Quantifying Security in Cyber-Physical Systems

Henrik Sandberg

Department of Automatic Control
ACCESS Linnaeus Centre, KTH Royal Institute of Technology
Stockholm, Sweden

Big Data Analytics for Societal Scale
Cyber-Physical Systems: Energy System
December 14, 2014

Acknowledgments

- André Teixeira (KTH)
- György Dán (KTH)
- Karl Henrik Johansson (KTH)

- Kin Cheong Sou (Chalmers)
- Iman Shames (Univ. Melbourne)

- Julien M. Hendrickx (UC Louvain)
- Raphael M. Jungers (UC Louvain)

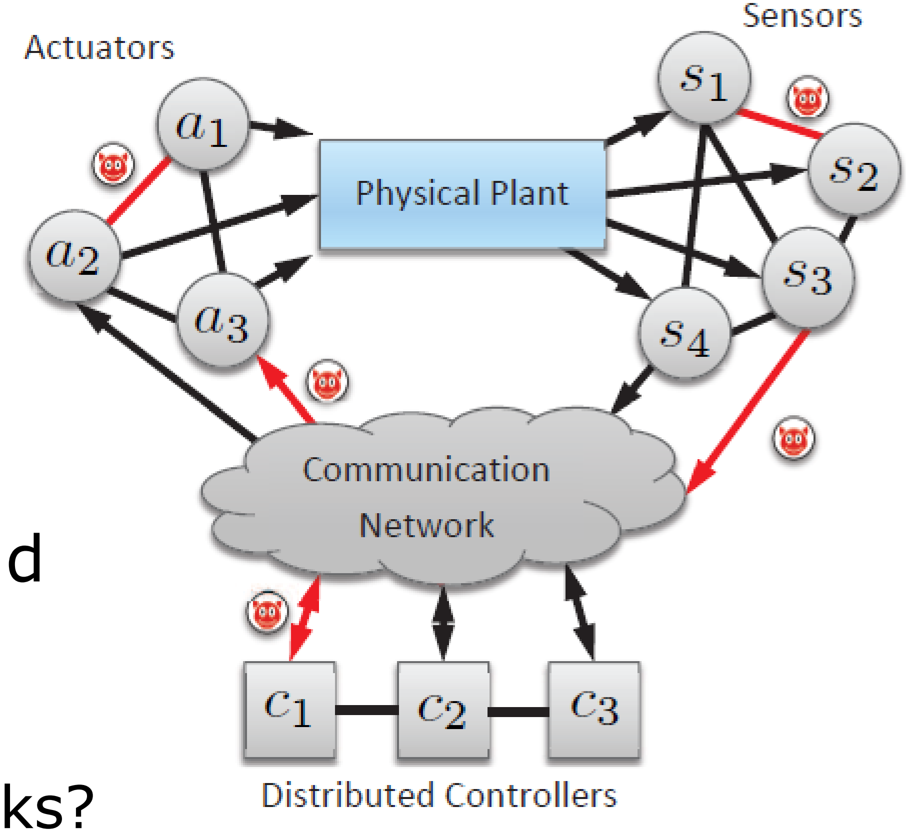
Outline

- Background and motivation
- Quantifying security using sparse optimization
- Quantifying security using game theory
- Summary

Cyber-Secure Control of CPS

Networked control systems

- are being **integrated with business/corporate networks**
- have many potential points of **cyber-physical attack**



Need tools and strategies to understand and mitigate attacks:

- Which threats should we care about?
- What impact can we expect from attacks?
- Which resources should we protect (more)?

- **Need for quantification!**

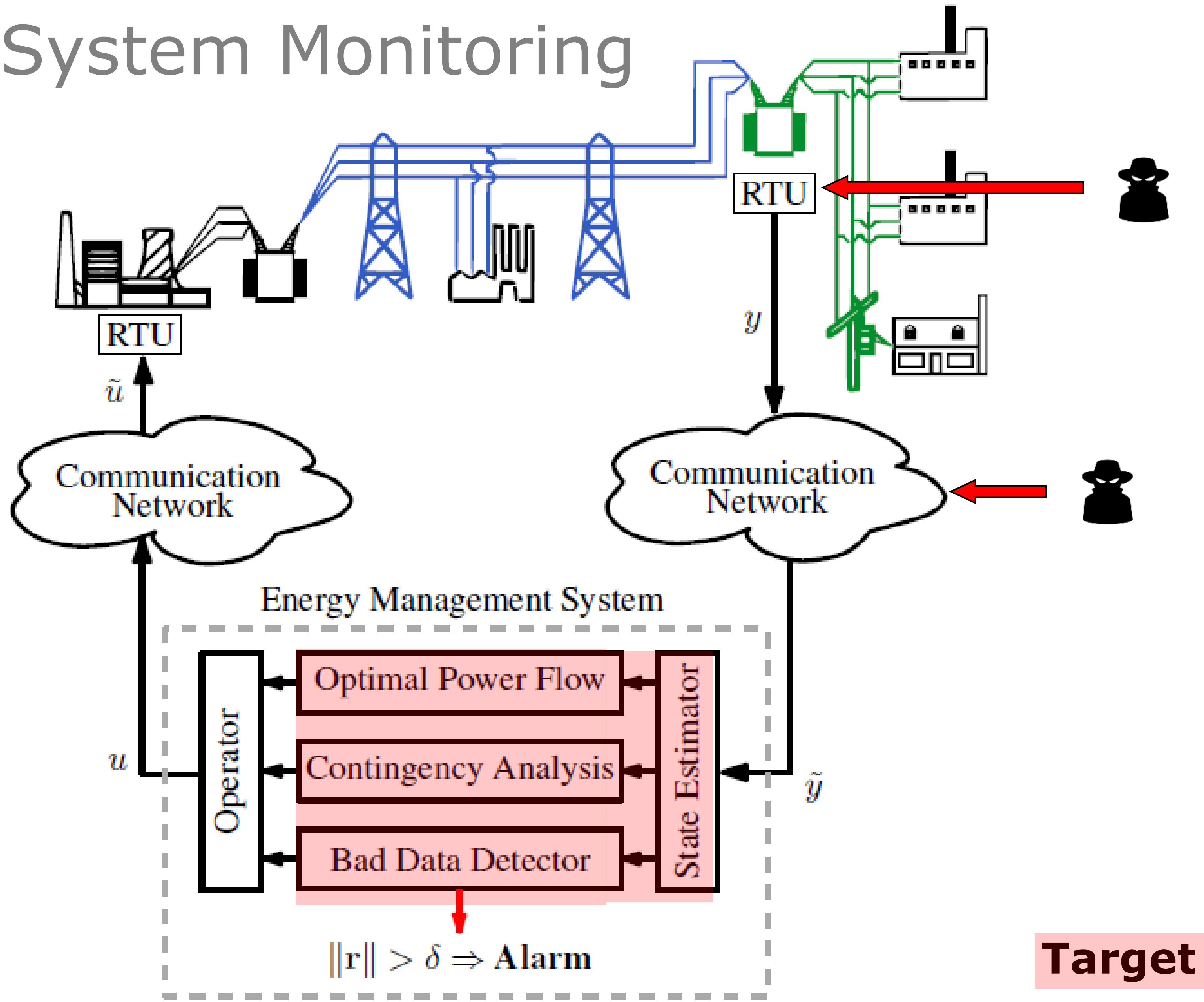
Outline

- Background and motivation
- Quantifying security using sparse optimization
- Quantifying security using game theory
- Summary

Power System Monitoring

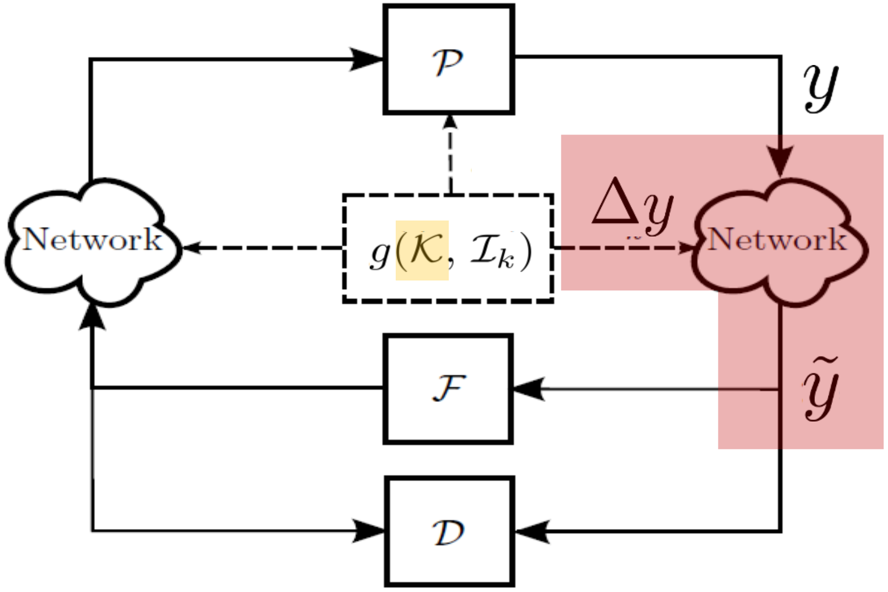
Practically motivated problem…

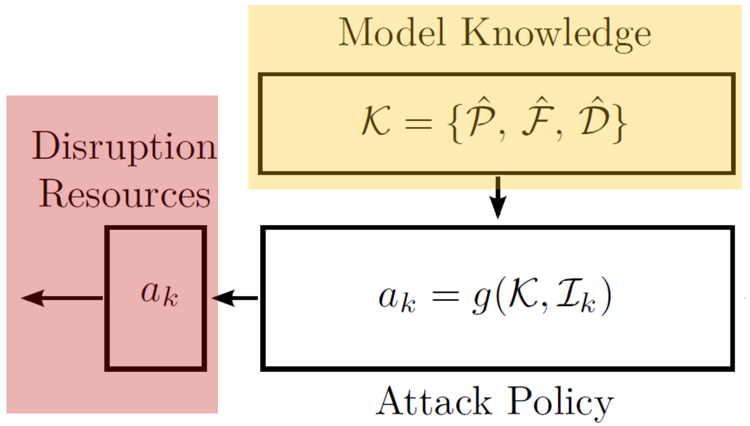
How much security does the Bad Data Detector provide?



[Giani *et al.*, IEEE ISRCS, 2009]
[Mohajerin Esfahani *et al.*, CDC, 2010]

Adversary Model





- **Attack policy:** Induce bias in power measurements without alarms
- **Model knowledge:** Steady-state model of power system
- **Disruption resources:** Small number of measurement channels

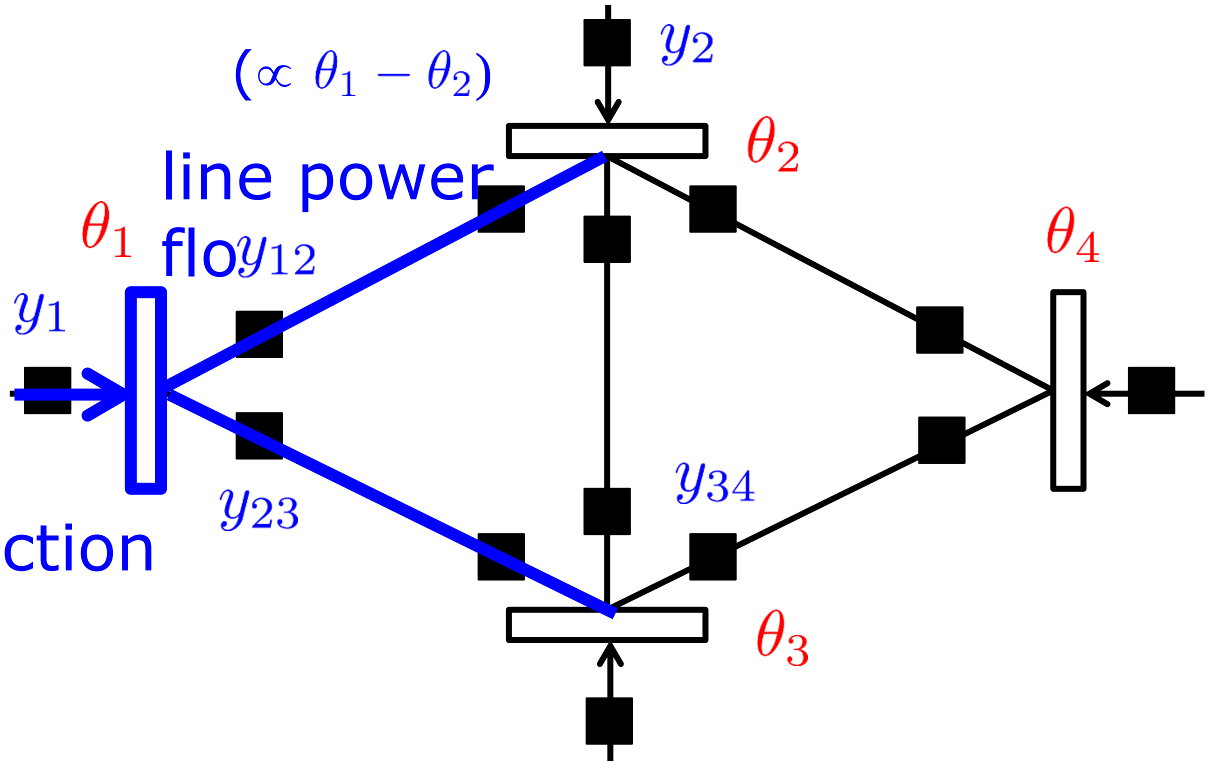
Can we quantify how hard such attacks would be?

Steady-State Power System Model

States (θ)
= bus voltage phase angles

(flow conservation)
bus injection

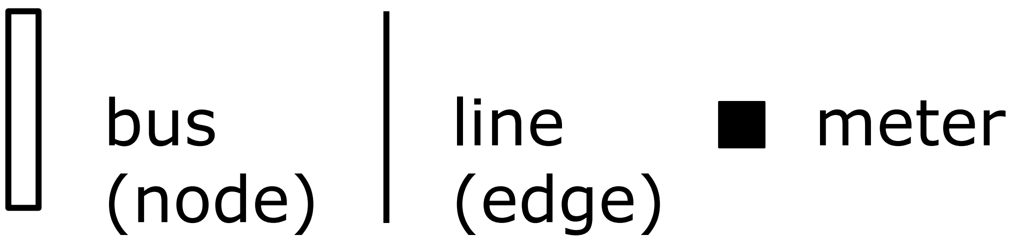
Measurements (y)
= line power flow & bus injection



"DC power flow model":

$$y = H\theta$$

measurement matrix



ROYAL INSTITUTE OF TECHNOLOGY

Structure of Measurement Matrix *H*

$$H = \begin{bmatrix} DA^T \\ -DA^T \\ ADA^T \end{bmatrix} \begin{matrix} \text{(flow measurements)} \\ \text{(flow measurements)} \\ \text{(injection measurements)} \end{matrix}$$

- A - directed incidence matrix of graph corresponding to power network topology
- D - nonsingular diagonal matrix containing reciprocals of reactance of transmission lines

- More measurements than states. Redundancy!

State Estimation by Least Squares

State estimator (LS)

$$y = H\theta$$

$$\Rightarrow \hat{\theta} = (H^T H)^{-1} H^T y$$

wrong

wrong

Contingency analysis

wrong

OPF calculations

⋮

What if the measurements were **wrong**?

$$\tilde{y} = y + \Delta y$$

→ random measurement noise

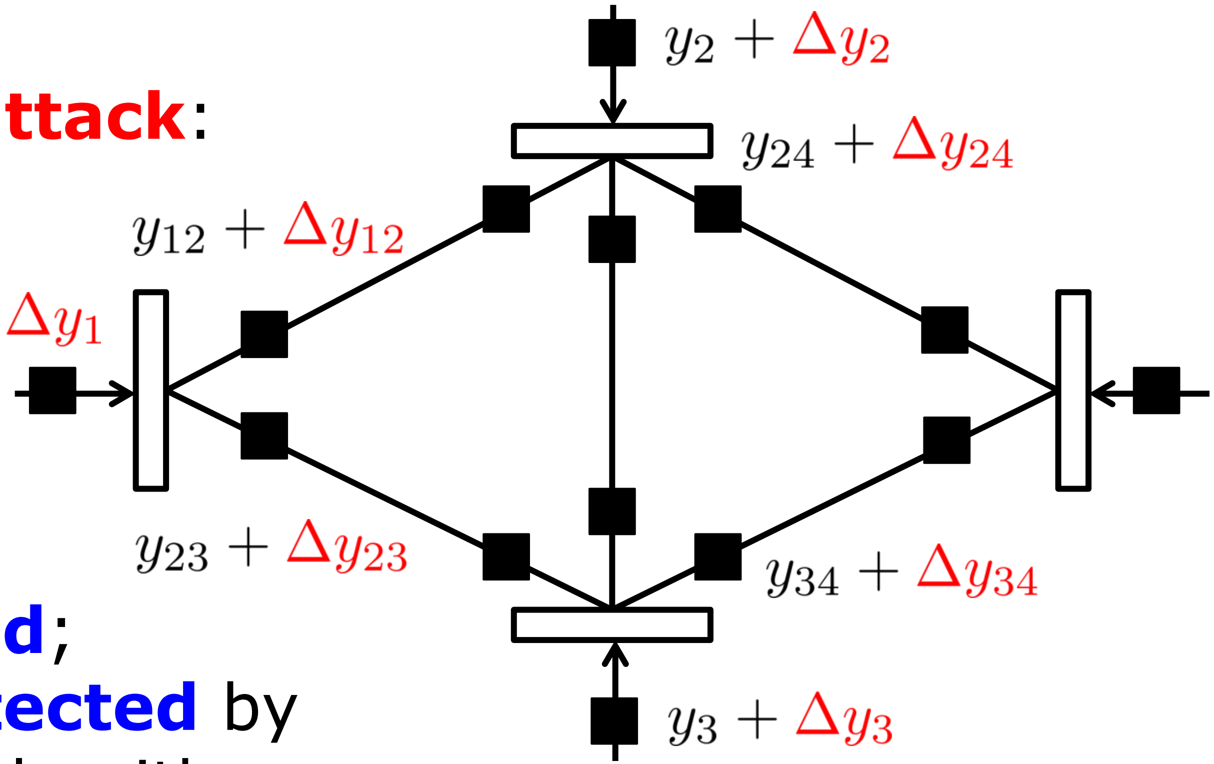
→ intentional data attack → $\tilde{\theta} = \hat{\theta} + \Delta\theta$

Stealthy Additive Deception Attack

Measurements subject to **attack**:

$$\tilde{y} = y + \Delta y$$

Is there a state explaining the received measurements?



Attack is **constrained**; otherwise will be **detected** by Bad Data Detection algorithm

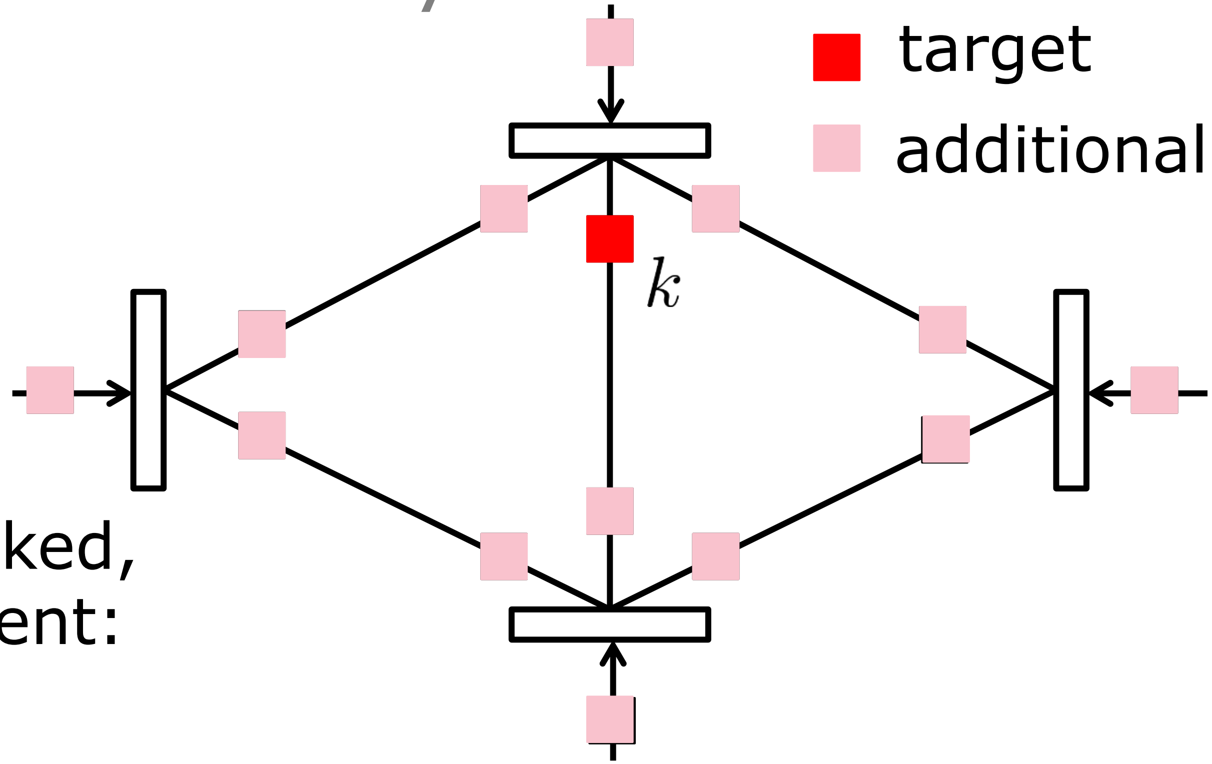
Stealth attack: $\Delta y = H \Delta \theta$

[Liu *et al*., ACM CCCS, 2009], [Sandberg *et al*., CPSWEEK, 2010]

Quantification: Security Index

Stealth attack $\Delta y = H\Delta\theta$

In general, $e_k \notin \operatorname{span}(H)$



Minimum # of meters attacked, targeting the k^{th} measurement:

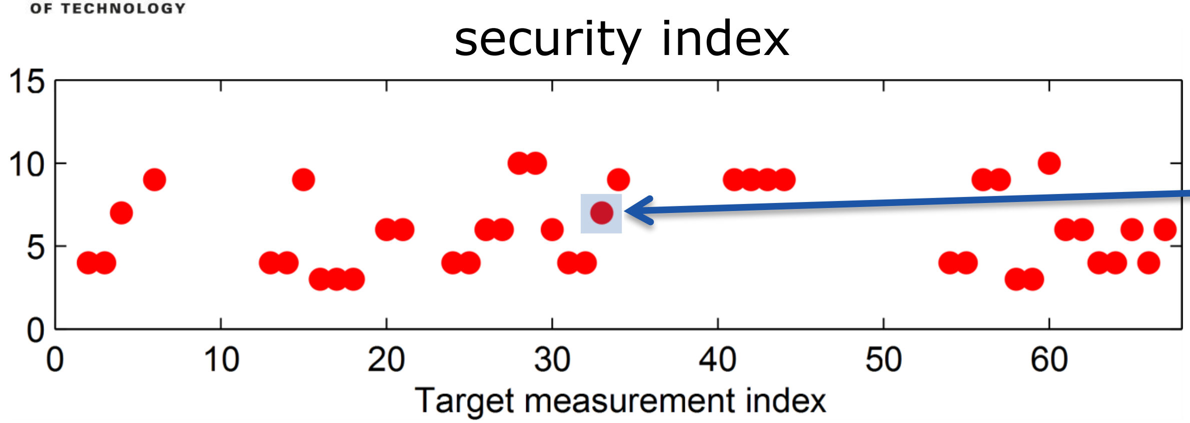
$$\min_{\Delta\theta} \|H\Delta\theta\|_0$$

$$\text{s.t. } H(k,:)\Delta\theta = 1$$

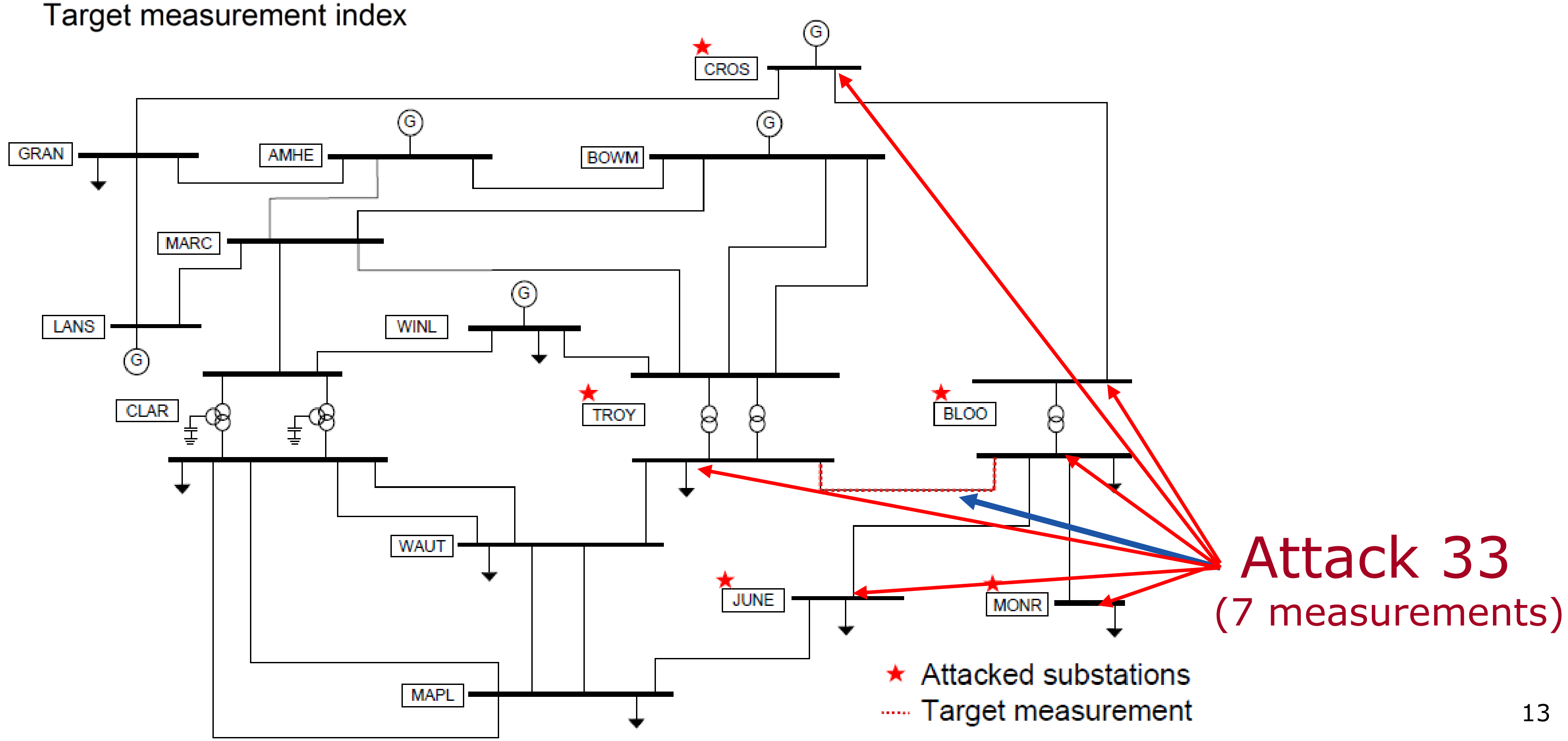
Minimum objective value = **security index**
[Sandberg *et al.*, CPSWEEK, 2010]

See also [Kosut *et al.*, IEEE TSG, 2011]

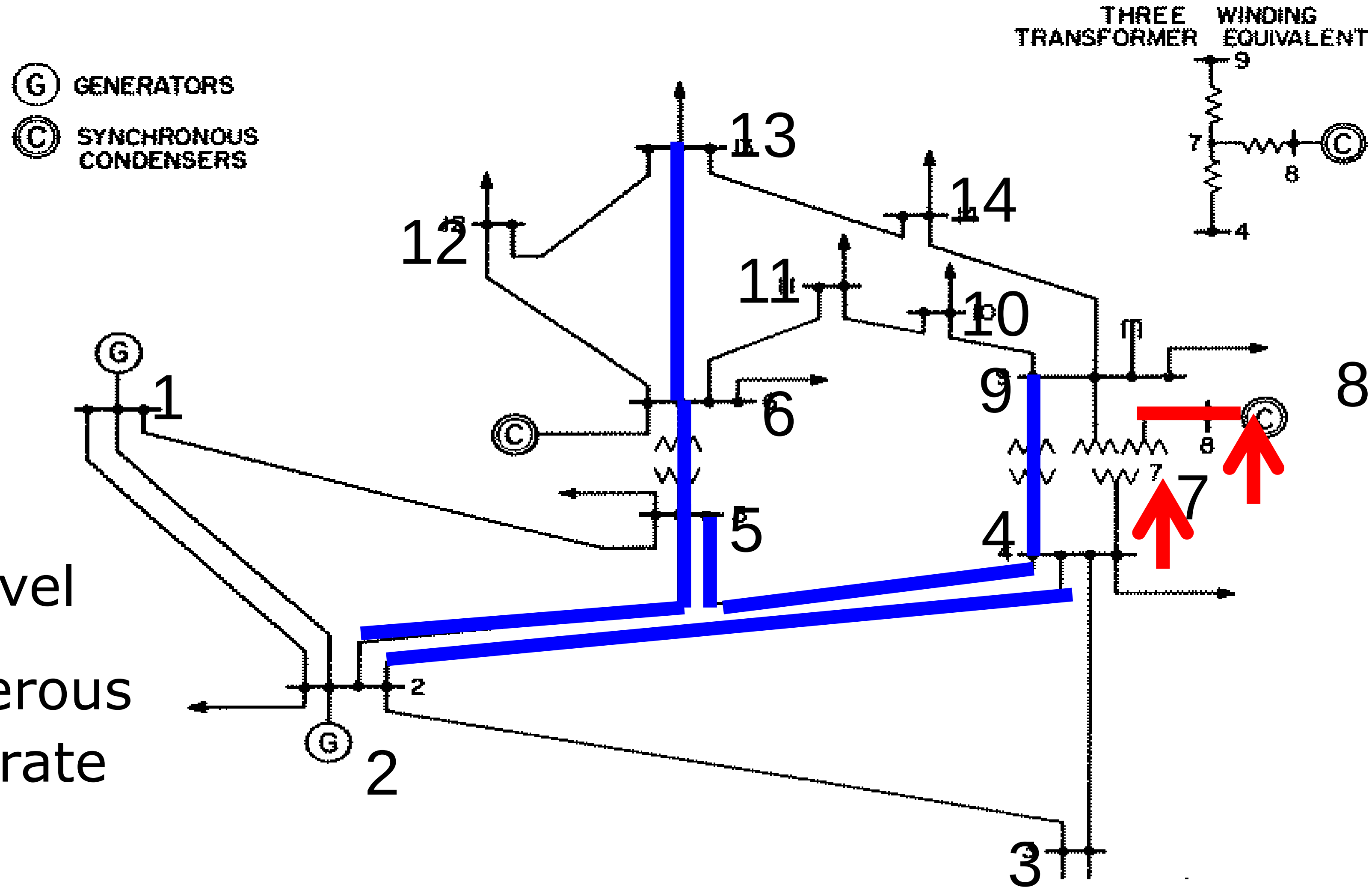
A Security Metric for 40-bus Network



At least 7 measurements involved in a stealth attack against measurement 33



The Goal: Quantify Security to Aid Allocation of Protection



Security level

- dangerous
- moderate
- safe

ROYAL INSTITUTE OF TECHNOLOGY

Security index problem

$$\min_{\Delta\theta} \|H\Delta\theta\|_0$$

$$\text{s.t. } H(k,:)\Delta\theta = 1$$

How to solve?

Closely related to compressed sensing and computation of **cospark** of *H* [Tillmann and Pfetsch, IEEE TIT, 2013]. Problem known to be **NP-hard** for arbitrary *H*.

Wish List

- Can we find solutions as **accurately** as MILP, and **faster** than LASSO?
  - Arbitrary *H*: **No**! (Problem NP-hard)
  - *H* with the special physical and measurement structure: **Yes**! (Min cut polynomial time algorithm next)

- Can we find methods giving more **problem insight**, and ideas for **assigning protection**?
  - **Yes**, exploit graph interpretation of solution

Binary Phase Assignment is Optimal

Security index problem

$$\min_{\Delta\theta} \|H\Delta\theta\|_0$$

s.t.

$$H(k,:)\Delta\theta = 1$$

[Sou *et al*., CDC, 2011]

$$\min_{\Delta\theta} \|H\Delta\theta\|_0$$

s.t.

$$H(k,:)\Delta\theta = 1$$

$$\Delta\theta_i \in \{0, 1\}$$

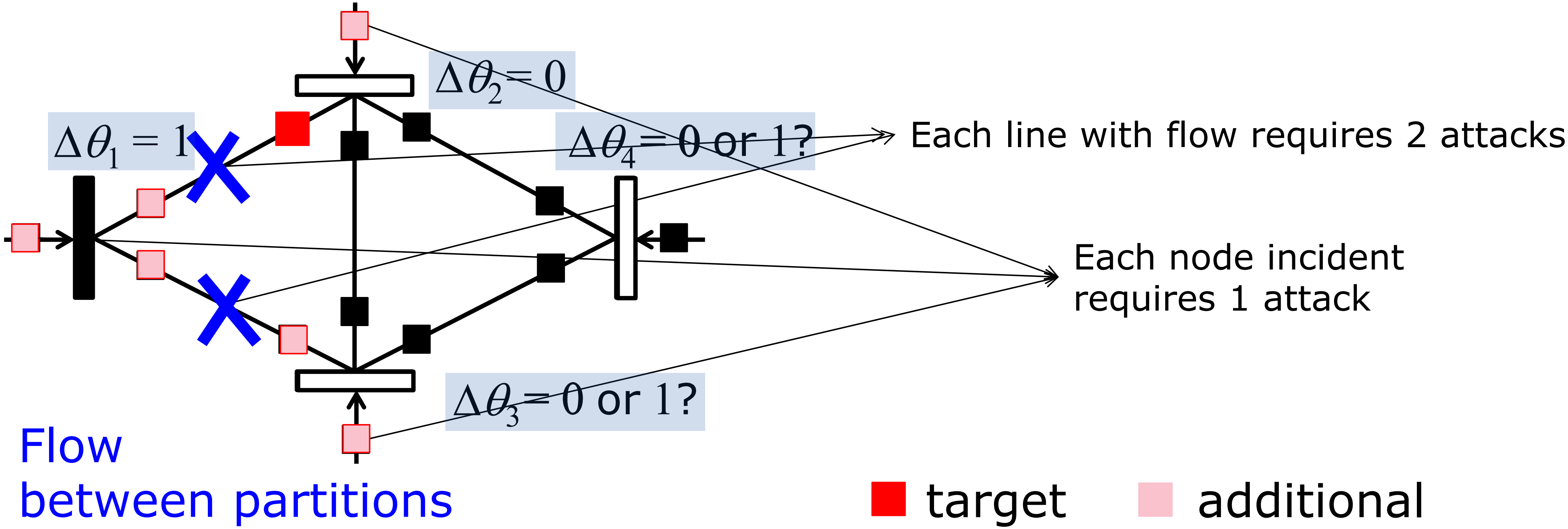
Theorem: Optimal $\Delta\theta_i$ can be restricted to 0 or 1, for all i

Proof: Restriction can never increase number of flows, given the structure of *H*

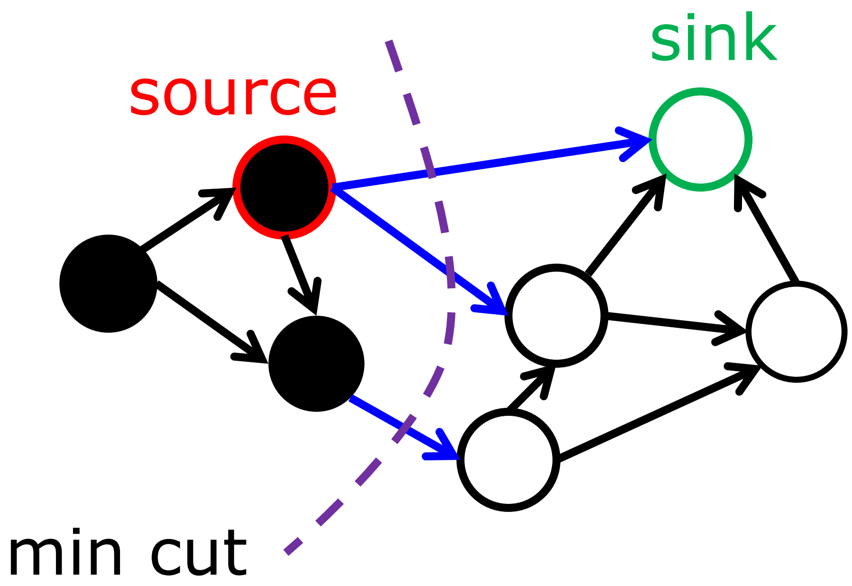
Reformulation as Node Partitioning

$$\min_{\Delta\theta} \|H\Delta\theta\|_0$$
$$\text{s.t.} \quad H(k,:)\Delta\theta = 1$$
$$\Delta\theta_i \in \{0,1\}$$

Security index problem:
Pick partition of minimum # of flows and incident nodes



Interlude: The Min Cut Problem



$|V|$ nodes

$|E|$ edges

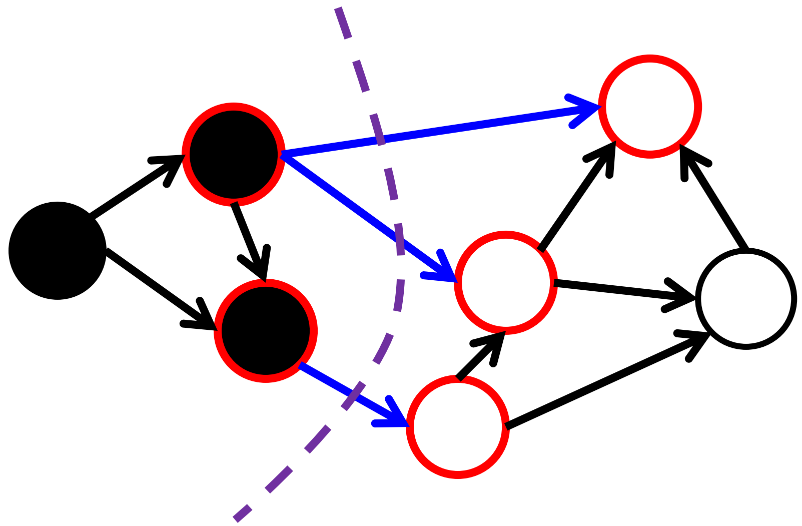
- Partition nodes into two sets (**black** and white) such that source is **black** and sink is white ("a cut")
- Find partitions with the smallest number of edges from source set to sink set ("a min cut")
- Problem solvable in $O(|V||E| + |V|^2 \log|V|)$ operations

ROYAL INSTITUTE OF TECHNOLOGY

Security index problem

$$\min_{\Delta\theta} \|H\Delta\theta\|_0$$
$$\text{s.t. } H(k,:)\Delta\theta = 1$$

Generalized Min Cut problem



How to solve generalized Min Cut?

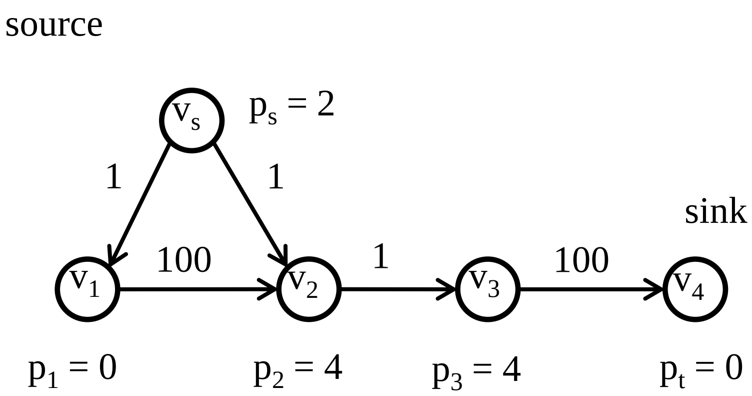
Standard Min Cut on Appended Graph

Generalized Min Cut = Standard Min Cut on **appended** graph

generalized min cut ⟺ standard min cut appended graph

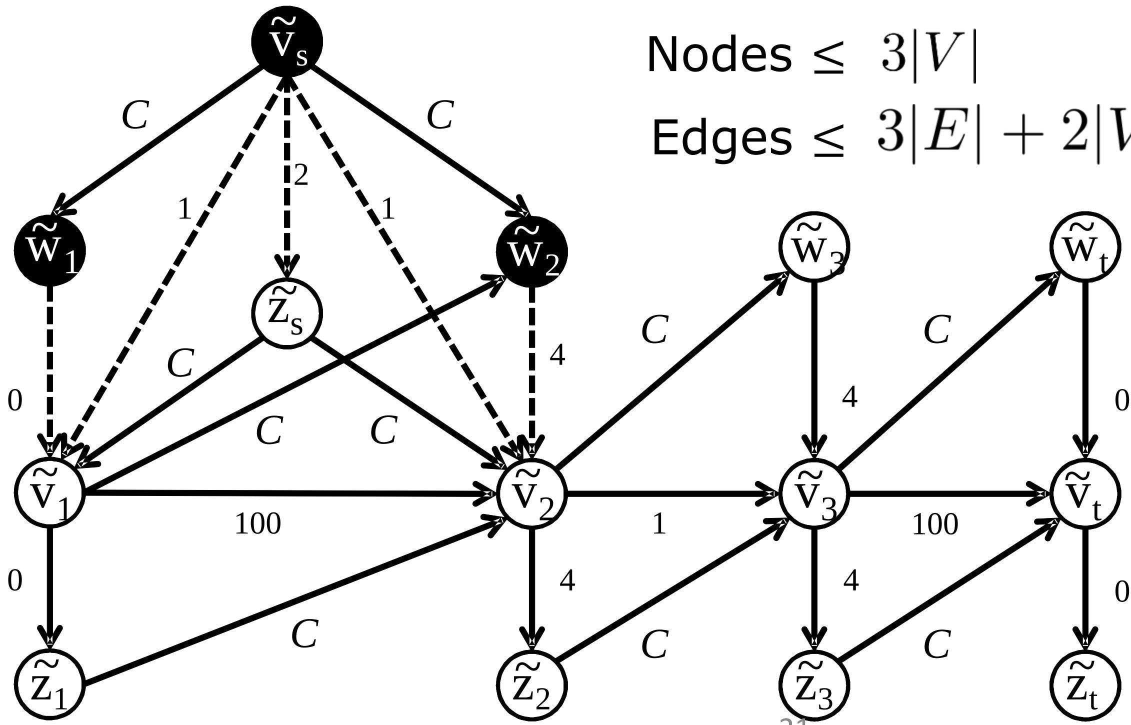
$|V|$ nodes

$|E|$ edges



Nodes $\leq 3|V|$

Edges $\leq 3|E| + 2|V|$



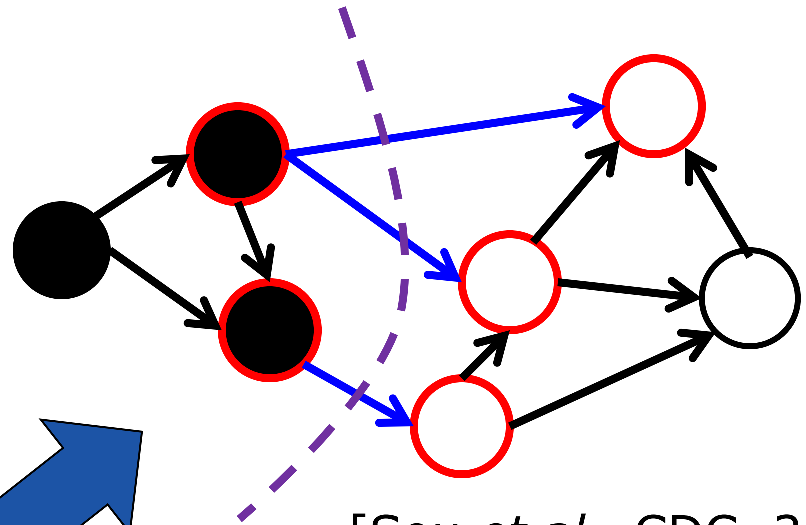
[Hendrickx *et al.*, TAC, 2014]

Security Index Problem – Summary

Security index problem

$$\min_{\Delta\theta} \|H\Delta\theta\|_0$$
$$\text{s.t. } H(k,:)\Delta\theta = 1$$

Generalized Min Cut problem



[Sou *et al*., CDC, 2011]

[Hendrickx *et al*., TAC, 2014]

Practical implications?

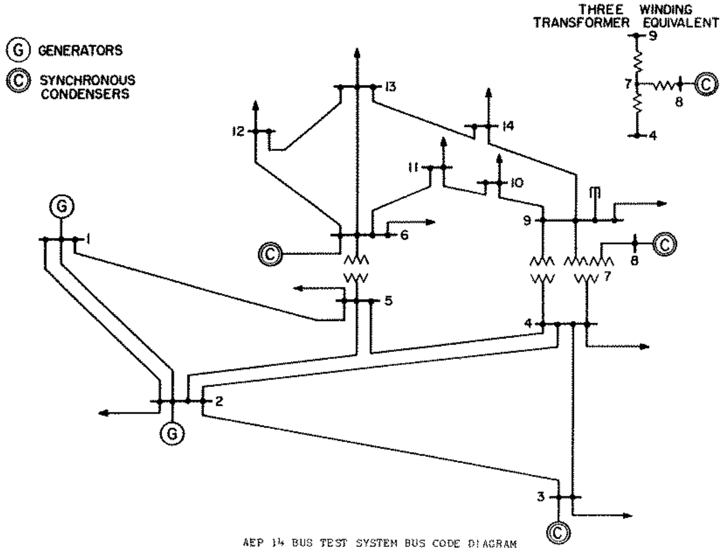
Standard Min Cut problem on an **appended** graph

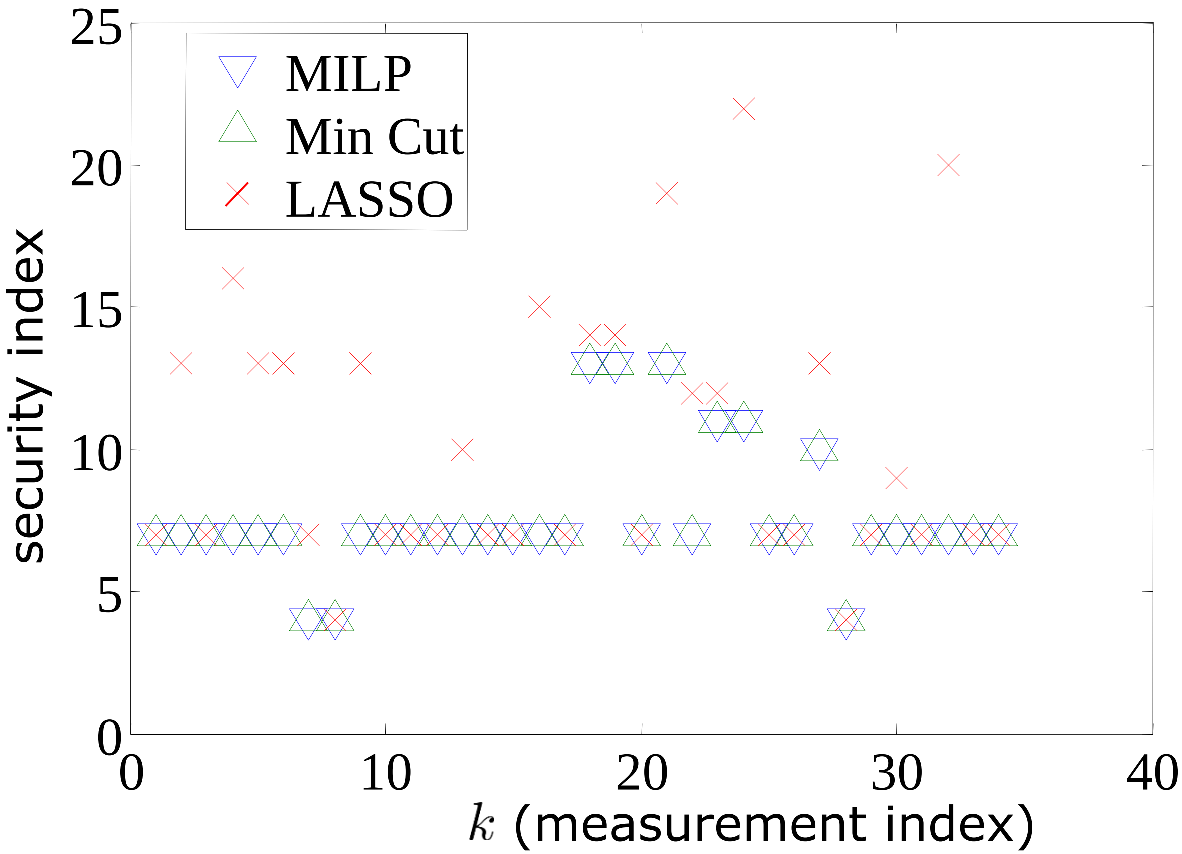
```
>> [maxflow,mincut] = max_flow(A,source,sink);
```

KTH VETENSKAP OCH KONST
ROYAL INSTITUTE OF TECHNOLOGY

IEEE 14 Bus Benchmark Test Result

Security indices for all measurements





Solve time: MILP 1.1s; LASSO 0.6s; Min Cut 0.02s

ROYAL INSTITUTE OF TECHNOLOGY

IEEE 118, 300, 2383 Bus Benchmarks

Min Cut solution is **exact**

Solve time comparison:

Method/Case	**118 bus**	**300 bus**	**2383 bus**
MILP	763 sec	6708 sec	About 5.7 days
Min Cut	0.3 sec	1 sec	31 sec

KTH VETENSKAP OCH KONST
ROYAL INSTITUTE OF TECHNOLOGY

Wish List

- Can we find solutions as **accurately** as MILP, and **faster** than LASSO?
  - Arbitrary *H*: **No**! (Problem NP-hard)
  - *H* with the special physical and measurement structure: **Yes**! (Min cut polynomial time algorithm next.)

- Can we find methods giving more **problem insight**, and ideas for **assigning protection**?
  - **Yes**, exploit graph interpretation of solution
  - **Securing sensors that are frequently cut gives indirect protection to many sensors!**

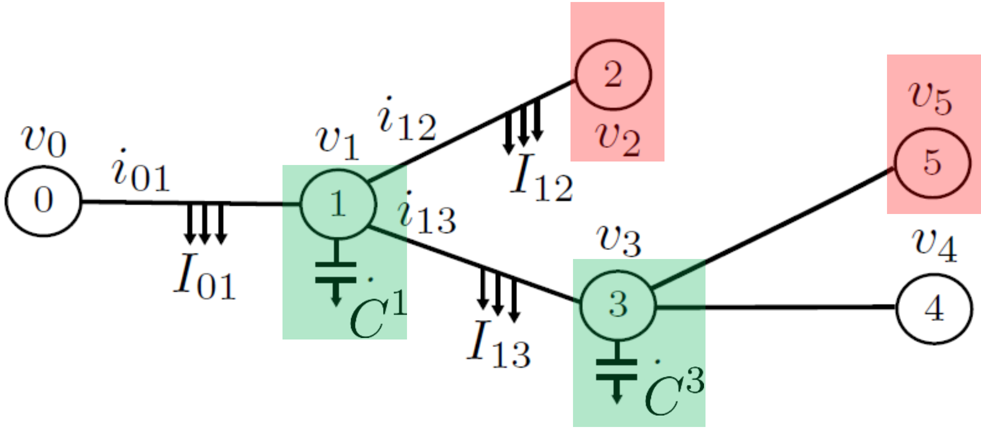
    [Vukovic *et al.*, JSAC, 2012]

ROYAL INSTITUTE OF TECHNOLOGY

Outline

- Background and motivation
- Quantifying security using sparse optimization
- Quantifying security using game theory
- Summary

Stealth Attack on Distribution System Volt/VAR Control



- **Operator's goal:** Switch capacitors C^1 and C^3 to make voltage levels as low as possible, but within safety limits.

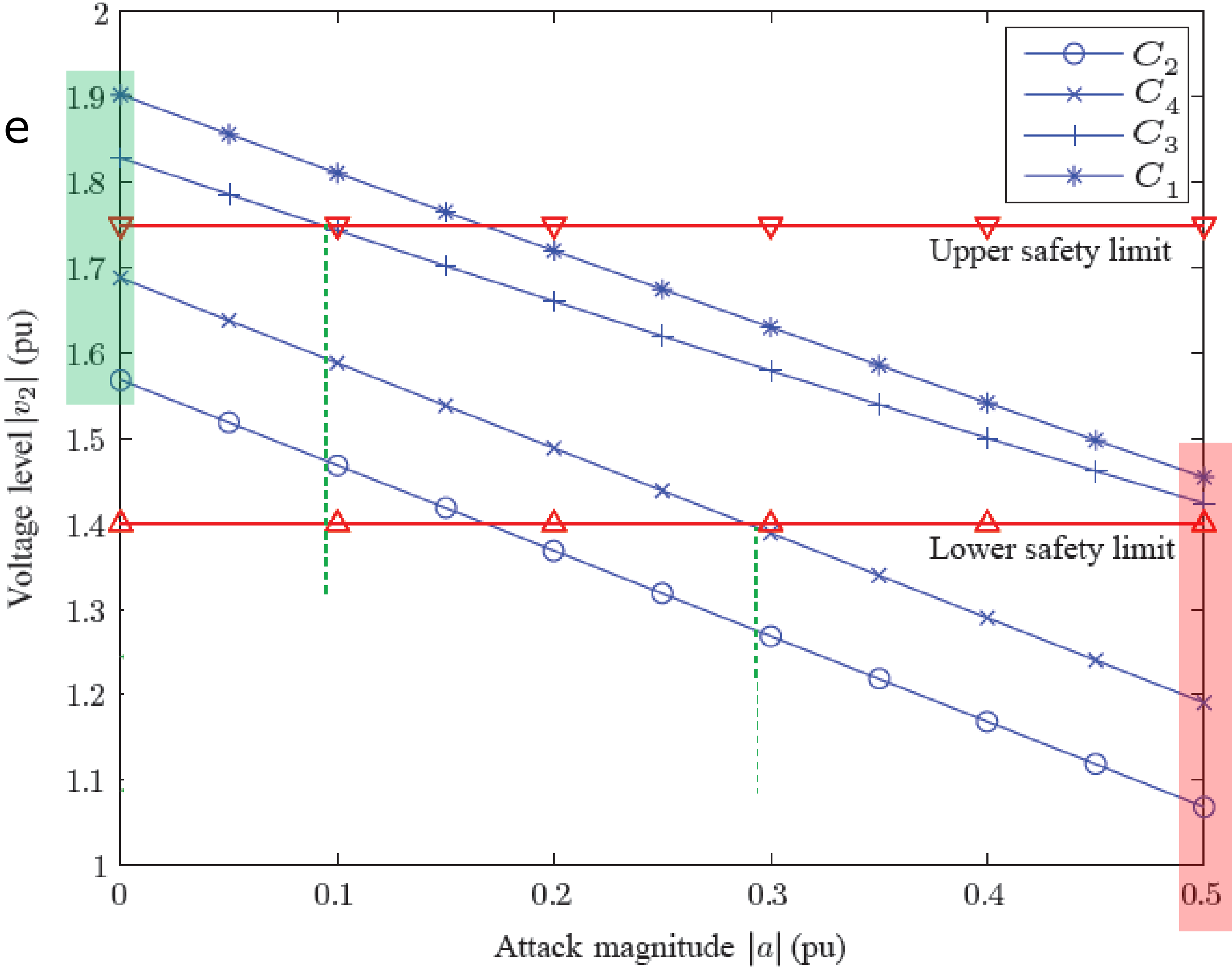
- The voltage measurements v_2 and v_5 are stealth attacked (*i.e.,* bias consistent with physical model)

- **Adversary's goal:** Make voltage levels unnecessarily high, but within safety limits (to avoid detection)

[Teixeira *et al.*, ACC, 2014]

Operator vs. Adversary Game

True voltage levels



Observed voltage levels ($|a| = 0.5$)

MP=Mixed operator strategy **BRP=Pure operator strategy**

ROYAL INSTITUTE OF TECHNOLOGY

Summary

- How to **quantify security** in CPS? Standard control metrics $(\mathcal{H}_2, \mathcal{H}_\infty, \ldots)$ not necessarily the relevant ones

- Security metric using sparse optimization (exactly computable using min cut)

$$\min_{\Delta\theta} \|H\Delta\theta\|_0 \quad \text{s.t.} \quad H(k,:)\Delta\theta = 1$$

- Game theory to quantify and limit possible damage of stealth attacks

- Many exciting opportunities in security for CPS!

Related References

- **Security metrics and sparse optimization:**
  - J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, K. C. Sou: "*Efficient Computations of a Security Index for False Data Attacks in Power Networks*". IEEE TAC: Special Issue on Control of Cyber-Physical Systems, Dec. 2014.
  - A. Teixeira, I. Shames, H. Sandberg, K. H. Johansson: "*A Secure Control Framework for Resource-Limited Adversaries*". Automatica, Jan. 2015.
- **Game example:**
  - A. Teixeira, G. Dan, H. Sandberg, R. Berthier, R. B. Bobba, A. Valdes: "*Security of Smart Distribution Grids: Data Integrity Attacks on Integrated Volt/VAR Control and Countermeasures*". ACC, June 2014.