A Zero-Sum Game Framework for Optimal Sensor Placement in Uncertain Networked Control Systems under Cyber-Attacks

Anh Tung Nguyen, Sribalaji C. Anand, and André Teixeira
Uppsala University, Sweden

IEEE Conference on Decision and Control
Cancún, Mexico, December 2022

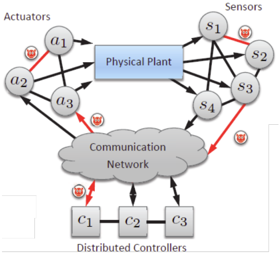
Swedish Research Council

Stiftelsen för Strategisk Forskning

Outline

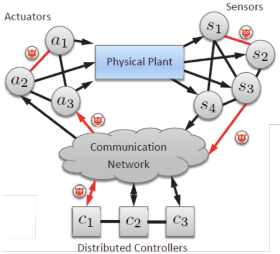
Outline

Motivation



Several cyber incidents on Cyber-physical systems in the past

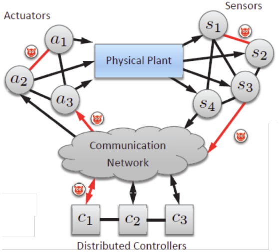
Motivation



Several cyber incidents on Cyber-physical systems in the past

1. DoS attack on the Ukrainian power grid in 2015.
2. Data injection attack on Kemuri water distribution company in 2016.
3. . . . and many more.

Motivation



Several cyber incidents on Cyber-physical systems in the past

1. DoS attack on the Ukrainian power grid in 2015.
2. Data injection attack on Kemuri water distribution company in 2016.
3. . . . and many more.

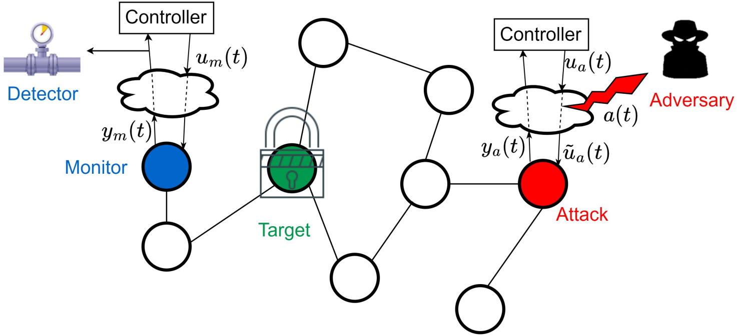
Lesson: Be proactive and protect the system, even uncertain system modeling

Outline

Problem description

The main research question

Given an uncertain networked control system (multi-agent system) under cyber-attacks, how to place a sensor at an agent s.t. minimizing the risk on a given local performance.



System description

- Undirected connected graph $\mathcal{G}$ with N agents

$$\dot{x}_i^{\Delta}(t) = \sum_{v_j \in \mathcal{N}_i} \ell_{ij}^{\Delta}\big(x_i^{\Delta}(t) - x_j^{\Delta}(t)\big) + \tilde{u}_i(t),\ \ v_i \in \big\{v_1, v_2, \ldots, v_N\big\},$$

$$y_{\tau}^{\Delta}(t) = x_{\tau}^{\Delta}(t),$$

- Healthy/Attacked local controller

$$\tilde{u}_i(t) = -\theta_i^{\Delta} x_i^{\Delta}(t) + \begin{cases} 0, & \text{if } v_i \text{ is healthy} \\ a(t), & \text{if } v_i \text{ is attacked} \end{cases}$$

System description

- Undirected connected graph $\mathcal{G}$ with N agents

$$\dot{x}_i^{\Delta}(t) = \sum_{v_j \in \mathcal{N}_i} \ell_{ij}^{\Delta}\big(x_i^{\Delta}(t) - x_j^{\Delta}(t)\big) + \tilde{u}_i(t),\ \ v_i \in \{v_1, v_2, \ldots, v_N\},$$

$$y_{\tau}^{\Delta}(t) = x_{\tau}^{\Delta}(t),$$

- Healthy/Attacked local controller

$$\tilde{u}_i(t) = -\theta_i^{\Delta} x_i^{\Delta}(t) + \begin{cases} 0, & \text{if } v_i \text{ is healthy} \\ a(t), & \text{if } v_i \text{ is attacked} \end{cases}$$

- Healthy closed-loop model ($a(t) = 0$)

$$\dot{x}^{\Delta}(t) = -L^{\Delta} x^{\Delta}(t),\ \ L^{\Delta} \triangleq \bar{L} + \Delta,\ \ \Delta \in \Omega.$$

Assume that Ω is a compact set.

UPPSALA UNIVERSITET

Detector and Adversary description

- **Revisit**: Undirected connected graph $\mathcal{G}$ (vertex set $\mathcal{V}$, edge set $\mathcal{E}$, L^{Δ}), protected target vertex v_τ, and closed-loop healthy system

$$\dot{x}^{\Delta}(t) = -L^{\Delta}x^{\Delta}(t), \quad L^{\Delta} \triangleq \bar{L} + \Delta, \quad \Delta \in \Omega.$$

UPPSALA UNIVERSITET

Detector and Adversary description

• **Revisit**: Undirected connected graph $\mathcal{G}$ (vertex set $\mathcal{V}$, edge set $\mathcal{E}$, L^{Δ}), protected target vertex v_{τ}, and closed-loop healthy system

$$\dot{x}^{\Delta}(t) = -L^{\Delta}x^{\Delta}(t), \quad L^{\Delta} \triangleq \bar{L} + \Delta, \quad \Delta \in \Omega.$$

• **Prior information**
Know: Sets $\mathcal{V}$, $\mathcal{E}$, Ω; location v_{τ}; nominal $\bar{L}$.
Don't know: Δ; their rivals' exact actions.

UPPSALA UNIVERSITET

Detector and Adversary Purpose

- Fixed local performance at protected vertex v_τ: $\|y_\tau\|^2_{\mathcal{L}_2[0,T]}$

Detector and Adversary Purpose

- Fixed local performance at protected vertex v_τ: $\|y_\tau\|^2_{\mathcal{L}_2[0,T]}$
- Adversary purpose

Choose $v_a \in \mathcal{V} \setminus \{v_\tau\}$; design $a(t)$ as **stealthy** $\|y_m^\Delta\|^2_{\mathcal{L}_2[0,T]} \leq \sigma$

And maximize $\|y_\tau\|^2_{\mathcal{L}_2[0,T]}$ where $\tilde{u}_a(t) = u_a(t) + a(t)$

Detector and Adversary Purpose

- Fixed local performance at protected vertex v_τ: $\|y_\tau\|^2_{\mathcal{L}_2[0,T]}$

- Adversary purpose

Choose $v_a \in \mathcal{V} \setminus \{v_\tau\}$; design $a(t)$ as **stealthy** $\|y_m^\Delta\|^2_{\mathcal{L}_2[0,T]} \leq \sigma$

And maximize $\|y_\tau\|^2_{\mathcal{L}_2[0,T]}$ where $\tilde{u}_a(t) = u_a(t) + a(t)$

- Detector purpose:

Choose $v_m \in \mathcal{V} \setminus \{v_\tau\}$ to detect cyber-attack $\|y_m^\Delta\|^2_{\mathcal{L}_2[0,T]} > \sigma$

And $\|y_\tau\|^2_{\mathcal{L}_2[0,T]}$ as low as possible

Outline

Risk on local performance

- Worst-case attack impact on local performance

$$\sup_{a \in \mathcal{L}_2[0,T]} J_\tau(v_a, v_m; \Delta, a),$$

$$J_\tau(v_a, v_m; \Delta, a) \triangleq \left\| y_\tau^\Delta \right\|^2_{\mathcal{L}_2[0,T]} \mathbb{I}_{\mathcal{A}}(a),$$

$$\mathcal{A} \triangleq \{a | \ \left\| y_m^\Delta \right\|^2_{\mathcal{L}_2[0,T]} \leq \sigma, \ x(0) = 0\},$$

Risk on local performance

- Worst-case attack impact on local performance

$$\sup_{a \in \mathcal{L}_2[0,T]} J_\tau(v_a, v_m; \Delta, a),$$

$$J_\tau(v_a, v_m; \Delta, a) \triangleq \left\| y_\tau^\Delta \right\|^2_{\mathcal{L}_2[0,T]} \mathbb{I}_{\mathcal{A}}(a),$$

$$\mathcal{A} \triangleq \{a | \ \left\| y_m^\Delta \right\|^2_{\mathcal{L}_2[0,T]} \leq \sigma, \ x(0) = 0\},$$

Difficulty: $\Delta \in \Omega$ is uncertain to both detector and adversary.

UPPSALA UNIVERSITET

Risk on local performance

- Worst-case attack impact on local performance

$$\sup_{a \in \mathcal{L}_2[0,T]} J_\tau(v_a, v_m; \Delta, a),$$

$$J_\tau(v_a, v_m; \Delta, a) \triangleq \left\|y_\tau^\Delta\right\|^2_{\mathcal{L}_2[0,T]} \mathbb{I}_\mathcal{A}(a),$$

$$\mathcal{A} \triangleq \{a| \ \left\|y_m^\Delta\right\|^2_{\mathcal{L}_2[0,T]} \leq \sigma, \ x(0) = 0\},$$

Difficulty: $\Delta \in \Omega$ is uncertain to both detector and adversary.

- Risk metric - Value at Risk (VaR_β) over uncertainty set Ω

$$\mathcal{J}_\tau(v_a, v_m) = \text{VaR}_{\beta,\Omega}\Big[\sup_{a \in \mathcal{L}_2[0,T]} J_\tau(v_a, v_m; \Delta, a)\Big]$$

Risk on local performance

- Worst-case attack impact on local performance

$$\sup_{a \in \mathcal{L}_2[0,T]} J_\tau(v_a, v_m; \Delta, a),$$

$$J_\tau(v_a, v_m; \Delta, a) \triangleq \left\| y_\tau^\Delta \right\|^2_{\mathcal{L}_2[0,T]} \mathbb{I}_\mathcal{A}(a),$$

$$\mathcal{A} \triangleq \{a| \ \left\| y_m^\Delta \right\|^2_{\mathcal{L}_2[0,T]} \leq \sigma, \ x(0) = 0\},$$

Difficulty: $\Delta \in \Omega$ is uncertain to both detector and adversary.

- Risk metric - Value at Risk (VaR_β) over uncertainty set Ω

$$\mathcal{J}_\tau(v_a, v_m) = \text{VaR}_{\beta,\Omega}\left[\sup_{a \in \mathcal{L}_2[0,T]} J_\tau(v_a, v_m; \Delta, a)\right]$$

Illustrate VaR →

Value at Risk

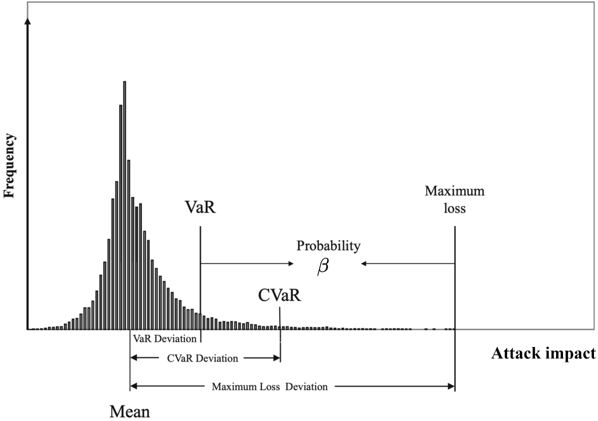


Figure: Risk metrics

UPPSALA UNIVERSITET

Problem formulation

Problem formulation (zero-sum game)

Given protected target vertex v_τ, game payoff $\mathcal{J}_\tau(v_a, v_m)$

$$\min_{v_m \neq v_\tau \in \mathcal{V}} \; \max_{v_a \neq v_\tau \in \mathcal{V}} \; \mathcal{J}_\tau(v_a, v_m).$$

[1] Zhu, Q., & Basar, T. (2015). Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. IEEE Control Systems Magazine, 35(1), 46-65.

Problem formulation

Problem formulation (zero-sum game)

Given protected target vertex v_τ, game payoff $\mathcal{J}_\tau(v_a, v_m)$

$$\min_{v_m \neq v_\tau \in \mathcal{V}} \max_{v_a \neq v_\tau \in \mathcal{V}} \mathcal{J}_\tau(v_a, v_m).$$

The detector and the adversary satisfy[1]

$$-\infty < \mathcal{J}_\tau(v_a, v_m^\star) \leq \mathcal{J}_\tau(v_a^\star, v_m^\star) \leq \mathcal{J}_\tau(v_a^\star, v_m) < \infty, \quad \forall v_a, v_m \in \mathcal{V} \setminus \{v_\tau\}.$$

[1] Zhu, Q., & Basar, T. (2015). Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. IEEE Control Systems Magazine, 35(1), 46-65.

Outline

Approximating game payoff

- Uncertainty set Ω, take M_1 sampled uncertainty values $\Delta_i \in \Omega,\ i = \{1, 2, \dots, M_1\}$

Theorem 4.1

Let $\epsilon_1, \beta_1 \in (0, 1)$ be chosen such that

$$\mathbb{P}\{|\mathbb{P}_\Omega(X < \gamma) - \hat{\mathbb{P}}_{M_1}| > \epsilon_1\} \leq \beta_1$$

where $\hat{\mathbb{P}}_{M_1} \triangleq \frac{1}{M_1} \sum_{i=1}^{M_1} \mathbb{I}\left(X \leq \gamma\right)$, where $M_1 \geq \frac{1}{2\epsilon_1^2} \log \frac{2}{\beta_1}$.
Then, VaR_β with an accuracy ϵ_1 and confidence β_1 by

$$\hat{\gamma} \triangleq \min \ \gamma \quad \text{s.t.} \ \hat{\mathbb{P}}_{M_1} \geq 1 - \beta.$$

Approximating game payoff

- Uncertainty set Ω, take M_1 sampled uncertainty values $\Delta_i \in \Omega,\ i = \{1, 2, \ldots, M_1\}$

Theorem 4.1

Let $\epsilon_1, \beta_1 \in (0,1)$ be chosen such that

$$\mathbb{P}\{|\mathbb{P}_\Omega(X < \gamma) - \hat{\mathbb{P}}_{M_1}| > \epsilon_1\} \leq \beta_1$$

where $\hat{\mathbb{P}}_{M_1} \triangleq \frac{1}{M_1}\sum_{i=1}^{M_1} \mathbb{I}\left(X \leq \gamma\right)$, where $M_1 \geq \frac{1}{2\epsilon_1^2}\log\frac{2}{\beta_1}$. Then, VaR_β with an accuracy ϵ_1 and confidence β_1 by

$$\hat{\gamma} \triangleq \min\ \gamma \quad \text{s.t.}\ \hat{\mathbb{P}}_{M_1} \geq 1 - \beta.$$

- Q: Should we evaluate M_1 game payoff values?

Evaluating game payoff

- We only need to evaluate $\lceil M_1(1-\beta_1)\rceil$ values *(Lemma 4.2)*

E.g., $\epsilon_1 = 0.06$, $\beta_1 = 0.08$, $M_1 \geq 450 \Rightarrow$ evaluate 414 values

[2] Ferrari, R. M., & Teixeira, A. M. (Eds.). (2021). Safety, Security and Privacy for Cyber-Physical Systems. Cham: Springer.

[3] Teixeira, A. et al. (2015). Strategic stealthy attacks: the output-to-output ℓ_2-gain. 54th IEEE CDC

Evaluating game payoff

- We only need to evaluate $\lceil M_1(1-\beta_1) \rceil$ values *(Lemma 4.2)*
E.g., $\epsilon_1 = 0.06$, $\beta_1 = 0.08$, $M_1 \geq 450 \Rightarrow$ evaluate 414 values
- Worst-case attack impact with a sampled uncertainty Δ_i.

$$\gamma_i^\star \triangleq \sup_{a \in \mathcal{L}_2[0,T]} \left\| y_T^{\Delta_i} \right\|^2 \quad \text{s.t.} \quad \left\| y_m^{\Delta_i} \right\|^2 \leq \sigma$$

[2]Ferrari, R. M., & Teixeira, A. M. (Eds.). (2021). Safety, Security and Privacy for Cyber-Physical Systems. Cham: Springer.

[3]Teixeira, A. et al. (2015). Strategic stealthy attacks: the output-to-output ℓ_2-gain. 54th IEEE CDC

Evaluating game payoff

- We only need to evaluate $\lceil M_1(1-\beta_1) \rceil$ values *(Lemma 4.2)*

E.g., $\epsilon_1 = 0.06$, $\beta_1 = 0.08$, $M_1 \geq 450 \Rightarrow$ evaluate 414 values

- Worst-case attack impact with a sampled uncertainty Δ_i.

$$\gamma_i^\star \triangleq \sup_{a \in \mathcal{L}_2[0,T]} \left\| y_\mathcal{T}^{\Delta_i} \right\|^2 \quad \text{s.t.} \quad \left\| y_m^{\Delta_i} \right\|^2 \leq \sigma$$

- Solved via LMIs[2]

[2] Ferrari, R. M., & Teixeira, A. M. (Eds.). (2021). Safety, Security and Privacy for Cyber-Physical Systems. Cham: Springer.

[3] Teixeira, A. et al. (2015). Strategic stealthy attacks: the output-to-output ℓ_2-gain. 54th IEEE CDC

UPPSALA UNIVERSITET

Evaluating game payoff

- We only need to evaluate $\lceil M_1(1-\beta_1)\rceil$ values *(Lemma 4.2)*

E.g., $\epsilon_1 = 0.06$, $\beta_1 = 0.08$, $M_1 \geq 450 \Rightarrow$ evaluate 414 values

- Worst-case attack impact with a sampled uncertainty Δ_i.

$$\gamma_i^\star \triangleq \sup_{a \in \mathcal{L}_2[0,T]} \left\| y_\tau^{\Delta_i} \right\|^2 \quad \text{s.t.} \quad \left\| y_m^{\Delta_i} \right\|^2 \leq \sigma$$

- Solved via LMIs[2]
- Always have $\gamma_i^\star < \infty$?

[2] Ferrari, R. M., & Teixeira, A. M. (Eds.). (2021). Safety, Security and Privacy for Cyber-Physical Systems. Cham: Springer.

[3] Teixeira, A. et al. (2015). Strategic stealthy attacks: the output-to-output ℓ_2-gain. 54th IEEE CDC

UPPSALA UNIVERSITET

Motivation

Problem Description

Problem Formulation

Proposed method

Numerical examples

Conclusions

Evaluating game payoff

- We only need to evaluate $\lceil M_1(1-\beta_1)\rceil$ values *(Lemma 4.2)*

E.g., $\epsilon_1 = 0.06$, $\beta_1 = 0.08$, $M_1 \geq 450 \Rightarrow$ evaluate 414 values

- Worst-case attack impact with a sampled uncertainty Δ_i.

$$\gamma_i^\star \triangleq \sup_{a\in\mathcal{L}_2[0,T]} \left\| y_\tau^{\Delta_i} \right\|^2 \quad \text{s.t.} \quad \left\| y_m^{\Delta_i} \right\|^2 \leq \sigma$$

- Solved via LMIs[2]
- Always have $\gamma_i^\star < \infty$?
- Invariant zeros[3] of $\Sigma_m = (-L^{\Delta_i}, e_a, e_m^\top, 0)$ where $y_m^{\Delta_i}(t)$ is its output: unstable finite and infinite

[2] Ferrari, R. M., & Teixeira, A. M. (Eds.). (2021). Safety, Security and Privacy for Cyber-Physical Systems. Cham: Springer.

[3] Teixeira, A. et al. (2015). Strategic stealthy attacks: the output-to-output ℓ_2-gain. 54th IEEE CDC

Invariant zeros

- Consider invariant zeros of $\Sigma_m = (A, B, C_m, 0)$ where $y_m(t)$ is its output.

$$\begin{bmatrix} \lambda I - A & -B \\ C_m & 0 \end{bmatrix} \begin{bmatrix} \bar{x} \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \bar{x} \neq 0. \tag{1}$$

Invariant zeros

- Consider invariant zeros of $\Sigma_m = (A, B, C_m, 0)$ where $y_m(t)$ is its output.

$$\begin{bmatrix} \lambda I - A & -B \\ C_m & 0 \end{bmatrix} \begin{bmatrix} \bar{x} \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \bar{x} \neq 0. \qquad (1)$$

- **Finite invariant zeros $\lambda < \infty$**

Lemma 4.4 (choice of parameters)

Finite invariant zeros of Σ_m can be shifted to LHP by local controllers.

Invariant zeros

- Consider invariant zeros of $\Sigma_m = (A, B, C_m, 0)$ where $y_m(t)$ is its output.

$$\begin{bmatrix} \lambda I - A & -B \\ C_m & 0 \end{bmatrix} \begin{bmatrix} \bar{x} \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \bar{x} \neq 0. \qquad (1)$$

- **Finite invariant zeros** $\lambda < \infty$

Lemma 4.4 (choice of parameters)

Finite invariant zeros of Σ_m can be shifted to LHP by local controllers.

- **Infinite invariant zeros** $\lambda = 1/s$ **where** $s = 0$ **satisfies (1)**

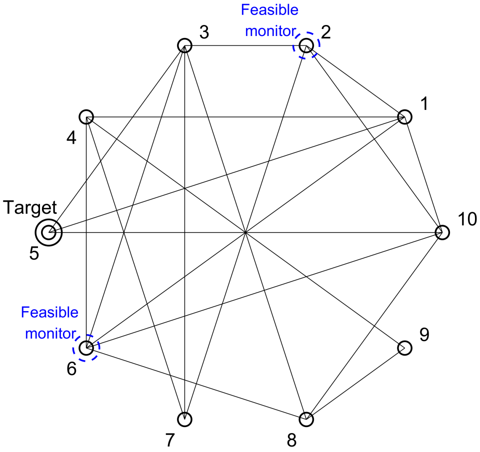
Relative degree r_Σ of a linear system Σ

Σ_m has output $y_m(t)$ and Σ_τ has output $y_\tau(t)$

$$r_{\ \Sigma_m} \leq r_{\ \Sigma_\tau}$$

Outline

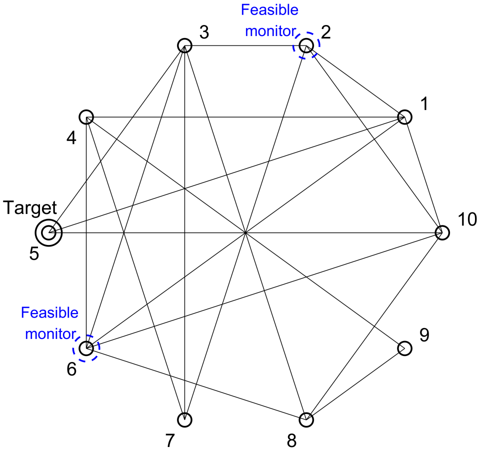
Numerical examples



Two cases of Value-at-Risk VaR_β where

1) $\beta = 0.08$
2) $\beta = 0.15$

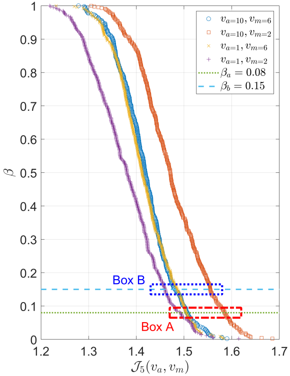
Numerical examples



Two cases of Value-at-Risk VaR_β where
1) $\beta = 0.08$
2) $\beta = 0.15$

What are the best choices for the detector and the adversary?

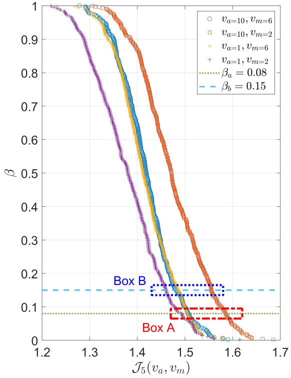
Numerical examples



- Case 1 (Box A): $\beta = 0.08$

$$\begin{aligned} &\mathcal{J}_5(\forall v_a \in \mathcal{V} \setminus \{v_5, v_{10}\}, v_{m=6}) \\ &< \mathcal{J}_5(v_{a=10}, v_{m=6}) \\ &< \mathcal{J}_5(v_{a=10}, v_{m=2}). \end{aligned}$$

Numerical examples



- Case 1 (Box A): $\beta = 0.08$

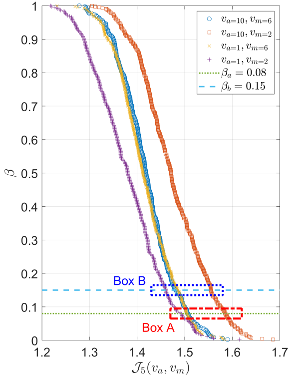
$$\mathcal{J}_5(\forall v_a \in \mathcal{V} \setminus \{v_5, v_{10}\}, v_{m=6}) < \mathcal{J}_5(v_{a=10}, v_{m=6}) < \mathcal{J}_5(v_{a=10}, v_{m=2}).$$

- Case 2 (Box B): $\beta = 0.15$

$$\mathcal{J}_5(v_{a=1}, v_{m=2}) = 1.4603,$$
$$\mathcal{J}_5(v_{a=10}, v_{m=6}) = 1.4803,$$
$$\mathcal{J}_5(v_{a=1}, v_{m=6}) = 1.4856,$$
$$\mathcal{J}_5(v_{a=10}, v_{m=2}) = 1.5550.$$

UPPSALA UNIVERSITET

Numerical examples



- Case 1 (Box A): $\beta = 0.08$

$$\mathcal{J}_5(\forall v_a \in \mathcal{V} \setminus \{v_5, v_{10}\}, v_{m=6}) < \mathcal{J}_5(v_{a=10}, v_{m=6}) < \mathcal{J}_5(v_{a=10}, v_{m=2}).$$

- Case 2 (Box B): $\beta = 0.15$

$$\mathcal{J}_5(v_{a=1}, v_{m=2}) = 1.4603,$$
$$\mathcal{J}_5(v_{a=10}, v_{m=6}) = 1.4803,$$
$$\mathcal{J}_5(v_{a=1}, v_{m=6}) = 1.4856,$$
$$\mathcal{J}_5(v_{a=10}, v_{m=2}) = 1.5550.$$

$$\mathbb{P}^\star(v_{m=6}) \approx 94.72\%, \ \mathbb{P}^\star(v_{m=2}) \approx 5.28\%,$$
$$\mathbb{P}^\star(v_{a=10}) \approx 25.29\%, \ \mathbb{P}^\star(v_{a=1}) \approx 74.71\%,$$
$$\mathbb{P}^\star(\forall v_a \in \mathcal{V} \setminus \{1, 5, 10\}) = 0\%.$$

Outline

UPPSALA UNIVERSITET

Conclusions

- We considered uncertain networked control systems under cyber-attacks
- The problem was formulated through zero-sum game framework
- We evaluated and computed the risk to find optimal sensor placement
- We illustrated the proposed method through a numerical example

anh.tung.nguyen@it.uu.se

Questions!!!