Security Analysis of Networked Systems in the Presence of Impulsive Attacks

Iman Shames, Farhad Farokhi, and Tyler H. Summers

***Abstract*—In this paper we study the effect of impulsive attacks, also known as initial condition attacks, on networked systems and propose a new security index to be able to analyze the impact of such attacks. In addition, we pose, and subsequently solve, optimization problems for selecting inputs or outputs that point to attacks with maximum impact and least detectability.**

***Index Terms*—Security, Networked Systems, Impulsive Attacks**

I. Introduction

Critical infrastructures, such as electricity grids, water distribution networks, and transport systems, are examples of cyber-physical systems. Among these systems, the energy/power assets are of significant importance as they underpin all facets of modern life (e.g. food, health, manufacturing, commerce and trade, etc). These systems consist of large-scale physical processes monitored and controlled by networked control systems running over a heterogeneous set of communication networks and computers. Although the use of such powerful software systems adds flexibility and scalability, it also increases the vulnerability to hackers and other malicious entities capable of cyber attacks through the IT systems. Several security breaches have been recently announced, e.g. see [1], [2] and references there-in.

To analyze the vulnerabilities of measurement systems in power networks to false data attack, a security index was introduced in [3]. The index was defined to be the minimum number of measurements that need to be tampered so as 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 be detectable. 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. It was shown that some inconsistent initial conditions, i.e., initial conditions that do not satisfy the algebraic equation in the descriptor systems, can stay undetected based on subsequent measurements. The authors proposed using impulsive attacks, also known as initial condition attacks, to create stealth attacks using this limitation.

In this paper, we study the scenarios where an adversarial agent's objective is to compromise a networked system via impulsive attacks. We propose an optimization framework that enables us to study the effect of impulsive attack on the outputs and states of a networked system and determine the attack strategies with the highest impact on the network.

The outline of this paper is as follows. In the next section, the required background, definitions, and the problem formulations are provided. In Section III, the solution to the problems introduced in Section II are provided. Section IV considers two networked systems, namely a 9 bus power network and a data network, and studies the impact of impulsive attacks in each system. Concluding remarks are presented in Section V.

II. Preliminaries Problem Statement

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

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

$$y = Cx \tag{2}$$

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, $u \in \mathbb{R}^m$ is an external input, and $C \in \mathbb{R}^{p \times n}$. The dynamics matrix $A \in \mathbb{R}^{n \times n}$ is assumed to be stable, and the input matrix $B \in \mathbb{R}^{n \times m}$ corresponds to a set of existing network inputs. 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*.

Throughout this paper, we assume that an adversary can carry out an attack consisting of a impulsive attacks. In other words, the attacker can inject an a-dimensional signal $\alpha = [\delta(t_a), \dots, \delta(t_a)]^\top$ into the system where $\delta(t_a)$ is the Dirac function and t_a is an arbitrary *attack time*. We call α the *impulsive attack signal*. Without loss of generality, we assume $t_a = 0$. The network dynamics under this adversarial input becomes

$$\dot{x} = Ax + Bu + H\alpha, \tag{3}$$

$$y = Cx \tag{4}$$

where $H \in \mathbb{R}^{n \times a}$ is the *attack matrix* to be chosen by the attacker. The columns of H are to be picked from a set of

I. Shames and F. Farokhi are with the Department of Electrical and Electronic Engineering, the University of Melbourne. T. H. Summers is with Automatic Control Lab, ETH. e-mails: {ishames,ffarokhi}@unimelb.edu.au,tsummers@control.ee.ethz.ch.

This work is supported by a McKenzie Fellowship. F. Farokhi was supported by Rubicon Water Pty Ltd.

possible *attack vectors* denoted by $\mathcal{H} = \{h_1, \ldots, h_m\}$ where $h_i \in \mathbb{R}^n$.

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. The attacker has to find the best attack matrix from the available attack vectors that achieves the following two objectives:

1) The total energy transferred to the states in $\mathcal{T}$ over a time period of length T after the attack is maximized.
2) The total energy transferred to 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 where they are 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 (3)-(4). 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

$$z = Ex. \tag{5}$$

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 optimization problem

$$\text{maximize} \quad w_A \mathbf{tr}(H^\top X_E H) - w_D \mathbf{tr}(H^\top X_C H) \tag{6}$$

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

$$X_E = \int_0^T e^{A^\top t} E^\top E e^{At} dt, \tag{7}$$

$$X_C = \int_0^T e^{A^\top t} C^\top C e^{At} dt, \tag{8}$$

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

$$A^\top X_E + X_E A + E^\top E = 0, \quad A^\top X_C + X_C A + C^\top C = 0.$$

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

Definition 1 (a-Impulsive Security Index): For the system described in Problem 1, where the target states and monitor outputs are fixed, the impulsive security index is the maximum of (6).

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 impulsive attack through the attack matrix H is maximized. This problem is formalised next.

Problem 2: Consider the system described by (3)-(4). 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 $T \in \mathbb{R}^{q \times n}$ 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 optimization problem:

$$\begin{aligned} &\text{maximize} \quad \mathbf{tr}(H^\top X_E H) \\ &\text{subject to} \quad X_E = \int_0^T e^{A^\top t} E^\top E e^{At} dt, \end{aligned} \tag{9}$$

where X_E is the observability Gramian associated with matrix E.

Similar to before, we propose the following definition for the *worst case impulsive security index* of a network.

Definition 2 ((q,a)-Worst Case Impulsive 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 (9) corresponds to the (q,a)-worst case impulsive security index of the networked system.

Remark 1: Note that solving (9) is equivalent to solving

$$\begin{aligned} &\text{maximize} \quad \mathbf{tr}(T Y_H T^\top) \\ &\text{subject to} \quad Y_H = \int_0^T e^{At} H H^\top e^{A^\top t} dt, \end{aligned} \tag{10}$$

where Y_H is the controllability Gramian associated with the input matrix H.

As before for the case where A is stable the Gramians can be uniquely obtained from solving Lyapunov equations. Note that h_i in Problem 2 can correspond to individual states of the network. Then, the attacks illustrate a sudden change in the value of each of the states. To solve these problems, we introduce some background material in the remainder of this section.

Furthermore, we have the following definitions. For a given finite set $\mathcal{V} = \{1, \ldots, m\}$, which represents a set of edges or nodes in a network, a set function $f : 2^{\mathcal{V}} \to \mathbb{R}$ assigns a real number to each subset of V. Cardinality constrained set function optimization problems have the form

$$\underset{\mathcal{A} \subseteq \mathcal{V},\ |\mathcal{A}| \leq \kappa}{\text{maximize}} \quad f(\mathcal{A}). \tag{11}$$

This finite combinatorial optimization problem can by solved by brute force by evaluating f for the all possible subsets of size κ and selecting the maximizing subset. However, this approach quickly becomes intractable even for moderate values of m and κ. However, if f is modular then the problem can be solved very efficiently.

Definition 3 (Modularity): A function f is modular if for any $\mathcal{A} \subseteq \mathcal{V}$:

$$f(\mathcal{A}) = g(\emptyset) + \sum_{i \in \mathcal{A}} g(i). \tag{12}$$

One can see that optimizing modular set functions is easy because each element of a subset gives an independent contribution to the function values. Thus, (11) is solved by evaluating the set function for each individual element and choosing the top κ individual elements to obtain the best size κ subset.

Definition 4 (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 5 (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 6 (Induced Biclique): An induced biclique of a graph $\mathcal{G}$ is a biclique graph as well as being an induced subgraph of $\mathcal{G}$.

III. Main Results

In this section, first, we propose a solution to Problem 1. Before continuing any further, we have the following result regarding Problem 1.

Proposition 1: The optimization problem (6) is equivalent to the following problem.

$$\underset{\mathcal{A}\subseteq\mathcal{H},\ |\mathcal{A}|=a}{\text{maximize}} \sum_{h_i\in\mathcal{A}} w_A(h_i^\top X_E h_i) - w_D(h_i^\top X_C h_i). \tag{13}$$

Moreover, the cost function is modular.

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, (6) 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 (6) is a solution to (13). The reverse direction can be shown in a similar fashion as well. Thus, the first part of the proof is completed.

The second part follows directly from the definition of modularity in Definition 3. ∎

Remark 2: The optimization problem (6) can be written as a mixed-integer program and then relaxed to be solved as a semidefinite programming (SDP) problem. However, as it will be clarified below, there is a much more efficient way to solve the problem. Moreover, large SDP problems cannot be solved efficiently while the method we propose below scales well to solve very large problems.

As a result of Proposition 1, (6) can be solved exactly. The solution is outlined in Algorithm 1.

Algorithm 1 An Exact Greedy Solution to (6).

Require: X_E, X_C, $\mathcal{H}$, w_D, w_A

1: $\mathcal{A} \leftarrow \emptyset$
2: **while** $|\mathcal{A}| \leq a$ **do**
3: $\quad h_i^\star = \underset{h_i\in\mathcal{H}\setminus\mathcal{A}}{\text{argmax}} \quad w_A(h_i^\top X_E h_i) - w_D(h_i^\top X_C h_i)$
4: $\quad \mathcal{A} \leftarrow \mathcal{A}\bigcup\{i^\star\}$
5: **end while**

It is worthwhile to observe that step 3 of the algorithm does not need to be evaluateed in every iteration. In fact, Algorithm 1 can be implemented 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 H to be the set of those h_i that correspond to the a largest values of $w_A(h_i^\top X_E h_i) - w_D(h_i^\top X_C h_i)$.

In what follows, we propose a solution to Problem 2. First, we present the following proposition.

Proposition 2: The optimization problem described by (9) is equivalent to

$$\begin{aligned}\text{maximize} \quad & \sum_{i=1}^{m}\sum_{j=1}^{n} \beta_i\gamma_j w_{ij}\\ \text{subject to} \quad & \sum_{i=1}^{m}\beta_i = a,\ \sum_{i=1}^{n}\gamma_i = q,\\ & \beta_i \in \{0,1\},\ j = 1,\dots,m,\\ & \gamma_i \in \{0,1\},\ i = 1,\dots,n,\end{aligned} \tag{14}$$

where $w_{ij} = h_i^\top X_j h_i \geq 0$ and

$$X_i = \int_0^T e^{At} s_i^\top s_i e^{A^\top t} dt, \quad i = 1,\dots,n. \tag{15}$$

Proof: Note that (9) is equivalent to

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

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 (15), this optimization problem can be written as

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

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

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

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 (14) to the famous maximum edge weight induced biclique problem which is

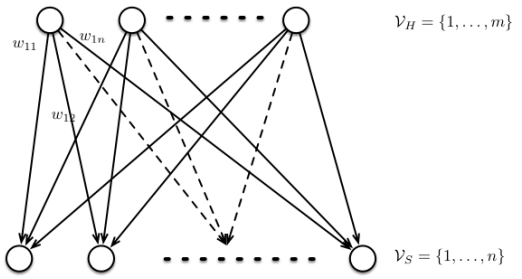

Fig. 1. The bipartite graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ described in Proposition 1.

postulated to be NP-complete in general, see [8]. For more information on different variants of this problem the reader may refer to [8]–[10].

Proposition 3: Define a complete bipartite graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ $\mathcal{V} = \mathcal{V}_H \bigcup \mathcal{V}_S = \{1, \ldots, m\} \bigcup \{1, \ldots, q\}$ and edge set $\mathcal{E} = \mathcal{V}_H \times \mathcal{V}_S$ with edge weights $w_{ij} = h_i^\top X_j h_i \geq 0$ where $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, q\}$. Let $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$ an induced biclique of $\mathcal{G}$ where $\mathcal{V}' = \mathcal{V}_A \bigcup \mathcal{V}_T$, $\mathcal{E} = \mathcal{V}_A \times \mathcal{V}_T$, $\mathcal{V}_A \subseteq \{1, \ldots, m\}$, $\mathcal{V}_T \subseteq \{1, \ldots, n\}$, $|\mathcal{V}_A| = a$, $\mathcal{V}_T = q$, and edge weights w_{ij}, $\forall (i,j) \in \mathcal{E}'$. Solving (14) is equivalent to finding $\mathcal{G}'$ that maximizes $\sum_{(i,j)\in\mathcal{E}'} w_{ij}$.

Proof: Let $\{\beta_i^\star\}_{i=1}^m$ and $\{\gamma_i^\star\}_{i=1}^n$ be the optimal solutions to (14) and the optimum value of the cost function in (14) be given as

$$J^\star = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_i^\star \gamma_j^\star w_{ij}.$$

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 $\mathcal{V} = \mathcal{V}_H \bigcup \mathcal{V}_S = \{1, \ldots, m\} \bigcup \{1, \ldots, q\}$ and edge set $\mathcal{E} = \mathcal{V}_H \times \mathcal{V}_S$ with edge weights $w_{ij} = h_i^\top X_j h_i \geq 0$ where $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, q\}$. 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 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 $\mathcal{G}' = (\mathcal{V}', \mathcal{E}')$, $\mathcal{V}' = \mathcal{V}_A \bigcup \mathcal{V}_T$, $\mathcal{E} = \mathcal{V}_A \times \mathcal{V}_T$, $\mathcal{V}_A \subseteq \{1, \ldots, m\}$, $\mathcal{V}_T \subseteq \{1, \ldots, n\}$, $|\mathcal{V}_A| = a$, $\mathcal{V}_T = q$, and edge weights w_{ij}, $\forall (i,j) \in \mathcal{E}'$. ∎

The bipartite graph of Proposition 3 is depicted in Fig. 1. The optimization problem (14) 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.

We conclude this section by briefly discussing the case where the networked system is described by discrete-time equations. Assume that the attack-free networked system is described by

$$x^+ = Ax + Bu, \quad y = Cx \tag{16}$$

where x^+ denotes the value of x in the next time-step. The corresponding model for the case that there is an attack in the system becomes

$$x^+ = Ax + Bu + H\alpha, \quad y = Cx \tag{17}$$

where α is the a-dimensional *discrete-time attack signal* and $\alpha = [\bar{\delta}[t_a], \ldots, \bar{\delta}[t_a]]^\top$ with $\bar{\delta}[t_a]$ is the discrete-time Dirac function and t_a is an arbitrary *attack time index*. As before, we assume $t_a = 0$. All the earlier problems and solutions can be extended to this case subject to using the following definitions for the finite-time observability Gramians of (7) and (8) and the finite-time controllability Gramian of (10):

$$X_E = \sum_{k=1}^{T} \left(A^\top\right)^k E^\top E A^k, \quad X_C = \sum_{k=1}^{T} \left(A^\top\right)^k C^\top C A^k,$$
$$Y_H = \sum_{k=1}^{T} A^k H H^\top \left(A^\top\right)^k.$$

IV. Applications

In this section, we analyse two networked systems and study the optimal impulsive attack vectors and the corresponding impulsive security indices for each system.

A. Impulsive Attacks in Power Networks

The first system that we consider models the active power flow in a power network. We determine the optimal attack vector for an adversary to launch an impulsive attack. The impulsive 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. To this aim, we consider the classical linearized synchronous machine model [14] for each node of the power network. The behaviour of each bus i can be described by the so-called swing equation:

$$m_i \ddot{\theta}_i + d_i \dot{\theta}_i - P_{mi} = -\sum_{j \in N_i} P_{ij}, \tag{18}$$

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. Considering that there are no power losses nor 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:

$$P_{ij} = k_{ij} \sin(\theta_i - \theta_j) \tag{19}$$

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 (19), rewriting the dynamics of bus i as:

$$m_i \ddot{\theta}_i + d_i \dot{\theta}_i = -\sum_{j \in N_i} k_{ij}(\theta_i - \theta_j) + P_{mi}. \tag{20}$$

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

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

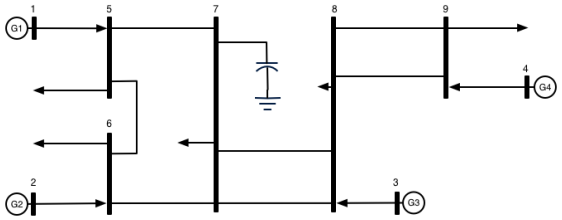

Fig. 2. A 9 bus power network.

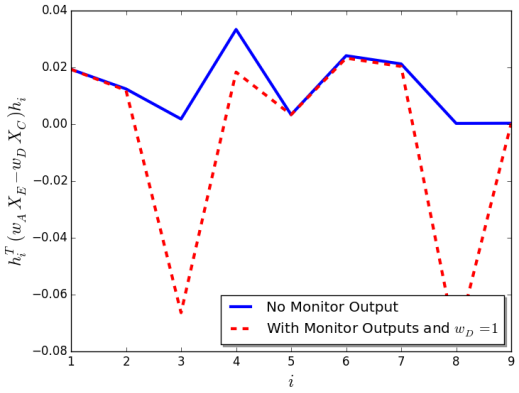

Fig. 3. The value of (13) for different h_i.

and L is the Laplacian matrix of graph $\mathcal{P}(\mathcal{V}_P, \mathcal{E})$ with $N = |\mathcal{V}_P|$ nodes, where 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 $\{i, j\} \in \mathcal{E}$.

In the rest of this section, we consider the 9 bus system depicted in Fig. 2. First, we solve Problem 1 for the case 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 $y = 0$, 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. In the next scenario, 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 impulsive security index for the network in the case where no monitor output was available is 0.33 and is obtained at $\mathcal{T} = \{h_4\}$ and it is 0.23 and is obtained at $\mathcal{T} = \{h_6\}$ for the case where $y = [\theta_8, \dot{\theta}_8]^\top$. In the next scenario, we consider Problem 2 for the same 9 bus network where $a = q = 1$. Choosing $\mathcal{T} = \{s_5\}$ and $\mathcal{A} = \{h_2\}$ correspond to the optimal solution of (9). The value of cost function for different choices of $\mathcal{T}$ and $\mathcal{A}$ are depicted in Fig. 4.

B. Impulsive Attacks in Network Congestion Control

The second networked system that is considered here arises from congestion control in data networks. In this scenario, the attack is a sudden change in the link prices. The attacker's

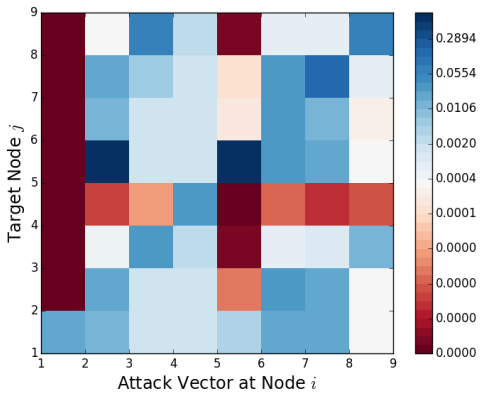

Fig. 4. The value of (9) for different choices of $\mathcal{T}$ and $\mathcal{A}$ where $a = q = 1$ in the 9 bus power network.

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.

One of the most powerful approaches in congestion control is to formulate the problem as a Network Utility Maximization (NUM) has emerged. Many of the existing solutions to the problem are based on the dual decomposition technique introduced in [15], where the optimal bandwidth sharing among N flows in a data network is posed as the optimizer of a convex optimization problem

$$\begin{array}{ll} \underset{x}{\text{maximize}} & \sum_i u_i(x_i) \\ \text{subject to} & Rx \leq c \end{array} \tag{21}$$

In this formulation x_i is the communication rate of flow i, and the strictly concave function $u_i(x_i)$ describes the utility that source i has of communicating at rate x_i. The routing matrix, $R \in \{0, 1\}^{\ell \times N}$ where ℓ is the number of links, has entries R_{li} equal to one if flow i travels through link l and zero otherwise. In other words, the entries of Rx correspond to the total traffic on each of the links, which in turn cannot exceed their capacities $c \in \mathbb{R}^n$. Moreover, we assume that for all link l, there exists a source i whose flow only goes through l, i.e. $R_{li} = 1$ and $R_{l'i} = 0$ for all $l' \neq l$. In the light of this assumption, $Rx \leq c$ in (21) can be replaced with $Rx = c$. Applying dual decompositions (see [16] and [15] for more information), we have

$$x_i^\star(\mu) = \arg\max \quad u_i(z) - z \sum_l R_{li}\mu_l, \tag{22}$$

$$\mu_l^+ = \mu_l + \rho \left(\sum_l R_{li} x_i^\star(\mu) - c_l \right) \tag{23}$$

where μ_l is the Lagrange multiplier associated with link l and ρ is an appropriately chosen constant step-size. Note that the updates can be done locally. For each link, if the traffic demand on the link exceeds capacity, the multiplier is increased, otherwise it is decreased. Furthermore, in this example, we assume that the utility functions are $u_i(x_i) = -\frac{1}{2}(x_i - \bar{x}_i)^2$

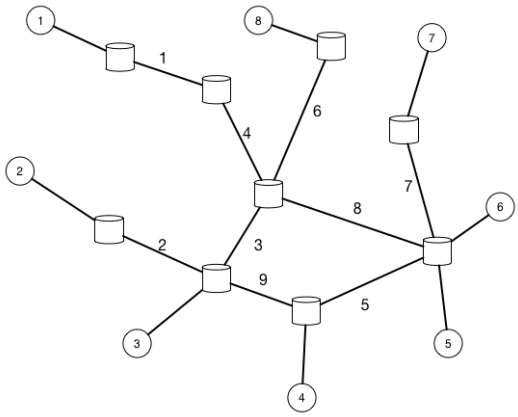

Fig. 5. A network with 9 links and 8 flow sources.

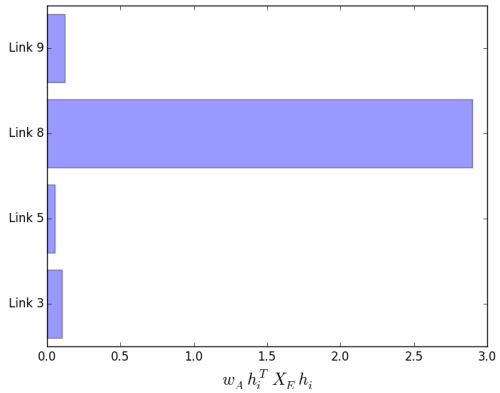

Fig. 6. The value of (6) for the case where $z = \mu_1$ for different attack vectors.

where $\bar{x}_i \gg 0$. Thus, $x_i^\star(\mu) = \bar{x}_i - \sum_l R_{li}\mu_l$. Hence, $A = I - \rho RR^\top$ if the system is written as (16). For the rest of this section, we consider the network depicted in Fig. 5 along with the routing matrix

$$R = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

The target link in this scenario is assumed to be link 1, i.e. $z = \mu_1$. The objective is to find the link among links $\mathcal{V}_H = \{3, 5, 8, 9\}$ where an impulsive change in its price has the highest impact on the price of link 1 and consequently its traffic. The optimal link for an impulsive attack is determined to be link 8. The value of (6) for each of the links is depicted in Fig. 6.

The simulations for this paper are carried out in `Python` and to conform with the guidelines of reproducible research[1] they can be found at [17].

[1]http://reproducibleresearch.net/

V. Conclusion

In this paper, we studied the impact of impulsive attacks on networked systems. We proposed a security index tailored for such attacks and considered the worst case scenario for impulsive 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 impulsive security index to the famous NP-complete problem of maximum induced biclique in graphs. We considered two networked systems, namely power networks and data networks, and studied the impact of impulsive attacks on them.

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] 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.

[9] 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.

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

[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] R. J. Gibbens and F. P. Kelly, "Resource pricing and the evolution of congestion control," *Automatica*, vol. 35, no. 12, pp. 1969–1985, 1999.

[16] S. Low and D. Lapsley, "Optimization flow control - i: Basic algorithm and convergence." *IEEE/ACM Transactions on Networking*, vol. 7 Issue: 6, pp. 861–874, 1999.

[17] 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