Control and filter design for cyber-physical systems under denial-of-service attacks and transmission failures: A Markovian approach

Márcio J. Lacerda

LONDON METROPOLITAN UNIVERSITY

Outline

1. Switched systems

2. Cyber-Physical systems

3. Control design for CPS under attacks

4. Markovian approach

5. Final remarks

Switched systems

Consider the following discrete-time switched system

$$x(k+1) = A(\xi(k))x(k), \tag{1}$$

where $x \in \mathbb{R}^n$ is the state vector, and the switching rule is unknown *a priori*.

Consider the following discrete-time switched system

$$x(k+1) = A(\xi(k))x(k), \tag{1}$$

where $x \in \mathbb{R}^n$ is the state vector, and the switching rule is unknown *a priori*. The dynamic matrix can be written as

$$A(\xi(k)) = \sum_{i=1}^{v} \xi_i(k)A_i = \xi_1(k)A_1 + \xi_2(k)A_2 + \ldots \xi_v(k)A_v, \tag{2}$$

and the indicator function is defined as

$$\xi_i(k) = \begin{cases} 1, & \text{for} \quad A_i \text{ (the } i\text{th mode is active)} \\ 0, & \text{otherwise} \end{cases} \qquad \forall i = 1, \ldots, v.$$

Consider the following discrete-time switched system

$$x(k+1) = A(\xi(k))x(k), \tag{1}$$

where $x \in \mathbb{R}^n$ is the state vector, and the switching rule is unknown *a priori*. The dynamic matrix can be written as

$$A(\xi(k)) = \sum_{i=1}^{v} \xi_i(k)A_i = \xi_1(k)A_1 + \xi_2(k)A_2 + \ldots \xi_v(k)A_v, \tag{2}$$

and the indicator function is defined as

$$\xi_i(k) = \begin{cases} 1, & \text{for} \quad A_i \text{ (the } i\text{th mode is active)} \\ 0, & \text{otherwise} \end{cases} \qquad \forall i = 1, \ldots, v.$$

Stability

How can we certify that system (1) is globally asymptotically stable?

Theorem

The zero equilibrium of $x(k+1) = f_k(x(k))$ is globally uniformly asymptotically stable if there is a function $V : \mathbb{Z}^+ \times \mathbb{R}^n \to \mathbb{R}$ such that:

- *V is a positive-definite function, decreasing along the trajectories, and radially unbounded;*
- *$\Delta V(k, x(k)) = V(k+1, x(k+1)) - V(k, x(k))$ is negative definite along the solutions of $x(k+1) = f_k(x(k))$.*

One can say that the Lyapunov function is positive-definite, decreasing along the trajectories, and radially unbounded if $V(k, 0) = 0, \forall k \geq 0$ and

$$\beta_1 \|x(k)\|^2 \leq V(k, x(k)) \leq \beta_2 \|x(k)\|^2 \tag{3}$$

for all $x(k) \in \mathbb{R}^n$ and $k \geq 0$ with β_1 and β_2 positive scalars.

Switched Lyapunov function[1] $V(k, x(k)) = x(k)^T P(\xi(k))x(k)$.

Theorem

If there exist symmetric matrices $P_1, \dots, P_v$, *such that*

$$\begin{bmatrix} P_i & A_i^T P_j \\ P_j A_i & P_j \end{bmatrix} > 0, \quad \forall (i, j) \in \mathcal{J} \times \mathcal{J}, \tag{4}$$

where $\mathcal{J} = \{1, \dots, v\}$, *then, the Lyapunov function* $V(k, x(k)) = x(k)^T P(\xi(k))x(k)$ *certify the stability of the switched system* $x(k+1) = A(\xi(k))x(k)$.

[1] J. Daafouz, P. Riedinger, and C. Iung, "Stability analysis and control synthesis for switched systems: a switched Lyapunov function approach," IEEE Transactions on Automatic Control, 2002.

Switched Lyapunov function[1] $V(k, x(k)) = x(k)^T P(\xi(k))x(k)$.

Theorem

If there exist symmetric matrices $P_1, \dots, P_v$, such that

$$\begin{bmatrix} P_i & A_i^T P_j \\ P_j A_i & P_j \end{bmatrix} > 0, \quad \forall (i, j) \in \mathcal{I} \times \mathcal{I}, \tag{4}$$

where $\mathcal{I} = \{1, \dots, v\}$, then, the Lyapunov function $V(k, x(k)) = x(k)^T P(\xi(k))x(k)$ certify the stability of the switched system $x(k+1) = A(\xi(k))x(k)$.

Idea of the proof:

$$\begin{aligned} \Delta(V) &= V(k+1, x(k+1)) - V(k, x(k)) < 0 \\ &= x(k+1)^T P(\xi(k+1))x(k+1) - x(k)^T P(\xi(k))x(k) < 0 \\ &= x(k)^T (A(\xi(k))^T P(\xi(k+1))A(\xi(k)) - P(\xi(k)))x(k) < 0 \end{aligned}$$

[1] J. Daafouz, P. Riedinger, and C. Iung, "Stability analysis and control synthesis for switched systems: a switched Lyapunov function approach," IEEE Transactions on Automatic Control, 2002.

Structured Lyapunov functions

By employing an augmented state vector in the Lyapunov function[2]

$$V(k) = \begin{bmatrix} x(k) \\ x(k+1) \\ \vdots \\ x(k+N-1) \end{bmatrix}^T \Psi \begin{bmatrix} x(k) \\ x(k+1) \\ \vdots \\ x(k+N-1) \end{bmatrix}$$

with

$$\Psi = \operatorname{blkdiag}(P_1(\xi(k)), P_2(\xi(k+1)), \ldots, P_N(\xi(k+N-1))),$$

we are able to derive necessary and sufficient conditions to certify the stability of the switched system $x(k+1) = A(\xi(k))x(k)$.

[2] M. J. Lacerda and T. D. S. Gomide. "Stability and stabilisability of switched discrete-time systems based on structured Lyapunov functions". IET Control Theory & Applications, 2020.

Structured Lyapunov functions

The use of Lyapunov functions with non-monotonic terms[3] $V_i(x(k)) = x(k)^T P_i(\xi(k))x(k)$ can also lead to necessary and sufficient conditions[4] to certify the stability of the switched system $x(k+1) = A(\xi(k))x(k)$.

$$\sum_{i=j}^{N} V_i(x(k)) > 0, \quad j = 1, \ldots N,$$

$$V_1(x(k+1)) - V_1(x(k)) + V_2(x(k+2)) - V_2(x(k)) + \ldots + V_N(x(k+N)) - V_N(x(k)) < 0.$$

[3] A. A. Ahmadi and P. A. Parrilo. "Non-monotonic Lyapunov functions for stability of discrete time nonlinear and switched systems." 47th IEEE Conference on Decision and Control, 2008.

[4] M. J. Lacerda and T. D. S. Gomide. "Stability and stabilisability of switched discrete-time systems based on structured Lyapunov functions". IET Control Theory & Applications, 2020.

Non-monotonic terms

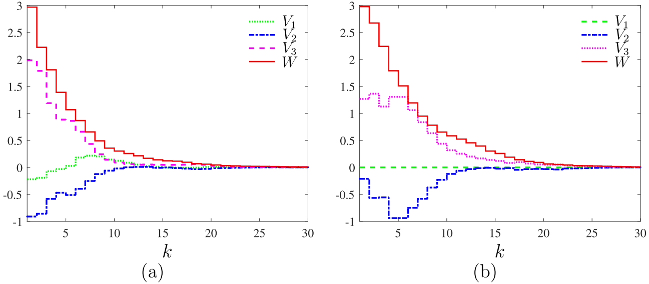


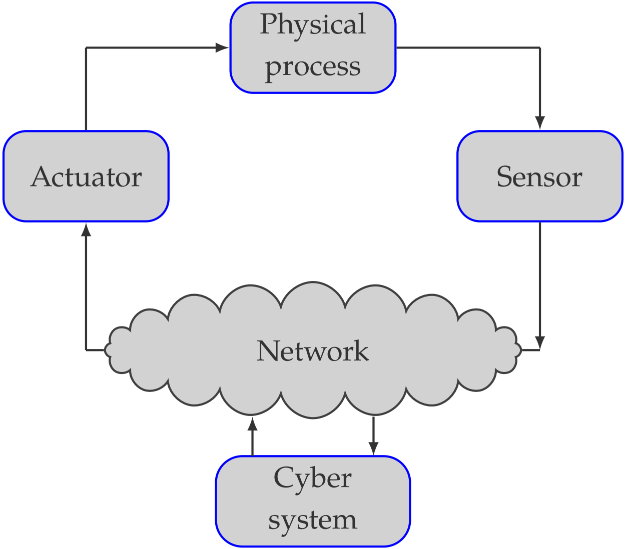
Fig. 1. Evolution of functions $V_1(x_k)$ (dotted green line), $V_2(x_k)$ (dashed dotted blue line), $V_3(x_k)$ (magenta dashed line) and the Lyapunov function $W(x_k)$ (straight red line) - Example 2. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

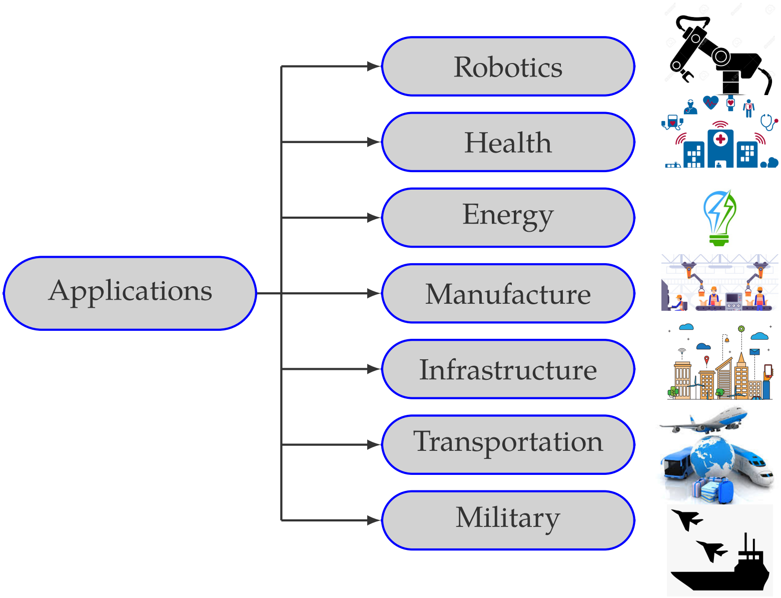
M.L.C. Peixoto et al./Journal of the Franklin Institute 357 (2020) 6595–6614

66(

Cyber-Physical systems

What is a cyber-physical system (CPS)?



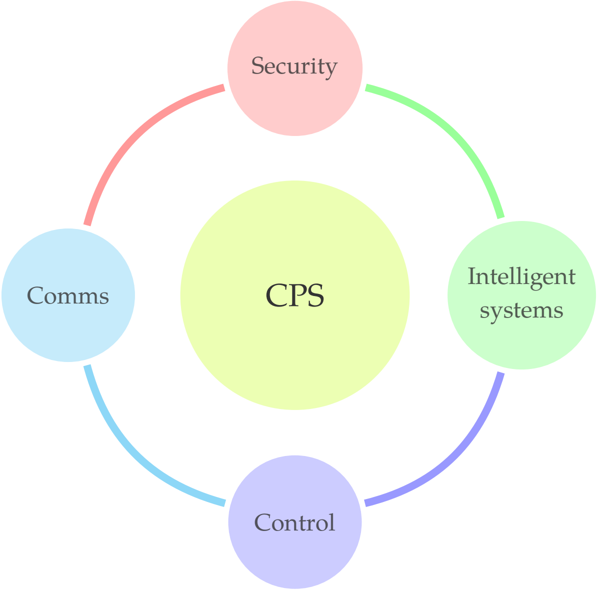


Applications

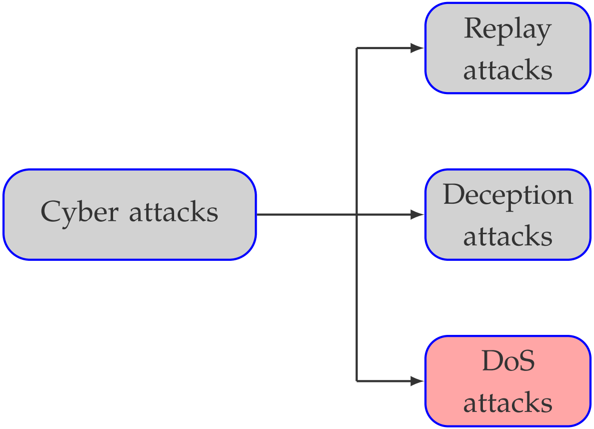
- Robotics
- Health
- Energy
- Manufacture
- Infrastructure
- Transportation
- Military

Source: Data & Analytics Facility for National Infrastructure (DAFNI) to advance UK infrastructure research.

Virtual organization of a CPS

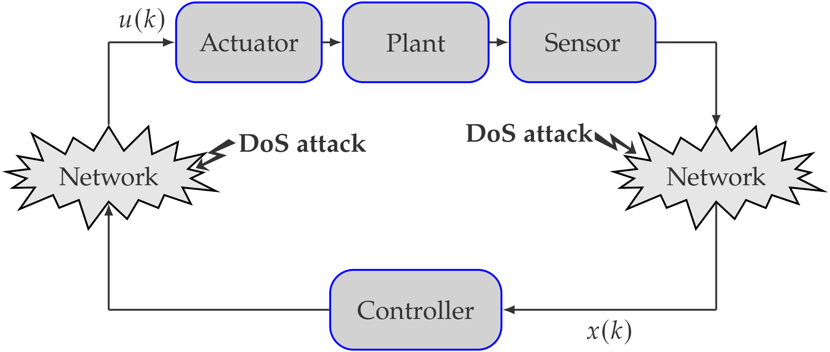


Cyber attacks on CPS[5]

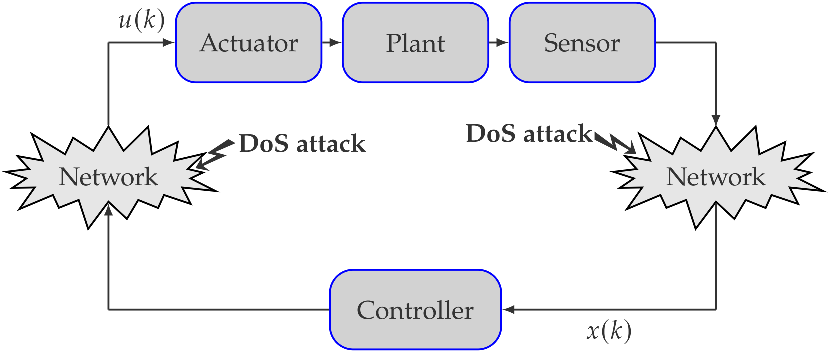


[5] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," Neurocomputing, vol. 275, pp. 1674 – 1683, 2018.

Structure of a CPS under DoS attacks.



Structure of a CPS under DoS attacks.



Problem

Does the designed controller ensure the stability of the closed-loop system under the presence of DoS attacks?

Control design for CPS under attacks

Control for cyber-physical systems

$$x(k+1) = A(\alpha)x(k) + B(\alpha)u(k) \tag{5}$$

where $x \in \mathbb{R}^n$ is the state vector, and $u \in \mathbb{R}^{n_u}$ the control input.

Control for cyber-physical systems

$$x(k+1) = A(\alpha)x(k) + B(\alpha)u(k) \tag{5}$$

where $x \in \mathbb{R}^n$ is the state vector, and $u \in \mathbb{R}^{n_u}$ the control input.

Scenario

- The matrices $A(\alpha)$ and $B(\alpha)$ belong to an uncertain domain.

$$\begin{bmatrix} A(\alpha) & B(\alpha) \end{bmatrix} = \sum_{i=1}^{V} \alpha_i \begin{bmatrix} A_i & B_i \end{bmatrix}, \quad \alpha \in \Lambda,$$

- V denotes the number of vertices of the polytope and Λ is the unit simplex

$$\Lambda = \left\{ \alpha \in \mathbb{R}^V : \sum_{i=1}^{V} \alpha_i = 1, \alpha_i \geq 0 \right\}.$$

Motivation

Consider a discrete-time uncertain system with matrices

$$A = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 - 0.1\delta \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0.1\kappa \end{bmatrix},$$

where $0.1s^{-1} \leq \delta \leq 10s^{-1}$, and $\kappa = 0.787rad^{-1}V^{-1}s^{-2}$.

Disregarding the existence of attack the following state-feedback control gain stabilizes the system

$$K = \begin{bmatrix} -6.6145 & -7.4944 \end{bmatrix}.$$

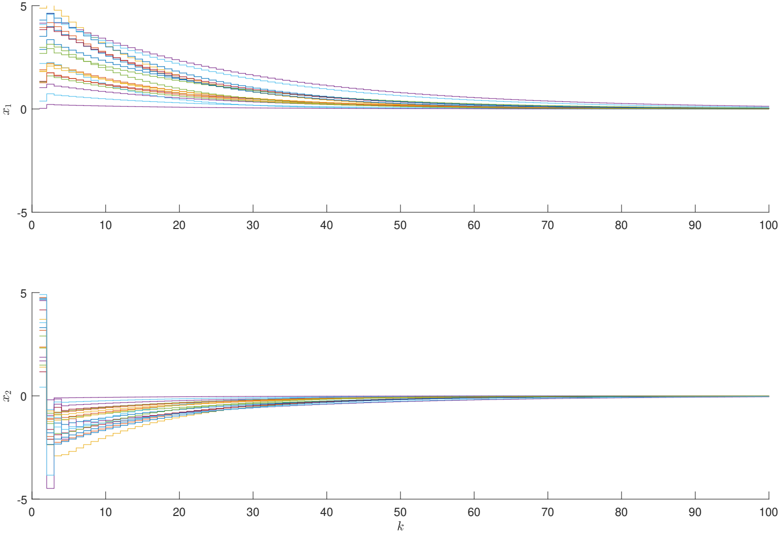


Figure 1: Trajectories for the closed-loop states.

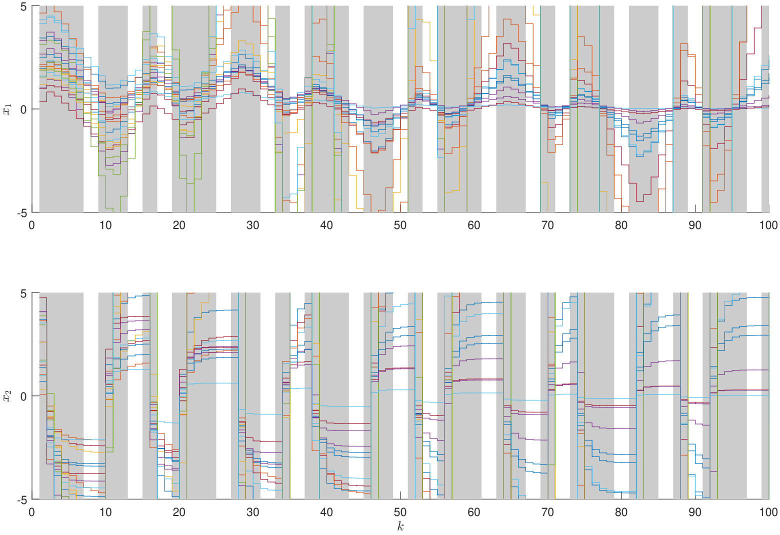


Figure 2: Trajectories for the closed-loop states during the presence of DoS attack.

Problem

How can we design a control strategy capable of ensuring the stability of the closed-loop uncertain system under the presence of DoS attacks?

- We need to construct a model that takes into account the presence of DoS attacks. Different control strategies can be employed[6]:
  - Hold strategy
  - Zero strategy
  - Packet of different controllers
- By using the Lyapunov theory, the design conditions will be written in the form of LMIs.

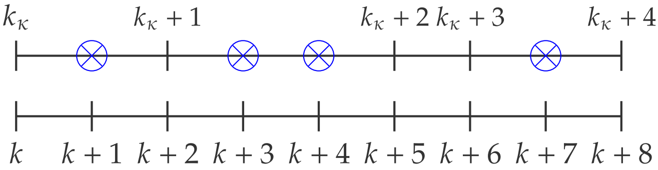
[6] L. Schenato, "To Zero or to Hold Control Inputs With Lossy Links?," IEEE Transactions on Automatic Control, 2009.

Problem Formulation: DoS modelling

Assumption: The duration of the DoS attack is bounded by the maximum number of consecutive control inputs samples that do not get to the actuator, being this number denoted by N.

- Switching signal $\sigma\left(k_\kappa\right)$ that assume values in $M \triangleq \{0, 1, \ldots, N\}$
- A new time scale k_κ that represents the time instant when the updated control input reaches the actuator

$$k_\kappa + 1 = k_\kappa + \sigma\left(k_\kappa\right) + 1, \quad k_0 = 0, \quad \sigma(k_\kappa) = \{1, 2, 0, 1\}$$



Problem Formulation: Hold Strategy

- The same control input $u(k) = Kx(k)$ available to the actuator is successively applied until the end of the attack (next successful transmission).

$N = 1$

$$
\begin{aligned}
x(k+1) &= A(\alpha)x(k) + B(\alpha)Kx(k),\\
x(k+2) &= A(\alpha)x(k+1) + B(\alpha)Kx(k),\\
\rightarrow x(k+2) &= A(\alpha)^2x(k) + A(\alpha)B(\alpha)Kx(k) + B(\alpha)Kx(k),
\end{aligned}
$$

Problem Formulation: Hold Strategy

- The same control input $u(k) = Kx(k)$ available to the actuator is successively applied until the end of the attack (next successful transmission).

$N = 1$

$$\begin{aligned} x(k+1) &= A(\alpha)x(k) + B(\alpha)Kx(k), \\ x(k+2) &= A(\alpha)x(k+1) + B(\alpha)Kx(k), \\ \rightarrow x(k+2) &= A(\alpha)^2x(k) + A(\alpha)B(\alpha)Kx(k) + B(\alpha)Kx(k), \end{aligned}$$

$N = 2$

$$\begin{aligned} x(k+3) &= A(\alpha)x(k+2) + B(\alpha)Kx(k), \\ \rightarrow x(k+3) &= A(\alpha)^3x(k) + A(\alpha)^2B(\alpha)Kx(k) + A(\alpha)B(\alpha)Kx(k) \\ &\quad + B(\alpha)Kx(k). \end{aligned}$$

Problem Formulation: Zero Strategy

- The control input is set to zero until the end of the attack (next successful transmission).

$N = 1$

$$\begin{aligned} x(k+1) &= A(\alpha)x(k) + B(\alpha)Kx(k), \\ x(k+2) &= A(\alpha)x(k+1) \\ \rightarrow x(k+2) &= A(\alpha)^2 x(k) + A(\alpha)B(\alpha)Kx(k), \end{aligned} \tag{6}$$

Problem Formulation: Zero Strategy

- The control input is set to zero until the end of the attack (next successful transmission).

$N = 1$

$$\begin{aligned} x(k+1) &= A(\alpha)x(k) + B(\alpha)Kx(k), \\ x(k+2) &= A(\alpha)x(k+1) \\ \rightarrow x(k+2) &= A(\alpha)^2x(k) + A(\alpha)B(\alpha)Kx(k), \end{aligned} \tag{6}$$

$N = 2$

$$\begin{aligned} x(k+3) &= A(\alpha)x(k+2), \\ \rightarrow x(k+3) &= A(\alpha)^3x(k) + A(\alpha)^2B(\alpha)Kx(k). \end{aligned}$$

Problem Formulation: Packet Strategy

- Different control inputs $u(k+i) = K_i\, x(k)$ are available to the actuator before an attack starts in $k+1$. These inputs are successively applied until the end of the attack (next successful transmission).

$N = 1$

$$x(k+1) = A(\alpha)x(k) + B(\alpha)K_0x(k),$$

$$x(k+2) = A(\alpha)x(k+1) + B(\alpha)K_1x(k),$$

$$\rightarrow x(k+2) = A(\alpha)^2x(k) + A(\alpha)B(\alpha)K_0x(k) + B(\alpha)K_1x(k),$$

Problem Formulation: Packet Strategy

- Different control inputs $u(k+i) = K_i\, x(k)$ are available to the actuator before an attack starts in $k+1$. These inputs are successively applied until the end of the attack (next successful transmission).

$N = 1$

$$
\begin{aligned}
x(k+1) &= A(\alpha)x(k) + B(\alpha)K_0 x(k),\\
x(k+2) &= A(\alpha)x(k+1) + B(\alpha)K_1 x(k),\\
\longrightarrow x(k+2) &= A(\alpha)^2 x(k) + A(\alpha)B(\alpha)K_0 x(k) + B(\alpha)K_1 x(k),
\end{aligned}
$$

$N = 2$

$$
\begin{aligned}
x(k+3) &= A(\alpha)x(k+2) + B(\alpha)K_2 x(k),\\
\longrightarrow x(k+3) &= A(\alpha)^3 x(k) + A(\alpha)^2 B(\alpha)K_0 x(k) + A(\alpha)B(\alpha)K_1 x(k)\\
&\quad + B(\alpha)K_2 x(k).
\end{aligned}
$$

Packet-based approach[7]

Packet of controllers

$$U(k) = \begin{bmatrix} u(k) \\ u(k+1) \\ \vdots \\ u(k+N) \end{bmatrix} = \begin{bmatrix} K_0 x(k) \\ K_1 x(k) \\ \vdots \\ K_N x(k) \end{bmatrix}, \tag{7}$$

is the package that gets to the actuator side every time that the communications channels are free of the attack.

[7] P. S. P. Pessim and M. J. Lacerda, "State-Feedback Control for Cyber-Physical LPV Systems Under DoS Attacks." *IEEE Control Systems Letters*, 2021.

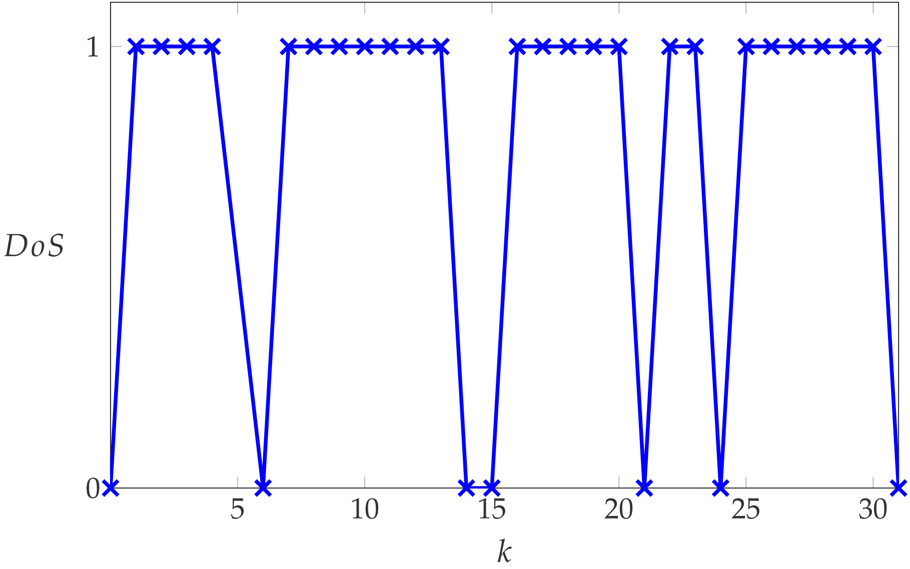


Figure 3: "1" - presence of DoS attacks and "0" - absence of DoS attacks. Sequence of attacks $\sigma(k_\kappa) = \{4, 7, 0, 5, 2, 6, \ldots\}$

$$U_1(k_\kappa) = \begin{bmatrix} u(k_\kappa) \\ u(k_\kappa+1) \\ u(k_\kappa+2) \\ u(k_\kappa+3) \\ u(k_\kappa+4) \\ u(k_\kappa+5) \\ u(k_\kappa+6) \\ u(k_\kappa+7) \end{bmatrix}, \; U_2(k_\kappa) = \begin{bmatrix} u(k_\kappa) \\ u(k_\kappa+1) \\ u(k_\kappa+2) \\ u(k_\kappa+3) \\ u(k_\kappa+4) \\ u(k_\kappa+5) \\ u(k_\kappa+6) \\ u(k_\kappa+7) \end{bmatrix}, \; U_3(k_\kappa) = \begin{bmatrix} u(k_\kappa) \\ u(k_\kappa+1) \\ u(k_\kappa+2) \\ u(k_\kappa+3) \\ u(k_\kappa+4) \\ u(k_\kappa+5) \\ u(k_\kappa+6) \\ u(k_\kappa+7) \end{bmatrix},$$

$$U_4(k_\kappa) = \begin{bmatrix} u(k_\kappa) \\ u(k_\kappa+1) \\ u(k_\kappa+2) \\ u(k_\kappa+3) \\ u(k_\kappa+4) \\ u(k_\kappa+5) \\ u(k_\kappa+6) \\ u(k_\kappa+7) \end{bmatrix}, \; U_5(k_\kappa) = \begin{bmatrix} u(k_\kappa) \\ u(k_\kappa+1) \\ u(k_\kappa+2) \\ u(k_\kappa+3) \\ u(k_\kappa+4) \\ u(k_\kappa+5) \\ u(k_\kappa+6) \\ u(k_\kappa+7) \end{bmatrix}, \; U_6(k_\kappa) = \begin{bmatrix} u(k_\kappa) \\ u(k_\kappa+1) \\ u(k_\kappa+2) \\ u(k_\kappa+3) \\ u(k_\kappa+4) \\ u(k_\kappa+5) \\ u(k_\kappa+6) \\ u(k_\kappa+7) \end{bmatrix}.$$

Problem Formulation: Switched System

- Case 0: DoS-free case

$$x(k_\kappa + 1) = (A(\alpha) + B(\alpha)K_0)\, x(k_\kappa),$$
$$x(k_\kappa + 1) = F_0(\alpha)x(k_\kappa)$$

- Case 1: The DoS attack occurs during one time-instant

$$x(k_\kappa + 1) = \left(A(\alpha)^2 + A(\alpha)B(\alpha)K_0 + B(\alpha)K_1\right) x(k_\kappa),$$
$$x(k_\kappa + 1) = F_1(\alpha)x(k_\kappa) = (A(\alpha)F_0(\alpha) + B(\alpha)K_1)\, x(k_\kappa).$$

- Case 2: The DoS attack occurs during two time-instants

$$x(k_\kappa + 1) = F_2(\alpha)x(k_\kappa) = (A(\alpha)F_1(\alpha) + B(\alpha)K_2)\, x(k_\kappa).$$

Problem Formulation: Switched System

A generic formulation is given as follows

$$F_i(\alpha) = A(\alpha)F_{i-1}(\alpha) + B(\alpha)K_i,$$

$i = 1, \ldots, N$, with $F_0(\alpha) = A(\alpha) + B(\alpha)K_0$. These matrices are used to construct the following switched system with $N + 1$ modes.

$$x(k_\kappa + 1) = F_{\sigma(k_\kappa)}x(k_\kappa).$$

Considering the indicator function $\xi\left(k_\kappa\right) = \left[\xi_0\left(k_\kappa\right), \ldots, \xi_N\left(k_\kappa\right)\right]^\top$

$$x(k_\kappa + 1) = F(\xi(k_\kappa))x(k_\kappa), \quad \xi_i\left(k_\kappa\right) = \begin{cases} 1, & \text{if } \sigma(k_\kappa) = i \\ 0, & \text{otherwise} \end{cases}$$

with $F(\xi(k_\kappa)) = \xi_0(k_\kappa)F_0 + \xi_1(k_\kappa)F_1 + \cdots + \xi_N(k_\kappa)F_N$.

How to design the gain matrices?

Existence of a Lyapunov function $V(x_{k_\kappa})$, that is positive definite, and has its time rate of change negative definite along the trajectories, i.e., $\Delta V(x_{k_\kappa}) < 0$.

How to design the gain matrices?

Existence of a Lyapunov function $V(x_{k_\kappa})$, that is positive definite, and has its time rate of change negative definite along the trajectories, i.e., $\Delta V(x_{k_\kappa}) < 0$.

Moreover, we need to employ

1. Change of variables.
2. Congruence transformation.
3. Schur complement.
4. Linear Matrix Inequalities.

Theorem

If there exist symmetric positive definite matrices $Q_i \in \mathbb{R}^{n \times n}$*, matrices* $X \in \mathbb{R}^{n \times n}$ *and* $Z_i \in \mathbb{R}^{n_u \times n}$*, such that*

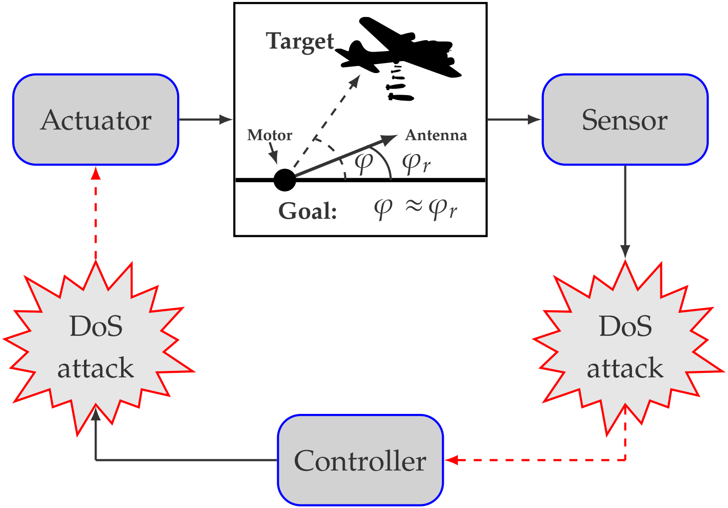
$$\begin{bmatrix} -Q_i(\alpha) & \star \\ \Psi_i & Q_j(\alpha) - X - X^T \end{bmatrix} < 0, \tag{8}$$

where

$$\Psi_i = A(\alpha)^{i+1} X + \sum_{m=0}^{i} A(\alpha)^m B(\alpha) Z_{i-m}, \tag{9}$$

with $A(\alpha)^0 = I_n$*,* $i, j \in M$*,* $M \triangleq \{0, 1, \ldots, N\}$*, then* $K_i = Z_i X^{-1}$ *are the state-feedback control gains that assure the closed-loop system* (5) *is asymptotically stable.*

Example: angular positioning system



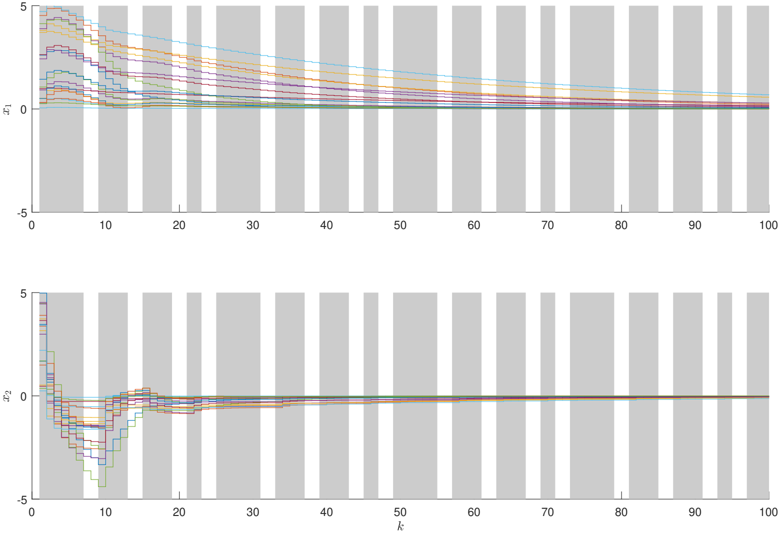


Figure 4: Trajectories for the closed-loop states during the presence of DoS attack $N = 7$, using hold strategy.

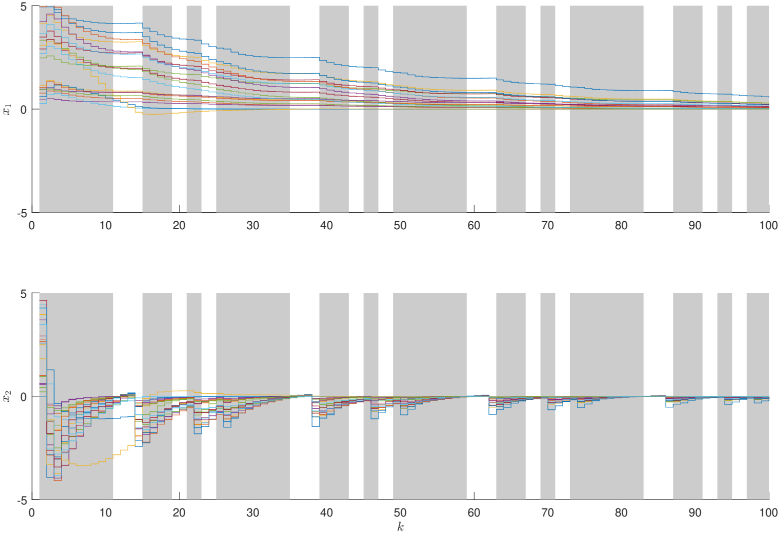


Figure 5: Trajectories for the closed-loop states during the presence of DoS attack $N = 11$, using the packet-based approach.

Problems addressed

- Output-feedback control for LPV systems[8].
- $\mathscr{H}_\infty$ performance for LPV systems[9].
- $\mathscr{H}_2$ performance for uncertain systems[10].

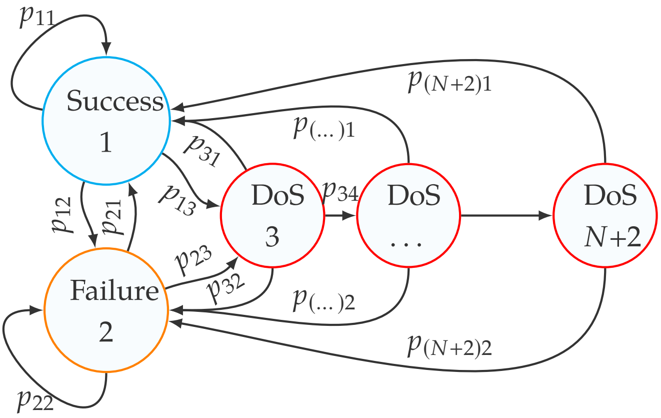
[8] P. S. P. Pessim and M. L. C. Peixoto and R. M. Palhares and M. J. Lacerda, "Static output-feedback control for Cyber-physical LPV systems under DoS attacks."*Information Sciences*, 2021.

[9] P. S. P. Pessim and M. J. Lacerda, "On the robustness of Cyber-physical LPV systems under DoS attacks." *Journal of the Franklin Institute*, 2022.

[10] P. M. Oliveira and J. M. Palma and M. J. Lacerda. "$\mathscr{H}_2$ state-feedback control for discrete-time cyber-physical uncertain systems under DoS attacks," *Applied Mathematics and Computation*, 2022.

Markovian approach

A model that includes DoS attack+packet loss for control design[11].



[11] P. M. Oliveira and J. M. Palma and M. J. Lacerda. " Control Design for an Unreliable Markovian Network Susceptible to Denial-of-Service Attacks", IEEE Transactions on Circuits and Systems II: Express Briefs, 2024.

Mode transition

The modes transition and definition are further discussed in the sequel

i) The transmission is successful and the network is operational ($\theta_k = 1$).

ii) Due to communication channel limitations, a transmission failure happens ($\theta_k = 2$).

iii) The communication channels suffer a DoS attack ($\theta_k = 3, \dots, N + 2$), which start in mode 3. From this point on, the attack may persist with a probability p_{34}.

Transition probability

The combination of i), ii), and iii) results in the proposed network model. Given the $N+2$ modes of the CPS network and its possible transitions, the generic transition probability matrix $\Psi \in \mathbb{R}^{(N+2)\times(N+2)}$ is given by:

$$\Psi = \begin{bmatrix} p_{11} & p_{12} & p_{13} & 0 & \dots & 0 \\ p_{21} & p_{22} & p_{23} & 0 & \dots & 0 \\ p_{31} & p_{32} & 0 & p_{34} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{(N+1)1} & p_{(N+1)2} & 0 & 0 & \dots & p_{(N+1)(N+2)} \\ p_{(N+2)1} & p_{(N+2)2} & 0 & 0 & \dots & 0 \end{bmatrix}. \tag{10}$$

Time-varying transition probability matrix

Obtaining the transition probabilities p_{ij} is a very challenging task in the proposed network model, mainly when taking into account the attack dynamics. As ways to circumvent this obstacle and introduce flexibility and robustness to the approach we consider[12]:

- ◎ uncertain probabilities with known bounds ($0 \leq \underline{p_{ij}} \leq p_{ij}(k) \leq \overline{p_{ij}} \leq 1$),
- ◎ and unknown probabilities (represented by '?') where ($0 = \underline{p_{ij}} \leq p_{ij}(k) \leq \overline{p_{ij}} \leq 1$) are modeled after time-varying parameters.

[12] C. F. Morais and M. F. Braga and R. C. L. F. Oliveira and P. L. D. Peres. $\mathscr{H}_2$ control of discrete-time Markov jump linear systems with uncertain transition probability matrix: improved linear matrix inequality relaxations and multi-simplex modelling. IET Control Theory & Applications, 2013.

Control design

Consider the discrete-time uncertain model of a CPS:

$$x(k+1) = A(\alpha)x(k) + B(\alpha)u_{\theta_k}(k). \tag{11}$$

We aim to design a state-feedback control law with the following structure

$$u_{\theta_k}(k) = \delta_{\theta_k} K_{\theta_k} x(k) + (1 - \delta_{\theta_k}) K_{\theta_k} x_l(k-1), \tag{12}$$

where $K_{\theta_k} \in \mathbb{R}^{n_u \times n_x}$ is the mode-dependent state-feedback gain, with a different gain being employed in each network mode, and x_l is the last transmitted reading.

Control design

The binary variable indicates if the transmission was successful, or a transmission failure/attack has prevented it,

$$\delta_{\theta_k} = \begin{cases} 1, & \text{if } \theta_k = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

If $\delta_{\theta_k} = 0$, there is no access to the current state, then $x_l(k-1)$, which is the last transmitted reading, will be employed to create the control signal. The signal $x_l(k)$ is updated as follows

$$x_l(k) = \delta_{\theta_k} x(k) + (1 - \delta_{\theta_k}) x_l(k-1). \tag{14}$$

Control design

By employing (11), (12), and (14), a MJLS augmented closed-loop system can be written as

$$\chi(k+1) = G(\theta_k, \alpha)\chi(k), \tag{15}$$

where $\chi = \begin{bmatrix} x(k)^T & x_l(k-1)^T \end{bmatrix}^T$, and

$$G(\theta_k, \alpha) = \begin{bmatrix} A(\alpha) + \delta_{\theta_k} B(\alpha) K_{\theta_k} & (1-\delta_{\theta_k}) B(\alpha) K_{\theta_k} \\ \delta_{\theta_k} I_{n_x} & (1-\delta_{\theta_k}) I_{n_x} \end{bmatrix}. \tag{16}$$

Every time the communication channels are operational a set of control inputs

$$\mathcal{U} = \begin{bmatrix} K_1 x(k) & K_2 x(k) & \dots & K_{N+2} x(k) \end{bmatrix},$$

is sent to the actuator.

Control design

Lemma

The system (15) is exponential stable in the mean square sense - CI, if there exist symmetric positive-definite matrices $Q_i(\alpha,\xi_k) \in \mathbb{R}^{2n_x \times 2n_x}$ *such that the following condition holds*

$$G_i(\alpha)^T \widehat{Q}_i(\alpha,\xi_{k+1}) G_i(\alpha) - Q_i(\alpha,\xi_k) < 0, \tag{17}$$

where

$$\widehat{Q}_i(\alpha,\xi_{k+1}) = \sum_{j=1}^{N+2} p_{ij}(\xi_k) Q_j(\alpha,\xi_{k+1}), \tag{18}$$

for each $i \in \mathbb{K}$, *for all* $(\alpha,\xi_k,\xi_{k+1}) \in \Lambda_V \times \Lambda_Z \times \Lambda_Z$.

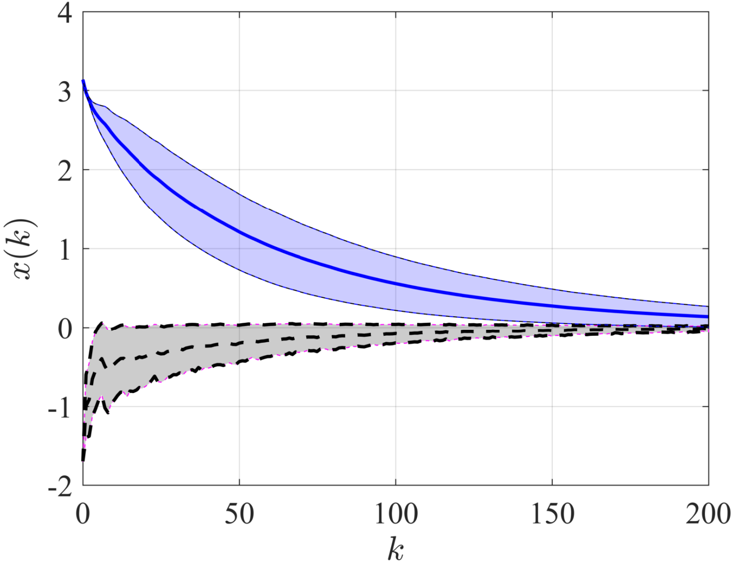
Consider the same example with

$$A(\alpha) = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 - 0.1\delta \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0.1\kappa \end{bmatrix},$$

where $0.1s^{-1} \leq \delta \leq 10s^{-1}$, and $\kappa = 0.787 rad^{-1} V^{-1} s^{-2}$. In this approach we need to take into account the transition probability matrix.

$$\Psi = \begin{bmatrix} 0.5 & c & d & 0 & 0 & 0 & 0 \\ 0.4 & ? & ? & 0 & 0 & 0 & 0 \\ 0.05 & 0.05 & 0 & 0.9 & 0 & 0 & 0 \\ 0.05 & 0.05 & 0 & 0 & 0.9 & 0 & 0 \\ 0.05 & 0.05 & 0 & 0 & 0 & 0.9 & 0 \\ 0.05 & 0.05 & 0 & 0 & 0 & 0 & 0.9 \\ 0.5 & 0.5 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{19}$$

where $c = \begin{bmatrix} 0.05 & 0.15 \end{bmatrix}$ and $d = \begin{bmatrix} 0.35 & 0.45 \end{bmatrix}$.


4
3
2
1
0
-1
-2
$x(k)$
0
50
100
150
200
k

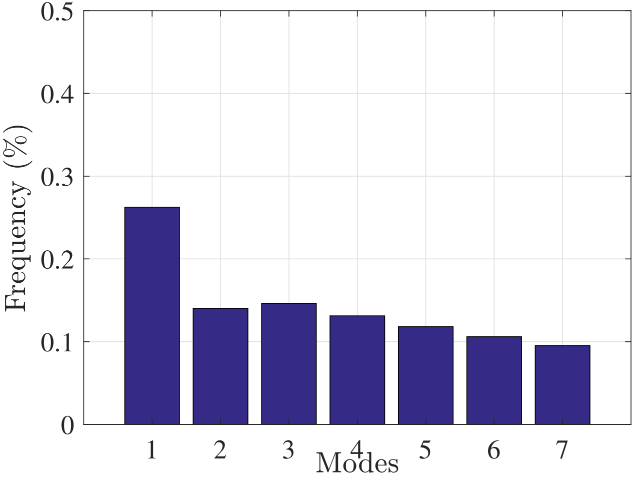


Figure 6: Histogram with the frequency of occurrence of each mode in the 1000 time-based simulations.

Filter design[13]

Consider the discrete-time uncertain model of a CPS:

$$\begin{cases} x(k+1) = A(\alpha)x(k) + B(\alpha)w(k), \\ z(k) = C_z(\alpha)x(k) + D_z(\alpha)w(k), \\ y(k) = C_y(\alpha)x(k) + D_y(\alpha)w(k), \end{cases} \tag{20}$$

We consider that the last transmitted measurement $y_m(k)$ may be stored in a memory in the filter by employing a Zero-Order Hold (ZOH):

$$y_m(k) = \delta_{\theta_k} y(k) + (1 - \delta_{\theta_k}) y_m(k-1). \tag{21}$$

The binary variable indicates if the transmission was successful, or not,

$$\delta_{\theta_k} = \begin{cases} 1, & \text{if } \theta_k = 1, \\ 0, & \text{otherwise.} \end{cases} \tag{22}$$

[13] P. M. Oliveira and J. M. Palma and M. J. Lacerda. "Filter design for Cyber-physical systems against DoS attacks and unreliable networks: A Markovian approach", IET CTA, 2024.

Filter Design

A full-order mode-dependent filter is then considered, which is described by

$$\mathscr{F} = \begin{cases} x_f(k+1) = Af_{\theta_k} x_f(k) + Bf_{\theta_k} y_m(k), \\ z_f(k) = Cf_{\theta_k} x_f(k) + Df_{\theta_k} y_m(k), \end{cases} \tag{23}$$

The estimation error is $e(k) = z(k) - z_f(k)$. By combining (20) with (23) and (21), the augmented system that evaluates the filtering error is described by the following Markov Jump Linear System (MJLS).

$$\begin{cases} \eta(k+1) = \bar{A}_i(\alpha)\eta(k) + \bar{B}_i(\alpha)w(k), \\ e(k) = \bar{C}_i(\alpha)\eta(k) + \bar{D}_i(\alpha)w(k), \end{cases} \tag{24}$$

where $\eta(k) = \begin{bmatrix} x(k)^T & y_m(k-1)^T & x_f(k)^T \end{bmatrix}^T \in \mathbb{R}^n$ and $e(k) \in \mathbb{R}^{n_z}$, where $n = 2n_x + n_y$.

Filter design

The matrices have compatible dimensions and are described in the sequel

$$\begin{aligned}
\bar{A}_i(\alpha) &= \begin{bmatrix} A(\alpha) & 0 & 0 \\ \delta_i C_y(\alpha) & (1-\delta_i) I_{n_y} & 0 \\ \delta_i B f_i C_y(\alpha) & (1-\delta_i) B f_i & A f_i \end{bmatrix}, \\
\bar{B}_i(\alpha) &= \begin{bmatrix} B(\alpha) \\ \delta_i D_y(\alpha) \\ \delta_i B f_i D_y(\alpha) \end{bmatrix}, \\
\bar{C}_i(\alpha) &= \begin{bmatrix} C_z(\alpha) - \delta_i D f_i C_y(\alpha) & -(1-\delta_i) D f_i & -C f_i \end{bmatrix}, \\
\bar{D}_i(\alpha) &= D_z(\alpha) - \delta_i D f_i D_y(\alpha).
\end{aligned} \tag{25}$$

Lemma

The system (24) *is exponential stable in the mean square sense - CI, and displays a norm* $\|\mathcal{H}_\infty\|^2 < \gamma$ *if and only if there exist positive definite symmetric matrices* $W_i(\xi_k, \alpha) \in \mathbb{R}^{n\times n}$, *and*

$$W_i^+ = \sum_{j=1}^{N+2} p_{ij}(\xi_k) W_j(\xi_{k+1}, \alpha), \tag{26}$$

such that

$$\begin{bmatrix} W_i(\xi_k, \alpha) & \bar{A}_i(\alpha)^T W_i^+ & 0 & \bar{C}_i(\alpha) \\ W_i^+ \bar{A}_i(\alpha) & W_i^+ & W_i^+ \bar{B}_i(\alpha) & 0 \\ 0 & \bar{B}_i(\alpha)^T W_i^+ & I_{n_w} & \bar{D}_i(\alpha)^T \\ \bar{C}_i(\alpha) & 0 & \bar{D}_i(\alpha) & \gamma I_{n_z} \end{bmatrix} > 0, \tag{27}$$

hold for $i \in \mathbb{K}$ *and for all* $(\alpha, \xi_k, \xi_{k+1}) \in \Lambda_V \times \Lambda_Z \times \Lambda_Z, \forall k \geq 0.$

Filter design

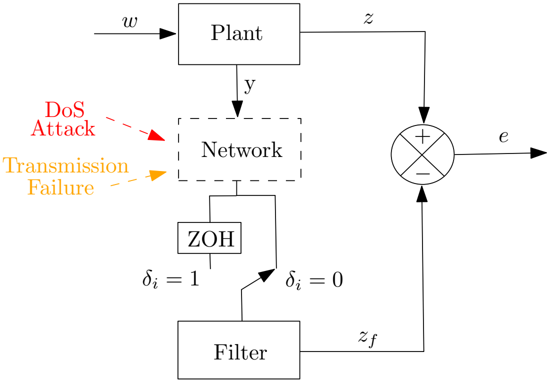


Figure 7: $\delta_i = 0$ indicates successful transmission and $\delta_i = 1$ denotes the presence of DoS attacks or transmission failures.

Filter design

Consider the following discrete-time uncertain system

$$\begin{aligned} A &= \begin{bmatrix} 0 & -0.5 \\ 1 & 1+\mu \end{bmatrix}, & B &= \begin{bmatrix} -6 & 0 \\ 1 & 0 \end{bmatrix}, \\ C_y &= \begin{bmatrix} -100 & 10 \end{bmatrix}, & D_y &= \begin{bmatrix} 0 & 1 \end{bmatrix}, \\ C_z &= \begin{bmatrix} 1 & 0 \end{bmatrix}, & D_z &= \begin{bmatrix} 0 & 0 \end{bmatrix}, \end{aligned}$$

where $|\mu| \leq 0.45$, resulting in $V = 2$ vertices,

Filter design

Considering a maximum of $N = 5$ consecutive attacks, the utilized transition probability matrix with uncertain and unknown parameters is as follows

$$\Psi = \begin{bmatrix} 0.45 & e & d & 0 & 0 & 0 & 0 \\ 0.5 & ? & ? & 0 & 0 & 0 & 0 \\ f & 0.05 & 0 & \rho & 0 & 0 & 0 \\ f & 0.05 & 0 & 0 & \rho & 0 & 0 \\ f & 0.05 & 0 & 0 & 0 & \rho & 0 \\ f & 0.05 & 0 & 0 & 0 & 0 & \rho \\ 0.45 & 0.55 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \tag{28}$$

where $f = (1 - 0.05 - \rho)$, $e \in \begin{bmatrix} 0.05 & 0.15 \end{bmatrix}$ and $d \in \begin{bmatrix} 0.4 & 0.5 \end{bmatrix}$. ρ is a parameter whose value defines if longer attacks are more likely to take place.

Filter design

The scenario with $N = 5$ maximum consecutive attacks was considered as well as a scenario with $N = 10$, which can be easily obtained by using the same values of rows 3 to 6 in (28), in accordance to the positioning defined by (10). The norm value in function of the value of ρ is provided in Table 1.

	Mode dependent		Mode independent	
ρ N	5	10	5	10
0.50	10.73	10.73	11.79	11.79
0.60	12.09	12.14	13.07	13.19
0.70	13.87	14.25	15.13	15.98
0.80	16.12	17.92	17.98	20.87
0.85	17.49	20.70	19.82	24.60
0.90	19.08	24.11	22.10	29.50
0.95	20.96	28.59	24.90	35.55

Filter design

Consider the following system matrices, obtained from a discretized model with sample time $0.1s$ of a mechanical system composed of two masses and two strings.

$$A_1 = A_2 = \begin{bmatrix} 0.99 & 0 & 0.1 & 0 \\ 0.01 & 0.99 & 0 & 0.1 \\ -0.19 & 0.10 & 0.94 & 0 \\ 0.19 & -0.19 & 0.01 & 0.90 \end{bmatrix}, \; B_1 = B_2 = \begin{bmatrix} 0 \\ 0 \\ 0.01 \\ 0 \end{bmatrix},$$

$$C_{y,1} = \begin{bmatrix} 0.3 & 0 & 0 & 0 \end{bmatrix},$$

$$C_{y,2} = \begin{bmatrix} 1.7 & 0 & 0 & 0 \end{bmatrix},$$

$$C_{z,1} = C_{z,2} = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix},$$

and $D_{y,1} = D_{y,2} = D_{z,1} = D_{z,2} = 0$.

Filter design

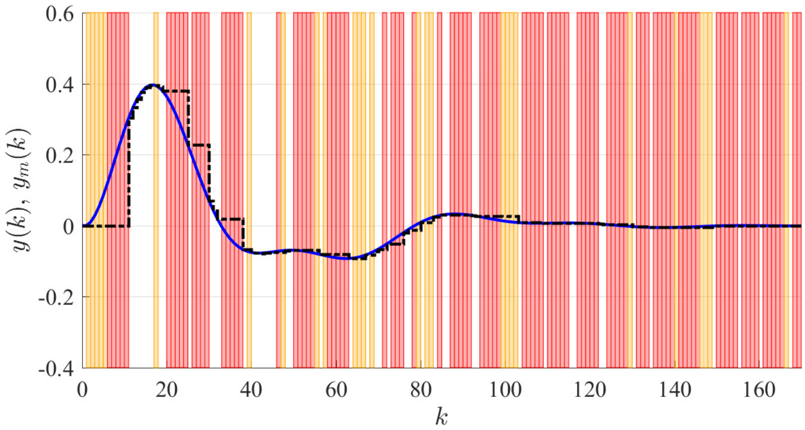


Figure 8: $y(k)$ (—) and $y_m(k)$ (- - -)

Filter design

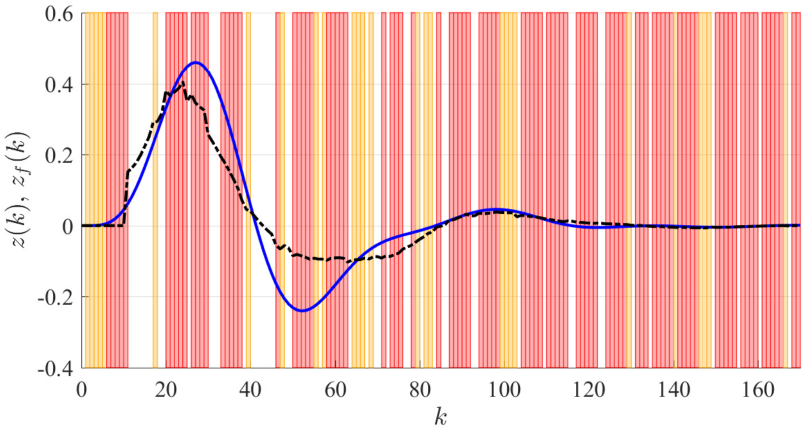


Figure 9: $z(k)$ (—) and $z_f(k)$ (- - -) with the mode-dependent filter

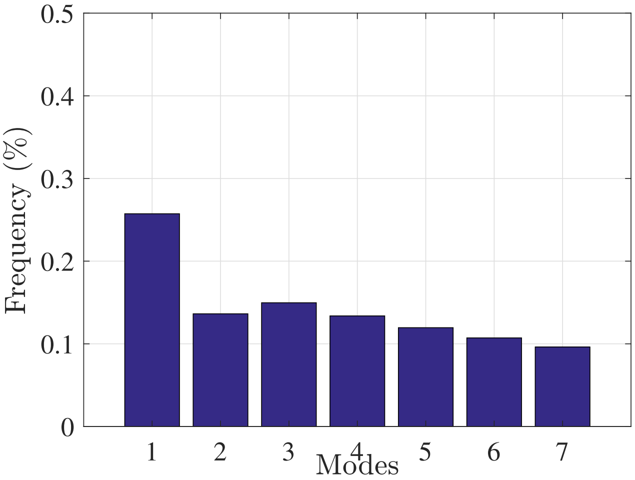


Figure 10: Histogram with the frequency of occurrence of each mode in the 1000 time-based simulations.

Perspectives for future research

Secure control

- Filter design for attack detection.
- Constrained control input such as saturation.
- Replay attacks and false data injection attacks.
- Hybrid model for the CPS under attack.

Final remarks

IEEE Control Systems Society™

An IEEE Control Systems Initiative

CONTROL FOR SOCIETAL-SCALE CHALLENGES: ROAD MAP 2030

Anuradha M. Annaswamy
Karl H. Johansson | George J. Pappas

Emerging Methodologies

- ◎ Safety Critical systems
- ◎ Resilient cyber-physical systems
- ◎ Cyber-physical human systems

Summary

- CPS present opportunities and new challenges for control design.
- Control theory can contribute to safety in CPS.

Summary

- CPS present opportunities and new challenges for control design.
- Control theory can contribute to safety in CPS.

Muchas Gracias!

m.lacerda@londonmet.ac.uk