A Robust Policy for Automatic Generation Control Cyber Attack in Two Area Power Network

Peyman Mohajerin Esfahani, Maria Vrakopoulou, Kostas Margellos,
John Lygeros and Göran Andersson

Abstract— **This paper develops methodologies to robustly destabilize a two-area power system in the case of a cyber attack in the Automatic Generation Control (AGC). In earlier work reachability methods were used to establish conditions under which an attacker can cause undesirable behavior by interrupting the AGC signals and introducing an appropriate fake signal. In this paper we investigate how to robustify this approach to deal with practical situations where the attacker only has partial information about the parameters of the power system and the values of its states. We first propose an open loop procedure, based on Markov Chain Monte Carlo optimization, to identify an optimal attack signal. Motivated by the fact that the results are very sensitive to parameter uncertainty, we develop a systematic algorithm, based on feedback linearization, to construct a feedback policy that an intruder may use to disrupt the network. The numerical simulations demonstrate the effectiveness of the resulting policy, as well as its robustness with respect to modeling uncertainty and imperfect state information.**

I. INTRODUCTION

The tight coupling between large power systems and SCADA systems gives rise to security issues [1]–[4]. An intruder into the IT infrastructure could gain access to various sensors and control signals, and through manipulating them disrupt wide areas of the power system. In this paper, two simulation based methodologies are proposed, that assess the impact of a cyber attack at the Automatic Generation Control (AGC) signal, the only automatic closed loop between the IT and the power system of a control area [5], [6].

We consider a two-area power system and analyze its behavior in the case where an attacker has gained access to the AGC signal of one of the two areas and is able to inject any undesirable input to the system. The task of identifying the worst attack pattern by evaluating the impact that it may have in the two area system is translated into an optimization problem. In earlier work [7], reachability methods were used to establish conditions under which an attacker can cause security issues by gaining access of the AGC signal. In this paper we investigate how to robustify this approach so as to deal with practical situations where the attacker has only partial knowledge of the state and the parameters of the system. Two different approaches are then used so as to solve the resulting problem.

The first method is an iterative process based on Markov Chain Monte Carlo (MCMC) optimization. That way, apart from coming up with a feasible (in terms of violation the constraints) attack trajectory, we are also able to cause a more specific system disturbance by optimizing a cost criterion. Since it is a randomized procedure even non convex objective functions can be used. The drawback of this scheme is that it provides only an open loop solution and hence cannot be efficiently used in case of model mismatching.

The second method overcomes this difficulty providing a feedback solution by linearizing the system. In the new coordinates a linear feedback with constant gain is used where the gain is optimally selected so as to ensure that the closed loop system will be unstable. For this purpose a variant of MCMC is used.

In Section II the physical description and the mathematical model of the two-area power system is presented, and also a brief introduction to Monte Carlo optimization methods is provided. Section III introduces the first approach, based on an open loop strategy to identify an attack signal, and provides the corresponding simulation results. In Section IV a systematic algorithm to construct feedback policy is proposed. This chapter includes also a short introduction to feedback linearization and the implementation details of an extended Luenberger nonlinear observer. In the end of this section simulation results that validate the robustness and the efficiency of the proposed scheme are presented. Finally in Section V we provide some concluding remarks and directions for future work.

II. SYSTEM DESCRIPTION AND MATHEMATICAL MODEL

A. Modeling of the Two-Area Power System

Consider the system of Fig. 1, which consists of two interconnected control areas, each one equipped with its own AGC, connected by a tie line of reactance X. According to [8], [9], each area is approximated by an equivalent generating unit equipped with primary frequency control. Consider now the case of a cyber attack in the second area. We assume that the attacker has disabled the AGC in this area and can instead inject an input $\mathbf{u}$, which acts as a bounded disturbance to our system.

The model of the two-area power system can be described by the following set of differential equations (see [7] for

Peyman Mohajerin Esfahani, Kostas Margellos 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. email: {mohajerin, margellos, 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. email: {vrakopoulou, andersson}@eeh.ee.ethz.ch

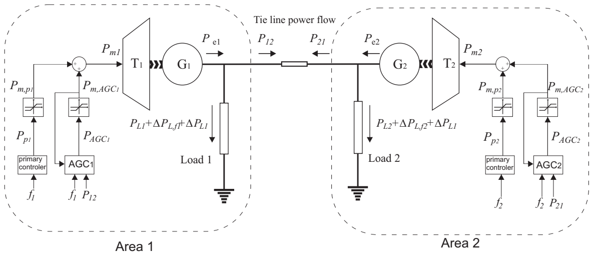

Fig. 1. Two-Area Power System with AGC

details).

$$
\begin{aligned}
\Delta\dot{f}_1 &= \frac{f_0}{2H_1S_{B_1}}\Big(\Delta P_{m,p_1} + \Delta P_{m,AGC_1} - \frac{1}{D_{l_1}}\Delta f_1 - P_T\sin(\Delta\phi + \phi_0) + P_{0_{12}}\Big),\\
\Delta\dot{f}_2 &= \frac{f_0}{2H_2S_{B_2}}\Big(\Delta P_{m,p_2} + \mathbf{u} - \frac{1}{D_{l_2}}\Delta f_2 + P_T\sin(\Delta\phi + \phi_0) - P_{0_{12}}\Big),\\
\Delta\dot{\phi} &= 2\pi(\Delta f_1 - \Delta f_2),\\
\Delta\dot{P}_{AGC_1} &= \Big(\frac{1}{D_{l_1}}\frac{C_{p_1}f_0}{2S_1H_1S_{B_1}} - \frac{1}{S_1}\frac{1}{T_{N_1}}\Big)\Delta f_1\\
&\quad - \frac{C_{p_1}f_0}{2S_1H_1S_{B_1}}\Delta P_{m,p_1} - \frac{C_{p_1}f_0}{2S_1H_1S_{B_1}}\Delta P_{m,AGC_1}\\
&\quad - \Big(\frac{1}{T_{N_1}} - \frac{C_{p_1}f_0}{2S_1H_1S_{B_1}}\Big)(P_T\sin(\Delta\phi + \phi_0) - P_{0_{12}})\\
&\quad - 2\pi C_{p_1}P_T(\Delta f_1 - \Delta f_2)\cos(\Delta\phi + \phi_0) - \frac{K_{a_1}}{T_{N_1}}p_1. \qquad (1)
\end{aligned}
$$

where $\Delta P_{p_i} = -1/S_i$ for i=1,2 and due to saturation we have

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

$$
\Delta P_{m,AGC_1} = \begin{cases} \Delta P_{AGC_1}^{min} & \text{if} \;\; \Delta P_{AGC_1} \le \Delta P_{AGC_1}^{min} \\ \Delta P_{AGC_1} & \text{if} \;\; \Delta P_{AGC_1}^{min} < \Delta P_{AGC_1} < \Delta P_{AGC_1}^{max} \\ \Delta P_{AGC_1}^{max} & \text{if} \;\; \Delta P_{AGC_1} \ge \Delta P_{AGC_1}^{max} \end{cases}
$$

$$
p_1 = \begin{cases} 0 \;\; \text{if} \quad \Delta P_{AGC_1}^{min} < \Delta P_{AGC_1} < \Delta P_{AGC_1}^{max} \\ \Delta P_{AGC_1} - \Delta P_{m,AGC_1} \qquad \text{else} \end{cases}
$$

Since we are interested in the impact of unreasonable changes of the AGC signal, no changes at the actual load of the areas are considered ($\Delta P_{L_i} = 0$) in the above model. Moreover, the scheduled transferred power in the tie line was not considered to be zero. So the deviation of the power flow on the tie-line from area 1 to area 2 is described by $\Delta P_{12} = P_T\sin(\Delta\phi+\phi_0)-P_{0_{12}}$, where ϕ_0 is the angle difference that corresponds to the scheduled transferred power i.e. $P_{0_{12}} = P_T\sin(\phi_0)$.

The numerical data used for the examples are based on Table I. The generators inertia, H_i, and schedule power, $P_{0_{12}}$, will be determined in the following sections. In the rest of paper, the model parameters $[H_1, H_2, \phi_0]$ are denoted by the vector w. Having defined the state vector $x = [x_1\ x_2\ x_3\ x_4]^T = [\Delta f_1\ \Delta f_2\ \Delta\phi\ \Delta P_{AGC_1}]^T$, the system (1) is described by

$$
\dot{x} = f(x, w) + g(x, w)u, \qquad (2)
$$

where the functions $f(x, w)$ and $g(x, w)$ can be simply obtained from the model presented in (1).

S_{B_i}	f_0	D_{l_i}	S_i	C_{p_i}	T_{N_i}
10 GW	50Hz	$\frac{1}{200}MW/Hz$	0.002Hz/MW	0.1	30
$\Delta P_{AGC_i}^{max}$	$\Delta P_{AGC_i}^{min}$	$\Delta P_{p_i}^{max}$	$\Delta P_{p_i}^{min}$	P_T	K_a
350MW	−350MW	75 MW	−75 MW	1000 MW	100

TABLE I

Parameter values for the two area power system

B. Safety Considerations

The frequency control outlined in the previous part is vital to the satisfactory performance of the power system. The controllers try to keep the frequency to its nominal value because large deviations could damage the power system devices. This action may in the end jeopardize the stability of the whole system and in the worst case lead to load shedding, generator tripping, and system blackout. In normal operation frequency deviation should not exceed 1.5Hz. For instance, maximum acceptable frequency decrease for thermal power plants is around 1.5Hz and any further decrease will result in the disconnection of the plant. This lack of generation will lead to further decrease of the frequency and through similar cascading actions the whole system may collapse. Hence we consider the system to be safe when the state trajectories of (2) lie inside the following safe set of the state space

$$
\begin{aligned}
x_1 &\in [-1.5, +1.5],\\
x_2 &\in [-1.5, +1.5].
\end{aligned} \qquad (3)
$$

One of the main challenges is to identify whether there exists an attack pattern that could lead the system to collapse. In earlier work [7], reachability was used to assess the impact of the intrusion in the AGC of a two-area power network. Based on the results of [7], an attacker could potentially use the theoretically optimal control signal obtained by the reachability analysis and steer the system trajectory towards the unsafe state space region. However, due to numerical limitations, the reachability approach is not sufficiently robust to state space discretization, making it difficult to accurately compute the optimal control signal and efficiently apply it on-line. Therefore, in this paper we provide two different control approaches, open and closed loop, to construct a suboptimal attack policy. The former is based on randomized optimization, whereas the latter is based on feedback linearization with control gains selected by Monte Carlo optimization.

C. Optimization Algorithm

In this section we describe a simulation based procedure to approximate optimizer of a bounded objective function. Let $J : \mathbf{\Theta} \to [0\ 1]$ be an objective function, where $\mathbf{\Theta} \subset \mathbb{R}^n$ is a bounded set. Since any bounded optimization criterion can be scaled to take values in interval [0 1], we can assume that J takes values in this range.

We consider equilibrium distributions defined by probability density functions proportional to $[J(\theta)+\delta]^I$ where I and δ are two positive parameters. Here δ is an offset which guarantees that the equilibrium densities are always positive and

I^{-1} plays the role of temperature in the sense of simulated annealing; as I increases the function $[J(\theta)+\delta]^I$ becomes increasingly peaked around the global maximizers. We use θ_k to denote the state of the chain and a conditional density $p_\theta(\cdot|\theta_k)$ is the proposal distribution and is chosen by the user providing that $\text{supp}J \subset \bigcup_{\theta\in\text{supp}J} \text{supp} \quad p_\theta(\cdot|\theta)$. The only requirement for the applicability of this approach is to extract a random variable $\bar{\theta}$ with conditional distribution $p_\theta(\cdot|\theta_k)$ and evaluate $J(\bar{\theta})$ pointwise. The problem of maximizing the optimization criterion is then reformulated as the problem of estimating the optimal points from extracted samples concentrated around them. These extractions are obtained through Monte Carlo Markov Chain (MCMC) simulation that relies on extracting a random variable $\bar{\theta}$ whose distribution has modes that coincide with the optimizers of J [10].

This algorithm is called Metropolis-Hastings which is associated with the objective function $[J(\theta)+\delta]^I$ and conditional distribution $p_\theta(\cdot|\theta_k)$. The algorithm produces a Markov chain θ_k as follows:

Algorithm 1 Metropolis-Hastings

```
Set $k = 0$ and $\theta_k \in \mathbf{\Theta}$.
Extract a new state $\bar{\theta} \sim p_\theta(\cdot|\theta_k)$.
Compute the acceptance probability rate
    $$\rho = \min\{1, \frac{p_\theta(\theta_k|\bar{\theta})}{p_\theta(\bar{\theta}|\theta_k)} \frac{[J(\bar{\theta})+\delta]^{I_k}}{[J(\theta)+\delta]^{I_k}}\}$$
Set
    $$\theta_{k+1} = \begin{cases} \bar{\theta} & \text{with probability } \rho \\ \theta_k & \text{with probability } 1-\rho \end{cases}$$
Set $k = k + 1$.
```

One can show that the Markov chain constructed through the above algorithm converges to the stationary distribution proportional to $[J(\theta)+\delta]^I$ [10]. On a continuous domain the equilibrium distributions are specified by probability densities [11].

III. OPEN LOOP POLICY

In this method we seek to find an open loop input signal $\mathbf{u}(t)$ that forces the trajectories of (2) to violate the safety margins. Figure 2 depicts the open loop strategy of the attacker where w and w_0 denote, respectively, the real model parameters and nominal values w_0.

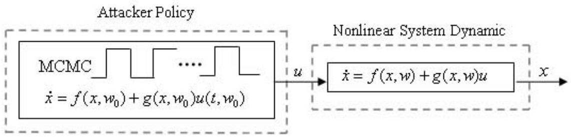
Attacker Policy
MCMC
····
$\dot{x} = f(x, w_0) + g(x, w_0)u(t, w_0)$
u
Nonlinear System Dynamic
$\dot{x} = f(x, w) + g(x, w)u$
x

Fig. 2. Block diagram of open loop policy for the attacker

A. Attack signal generated by MCMC optimization

Due to the input affine dynamics (2) and the input bounds, we restrict the search of $\mathbf{u}(t)$ to the class of piecewise constant input trajectories of the form

$$\mathbf{u}(t) = u_\kappa, \quad \frac{T}{N}\kappa \le t < \frac{T}{N}(\kappa+1) \quad \kappa = 0, ..., N-1, \qquad (4)$$

where $u_\kappa \in \{-350, 350\}$, T denotes the optimization horizon and T/N is the time discretization step. Therefore, finding an optimal control strategy for the attacker to violate the frequency constraints (3) is relaxed to a nonlinear optimization problem over the discrete domain $\mathbf{\Theta} = \{-350, 350\}^N$ with 2^N variables.

Here we resort to an optimization method based on a variant of the Metropolis-Hastings algorithm introduced in Section II-C, with $J_1 = e^{\int_0^T x_2^2 dt}$, $I_\kappa = 5$ and $\delta = 0$.

Problem Statement. *Determine the decision variables* $(u_1, \cdots, u_N) \in \mathbf{\Theta}$ *of (4) to maximize the cost function* J_1 *subject to the system dynamic (2).*

B. Simulation Results for the Open Loop Policy

Based on the algorithm described in the Section II-C, we attempt to obtain a suboptimal policy (4) to maximize J_1. In the first simulation, we assume that the attacker has perfect knowledge of the power network i.e. $w = w_0$. In the second part, we consider some parameter mismatching and investigate how robust the attacker's policy is under these parameter uncertainties.

*1) **Perfect Model**:* We consider a scenario with equally sized areas, both with the same inertia, $H_1 = 5, H_2 = 5$, and scheduled power exchange equal to $P_{0_{12}} = -500MW$ through the tie line. We assume the attacker has full knowledge of the power network ($w = w_0$) with the nominal model parameter values $w_0 = [H_1, H_2, \phi_0] = [5, 5, -30°]$. For the simulations, the optimization horizon T is $40sec$ and the number of decision variable N is 40. We performed in total 82306 iterations until the accepted states of the chain were 50000. The ratio between accepted and total states of the chain is 0.61.

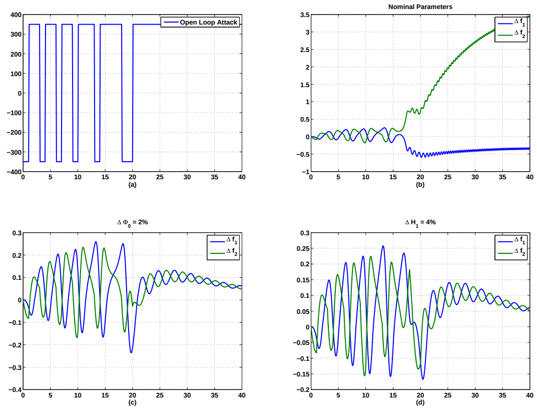

Fig. 3. (a) Open loop policy, (b) Frequency trajectories for perfect model, (c) Frequency trajectories for imperfect model with $\Delta\phi_0 = 2\%$, and (d) Frequency trajectories for imperfect model with $\Delta H_1 = 4\%$

Fig 3.a depicts an open loop strategy for the attacker, obtained through the MCMC optimization method. Fig 3.b

depicts the frequency response of the two areas. Clearly, the impact of the suboptimal attack signal is extremely severe. The swings of the transferred power on the tie line will result in triggering the out of step relay. If the system was not equipped with such a protection scheme, the generators of the second area would start to trip by the time that the frequency of that area would exceed the safety margins. The latter could lead in cascading failures and even in a wide-area blackout.

*2) **Model with Parameter Uncertainty**:* In Fig 3.*c* and 3.*d*, we assume that the attacker does not have perfect information of the system. Hence, there will be a small parameter mismatching, for scheduled power $P_{0_{12}} = -484.8MW$ and inertia time constant $H_1 = 4.8sec$ respectively. The parameter uncertainty for the scheduled power is considered as a small perturbation in the voltage phase deviation $\Delta\phi_0 = 2\%$, whereas for the inertia time constant of the first area is equal to $\Delta H_1 = 4\%$. It is clear that the open loop strategy is extremely sensitive to such a model mismatching and hence the open loop policy does not serve practically as an efficient solution. Motivated by this, we seek to find a feedback strategy robust to model mismatching.

IV. FEEDBACK POLICY

In this section, we propose a class of feedback strategy to derive a suboptimal control input for the attacker to disrupt the system. The attacker, based on feedback linearization and the Metropolis-Hastings algorithm, can construct an attack policy **u**. Having some output measurements y, the attacker can build up a nonlinear observer to estimate the states of the system. Given that the attacker has imperfect knowledge of the system parameters, let w_0 as in the previous section denote the nominal parameter values. The procedure of designing the feedback policy is depicted in Figure 4.

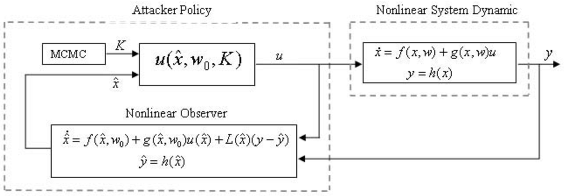

Fig. 4. Block diagram that indicates the construction of the feedback attack policy

A. Feedback Linearization

In this section, we design a feedback control law **u** using feedback linearization. The feedback gain can be optimized by tuning some constant parameters so as to meet the attacker's goal. The basic approach of input-output linearization is simply to differentiate the output function repeatedly until the input **u** appears. Considering the input affine nonlinear system (2) and defining an arbitrary output $y = l(x)$, the differentiated output can then be rewritten using the following expression

$$\begin{aligned} y &= l(x) = L_f^0 l(x), \\ \tfrac{dy}{dt} &= L_f^1 l(x), \\ &\vdots \\ \tfrac{d^{\rho-1}y}{dt^{\rho-1}} &= L_f^{\rho-1} l(x), \\ \tfrac{d^{\rho}y}{dt^{\rho}} &= L_f^{\rho}(l(x)) + L_g L_f^{\rho-1} l(x)u. \end{aligned}$$

where $L_f^1 l(x) = \frac{\partial l}{\partial x} f$ is called the Lie Derivative of l with respect to f.

Note that since the whole idea of this section is to derive a feedback policy, the output $y = l(x)$ does not have to be practically justified. Moreover, due to the saturation of primary and secondary loop control in (1), the vector field $f(\cdot, w)$ is not smooth and consequently $L_f^i l(x)$ may not be well defined. However, let assume now that none of the dynamic saturations is activated and $f(\cdot, w)$ is sufficiently smooth. The AGC bound will be explicitly taken into account for the design of the attack signal.

Definition 1: The nonlinear system (2) with output $y = l(x)$ is said to have relative degree ρ, $1 \leq \rho \leq n$, in a region $D \subset \mathbb{R}^n$ if $L_g L_f^{i-1} l(x) = 0$ for $i = 1, 2, \cdots, \rho - 1$, and $L_g L_f^{\rho-1} l(x) \neq 0$ for all $x \in D$.

Suppose that the above system has relative degree $\rho \leq n$ in $D \subset \mathbb{R}^n$, therefore for every $x_0 \in D$, a neighborhood N of x_0 and smooth functions, $\varphi_1(x), \ldots, \varphi_{n-\rho}(x)$ exist such that $\frac{\partial \varphi_i(x)}{\partial x} g(x) = 0$, $i = 1, \cdots, n - \rho$, $\forall x \in N$ is satisfied for all $x_0 \in N$, and the map $T(x, w)$

$$z = T(x,w) = \begin{pmatrix} \varphi_1(x) \\ \vdots \\ \varphi_{n-\rho}(x) \\ --- \\ l(x) \\ \vdots \\ L_f^{\rho-1} l(x) \end{pmatrix} = \begin{pmatrix} \Phi(x) \\ --- \\ \Psi(x) \end{pmatrix} = \begin{pmatrix} \eta \\ - \\ \xi \end{pmatrix}, \tag{5}$$

is diffeomorphism on N [12], [13]. The input-output linearization technique is based on applying $z = T(x, w)$, and $v = \alpha(x, w) + \beta(x, w)u$, where $z = T(x, w)$ is an admissible state transformation expressed in (5) and v is the new control input signal. The functions $\alpha(x, w)$ and $\beta(x, w)$ are then expressed as $\alpha(x, w) = L_f^{\rho} l(x)$, $\beta(x, w) = L_g L_f^{\rho-1} l(x)$. Upon using the linearizing transformation T and the associated functions α and β, the representation (2) will change to the normal form as

$$\begin{aligned} \dot{\eta} &= f_0(\eta, \xi), \\ \dot{\xi} &= A_c \xi + B_c v, \\ y &= C_c \xi, \end{aligned} \tag{6}$$

where A_c, B_c and C_c are canonical controllability matrices [14]. This form decomposes the system into a linear subsystem described by ξ and an internal nonlinear subsystem described by η. Here our main goal is to push the system trajectories to the unsafe region in contrast to the usual stabilization idea. Hence, unstable behavior of the internal dynamics would be a benefit for our objectives, i.e. destabilize the system.

Having transformed (2) into (6) and applied linear feedback control $v = K\xi$, the feedback law is

$$u(x, w, K) = \frac{K\xi - \alpha(x, w)}{\beta(x, w)} = \frac{K[0 \quad I]T(x, w) - \alpha(x, w)}{\beta(x, w)},$$

where K is an $1 \times \rho$ constant vector. To consider the input bound and saturation limit of AGC, $|u(x, w, K)| \leq U_0$, we pass the control law through a saturation operator as

$$\begin{aligned} \bar{u}(x, w, K) &= \mathrm{sat}(u(x, w, K), U_0) \\ &= \begin{cases} u(x, w, K) & |u(x, w, K)| \leq U_0, \\ U_0 \ \mathrm{sign}(u(x, w, K)) & |u(x, w, K)| > U_0. \end{cases} \end{aligned} \tag{7}$$

According to the frequency constraint (3), define the cost function $J_2 = \max(\|x_1\|_\infty, \|x_2\|_\infty)$. Regarding the new formulation, we restrict the class of input signals from any bounded measurable functions to the class of all functions generated through the feedback control law (7). The gain $K = [k_1, k_2, \cdots, k_\rho]^T$ is a tuning coefficient vector which will be determined so as to maximize J_2. Note that J_2 is different from J_1 since with that setting better results were achieved for each case.

Problem Statement. *For the nonlinear system (2), determine the coefficient K in (7) to maximize J_2.*

Hence, similar to the previous approach, finding an optimal feedback policy for the attacker to violate the frequency constraints is relaxed to a nonlinear optimization problem.

As mentioned earlier, in most real systems the attacker does not have full access to the states in order to apply the proposed feedback policy (7). Therefore, in the next section we introduce a nonlinear observer that allows the attacker to estimate the states of the system.

B. Nonlinear Observer

The method adopted in this paper is a nonlinear observer based on extended Luenberger observer proposed by [15], [16], which is a relaxation of the normal form observer developed by [17]. Following [18], consider a multi-output system with $y = h(x) = [h_1(x) \ h_2(x) \ \ldots \ h_p(x)]^T$ where the state x is governed by the differential equations (2). Then the observability map is given by $q(x) = [h_1(x) \ \ldots \ L_f^{p_1-1}h_1(x) \ \ldots \ h_p(x) \ \ldots \ L_f^{p_p-1}h_p(x)]^T$, where $p_1 + \ldots + p_p = n$. That way the system is decomposed into p decoupled subsystems, each one with dimension p_i. The system is said to be locally observable if the observability matrix $Q(x) = \frac{\partial q(x)}{\partial x} = [dh_1(x) \ \ldots \ dL_f^{p_1-1}h_1(x) \ \ldots \ dh_p(x) \ \ldots \ dL_f^{p_p-1}h_p(x)]^T$, has full rank, i.e. $rank(Q) = n$.

The dynamics of the observer are then described by

$$\dot{\hat{x}} = f(\hat{x}, w) + g(\hat{x}, w)u + L(\hat{x}, w)(h(x) - h(\hat{x})). \tag{8}$$

As stated in [19], $L(\hat{x}, w) = [a_1(ad_f) \circ s_1 \ \ldots \ a_p(ad_f) \circ s_p]B^{-1}$, and $B = \frac{\partial h(\hat{x})}{\partial \hat{x}}[ad_f^{p_1-1} \circ s_1 \ \ldots \ ad_f^{p_p-1} \circ s_p]$. In the above equations $ad_f^i s := [f, \ ad_f^{i-1}s]$ for $i \geq 0$ is the i^{th} Lie Bracket, with $ad_f^0 s := s$ and $[f, s] = \frac{\partial s}{\partial x}f - \frac{\partial f}{\partial x}s$. The vector s_i is the k_i vector of $Q(x)^{-1}$, where $k_i = \sum_{j=1}^{i} p_j$. $a_i(\lambda) = c_{i0} + c_{i1}\lambda + \ldots + c_{ip_i-1}\lambda^{p_i-1} + \lambda^{p_i}$ is the characteristic polynomial of the i subsystem, and the coefficients c_{ij} are design parameters that are selected so as to place the eigenvalues at the desired position.

According to (2), (8) and (7), the system can be represented by

$$\begin{bmatrix} \dot{x} \\ \dot{\hat{x}} \end{bmatrix} = \begin{bmatrix} f(x, w) + g(x, w)\bar{u}(\hat{x}, w_0, K) \\ f(\hat{x}, w_0) + g(\hat{x}, w_0)\bar{u}(\hat{x}, w_0, K) + L(\hat{x}, w_0)(h(x) - h(\hat{x})) \end{bmatrix}, \tag{9}$$

where the controller gain K has been tuned as described in the previous section based on the nominal model parameters w_0 so as to maximize J_2.

C. Simulation Results for the Feedback Policy

Similar to Section III-B, we consider an attack intrusion in the second area with the same nominal model parameters w_0. It is then reasonable to assume that the intruder has access to the measurements Δf_2 and $\Delta\phi$. Therefore, the output measurement vector is $y = h(x) = [x_2 \quad x_3]^T$. Considering $p_1 = 1$ and $p_2 = 3$, one can check that the observability matrix Q is indeed full rank. Similarly, if we choose $y = h(x) = [x_1 \quad x_1]^T$, and $l(x) = x_3$, we have $\rho = 2$.

In the first part we assume that the attacker has perfect knowledge of the model of the power network and constructs a feedback policy based on a state estimate generated by the nonlinear observer of Section IV-B. In the second part, we consider some parameter mismatching and investigate how robust the attacker's policy is under these parameter uncertainties.

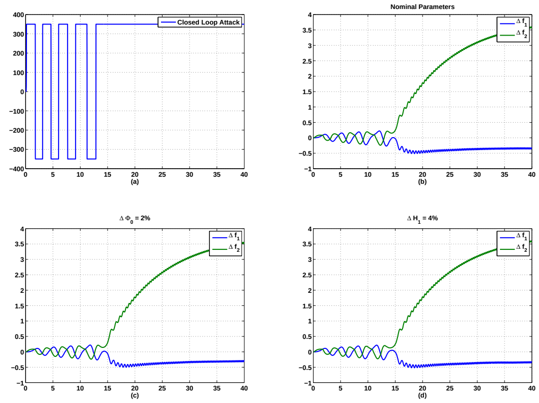

Fig. 5. (a) Closed loop policy, (b) Frequency trajectories for perfect model, (c) Frequency trajectories for imperfect model with $\Delta\phi_0 = 2\%$, and (d) Frequency trajectories for imperfect model with $\Delta H_1 = 4\%$

*1) **Perfect Model:*** Here we assume that $w = w_0$ and apply the Metropolis-Hastings algorithm to obtain the coefficient K in (7) to maximize J_2. Fig 5.a depicts the feedback policy of the attacker and Fig 5.b shows the frequency trajectory of each area and proves the severe impact that a suboptimal attack signal could have on the system. For the simulations, T was chosen to be $40sec$ and K was the number of decision variables. Since the objective function is absolutely positive, we can select $\delta = 0$. The parameter $I_k = 5$ is fixed and the set $\mathbf{\Theta}$ is set to $[-100, 100]^2$.

*2) **Model with Parameter Uncertainty**:* Similar to the open loop simulations (Fig 5.c, 5.d), we assume that the attacker has an imperfect knowledge of the system by introducing $P_{0_{12}} = -484.8MW$ and $H_1 = 4.8sec$. This parameter mismatching is associated to $\Delta\phi_0 = 2\%$ and $\Delta H_1 = 4\%$. Note that these deviations are just considered for the actual model, whereas the power system model and observer dynamics that the attacker uses to generate his policy are still designed based on w_0. In contrast to the open loop strategy, the feedback policy is considerably robust to such a model mismatching and consequently it provides an effective and practical solution to construct an attack signal.

*3) **Robustness Observation and Level of Frequency Violation**:* To investigate how robust the generated policy is, we now fix the coefficient K obtained for the nominal case with w_0 and apply the policy (7) to a larger domain of parameter uncertainties.

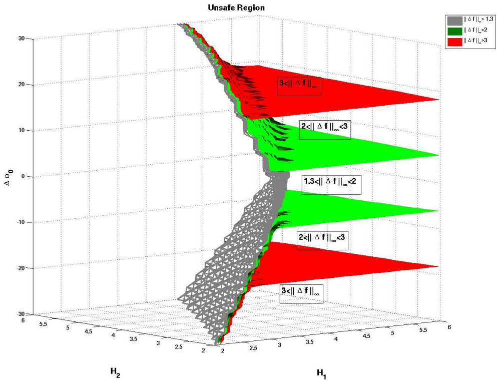

Fig. 6. Unsafe region and level of frequency violation

In Figure 6, the x, y and z axes depict the first and second inertia time constant H_i, and the voltage phase displacement of the tie line $\Delta\phi$ respectively. Each point in this region represents a certain set of dynamic parameters for the two-area power network. Having considered the frequency violation threshold equal to $1.3Hz$ and applied the nominal feedback policy on the second area for different parameters w, one can observe that the region is separated to two parts, namely "**Safe**" and "**Unsafe**". It is of interest that the power network is more vulnerable to AGC intrusion if the area with smaller inertia time constant is attacked. This is reasonable also from a physical point of view, since the other area will need more time to react to the attack signal. Moreover, roughly speaking, the inertia size determines the "**Safe**" and "**Unsafe**" regions whereas the level of frequency violation (different color regions in Fig 6) is highly dependent on the scheduled power.

V. Conclusion

In this paper, two approaches on designing an optimal control strategy to destabilize a two-area power system in the case of a cyber attack in AGC are developed. The first approach, is an open loop policy based on Markov Chain Monte Carlo optimization. However, via simulations it was demonstrated that this policy is extremely sensitive to parameter uncertainty. Motivated by this a systematic algorithm based on feedback linearization was developed so as to construct an attack signal. The proposed scheme was tested numerically and its robustness to parameter mismatching were verified from the obtained simulation results. Current work concentrates on the implementation of the proposed scheme on a realistic, IEEE benchmark network.

VI. Acknowledgment

This research work is supported by the European Commission under the project VIKING, FP7-ICT-SEC-2007-1.

References

[1] *Forbes, Congress Alarmed at Cyber-Vulnerability of Power Grid, available at http://www.forbes.com/2008/05/22/cyberwar-breach-government-tech-security_cx_ag_0521cyber.html.*

[2] *CNN, Sources: Staged cyber attack reveals vulnerability in power grid, available at http://www.cnn.com/2007//US/09/26/power.at.risk/index.html.*

[3] *Comptuterworld, DHS to review report on vulnerability in West Coast power grid, available at http://www.computerworld.com/s/article/9138017.*

[4] J.-W. Wang and L.-L. Ronga, "Cascade-based attack vulnerability on the us power grid," *Elsevier, Safety science*, vol. 47, no. 10, pp. 1332–1336, 2009.

[5] D. Kirschen and F. Bouffard, "Keep the Lights On and the Information Flowing," *Power and Energy Magazine, IEEE*, vol. 7, no. 1, pp. 50–60.

[6] *Viking Project, http://www.vikingproject.eu.*

[7] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two-area power system: Impact identification using reachability," *to appear in American Control Conference 2010.*

[8] G. Andersson, *Dynamics and Control of Electric Power Systems*. ETH Zürich, 2009.

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

[10] C. Robert and G. Casella, *Monto Carlo Statistical Methods*. Springer Verlag.

[11] A. Lecchini, J. Lygeros, and J. Maciejowski, "Simulated annealing: Rigorous finite-time guarantees for optimization on continuous domains," *Advances in Neural Information Processing Systems*.

[12] S. Sastry, *Nonlinear Systems*. New York: Springer-Verlag, 1999.

[13] A. Isidori, *Nonlinear Control Systems*. NJ: Springer, Berlin, Third Edition, 2002.

[14] H. Khalil, *Nonlinear Systems*. NJ: Prentice-Hall, Upper Saddle River, Third Edition, 2002.

[15] D. Bestle and M. Zeitz, "Canonical form observer design for non-linear time-invariant systems," *International Journal of Control*, vol. 38, no. 2, pp. 419–431, 1983.

[16] J. Birk and M. Zeitz, "Extended luenberger observer for non-linear multivariable systems," *International Journal of Control*, vol. 47, no. 6, pp. 1823–1835, 1988.

[17] A. Krener and A. Isidori, "Linearization by output injection and nonlinear observers," *Systems and Control Letters*, vol. 3.

[18] E. Ergueta, R. Seifried, R. Horowitz, and M. Tomizuka, "Extended luenberger observer for a mimo nonlinear nonholonomic system," *Proceedings of the 17th World Congress, The International Federation of Automatic Control, Seoul, Korea.*

[19] K. Roebenack, "Computation of the observer gains for extended luenberger observer using automatic differentiation," *IMA Journal of Mathematical Control and Information*, vol. 21.