Voltage control for interconnected microgrids under adversarial actions

André Teixeira, Kaveh Paridari, Henrik Sandberg, Karl H. Johansson
ACCESS Linnaeus Centre, KTH Royal Institute of Technology, Stockholm, Sweden
{andretei,paridari,hsan,kallej}@kth.se

***Abstract*—In this paper, we study the impact of adversarial actions on voltage control schemes in interconnected microgrids. Each microgrid is abstracted as a power inverter that can be controlled to regulate its voltage magnitude and phase-angle independently. Moreover, each power inverter is modeled as a single integrator, whose input is given by a voltage droop-control policy that is computed based on voltage magnitude and reactive power injection measurements. Under mild assumptions, we then establish important properties of the nominal linearized closed-loop system, such as stability, positivity, and diagonal dominance. These properties play an important role when characterizing the potential impact of different attack scenarios. In particular, we discuss two attack scenarios where the adversary corrupts measurement data and reference signals received by the voltage droop controllers. The potential impact of instances of each scenario is analyzed using control-theoretic tools, which may be used to develop methodologies for identifying high-risk attack scenarios, as is illustrated by numerical examples.**

I. Introduction

Motivated by environmental, economic and technological aspects, interests in renewable energy sources is growing worldwide. Most of these sources are small-scale inverter-based distributed generation (DG) units connected at the low voltage (LV) and medium voltage (MV) levels. Thus, the power generation infrastructure is moving from purely large centralized plants at the high voltage levels to a mixed generation pool consisting of conventional large plants and smaller distributed generation units at lower voltage levels. In this new paradigm, it is more challenging to operate the electric power networks in a reliable and resilient mode. These challenges may be tackled by facilitating a local integration of renewable energy sources, which las led to the concept of microgrids (MGs) [1], [2]. An MG is a low-voltage electrical network, composed of several DGs, energy storage elements, and controllable loads, and their integration with the main grid is accomplished by using power inverters. In addition, an MG is able to operate in the grid-connected mode (connected to the wide-area electric power system), and also in the islanded mode (disconnected from the main grid).

Electrical power networks in the new energy generation paradigm are very complex and face numerous challenges. To facilitate their safe and reliable operation, they need to be tightly coupled with the supervisory control and data acquisition (SCADA) systems that monitor and operate the power infrastructure by collecting data from remote facilities and meters, and sending back supervisory control commands. On the other hand, the power networks coupled with the SCADA systems face new challenges, as these systems may become susceptible to malicious cyber threats through the communication infrastructure. The safe and stable operation of power networks must be ensured, not only in the normal situations, but also in the cases when the cyber security of SCADA systems is threatened by malicious attacks [3]. Thus, it is also important to analyze potential vulnerabilities of the system, by modeling and studying different threats to the controlled system, and devise resilient schemes to mitigate high-risk threats.

Recently, there has been a substantial work on cyber security of power transmission networks, addressing, for instance, certain classes of undetectable false data injection attacks [4]–[7]. In addition, the impact of these attacks on the system operation [8], [9] and possible protective and countermeasures [10], [11] have been investigated.

In comparison with transmission level, as mentioned in [12], security issues at the distribution system level have not been as extensively studied. The impact of cyber attacks on centralized voltage regulation in distribution systems was considered in [12], where a detection algorithm was proposed to mitigate the impact of sparse attacks. The vulnerabilities that may be introduced by the integrated Volt-VAR control scheme when an adversary is able to inject false data measurements into the system is studied in [13]. To the best of our knowledge, none of the previous works have studied the consequences of cyber attacks on inverter-based microgrids. However, [14] recently performed a thorough investigation of cyber attacks against the manufacturing message specification of IEC 61850, which is one of the widely used communication services in Smart Grids. The experiments in [14] have demonstrated the capability of cyber adversaries to tamper with the IEC 61850 data flow controlling electrical devices and, thus, affect the underlying physical system operation. The cyber attack objectives were achieved via malicious manipulation of power setpoints to change the operation of power inverter devices, or indeed to cause them to switch off.

In this paper, we first tackle the problem of voltage stability and reactive power balancing in the droop-controlled MGs, and provide criteria for designing the controller gains in terms of the power system parameters. Stability and power sharing analysis of droop-controlled MGs has been carried out in several studies in the literature. For radial lossless microgrids, and

978-1-4673-7929-8/15/$31.00

under the assumption of constant voltage amplitudes, analytic conditions for proportional power sharing and synchronization of have been derived in [15]. Conditions for voltage stability for lossless parallel MGs with one common load have been derived in [16]. In addition, [17] gives conditions on the droop gains to ensure stability of droop-controlled lossless MGs with general meshed topology. In contrast to [15]–[17] no assumptions of constant voltage amplitudes, small phase-angle differences, or lossless MGs are made in this paper.

Having established relevant properties of the power system, we identify potential vulnerabilities in the interface between the physical and the IT infrastructures that may lead to an abnormal operation of the distribution network. In particular, relevant attack scenarios are introduced, together with their threat models, based on which impact analysis are performed. The attack scenarios in this work consider cyber adversaries that may corrupt a few measurements and reference signals, which may degrade the system's reliability and even destabilize the voltage magnitudes. For example, we show that a cyber adversary, without having substantial model knowledge, may destabilize the power system by merely redirecting measurements communicated through the communication network.

The paper is organized as follows. Some definitions and known results are reviewed in Section II. The system configuration and controller structure for the inverter-based MGs are described in Section III. Conditions for the power network parameters and controller gains that ensure the system to be positive and stable are given in Section IV. Different attack scenarios against the droop-controlled MGs and preliminary results on their impact are proposed in Section V. Final remarks and conclusions are drawn in Section VI.

II. Preliminaries

In this section, we recall important properties of certain classes of linear time-invariant (LTI) systems that will be useful in the subsequent sections. Let us consider a general LTI system of the form:

$$\begin{cases} \dot{x}(t) = Ax(t) + Fu(t) \\ y(t) = Cx(t) + Du(t), \end{cases} \tag{1}$$

where $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$ and $y(t) \in \mathbb{R}^p$ are the system state, the control input, and the controlled output at time t, respectively. Denoting $a_{ij} = [A]_{i,j}$ as the entry of A in the i-th row and j-th column, the class of diagonally dominant matrices is defined as follows.

Definition 1 (Diagonally dominant matrices)**.** *The matrix A is said to be row-diagonally dominant if its entries satisfy the conditions*

$$|a_{ii}| \geq \sum_{j \neq i} |a_{ij}|, \ \forall i \in \{1, \ldots, n\}. \tag{2}$$

Given the above definition, the system (1) is said to be row-diagonally dominant if the state matrix A is row-diagonally dominant.

Another relevant class of systems is that of positive systems (see [18], for instance), which play an important role throughout this paper.

Definition 2 (Positive systems)**.** *The LTI system* (1) *is said to be positive if the following conditions hold:*

1) *The matrix A is Metzler, i.e., it has non-negative off-diagonal entries;*
2) *The matrices F, C and D are non-negative, i.e., they only have non-negative entries.*

Positive systems have several interesting properties, e.g., $x(0) \geq 0$ and $u(t) \geq 0$ result in trajectories satisfying $x(t) \geq 0$ for all t, where $x \geq 0$ denotes element-wise inequalities. In particular, the following properties of positive systems are instrumental in our analysis.

Lemma 1 ([18])**.** *If the system* (1) *is positive, the following statements hold:*

1) *The matrix A is Hurwitz (every eigenvalue of A has strictly negative real part) if, and only if, there exists a $\xi \in \mathbb{R}^n$ such that $\xi > 0$ and $A\xi < 0$.*
2) *Let $m = p = 1$, define $H(s) = C(sI - A)^{-1}F + D$ as the transfer function of the system* (1)*, and suppose A is Hurwitz. The $\mathcal{L}_\infty$-induced norm of* (1) *is given by*

$$\| H \|_{\mathcal{L}_\infty - ind} = \sup_{\| u \|_{\mathcal{L}_\infty} < \infty} \frac{\| y \|_{\mathcal{L}_\infty}}{\| u \|_{\mathcal{L}_\infty}} = H(0). \tag{3}$$

The first property relates the stability of positive systems to a set of inequality constraints, which is helpful to derive stability conditions. Regarding the input-output behavior of the system, the second property characterizes the maximum amplitude of the output signal $y(t)$ that can be achieved by an input $u(t)$ with bounded amplitude

$$\| u \|_{\mathcal{L}_\infty} := \sup_{t \geq 0} |u(t)| < \infty.$$

In particular, constraining the input's amplitude to be at most 1, i.e., $\| u \|_{\mathcal{L}_\infty} \leq 1$, the corresponding output satisfies the tight inequality $\sup_{t \geq 0} |y(t)| \leq \| H \|_{\mathcal{L}_\infty - ind}$, which holds with equality for a constant input $u(t) = 1$.

Moreover, the second property leads to other relevant features of positive systems in terms of input-output behavior. On one hand, for input signals $u(t)$ corresponding to reference signals, it establishes the absence of output overshoot for step changes in the reference. On the other hand, considering $u(t)$ to be a possible disturbance or anomaly, the $\mathcal{L}_\infty$-induced norm quantifies the worst-case impact that the anomaly can have on the output signal, in terms of signal amplitudes. In this paper, both of these interpretations are further discussed and illustrated in the context of power systems.

III. Problem Formulation

The power distribution system is considered to be a set of interconnected MGs that may be connected to the main grid through the feeder substation, where each MG may contain several inverter-based distributed energy resources (DER) and

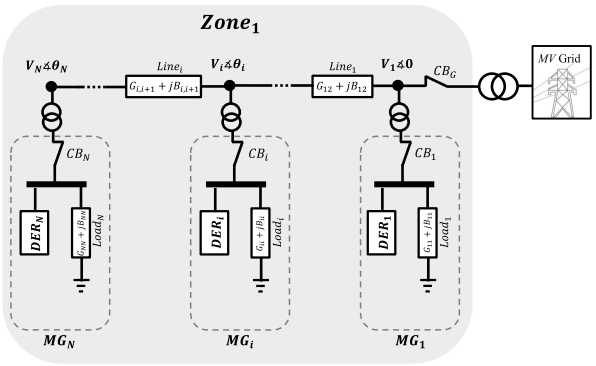


Figure 1. A power distribution system comprised of interconnected microgrids with inverter-based DERs.

loads. The distribution system is depicted in Fig. 1, where each MG is represented by a bus and the multiple DERs and loads within a given MG are lumped together and modeled as a single DER and load, respectively.

Although Fig. 1 depicts a line network, we consider generic connected topologies where the network is characterized by the undirected graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the vertex set, $\mathcal{E}$ is the edge set, and $\mathcal{N}_i = \{j \in \mathcal{V} : (i,j) \in \mathcal{E}\}$ denotes the neighbor set of the i-th bus. In this system, the states are defined as V_i and θ_i, which are voltage magnitude and voltage angle of the i-th bus, respectively, and $i \in \mathcal{V}$.

Assumption 1. *In the power distribution network under study, the following assumptions are made:*

1) *The three-phase power network is balanced (so that it can be represented as an equivalent single-phase system);*
2) *All N buses are assumed to be inverter buses [2], each represented by V_i and θ_i for $i = 1, \dots, N$.*

Under Assumption 1, the active and reactive power injections at bus i is given respectively by

$$\begin{aligned} P_i &= V_i^2 G_i - \sum_{j\in\mathcal{N}_i} V_i V_j (G_{ij}\cos(\theta_{ij}) + B_{ij}\sin(\theta_{ij})), \\ Q_i &= -V_i^2 B_i - \sum_{j\in\mathcal{N}_i} V_i V_j (G_{ij}\sin(\theta_{ij}) - B_{ij}\cos(\theta_{ij})), \end{aligned} \tag{4}$$

in which $G_{ij} = R_{ij}/(R_{ij}^2 + X_{ij}^2) \geq 0$ and $B_{ij} = -X_{ij}/(R_{ij}^2 + X_{ij}^2) \leq 0$ are, respectively, the conductance and susceptance of the transmission line between the i-th and j-th buses, and R_{ij} and X_{ij} are resistance and reactance of the same line between the same buses, respectively. In addition, self-conductance and self-susceptance are defined as $G_i = G_{ii} + \sum_{j\in\mathcal{N}_i} G_{ij}$ and $B_i = B_{ii} + \sum_{j\in\mathcal{N}_i} B_{ij}$, respectively. Note that the angle difference between node i and j, $\theta_i - \theta_j$, is simply written as θ_{ij} in the rest of the paper.

Assumption 2. *In the power distribution system under study, the transmission line impedances are assumed to have the same ratio $R_{ij}/X_{ij} = -G_{ij}/B_{ij} = \rho \geq 0$ for all lines $(i,j) \in \mathcal{E}$.*

The line ratio is related to the nature of the power system: power systems with inductive transmission lines ($R_{ij} << X_{ij}$) have a small ratio $\rho > 0$, while systems with resistive lines have a higher ratio. The latter is often the case for medium- and low-voltage distribution grids. Since the line ratio ρ depends on the transmission line characteristics, Assumption 2 naturally holds for systems with homogeneous transmission lines that have similar characteristics. Moreover, Assumption 2 is commonly used in the literature, often restricted to the case of purely inductive lines ($\rho = 0$) [16], [17].

A. Controller structure

In terms of the voltage and phase-angle dynamics, each MG i is modeled as a pair of single integrators

$$\begin{aligned} \tau_i \dot{V}_i(t) &= u_{V_i}(t), \\ \tau_{\theta_i} \dot{\theta}_i(t) &= u_{\theta_i}(t), \end{aligned} \tag{5}$$

where $\tau_i > 0$ and $\tau_{\theta_i} > 0$ are the inverter's time-constants and $u_{V_i}(t)$ and $u_{\theta_i}(t)$ are the control signals computed by the droop controller at time $t \geq 0$. The architecture of the control system is illustrated in Fig. 2, which depicts the measurements and reference signals available to each controller. Using the capabilities of the local inverter-based DERs, each MG is controlled by a droop controller, which receives the reference signal computed remotely (V_i^* as the reference voltage for the i-th bus) and measurements (V_j and θ_j, as the voltage magnitude and voltage angle of the j-th bus, respectively) through the communication network, using a suitable communication protocol such as the IEC 61850.

Since we are mainly interested in the voltage dynamics of the power system, the phase-angle dynamics are neglected and the following assumptions is considered throughout the remainder of the paper.

Assumption 3. *The phase-angle differences between any neighboring nodes, θ_{ij} for $(i,j) \in \mathcal{E}$, is assumed to be constant.*

Note that the analysis under Assumption 3 may be interpreted as a local analysis in scenarios where the phase-angles remain in the neighborhood of the original equilibrium point. Additionally, we highlight that the assumption is valid if there exists a time-scale separation between the phase-angle and the voltage dynamics.

To compute the voltage control signals, we consider the voltage quadratic droop controller [15, equation (7)] described by

$$u_{V_i}(t) = -\kappa_i V_i^c(t)\left(V_i^c(t) - V_i^{c\star}(t)\right) - Q_i^c(t), \tag{6}$$

where $\kappa_i > 0$ is the droop control gain and $V_i^c(t)$, $Q_i^c(t)$, and $V_i^{c\star}(t)$ are the voltage measurement, reactive injection measurement, and voltage reference signal with respect to bus i, respectively, that are received by the droop controller, as illustrated in Fig. 2. Under nominal operation, these signals

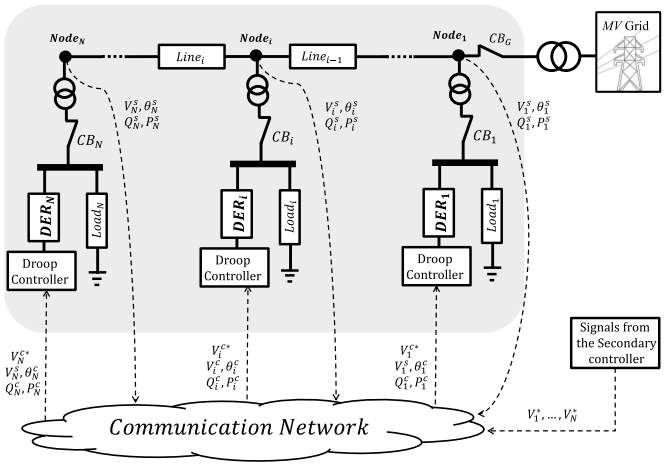


Figure 2. The inverter-based DERs of a MG are controlled by a droop controller. The physical quantities are measured by sensors at each node, which then transmit their measurements (denoted by the superscript *s*) to the droop controllers. The control signal is computed based on the measurements and reference signals received by the controller (denoted with the superscript *c*).

match the corresponding physical variables and reference signals, i.e., $V_i^c(t) = V_i(t)$, $Q_i^c(t) = Q_i(t)$, and $V_i^{c\star}(t) = V_i^\star(t)$ ($V_i^\star(t)$ is sent by a higher level controller which is called Secondary controller). Under nominal operation, the closed-loop dynamics of the i-th MG are given by the differential equations

$$\begin{aligned}\tau_i \dot{V}_i &= -\kappa_i V_i \left(V_i - V_i^\star\right) - Q_i \\ &= -V_i \left(\kappa_i V_i - \kappa_i V_i^\star + \sum_{j \in \mathcal{V}} l_{ij}(\theta) V_j \right), \ \forall i = 1, \dots, N,\end{aligned} \tag{7}$$

where the time argument has been omitted. In addition, under the Assumption 2, the parameter l_{ij} is written as

$$l_{ij} = \begin{cases} B_{ij}(\rho \sin(\theta_{ij}) + \cos(\theta_{ij})), & i \neq j \\ -B_i, & i = j. \end{cases} \tag{8}$$

Denoting $V = [V_1 \ \dots \ V_N]^\top$, $\tau = [\tau_1 \ \dots \ \tau_N]^\top$, $\kappa = [\kappa_1 \ \dots \ \kappa_N]^\top$, and $[V]$ as the diagonal matrix with V_i as the i-th diagonal entry, the voltage dynamics under the quadratic droop control can be written in vector form as

$$[\tau]\dot{V} = [V]\left([\kappa]V^\star - \left([\kappa] + L(\theta)\right)V\right), \tag{9}$$

where the matrix $L(\theta)$ is defined as $[L(\theta)]_{ij} = l_{ij}(\theta)$.

B. Linearization of the voltage dynamics

In the following sections, we consider that the power system (9) is linearized around an equilibrium point $(\bar{V}, \bar{V}^{c\star})$ such that $-\left([\kappa] + L(\theta)\right)\bar{V} + [\kappa]\bar{V}^\star = 0$. By Assumption 3, and denoting $x(t) = V(t) - \bar{V}$ and $u(t) = V^{c\star}(t) - \bar{V}^{c\star}$ as the voltage and reference deviations, respectively, the corresponding linearized system is given by

$$\dot{x}(t) = Ax(t) + Fu(t), \tag{10}$$

where $A = -[\bar{V}][\tau]^{-1}\left([\kappa] + L(\theta)\right)$ and $F = [\bar{V}][\tau]^{-1}[\kappa]$. For simplicity, in the following we suppose that $\bar{V} = \mathbf{1}\text{pu}$, where $\mathbf{1}$ denotes a vector with all entries equal to 1.

IV. Stability analysis

In this section, we provide necessary and sufficient conditions on the power system parameters so that the linearized dynamics are positive and row-diagonally dominant. These properties are then used to establish the asymptotic stability of the linearized system. Moreover, they play an important role when studying the power system under the attack scenarios in subsequent sections.

A. System properties

First we derive necessary and sufficient conditions for the linearized system (10) to be positive, which requires the following assumption.

Assumption 4. *The maximum phase difference between any two neighboring nodes, defined as*

$$\Delta_\theta := \max_{(i,j)\in\mathcal{E}} |\theta_{ij}|, \tag{11}$$

satisfies the inequality $\Delta_\theta < \pi/2$.

Recall that the constraint $\Delta_\theta < \pi/2$ is an operational requirement for any conventional power system [17], which is required for the stability of the phase-angle dynamics. Under the previous assumptions, the following result is established.

Theorem 1. *Consider the power distribution network under study, having active and reactive power injections* (4) *at bus i with $\Delta_\theta < \pi/2$, and applying the quadratic droop controller* (7) *for each MG. Then a necessary and sufficient condition for the corresponding linearized system* (10) *to be positive is*

$$\rho \leq |\cot(\Delta_\theta)|. \tag{12}$$

Proof. This proof and the subsequent ones in the paper are omitted. □

Note that several of the properties of positive systems stated in Section II have important consequences in the context of power systems and, in particular, the voltage dynamics. Letting the input $u(t)$ be the voltage reference at one individual bus and $x(t)$ and the voltages of all buses, the closed-loop system being positive implies that an increase in the voltage reference $u(t)$ translates to an increase in all the voltages $x(t)$. Hence, there is no contradictory effect where a desired increase in voltage at one bus inadvertently decreases the voltage in other buses. Additionally, positivity of the closed-loop system also reduces the voltage overshoots in response to step changes in the voltage reference.

Remark 1. *While the latter discussion motivates positivity as a desirable system feature, Theorem 1 provides a design objective for the phase-angle controller that ensures positivity of the voltage dynamics, namely the inequality* (12)*. In fact, since the line ratio ρ is a system parameter that depends*

solely on the transmission lines' characteristics, (12) *can be interpreted as a bound on the phase-angle differences that is parameterized by the line ratio ρ. Rewriting* (12) *as $|\tan(\Delta_\theta)| \leq \rho^{-1}$, we have that a resistive system with a large ρ yields a strict bound on the maximum phase-angle difference Δ_θ, while a purely inductive system with $\rho = 0$ does not constrain the phase-angle difference.*

Next we characterize necessary and sufficient conditions for a linearized positive system to be row-diagonally dominant.

Lemma 2. *Suppose the linearized system* (10) *is positive. The system* (10) *is row-diagonally dominant if, and only if, the following inequality holds*

$$\kappa_i + |B_{ii}| \geq (\sqrt{\rho^2+1} - 1) \sum_{j \in \mathcal{N}_i} |B_{ij}|. \tag{13}$$

These properties play important roles in the characterization of the attack impacts, and they are also used in analyzing the stability of the linearized system.

B. Stability of the power system

Next we establish the stability of the linearized system, using the positivity and row-diagonally dominance properties of the linearized system. Specifically, when the system is positive, the next result states the necessary and sufficient conditions for stability and then shows that row-diagonally dominance ensures stability.

Theorem 2. *Consider the linearized dynamics of the power system* (10) *and suppose the system is positive. Then the following statements hold:*

1) *the system is asymptotically stable if and only if there exist positive scalars $\xi_i > 0$ such that the following inequality holds for all $i = 1, \ldots, n$:*

$$\xi_i |-\kappa_i + B_i| > \sum_{j \in \mathcal{N}_i} \xi_j |-B_{ij}(\rho \sin(\theta_{ij}) + \cos(\theta_{ij}))|;$$

2) *the system is asymptotically stable if it is row-diagonally dominant, i.e., the following inequality holds for all $i = 1, \ldots, n$:*

$$|-\kappa_i + B_i| > \sum_{j \in \mathcal{N}_i} |-B_{ij}(\rho \sin(\theta_{ij}) + \cos(\theta_{ij}))|.$$

Remark 2. *Note that we may not have control on self-susceptance (B_{ii}) and it belongs to the interval $[0, \bar{B}_{ii}]$, so to be more conservative, the sufficient condition in Proposition 2 can be written as:*

$$\kappa_i \geq \sum_{j \in \mathcal{N}_i} (\sqrt{\rho^2+1} - 1)|B_{ij}|. \tag{14}$$

Remark 3. *It could be interesting to characterize conditions on* (10) *under which V satisfies $|V - \mathbf{1}| < \delta$. This problem is related to the validity of* (10)*, which assumes that V is positive. It also relates to how $V^{c\star}$ should be constrained so that the system is safe.*

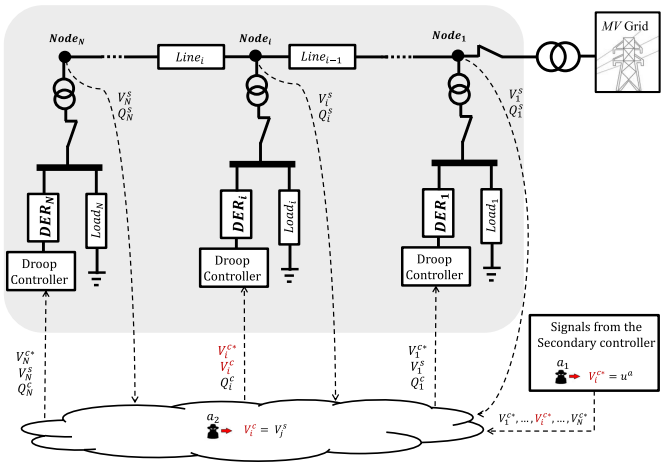


Figure 3. An inverter-based droop controller under (a1) a reference signal attack at bus i, where the adversary corrupts $V_i^{c\star}$, and (a2) a measurement routing attack at bus i, where the adversary redirects the voltage measurement from bus j to the controller at bus i, as if it were a measurement from bus i.

V. Impact of Adversarial Actions

Recently, [14] investigated the implementation of cyber attacks against a common application-level protocol in Smart Grid applications, the IEC 61850. In the considered attack scenario, cyber adversaries built a custom tool to execute man-in-the-middle attacks and manipulate data transmitted to a photovoltaic power inverter, thus affecting the physical power system. In this section, the potential consequences of such cyber attacks on the power grid are investigated.

The following subsections follow a similar structure and each one considers a specific attack scenario. In particular, each subsection begins by describing the adversarial model and how it affects the droop controller. Then, the impact of the attack is characterized based on properties of the linearized system, such as stability and input-output induced-norm. Such characterizations also aim at identifying which sets of attacked nodes yield possibly higher impacts, thus indicating which threats may pose a high risk to the system. The theoretical analysis is then complemented with numerical simulations of the attack scenarios in the nonlinear system (9).

A. Voltage reference attack

The present scenario considers an adversary that injects false-data into the communication network supporting the control system. In particular, we consider reference signals attacks defined as follows.

Definition 3 (Reference signal attack)**.** *In a reference signal attack on bus j, the reference signal of bus j is corrupted, as depicted in Fig. 3, so that*

$$V_j^{c\star}(t) = u^a(t), \tag{15}$$

where the signal $u^a(t)$ is defined by the adversary. Furthermore, the control signal at bus j under a reference signal attack is given by

$$u_{V_j} = -\kappa_j V_j^c \left(V_j^c - u^a(t)\right) - Q_j^c. \tag{16}$$

The impact of the attack is measured in terms of the resulting changes to the voltage magnitude at another bus $i \neq j$ in the network, i.e. V_i. The resulting linearized system can be expressed as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \tau_j^{-1}\kappa_j e_j u^a(t) \\ y_i(t) &= e_i^\top x(t) \end{aligned} \tag{17}$$

where $A = -[\tau]^{-1}([\kappa] + L(\theta))$ and $e_i \in \mathbb{R}^n$ is the i-th column of the n-dimensional identify matrix. In particular, we quantify the attack's impact as the maximum deviation of $y_i(t)$ caused by a corrupted reference $u^a(t)$ that is bounded as $|u^a(t)| \leq 1$. In fact, as discussed in Section II, this metric corresponds to the $\mathcal{L}_\infty$-induced norm of (17). For power systems satisfying the conditions of Theorem 1 and Lemma 2, i.e., the system (17) is positive and stable, the following characterization of the worst-case attack naturally follows from Lemma 1.

Lemma 3. *Consider the linearized power system* (10)*, which is assumed to be positive and asymptotically stable, and suppose that bus j is under a reference signal attack. Let $H_{ij}(s)$ be the transfer function of* (17)*. The worst-case impact on bus i of a reference signal attack on bus j, characterized as the $\mathcal{L}_\infty$-induced norm of* (17)*, is given by $H_{ij}(0) = -\tau_j^{-1}\kappa_j e_i^\top A^{-1} e_j = \tau_j^{-1}\kappa_j [-A^{-1}]_{i,j}$.*

Such characterization of the worst-case impact can be leveraged to compare different attacks and identify scenarios with higher impact. In particular, supposing bus j is attacked, we are interested in assessing which other bus $i \neq j$ is most affected by the attack. That is, we seek to compute

$$i^\star = \arg\max_i H_{ij}(0) = \arg\max_i [-A^{-1}]_{i,j},$$

where the common factor $\tau_j^{-1}\kappa_j$ has been omitted.

Although solving such problem would, in general, require the computation of all entries of $-A^{-1}$, specific power system topologies admit simpler solutions. Specifically, for power systems whose topology corresponds to a line graph, the following result establishes that the $\mathcal{L}_\infty$-induced norm $[-A^{-1}]_{i,j}$ decreases as the distance between i and j increases.

Theorem 3. *Consider a power system whose topology corresponds to a line graph and the respective linearized dynamics* (10) *are positive and row-diagonally dominant. Furthermore, suppose the droop controller at bus j is under a reference signal attack. Then the $\mathcal{L}_\infty$-induced norm of the linearized system under attack* (17) *is given by $H_{ij}(0) = \tau_j^{-1}\kappa_j [-A^{-1}]_{i,j}$, which satisfies the monotonicity conditions*

$$\begin{aligned} [-A^{-1}]_{i,j} &> [-A^{-1}]_{i+1,j}, \ \forall j \leq i \\ [-A^{-1}]_{i,j} &> [-A^{-1}]_{i-1,j}, \ \forall j \geq i. \end{aligned} \tag{18}$$

Considering line graphs, using the results of Theorem 3, we conclude that the impact of a reference attack decays as the distance to the attacked bus increases. Moreover, the bus most affected by the attack at bus j, defined as $i^\star = \arg\max_i H_{ij}(0)$, corresponds to one of the neighboring buses of j, i.e., $i^\star = \arg\max_{i \in \{j-1,\ j+1\}} [-A^{-1}]_{i,j}$.

Numerical example: To illustrate the impact of the attack on the reference signal, we consider an islanded 4-bus power system with a line topology, as depicted in Fig. 1 with $N = 4$, and assume identical power lines, loads, and inverters. The power system is characterized by (4) with the parameters $\rho = 0.5$, $B_{ij} = -0.2$, and $G_{ij} = -\rho B_{ij}$ for all edges $(i,j) \in \mathcal{E}$ and $B_{ii} = -0.001$ and $G_{ii} = \rho|B_{ii}|$ for all buses. The power inverters are modeled by (5) and (6) with parameters $\tau_i = 10^{-4}$, $\tau_{\theta_i} = 10^{-2}$, and $\kappa_i = 0.2$ for all buses. To motivate Assumption 3, two sets of simulations are performed: one where Assumption 3 is satisfied, since the phase-angle differences are constant throughout the simulation of the voltage dynamics and are given by $\theta_{12} = -0.11\text{rad}$, $\theta_{23} = 0.045\text{rad}$, and $\theta_{34} = -0.11\text{rad}$; another where a suitable droop controller is used for the phase-angle dynamics, with the previous set of phase-angle differences as an initial condition, and with noise in the voltage measurements.

The voltage dynamics are described by the nonlinear differential equations (9), with the corresponding linearized dynamics characterized by (10) with

$$A = 10^{-4} \cdot \begin{bmatrix} -4.01 & 1.88 & 0 & 0 \\ 2.1 & -6.01 & 2.04 & 0 \\ 0 & 1.95 & -6.01 & 1.88 \\ 0 & 0 & 2.1 & -4.01 \end{bmatrix}.$$

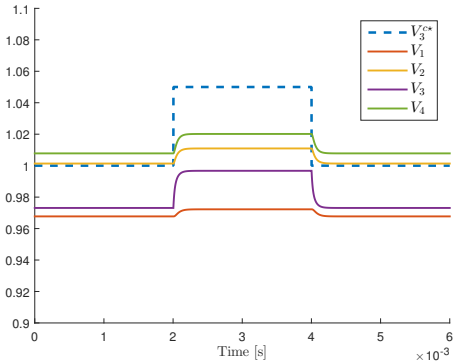
Clearly, the system is positive and row-diagonally dominant. Since the diagonal entries A are negative, the system is also asymptotically stable.

Now consider the reference signal attack scenario where the voltage reference transmitted to bus 3 is corrupted by an adversary, as per Definition 3. Following the discussion in this section, we seek to assess which buses, other than bus 3, are most affected by such attack. From Lemma 3, the worst-case impact of such attack on a given bus i in the network corresponds to $H_{i3}(0) = -K_3\tau_3^{-1} e_i^\top A^{-1} e_3$. In present example, the set of worst-case gains to buses 1, 2, and 4 are given by $H_{13}(0) = 0.09$, $H_{23}(0) = 0.19$, and $H_{43}(0) = 0.25$, respectively. As stated by Theorem 3, for line graphs, the largest worst-case impact takes place at one of the neighbors of bus 3, which here corresponds to bus 4.

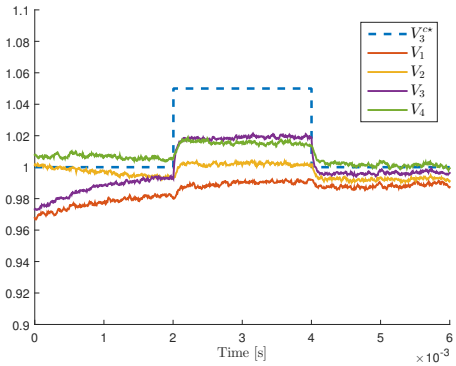
The decrease of the impact as the distance to bus 3 increases is visible on the voltage trajectories of the nonlinear system under a reference attack on bus 3, as depicted in Fig. 4(a). A similar behavior is also observed with varying phase-angles and measurement noise, as illustrated in Fig. 4(b).

B. Voltage measurement routing attack

Here we consider an adversary that is able to redirect truthful data from its intended destination to another receiving bus in the network. In particular, we consider measurement routing attacks defined as follows.



(a) Constant phase-angles



(b) Varying phase-angles and measurement noise

Figure 4. Trajectories of the voltage magnitudes under a reference signal attack at bus 3.

Definition 4 (Measurement routing attack)**.** *In a measurement routing attacks on bus i, the adversary redirects the voltage measurement from bus j as if it were a measurement from bus i, which is captured by having*

$$V_i^c = V_j^s = V_j.$$

Furthermore, the corresponding control signal under attack is described as

$$\begin{aligned} u_{V_i} &= -\kappa_i V_j^s \left(V_j^s - V_i^{c\star}\right) - Q_i^c \\ u_{V_k} &= -\kappa_k V_k^c \left(V_k^c - V_k^{c\star}\right) - Q_k^c, \ \forall k \neq i. \end{aligned} \tag{19}$$

The resulting linearized system under a measurement routing attack at bus i can be expressed as

$$\dot{x}(t) = \left(A - \tau_i^{-1}\kappa_i e_i (e_j - e_i)^\top\right) x(t), \tag{20}$$

where the term $-\tau_i^{-1}\kappa_i e_i(e_j - e_i)^\top x(t)$ can be interpreted as replacing the nominal feedback term $\tau_i^{-1}\kappa_i V_i$ by the corrupted feedback $\tau_i^{-1}\kappa_i V_j$ at bus i. In fact, such attack scenario can be rewritten as the following static output-feedback law

$$\begin{aligned} \dot{x}(t) &= \underbrace{(A + \tau_i^{-1}\kappa_i e_i e_i^\top)}_{=\tilde{A}_i} x(t) + \tau_i^{-1} e_i u(t) \\ y_j(t) &= e_j^\top x(t) \\ u(t) &= -\kappa_i y_j(t), \end{aligned} \tag{21}$$

where the matrix $\tilde{A}_i$ is independent of the control gain κ_i.

Note that the closed-loop system under attack (20) is no longer positive, nor diagonally dominant, since we have $[A - \tau_i^{-1}\kappa_i e_i(e_j - e_i)^\top]_{i,j} = -\kappa_i < 0$ and $[A - \tau_i^{-1}\kappa_i e_i(e_j - e_i)^\top]_{i,i} = [A]_{ii} + \kappa_i$. As such, the results of Section IV may not be used to establish the stability of (20). In fact, the closed-loop system (20) may indeed be unstable for certain values of $\kappa_i \geq 0$, as established by the following result.

Theorem 4. *Consider a power system whose linearized dynamics* (10) *are positive. Furthermore, suppose the droop controller at bus i is under a measurement routing attack that feeds the controller with the voltage measurement from the j-th bus, as per Definition 4. Then there exists a control gain $\kappa_i \geq 0$ for which the linearized system under attack* (20) *is unstable if* $\mathrm{dist}(j,i) \geq 2$*, where* $\mathrm{dist}(j,i)$ *is the shortest length between buses i and j.*

Theorem 4 establishes the existence of a positive gain κ_i for which the attacked system becomes unstable when $\mathrm{dist}(j,i) \geq 2$. In other words, for a particular choice of control gains, a measurement routing attack on buses that are not adjacent can lead the system to instability and have severe consequences. Similar results were derived in [19] under the assumption that the open-loop system remains diagonally dominant, which does not hold for the present system.

Numerical example: Recall the example described in Section V-A and consider the measurement routing attack scenario where an adversary replaces the voltage measurement at bus 1 with the voltage measurement of bus 4, which is modeled by (20) with $i = 1$ and $j = 4$. The resulting closed-loop state matrix is

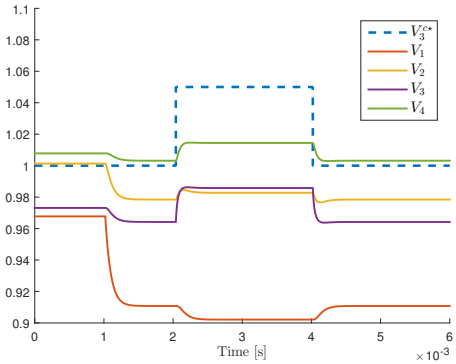
$$\tilde{A}_1 - K_1 e_1 e_4^\top = 10^{-4} \cdot \begin{bmatrix} -2.01 & 1.88 & 0 & -2 \\ 2.1 & -6.01 & 2.04 & 0 \\ 0 & 1.95 & -6.01 & 1.88 \\ 0 & 0 & 2.1 & -4.01 \end{bmatrix},$$

which is clearly not diagonally dominant, nor positive. Despite stability, the lack of such properties leads to contradictory behaviors, as illustrated by the response to a step-change in one reference, depicted in Fig. 5. Despite the increase in the reference signal, bus 1 further decreased its voltage.

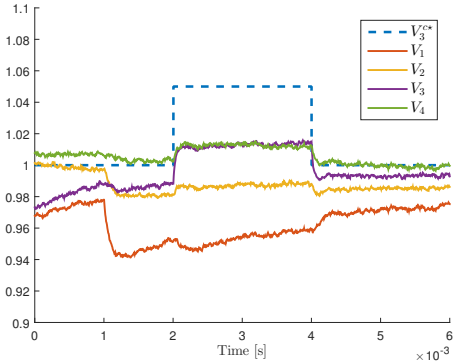
As stated in Theorem 4, since the distance between buses 1 and 4 is greater than 1, there exists a gain $K_1 \geq 0$ for which the system under attack becomes unstable. This is illustrated through the corresponding root-locus depicted in Fig. 6.

VI. Conclusion

In this paper, we studied the properties of a voltage droop control scheme in interconnected microgrids under adversarial actions. First the power system dynamics under nominal operation were analyzed, and conditions ensuring relevant system properties, including stability, were derived. Then, two attack scenarios were discussed, where the adversary is able to manipulate the measurement data and reference signals



(a) Constant phase-angles



(b) Varying phase-angles and measurement noise

Figure 5. Trajectories of the voltage magnitudes under a voltage measurement routing attack that feeds a measurement from bus 4 to bus 1, followed by a reference change at bus 3.

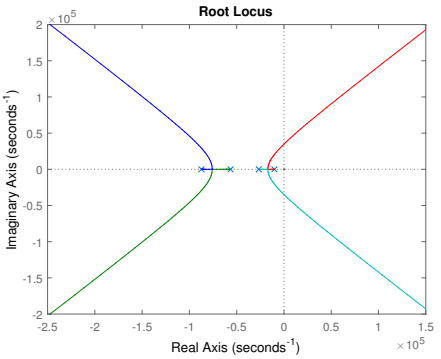


Figure 6. Root-locus of the system (21) with respect to $K_1 \geq 0$.

received by the voltage droop controllers. Each attack scenario admits multiple instances, depending of which set of nodes are attacked. The potential impact of different instances of each scenario were compared using control-theoretic tools, which provides a basis to identify high-risk attack instance in each scenario. Our methodology was illustrated on a line network through numerical examples.

Acknowledgements

This work has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 608224, the Swedish Research Council under Grants 2009-4565 and 2013-5523, the Swedish Foundation for Strategic Research, and the Knut and Alice Wallenberg Foundation.

References

[1] N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay, "Microgrids," *Power and Energy Magazine, IEEE*, vol. 5, no. 4, pp. 78–94, July 2007.

[2] F. Shahnia, R. P. Chandrasena, S. Rajakaruna, and A. Ghosh, "Primary control level of parallel distributed energy resources converters in system of multiple interconnected autonomous microgrids within self-healing networks," *IET Generation, Transmission & Distribution*, vol. 8, no. 2, pp. 203–222, 2014.

[3] G. Andersson, P. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, A. Teixeira, G. Dan, H. Sandberg, and K. Johansson, "Cyber-security of scada systems," in Proc. *IEEE PES Innovative Smart Grid Technologies*, 2012.

[4] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in Proc. *16th ACM Conference on Computer and Communications Security*, 2009.

[5] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in Proc. *First Workshop on Secure Control Systems, CPSWeek*, Stockholm, Sweden, Apr. 2010.

[6] G. Hug and J. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[7] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in Proc. *50th IEEE Conference on Decision and Control*, 2011.

[8] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in Proc. *First IEEE International Conference on Smart Grid Communications*, 2010.

[9] A. Teixeira, H. Sandberg, G. Dán, and K. H. Johansson, "Optimal power flow: closing the loop over corrupted data," in Proc. *American Control Conference*, 2012.

[10] O. Kosut, L. Jia, R. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in Proc. *First IEEE International Conference on Smart Grid Communications*, 2010.

[11] O. Vukovic, K. C. Sou, G. Dán, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1108–1118, 2012.

[12] Y. Isozaki, S. Yoshizawa, Y. Fujimoto, H. Ishii, I. Ono, T. Onoda, and Y. Hayashi, "On detection of cyber attacks against voltage control in distribution power grids," in Proc. *IEEE International Conference on Smart Grid Communications*, 2014.

[13] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. Bobba, and A. Valdes, "Security of smart distribution grids: Data integrity attacks on integrated Volt/VAR control and countermeasures," in Proc. *American Control Conference*, 2014.

[14] B. Kang, P. Maynard, K. McLaughlin, S. Sezer, T. Strasser, F. Andrén, F. Kupzog, and C. Seitl, "Investigating cyber-physical attacks against iec 61850 photovoltaic inverter installations," in Proc. *20th IEEE International Conference on Emerging Technologies and Factory Automation*, 2015, to appear.

[15] J. W. Simpson-Porco, F. Drfler, and F. Bullo, "Synchronization and power sharing for droop-controlled inverters in islanded microgrids," *Automatica*, vol. 49, no. 9, pp. 2603 – 2611, 2013.

[16] J. Simpson-Porco, F. Dorfler, and F. Bullo, "Voltage stabilization in microgrids via quadratic droop control," in Proc. *IEEE 52nd Conference on Decision and Control*, Dec. 2013, pp. 7582–7589.

[17] J. Schiffer, R. Ortega, A. Astolfi, J. Raisch, and T. Sezi, "Conditions for stability of droop-controlled inverter-based microgrids," *Automatica*, vol. 50, no. 10, pp. 2457–2469, 2014.

[18] A. Rantzer, "Scalable control of positive systems," *European Journal of Control*, vol. 24, pp. 72–80, 2015.

[19] J. A.Torres and S. Roy, "Stabilization and destabilization of network processes by sparse remote feedback: Graph-theoretic approach," in Proc. *American Control Conference*, 2014.