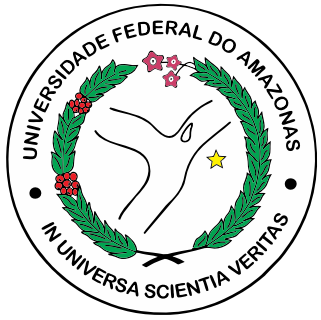
Resilient Event-Triggered Control for Cyber-Physical Systems under Denial-of-Service Attacks

Workshop on Trustworthy Artificial Intelligence and Cyber-Physical Systems (TAC 2024)

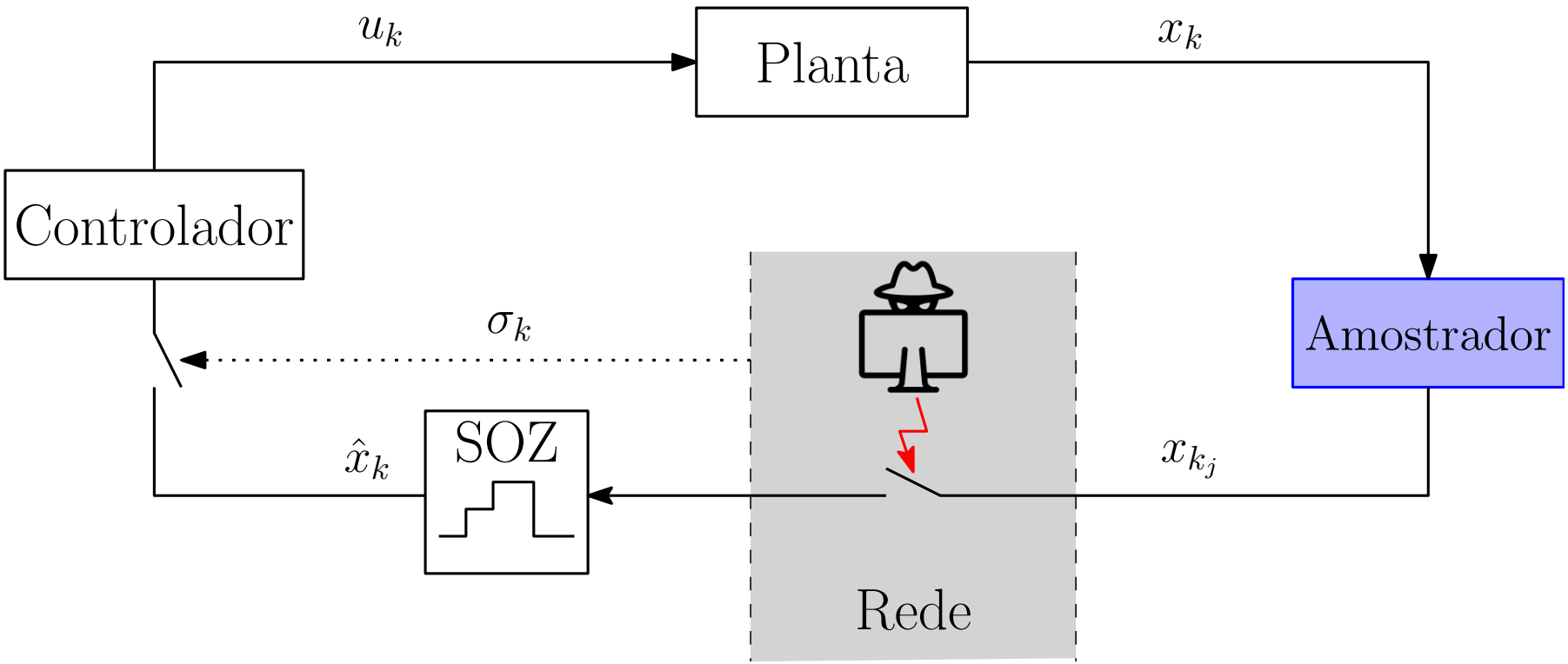
Pedro Henrique Silva Coutinho

Universidade do Estado do Rio de Janeiro

12 de agosto de 2024



Sistemas ciberfísicos sujeitos a ataques cibernéticos



Classes de ataques cibernéticos

"Ataques em sistemas de controle em rede podem ser mais graves do que em outros casos, pois esses sistemas garantem a operação de diversas infraestruturas críticas."[1]

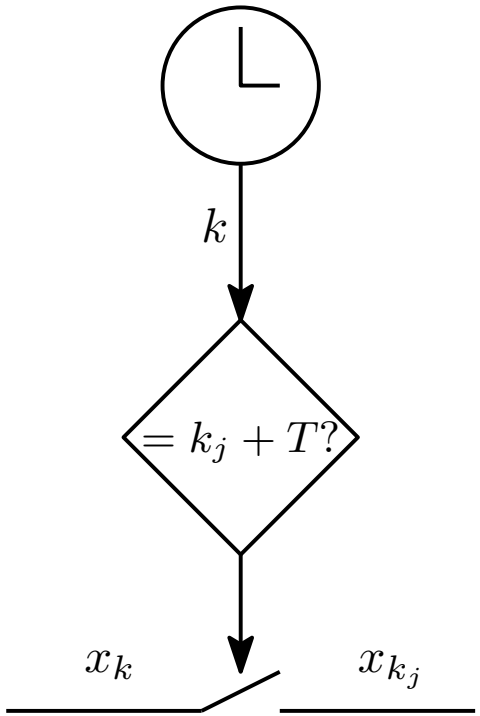
$$\text{Ataques cibernéticos} \begin{cases} \text{Deceptivos} \\ \text{Negação de serviço (DoS)} \end{cases}$$

Deceptivos: sensores ou atuadores recebem dados falsos
DoS: sensores ou atuadores não estão disponíveis

[1] SÁNCHEZ, H. S. et al. Bibliographical review on cyber attacks from a control oriented perspective. Annual Reviews in Control, v. 48, p. 103-128, 2019.

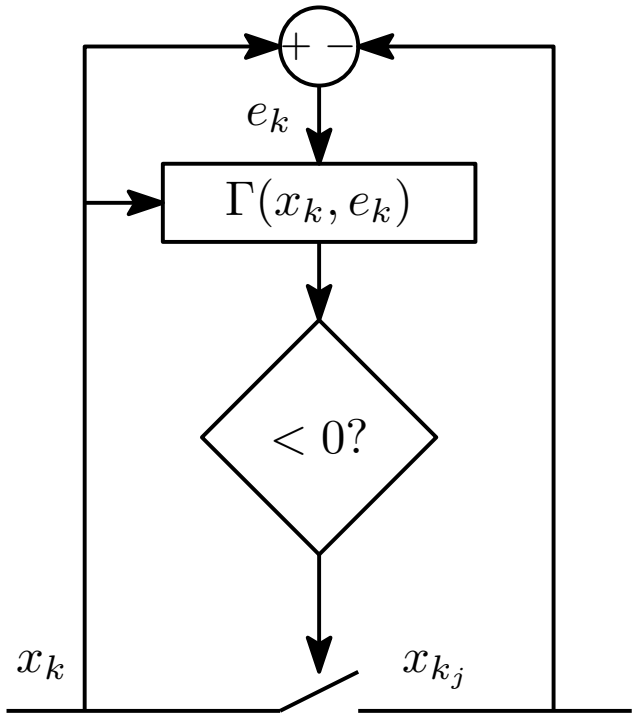
Como economizar recursos de comunicação?

Acionamento por tempo



$$k_{j+1} = k_j + T$$

Acionamento por eventos



$$k_{j+1} = \min_{k>k_j} \{\Gamma(x_k, e_k) < 0\}$$

Objetivos e contribuições

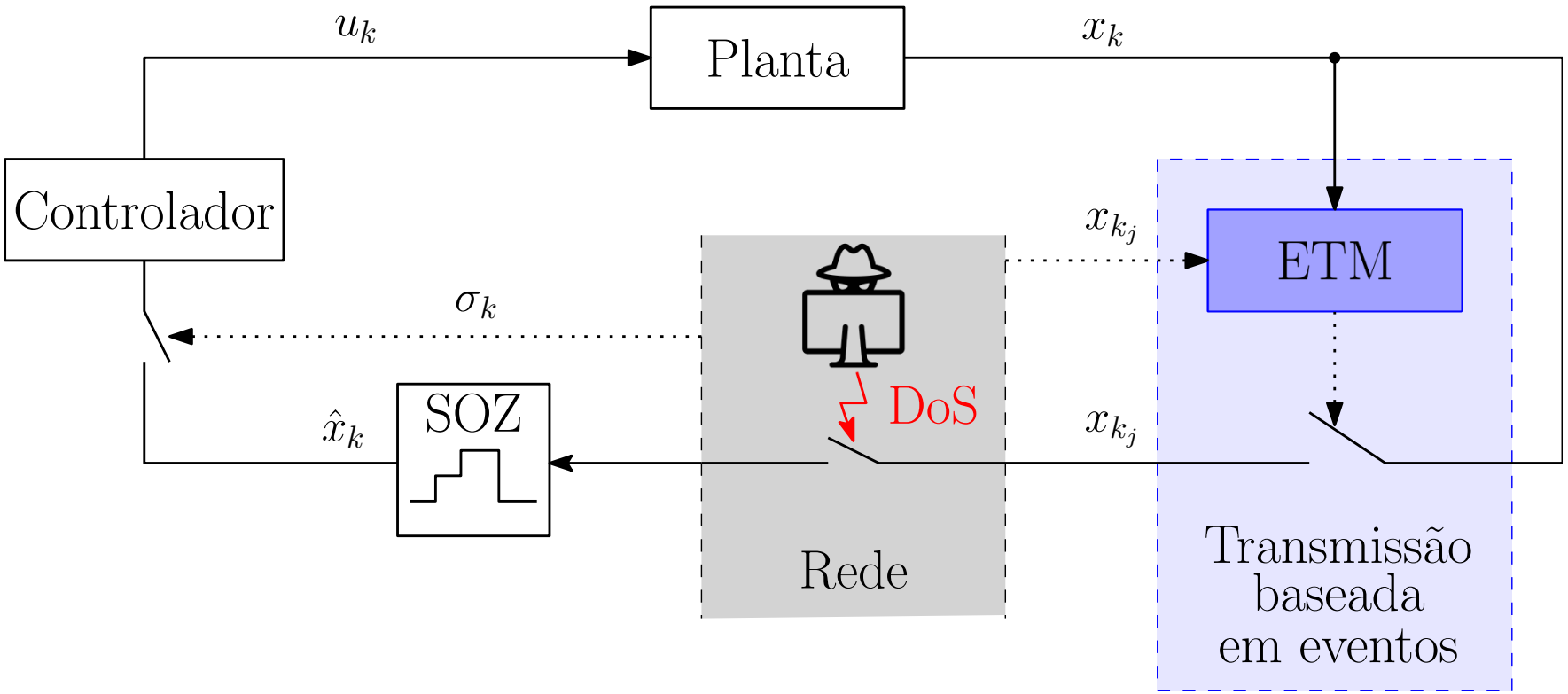
Objetivos

- Desenvolver uma estratégia de controle resiliente com acionamento por eventos a ataques DoS;
- Definir critérios de estabilidade, economia de recursos e resiliência para sistemas sujeitos a ataques DoS.

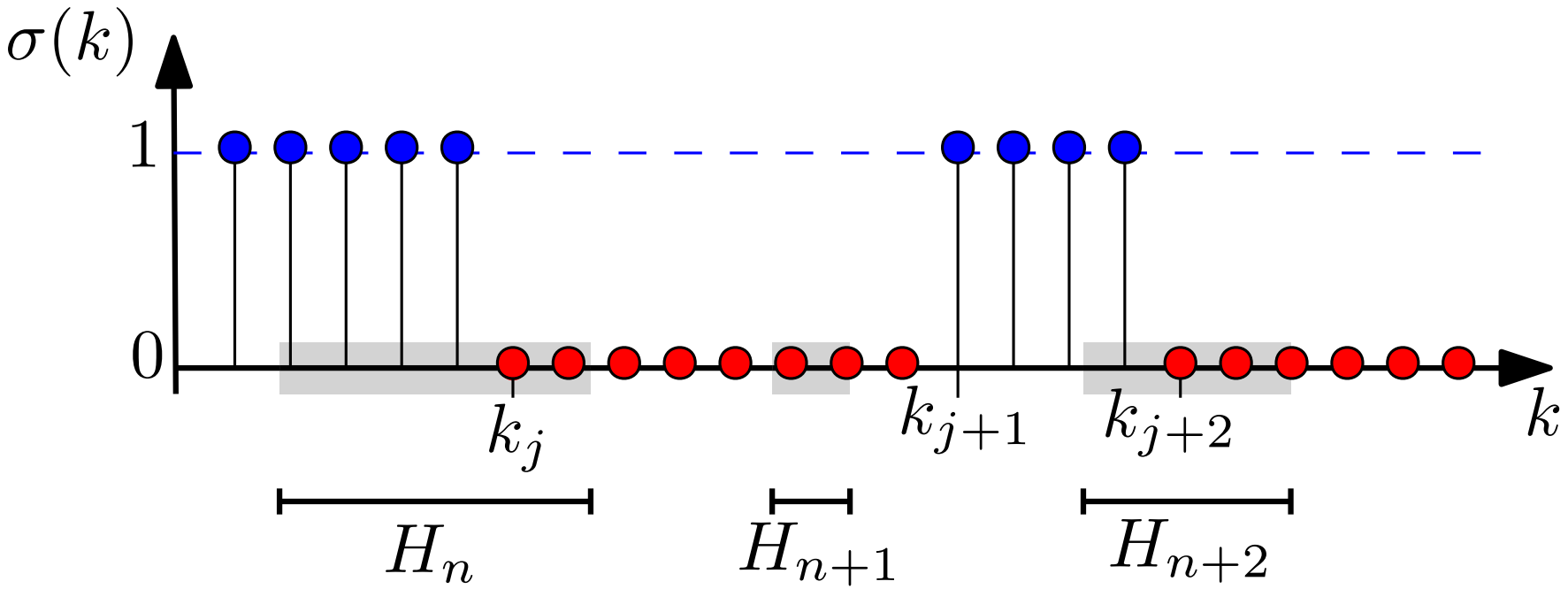
Contribuições

- Nova condição para o projeto de mecanismos de acionamento que garanta a operação resiliente de sistemas sujeitos a ataques DoS;
- Problema de otimização para realizar o projeto maximizando a resiliência a ataques e minimizando o número de transmissões efetuadas.

Configuração do sistema sujeito a ataques DoS



Estratégia de controle resiliente



Descrição dos componentes do sistema

Planta: $x_{k+1} = Ax_k + Bu_k$

Controlador: $u_k = \sigma_k K \hat{x}_k$

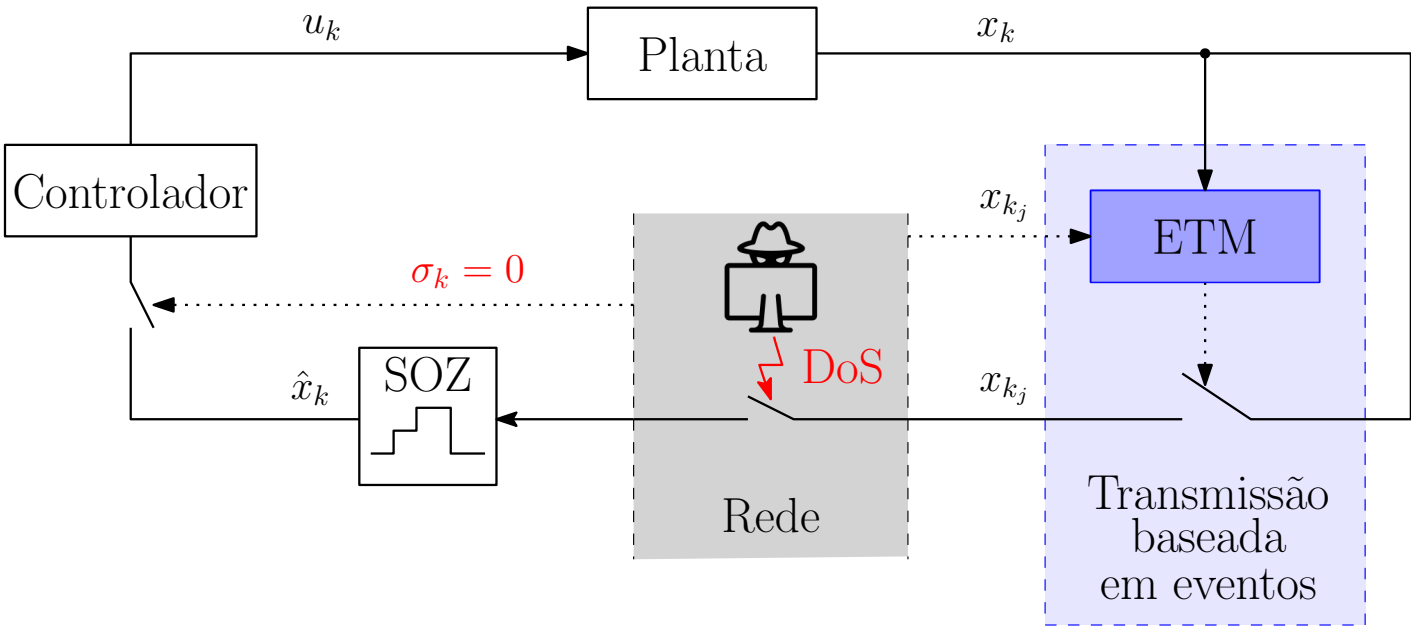
Mecanismo de acionamento: $k_{j+1} = \min_{k>k_j} \{\Gamma(\sigma_k, z_k) < 0\}$

$$\Gamma(\sigma_k, z_k) = \sigma_k \left(1 + z_k^\top \Psi z_k\right) - 1$$

onde $z_k = (x_k, e_k)$ e

$$\Psi \triangleq \begin{bmatrix} \Psi_x & \Psi_{xe} \\ \star & -\Psi_e \end{bmatrix}, \quad \Psi_x > 0, \quad \Psi_e > 0$$

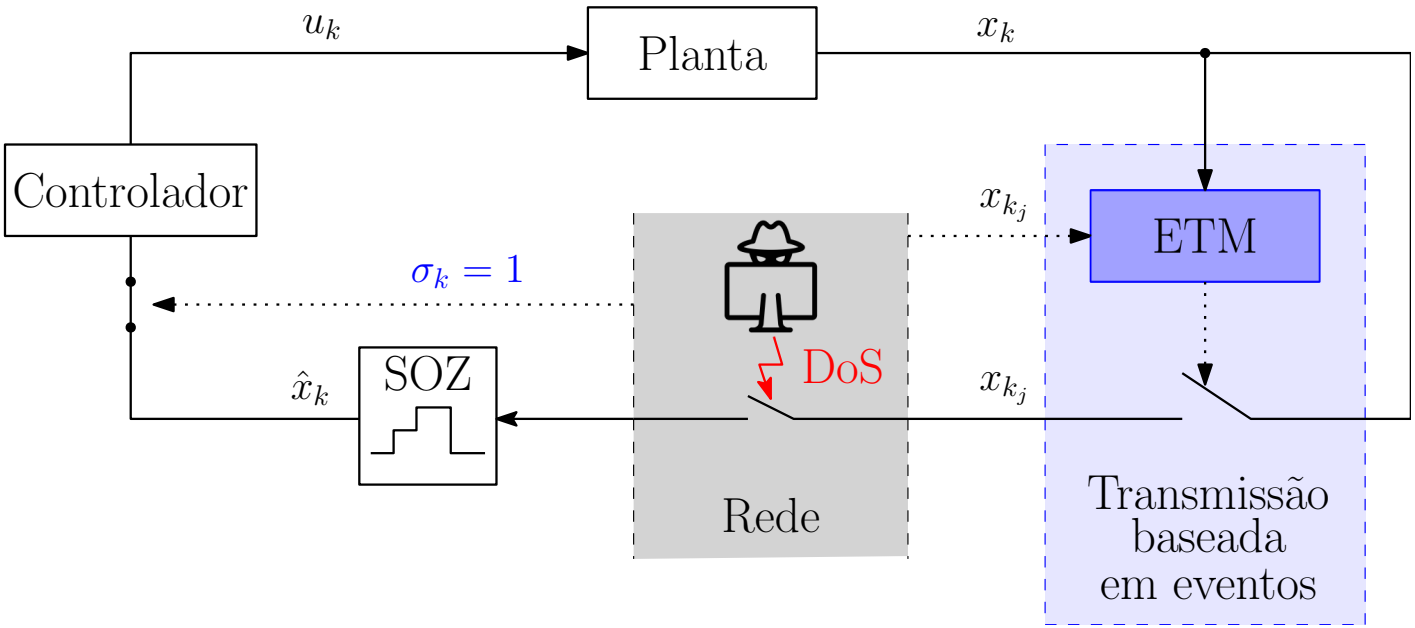
Configuração do sistema quando $\sigma_k = 0$



TRANSMISSÃO MALSUCEDIDA:

$$x_{k+1} = Ax_k$$
$$\Gamma(0, z_k) = -1, \quad \forall k \in \mathcal{K}_j$$

Configuração do sistema quando $\sigma_k = 1$



TRANSMISSÃO BEM-SUCEDIDA:

$$x_{k+1} = (A + BK)x_k + BKe_k$$
$$\Gamma(1, z_k) = z_k^\top \Psi z_k, \quad \forall k \in \mathcal{K}_j$$

Formulação do problema

Sistema chaveado com dois modos de operação:

$$x_{k+1} = F(\sigma_k)x_k + G(\sigma_k)e_k,$$

sendo

$$F(\sigma_k) \triangleq A + \sigma_k BK,$$
$$G(\sigma_k) \triangleq \sigma_k BK.$$

Declaração do problema:
Projetar o mecanismo de acionamento por eventos tal que o sistema em malha fechada seja exponencialmente estável na presença de ataques DoS com duração restrita.

Ataques DoS determinísticos

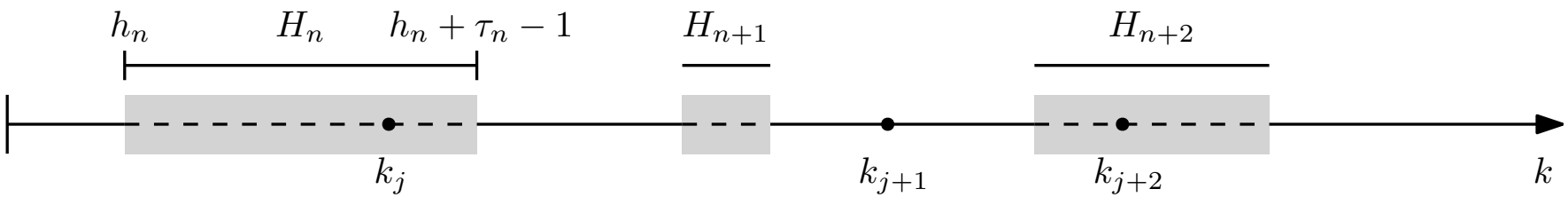


Figura: Ilustração dos intervalos afetados por ataques DoS.

Restrição sobre o número de amostras afetadas pelo ataque

Seja $\Xi(k) = \bigcup_{n\in\mathbb{Z}^+} H_n \bigcap \{0,\ldots,k\}$ o intervalo total de ataques DoS. Existem $\eta \geq 0$ e $\nu \in [0,1]$ tal que, para $k \in \mathbb{Z}^+$:

$$\Phi(k) \leq \eta + \nu k,$$

sendo $\Phi(k) = |\Xi(k)|$ o número total de amostras afetadas por ataques DoS em $\{0,\ldots,k\}$.

Condição de estabilidade

Seja $\Lambda(k) \triangleq \left\{ k \in \mathbb{Z}^+ : k \in \bigcup_{j \in \mathbb{Z}^+} \mathcal{K}_j \wedge \sigma_k = 0 \right\}$.

Se $V(x_k) = x_k^\top P x_k$, $P > 0$, satisfaz:

$$V(x_{k+1}) < \alpha V(x_k), \quad \forall k \in \Lambda(k)$$

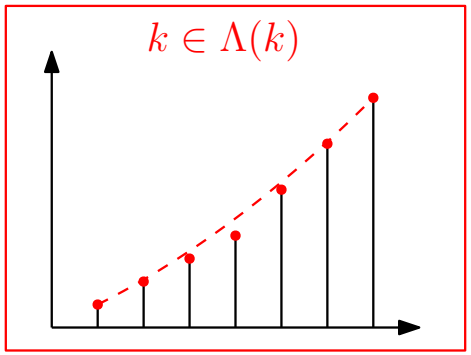
$$V(x_{k+1}) < \beta V(x_k), \quad \forall k \in \overline{\Lambda}(k)$$

para algum $\alpha > 1$ e $0 < \beta < 1$ e

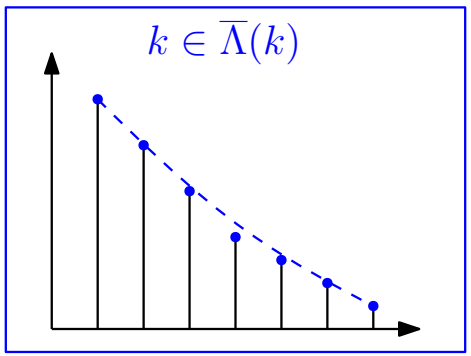
$$\nu < \frac{-\ln \beta}{\ln \alpha - \ln \beta} \triangleq \bar{\nu}(\alpha, \beta)$$

então o sistema em malha fechada é exponencialmente estável.

Transmissão malsucedida



Transmissão bem-sucedida



Critérios de projeto

Aumento da resiliência a ataques DoS

Está relacionado à maximização de:

$$f_1 = \bar{\nu}\left(\alpha, \beta\right) = \frac{-\ln \beta}{\ln \alpha - \ln \beta}$$

Redução do número de transmissões (economia de recursos)

Está relacionada à minimização de

$$f_2 = \mathrm{tr}\left(\tilde{\Psi}_x + \Psi_e\right)$$

Problema multiobjetivo resolvido via método ε-restrito.

Problema de otimização ε-restrito

Dados $0 < \beta < 1$, $\alpha > 1$ e $\varepsilon > 0$

$$
\begin{aligned}
\text{maximize} \quad & \bar{\nu}(\alpha, \beta) \\
\text{sujeito a} \quad & \operatorname{tr}\left(\tilde{\Psi}_x + \Psi_e\right) \leq \varepsilon, \\
& P > 0, \ \tilde{\Psi}_x > 0, \ \Psi_e > 0, \\
& F_0^\top P F_0 - \alpha P < 0, \\
& \begin{bmatrix} F_1^\top P F_1 - \beta P & F_1^\top P G_1 + \Psi_{xe} & \mathrm{I} \\ \star & G_1^\top P G_1 - \Psi_e & 0 \\ \star & \star & -\tilde{\Psi}_x \end{bmatrix} < 0
\end{aligned}
$$

Experimentos numéricos

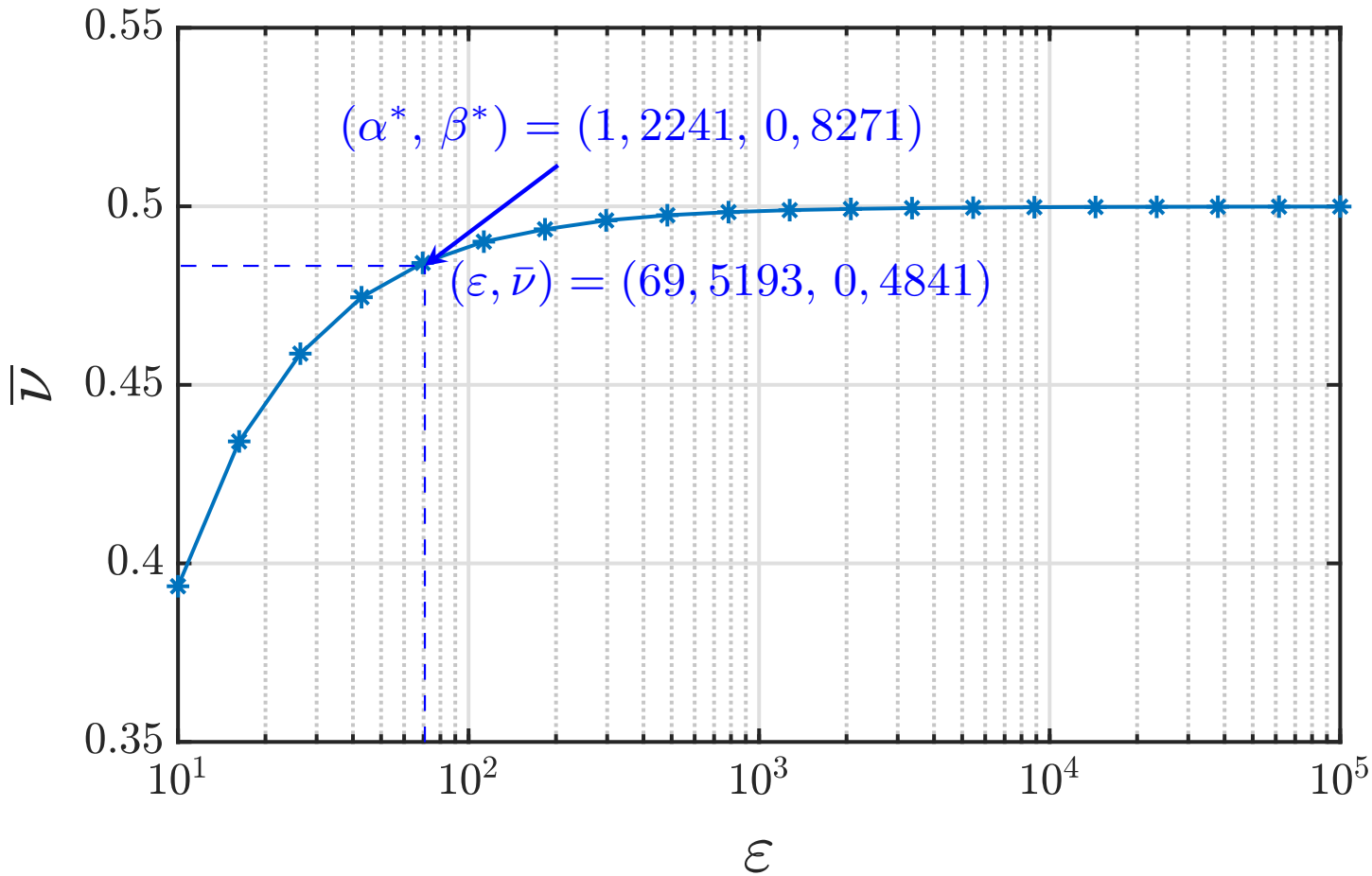
$$x_{k+1} = \underbrace{\begin{bmatrix} 1,0050 & 0,0501 \\ 0,2003 & 1,0050 \end{bmatrix}}_{A} x_k + \underbrace{\begin{bmatrix} 0,0501 \\ 0,0050 \end{bmatrix}}_{B} u_k$$

$$u_k = \underbrace{\begin{bmatrix} -6 & -3 \end{bmatrix}}_{K} x_k$$

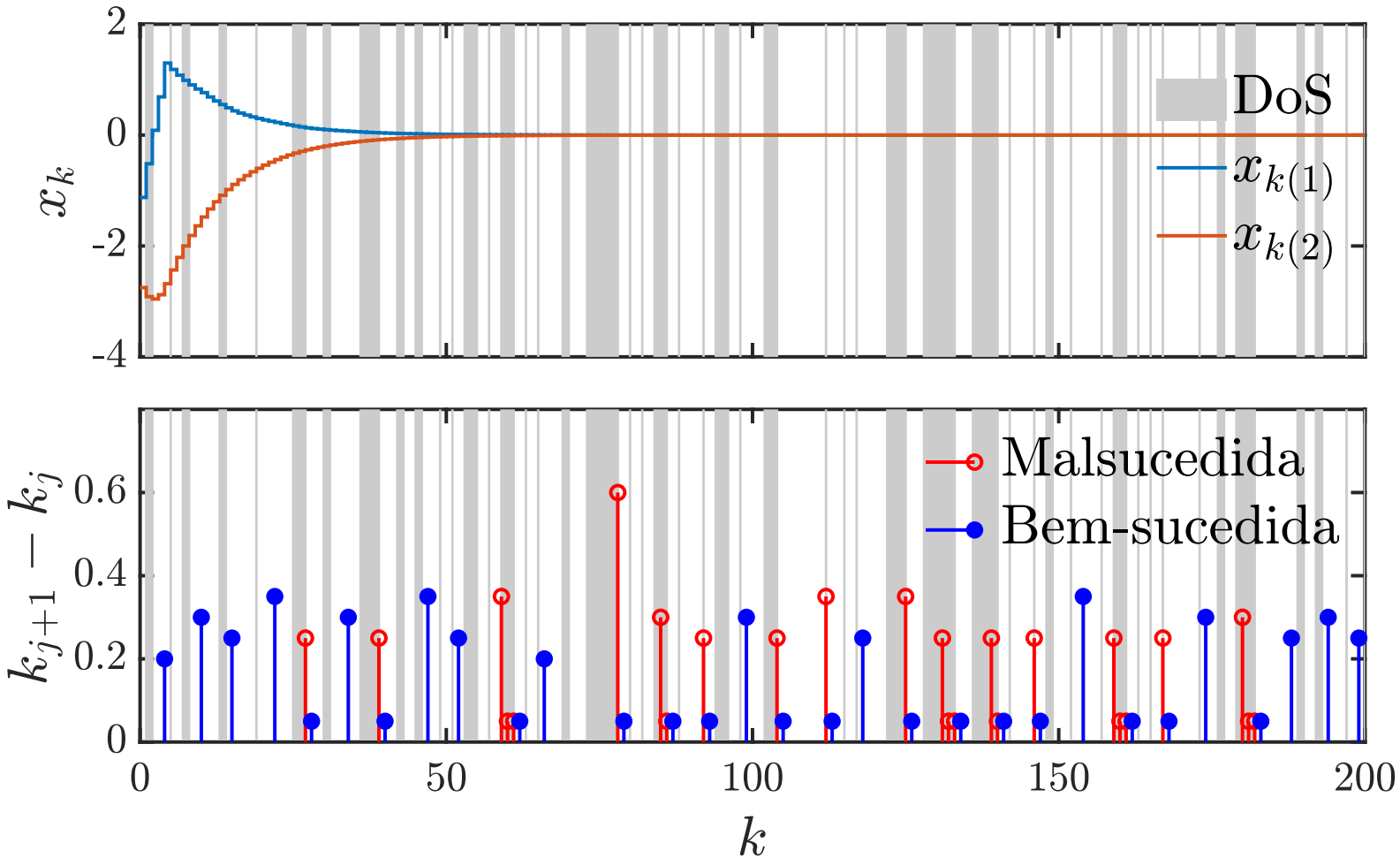
Autovalores de $A + BK$ são $0,7897$ e $0,9048$.

- São considerados 20 valores de ε espaçados igualmente em escala logarítmica entre 10^1 e 10^5;
- Para cada ε, o par (α^*, β^*) que maximiza a função objetivo $f_1 = \bar{\nu}$ é obtido via bisseção sobre os parâmetros α e β.

Estimativa da fronteira de Pareto



Simulação em malha fechada com $\bar{\nu} = 0.4841$



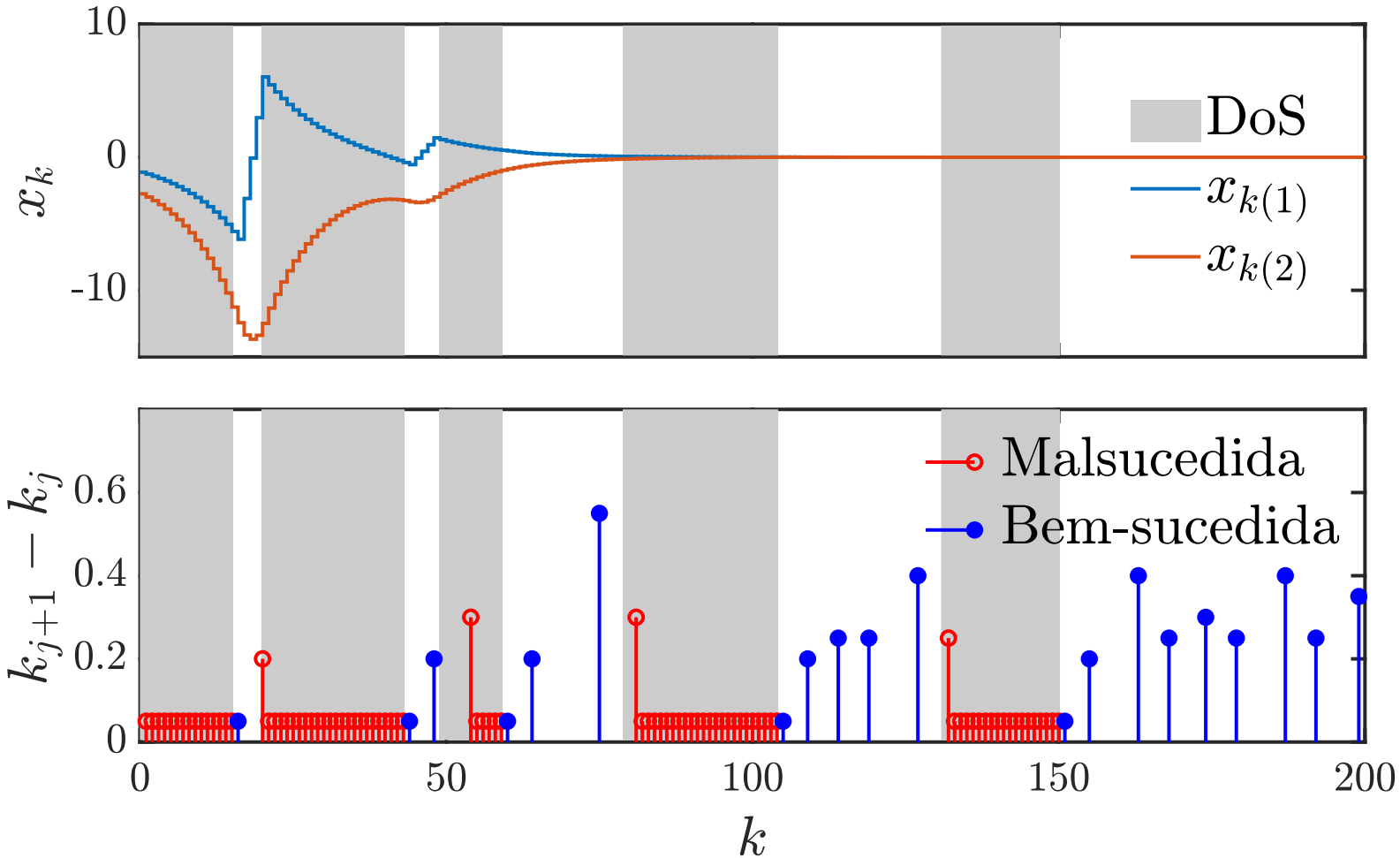
Comparação com transmissão periódica

Tabela: Número de transmissões para cada política de transmissão.

Acionamento por eventos		
Bem-sucedidas	Malsucedidas	Total
31	25	56
Transmissão periódica		
104	97	201

Economia de 72,13 % no número de transmissões em relação à amostragem periódica.

Simulação em malha fechada com $\bar{\nu} = 0.4841$



Referências

1. Coutinho, P. H. S., Bessa, I., Peixoto, M. L., Pessim, P. S., Pires, P. O., & Palhares, R. M. (2022, October). Controle com Acionamento por Eventos Resiliente a Ataques de Negaçao de Serviço. In Congresso Brasileiro de Automática-CBA (Vol. 3, No. 1).
2. Coutinho, P. H. S., Bessa, I., Pessim, P. S., & Palhares, R. M. (2023). A switching approach to event-triggered control systems under denial-of-service attacks. Nonlinear Analysis: Hybrid Systems, 50, 101383.

Agradecimentos

Contato: phcoutinho@eng.uerj.br