University Library



A gateway to Melbourne's research publications

Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:
Shames, I;Farokhi, F;Summers, TH

Title:
Security analysis of cyber-physical systems using H-2 norm

Date:
2017-07-14

Citation:
Shames, I., Farokhi, F. & Summers, T. H. (2017). Security analysis of cyber-physical systems using H-2 norm. IET CONTROL THEORY AND APPLICATIONS, 11 (11), pp.1749-1755. https://doi.org/10.1049/iet-cta.2016.1391.

Persistent Link:
https://hdl.handle.net/11343/251423

Security Analysis of Cyber-Physical Systems Using $\mathcal{H}_2$ Norm

Iman Shames[1,*], Farhad Farokhi[1], Tyler H. Summers[2]

[1]Department of Electrical and Electronic Engineering, the University of Melbourne
[2]Department of Mechanical Engineering, University of Texas at Dallas
[*]email: ishames@unimelb.edu.au

Abstract: In this paper, we study the effect of attacks on networked systems and propose a new security index to analyze the impact of such attacks using $\mathcal{H}_2$ norms of attacks to target and monitoring outputs. In addition, we pose, and subsequently solve, optimisation problems for selecting inputs or outputs that point to attacks with maximum impact and least detectability. To demonstrate the applicability of the analysis methods proposed in this paper IEEE 9-bus and 50-generator 145-bus systems are considered as test cases.

1. Introduction

Critical infrastructures, such as electricity grids, water distribution networks, and transport systems, are of significant importance as they underpin all facets of modern life and are thus lucrative targets for malicious agents. Recently, many studies have focused on security of the cyber-physical systems [1, 2]. For instance, to analyze the vulnerabilities of measurement systems in power networks to false data attacks, a security index was introduced in [3]. The index was defined to be the minimum number of measurements that need to be tampered so that an attack on a specific bus in the network goes unnoticed when using linear static estimators. The buses that have a small security index are particularly vulnerable as the effort and/or the resources needed for attacking them is small. Calculating this security index was shown to be NP-hard in general; however, efficient algorithms were proposed for determining the index in special situations, such as the full measurement case [4]. This idea was further generalized to linear dynamic estimators in [5]. Alternatively, controllability and observability notions were used in [6] to identify the most impactful attacks that are difficult to detect. A wide range of attacks in the presence of different estimators were studied in [7] to investigate the security of descriptor systems arising in smart grids and irrigation networks.

In this paper, we study the scenarios where an adversarial agent's objective is to compromise a networked system. In this paper, an optimisation framework for studying the effect of attacks injected by an adversarial agent on the outputs and states of a networked system is proposed. Particularly, the $\mathcal{H}_2$ norms of attacks to target and monitoring outputs is used as a performance measure. Although the use of $\mathcal{H}_2$ norm was studied in the fault detection community, e.g., [8, 9], its role in cyber-security is mostly unexplored. The aforementioned framework enables us to determine the attack structures with the highest impact on the network. More specifically, we consider an optimisation problem to select the points to inject the attacks on the systems to attain the most influence while raising the least amount of suspicion. To reflect this criteria, the cost function balances the amount of the caused deviation in the target outputs, measured by the dissipated energy through the

target outputs caused by the injected attacks, with the residual observed in the monitored outputs, similarly measured by the dissipated energy through the monitored outputs caused by the injected attacks. We refer to the optimal value of this cost as a security index denoting the ease with which one can tamper with the target outputs while not being discovered. The lower this index is for a target output, the less secure those outputs are. Further, we generalize the problem formulation to select the attack points and target output to inflict the most amount of damage while reducing the energy observed by monitoring nodes. To the best of our knowledge, the simultaneous selection of inputs and target states has not been considered previously. We prove that this problem, in general, is NP-complete by reducing it to the famous maximum edge weight induced biclique problem, e.g., [10]. In this case, we can use heuristic algorithms, e.g., [11–13], to provide approximate solutions. Finally, we show that the it is possible to solve a larger mixed-integer linear program to extract the solution of this problem. We demonstrate the applicability of the proposed analysis tools developed in this paper on a power grid. The network operator can use the developed results in multiple ways to improve the security and the robustness of the system. Firstly, it can reshape the dynamics of the system by employing a new or modifying the existing controllers to reduce the impact of various attacks or to achieve its desired security index. Alternatively, the system operator can add additional monitoring outputs for increasing the complexity of attacks on sensitive target states.

The outline of this paper is as follows. In Section 2, the required background, definitions, and the problem formulations are provided. In Section 3, the solution to the introduced problems are provided. Numerical examples and concluding remarks are respectively presented in Sections 4 and 5.

2. Preliminaries and Problem Statement

In what follows, we set up the general problem formulation and formalize the problems of interest. We start with the case where the targets are fixed.

2.1. Optimal Attack Structure with Given Targets

Assume that the attack-free networked system of interest is modelled by the following continuous-time linear time-invariant dynamical system

$$\dot{x} = Ax + Bu + H\alpha, \tag{1a}$$

$$y = Cx \tag{1b}$$

where $x = [x_1^\top, \dots, x_N^\top]^\top \in \mathbb{R}^n$ is the network state with $x_i \in \mathbb{R}^{n_i}$ being the state of system $i \in \{1, \dots, N\}$, $u \in \mathbb{R}^b$ is an external input, and $C \in \mathbb{R}^{p \times n}$. Further, $\alpha \in \mathbb{R}^a$ denotes the injected *attack signal*, which is a vector consisting of a attacks, and $H \in \mathbb{R}^{n \times a}$ is the *attack matrix* to be chosen by the attacker. The columns of H are to be picked from a set of possible *attack points* denoted by $\mathcal{H} = \{h_1, \dots, h_m\}$, where $h_i \in \mathbb{R}^n$. The dynamics matrix $A \in \mathbb{R}^{n \times n}$ is assumed to be stable, and the input matrix $B \in \mathbb{R}^{n \times b}$ corresponds to a set of existing network inputs. The use of linear dynamical systems is common place in study of transient stability (see, e.g., [14]) and these models also lend themselves to solving the economic dispatch problems among other cyber-physical problems (see Remark 7). The measurement y is assumed to be available to the *network monitor* and is used for anomaly and attack detection in the system. Therefore, we call y *monitoring outputs*. In what follows, we set $u = 0$. This is without loss of generality since, in

practice, feedback rules of the form $u = Kx$ are implemented to achieve a required closed-loop performance in which case we can replace A with $A + BK$ and avoid introducing external inputs. The network dynamics under this assumption becomes

$$\dot{x} = Ax + H\alpha, \tag{2a}$$
$$y = Cx. \tag{2b}$$

Moreover, we define a set of $q \leq n$ *target states*, $\mathcal{T} \subseteq \{x_1, \ldots, x_n\}$. Let z be the vector obtained from concatenating the states in the target set. These states are the ultimate target of the attacker.

Assumption 1. The attacker has the knowledge of closed-loop dynamics, or of open-loop dynamics and the network operator's control law.

Remark 1. Note that Assumption 1 results in a worst-case scenario result. Evidently, if the correct extent of the attacker's knowledge is not known by the operator, the safest choice is to design and analyse the system under this assumption.

In this paper, we consider the problem in which the attacker wants to select the points of attack (and not the attacks themselves). That is, the attackers wants to select columns of the matrix H, i.e., the places of attack injections, and/or the entries of the target output, i.e., where to inflict its damage. This problem can be seen as the first step of an attack where the attacker pinpoints the vulnerabilities in the network. The attacker has to find the best attack matrix from the available attack vectors that achieves the following two objectives:

1. The total disruption in the target states in $\mathcal{T}$ over a time period of length T after the attack is maximized;
2. The total effect of the attack on monitoring measurements y over a time period of length T after the attack is minimized.

The first objective is to drive the crucial states as far as possible from their nominal value and the second objective captures the fact that the attacker does not want to trigger the network monitor's anomaly detection. This problem is formalised in what follows.

Problem 1. Consider the system described by (2a)-(2b). Let z be a vector of length $q \leq n$ whose entries are a subset of x, i.e. there exists a matrix E with q rows of all zeros except for one entry equal to one such that

$$z = Ex. \tag{3}$$

Furthermore, let $\mathcal{H} = \{h_1, \ldots, h_m\}$ be a finite set of arbitrary vectors $h_i \in \mathbb{R}^n$. Addressing the following questions is of interest. For given $w_A \geq 0$, $w_D \geq 0$, and $a \leq m$, find $H \in \mathbb{R}^{n \times a}$ whose columns are members of $\mathcal{A} \subseteq \mathcal{H}$, $|\mathcal{A}| = a$, that solves the following optimisation problem

$$\text{maximize} \quad w_A \mathbf{tr}(H^\top X_E H) - w_D \mathbf{tr}(H^\top X_C H) \tag{4}$$

where X_E and X_C are the finite-time observability Gramians over the interval $[0, T]$ associated with measurement matrices E and C, respectively.

The finite-time observability Gramians in Problem 1 are given by

$$X_E = \int_0^T e^{A^\top t} E^\top E e^{At} dt, \tag{5a}$$

$$X_C = \int_0^T e^{A^\top t} C^\top C e^{At} dt, \tag{5b}$$

which for the case that A is stable and $T \to \infty$ are the unique positive-semidefinite solutions of the following Lyapunov equations

$$A^\top X_E + X_E A + E^\top E = 0, \tag{6a}$$

$$A^\top X_C + X_C A + C^\top C = 0. \tag{6b}$$

The relative magnitude of coefficients w_A and w_D determines which objective is more important. If $w_A > w_D$ the first objective, i.e. influencing z, out-weighs the risk of being detected by the monitor and vice versa.

Remark 2. For $T = \infty$, the term $\mathbf{tr}(H^\top X_E H)$ is equal to $\mathcal{H}_2$-norm of the transfer function from the attack vector α to the target outputs z. Hence, the presented formulation is more general than the study of attacks. The formulation is rather about picking points from which the required effort for inflicting damage on the target states is minimized. Similarly, the term $\mathbf{tr}(H^\top X_C H)$ is equal to $\mathcal{H}_2$-norm of the transfer function from the attack vector α to the monitoring outputs y. Combining these observations, we can note that the objective of the attacker in (4) is to make sure that 1) $\mathcal{H}_2$ norm from the point of attack α to target outputs is large (thus foreseeing a large disruption) and 2) $\mathcal{H}_2$ norm from the point of attack to monitoring outputs is small (therefore the attack goes undetected). For finite horizons $T < \infty$, the terms still posses a similar interpretation as the $\mathcal{H}_2$ norm capturing the energy transferred from possible attack points to the outputs.

Remark 3. Inclusion of process noise or measurement noise in the dynamical system in (2) does not change the methods utilized in this paper for solving the problem. The additive noise simply adds a constant terms to the cost function of the optimisation problem in (4). This is due to the linearity of the underlying system, which allows us to separate the effects of the attack signal α, the process noise, and the output noise.

Remark 4. All of our results generalize straightforwardly to discrete-time networked systems. The corresponding model for the case that there is an attack in the system becomes $x^+ = Ax + H\alpha$ with the measurement vector $y = Cx$, where, similarly, α is the a-dimensional *discrete-time attack signal*. All the earlier problems can be extended to this case subject to using appropriate definitions for the finite-time observability and controllability Gramians.

Now, we propose the following definition for the *security index* of a network.

Definition 1 (a-Security Index)**.** For the system described in Problem 1, where the target states and monitor outputs are fixed, the security index is the maximum of (4).

This security index is a function of the system dynamics A, the choice of monitoring outputs C, and the selection of target states E. The system operator can change the system dynamics A and the monitoring outputs C by, respectively, designing a new controller and adding extra monitoring outputs to make the system more robust and secure. In addition, the attacker can change the target states to inflict more damage by less complex attacks. The latter is the subject of the problem formulation in the next subsection.

2.2. Joint Attack Structure and Target Selection

In the previous subsection, the targets of the attacker were assumed to be given. An attacker may attempt to simultaneously select an attack matrix and target matrix to inflict maximal damage. This can be considered as a worst-case possible scenario. The next problem of interest is described below. Given a set of attack vectors $\mathcal{H}$ and all the states, it is desired to find an attack matrix H and a target matrix E such that the energy transferred to $z = Ex$ by an attack through the attack matrix H is maximized. This problem is formalised next.

Problem 2. Consider the system described by (2a)-(2b). Let $\mathcal{S} = \{s_1, \ldots, s_n\}$ be a finite set of row vectors $s_i \in \mathbb{R}^{1\times n}$ that corresponds to measuring each state of the network, i.e. all the entries are zero except for and entry equal to one that corresponds to each of the states. Similarly, let $\mathcal{H} = \{h_1, \ldots, h_m\}$ be a finite set of attack vectors $h_i \in \mathbb{R}^n$ and $m \leq n$. For given $q > 0$ and $a > 0$, the goal is to find matrices $E \in \mathbb{R}^{q\times n}$ with q rows from $\mathcal{T} \subseteq \mathcal{S}$ and $H \in \mathbb{R}^{n\times a}$ with a columns from $\mathcal{A} \subseteq \mathcal{H}$, that solves the following optimisation problem:

$$\text{maximize} \quad w_A \mathbf{tr}(H^\top X_E H) - w_D \mathbf{tr}(H^\top X_C H) \tag{7}$$

where X_E is the observability Gramian associated with matrix E.

We propose the following definition for the *worst case security index* of a network.

Definition 2 ((q, a)-Worst Case Security Index)**.** For the system described in Problem 2, where a attack vectors and q target states are to be chosen, respectively, from sets $\mathcal{H}$ and $\mathcal{S}$, the maximum of (7) corresponds to the (q, a)-worst case security index of the networked system.

Remark 5. Note that solving (7) is equivalent to solving

$$\text{maximize} \quad w_A \mathbf{tr}(E Y_H E^\top) - w_D \mathbf{tr}(H^\top X_C H) \tag{8}$$

where Y_H is the controllability Gramian associated with the input matrix H and is defined as

$$Y_H = \int_0^T e^{At} H H^\top e^{A^\top t} dt.$$

As before for the case where A is stable the Gramians can be uniquely obtained from solving Lyapunov equations.

We conclude this section by introducing the following definitions.

Definition 3 (Complete Bi-partite Graph)**.** The complete bi-partite graph, or a biclique, $\mathcal{G} = (\mathcal{V}_1 \bigcup \mathcal{V}_2, \mathcal{E})$ is such that $\mathcal{V}_1 \bigcap \mathcal{V}_2 = \emptyset$ and $\mathcal{E} = \mathcal{V}_1 \times \mathcal{V}_2$.

Definition 4 (Induced Subgraph)**.** An induced subgraph of the vertices of a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is a subset of vertices of $\mathcal{G}$ together with any edge in $\mathcal{E}$ whose endpoints are both in this subset.

Definition 5 (Induced Biclique)**.** An induced biclique of a graph $\mathcal{G}$ is a biclique graph as well as being an induced subgraph of $\mathcal{G}$.

3. Main Results

3.1. Optimal Attack Structure with Given Targets

The optimisation problem (4) can be written as a mixed-integer program and then relaxed to be solved as a semidefinite programming (SDP) problem. However, such techniques often suffer from two drawbacks: (i) they generally return a suboptimal solution with no performance guarantees, and (ii) the semidefinite programs that emerge out of such relaxations, though computationally efficient in theory, are numerically cumbersome and are virtually unsolvable with modern general purpose solvers for networks with size larger than 100 nodes[1]. As it will be clarified below, there is a much more efficient way to solve the problem. Before continuing any further, we have the following result regarding Problem 1.

Proposition 1. The optimisation problem (4) is equivalent to the following problem.

$$\underset{\mathcal{A}\subseteq\mathcal{H},\,|\mathcal{A}|=a}{\text{maximize}} \sum_{h_i\in\mathcal{A}} w_A(h_i^\top X_E h_i) - w_D(h_i^\top X_C h_i). \tag{9}$$

Proof. First, note that for any solution H, we have $H = \begin{bmatrix}\dots & h_i & \dots\end{bmatrix}$, where $h_i \in \mathcal{A}$. Thus, (4) can be written as

$$\begin{aligned}\underset{\mathcal{A}\subseteq\mathcal{H},\,|\mathcal{A}|=a}{\text{maximize}} \quad & w_A\mathbf{tr}(H^\top X_E H) - w_D\mathbf{tr}(H^\top X_C H)\\ \text{subject to} \quad & H = \begin{bmatrix}\dots & h_i & \dots\end{bmatrix},\ h_i \in \mathcal{A},\end{aligned}$$

and equivalently

$$\begin{aligned}\underset{\mathcal{A}\subseteq\mathcal{H},\,|\mathcal{A}|=a}{\text{maximize}} \quad & w_A\mathbf{tr}(HH^\top X_E) - w_D\mathbf{tr}(HH^\top X_C)\\ \text{subject to} \quad & H = \begin{bmatrix}\dots & h_i & \dots\end{bmatrix},\ h_i \in \mathcal{A}.\end{aligned}$$

In turn, it can be written as

$$\underset{\mathcal{A}\subseteq\mathcal{H},\,|\mathcal{A}|=a}{\text{maximize}} \quad w_A\mathbf{tr}(\sum_{h_i\in\mathcal{A}} h_i h_i^\top X_E) - w_D\mathbf{tr}(\sum_{h_i\in\mathcal{A}} h_i h_i^\top X_C),$$

which in light of the linearity of trace and the fact that $\mathbf{tr}(CAB) = \mathbf{tr}(ABC)$ establishes that any solution to (4) is a solution to (9). The reverse direction can be shown in a similar fashion as well. Thus, the first part of the proof is completed. □

As a result of Proposition 1, (4) can be solved exactly. This can be done efficiently by sorting the value of $w_A(h_i^\top X_E h_i) - w_D(h_i^\top X_C h_i)$ for different $h_i \in \mathcal{H}$ and choosing $\widetilde{H}$ to be the set of those h_i that correspond to the a largest values of $w_A(h_i^\top X_E h_i) - w_D(h_i^\top X_C h_i)$. Moreover, the values of $w_A(h_i^\top X_E h_i) - w_D(h_i^\top X_C h_i)$ can be calculated independently and in parallel, thus, reducing the computational time by dividing computing loads.

[1]Note that commercial semi-definite programming toolboxes (e.g., SDPA in `http://sdpa.sourceforge.net/family.html`) can at most handle 20,000 decision variables, which is the number of free variables in a symmetric matrix with 200 rows and columns.

3.2. Joint Attack Structure and Target Selection

In what follows, we show how Problem 2 can be recast as a maximum edge weight biclique problem, whose solution can be approximated by a variety of methods from the literature. First, we present the following proposition.

Proposition 2. The optimisation problem described by (7) is equivalent to

$$\text{maximize} \quad \sum_{i=1}^{m}\sum_{j=1}^{n}\beta_i\gamma_j w_{ij} + \sum_{i=1}^{m}\beta_i\xi_i \tag{10a}$$

$$\text{subject to} \quad \sum_{i=1}^{m}\beta_i = a,\ \sum_{i=1}^{n}\gamma_i = q, \tag{10b}$$

$$\beta_i \in \{0,1\},\ j = 1,\dots,m, \tag{10c}$$

$$\gamma_i \in \{0,1\},\ i = 1,\dots,n, \tag{10d}$$

where $w_{ij} = w_A h_i^\top X_j h_i$ and $\xi_i = -w_D h_i^\top X_C h_i$ with

$$X_i = \int_0^T e^{At} s_i^\top s_i e^{A^\top t} dt, \quad i = 1,\dots,n. \tag{11}$$

Proof. Note that (7) is equivalent to

$$\begin{aligned} \text{maximize} \quad & w_A \mathbf{tr}(H^\top X_E H) - w_D \mathbf{tr}(H^\top X_C H) \\ \text{subject to} \quad & X_E = \sum_{s_i\in\mathcal{T}} \int_0^T e^{At} s_i^\top s_i e^{A^\top t} dt, \end{aligned}$$

where the decision variables are the sets $\mathcal{A} \subseteq \mathcal{H}$ and $\mathcal{T} \subseteq \mathcal{S}$ where $|\mathcal{A}| = a$ and $|\mathcal{T}| = q$. Along with (11), this optimisation problem can be written as

$$\begin{aligned} \text{maximize} \quad & w_A \mathbf{tr}(H^\top X_E H) - w_D \mathbf{tr}(H^\top X_C H) \\ \text{subject to} \quad & X_E = \sum_{s_j\in\mathcal{T}} \gamma_j X_j. \end{aligned}$$

Replacing the constraint in the cost function and similar to the proof of Proposition 1, we have

$$\text{maximize} \quad w_A \sum_{h_i\in\mathcal{A}}\sum_{s_j\in\mathcal{T}} (h_i^\top X_j h_i) - w_D \sum_{h_i\in\mathcal{A}} (h_i^\top X_C h_i).$$

Note that the membership in sets $\mathcal{T}$ and $\mathcal{A}$ can be checked by binary variables $\{\gamma_i\}_{i=1}^m$ and $\{\beta_i\}_{i=1}^n$ where $\gamma_i = 1$ if $s_i \in \mathcal{T}$ and 0 otherwise, and $\beta_i = 1$ if $h_i \in \mathcal{A}$ and 0 otherwise. The cardinality constraints on $\mathcal{T}$ and $\mathcal{A}$ can be ensured by enforcing constraints on the summations $\sum_{i=1}^n \gamma_i = q$ and $\sum_{i=1}^m \beta_i = a$. □

In the next proposition, we relate (10) to the famous maximum edge weight induced biclique problem which is postulated to be NP-complete in general, see [10]. For more information on different variants of this problem the reader may refer to [10, 15, 16].

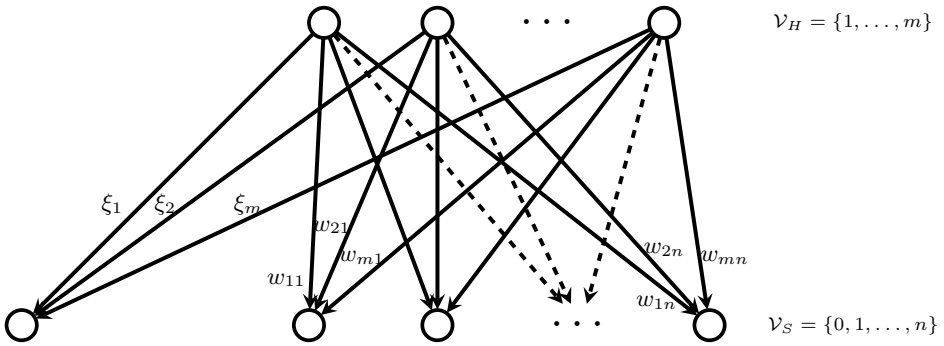


Fig. 1. *The bipartite graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ described in Proposition 3.*

Proposition 3. Define a complete bipartite graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with the vertex set $\mathcal{V} = \mathcal{V}_H \bigcup \mathcal{V}_S = \{1, \ldots, m\} \bigcup \{0,1, \ldots, n\}$ and edge set $\mathcal{E} = \mathcal{V}_H \times \mathcal{V}_S$ with edge weights $w_{ij} = h_i^\top X_j h_i$ for all $(i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\}$ and ξ_i for all $(i, j) \in \{1, \ldots, m\} \times \{0\}$. Let $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ an induced biclique of $\mathcal{G}$ where $\mathcal{V}' = \mathcal{V}_A \bigcup \mathcal{V}_T$, $\mathcal{E}' = \mathcal{V}_A \times \mathcal{V}_T$, $\mathcal{V}_A \subseteq \{1, \ldots, m\}$, $\{0\} \subseteq \mathcal{V}_T \subseteq \{0, 1, \ldots, n\}$, $|\mathcal{V}_A| = a$, $|\mathcal{V}_T| = q + 1$. Solving (10) is equivalent to finding $\mathcal{G}'$ that maximizes the sum of the edge weights.

Proof. Let $\{\beta_i^\star\}_{i=1}^m$ and $\{\gamma_i^\star\}_{i=1}^n$ be the optimal solutions to (10) and the optimum value of the cost function in (10) be given as $J^\star = \sum_{i=1}^m \sum_{j=1}^n \beta_i^\star \gamma_j^\star w_{ij} + \sum_{i=1}^m \beta_i^\star \xi_i$. The optimum value is the sum of all w_{ij} such that $\beta_i = \gamma_j = 1$. Now consider the complete bipartite graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ where $\mathcal{V} = \mathcal{V}_H \bigcup \mathcal{V}_S = \{1, \ldots, m\} \bigcup \{0,1, \ldots, n\}$ and edge set $\mathcal{E} = \mathcal{V}_H \times \mathcal{V}_S$ with edge weights $w_{ij} = h_i^\top X_j h_i$ for all $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, n\}$ and ξ_i for all $i \in \{1, \ldots, m\}$ and $j \in \{0\}$. It can be seen that $\beta_i = \gamma_j = 1$ corresponds to $(i, j) \in \mathcal{E}'$. So the problem can be cast as selecting a nodes from $\mathcal{V}_H$ and $q + 1$ nodes from $\mathcal{V}_T$ such that the sum of edge weights is maximized. This is exactly the problem of finding the induced graph of $\mathcal{G}$, $\mathcal{G}'$, with maximum edge weights where $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$, $\mathcal{V}' = \mathcal{V}_A \bigcup \mathcal{V}_T$, $\mathcal{E} = \mathcal{V}_A \times \mathcal{V}_T$, $\mathcal{V}_A \subseteq \{1, \ldots, m\}$, $\{0\} \subseteq \mathcal{V}_T \subseteq \{0,1, \ldots, n\}$, $|\mathcal{V}_A| = a$, $|\mathcal{V}_T| = q + 1$. □

The bipartite graph of Proposition 3 is depicted in Fig. 1. The optimisation problem (10) is an integer programming problem with a bilinear cost function and linear constraints. There are many methods proposed to approximately solve this problem, for example the reader may refer to the methods proposed in [11–13] and the references there-in. The following proposition uses ideas from [11] to transform this problem into a mixed-integer linear programming problem.

Proposition 4. Let $((\alpha^*_{ij})_{j=1}^n, \beta^*_i)_{i=1}^n$ denote the solution of the mixed-integer linear program

$$\text{maximize} \quad \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ij} w_{ij} + \sum_{i=1}^{m} \beta_i \xi_i \tag{12a}$$

$$\text{subject to} \quad \sum_{i=1}^{m} \beta_i = a, \; \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ij} = aq, \tag{12b}$$

$$\beta_i \in \{0,1\}, \; i = 1, \ldots, m, \tag{12c}$$

$$\alpha_{ij} \in \{0,1\}, \; i = 1, \ldots, m \wedge j = 1, \ldots, n, \tag{12d}$$

$$\alpha_{ij} \leq \beta_i, \; i = 1, \ldots, m \wedge j = 1, \ldots, n, \tag{12e}$$

$$|\alpha_{ij} - \alpha_{kj}| \leq |\beta_i - \beta_k|, \; i, k = 1, \ldots, m \wedge j = 1, \ldots, n, \tag{12f}$$

Then the solution to the optimisation problem (10) is given by $(\gamma^*_j)_{j=1}^n$ and $(\beta^*_i)_{i=1}^n$, where

$$\gamma^*_j = \begin{cases} 1, & \exists i = 1, \ldots, m : \beta^*_i = 1 \wedge \alpha^*_{ij} = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. First, note that, by construction, $(\gamma^*_j)_{j=1}^n$ and $(\beta^*_i)_{i=1}^n$ satisfy the constraints of the optimisation problem (10). This is evident for all constraints except the one concerning $\sum_j \gamma^*_j$. Let $\mathbb{1}$ denote the characteristic function, i.e., $\mathbb{1}_p$ is equal to one if p holds and is equal to zero otherwise. It can be shown that

$$\mathbb{1}_{\exists i : \beta^*_i = 1 \wedge \alpha^*_{ij} = 1} = \sum_{k=1}^{m} \mathbb{1}_{\beta^*_k = 1 \wedge \alpha^*_{kj} = 1} \Big/ \sum_{k=1}^{m} \mathbb{1}_{\beta^*_k = 1} = \sum_{k=1}^{m} \mathbb{1}_{\beta^*_k = 1 \wedge \alpha^*_{kj} = 1} \Big/ \sum_{k=1}^{m} \beta^*_k = \sum_{k=1}^{m} \mathbb{1}_{\beta^*_k = 1 \wedge \alpha^*_{kj} = 1} / a,$$

where the first equality follows from the constraint in (12f), i.e., $\alpha_{ij} = \alpha_{kj}$ if $\beta_i = \beta_k = 1$. Further, note that

$$\mathbb{1}_{\beta^*_k = 1 \wedge \alpha^*_{kj} = 1} = \mathbb{1}_{\alpha^*_{kj} = 1} = \alpha^*_{kj},$$

where the first equality follows from (12e), i.e., α^*_{kj} can only be non-zero if $\beta^*_k = 1$. Now, note that

$$\sum_{j=1}^{n} \gamma^*_j = \sum_{j=1}^{n} \mathbb{1}_{\exists i : \beta^*_i = 1 \wedge \alpha^*_{ij} = 1} = \sum_{j=1}^{n}\sum_{k=1}^{m} \alpha^*_{kj} / a = q.$$

We we choose to prove this statement by contraposition. To do so, assume that there exist $(\gamma'_j)_{j=1}^n$ and $(\beta'_i)_{i=1}^n$ which are the solutions of (10) and satisfy the inequality

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \beta^*_i \gamma^*_j w_{ij} + \sum_{i=1}^{m} \beta^*_i \xi_i < \sum_{i=1}^{m}\sum_{j=1}^{n} \beta'_i \gamma'_j w_{ij} + \sum_{i=1}^{m} \beta'_i \xi_i. \tag{13}$$

Let us construct $\alpha'_{ij} = \gamma'_j \beta'_i$. Clearly, $\alpha'_{ij} \leq \beta'_i$ because $\gamma'_j \in \{0,1\}$. In addition, we have

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \alpha'_{ij} = \sum_{i=1}^{m}\sum_{j=1}^{n} \gamma'_j \beta'_i = \Big(\sum_{i=1}^{m} \beta'_i\Big)\Big(\sum_{j=1}^{n} \gamma'_j\Big) = aq.$$

Finally,

$$|\alpha'_{ij} - \alpha'_{kj}| = \gamma'_j |\beta_i - \beta_k| \leq |\beta_i - \beta_k|.$$

Therefore, $((\alpha'_{ij})_{j=1}^n, \beta_i^*)_{i=1}^n$ also satisfies the constraints of (12). Now, (13) implies that

$$\sum_{i=1}^{m}\sum_{j=1}^{n} \alpha_{ij}^* w_{ij} + \sum_{i=1}^{m} \beta_i^* \xi_i < \sum_{i=1}^{m}\sum_{j=1}^{n} \alpha'_{ij} w_{ij} + \sum_{i=1}^{m} \beta'_i \xi_i.$$

This contradicts the assumption that $((\alpha_{ij}^*)_{j=1}^n, \beta_i^*)_{i=1}^n$ is the solution of (12). □

Proposition 4 shows that the optimisation problem (10) can be transformed it into a mixed-integer linear program. Subsequently, the proposed mixed-integer program can be solved used off-the-shelf solvers, such as CPLEX. It is pivotal to note that the proposed transformation does not reduce the computational complexity of the problem as mixed-integer linear programs are also NP-complete [17]. The transformation in fact dramatically increases the number of decision variables. After recasting (12) in the standard form to be able to use commercial solvers, the number of decision variables grows to $2(n+1)m$. In contrast, the original bilinear mixed-integer problem had $m+n$ decision variables.

Remark 6. The network operator can use the developed results in multiple ways. For instance, the system operator can reshape the dynamics of the system $A + BK$ by modifying the controller K to reduce the impact of the various attacks and to achieve its desired security index. Alternatively, the system operator can figure out the ease with which an important set of outputs can be targeted and add additional monitoring outputs for increasing the complexity of such attacks.

4. Numerical Examples

In this section, we introduce a scenario arising in smart grids where the security analysis of the type introduced in this paper is applicable. The system that we consider models the active power flow in a power network. We determine the optimal points for an adversary to launch an attack. The attack here corresponds to injection or drainage of active power in the buses of the network; therefore the attacks points are the compromised buses at which injection or drainage occur. To this aim, we consider the classical linearized synchronous machine model [14] for each node of the power network. The behaviour of bus i can be described by the so-called swing equation:

$$m_i \ddot{\theta}_i + d_i \dot{\theta}_i - P_{mi} = -\sum_{j \in N_i} P_{ij}, \tag{14}$$

where θ_i is the phase angle of bus i, m_i and d_i are, respectively, the inertia and the damping coefficients, P_{mi} is the mechanical input power and P_{ij} is the active power flow from bus i to j. Assuming that there are no power losses, neglecting ground admittances, and letting $V_i = |V_i|\, e^{j\theta_i}$ be the complex voltage of bus i, the active power flow between bus i and bus j, P_{ij}, is given by:

$$P_{ij} = k_{ij} \sin(\theta_i - \theta_j) \tag{15}$$

where $k_{ij} = |V_i|\,|V_j|\, b_{ij}$ and b_{ij} is the susceptance of the power line connecting buses i and j. Since the phase angles are close, we can linearize (15), rewriting the dynamics of bus i as:

$$m_i \ddot{\theta}_i + d_i \dot{\theta}_i = -\sum_{j \in N_i} k_{ij}(\theta_i - \theta_j) + P_{mi}. \tag{16}$$

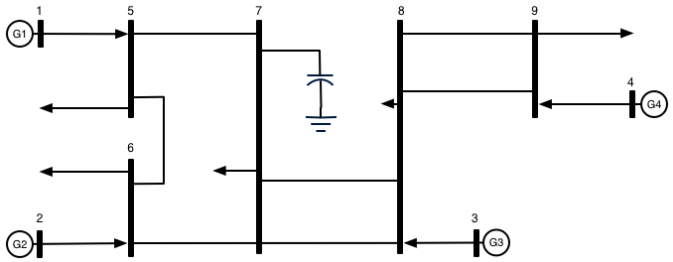


Fig. 2. *A 9-bus power network.*

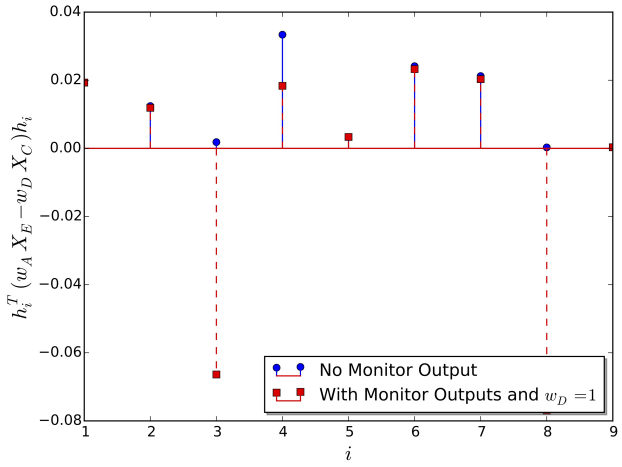


Fig. 3. *The value of* (9) *for different* h_i.

Letting $x = [\theta_1, \cdots, \theta_N, \dot{\theta}_1, \cdots, \dot{\theta}_N]^\top$ and $u = [P_{m1} \ \cdots \ P_{mN}]^\top$, we obtain

$$\dot{x} = Ax + Bu + H\alpha,$$

where

$$A = \begin{bmatrix} 0_N & I_N \\ -ML & -DM \end{bmatrix}, \quad B = [0_N \ M]^\top,$$
$$M = \text{diag}\left(\frac{1}{m_1}, \cdots, \frac{1}{m_N}\right), \quad D = \text{diag}\left(d_1, \cdots, d_N\right),$$

and L is the Laplacian matrix of graph $\mathcal{P}(\mathcal{V}_P, \mathcal{E})$ with $N = |\mathcal{V}_P|$ nodes. Each node corresponds to a bus in the power network and the undirected edge $\{i, j\} \in \mathcal{E}_P$ if bus i is connected to bus j with edge weight k_{ij} for all $\{i, j\} \in \mathcal{E}$. Note that since, in this case, the matrix A has zero eigenvalues, thus for the sake of simplicity we work with the finite-horizon observability and controllability Gramians. The matrix H can have a columns of the matrix B to show that the points that the compromised buses at which injection or drainage of power occur. It is desirable to address Problems 1 and 2 to identify the vulnerabilities of power networks when active power is injected into or drawn out of a power network.

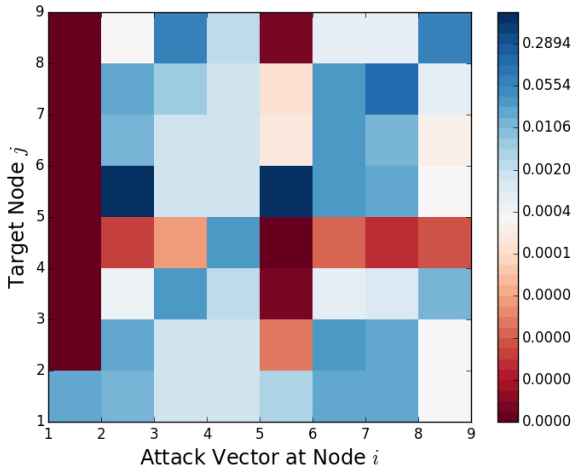


Fig. 4. *The value of* (7) *for different choices of* $\mathcal{T}$ *and* $\mathcal{A}$ *where* $a = q = 1$ *in the 9-bus power network.*

Remark 7. Another application area can arise from solving the economic dispatch problem with DC power flow equations in power networks. In this scenario, the attack corresponds changes in the prices of the generator flows. The attacker's objective is to introduce the biggest shift in a set of target buses' prices by changing the prices in another part of the network. Depending on the attack this may result in an increased price or a drop in a price in the target buses and consequently undesirable changes in the power injected by a given generator. The existing numerical algorithms for the problem are often based on the dual decomposition technique, where the optimal power among the generators is extracted from a convex optimisation problem with linear equality constraints on demand-response satisfaction. For quadratic cost functions, under appropriate conditions, the iterations of the dual decomposition can be written as a linear update rule. Now, a compromised agent can opt not to follow the update rule to achieve its desired effect on the price vector (i.e., the Lagrange multiplier in the dual decomposition algorithm). Another problem that can be solved using a similar optimisation based method described above is congestion control in data networks. Here, the attacker's objective is to introduce the biggest shift in a set of target links' prices by changing the prices in another part of the network. This depending on the attack may result in an increased congestion or increased under-utility, i.e. lack of traffic, in the target links. Other cyber-physical systems, such as intelligent transportation systems, can also be efficiently analyzed using these techniques to pinpoint their vulnerabilities.

In the remainder of this section, we study the vulnerability of power networks to attacks on generators. We determine the optimal attack vector for an adversary to launch an attack. The attack here corresponds to a sudden addition or draining of active power in the buses of the network. Specifically, the optimal attack vector indicates a sudden change in the load of which buses has the largest impact on the states of target buses.

4.1. IEEE 9-Bus System

In the this subsection, we consider the 9-bus system depicted in Fig. 2. First, we solve Problem 1 for the active power flow model in (16) where $\mathcal{H} = \{h_1, \ldots, h_9\}$ with h_i being a vector of all zeros except for the $(i+9)$-th entry that is equal to one, $a = 1$, $z = [\dot{\theta}_1, \dot{\theta}_4]^\top$, $T = 5$, $w_A = 1$, and

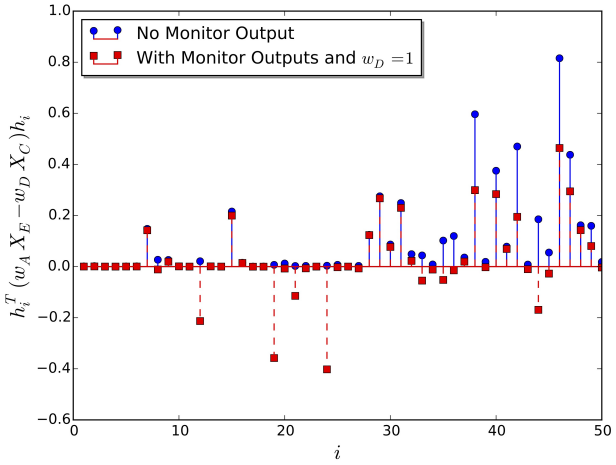


Fig. 5. *The value of* (9) *for different* h_i.

$y = 0$, i.e. no monitor outputs. The optimal attack vector in this scenario is h_4, i.e. attacking the input of bus 4 yields the highest gain from the attacker's point of view. Next, we assume that an anomaly detecter has access to the monitor output $y = [\theta_8, \dot{\theta}_8]^\top$. Moreover, we assume that all the parameters are identical to the previous case except for $w_D = 1$. The optimal attack vector for this scenario is h_6. The values of $h_i^\top(w_A X_E - w_D X_C)h_i$ are presented in Fig. 3 for both of the aforementioned scenarios. The security index for the network in the case where no monitor output was available is 0.033 and is obtained at $\mathcal{T} = \{h_4\}$ and it is 0.023 and is obtained at $\mathcal{T} = \{s_6\}$ for the case where $y = [\theta_8, \dot{\theta}_8]^\top$.

Second, we consider Problem 2 for the same 9-bus network described by (16) where $a = q = 1$. Choosing $\mathcal{T} = \{s_5\}$ and $\mathcal{A} = \{h_2\}$ correspond to the optimal solution of (7). The value of cost function for different choices of $\mathcal{T}$ and $\mathcal{A}$ are depicted in Fig. 4.

4.2. IEEE 50-Generator 145-Bus System

Here, we show that the methods developed in this paper can be easily applied to larger scale systems. To this aim we investigate Problem 1 for (16) where, as for the IEEE 50-generator 145-bus system system, $\mathcal{H} = \{h_1, \ldots, h_{50}\}$ with h_i being a vector of all zeros except for the $(i+50)$-th entry that is equal to one, $a = 1$, $z = [\dot{\theta}_{15}, \dot{\theta}_{29}]^\top$ (the targets are the frequencies of generators 15 and 29), $T = 5$, $w_A = 1$, and $y = 0$, i.e. no monitor outputs. The optimal attack vector in this scenario is h_{46}, i.e. attacking the input of generator 46 yields the highest gain from the attacker's point of view. Next, we repeat the same test while considering an anomaly detecter having access to the monitor output $y = [\theta_{26}, \dot{\theta}_{26}]^\top$, i.e the phase and the frequency of generator 26. Moreover, we assume that all the parameters are identical to the previous case except for $w_D = 1$. The optimal attack vector for this scenario remains h_{46}. The values of $h_i^\top(w_A X_E - w_D X_C)h_i$ for the scenarios described above are presented in Fig. 5.

The simulations for this paper are carried out in `Python` and to conform with the guidelines of reproducible research[2] they can be found at [18].

[2] `http://reproducibleresearch.net/`

5. Conclusion

In this paper, we studied the impact of attacks on networked systems using $\mathcal{H}_2$ norm of the attack to the target and monitoring outputs. We proposed a security index tailored for such attacks and considered the worst case scenario for attacks. We commented on the fact that the index can be applied to both continuous- and discrete-time systems and related the problem of finding the worst case security index to the famous NP-complete problem of maximum induced biclique in graphs. We considered problems that rise in power networks and studied the impact of attacks on them. Future research can focus on studying the case where the attacher does not have access to the system dynamics with some uncertainty.

6. Acknowledgment

This work is supported by a McKenzie Fellowship, an early career grant from Melbourne School of Engineering at the University of Melbourne, the Australian Research Council (LP130100605), and Defence Science and Technology Group through the Research Agreement MyIP:6288.

7. References

[1] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in *Proceedings of the 49th IEEE Conference on Decision and Control*, 2010, pp. 5991–5998.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[3] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proceedings of the 1st Workshop on Secure Control Systems (CPSWEEK 2010)*, 2010.

[4] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3194–3208, 2014.

[5] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Quantifying cyber-security for networked control systems," in *Control of Cyber-Physical Systems*, ser. Lecture Notes in Control and Information Sciences, D. C. Tarraf, Ed. Springer International Publishing, 2013, vol. 449, pp. 123–142.

[6] S. Pushpak, A. Diwadkar, M. Fardad, and U. Vaidya, "Vulnerability analysis of large-scale dynamical networks to coordinated attacks," in *Proceedings of the Australian Control Conference*, 2014.

[7] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[8] A. Varga, "Integrated algorithm for solving H_2-optimal fault detection and isolation problems," in *2010 Conference on Control and Fault-Tolerant Systems (SysTol)*, 2010, pp. 353–358.

[9] M. J. Khosrowjerdi, R. Nikoukhah, and N. Safari-Shad, "A mixed H_2/H_∞ approach to simultaneous fault detection and control," *Automatica*, vol. 40, no. 2, pp. 261–267, 2004.

[10] M. Dawande, P. Keskinocak, J. M. Swaminathan, and S. Tayur, "On bipartite and multipartite clique problems," *Journal of Algorithms*, vol. 41, no. 2, pp. 388–403, 2001.

[11] A. S. Freire, E. Moreno, and J. P. Vielma, "An integer linear programming approach for bilinear integer programming," *Operations Research Letters*, vol. 40, no. 2, pp. 74–77, 2012.

[12] T. Ibaraki, "Integer programming formulation of combinatorial optimization problems," *Discrete Mathematics*, vol. 16, no. 1, pp. 39–52, 1976.

[13] M. Padberg, "The boolean quadric polytope: some characteristics, facets and relatives," *Mathematical programming*, vol. 45, no. 1-3, pp. 139–172, 1989.

[14] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. McGraw-hill New York, 1994, vol. 7.

[15] Y. Zhang, C. A. Phillips, G. L. Rogers, E. J. Baker, E. J. Chesler, and M. A. Langston, "On finding bicliques in bipartite graphs: a novel algorithm and its application to the integration of diverse biological data types," *BMC bioinformatics*, vol. 15, no. 1, p. 110, 2014.

[16] R. Peeters, "The maximum edge biclique problem is NP-complete," *Discrete Applied Mathematics*, vol. 131, no. 3, pp. 651–654, 2003.

[17] C. H. Papadimitriou and K. Steiglitz, *Combinatorial Optimization: Algorithms and Complexity*, ser. Dover Books on Computer Science. Dover Publications, 2013.

[18] I. Shames, F. Farokhi, and T. H. Summers. (2014) Simulations scripts of 'Security Analysis of Networked Systems in the Presence of Impulsive Attacks'. [Online]. Available: https://dl.dropboxusercontent.com/u/4527019/Simulations/imp-sim.zip