Research paper

REVISTA Ingeniería

Optimized Hierarchical Control for an AC Microgrid Under Attack

Control Jerárquico Optimizado para una Microrred de CA Bajo Ataque

***Vladimir Toro*[*,1], *Eder Baron-Prada*[1], *Eduardo Mojica-Nava*[1]**

[1]Universidad Nacional de Colombia

[*]Correspondence email: bwtorot@unal.edu.co

Received: 30-08-2018. Modified: 09-11-2018. Accepted: 22-01-2019

Abstract

Context: An inverter-based microgrid working in islanded mode can suffer cyber-attacks, these can be done against either the local controller or the communication links among the inverters. Secondary control is able to reject those attacks, however, a tertiary control action is necessary in order to stabilize the power flow among the microgrid.

Method: Confidence factor technique allows to reject attacks in a microgrid acting directly over the secondary control, however, this technique omits other factor related to the power available. In this case, secondary control was complemented with a tertiary control that includes optimization criteria.

Results: An inverter-based microgrid is simulated in Matlab for different scenarios and under cyber-attack, this allows checking the correct response of the controller under attacks and the effective power-sharing among inverters.

Conclusions: The tertiary control allows stabilizing the active power of the system after the rejection of a cyber-attack by the secondary control. Each inverter supplies active power according to its maximum power rating without affecting the stability of the whole system.

Keywords: Microgrid, cyber-attack, distributed control, hierarchical control

Language: English.

Cite this paper as: V. Toro, E. Baron-Prada, E. Mojica-Nava.: Optimized Hierarchical Control for an AC Microgrid Under Attack, Vol. 24, Num. 1 pp. 64-82, Jan-Apr 2019 .

DOI: https://doi.org/10.14483/23448393.13760

Resumen

Contexto: Una microrred de CA (corriente alterna) basada en inversores y que funciona en modo isla puede ser víctima de ciberataques, estos pueden ir contra el controlador o contra el sistema de comunicaciones entre los nodos; el control secundario puede rechazar el ataque, sin embargo, la acción de un controlador terciario es necesaria para estabilizar el flujo de potencia en la microrred.
Método: La técnica basada en factores de confianza permite repeler ataques a la microrred actuando directamente sobre el controlador secundario, sin embargo, esta técnica omite factores de optimización; en este caso, las señales de control generadas a partir de los factores de confianza fueron complementadas en un controlador terciario para incluir criterios de optimización.
Resultados: Se simula una microrred en Matlab para diferentes escenarios y ataques, permitiendo verificar la acertada respuesta del controlador ante ataques cibernéticos.
Conclusiones: El control terciario permite estabilizar la potencia del sistema ante el rechazo de un ciberataque por parte del control secundario. Cada inversor entrega potencia de acuerdo con su rango máximo de potencia, sin afectar la estabilidad de todo el sistema.
Palabras clave: Ciberataque, control distribuido, control jerárquico, microrred

1. Introduction

A microgrid consists of a set of distributed generators and energy storage devices connected to a common DC or AC bus, where loads can be connected with the distributed generators or directly to the common bus [1]. Additionally, a microgrid can work either connected to a distribution network or in an islanded mode. A microgrid, based on inverters, is controlled by a three-level hierarchical scheme, usually, assuming a decoupling between active and reactive power, and a highly inductive output impedance at each inverter. Thus, a direct relation between active power and frequency can be assumed [2]. Primary control is usually decentralized and based on droop control, this allows to avoid high circulating current and the power-sharing condition (the condition in which each inverter supply power according to its maximum power rating) is guaranteed [3]. Secondary control is in charge to return voltage and frequency to its reference values, this can be done either in a centralized or distributed manner [4]. Finally, tertiary control is generally centralized and allows solving optimization problems and economic dispatch [5].

A microgrid controlled in a distributed way can be prone to cyber-attacks. Those can be done over an inverter controller or actuator, and attacks over a communication link [6]. Attacks can be repelled including a variable gain term in the frequency secondary control which includes reliability factors such as *confidence factor* related with the information measured at each inverter, and *trust factor* related with the reliability of the data received from the other inverters. These factors use a distance measure through a Euclidean norm given by the error between the measured frequency and the frequency of reference, compared with an already defined threshold value.

Dynamic gains are included directly over the secondary control of each inverter. However, those factors do not consider the power availability of each one, and there is not an optimization criteria to repeal the cyber-attack without saturating some of the inverters. These optimal references not only guarantee that the cyber-attack is repelled but also, keep the signal inside the limits allowed by the system.

This document is organized as follows: Section 2 presents the equation for primary and secondary control and the equations for attack rejection. Section 3 presents the basics of tertiary control, the economic dispatch problem and the design of the controller based on the population games approach. Simulation results are presented in Section 4, and finally, conclusions are shown in Section 5.

2. Hierarchical Control and Cyber-Attacks Over an AC Microgrid

This section shows the design of primary and secondary controllers for an AC microgrid. Assuming a linear relationship between frequency and active power secondary control is designed following a distributed scheme in which two consensus equations are used: one for achieving power sharing, and the other for synchronization purposes. Next, the equation for cyber-attack rejection [6] is considered.

2.1. Distributed frequency control

An inverter based AC microgrid is controlled following a hierarchical frame. In the first level, the primary control avoids the appearing of high circulating currents when inverters are connected in parallel. Primary control drops the frequency according to the active power demanded by loads [3], this linear relation is represented by (1)

$$f_i = f_{ref} - m_i(P_i - P_i^*) \tag{1}$$

where f_{ref} is the frequency of reference in Hz, m_i is the droop coefficient, P_i is the medium power at inverter i, and P_i^* is the active power reference for inverter i.

The power reference value P_i^* can be modified based on the requirements of each inverter or some programmed event. However, reference values cannot be achieved only by primary control, because in an isolated microgrid not always the power generated equals the power demanded [7]. In fact, those values are better generated by a tertiary control capable of optimize them according to power availability criteria.

Primary control also assures that each inverter supplies power according to its maximum active power value, a condition known as power-sharing presented in (2)

$$mp_1 = mp_2 = mp_i = \cdots = mp_j \tag{2}$$

Then, the equation that represents the frequency for inverter i in an a.c microgrid with primary droop control, and secondary frequency control [4] is given by

$$f_i = f_{ref} - m_i P_i + \delta f_i \tag{3}$$

where δf_i is the secondary control term.

The secondary control shifts the droop control function returning the frequency to its reference value. Secondary frequency control can include a leader node (not necessarily unique) that knows the reference value. So, consensus problem changes into a synchronization problem. Secondary control is given by (4)

$$\delta f_i = \sum_{N_{ij}} a_{ij}(mp_j - mp_i) + \sum_{N_{ij}} a_{ij}(f_j - f_i) + g_i(f_{ref} - f_i) \tag{4}$$

where N_{ij} is the set of neighbors of agent i, a_{ij} represents the ij-th elements of the adjacency matrix, f_i y f_j are the frequencies measured in the inverters i and j, respectively. g_i represent the elements of the pinning vector, and f_{ref} represents the frequency reference value.

2.2. Cyber-attacks over an AC microgrid

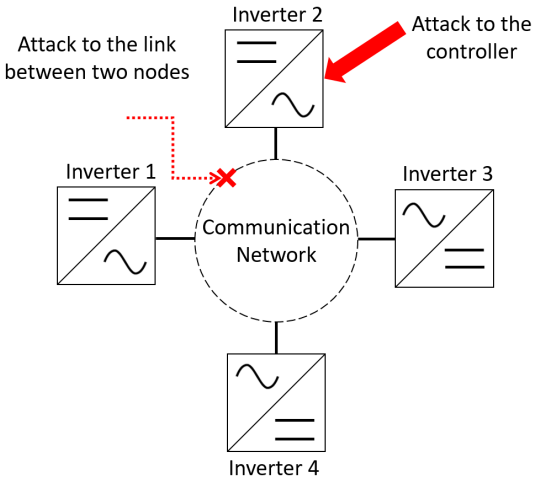

Figure 1. Types of attacks in a microgrid

A distributed control gathers data from neighbors through a local communication system, because of this is more susceptible to cyber-attacks. According to Figure 1 attacks can be classified as attacks to local controllers, and attacks to the communications links between nodes [8].

If the attack occurs over the controller of the i-th inverter, the frequency at inverter i is given by (5)

$$f_i^c = f_i + \eta_i f_i^a \tag{5}$$

where f_i^c is the corrupted frequency at inverter i after the attack, η_i indicates if there is an attack or not, and f_i^a is a perturbation injected by the controller.

Similarly, if the attack occurs in the link between two nodes this is model as it is shown in (6)

$$f_i^j = f_i + \eta_i f_i^a \tag{6}$$

where f_i^j is the frequency measured between inverters i and j, and η_i indicates the presence of the attack [8].

The error in inverter i is given by (7)

$$e_i = \sum_{N_{ij}} a_{ij}(\hat{f}_j - \hat{f}_i) + g_i(f_{ref} - \hat{f}_i) \tag{7}$$

where the values $\hat{f}_i$ and $\hat{f}_j$ correspond to the observed values in the nodes i and j, respectively.

So, it is defined as the norm of the error (7) as

$$\varepsilon_i = \|e_i\| \tag{8}$$

and the sum of the norms of the errors as

$$\sigma_i = \sum_{N_{ij}} a_{ij}\|(\hat{f}_j - \hat{f}_i)\| + g_i\|(f_{ref} - \hat{f}_i)\| \tag{9}$$

Then, the following factor is defined

$$d_i(t) = \frac{\Delta_i}{\Delta_i + \|\sigma_i(t) - \varepsilon_i(t)\|} \tag{10}$$

where Δ_i represents a threshold value that considers the effect of other factors rather than attacks. Having into account this factor, the confidence factor is defined as

$$\dot{C}_i(t) = \alpha d_i(t) - \alpha C_i(t) \tag{11}$$

The confidence factor only can take values between zero and one $(0 \leq C_i \leq 1)$.
The control of frequency is modified as it is shown in (12)

$$\dot{\hat{f}}_i = \sum_{N_{ij}} a_{ij} C_j(t)(\hat{f}_j - \hat{f}_i) + g_i(f_{ref} - \hat{f}_i) \tag{12}$$

The trust factor is another coefficient that determines the reliability of the measures that a node received from its neighbors. The measurements that exceed the threshold value are rejected. First, it is calculated the factor defined in (16)

$$s_{ij} = \frac{\Theta_i}{(\Theta_i + \|\hat{f}_j(t) - \frac{1}{|N_i|}\sum_{N_i} \hat{f}_k(t)\|)} \tag{13}$$

where Θ_i corresponds to a threshold value, and $|N_i|$ is the number of neighbors of the inverter.
The trust factor is defined as

$$\dot{b}_{ij}(t) = \xi s_{ij}(t) - \xi b_{ij}(t) \tag{14}$$

$$T_{ij} = max(C_i(t), b_{ij}(t)) \tag{15}$$

where $0 \leq T_{ij} \leq 1$.

The control of frequency is modified as it is shown in (16)

$$\dot{\hat{f}}_i = \sum_{N_{ij}} a_{ij} C_j(t) T_{ij}(t)(\hat{f}_j - \hat{f}_i) + g_i(f_{ref} - \hat{f}_i) \tag{16}$$

Assuming an AC microgrid with predominantly inductive transmission lines, the instantaneous active power exchange is given by the following expression

$$p_i = \sum_{j \in N_i}^{n} |Y_{ij}| E_i E_j (\theta_j - \theta_i), \tag{17}$$

where $|Y_{ij}|$ is the magnitude of the line admittance between inverter i and j, V_i and V_j are the bus voltages at inverters i and j, respectively.

Taking the first derivative of p along time, and considering the relation $\dfrac{d\theta_i}{dt} = \omega_i$, expression (17) becomes

$$\dot{p}_i = \sum_{j \in N_i}^{n} |Y_{ij}| E_i E_j (f_j - f_i), \tag{18}$$

Taking the first derivative of (3) along time expression is written as

$$\dot{f}_i = -m_i \dot{P}_i + \dot{\delta} f_i \tag{19}$$

Then replacing (18), and (16) in (19) the following expression is obtained

$$\dot{f}_i = -m_i \left[\sum_{j \in N_{ij}} b_{ij} |Y_{ij}| E_i E_j (f_j - f_i) \right] + C_j(t) T_{ij}(t) \left[\sum_{j \in N_{ij}} a_{ij}(f_j - f_i) + (f_{ref} - f_i) \right] \tag{20}$$

Expression (20) is written in matrix form as follows

$$\dot{\Delta} F = -M L_c F - CT(L + G)F, \tag{21}$$

where M is a diagonal matrix with the droop coefficients, L_c is a Laplacian matrix for the physical connection among inverters whose values are given by $\omega ij = E_i E_j |Y_{ij}|$, F is the vector that contains the frequency measured at each inverter, C and T are diagonal matrices whose values are the coefficient and trust parameters, respectively. L is the Laplacian matrix who represents the connections among agents. G is the diagonal matrix that determines if an agent is a leader or not.

Expression (21), can be written as $\dot{\Delta} F = -(ML_c + CT(L+G))F$, the solution of this differential equation is of the form $F(t) = Ae^{-t(ML_c + CT(L+G))}$. This expression is asymptotically stable if term $ML_c + CT(L+G)$ remains positive. Notice that, Laplacian matrices are positive defined, as matrices M, C, T, and G are diagonal matrices whose values are real and positive, the product of those matrices is positive defined too, then the expression holds.

3. Tertiary Control for Active Power Control

In this section, the design of the tertiary control is presented. The economic dispatch problem is introduced, and then a population game approach is studied. Tertiary control gathers information of power consumption from the whole microgrid, and based on this data, generates the signal for each inverter according to optimization criteria.

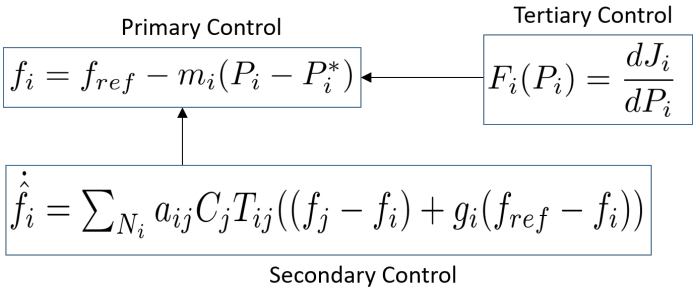

Figure 2. Hierarchical control layers

Tertiary control sends the set-point values for primary control at each inverter. As it is shown in Figure 2 primary control uses the frequency droop control with power reference P_i^*, this value is sent by tertiary control after an optimization process represented by functional $F_i(P_i)$. Additionally, secondary control sends the frequency reference value to the droop control and receive the information of frequency and active power value from each inverter.

Next, an economic dispatch control strategy is presented. This control algorithm sets the optimal power values for each generator based on economic criteria. Then some basics concepts of the proposed population games approach are shown.

3.1. Economic Dispatch Problem

Tertiary control is considered the last layer in hierarchical control, and it is related with the optimization of the dispatch of the resources available in the power system, which is also called economic dispatch [9], [10]. Economic dispatch is a highly studied problem, some approaches use convex optimization methods, principally derived from the work of Nedić et al. in [11], based on this work several approaches have been made [12]–[14]. Moreover, other approaches using game theoretical approaches have been made [15]–[18] proving the effectiveness of game theory to handle economic dispatch problems. Tertiary control can be either centralized or distributed, distributed controllers are used in large-scale systems where centralized controllers often suffer from computation and communication overheads. However, instead of several advantages of distributed controllers, centralized controllers are highly used due to their robustness and easily configured and maintained under operation.

Economical dispatch denotes the problem of determining the optimum output power of a set of generators in a power system in order to satisfy loads and fulfill power system requirements. Economic dispatch problem consists of minimizing the total generation cost [18], [19]. Here, the cost of the power supplied by each generator is minimized using an utility function based on a

quadratic function [12], [13], [20] such as

$$F(p_i) = \frac{\alpha_i}{2} p_i^2 + \beta_i p_i + \zeta \tag{22}$$

where $F(p_i)$ is the utility function of generator i, p_i is the power generated by generator i. Moreover, $\alpha_i, \beta_i, \zeta \in \mathbb{R}_{\geq 0}$ are utility coefficients. Using the utility function of all agents in the power system we can formulate the economic dispatch problem as follows

$$\begin{aligned} \underset{p_i \ \forall \ i \in G}{\text{minimize}} \quad & \sum_{i=0}^{N} F(p_i) \\ \text{subject to} \quad & \sum_{i=0}^{N} p_i = P_L \\ & \overline{p_i} \geq p_i \geq \underline{p_i} \quad \forall i \in G \end{aligned} \tag{23}$$

where P_L is the power demanded by the load in the system, N is the number of generators in the power system, $\overline{p_i}$ and $\underline{p_i}$ are the maximum and minimum power capacity respectively. Economic dispatch problem in (23) is solved when constraints (23) and (23) are fulfilled, moreover the economic dispatch criterion states that all agents should operate with the same marginal utilities as follows

$$\theta = \frac{\partial F(p_1)}{\partial p_1} = \frac{\partial F(p_2)}{\partial p_2} = \cdots = \frac{\partial F(p_N)}{\partial p_N} \tag{24}$$

where $\theta \in \mathbb{R} > 0$. In order to solve (23) a game theoretical method based on population games is used, specifically, replicator dynamics solve iteratively the economic dispatch problem using criterion (24). The before statement can be summarized in the following lemma

Lemma 1 *A solution of problem (23), P^* belonging to the feasible set Δ, is an optimal solution if and only if $\nabla_i S_W(P_i^*) = \nabla_j S_W(P_j^*)$ for all i, j.*

3.2. Population Games Approach

One of the main contributions of this work is to optimize, through a tertiary control, the response of a microgrid against an attack. In order to reach this contribution, a centralized population dynamics control based on game theory is proposed. Population dynamics represent how a pure population strategy progress over time. In population games, replicator dynamics have been used in several engineering applications such as economic power dispatch, lighting systems, and urban drainage systems [18]. These applications have been made considering some implementation benefits, such as robustness to dynamic environmental uncertainties.

The replicator dynamics solves the economic dispatch problem as a resource allocation problem. Replicator dynamics considers $G = \{1, 2, 3 \ldots N\}$ finite number of generators, who adopt a i-th strategy from a finite set of pure strategies. Accordingly, to achieve an appropriate performance in the steady state, the power demanded by the load should be the sum of all power set points. The

payoff function (F_i) is associated with the chosen strategy, therefore, a continuous time implementation is also used. In its general form, the replicator dynamics can be represented as

$$\dot{p}_i = \beta(F_i - \bar{F}(\mathbf{p}))p_i \tag{25}$$

where β is a parameter that permits modify the convergence speed [21]. The average payoff in the population $\bar{F}(\mathbf{p})$ is given by

$$\bar{F}(\mathbf{p}) = \frac{1}{P_L}\sum_{i=0}^{N} p_i F_i \tag{26}$$

The results in [22] are used to guarantee the power balance, the choice of (26) guarantees the invariance of the constraint set Δ defined as

$$\Delta = \left\{ p_i \in \mathbb{R}^N_{\geq 0} : \sum_{i=0}^{N} p_i = P_L \right\} \tag{27}$$

This result ensures that if $p_i(0) \in \Delta$, $\forall i \in G$, all $p_i(t) \in \Delta$ with $t \geq 0$. In other words, the power demanded by the loads in the system always is dispatched i.e, the replicator dynamic algorithm guarantees a perfect balance between the power demanded and the power generated. One of the characteristics of the replicator dynamics algorithm is that in the stationary state the fitness function of all agents is equal to the average fitness $(\bar{F})$. This condition allows solving the problem of economic dispatch through the replicator dynamics since the fitness function is derived from the utility function. In order to include the constraints in (23), we use Lagrange Multipliers as

$$L(p, \mu) = \sum_{i=0}^{N} F(p_i) + \mu(\mathbf{R}p - r) \tag{28}$$

where μ is the Lagrange Multipliers, the fitness functions are defined as

$$\nabla_p L(p, \mu) = \nabla \sum_{i=0}^{N} F(p_i) + \mathbf{R}^\top \mu = F(p) \tag{29}$$

$$\nabla_\mu L(p, \mu) = -\mathbf{R}p + r = F(\mu) \tag{30}$$

Finally, the fitness functions for this replicator dynamics are

$$F(p_i) = \alpha_i p_i + \beta_i + \mu_i \qquad \forall i \in G \tag{31}$$

$$F(\mu) = -\sum_{i=1}^{N} p_i + r \qquad \forall i \in G \tag{32}$$

Notice that ∇ stands for the Jacobian of a function. Now, we state the following theorem in order to characterize the optimality of the proposed algorithm

Theorem 1 *Assume a convergence constant $\beta \in \mathbb{R}$. Furthermore, let $P_i(k)$, with $i \in \mathcal{N}$, being the set points generated by executing (25), with fitness functions defined as in (31) and (32). Then, $P_i(k)$ with $i \in \mathcal{N}$ converges to the optimal solution P_i^* that belongs to the feasible set of power, that is*

$$\lim_{k \to \infty} P_i(k) = P_i^*.$$

Proof.

Since we have defined fitness functions as (31) and (32), by definition a potential function for the population game (25) is $h(P,\mu) = \mathcal{L} = S_W(P) - \mu^\top(\mathbf{R}P - r)$ and considering the form of the economic dispatch in (23), it can be shown that the game satisfies the external symmetry (24). When the optimality condition in Lemma 1 is reached then $F_i(p_i) = F_j(p_j)$ for all i, j and it is noticed that in the replicator dynamics (25) we have

$$\beta\left(F_i - \frac{1}{P_L}\sum_{i=0}^{N} p_i F_i\right) p_i = \beta\left(F_j - \frac{1}{P_L}\sum_{i=0}^{N} p_i F_i\right) p_j \tag{33}$$

To reach optimality, both sides of the equation must be equal. At the optimal point, this only can be equal to zero. It is possible to see through Lemma 1, that

$$F_i = F_j \ ... \ \forall\, i, j \in \mathcal{N} \tag{34}$$

Then, it is possible to see that

$$F_j = \frac{1}{P_L}\sum_{i=0}^{N} p_i F_i \tag{35}$$

Then, (33) is

$$\beta\,(0)\, p_i = \beta\,(0)\, p_j \tag{36}$$

$$= 0 \tag{37}$$

which implies that (25) reaches an optimal point. ■

4. Simulation Results

A five inverter-based microgrid is simulated using Simulink®, inverters are considered as controlled three-phase voltage sources. Each inverter is connected to a common bus in parallel as it is shown in Figure 3. Three different scenarios are simulated: the first one shows the performance of tertiary control without any attack; the second one shows the performance of controllers when the controller of inverter one is attacked, and finally, the third one shows the performance of the system when false data is added to the measured frequency at inverter one.

Microgrid parameters are presented in Table I. Each inverter has a different nominal active power value, and a different low-pass filter constant. Transmission lines among inverters are considered similar to visualized clearly the changes introduced by tertiary and secondary control.

The five inverter microgrid has a communication system defined by an undirected graph with its related adjacency matrix as it is shown in Figure 4.

The nominal power for each inverter is set at the tertiary control: $Pnom_1 = 1000$W, $Pnom_2 = 2000$W, $Pnom_3 = 4000$W, $Pnom_4 = 6000$W, $Pnom_5 = 7000$W.

First case A load $P_{load} = 20000$W is connected at $t = 1$s and a similar load is connected at $t = 4$s.

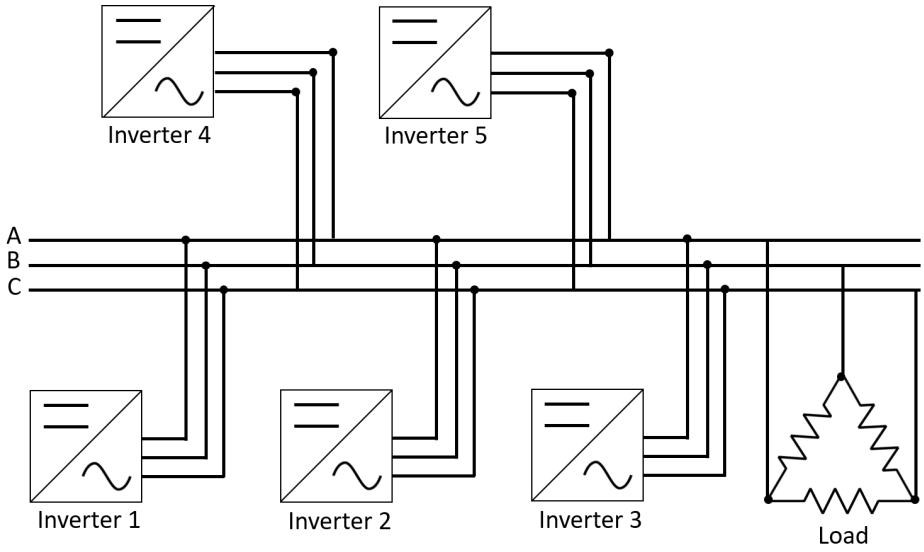

Figure 3. Microgrid Schematic

Table I. Microgrid Parameters

	$P_{max}(kW)$	$m = \frac{\Delta f}{P_{max}}$	$\tau(s)$	$R(\Omega)$	$L(mH)$
Inverter 1	2	$5 * 10^{-5}$	0,01	0.1	1
Inverter 2	4	$2{,}5 * 10^{-5}$	0,02	0.1	1
Inverter 3	5	$2 * 10^{-5}$	0,03	0.1	1
Inverter 4	8	$1{,}25 * 10^{-5}$	0,04	0.1	1
Inverter 5	10	$1 * 10^{-5}$	0,05	0.1	1

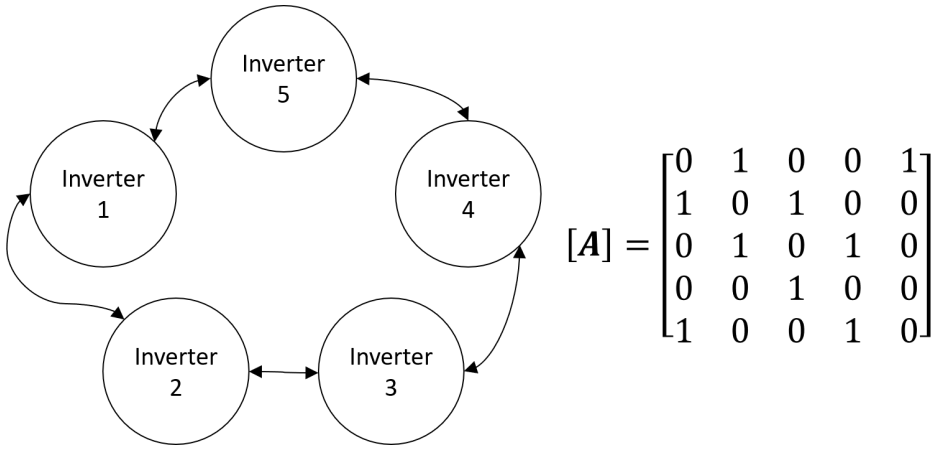

Figure 4. Graph representation and adjacency matrix of the communication links between nodes

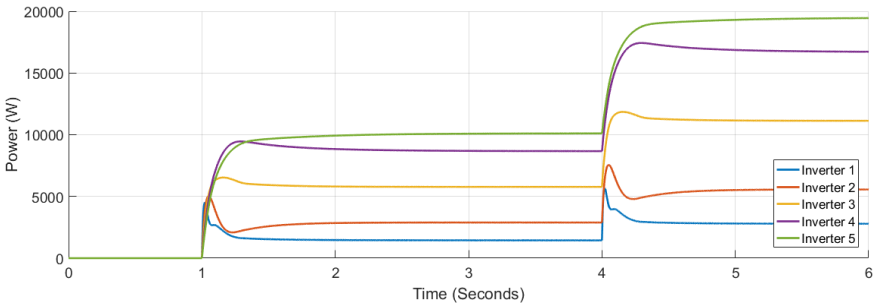

Figure 5. Active power for each inverter

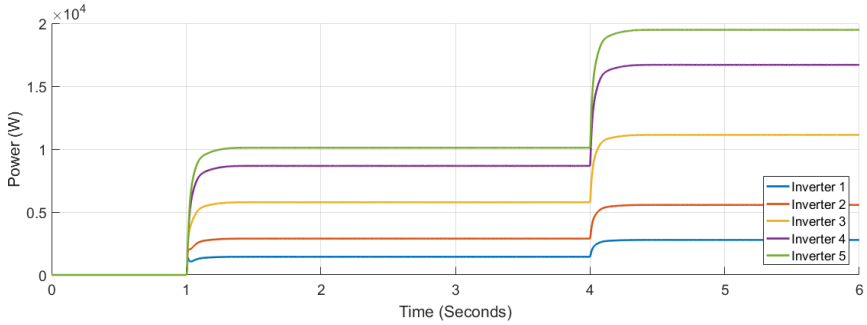

Figure 6. Output from tertiary controller

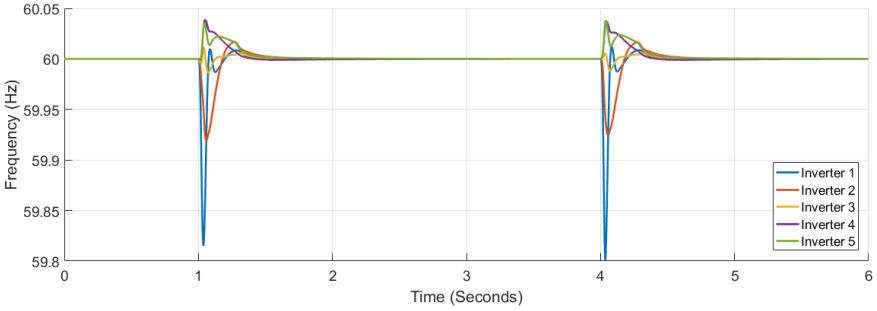

Figure 7. Frequency measured at each inverter

Figure 5 shows the power at each inverter when loads are connected at $t = 1$s and $t = 4$s. The action of tertiary control is implicit in the behavior of power-sharing at each inverter, so its power capacity is taken into account. Tertiary control action is depicted in Figure 6 while Figure 7 shows the behavior of frequency at each inverter, notice that the changes at $t = 1$s and $t = 4$s when loads are connected are similar, and frequency reference value is achieved in steady state. Figure 8 and Figure 9 show the behavior of confidence and trust values when the microgrid is not under attack. Trust and confidence values drop to less than 0.2 when their threshold values are set at 0.9.

Second case A load $P_{load} = 20000$W is connected at $t = 0{,}5$s and a false data signal is introduced controller of inverter 1 between t =2s and t =4s.

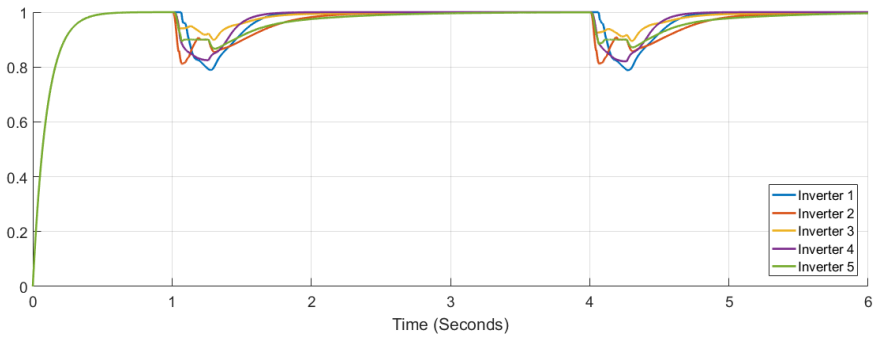

Figure 8. Confidence factor

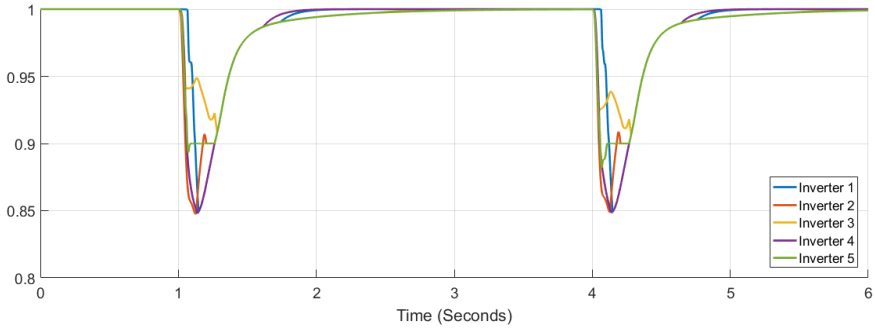

Figure 9. Trust factor

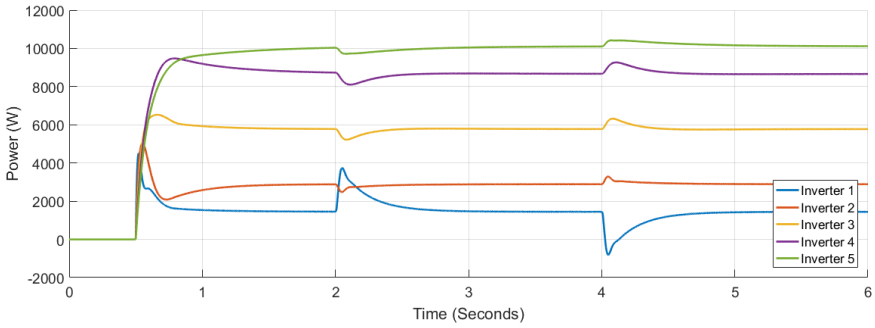

Figure 10. Active power for each inverter under attack in case 2

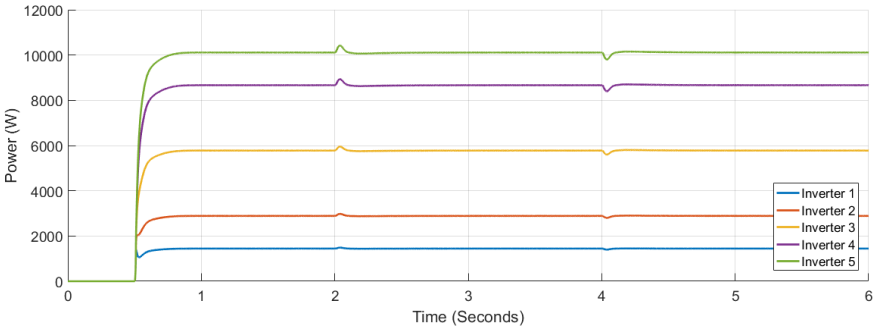

Figure 11. Output from tertiary controller when is under attacks in case 2

Figure 10 and Figure 11 show the active power supplied by each inverter, and the tertiary control response, respectively. Inverter 1 is able to supply or to absorb active power. At Figure 12 frequency variations appears at $t = 0{,}5$s when the load is connected, and at $t = 2$s and $t = 4$s when false data is introduced at the controller of inverter one. Finally, in Figure 13 and Figure 14 a variation of less than 0.2 for confidence and 0.1 for trust is shown. Notice that only for the trust coefficient the threshold value of 0.9 is achieved.

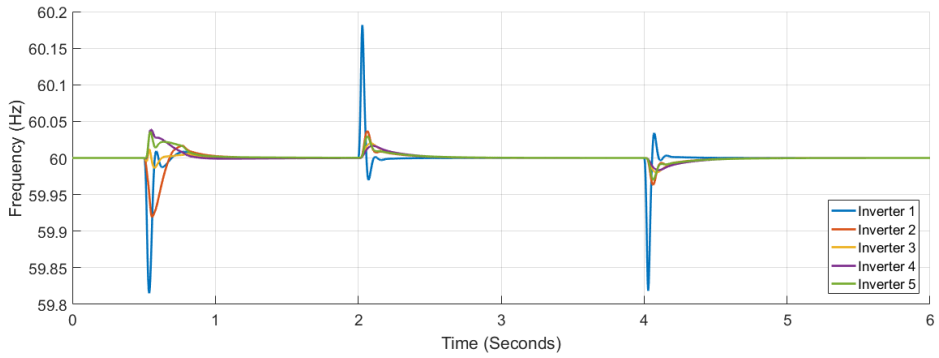

Figure 12. Frequency measured at each inverter when under attack

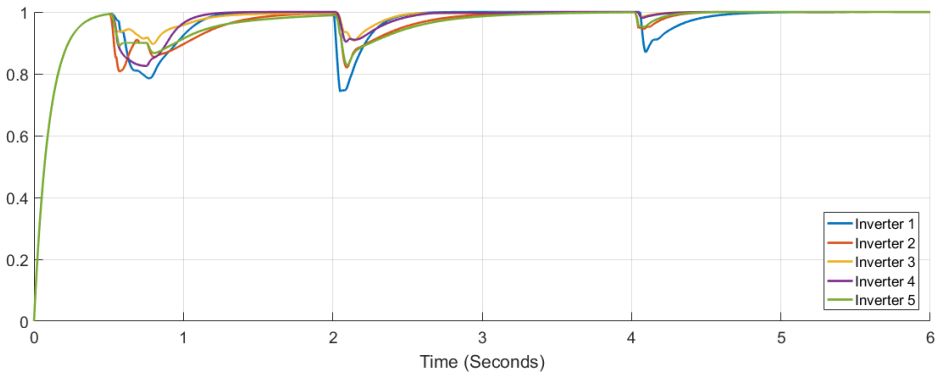

Figure 13. Confidence factor when inverter 1 is under attack

Third case A load $P_{load} = 20000$W is connected at $t = 0{,}5$s and a false data signal is introduced at the communication channel of inverter at $t =$2s.

Figure 15 and Figure 16 present the power variation at each inverter after the attack, there is a little variation in the power at each inverter, and no much variation at the tertiary controller response. In Figure 17 the frequency response is shown, notice the attack over the frequency measurement at inverter one; a constant signal of 0.2 Hz is added at $t = 2$s. Figure 18 shows the frequency at inverter one, the variation of frequency after a load variation is larger than the variation after the attack. Figure 19 shows the confidence factor variation after cyber-attack, this factor drops below 0.4 for inverter five, while Figure 20 shows the variation for trust factor, trust factor drops below 0.75 for inverter five while other inverters do not drop below the threshold value of 0.9.

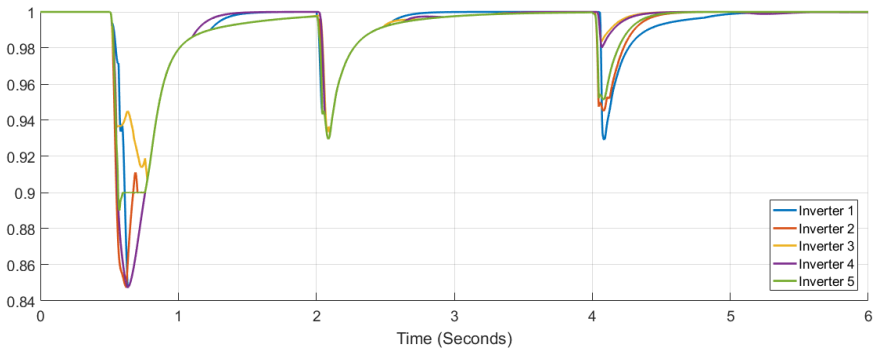

Figure 14. Trust factor when inverter 2 is under attack

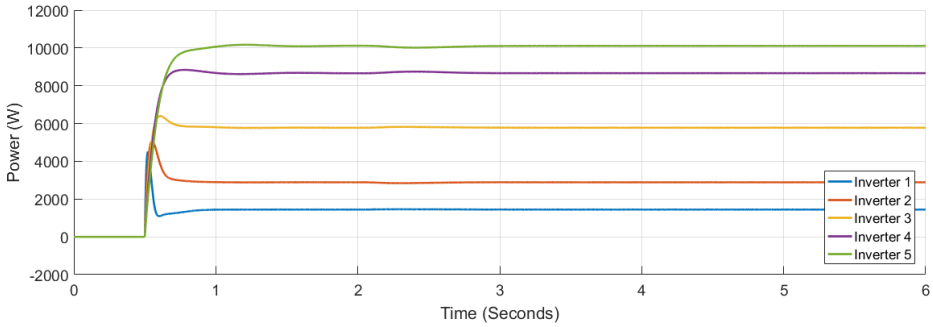

Figure 15. Active power for each inverter under attack in case 3

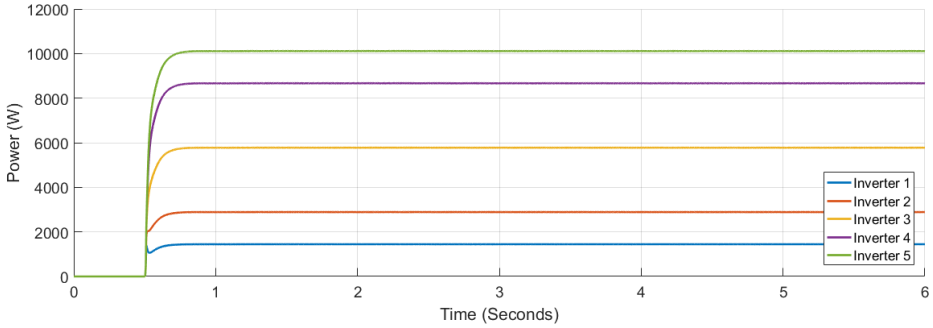

Figure 16. Output from the tertiary controller when is under attacks in case 3

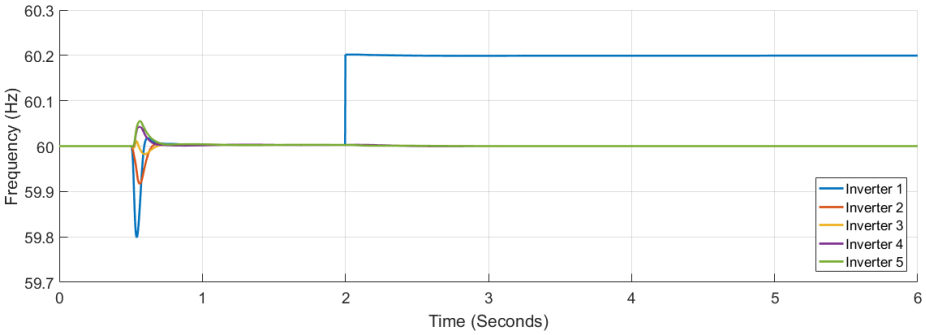

Figure 17. Frequency measured at each inverter when under attack

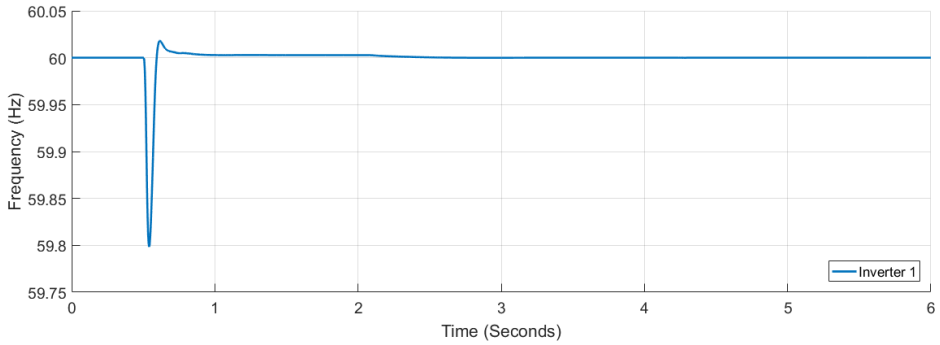

Figure 18. Frequency measured at inverter 1 under attack

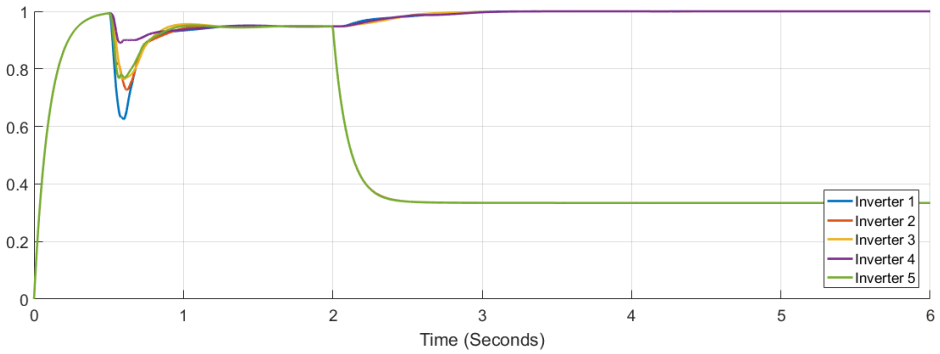

Figure 19. Confidence factor when inverter 1 is under attack

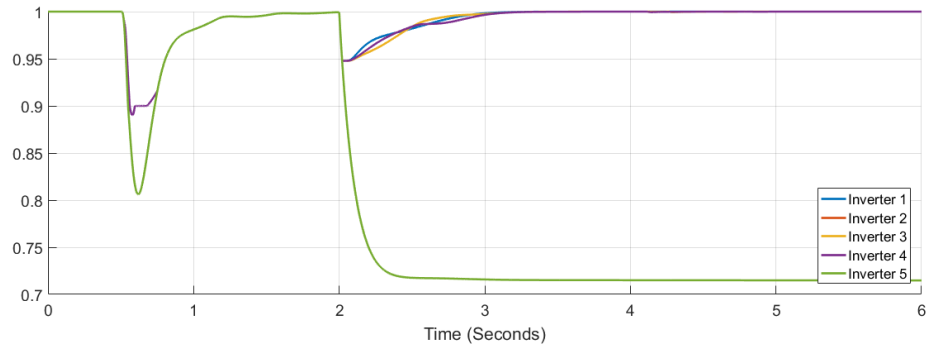

Figure 20. Trust factor when inverter 3 is under attack

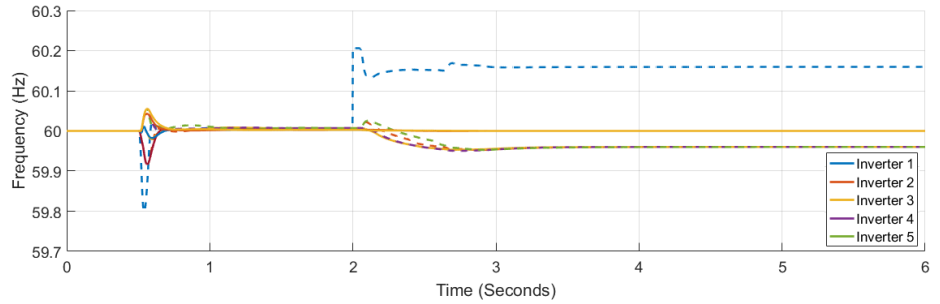

Figure 21. Frequency response of the system with (complete line) and without (dash line) trust and confidence factors

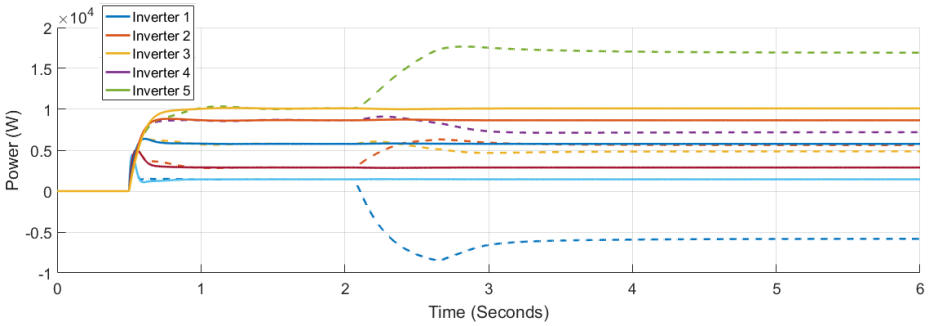

Figure 22. Active power response of the system for all the inverters with (complete line) and without (dash lines) trust and confidence factors

Finally, the comparison between the active power and frequency responses with and without confidence and trust factors are presented in Figure 21, and Figure 22. The frequency without those factors deviates from the reference value, not only in the inverter that suffers the attack but in all the other inverters. The active power varies abruptly when the system is under attack. Notice that the inverter that is attacked change from supply to absorb power. In contrast, active power has not changed when confidence and trust factors are used.

5. Conclusions

The distributed tertiary control is able to stabilize the active power flow in the microgrid after the cyber-attack. The power references for the primary control are modified to overcome the perturbation created by the cyber-attack without changing the frequency at steady state. Attacks on local controller and communication channels are simulated and the effectiveness of attack rejection is proved. The tertiary control shows its effectiveness to avoid inverters saturation and to keep the necessary conditions for optimal economical dispatch; such as maximum active power ratings, and maximum frequency deviation.

References

[1] R. H. Lasseter, "Microgrids," *in IEEE Power Engineering Society winter Meeting*, pp. 305–308, 2002 ↑. 65

[2] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. De Vicuña, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids - A general approach toward standardization," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158–172, 2011 ↑. 65

[3] M. C. Chandorkar, D. M. Divan, and R. Adapa, "Control of parallel connected inverters in standalone ac supply systems," *IEEE Transactions on Industry Applications*, vol. 29, no. 1, pp. 136–143, 1993 https://doi.org/10.1109/28.195899 ↑. 65, 66

[4] F. L. Lewis, Z. Qu, A. Davoudi, and A. Bidram, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Generation, Transmission and Distribution*, vol. 7, pp. 822–831, 2013 https://doi.org/10.1049/iet-gtd.2012.0576↑. 65, 66

[5] F. Dörfler, J. W. Simpson-Porco, and F. Bullo, "Breaking the Hierarchy : Distributed Control and Economic Optimality in Microgrids," vol. 3, no. 3, pp. 241–253, 2016 ↑. 65

[6] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, 2017 https://doi.org/10.1109/TSG.2017.2721382 ↑. 65, 66

[7] J. M. Guerrero, M. Chandorkar, T. Lee, and P. C. Loh, "Advanced Control Architectures for Intelligent Microgrids; Part I: Decentralized and Hierarchical Control," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 4, pp. 1254–1262, 2013 https://doi.org/10.1109/TIE.2012.2194969 ↑. 66

[8] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, pp. 2715–2729, Nov 2013 https://doi.org/10.1109/TAC.2013.2266831 ↑. 67

[9] J. M. Guerrero, P. C. Loh, T. L. Lee, and M. Chandorkar, "Advanced control architectures for intelligent microgridsPart II: Power quality, energy storage, and AC/DC microgrids," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 4, pp. 1263–1270, 2013 ↑. 70

[10] M. S. Mahmoud, M. Saif Ur Rahman, and F. M. A.L.-Sunni, "Review of microgrid architectures – a system of systems perspective," *IET Renewable Power Generation*, vol. 9, no. 8, pp. 1064–1078, 2015 https://doi.org/10.1049/iet-rpg.2014.0171 ↑. 70

[11] A. Nedić and A. Ozdaglar, "Subgradient methods for saddle-point problems," *Journal of Optimization Theory and Applications*, vol. 142, no. 1, pp. 205–228, 2009 https://doi.org/10.1007/s10957-009-9522-7 ↑. 70

[12] F. Guo, C. Wen, J. Mao, J. Chen, and Y. Song, "Hierarchical decentralized optimization architecture for economic dispatch: A new approach for large-scale power system," *IEEE Transactions on Industrial Informatics*, vol. 14, pp. 523–534, Feb 2018 https://doi.org/10.1109/TII.2017.2749264 ↑. 70, 71

[13] F. Guo, C. Wen, J. Mao, J. Chen, and Y.-D. Song, "Hierarchical Decentralized Optimization Architecture for Economic Dispatch: A New Approach for Large-scale Power System," *IEEE Transactions on Industrial Informatics*, 2017 ↑. 70, 71

[14] E. Baron-Prada, C. A. Uribe, and E. Mojica-Nava, "A Method for Distributed Transactive Control in Power Systems based on the Projected Consensus Algorithm," *IFAC-PapersOnLine*, vol. 51, pp. 379–384, jan 2018 https://doi.org/10.1016/j.ifacol.2018.12.065 ↑. 70

[15] C. A. Macana and H. R. Pota, "Optimal energy management system for strategic prosumer microgrids: An average bidding algorithm for prosumer aggregators," in *2017 11th Asian Control Conference (ASCC)*, pp. 705–710, Dec 2017 https://doi.org/10.1109/ASCC.2017.8287256 ↑. 70

[16] C. A. Macana, S. M. Mohiuddin, H. R. Pota, and M. A. Mahmud, "Online energy management strategy for islanded microgrids with feedback linearizing inner controllers," in *IEEE Innovative Smart Grid Technologies (ISGT-Asia)*, pp. 1–6, Dec 2017 ↑. 70

[17] E. Mojica-Nava, S. Rivera, and N. Quijano, "Distributed dispatch control in microgrids with network losses," in *IEEE Conference on Control Applications (CCA)*, pp. 285–290, Sep. 2016 https://doi.org/10.1109/CCA.2016.7587850 ↑. 70

[18] N. Quijano, C. Ocampo-Martinez, J. Barreiro-Gomez, G. Obando, A. Pantoja, and E. Mojica-Nava, "The role of population games and evolutionary dynamics in distributed control systems: The advantages of evolutionary game theory," *IEEE Control Systems Magazine*, vol. 37, pp. 70–97, Feb 2017 https://doi.org/10.1109/MCS.2016.2621479 ↑. 70, 71

[19] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control*. New Jersey: J. Wiley & Sons, 1996 ↑. 70

[20] Z. Li, C. Zang, P. Zeng, H. Yu, and S. Li, "Agent-based distributed and economic automatic generation control for droop-controlled AC microgrids," *IET Generation, Transmission and Distribution*, vol. 10, no. 14, pp. 3622–3630, 2016 https://doi.org/10.1049/iet-gtd.2016.0418 ↑. 71

[21] J. N. Webb, *Game theory: decisions, interaction and Evolution*. Berlin: Springer, 2007 ↑. 72

[22] J. Hofbauer and K. Sigmund, *Evolutionary Games and Population Dynamics*. Cambridge University Press, 1998 https://doi.org/10.1017/CBO9781139173179 ↑. 72

Vladimir Toro

Received the B.S. degree in electronics engineering from the Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, in 2009; the M.Sc. degree in electrical engineering from the Universidad Nacional de Colombia, Bogotá, Colombia in 2018. He is currently pursuing the Ph.D degree at Universidad Nacional de Colombia, Bogotá. His current research interests include microgrid's control, optimization, and control of multi-agent systems.

Eder Baron-Prada

Received the B.S. degree in electrical engineering from the Universidad Nacional de Colombia, Bogotá, Colombia, in 2016; He is currently pursuing the master degree in Industrial Automation at National University of Colombia, Bogotá. His current research interests include microgrid control, optimization, and control of multi-agent systems.

Eduardo Mojica-Nava

Received the B.S. degree in electronics engineering from the Universidad Industrial de Santander, Bucaramanga, Colombia, in 2002; the M.Sc. degree in electronics engineering from the Universidad de Los Andes (UAndes), Bogotá, Colombia; and the Ph.D. degree in automatique et informatique industrielle from the Ecole des de Nantes, Nantes, France in co-tutelle with UAndes in 2010. He is currently an associate professor with the Department of Electrical and Electronics Engineering, Universidad Nacional de Colombia, Bogotá. His current research interests include optimization and control of complex networked systems, switched and hybrid systems, and control in smart grids applications.