Fault detection with discrete-time measurements: An application for the cyber security of power networks

Erasmia Evangelia Tiniou, Peyman Mohajerin Esfahani, and John Lygeros

***Abstract*— This article concerns an application of a model-based fault detection and isolation (FDI) method for the cyber security of power systems in a realistic framework, where the system dynamics are expressed in continuous-time, whilst system measurements are applied to an FDI filter in discrete-time samples. Towards the development of a tractable approach for high dimensional nonlinear systems, an existing optimization-based technique for residual generator design is reviewed. However, this requires that both system dynamics and measurements are in the same time scale, i.e., either continuous or discrete. To this end, we investigate different variants of discrete-time modeling approaches for state-space systems, specifically tailored to meet the needs of the existing FDI filter design methodology. Finally,the efficiency and limitations of the presented scheme are illustrated through simulation results for a two-area power system network, in which the objective is the diagnosis of a cyber attack at the Automatic Generation Control signal.**

I. Introduction

In modern electric power systems, the interaction of IT infrastructure, such as the SCADA system used for monitoring and protection, with the physical power system renders the system vulnerable not only to operational errors but also to external attacks. Hence, there is an emerging need for cyber-security measures alerting the system operator in case of a signal manipulation. The impacts of such attacks were studied in [11], [12], where it was assumed that an attacker could manipulate the control signal of the secondary control loop existing in power systems, the so called Automatic Generation Control (AGC). The essential objective of AGC is to regulate the system frequency as well as guarantee that power flow in tie lines between interconnected control areas (e.g. different countries) is in accordance with prescheduled values. Indeed, AGC is one of the few control loops that are closed over the SCADA system without human operator intervention, which renders the signal vulnerable. In case of an attack, it was shown that unacceptable power oscillations and frequency deviations are likely to occur causing several detrimental effects. Nevertheless, in case the intrusion of a malicious signal is detected sufficiently fast, the manipulated signal can be disconnected from the system, preventing any further severe damage to the network. Towards this objective, in this article we study the implementation of FDI techniques, as a protection layer mitigating the aforementioned cyber security concern.

Research supported by the European Commission under the project VIKING (FP7-ICT-SEC-2007-1).

The authors are with the Automatic Control Laboratory, ETH Zürich, 8092 Zürich, Switzerland; Emails: etiniou@student.ethz.ch, {mohajerin,lygeros}@control.ee.ethz.ch

A significant variety of model-based FDI methods exists in literature, based on different mathematical models of the monitored system, e.g., in the context of linear dynamics for descriptor models in [15], [5], state-space models [7] and models described by general linear differential-algebraic equations in [3], [13], covering all the previous specific classes of functions. Regarding nonlinear system models, a technique through which the problem of FDI has been tackled is the linearization of the system around an operating point and the treatment of the nonlinear terms as disturbances. The goal is then to decouple these disturbance signals from the residual, with the aid of an unknown input observer [4], [16]. The efficiency of this strategy requires that the assumption of the system operation around an equilibrium point holds in reality. This assumption is quite problematic, since some systems may have a wide operating range, which would cause a significant model-reality mismatch between the plant dynamics and the model employed for FDI. An alternative approach is the perfect decoupling of disturbance signals, [2], [14]. The aforementioned studies essentially require to deal with a high-order differential equation, which however, renders it effectively intractable for large systems with complex dynamics.

The FDI approach presented in this note follows the work of [10], which proposed a novel quadratic programming (QP) based methodology for the design of FDI filters, applied to high dimensional nonlinear systems, achieving a compromise between theoretical soundness and practical feasibility. The proposed FDI scheme suggests a protection layer to enhance the cyber-security of power transmission systems and led to an EU patent sponsored by ETH Zurich [9].

In the model-based FDI framework, the concept of residual generation has a principle role. The FDI task involves the design of a filter generating a diagnostic signal, which indicates the presence of a fault, when applied to all known system measurements, while being insensitive to unknown disturbances. The model-based framework is illustrated in Fig. 1, where signals d, u, f represent the unknown exogenous disturbances, the control inputs and the signals to be detected (faults) respectively, while y_{meas} contains all the available measurements. The signal r denotes the generated residual which diagnoses the presence of fault f. Earlier approaches in the literature only studied cases in which both system dynamics and FDI filter are expressed in the same time-scale evolution, e.g., [13] for linear dynamics and [10] for

an extension to nonlinear systems. However, in practice, an

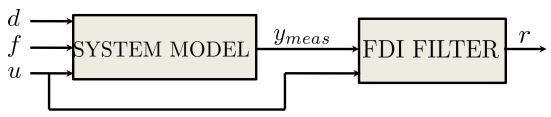


Fig. 1. FDI setup.

FDI filter is applied to known signals, such as measurements and control inputs, which are available in samples. At the same time, the use of continuous-time models in engineering problems such as power systems is highly motivated, since the expression of many governing physical laws is made through differential equations. Hence, in reality, the given precise system model is based on continuous-time dynamics but at the same time, the output signals are only available in samples, measured by a suitable device.

The main focus of the present work is to examine the application of the FDI scheme proposed in [10] for the cyber security of a 2-area power network and extend it in a different system dynamics setting, examining the challenges occurring from the combination of an available continuous-time model and discrete-time measured signals. To this end, we study alternative approaches of discrete-time modeling of the plant, specifically tailored to meet the requirements for the design of an FDI filter. We then examine the efficiency of the aforementioned techniques in this practical framework.

The paper is organized as follows. Section II is concerned with a review of the existing FDI filter design methodology derived in [10], extended to meet the needs of a discrete-time modeling framework. In addition, in Section II, we discuss alternative approaches for discrete-time modeling of state-space nonlinear systems. In Section III, as a case study power system, we provide the mathematical model of the IEEE 118-bus power network, to which the discussed FDI methodology and discrete-time modeling techniques will be implemented towards the objective of detecting an external attack injected in the AGC signal. Simulation results are provided to illustrate the efficiency and practical feasibility of the discussed methods and the paper is concluded in Section IV.

II. FDI FILTER DESIGN METHODOLOGY

A. Mathematical model description

As a mathematical model describing the dynamic behaviour of the system under discussion, we consider the continuous-time, classical nonlinear ordinary differential equation:

$$\begin{aligned}\dot{X}(t) &= e_x\big(X(t), d(t)\big) + AX(t) + B_u u(t) + B_d d(t) + B_f f(t)\\ y_{meas} &= e_y\big(X(t), d(t)\big) + CX(t) + D_u u(t) + D_d d(t) + D_f f(t)\end{aligned} \tag{1}$$

where X represents the internal system states, d the unknown disturbances, f the fault, u the known input signals, y_{meas} the available measurements and e_x, e_y denote the nonlinear terms of the system.

Assumption: The signals d, f and u in (1) are considered as piecewise constant within the sampling intervals, as follows: $d(t) = d(t_\kappa), f(t) = f(t_\kappa), u(t) = u(t_\kappa), \quad \forall t \in [t_\kappa, t_{\kappa+1})$.

B. FDI filter design for discrete-time systems

In this section, we review the FDI methodology for nonlinear systems proposed in [10], but expressed in a discrete-time framework as this will be the main focus of the present work. Along with the system formulation assumed in the aforementioned study, we consider systems modeled by Difference Algebraic Equations (DAE):

$$E(x(\kappa)) + H(q)x(\kappa) + L(q)z(\kappa) + F(q)f(\kappa) = 0, \tag{2}$$

where x represents the vector of unknown signals samples, for instance internal system states and exogenous disturbances, z contains all known signals samples, such as available measurements and control inputs and f denotes the signal to be detected. H, L, F are polynomial matrices in the time-shift operator q and E represents the nonlinear term of the system, as a function of the unknown signal x. It is straightforward to fit a discrete-time state-space model into the form of a DAE (2). We refer to [10] for a similar assertion in the context of continuous-time dynamics, in particular to the connection between ordinary differential equations and differential algebraic equations.

A first principal goal in FDI is that the filter (residual generator) achieves the decoupling of the residual from unknown signals x. To this end, [10] proposed a residual generator with transfer operator of the form $R(q) = a^{-1}(q)N(q)L(q)$, where N is a polynomial vector, of a predefined order d_N, to be designed such that its rows form an irreducible polynomial basis for the left null-space of matrix H. In order for the filter to be physically realizable, stable dynamics $a(q)$ of sufficient order need to be added as denominator[1]. When the filter $R(q)$ is applied to the known signals z, the residual is obtained as:

$$\begin{aligned}r &:= R(q)z = -a^{-1}(q)N(q)(F(q)f + E(x))\\ &=: -a^{-1}(q)(r_f + r_E),\end{aligned} \tag{3}$$

which consists of two terms. The first is related to the faults appearing in the process, defined as $r_f := N(q)F(q)f$, while the second represents the effect of the nonlinear part of the system on the residual, defined as $r_E := N(q)E(x)$.

The authors of [10] proposed a QP-based technique for the design of $N(q)$, which is tractable for high dimensional non-linear systems and focuses on the minimization of the impact of nonlinearities on the residual (r_E in (3)), when the class of disturbances is restricted to certain signatures. In fact, the filter is *trained* to distinguish the normal operation of the system in the presence of these disturbances. The

[1]All the roots are strictly contained in the unit circle.

method is based on a finite dimensional projection in which the projection error decreases as the dimension increases. However, it can be inspected that in the discrete-time framework the projection error can be set to zero with adequate number of basis, due to the finite dimension of functional vector space over a finite horizon. In this way, the procedure introduced for continuous-time dynamics in [10] is simplified as follows. In order to *train* the filter we extract the pattern of the discrete-time nonlinear signal $E(\kappa) = E(x(\kappa T_s))$ for a time horizon $[0, T]$, i.e., for $\kappa = 0, 1, ..., \frac{T}{T_s}$, where T_s denotes the sampling time. Note that this is achieved by considering a collected set of signatures for the system states x, according to the certain disturbance signature that has been assumed. By translating the linear operator q as a matrix left shift operator $D : E(\kappa) \mapsto E(\kappa + 1)$, the error of residual can be written as $r_E(\kappa) = \bar{N}\tilde{D}E(\kappa)$, where $\tilde{D} = [I \; D' \; \cdots \; (D')^{d_N}]'$ and d_N is the chosen degree of filter. Then, we can write the ℓ_2-norm of the signal r_E, as defined in the finite dimensional space equipped with the inner product $\langle f, g\rangle := f'g$:

$$\|r_E\|_{\ell_2}^2 = \bar{N}\tilde{D}\tilde{D}'\bar{N}' =: \bar{N}Q\bar{N}' \tag{4}$$

Note that matrix Q in (4) corresponds to a specific disturbance signature $d(\cdot)$. In practice, it may be required to train the FDI filter for different possible signatures, e.g., $(x_i)_{i=1}^n$.In the same spirit of [10, Remark 3.5] one can compute the corresponding positive matrix Q_i for each signature and arrive at the following QP formulation:

$$\begin{aligned} &\min_{\bar{N}} \bar{N}Q\bar{N}', \qquad Q := \frac{1}{n}\sum_{i=1}^{n} Q_i \\ &s.t. \begin{cases} \bar{N}\bar{H} = 0 \\ \left\|\bar{N}\bar{F}\right\|_\infty \geq 1 \end{cases} \end{aligned} \tag{5}$$

where $\bar{N}$ contains the decision variables representing all the coefficients of the polynomial vector N. For the construction of $\bar{N}$, $\bar{H}$ and $\bar{F}$ one should refer to [10, Lemma 3.2].

It should be highlighted that the optimization problem in (5) is not a standard QP problem but as explained in [10, Remark 3.3], the formulation can be viewed as a family of d_N standard QP programs.

Remark 2.1: In the recent work [8], the authors consider the case where the disturbance signatures are random variables on a prescribed probability space, and the objective is to minimize $\mathbb{E}[||r_E||_{\ell_2}^2]$. To tackle the problem, one can generate n independent identically distributed signatures and invoke the formulation (5) to obtain the filter coefficients. Notice that the solution is naturally stochastic as it depends on generated signature samples. We refer to [8, Sec. 4.C] for the theoretical results and probabilistic performance of the proposed scheme in the aforementioned setting.

C. Discrete-time modeling methods

As explained earlier, before applying the discussed FDI techniques, it is essential to transform the continuous-time model to a discrete-time model of the system. In this section, we discuss three different discrete-time modeling approaches, in which the original continuous-time model is in the form of (1). Let us first clarify that the objective of the discussed discrete-time modeling approaches is not to precisely mimic the dynamic behavior of the continuous time system. Instead, they are tailored to meet the needs of a residual generator design in the FDI framework. Furthermore, for a continuous-time system modeled by (1), let us define the class of discrete-time nonlinear state-space models that will be considered, as:

$$\tilde{X}(t_{\kappa+1}) = \tilde{e}_x(t_k) + \tilde{A}\tilde{X}(t_k) + + \tilde{B}_u u(t_k) + \tilde{B}_d d(t_k) + \tilde{B}_f f(t_k),$$

where $\tilde{X}$ denotes the discrete-time state signal, $\tilde{A}, \tilde{B}_u, \tilde{B}_d, \tilde{B}_f$ represent the discrete-time versions of the corresponding continuous-time matrices and $\tilde{e}_x(t_k)$ is the discrete-time analog of the nonlinear term in (1). The objective is to determine both the particular matrices and the discrete version $\tilde{e}_x(t_k)$, that will allow us to obtain a discrete-time model for the FDI approach in Section II-B.

1) Approach 1: : As a first approach we consider the classical forward Euler approximation, where the discrete-time matrices and discrete-time version of the nonlinear signal are expressed by:

$$\begin{aligned} &\tilde{A} := T_s A + I \qquad \tilde{B}_d := T_s B_d \qquad \tilde{B}_f := T_s B_f \\ &\tilde{B}_u := T_s B_u \qquad \tilde{e}_x(t_k) := T_s e_x\big(X(t_k)\big) \end{aligned} \tag{6}$$

In the above equation, T_s denotes the sampling time, which has a considerable impact on the efficiency of this method. In particular, T_s has to be sufficiently small, such that the approximation of the continuous-time dynamics is satisfactory. One may observe that even in the case of linear dynamics, the Euler discretization is not exact and the performance substantially deteriorates as the sampling time increases. To address this issue, we propose the following heuristic approach.

2) Approach 2: : For this approach, let us first define the following operators for an arbitrary matrix W, given matrix A and sampling time T_s:

$$[W]^1 := e^{WT_s}, \qquad [W]^2 := \int_0^{\bar{T}} e^{A(T_s-\tau)} W d\tau, \tag{7}$$

By using the above matrix transformations, we define the corresponding components of the discrete-time system, as we did for Approach 1, as:

$$\begin{aligned} &\tilde{A} := [A]^1 \qquad \tilde{B}_d := [B_d]^2 \qquad \tilde{B}_f := [B_f]^2 \\ &\tilde{B}_u := [B_u]^2 \qquad \tilde{e}_x(t_k) := T_s e_x(X(t_k)) \end{aligned} \tag{8}$$

Indeed, the above discrete-time matrices correspond to the analytical solution for the discretization of the linearized version of (1), which is based on properties of the matrix exponential. In (8), the linearized part of the model is enriched with the discrete-time version of e_x. As we observe, the matrix $(T_s A + I)$ appearing in (6) is only the first order Taylor series of $[A]^1$. Moreover, the discrete-time modeling of the nonlinear term in (8) is identical to (6).

3) Approach 3: The reasoning behind the third approach is that the nonlinearity e_x appearing in (1) can be considered as an *extra* input in the linearized system, for which the corresponding matrix is just the identity matrix, denoted by $B_e := I$. The discrete-time matrices $\tilde{A}$, $\tilde{B}_d$, $\tilde{B}_f$ and $\tilde{B}_u$ are the same as the ones obtained with Approach 2 (8). However, the discrete-time version of e is given by:

$$\tilde{e}_x := [B_e]^2 = [I]^2, \tag{9}$$

which essentially aims to improve the precision of transition from continuous to discrete-time for the nonlinear term. Approach 3 seems to be the most precise one, though the scheme is not yet exact, as the error signal e_x is not necessarily piece-wise constant within the sampling intervals.

The above discrete-time modeling approaches present different levels of precision regarding the discretization of the linear and nonlinear part of a continuous state space equation. The first approach, namely the classical Euler approximation, may achieve to describe the system dynamics only if T_s is significantly small, even for linear systems. Approach 2 uses the same form of the discrete-time nonlinear term as Euler method, but it improves the accuracy for the linear part of the system. Indeed, it is the exact discrete-time modeling of a linear state space system when e_x vanishes, but its accuracy decreases as the nonlinear term contribution increases. Finally, in Approach 3 the goal is to improve the precision of the discrete-time modeling of the nonlinear signal e_x.

III. Multi-machine 2-area power network

In order to validate the efficiency of the discussed methodology towards the cyber security of power systems, we employ the model of an IEEE 118-bus network: a multi-machine system consisting of 19 generators, 177 lines, 99 load buses, 7 transmission level transformers and 19 extra transformers for the connection of the medium-voltage generator buses with the high voltage transmission buses. The model is obtained from the analysis made in [10], in which the system is arbitrarily divided into two control areas, representing, e.g., two interconnected countries. The generators are equipped with primary frequency control, while each area is governed by an AGC scheme, aiming at adjusting the set points at particular generators appropriately, as already explained above. The system is based only on frequency dynamics, whereas voltage dynamics are neglected. According to the analysis of [10], after a node elimination procedure, we result in a 59th-order nonlinear continuous-time model of the form:

$$\begin{aligned} \dot{X}(t) &= h(X(t)) + B_d d(t) + B_f f(t) \\ y_{meas} &= CX(t), \end{aligned} \tag{10}$$

where $X(t) = [\delta_1^{19}, f_{r,1}^{19}, P_{m,a1}, P_{m,a2}, \Delta P_{agc1}, \Delta P_{agc2}]'$ denotes the internal system states vector, composed by the rotor angles and the frequencies at the generators, the generated mechanical powers by generators in Area 1 and Area 2 and the AGC control signals in the two areas. In the FDI context, the disturbance vector $d(t) = \Delta P_{load1}^{19}$ represents the unknown load deviations that may occur at the generators, ΔP_{agc1} and ΔP_{agc2} are the AGC control inputs for areas 1 and 2 respectively and $y_{meas}(t) = [f_{r,1}^{19}, P_{m,a1}, P_{m,a2}]'$ contains the measured system states. The fault vector $f(t) = [f_1, f_2]'$ corresponds to malicious signals superimposed in the AGC control input of Area 1 and Area 2 respectively, representing possible cyber attacks in the network. In this work, we consider the case where one of the two areas has been attacked but not both of them simultaneously. Therefore, we consider either $f_1 = U$ or $f_2 = U$ as a fault additive to AGC, which is crucial to be detected sufficiently fast.

As explained earlier, the principal goal of this paper is to implement FDI techniques in a practical framework, where the available power system model is in continuous-time, whilst the FDI filter is given the measured signals, provided by a measurement device at a specific sampling rate T_s. Hence, in order to employ the discussed FDI methodology, we first write (10) in the form of (1), where $A = \frac{\partial h}{\partial X}$ results from the linearization around the operation point X_e, $e_x(X) = h(X) - A(X - X_e)$ represents the nonlinear term of the system and B_u, D_u, D_d, D_f are all zero matrices. The next step is to bring the system into a discrete-time state space representation form by utilizing the discussed discrete-time modeling techniques in Section II-C and finally into the form of (2).

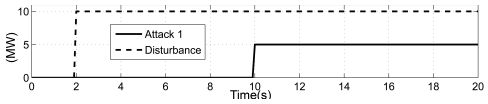
A. Simulation results

In the current section, we provide simulation results from the application of the QP-based technique and the discrete-time modeling approaches discussed in the previous sections, for the detection of attacks in the test case power system. The designed FDI filter is provided with all available system measurements and is expected to indicate the undesirable manipulation of the AGC signal by producing a protective alarm, whilst being insensitive to acceptable load deviations-disturbances that happen on a daily basis in the power network. In the following simulation results the sampling time is $T_s = 0.1$ sec and the degree of the filter is fixed to $d_N = 7$. For the solution of the QP (5) optimization problem, we have used the YALMIP toolbox [6].

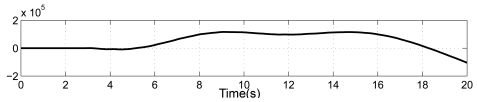
1) Disturbances modeled by step signals: To begin with, we consider the case in which an attack $U = 5$MW is injected in Area 1 at 10s, while one of its nodes is subjected to a step load deviation $\Delta P_{load} = 10$MW at 2s, both shown in Fig. 2(a). Hence, for the QP formulation (5) of the problem, the disturbance signals are considered to be step functions of certain amplitude.

We aim to minimize this undesirable impact of the nonlinearities on the residual, with the aid of the QP formulation (5). By considering step functions for the load deviation (disturbance) signals, appearing individually at each node-generator, we extract a number of signatures of the nonlinear signal E within a time horizon $[0, 10]$s.

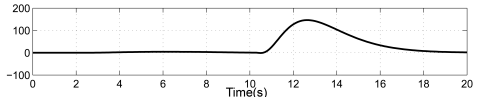
The simulation results presented in Fig. 2(b), 2(c), 2(d) describe the dimensionless residual signal, generated when the (5) is applied in combination with the three discrete-time modeling approaches, (6), (8), (9) respectively. In detail, the QP formulation in which Approach 1, (6), is used as discretization method, does not succeed in indicating the attack. This is not surprising, since Euler approximation with the particular size of discretization step is not sufficient to provide considerable information on the dynamics of the system. On the contrary, the results are quite promising when we employ Approaches 2, (8), and 3, (9), and the QP formulation for the FDI filter design. The residual which is generated is sensitive to the attack and at the same time, it is significantly decoupled from the contribution of the nonlinear terms in presence of disturbances.



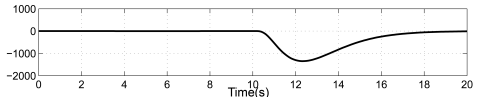
(a) Disturbance at node 15 and AGC attack in Area 1



(b) Residual of QP-Approach 1



(c) Residual of QP-Approach 2



(d) Residual of QP-Approach 3

Fig. 2. Results of the FDI filter for step disturbances ΔP_{load}

2) Disturbances modeled by stochastic sinusoidal signals: In order to design an FDI filter which can be efficient in a more realistic framework, we extend the considered functions for ΔP_{load} from step functions to stochastic signals. In particular, we are motivated by the fact that in a power network, small imbalances between load and generation arise continuously, appearing as disturbances at the system's nodes. These disturbances are caused by different reasons, such as load fluctuations, load prediction errors, distributed generation sources and electricity trading. In specific, based on realistic data of disturbances in power systems, provided in [1, p. 59], we consider disturbances modeled by the superposition of sinusoidal functions in the form:

$$\Delta P_{load} = \alpha + \sum_{i=1}^{n_{sin}} g_i sin(2\pi f_i t + \varphi_i), \qquad (11)$$

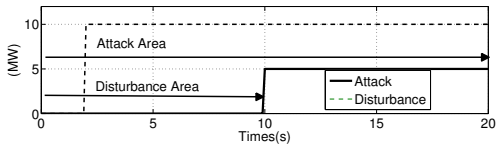
where $\alpha, g_i, f_i, \varphi_i, n_{sin}$ are random variables, which are assumed to belong to certain bimodal distributions with a high and a low frequency mode.

In the following, we provide simulation results for a number of independent experiments, in which an FDI filter is designed to diagnose a fault occurring in Area 1, in the presence of random disturbances at the generators. However, before proceeding to the simulation results, let us first describe the way we use to evaluate the performance of the designed filter, when tested in a large number N of experiments for random disturbance signals. Fig.3(a) shows a sample case, in which a disturbance ΔP_{load} occurs at a generator-node and an AGC attack U is injected in the system, both expressed in MW. In the particular figure, two regions are indicated by arrows. The region denoted as *Disturbance Region* contains the part of the residual signal from $t = 0$s to the time instant where the attack occurs, whereas the region denoted as *Attack Region* contains the residual signal within the whole time interval of observation. For evaluating the performance of the filter, we define the following quantity, which is essentially dimensionless:

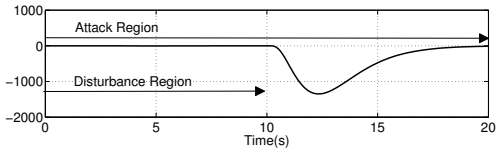
$$ratio = \frac{max(r_{Disturbance\ Region})}{max(r_{Attack\ Region})} \in [0, 1]$$

Ideally, the FDI filter generates a residual with small ratio values when a attack is present. In particular, in a case of successful fault detection, the filter succeeds in distinguishing the attack from the unknown disturbances, as shown in Fig.3(b) where $ratio \ll 1$. In fact, perfect decoupling of the disturbances and the contribution of the nonlinear terms results in $ratio \approx 0$. On the contrary, for an unsuccessful case it holds that $ratio \approx 1$, as shown in Fig. 3(c). In practice, a fault can be detected by the comparison of the ratio, which is monitored in real-time, with a threshold function, which can be a predefined constant tailored to the application. A ratio value exceeding this threshold represents normal operation of the system, whereas a lower value indicates the presence of an attack. Indeed, the size of the observation period is related to how rapidly fault detection is achieved.

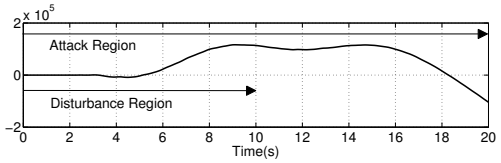
Based on the aforementioned evaluation method and in view of the *Remark 2.1*, the FDI filter is tested in $N = 1000$ independent experiments, in which 2 randomly selected generators-nodes in the network are subjected to random disturbances at 2s, generated by (11), when an attack signal of 5 MW is injected to the AGC of Area 1 at 10s. In all experiments, we consider that the observation period is until 3s after the attack, in which it is desired that the filter diagnoses the fault. Fig. 4 shows the ratio values for FDI filters designed with the aid of the QP formulation (5). In particular, Fig. 4(a) and 4(b) show that QP formulation with both discrete-time modeling approaches 2, (8), and 3, (9), result in successful FDI filters in all N experiments. In fact, the comparison of the threshold value with the ratio obtained by a residual signal declares the occurrence or absence of an attack. An example would be to set the threshold value at 0.3, for which we observe that the success rate of the above FDI filters is 100%. Fig. 5(a) and 5(b) illustrate the results of filters designed for $T_s = 0.5$s in terms of ratio



(a) Regions used for filter performance evaluation

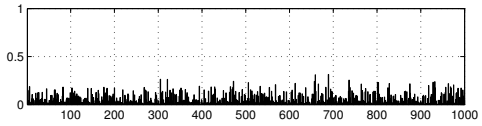


(b) Example residual of successful filter ($ratio \ll 1$)

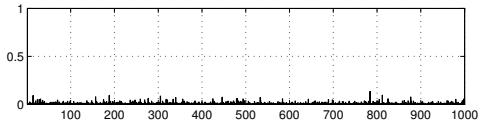


(c) Example residual of unsuccessful filter ($ratio \approx 1$)

Fig. 3. Evaluation of FDI filter performance



(a) Ratio of filter obtained by QP and Approach 2



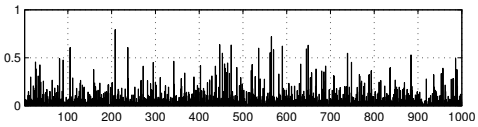
(b) Ratio of filter obtained by QP and Approach 3

Fig. 4. Results for random ΔP_{load} with $T_s = 0.1s$ (N=1000 experiments)

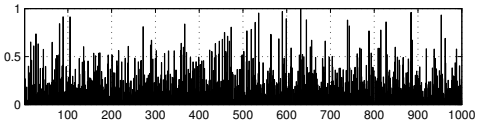
values, where it can be observed that sampling time has a considerable effect on the FDI performance. Indeed, as the sampling time increases, the results deteriorate due to less information provided to the filter. Nevertheless, a significant rate of success can be observed by adjusting the threshold value appropriately.

IV. Conclusion

We investigated a model-based FDI method for the cyber security of power networks, based on an existing QP-based technique, extending it in a realistic framework to tackle the difficulties occurring from the combination of continuous-time dynamics of the monitored system and discrete-time measurements. Different variants of discrete-time modeling approaches were investigated, enabling us to utilize the discussed FDI method to establish a transition from the original continuous-time model to the required discrete-time expression. Finally, simulation results illustrate the efficiency of the discussed technique, through the application to the test case system of a two-area power network.



(a) Ratio of filter obtained by QP and Approach 2



(b) Ratio of filter obtained by QP and Approach 3

Fig. 5. Results for random ΔP_{load} with $T_s = 0.5s$ (N=1000 experiments)

References

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

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

[3] E. Frisk and M. Nyberg, *Residual generation for fault diagnosis of system described by linear differential-algebraic equations*, ISY, Linkoping, Sweden, Technical Report. [Online], (2005).

[4] 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.

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

[6] 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.

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

[8] P. Mohajerin Esfahani and J. Lygeros, *A tractable fault detection and isolation approach for nonlinear systems with probabilistic performance*, Manuscript to be submitted for publication, (2013). [Current draft]. Available: http://control.ee.ethz.ch/index.cgi?page=publications;action=details;id=4344.

[9] P. Mohajerin Esfahani, M. Vrakopoulou, G. Andersson, and J. Lygeros, *Intrusion detection in electric power networks*. Patent applied for EP-12005375, filed 24 July 2012.

[10] ———, *A tractable nonlinear fault detection and isolation technique with application to the cyber-physical security of power systems*, in 51th IEEE Conference Decision and Control, 2012. [Online]. Full version: http://control.ee.ethz.ch/index.cgi?page=publications;action=details;id=4196.

[11] P. Mohajerin 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] 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.

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

[15] 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.

[16] 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.