UPPSALA UNIVERSITET

Uppsala Secure Learning and Control Lab

Security Allocation in Networked Control Systems

Anh Tung Nguyen

Dissertation for the degree of Licentiate

October 13, 2023

Stiftelsen för Strategisk Forskning

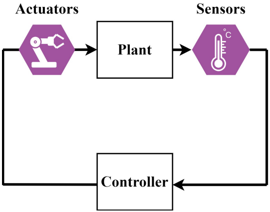
Swedish Research Council

Outline

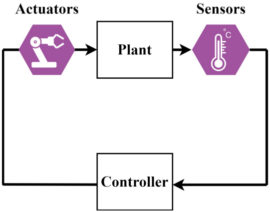
1. Introduction
2. Security in Networked Control Systems
3. Problem Formulation
4. Contributions
   - Paper I
   - Paper II
   - Paper III
   - Paper IV
5. Conclusion and Future Work

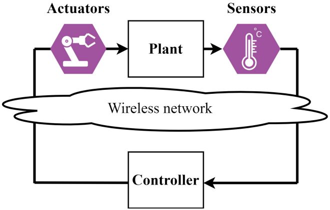
Critical Infrastructure

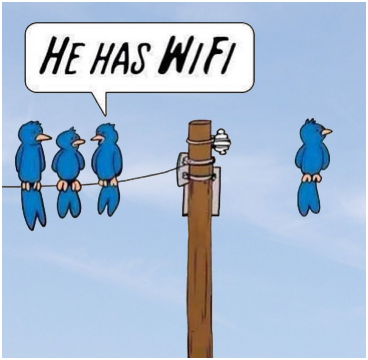
Control of Critical Infrastructure



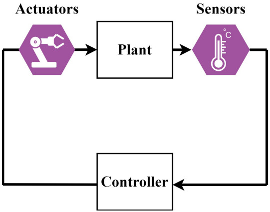
Control of Critical Infrastructure

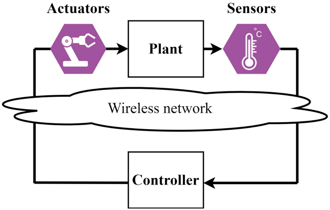


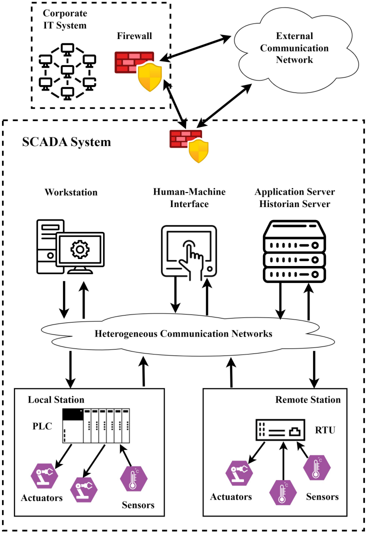




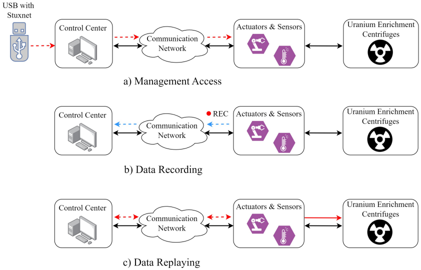
Control of Critical Infrastructure





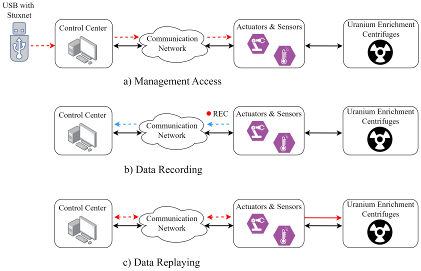


Vulnerabilities in Critical Infrastructure

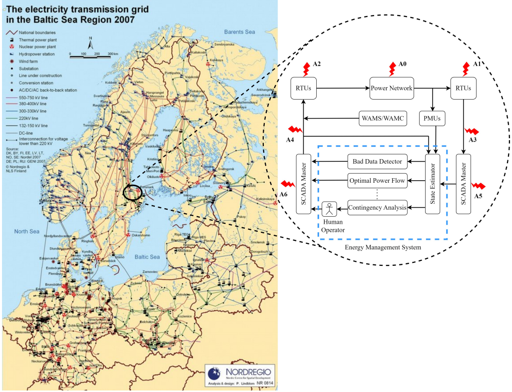


Stuxnet

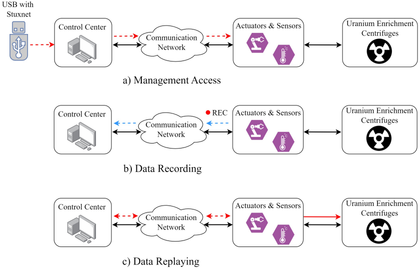
Vulnerabilities in Critical Infrastructure



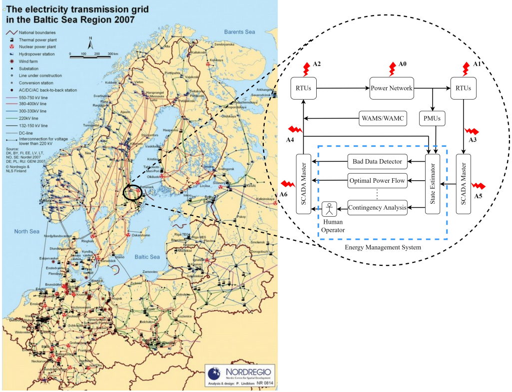
Stuxnet



Vulnerabilities in Critical Infrastructure



Stuxnet



Motivation

Critical Infrastructure should be protected actively

Outline

1 Introduction

2 Security in Networked Control Systems

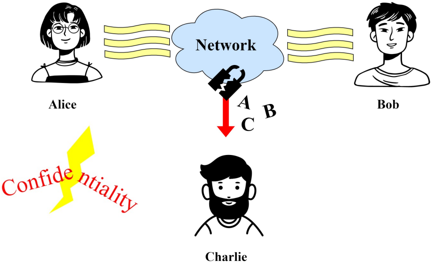
3 Problem Formulation

4 Contributions
- Paper I
- Paper II
- Paper III
- Paper IV

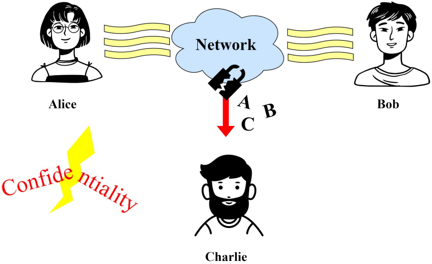
5 Conclusion and Future Work

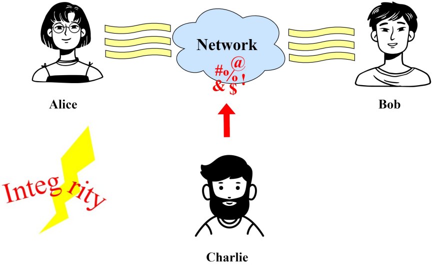
Security Triad and Threats

Security Triad and Threats

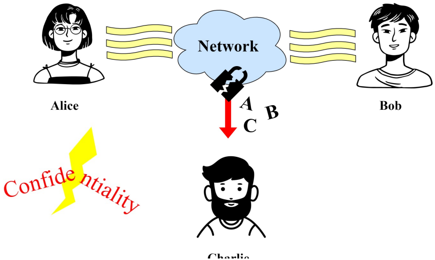


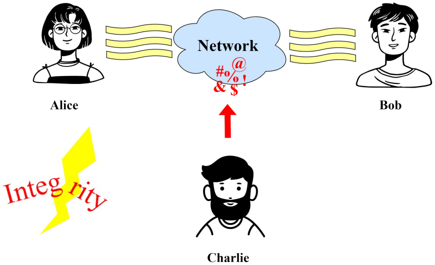
Security Triad and Threats

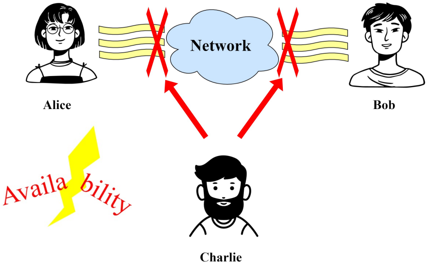




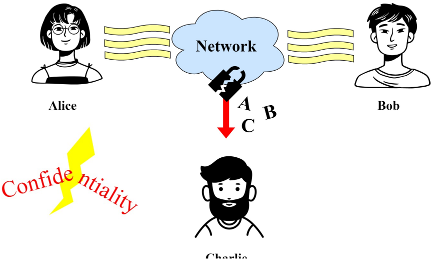
Security Triad and Threats

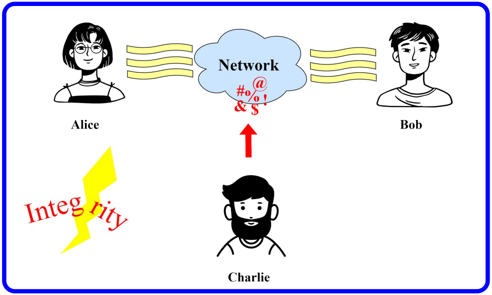


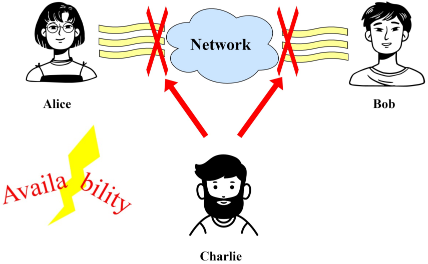




Security Triad and Threats



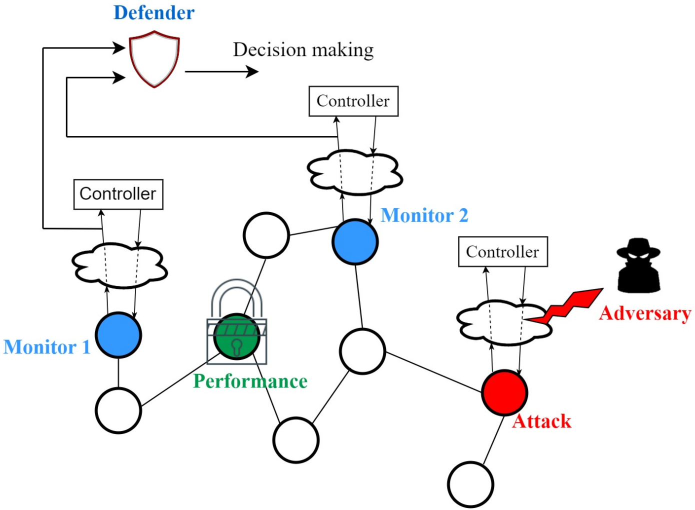




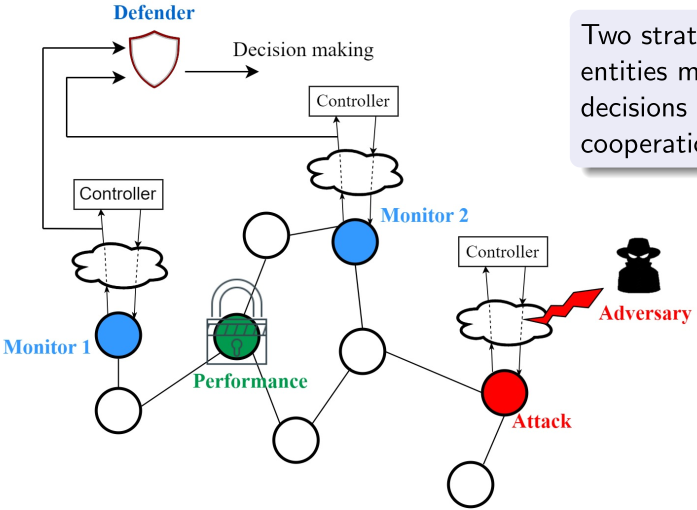
Outline

1. Introduction
2. Security in Networked Control Systems
3. Problem Formulation
4. Contributions
   - Paper I
   - Paper II
   - Paper III
   - Paper IV
5. Conclusion and Future Work

Problem description



Problem description



Two strategic entities make decisions without cooperation

Problem analysis

- Purpose: protect the system

- Purpose: attack the system

Problem analysis

- Purpose: protect the system
- Action: monitor what?

- Purpose: attack the system
- Action: attack what?

Problem analysis

- Purpose: protect the system
- Action: monitor what?

- Purpose: attack the system
- Action: attack what?

Action order:

1) Make decisions simultaneously

2) The defender goes first

Problem analysis

- Purpose: protect the system
- Action: monitor what?

- Purpose: attack the system
- Action: attack what?

Action order:

1) Make decisions simultaneously

2) The defender goes first

Non-cooperative two-player game

Problem analysis

- Purpose: protect the system
- Action: monitor what?

- Purpose: attack the system
- Action: attack what?

Action order:

1) Make decisions simultaneously

2) The defender goes first

Problem variations

▷ System models
▷ Resources & knowledge
▷ Action order

Problem variations


Defender


Adversary


Performance ρ

Paper I
- Certain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper II
- Uncertain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper III
- Certain LSO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper IV
- Certain LFO
- Performance ρ is uncertain
- Adv. chooses one, Def. chooses several
- Def. takes action firstly

Problem variations


Defender


Adversary


Performance ρ

Paper I

- Certain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper II

- Uncertain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper III

- Certain LSO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper IV

- Certain LFO
- Performance ρ is uncertain
- Adv. chooses one, Def. chooses several
- Def. takes action firstly

Problem variations

Defender

Adversary

Performance ρ

Paper I

- Certain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper II

- Uncertain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper III

- Certain LSO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper IV

- Certain LFO
- Performance ρ is uncertain
- Adv. chooses one, Def. chooses several
- Def. takes action firstly

Problem variations

Defender

Adversary

Performance ρ

Paper I

- Certain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper II

- Uncertain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper III

- Certain LSO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper IV

- Certain LFO
- Performance ρ is uncertain
- Adv. chooses one, Def. chooses several
- Def. takes action firstly

Problem formulation

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

$$\begin{aligned} \dot{x}_i(t) =& A_i x_i(t) + b\tilde{u}_i(t), \\ y_i(t) =& c^\top x_i(t). \end{aligned}$$

Problem formulation

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

$$\begin{aligned}\dot{x}_i(t) =& A_i x_i(t) + b\tilde{u}_i(t),\\ y_i(t) =& c^\top x_i(t).\end{aligned}$$

- Local performance: $\|y_\rho\|^2_{\mathcal{L}_2[0,T]} = \frac{1}{T}\int_0^T |y_\rho(t)|^2 \, \mathrm{d}t$

Problem formulation

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

$$\dot{x}_i(t) = A_i x_i(t) + b\tilde{u}_i(t),$$
$$y_i(t) = c^\top x_i(t).$$

Adversary chooses node a

- Local performance: $\|y_\rho\|^2_{\mathcal{L}_2[0,T]} = \frac{1}{T}\int_0^T |y_\rho(t)|^2 \, \mathrm{d}t$

- Healthy/attacked local controller

$$\tilde{u}_i(t) = \underbrace{\sum_{j \in \mathcal{N}_i} \phi_{ij}(x_i, x_j)}_{\text{healthy}} + \begin{cases} 0, & \text{if } i \neq a \\ \zeta(t), & \text{if } i \equiv a \end{cases}$$

$\Rightarrow$ Closed-loop system: $\dot{x}(t) = Ax(t) + b \otimes e_a \zeta(t)$

Problem formulation (Cont.)

- Closed-loop system:

$$\dot{x}(t) = Ax(t) + b \otimes e_a \zeta(t), \quad x(0) = 0$$

Problem formulation (Cont.)

- Closed-loop system:

$$\dot{x}(t) = Ax(t) + b \otimes e_a \zeta(t), \quad x(0) = 0$$

- The defender can choose several nodes $\mathcal{M} = \{m_1, m_2, \dots, m_{|\mathcal{M}|}\}$

$$y_{m_1}(t) = e_{m_1}^\top x(t), \quad y_{m_2}(t) = e_{m_2}^\top x(t), \quad \dots \quad y_{|\mathcal{M}|}(t) = e_{|\mathcal{M}|}^\top x(t).$$

- Monitor outputs such that at least

$$\|y_{m_k}\|_{\mathcal{L}_2}^2 = \frac{1}{T}\int_0^T |y_{m_k}(t)|^2 \, \mathrm{d}t > \delta_{m_k} \quad \Rightarrow \quad \text{Attack is detected!!!}$$

Problem formulation (Cont.)

- Closed-loop system:

$$\dot{x}(t) = Ax(t) + b \otimes e_a\zeta(t), \quad x(0) = 0$$

- The defender can choose several nodes $\mathcal{M} = \{m_1, m_2, \dots, m_{|\mathcal{M}|}\}$

$$y_{m_1}(t) = e_{m_1}^\top x(t), \quad y_{m_2}(t) = e_{m_2}^\top x(t), \quad \dots \quad y_{|\mathcal{M}|}(t) = e_{|\mathcal{M}|}^\top x(t).$$

- Monitor outputs such that at least

$$\|y_{m_k}\|_{\mathcal{L}_2}^2 = \frac{1}{T}\int_0^T |y_{m_k}(t)|^2 \, \mathrm{d}t > \delta_{m_k} \quad \Rightarrow \quad \text{Attack is detected!!!}$$

- Adversary's purpose: stay stealthy

$$\|y_{m_k}\|_{\mathcal{L}_2}^2 = \frac{1}{T}\int_0^T |y_{m_k}(t)|^2 \, \mathrm{d}t \leq \delta_{m_k} \quad \forall m_k \in \mathcal{M}$$

$\Rightarrow$ Stealthy False Data Injection Attacks (Stealthy FDI Attacks)

Challenges

Attack, Monitor, Performance

$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|^2_{\mathcal{L}_2} \tag{1}$$

$$\text{s.t.} \quad \|y_{m_k}\|^2_{\mathcal{L}_2} \leq \delta_{m_k},\ \forall m_k \in \mathcal{M}$$

Challenges

Attack → a, Monitor → $\mathcal{M}$, Performance → ρ

$$J_{\rho}(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_{\rho}\|^2_{\mathcal{L}_2} \qquad (1)$$

$$\text{s.t.} \quad \|y_{m_k}\|^2_{\mathcal{L}_2} \leq \delta_{m_k}, \ \forall m_k \in \mathcal{M}$$

The defender minimizes $J_{\rho}(a, \mathcal{M})$

The adversary maximizes $J_{\rho}(a, \mathcal{M})$

Challenges

Attack, Monitor, Performance

$$J_{\rho}(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_{\rho}\|_{\mathcal{L}_2}^2 \quad (1)$$

$$\text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k},\ \forall m_k \in \mathcal{M}$$

The defender minimizes $J_{\rho}(a, \mathcal{M})$

The adversary maximizes $J_{\rho}(a, \mathcal{M})$

$$\min_{\mathcal{M} \subset \mathcal{V}} \max_{a \in \mathcal{V}_{-\rho}} J_{\rho}(a, \mathcal{M})$$

Challenges

Attack → a, Monitor → $\mathcal{M}$, Performance → ρ

$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|^2_{\mathcal{L}_2} \quad (1)$$

$$\text{s.t.} \quad \|y_{m_k}\|^2_{\mathcal{L}_2} \leq \delta_{m_k},\ \forall m_k \in \mathcal{M}$$

The defender minimizes $J_\rho(a, \mathcal{M})$

The adversary maximizes $J_\rho(a, \mathcal{M})$

$$\min_{\mathcal{M} \subset \mathcal{V}} \ \max_{a \in \mathcal{V}_{-\rho}} \ J_\rho(a, \mathcal{M})$$

Combinatorial optimization problem

Challenges

Attack → a, Monitor → $\mathcal{M}$, Performance → ρ

$$J_\rho(a,\mathcal{M}) \triangleq \sup_{\zeta\in\mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|^2_{\mathcal{L}_2} \quad \text{s.t.} \quad \|y_{m_k}\|^2_{\mathcal{L}_2} \leq \delta_{m_k},\ \forall m_k \in \mathcal{M} \tag{1}$$

The defender minimizes $J_\rho(a,\mathcal{M})$

The adversary maximizes $J_\rho(a,\mathcal{M})$

$$\min_{\mathcal{M}\subset\mathcal{V}} \max_{a\in\mathcal{V}_{-\rho}} J_\rho(a,\mathcal{M})$$

Combinatorial optimization problem ⇒ Computational burden

Challenges

Attack, Monitor, Performance

$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|^2_{\mathcal{L}_2} \quad \text{s.t.} \quad \|y_{m_k}\|^2_{\mathcal{L}_2} \leq \delta_{m_k},\ \forall m_k \in \mathcal{M} \tag{1}$$

The defender minimizes $J_\rho(a, \mathcal{M})$

The adversary maximizes $J_\rho(a, \mathcal{M})$

$$\min_{\mathcal{M} \subset \mathcal{V}} \max_{a \in \mathcal{V}_{-\rho}} J_\rho(a, \mathcal{M})$$

Combinatorial optimization problem $\Rightarrow$ Computational burden

Shrink defender action space $\mathcal{M} \subset \mathbb{D} \subset \mathcal{V}$

Challenges

Attack → a, Monitor → $\mathcal{M}$, Performance → ρ

$$J_\rho(a,\mathcal{M}) \triangleq \sup_{\zeta\in\mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|^2_{\mathcal{L}_2} \tag{1}$$

$$\text{s.t.} \quad \|y_{m_k}\|^2_{\mathcal{L}_2} \le \delta_{m_k},\ \forall m_k \in \mathcal{M}$$

The defender minimizes $J_\rho(a,\mathcal{M})$

The adversary maximizes $J_\rho(a,\mathcal{M})$

$$\min_{\mathcal{M}\subset\mathcal{V}} \max_{a\in\mathcal{V}_{-\rho}} J_\rho(a,\mathcal{M})$$

Combinatorial optimization problem ⇒ Computational burden

Shrink defender action space $\mathcal{M}\subset\mathbb{D}\subset\mathcal{V}$ ⇒ Efficiently allocate defense resources

Challenges

Attack ↘ Monitor ↙

$$J_{\rho}(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_{\rho}\|_{\mathcal{L}_2}^2 \quad (1)$$

↗ Performance

$$\text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k},\ \forall m_k \in \mathcal{M}$$

The defender minimizes $J_{\rho}(a, \mathcal{M})$

The adversary maximizes $J_{\rho}(a, \mathcal{M})$

$$\min_{\mathcal{M} \subset \mathcal{V}} \max_{a \in \mathcal{V}_{-\rho}} J_{\rho}(a, \mathcal{M})$$

Combinatorial optimization problem ⇒ Computational burden

Shrink defender action space $\mathcal{M} \subset \mathbb{D} \subset \mathcal{V}$ ⇒ Efficiently allocate defense resources

⇑

$\mathbb{D}$ guarantees the boundedness of (1)

Challenges

Attack ↘ Monitor ↙

$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|^2_{\mathcal{L}_2} \tag{1}$$

↗ Performance

$$\text{s.t.} \quad \|y_{m_k}\|^2_{\mathcal{L}_2} \le \delta_{m_k}, \ \forall m_k \in \mathcal{M}$$

The defender minimizes $J_\rho(a, \mathcal{M})$

The adversary maximizes $J_\rho(a, \mathcal{M})$

$$\min_{\mathcal{M} \subset \mathcal{V}} \ \max_{a \in \mathcal{V}_{-\rho}} \ J_\rho(a, \mathcal{M})$$

Combinatorial optimization problem ⇒ Computational burden

Shrink defender action space $\mathcal{M} \subset \mathbb{D} \subset \mathcal{V}$ ⇒ Efficiently allocate defense resources

⇑

$\mathbb{D}$ guarantees the boundedness of (1) ⇐

Main contributions

Characterize $\mathbb{D}$

Preliminary results

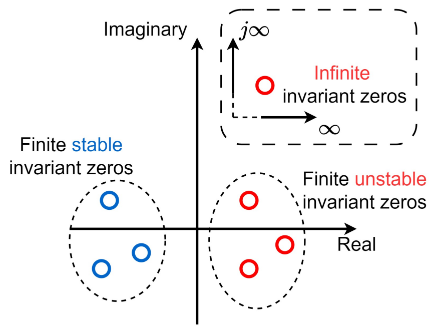
Boundedness of the worst-case impact of stealthy FDI attacks

$\Leftrightarrow$ Invariant zeros

Preliminary results

Boundedness of the worst-case impact of stealthy FDI attacks

⇔ Invariant zeros

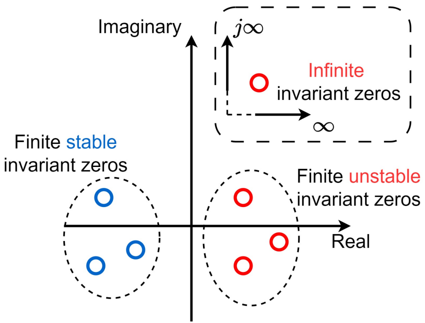


Preliminary results

Boundedness of the worst-case impact of stealthy FDI attacks

$\Leftrightarrow$ Invariant zeros

$$\dot{x}(t) = Ax(t) + b \otimes e_a \zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_{m_k}(t) = e_{m_k}^\top x(t), \ \forall m_k \in \mathcal{M}$$



- Systems $\Sigma_\rho = \big(A, b \otimes e_a, e_\rho^\top, 0\big)$ and $\Sigma_{m_k} = \big(A, b \otimes e_a, e_{m_k}^\top, 0\big)$

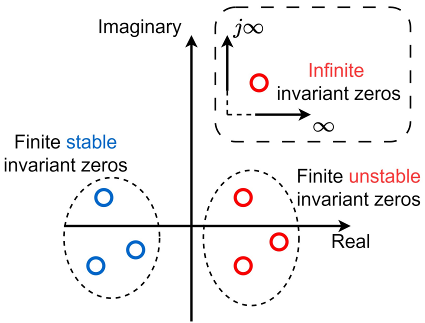
$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k}, \ \forall m_k \in \mathcal{M}$$

Preliminary results

Boundedness of the worst-case impact of stealthy FDI attacks

$\Leftrightarrow$ Invariant zeros

$$\dot{x}(t) = Ax(t) + b \otimes e_a \zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_{m_k}(t) = e_{m_k}^\top x(t), \ \forall m_k \in \mathcal{M}$$



- Systems $\Sigma_\rho = \big(A, b \otimes e_a, e_\rho^\top, 0\big)$ and $\Sigma_{m_k} = \big(A, b \otimes e_a, e_{m_k}^\top, 0\big)$

$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k}, \ \forall m_k \in \mathcal{M}$$

- At least Σ_{m_k}, its λ_{m_k} (Re$[\lambda_{m_k}] > 0$) is also invariant zero of Σ_ρ,

if, and only if, $J_\rho(a, \mathcal{M}) < \infty$

Outline

1. Introduction
2. Security in Networked Control Systems
3. Problem Formulation
4. Contributions
   - Paper I
   - Paper II
   - Paper III
   - Paper IV
5. Conclusion and Future Work

Outline

1. Introduction
2. Security in Networked Control Systems
3. Problem Formulation
4. Contributions
   - Paper I
   - Paper II
   - Paper III
   - Paper IV
5. Conclusion and Future Work

Paper I - Problem variation


Defender


Adversary


Performance ρ

Paper I
- Certain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper II
- Uncertain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper III
- Certain LSO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper IV
- Certain LFO
- Performance ρ is uncertain
- Adv. chooses one, Def. chooses several
- Def. takes action first

Challenges

- Unweighted graph $\mathcal{G}$ with N vertices, certain Laplacian matrix L

$$\dot{x}(t) = -Lx(t) + e_a\zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_m(t) = e_m^\top x(t) \quad (\mathcal{M} = \{m\}).$$

- Worst-case impact of stealthy FDI attacks

$$J_\rho(a, m) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \|y_m\|_{\mathcal{L}_2}^2 \leq \delta_m$$

Challenges

- Unweighted graph $\mathcal{G}$ with N vertices, certain Laplacian matrix L

$$\dot{x}(t) = -Lx(t) + e_a\zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_m(t) = e_m^\top x(t) \quad (\mathcal{M} = \{m\}).$$

- Worst-case impact of stealthy FDI attacks

$$J_\rho(a, m) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \|y_m\|_{\mathcal{L}_2}^2 \leq \delta_m$$

No finite unstable invariant zeros[1]

1. J. A. Torres & S. Roy, "Graph-theoretic analysis of network input-output processes: Zero structure and its implications on remote feedback control", *Automatica*, 2015

Challenges

- Unweighted graph $\mathcal{G}$ with N vertices, certain Laplacian matrix L

$$\dot{x}(t) = -Lx(t) + e_a\zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_m(t) = e_m^\top x(t) \quad (\mathcal{M} = \{m\}).$$

- Worst-case impact of stealthy FDI attacks

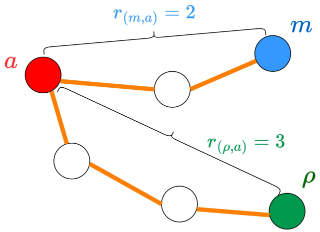
$$J_\rho(a, m) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|_{\mathcal{L}_2}^2 \quad \text{s.t.} \quad \|y_m\|_{\mathcal{L}_2}^2 \leq \delta_m$$

No finite unstable invariant zeros[1]

Challenge

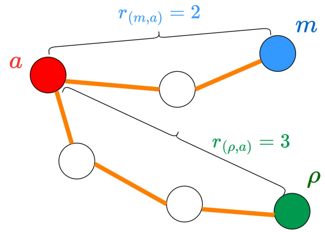
Infinite invariant zeros

1. J. A. Torres & S. Roy, "Graph-theoretic analysis of network input-output processes: Zero structure and its implications on remote feedback control", *Automatica*, 2015



Main results

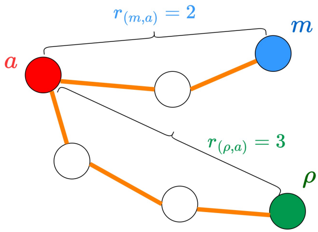
Σ_m: output at m, relative degree $r_{(m,a)}$
Σ_ρ: output at ρ, relative degree $r_{(\rho,a)}$



Main results

Σ_m: output at m, relative degree $r_{(m,a)}$
Σ_ρ: output at ρ, relative degree $r_{(\rho,a)}$

$\#$ inf. inv. zero $=$ relative degree



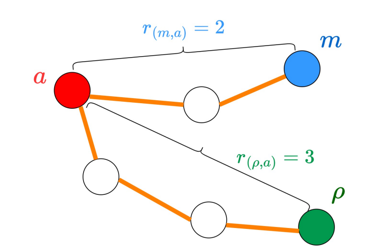
Main results

Σ_m: output at m, relative degree $r_{(m,a)}$
Σ_ρ: output at ρ, relative degree $r_{(\rho,a)}$

inf. inv. zero = relative degree

Theorem 1

$$\#\text{ inf. inv. zero of } \Sigma_m \leq \#\text{ inf. inv. zero of } \Sigma_\rho$$
$$\Leftrightarrow r_{(m,a)} \leq r_{(\rho,a)} \Leftrightarrow J_\rho(a,m) < \infty$$



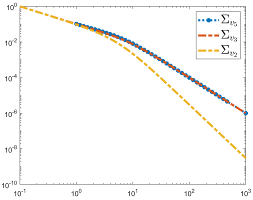
Main results

Σ_m: output at m, relative degree $r_{(m,a)}$
Σ_ρ: output at ρ, relative degree $r_{(\rho,a)}$

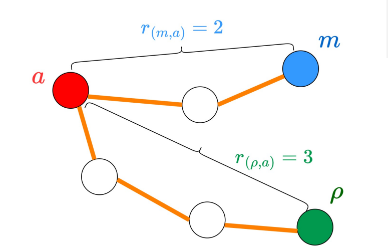
inf. inv. zero = relative degree

Theorem 1

$$\#\text{ inf. inv. zero of } \Sigma_m \leq \#\text{ inf. inv. zero of } \Sigma_\rho$$
$$\Leftrightarrow r_{(m,a)} \leq r_{(\rho,a)} \Leftrightarrow J_\rho(a, m) < \infty$$



Main results



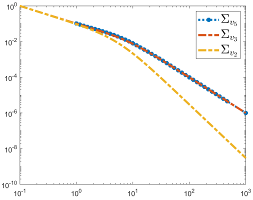
Σ_m: output at m, relative degree $r_{(m,a)}$

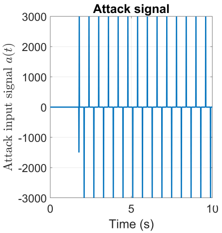
Σ_ρ: output at ρ, relative degree $r_{(\rho,a)}$

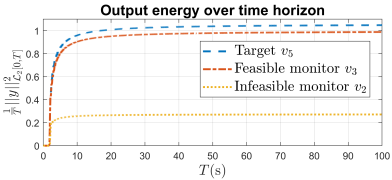
inf. inv. zero = relative degree

Theorem 1

$$\# \text{ inf. inv. zero of } \Sigma_m \leq \# \text{ inf. inv. zero of } \Sigma_\rho$$
$$\Leftrightarrow r_{(m,a)} \leq r_{(\rho,a)} \Leftrightarrow J_\rho(a,m) < \infty$$







Outline

1. Introduction
2. Security in Networked Control Systems
3. Problem Formulation
4. Contributions
   - Paper I
   - Paper II
   - Paper III
   - Paper IV
5. Conclusion and Future Work

Paper II - Problem variation

Defender

Adversary

Performance ρ

Paper I	Paper II
• Certain LFO • Performance ρ is fixed • Def./Adv. chooses one • Take actions simultaneously	• Uncertain LFO • Performance ρ is fixed • Def./Adv. chooses one • Take actions simultaneously
Paper III	**Paper IV**
• Certain LSO • Performance ρ is fixed • Def./Adv. chooses one • Take actions simultaneously	• Certain LFO • Performance ρ is uncertain • Adv. chooses one, Def. chooses several • Def. takes action first

Challenges

- Uncertain weighted graph $\mathcal{G}$ with N vertices, uncertain L^{Δ}

$$\dot{x}^{\Delta}(t) = -L^{\Delta}x^{\Delta}(t) + e_a\zeta(t),$$
$$y^{\Delta}_{\rho}(t) = e_{\rho}^{\top}x^{\Delta}(t),$$
$$y^{\Delta}_{m}(t) = e_{m}^{\top}x^{\Delta}(t) \quad (\mathcal{M} = \{m\}).$$

$L^{\Delta} = \bar{L} + \Delta$
$\Delta \in \Omega$

Challenges

- Uncertain weighted graph $\mathcal{G}$ with N vertices, uncertain L^Δ

$$\dot{x}^\Delta(t) = -L^\Delta x^\Delta(t) + e_a\zeta(t),$$
$$y_\rho^\Delta(t) = e_\rho^\top x^\Delta(t),$$
$$y_m^\Delta(t) = e_m^\top x^\Delta(t) \quad (\mathcal{M} = \{m\}).$$

$$L^\Delta = \bar{L} + \Delta$$
$$\Delta \in \Omega$$

$$J_\rho^\Delta(a,m) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \left\|y_\rho^\Delta\right\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \left\|y_m^\Delta\right\|_{\mathcal{L}_2}^2 \le \delta_m$$

Challenges

- Uncertain weighted graph $\mathcal{G}$ with N vertices, uncertain L^{Δ}

$$\dot{x}^{\Delta}(t) = -L^{\Delta}x^{\Delta}(t) + e_a\zeta(t),$$
$$y_{\rho}^{\Delta}(t) = e_{\rho}^{\top}x^{\Delta}(t),$$
$$y_{m}^{\Delta}(t) = e_{m}^{\top}x^{\Delta}(t) \quad (\mathcal{M} = \{m\}).$$

$L^{\Delta} = \bar{L} + \Delta$
$\Delta \in \Omega$

$$J_{\rho}^{\Delta}(a,m) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \left\| y_{\rho}^{\Delta} \right\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \left\| y_{m}^{\Delta} \right\|_{\mathcal{L}_2}^2 \leq \delta_m$$

Challenges

1) Finite unstable inv. zeros[1]
2) Infinite inv. zeros
3) Evaluate worst-case attack impact

1. J. A. Torres & S. Roy, "Graph-theoretic analysis of network input-output processes: Zero structure and its implications on remote feedback control", *Automatica*, 2015

Challenges

- Uncertain weighted graph $\mathcal{G}$ with N vertices, uncertain L^{Δ}

$$\dot{x}^{\Delta}(t) = -L^{\Delta}x^{\Delta}(t) + e_a\zeta(t),$$
$$y_{\rho}^{\Delta}(t) = e_{\rho}^{\top}x^{\Delta}(t),$$
$$y_{m}^{\Delta}(t) = e_{m}^{\top}x^{\Delta}(t) \quad (\mathcal{M} = \{m\}).$$

$L^{\Delta} = \bar{L} + \Delta$
$\Delta \in \Omega$

$$J_{\rho}^{\Delta}(a, m) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \left\|y_{\rho}^{\Delta}\right\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \left\|y_{m}^{\Delta}\right\|_{\mathcal{L}_2}^2 \leq \delta_m$$

Challenges

1) Finite unstable inv. zeros[1]
2) Infinite inv. zeros
3) Evaluate worst-case attack impact

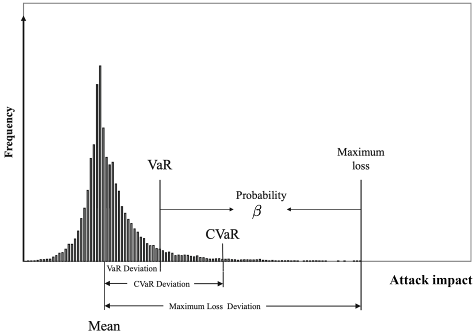
1. J. A. Torres & S. Roy, "Graph-theoretic analysis of network input-output processes: Zero structure and its implications on remote feedback control", *Automatica*, 2015

Value-at-Risk

$$\mathcal{J}_{\rho}(a, m) = \mathsf{VaR}_{\beta,\Omega}\Big[\sup_{\zeta \in \mathcal{L}_{2e}} J_{\rho}(a, m; \Delta, \zeta)\Big]$$

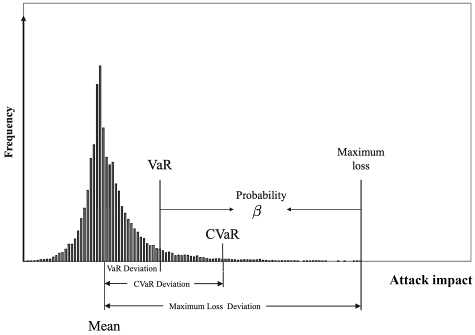
Value-at-Risk

$$\mathcal{J}_{\rho}(a, m) = \mathsf{VaR}_{\beta,\Omega}\Big[\sup_{\zeta \in \mathcal{L}_{2e}} J_{\rho}(a, m; \Delta, \zeta)\Big]$$



Value-at-Risk

$$\mathcal{J}_\rho(a, m) = \mathsf{VaR}_{\beta,\Omega}\Big[\sup_{\zeta\in\mathcal{L}_{2e}} J_\rho(a, m; \Delta, \zeta)\Big]$$



Theorem 1 & Lemma 2

M_1 values from Ω

Evaluate $\lceil M_1(1-\beta_1)\rceil$ values with ϵ accuracy

$M_1 \geq \frac{1}{2\epsilon_1^2}\log\frac{2}{\beta_1}$

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

Outline

1. Introduction
2. Security in Networked Control Systems
3. Problem Formulation
4. Contributions
   - Paper I
   - Paper II
   - Paper III
   - Paper IV
5. Conclusion and Future Work

Paper III - Problem variation


Defender


Adversary


Performance ρ

Paper I

- Certain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper II

- Uncertain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper III

- Certain LSO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper IV

- Certain LFO
- Performance ρ is uncertain
- Adv. chooses one, Def. chooses several
- Def. takes action first

Challenges

- **Main focus:** Power networks by linearized swing equations

$$m_i\ddot{p}_i(t) + h_i\dot{p}_i(t) = \sum_{j\in\mathcal{N}_i} \ell_{ij}\Big(p_i(t) - p_j(t)\Big) + \tilde{u}_i(t),$$

- Closed-loop system

$$\begin{aligned}\dot{x}(t) &= Ax(t) + e_a\zeta(t),\\ y_i(t) &= C_i x(t), \quad \forall i \in \mathcal{V},\\ y_\rho(t) &= C_\rho x(t),\end{aligned}$$

- Local performance: $\|y_\rho\|^2_{\mathcal{L}_2[0,T]} = \frac{1}{T}\int_0^T |y_\rho(t)|^2 \,\mathrm{d}t$

Challenges

- **Main focus:** Power networks by linearized swing equations

$$m_i\ddot{p}_i(t) + h_i\dot{p}_i(t) = \sum_{j\in\mathcal{N}_i} \ell_{ij}\Big(p_i(t) - p_j(t)\Big) + \tilde{u}_i(t),$$

- Closed-loop system

$$\begin{aligned}\dot{x}(t) &= Ax(t) + e_a\zeta(t),\\ y_i(t) &= C_i x(t), \quad \forall i \in \mathcal{V},\\ y_\rho(t) &= C_\rho x(t),\end{aligned}$$

- Local performance: $\|y_\rho\|^2_{\mathcal{L}_2[0,T]} = \frac{1}{T}\int_0^T |y_\rho(t)|^2 \,\mathrm{d}t$
- At node $m \in \mathcal{V}_{-\rho}$ where (A, C_m) is detectable,

Detector

$$\begin{aligned}\dot{\hat{x}}_m(t) &= A\hat{x}_m(t) + K_m\eta_m(t), \quad \hat{x}_m(0) = 0,\\ \eta_m(t) &= y_m(t) - C_m\hat{x}_d(t),\end{aligned}$$

Challenges

- **Main focus:** Power networks by linearized swing equations

$$m_i\ddot{p}_i(t) + h_i\dot{p}_i(t) = \sum_{j\in\mathcal{N}_i} \ell_{ij}\Big(p_i(t) - p_j(t)\Big) + \tilde{u}_i(t),$$

- Closed-loop system

$$\begin{aligned}\dot{x}(t) &= Ax(t) + e_a\zeta(t),\\ y_i(t) &= C_i x(t), \quad \forall i \in \mathcal{V},\\ y_\rho(t) &= C_\rho x(t),\end{aligned}$$

- Local performance: $\|y_\rho\|^2_{\mathcal{L}_2[0,T]} = \frac{1}{T}\int_0^T |y_\rho(t)|^2 \, \mathrm{d}t$
- At node $m \in \mathcal{V}_{-\rho}$ where (A, C_m) is detectable,

Detector

$$\begin{aligned}\dot{\hat{x}}_m(t) &= A\hat{x}_m(t) + K_m\eta_m(t), \quad \hat{x}_m(0) = 0,\\ \eta_m(t) &= y_m(t) - C_m\hat{x}_d(t),\end{aligned}$$

- The defender monitors $\|\eta_m\|^2_{\mathcal{L}_2[0,T]} = \frac{1}{T}\int_0^T |\eta_m(t)|^2 \, \mathrm{d}t$

Challenges

- **Main focus:** Power networks by linearized swing equations

$$m_i \ddot{p}_i(t) + h_i \dot{p}_i(t) = \sum_{j \in \mathcal{N}_i} \ell_{ij} \Big(p_i(t) - p_j(t) \Big) + \tilde{u}_i(t),$$

- Closed-loop system

$$\begin{aligned} \dot{x}(t) &= Ax(t) + e_a \zeta(t), \\ y_i(t) &= C_i x(t), \quad \forall i \in \mathcal{V}, \\ y_\rho(t) &= C_\rho x(t), \end{aligned}$$

Challenges

1) Finite unstable inv. zeros
2) Infinite inv. zeros

- Local performance: $\|y_\rho\|^2_{\mathcal{L}_2[0,T]} = \frac{1}{T} \int_0^T |y_\rho(t)|^2 \, \mathrm{d}t$
- At node $m \in \mathcal{V}_{-\rho}$ where (A, C_m) is detectable,

Detector

$$\begin{aligned} \dot{\hat{x}}_m(t) &= A\hat{x}_m(t) + K_m \eta_m(t), \quad \hat{x}_m(0) = 0, \\ \eta_m(t) &= y_m(t) - C_m \hat{x}_d(t), \end{aligned}$$

- The defender monitors $\|\eta_m\|^2_{\mathcal{L}_2[0,T]} = \frac{1}{T} \int_0^T |\eta_m(t)|^2 \, \mathrm{d}t$

Main results

- The worst-case impact of stealthy FDI attacks

$$J_\rho(a,m) \triangleq \sup_{\zeta\in\mathcal{L}_{2e},\ \text{zero init. states}} \|y_\rho\|^2_{\mathcal{L}_2} \quad \text{s.t.} \quad \|\eta_m\|^2_{\mathcal{L}_2} \le \delta$$

- Systems $\Sigma_\rho = \big(A, e_a, C_\rho, 0\big)$ and $\Sigma_m = \big(A, e_a, C_m, 0\big)$
- Denote $r_{(\rho,a)}$ and $r_{(m,a)}$ as the relative degrees of Σ_ρ and Σ_m

Main results

- The worst-case impact of stealthy FDI attacks

$$J_\rho(a,m) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. states}} \|y_\rho\|^2_{\mathcal{L}_2} \quad \text{s.t.} \quad \|\eta_m\|^2_{\mathcal{L}_2} \leq \delta$$

- Systems $\Sigma_\rho = \big(A, e_a, C_\rho, 0\big)$ and $\Sigma_m = \big(A, e_a, C_m, 0\big)$
- Denote $r_{(\rho,a)}$ and $r_{(m,a)}$ as the relative degrees of Σ_ρ and Σ_m

Lemma 3 (choice of parameters)

Finite unstable invariant zeros λ_m of Σ_m can be excluded by proper local control parameters. Then, $J_\rho(a,m) < \infty$.

Main results

- The worst-case impact of stealthy FDI attacks

$$J_\rho(a,m) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. states}} \|y_\rho\|_{\mathcal{L}_2}^2 \quad \text{s.t.} \quad \|\eta_m\|_{\mathcal{L}_2}^2 \le \delta$$

- Systems $\Sigma_\rho = \big(A, e_a, C_\rho, 0\big)$ and $\Sigma_m = \big(A, e_a, C_m, 0\big)$
- Denote $r_{(\rho,a)}$ and $r_{(m,a)}$ as the relative degrees of Σ_ρ and Σ_m

Lemma 3 (choice of parameters)

Finite unstable invariant zeros λ_m of Σ_m can be excluded by proper local control parameters. Then, $J_\rho(a,m) < \infty$.

Theorem 3.1 (relative degree condition)

$$r_{(m,a)} \le r_{(\rho,a)}$$

$$\Rightarrow \quad J_\rho(a,m) < \infty$$

Outline

1. Introduction
2. Security in Networked Control Systems
3. Problem Formulation
4. Contributions
   - Paper I
   - Paper II
   - Paper III
   - Paper IV
5. Conclusion and Future Work

Paper IV - Problem variation

Defender

Adversary

Performance ρ

Paper I

- Certain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper II

- Uncertain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper III

- Certain LSO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper IV

- Certain LFO
- Performance ρ is uncertain
- Adv. chooses one, Def. chooses several
- Def. takes action first

Challenges

- Unweighted graph $\mathcal{G}$ with N vertices, certain Laplacian matrix L

$$\dot{x}(t) = -Lx(t) + e_a\zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_{m_k}(t) = e_{m_k}^\top x(t) \ \boxed{(\mathcal{M} = \{m_1, m_2, \ldots, m_{|\mathcal{M}|}\}).}$$

- Worst-case attack impact

$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k} \quad \forall m_k \in \mathcal{M}$$

Challenges

- Unweighted graph $\mathcal{G}$ with N vertices, certain Laplacian matrix L

$$\dot{x}(t) = -Lx(t) + e_a\zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_{m_k}(t) = e_{m_k}^\top x(t) \quad \boxed{(\mathcal{M} = \{m_1, m_2, \dots, m_{|\mathcal{M}|}\}).}$$

- Worst-case attack impact

$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k} \quad \forall m_k \in \mathcal{M}$$

$$Q(a, \mathcal{M}) \triangleq \sum_{\rho \in \mathcal{V}_{-a}} \pi^a(\rho|a) J_\rho(a, \mathcal{M})$$

Challenges

- Unweighted graph $\mathcal{G}$ with N vertices, certain Laplacian matrix L

$$\dot{x}(t) = -Lx(t) + e_a\zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_{m_k}(t) = e_{m_k}^\top x(t) \quad (\mathcal{M} = \{m_1, m_2, \ldots, m_{|\mathcal{M}|}\}).$$

- Worst-case attack impact

$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|^2_{\mathcal{L}_2}$$
$$\text{s.t.} \quad \|y_{m_k}\|^2_{\mathcal{L}_2} \leq \delta_{m_k} \quad \forall m_k \in \mathcal{M}$$

$$Q(a, \mathcal{M}) \triangleq \sum_{\rho \in \mathcal{V}_{-a}} \pi^a(\rho|a) J_\rho(a, \mathcal{M})$$

$$R(a, \mathcal{M}) \triangleq \mathfrak{c}(|\mathcal{M}|) + \sum_{\rho \in \mathcal{V}_{-a}} \pi^d(\rho|a) J_\rho(a, \mathcal{M})$$

Challenges

- Unweighted graph $\mathcal{G}$ with N vertices, certain Laplacian matrix L

$$\dot{x}(t) = -Lx(t) + e_a\zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_{m_k}(t) = e_{m_k}^\top x(t) \quad (\mathcal{M} = \{m_1, m_2, \dots, m_{|\mathcal{M}|}\}).$$

- Worst-case attack impact

$$J_\rho(a, \mathcal{M}) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k} \quad \forall m_k \in \mathcal{M}$$

$$Q(a, \mathcal{M}) \triangleq \sum_{\rho \in \mathcal{V}_{-a}} \pi^a(\rho|a) J_\rho(a, \mathcal{M})$$

$$R(a, \mathcal{M}) \triangleq \mathfrak{c}(|\mathcal{M}|) + \sum_{\rho \in \mathcal{V}_{-a}} \pi^d(\rho|a) J_\rho(a, \mathcal{M})$$

Challenges

1) Finite unstable inv. zeros
2) Infinite inv. zeros

Challenges

- Unweighted graph $\mathcal{G}$ with N vertices, certain Laplacian matrix L

$$\dot{x}(t) = -Lx(t) + e_a\zeta(t),$$
$$y_\rho(t) = e_\rho^\top x(t),$$
$$y_{m_k}(t) = e_{m_k}^\top x(t) \quad \boxed{(\mathcal{M} = \{m_1, m_2, \ldots, m_{|\mathcal{M}|}\}).}$$

- Worst-case attack impact

$$J_\rho(a,\mathcal{M}) \triangleq \sup_{\zeta\in\mathcal{L}_{2e},\ \text{zero init. state}} \|y_\rho\|_{\mathcal{L}_2}^2$$
$$\text{s.t.} \quad \|y_{m_k}\|_{\mathcal{L}_2}^2 \leq \delta_{m_k} \quad \forall m_k \in \mathcal{M}$$

$$Q(a,\mathcal{M}) \triangleq \sum_{\rho\in\mathcal{V}_{-a}} \pi^a(\rho|a) J_\rho(a,\mathcal{M})$$

$$R(a,\mathcal{M}) \triangleq \mathfrak{c}(|\mathcal{M}|) + \sum_{\rho\in\mathcal{V}_{-a}} \pi^d(\rho|a) J_\rho(a,\mathcal{M})$$

Challenges

1) Finite unstable inv. zeros
2) Infinite inv. zeros

Players' strategies

Defender strategy

$$\mathcal{M}^\star = \arg\min_{\mathcal{M}\subset\mathbb{D}} \text{Defense cost}\big|_{a^\star(\mathcal{M})}$$

$$a^\star(\mathcal{M}) = \arg\max_{a\in\mathbb{A}} \text{Defense cost}$$

Players' strategies

Defender strategy

$$\mathcal{M}^\star = \arg\min_{\mathcal{M}\subset\mathbb{D}} \text{Defense cost}\big|_{a^\star(\mathcal{M})}$$

$$a^\star(\mathcal{M}) = \arg\max_{a\in\mathbb{A}} \text{Defense cost}$$

Adversary response

$$a^\star = \arg\max_{a\in\mathbb{A}} \text{Attack impact}\big|_{\mathcal{M}^\star}$$

Players' strategies

Defender strategy

$$\mathcal{M}^\star = \arg\min_{\mathcal{M}\subset\mathbb{D}} \text{Defense cost}\big|_{a^\star(\mathcal{M})}$$

$$a^\star(\mathcal{M}) = \arg\max_{a\in\mathbb{A}} \text{Defense cost}$$

Adversary response

$$a^\star = \arg\max_{a\in\mathbb{A}} \text{Attack impact}\big|_{\mathcal{M}^\star}$$

Players' strategies

Defender strategy

$$\mathcal{M}^\star = \arg\min_{\mathcal{M}\subset\mathbb{D}} \text{Defense cost}|_{a^\star(\mathcal{M})}$$

$$a^\star(\mathcal{M}) = \arg\max_{a\in\mathbb{A}} \text{Defense cost}$$

Adversary response

$$a^\star = \arg\max_{a\in\mathbb{A}} \text{Attack impact}|_{\mathcal{M}^\star}$$

Combinatorial optimization problem $\Rightarrow$ Computational burden

Players' strategies

Defender strategy

$$\mathcal{M}^\star = \arg\min_{\mathcal{M}\subset\mathbb{D}} \text{Defense cost}|_{a^\star(\mathcal{M})}$$

$$a^\star(\mathcal{M}) = \arg\max_{a\in\mathbb{A}} \text{Defense cost}$$

Adversary response

$$a^\star = \arg\max_{a\in\mathbb{A}} \text{Attack impact}|_{\mathcal{M}^\star}$$

Combinatorial optimization problem $\Rightarrow$ Computational burden

Shrink defender action space $\mathcal{M} \subset \mathbb{D} \subset \mathcal{V}$ $\Rightarrow$ Efficiently allocate defense resources

$\Uparrow$

$\mathbb{D}$ s.t. defense cost/attack impact $< \infty$

Players' strategies

Defender strategy

$$\mathcal{M}^\star = \arg\min_{\mathcal{M}\subset\mathbb{D}} \text{Defense cost}\big|_{a^\star(\mathcal{M})}$$

$$a^\star(\mathcal{M}) = \arg\max_{a\in\mathbb{A}} \text{Defense cost}$$

Adversary response

$$a^\star = \arg\max_{a\in\mathbb{A}} \text{Attack impact}\big|_{\mathcal{M}^\star}$$

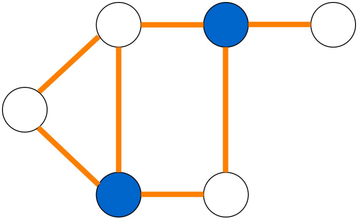
Combinatorial optimization problem $\Rightarrow$ Computational burden

Shrink defender action space $\mathcal{M} \subset \mathbb{D} \subset \mathcal{V}$ $\Rightarrow$ Efficiently allocate defense resources

$\Uparrow$

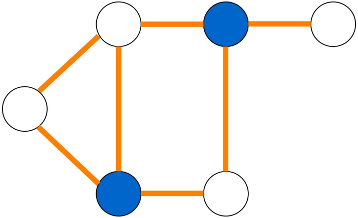
$\mathbb{D}$ s.t. defense cost/attack impact $< \infty$ $\Leftarrow$ **Characterize $\mathbb{D}$**

Main results



Dominating set

Main results



Dominating set

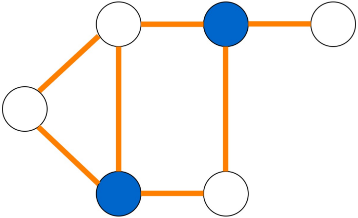
Theorem 2 (necessary and sufficient condition)

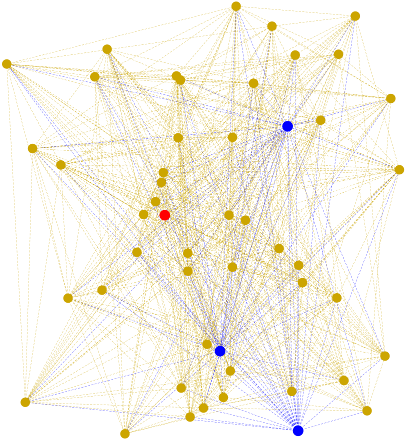
$\mathcal{M}$ is a dominating set

$\Leftrightarrow$ def. cost $R(a, \mathcal{M}) < \infty$

& attack impact $Q(a, \mathcal{M}) < \infty$

Main results





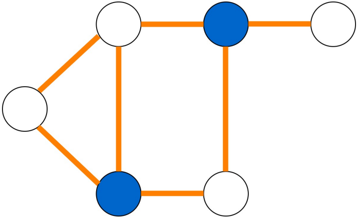
Theorem 2 (necessary and sufficient condition)

$\mathcal{M}$ is a dominating set

$\Leftrightarrow$ def. cost $R(a, \mathcal{M}) < \infty$

& attack impact $Q(a, \mathcal{M}) < \infty$

Main results



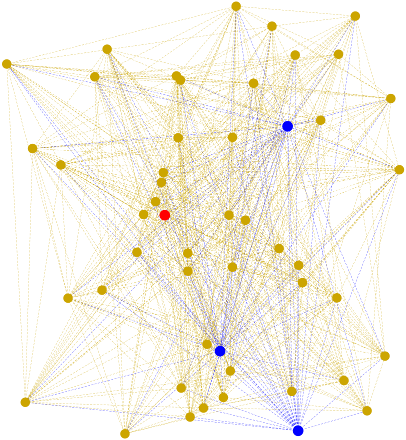
Dominating set

Theorem 2 (necessary and sufficient condition)

$\mathcal{M}$ is a dominating set

$\Leftrightarrow$ def. cost $R(a, \mathcal{M}) < \infty$

& attack impact $Q(a, \mathcal{M}) < \infty$



$$R(a, \mathcal{M}) \leq 50.2456$$
$$Q(a, \mathcal{M}) \leq 48.4235$$

Outline

1 Introduction

2 Security in Networked Control Systems

3 Problem Formulation

4 Contributions
- Paper I
- Paper II
- Paper III
- Paper IV

5 Conclusion and Future Work

Conclusion and Future Work

This Licentiate thesis has

1. considered several types of NCSs under attacks
2. intensively investigated the worst-case impact of stealthy FDI attacks
3. found system- and graph-theoretic conditions
4. assisted the defender in allocating defense resources

Conclusion and Future Work

This Licentiate thesis has

1. considered several types of NCSs under attacks
2. intensively investigated the worst-case impact of stealthy FDI attacks
3. found system- and graph-theoretic conditions
4. assisted the defender in allocating defense resources

Toward the PhD thesis, it will be extended to

1. overcome combinatorial optimization problem
2. consider uncompleted information
3. consider multiple adversaries
4. assist the defender in designing detectors
5. ......

Defender

Adversary

Performance ρ

Paper I

- Certain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper II

- Uncertain LFO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper III

- Certain LSO
- Performance ρ is fixed
- Def./Adv. chooses one
- Take actions simultaneously

Paper IV

- Certain LFO
- Performance ρ is uncertain
- Adv. chooses one, Def. chooses several
- Def. takes action first

Thanks for listening!!!