STEALTHY CONTROL SIGNAL ATTACKS IN SCALAR LQG SYSTEMS

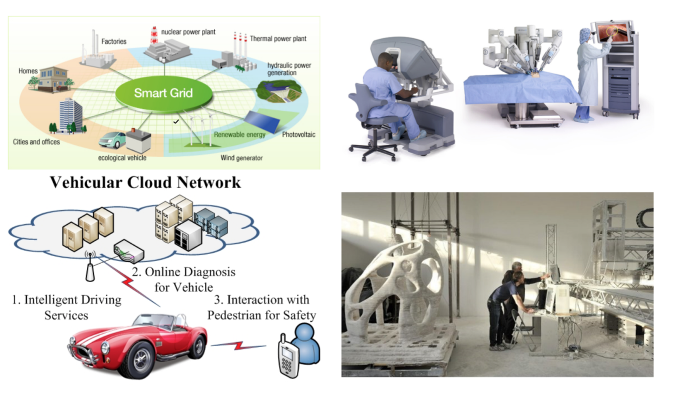
Ruochi Zhang, Parv Venkitasubramaniam

December 14, 2015

Electrical and Computer Engineering
Lehigh University, USA
{*ruz614,parv.v*}*@lehigh.edu*

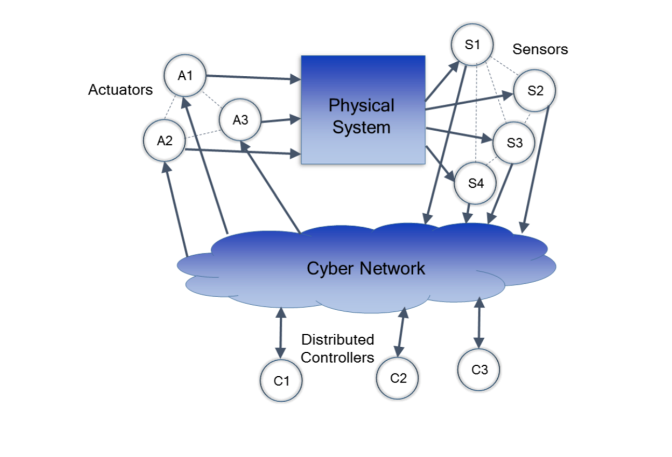
INTRODUCTION

- Cyber-physical systems



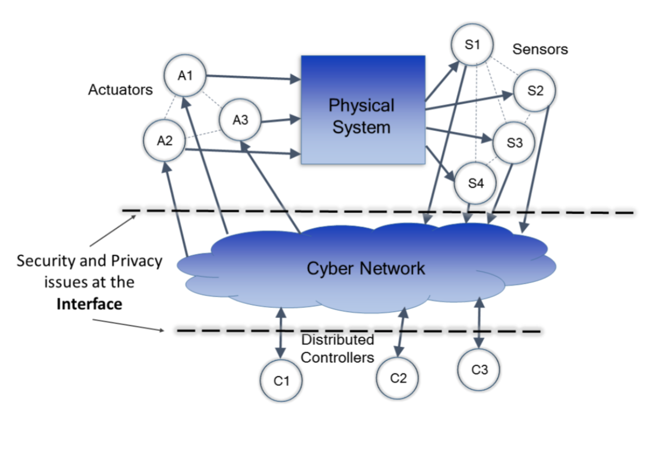
INTRODUCTION: CYBER-PHYSICAL SYSTEMS

- Cyber-physical systems: structure



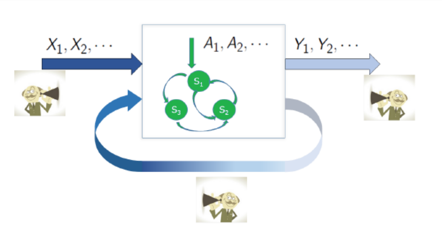
INTRODUCTION: CYBER-PHYSICAL SYSTEMS

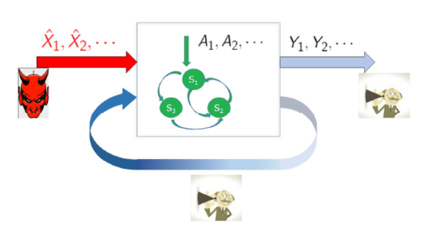
- Cyber-physical systems: security issues



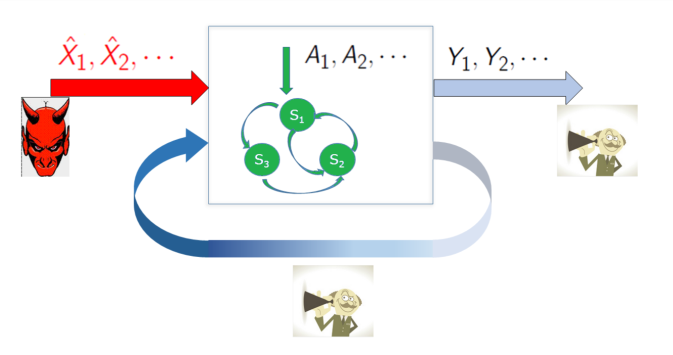
INTRODUCTION: CYBER-PHYSICAL SYSTEMS

- Security vulnerabilities in cyber communication





- False data injection



False data injection

- wireless sensor networks
- smart grids
- computer systems

- Linear-quadratic-Gaussian (LQG) control systems

- H. Fawzi *et. al.* 2011, “Secure state-estimation for dynamical systems under active adversaries” : LQG systems data injection attacks, resistance to specific detection schemes
- C. Bai *et. al.* 2014, “On kalman filtering in the presence of a compromised sensor: Fundamental performance bounds”:
  Infinite horizon stationary LQG systems with the objective of increasing the estimation error of the supporting Kalman filter

PROBLEM FORMULATION

LQG SYSTEM MODEL

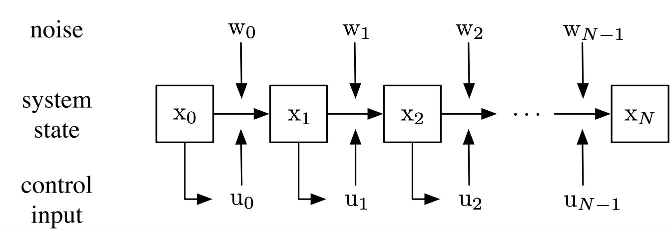


Figure 1: Single-input single-output finite horizon LQG system.

$$\mathrm{x}_{k+1} = A_k \mathrm{x}_k + B_k \mathrm{u}_k + \mathrm{w}_k, \quad \mathrm{w}_k \sim \mathcal{N}(0, \sigma_k^2)$$

Goal of the controller: minimize the quadratic cost

$$J = \mathbb{E}\left\{ Q_N \mathrm{x}_N^2 + \sum_{k=0}^{N-1} (Q_k \mathrm{x}_k^2 + R_k \mathrm{u}_k^2) \right\}$$

THE POLICY OF THE CONTROLLER

Optimal input u_k^*: linear function of state x_k

$$\mathrm{u}_k^* = L_k \mathrm{x}_k$$

L_k, F_k, G_k are given recursively by

$$\begin{aligned}
F_k &= Q_k + F_{k+1} A_k^2 - \frac{F_{k+1}^2 A_k^2 B_k^2}{R_k + F_{k+1} B_k^2} \\
G_k &= R_k + F_{k+1} B_k^2 \\
L_k &= -\frac{F_{k+1} A_k B_k}{R_k + F_{k+1} B_k^2} \\
F_N &= Q_N \\
G_N &= 0
\end{aligned}$$

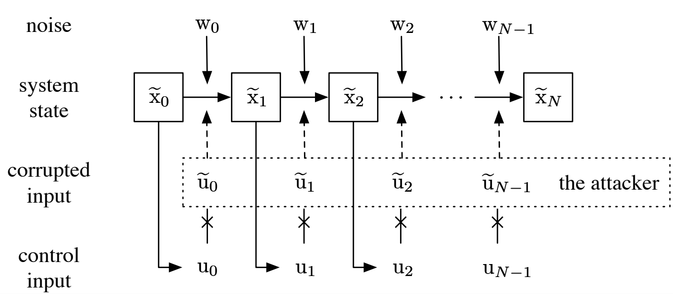


Figure 2: The corrupted LQG control system.

$$\widetilde{x}_{k+1} = A_k \widetilde{x}_k + B_k \widetilde{u}_k + w_k, \qquad k = 0, 1, \cdots, N-1$$

THE ATTACKER'S GOAL

The attacker's goal: maximize

$$\widetilde{J}(\pi) = \mathbb{E}\left\{ Q_N \widetilde{\mathrm{x}}_N^2 + \sum_{k=0}^{N-1} (Q_k \widetilde{\mathrm{x}}_k^2 + R_k \widetilde{\mathrm{u}}_k^2) \right\}$$

- Infinite power?
- Need constraint on stealthiness (stealth)

Definition: Kullback-Leibler divergence

Let x_1^k and y_1^k be to random sequences with probability density functions (p.d.f.) $f_{\mathrm{x}_1^k}$ and $f_{y_1^k}$, respectively. If $f_{\mathrm{y}_1^k}(\xi_1^k) = 0$ implies $f_{\mathrm{x}_1^k}(\xi_1^k) = 0$ for all $\xi_1^k \in \mathbb{R}^k$,

$$D(\mathrm{x}_1^k || \mathrm{y}_1^k) := \int_{\{\xi_1^k | f_{\mathrm{x}_1^k}(\xi_1^k) > 0\}} \log \frac{f_{\mathrm{x}_1^k}(\xi_1^k)}{f_{\mathrm{y}_1^k}(\xi_1^k)} f_{\mathrm{x}_1^k}(\xi_1^k) \mathrm{d}\xi_1^k$$

- Measure of statistical deviation
- Assume: controller knows the attack policy

THE PROBLEM

Attacker's reward:

$$S(\pi) = \widetilde{J}(\pi) - J$$

Attacker's stealthiness:

$$D(\pi) = D(\widetilde{\mathrm{x}}_1^N || \mathrm{x}_1^N)$$

The problem

Given $\delta > 0$, find the optimal policy π^* that

$$\text{minimize } D(\pi), \text{ subject to } S(\pi) \geq \delta$$

MAIN RESULTS

The optimal attack is

$$\widetilde{\mathrm{u}}_k = \mathrm{u}_k + \widetilde{\mathrm{v}}_k$$

- The attacker adds noises into inputs at each step.
- Zero-mean, Gaussian, and independent of system dynamics.

Theorem (Optimal Attack)

The optimal attack subject to $S(\pi) \geq \delta$ is given by

$$\widetilde{\mathrm{v}}_k := \widetilde{\mathrm{u}}_k - \mathrm{u}_k \sim \mathcal{N}(0, \frac{\delta_k}{G_k})$$

independent of the system dynamics at every step. The δ_k is given by

$$\delta_k = \frac{1}{c_k - \theta} - \frac{1}{c_k}$$

where $c_k = \frac{B_k^2}{\sigma_k^2 G_k}$, and $0 < \theta < \min_{0 \leq k \leq N-1} c_k$ is a constant such that

$$\sum_{k=0}^{N-1} \frac{1}{c_k - \theta} - \sum_{k=0}^{N-1} \frac{1}{c_k} = \delta$$

Stationary system: if $c_k = \frac{B_k^2}{\sigma_k^2 G_k} = c$ for every k, the optimal attack will be

$$\widetilde{\mathrm{v}}_k \sim \mathcal{N}(0, \frac{\delta}{NG_k})$$

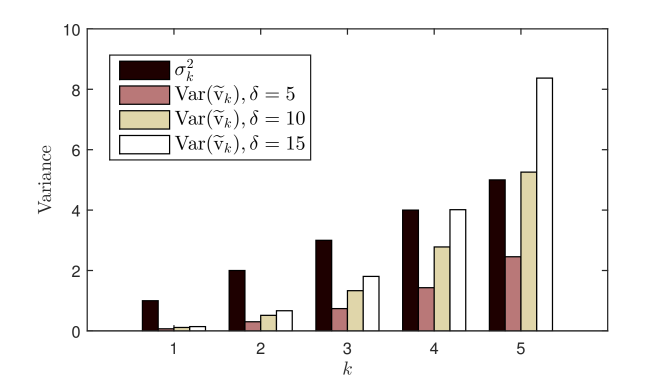


Figure 3: Variance of optimal attack $\widetilde{\mathrm{v}}_k$ in a simple LQG system. $N = 5$, $Q_k = 1$, $R_k = 0$, $A_k = 1$, $B_k = 1$, and $\sigma_k^2 = k$ for every k.

OPTIMAL TRADEOFF

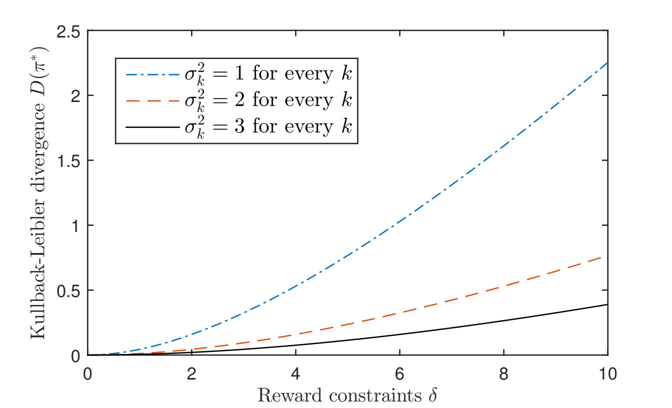


Figure 4: Kullback-Leibler divergence vs reward constraint for constant parameter LQG systems with different noise levels. $Q_k = 1$, $R_k = 0$, $A_k = 1$, and $B_k = 1$

PROOF OUTLINE

PROOF OUTLINE: SINGLE-STEP PROBLEM

Single-step problem:

$$\mathrm{x}_1 = A_0\mathrm{x}_0 + B_0\mathrm{u}_0 + \mathrm{w}_0$$
$$\widetilde{\mathrm{x}}_1 = A_0\mathrm{x}_0 + B_0\mathrm{u}_0 + B_0\widetilde{\mathrm{v}}_0 + \mathrm{w}_0$$

KL Divergence and Reward:

$$D(\widetilde{\mathrm{x}}_1||\mathrm{x}_1) = D(B_0\widetilde{\mathrm{v}}_0 + \mathrm{w}_0||\mathrm{w}_0)$$
$$S(\pi) = G_0\mathbb{E}\{\widetilde{\mathrm{v}}_0^2\}$$

Goal:

minimize $D(B_0\widetilde{\mathrm{v}}_0 + \mathrm{w}_0||\mathrm{w}_0),$ subject to $\mathbb{E}\{\widetilde{\mathrm{v}}_0^2\} \geq \delta/G_0$

PROOF OUTLINE: SINGLE-STEP PROBLEM

$$
\begin{aligned}
D(B_0\widetilde{\mathrm{v}}_0 + \mathrm{w}_0 || \mathrm{w}_0) = & \frac{1}{2}\log(2\pi e \sigma_0^2) + \frac{B_0^2 \mathbb{E}\{\widetilde{\mathrm{v}}_0^2\}}{2\sigma_0^2} \\
& - h(B_0\widetilde{\mathrm{v}}_0 + \mathrm{w}_0)
\end{aligned}
$$

- maximum entropy theorem
- $\widetilde{\mathrm{v}}_0 \sim \mathcal{N}(0, \frac{\delta}{G_0})$ is optimal

PROOF OUTLINE: MULTI-STEP PROBLEM

The reward of a policy π can be expressed as sum of single step rewards,

$$S(\pi) = \sum_{k=0}^{N-1} S_k(\pi)$$

where the single step reward S_k is given by

$$S_k(\pi) = G_k \mathbb{E}\{\widetilde{\mathrm{v}}_k^2\}, \qquad k = 0, 1, \cdots, N-1$$

PROOF OUTLINE: MULTI-STEP PROBLEM

Similarly, the KLD of a policy π can be expressed as sum of single step KLDs,

$$D(\pi) = \sum_{k=0}^{N-1} D_k(\pi)$$

where $D_k(\pi)$ is the single step KLD

$$\begin{aligned} D_0(\pi) &= D(\widetilde{\mathrm{x}}_1 || \mathrm{x}_1) \\ D_k(\pi) &= \int f_{\widetilde{\mathrm{x}}_1^k}(x_1^k) D(\widetilde{\mathrm{x}}_{k+1} || \mathrm{x}_{k+1} | x_1^k) \mathrm{d}x_1^k, \\ & \qquad k = 1, 2, \cdots, N-1 \end{aligned}$$

PROOF OUTLINE: MULTI-STEP PROBLEM

Divide total reward constraint into stepwise:

$$\delta = \sum_{k=0}^{N-1} \delta_k, \qquad \delta_k \geq 0$$

- For each k, solve a single-step problem

Stepwise optimization

Given $\delta_k > 0$, find the optimal policy π^* that

$$\text{minimize } D_k(\pi), \text{ subject to } S_k(\pi) \geq \delta_k$$

- Memoryless
- $\widetilde{\mathrm{v}}_k \sim \mathcal{N}(0, \frac{\delta_k}{G_k})$ is optimal with single-step constraint $S_k(\pi) \geq \delta_k$.

- The optimal attack should be stepwise optimal
- It suffices to solve

Optimal allocation

Given $\delta > 0$, find the optimal allocation $\{\delta_k\}_{k=0}^{N-1}$ that

$$\text{minimize } \sum_{k=0}^{N-1} D_k^*(\pi), \text{ subject to } \delta_k \geq 0, \sum_{k=0}^{N-1} \delta_k = \delta$$

Theorem (Optimal Attack)

The optimal attack subject to $S(\pi) \geq \delta$ is given by

$$\widetilde{\mathrm{v}}_k := \widetilde{\mathrm{u}}_k - \mathrm{u}_k \sim \mathcal{N}(0, \frac{\delta_k}{G_k})$$

independent of the system dynamics at every step. The δ_k is given by

$$\delta_k = \frac{1}{c_k - \theta} - \frac{1}{c_k}$$

where $c_k = \frac{B_k^2}{\sigma_k^2 G_k}$, and $0 < \theta < \min_{0 \leq k \leq N-1} c_k$ is a constant such that

$$\sum_{k=0}^{N-1} \frac{1}{c_k - \theta} - \sum_{k=0}^{N-1} \frac{1}{c_k} = \delta$$

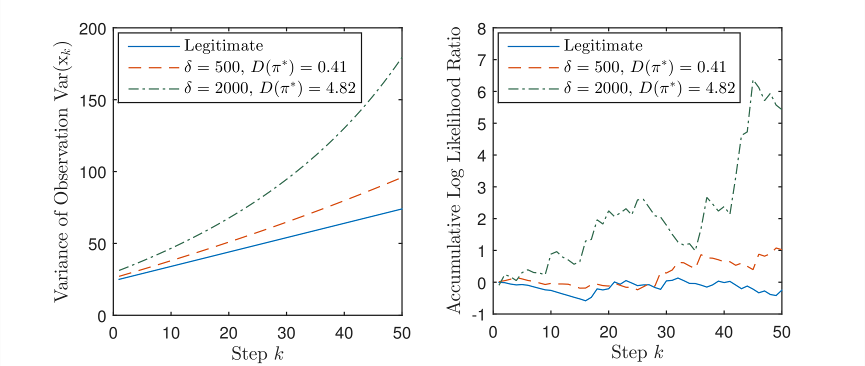


Figure 5: Legitimate and Falsified dynamics in a scalar LQG system: $N = 50$, $A_k = B_k = Q_k = 1$, $R_k = 0$ and $\sigma_k^2 = k + 25 \quad \forall k$

FUTURE WORKS

- Vector LQG systems
- Imperfect observations
- Attack under specific detection schemes

QUESTIONS?