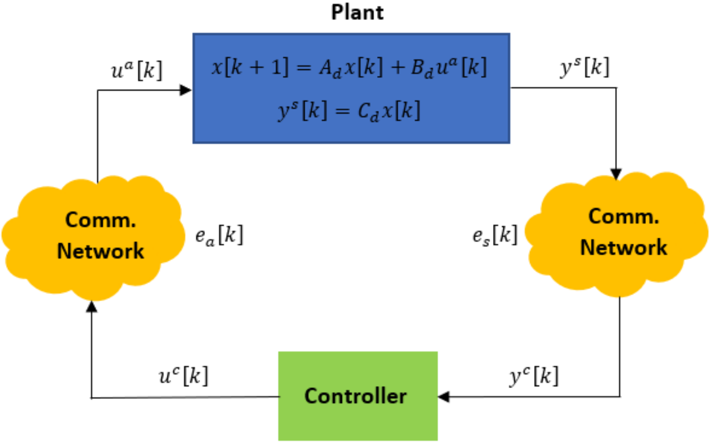
ECE 68000: MODERN AUTOMATIC CONTROL

Professor Stan Żak

Modeling Networked Control Systems Corrupted by Unknown Input and Output Sparse Errors

Networked Control System Corrupted by Unknown Input and Output Sparse Errors



Plant Design Model

$$\left.\begin{array}{rcl}\boldsymbol{x}[k+1] & = & \boldsymbol{A}\boldsymbol{x}[k]+\boldsymbol{B}\boldsymbol{u}^a[k] \\ \boldsymbol{y}^s[k] & = & \boldsymbol{C}\boldsymbol{x}[k]\end{array}\right\}$$

where

- $\boldsymbol{A} \in \mathbb{R}^{n\times n}$, $\boldsymbol{B} \in \mathbb{R}^{n\times m}$, $\boldsymbol{C} \in \mathbb{R}^{p\times n}$
- $\boldsymbol{B}$ full column rank, that is, $\operatorname{rank} \boldsymbol{B} = m$
- $\boldsymbol{u}^a[k] \in \mathbb{R}^m$—input received by actuators
- $\boldsymbol{y}^s[k] \in \mathbb{R}^p$—output measured by sensors

Modeling Malicious Attacks on Sensors

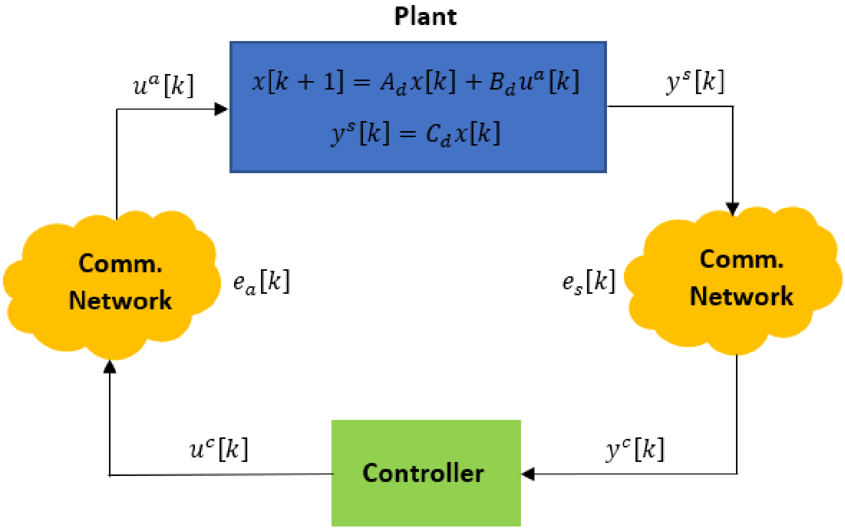
- Sensor measurements, $\boldsymbol{y}^s[k]$, are being sent to the controller through a communication network
- Malicious attacks cause packet drops in the communication network
- Malicious packet drops model:

$$\boldsymbol{\Gamma}(k) = \mathrm{diag}\{\gamma_1(k), \gamma_2(k), \cdots, \gamma_p(k)\}$$

  where $\gamma_i(k), i = 1, \ldots, p$ are Boolean variables, $\gamma_i(k) = 1$ if the packet is correctly received; $\gamma_i(k) = 0$ if the packet is dropped
- Signal received by the controller:

$$\boldsymbol{y}^c[k] = \boldsymbol{\Gamma}(k)\boldsymbol{y}^s[k]$$

NCS


Plant
$x[k+1] = A_d x[k] + B_d u^a[k]$
$y^s[k] = C_d x[k]$
$u^a[k]$
$y^s[k]$
Comm. Network
$e_a[k]$
$e_s[k]$
Comm. Network
$u^c[k]$
Controller
$y^c[k]$

Modeling Malicious Attacks on Actuators

- The control signal is being sent to the plant through a communication network
- Malicious packet drops model:

$$\mathbf{\Lambda}(k) = \mathrm{diag}\{\lambda_1(k), \lambda_2(k), \cdots, \lambda_m(k)\}$$

  where $\lambda_i(k), i = 1, \ldots, m$ are Boolean variables, $\lambda_i(k) = 1$ if the packet is correctly received; $\lambda_i(k) = 0$ if the packet is dropped by the actuator
- Signal received by the actuator:

$$\boldsymbol{u}^a[k] = \mathbf{\Lambda}(k)\boldsymbol{u}^c[k]$$

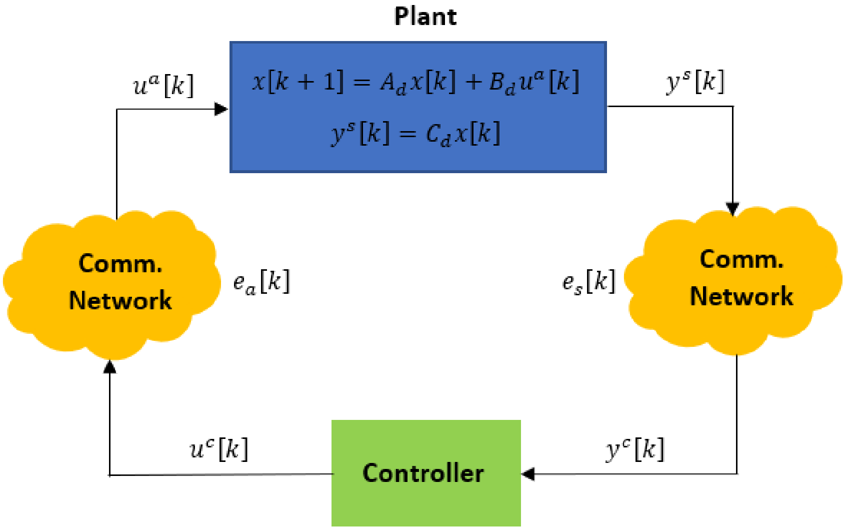
Errors in communication between sensors and the controller

- Network communication errors in the communication flow from the sensor to the controller—$\boldsymbol{e}_s[k]$
- Hence,
$$\boldsymbol{e}_s[k] = \boldsymbol{y}^c[k] - \boldsymbol{y}^s[k] \in \mathbb{R}^p$$

Errors in communication between the controller and actuators

- Errors in the communication between the controller to the actuator—$\boldsymbol{e}_a[k]$
- Hence,
$$\boldsymbol{e}_a[k] = \boldsymbol{u}^a[k] - \boldsymbol{u}^c[k] \in \mathbb{R}^m$$

NCS considered



NCS model

- Let $\overline{\mathbf{\Gamma}}(k) = \mathbf{\Gamma}(k) - \boldsymbol{I}_p \in \mathbb{R}^{p \times p}$ and $\overline{\mathbf{\Lambda}}(k) = \mathbf{\Lambda}(k) - \boldsymbol{I}_m \in \mathbb{R}^{m \times m}$
- Then
$$\boldsymbol{e}_s[k] = \overline{\mathbf{\Gamma}}(k)\boldsymbol{y}^s[k] \text{ and } \boldsymbol{e}_a[k] = \overline{\mathbf{\Lambda}}(k)\boldsymbol{u}^c[k]$$
- We analyze the case when malicious packet drops are sparse
- The system model under consideration
$$\left.\begin{array}{rcl} \boldsymbol{x}[k+1] & = & \boldsymbol{A}\boldsymbol{x}[k] + \boldsymbol{B}(\boldsymbol{u}^c[k] + \boldsymbol{e}_a[k]) \\ \boldsymbol{y}^c[k] & = & \boldsymbol{C}\boldsymbol{x}[k] + \boldsymbol{e}_s[k] \end{array}\right\}$$
- **Objective**: obtain an estimate of the state $\boldsymbol{x}[k]$ of the NCS in the presence of malicious packet drops $\boldsymbol{e}_s[k]$ and $\boldsymbol{e}_a[k]$

An alternative approach to the problem

- Plant linear model

$$\left.\begin{array}{rcl} \boldsymbol{x}[k+1] & = & \boldsymbol{A}\boldsymbol{x}[k] + \boldsymbol{B}(\boldsymbol{u}^c[k] + \boldsymbol{e}_a[k]) \\ \boldsymbol{y}^c[k] & = & \boldsymbol{C}\boldsymbol{x}[k] + \boldsymbol{e}_s[k] \end{array}\right\}$$

- Communication links subject to attacks
  - $\boldsymbol{e}_a[k]$—sparse attacks injected in the actuators
  - $\boldsymbol{e}_s[k]$—sparse attacks injected in the sensors
- **Objective**: correctly estimate the initial state

H. Fawzi, P. Tabuada, S. Diggavi, *Secure estimation and control for cyber-physical systems under adversarial attacks*, IEEE TAC, Vol. 59, No. 6, pp. 1454–1467, June 2014

Our Approach—Use State Observer