A Tractable Nonlinear Fault Detection and Isolation Technique with Application to the Cyber-Physical Security of Power Systems

P. Mohajerin Esfahani, M. Vrakopoulou, G. Andersson, and J. Lygeros

Abstract— **This article consists of two parts: a theoretical part concerned with fault detection schemes, and an application part dealing with cyber security of power systems. In the first part, we develop a tractable approach to design a robust residual generator to detect and isolate faults in high dimensional nonlinear systems. Previous approaches on fault detection and isolation problems are either confined to linear systems or they are only applicable to low dimensional dynamics with more specific structures. In contrast, we propose a novel methodology to robustify a linear residual generator for a nonlinear system in the presence of certain disturbance signatures. To this end, we formulate the problem into the framework of quadratic programming which enables us to solve relatively high dimensional systems. In the second part, the application is motivated by the emerging problem of cyber security in power networks. We provide description of a multi-machine power system that represents a two-area power system, and we model a cyber-physical attack emanating from the vulnerabilities introduced by the interaction between IT infrastructure and power system. The algorithm developed in the first part is finally used to diagnose such an intrusion before the functionality of the power system is disrupted.**

I. Introduction

The task of fault detection and isolation (FDI) in dynamical systems is the problem of generating a diagnostic signal sensitive to the occurrence of specific faults. This problem essentially has the connotation of designing a filter with all available information as inputs which leads to a non-interactive map from faults to residual. Therefore the concept of residual plays a central role for the FDI problem. Earlier works on residual generators for linear systems are commonly concerned with more specific classes of models such as transfer function [15], state-space model [9], and descriptive model [17]. Roughly speaking, for the aforementioned models the residual generators are classified into two categories: observer-based and parity-space-like approaches.

In the observer-based approach, Beard [7] and Jones [19] are the first pioneers where the filter is a Luenberger observer such that failures of different system components affect the residuals in linearly independent directions. Some inherent limitation of Beard-Jones approach was improved in Massoumnia et al. [25]. Later, this approach was extended to more general classes of systems by Seliger and Frank [29] surveyed in [13], and was comprehensively investigated by Speyer and coauthors in the presence of measurement noise, see [10] and [6].

Parity-space-like approaches have been studied in the framework of descriptor models in several papers e.g. [23] and [26]. In more recent work, Nyberg and Frisk extended the class of systems as well as the notion of detectability [26]. In this article the class of functions is extended to linear differential-algebraic equations (DAEs) that covers all the previous classes, and fault detectability is rather defined as a system property. DAE models appear in many applications such as electrical systems, robotic manipulators, and mechanical systems. For instance, a motion of robot constrained to a certain geometrical area can be modelled in this class.

In the context of nonlinear systems, a natural approach is to linearize the model at an operating point, and then invoke robust techniques, e.g. [18], to treat nonlinear terms as disturbances and decouple their effects from the residual using an unknown input observer [30], [16]. This strategy only works well if either the system closely operates around the operating point, or the precise decoupling is possible. The former in the presence of unknown inputs can be even more problematic as the system may have a wide dynamic operating range, and the linearization causes a large mismatch between linear model and nonlinear behavior. The latter for general nonlinear dynamic is a formidable one; for a restricted class of nonlinear systems, in particular bilinear systems, see [8, Section 9.2] and references therein. A practical limitation for the aforementioned reference is to transfer the system into the required form that involves solving a high order partial differential equation.

Along the perfect decoupling scheme, De Presis and Isidori [27] have proposed a differential geometric approach to extend the approach of [24], and design the FDI filter for the observation of certain states in the presence of unknown disturbances. The problem of fault detection and isolation has been characterized in terms of the properties of certain distribution, which can be considered as the nonlinear analog of the unobservibility subspaces first introduced in [24, Section IV]. However, as one is required to verify the conditioned invariant property of certain distributions, the approach is rather intractable for relatively large and sophisticated dynamics.

Motivated by this fact, in this article we aim to find a compromise between theoretical soundness and practical

Research supported by the European Commission under the project VIKING (FP7-ICT-SEC-2007-1) and the Network of Excellence HYCON2 (FP7-ICT-257462).

Peyman Mohajerin Esfahani and John Lygeros are with the Automatic Control Laboratory, Department of Electrical Engineering, Swiss Federal Institute of Technology (ETH), Physikstrasse 3, ETL I22, 8092, Zürich, Switzerland. Emails: {mohajerin, lygeros}@control.ee.ethz.ch

Maria Vrakopoulou and Göran Andersson are with the Power Systems Laboratory, Department of Electrical Engineering, Swiss Federal Institute of Technology (ETH), Physikstrasse 3, ETL G26, 8092, Zürich, Switzerland. Emails: {vrakopoulou, andersson}@eeh.ee.ethz.ch

feasibility. For this purpose, we restrict the class of FDI filters to linear residual generators which allows us to explicitly track the contributions of linear and nonlinear dynamic terms as well as fault signals into the residual. Our main goal is then to control the nonlinear term contributions in the presence of certain disturbance patterns. In another word, in contrast to existing literature toward FDI methods, we impose constraints on disturbance signals rather than nonlinearity structure of the system dynamic.

In more details, we first review some results developed for linear systems of [26] in §III-A. We then propose a linear programming (LP) formulation, Lemma 3.2, as an alternative characterization of residual generators. This is in fact an LP counterpart of matrix polynomial formulation in the literature. In §III-B, we generalize the DAE model to contain nonlinear terms as well, see (6). In order to extend the scheme to the nonlinear model, we propose two approaches where each approach may be viewed from a certain class of applications. The first approach in §III is a straightforward extension of the LP formulation developed in the preceding subsection, thank to the fact that the FDI filter can be designed up to a scaler. The idea may be justified in applications that the system works during normal operation in a neighbourhood of an equilibrium. This suggests to neglect the contribution of nonlinear terms, and mainly focus on the mapping from fault signal into the residual. The second approach in §III is the main contribution of the article. Given some particular signatures of possible disturbances, we approximate the contributions of the nonlinear terms into the residual. The approximation scheme is based on the projection of these contributions into a finite-dimensional function space which is closed under differentiation operator. In the following we formulate the $\mathcal{L}_2$ norm of errors in terms of a family of quadratic programming (QP) problems where the number of QP problems is the degree of the FDI filter.

In the second part of the article, §IV, we first describe the mathematical model of the IEEE 118-bus power network equipped with primary and secondary frequency control. The latter is also referred as Automatic Generation Control (AGC) and is one of the few control loops that are closed over the SCADA system without human operator intervention. This interaction with the IT infrastructure may give rise to cyber security issues which are investigated in our earlier work [11], [12]. It was shown that if an attacker gains access to the AGC signal, unacceptable frequency deviations and power oscillations may occur. This can trigger out-of-step, under frequency and generator frequency protection relays, and hence lead to load shedding and generation tripping. If the intrusion is detected on time, one may prevent further damage by disconnecting the AGC. Therefore, it is crucial to utilize available measurements to diagnose the AGC intrusion sufficiently fast, even in the presence of unknown load deviations. By invoking the proposed FDI scheme, a protection layer is constructed that permits us to address the aforementioned security concern.

The article is organized as follows. In §II a general class of linear model is described, and basic definitions of residual generators and detectability notion are introduced. §III provides two algorithms to tackle nonlinear FDI problems. We then explain a multi-machine power system equipped with AGC in §IV, and in §V apply our technique developed in the preceding sections to diagnose the AGC intrusion. We conclude with some remarks and directions for future work in §VI.

II. Model Description and Basic Definitions

In this section we introduce the class of linear models proposed in [26], and follow the basic definitions in this article. The model is considered as

$$H(p)x + L(p)z + F(p)f = 0, \tag{1}$$

where p is the distributional derivative operator [2, Section I], and H, L, F are polynomial matrices in the operator p. We assume that x, y, z are piece-wise continuous functions from $\mathbb{R}_+$ into $\mathbb{R}^{n_x}, \mathbb{R}^{n_z}, \mathbb{R}^{n_f}$ respectively. We denote these sets by $\mathcal{W}^{n_x}, \mathcal{W}^{n_z}, \mathcal{W}^{n_f}$. In the model (1), x represents all unknowns signals, e.g. internal system states and unknown exogenous disturbances. z contains all the known signals, for instance control signals and state measurements, and f stands for the signals to be detected such as faults or intrusion signals.

One may extend the space of functions x, z, f to Sobolev spaces, but an elaborate discussion regarding this issue is outside the scope of our study. On the other hand, if these spaces are restricted to the smooth functions, then the operator p can be understood as the classical differentiation operator. Throughout this article we will focus on continuous-time models, but one can obtain similar results for discrete-time models by changing the operator p to the time-shift operator q. In the rest of the article, we use p when the matrices involved are viewed as an operator, e.g. $H(p)$, and if they are dealt as a polynomial matrices, we shall use the complex variable s instead of p, e.g. $H(s)$.

The following example indicates that an ordinary state-space description is indeed a particular case of the linear model (1). Consider the model

$$\begin{cases} E\dot{X}(t) = AX(t) + B_u u(t) + B_d d(t) + B_f f(t) \\ Y(t) = CX(t) + D_u u(t) + D_d d(t) + D_f f(t) \end{cases} \tag{2}$$

where $u(\cdot)$ is the input signal, $d(\cdot)$ unknown disturbance, $Y(\cdot)$ state measurements, and $f(\cdot)$ possible faults/attack signal to be detected. Therefore, defining

$$x := \begin{bmatrix} X \\ d \end{bmatrix}, \quad z := \begin{bmatrix} Y \\ u \end{bmatrix}$$

and matrices

$$H(p) := \begin{bmatrix} -pE + A & B_d \\ C & D_d \end{bmatrix}, \quad L(p) := \begin{bmatrix} 0 & B_u \\ -I & D_u \end{bmatrix},$$
$$F(p) := \begin{bmatrix} B_f \\ D_f \end{bmatrix},$$

directly fits the model (2) to (1).

Note that the model (1) affords an appropriate framework to deal with the algebraic constraints. Moreover, we do not assume any condition on initial values of the signals x, z, f. The only assumption one may impose on the model matrices (1) is that there is no linear dependency in the model when $f \equiv 0$. This condition is satisfied when $[H(s)\ L(s)]$ has full row rank.

Let us proceed with some basic definitions and clarify what we mean by *sensitivity* and *residual generator*. To this end, let us formally characterize all possible observations of the model (1) in the absence of the fault signal f:

$$\mathcal{M} := \big\{ z \in \mathcal{W}^{n_z} \big|\ \exists x \in \mathcal{W}^{n_x} : \quad H(p)x + L(p)z = 0 \big\}.$$

This set of observation is called *behavior* of the system used in the behavioral approach to systems theory, see [28, Section 2.4] for more details.

Definition 2.1 (Residual Generator): A proper linear time invariant filter $r := R(p)z$ is a residual generator for (1) if for all $z \in \mathcal{M}$, it holds that $\lim_{t\to\infty} r(t) = 0$.

The following Definition provides a notion of sensitivity for the above residual generators with respect to a specific fault:

Definition 2.2 (Fault Sensitivity): The residual generator introduced in Definition 2.1 is sensitive to fault f_i if the transfer function from f_i to r is nonzero, where f_i is the i^{th} element of the signal f.

III. Design of Residual Generator

The main objective of this section is to establish a tractable approach, possibly for nonlinear systems, to design a sensitive linear residual generator in the sense of Definitions 2.1 and 2.2. For this purpose we first characterize the residual generator as a polynomial matrix equation and then make a link from the polynomial matrix formulation to an LP problem. In the sequel we extend the approach to a class of nonlinear models. To that end, we propose a new framework, in a QP formulation, so as to minimize the contributions of nonlinear terms into the residual of the designed filter.

A. Linear Models

Consider a linear model as defined in (1). Along the same vein as [28, Section 2.5.2], one may observe that the behavior set $\mathcal{M}$ can alternatively be characterized as

$$\mathcal{M} = \big\{ z \in \mathcal{W}^{n_z} \big|\ N_H(p)L(p)z = 0 \big\},$$

where the collection of the rows of $N_H(s)$ forms an irreducible polynomial basis for the left null-space of the matrix $H(s)$. This representation is the basic idea to design a residual generator of model (1). Namely, by picking a linear combination of $N_H(p)$ rows and adding stable dynamic $d(p)$ of sufficiently order, we arrive at a residual generator in the sense of Definition 2.1 with transfer operator

$$R(p) = d^{-1}(p)\gamma(p)N_H(p)L(p) := d^{-1}(p)N(p)L(p) \qquad (3)$$

The above filter can easily be realized by an explicit state-space description (2) with the input z and output r. Hence, a sensitive residual generator can be characterized as the polynomial matrix equations

$$N(s)H(s) = 0, \qquad (4a)$$
$$N(s)F(s) \neq 0, \qquad (4b)$$

where the polynomial vector $N(s)$ is to be chosen. Let us recall that equations (4a) and (4b) in fact address the required conditions of Definition 2.1 and Definition 2.2 respectively.

Remark 3.1 (Fault Isolation): Consider the model in (1) and suppose $n_f > 1$. The goal is to design a filter in order to only detect one of the fault signal, say f_1, and isolate the residual from the other faults $f_i, i \in \{2, \cdots, n_f\}$. To this end, one can easily infer that augmenting the unknown signal with all the faults f_i $(i \geq 2)$ leads to a new model that indeed addresses the goal, i.e.,

$$[H(p)\ \widetilde{F}(p)] \begin{bmatrix} x \\ \tilde{f} \end{bmatrix} + L(p)z + F_1(p)f = 0,$$

where $F_1(p)$ is the first column of $F(p)$, $\widetilde{F}(p) := [F_2(p), \cdots, F_{n_f}(p)]$, and $\tilde{f} := [f_2, \cdots, f_{n_f}]$, see [14, Theorem 2] for more details on fault isolation.

Next, we move on to translate the nontrivial matrix polynomial equations (4) to a linear programming framework.

Lemma 3.2: Let $N(s)$ be the solution of (4), where

$$H(s) := \sum_{i=0}^{d_H} H_i s^i, \quad F(s) := \sum_{i=0}^{d_F} F_i s^i,$$
$$N(s) := \sum_{i=0}^{d_N} N_i s^i.$$

Then the conditions in (4) can equivalently be written as

$$\bar{N}\bar{H} = 0, \qquad (5a)$$
$$\big\|\bar{N}\bar{F}\big\|_\infty \geq 1, \qquad (5b)$$

where $\|\cdot\|_\infty$ is infinite vector norm, and

$$\bar{N} := \begin{bmatrix} N_0 & N_1 & \cdots & N_{d_N} \end{bmatrix},$$
$$\bar{H} := \begin{bmatrix} H_0 & H_1 & \cdots & H_{d_H} & 0 & \cdots & 0 \\ 0 & H_0 & H_1 & \cdots & H_{d_H} & 0 & \vdots \\ \vdots & & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & H_0 & H_1 & \cdots & H_{d_H} \end{bmatrix},$$
$$\bar{F} := \begin{bmatrix} F_0 & F_1 & \cdots & F_{d_F} & 0 & \cdots & 0 \\ 0 & F_0 & F_1 & \cdots & F_{d_F} & 0 & \vdots \\ \vdots & & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & F_0 & F_1 & \cdots & F_{d_F} \end{bmatrix}.$$

Proof: By definitions, it is easy to observe that

$$N(s)H(s) = \bar{N}\bar{H}[I\ sI\ \cdots\ s^k I]', \quad k := d_N + d_H.$$

Moreover, in light of the linear structure of equations (4), one can simply scale the equations and arrive at the assertion of the Lemma. ■

Remark 3.3: It is straightforward to inspect that if $\bar{N}$ is a solution to (5), then so is $-\bar{N}$. Hence, the inequality (5b) can be understood as an m different LP problems where $m = n_f(d_F + d_N + 1)$ is the number of $\bar{F}$ columns, and n_f is the dimension of signal f in the model (1). That is, in each true LP problem, one can only focus on a component of the vector $\bar{N}\bar{F}$ and replace the inequality (5b) with

$$\bar{N}\bar{F}v \geq 1, \qquad v := [0, \cdots, 1, \cdots, 0]'.$$

We close this section with the following Fact that provides a necessary and sufficient condition for the existence of the solution to polynomial matrix equations (4).

Fact 3.4: There exists a solution $N(s)$ to (4) if and only if Rank $[H(s)\ F(s)] >$ Rank $H(s)$.

Note that the formulation of Lemma 3.4 is indeed an alternative implication of Fact 3.4, see [14, Corollary 3] for a similar result.

B. Nonlinear Models

In this section we extend the model of (1) with a nonlinear term $E(\cdot)$ as a function of unknown signal x:

$$E(x) + H(p)x + L(p)z + F(p)f = 0. \tag{6}$$

It is straightforward to see that the residual of the filter (3) is obtained as

$$r := R(p)z = -d^{-1}(p)N(p)\big(F(p)f + E(x)\big). \tag{7}$$

Therefore, the main objective, roughly speaking, is to reduce the contribution of $E(x)$ into residual (7) while increase the residual sensitivity with respect to the fault f. For this purpose, we propose two approaches focusing on different terms of the residual (7). In both approaches we assume that the denominator of the FDI filter is fixed and the main target to design is the numerator coefficients, i.e., $N(p)$ in (7).

Approach (I): The main objective of this approach is to somehow increase the sensitivity of the residual (7) with respect to the fault f. Without loss of generality, one may extract the linear part of $E(x)$ and assume that

$$\lim_{x \to x_e} \frac{\|E(x)\|}{\|x - x_e\|} = 0,$$

where $x_e \in \mathbb{R}^{n_x}$ is an equilibrium state of the system, and $\|\cdot\|$ stands for the Euclidean norm of a vector. Therefore, one may assume that the contribution of the nonlinear term $E(x)$ can be neglected providing that the system (6) normally works around the equilibrium point x_e. From practical perspective this could be a reasonable assumption since in many applications a system dynamic is considerably deviated from a nominal operating point if there exists a fault/attack signal. In these cases it is essentially important to only detect the fault/attack signal on time. However, since the signal $E\big(x(\cdot)\big)$ passes through the FDI filter, and consequently the derivatives of the contribution signals are also involved, it is not clear any more if the assumption holds in view of the residual. This issue will be addressed in the next approach. Hence, as a first approach, one can slightly modify the formulation in (5) and arrive at

$$\max_{\bar{N}} \|\bar{N}\bar{F}\|_\infty \tag{8a}$$

$$\text{s.t.} \begin{cases} \bar{N}\bar{H} = 0 \\ \|\bar{N}\|_\infty \leq 1 \end{cases} \tag{8b}$$

where the objective function (8a) targets the contribution of signal f into the residual. Let us recall that $\bar{N}\bar{F}$ is the vector containing all numerator coefficients of the transfer function from signal f to residual r, i.e., $N(s)$ in (4a). Moreover, in a similar fashion as Remark 3.3, it is immediate to consider the objective function (8a) essentially as an m different LP formulations, where m is the number of $\bar{F}$ columns. Regarding the optimization constraints, we add the second constraint in (8b) to avoid unbounded solutions. Obviously this constraint does not loose generality as the filter $R(p)$ in (6) can be computed up to a scalar. It is also a classical result that the second constraint in (8b) is indeed an LP constraint in an augmented state space, see for instance [22, Section 5.4.3].

Approach (II): This approach is the main theoretical contribution of the article. In contrast to existing literature on nonlinear FDI methods, here we impose constraints on disturbance signals rather than nonlinearity structure of system dynamics. Namely, we assume that some rough information about the disturbances pattern is available, i.e., we restrict the disturbances to a certain family of signatures. We then aim to control the contribution of the nonlinear term $E(x)$ into the residual in the presence of these disturbances. In essence, the main objective is to train the FDI filter in order to identify the normal behavior of the system while such disturbances appear. For this purpose, let us fix a certain pattern for the signal x. We approximate the mapping $t \mapsto E\big(x(t)\big)$ in the presence of this disturbance over a given time horizon $[0, T]$. The approximation step is in fact the projection of the function $E_k\big(x(\cdot)\big)$, k^{th} component of $E\big(x(\cdot)\big)$, into the linear vector space $\mathcal{N} := span\{b_0, b_1, \cdots, b_n\}$ where $\{b_i(\cdot)\}_{i=0}^n$ is a basis of smooth functions for $\mathcal{N}$. Let formally introduce this step as

$$e(t) := E\big(x(t)\big) \approx \sum_{i=0}^{n} \beta_i b_i(t) = \beta B(t), \quad t \in [0, T] \tag{9}$$

where $\beta := [\beta_0, \cdots, \beta_n]$ is a constant matrix, and $B := [b_0, \cdots, b_n]'$ is a vector of smooth functions. Further, we assume that the subspace $\mathcal{N}$ is closed under differentiation operator p. This requirement, for instance, is satisfied for the polynomial or Fourier basis. The aforementioned assumption gives rise to translate the linear operator p as a matrix operator, i.e.,

$$pB(t) := \frac{\mathrm{d}}{\mathrm{d}t}B(t) = DB(t). \tag{10}$$

Let us define $r_e(t) := N(p)e(t)$. In accordance to approximation (9) and operator (10), and in view of projection into the subspace $\mathcal{N}$, one can also approximate the error of residual as follows:

$$r_e(t) \approx \bar{N}\widetilde{D}B(t), \qquad \widetilde{D} := \begin{bmatrix} \beta \\ \beta D \\ \vdots \\ \beta D^{d_N} \end{bmatrix} \tag{11}$$

where $\bar{N}$ is defined as in Lemma 3.2, and d_N is the degree of FDI filter. Hence, it is now straightforward to formulate the $\mathcal{L}_2$ norm of r_e as a quadratic function of the FDI filter coefficients $\bar{N}$. Namely

$$\|r_e\|^2_{\mathcal{L}_2} \approx \bar{N}\widetilde{D}G\widetilde{D}'\bar{N}', \qquad G_{ij} := \int_0^T b_{i-1}b_{j-1}\mathrm{d}t, \tag{12}$$

where the matrix $\widetilde{D}$ is defined as in (11) and G is a symmetric matrix with dimension (d_N+1). Note that G is indeed the *Gram* matrix of the subspace $\mathcal{N}$ contained in a Hilbert space endowed with the inner product $\langle f, g\rangle := \int_0^T fg\,\mathrm{d}t$ [21, Section 3.6]. Now we are at a place to modify the formulation (8) in order to control the nonlinear term contribution into the residual. To this end, we suggest the following QP type formulation:

$$\min_{\bar{N}} \bar{N}Q\bar{N}', \qquad Q := \widetilde{D}G\widetilde{D}' \tag{13a}$$

$$\text{s.t.} \begin{cases} \bar{N}\bar{H} = 0 \\ \|\bar{N}\bar{F}\|_\infty \geq 1 \end{cases} \tag{13b}$$

where $\widetilde{D}$ and G are defined in (11) and (12), respectively. Let us recall once again that in light of Remark 3.3 the formulation (13) can be viewed as m different true QP problem where $m = n_f(d_F + d_N + 1)$.

Remark 3.5: In practice it may be required to robustify the FDI filter to more than one disturbance pattern, say $\{x_i(\cdot)\}_{i=1}^n$. For this purpose it suffices to first compute the matrices Q_i corresponding to each of $x_i(\cdot)$ and then solve the QP problem in (13) with $Q := \sum_{i=1}^n Q_i$.

IV. Case study: Multi-machine Two-Area Power Network

In this section a multi-machine power system, based only on frequency dynamics, is described [5]. The system is arbitrarily divided into two control areas. The generators are equipped with primary frequency control and each area is under the so called Automatic Generation Control (AGC) which adjusts the generating setpoints of specific generators so as to regulate frequency and maintain the power exchange between the two areas to its scheduled value.

A. System description

We consider a system comprising of n buses and g number of generators. Using the classical generator model every synchronous machine is modelled as constant voltage source behind its transient reactance x'_d. Therefore, for each generator a virtual node (the so called internal generator node) is added to represent the internal voltage source, resulting in a system with $n+g$ buses. Denote by $E_G \in \mathbb{C}^g$ a vector consisting of the generator internal node voltages $E_{Gi} = |E^0_{Gi}|\angle\delta_i$ for $i = 1, \dots, g$ The phase angle of the generator voltage node is assumed to coincide with the rotor angle δ_i and $|E^0_{Gi}|$ is a constant. The voltages of the rest of the nodes are included in $V_N \in \mathbb{C}^n$, whose entries are $V_{Ni} = |V_{Ni}|\angle\theta_i$ for $i = 1, \dots, n$.

Assuming that the turbine dynamics are represented by a first order transfer function, we introduce the equations of oscillation of generator i.

$$\begin{aligned} \dot{\delta}_i &= 2\pi(f_i - f_0), \\ \dot{f}_i &= \frac{f_0}{2H_iS_{B_i}}(P_{m_i} - P_{e_i} - \frac{1}{D_i}(f_i - f_0) - \Delta P_{Load_i}), \\ \dot{P}_{m_i} &= \frac{1}{T_{ch,i}}(P^0_{m_i} + \Delta P_{p_i} + \Delta P_{agc} - P_{m_i}), \end{aligned}$$

where δ_i (rad) and f_i (Hz) represent the rotor angle and the rotor electrical frequency respectively. P_{mi} (MW) is the generated power (output of the turbine), P_{ei} $(MW)$is the electrical consumed power and $\Delta P_{Load_i})$ represents a load deviation that may occur on the generator node. The initial frequency steady state value is represented by f_0, H_i (sec) denotes the inertia time constant, S_{B_i} (MVA) is the generator's rated power of the machine and D_i represents the frequency dependency of the load. $T_{ch,i}$ denotes the time constant of the turbine and $P^0_{m_i}$ the initial setpoint of the generator. The terms $\Delta P_{m,p_i}$ and $\Delta P_{m,agc}$ correspond to the primary frequency control and the AGC respectively.

In the above equations $\Delta P_{m,p_i}$ depends directly on the frequency of the generator, whereas P_{e_i} and $\Delta P_{m,agc_a}$ are related to the dynamic states via algebraic equations. Recall that the power flows can be expressed only by the voltages and the bus admittance matrix of the network. The objective then is to express the power flows as a function of the voltage of the internal node E_{G_i}. As already mentioned $E^0_{G_i}$ is assumed to be constant and hence the power flows will depend only on the dynamic state δ ($\delta = [\delta_1, \dots, \delta_g]'$). Specifically, $\Delta P_{m,agc}$ depends on the active power exchanged between the two areas and hence both P_{e_i} and $\Delta P_{m,agc_a}$ can be expressed as a function of δ. To represent the system by a set of differential equations we eliminate the algebraic states.

B. Algebraic state elimination

To remove the algebraic constraints, we retain the internal nodes (behind the transient reactance) of the generators and eliminate the rest of the nodes. For this purpose we assume constant impedance loads so that they can be included in the network admittance matrix.

Partitioning the nodal equation of the augmented network into the injection currents (and also the node voltages) of the n nodes of the system and the additional g internal generator nodes we get

$$I = YV \Leftrightarrow \begin{bmatrix} I_G \\ I_N \end{bmatrix} = \begin{bmatrix} Y_{GG} & Y_{GN} \\ Y_{NG} & Y_{NN} \end{bmatrix} \begin{bmatrix} E_G \\ V_N \end{bmatrix},$$

where the bus admittance matrix $Y \in \mathbb{C}^{(g+n)\times(g+n)}$ includes the transient reactances of the generators and the admittances that represent the loads. The current injection to the nodes without generation is equal to zero, i.e $I_N = \mathbf{0}$. Hence,

$$I_G = Y_G E_G, \tag{14a}$$
$$V_N = K_V E_G + Y_{NN}^{-1}, \tag{14b}$$

where $Y_G = Y_{GG} - Y_{GN} Y_{NN}^{-1} Y_{NG},\ \ K_V = -Y_{NN}^{-1} Y_{NG}$.

Equations (14a) and (14b) are used to express the power flows as a function of δ. Specifically, $P_{ei} = \Re(E_{Gi} I_{Gi}{}^{*})$ is the electrical power for the generator i, and using (14a) we get

$$P_{ei} = \sum_{j=1}^{g} |E_{Gi}^0||E_{Gj}^0|(B_{ij}^{red}\sin(\delta_i - \delta_j) + G_{ij}^{red}\cos(\delta_i - \delta_j)),$$

where G_{ij}^{red}, B_{ij}^{red} are the real and imaginary entries of the reduced admittance matrix Y_G, respectively. In general, the active power flow on line connecting the nodes k,m is expressed by

$$P_{km} = \Re(V_k(V_k - V_m)^* Y_{G_{km}}^*),$$

and using (14b) is expressed as a function of δ as well. That way the multi-machine system is described by a set of nonlinear differential equations without algebraic constraints.

C. Two-Area frequency dynamics

In this subsection, we consider a reduced network, as described in previous §IV-A and IV-B and focus on the case that the is divided in two control areas. Each area is equipped with primary and secondary frequency (AGC) control. Let $G = \{i\}_1^g$ denote the set of generator indices. Denote then by $A_1 = \{i \in G \mid i \text{ in Area 1}\}$ and $A_2 = \{i \in G \mid i \text{ in Area 2}\}$ the set of generators that belong to Area 1 and Area 2, respectively. Let also $L_{tie} = \{(k,m)|k,m \text{ edges of a tie line and } k \in A1,\ m \in A2\}$ where a tie line is a line connecting the two independently controlled areas. The model of the two area power system is described by the following set of equations.

$$\dot{\delta}_i = 2\pi(f_i - f_0), \tag{15a}$$
$$\dot{f}_i = \frac{f_0}{2H_i S_{B_i}}(P_{m_i} - P_{e_i}(\delta) - \frac{1}{D_i}(f_i - f_0) - \Delta P_{load_i}), \tag{15b}$$
$$\dot{P}_{m,a_1} = \frac{1}{T_{ch,a_1}}(P_{m,a_1}^0 + v_{a_1}\Delta P_{p,a_1}^{sat} + w_{a1}\Delta P_{agc_1}^{sat} - P_{m,a_1}), \tag{15c}$$
$$\dot{P}_{m,a_2} = \frac{1}{T_{ch,a_2}}(P_{m,a_2}^0 + v_{a_2}\Delta P_{p,a_2}^{sat} + w_{a2}\Delta P_{agc_2}^{sat} - P_{m,a_2}), \tag{15d}$$

$$\begin{aligned}\Delta\dot{P}_{agc_1} = &\sum_{j\in A_1} c_{1j}(f_j - f_0)\\ &+ \sum_{j\in A_1} b_{1j}(P_{m_j} - P_{e_j}(\delta) - \Delta P_{load_j})\\ &- \frac{1}{T_{N_1}} g_{11}(\delta, f) - C_{p_1} g_{12}(\delta, f)\\ &- \frac{K_1}{T_{N_1}}(\Delta P_{agc_1} - \Delta P_{agc_1}^{sat}).\end{aligned}$$

$$\begin{aligned}\Delta\dot{P}_{agc_2} = &\sum_{j\in A_2} c_{2j}(f_j - f_0)\\ &+ \sum_{j\in A_2} b_{2j}(P_{m_j} - P_{e_j}(\delta) - \Delta P_{load_j})\\ &- \frac{1}{T_{N_2}} g_{22}(\delta, f) - C_{p_2} g_{21}(\delta, f)\\ &- \frac{K_2}{T_{N_2}}(\Delta P_{agc_2} - \Delta P_{agc_2}^{sat}).\end{aligned}$$

where,

$$\Delta P_{p_i} = -\frac{1}{S_i}(f_i - f_0), \tag{16}$$

$$\Delta P_{p_i}^{sat} = \begin{cases} \Delta P_{p_i}^{min} & \text{if} \quad \Delta P_{p_i} \le \Delta P_{p_i}^{min}, \\ \Delta P_{p_i} & \text{if} \quad \Delta P_{p_i}^{min} < \Delta P_{p_i} < \Delta P_{p_i}^{max}, \\ \Delta P_{p_i}^{max} & \text{if} \quad \Delta P_{p_i} \ge \Delta P_{p_i}^{max}. \end{cases} \tag{17}$$

$$\Delta P_{agc_i}^{sat} = \begin{cases} \Delta P_{agc_i}^{min} & \text{if} \quad \Delta P_{agc_i} \le \Delta P_{agc_i}^{min}, \\ \Delta P_{agc_i} & \text{if} \quad \Delta P_{agc_i}^{min} < \Delta P_{agc_i} < \Delta P_{agc_i}^{max}, \\ \Delta P_{agc_i}^{max} & \text{if} \quad \Delta P_{agc_i} \ge \Delta P_{agc_i}^{max}, \end{cases}$$

$$P_{ei} = \sum_{j=1}^{g} E_{G_i} E_{G_j}(B_{ij}\sin(\delta_i - \delta_j) + G_{ij}\cos(\delta_i - \delta_j)) \ \ ,$$

$$g_{11}(\delta) = \Delta P_{T_{12}} = \sum_{(i,j)\in L_{tie}} P_{ij} - P_{T_{12}^0},$$
$$g_{22}(\delta) = \Delta P_{T_{21}} = \sum_{(i,j)\in L_{tie}} P_{ji} - P_{T_{21}^0},$$

with,

$$P_{ij} = |V_{N_i}||V_{N_j}|\Big(G_{ij}\cos(\theta_i - \theta_j) + B_{ij}\sin(\theta_i - \theta_j)\Big),$$

and $g_{12}(\delta) = \Delta\dot{P}_{T_{12}}$, $g_{21}(\delta, f) = \Delta\dot{P}_{T_{21}}$. The power flows P_{ij} correspond to the tie lines and hence G_{ij} and B_{ij} are based to the initial network admittance matrix Y_{NN}. Note that in (15) $i \in G$, $a_1 \in A_1$ and $a2 \in A2$.

Inside each area only some of the generators are equipped with primary frequency control. To encode this we introduce the binary vector v, see (15c), (15d). The primary frequency control is activated independently and locally for each generator with objective to regulate the frequency by adjusting the generating power as described by (16). The control signal is subjected to saturation limits as shown in (17).

AGC utilizes frequency measurements from its control area and power flow measurements on the tie lines so as to bring their values back to their operating setpoints (i.e f_0 for the frequency, ΔP_{Tij}^0 for the total active power exchange). AGC centralized signal is distributed to some generators inside its control area. The participation of the generators in the AGC action is represented by a weighted vector w (see 15c,15d), whose elements are based on the contracts that the generation utilities have established with the Transmission System Operator (TSO) of the area. The AGC signal is also subjected to saturation limits. Constants c and b are based on the weighted frequency measurement that AGC gets as an input. T_N, C_p and K are design constants for the AGC control loop. For details on the AGC modelling one should refer to [11] and [4].

The demonstration of the FDI methodology will be based on a undesirable signal U additive to the AGC signal. For instance, if the attack signal is imposed in Area i, equation (15c) or (15d) will be modified as

$$\dot{P}_{m,a_i} = \frac{1}{T_{ch,a_i}}(P^0_{m,a_i} + v_{a_i}\Delta P^{sat}_{p,a_i} + w_{a1}(\Delta P^{sat}_{agc_i} + \mathbf{U}) - P_{m,a_i}),$$

The described model can be compactly written as

$$\begin{cases} \dot{X}(t) = h(X(t)) + B_d d(t) + B_f f(t) \\ Y(t) = CX(t) \end{cases} \tag{18}$$

where $X := [\{\delta_i\}_1^g, \{f_i\}_1^g, \{P_{m,a_1}\}_{a_1\in A_1}, \{P_{m,a_2}\}_{a_1\in A_1}, \Delta P_{agc_1}, \Delta P_{agc_2}]'$, $d := \{\Delta P_{Load}(t)\}_1^g$ is the unknown load disturbance, and $f(t) := \mathbf{U}$ corresponds to the fault signal we want to detect. The measurement state $Y(\cdot)$ is assumed to be $Y := [\{f_i\}_1^g, \{P_{m,a_1}\}_{a_1\in A_1}, \{P_{m,a_2}\}_{a_1\in A_1}]'$. The nonlinear function $h(\cdot)$ and the constant matrices B_d, B_f and C can be easily obtained by the mapping between the analytical model (15) and (18).

The model can be then written in the form of (6) by defining $x := \begin{bmatrix} X - X_e \\ d \end{bmatrix}$, $z := Y - CX_e$ and

$$E(x) := \begin{bmatrix} h(X) - A(X - X_e) \\ 0 \end{bmatrix}, \quad L(p) := \begin{bmatrix} 0 \\ -I \end{bmatrix},$$

$$H(p) := \begin{bmatrix} -p + A & B_d \\ C & 0 \end{bmatrix}, \quad F(p) := \begin{bmatrix} B_f \\ 0 \end{bmatrix},$$

where X_e is the equilibrium of (15), i.e., $h(X_e) = 0$, and $A := \frac{\partial h}{\partial X}\big|_{X=X_e}$. The following section will highlight via simulations the security and reliability of the filter.

V. Simulation Results

A. Test System

To illustrate the FDI methodology we employed the IEEE 118-bus system. The data of the model are retrieved from a snapshot available at [1]. It includes 19 generators, 177 lines, 99 load buses and 7 transmission level transformers. To render the model in a more realistic configuration, the 19 more transformers are added connecting the medium-voltage generator buses (6.9 24 kV) with the high voltage transmission level buses (400 kV). Moreover, since there were no dynamic data available, typical values provided by [3] were used for the simulations. Figure 1 shows a single-line diagram of the network and the boundaries of the two control areas that is divided into. The nonlinear frequency model of the network was developed according to §IV so as to be the test case for the filter described in §III.

B. Diagnosis filters

In this part we apply the FDI schemes proposed in (8) and (13) to detect the cyber attack on the AGC of the first area, in the presence of load deviations ΔP_{Load} in all nodes. The filter must be insensitive to the normal situation of the network operating conditions (including acceptable load deviations), and highly reflects any undesirable intrusion in the AGC command. That is, as long as available measurements are consistent with the normal settings of the power network and small deviations are normally caused due to load deviations, the filter does not show anything on the monitor. However, once an attack signal $\mathbf{U}$ is injected to the AGC, the filter alarms in a few seconds from the time it started. In the following simulations we fix the degree of filters as $d_N = 7$, and solve the equations introduced in (8) and (13) using YALMIP toolbox [20].

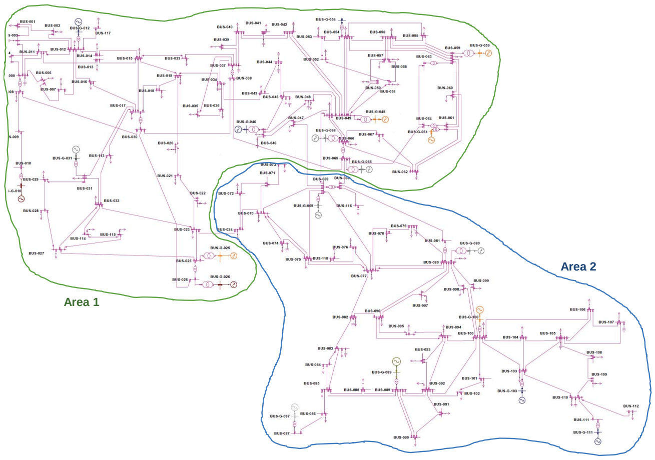
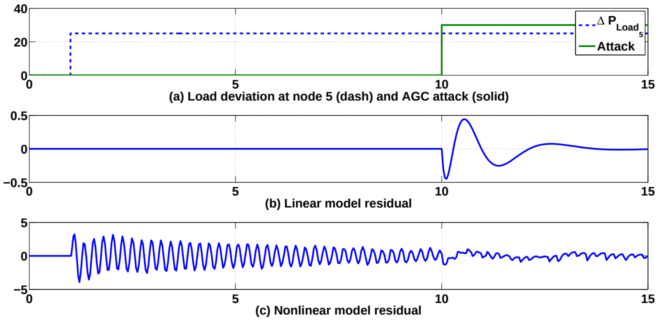


Fig. 1. IEEE 118-bus system divided into two control areas



(a) Load deviation at node 5 (dash) and AGC attack (solid)

(b) Linear model residual

(c) Nonlinear model residual

Fig. 2. Results of the FDI filter obtained in the first approach

Figure 2 illustrates the results of the FDI filter obtained from the LP formulation in (8). Fig.2.a depicts a load deviation in node 5 (ΔP_{Load_5}) at time $t = 1$, and an attack signal in the first area AGC at time $t = 10$. As demonstrated in Fig.2.b, the FDI filter works very well while the inputs are measurements from an ideal linearized model. However, as shown in Fig.2.c, the filter is highly sensitive to nonlinearities and immediately reacts to the load deviation at node 5.

In the second simulation, we aim to overcome the non-linearities contributions into the residual with the aid of QP formulation of (13). To this end, we choose the polynomial functions up to degree $n = 40$ as the basis of approximation scheme. Namely, $b_i(t) := t^i$ for i in $\{0, 1, \cdots, n\}$ and

$$B(t) := [1, t, \cdots, t^n]'.$$

Moreover, in light of polynomial basis, one can simply deduce that the differentiation matrix D and Gram matrix

G, introduced respectively in (10) and (12), are

$$D = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & n & 0 \end{bmatrix}, \quad G_{ij} = \frac{T^{i+j-1}}{i+j-1},$$

where we select $T = 10$ as the approximation horizon. We further assume step functions as particular signatures of load deviations which individually appear at each node. Therefore, each load deviation results in a certain pattern of $e(t)$ introduced as in (9). For the approximation step in (9) and computation of matrix β, we refer the reader to [21, Chapter 3].

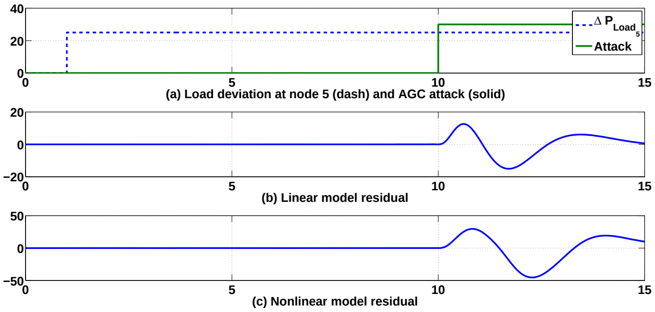


Fig. 3. Results of the FDI filter obtained in the second approach

Figure 3 illustrates the results of the FDI filter obtained from the QP formulation in (8). As demonstrated in Fig.2.*c*, not only is the residual sensitive to the attack signal in the first area, but also the contribution of nonlinear terms in the presence of load deviation is significantly decoupled.

VI. Concluding Remarks and Future Directions

We proposed a tractable algorithm to design an FDI residual generator for nonlinear systems. The technique has been formulated as a family of QP problems that the number of problems is linear with respect to the degree of FDI filter. To illustrate the performance of our theoretical results, we applied the proposed diagnosis filter to a two-area power system so as to detect a cyber intrusion in the AGC signal. It was shown that the filter which takes into account the nonlinear terms succeeds to identify the intrusion whereas the filter neglecting the nonlinear contributions fails. In future work, we plan to test the effectiveness of the proposed approach on a large scale power network, including also voltage dynamics. Moreover, we aim to extend the framework to address a larger class of disturbances in a probabilistic fashion.

References

[1] *Power systems test case archive, college of engineering,university of washington*, URL: http://www.ee.washington.edu/research/pstca/.

[2] R. A. Adams, *Sobolev spaces*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1975. Pure and Applied Mathematics, Vol. 65.

[3] P. M. Anderson and A. A. Fouad, *Power System Control and Stability*, IEEE Computer Society Press, 2002.

[4] G. Andersson, *Dynamics and Control of Electric Power Systems*, Power System Laboratory, ETH Zurich,.

[5] ———, *Power System Analysis*, Power System Laboratory, ETH Zurich,.

[6] R. N. Banavar and J. L. Speyer, *A linear-quadratic game approach to estimation and smoothing*, in American Control Conference, 1991, pp. 2818–2822.

[7] R. V. Beard, *Failure accommodation in linear systems through self-reorganization*, PhD thesis, Massachusetts Inst. Technol., Cambridge, MA, 1971.

[8] J. Chen and R. Patton, *Robuts model based fautls diagnosis for dynamic systems*, Dordrecht: Kluwer Academic Publishers, New York, 1982.

[9] J. Chen and R. Patton, *Robust model-based fault diagnosis for dynamic systems*, Kluwer, Norwell, MA, 1999.

[10] W. H. Chung and J. L. Speyer, *A game-theoretic fault detection filter*, IEEE Trans. Automat. Control, 43 (1998), pp. 143–161.

[11] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, *Cyber attack in a two-area power system: Impact identification using reachability*, in American Control Conference, 2010, pp. 962 – 967.

[12] ———, *A robust policy for automatic generation control cyber attack in two area power network*, in 49th IEEE Conference Decision and Control, 2011, pp. 5973 – 5978.

[13] P. Frank, *Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy — survey*, Automatica, 26 (1990), pp. 459–474.

[14] E. Frisk, M. Krysander, and J. Aslund, *Sensor placement for fault isolation in linear differential-algebraic systems*, Automatica, 45 (2009), pp. 364–371.

[15] J. Getler, *Fault detection and diagnosis in engineering systems*, Marcel Dekker, New York, 1998.

[16] H. Hammouri, M. Kinnaert, and E. El Yaagoubi, *Observer-based approach to fault detection and isolation for nonlinear systems*, Automatic Control, IEEE Transactions on, 44 (1999), pp. 1879 –1884.

[17] M. Hou, *Fault detection and isolation for the descriptor systems*, Issues on fault diagnosis for dynamic systems, ch. 5 (2000).

[18] M. Hou and R. Patton, *An lmi approach to H_-/H_∞ fault detection observers*, in Control '96, UKACC International Conference on (Conf. Publ. No. 427), vol. 1, sept. 1996, pp. 305 – 310 vol.1.

[19] H. L. Jones, *Failure detection in linear systems*, PhD thesis, Massachusetts Inst. Technol., Cambridge, MA, 1973.

[20] J. Lofberg, *Yalmip : a toolbox for modeling and optimization in matlab*, in Computer Aided Control Systems Design, 2004 IEEE International Symposium on, sept. 2004, pp. 284 –289.

[21] D. G. Luenberger, *Optimization by vector space methods*, John Wiley & Sons Inc., New York, 1969.

[22] J. M. Maciejowski, *Predictive control with constrains*, Pearson Education, Harlow, 2002.

[23] D. Maquin, B. Gaddouna, and J. Ragot, *Generation of parity equations for singular systems: Application to diagnosis*, in Proceedings international conference system, vol. 3, 1993, pp. 400–405.

[24] M.-A. Massoumnia, *A geometric approach to the synthesis of failure detection filters*, IEEE Trans. Automat. Control, 31 (1986), pp. 839–846.

[25] M.-A. Massoumnia, G. C. Verghese, and A. S. Willsky, *Failure detection and identification*, IEEE Transaction on Automatic Control, 34 (1989), pp. 316–321.

[26] M. Nyberg and E. Frisk, *Residual generation for fault diagnosis of system described by linear differential-algebraic equations*, IEEE Transaction on Automatic Control, 51 (2006), pp. 1995–2000.

[27] C. D. Persis and A. Isidori, *A geometric approach to nonlinear fault detection and isolation*, IEEE Trans. Automat. Control, 46 (2001), pp. 853–865.

[28] J. W. Polderman and J. C. Willems, *Introduction to mathematical systems theory*, vol. 26 of Texts in Applied Mathematics, Springer-Verlag, New York, 1998. A behavioral approach.

[29] R. Seliger and P. Frank, *Fault diagnosis by disturbance-decoupled nonlinear observers*, in Proceedings of the 30th IEEE Conference on Decision and Control, 1991, pp. 2248–2253.

[30] J. Stoustrup and H. Niemann, *Fault detection for nonlinear systems - a standard problem approach*, in Decision and Control, 1998. Proceedings of the 37th IEEE Conference on, vol. 1, 1998, pp. 96 –101 vol.1.