Load-altering attack detection on smart grid using functional observers

Álan C E Sousa, Nadhir Messai, Noureddine Manamanni

Version of Record: https://www.sciencedirect.com/science/article/pii/S1874548222000099
Manuscript_b6d0bbd96659924c03105ca4a2fbbbda

Load-altering attack detection on smart grids using functional observers

Álan e Sousa[a], Nadhir Messai[a], Noureddine Manamanni[a]

[a] *University of Reims Champagne-Ardenne — CReSTIC EA3804 — UFR Sciences Exactes et Naturelles — Moulin de la Housse BP1039 — 51687 Reims Cedex 2 — FRANCE*

Abstract

Smart grids are becoming more common due to their capacity to accommodate secondary sources, like green energies from solar panels or wind farms. However, the attack surface also grows with more equipment in the network, making it necessary to secure appropriately. With more sensors distributed on the network, it becomes easier for an attacker to hack into one and send false information to the central to destabilize the power generation and distribution. Load-altering attacks do precisely that and have a destructive potential since the generator reaction can cause network instability. Traditional techniques, like those based on the Kalman filter, for example, may pose numerical issues due to the large size and sparsity of the system matrices, failing to provide good results or wasting computational resources. We propose an LMI-based approach to design a bank of residual generators for functional observers to detect such attacks. This approach has the advantage of using a reduced order arbitrary dynamic system, making it suitable for large-scale smart grids, and the use of LMI, allowing the easy insertion of restrictions.

Keywords: functional observer, residual generator, attack detection, power grid, LMI optimization

1. Introduction

The traditional electricity distribution is static and centralized, in which the energy generated in power plants reaches the consumers through successive voltage drops [1]. However, this centralized approach is not well suited for today's needs, as it can not accommodate green energies, such as in-house generators. Also, it can not respond to demand changes or fine control carbon emission. Such shortcomings directly impact people, either by increasing the energy cost or by allowing long-lasting blackouts [2].

One solution for this problem is the smart grid. Its highly connected, two-directional communication channels integrate the generation, distribution and consumption of electricity. As a result, it better accommodates green sources and can, in some cases, even control loads to minimize consumer price and subnetwork load [3–7]. For example, it can control houses' heating systems: the user sets the desired parameters, and the smart grid controls the actual operation, using pricing and load information to decide when to activate the system [8].

However, since the smart grid is a highly connected system containing much information about the power system and individual consumers, it is highly susceptible to attacks [9]. Attackers can get private information about users, but they can also destabilize the whole network by controlling the flow of information or altering the transmitted information. Even though the smart grid is considered highly resilient, it is still susceptible to attacks [10].

Known attacks already caused outages and consequential losses[11, 12]. For example, in 2016, Russians supposedly hacked the Ukrainian power system, leaving parts of Kyiv without electricity for an hour [13]. In 2017, Saudi Aramco's petrochemical plants became a target [14]. In 2019, the US Army attacked a Russian power system [15].

There are many types of attacks against smart grids, which try to affect the system in different ways, from falsifying readings to pretending that the network's physical connections changed. One of such attacks, called False Data Injection, recently gained attention for its stealthy nature, making it difficult to detect [16–20]. In this attack, the attacker controls the signal's trajectory over time to make the change undetectable. The goal is to make the signal's change smooth, so it seems like a natural change. Similarly, zero dynamics attacks also pose a detection challenge, as it exploits the system's zero dynamics to hide the attack. In this attack, the change in some signal does not appear in the system's output, so it cannot be measured. Both attacks have a high potential for service disruption [21–24]. There are also Load Redistribution attacks, where the attacker changes the load information measured by the system, making it react to an inexistent change in load [25–27]. Similarly, Load Altering attacks change the measurement of specific loads to overload a particular network and may target distinct customers, like factories [8, 28–30]. In Topology attacks, the attacker tries to make the operator believe the network topology has changed, which will have consequences if he tries to adjust [8, 31]. Markets are also targets and can affect the network. For example, by informing incorrect pricing to smart meters, a real, unexpected load can cause power redirection and outages, as well as a self-evident financial problem [8].

This list of attacks is non-exhaustive, so there is interest in the constant development of new techniques to defend against them. Cyber-attack defence comes on two fronts: from the Information Technology (I.T.) perspective, security measures such as firewalls, encryption and access control help keep unauthorized people away from the network. It is, however, not enough since hackers can use employees to circumvent such measures, for example. Thus, from the automation perspective, both attack resilient controllers and observers and attack detection schemes make it possible to identify an attack and recover from it. Therefore, I.T. works as a first layer of protection and automation as a second one [2].

Standard automation tools used to detect attacks are observers and residual generators, commonly employed with consecrated techniques such as Kalman filters. However, given that smart grids have numerous states, sometimes on the hundreds, such techniques are not applicable, posing numerical issues [32]. Moreover, even when the techniques yield valid results, they may waste computational resources by estimating more states than necessary for attack detection [33].

Graph theory can help deal with the system's scale problem by using the system's topology. It leads to the concepts of topological stability, controllability and observ-

ability, which depend not only on the system's dynamic but also on the topology of its connections [34, 35]. The tools applied are well suited for large and sparse systems, avoiding numerical problems. Another advantage is the classification of the observability as a scale instead of the binary observable/not observable. Different selections of measured and observed nodes result in different observability indexes, making it possible to compare different observable paths in a graph representing the system's dynamics and assess which renders better observability of the desired states [33, 34].

Another advantage of the graph theory approach is estimating a subset of the states, since the estimation of all states is often not necessary for control or diagnostics purposes [36]. It differs from the well-known reduced-order Luenberger observer because the latter still estimates all unmeasured states, whereas the former only estimates a subset of the states necessary for the correct estimation of the desired subset. For example, in a system with ten states and three sensors, the Luenberger observer will estimate seven states, even if we only desire to estimate one of them. In contrast, the functional observer will estimate as many states as necessary to estimate the desired one correctly, estimating seven only in a worst-case scenario [37, 38].

Residuals observers are the most common way of detecting attacks on dynamic systems. It works by detecting variations between what is measured and the estimation for those measurements. There are some functional residual generators in the literature, formulated mainly through direct algebra manipulation [39–43]. They mostly follow the idea of separating the system between used and unused states through similarity transformation and need to calculate the null space of some matrix at some point, which we wanted to avoid. The direct approach also limits the manipulation of the observer dynamics, as it is hard to link it to the system's dynamics.

We present a bank of functional residual generators capable of detecting load-altering attacks, composed of one observer and one residual generator for each attacked sensor. The proposed approach uses LMI (Linear Matrix Inequality) to design an observer insensitive to attacks on a sensor, making it possible to isolate the attacked sensor on single target attacks. The use of LMI also allows restrictions, like pole placement, to control the observer dynamics.

This article is organized as follows: Section 2 introduces the idea and model of the smart grid. Section 3 presents the load-altering attack we want to detect. In Section 4 we describe the Functional Observer and show how to design a bank of residual generators. Lastly we show a simulation to illustrate the application of the proposed technique.

Notation: The set of real numbers is denoted by $\mathbb{R}$. $\mathbb{R}^n$ denotes a vector of n real elements. $M^\top$ represents the transpose of M. M^+ denotes the Moore-Penrose inverse of M.

2. Smart Grid

Smart grids are electric grids focused on intelligent distribution and load balancing, renewable energy sources, advanced metering and efficient resource usage. Markets directly influence decisions in generation and distribution by using IoT-enabled meters to provide real-time information about consumption and generation to the controllers.

Smart grids are composed of several distributed and heterogeneous subsystems. PMUs (phasor measurement units) and smart meters allow the control center to have information about the energy in both generator and consumer ends, respectively. From the point of view of control, the smart grid becomes a network of generator nodes and load buses [44].

A common way of modelling the dynamics of such networks is by using coupled second-order Kuramoto oscillators [45, 46]. It models buses' frequencies and phases and assumes that the whole network will have an equilibrium frequency, which is valid for electric systems. Each oscillator is given by

$$\frac{2H_i}{\omega_R}\ddot{\phi}_i + \frac{D_i}{\omega_R}\dot{\phi}_i = A_i + \sum_{j=1, j\neq i}^{N} K_{ij}\sin(\phi_j - \phi_i + \gamma_{ij}), \tag{1}$$

where N is the number of nodes, $\phi_i(t)$ is the phase angle of the i^{th} oscillator relative to a frame that rotates at the reference frequrency ω_R, H_i and D_i are inertia and damping constants, respectively, A_i is related to the power injection of node i, K_{ij} is the coupling weight related to the maximum power transfer capacity in the respective transmission line interconnecting the nodes i and j, and γ_{ij} is the corresponding phase shift.

When written in state-space form, the system is described by

$$\begin{bmatrix}\dot{\phi}_G \\ \ddot{\phi}_G \\ \dot{\phi}_L\end{bmatrix} = \begin{bmatrix}\dot{\phi}_G \\ \frac{\omega_R}{2H(A-\frac{D}{\omega_R})\dot{\phi}_G + \mathcal{S}} \\ \frac{\omega_R}{D} * (A + \mathcal{S})\end{bmatrix}, \tag{2}$$

$$\mathcal{S} = \sum_{j=1, j\neq i}^{N} K_{ij}\sin(\phi_j - \phi_i + \gamma_{ij}), \tag{3}$$

where ϕ_G concerns the generators and ϕ_L the loads, and all matrices needs to be properly partitioned to match this division. We will use a linearized version of this system.

3. Load Altering Attack

Smart grids use real-time measurements to control the generators, ensuring they supply the requested load without waste. This balance is vital to the correct operation of the network [30]. When there is an imbalance between the generated and consumed power, one can get blackouts, reactions of transformers relays and curtailment of electrical loads, for example [29]. Thus, it is necessary to keep the network balanced.

Since imbalance can affect the network so much, attackers may explore it to damage the distribution system or a specific factory. The load-altering attack sends false measurements to the network, making the central think that more or less load is present [28]. The goal of the false data is to make the generators adapt, creating an actual imbalance that will damage devices.

With the advent of IoT devices and smart meters on the client-side, this kind of attack becomes more feasible, especially when many devices' designs do not consider cybersecurity seriously, providing access points to attackers without the first IT layer of protection [28]. It is then up to the control layer to identify and mitigate such attacks.

To detect load altering attacks, we can model it in three ways:

$$\tilde{\phi}_j = \phi_i, \tag{4}$$

$$\tilde{\phi}_j = \phi_j + \delta, \tag{5}$$

$$\tilde{\phi}_j = \phi_j \cdot \alpha, \tag{6}$$

where ϕ is real state value, $\tilde{\phi}$ the measured value, and ϕ_j the j^{th} vector entry. The first attack replaces a measurement with a value taken from another state, as seen in Eq. (4); the second attack adds a constant bias to the measurement, as seen in Eq. (5) and the third attack multiplies the measured value by a constant, as seen in Eq. (6).

4. Functional observers

Luenberger first introduced the concept of functional observers [47]. At the core of the functional observer is a system with arbitrary dynamics that estimates a smaller linear combination of the original system's states. The design challenge is to find what states are needed and the arbitrary system's matrices.

Let us define a dynamic system as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + Lf(t), \\ y(t) &= Cx(t), \\ z(t) &= Fx(t), \end{aligned} \tag{7}$$

where $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times p}$, and $C \in \mathbb{R}^{q\times n}$ are system matrices, $L \in \mathbb{R}^{n\times r}$ maps the attacks $f(t) \in \mathbb{R}^r$ to the state vector $x \in \mathbb{R}^n$ and $F \in \mathbb{R}^{s\times n}$ maps the state vector into $z(t) \in \mathbb{R}^s$, the vector of estimated states, with L a zero matrix with only one entry 1 on every column, on the line of the affected state and, similarly, F a zero matrix only having one entry 1 on each row, on the column of the desired state.

Note that $z(t)$ is just an output from the system's perspective, like $y(t)$. They are, however, semantically different in that $y(t)$ represents a measurable output, that is, this output maps directly to sensors in the real plant, whereas $z(t)$ is a linear combination of states that we want the observer to estimate. For our purposes, both $y(t)$ and $z(t)$ are direct maps into $x(t)$, so C and F have only one non-null entry per row, with a value of exactly 1.

To estimate $z(t)$ given $y(t)$ it is necessary to estimate a subset of $x(t)$ which is a superset of $z(t)$. That is due to system dynamics, and an observer created using only $z(t)$ will most likely not have the right dynamics and therefore not be able to estimate $z(t)$ correctly.

Definition 4.1. The triplet (A, C, F) from system (7) is said functional observable if for any initial state $x(0)$ the knowledge of $u(t)$ and $y(t)$ sufices to estimate $z(0) = Fx(0)$ over a finite time $t > 0$. Otherwise it is said functional unobservable [37].

Definition 4.1 is very close to the general definition of observers. This is because it is a specialization, as the functional observer can not observe anything that the output can not observe itself, leading to Theorem 4.1, which gives a rank condition to determine if a triplet (A, C, F) is functional observable.

Theorem 4.1. The triplet (A, C, F) is functional observable if and only if [37]

$$rank \begin{bmatrix} C \\ CA \\ F \\ FA \end{bmatrix} = rank \begin{bmatrix} C \\ CA \\ F \end{bmatrix}. \tag{8}$$

Proof. The functional observer can observe at most what the system's output can observe, therefore the observed states must be a subset of the outputs, and hence a linear combination of it. As the rank calculates the number of linear independent rows in the matrix, it assures that there is no state in $z(t)$ not observable by $y(t)$. A much longer, mathematical proof can be found in [37]. □

To find out what states we need to observe, we first have to define the sets of sensors and desired states. Since our goal is to develop a residual generator, we want $y(t) \subseteq z(t)$, to make it possible to calculate the estimation error. However, $z(t)$ might need to be slightly larger than $y(t)$ to make sure the observer is not simply copying $y(t)$ into $z(t)$.

There is no algebraic way (at least yet) of discovering the set of required states, so graph theory algorithms became a common way of finding it. The main advantage of this approach is that it scales well for large systems. Algorithm 1 [48] presents a way of finding the set of states which needs to be observed given $z(k)$. It does so by turning the system into a graph, where each node is a state and the connections are the dynamics, and then finding a path between the state to be estimated and an ouput.

Algorithm 1 Functional observable set finding

1: **input:** triplet (A,C,S_0)
2: **output:** set S of states needed to observe S_0
3: **let** $F \leftarrow$ matrix for S_0, $\mathcal{M}_1 \leftarrow \emptyset$, $\mathcal{M}_2 \leftarrow \emptyset$, $r_0 \leftarrow \text{rank}(F)$
4: **repeat**
5: **let** $G \leftarrow [\ C^\top\ (CA)^\top\ F^\top\ ]^\top$
6: build a bipartite graph $\mathcal{B}(\mathcal{V}, \mathcal{X}, \mathcal{E}_\mathcal{V}, \mathcal{X})$, where $\mathcal{V} = \{v_1, \ldots, v_{2q+r_0}\}$ is a set of nodes where each element corresponds to a row of $\mathcal{G}$, $\mathcal{X} = \{x_1, \ldots, x_n\}$ is the set of state nodes (where each element also corresponds to a column of $\mathcal{G}$), and (v_i, x_j) is an undirected edge in $\mathcal{E}_\mathcal{V}$ if $\mathcal{G}_{ij}$ is a non-zero entry;
7: find the maximum matching set $\mathcal{E}_m$ associated with $\mathcal{B}(\mathcal{V}, \mathcal{X}, \mathcal{E}_\mathcal{V}, \mathcal{X})$ (e.g., via the Hopcroft-Karp algorithm);
8: $\forall x_i \in \mathcal{X}$, if x_i is connected to an edge in $\mathcal{E}_m$, then update the set of right matched nodes $\mathcal{M}_1 \leftarrow \mathcal{M}_1 \cup \{x_i\}$;
9: define the set of candidate nodes $C = \mathcal{M}_2 \setminus \mathcal{M}_1$, where $x_j \in \mathcal{M}_2$ if $[FA]_{ij}$ is a non-zero entry;
10: draw an element $x_k \in C$ and update $F \leftarrow [\ F^\top\ (F')^{top}\ ]$ and $r_0 = r_0 + 1$, where $F' \in \mathbb{R}^{1\times n}$ and $[F']_{ij} = 1$ if $j = k$ and 0 otherwise;
11: **until** $C \neq \emptyset$

Algorithm 1 adds nodes from the paths between the measured and desired states to the S set until the system becomes functional observable.

4.1. Bank of observers

To detect load-altering attacks on smart grids, we propose a bank of functional observers. Its reduced-order alleviates the computational burden, and the fact that different state paths result in observers with different dynamics gives the possibility of redundancy.

The bank is composed of r observers, one for each attacked node. They are identical, except for the system's L matrix used, which maps the attack to the state. Since each observer in the bank is only sensitive to one attack, it allows attack isolation. Each observer has its own associated residual generator, which will provide the estimation error, allowing to identify the presence of an attack. The final bank of observers and residual generators will have the schematic shown in Figure 1.

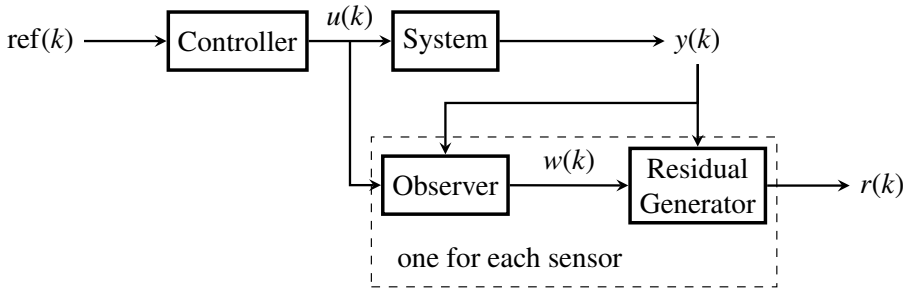

Figure 1: Observer's block diagram

We propose an observer formulation based on LMIs. This kind of formulation has the advantage of allowing the addition of extra constraints to the system by simply adding more restrictions to the LMI. Most of the already proposed functional observer designs for residual generator, as [38–41, 43, 49–55], for example, use a direct formulation, which does not give room for such restrictions, so the designer does not have much control over the observer's dynamics, for example. This formulation sets itself appart in that regard. The design of the proposed observer is as follows:

Theorem 4.2. Given the system (7), with the triplet (A,C,F) functional observable according to Definition 4.1 and Theorem 4.1, an observer of the form[1]

$$\begin{aligned} \dot{w}(t) &= Nw(t) + Jy(t) + Hu(t), \\ \hat{z}(t) &= w(t) + Ey(t), \end{aligned} \tag{9}$$

exists and is able to estimate $\hat{z}(t) \approx z(t)$ given $y(t)$ and $u(t)$ if there exists a solution to the LMI

$$\begin{aligned} &\arg\min \ \|P\|_2 \\ &\text{s.t. } \dot{V} \prec 0 \\ &\quad P \succ 0, \end{aligned} \tag{10}$$

[1]The variable H is not related to that of Equation (1)

where

$$\dot{V} \equiv \begin{bmatrix} X & W \\ W^\top & -I \end{bmatrix}, \tag{11}$$

$$\lambda \in \mathbb{R}^+ \text{ is a free constant,} \tag{12}$$

$$P \text{ is a semidefinite positve matrix} \tag{13}$$

with

$$\begin{aligned} X =& \hat{A}^\top F^\top P - \hat{A}^\top C^\top \hat{E}^\top - \\ & \hat{C}^\top \hat{K}^\top + PF\hat{A} - \hat{E}C\hat{A} - \hat{K}\hat{C} - \lambda I, \end{aligned} \tag{14}$$

$$W = \sqrt{\lambda}(PF - \hat{E}C). \tag{15}$$

$$\tag{16}$$

where

$$\hat{A} = AF^+, \tag{17}$$

$$\hat{C} = CF^+, \tag{18}$$

$$\hat{E} = PE = PU + \hat{Y}V, \tag{19}$$

$$\hat{K} = PK, \tag{20}$$

$$\hat{Y} = PY. \tag{21}$$

The observer's matrices are recovered as

$$K = P^{-1}\hat{K}, \tag{22}$$

$$Y = P^{-1}\hat{Y}, \tag{23}$$

$$E = U + YV, \tag{24}$$

$$R = F - EC, \tag{25}$$

$$N = (RA - KC)F^+, \tag{26}$$

$$J = K + NE, \tag{27}$$

$$H = RB, \tag{28}$$

Proof. First, define the estimation error as (we drop the time dependence of the vectors to simplify notation)

$$\begin{aligned} e &= \hat{z} - z \\ &= w + Ey - Fx \\ &= w + ECx - Fx. \end{aligned} \tag{29}$$

Then define the error dynamics to be

$$\begin{aligned}
\dot{e} =& \dot{w} + (EC - F)\dot{x} && (30)\\
=& Nw + Jy + Hu + (EC - F)(Ax + Bu + Lf) && (31)\\
=& N(e + Fx - ECx) + JCx + Hu + \\
& ECAx + ECBu + ECLf - FAx - \\
& FBu - FLf && (32)\\
=& Ne + (NF - NEC + ECA - FA + JC)x + \\
& (H + ECB - FB)u + (ECL - FL)f. && (33)
\end{aligned}$$

As such, for $\hat{z}$ to converge to z, the following conditions must be satisfied:

$$\begin{aligned}
N \text{ must be Hurwitz-stable}, && (34)\\
N(F - EC) - (F - EC)A + JC = 0, && (35)\\
H - (F - EC)B = 0, && (36)\\
(F - EC)L = 0. && (37)
\end{aligned}$$

However, to make the observer insensitive to only one sensor attack, we need to redefine the condition in Equation 37. Let $L = [\, L_i \; L_n \,]$, where $L_i \in \mathbb{R}^{n\times 1}$ maps the insensitive attack, and $L_n \in \mathbb{R}^{n\times l-1}$ maps the sensitive attacks. Then, to satisfy the property that each observer must be insensitive to one attack and sensitive to the others, we define

$$\begin{aligned}
(F - EC)L_i = 0, && (38)\\
(F - EC)L_n \neq 0. && (39)
\end{aligned}$$

We now need to find matrices N, J, H and E. An LMI can find values for those matrices after we turn the inequality into equality. First we define the Lyapunov candidate function

$$V = e^\top Pe. \tag{40}$$

The error function, taking into account the required restrictions, becomes

$$\dot{e} = Ne - (F - EC)L_n f. \tag{41}$$

To rewrite the attack as an error, we define the error as proportional to the fault

$$e \propto L_n f, \tag{42}$$

which yields

$$\|L_n f\| = \lambda \|e\|, \tag{43}$$

where $\lambda \in \mathbb{R}^+$ scales the attack in proportion to the error, and is a free, tunnable variable.

As that, with

$$R = F - EC, \tag{44}$$

the derivative of the candidate function becomes

$$\begin{aligned}\dot{V} &= \dot{e}^\top Pe + e^\top P\dot{e} \\ &= (Ne - \lambda R\,\|e\|)^\top Pe + e^\top P(Ne - \lambda R\,\|e\|) \\ &= e^T(N^\top P + PN)e - 2\lambda \left\|e^\top PR\right\| \cdot \|e\| \\ &\leq e^T(N^\top P + PN)e - \lambda(\left\|e^\top PR\right\|^2 + \|e\|^2) \\ &= e^T(N^\top P + PN - \lambda PRR^\top P - \lambda I)e,\end{aligned} \tag{45}$$

where I is the identity marix of appropriate size.

This BMI (Bilinear Matrix Inequality), so far, only guarantees the stability of the N matrix. To include restriction (35) let

$$N(F - EC) = RA - JC, \tag{46}$$
$$NF = RA - (J - NE)C, \tag{47}$$
$$K = J - NE, \tag{48}$$
$$N = RAF^+ - KCF^+, \tag{49}$$

where $K \in \mathbb{R}^{s\times q}$ is a full matrix the optimization will find and F^+ is Moore-Penrose inverse of matrix F.

To include restriction (38), let

$$(F - EC)L_i = 0, \tag{50}$$
$$ECL_i = FL_i, \tag{51}$$
$$E = FL_i(CL_i)^+ + Y(I - (CL_i)(CL_i)^+), \tag{52}$$
$$U = ECL_iL_i^+, \tag{53}$$
$$V = I - L_iL_i^+, \tag{54}$$
$$E = U + YV. \tag{55}$$

recalling eqs. (17) to (21).

Equation (45) becomes

$$\begin{aligned}\dot{V} = e^T((R\hat{A} - EC\hat{A} - K\hat{C})^\top P + \\ P(R\hat{A} - EC\hat{A} - K\hat{C}) - \lambda PRR^\top P - \lambda I)e.\end{aligned}$$

After further expanding and making all necessary variable substitutions, the final candidate function derivative is

$$\begin{aligned}\dot{V} = \hat{A}^\top F^\top P - \hat{A}^\top C^\top \hat{E}^\top - \hat{C}^\top K^\top + \\ PF\hat{A} - \hat{E}C\hat{A} - K\hat{C} - \lambda PRR^\top P - \lambda I.\end{aligned} \tag{56}$$

However, R is still unexpanded and contains a variable, which is making $\dot{V}$ bilinear.

Using Schur complement one gets [56]

$$X = \hat{A}^\top F^\top P - \hat{A}^\top C^\top \hat{E}^\top \hat{C}^\top K^\top + PF\hat{A} - \hat{E}C\hat{A} - K\hat{C} - \lambda I, \tag{57}$$

$$W = \sqrt{\lambda}(PF - \hat{E}C), \tag{58}$$

$$\dot{V} \equiv \begin{bmatrix} X & W \\ W^\top & -I \end{bmatrix}. \tag{59}$$

□

4.2. Residual generators

A residual is a signal designed to have close to zero value in the absence of attacks and to deviate significantly from zero in its presence. A function can then give a binary output given a residual to flag an attack in the system, like, for example, based on a threshold. This subsection is concerned with the residual dynamics, not with the binary function.

The proposed residual generator uses the designed observer, insensitive to one attack, to generate an output corresponding to the estimation error, called the residual. Thus, it is a measurement of how well the observer can estimate the state. Therefore, since the attack is an exogenous, not measured signal, the observer will not correctly estimate the state in its presence, which will cause a significant change in the residual. As such, we have that:

Lemma 4.3. A residual signal of the form

$$r(t) = Gw(t) + My(t), \tag{60}$$

with

$$M = (C(1 - L_i))^\top, \tag{61}$$

$$G = -M(I - CF^+E)^{-1}CF^+, \tag{62}$$

where $1 - L_i$ is an entry-wise operation, is a residual generator for observer (9) designed using Lemma 4.2.

Proof. Writting the error equation for the residual generator using the observer's matrices, we have

$$\begin{aligned} r &= Gw + My \\ &= G(e + Fx - ECx) + MCx \\ &= Ge + (G(F - EC) + MC)x, \end{aligned} \tag{63}$$

where we can see that the following restriction is required for the residual generator to go to zero when there is no error:

$$G(F - EC) + MC = 0. \tag{64}$$

Writting the error equation in terms of the output we have:

$$\begin{aligned} r &= Gw + My \\ &= Q(y - Cx) \\ &= Q(y - CF^{-1}\hat{z}) \\ &= Q(y - CF^{-1}(w + Ey)) \\ &= Q((I - CF^{-1}E)y - CF^{-1}w), \end{aligned} \tag{65}$$

$$M = Q(I - CF^{-1}E), \tag{66}$$

$$G = -QCF^{-1}. \tag{67}$$

By replacing Eq. (66) and Eq. (67) into Eq. (64) we can see that it satisfies the condition no matter what value of Q, therefore Q can be used to tune the magnitude of the residual. For this, M can be defined using the matrix L as

$$M = (C(1 - L_i))^\top, \tag{68}$$

which is the sum of all error-prone outputs $y(t)$, except the insensitive one. Replacing Eq. (68) into Eq. (66) and eliminating Q from Eq. (67) we get

$$M = (C(1 - L_i))^\top, \tag{69}$$

$$G = -M(I - CF^{+}E)^{-1}CF^{+}. \tag{70}$$

Note that Equations (66) and (67) can be used directly by finding a matrix Q with desired properties, such as one that makes the residual have a large enough absolute value in the presence of the expected attacks. □

5. Simulation results

To illustrate the efficiency of our approach let us consider the IEEE 118-bus test case approximates the U.S. Midwest electric power system. It contains 19 generators, 35 synchronous condensers, 177 lines, nine transformers and 91 loads. Figure 2 shows the network's schematic. The data file hosted on github[2] is a MATLAB file containing the constants for Equation (1) in matricial form. The data in IEEE Common Data Format is available here[3]. The data is mostly real, except for the base KV levels, which are guesses, since they were not available on the original dataset.

We simulated the IEEE 118 power grid model using the dynamic system shown in Equation (3), linearized around its equilibrium point. Figure 3 shows the system's dynamic graph, discriminating the generators, loads and sensors. It shows that the system is sparsely connected, with an average node degree of 2. It also shows that the system has a high betweenness centrality, making the paths between sensors and desired states longer and making the states in the middle essential for the observation.

[2] https://github.com/acristoffers/SmartGrid/blob/master/powergrid/IEEE118pg.mat
[3] https://labs.ece.uw.edu/pstca/pf118/pg_tca118bus.htm

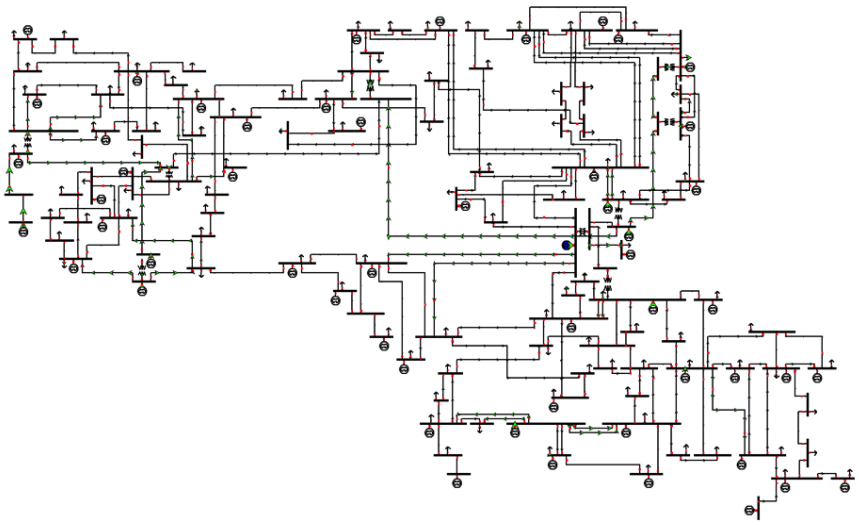

Figure 2: IEEE 118-bus network's schematic

To observe the desired states, the observer needs to estimate around 150 other states from 226 total ($\approx 66\%$), which makes more evident the benefit of using a functional observer.

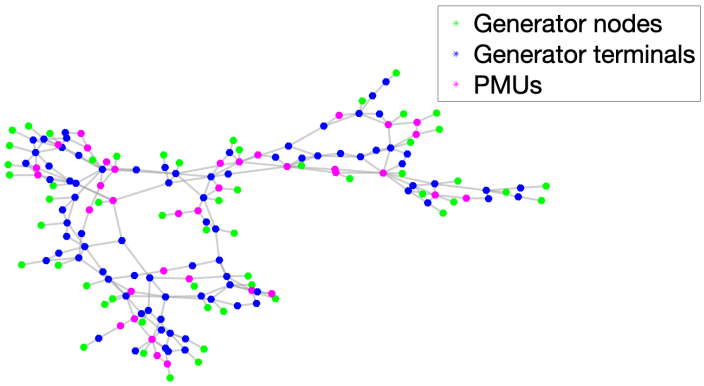

Figure 3: IEEE 118's dynamic graph representation.

The choice of sensors was random, placing PMUs on 30% of the generator's and load's terminals to a total of 35 sensors. Algorithm 1 returned a set S containing 126 states. Using lemmas 4.2 and 4.3 we derived a bank of observers and residual

generators for the system capable of detecting load-altering attacks.

We simulated the load-altering attack in three ways: attack one copies another state's value into the attacked node, attack two adds a constant value to the existing signal and attack three multiplies the state value by a constant. Figures 4, 5 and 6 show the residual generators' outputs for each attack.

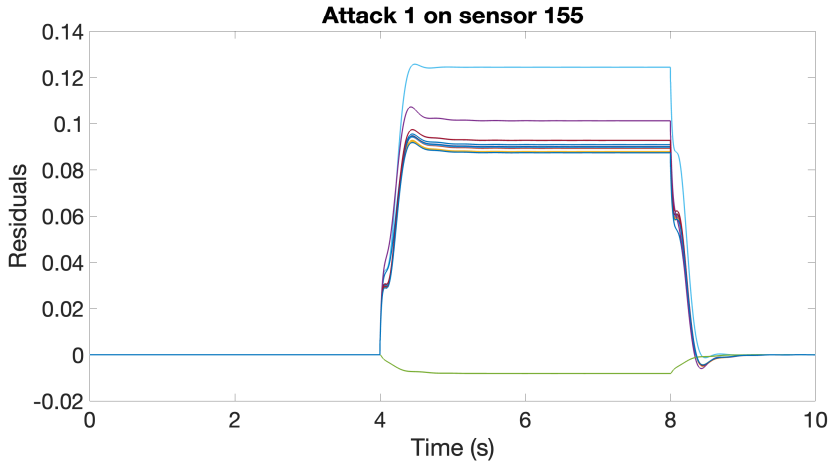

Figure 4: Residuals for attack 1 (state's value copy) on state 155

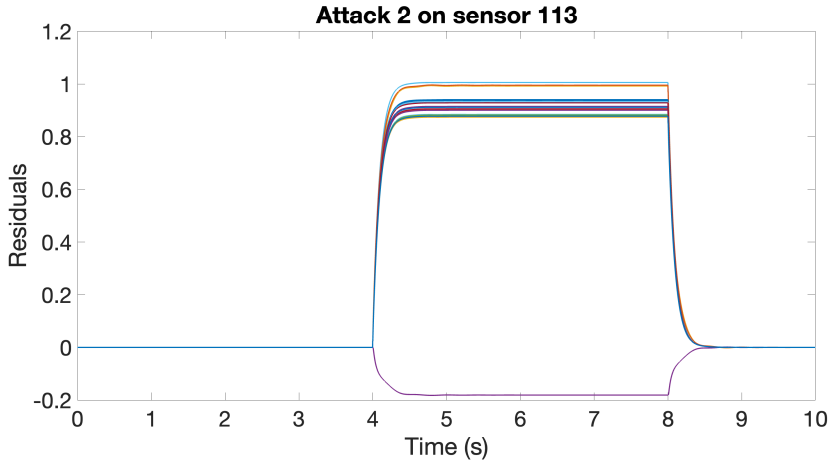

Figure 5: Residuals for attack 2 (additive) on state 113

The proposed residual generators were able to identify the attack in all cases. The residuals are zero until the beginning of the attack, become non-zero when it starts, and return to zero after it ends. One residual remained close to zero in all cases, as its observer is insensitive to the attack on that sensor, making it always possible to

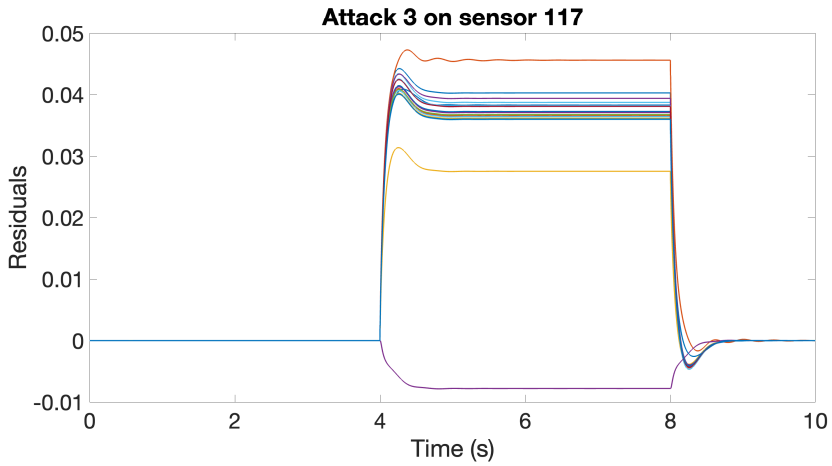

Figure 6: Residuals for attack 3 (multiplicative) on state 221

choose a threshold that correctly identifies the occurrence of the attack and isolates the attacked node.

The code for this simulation is available online[4], as well as the `MAT` file with all generated matrices.

6. Conclusion

We presented a simple LMI-based design for a bank of functional observer residual generators, which detects load-altering attacks. Because of its simplicity, this approach allows to easily extend the design with constraints in the observer's dynamics. Moreover, the design methodology also lends to other uses, such as state-observation with disturbance rejection, fault detection and probably other kinds of attacks.

The main advantage of this method over the ones found in the literature is its simplicity. Other LMI-based methods follow a more convoluted formulation that makes it hard to further constraint and tune. The non-LMI based formulations are mostly direct algebra manipulations that do not lend the power of the LMI-based solution when it comes to controlling the observer's dynamics and using mathematical tricks that further limit the applicability of the techniques.

We tested the method on a power grid model, showing that it allows for a significant reduction in the number of observed states, which translates to a smaller observer system and faster computation times. Future works can explore the generation of observers with different observed paths for the same output to provide redundancy to the system. Another possibility is to use different sets of outputs to observe the same sensor, making it harder to execute stealth attacks that rely on the observer's dynamics.

[4] `https://github.com/acristoffers/SmartGrid`

References

[1] E. Knapp, R. Samani, Applied cyber security and the smart grid implementing security controls into the modern power infrastructure., 2013, oCLC: 1073951674.

[2] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, H. E. Ghazi, Cyber-security in smart grid: Survey and challenges, Computers and Electrical Engineering 67 (2018) 469–482. doi:10.1016/j.compeleceng.2018.01.015.

[3] Office of the National Coordinator for Smart Grid Interoperability, Nist framework and roadmap for smart grid interoperability standards, release 2.0, Tech. rep., National Institute of Standards and Technology, Gaithersburg, MD (2 2012). doi:10.6028/NIST.SP.1108r2.

[4] J. Lai, X. Lu, Z. Dong, R. Tang, X. Li, Robustness-oriented distributed cooperative control for ac microgrids under complex environments 13 (10) 1473–1482. doi:10.1049/iet-cta.2018.5698.

[5] J. Wang, X. Gao, Y. Xu, Intermittent control for demand-side management of a class of networked smart grids 13 (8) 1166–1172. doi:10.1049/iet-cta.2018.5612.

[6] H. Xing, Z. Lin, M. Fu, B. F. Hobbs, Distributed algorithm for dynamic economic power dispatch with energy storage in smart grids 11 (11) 1813–1821. doi:10.1049/iet-cta.2016.1389.

[7] S. E. Shafiei, T. Knudsen, R. Wisniewski, P. Andersen, Data-driven predictive direct load control of refrigeration systems 9 (7) 1022–1033. doi:10.1049/iet-cta.2014.0666.

[8] F. Liberati, E. Garone, A. D. Giorgio, Review of cyber-physical attacks in smart grids: A system-theoretic perspective, Electronics (Switzerland) 10 (10) (2021) 1–39. doi:10.3390/electronics10101153.

[9] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, K. Jones, A survey of cyber security management in industrial control systems 9 52–80. doi:10.1016/j.ijcip.2015.02.002.

[10] F. Mohammadi, Emerging challenges in smart grid cybersecurity enhancement: A review, Energies 14 (5) (2021) 1380. doi:10.3390/en14051380.

[11] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, B. Green, Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems 35 100464. doi:10.1016/j.ijcip.2021.100464.

[12] K. Kimani, V. Oduol, K. Langat, Cyber security challenges for IoT-based smart grid networks 25 36–49. doi:10.1016/j.ijcip.2019.01.001.

[13] BBC, Ukraine power cut 'was cyber-attack' (2017).
URL https://bbc.in/3kT7Ig0

[14] Independent, A cyber attack in saudi arabia failed to cause carnage, but the next attempt could be deadly (2017).
URL https://bit.ly/3AXRyrt

[15] New York Times, U.s. escalates online attacks on russia's power grid (2019).
URL https://nyti.ms/2WoS4Q2

[16] K. Pedramnia, S. Shojaei, Detection of false data injection attack in smart grid using decomposed nearest neighbor techniques, in: 2020 10th Smart Grid Conference (SGC), IEEE, 2020, pp. 1–6. doi:10.1109/SGC52076.2020.9335732.

[17] X. Xiong, D. Sun, S. Hao, G. Lin, H. Li, Detection of false data injection attack based on improved distortion index method, in: 2020 IEEE 20th International Conference on Communication Technology (ICCT), Vol. 2020-Octob, IEEE, 2020, pp. 1161–1168. doi:10.1109/ICCT50939.2020.9295794.

[18] H. Shi, L. Xie, L. Peng, Detection of false data injection attacks in smart grid based on a new dimensionality-reduction method, Computers and Electrical Engineering 91 (2021) 107058. doi:10.1016/j.compeleceng.2021.107058.

[19] Z. Wang, J. Hu, H. Sun, False data injection attacks in smart grid using gaussian mixture model, in: 2020 16th International Conference on Control, Automation, Robotics and Vision (ICARCV), IEEE, 2020, pp. 830–837. doi:10.1109/ICARCV50220.2020.9305398.

[20] J. Khazaei, M. H. Amini, Protection of large-scale smart grids against false data injection cyberattacks leading to blackouts 35 100457. doi:10.1016/j.ijcip.2021.100457.

[21] A. Baniamerian, K. Khorasani, N. Meskin, Monitoring and detection of malicious adversarial zero dynamics attacks in cyber-physical systems, CCTA 2020 - 4th IEEE Conference on Control Technology and Applications (2020) 726–731doi:10.1109/CCTA41146.2020.9206295.

[22] M. Liu, C. Zhao, R. Deng, P. Cheng, W. Wang, J. Chen, False data injection attacks and countermeasures in smart microgrid systems, no. January, Elsevier Inc., 2020. doi:10.1016/b978-0-12-816946-9.00010-4.

[23] J. Kim, H. Shim, A countermeasure against zero-dynamics sensor attack via generalized hold feedback, 2019 58th Annual Conference of the Society of Instrument and Control Engineers of Japan, SICE 2019 (2019) 663–668doi:10.23919/SICE.2019.8859930.

[24] Y. Mao, H. Jafarnejadsani, P. Zhao, E. Akyol, N. Hovakimyan, Novel stealthy attack and defense strategies for networked control systems, arXiv 65 (9) (2019) 3847–3862.

[25] D. Choeum, D. H. Choi, Vulnerability assessment of conservation voltage reduction to load redistribution attack in unbalanced active distribution networks, IEEE Transactions on Industrial Informatics 17 (1) (2021) 473–483. doi:10.1109/TII.2020.2980590.

[26] Z. Liu, L. Wang, Defense strategy against load redistribution attacks on power systems considering insider threats, IEEE Transactions on Smart Grid 12 (2) (2021) 1529–1540. doi:10.1109/TSG.2020.3023426.

[27] R. Kaviani, K. W. Hedman, A detection mechanism against load-redistribution attacks in smart grids, IEEE Transactions on Smart Grid 12 (1) (2021) 704–714. doi:10.1109/TSG.2020.3017562.

[28] S. Lakshminarayana, S. Adhikari, C. Maple, Analysis of iot-based load altering attacks against power grids using the theory of second-order dynamical systems, IEEE Transactions on Smart Grid (2021). doi:10.1109/TSG.2021.3070313.

[29] S. Yankson, M. Ghamkhari, Transactive energy to thwart load altering attacks on power distribution systems, Future Internet 12 (1) (1 2020). doi:10.3390/fi12010004.

[30] P. Xun, P. dong Zhu, S. Maharjan, P. shuai Cui, Successive direct load altering attack in smart grid, Computers and Security 77 (2018) 79–93. doi:10.1016/j.cose.2018.03.009.

[31] Z. Wang, H. He, Z. Wan, Y. Sun, Coordinated topology attacks in smart grid using deep reinforcement learning, IEEE Transactions on Industrial Informatics 17 (2) (2021) 1407–1415. doi:10.1109/TII.2020.2994977.

[32] G.-R. CHEN, Problems and challenges in control theory under complex dynamical network environments, Acta Automatica Sinica 39 (4) (2013) 312–321. doi:10.1016/s1874-1029(13)60032-4.

[33] A. N. Montanari, L. A. Aguirre, Observability of network systems: A critical review of recent results, Journal of Control, Automation and Electrical Systems 31 (6) (2020) 1348–1374. doi:10.1007/s40313-020-00633-5.

[34] L. A. Aguirre, L. L. Portes, C. Letellier, Structural, dynamical and symbolic observability: From dynamical systems to networks, PLoS ONE 13 (10) (2018) 1–21. doi:10.1371/journal.pone.0206180.

[35] N. J. Cowan, E. J. Chastain, D. A. Vilhena, J. S. Freudenberg, C. T. Bergstrom, Nodal dynamics, not degree distributions, determine the structural controllability of complex networks, PLoS ONE 7 (6) (2012). doi:10.1371/journal.pone.0038398.

[36] A. E. Motter, Networkcontrology, Chaos 25 (9) (2015). doi:10.1063/1.4931570.

[37] L. S. Jennings, T. L. Fernando, H. M. Trinh, Existence conditions for functional observability from an eigenspace perspective, IEEE Transactions on Automatic Control 56 (12) (2011) 2957–2961. doi:10.1109/TAC.2011.2160019.

[38] T. L. Fernando, Hieu Minh Trinh, L. Jennings, Functional observability and the design of minimum order linear functional observers, IEEE Transactions on Automatic Control 55 (5) (2010) 1268–1273. doi:10.1109/TAC.2010.2042761.

[39] T. N. Pham, A. M. T. Oo, H. Trinh, Detecting and isolating false data injection attacks on electric vehicles of smart grids using distributed functional observers, IET Generation, Transmission and Distribution 15 (4) (2021) 762–779. doi:10.1049/gtd2.12057.

[40] S. I. Islam, C. C. Lim, P. Shi, Robust fault detection of t-s fuzzy systems with time-delay using fuzzy functional observer, Fuzzy Sets and Systems 392 (2020) 1–23. doi:10.1016/j.fss.2019.03.020.

[41] H. M. Tran, H. Trinh, Minimal-order functional observer-based residual generators for fault detection and isolation of dynamical systems, Mathematical Problems in Engineering 2016 (2016). doi:10.1155/2016/2740645.

[42] H. M. Tran, H. Trinh, P. T. Nam, Functional observer-based fault detection of time-delay systems via an lmi approach, 2015 Australian Control Conference, AUCC 2015 (2015) 194–199.

[43] H. Trinh, T. Fernando, K. Emami, D. C. Huong, Fault detection of dynamical systems using first-order functional observers, 2013 IEEE 8th International Conference on Industrial and Information Systems, ICIIS 2013 - Conference Proceedings (2013) 197–200doi:10.1109/ICIInfS.2013.6731980.

[44] A. N. Montanari, E. I. Moreira, L. A. Aguirre, Effects of network heterogeneity and tripping time on the basin stability of power systems, Communications in Nonlinear Science and Numerical Simulation 89 (2020) 105296. doi:10.1016/j.cnsns.2020.105296.

[45] F. Dörfler, M. Chertkov, F. Bullo, Synchronization in complex oscillator networks and smart grids, Proceedings of the National Academy of Sciences of the United States of America 110 (6) (2013) 2005–2010. doi:10.1073/pnas.1212134110.

[46] T. Nishikawa, A. E. Motter, Comparative analysis of existing models for power-grid synchronization, New Journal of Physics 17 (1) (2015) 015012. doi:10.1088/1367-2630/17/1/015012.

[47] D. Luenberger, Observers for multivariable systems 11 (2) 190–197, conference Name: IEEE Transactions on Automatic Control. doi:10.1109/TAC.1966.1098323.

[48] A. N. Montanari, Observability of dynamical networks, Phd thesis, Universidade Federal de Minas Gerais (UFMG) (2021).

[49] D. Zhao, H. K. Lam, Y. Li, S. X. DIng, S. Liu, A novel approach to state and unknown input estimation for takagi-sugeno fuzzy models with applications to fault detection, IEEE Transactions on Circuits and Systems I: Regular Papers 67 (6) (2020) 2053–2063. doi:10.1109/TCSI.2020.2968732.

[50] C. Rios-Ruiz, G. L. Osorio-Gordillo, H. Souley-Ali, M. Darouach, C. M. Astorga-Zaragoza, Finite time functional observers for descriptor systems. application to fault tolerant control, 27th Mediterranean Conference on Control and Automation, MED 2019 - Proceedings (2) (2019) 165–170. doi:10.1109/MED.2019.8798552.

[51] H. M. Tran, H. Trinh, Distributed functional observer based fault detection for interconnected time-delay systems, IEEE Systems Journal 13 (1) (2019) 940–951. doi:10.1109/JSYST.2017.2759257.

[52] H. Haes Alhelou, M. E. H. Golshan, N. D. Hatziargyriou, A decentralized functional observer based optimal lfc considering unknown inputs, uncertainties, and cyber-attacks, IEEE Transactions on Power Systems 34 (6) (2019) 4408–4417. doi:10.1109/TPWRS.2019.2916558.

[53] K. Emami, T. Fernando, B. Nener, H. Trinh, Y. Zhang, A functional observer based fault detection technique for dynamical systems, Journal of the Franklin Institute 352 (5) (2015) 2113–2128. doi:10.1016/j.jfranklin.2015.02.006.

[54] K. Emami, B. Nener, V. Sreeram, H. Trinh, T. Fernando, A fault detection technique for dynamical systems, 2013 IEEE 8th International Conference on Industrial and Information Systems, ICIIS 2013 - Conference Proceedings (2013) 201–206doi:10.1109/ICIInfS.2013.6731981.

[55] C. Svärd, M. Nyberg, Observer-based residual generation for linear differential-algebraic equation systems, IFAC Proceedings Volumes (IFAC-PapersOnline) 17 (1 PART 1) (2008). doi:10.3182/20080706-5-KR-1001.2367.

[56] C. Weitian, M. Saif, Unknown input observer design for a class of nonlinear systems: An lmi approach, Proceedings of the American Control Conference 2006 (1) (2006) 834–838. doi:10.1109/acc.2006.1655461.