2013 European Control Conference (ECC)
July 17-19, 2013, Zürich, Switzerland.

On Optimal Sensor Placement for Mitigation of Vulnerabilities to Cyber Attacks in Large-Scale Networks

U. Vaidya and M. Fardad

Abstract— **We propose a system theoretic approach to the identification and mitigation of vulnerabilities to cyber attacks, in networks of dynamical systems. Using the controllability and observability gramians, we define a network's vulnerability in terms of the impact of an attack input and the degree of difficulty with which this impact can be detected. In this framework, a network is deemed as vulnerable if it is easy for an attacker to steer it to a certain state and yet such a state is hard to observe through the network's sensing mechanisms. We propose strategies for finding the optimal location of a small number of sensors that minimize the network's vulnerability. Such strategies are obtained as the solution of convex optimization problems, formulated so as to strike a balance between maximal reduction of the system's vulnerability and employing a minimal number of sensors. The utility of the developed framework is demonstrated on a standard IEEE nine bus power system network model.**

Index Terms— **Convex optimization, large-scale systems, power networks, relaxation, semidefinite programming, sensing strategy, smart grid.**

I. Introduction

Cyber security of critical infrastructure is one of the pressing problems of the present day. A recent survey by McAfee acknowledges that many critical components of infrastructure have been the target of some form of cyber attack [1]. The increasing dependence of our infrastructure on advanced communication technology, and the use of the Internet for its routine operation, have further raised concerns about the magnitude of this problem. Arguably, the electric power grid is the most important example of this. With the vision of building a smart gird, the modern electric power grid has witnessed an enormous level of automation. The automation includes use of supervisory control and data acquisition (SCADA) and emerging wide area monitoring systems in the form of phasor measuring units (PMUs) [2].

Cybersecurity of the power grid is an emerging area of research. A model-based approach for the detection of attacks, and anomaly from malicious electronic activities, is studied in [3], [4]. In [5] problems related to unobservability of static state estimation schemes for power networks is studied. The observability of the system is used in [6] to determine the detectability of an attack. [6] further uses system theoretic tools to identify fundamental limitations for static state estimation methods. A taxonomy of SCADA-specific intrusion detection research efforts has been developed in [7].

Financial support from the National Science Foundation for U. Vaidya under award ECCS-1002053 and for M. Fardad under award CMMI-0927509 is gratefully acknowledged. U. Vaidya is with the Department of Electrical & Computer Engineering, Iowa State University, Ames, IA 50011. M. Fardad is with the Department of Electrical Engineering and Computer Science, Syracuse University, NY 13244. E-mail: ugvaidya@iastate.edu, makan@syr.edu.

In this paper, we propose a system theoretic framework for the identification and mitigation of vulnerabilities in dynamical networks. We define new measures of network vulnerability, which simultaneously capture both the impact of attacks and the degree of difficulty with which attacks can be detected. We argue that the level of 'unobservability' of an attack is not, by itself, a good measure for characterizing the system's vulnerability to it. Indeed, it is important to also incorporate a characterization of the impact of the attack on the network. We then use the notions of observability and controllability of a system to define a variety of vulnerability measures.

The following are the main contributions of this paper. We propose new measures of network vulnerability by using the controllability and observability gramians and defining a vulnerability ellipsoid that characterizes the relative vulnerability of various directions in state-space. We develop mitigation strategies, that determine the optimal location of PMUs, by minimizing the vulnerability measures in a convex optimization framework. While the framework developed here can be applied to address problems of cybersecurity in general dynamical systems, in this paper we focus on the cybersecurity of power networks. Towards this goal, we provide numerical results for the IEEE nine bus power system.

The rest of the paper is organized as follows. In Section II we discuss the attack model and define multiple vulnerability measures. In Section II-B we extend the definition of vulnerability to networks of dynamical systems. Convex optimization based mitigation strategies, that determine the optimal location of a small number of sensors, is proposed in Section III. Simulation results for a power system network model are provided in Section IV, followed by conclusions in Section V.

II. Attack model and measures of vulnerability

Consider the linear time invariant dynamical system

$$\begin{aligned} \dot{x} &= Ax + Bu \\ y &= Cx, \end{aligned} \tag{1}$$

U.S. Government work not protected by U.S. copyright

where $x \in \mathbb{R}^n$, $y \in \mathbb{R}^p$, and $u \in \mathbb{R}^q$. We assume that the vector u models the attacks on the state x, and the vector y models sensor measurements. In the above description, the states are subjected to an attack through the input matrix B. This model is general enough to describe various attack scenarios of interest. In particular, we demonstrate the application of this model for the analysis of vulnerabilities to attacks in power networks. We make the following additional assumption on the system equations (1).

Assumption 1: The system matrix A is stable with all its eigenvalues contained in the open left half of the complex plane. Furthermore, the pairs (A, B) and (C, A) are assumed to be controllable and observable, respectively [8].

To characterize the impact of the attack function u on the state x, we use the following standard result from systems theory.

Proposition 2: Suppose the pair (A, B) is controllable. Then the controllability gramian X_c, obtained as the solution of the Lyapunov equation

$$AX_c + X_c A^T = -BB^T,$$

is nonsingular. Furthermore, the set of all states x_0 that are reachable from the origin with input $u \in L_2(-\infty, 0]$ of at most unit norm,

$$x_0 = \int_{-\infty}^{0} e^{-A\tau} B\, u(\tau)\, d\tau, \quad \|u\|_{L_2} \leq 1,$$

is given by $\{X_c^{\frac{1}{2}} x_c \mid x_c \in \mathbb{R}^n,\ \|x_c\| \leq 1\}$.

We refer the reader to [9] for a proof. This results implies that all states x_0 reachable with u satisfying $\|u\|_{L_2} \leq 1$ are given by $x_0 = X_c^{\frac{1}{2}} x_c$, where $\|x_c\| \leq 1$. We hence define the controllability ellipsoid by

$$\mathcal{E}_c = \{X_c^{\frac{1}{2}} x_c \mid x_c \in \mathbb{R}^n,\ \|x_c\| = 1\}.$$

Let $\mu_1 \geq \mu_2 \ldots \geq \mu_n > 0$ denote the eigenvalues of $X_c^{\frac{1}{2}}$, and let $v_1, \ldots, v_n$ denote the corresponding orthonormal eigenvectors. The eigenvectors and eigenvalues of the controllability ellipsoid provide information about the relative degree of controllability of different directions in state-space. If $\mu_k > \mu_\ell$, then states aligned with v_k are more controllable than those aligned with v_ℓ. And degree of controllability of any state x_c can be characterized by $x_c^T X_c x_c$.

For systems with sensors and measurements, the impact of an attack can be marginalized if one can detect the attack. In particular, even if a certain direction in state-space is prone to attacks, better detection capabilities along that direction can help minimize the impact of the attacks. The issue of detection brings forward the notion of observability of various state directions. In systems theory, the concept of controllability and observability are dual to each other [8]. The following result from the systems theory literature will help characterize the observability of various state directions.

Proposition 3: Suppose the pair (C, A) is observable. Then the observability gramian X_o, obtained as the solution of the Lyapunov equation

$$A^T X_o + X_o A = -C^T C,$$

is nonsingular. Furthermore, the energy in the output $y \in L_2[0, \infty)$, $y = Ce^{At}x_0$, when the state is intialized at $x_0 \in \mathbb{R}^n$ is given by $\|y\|_{L_2}^2 = x_0^T X_o x_0$.

We refer the reader to [9] for a proof. The observability gramian X_o can be used to describe the observability ellipsoid

$$\mathcal{E}_o = \{X_o^{\frac{1}{2}} x_0 \mid x_0 \in \mathbb{R}^n,\ \|x_0\| = 1\}.$$

Let $\eta_1 \geq \eta_2 \geq \ldots \geq \eta_n > 0$ denote the eigenvalues of $X_o^{\frac{1}{2}}$, and let $w_1, \ldots, w_n$ denote the corresponding orthonormal eigenvectors. The eigenvectors and eigenvalues of the observability ellipsoid provide information about the relative degree of observability of different directions in state-space. If $\eta_k > \eta_\ell$, then the output energy resulting from initial state w_ℓ is smaller than that observed when the initial state is w_k. And the degree of observability of any state x_0 can be characterized by $x_0^T X_o x_0$ [9], [10].

A. Vulnerability ellipsoid

Propositions 2, 3 motivate the definition of the vulnerability of state x as

$$V(x) = \frac{x^T X_c x}{x^T X_o x},$$

based on the rationale that state x is vulnerable if it is easy to reach but difficult to observe. Since $X_o > 0$, we can write $X_o = X_o^{\frac{1}{2}} X_o^{\frac{1}{2}}$. Setting $z = X_o^{\frac{1}{2}} x$ and assuming $\|z\| = 1$, with a slight abuse of notation we have

$$V(z) = z^T X_o^{-\frac{1}{2}} X_c X_o^{-\frac{1}{2}} z.$$

Definition 4 (Vulnerability ellipsoid): The vulnerability ellipsoid is given by

$$\mathcal{E}_v = \{X_c^{\frac{1}{2}} X_o^{-\frac{1}{2}} x \mid x \in \mathbb{R}^n,\ \|x\| = 1\}.$$

Let $\lambda_1 \geq \lambda_2 \ldots \geq \lambda_n$ and $p_1, \ldots, p_n$, respectively, denote the eigenvalues and eigenvectors of the vulnerability matrix

$$X_v = X_o^{-\frac{1}{2}} X_c X_o^{-\frac{1}{2}}.$$

The eigenvalues and eigenvectors of X_v provide information about the relative degree of vulnerability of various directions in state-space. In particular, if $\lambda_k > \lambda_\ell$, then states aligned with p_k are more vulnerable than those aligned with p_ℓ. Indeed, the direction corresponding to maximum (minimum) eigenvalue of X_v is the most (least) vulnerable.

It is important to emphasize that the matrix X_v only provides information about the relative vulnerability of various states and not their absolute vulnerability. This motivates us to consider the different measures of system vulnerability introduced in the next section.

B. Measures of vulnerability

From the definition of $V(z)$ and the properties of the trace, we have

$$V(z) = z^T X_o^{-\frac{1}{2}} X_c X_o^{-\frac{1}{2}} z = \mathrm{trace}(X_c^{\frac{1}{2}} X_o^{-\frac{1}{2}} z\, z^T X_o^{-\frac{1}{2}} X_c^{\frac{1}{2}}),$$

with $\|z\| = 1$. Let $\{z_i\}_{i=1}^n$ be a set composed of orthonormal vectors that provide a resolution of the identity, i.e., $\|z_i\| = 1$ and $\sum_{i=1}^n z_i\, z_i^T = I$. For example, each z_i can be chosen as the ith standard basis vector in $\mathbb{R}^n$. Then an average measure of the vulnerability of a system can be written as

$$\begin{aligned} V_1 &= \sum_{i=1}^n V(z_i) = \sum_{i=1}^n \mathrm{trace}(X_c^{\frac{1}{2}} X_o^{-\frac{1}{2}} z_i\, z_i^T X_o^{-\frac{1}{2}} X_c^{\frac{1}{2}}) \\ &= \mathrm{trace}(X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}) \end{aligned}$$

Note that $V_1 = \mathrm{trace}(X_v)$. A similar average measure of vulnerability can be defined as

$$\begin{aligned} V_2 &= \mathrm{trace}(X_v^2) = \mathrm{trace}(X_c X_o^{-1} X_c X_o^{-1}) \\ &= \|X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}\|_F^2, \end{aligned}$$

where $\|\cdot\|_F$ denotes the Frobenius norm of a matrix. Finally, we define a worst-case measure of vulnerability as

$$\begin{aligned} V_\infty &= \sup_{\|z\|=1} V(z) = \lambda_{\max}(X_o^{-\frac{1}{2}} X_c^{\frac{1}{2}} X_c^{\frac{1}{2}} X_o^{-\frac{1}{2}}) \\ &= \lambda_{\max}(X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}), \end{aligned}$$

where $\lambda_{\max}(\cdot)$ denotes the largest eigenvalue of a matrix. We point out that, since $X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}$ is a positive definite matrix, its maximum eigenvalue is equal to its maximum singular value, and thus V_∞ is also equal to the matrix 2-norm of $X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}$.

Definition 5: Let

$$\begin{aligned} V_1 &= \mathrm{trace}(X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}), \\ V_2 &= \|X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}\|_F^2, \\ V_\infty &= \lambda_{\max}(X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}). \end{aligned}$$

We refer to V_1 and V_2 as measures of *average vulnerability* and V_∞ as a measure of *worst-case vulnerability*.

We make use of these vulnerability measures in Section III to formulate optimization problems that render optimal strategies for vulnerability mitigation and the design of sensor networks.

Remark 6: For a system described by (1), it follows readily from the definitions of the controllability and observability gramians that all vulnerability measures V_i, $i = 1, 2, \infty$ are invariant to scalings (by a positive factor) of the matrix A. This, in particular, implies that the mere distance of the spectrum of A from the imaginary axis is not a determining factor in a system's vulnerability. However, scalings of the B and C matrices *do* change the vulnerability of a system. Furthermore, the vulnerability measures V_i are *not* invariant under similarity transformations.

C. Extension to networks of dynamical systems

The objective of this section is to extend the vulnerability measures defined in the previous section to a network of interconnected dynamical systems. In particular, we would like to define a measure that can indicate the vulnerability of a subsystem or certain components of a large network of coupled dynamical systems. The motivation for such an extension comes from the fact that in large-scale dynamical system it not always necessary to protect all subsystems against a cyber attack equally. For instance, in a power system network there may be a group of generators that, based on their size or geographical location, are more important to protect than other generators.

Consider

$$\begin{aligned} \dot{x} &= \widetilde{A}x - Fy + Bu = (\widetilde{A} - FC)x + Bu \\ y &= Cx, \end{aligned} \tag{2}$$

where $x = (x_1^T, \ldots, x_M^T)^T$ with $x_k \in \mathbb{R}^{n_k}$, $k = 1, \ldots, M$, is the state of the system, and x_k is the state of the kth subsystem. We define $n = \sum_{k=1}^M n_k$. We assume that $\widetilde{A} = \mathrm{diag}(A_1, \ldots, A_M)$, where the matrix A_k describes the internal dynamics of the kth subsystem in the absence of coupling between the subsystems. The matrix F models the subsystems' interconnection. We assume $C = \mathrm{diag}(C_1, \ldots, C_M)$, where the matrix C_k describes the sensor measurement of the kth subsystem. The function u models the attacker's input to the system. Finally, we assume that $A := \widetilde{A} - FC$ has eigenvalues in the open left half of the complex plane.

As before, we define X_c and X_o as the controllability and observability gramians of the network system, obtained as solutions of the Lyapunov equations

$$AX_c + X_c A^T = -BB^T, \qquad A^T X_o + X_o A = -C^T C.$$

To define the vulnerability ellipsoids for individual subsystems, we take the projection of X_v along the subspace corresponding to the states of the individual subsystems.

Let $\mathcal{S}_k$ be the subspace corresponding to the states of the kth subsystem and let P_k,

$$P_k = \mathrm{diag}(0, \ldots, 0, I_{n_k}, 0, \ldots, 0)$$

be the corresponding projection matrix, where I_{n_k} is the identity matrix of size n_k starting at the $\sum_{j=1}^{k-1} n_j$ location. The projected ellipsoid $\mathcal{E}_{S_k}$ is represented by the matrix $X_v^k \in \mathbb{R}^{n_k \times n_k}$ defined as

$$X_v^k = P_k X_v P_k, \quad k = 1, \ldots, M.$$

The matrix X_v^k is singular and hence represents a degenerate ellipsoid.

Let $\kappa_k \geq 0$, $k = 1, \ldots, M$, denote the weights associated with the individual subsystems. These weights are assumed to be known a priori and determine the relative importance of the different subsystems in the network; if $\kappa_k > \kappa_\ell$ then

the kth subsystem is more important than the ℓth subsystem. We define the vulnerability of the network as

$$X_v = \sum_{k=1}^{M} \kappa_k X_v^k \tag{3}$$

The vulnerability matrix X_v can now be used to define measures of vulnerability for the network system, as in Definition 5.

III. Mitigation of vulnerability

In this section we formulate, and propose methods for solving, vulnerability minimization problems using the vulnerability measures defined in Section II. We consider sensor locations as design variables and employ methods from convex optimization.

Let the ith row of the matrix H describe the state measurement that would be made by a sensor if it were placed in location i. For example, if we denote the ith row of H by h_i^T, then the measurement made by a sensor placed in location i would be $h_i^T x$. Let $C = DH$, where D is a diagonal matrix with binary entries $D_{ii} \in \{0, 1\}$. If the ith diagonal entry of D is zero, then the sensor in location i is inactive and can be eliminated from the system. Thus the nonzero rows of the matrix C correspond to the placement of active sensors at particular locations, while zero rows correspond to the absence of sensors. We have

$$C^T C = H^T D^2 H = H^T D H,$$

since $D^2 = D$.

We next consider the problem of optimal sensor placement for the purpose of vulnerability mitigation. Clearly, in the absence of any limitations on sensor usage, one would employ a sensor (or multiple sensors) at every desired location in the network. In practice we would like to strike a balance between vulnerability minimization and sensor usage. We thus formulate optimization problems whose objective is composed of two pars: a part that seeks to minimize a vulnerability measure, and a part that *penalizes the number of sensors used*. This penalty is introduced by incorporating the term $\gamma \operatorname{trace}(D)$ in the objective function, where γ is a positive scalar whose magnitude characterizes our emphasis on using a small number of sensors; large values of γ promote a *sparse* selection of sensors. Similar sparsity-promoting optimization problems, in the context of control and network design, have been recently considered in [11], [12], [13], [14], [15].

A. Average vulnerability

Using the vulnerability measure V_1, we consider the optimization problem

$$\begin{array}{ll} \text{minimize} & \operatorname{trace}(X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}) + \gamma \operatorname{trace}(D) \\ \text{subject to} & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0, 1\}, \end{array} \tag{4}$$

where the optimization variables are the matrices X_o, D.

We can write this problem as [16]

$$\begin{array}{ll} \text{minimize} & \operatorname{trace}(W) + \gamma \operatorname{trace}(D) \\ \text{subject to} & W \succeq X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}} \\ & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0, 1\}, \end{array}$$

or equivalently

$$\begin{array}{ll} \text{minimize} & \operatorname{trace}(W) + \gamma \operatorname{trace}(D) \\ \text{subject to} & \begin{bmatrix} W & X_c^{\frac{1}{2}} \\ X_c^{\frac{1}{2}} & X_o \end{bmatrix} \succeq 0 \\ & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0, 1\}, \end{array}$$

where the optimization variables are the matrices W, X_o, D. If we relax the binary conditions to $0 \leq D_{ii} \leq 1$, then this optimization problem becomes an SDP.

If we choose to use the vulnerability measure V_2, then we can consider the optimization problem

$$\begin{array}{ll} \text{minimize} & \|X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}\|_F^2 + \gamma \operatorname{trace}(D) \\ \text{subject to} & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0, 1\}, \end{array} \tag{5}$$

where the optimization variables are the matrices X_o, D.

We can write this problem as [16]

$$\begin{array}{ll} \text{minimize} & \operatorname{trace}(Z) + \gamma \operatorname{trace}(D) \\ \text{subject to} & Z \succeq W^2, \quad W \succeq X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}} \\ & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0, 1\}, \end{array}$$

or equivalently

$$\begin{array}{ll} \text{minimize} & \operatorname{trace}(Z) + \gamma \operatorname{trace}(D) \\ \text{subject to} & \begin{bmatrix} Z & W \\ W & I \end{bmatrix} \succeq 0 \\ & \begin{bmatrix} W & X_c^{\frac{1}{2}} \\ X_c^{\frac{1}{2}} & X_o \end{bmatrix} \succeq 0 \\ & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0, 1\}, \end{array}$$

where the optimization variables are the matrices Z, W, X_o, D. If we relax the binary conditions to $0 \leq D_{ii} \leq 1$, then this optimization problem becomes an SDP.

B. Worst-case vulnerability

Consider the optimization problem

$$\begin{array}{ll} \text{minimize} & \lambda_{\max}(X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}}) + \gamma \operatorname{trace}(D) \\ \text{subject to} & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0, 1\}, \end{array}$$

where the optimization variables are the matrices X_o, D.

We can write this problem as [16]

$$\begin{aligned} \text{minimize} \quad & \sigma + \gamma \,\mathrm{trace}(D) \\ \text{subject to} \quad & \sigma I \succeq X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}} \\ & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0,1\}, \end{aligned}$$

or equivalently

$$\begin{aligned} \text{minimize} \quad & \sigma + \gamma \,\mathrm{trace}(D) \\ \text{subject to} \quad & \begin{bmatrix} \sigma I & X_c^{\frac{1}{2}} \\ X_c^{\frac{1}{2}} & X_o \end{bmatrix} \succeq 0 \\ & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0,1\}, \end{aligned} \tag{6}$$

where the optimization variables are the matrices X_o, D, and the scalar σ. If we relax the binary conditions to $0 \le D_{ii} \le 1$, then this optimization problem becomes an SDP.

C. Weighted worst-case vulnerability

Consider the optimization problem

$$\begin{aligned} \text{minimize} \quad & \lambda_{\max}\left(\textstyle\sum_{k=1}^{M} \kappa_k P_k X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}} P_k\right) + \gamma \,\mathrm{trace}(D) \\ \text{subject to} \quad & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0,1\}, \end{aligned}$$

where the optimization variables are the matrices X_o, D. We point out that we have used the term $\sum_{k=1}^{M} \kappa_k P_k X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}} P_k$ in the objective function as a proxy for $\sum_{k=1}^{M} \kappa_k P_k X_o^{-\frac{1}{2}} X_c X_o^{-\frac{1}{2}} P_k$, to allow for the formulation of a semidefinite program, as we demonstrate in what follows.

To simplify the summation in the objective, we note that

$$\begin{aligned} & \textstyle\sum_{k=1}^{M} \kappa_k P_k X_c^{\frac{1}{2}} X_o^{-1} X_c^{\frac{1}{2}} P_k \\ & = \begin{bmatrix} \sqrt{\kappa_1}\, X_c^{\frac{1}{2}} P_1 \\ \vdots \\ \sqrt{\kappa_M}\, X_c^{\frac{1}{2}} P_M \end{bmatrix}^T \begin{bmatrix} X_o^{-1} & & \\ & \ddots & \\ & & X_o^{-1} \end{bmatrix} \begin{bmatrix} \sqrt{\kappa_1}\, X_c^{\frac{1}{2}} P_1 \\ \vdots \\ \sqrt{\kappa_M}\, X_c^{\frac{1}{2}} P_M \end{bmatrix} \\ & = P^T (I \otimes X_o^{-1})\, P, \end{aligned}$$

where $\otimes$ denotes the Kronecker product and

$$P = \begin{bmatrix} \sqrt{\kappa_1}\, X_c^{\frac{1}{2}} P_1 \\ \vdots \\ \sqrt{\kappa_M}\, X_c^{\frac{1}{2}} P_M \end{bmatrix}.$$

The optimization problem thus becomes

$$\begin{aligned} \text{minimize} \quad & \lambda_{\max}(P^T (I \otimes X_o^{-1})\, P) + \gamma \,\mathrm{trace}(D) \\ \text{subject to} \quad & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0,1\}, \end{aligned}$$

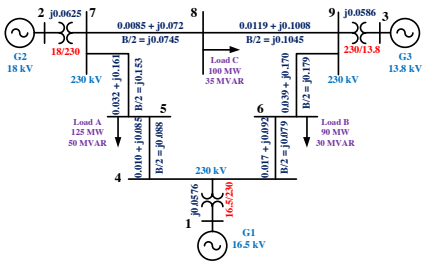

Fig. 1. IEEE nine bus system

which can be rewritten as [16]

$$\begin{aligned} \text{minimize} \quad & \sigma + \gamma \,\mathrm{trace}(D) \\ \text{subject to} \quad & \begin{bmatrix} \sigma I & P^T \\ P & I \otimes X_o \end{bmatrix} \succeq 0 \\ & -A^T X_o - X_o A = H^T D H \\ & D \text{ diagonal}, \quad D_{ii} \in \{0,1\}, \end{aligned} \tag{7}$$

where the optimization variables are the matrices X_o, D, and the scalar σ. If we relax the binary conditions to $0 \le D_{ii} \le 1$, then this optimization problem becomes an SDP.

IV. Example

In this section we give an illustrative example of vulnerability mitigation using the optimization framework of the previous section. For all computations we use `CVX`, a package for specifying and solving convex programs [17], [18].

A. Cyber attacks on an illustrative power network

We use a multimachine power system model with a constant impedance load. The power system network consists of generators and load buses. For the purpose of numerical computations, we use the IEEE nine bus power system model consisting of three generator buses and three load buses. The line diagram for the nine bus system is shown in Fig. 1.

For the constant impedance load model, the only dynamical equations are the ones used to model the generator dynamics. Each generator dynamics is described as

$$\dot{x} = f(x, v, T_m, t), \tag{8}$$

where, x is the state vector, v is the vector of bus voltages, and T_m is the mechanical torque. With the constant impedance load model, the above dynamical equation is augmented with an algebraic equation that describes the relation between the voltages and currents across the power network. The size of x depends upon the complexity of the model used to describe the generator dynamics.

In this paper, we use two different models to describe the generator dynamics. Following [19] we use the classical two-state model for generator 1. Generators 2 and 3 are modeled using the four-state two-axis model. The nonlinear dynamics (8) are linearized around the nominal operating condition. The linearized state-space model for the nine bus system, after elimination of the state variables at all but the generator buses, is described by the first equation in (1),

namely $\dot{x} = Ax + Bu$.

The state x now consists of generator angles δ, frequencies ω, and internal voltages E_d and E_q required for the two-axis representation of the generator dynamics. The input u consists of the mechanical torque input and generator field excitation voltages. The numerical values for the entries of the matrix A and B are taken from [19, Chapter 9]. For the purpose of measurement we assume that sensors, in the form of PMU devices, can be placed at all buses. Additionally, we assume that the generator angles δ at the generator buses, and voltage phasors v at the remaining buses, can be measured using PMUs. Therefore we have

$$y_\delta = C_\delta \delta, \quad y_v = C_v v,$$

where C_δ and C_v are assumed to be diagonal matrices consisting of binary entries. Now, since the state x only consists of generator angles δ, we need to eliminate the voltage phasors v from the above measurement equation. The voltage phasors can be expressed in terms of the bus angles using the admittance matrix Y of the power network. The output equation after this reduction can be written as

$$y = Cx,$$

where the matrix C no longer contains binary entries but is function of C_δ, C_v, and the admittance matrix Y [19].

With reference to Section III, we solve the relaxed optimization problem (6) as a semidefinite program to minimize the worst-case vulnerability measure. In general the optimal solution D^* to the relaxed problem will not have binary diagonal entries. However, D^* can be used in a variety of ways to provide a suboptimal solution to the original non-relaxed sensor selection problem. For example, when searching for the optimal location of p sensors, one can consider the indices of the largest p diagonal entries of the matrix D^* as indicating the optimal location of these sensors.

For $\gamma = 0$ the optimal solution is given by $D^* = I$, which corresponds to the case of placing PMUs at all buses. Such a solution is expected, as $\gamma = 0$ impose no cost on the number of sensors. For $\gamma = 100$ we obtain $D^* = \mathrm{diag}(0.17, 0.17, 0.17, 0, 0, 0, 0, 0, 0)$, where the diagonal entries in the matrix D are indexed based on the the bus location (i.e., D_{ii} corresponds to the i^{th} bus). Hence for $\gamma = 100$ the generator buses $1, 2$, and 3 are the optimal locations for three PMUs.

V. Conclusions

We provide a system theoretic approach for the identification and mitigation of cyber attacks in networks of dynamical systems. Measures of vulnerability are defined and optimization-based approaches are proposed for vulnerability mitigation. An application of the developed framework is demonstrated on the IEEE nine bus power system model. In general, vulnerability should be incorporated into the design and control of large dynamical networks. For example, as part of a controller design problem, one could formulate an optimization problem that in addition to performance measures also includes vulnerability measures in its objective. Such a design would seek to strike a balance between good control performance and low vulnerability. We will explore such directions in our future work.

VI. Acknowledgement

The first author would like to thank Prof. Govindarasu Manimaran, from Iowa State University, for useful discussions.

References

[1] S. W. S. Baker and G. Ivanov, "In the Crossfire: Critical Infrastructure in the Age of Cyber War," *McAfee*, 2009.

[2] F. F. Wu, K. Moslehi, and A. Bose, "Power system control centers: Past, present, and future," *Proc. the IEEE*, vol. 93, no. 11, pp. 1890–1908, 2005.

[3] N. Ye, J. Giordano, and J. Feldman, "A process control approach to cyber attack detection," *Commun. the ACM*, vol. 44, no. 8, pp. 76–82, 2001.

[4] C. Ten, C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for scada systems using attack trees," in *Proc. IEEE PES General Meeting*, 2007, pp. 1–8.

[5] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures." *Proc. the IEEE Smart Grid Commun.*, 2011.

[6] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Proceeding of IEEE Decision and Control and European Control Conference*, 2011.

[7] B. Zhu and S. Sastry, "Scada-specific intrusion detection/prevention systems: A survey and taxonomy," in *First Workshop on Secure Control Systems (SCS)*, 2010.

[8] K. Zhou, J. Doyle, and K. Glover, *Robust and Optimal Control*. Prentice Hall, 1996.

[9] G. E. Dullerud and F. Paganini, *A Course in Robust Control Theory*. Springer-Verlag, New York, 1999.

[10] U. Vaidya, "Observability gramian for nonlinear systems," in *Proceedings of IEEE Conference on Decision and Control*, New Orleans, LA, 2007, pp. 3357–3362.

[11] F. Lin, M. Fardad, and M. R. Jovanović, "Design of optimal sparse feedback gains via the alternating direction method of multipliers," *IEEE Transactions on Automatic Control*, 2013, conditionally accepted; also arXiv:1111.6188v3.

[12] E. Masazade, M. Fardad, and P. K. Varshney, "Sparsity-promoting extended Kalman filtering for target tracking in wireless sensor networks," *IEEE Signal Processing Letters*, vol. 19, pp. 845–848, 2012.

[13] M. Fardad, F. Lin, and M. R. Jovanović, "On the optimal synchronization of oscillator networks via sparse interconnection graphs," in *Proceedings of the 2012 American Control Conference*, 2012, pp. 4777–4782.

[14] F. Lin, M. Fardad, and M. R. Jovanović, "Algorithms for leader selection in large dynamical networks: Noise-corrupted leaders," in *Proceedings of the 50th IEEE Conference on Decision and Control*, 2011, pp. 2932–2937.

[15] M. Fardad, F. Lin, and M. R. Jovanović, "Sparsity-promoting optimal control for a class of distributed systems," in *Proceedings of the 2011 American Control Conference*, 2011, pp. 2050–2055.

[16] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[17] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 1.21," http://cvxr.com/cvx/, 2011.

[18] ——, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds. Springer-Verlag Limited, 2008, pp. 95–110.

[19] P. Anderson and A. Fouad, *Power Stsrem Control and Stability*. Wiley Interscience, 2003.