A graph-theoretical characterization of power network vulnerabilities

Fabio Pasqualetti, Antonio Bicchi, and Francesco Bullo

***Abstract*— This work is concerned with the security of a power network against components failure and external attacks. We model a power plant as a linear continuous-time descriptor system. We adopt the framework of structural control theory, and we associate a digraph with the power plant. We provide a necessary and sufficient graph theoretic condition for the existence of vulnerabilities that are inherent to the power network interconnection structure. From a system theoretic perspective, we generalize a known result on the structural rank of the transfer matrix of a state space system to take into account a set of algebraic constraints.**

I. Introduction

Recent studies have shown the inability of the existing power grid to provide a reliable service in the face of network failures and, possibly, malignant actions [1]. For security and reliability to be guaranteed, self-recovering and self-healing mechanisms need to be included in a "smarter" and more autonomous power plant. Additionally, the large dimensionality and spatial distribution of power grids forbid the use of classical security methods, and require, instead, the development of new distributed algorithms [2].

During the last decades, a big effort has been devoted to the modeling of the dynamic behavior of a power network. A classical model for a power plant consists of a set of differential and algebraic equations [3]. Specifically, referring to the network-preserving model of a power network, generators dynamics are described by the differential *swing* equation, while power flows through the buses by the algebraic *load-flow* equation. In this work, we consider the linear continuos-time descriptor model of a power network [4], which arises from the linearization around the load-flow solution of the network-preserving model [5].

In a large-scale system, the absence of an omniscient entity that monitors the status of each component creates vulnerabilities which, if exploited by an adversarial agent, may lead to a complete disruption of the system functionalities. The case of linear discrete-time networks in the presence of misbehaving components is studied, among others, in [6], [7], where it is shown how malignant agents may collude to arbitrarily drive the network while remaining undetected at certain observing stations. As discussed above, because power network dynamics evolve as a linear continuous-time descriptor system, the results presented in [6], [7] cannot be used in a straightforward manner for the study of power networks vulnerabilities. It is worth mentioning that the problem of detecting external attacks in a power network has recently been studied in [8], where, however, algebraic constraints are not included in the power network model.

The study of dynamical systems in descriptor form has received sensible attention from the control community, e.g., see [9], [10]. In these works, authors characterize system theoretic properties of descriptor systems, including controllability, observability, and fault detectability. The conditions they describe usually require algebraic or decomposition techniques to be checked, and they depend upon the specific system matrices. On the other hand, a mathematical model only approximates the real behavior of a physical plant, and, consequently, a property which holds for a specific numerical model, might not be verified for the actual real system. We capture this uncertainty in the network dynamics by allowing the system matrices, which corresponds to physical network parameters, to be uncertain within a certain range, rather than being fixed at a specific value. The theory of structured systems, where only the interconnection pattern of the state variables and not their numerical value is considered, offers a suitable framework for the structural study of power systems. We refer the reader to [11], [12] for a comprehensive discussion of structured state space systems.

The structural study of descriptor systems has not received intensive attention, a few exceptions including [13], [14]. In these works, the underlying assumption is made that the nonzero entries are independent of each other, and that they can take an arbitrary value. For many physical systems, and indeed also for a power network, this assumption is not verified, because of physical relations that the parameters need to satisfy. Because of this constraint, classical structural results do not apply to our case of study.

The main contributions of this work are as follows. First, we propose the use of graph theoretic techniques to study structural properties of power networks modeled via linear continuous-time descriptor systems. We define the concept of network vulnerability, which we identify with the possibility for an attacker (or a failure) to affect the network dynamics without being detected through the monitoring measurements. Second, we geometrically characterize the set of admissible power networks realizations. To be more precise, if d is the number of indeterminate parameters of a structured system, we show that the set of admissible power network realizations describes a polytope in $\mathbb{R}^d$. This characterization allows us to show the existence of network vulnerabilities that are inherent to the network interconnection structure, and hence independent of the specific numerical value of the network parameters. In other words, we show that the presence of network vulnerabilities is a structural property with

This material is based in part upon work supported by ICB ARO grant DAAD19-03-D-0004 and NSF grant CNS-0834446.

Fabio Pasqualetti and Francesco Bullo are with the Center for Control, Dynamical Systems and Computation, University of California at Santa Barbara, {fabiopas,bullo}@engineering.ucsb.edu

Antonio Bicchi is with the Centro I. R. "E. Piaggio", Università di Pisa, Pisa, Italy bicchi@ing.unipi.it

respect to the admissible realizations space. Consequently, in the presence of a structural vulnerability, it holds that every structurally equivalent network has a vulnerability in the usual numerical sense. Conversely, in the absence of structural vulnerabilities, almost every admissible network realization has no vulnerabilities. Third, we provide a necessary and sufficient graph theoretic condition for the existence of structural vulnerabilities, which, additionally, constitutes a necessary condition for the absence of vulnerability in any network realization. Finally, through a simulation study, we show how a malignant attacker can exploit structural vulnerabilities to destabilize the network.

The rest of the paper is organized as follows. Section II recalls some basic facts and definitions. In Section III we describe the mathematical setup and the problem under consideration. Section IV contains our results concerning the vulnerabilities of a power network. Sections V and VI contain, respectively, a numerical study and our conclusion.

II. Preliminaries

For the readers convenience, we recall some facts about dynamical systems, graph theory, and algebraic geometry.

A. Zero dynamics ([15])

Let (E, A, B, C, D) denote the regular[1] descriptor system

$$E\dot{x}(t) = Ax(t) + Bu(t),$$
$$y(t) = Cx(t) + Du(t),$$

and let $y(x_0, u, t)$ denote the output signal generated from the initial state x_0 under the input $u(t)$. The system (E, A, B, C, D) is *left-invertible* if there is no input signal such that $y(0, u, t) = 0$ at all times $t \in \mathbb{R}_{\geq 0}$. Equivalently, the system (E, A, B, C, D) is left-invertible if and only if

$$\operatorname{rank}\left(\begin{bmatrix} sE - A & -B \\ C & D \end{bmatrix}\right) = n + \operatorname{rank}\left(\begin{bmatrix} -B \\ D \end{bmatrix}\right), \qquad (1)$$

for all but finitely many values of $s \in \mathbb{C}$, where n is the dimension of the square matrix A. Additionally, the value $\bar{s} \in \mathbb{C}$ is an *invariant zero* of (E, A, B, C, D) if there exists a pair $(x_0, u(t))$ such that $y(x_0, u, t) = 0$ at all times $t \in \mathbb{R}_{\geq 0}$, or, equivalently, if equation (1) fails to hold for the value $\bar{s}$.

B. Linkings and cycle families ([12])

Consider the graph $G = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ and $\mathcal{E}$ denote the vertex and the edge set, respectively. A path is a sequence of vertices where each vertex is connected to the following one in the sequence. A path is simple if every vertex on the path (except possibly the first and the last vertex) occurs only once. Two paths are disjoint if they consist of disjoint sets of vertices. A set of l mutually disjoint and simple paths between two sets of vertices S_1 and S_2 is called a *linking* of size l from S_1 to S_2. A simple path in which the first and the last vertex coincide is called cycle; a *cycle family* of size l is a set of l mutually disjoint cycles. The length of a cycle family equals the total number of edges in the family.

[1]A descriptor system is regular if the determinant $|sE - A|$ is not identically zero [4].

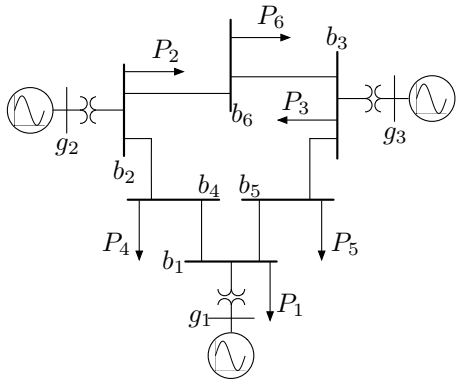

Fig. 1. A power network with 3 generators, 3 terminal buses, and 3 load buses. The numerical value of the network parameters can be found in [5].

C. Structured systems and structural properties ([11], [16])

Let a structure matrix $[M]$ be a matrix in which each entry is either a fixed zero or an indeterminate parameter, and let a structured dynamical system be a tuple $([E], [A], [B], [C], [D])$ of structure matrices of appropriate dimension. A system (E, A, B, C, D) is an admissible realization of $([E], [A], [B], [C], [D])$ if it can be obtained by fixing the indeterminate entries at some particular value. Two systems are structurally equivalent if they are both an admissible realization of the same structured system. Let d be the number of indeterminate entries altogether. By collecting the indeterminate parameters into a vector, an admissible realization is mapped to a point in the Euclidean space $\mathbb{R}^d$. A property which can be asserted on a dynamical system is called *structural* if, informally, it holds for *almost all* admissible realizations. To be more precise, we say that a property is structural if and only if the set of admissible realizations satisfying such property forms a dense subset of the parameters space.[2] For instance, left-invertibility of a system is a structural property with respect to $\mathbb{R}^d$. In Lemma 4.1, we show that left-invertibility is also a structural property when the parameters space coincides with a polytope of $\mathbb{R}^d$.

III. Mathematical model and problem definition

A. Mathematical modeling of a power network

During the last decades, a big effort has been devoted to the modeling of the dynamic behavior of a power network, e.g., see [3]. In this paper, we consider a classical linearized version of the swing model, which we now briefly derive. Consider a connected power network with n generators and $m > n$ buses indexed by $g_1, \ldots, g_n$ and $b_1, \ldots, b_m$, respectively. Let $b_1, \ldots, b_n$ be the generator terminal buses, each one connected to exactly one generator, and let $b_{n+1}, \ldots, b_m$ be the load buses. See Fig. 1 for an example. As usual in transient stability studies, the generator dynamics are given by the transient constant-voltage behind reactance model. With the i-th machine, we associate the the voltage modulus E_i, the rotor angle δ_i, the inertia M_i, the damping coefficient

[2]A subset $S \subseteq P \subseteq \mathbb{R}^d$ is dense in P if, for each $r \in P$ and every $\varepsilon > 0$, there exists $s \in S$ such that the Euclidean distance $\|s - r\| \leq \varepsilon$.

D_i, the transient reactance z_i, and the mechanical power input $P_{\mathrm{g},i}$. With the i-th bus we associate the voltage modulus V_i, the phase angle θ_i, the active and the reactive power demands P_i and Q_i, respectively. With the above notation, the i-th generator dynamics, $i = 1, \dots, n$, become

$$\begin{aligned} \dot{\delta}_i(t) &= \omega_i(t), \\ M_i\dot{\omega}_i(t) &= P_{\mathrm{g},i}(t) - \frac{E_i V_i}{z_i}\sin(\delta_i(t) - \theta_i(t)) - D_i\omega_i(t). \end{aligned} \tag{2}$$

We adopt a ZP load model for every bus, and we denote with G_{ij} and B_{ij} the conductance and susceptance of the transmission line $\{b_i, b_j\}$ [3]. Then, for $k = 1, \dots, n$ the power flow equation at the k-th generator terminal bus is[3]

$$\begin{aligned} P_k =& \frac{E_k V_k}{z_k}\sin(\theta_k - \delta_k) + \sum_{j=1, j\neq k}^{m} V_k V_j B_{kj}\sin(\theta_k - \theta_j) \\ &+ V_k^2 G_{kk} + \sum_{j=1, j\neq k}^{m} V_k V_j G_{kj}\cos(\theta_k - \theta_j), \\ Q_k =& -\frac{E_k V_k}{z_k}\cos(\theta_k - \delta_k) + \sum_{j=1, j\neq k}^{m} V_k V_j G_{kj}\sin(\theta_k - \theta_j) \\ &- V_k^2 B_{kk} - \sum_{j=1, j\neq k}^{m} V_k V_j B_{kj}\cos(\theta_k - \theta_j) - \frac{1}{x_{di}}V_k^2. \end{aligned} \tag{3}$$

Analogously, for $k = n+1, \dots, m$, the power flow equation at the k-th load bus is

$$\begin{aligned} P_k =& \sum_{j=1, j\neq k}^{m} V_k V_j B_{kj}\sin(\theta_k - \theta_j) + V_k^2 G_{kk} \\ &+ \sum_{j=1, j\neq k}^{m} V_k V_j G_{kj}\cos(\theta_k - \theta_j), \\ Q_k =& \sum_{j=1, j\neq k}^{m} V_k V_j G_{kj}\sin(\theta_k - \theta_j) - V_k^2 B_{kk} \\ &- \sum_{j=1, j\neq k}^{m} V_k V_j B_{kj}\cos(\theta_k - \theta_j). \end{aligned} \tag{4}$$

A linear small signal model can be derived from the non-linear model (2) - (4) under the usual assumptions that all angular differences are small, that the network is lossless, and that the voltages are close to their nominal rated value. In other words, the assumption is made that for all generators g_i and all pairs of buses b_j, b_k it holds $|\delta_i - \theta_j| \ll 1$, $|\theta_j - \theta_k| \ll 1$, $G_{jk} = 0$, and $E_i = V_i = 1$. With these assumptions, linearization of equations (2) - (4) about the (synchronized) network steady state condition yields the dynamic linearized swing equation and the algebraic DC power flow equation[4]

$$\underbrace{\begin{bmatrix} I & 0 & 0 \\ 0 & M & 0 \\ 0 & 0 & 0 \end{bmatrix}}_{E} \begin{bmatrix} \dot{\delta}(t) \\ \dot{\omega}(t) \\ \dot{\theta}(t) \end{bmatrix} = \underbrace{-\begin{bmatrix} 0 & -I & 0 \\ L_{\mathrm{gg}} & D & L_{\mathrm{gl}} \\ L_{\mathrm{lg}} & 0 & L_{\mathrm{ll}} \end{bmatrix}}_{A} \begin{bmatrix} \delta(t) \\ \omega(t) \\ \theta(t) \end{bmatrix} + \underbrace{[\mathbf{0}_n^{\mathsf{T}}, P_{\mathrm{g},1}, \dots, P_{\mathrm{g},n}, P_1, \dots, P_m]^{\mathsf{T}}}_{P(t)}, \tag{5}$$

where $M = \mathrm{diag}(M_1, \dots, M_n)$ and $D = \mathrm{diag}(D_1, \dots, D_n)$. By letting $x(t) = [\delta^{\mathsf{T}}(t)\ \omega^{\mathsf{T}}(t)\ \theta^{\mathsf{T}}(t)]^{\mathsf{T}}$, the model (5) can be written as the linear continuous-time descriptor system

$$E\dot{x}(t) = Ax(t) + P(t). \tag{6}$$

As a result of the above simplifying assumptions, the matrix $L = \left[\begin{smallmatrix} L_{\mathrm{gg}} & L_{\mathrm{gl}} \\ L_{\mathrm{lg}} & L_{\mathrm{ll}} \end{smallmatrix}\right] \in \mathbb{R}^{(n+m)\times(n+m)}$ is a Laplacian matrix, L_{gg} is diagonal, L_{ll} is invertible, and $L_{\mathrm{lg}} = L_{\mathrm{gl}}^{\mathsf{T}}$.

B. Problem definition

The focus of this work is to characterize the presence of undetectable failures (or attacks) for the power network (6). More specifically, we model the failure of a network component and the action of an external attacker by adding an unknown input $Ff(t)$ to the system (6). We assume to continuously measure a combination of the state variables, and we let $y(t) = Cx(t)$ denote such measurements vector. We aim at determining the existence of an input $Ff(t)$ undetectable through the measurements $y(t)$.

It should be noticed that the failure $Ff(t)$ may remain undetected from the measurements if and only if there exists a normal operating condition under which the observations $y(t)$ are the same as under the perturbation due to the failure. Because the input term $P(t)$ is assumed to be known, it is always possible to subtract its effect from the system measurements (due to the linearity of (6)). Therefore, since the input $P(t)$ does not affect the solvability of our detection problem, without affecting generality, we let $P(t) = 0$.

In the presence of the failure (or attack) $Ff(t)$, the descriptor system with measurements $y(t)$ modeling the faulty network dynamics reads as

$$\begin{aligned} E\dot{x}(t) &= Ax(t) + Ff(t), \\ y(t) &= Cx(t). \end{aligned} \tag{7}$$

The model (7) is very general and can capture the occurrence of several types of failures or external attacks. For instance, being $e_1, \dots, e_n$ the vectors of the canonical basis,

(i) a sudden change in the i-th load consumption is represented by a step input on the input matrix $F = e_{2n+i}$;
(ii) a line outage occurring on line h (directed from bus s to bus t) is modeled by the input matrix $F = [e_s\ e_t]$, and the input signal $[k_s(t)\ k_t(t)]^{\mathsf{T}}$, where $k_s(t)$, $k_t(t)$ depend upon the network parameters [5]; and
(iii) a change in the i-th generator input mechanical power is described by an appropriate input signal on the input matrix $F = e_{n+i}$.

[3]For brevity, the dependence of the variables on the time t is here omitted.

[4]After linearization, the reactive power equations become independent of the variations of the voltage angles.

Clearly, if the failure is caused by an omniscient attacker, then we expect the input signal to be appositely casted to maximally disrupt the network functionalities.

A careful reader may have noticed that, because of our assumptions, the model (7) only approximates the real behavior of the corresponding power network. We capture this discrepancy by allowing the system matrices, which are related to network parameters, to take an unknown value within a certain range. Consequently, instead of studying the failure detection problem with respect to a specific numerical realization of (7), we consider the solvability of the failure detection problem with respect to the interconnection structure of the power plant. In other words, we look for network vulnerabilities, i.e., undetectable failures, that are inherent to the network interconnection structure, rather than dependent upon the specific value of the network matrices. For our purposes, we adopt the framework of structured systems, and we say that the structured power network $([E],[A],[C])$ has a structural vulnerability if, for some input matrix $[F]$, there exists an undetectable (from measurements) failure in every admissible numerical realization (E,A,C). Hence, in this paper, we address the following problem.

Problem 1 (Existence of vulnerability): For the structured power network model $([E],[A],[C])$, determine the existence of a structural vulnerability.

Let $([E],[A],[C])$ be a structured descriptor system with d free parameters altogether. For the triple (E,A,C) to be an admissible power network realization, the entries of A cannot be chosen independently of one another. Indeed, the matrix L needs to be a Laplacian matrix, i.e., L needs to be symmetric, with zero row sums, and with $L_{ij} \leq 0$ for all $i \neq j$.[5] Because some entries cannot be freely assigned, the admissible parameters space is a subset of $\mathbb{R}^d$, and the classical structural system-theoretic results are here invalid [11]. We conclude this section with the following lemma.

Lemma 3.1 (Admissible parameters space): Let d be the number of indeterminate parameters of the structured system $([E],[A],[C])$. The set of all the admissible power network realizations of $([E],[A],[C])$ describes a polytope of $\mathbb{R}^d$.

Proof: Because a realization of a structured system with d parameters corresponds to a vector in $\mathbb{R}^d$, the power network parameters space is $S = \{x \in \mathbb{R}^d | M_1 x = 0, M_2 x \succeq 0\}$, where $\succeq$ denotes componentwise inequality, and M_1, M_2 are defined by the constraints $L = L^{\mathsf{T}}$, $L\mathbf{1} = 0$, and $L_{ij} \leq 0$, for all $i \neq j$. Clearly, S is a polytope of $\mathbb{R}^d$. ∎

IV. Structural vulnerability in power networks

We derive in this section a graph theoretic condition for the existence of structural vulnerabilities in power networks. We consider two cases. First, we assume that the network state is known at the failure initial time,[6] and then we focus on the more general case of unknown failure initial state. We start by defining a mapping between dynamical systems in descriptor form and digraphs. Let ([E],[A],[F],[C]) be a faulty structured power network. We associate a directed graph $G = (\mathcal{V}, \mathcal{E})$ with the quadruple $([E],[A],[F],[C])$, where $\mathcal{V} = \mathcal{F} \cup \mathcal{X} \cup \mathcal{Y}$, with $\mathcal{F} = \{f_1, \ldots, f_{\bar{m}}\}$ the set of failure vertices, $\mathcal{X} = \{x_1, \ldots, x_{\bar{n}}\}$ the set of state vertices, and $\mathcal{Y} = \{y_1, \ldots, y_{\bar{p}}\}$ the set of output vertices. The indices $\bar{n}$, $\bar{m}$, and $\bar{p}$ denote respectively the dimension of the state space, the input space, and the output space. If (i,j) denotes the edge from the vertex i to the vertex j, then the edge set $\mathcal{E}$ is $\mathcal{E}_{[E]} \cup \mathcal{E}_{[A]} \cup \mathcal{E}_{[F]} \cup \mathcal{E}_{[C]}$, with $\mathcal{E}_{[E]} = \{(x_j, x_i) : [E]_{ij} \neq 0\}$, $\mathcal{E}_{[A]} = \{(x_j, x_i) : [A]_{ij} \neq 0\}$, $\mathcal{E}_{[F]} = \{(f_j, x_i) : [F]_{ij} \neq 0\}$, and $\mathcal{E}_{[C]} = \{(x_j, y_i) : [C]_{ij} \neq 0\}$. In the latter, for instance, the expression $[E]_{ij} \neq 0$ means that the (i,j)-th entry of $[E]$ is a free parameter. Notice that the set $\mathcal{E}_{[E]}$ consists of a set of self-loops for the generators state variables.

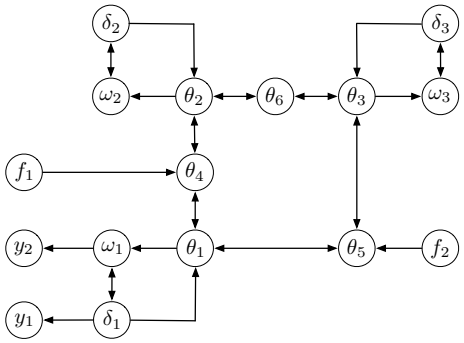

Fig. 2. The digraph associated with the network in Fig. 1. The self-loops of the vertices $\{\delta_1, \delta_2, \delta_3\}$, $\{\omega_1, \omega_2, \omega_3\}$, and $\{\theta_1, \ldots, \theta_6\}$ are not drawn. The inputs f_1 and f_2 affect respectively the bus b_4 and the bus b_5. The measured variables are the rotor angle and frequency of the first generator.

Example 1: Consider the network in Fig. 1, where we take $[E] = \text{blk-diag}(1,1,1,M_1,M_2,M_3,0,0,0,0,0,0)$, $[F] = [e_8\ e_9]$, $[C] = [e_1\ e_4]^{\mathsf{T}}$, and $[A]$ equal to

$$\begin{bmatrix}
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
a_{4,1} & 0 & 0 & a_{4,4} & 0 & 0 & a_{4,7} & 0 & 0 & 0 & 0 & 0 \\
0 & a_{5,2} & 0 & 0 & a_{5,5} & 0 & 0 & a_{5,8} & 0 & 0 & 0 & 0 \\
0 & 0 & a_{6,3} & 0 & 0 & a_{6,6} & 0 & 0 & a_{6,9} & 0 & 0 & 0 \\
a_{7,1} & 0 & 0 & 0 & 0 & 0 & a_{7,7} & 0 & 0 & a_{7,10} & a_{7,11} & 0 \\
0 & a_{8,2} & 0 & 0 & 0 & 0 & 0 & a_{8,8} & 0 & a_{8,10} & 0 & a_{8,12} \\
0 & 0 & a_{9,3} & 0 & 0 & 0 & 0 & 0 & a_{9,9} & 0 & a_{9,11} & a_{9,12} \\
0 & 0 & 0 & 0 & 0 & 0 & a_{10,7} & a_{10,8} & 0 & a_{10,10} & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & a_{11,7} & 0 & a_{11,9} & 0 & a_{11,11} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & a_{12,8} & a_{12,9} & 0 & 0 & a_{12,12}
\end{bmatrix}$$

The digraph associated with $([E],[A],[F],[C])$ is in Fig. 2.

A. Network vulnerability with known initial state

Consider the faulty power network described by the matrices (E,A,F,C), and let $y(x_0,f,t)$ be the output signal generated from the initial state x_0 under the failure f. Notice that, if the state x_0 is known at the failure initial time, then there exists an undetectable failure f, i.e., such that $y(x_0,f,t) = y(x_0,0,t)$ at all times $t \in \mathbb{R}_{\geq 0}$, if and only if the system (E,A,F,C) is not left-invertible. Recall that a subset $S \subseteq \mathbb{R}^d$ is an *algebraic variety* if it coincides with the locus of common zeros of a finite number of polynomials. For a structured system with d parameters, it is know that the set of not left-invertible realizations lies on an algebraic variety of $\mathbb{R}^d$ [11]. Consider the following observation.

[5]The fact that some system entries are fixed to one does not affect genericity.

[6]The failure initial state can be estimated through a state observer [5].

Lemma 4.1 (Left-invertible realizations space): Let $S \subseteq \mathbb{R}^d$ be a polytope, and let $T \subseteq \mathbb{R}^d$ be an algebraic variety. Then, either $S \subseteq T$, or $S \setminus (S \cap T)$ is dense in S.

Proof: Let $T \subseteq \mathbb{R}^d$ be the algebraic variety described by the locus of common zeros of the polynomials $\{\phi_1(x), \ldots, \phi_t(x)\}$, with $t \in \mathbb{N}$, $t < \infty$. Let $P \subseteq \mathbb{R}^d$ be the smallest vector subspace containing the polytope S. Then $P \subseteq T$ if and only if every polynomial ϕ_i vanishes identically on P. Suppose that the polynomial ϕ_i does not vanish identically on P. Then, the set $T \cap P$ is contained in the algebraic variety $\{x \in P : \phi_i(x) = 0\}$, and, therefore [16], the complement $P \setminus (P \cap T)$ is dense in P. By definition of dense set, the set $S \setminus (S \cap T)$ is also dense in S. ∎

In Lemma 4.1, interpret the polytope S as the set of parameters defining a power network (cf. Lemma 3.1). Then, we have shown that the left-invertibility of a power network is a structural property with respect to the power network parameters space. Consequently, given a structured system, either every admissible power network realization has a vulnerability, or there is no vulnerability in almost all admissible realizations. Moreover, in order to show that almost all realizations have no vulnerabilities, it is sufficient to prove that this is the case for some specific admissible realizations. Before presenting our main result, we recall the following theorem. Let $\bar{E}$ and $\bar{A}$ be N-dimensional square matrices, and let $G(s\bar{E} - \bar{A})$ be the graph associated with the matrix $s\bar{E} - A$ that consists of N vertices, and an edge from vertex j to i if $A_{ij} \neq 0$ or $E_{ij} \neq 0$. The matrix $s[\bar{E}] - [\bar{A}]$ is said to be structurally degenerate if $\det(s\bar{E} - \bar{A}) = 0$ for all $s \in \mathbb{C}$, and all admissible realizations of $[E]$ and $[A]$.

Theorem 4.2 (Structural rank of a square matrix [13]): The structure N-dimensional matrix $s[\bar{E}] - [\bar{A}]$ is structurally degenerate if and only if there exists no cycle family of length N in $G(s[\bar{E}] - [\bar{A}])$.

We are now able to state our main result.

Theorem 4.3 (Structurally undetectable failure): Let the parameters space of the structured system $([E], [A], [F], [C])$ define a polytope in $\mathbb{R}^d$. Assume that $s[E] - [A]$ is structurally non-degenerate. The system $([E], [A], [F], [C])$ is structurally left-invertible if and only if there exists a linking of size $|\mathcal{F}|$ from $\mathcal{F}$ to $\mathcal{Y}$.

Proof: Because of Lemma 3.1 and Lemma 4.1, we need to show that, if there are $|\mathcal{F}|$ disjoint paths from $\mathcal{F}$ to $\mathcal{Y}$, then there exists admissible left-invertible realizations. Conversely, if there are at most $|\mathcal{F}| - 1$ disjoint paths from $\mathcal{F}$ to $\mathcal{Y}$, then every admissible realization is not left-invertible.

(If) Let (E, A, F, C), with $|sE - A| \neq 0$, be an admissible realization, and suppose there exists a linking of size $|\mathcal{F}|$ from $\mathcal{F}$ to $\mathcal{Y}$. Without affecting generality, assume $|\mathcal{Y}| = |\mathcal{F}|$. For the left-invertibility property, we need

$$\left| \begin{bmatrix} sE - A & -F \\ C & 0 \end{bmatrix} \right| = |sE - A| \left| C(sE - A)^{-1} F \right| \neq 0,$$

and hence $\left| C(sE - A)^{-1} F \right| \neq 0$. Notice that $C(sE - A)^{-1} F$ corresponds to the transfer matrix from the faults to the output. Since there are $|\mathcal{F}|$ independent paths from $\mathcal{F}$ to $\mathcal{Y}$, the matrix $C(sE - A)^{-1} F$ can be made nonsingular and diagonal by removing some connection lines from the network. Then there exist admissible left-invertible realizations, and hence $([E], [A], [F], [C])$ is structurally left-invertible.

(Only if) Take any subset of $|\mathcal{F}|$ output vertices, and let $|\mathcal{F}| - 1$ be the maximum size of a linking from $\mathcal{F}$ to $\mathcal{Y}$. Let $[\bar{E}]$ and $[\bar{A}]$ be such that $s[\bar{E}] - [\bar{A}] = \begin{bmatrix} s[E] - [A] & [F] \\ [C] & 0 \end{bmatrix}$. Consider the previously defined graph $G(s[\bar{E}] - [\bar{A}])$, and notice that there are no self-loops corresponding to the vertices $n + 1, \ldots, n + m$, being n and m the number of column of $[A]$ and $[F]$ respectively. Because a path from $\mathcal{F}$ to $\mathcal{Y}$ in the digraph associated with the structured system corresponds to a cycle in $G(s[\bar{E}] - [\bar{A}])$, we have that there exists at least a vertex $v \in \{n+1, \ldots, n+m\}$ which is not part of a cycle family. Equivalently, there is no cycle family of length $n+m$ in $G(s[\bar{E}] - [\bar{A}])$. By Theorem 4.2, $s[\bar{E}] - [\bar{A}]$ is structurally degenerate, and the theorem follows. ∎

Theorem 4.3 can be interpreted in the context of power networks. Indeed, since $|sE - A| \neq 0$ for any power network [5], and since the power network parameters space coincides with a polytope in $\mathbb{R}^d$ (cf. Lemma 3.1), Theorem 4.3 states that there exists a structural network vulnerability if and only if there is no linking of size $|\mathcal{F}|$ from $\mathcal{F}$ to $\mathcal{Y}$, provided that the network state at the failure time is known. To conclude this section, we remark that Theorem 4.3 is an extension of [17] to regular descriptor systems.

B. Network vulnerability with unknown initial state

If the failure initial state is unknown, then a vulnerability is identified by the existence of a pair of initial conditions x and $\bar{x}$, and a failure f such that $y(x, 0, t) = y(\bar{x}, f, t)$, or, equivalently, by the existence of an invariant zero for the dynamical network. We will now show that, provided that a power network is left-invertible, its invariant zeros can be computed by simply looking at a reduced linear system with no algebraic constraints. Let the state vector x be partitioned as $[x_1^\mathsf{T}\ x_2^\mathsf{T}]^\mathsf{T}$, where x_1 corresponds to the first $2n$ variables. Let the network matrices E, A, B, F, and C be partitioned accordingly. The state space system

$$\begin{aligned} \dot{x}_1(t) &= E_{11}^{-1} A_{11} x_1(t) + E_{11}^{-1} F_1 f(t) + E_{11}^{-1} A_{12} x_2(t), \\ \tilde{y}(t) &= \begin{bmatrix} A_{21} \\ C_1 \end{bmatrix} x_1(t) + \begin{bmatrix} A_{22} & F_2 \\ C_2 & 0 \end{bmatrix} \begin{bmatrix} x_2(t) \\ f(t) \end{bmatrix}, \end{aligned}$$

is referred to as the reduced system of (E, A, F, C).

Theorem 4.4 (Equivalence of invariant zeros): For the structured system $([E], [A], [F], [C])$, assume there exists a linking of size $|\mathcal{F}|$ from $\mathcal{F}$ to $\mathcal{Y}$. Then, in almost all admissible realizations, the invariant zeros coincide with those of the associated reduced system.

Proof: From Theorem 4.3, the above descriptor system is structurally left-invertible. Let (E, A, F, C) be a left-invertible realization. With a procedure similar to [18] (cf. Proposition 8.4), the invariant zeros of (E, A, F, C) coincide with those of its reduced system. The statement follows. ∎

It should be noticed that, because of Theorem 4.4, under the assumption of left-invertibility, classical linear systems techniques can be used to investigate the presence of structural vulnerabilities in a power network, e.g., see [12].

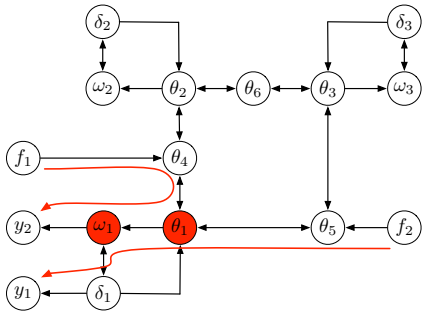

Fig. 3. In the above network, there is no linking of size 2 from the input to the output vertices. Indeed, the vertices θ_1 and ω_1 belong to every path from $\{u_1, u_2\}$ to $\{y_1, y_2\}$. Two input to output paths are depicted in red.

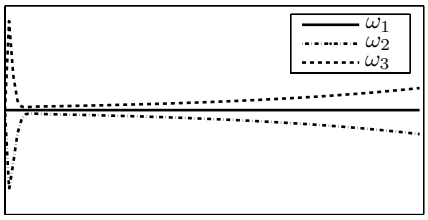

Fig. 4. The velocities ω_2 and ω_3 are driven unstable by the signals $f_1(t)$ and $f_2(t)$, which are undetectable from the measurements of ω_1 and δ_1.

V. A NUMERICAL STUDY

Consider the power network of Fig. 1, and let the variables θ_4 and θ_5 be affected, respectively, by the unknown and unmeasurable signals $f_1(t)$ and $f_2(t)$. Suppose that a monitoring unit is allowed to measure directly the state variables of the first generator, i.e., $y_1(t) = \delta_1(t)$ and $y_2(t) = \omega_1(t)$. Notice that the maximum size of a linking from the failure to the output vertices is 1 (cf. Fig. 3), so that, by Theorem 4.3, there exists a structural vulnerability. In other words, for every choice of the network matrices, there exist nonzero $f_1(t)$ and $f_2(t)$ that are not detected through the measurements.[7] For example, let $E = \text{blk-diag}(1, 1, 1, .125, .034, .016)$, $D = \text{blk-diag}(.125, .068, .048)$, $F = [e_8\ e_9]$, $C = [e_1\ e_4]^\mathsf{T}$, and

$$L = \begin{bmatrix} .058 & 0 & 0 & -.058 & 0 & 0 & 0 & 0 & 0 \\ 0 & .063 & 0 & 0 & -.063 & 0 & 0 & 0 & 0 \\ 0 & 0 & .059 & 0 & 0 & -.059 & 0 & 0 & 0 \\ -.058 & 0 & 0 & .235 & 0 & 0 & -.085 & -.092 & 0 \\ 0 & -.063 & 0 & 0 & .296 & 0 & -.161 & 0 & -.072 \\ 0 & 0 & -.059 & 0 & 0 & .330 & 0 & -.170 & -.101 \\ 0 & 0 & 0 & -.085 & -.161 & 0 & .246 & 0 & 0 \\ 0 & 0 & 0 & -.092 & 0 & -.170 & 0 & .262 & 0 \\ 0 & 0 & 0 & 0 & -.072 & -.101 & 0 & 0 & .173 \end{bmatrix}.$$

Let $F_1(s)$ and $F_2(s)$ be the Laplace transform of the failure signals $f_1(t)$ and $f_2(t)$, and let

$$\begin{bmatrix} F_1(s) \\ F_2(s) \end{bmatrix} = \begin{bmatrix} \frac{-1.024s^4 - 5.121s^3 - 10.34s^2 - 9.584s - 3.531}{s^4 + 5s^3 + 9.865s^2 + 9.173s + 3.531} \\ 1 \end{bmatrix} U(s),$$

for some nonzero signal $U(s)$. It can be verified that the failure cannot be detected through the measurements $y_1(t)$ and $y_2(t)$. An example is in Fig. 4, where the second and the third generator are driven unstable by the failure, but yet the first generator does not deviate from the nominal working condition. Suppose now that $C = [e_1\ \ e_{12}]^\mathsf{T}$. Then, there exists a linking of size 2 from $\mathcal{F}$ to $\mathcal{Y}$, and the system (E, A, F, C) is left-invertible. Following Theorem 4.4, the invariant zeros of the power network can be computed by looking at its reduced system, and they are $-1.6864 \pm 1.8070i$ and $-0.8136 \pm 0.2258i$. Consequently, if the network state is unknown at the failure time, there exists vulnerabilities that an attacker may exploit to affect the network while remaining undetected.

[7] The loads f_1, f_2 are entirely sustained by the second and third generator.

VI. CONCLUSION

We characterize network vulnerabilities that may be exploited by a malignant attacker to affect the network while remaining undetected. By adopting the framework of structured system theory, we identify vulnerabilities that are inherent to the network interconnection structure, and that do not depend upon the specific network operating point. Our results can be used for the investigation of other structural system-theoretic properties of power networks, such as controllability and observability, and they ultimately lead to security-aware power grids design criteria.

REFERENCES

[1] M. Amin, "Guaranteeing the security of an increasingly stressed grid," *IEEE Smart Grid Newsletter*, Feb. 2011.

[2] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99 –107, 2010.

[3] P. Kundur, *Power System Stability and Control*. McGraw-Hill, 1994.

[4] P. Kunkel and V. Mehrmann, *Differential-Algebraic Equations: Analysis and Numerical Solution*. European Mathematical Society, 2006.

[5] E. Scholtz, "Observer-based monitors and distributed wave controllers for electromechanical disturbances in power systems," Ph.D. dissertation, Massachusetts Institute of Technology, 2004.

[6] S. Sundaram and C. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Transactions on Automatic Control*, vol. PP, no. 99, pp. 1 –1, 2010, to appear.

[7] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, Feb. 2010, to appear.

[8] A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks," in *American Control Conference*, Baltimore, MD, USA, Jun. 2010, pp. 3690–3696.

[9] F. L. Lewis, "A tutorial on the geometric analysis of linear time-invariant implicit systems," *Automatica*, vol. 28, no. 1, 1992.

[10] B. Marx, D. Koenig, and D. Georges, "Robust fault-tolerant control for descriptor systems," *IEEE Transactions on Automatic Control*, vol. 49, no. 10, pp. 1869–1876, 2004.

[11] K. J. Reinschke, *Multivariable Control: A Graph-Theoretic Approach*. Springer, 1988.

[12] J. M. Dion, C. Commault, and J. van der Woude, "Generic properties and control of linear structured systems: a survey," *Automatica*, vol. 39, no. 7, pp. 1125–1144, 2003.

[13] K. J. Reinschke, "Graph-theoretic approach to symbolic analysis of linear descriptor systems," *Linear Algebra and its Applications*, vol. 197, pp. 217–244, 1994.

[14] T. Boukhobza, F. Hamelin, and D. Sauter, "Observability of structured linear systems in descriptor form: A graph-theoretic approach," *Automatica*, vol. 42, no. 4, pp. 629–635, 2006.

[15] H. L. Trentelman, A. Stoorvogel, and M. Hautus, *Control Theory for Linear Systems*. Springer, 2001.

[16] W. M. Wonham, *Linear Multivariable Control: A Geometric Approach*, 3rd ed. Springer, 1985.

[17] J. W. van der Woude, "A graph-theoretic characterization for the rank of the transfer matrix of a structured system," *Mathematics of Control, Signals and Systems*, vol. 4, no. 1, pp. 33–40, 1991.

[18] J. Tokarzewski, *Finite Zeros in Discrete Time Control Systems*, ser. Lecture notes in control and information sciences. Springer, 2006.