On the Impact of Synchronization Attacks on Distributed and Cooperative Control in Microgrid Systems

Mingxiao Ma, Abdelkader Lahmadi

On the Impact of Synchronization Attacks on Distributed and Cooperative Control in Microgrid Systems

Mingxiao Ma, Abdelkader Lahmadi
Université de Lorraine, CNRS, Inria, Loria, F-54000 Nancy, France
Email: {mingxiao.ma, abdelkader.lahmadi}@loria.fr

***Abstract*—Microgrids are adopted to provide distributed generation of renewable energy resources and scalable integration of loads. To ensure the reliability of their power system operations, distributed and cooperative control schemes are proposed by integrating communication networks at their control layers. However, the information exchanged at the communication channels is vulnerable to malicious attacks aiming to introduce voltage instability and blackouts. In this paper, we design and evaluate a novel type of attacks on the cooperative control and communication layers in microgrids, where the attacker targets the communication links between distributed generators (DGs) and manipulates the reference voltage data exchanged by their controllers. We analyze the control-theoretic and detectability properties of this attack to assess its impact on reference voltage synchronization at the different control layers of a microgrid. Results from numerical simulation are presented to demonstrate this attack, and the maximum voltage deviation and inaccurate reference voltage synchronization it causes in the microgrid.**

I. Introduction

Modern electric power distribution networks integrate various distributed generators (DGs), including photovoltaic (PV) and wind power generation systems to address environmental concerns [9]. DGs are designed to support renewable energy resources by interfacing them through voltage source inverters (VSI), which provide the required control inputs. To successfully coordinate DGs, autonomous subsystems called microgrids are introduced to the power networks. A microgrid is a small-scale low-voltage electrical network, consisting of generation units, loads and storage elements, where dedicated control systems enable them to provide guaranteed power quality for local loads and have a high integration of distributed generation.

To guarantee safe and reliable operations of microgrids, power networks need to be tightly coupled with supervisory control and data acquisition (SCADA) systems. SCADA systems collect data from remote sensors and send back supervisory control commands to monitor and operate power facilities. Communication networks play an increasingly important role in this process because more information need to be collected and transmitted due to the rapidly growing of penetration of distributed generation [3]. However, the widely use of communication networks introduces new challenges to the power infrastructure coupled with SCADA, as these systems are vulnerable to malicious cyber attacks. A power outage incident caused by the malware "BlackEnergy" in Ukraine during 2015 has proved that cyber attacks could cause a major damage on power quality and devices. Thus, it is important to study potential vulnerabilities of these systems and design mitigation or prevention schemes against their high-risk threats [12].

In [2] and [5], the authors propose cyber security modeling frameworks including both power system and communication networks. The analysis of cyber threats of centralized voltage regulation in distribution grid and their respective detection and mitigation schemes is explored in [3]. In particular, stealthy attacks targeting transmitted data integrity of the integrated Volt-VAR control system is studied in [11]. Furthermore, the capability of attackers to falsify the IEC 61850 data flow controlling the inverters is studied in [4], which could cause damage to the underlying physical system. However, none of these works give a comprehensive analysis about the consequences of cyber attacks on the power system.

Specifically, regarding cyber attacks on the voltage/frequency control systems of microgrid systems, in [12], the authors consider two types of attack scenario, reference signal attack and measurement routing attack, and study their impact on voltage stability and deviation in the droop-controlled DGs. Risk assessment methods to quantify the impact of measurement falsification attacks on a microgrid system are studied in [6]. To the best of our knowledge, these previous works only consider threat models targeting primary control level of a microgrid system.

In this paper, we consider a more comprehensive control structure for a microgrid system, mainly a hierarchical control approach consisting of three control levels: primary, secondary and tertiary control [1]. Specifically, we design a distributed cooperative hierarchical control system consisting of droop control as primary control and cooperative control as secondary control. We believe this control scheme is more realistic and reliable than the control architecture considered in [12] and [6], because of its better support for scalable integration of local loads and high integration of distributed generation.

Based on the above control model, we consider cyber attacks that may target the communication links between DGs, and we use risk assessment methods to quantitively analyze the impact of these attacks on voltage deviation at the primary control level and reference voltage synchronization at

the secondary control level. Our impact analysis results are valuable for microgrid system designers to help them evaluate potential cyber threats targeting these systems.

The rest of the paper is organized as follows. In Section II, we present the microgrid model with a hierarchical control structure and we provide the basic settings for the power grid and the communication network. In Section III, we design a distributed cooperative control system and detail it details at the primary and secondary control levels. In Section IV, we detail the reference attack scenarios and perform its impact analysis in terms of voltage deviation and reference synchronization. In Section V, we present our simulations experiments to validate the theoretical analysis of the attack impact. Finally, we conclude the paper in Section VI.

II. System Model

In this section, we describe the model of a microgrid system in terms of its hierarchical control structure and communication network.

A. Microgrid System with Hierarchical Control Structure

Microgrids are designed to work in both gird-connected and islanded operating modes, depending on whether connecting or not to the main grid. The task of the microgrid control system is to regulate voltage and frequency for different operating modes, to achieve proper load sharing among DGs, to control the power flow between the main grid and the microgrid, and to optimize the cost of its operations.

Currently, a hierarchical control structure is designed to achieve the above operating goals [1]. As shown in Figure 1, the hierarchical control structure consists of primary, secondary and tertiary control levels. Each control level has its own control goals because of operating in different timescales. The primary control operates on a fast timescale, and is responsible for the control of transients to stabilize the voltage and frequency of the microgrid during changing of load or generation, or subsequent to an islanding event. Secondary control is designed to compensate for voltage and frequency deviations caused by primary control in terms of fault conditions. Finally, tertiary control, as the highest and slowest control level, optimizes the operations in both operating modes and manages to control the power flow between the main grid and the microgrid.

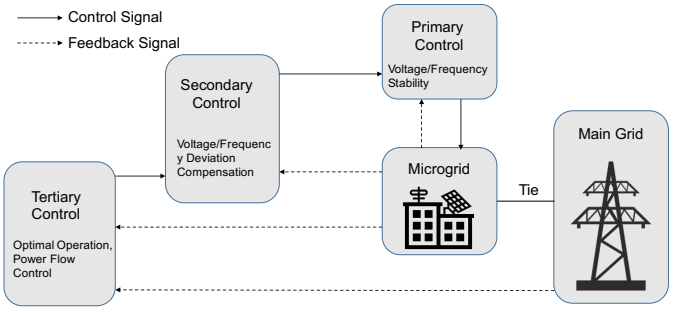

Fig. 1. The hierarchical control structure of a microgrid consisting of primary, secondary and tertiary control levels as specified in [1].

In this paper, we mainly consider the primary and secondary control levels of microgrid with balanced loads. The primary control is locally implemented at each DG, e.g., droop control for inverter-based distributed energy resources (DER). However, the secondary control usually relies on a centralized control structure. Central controllers are designed to issue global commands requiring information gathered from the whole system and thus a complex two-way communication network is also needed. This kind of communication network makes it vulnerable and may effect the system reliability. In [1], the authors replace the existing standard centralized secondary control with an efficient distributed control structure. They consider the microgrid as a multi-agent system where each DG is an agent. A voltage source inverter (VSI) is employed to connect a DG to the microgrid. The VSIs are interconnected through the physical power network configuration.

A sparse communication network, which overlays the physical power network, is integrated in the control system. The controllers use this communication network to only communicate in a distributed way with neighboring nodes. The secondary controller also uses cooperative multi-agent control techniques to make all agents act as a one group to a common synchronization goal and follow cooperative decisions.

In this paper, we consider a distributed cooperative control structure similar to [1]. The microgrid with N DG units is depicted in Figure 2. Each DG unit is represented by a bus. The lumped DERs and loads within one DG unit are respectively modeled as a single DER and load. We set the DG unit directly connected to main grid as DG Unit$_1$.

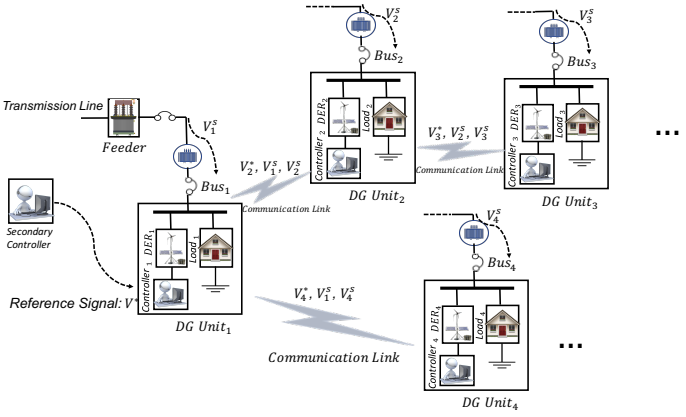

Fig. 2. A microgrid control system with primary and secondary controllers. Sparse communication networks are employed for data exchange between neighboring DG units, e.g., transmitting reference signals and measurements (denoted by the superscript s).

In this work, we assume that the three-phase power network under study is balanced, which means it can be represented as an equivalent single-phase system. Moreover, all N buses are inverter buses and the corresponding voltage magnitude and voltage angle of the i-th bus are respectively represented as V_i and θ_i for $i = 1, \ldots, N$.

Hence we define the active and reactive power injections [12] at bus i as:

$$P_i = V_i^2 G_i - \sum_{j\in N_i} V_i V_j (G_{ij}\cos(\theta_{ij}) + B_{ij}\sin(\theta ij)),$$
$$Q_i = -V_i^2 B_i - \sum_{j\in N_i} V_i V_j (G_{ij}\sin(\theta_{ij}) - B_{ij}\cos(\theta ij)), \quad (1)$$

where $G_{ij} = R_{ij}/(R_{ij}^2 + X_{ij}^2) \geq 0$ and $B_{ij} = -X_{ij}/(R_{ij}^2 + X_{ij}^2) \leq 0$ are the conductance and susceptance of the transmission line between bus i and bus j, respectively. Additionally, $G_i = G_{ii} + \sum_{j\in N_i} G_{ij} \geq 0$ and $B_i = B_{ii} + \sum_{j\in N_i} B_{ij} \leq 0$ are the self-conductance and self-susceptance, respectively [12]. Note $\theta_{ij} = \theta_i - \theta_j$ represents the angle difference between node i and j. We also assume that the phase-angle difference θ_{ij} between any neighboring nodes for $(i,j) \in \mathcal{V}$ to be constant.

B. Communication Network

In the microgrid system, DG units are considered as the nodes of the communication graph and the corresponding communication links represent its edges. Figure 2 describes a line network, however a generic network topology of a microgrid system is usually characterized by a directed graph (digraph) $\mathcal{G} = (\mathcal{V}, \mathcal{E}, A_G)$ with a nonempty finite set of N nodes $\mathcal{V} = \{v_1, v_2, \ldots, v_N\}$, a set of edges $\mathcal{E} \subseteq \mathcal{V}\times\mathcal{V}$, and the associated adjacency matrix A_G. The set $\mathcal{N}_i = \{j \in \mathcal{V} : (i,j) \in \mathcal{E}\}$ denotes the neighbor set of node i. The weight is represented by a_{ij} for the edge from node j to node i, and $a_{ij} = 0$ if there is no data transfer from node j to node i. Considering N nodes on the graph, the adjacency matrix is defined as $A_G = [a_{ij}] \in \mathbb{R}^{N\times N}$.

We define the diagonal in-degree matrix $D = diag\{d_i\} \in \mathbb{R}^{N\times N}$, where d_i is the sum of communication weights from neighbors of node i, $d_i = \sum_{j\in\mathcal{N}_i} a_{ij}$.

The Laplacian matrix of the graph is defined as $L = D - A_G$. One property of the Laplacian matrix L is that the row sums of L are all zero, because the row sums of D and A_G are equal.

A directed path from node i to node j is a sequence of edges depicted as $\{(v_i, v_k), (v_k, v_l), \ldots, (v_m, v_j)\}$. A graph is considered to have a *spanning tree* if there exists a *root node* with a directed path from that node to every other node in this graph. A graph is *strongly connected* if there exists a directed path between every two nodes, i.e., there exists a spanning tree where every node is a root node [1] [7].

III. Distributed Cooperative Control system

In this section, we rely on existing control models to propose a distributed cooperative control scheme for voltage dynamics. We give a detailed description of both the primary and secondary control of the microgrid system under study.

A. Primary Control

Figure 2 illustrates how the reference signals and measurements are available to each controller. Making use of the capabilities of inverter-based DERs, each DG unit is controlled by a droop controller. The droop controller receives reference signal through synchronization process between neighboring nodes and voltage measurements from local meters. Let V^* be the reference voltage sent from the secondary controller and V_j and θ_j, be the voltage magnitude and voltage angle of the j-th bus, respectively.

The voltage dynamics of each DG unit is modeled as a single integrator [12], and we choose the voltage quadratic droop controller developed in [10] to compute the voltage control output signals. The primary droop control law is described as:

$$\tau_i \dot{V}_i(t) = -\kappa_i V_i^c(t)(V_i^c(t) - V_i^{c*}(t)) - Q_i^c(t), \quad (2)$$

where $\tau_i > 0$ is the inverter's time-constant, $\kappa_i > 0$ is the control gain of the droop controller, $V_i^c(t)$ and $Q_i^c(t)$ respectively represent the received voltage measurement and reactive power injection measurement with respect to bus i, and $V_i^{c*}(t)$ is the received voltage reference signal determined by the secondary controller. For nominal operations, 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 $V_i^{c*}(t) = V_i^*(t)$. Nominally, the closed-loop dynamics of the i-th DG unit are given by the differential equations

$$\begin{aligned}\tau_i \dot{V}_i &= -\kappa_i V_i(V_i - V_i^*) - Q_i \\ &= -V_i(\kappa_i V_i - \kappa_i V_i^* + \sum_{j\in\mathcal{V}} l_{ij}(\theta) V_j), \forall i = 1, \ldots, N,\end{aligned} \quad (3)$$

with the time argument omitted.

Assume the studied transmission line impedances have the same ratio $R_{ij}/X_{ij} = -G_{ij}/B_{ij} = \rho \geq 0$ for all lines $(i,j) \in \mathcal{E}$, where R_{ij} and X_{ij} are respectively the resistance and reactance of bus i and bus j. Under this assumption, the parameter $l_{ij}(\theta)$ is written as:

$$l_{ij}(\theta) = \begin{cases} B_{ij}(\rho\sin(\theta_{ij}) + \cos(\theta_{ij})), & i \neq j \\ -B_i, & i = j. \end{cases} \quad (4)$$

Denote $V = [V_1 \ldots V_N]^\top$, $\tau = [\tau_1 \ldots \tau_N]^\top$, $\kappa = [\kappa_1 \ldots \kappa_N]^\top$, and $[V] = diag\{V\}$ as the diagonal matrix with V_i as the i-th diagonal entry, and similarly we have $[\tau] = diag\{\tau\}$, $[\kappa] = diag\{\kappa\}$. We can obtain the voltage dynamics under the quadratic droop control in a vector form:

$$[\tau]\dot{V} = [V]([\kappa]V_i^* - ([\kappa] + L(\theta))V), \quad (5)$$

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

Linearization of the voltage dynamics. For convenience of theoretic analysis, we consider the *Jacobian linearization* of the power system (5) 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. The corresponding linearized system is described by

$$\dot{x}(t) = Ax(t) + Bu(t), \quad (6)$$

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

B. Secondary Control

In this work, the goal of the secondary controller is to generate the voltage reference signal for the primary controller at each DG unit. We employ the distributed cooperative control of multi-agent systems [1] to design the secondary voltage controller for our microgrid system.

DGs are assumed to be able to communicate with each other through the communication network $\mathcal{G}$. We assume that only one *leader* DG node i has access to the reference V^* by a weight factor called the *pinning gain* g_i. The pinning matrix G is defined to carry all the pinning gains of the graph $G = diag\{g_i\} \in \mathbb{R}^{N\times N}$. The computation of the global reference voltage V^* is based on the load deferences between loads in this microgrid and its neighbors, as specified in [7].

The synchronization of reference values of DGs in a communication network $\mathcal{G}$ can be modeled as a *tracking problem* in cooperative control. The consensus all DG nodes need to reach is determined by the leader node.

Note that V_i^* is the voltage reference set point for DG i, and denote $V_{ref} = [V_1^* \dots V_N^*]^\top$. The DGs synchronize their references to hold

$$\dot{V}_{ref} = -(L+G)(V_{ref} - \mathbf{1}\cdot V^*) \tag{7}$$

at the steady state. Note that all eigenvalues of $L+G$ have positive real values, so equation (7) leads to the desired tracking performance at the steady state. For each DG unit in the microgrid, the voltage reference set point is written as

$$\dot{V}_i^* = \sum_{j\in\mathcal{N}_i} a_{ij}(V_j^* - V_i^*) + g_i(V^* - V_i^*) \tag{8}$$

IV. Cyber attacks on voltage control and Impact Analysis

In this section we consider the model of the microgrid system described in section II and we study the possible adversary actions on the reference signal transmitted by the communication network at the primary and secondary control levels.

It is natural to consider a naive attack where an attacker simply falsifies the reference voltage value V_i^* for DG i. However, it is easy to be detected by simple detection algorithms [3] considering the admissible range

$$V_{min}^* \le V_i^* \le V_{max}^*, \tag{9}$$

where V_{min}^* and V_{max}^* are respectively the lower and upper limit for the reference value.

In this work, we identify a novel type of of attack scenarios: "measurement as reference " attack. Under the assumption that the attacker has knowledge about the hierarchical control structure, it targets the communication link between DG units and maliciously replaces the reference signal with the measurement of the previous node. Since the two signals have very close values and follow the same dynamic changes, this attack is "naturally stealthy", and is possible to cause a serious impact without being detected by traditional intrusion detection algorithms.

First we describe the considered attack scenario and we give its mathematical definition. Then we describe how the attack influences the voltage control systems. We characterize the attack impact by the maximum voltage magnitude deviation and inaccurate reference voltage synchronization it causes.

A. measurement as reference attack

Without loss of generality, we assume the attacker replaces the reference signal V_{i+1}^* for node $i+1$ with the voltage measurement V_i^s of node i when defining the attack.

The goal of measurement as reference attack is set to cause voltage fluctuations and irregular regulations to harm the loads without violating the admissible range (9). For convenience of analysis, we assume only one communication link is under attack. The definition of measurement as reference attack is given as follows.

Definition 1 (measurement as reference attack): In a measurement as reference attack on the communication link between DG unit i and $i+1$, the attacker manipulates the exchanged data by replacing the reference signal $V_{i+1}^*(t)$ for DG unit $i+1$ with the voltage measurement $V_i^s(t)$ of DG unit i , so that

$$V_{i+1}^*(t) = V_i^s(t), \tag{10}$$

Furthermore, the droop control signal at DG unit $i+1$ under attack is given by

$$\tau_i \dot{V}_{i+1}(t) = -\kappa_{i+1}V_{i+1}^c(t)(V_{i+1}^c(t) - V_i^s(t)) - Q_{i+1}^c(t) \tag{11}$$

B. Attack Impact on Voltage Deviation

One impact of the measurement as reference attack is voltage magnitude deviations . Consider the resulting changes to the voltage magnitude at DG j in the network, i.e., V_j. The resulting linearized system under attack can be written as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + \tau_{i+1}^{-1}\kappa_{i+1}e_{i+1}u(t) \\ y_j(t) &= e_j^\top x(t) \\ u(t) &= e_i^\top x(t), \end{aligned} \tag{12}$$

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. The attack impact can be quantified as the maximum deviation of $y_j(t)$ caused by a corrupted input $u(t) = e_i^\top x(t)$, which is bounded by $|u(t)| \le \delta$, where $V_{min}^* \le \delta \le V_{max}^*$.

Computation of maximum voltage deviation. We use $\sup_{t\ge 0}|y_j(t)|$ to represent the maximum voltage magnitude of DG j under a measurement as reference attack (10) on the link between DG i and $i+1$. We know that the linearized system (12) under attack is a positive system [8] since A is a *Metzler* matrix with non-negative off-diagonal entries and $\tau_{i+1}^{-1}\kappa_{i+1}e_{i+1}$, $e_j^\top$ are non-negative [12]. Let's define the transfer function of the system (12) as $H(s) = Y(s)/U(s) = \mathcal{L}\{y(t)\}/\mathcal{L}\{u(t)\}$, where $\mathcal{L}$ means Laplace transform. Thus we can compute

$$H(s) = \tau_{i+1}^{-1}\kappa_{i+1}e_j^\top(sI - A)^{-1}e_{i+1}. \tag{13}$$

According to the properties of positive systems [8], we know that the $\mathcal{L}_\infty$-induced norm of system (12) is given as

$$\|H\|_{\mathcal{L}_\infty - ind} = \sup_{\|u\|_{\mathcal{L}_\infty} < \infty} \frac{\|y\|_{\mathcal{L}_\infty}}{\|u\|_{\mathcal{L}_\infty}} = H(0), \tag{14}$$

which characterizes the maximum amplitude of the output signal $y_j(t)$ which can be achieved by an input $u(t)$ with bounded amplitude

$$\|u\|_{\mathcal{L}_\infty} := \sup_{t \geq 0} |u(t)| \leq \delta. \tag{15}$$

So we can compute

$$\begin{aligned} \sup_{t\geq 0} |y_j(t)| &= \|H\|_{\mathcal{L}_\infty - ind} \cdot \|u\|_{\mathcal{L}_\infty} \\ &\leq H(0) \cdot \delta \\ &= -\tau_{i+1}^{-1} \kappa_{i+1} \delta e_j^\top A^{-1} e_{i+1} \\ &= \tau_{i+1}^{-1} \kappa_{i+1} \delta [-A^{-1}]_{j,i+1}, \end{aligned} \tag{16}$$

where $[-A^{-1}]_{j,i+1}$ is the element of row j column $i+1$ from matrix $-A^{-1}$. So $\tau_{i+1}^{-1}\kappa_{i+1}\delta[-A^{-1}]_{j,i+1}$ gives the upper bound of the voltage deviation caused by the attack. Since the δ value in (15) is determined by the system state, the the upper bound in (16) is tight because the maximum is reachable. Therefore, we find that the impact on voltage deviation of each node depends on the structure of matrix A, which reflects the power system topology.

C. Impact on Reference Voltage Synchronization

Besides the voltage deviation, the attack also affects the reference synchronization regarding the secondary control level. Note that the reference of each DG unit will follow the differential equation (7) under nominal operations. So the problem of studying what is the attack impact on reference synchronization is mapped to seeking for the initial conditions of differential equation (7) caused by the attack.

Since the primary control is operating much faster than the secondary control, the voltage state of each DG node would become stable again very quickly and reaches a new equilibrium point when the secondary controller regulates the reference signals. To compute this equilibrium point, we let $\dot{V} = 0$ in (5), i.e., $[\kappa]V_i^* - ([\kappa] + L(\theta))V = 0$. According to the definition of measurement as reference attack $V_{i+1}^*(t) = V_i^s(t)$, we have

$$V_{i+1}^* = V_i = e_i^\top ([\kappa] + L(\theta))^{-1} [\kappa] V_{ref}. \tag{17}$$

So we can get the initial conditions of differential equation (7) under attack as

$$(e_i^\top ([\kappa] + L(\theta))^{-1} [\kappa] - e_{i+1}^\top) V_{ref} = 0. \tag{18}$$

The differential equation (17) with initial condition (18) describes the reference signal synchronization process under attack for each node. When the secondary controller regulates the set point V^*, all references of the nodes relying on communication with node $i+1$ for synchronization, are not able to reach the consensus V^*.

V. Simulation

In this section, we use simulation tools to validate the theoretical analysis of the measurement as reference attack and its impact proposed in the previous section.

A. Simulation Settings

We use Matlab and Simulink tools to build the microgrid control system described in Figure 2 and model the measurement as reference attack provided in Definition 1.

For the power system simulation settings, we consider a microgrid system with 4 DG units in Figure 2, i.e., $N = 4$. We follow the model settings proposed in [12] and [6], where all power lines, DERs and loads are identical. The power system is characterized by (1) with parameters: $\rho = 0.5$, $B_{ij} = -0.2$, 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.

For the primary control, we set the parameters $\theta_{12} = -0.01$rad, $\theta_{23} = -0.045$rad, and $\theta_{34} = -0.01$rad, to make sure that the phase-angle differences between any neighboring nodes are constant. The quadratic droop control modeled by (5) and (2) is characterized by parameters $\tau_i = 10^{-4}$, $\tau_{\theta_i} = 10^{-2}$, and $\kappa_i = 0.2$ for all buses.

The voltage dynamics under primary control are defined by the nonlinear differential equations (5). Through Jacobian linearization, the corresponding linearized dynamics characterized by (6) is given as

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

Clearly the above system is positive and the properties of positive systems [8] are applicable.

Finally, we choose typical parameters for the secondary control. As depicted in Figure 2, the network is a 4-node line topology and DG 1 is the only pinned root node. Considering the communication network topology and a proper synchronization rate, we set the adjacency matrix $A_G = [a_{ij}]$ carrying the communication weights of $a_{21} = 12$, $a_{32} = 11$, $a_{41} = 10$ and all other weights equal to zero, and the pinning matrix $G = diag\{g_i\}$ carrying all pinning gains of $g_1 = 10$, $g_2 = g_3 = g_4 = 0$.

B. Simulation Results

Considering the above simulation settings, the voltage of each DG is in stable state and the global reference set point $V^* = 1$pu. At time $t = 2 \times 10^{-3}$s, the attacker introduces the measurement as reference attack by replacing the reference signal V_2^* at node 2 with the voltage measurement V_1 at node 1.

As shown in Figure 3, the attack cause voltage deviation at each DG unit, which is a short-term impact on the primary control. We can see the voltages reach a stable state again very quickly. Comparing the voltage deviation of the simulated non-linear system under attack with the linearization analysis in Section IV, we can find that the voltage deviation caused by

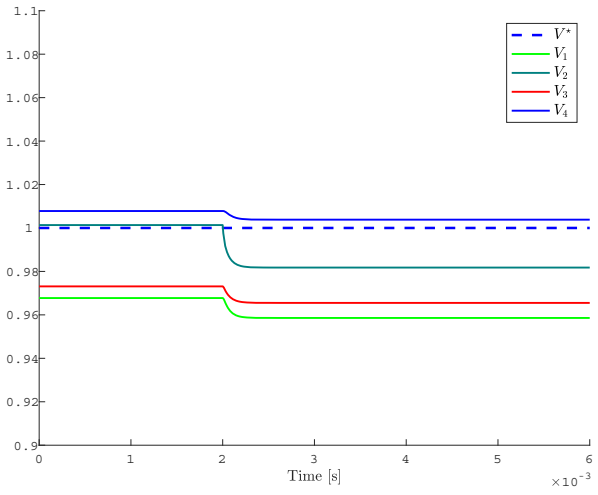

Fig. 3. The impact of the measurement as reference attack on voltage deviation.

the attack is within boundary computed in (16). Comparison result shows that the voltage deviation of the simulated non-linear system under attack is the same to the linearized system, which shows our linearization analysis in Section IV is valid.

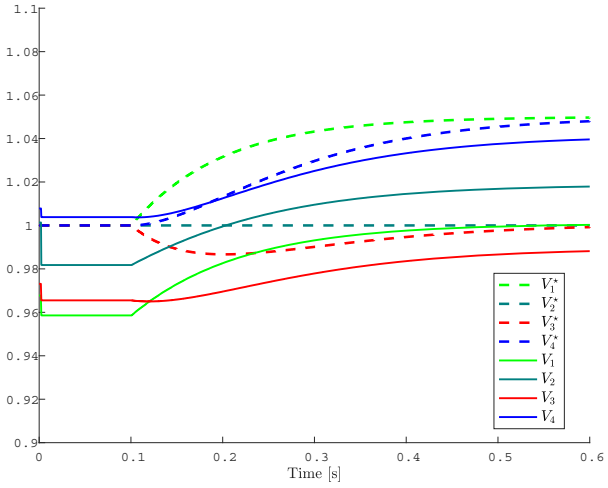

Fig. 4. The impact of the measurement as reference attack on reference synchronization.

How the attack influences the reference synchronization is shown in Figure 4. At time $t = 0.1$s, the secondary controller regulates the reference set point from $V^* = 1$pu to $V^* = 1.05$pu. After about 0.5s, the reference signals finish the synchronization process. We find that DG 2 and DG 3 no longer reach the consensus V^*, which could lead to a heavy impact on voltage regulation in a microgrid system.

VI. Conclusions and Future work

In this paper, we develop and design measurement as reference cyber-attack targeting both primary and secondary control levels of a distributed cooperative control scheme for a microgrid. We analyze the impact of this attack where the goal of the attacker is to introduce a reference voltage deviation by manipulating the synchronization data exchanged between the distributed controllers. We use control-theoretic tools to derive the maximum voltage deviation introduced by this attack where the system will not synchronize to the correct setting point provided by the secondary controller. Moreover, the theoretical analysis results of the impact are validated by simulation. As a future work, the impact of this attack on frequency synchronization and attack detection algorithms will be investigated.

Acknowledgment

This work has been funded by the French Government under grant FUI 23 PACLIDO (Protocoles et Algorithmes Cryptographiques Légers pour l'Internet Des Objets). We would like to thank Prof. Babak Nahid-Mobarakeh for his valuable feedback on the power system model.

References

[1] A. Bidram, F. Lewis, and A. Davoudi. Distributed control systems for small-scale power networks: Using multiagent cooperative control theory. *IEEE Control Systems*, 34(6):56–77, 2014.

[2] A. Giacomoni, S. M. Amin, and B. Wollenberg. 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, 2011.

[3] 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 *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, pages 842–847. IEEE, 2014.

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

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

[6] M. Ma, A. Teixeira, J. van den Berg, and P. Palensky. Voltage control in distributed generation under measurement falsification attacks. *IFAC-PapersOnLine*, 50(1):8379–8384, 2017.

[7] S. Moayedi and A. Davoudi. Distributed tertiary control of dc microgrid clusters. *IEEE Transactions on Power Electronics*, 31(2):1717–1733, 2016.

[8] A. Rantzer. Scalable control of positive systems. *European Journal of Control*, 24:72–80, 2015.

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

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

[11] 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 *American Control Conference (ACC), 2014*, pages 4372–4378. IEEE, 2014.

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