Optimal Detector Placement in Networked Control Systems under Cyber-attacks with Applications to Power Networks

Anh Tung Nguyen, Sribalaji C. Anand,
André M. H. Teixeira, and Alexander Medvedev
Uppsala University, Sweden
IFAC World Congress
Yokohama, Japan, July 2023

Swedish Research Council

Stiftelsen för Strategisk Forskning

Outline

Outline

UPPSALA UNIVERSITET

Motivation

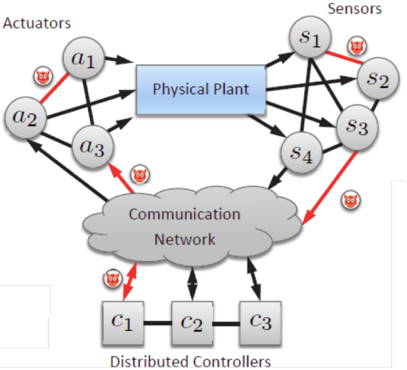
Problem Formulation

Optimal Detector Placement

A case study

Conclusion and future work

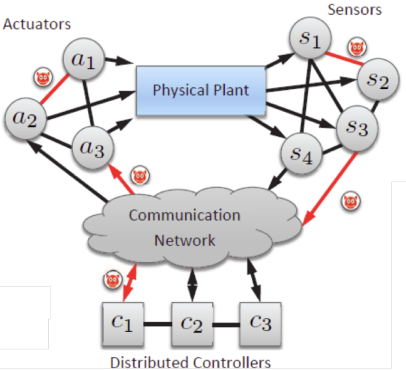
Motivation



Several cyber incidents on Cyber-physical systems in the past

July 2023

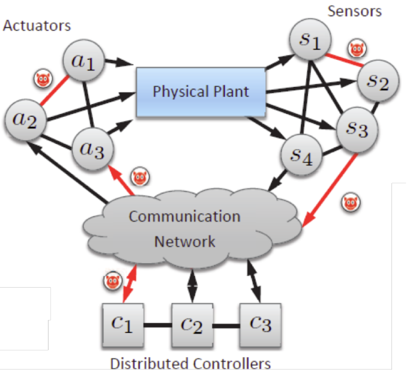
Motivation



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 . . . and 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 . . . and more.

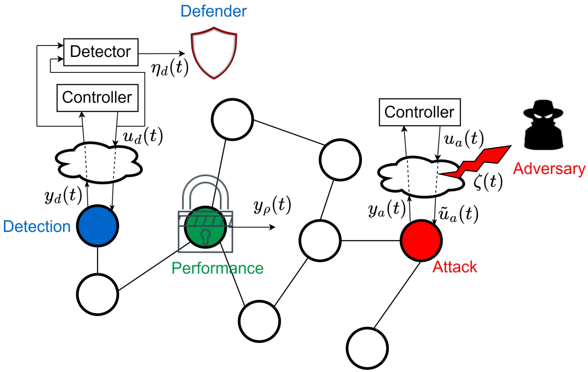
Lesson: Be proactive and protect the system.

Outline

Problem description

The main research question

Given a networked control system (multi-agent system) under stealthy attacks, which detector should be monitored to minimize the risk on a given local performance.



UPPSALA UNIVERSITET

System Description

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

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

System Description

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

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

- Control input under attacks

$$\tilde{u}_i(t) = u_i(t) + \begin{cases} 0, & i \in \mathcal{V}_{-a}, \\ \zeta(t), & i \equiv a \end{cases}$$

- Healthy $u_i(t)$ is designed s.t. $p_i(t),\ \dot{p}_i(t) \to 0$ (*Lemma 1*)

UPPSALA UNIVERSITET

System Description

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

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

- Control input under attacks

$$\tilde{u}_i(t) = u_i(t) + \begin{cases} 0, & i \in \mathcal{V}_{-a}, \\ \zeta(t), & i \equiv a \end{cases}$$

- Healthy $u_i(t)$ is designed s.t. $p_i(t),\ \dot{p}_i(t) \to 0$ (*Lemma 1*)

Assumption: The entire network is at its equilibrium $(p_e = 0,\ \dot{p}_e = 0)$ before being attacked.

UPPSALA UNIVERSITET

System Description (Cont.)

- Network under cyber-attacks

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

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

System Description (Cont.)

- Network under cyber-attacks

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

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

Assumption: Performance agent ρ is protected

System Description (Cont.)

- Network under cyber-attacks

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

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

Assumption: Performance agent ρ is protected

- At agent $d \in \mathcal{V}_{-\rho}$ where (A, C_d) is detectable,

$$\dot{\hat{x}}_d(t) = A\hat{x}_d(t) + K_d \eta_d(t), \quad \hat{x}_d(0) = 0,$$
$$\eta_d(t) = y_d(t) - C_d \hat{x}_d(t),$$

System Description (Cont.)

- Network under cyber-attacks

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

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

Assumption: Performance agent ρ is protected

- At agent $d \in \mathcal{V}_{-\rho}$ where (A, C_d) is detectable,

$$\dot{\hat{x}}_d(t) = A\hat{x}_d(t) + K_d\eta_d(t), \quad \hat{x}_d(0) = 0,$$
$$\eta_d(t) = y_d(t) - C_d\hat{x}_d(t),$$

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

Resources and Strategies

- Attacks detected if $\|\eta_d\|^2_{\mathcal{L}_2[0,T]} > \delta^2$

Resources and Strategies

- Attacks detected if $\|\eta_d\|^2_{\mathcal{L}_2[0,T]} > \delta^2$

- **System knowledge**:

Location of performance ρ, the appearance of competitors, system parameters, and the detection mechanism

- **Defense strategy**: Select agent d and monitor $\|\eta_d\|^2_{\mathcal{L}_2[0,T]}$ such that minimizing the disruption $\|y_\rho\|^2_{\mathcal{L}_2[0,T]}$

Resources and Strategies

- Attacks detected if $\|\eta_d\|^2_{\mathcal{L}_2[0,T]} > \delta^2$
- **System knowledge**:
Location of performance ρ, the appearance of competitors, system parameters, and the detection mechanism
- **Defense strategy**: Select agent d and monitor $\|\eta_d\|^2_{\mathcal{L}_2[0,T]}$ such that minimizing the disruption $\|y_\rho\|^2_{\mathcal{L}_2[0,T]}$
- **Attack policy**: Select agent a and design stealthy attack $\zeta(t)$ such that
  1) be stealthy $\|\eta_d\|^2_{\mathcal{L}_2[0,T]} \leq \delta^2$; and
  2) maximize the disruption $\|y_\rho\|^2_{\mathcal{L}_2[0,T]}$

UPPSALA UNIVERSITET

Worst-case impact of stealthy attacks

- Given a protected performance ρ, the defender selects agent d and the adversary selects agent a

$$\gamma_\rho^\star(a,d) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. states}} \quad \|y_\rho\|^2_{\mathcal{L}_2[0,T]} \qquad \text{s.t.} \quad \|\eta_d\|^2_{\mathcal{L}_2[0,T]} \le \delta^2 \tag{1}$$

Worst-case impact of stealthy attacks

- Given a protected performance ρ, the defender selects agent d and the adversary selects agent a

$$\gamma_\rho^\star(a,d) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. states}} \|y_\rho\|^2_{\mathcal{L}_2[0,T]} \quad \text{s.t.} \quad \|\eta_d\|^2_{\mathcal{L}_2[0,T]} \leq \delta^2 \tag{1}$$

- If (1) is feasible, obtain finite $\gamma_\rho^\star(a,d)$ by solving

$$\gamma_\rho^\star(a,d) \triangleq \min_{\gamma_\rho \in \mathbb{R}_+, F=F^\top \geq 0} \gamma_\rho \quad \text{s.t.} \quad R\big(\Sigma_{\text{closed-loop}}, F, \gamma_\rho\big) \leq 0,$$

Note: $R\big(\Sigma_{\text{closed-loop}}, F, \gamma_\rho\big)$ is an LMI.

Worst-case impact of stealthy attacks

- Given a protected performance ρ, the defender selects agent d and the adversary selects agent a

$$\gamma_\rho^\star(a,d) \triangleq \sup_{\zeta \in \mathcal{L}_{2e},\ \text{zero init. states}} \|y_\rho\|^2_{\mathcal{L}_2[0,T]} \quad \text{s.t.} \quad \|\eta_d\|^2_{\mathcal{L}_2[0,T]} \leq \delta^2 \tag{1}$$

- If (1) is feasible, obtain finite $\gamma_\rho^\star(a,d)$ by solving

$$\gamma_\rho^\star(a,d) \triangleq \min_{\gamma_\rho \in \mathbb{R}_+, F=F^\top \geq 0} \gamma_\rho \quad \text{s.t.} \quad R\big(\Sigma_{\text{closed-loop}}, F, \gamma_\rho\big) \leq 0,$$

Note: $R\big(\Sigma_{\text{closed-loop}}, F, \gamma_\rho\big)$ is an LMI.

- If (1) is infeasible, $\gamma_\rho^\star(a,d) \to \infty$

Worst-case impact of stealthy attacks

- Given a protected performance ρ, the defender selects agent d and the adversary selects agent a

$$\gamma_\rho^\star(a,d) \triangleq \sup_{\zeta\in\mathcal{L}_{2e},\ \text{zero init. states}} \|y_\rho\|^2_{\mathcal{L}_2[0,T]} \quad \text{s.t.} \quad \|\eta_d\|^2_{\mathcal{L}_2[0,T]} \le \delta^2 \tag{1}$$

- If (1) is feasible, obtain finite $\gamma_\rho^\star(a,d)$ by solving

$$\gamma_\rho^\star(a,d) \triangleq \min_{\gamma_\rho\in\mathbb{R}_+, F=F^\top\ge 0} \gamma_\rho \quad \text{s.t.} \quad R\big(\Sigma_{\text{closed-loop}}, F, \gamma_\rho\big) \le 0,$$

Note: $R\big(\Sigma_{\text{closed-loop}}, F, \gamma_\rho\big)$ is an LMI.

- If (1) is infeasible, $\gamma_\rho^\star(a,d) \to \infty$

Problem: The defender selects d such that $\gamma_\rho^\star(a,d) < \infty$

Outline

Worst-case impact analysis

- Invariant zeros of system $\bar{\Sigma} \triangleq (\bar{A}, \bar{B}, \bar{C}, 0)$

$$\begin{bmatrix} \lambda I - \bar{A} & -\bar{B} \\ \bar{C} & 0 \end{bmatrix} \begin{bmatrix} \bar{x} \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \bar{x} \neq 0. \qquad (2)$$

$\lambda < \infty$: finite invariant zero
$\lambda = 1/s,\ s = 0$: infinite invariant zero
Input of $\bar{\Sigma}:\ ge^{\lambda t}$, output of $\bar{\Sigma} \to 0$

UPPSALA UNIVERSITET

Worst-case impact analysis

- Invariant zeros of system $\bar{\Sigma} \triangleq (\bar{A}, \bar{B}, \bar{C}, 0)$

$$\begin{bmatrix} \lambda I - \bar{A} & -\bar{B} \\ \bar{C} & 0 \end{bmatrix} \begin{bmatrix} \bar{x} \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad \bar{x} \neq 0. \qquad (2)$$

$\lambda < \infty$: finite invariant zero
$\lambda = 1/s,\ s = 0$: infinite invariant zero
Input of $\bar{\Sigma}$: $ge^{\lambda t}$, output of $\bar{\Sigma} \to 0$

- Systems $\Sigma_\rho = \left(A_d, \bar{E}_a, \bar{C}_\rho, 0\right)$ and $\Sigma_d = \left(A_d, \bar{E}_a, \bar{C}_d, 0\right)$

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

- λ_d of Σ_d (Re$[\lambda_d] > 0$) is also invariant zero of Σ_ρ if, and only if, $\gamma_\rho^\star(a,d) < \infty$

UPPSALA UNIVERSITET

Worst-case impact analysis

- Systems $\Sigma_\rho = \left(A_d, \bar{E}_a, \bar{C}_\rho, 0\right)$ and $\Sigma_d = \left(A_d, \bar{E}_a, \bar{C}_d, 0\right)$
- Denote $r_{(\rho,a)}$ and $r_{(d,a)}$ as the relative degrees of Σ_ρ and Σ_d
- Worst-case impact of stealthy attacks $\gamma_\rho^\star(a,d)$

UPPSALA UNIVERSITET

Worst-case impact analysis

- Systems $\Sigma_\rho = \left(A_d, \bar{E}_a, \bar{C}_\rho, 0\right)$ and $\Sigma_d = \left(A_d, \bar{E}_a, \bar{C}_d, 0\right)$
- Denote $r_{(\rho,a)}$ and $r_{(d,a)}$ as the relative degrees of Σ_ρ and Σ_d
- Worst-case impact of stealthy attacks $\gamma_\rho^\star(a, d)$

Main contributions

Worst-case impact analysis

- Systems $\Sigma_\rho = \big(A_d, \bar{E}_a, \bar{C}_\rho, 0\big)$ and $\Sigma_d = \big(A_d, \bar{E}_a, \bar{C}_d, 0\big)$
- Denote $r_{(\rho,a)}$ and $r_{(d,a)}$ as the relative degrees of Σ_ρ and Σ_d
- Worst-case impact of stealthy attacks $\gamma_\rho^\star(a,d)$

Main contributions

- **Finite invariant zeros λ_d of Σ_d** $<\infty$ (Re$[\lambda_d] > 0$)

Lemma 3 (choice of parameters)

Finite unstable invariant zeros λ_d of Σ_d can be excluded by proper local control parameters. Then, $\gamma_\rho^\star(a,d) < \infty$.

Worst-case impact analysis

- Systems $\Sigma_\rho = \big(A_d, \bar{E}_a, \bar{C}_\rho, 0\big)$ and $\Sigma_d = \big(A_d, \bar{E}_a, \bar{C}_d, 0\big)$
- Denote $r_{(\rho,a)}$ and $r_{(d,a)}$ as the relative degrees of Σ_ρ and Σ_d
- Worst-case impact of stealthy attacks $\gamma_\rho^\star(a,d)$

Main contributions

- **Finite invariant zeros λ_d of Σ_d** $< \infty$ $(\mathrm{Re}[\lambda_d] > 0)$

Lemma 3 (choice of parameters)

Finite unstable invariant zeros λ_d of Σ_d can be excluded by proper local control parameters. Then, $\gamma_\rho^\star(a,d) < \infty$.

- **Infinite invariant zeros λ_d** $= 1/s$ **where** $s = 0$

Theorem 3.1 (relative degree condition)

If $r_{(d,a)} \leq r_{(\rho,a)}$, then, λ_d is also infinite invariant zero of Σ_ρ, leading to $\gamma_\rho^\star(a,d) < \infty$.

Optimal detector placement

- Admissible detection agents for the defender fulfill

i) *the choice of parameters* and
ii) *the relative degree condition*.

Optimal detector placement

- Admissible detection agents for the defender fulfill

i) *the choice of parameters* and
ii) *the relative degree condition*.

- **Assumption:** Admissible detection set $\mathcal{D}$ is not empty.

Optimal detector placement

- Admissible detection agents for the defender fulfill

i) *the choice of parameters* and

ii) *the relative degree condition*.

- **Assumption:** Admissible detection set $\mathcal{D}$ is not empty.

- The defender and the adversary solve the zero-sum game

$$\max_{a \in \mathcal{V}_{-\rho}} \quad \min_{d \in \mathcal{D}} \quad \gamma_{\rho}^{\star}(a, d) < \infty. \text{ (pure Nash equilibrium)}$$

Optimal detector placement

- Admissible detection agents for the defender fulfill

i) *the choice of parameters* and

ii) *the relative degree condition*.

- **Assumption:** Admissible detection set $\mathcal{D}$ is not empty.

- The defender and the adversary solve the zero-sum game

$$\max_{a\in\mathcal{V}_{-\rho}} \min_{d\in\mathcal{D}} \gamma_\rho^\star(a,d) < \infty. \text{ (pure Nash equilibrium)}$$

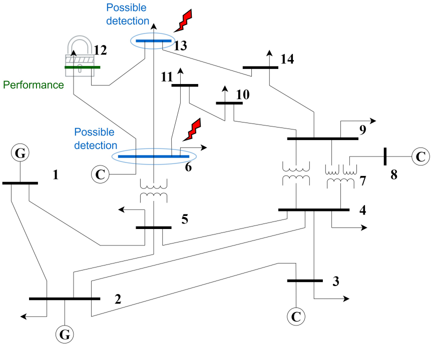
$$\max_{\mathfrak{q}(a)} \min_{\mathfrak{p}(d)} \sum_{a\in\mathcal{V}_{-\rho}} \sum_{d\in\mathcal{D}} \mathfrak{p}(d)\gamma_\rho^\star(a,d)\mathfrak{q}(a)$$

$$\text{s.t.} \sum_{a\in\mathcal{V}_{-\rho}} \mathfrak{q}(a) = 1, \quad \sum_{d\in\mathcal{D}} \mathfrak{p}(d) = 1, \text{ (mixed-strategy equilibrium)}$$

Outline

UPPSALA UNIVERSITET

Simulation results

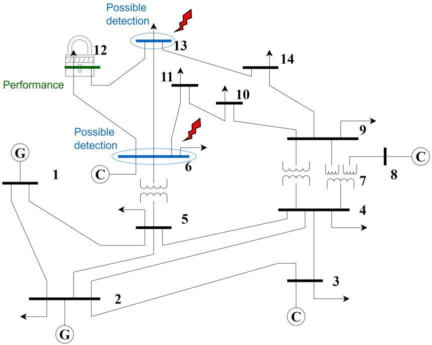


- Defender: maximal cost $[4.7449,\ 4.3917] \rightarrow \min = 4.3917$

UPPSALA UNIVERSITET

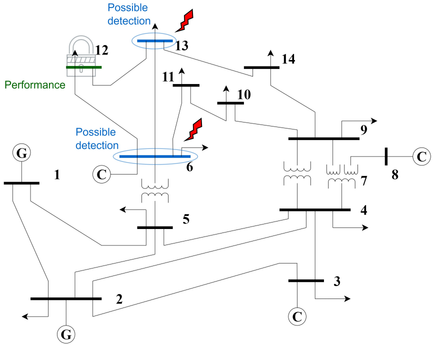
- Motivation
- Problem Formulation
- Optimal Detector Placement
- **A case study**
- Conclusion and future work

Simulation results



- Defender: maximal cost $[4.7449,\ 4.3917] \rightarrow \min = 4.3917$
- Adversary: minimal cost $[2.4494,\ 2.5561,\ 2.6185,\ 2.5585,\ 2.4198,\ 2.3087,\ 2.5199,\ 2.5257,\ 2.4695,\ 2.4673,\ 2.3705,\ 2.0717,\ 2.2119] \rightarrow \max = 2.6185$

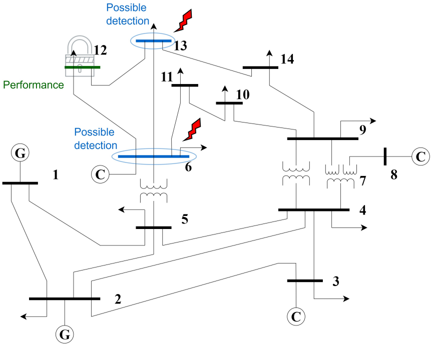
Simulation results



- Defender: maximal cost $[4.7449,\ 4.3917] \rightarrow \min = 4.3917$
- Adversary: minimal cost $[2.4494,\ 2.5561,\ 2.6185,\ 2.5585,\ 2.4198,\ 2.3087,\ 2.5199,\ 2.5257,\ 2.4695,\ 2.4673,\ 2.3705,\ 2.0717,\ 2.2119] \rightarrow \max = 2.6185$
- No accord⇒No pure NE

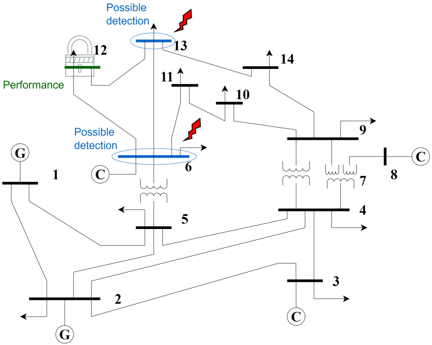
UPPSALA UNIVERSITET

Simulation results



- Defender: maximal cost $[4.7449, \ 4.3917] \rightarrow \min = 4.3917$
- Adversary: minimal cost $[2.4494, \ 2.5561, \ 2.6185, \ 2.5585, \ 2.4198, \ 2.3087, \ 2.5199, \ 2.5257, \ 2.4695, \ 2.4673, \ 2.3705, \ 2.0717, \ 2.2119] \rightarrow \max = 2.6185$
- No accord⇒No pure NE
- Mixed-strategy needed

Simulation results

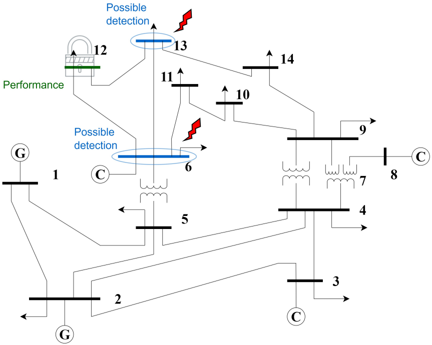


- Defender: maximal cost $[4.7449,\ 4.3917] \rightarrow \min = 4.3917$
- Adversary: minimal cost $[2.4494,\ 2.5561,\ 2.6185,\ 2.5585,\ 2.4198,\ 2.3087,\ 2.5199,\ 2.5257,\ 2.4695,\ 2.4673,\ 2.3705,\ 2.0717,\ 2.2119] \rightarrow \max = 2.6185$
- No accord$\Rightarrow$No pure NE
- Mixed-strategy needed

$\mathfrak{p}_6^\star = 0.562$, $\mathfrak{p}_{13}^\star = 0.438$, $\mathfrak{q}_{i\in\mathcal{V}\backslash\{6,\ 12,\ 13\}}^\star = 0$, $\mathfrak{q}_6^\star = 0.4878$, and $\mathfrak{q}_{13}^\star = 0.5122$

UPPSALA UNIVERSITET

Simulation results



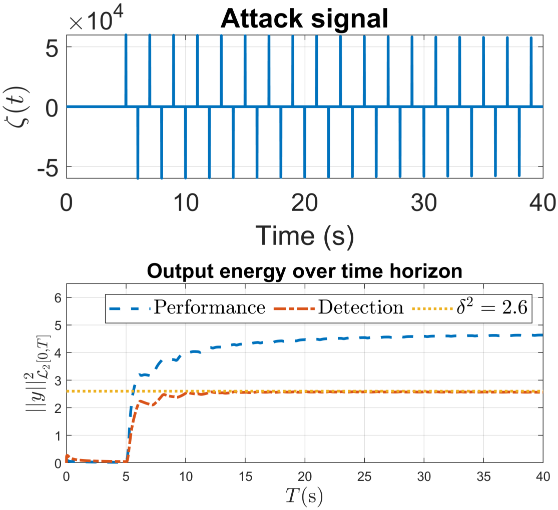
- Defender: maximal cost $[4.7449,\ 4.3917] \rightarrow \min = 4.3917$
- Adversary: minimal cost $[2.4494,\ 2.5561,\ 2.6185,\ 2.5585,\ 2.4198,\ 2.3087,\ 2.5199,\ 2.5257,\ 2.4695,\ 2.4673,\ 2.3705,\ 2.0717,\ 2.2119] \rightarrow \max = 2.6185$
- No accord⇒No pure NE
- Mixed-strategy needed

$\mathfrak{p}_6^\star = 0.562$, $\mathfrak{p}_{13}^\star = 0.438$, $\mathfrak{q}_{i\in\mathcal{V}\setminus\{6,\ 12,\ 13\}}^\star = 0$, $\mathfrak{q}_6^\star = 0.4878$, and $\mathfrak{q}_{13}^\star = 0.5122$

- How can the adversary launch stealthy attacks on the network?

(Next slide) →

Numerical results (Cont.)



Outline

Conclusion and future work

Conclusion

- We study the problem of optimal detector placement in a networked control system under stealthy attacks
- The worst-case impact of stealthy attacks is intensively investigated
- Control design and sufficient (relative degree) condition are proposed
- Admissible strategies for the defender are characterized
- Optimal detector placement is solved by game-theoretic approach
- Applications to Power Network is illustrated

Conclusion and future work

Conclusion

- We study the problem of optimal detector placement in a networked control system under stealthy attacks
- The worst-case impact of stealthy attacks is intensively investigated
- Control design and sufficient (relative degree) condition are proposed
- Admissible strategies for the defender are characterized
- Optimal detector placement is solved by game-theoretic approach
- Applications to Power Network is illustrated

Future work

- Keep the performance agent secret
- Re-design detector parameters to minimize the risk
- . . .

Thanks for your listening!!!
Questions?