Voltage Control in Distributed Generation under Measurement Falsification Attacks

Ma, Mingxiao; Herdeiro Teixeira, André; van den Berg, Jan; Palensky, Peter

DOI
10.1016/j.ifacol.2017.08.1562

Publication date
2017

Document Version
Final published version

Published in
IFAC-PapersOnLine

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.

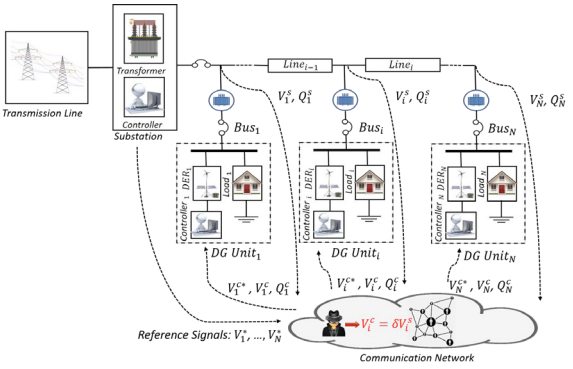

Fig. 1. A power distribution system consisting of interconnected DG units with inverter-based DERs, controllers and loads.

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

the same ratio $R_{ij}/X_{ij} = -G_{ij}/B_{ij} = \rho \geq 0$ for all lines $(i,j) \in \mathcal{E}$.

3.2 Controller Structure

For each DG unit, the voltage and phase-angle dynamics can be respectively modeled by a single integrator

$$\begin{aligned} \tau_i \dot{V}_i(t) &= u_{v_i}(t), \\ \tau_{\theta_i} \dot{\theta}_i(t) &= u_{\theta_i}(t), \end{aligned} \tag{4}$$

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 $t \geq 0$. As illustrated in Fig. 1, the measurements and reference signals are available to each controller from the architecture of the control system. Each DG unit is controlled by a droop controller based on the capabilities of the local inverter-based DERs. Each controller receives the reference signal computed remotely and measurements through the communication network. Let V_i^* be the reference voltage for the i-th bus and V_j and θ_j, be the voltage magnitude and voltage angle of the j-th bus, respectively. A suitable communication protocol is needed for the transmission of these data, e.g., IEC 61850.

In this paper, we are mainly interested in the voltage dynamics of the power distribution system. So we consider the following assumption and neglect the phase-angle dynamics throughout the rest of the paper.

Assumption 3. The phase-angle difference θ_{ij} between any neighboring nodes i and j is assumed to be constant.

Note that Assumption 3 could be employed to in a local analysis when the phase-angles remain in the neighborhood of the original equilibrium point. In addition, we underline that the assumption is valid if there exists a time-scale separation between the voltage dynamics and the phase-angle.

In order to compute the control output signals, we refer to the voltage quadratic droop controller (Simpson-Porco et al., 2013) described by

$$u_{V_i}(t) = -\kappa_i V_i^c(t)(V_i^c(t) - V_i^{c*}(t)) - Q_i^c(t), \tag{5}$$

where $\kappa_i > 0$ is the control gain of the droop controller. Additionally, $V_i^c(t)$, $V_i^{c*}(t)$ and $Q_i^c(t)$ respectively represent the voltage measurement, voltage reference signal with respect to bus i and reactive power injection measurement. They are received by the droop controller, as illustrated in Fig. 1. Under nominal operation, these signals 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 $V_i^{c*}(t) = V_i^*(t)$ ($V_i^*(t)$ is sent by a higher level controller from the substation). The closed-loop dynamics of the i-th DG unit under nominal operation are described by the differential equations

$$\begin{aligned} \tau_i \dot{V}_i &= -\kappa_i V_i (V_i - V_i^*) - Q_i \\ &= -V_i(\kappa_i V_i - \kappa_i V_i^* + \sum_{j \in \mathcal{V}} l_{ij}(\theta) V_j), \forall i = 1, \ldots, N, \end{aligned} \tag{6}$$

with the time argument omitted. Additionally, under the Assumption 2, the parameter $l_{ij}(\theta)$ is described as

$$l_{ij}(\theta) = \begin{cases} B_{ij}(\rho \sin(\theta_{ij}) + \cos(\theta_{ij})), & i \neq j \\ -B_i, & i = j. \end{cases} \tag{7}$$

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

$$[\tau]\dot{V} = [V]([\kappa]V^* - ([\kappa] + L(\theta))V), \tag{8}$$

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

Linearization of the voltage dynamics. In the subsequent sections, we consider the Jacobian linearization of the power system (8) around an equilibrium point $(\bar{V}, \bar{V}^{c*})$ such that $-([\kappa] + L(\theta))\bar{V} + [\kappa]\bar{V}^* = 0$. Denote $x(t) = V(t) - V$ and $u(t) = V^{c*}(t) - \bar{V}^{c*}$ as the voltage and reference deviations, respectively. By Assumption 3, the corresponding linearized system is described by

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{9}$$

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

3.3 System properties

In this subsection, necessary and sufficient conditions for the linearized power system to be positive are elaborated. These conclusions will play an important role in the impact analysis for the power system under attack in subsequent sections.

Firstly, the following assumption is required to derive necessary and sufficient conditions for the linearized system (9) to be positive.

Assumption 4. The maximum phase difference between any two neighboring nodes, defined as $\Delta_\theta := \max_{(i,j)\in\mathcal{E}} |\theta_{ij}|$, satisfies the inequality $\Delta_\theta < \pi/2$.

For any conventional power system, the constraint $\Delta_\theta < \pi/2$ is required for the stability of the phase-angle dynamics (Schiffer et al., 2014). Under the previous assumptions, we establish the following result for system positivity.

Lemma 3. (Teixeira et al. (2015)). Consider the power distribution system under study, having active and reactive power injections (3) at bus i with $\Delta_\theta < \pi/2$, and applying the quadratic droop controller (6) for each DG unit. Then a necessary and sufficient condition for the corresponding linearized system (9) to be positive is

$$\rho \leq |\cot(\Delta_\theta)|. \tag{10}$$

The properties of positive systems will play important roles in analyzing the stability of the linearized system under attack, and they are also used in the characterization of the attack impacts.

4. ATTACK IMPACT ASSESSMENT

In this section, we assess the impact of adversary actions in terms of the distribution system described in the previous section. We mainly consider one specific type of attack scenarios: measurement falsification attack, as is shown in Fig. 1. First we give definition to the considered attack scenario and describe how it influences the droop controller. Then, we mathematically characterize the attack impact on system stability and voltage magnitude deviation by employing properties of the linearized system.

4.1 Measurement Falsification Attack

We set the goal of the attacker to cause overvoltage and undervoltage as much as possible, within the limitation of attacking one node only. In particular, we consider the measurement falsification attack defined as follows.

Definition 3. (Measurement falsification attack). In a measurement falsification attack on bus i, the attacker manipulates the voltage measurement of bus i by multiplying a measurement falsification ratio $\delta \in (0, +\infty)$, so that

$$V_i^c(t) = \delta V_i(t), \tag{11}$$

where $V_i^c(t)$ is the voltage measurement at bus i, $V_i(t)$ is the real voltage magnitude at bus i.

Note that, if $\delta > 1$, the attacker increases the voltage measurement; if $0 < \delta < 1$, the attacker decreases the voltage measurement. Furthermore, the control signal at bus i under a measurement falsification attack is given by

$$u_{V_i}(t) = -\kappa_i \delta V_i(t)(\delta V_i(t) - V_i^{c*}(t)) - Q_i^c(t). \tag{12}$$

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

$$\dot{x}(t) = (A - (\delta - 1)\tau_i^{-1}\kappa_i e_i e_i^\top)x(t), \tag{13}$$

where the term $-(\delta - 1)\tau_i^{-1}\kappa_i e_i e_i^\top x(t)$ can be interpreted as replacing the nominal feedback term $\tau_i^{-1}\kappa_i V_i$ by the corrupted term $\delta\tau_i^{-1}\kappa_i V_i$ at bus i.

4.2 Stability under Attack

The stability analysis of the power system under attack is a very important part of the risk assessment. Next we employ the positivity and row-diagonally dominance properties to establish the stability of the linearized system under attack.

Lemma 4. Consider the linearized dynamics of the power system (9) and suppose the system is positive. Note that $[A - (\delta - 1)\tau_i^{-1}\kappa_i e_i e_i^\top]_{i,i} = [A]_{i,i} - (\delta - 1)\kappa_i$, and $[A - (\delta - 1)\tau_i^{-1}\kappa_i e_i e_i^\top]_{i,j} = [A]_{i,j}$ for $j \neq i$. Therefore the linearized system under measurement falsification attack (13) is positive.

Lemma 4 ensures the positivity of the attacked system. Here we give the stability criterion of system under attack as follows:

Theorem 1. (Stability with specific δ value). Consider a power system whose linearized dynamics (9) are positive. Furthermore, suppose the droop controller at bus i is under a measurement falsification attack that feeds the controller with the voltage measurement by multiplying a measurement falsification ratio δ, as per Definition 3. Then the following statements hold:

1) the system under attack with a specific $\delta \in (0, +\infty)$ is asymptotically stable if and only if there exist positive scalars $\xi > 0$ such that the following inequality holds for all $l = 1, \ldots, n$ and $\delta \in (0, +\infty)$:
$$\begin{cases} \xi_l \left|\kappa_l + B_l\right| > \sum\limits_{j \in \mathcal{N}_l} \xi_j \left|-B_{lj}(\rho \sin(\theta_{lj}) + \cos(\theta_{lj}))\right|, & l \neq i, \\ \xi_l \left|-\delta\kappa_l + B_l\right| > \sum\limits_{j \in \mathcal{N}_l} \xi_j \left|-B_{lj}(\rho \sin(\theta_{lj}) + \cos(\theta_{lj}))\right|, & l = i. \end{cases}$$
2) the system under attack with a specific $\delta \in (0, +\infty)$ is asymptotically stable if it is row-diagonally dominant, i.e., the following inequality holds for all $l = 1, \ldots, n$ and $\delta \in (0, +\infty)$:
$$\begin{cases} \left|\kappa_l + B_l\right| > \sum\limits_{j \in \mathcal{N}_l} \left|-B_{lj}(\rho \sin(\theta_{lj}) + \cos(\theta_{lj}))\right|, & l \neq i, \\ \left|-\delta\kappa_l + B_l\right| > \sum\limits_{j \in \mathcal{N}_l} \left|-B_{lj}(\rho \sin(\theta_{lj}) + \cos(\theta_{lj}))\right|, & l = i. \end{cases}$$

Proof. According to (7) and (13), the entries of $(A - (\delta - 1)\tau_i^{-1}\kappa_i e_i e_i^\top)$ can be written as

$$a_{ij} = \begin{cases} -\tau_i^{-1} B_{ij}(\rho \sin(\theta_{ij}) + \cos(\theta_{ij})), & i \neq j \\ \tau_i^{-1}(-\delta \cdot \kappa_i + B_{ii} + \sum\limits_{j \in \mathcal{N}_i} B_{ij}), & i = j. \end{cases} \tag{14}$$

The necessary and sufficient condition for stability follows directly from the positivity of the system (Lemma 1) and its related properties (Lemma 2), i.e., the existence of a positive vector $\xi > 0$ such that $(A - (\delta - 1)\tau_i^{-1}\kappa_i e_i e_i^\top)\xi < 0$.

On the other hand, the sufficient condition for stability is obtained by considering $\delta = 0$ and $\xi_i = 1$ for all i and verifying that $A\mathbf{1} < 0$, given that τ_i and $(\rho \sin(\theta_{ij}) + \cos(\theta_{ij}))$ are positive and B_{ij} is negative. □

Theorem 1 establishes the stability of the linearized system (9) under measurement falsification attack with a specific $\delta \in (0, +\infty)$. On the other hand, we are also interested in the general stability conditions under attack without a specific δ value, i.e., for $\forall \delta \in (0, +\infty)$, the system under attack is always stable.

For the convenience of analyzing the general system stability under attack, we can rewrite the attack scenario (13) as the following static output-feedback law

$$\begin{aligned} \dot{x}(t) &= (A + \tau_i^{-1}\kappa_i e_i e_i^\top)x(t) + \tau_i^{-1}\kappa_i e_i u(t) \\ y_i(t) &= e_i^\top x(t) \\ u(t) &= -\delta y_i(t), \end{aligned} \tag{15}$$

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. Then the general system stability under attack is equivalent to stability of linearized system (15) for $\forall \delta \in (0, +\infty)$.

Corollary 1. (General stability under attack). Consider a power system with positive linearized dynamics (9) and the droop controller at bus i is under a measurement falsification attack as per Definition 3. Then the system under attack is asymptotically stable for $\forall \delta \in (0, +\infty)$ if and only if the matrix $(A + \tau_i^{-1}\kappa_i e_i e_i^\top)$ is Hurwitz.

Proof. Note that system (15) is positive according to Lemma 1. Using Lemma 2, the matrix $(A + \tau_i^{-1}\kappa_i e_i e_i^\top)$ is Hurwitz, if and only if there exist positive scalars $\xi > 0$ such that the following inequality holds for all $l = 1, \ldots, n$:

$$\begin{cases} \xi_l \left|\kappa_l + B_l\right| > \sum\limits_{j \in \mathcal{N}_l} \xi_j \left|-B_{lj}(\rho \sin(\theta_{lj}) + \cos(\theta_{lj}))\right|, & l \neq i, \\ \xi_l \left|B_l\right| > \sum\limits_{j \in \mathcal{N}_l} \xi_j \left|-B_{lj}(\rho \sin(\theta_{lj}) + \cos(\theta_{lj}))\right|, & l = i. \end{cases}$$

Note that $\kappa_l > 0$ and $B_l \leq 0$, so we have $|-\delta\kappa_l + B_l| > |B_l|$ for $\forall \delta \in (0, +\infty)$. So the necessary and sufficient condition in Theorem 1 holds for $\forall \delta \in (0, +\infty)$. □

Remark 1. From Corollary 1, we can draw a further conclusion that, for a linearized system under attack (13), if the system is stable for $\delta = 0$, then it is stable for $\forall \delta \in (0, +\infty)$.

4.3 Voltage Magnitude Deviation

In addition to system stability, the impact of measurement falsification attack also includes the resulting changes to the voltage magnitudes in the network. Consider the power system satisfying the conditions of Lemma 3 and suppose the system under attack (13) is positive and stable. Let $\bar{x}$ and $\tilde{x}$ be the stable system states before and after a measurement falsification attack, respectively. And $\bar{x}_i$ and $\tilde{x}_i$ represents the i-th entry of $\bar{x}$ and $\tilde{x}$, respectively.

The attack impact can be measured in terms of the stable state voltage magnitude deviation $\Delta x = |\tilde{x} - \bar{x}|$. In particular, we quantify the attacker's impact at another bus $j \neq i$ as the maximum deviation caused by a measurement falsification attack at bus i. We establish the following characterization of the worst-case impact under attack.

Theorem 2. Consider the linearized power system (9), which is assumed to be positive and asymptotically stable with bus i under a measurement falsification attack (13), where the measurement falsification ratio $\delta \in (0, +\infty)$ is bounded as $|\delta - 1| \leq \varepsilon$. For constant references, Define $\Delta x_j^* = \max_{\delta} |\tilde{x}_j - \bar{x}_j|$ be the worst-case impact on bus j. Then we have $\Delta x_j^* = \zeta_i \bar{x}_i [-A]_{j,i}$, where $\zeta_i = \min\left\{ |\frac{\tau_i}{\varepsilon \kappa_i} - [A^{-1}]_{i,i}|, |\frac{\tau_i}{-\varepsilon \kappa_i} - [A^{-1}]_{i,i}| \right\}$.

Proof. Considering the linearized system (9), let $\dot{x} = 0$ and we get $\bar{x} = -A^{-1}Bu$, i.e., $Bu = -A\bar{x}$. Substituted into (13), we get

$$\tilde{x} = (A - (\delta - 1)\tau_i^{-1}\kappa_i e_i e_i^\top)^{-1} A\bar{x}.$$

Using the Woodbury matrix identity, we get

$$\tilde{x} = \bar{x} + (\frac{\tau_i}{(\delta - 1)\kappa_i} - [A^{-1}]_{i,i})^{-1} A^{-1} e_i \bar{x}_i,$$

Since $\zeta_i = \min\left\{ |\frac{\tau_i}{\varepsilon \kappa_i} - [A^{-1}]_{i,i}|, |\frac{\tau_i}{-\varepsilon \kappa_i} - [A^{-1}]_{i,i}| \right\}$ and we have $-A^{-1} > 0$ according to Lemma 2, so we get

$$\begin{aligned} \Delta x_j^* &= \max_{\delta} |\tilde{x}_j - \bar{x}_j| \\ &= \max_{\delta} |(\frac{\tau_i}{(\delta - 1)\kappa_i} - [A^{-1}]_{i,i})^{-1} \bar{x}_i [A^{-1}]_{j,i}| \\ &= \zeta_i \bar{x}_i [-A^{-1}]_{j,i}. \end{aligned}$$

□

Lemma 5. Considering the linearized power system (9) under attack (13), where the measurement falsification ratio $\delta \in (0, +\infty)$ is bounded as $|\delta - 1| \leq \varepsilon$ at bus i, the following equation holds:

$$\zeta_i = |\frac{\tau_i}{-\varepsilon \kappa_i} - [A^{-1}]_{i,i}|. \tag{16}$$

Proof. Note that $\tau_i > 0$, $\kappa_i > 0$, and $-[A^{-1}]_{i,i} > 0$ according to Lemma 2, so inequality $|\frac{\tau_i}{\varepsilon \kappa_i} - [A^{-1}]_{i,i}| > |\frac{\tau_i}{-\varepsilon \kappa_i} - [A^{-1}]_{i,i}|$ holds for $\forall \varepsilon > 0$. □

Remark 2. From Lemma 5, we can draw the conclusion that, for attack (13) at bus i with boundary $|\delta - 1| \leq \varepsilon$, decreasing the voltage measurement can cause a higher impact on the maximum deviation at other buses than increasing the measurement.

4.4 Identification of Most Affected Buses

The worst-case impact characterization can be used to identify which buses are more vulnerable than others under certain attack scenarios. In the case of measurement falsification attack at bus i, we are interested to identify the most affected bus, i.e., we want to find

$$j^* = \arg\max_j \Delta x_j^* = \arg\max_j [-A^{-1}]_{j,i},$$

where the common factor $\zeta_i \bar{x}_i$ has been omitted.

Every entry of $-A^{-1}$ would be needed to solve the problem generally. However, properties of specific network topologies (e.g., line network) could give simpler answers to this problem. In Teixeira et al. (2015), the authors prove that for a power distribution system with line topology and positive and row-diagonally dominant linearized dynamics (9), the following inequalities hold:

$$\begin{aligned} [-A^{-1}]_{j,i} &> [-A^{-1}]_{j+1,i}, \forall i \leq j \\ [-A^{-1}]_{j,i} &> [-A^{-1}]_{j-1,i}, \forall i \geq j. \end{aligned} \tag{17}$$

According to (17), we have the following Lemma:

Lemma 6. Consider a power distribution network with a line topology and the respective linearized dynamics (9) are positive and asymptotically stable with bus i under a measurement falsification attack (13), whose worst-case impact on bus j is given by $\Delta x_j^* = \zeta_i \bar{x}_i [-A]_{j,i}$. The worst-case impact Δx_j^* decreases as the distance between j and i increases, i.e., the bus most affected by the attack at bus i, defined as $j^* = \arg\max_j [-A^{-1}]_{j,i}$, corresponds to one of the neighboring buses of i, i.e., $j^* = \arg\max_{j \in \{i-1, i+1\}} [-A^{-1}]_{j,i}$.

5. SIMULATION

In this section, we verify the risk assessment methodology proposed in the previous section via simulation.

5.1 Simulation Settings

For our simulation studies on the risk assessment of the attack on the voltage measurement at different nodes, we use simulink tools provided by Matlab.

In our simulation settings, an islanded 4-bus power distribution network with a line topology is considered. As depicted in Fig. 1, we assume $N = 4$ and all power lines, loads, and inverters are identical. We characterize the power system by (3) and set the parameters as follows: $\rho = 0.5$, $B_{ij} = -0.2$, and $G_{ij} = -\rho B_{ij}$ for all edges $(i, j) \in \mathcal{E}$ and $B_{ij} = -0.2$ and $G_{ii} = -\rho |B_{ii}|$ for all buses. We also model the power inverters by (4) and (5) and set the parameters as follows; $\tau_i = 10^{-4}$, $\tau_{\theta_i} = 10^{-2}$, and $\kappa_i = 0.2$ for all buses. To satisfy the conditions in Assumption 3, we set the phase-angle differences as $\theta_{12} = -0.01$rad, $\theta_{23} = -0.045$rad, and $\theta_{34} = -0.01$rad. Thus we perform simulations under the condition that the phase-angle differences are constant throughout the simulation of the voltage dynamics

Consider the voltage dynamics described by the nonlinear differential equations (8). By Jacobian linearization, we

get the corresponding linearized dynamics characterized by (9) 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.

Now consider the measurement falsification attack scenario where the voltage measurement at bus 2 is corrupted by an attacker by multiplying a measurement falsification ratio $\delta = 1.1$ and $\delta = 0.9$, as per Definition 5. Following the discussion in this section, we will analyze the stability under attack and seek to assess which buses, other than bus 1, are most affected by such attack.

5.2 Simulation Results

Considering above simulation settings, for two specific measurement falsification ratios $\delta = 0.9$ and $\delta = 1.1$, the sufficient conditions in Theorem 1 are satisfied. So the linearized system (9) under attack (13) with $\delta = 0.9$ and $\delta = 1.1$ is asymptotically stable. Moreover, we can also draw the conclusion that the closed-loop system (9) under attack is asymptotically stable for $\forall \delta \in (0, +\infty)$ by employing Corollary 1.

In Fig. 2, we observe how the worst-case impact Δx_j^* on bus j of a measurement falsification attack on bus $i = 2$ scales with an increasing $\delta \in (0, +\infty)$ and different values of j. Note the curve slope differences between interval $\delta < 1$ and interval $\delta > 1$, Fig. 2 also proves the correctness of Lemma 5, i.e., when $\delta \in (0, +\infty)$ is bounded as $|\delta - 1| \leq \varepsilon$ at bus i, decreasing the voltage measurement at bus i can cause a more severe impact on the maximum deviation at other buses than increasing the measurement.

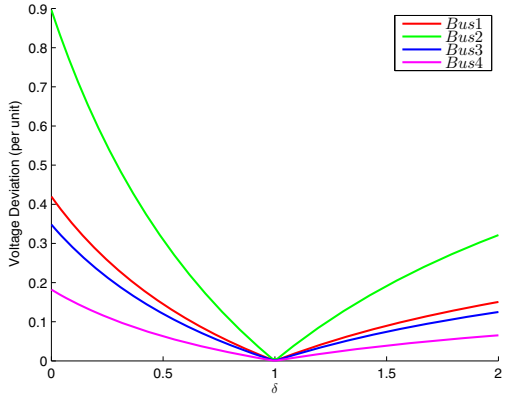

Fig. 2. Trajectories of the voltage deviations under a measurement falsification attack at bus 2 with respect to $\delta > 0$.

6. CONCLUSION

In this paper, we assess the impact of measurement falsification attacks on droop controlled DG units under cyber attacks. The potential impact of measurement falsification attack was derived using control-theoretic tools, which provides a basis to identify high-risk attack instance in each scenario. We find that decreasing the voltage measurement results in a higher impact than increasing it and neighboring nodes suffer more from the attacked node in a line network. It is interesting but challenging to develop methodologies to asses the impact of more detailed and complex system models and more sophisticated attack scenarios. This will be left as a future work and we could get inspirations from this work.

REFERENCES

Giacomoni, A., Amin, S.M., and Wollenberg, B. (2011). A control and communications architecture for a secure and reconfigurable power distribution system: An analysis and case study. *IFAC Proceedings Volumes*, 44(1), 1678–1684.

Isozaki, Y., Yoshizawa, S., Fujimoto, Y., Ishii, H., Ono, I., Onoda, T., and Hayashi, Y. (2014). On detection of cyber attacks against voltage control in distribution power grids. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, 842–847. IEEE.

Kang, B., Maynard, P., McLaughlin, K., Sezer, S., Andren, F., Seitl, C., Kupzog, F., and Strasser, T. (2015). Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations. In *Emerging Technologies & Factory Automation (ETFA), 2015 IEEE 20th Conference on*, 1–8. IEEE.

Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T., and Butler-Purry, K. (2011). Towards modelling the impact of cyber attacks on a smart grid. *International Journal of Security and Networks*, 6(1), 2–13.

Rantzer, A. (2015). Scalable control of positive systems. *European Journal of Control*, 24, 72–80.

Sandberg, H., Teixeira, A., and Johansson, K. (2010). On security indices for state estimators in power networks. In *First Workshop on Secure Control Systems (SCS), Stockholm, 2010*.

Schiffer, J., Ortega, R., Astolfi, A., Raisch, J., and Sezi, T. (2014). Conditions for stability of droop-controlled inverter-based microgrids. *Automatica*, 50(10), 2457–2469.

Simpson-Porco, J., Dörfler, F., and Bullo, F. (2013). Synchronization and power sharing for droop-controlled inverters in islanded microgrids. *Automatica*, 49(9), 2603–2611.

Sou, K., Sandberg, H., and Johansson, K. (2011). Electric power network security analysis via minimum cut relaxation. In *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*, 4054–4059. IEEE.

Teixeira, A., Dán, G., Sandberg, H., Berthier, R., Bobba, R., and Valdes, A. (2014). Security of smart distribution grids: Data integrity attacks on integrated volt/var control and countermeasures. In *American Control Conference (ACC), 2014*, 4372–4378. IEEE.

Teixeira, A., Paridari, K., Sandberg, H., and Johansson, K. (2015). Voltage control for interconnected microgrids under adversarial actions. In *Emerging Technologies & Factory Automation (ETFA), 2015 IEEE 20th Conference on*, 1–8. IEEE.