Security constrained control under denial-of-service attacks.

Saurabh Amin[1] Alvaro Cárdenas[2]
Alexandre Bayen[1] Shankar Sastry[2]

[1]Systems engineering, Civil and Environmental Engineering
University of California, Berkeley

[2]Electrical Engineering and Computer Sciences
University of California, Berkeley

TRUST Autumn 2008 Conference

Outline.

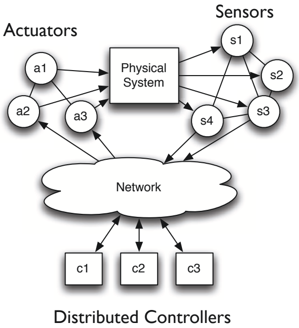
Outline

Motivation to study security of control systems.
- Distributed control systems: vulnerabilities and threats.
- Research challenges for security of control systems.

Our Results/Contribution.
- Taxonomy of attacks to control systems.
- Secure control problem under DoS attacks.

Distributed Control Systems (DCS).

- Sensor-actuator networks that monitor and control physical processes,
- Safety-critical: their disruption can cause irreparable harm.



New Vulnerabilities and New Threats.

- Controllers are computers,
- Networked,
- Commodity IT solutions,
- Open design
- New functionalities,
- Highly skilled global workforce,
- Cybercrime

Vulnerabilities can be exploited.

Experimental cyber-attack caused generator to self-destruct.

Polish teen hacks city's tram system with homemade transmitter to derail four trams

Sewage control system exploited by insider to cause sewage to flood the surroundings.

LA' traffic engineers hack computer system that controls traffic lights.

Outline

Motivation to study security of control systems.
- Distributed control systems: vulnerabilities and threats.
- Research challenges for security of control systems.

Our Results/Contribution.
- Taxonomy of attacks to control systems.
- Secure control problem under DoS attacks.

What is new and fundamentally different.

- Studying security of control systems is important,
- Does the problem pose new research challenges beyond previous research in
  - Traditional IT security
  - Robust and networked control

Research challenges.

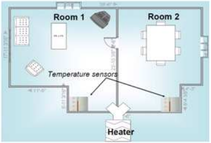
- Investigate realistic **models of attacks** to control systems from the "systems viewpoint".
- Understand the **consequences of an attack**: How can the adversary select an attack strategy after obtaining unauthorized access to some control system components?
- Design **attack-detection algorithms**: Based on measurements, how to identify if attacker is tampering with control and/or sensor data?
- Design **attack-resilient algorithms and architectures**: After detecting an attack, how to change state estimates and control commands to improve system's resiliency?

Outline

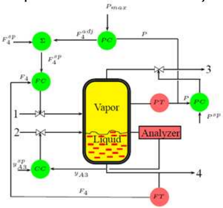
- Motivation to study security of control systems.
  - Distributed control systems: vulnerabilities and threats.
  - Research challenges for security of control systems.
- Our Results/Contribution.
  - Taxonomy of attacks to control systems.
  - Secure control problem under DoS attacks.

Example cases

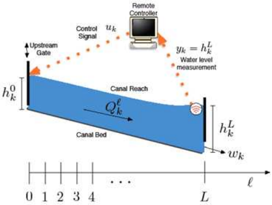
Room temperature control system



Two-phase chemical reactor system



Water canal control system

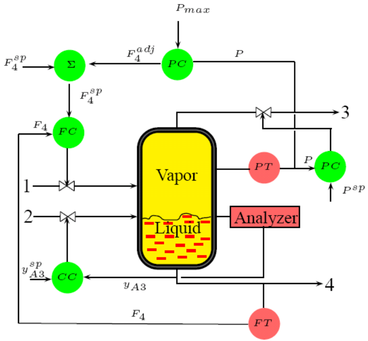


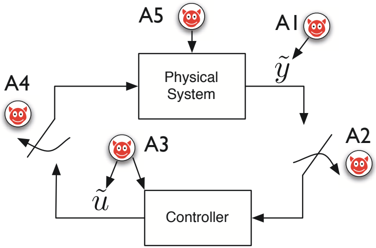
Traffic estimation system based on GPS phones

Operational goals and security attributes.

System	Model	Operational goal	Security attribute
Temperature control	linear/hybrid ODE	safety	random delay
Chemical reactor	**linear/nonlin ODE**	**safety, stability, MPC**	**DoS, deception**
Canal control	linear PDE	safety, perf. max.	DoS, demand fluctuation
Traffic estimation	nonlinear PDE	estimation accuracy	location privacy

Attacks on chemical reactor control system.





*A*1 & *A*3: integrity attacks; *A*2 & *A*4: DoS attacks; *A*5: Physical attack.

Effect of attacks on safety and performance.

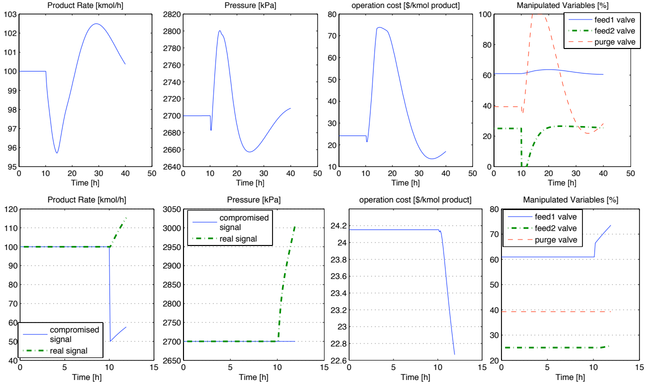


Figure: a. DoS attack on controller. b. DoS & deception attacks on sensors.

Outline

- Motivation to study security of control systems.
  - Distributed control systems: vulnerabilities and threats.
  - Research challenges for security of control systems.
- Our Results/Contribution.
  - Taxonomy of attacks to control systems.
  - Secure control problem under DoS attacks.

Secure control problem for DoS attacks.

Availability

The ability of a control system of being accessible and usable upon demand; lack of availability results in DoS of sensor and control data.

Secure control problem for DoS attacks

To design a (predictive) control strategy that (1) minimizes operating costs, and/or (2) satisfies safety constraints, and/or (3) maintains closed-loop stability; by surviving DoS attacks to the measurements and control data under a well-defined adversary model.

Secure control under DoS attacks.

Design robust (minimax) control for system under DoS attacks (γ_k, ν_k):

$$\begin{aligned} x_{k+1} &= Ax_k + Bu_k^a + w_k & k &= 0, \dots, N-1, \\ u_k^a &= \nu_k u_k & \nu_k &\in \{0,1\}, \\ x_k^a &= \gamma_k x_k & \gamma_k &\in \{0,1\}, \end{aligned}$$

to minimize

$$J_N(\bar{x}, P_0, u_0^{N-1}) = \mathbf{E}\left[x_N^\top Q^{xx} x_N + \sum_{k=0}^{N-1} \begin{pmatrix} x_k \\ \nu_k u_k \end{pmatrix}^\top Q \begin{pmatrix} x_k \\ \nu_k u_k \end{pmatrix} \middle| u_0^{N-1}, \bar{x}, P_0 \right]$$

subject to power constraints in an expected sense

$$\mathbf{E}\left[\begin{pmatrix} x_k \\ \nu_k u_k \end{pmatrix}^\top H_i \begin{pmatrix} x_k \\ \nu_k u_k \end{pmatrix} \right] \leq \beta_i \qquad \text{for } i = 1, \dots, L, \text{ and } k = 0, \dots, N-1$$

as well as safety constraints in a probabilistic sense

$$\mathbf{P}\left[(Cx_k + \nu_k D u_k) \in \mathcal{T} \right] \geq (1 - \varepsilon) \qquad \text{for } k = 0, \dots, N-1$$

Attack models.

Random adversary

$$\mathcal{A}_{\text{Ber}(\bar{\gamma},\bar{\nu})} = \{(\gamma_0^{N-1}, \nu_0^{N-1}) | \mathbf{P}(\gamma_k = 1) = \bar{\gamma}, \mathbf{P}(\nu_k = 1) = \bar{\nu},\ k = 0, \dots, N-1\}.$$

Resource constrained adversary

$$\mathcal{A}_{pq} = \{(\gamma_0^{N-1}, \nu_0^{N-1}) \in \{0,1\}^{2N} |\ \| \gamma_0^{N-1} \|_1 \geq N - p, \| \nu_0^{N-1} \|_1 \geq N - q\},$$

Advsersary with internal state

Stochastic dynamical model of adversary's cognitive functions composed with control system.

Secure control problem for random adversary.

Theorem

The solution to the secure control problem for the $(\gamma_0^{N-1}, \nu_0^{N-1}) \in \mathcal{A}_{Ber(\bar{\gamma},\bar{\nu})}$ attack model using the affine error-feedback parameterization

$$u_k = u_k^\circ + \sum_{j=0}^{k} \gamma_j M_{k,j}(x_j - \hat{x}_{j|j-1}), \qquad k = 0, \ldots, N-1$$

can be obtained as a solution of a semi-definite program. Here $u_k^\circ \in \Re^m$ is the open-loop part of the control, and $M_{k,j} \in \Re^{m \times n}$ is the feedback gain or the recourse at time k from sensor measurement x_j.

Optimal attack plan for resource constrained attacker.

Theorem

The optimal attack plan $\{\gamma_0^{N-1^*}, \nu_0^{N-1^*}\}$ that maximizes the minimum cost for the $\mathcal{A}_{pq}$ attack model is the solution of the following:

$$(\gamma_k^*, \nu_k^*) = \underset{\substack{\gamma_k, \nu_k \in \{0,1\}^2 \\ \|\gamma_k^{N-1}\|_1 \geq (N-p) \\ \|\nu_k^{N-1}\|_1 \geq (N-q)}}{\arg\max} \mathbf{E}[x_k^\top S_k x_k | \mathcal{I}_k] + c_k$$

$$S_k = A^\top S_{k+1} A + Q^{xx} - \nu_{k+1}^* A^\top S_{k+1} B (B^\top S_{k+1} B + Q^{uu})^{-1} B^\top S_{k+1} A$$

$$c_k = \mathbf{Tr}\{(A^\top S_{k+1} A + Q^{xx} - S_k)\Sigma_{k|k}\} + \mathbf{Tr}(S_{k+1} Q) + c_{k+1}$$

starting with $S_N = Q^{xx}$ *and* $c_N = 0$ *and*

$$\Sigma_{k|k} = \prod_{j=0}^{k} (1 - \gamma_j) A^k P_0 A^{k\top} + \sum_{i=0}^{k-1} \prod_{j=(k-i)}^{k} (1 - \gamma_j) A^i Q A^{i\top}.$$

Summary and current focus.

- Defined secure control problem for random and resource-constrained adversaries.
- Controller synthesis using convex and dynamic programming.
- Current focus on
  - Proving closed-loop stability for receding horizon control law,
  - Using IDS to detect coordinated integrity attacks on sensor and control channels using limited number of sensors,
- Framework extensible to other systems such as highway traffic estimation using mobile phone data under privacy constraints.

A. Cárdenas, S. Amin, S. Sastry.
Research challenges for the security of control systems.
HotSec, 2008.

S. Amin, A. Bayen, A. Cárdenas, S. Sastry.
Security constrained control under DoS attacks.
Under review, 2008.