F	✓	✓	✓	✓
		F & V			✓	✓

Table 5-3: Implemented cyber-attack experiments.

observer-based cooperative control with design 1, described in Section 5.4.1, and 3) the observer-based cooperative control with design 2, described in Subsection 5.4.2, under the cases (A - 1), (A - 2), (B - 1), and (B - 2). Table **5-3** shows with a check-mark the implemented experiments.

1) Conventional Cooperative Control

1) Case A - 1: Constant Disturbance in the Controller

Figure **5-16** shows the performance of the conventional cooperative control in the frequency response under a constant disturbance attack in the controller of inverter 2. It can be seen that in $t = 1$ s, f_2 takes the value of 60.2, the control corrects the deviation, and f_2 recovers the reference to 60. Then, the frequencies from inverters synchronize appropriately.

Figure **5-17** shows the performance of the conventional cooperative control in the voltage response under a constant disturbance attack in the controller of inverter 2. It can be seen that in $t = 1$ s the voltage values from all the inverters have a slight deviation from the reference but those back immediately to the original reference and synchronize adequately. In Figures **5-17** (b) and **5-17** (c) is zoomed the voltage response, it can be seen that the values from the inverters different of 2 synchronize perfectly, and the response of 2 slightly deviates.

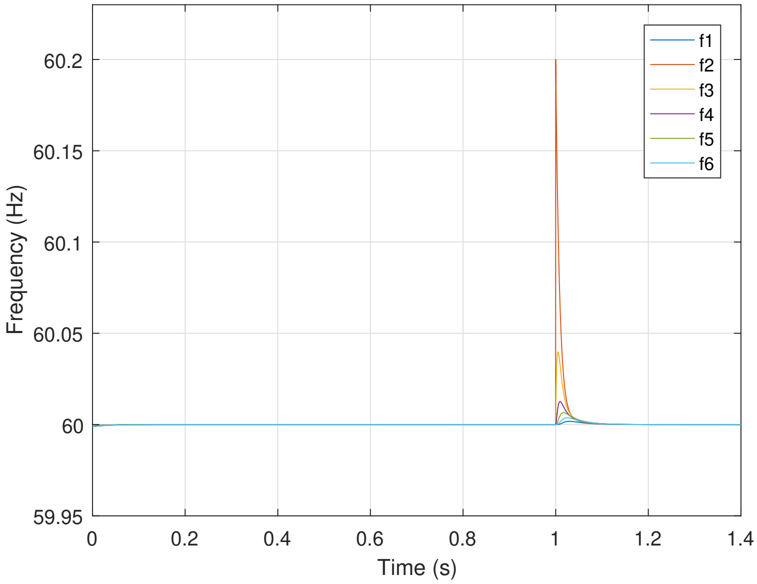

Figure 5-16: Frequency response of the system with the conventional cooperative control under a constant disturbance attack of 0.2 Hz in the controller of inverter 2 in $t = 1$ s.

1) Case A - 2: Hijacking of the Controller

Figure **5-18** shows the performance of the conventional cooperative control in the frequency response under a controller hijacking attack. f_3 who is the direct follower of f_2, tries to track the reference that f_2 imposes. The frequencies from all inverters do not reach synchronization.

Figure **5-19** shows the performance of the conventional cooperative control in the voltage response under a controller hijacking attack. It can be seen that voltage values from all the inverters do not reach the synchronization.

1) Case B - 1: Constant Disturbance of the Communication Link

Figure **5-20** shows the performance of the frequency response using the conventional cooperative control under a constant disturbance attack in the communication link. Figures **5-20** (a) and **5-20** (b) show the frequency response before the attack and after the attack, respectively. The attack conducts to trick the system, it can be seen that the signal received by the secondary control (Figure **5-20** (b)) seems to work adequately; however, f_2 is behaving as seen in Figure **5-20** (a), i.e., at 59.8 Hz.

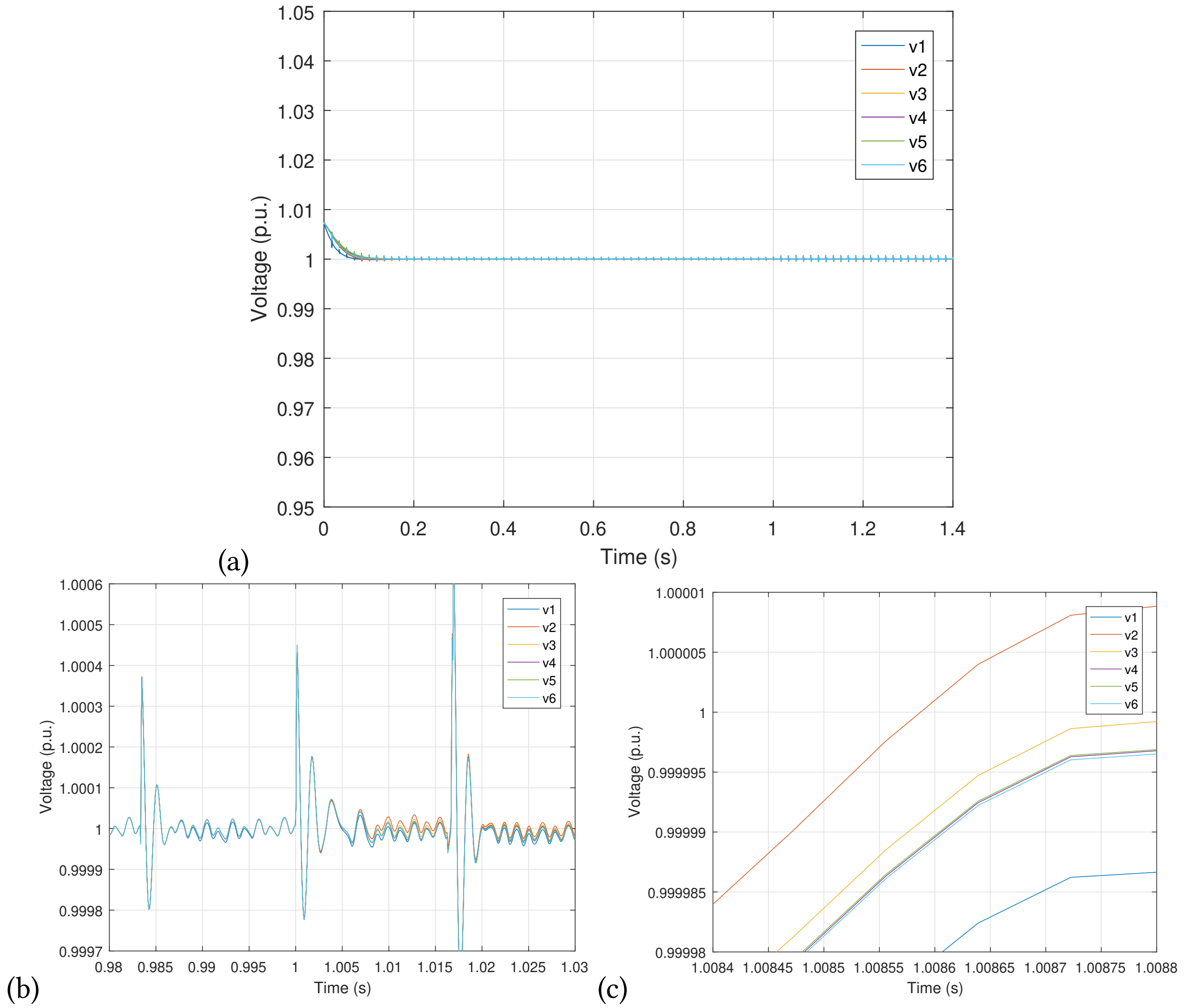

Figure 5-17: Voltage response of the system with the conventional cooperative control under a constant disturbance attack of 0.2 Hz in the controller of inverter 2 in $t = 1$ s.

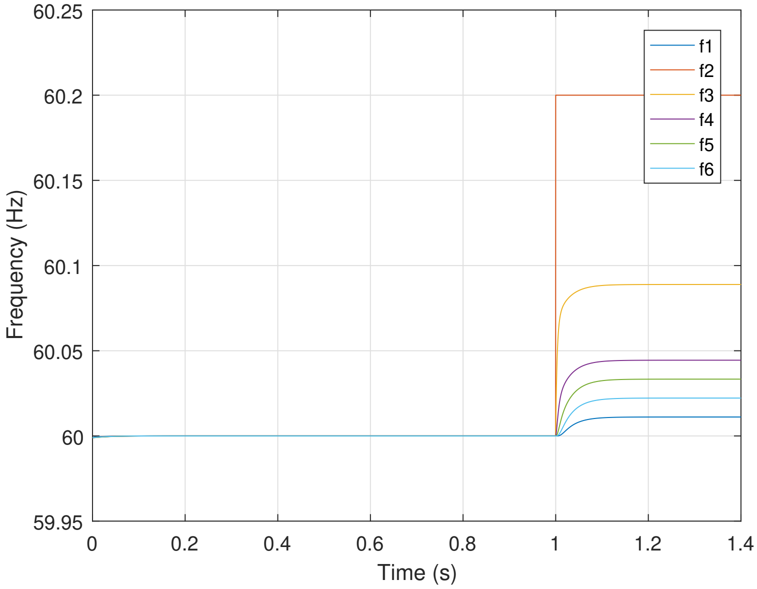

Figure 5-18: Frequency response of the system with the conventional cooperative control under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s.

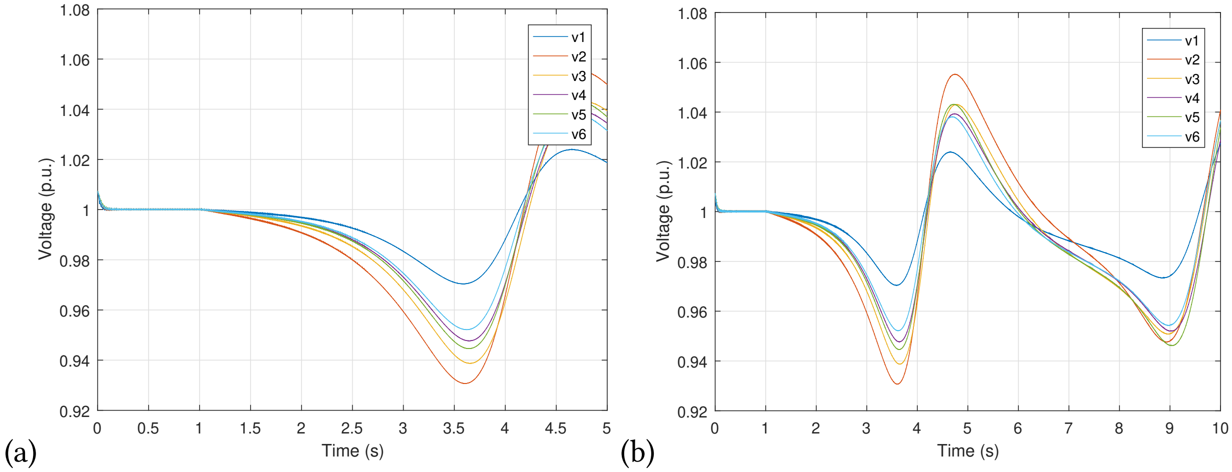

Figure 5-19: Voltage response of the system with the conventional cooperative control under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s.

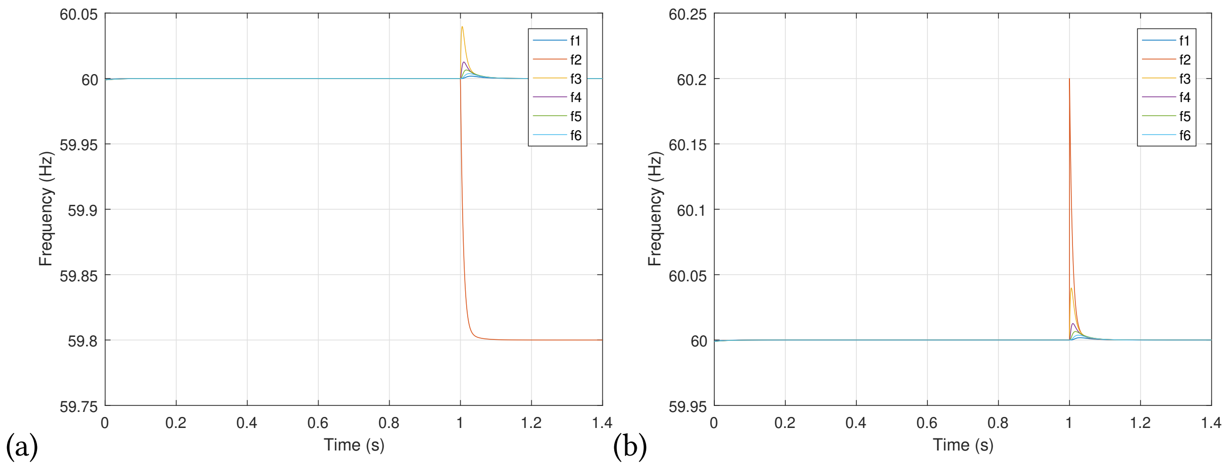

Figure 5-20: Frequency response of the system using the conventional cooperative control under a constant disturbance attack of 0.2 Hz in the communication link of inverter 2 in $t = 1$ s. (a) Frequency response before the attack deployment (measured value). (b) Frequency signal received by the secondary control

Figure **5-21** shows the performance of the conventional cooperative control in the voltage response under a constant disturbance attack in the communication link. It can be seen that voltage values from inverters do not synchronize as is expected.

1) Case B - 2: Hijacking of the Communication Link

The conventional cooperative control does not perform adequately under a hijacking attack in the communication link of inverter 2, and it is produced a collapse of the system. The frequency and voltage responses cannot follow the reference and consequently do not reach synchronization.

2) Observer-based Cooperative Control with Design 1

2) Case A - 1: Constant Disturbance in the Controller

Although it was not required an improvement in the performance of the system under a constant disturbance attack in the controller, they were implemented the frequency and voltage observers from Equations (5-38) and (5-41). The responses for both frequency and voltage were the same

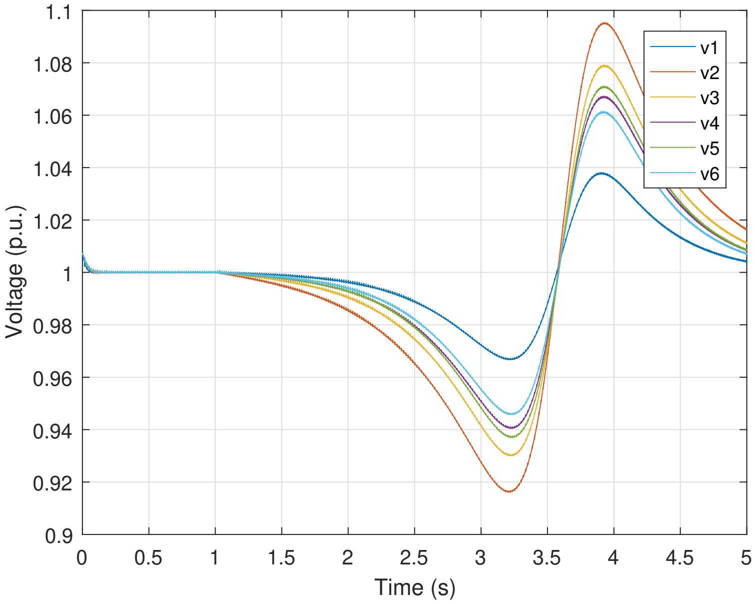

Figure 5-21: Voltage response of the system using the conventional cooperative control under a constant disturbance attack of 0.2 Hz in the communication link of inverter 2 in $t = 1$ s.

obtained with the conventional cooperative control in Figures **5-16** and **5-17**, respectively.

2) Case A - 2: Hijacking of the Controller

In this scenario were implemented four experiments; a) frequency observer, b) frequency observer with disconnection of the affected node, i.e., the inverter 2, c) frequency and voltage observers, and d) frequency and voltage observers with disconnection of the affected node.

Frequency Observer

Figure **5-22** shows the performance of the frequency response with a frequency observer-based cooperative control (design 1) under a hijacking attack in the controller of inverter 2. It can be seen that even when the affected node remains in the wrong reference of 60.2 Hz, the remaining frequency responses from the inverters synchronize appropriately and track the reference in 60 Hz.

Figure **5-23** shows the performance of the voltage response with a frequency observer-based

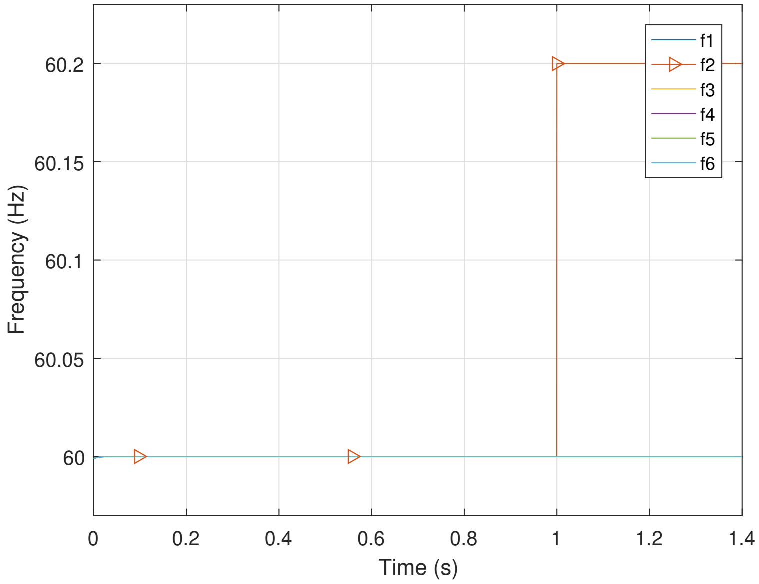

Figure 5-22: Frequency response of the system using a frequency observer-based cooperative control (design 1) under a a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s.

cooperative control (design 1) under a hijacking attack in the controller of inverter 2 for two different values of coupling gain, C_v. Additionally, it can be seen that the synchronization cannot be reached, and the reference is not followed adequately.

Frequency Observer and Disconnection of the Affected Node

Figure **5-24** shows the performance of the frequency response once the affected node is disconnected from the graph in $t = 6$ s. The adjacency matrix changes from Equation (5-49) to the one in Equation (5-51) and the graph becomes the one in Figure **5-14**. It can be seen that the performance of the response has the desired behavior once the node is disconnected.

Figure **5-25** shows the performance of the voltage response once the affected node is disconnected from the graph in $t = 6$ s. The adjacency matrix changes from Equation (5-49) to the one in Equation (5-51) and the graph becomes the one in Figure **5-14**. It can be seen that the performance of the response has the desired behavior once the node is disconnected, even when the controller used has not a voltage observer.

Frequency and Voltage Observers

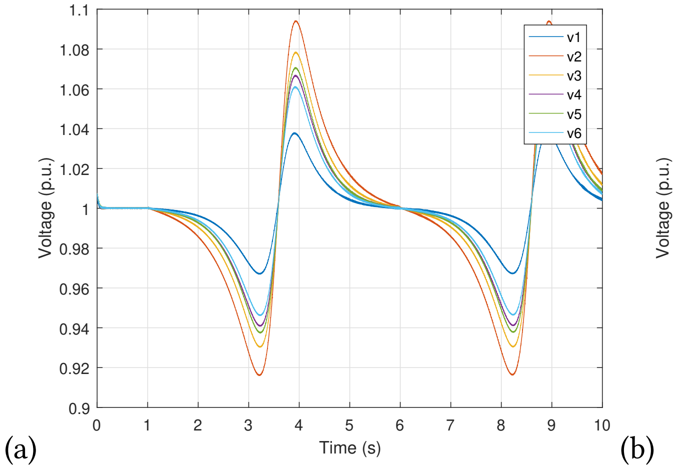

Figure 5-23: Voltage response of the system using a frequency observer-based cooperative control (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s for two different values of coupling gain: (a) $c_v = 120$ and (b) $c_v = 200$.

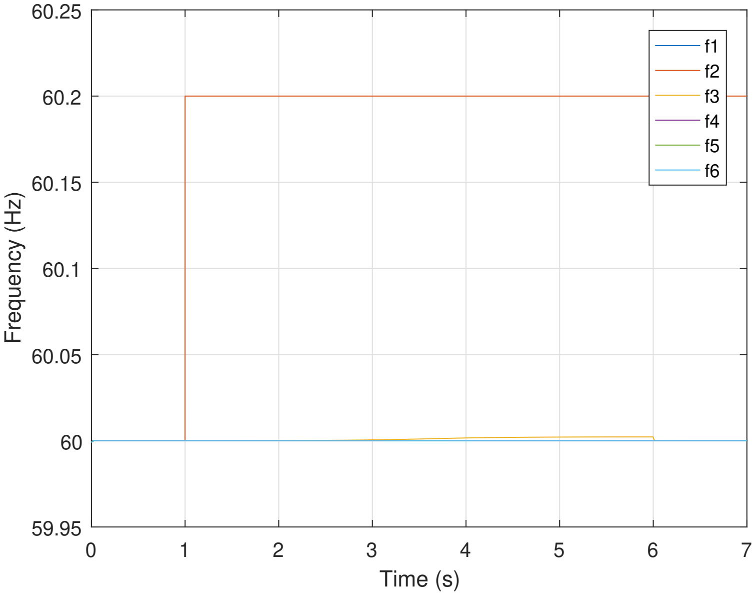

Figure 5-24: Frequency response of the system using a frequency observer-based cooperative control (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. Disconnection of node 2 from the graph in $t = 6$ s.

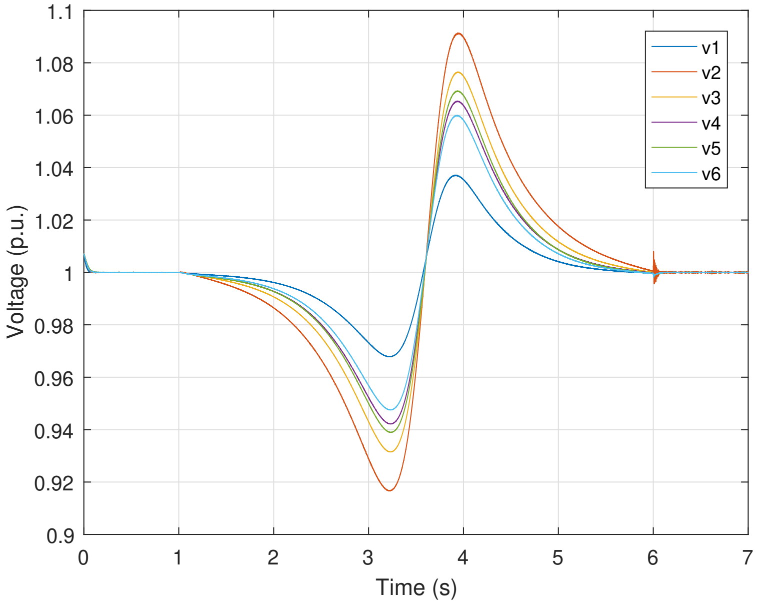

Figure 5-25: Voltage response of the system with a frequency observer-based cooperative control (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. Disconnection of node 2 from the graph in $t = 6$ s.

The performance of the frequency response with a cooperative control with observers for frequency and voltage (design 1) under a hijacking attack in the controller of inverter 2, is the same obtained in Figure **5-22**, where the performance was not adequate. However, Figure **5-26** shows an improvement in the voltage performance response, i.e., even when inverter 2 moves away from the reference, the responses of the other inverters reach synchronization and follow the reference.

Frequency and Voltage Observers and Disconnection of the Affected Node

The performance of the frequency response with the disconnection of the affected node is the same obtained in Figure **5-24**, where there is no observer for voltage.

Figure **5-27** shows the performance of the voltage response once the affected node is disconnected from the graph in $t = 6$ s. The adjacency matrix changes from Equation (5-49) to the one in Equation (5-51) and the graph becomes the one in Figure **5-14**. It can be seen that the performance of the response has the desired behavior once the node is disconnected. This is the performance expected independent of the controller applied.

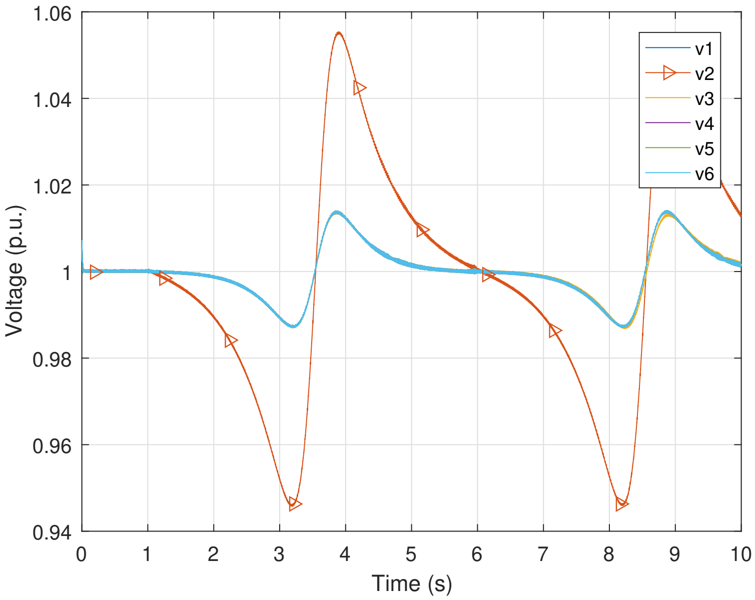

Figure 5-26: Voltage response of the system with a cooperative control using observers for frequency and voltage (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s.

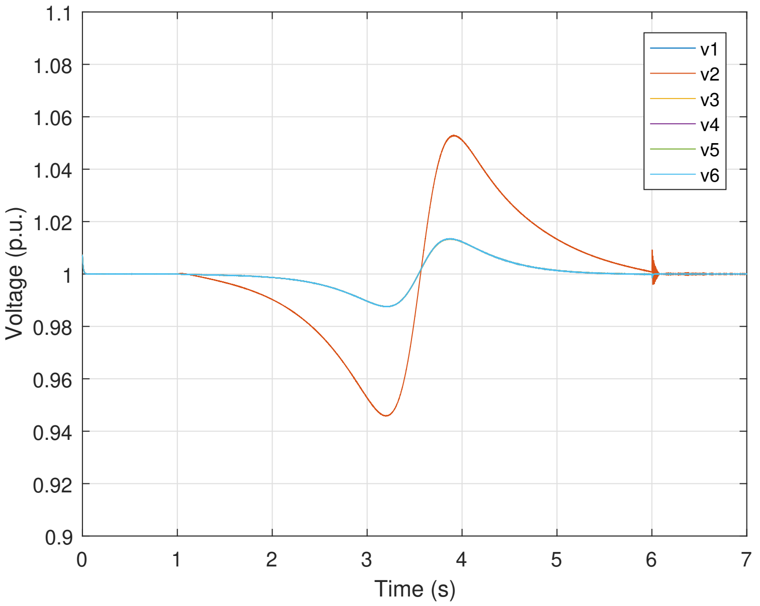

Figure 5-27: Voltage response of the system with a cooperative control using observers for frequency and voltage (design 1) under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s. Disconnection of node 2 from the graph in $t = 6$ s.

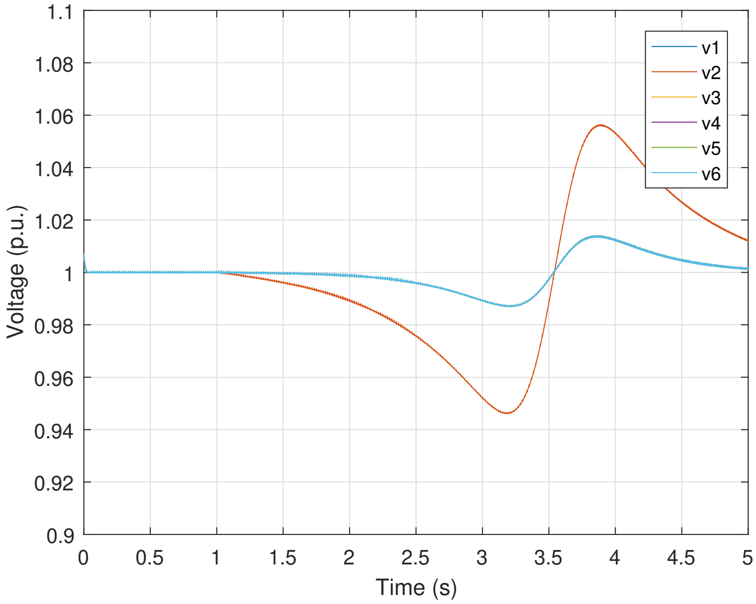

Figure 5-28: Voltage response of the system with a cooperative control using observers for frequency and voltage (design 1) under a constant disturbance attack of 0.2 Hz in the communication link of inverter 2 in $t = 1$ s.

2) Case B - 1: Constant Disturbance of the Communication Link

The performance of frequency response before and after the attack using a cooperative control with observers for frequency and voltage (design 1) under a constant disturbance attack in the communication link are the same of Figure **5-20**. However, Figure **5-28** shows that the performance of voltage response improves, i.e., inverters not affected reach the synchronization, as well as the tracking of the reference.

2) Case B - 2: Hijacking of the Communication Link

Similar to the case of conventional cooperative control, the system does not perform adequately under a hijacking attack in the communication link of inverter 2 using the design 1 for frequency and voltage observers. The frequency and voltage responses cannot follow the reference and consequently do not reach synchronization.

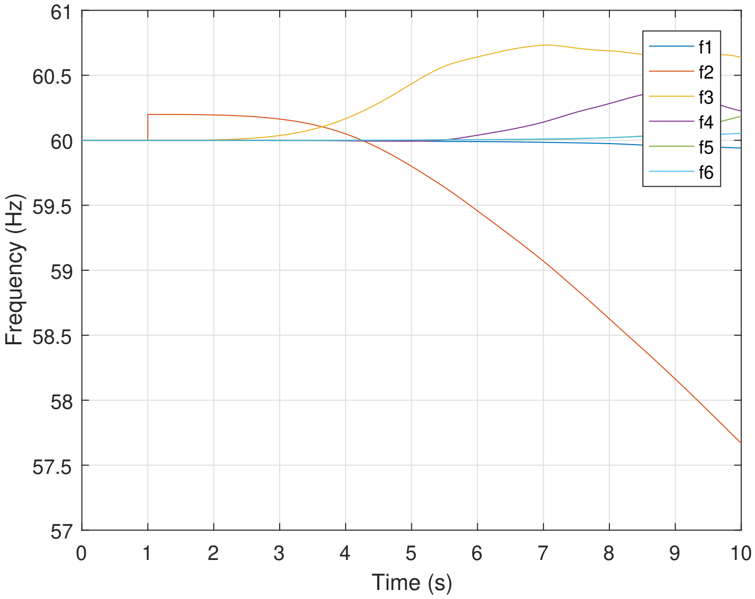

Figure 5-29: Frequency response of the system using the design 2 of the observer based-cooperative control under a constant disturbance attack of 0.2 Hz in the controller of inverter 2 in $t = 1$ s.

3) Observer-based Cooperative Control with Design 2

Case A - 1: Constant Disturbance in the Controller

Figure **5-29** shows the performance of the frequency response with a frequency observer-based cooperative control (design 2) under a constant disturbance attack in the controller. This control strategy does not work adequately for this scenario; the frequency responses lose the tracking of the reference.

Figure **5-30** shows the performance of the voltage response with a frequency observer-based cooperative control (design 2) under a constant disturbance attack in the controller. This control strategy does not work adequately for this scenario; the voltage responses lose the tracking of the reference and do not reach synchronization.

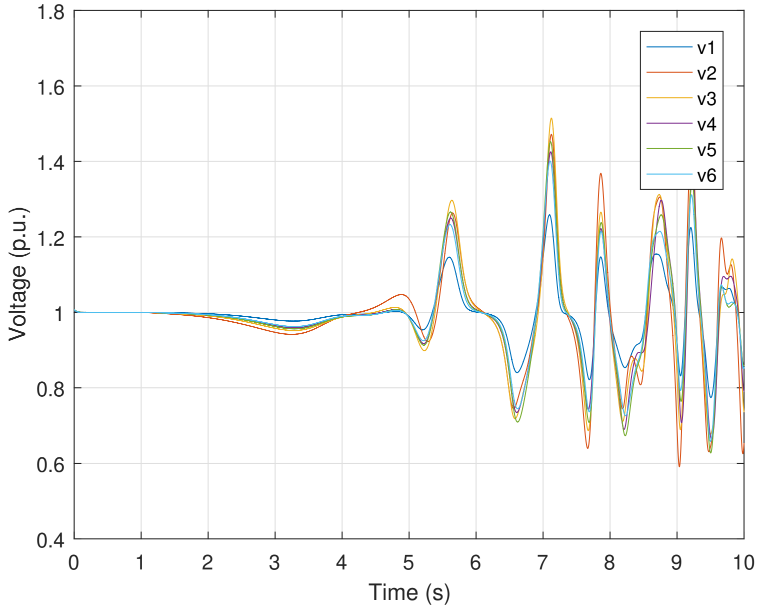

Figure 5-30: Voltage response of the system using the design 2 of the observer based-cooperative control under a constant disturbance attack of 0.2 Hz in the controller of inverter 2 at $t = 1$ s.

3) Case A - 2: Hijacking of the Controller

Figure **5-31** shows the performance of the frequency response with a frequency observer-based cooperative control (design 2) under a hijacking attack in the controller of inverter 2. The design of this controller does not have a stable performance under this scenario of attack, the frequency response loses the reference tracking, and consequently, the synchronization is lost.

Figure **5-32** shows the performance of the voltage response with a frequency observer-based cooperative control (design 2) under a hijacking attack in the controller of inverter 2. The design of this controller does not have a stable performance under this scenario of attack, the voltage response loses the reference tracking, and consequently, the synchronization is lost.

3) Case B - 1: Constant Disturbance of the Communication Link

Figure **5-33** shows the performance of the frequency response with a frequency and voltage observer-based cooperative control (design 2) under a constant disturbance attack in the com-

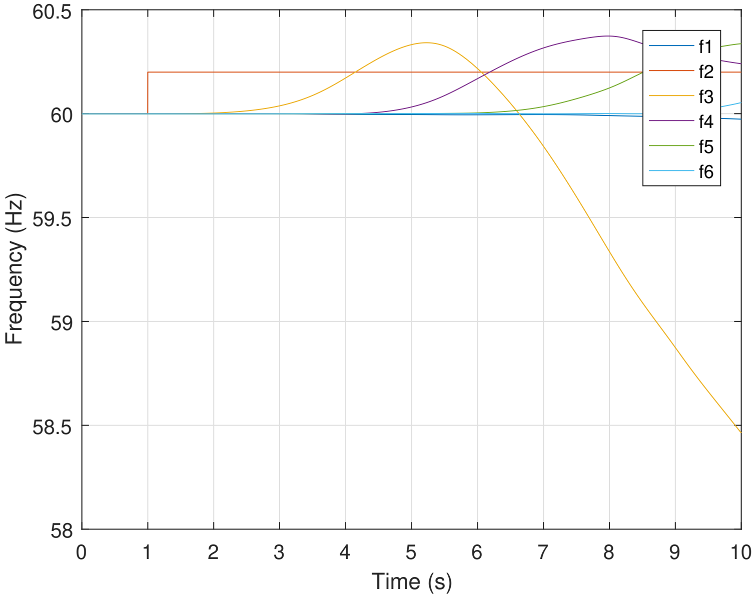

Figure 5-31: Frequency response of the system using the design 2 of the observer-based cooperative control under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s.

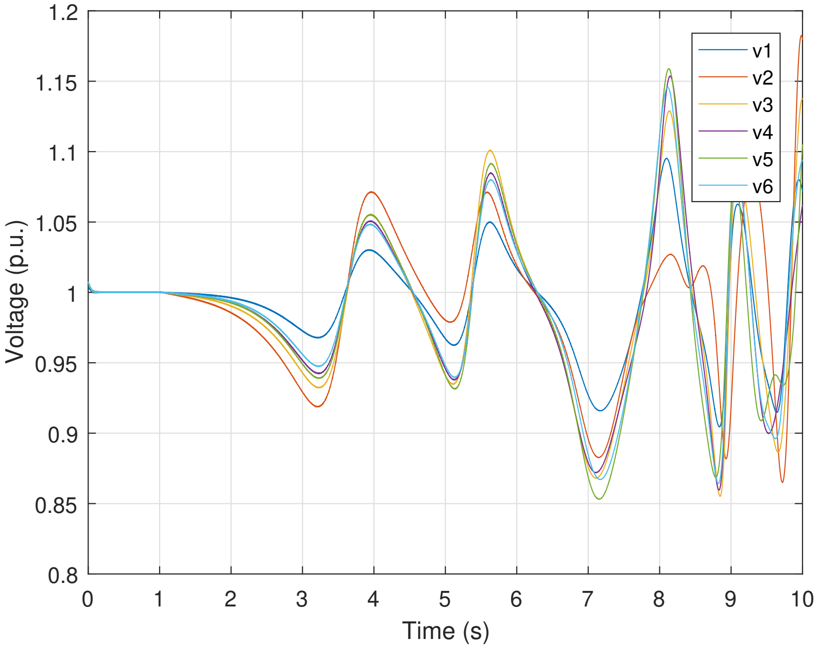

Figure 5-32: Voltage response of the system using the design 2 of the observer-based cooperative control under a hijacking attack of 60.2 Hz in the controller of inverter 2 in $t = 1$ s.

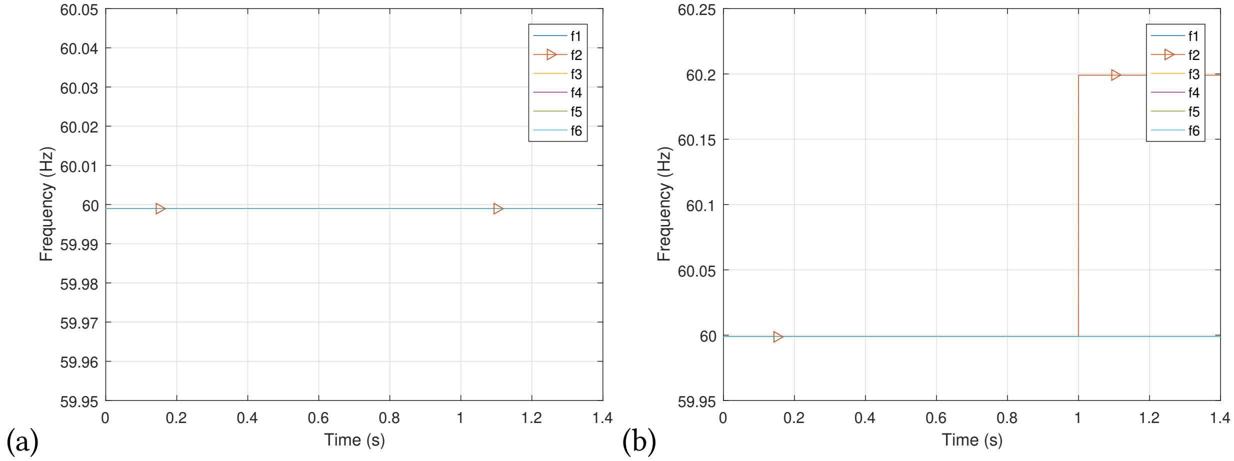

Figure 5-33: Frequency response of the system with the design 2 of the observer-based cooperative control under a constant disturbance attack of 0.2 in the communication link of inverter 2 in $t = 1$ s. (a) Frequency response before the attack deployment (measured value). (b) Frequency signal received by the secondary control.

munication link. Figures **5-33** (a) and **5-33** (b) show the frequency response before the attack, and after the attack, respectively. With this control strategy the attack does not get to trick the system, it can be seen that the signal received by the secondary control (Figure **5-33** (b)) is the actual behavior of the frequency response, i.e., $f_2 = 60.2$ Hz, and in Figure **5-33** (a) it can be seen that the control corrects the error. Hence f_2 follows the reference and, in consequence, the synchronization is achieved.

Figure **5-34** shows the performance of the voltage response with a frequency and voltage observer-based cooperative control (design 2) under a constant disturbance attack in the communication link. With this control strategy, the voltage response follows the reference, and the synchronization is achieved.

3) Case B - 2: Hijacking of the Communication Link

Figure **5-35** shows the performance of the frequency response with a frequency and voltage observer-based cooperative control (design 2) under a hijacking attack in the communication link. Figures **5-35** (a) and **5-35** (b), show the frequency response before the attack, and after the attack, respectively. With this control strategy, the attack does not get to trick the system, it can be seen that the signal received by the secondary control (Figure **5-35** (b)) is the actual behavior

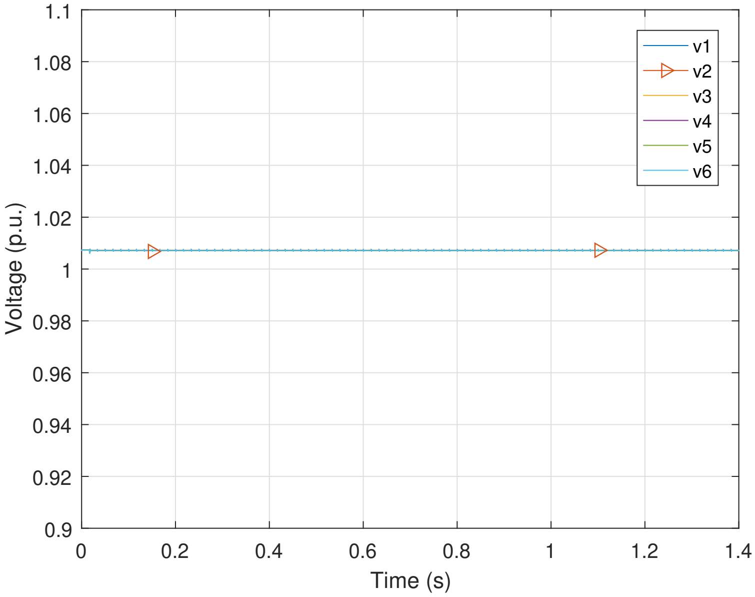

Figure 5-34: Voltage response of the system with the design 2 of the observer-based cooperative control under a constant disturbance attack of 0.2 Hz in the communication link of inverter 2 in $t = 1$ s.

of the frequency response, i.e., $f_2 = 60.2$ Hz, and in Figure **5-35** (a) it can be seen that the control corrects the error. Hence f_2 follows the reference and the synchronization is achieved.

Figure **5-36** shows the performance of the voltage response with a frequency and voltage observer-based cooperative control (design 2) under a hijacking attack in the communication link. With this control strategy, the voltage response follows the reference, and the synchronization is achieved appropriately.

Summary of Results

Table **5-4** presents a summary of results for all the experiments implemented. The check-mark (✓) indicates the combination of attack and controller with an adequate performance of synchronization and reference tracking. Hence, the blue check-mark (✓) indicates the best combination of all the strategies proposed. The *'x'* symbol indicates the combination of attack and controller that did not present a desirable performance. Finally, *'NA'* indicates that the experiment was not implemented.

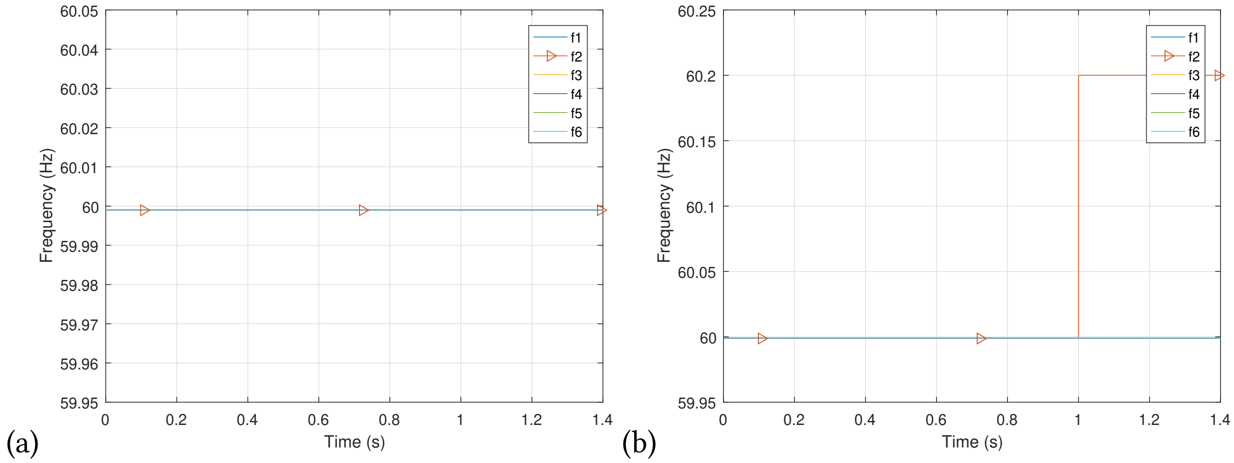

Figure 5-35: Frequency response of the system with the design 2 of the observer-based cooperative control under a hijacking attack of 60.2 Hz in the communication link of inverter 2 in $t = 1$ s. (a) Frequency response before the attack deployment (measured value). (b) Frequency signal received by the secondary control.

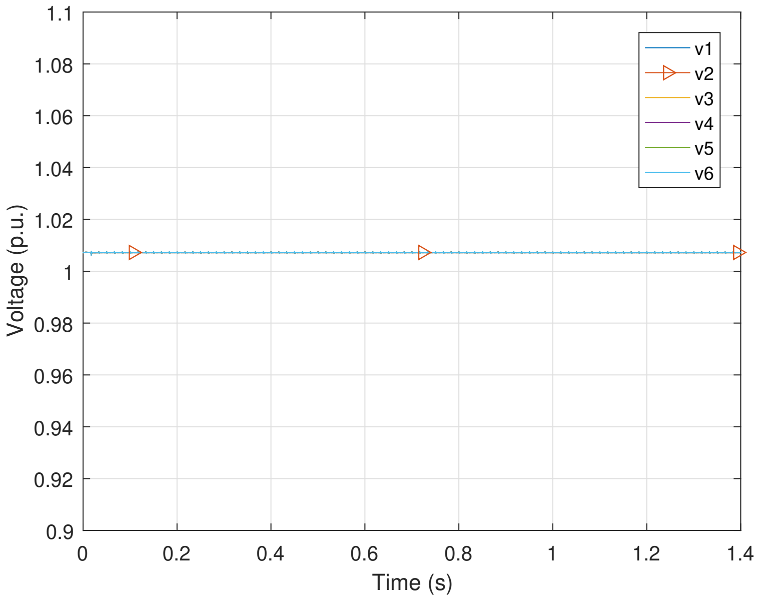

Figure 5-36: Voltage response of the system with the design 2 of the observer-based cooperative control under a hijacking attack of 60.2 Hz in the communication link of inverter 2 in $t = 1$ s.

			ATTACK							
			A. Controller				B. Communication Link			
			1. Constant Disturbance		2. Hijacking		1. Constant Disturbance		2. Hijacking	
			F Sync.	V Sync.	F Sync.	V Sync.	F Sync.	V Sync.	F Sync.	V Sync.
CONTROL	Cooperative Control		✓	✓	x	x	x	x	x	x
	Observer Design 1	F	✓	✓	✓	x	NA	NA	x	x
		F & V	✓	✓	✓	✓	x	✓	x	x
		Disconnection	NA	NA	✓	✓	NA	NA	NA	NA
	Observer Design 2	F	x	x	x	x	✓	✓	✓	✓
		F & V	NA	NA	NA	NA	✓	✓	✓	✓

Table 5-4: Performance response of the control schemes under different attack scenarios.

6 Conclusions and Recommendations

6.1. Conclusions

This document presents a cooperative control strategy that allows the synchronization of frequency and voltage under an attack of a constant disturbance addition in the controller. Also, a resilient observer-based cooperative control is presented for the synchronization of inverters under a hijacking attack in the controller.

For communication link attacks it is presented a more robust control strategy to guarantee the synchronization of inverters' frequency and voltage values. This strategy is also cooperative and is based on an observer with two estimation levels.

The three strategies presented, i.e., the conventional cooperative control and the observer-based cooperative controls with designs 1 and 2 are implemented for both voltage and frequency secondary levels. The inclusion of voltage control is crucial for an adequate synchronization and reference tracking.

The design of the proposed observer in Subsection 5.4.1 is focused on the internal dynamics of the system. Then for an attack in the controller, this approach presents a better response in the system. On the other hand, the design of the proposed observer in Subsection 5.4.2 is focused on the communication dynamics. Then, for communication link attacks, this approach is the most appropriate among the strategies presented.

An attack in the communication link is a very sophisticated attack that drives to trick the system. Hence, a conventional control technique is not sufficient to make the system resilient.

The response of the system when the affected node is disconnected presents the same behavior for all the control strategies under all the attack scenarios, i.e., the inverters follow the reference and reach the synchronization.

A sophisticated design of an attack considers hardly detectable perturbations. Hence, the disturbances are slight perturbations that destabilize the system but not sufficient to produce a breakdown. In consequence, in some cases, none control actions are executed, even when the system works wrongly.

6.2. Recommendations

The distributed architecture can be modified for hybrid architecture. A hybrid architecture enables similar knowledge to the provided from a full-connected graph but communicating data peer to peer. Hybrid models are a 4.0 industry and merge the best of both architectures centralized and distributed.

The benefits from both observers' schemes for control, i.e., the described in Subsections 5.4.1 and 5.4.2, can be combined into a hybrid control to make the system resilient to different cyber-attack scenarios.

In case that none control strategy responds appropriate for the system, the disconnection of the affected node is an alternative to reach the synchronization. This alternative avoids the propagation of the attack effects across the network.

The experiments' simulation should include the control models for both frequency and voltage in order to obtain a closer design for a real scenario. Many research works implement one of the models and assume a similar response in the other one.

Bibliografía

[1] Abhinav, S. ; Modares, H. ; Lewis, F. L. ; Ferrese, F. ; Davoudi, A.: Synchrony in Networked Microgrids Under Attacks. In: *IEEE Transactions on Smart Grid* 9 (2018), Nov, Nr. 6, S. 6731–6741. – ISSN 1949–3053

[2] Abhinav, S. ; Schizas, I. D. ; Davoudi, A.: Noise-resilient synchrony of AC microgrids. In: *2015 Resilience Week (RWS)*, 2015. – ISSN null, S. 1–6

[3] Amin, Saurabh ; Schwartz, Galina A. ; Sastry, S S.: Security of interdependent and identical networked control systems. In: *Automatica* 49 (2013), Nr. 1, S. 186–192

[4] Antsaklis, P.: Goals and Challenges in Cyber-Physical Systems Research Editorial of the Editor in Chief. In: *IEEE Transactions on Automatic Control* 59 (2014), Dec, Nr. 12, S. 3117–3119. – ISSN 2334–3303

[5] Ayas, M. S. ; Djouadi, S. M.: Undetectable sensor and actuator attacks for observer based controlled Cyber-Physical Systems. In: *2016 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2016. – ISSN null, S. 1–7

[6] Basseville, Michèle ; Nikiforov, Igor V. [u. a.]: *Detection of abrupt changes: theory and application.* Bd. 104. . Prentice Hall Englewood Cliffs, 1993

[7] Bidram, A. ; Davoudi, A.: Hierarchical Structure of Microgrids Control System. In: *IEEE Transactions on Smart Grid* 3 (2012), Dec, Nr. 4, S. 1963–1976. – ISSN 1949–3053

[8] Bidram, A. ; Davoudi, A. ; Lewis, F. L. ; Qu, Z.: Secondary control of microgrids based on distributed cooperative control of multi-agent systems. In: *IET Generation, Transmission Distribution* 7 (2013), Aug, Nr. 8, S. 822–831. – ISSN 1751–8687

[9] Bidram, A. ; Lewis, F. L. ; Davoudi, A.: Distributed Control Systems for Small-Scale Power

Networks: Using Multiagent Cooperative Control Theory. In: *IEEE Control Systems Magazine* 34 (2014), Dec, Nr. 6, S. 56–77. – ISSN 1066–033X

[10] Bidram, A. ; Lewis, F. L. ; Davoudi, A. ; Qu, Z.: Frequency control of electric power microgrids using distributed cooperative control of multi-agent systems. In: *2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems*, 2013. – ISSN null, S. 223–228

[11] Bidram, Ali: *Distributed cooperative control of AC microgrids*, The University of Texas at Arlington, Dissertation, 2014

[12] Bolden, Scott ; Bolden, Scott (Hrsg.): NARUC Releases Two New Cybersecurity Manual Resources. 2019. – Forschungsbericht. .

[13] Bollobás, Béla ; Axler, S. (Hrsg.) ; Gehring, F.w. (Hrsg.) ; Ribet, K.A. (Hrsg.): *Modern graph theory*. Bd. 184. 1. Springer Science & Business Media, 2013. – ISBN 978–1–4612–0619–4

[14] Chandorkar, M. C. ; Divan, D. M. ; Adapa, R.: Control of parallel connected inverters in standalone AC supply systems. In: *IEEE Transactions on Industry Applications* 29 (1993), Jan, Nr. 1, S. 136–143

[15] Chen, Chia-Mei ; Hsu, Sung-Chien ; Lai, Gu-Hsin: Defense Denial-of Service Attacks on IPv6 Wireless Sensor Networks. In: Zin, Thi T. (Hrsg.) ; Lin, Jerry Chun-Wei (Hrsg.) ; Pan, Jeng-Shyang (Hrsg.) ; Tin, Pyke (Hrsg.) ; Yokota, Mitsuhiro (Hrsg.): *Genetic and Evolutionary Computing*. Cham : Springer International Publishing, 2016. – ISBN 978–3–319–23204–1, S. 319–326

[16] Chen, Wei ; Xiao, Fei ; Liu, Jilong ; Wang, Hengli: Study on the topology of three-phase inverter systems based on parallel-connected bridges. In: *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC)* IEEE, 2013, S. 3678–3682

[17] Costantini, Lynn P. ; Acho, Matthew: *Understanding Cybersecurity Preparedness: Questions for Utilities*. 1. https://pubs.naruc.org/pub/3BACB84B-AA8A-0191-61FB-E9546E77F220: NARUC, June 2019

[18] Dhakne, A. R. ; Chatur, P. N.: Detailed Survey on Attacks in Wireless Sensor Network. In: Satapathy, Suresh C. (Hrsg.) ; Bhateja, Vikrant (Hrsg.) ; Joshi, Amit (Hrsg.): *Proceedings of*

the International Conference on Data Engineering and Communication Technology. Singapore : Springer Singapore, 2017. – ISBN 978–981–10–1678–3, S. 319–331

[19] Du, Xiaona ; Yu, Hui: Consensus of multi-agent systems with delayed sampled-data and directed topologies. In: *Neurocomputing* 363 (2019), S. 78 – 87. – ISSN 0925–2312

[20] Farwell, James P. ; Rohozinski, Rafal: Stuxnet and the future of cyber war. In: *Survival* 53 (2011), Nr. 1, S. 23–40

[21] Fax, J. A. ; Murray, R. M.: Information flow and cooperative control of vehicle formations. In: *IEEE Transactions on Automatic Control* 49 (2004), Sep., Nr. 9, S. 1465–1476. – ISSN 1558–2523

[22] García, Diana C.: Visión WEC en torno a la Transición Energética. In: *IV Seminario de Actualización en Sistemas Eléctricos* Rama Estudiantil de la IEEE Universidad Tecnológica de Pereira, 2019

[23] 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. In: *IEEE Transactions on Industrial Electronics* 58 (2011), Jan, Nr. 1, S. 158–172. – ISSN 1557–9948

[24] Guerrero, Josep M. ; Chandorkar, Mukul ; Lee, Tzung-Lin ; Loh, Poh C.: Advanced control architectures for intelligent microgrids, Part I: Decentralized and hierarchical control. In: *IEEE Transactions on Industrial Electronics* 60 (2013), Nr. 4, S. 1254–1262

[25] Hossam-Eldin, Ahmed ; Abdelsalam, Ahmed K. ; Refaey, Mostafa ; Ali, Ahmed A.: A topological review on recent improvements of three-phase impedance source inverter. In: *2017 Nineteenth International Middle East Power Systems Conference (MEPCON)* IEEE, 2017, S. 1106–1112

[26] Jadbabaie, A. ; Jie Lin ; Morse, A. S.: Coordination of groups of mobile autonomous agents using nearest neighbor rules. In: *IEEE Transactions on Automatic Control* 48 (2003), June, Nr. 6, S. 988–1001. – ISSN 1558–2523

[27] Jin, X. ; Haddad, W. M. ; Yucelen, T.: An Adaptive Control Architecture for Mitigating Sensor and Actuator Attacks in Cyber-Physical Systems. In: *IEEE Transactions on Automatic Control* 62 (2017), Nov, Nr. 11, S. 6058–6064. – ISSN 2334–3303

[28] Kaur, Gurjit ; Tomar, Pradeep ; Agrawal, Archit ; Singh, Prabhjot: Attacks and Their Solution at Data Link Layer in Cognitive Radio Networks. In: Somani, Arun K. (Hrsg.) ; Shekhawat, Rajveer S. (Hrsg.) ; Mundra, Ankit (Hrsg.) ; Srivastava, Sumit (Hrsg.) ; Verma, Vivek K. (Hrsg.): *Smart Systems and IoT: Innovations in Computing*. Singapore : Springer Singapore, 2020. – ISBN 978–981–13–8406–6, S. 351–361

[29] Khoo, S. ; Xie, L. ; Man, Z.: Robust Finite-Time Consensus Tracking Algorithm for Multirobot Systems. In: *IEEE/ASME Transactions on Mechatronics* 14 (2009), April, Nr. 2, S. 219–228. – ISSN 1941–014X

[30] Lewis, F.L. ; Zhang, H. ; Hengster-Movric, K. ; Das, A.: *Cooperative Control of Multi-Agent Systems: Optimal and Adaptive Design Approaches.* . Springer London, 2013 (Communications and Control Engineering). – ISBN 9781447155744

[31] Liu, X. ; Li, Z.: Local Load Redistribution Attacks in Power Systems With Incomplete Network Information. In: *IEEE Transactions on Smart Grid* 5 (2014), July, Nr. 4, S. 1665–1676. – ISSN 1949–3053

[32] LLC, The Cadmus G.: *Cybersecurity Preparedness Evaluation Tool.* 1. U.S.A: NARUC, Juni 2019

[33] Lopes, J. A. P. ; Moreira, C. L. ; Madureira, A. G.: Defining control strategies for MicroGrids islanded operation. In: *IEEE Transactions on Power Systems* 21 (2006), May, Nr. 2, S. 916–924

[34] Lu, Zhiguo ; Wu, Chunjun ; Zhao, Lili ; Zhu, Wanping: A new three-phase inverter built by a low-frequency three-phase inverter in series with three high-frequency single-phase inverters. In: *Proceedings of The 7th International Power Electronics and Motion Control Conference* Bd. 3 IEEE, 2012, S. 1573–1577

[35] Mehrizi-Sani, A. ; Iravani, R.: Potential-Function Based Control of a Microgrid in Islanded and Grid-Connected Modes. In: *IEEE Transactions on Power Systems* 25 (2010), Nov, Nr. 4, S. 1883–1891

[36] Mesbahi, Mehran ; Egerstedt, Magnus: *Graph theoretic methods in multiagent networks.* Bd. 33. . Princeton University Press, 2010. – ISBN 978–0–691–14061–2

[37] Mohan, Apurva ; Khurana, Himanshu: Implementing Cyber Security Requirements and

Mechanisms in Microgrids. In: Rice, Mason (Hrsg.) ; Shenoi, Sujeet (Hrsg.): *Critical Infrastructure Protection IX*. Cham : Springer International Publishing, 2015. – ISBN 978–3–319–26567–4, S. 229–244

[38] Mohsenian-Rad, A. ; Leon-Garcia, A.: Distributed Internet-Based Load Altering Attacks Against Smart Power Grids. In: *IEEE Transactions on Smart Grid* 2 (2011), Dec, Nr. 4, S. 667–674. – ISSN 1949–3053

[39] Mojica, Eduardo ; Toro, Wladimir ; Gaona, Eduardo ; Trujillo, Leonardo: *Control de microrredes eléctricas inteligentes*. Primera Edición. Editorial Universidad Distrital, April 2017. – ISBN 978–958–5434–31–8

[40] Mwakabuta, N. ; Sekar, A.: Comparative Study of the IEEE 34 Node Test Feeder under Practical Simplifications. In: *2007 39th North American Power Symposium*, 2007. – ISSN null, S. 484–491

[41] Nagireddy, Vyshnavi ; Parwekar, Pritee: Attacks in Wireless Sensor Networks. In: Satapathy, Suresh C. (Hrsg.) ; Bhateja, Vikrant (Hrsg.) ; Das, Swagatam (Hrsg.): *Smart Intelligent Computing and Applications*. Singapore : Springer Singapore, 2019. – ISBN 978–981–13–1927–3, S. 439–447

[42] Nasirian, V. ; Shafiee, Q. ; Guerrero, J. M. ; Lewis, F. L. ; Davoudi, A.: Droop-Free Distributed Control for AC Microgrids. In: *IEEE Transactions on Power Electronics* 31 (2016), Feb, Nr. 2, S. 1600–1617. – ISSN 1941–0107

[43] Nguyen, T. L. ; Tran, Q. ; Caire, R. ; Gavriluta, C. ; Nguyen, V. H.: Agent based distributed control of islanded microgrid AC Real-time cyber-physical implementation. In: *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2017, S. 1–6

[44] Olfati-Saber, R. ; Murray, R. M.: Consensus problems in networks of agents with switching topology and time-delays. In: *IEEE Transactions on Automatic Control* 49 (2004), Sep., Nr. 9, S. 1520–1533. – ISSN 1558–2523

[45] Palizban, O. ; Kauhaniemi, K.: Secondary control in AC microgrids challenges and solutions. In: *2015 International Conference on Smart Cities and Green ICT Systems (SMARTGREENS)*, 2015, S. 1–6

[46] Pasqualetti, F. ; Bicchi, A. ; Bullo, F.: Consensus Computation in Unreliable Networks:

A System Theoretic Approach. In: *IEEE Transactions on Automatic Control* 57 (2012), Jan, Nr. 1, S. 90–104. – ISSN 0018–9286

[47] Pasqualetti, Fabio ; Dörfler, Florian ; Bullo, Francesco: Attack detection and identification in cyber-physical systems. In: *IEEE transactions on automatic control* 58 (2013), Nr. 11, S. 2715–2729

[48] Puentes, Camila: Conferencia Técnica. In: *IV Seminario de Actualización en Sistemas Eléctricos* Rama Estudiantil de la IEEE Universidad Tecnológica de Pereira, 2019

[49] Ren, W.: Second-order Consensus Algorithm with Extensions to Switching Topologies and Reference Models. In: *2007 American Control Conference*, 2007. – ISSN 2378–5861, S. 1431–1436

[50] Ren, Wei ; Atkins, Ella: *Second-order Consensus Protocols in Multiple Vehicle Systems with Local Interactions.* . 2005. – . S

[51] Ren, Wei ; Moore, Kevin L. ; Chen, Yangquan: High-Order and Model Reference Consensus Algorithms in Cooperative Control of MultiVehicle Systems. In: *Journal of Dynamic Systems, Measurement, and Control* 129 (2006), 12, Nr. 5, S. 678–688. – ISSN 0022–0434

[52] Shafiee, Q. ; Guerrero, J. M. ; Vasquez, J. C.: Distributed Secondary Control for Islanded Microgrids - A Novel Approach. In: *IEEE Transactions on Power Electronics* 29 (2014), Feb, Nr. 2, S. 1018–1031. – ISSN 1941–0107

[53] Shi, D. ; Guo, Z. ; Johansson, K. H. ; Shi, L.: Causality Countermeasures for Anomaly Detection in Cyber-Physical Systems. In: *IEEE Transactions on Automatic Control* 63 (2018), Feb, Nr. 2, S. 386–401. – ISSN 0018–9286

[54] Slay, Jill ; Miller, Michael: Lessons learned from the maroochy water breach. In: *International Conference on Critical Infrastructure Protection* Springer, 2007, S. 73–82

[55] de Souza, A. C. Z. ; De Nadai N., B. ; Portelinha, F. M. ; Marujo, Diogo ; Oliveira, D. Q.: Microgrids Operation in Islanded Mode. In: Azzopardi, Brian (Hrsg.): *Sustainable Development in Energy Systems.* Cham : Springer International Publishing, 2017. – ISBN 978–3–319–54808–1, S. 193–215

[56] Sun, F. ; Tuo, M. ; Li, Y. ; Liu, F.: Finite-time Consensus for First-order Multi-agent Systems

with Measurement Noises. In: *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, 2019, S. 1818–1822

[57] Tran, Van-Thuan ; Nguyen, Minh-Khai ; Yoo, Myoung-Han ; Choi, Youn-Ok ; Cho, Geum-Bae: A three-phase cascaded H-bridge quasi switched boost inverter for renewable energy. In: *2017 20th International Conference on Electrical Machines and Systems (ICEMS)* IEEE, 2017, S. 1–5

[58] Vasquez, J. C. ; Guerrero, J. M. ; Miret, J. ; Castilla, M. ; de Vicuna, L. G.: Hierarchical Control of Intelligent Microgrids. In: *IEEE Industrial Electronics Magazine* 4 (2010), Dec, Nr. 4, S. 23–29. – ISSN 1932–4529

[59] Wu, Bin ; Narimani, Mehdi: Cascaded H-bridge multilevel inverters. (2017)

[60] Wu, Lizhen ; Yang, Xusheng ; Zhou, Hu ; Hao, Xiaohong: Modeling and Stability Analysis for Networked Hierarchical Control of Islanded Microgrid. In: Deng, Zhidong (Hrsg.) ; Li, Hongbo (Hrsg.): *Proceedings of the 2015 Chinese Intelligent Automation Conference.* Berlin, Heidelberg : Springer Berlin Heidelberg, 2015. – ISBN 978–3–662–46463–2, S. 91–99

[61] Yamaguchi, Hiroaki ; Arai, Tamio ; Beni, Gerardo: A distributed control scheme for multiple robotic vehicles to make group formations. In: *Robotics and Autonomous Systems* 36 (2001), Nr. 4, S. 125 – 147. – ISSN 0921–8890

[62] Yang, Yanping ; Zhang, Xian-Ming ; He, Wangli ; Han, Qing-Long ; Peng, Chen: Sampled-position states based consensus of networked multi-agent systems with second-order dynamics subject to communication delays. In: *Information Sciences* 509 (2020), S. 36 – 46. – ISSN 0020–0255

[63] Yu, W. ; Wen, G. ; Chen, G. ; Cao, J.: *Distributed Cooperative Control of Multi-agent Systems.* . Wiley, 2017. – ISBN 9781119246206

[64] Yu, Wenwu ; Zheng, Wei X. ; Chen, Guanrong ; Ren, Wei ; Cao, Jinde: Second-order consensus in multi-agent dynamical systems with sampled position data. In: *Automatica* 47 (2011), Nr. 7, S. 1496 – 1503. – ISSN 0005–1098

[65] Zhang, H. ; Lewis, F. L. ; Das, A.: Optimal Design for Synchronization of Cooperative Systems: State Feedback, Observer and Output Feedback. In: *IEEE Transactions on Automatic Control* 56 (2011), Aug, Nr. 8, S. 1948–1952. – ISSN 1558–2523