

# Security of CPS

Bruno Sinopoli

## Elements of security in CPS

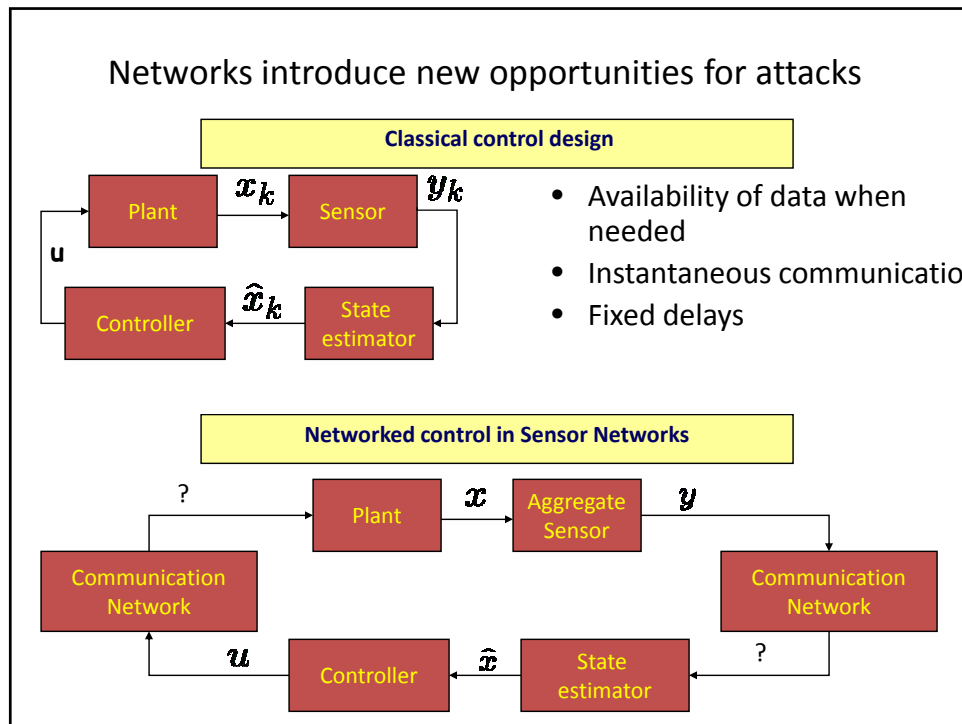
- Threat model
  - Type of attacks
- Detection methods
  - Model based, software-based, data driven
- Survivability
  - attack tolerant
- Restoration
  - Reconfigurable systems

## CPS security: models, challenges opportunities

- What are the unique characteristics of CPS
  - Threat models are different
    - IT attacks affect computing, communication
      - Availability, integrity, replay attacks
    - Physical attacks change the physical system (cut a transmission line)
    - IT and Physical attacks are CPS attacks
    - Unique threats to CPS involve time
      - Value of information decreases with time
      - Delays, time synch attacks
    - Energy must be included in the model
- How do unique properties of CPS affect security?
  - Coupling with physical systems
  - Humans in the loop
  - Challenge
    - Response needs to satisfy dynamic constraints
    - Operational continuity must be guaranteed
  - An opportunity
    - Dynamical systems introduces inertia (~delay) in the attack
    - Provides time to react
    - Use physical models to detect cyber attacks
    - Use data to detect physical attacks

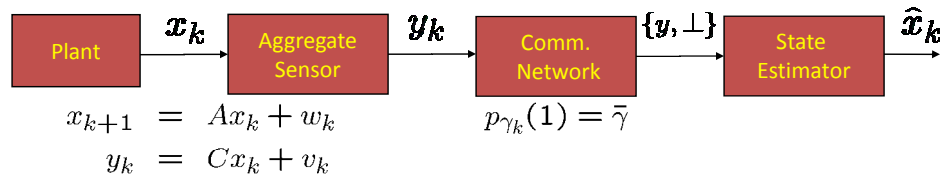
## IT security vs CPS security

- Attack prevention methods existing in IT security can be used
- Some detection schemes are reusable
- Model based methods need to be used
  - Detection
  - Survivable solutions
  - Reconfiguration

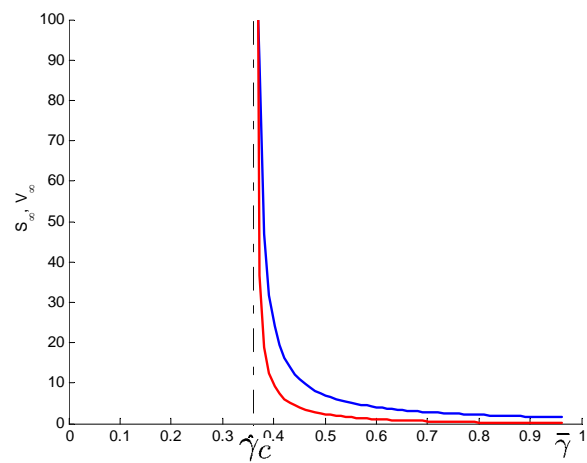


## Jamming attacks

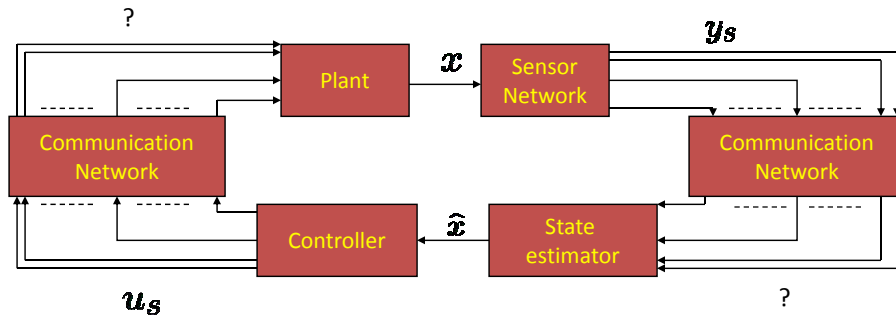
## Optimal estimation over erasure channels



## Fundamental limitations



## Networked Control System: TCP-like with multiple channels



Questions:

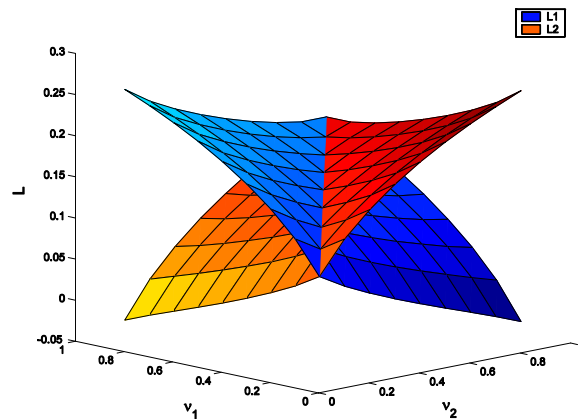
Given a statistical description of the communication channels:

- How do you send sensory information so as to maximize estimation performance?
- How do you design and send control inputs to the actuators?

## Example

- Consider the following  $x(t+1) = -0.5x(t) + \begin{pmatrix} 1 & 1 \end{pmatrix} u(t)$

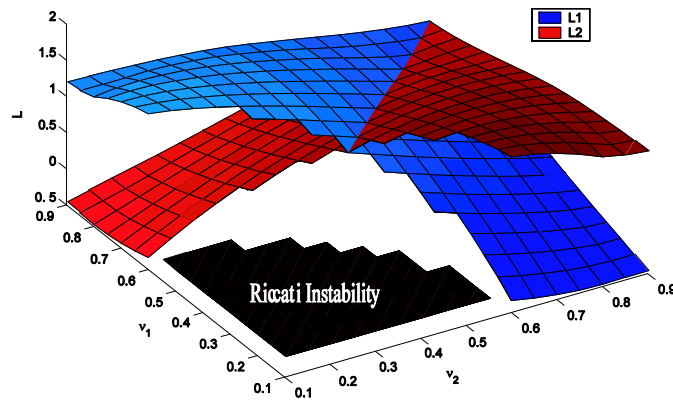
Constant Gain vs Arrival Rate



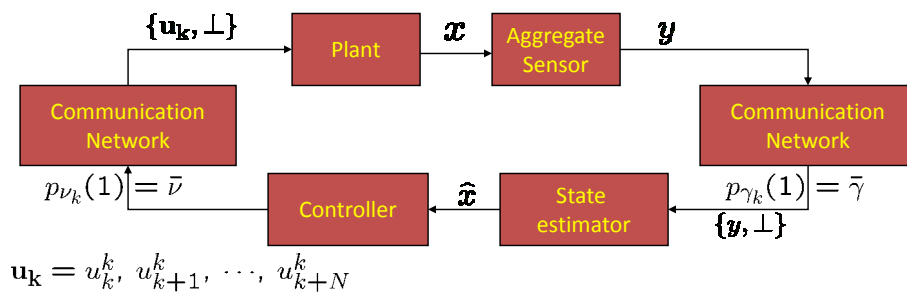
## Unstable plant

$$x(t+1) = -1.6x(t) + \begin{pmatrix} 1 & 1 \end{pmatrix} u(t)$$

CONTROL GAIN VS ARRIVAL RATE

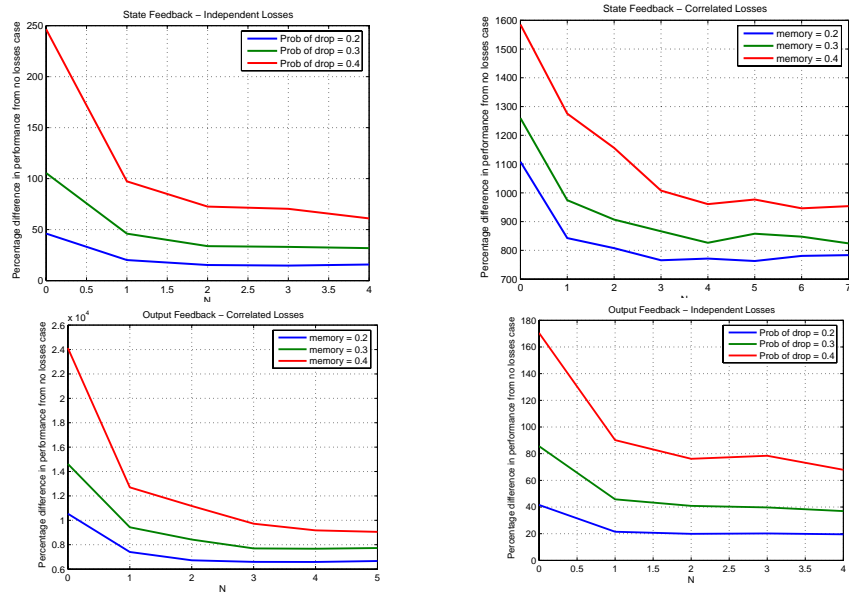


## Receding Horizon Networked Control



- Separation principle holds
- Stability is preserved under the given channel model
- The optimal estimator and controller are still linear
- What is the optimal horizon length?

## Cost vs. length of horizon



## Current work

- Scada testbeds
- Software-based attestation