Security and Limitations of Cyber-Physical Systems

Exercises, 2015–08–26

Henrik Sandberg and André Teixeira

1. Consider the power networks (i)–(iii) illustrated in Figure 1, where power flow/injection meters are indicated by squares. The security index α_i of a meter i is defined as

$$\begin{aligned} \alpha_i := \min_{\Delta\theta \in \mathbb{R}^{n+1}} \ & \text{card}(H\Delta\theta) \\ \text{subject to} \quad & H(i,:)\Delta\theta = 1, \end{aligned}$$

   where H is the measurement matrix and $\Delta\theta$ is the phase angles of the $n+1$ buses. See [1] for details.

   (a) Construct measurement matrices H for the power networks (pick an arbitrary diagonal nonsingular D).

   (b) Compute the indices α_i for all meters i using a mixed-integer linear program.

   (c) Compute the indices α_i for all meters i (or only bound if exact computation is not possible) by solving the optimization problem (11) in [1].

2. In this problem we shall investigate how protective measures influence the security index, as defined in Problem 1.

   (a) Consider the power network in Figure 2–(i). Assume that it is known a priori that the indicated power injection is exactly zero. How does this constraint influence the security indices of the meters, as compared to the network in Figure 1–(i)? (Hint: With the given constraint, is it possible to simplify the graph topology?)

   (b) Consider the power network in Figure 2–(ii). Assume that the encircled meter is protected, and hence immune to data integrity attacks. How does this constraint influence the security indices of the remaining meters, as compared to the network in Figure 1–(i)? (Hint: Investigate how the weight c in the optimization problem (11) in [1] can be used to affect solutions.)

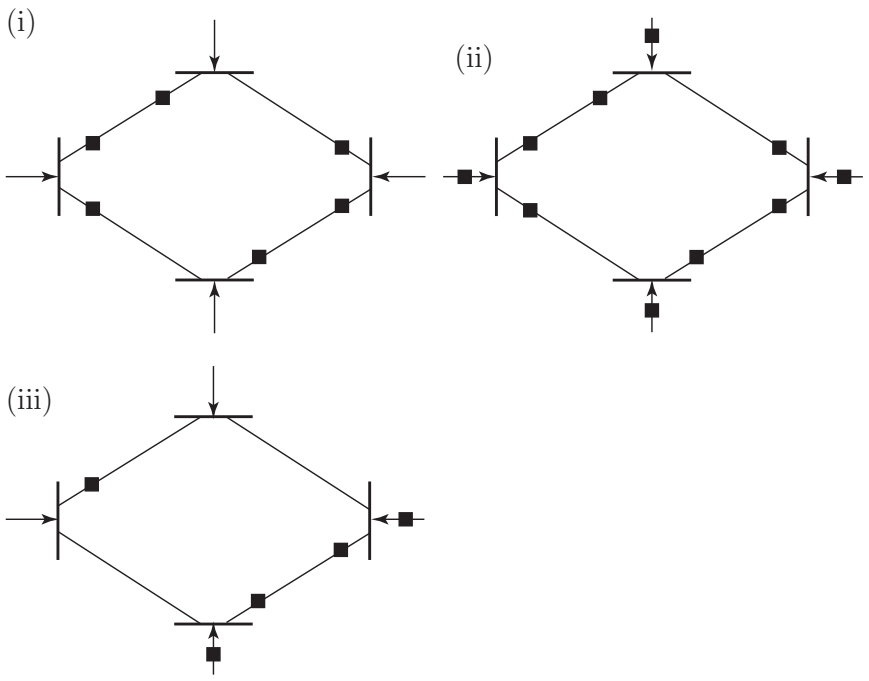

Figure 1: Power networks for Problem 1.

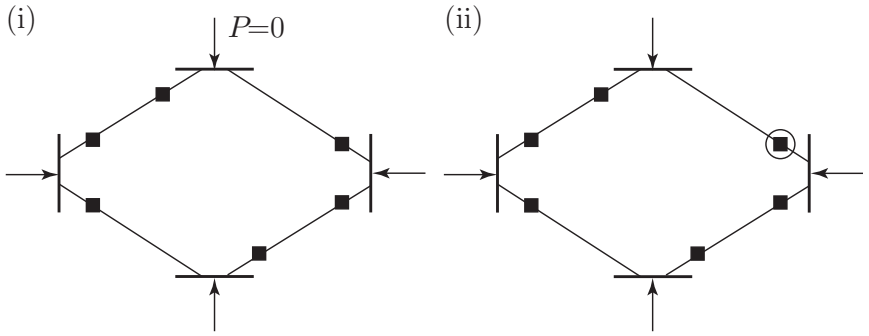

Figure 2: Power networks for Problem 2.

3. In power network observability analysis, so-called *critical k-tuples* are of interest. A critical k-tuple is a set of k meters such that if all these meters fail simultaneously, then observability is lost. However, losing any subset $p < k$ of the meters would not result in the loss of observability. See [2] for details.

   In this problem we shall investigate the relation between critical k-tuples and the security index.

   Suppose a measurement system

   $$\Delta z = H\Delta\theta$$

   is observable, i.e., that H has full column rank. Let us define

   $$\begin{aligned} \Delta\theta^\star := \arg \min_{\Delta\theta\in\mathbb{R}^{n+1}} \ & \mathrm{card}(H\Delta\theta) \\ \text{subject to} \quad & H(i,:)\Delta\theta = 1, \end{aligned} \tag{1}$$

   such that $\alpha_i = \mathrm{card}(H\Delta\theta^\star)$.

   (a) Prove that the meter set $\{j : (H\Delta\theta^\star)_j \neq 0\}$ forms a critical α_i-tuple. [$(H\Delta\theta^\star)_j$ denotes the j-th entry of the vector $H\Delta\theta^\star$.]

   (b) Suppose a critical k-tuple for the measurement system is known. Show that each meter in the tuple has security index k, and how to find a certificate $\Delta\theta^\star$ without solving the optimization problem (1).

4. Consider the dynamical system

   $$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t), \quad x(0) = x_0 \\ y(t) &= Cx(t) + a(t), \\ \left(\begin{bmatrix} y_1(t) \\ y_2(t) \end{bmatrix} \right. &= \left. \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} x(t) + \begin{bmatrix} a_1(t) \\ a_2(t) \end{bmatrix} \right) \end{aligned}$$

   where (A, C) is observable, but (A, C_1) is unobservable.

   (a) Parameterize all undetectable measurement data attacks $a(t)$. (An attack $a(t)$ is undetectable if, and only if, $y(x_0, a, t) = y(x_1, 0, t)$, for all $t \geq 0$ and for some initial state x_1. For details, see Definition 1 in [3].)

   (b) Is it possible (yes/no/not enough information given) to perform undetectable measurement data attacks that only corrupt the measurements $y_2(t)$ (i.e., $a_1(t) \equiv 0$)?

   (c) Is it possible (yes/no/not enough information given) to perform undetectable measurement data attacks that only corrupt the measurements $y_1(t)$ (i.e., $a_2(t) \equiv 0$)?

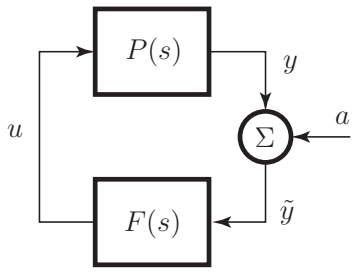

Figure 3: Feedback loop for Problem 6.

5. In Figure 1 in [4], it is indicated that "Zero dynamics attacks" require more model knowledge than "Bias injection attacks". In certain situations it is possible to argue that the reverse holds. When may such an argument be justified?

6. Consider the closed-loop system in Figure 3, with plant transfer function $P(s)$ and controller transfer function $F(s)$. Characterize the undetectable attacks a. Does there exist undetectable attacks a that are independent on the feedback controller $F(s)$?

7. Consider the static system

$$\begin{aligned} y &= Cx + Da, \\ \left(\begin{bmatrix} y_p \\ y_r \end{bmatrix} &= \begin{bmatrix} C_p \\ C_r \end{bmatrix} x + \begin{bmatrix} D_p \\ D_r \end{bmatrix} a \right) \end{aligned}$$

where $\|y_p\|_2^2$ is an impact measure and the attack is stealthy if $\|y_r\|_2^2 \leq 1$ holds. The maximum impact achieved by an attack is characterized as

$$\begin{aligned} J := \max_{a \in \mathbb{R}^{n_a}} \ & \|y_p\|_2^2 \\ \text{subject to} \quad & \|y_r\|_2^2 \leq 1 \end{aligned}$$

   (a) Let $x = 0$, $D_r = I_2$, and $D_p = \text{diag}([2\sqrt{2}, 3\sqrt{2}])\text{R}(\frac{\pi}{4})$, where $R(\theta)$ is a rotation matrix:

$$R(\theta) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}.$$

   Recalling that the set $\{x \in \mathbb{R}^n : x^\top P x \leq 1\}$ represents an ellipsoid in $\mathbb{R}^n$, compute J and $a^\star$. (*Hint: Use a geometric argument with the ellipses* $\|y_r\|_2^2 \leq 1$ *and* $\|y_p\|_2^2 = J$.)

   (b) Let $x = 0$, $D_r = \text{diag}([1\ 0])$, and $D_p = \text{diag}([2\sqrt{2}\ 3\sqrt{2}])\text{R}(\theta)$. For what values of $\theta \in [-\pi, \pi]$ is J unbounded? (*Hint: Use a geometric argument.*)

   (c) For $x = 0$, under what conditions is J unbounded? (*Hint: Consider* D_r *to be singular.*)

8. Consider the discrete-time dynamical system

$$\begin{aligned} x[k+1] &= Ax[k] + Ba[k], \quad x[0] = 0 \\ y[k] &= Cx[k] + Da[k], \\ \left(\begin{bmatrix} y_p[k] \\ y_r[k] \end{bmatrix} \right. &= \left. \begin{bmatrix} C_p \\ C_r \end{bmatrix} x[k] + \begin{bmatrix} D_p \\ D_r \end{bmatrix} a[k] \right) \end{aligned}$$

where $\|y_p\|^2_{\ell_2[0,T]}$ is an impact measure and the attack is stealthy if $\|y_r\|^2_{\ell_2[0,T]} \leq 1$ holds. The maximum impact achieved by an attack over the time-interval $[0, T]$ is characterized as

$$\begin{aligned} J := \max_{a[k] \in \ell_2[0,T]} & \|y_p\|^2_{\ell_2[0,T]} \\ \text{subject to} \quad & \|y_r\|^2_{\ell_2[0,T]} \leq 1 \end{aligned}$$

(a) Given $T < \infty$, parameterize the optimal solution $a^\star$ and J in terms of the lifted representation of the system.

(b) Given $T < \infty$, under what conditions is J unbounded? (*Hint: Compare to Exercise 7c and relate the former result to the null-space of the matrices obtained by lifting the system* (A, B, C_r, D_r).)

(c) Let $T \to \infty$. Under what conditions is J unbounded? Relate them to the zeros of the systems (A, B, C_p, D_p) and (A, B, C_r, D_r). (*Hint: Relate the null-space of the matrices of the lifted system, as* $T \to \infty$*, to the zeros of* (A, B, C_r, D_r).)

9. Consider the discrete-time dynamical system

$$\begin{aligned} x[k+1] &= Ax[k] + BWa[k], \quad x[0] = x_0 \\ y[k] &= Cx[k], \end{aligned}$$

where W is an invertible matrix and the input $a[k]$ is generated as

$$\begin{aligned} \tilde{x}[k+1] &= (A + BF)\tilde{x}[k], \quad \tilde{x}[0] = \tilde{x}_0 \\ a[k] &= F\tilde{x}[k], \end{aligned}$$

with F and $\tilde{x}_0 \neq 0$ such that $C\tilde{x}_0 = 0$ and $(A + BF)\tilde{x}_0 = \lambda \tilde{x}_0$, for some $\lambda \in \mathbb{C}$.

(a) Show that, if $W = I$ and $x_0 = \tilde{x}_0$, then the input signal $a[k]$ is undetectable, i.e., it yields $y[k] = 0$ for all $k \geq 0$. Relate $\tilde{x}_0$, $F\tilde{x}_0$, and λ to the zero dynamics of (A, B, C).

(b) Let $W = I$, $e_0 = x_0 - \tilde{x}_0 \neq 0$, and $\tilde{x}_0 \neq 0$. Characterize the output signal generated by the input signal $a[k]$ in terms of the error variable $e[k] = x[k] - \tilde{x}[k]$. Is the input $a[k]$ still undetectable?

(c) Suppose $x_0 = \tilde{x}_0$, which renders the input $a[k]$ undetectable with respect to the system (A, B, C). To detect the attack $a[k]$, the invertible matrix W may be chosen appropriately, so that $a[k]$ is not undetectable with respect to (A, BW, C).

i. Characterize the perturbations W for which the attack remains undetectable.

ii. Let $W = \alpha I$. Characterize the output signal generated by the input $a[k]$ in terms of the error variable $e[k] = x[k] - \tilde{x}[k]$. For what values of α is the input $a[k]$ detectable? Given the range $\alpha \in (0,\ 2]$, which value of α yields the largest output energy $\|y\|_{\ell_2}^2$?

References

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

[2] K. C. Sou, H. Sandberg, and K. H. Johansson, "Computing critical k-tuples in power networks," *Power Systems, IEEE Transactions on*, vol. 27, no. 3, pp. 1511–1520, Aug 2012.

[3] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *Control Systems, IEEE*, vol. 35, no. 1, pp. 110–127, Feb 2015.

[4] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135 – 148, 2015.