Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online CONFERENCE PAPER ARCHIVE

IFAC PapersOnLine 50-1 (2017) 8379–8384

Voltage Control in Distributed Generation under Measurement Falsification Attacks ⋆

Mingxiao Ma * **André M. H. Teixeira** ** **Jan van den Berg** *,** **Peter Palensky** *

* *Faculty Electrical Engineering, Mathematics and Computer Science,*
** *Faculty of Technology, Policy and Management,*
Delft University of Technology, Delft, The Netherlands
(e-mail: {m.ma-3, andre.teixeira, j.vandenBerg, p.palensky}@tudelft.nl).

Abstract: Low-voltage distribution grids experience a rising penetration of inverter-based, distributed generation. In order to not only contribute to but also solve voltage problems, these inverters are increasingly asked to participate in intelligent grid controls. Communicating inverters implement distributed voltage droop controls. The impact of cyber-attacks to the stability of such distributed grid controls is poorly researched and therefore addressed in this article. We characterize the potential impact of several attack scenarios by employing the positivity and diagonal dominance properties. In particular, we discuss measurement falsification scenarios where the attacker corrupts voltage measurement data received by the voltage droop controllers. Analytical, control-theoretic methods for assessing the impact on system stability and voltage magnitude are presented and validated via simulation.

Keywords: Cyber security, distribution network, voltage control, stability, risk assessment.

1. INTRODUCTION

Various distributed generations (DG) are introduced to the power grid due to environmental, economic and technological reasons (Schiffer et al., 2014). To facilitate the reliability and resiliency of the complex energy generation paradigm, power networks need to be tightly coupled with the supervisory control and data acquisition (SCADA) systems. Communication networks play an increasingly important role in the SCADA systems because more information must be collected, transmitted and processed for estimation and control of power generation, consumption, and storage (Isozaki et al., 2014). However, the power infrastructure coupled with SCADA systems is vulnerable to malicious cyber attacks due to the wide use of communication networks. To ensure the safe and stable operation of power systems, increasing attention has been given to analyze potential vulnerabilities of the system and design resilient schemes to mitigate or prevent high-risk threats (Teixeira et al., 2015).

Compared to the substantial efforts invested in the cyber security concerns of power transmission networks (Sandberg et al., 2010), security issues at the distribution level have not been extensively explored. Cyber-secure modeling frameworks are proposed in Giacomoni et al. (2011) and Kundur et al. (2011), considering both the power grid and the communication networks, but the impact of cyber attacks are not addressed. Isozaki et al. (2014) studies the the impact of cyber attacks on centralized voltage regulation in distribution systems and proposes a detection algorithm to mitigate the attack impact. Teixeira et al. (2014) studies the vulnerabilities that may be introduced by stealthy data integrity attacks against the integrated Volt-VAR control system. None of the previous works have studied the consequences of cyber attacks on inverter-based distributed energy resource. However, the recent work of Kang et al. (2015) studies the capability of cyber attackers to falsify the IEC 61850 data flow controlling inverter-based devices and, thus, causes damage to the underlying physical system. Further more, another recent work Teixeira et al. (2015) first tackles the revelent attack scenarios and threat models against voltage stability and reactive power balancing in the droop-controlled inverters, and provide criteria for designing the controller gains in terms of the power system parameters.

In this paper, we introduce risk assessment methods in the context of voltage control in distribution systems with droop-controlled DGs. We focus on the case of reactive power control of DGs through interfacing equipments and study cyber attacks against droop controllers in the DG level. And different from Teixeira et al. (2015), this paper specifically considers attacks on sensor measurements and studies their impacts on stability and voltage deviation by control-theoretic analysis and simulations.

We consider cyber attackers that may corrupt the sensor measurements through a multiplicative bounded scaling factor, and perform quantitative analysis on the degradation of the system's stability and voltage levels in the presence of attacks. These results help to indicate high-risk threats to the system, which are valuable for the system designers to evaluate vulnerabilities and propose system designs with high cyber security standards.

⋆ This work is sponsored by Chinese Scholarship Council (CSC).

10.1016/j.ifacol.2017.08.1562

The rest of the paper is organized as follows. In Section II, we provide an overview on some definitions and known results. Section III describes the system model and controller structure for the inverter-based DGs and formulates the problem to be studied. In Section IV, we describe the measurement falsification attack scenarios and perform the impact assessment in terms of stability under attack and voltage magnitude deviation. In Section V, we run the simulation experiments and further illustrate the attack impacts of measurement falsification attack. Finally remarks and conclusions are given in Section VI.

2. PRELIMINARIES

In this section, we review several important definitions and properties with regard to certain classes of linear time-invariant (LTI) systems that will be useful in building our system model and running further theoretical analysis. Consider a state-space represented continuous LTI system:

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

In the LTI system (1), $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$ and $y(t) \in \mathbb{R}^p$ are the state vector, the input vector, and the output vector at time t, respectively. And A, B, C and D are the dynamics matrix, input matrix, output matrix and feedthrough matrix 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). A square matrix A is called 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 Definition 1, the system (1) is called to be row-diagonally dominant if the dynamics matrix A is row-diagonally dominant.

Besides row-diagonally dominant systems, another important class of systems throughout this paper is that of positive systems. Next we describe the definition and properties of positive systems.

Definition 2. (Positive systems). The LTI system (1) is said to be (internally) positive if and only if its state $x(t)$ and output $y(t)$ are non-negative for every non-negative input $u(t)$ and every non-negative initial state $x(0)$.

Lemma 1. (Positivity). The LTI system (1) is positive if and only if A is a Metzler-matrix, i.e., it has non-negative off-diagonal entries, and B, C and D are non-negative, i.e., they only have non-negative entries.

Lemma 2. (Rantzer (2015)). If the system (1) is positive, the following statements are equivalent:

1) the matrix A is Hurwitz, i.e., every eigenvalue of A has strictly negative real part).
2) There exists a $\xi \in \mathbb{R}^n$ such that $\xi > 0$ and $A\xi < 0$.
3) The matrix $-A^{-1}$ exists and has nonnegative entries.

3. PROBLEM FORMULATION

3.1 System Model

As illustrated in Fig. 1, the power distribution system consists of a set of interconnected DG units. Each DG unit may contain several inverter-based distributed energy resources (DER), controllers and loads. These DG units may be connected to the main grid through the feeder substation.

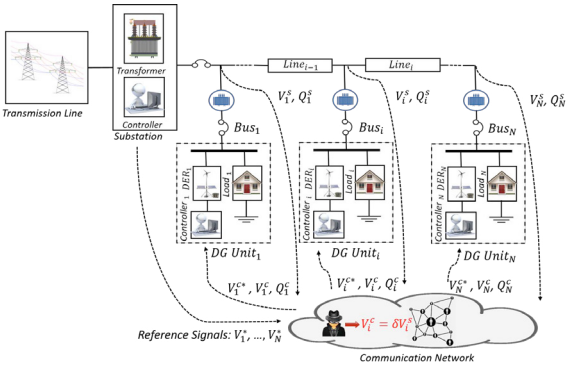

Fig. 1. A power distribution system consisting of interconnected DG units with inverter-based DERs, controllers and loads.

The generic network topology can be 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. Fig. 1 depicts a distribution network with line topology. 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 system under study, we make the following assumptions:

1) The system has balanced three-phase power network, i.e., it can be represented as an equivalent single-phase system;
2) All N buses are inverter-based, and represented by V_i and θ_i for $i = 1, \ldots, N$.

Let R_{ij} and X_{ij} be resistance and reactance of the transmission line between bus i and bus j, respectively, thus under Assumption 1, the active and reactive power injections at bus i is given respectively by

$$\begin{aligned} P_i &= V_i^2 G_i - \sum_{j \in N_i} V_i V_j (G_{ij} \cos(\theta_{ij}) + B_{ij} \sin(\theta ij)), \\ Q_i &= -V_i^2 B_i - \sum_{j \in N_i} V_i V_j (G_{ij} \sin(\theta_{ij}) - B_{ij} \cos(\theta ij)), \end{aligned} \tag{3}$$

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 bus i and bus j. Additionally, we define self-conductance and self-susceptance as $G_i = G_{ii} + \sum_{j \in N_i} G_{ij} \geq 0$ and $B_i = B_{ii} + \sum_{j \in N_i} B_{ij} \leq 0$, respectively. Note that we use $\theta_{ij} = \theta_i - \theta_j$ to represent the angle difference between node i and j in the remainder of this paper.

Assumption 2. In the power distribution system under study, we assume the transmission line impedances have