



On Cyber-Security of State Estimators and Fault Analysis of the Transmission Grid

H. Sandberg, G. Dán, A. Teixeira,
K. C. Sou, O. Vukovic, K. H. Johansson

ACCESS Linnaeus Center
KTH Royal Institute of Technology, Stockholm, Sweden

EKC2 and ACCESS Smart Grids Workshop
May 24, 2011

Outline

- On state estimation, bad-data detection, and cyber stealth attacks in power systems
- A security index
 - Definition and experimental validation
 - Computation
 - Protection and mitigation strategies
- Conclusions

Background and Motivation

- Northeast U.S. Blackout of August 14th, 2003:
55 million people affected
- Software bug in energy management system stalled
alarms in state estimator for over an hour
- Cyber attacks against the power network control
center systems pose a real threat to society



Attack



From security requirements to societal cost

SCADA system



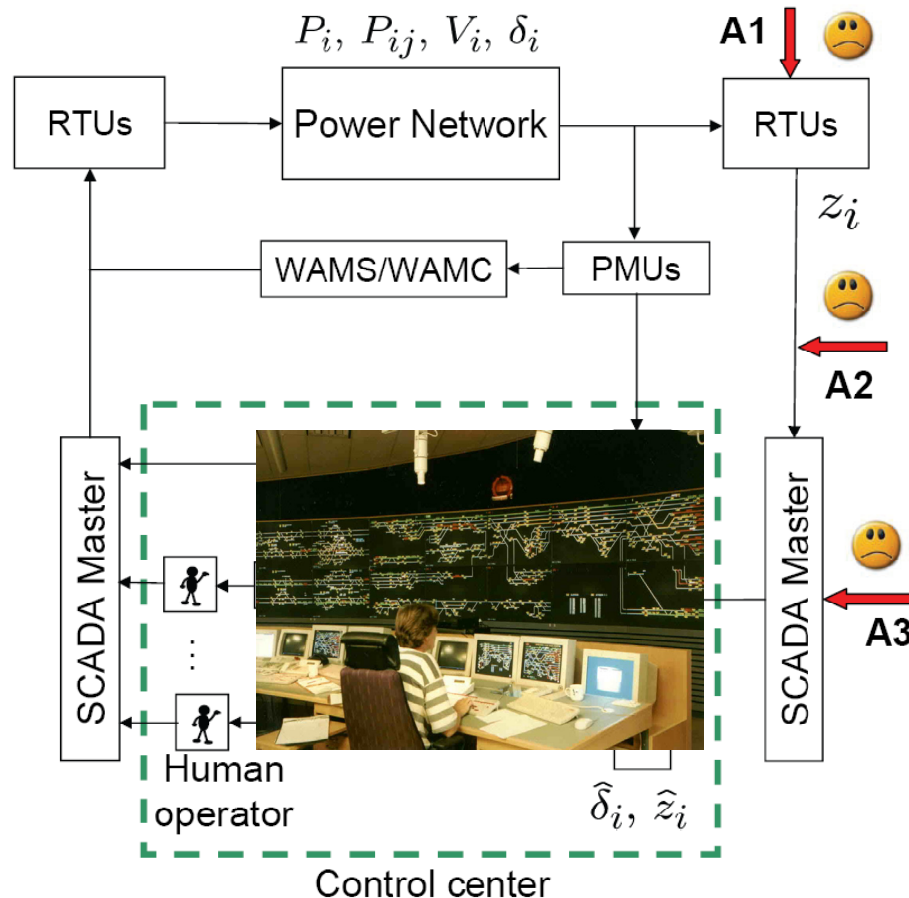
Power network



Societal cost



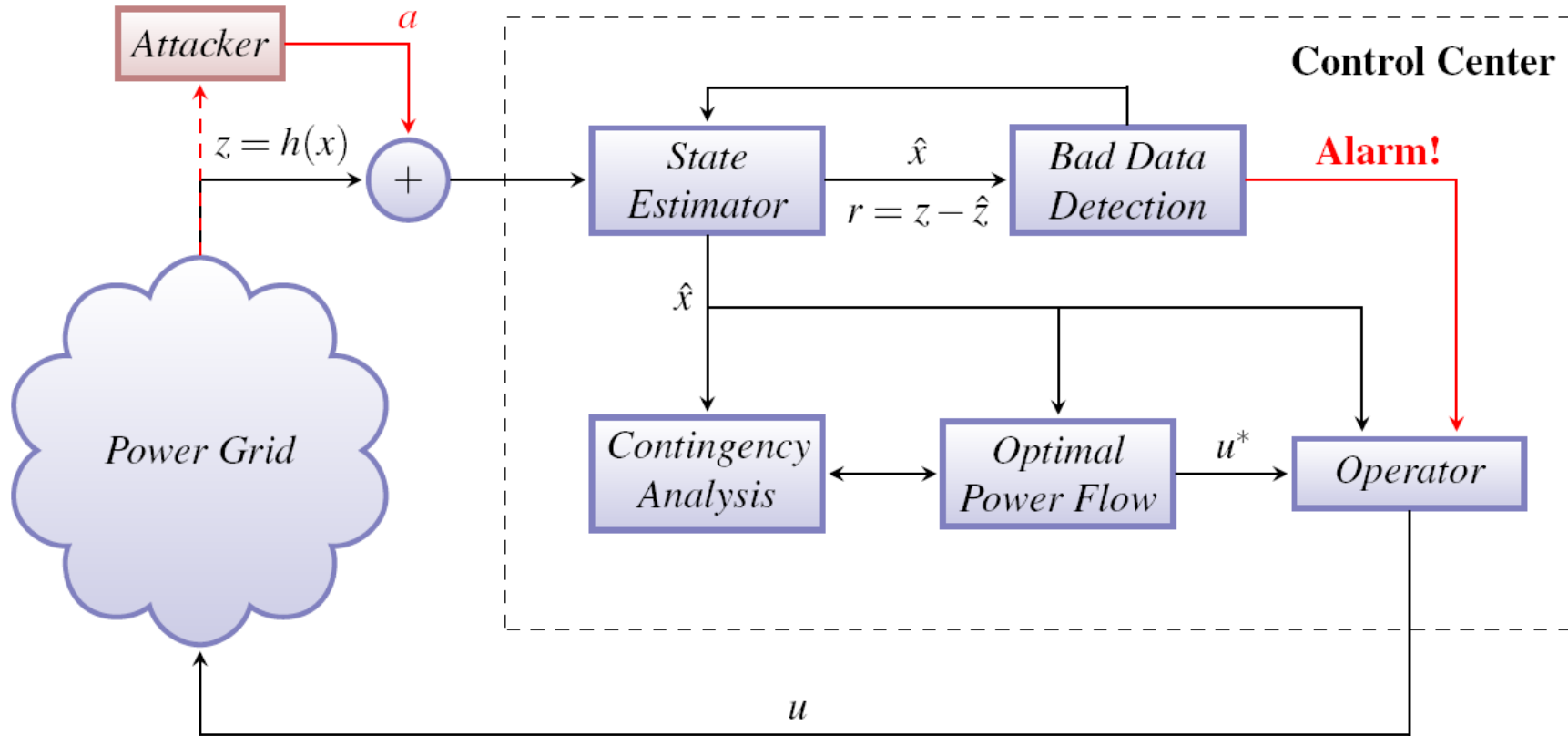
SCADA Systems and False-Data Attacks



- SCADA/EMS used to obtain *accurate state information* to identify faulty equipment, power flow optimization, contingency analysis,...
- Redundant power flow and voltage measurements (z_i) often sent over *unencrypted communication networks*
- How do we strengthen security incrementally against attacks A1-A3?

(SCADA/EMS = Supervisory Control and Data Acquisition/Energy Management Systems)

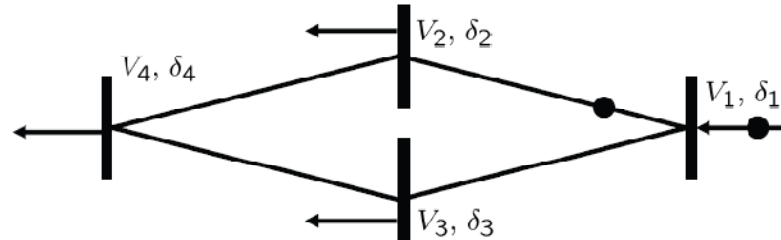
Attack Model



- **Scenario:** Attacker injects **malicious data** a to corrupt analog measurements in the power grid, in order to change state estimates without generating bad data detection alarm
- How characterize the set of **undetectable** malicious data a ?

Power Network and Estimator Models

- Steady-state models:



$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} \frac{V_1 V_2}{X_{12}} \sin(\delta_1 - \delta_2) + \frac{V_1 V_3}{X_{13}} \sin(\delta_1 - \delta_3) \\ \frac{V_1 V_2}{X_{12}} \sin(\delta_1 - \delta_2) \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = h(x) + e \in \mathbb{R}^m$$

- WLS-Estimates of bus phase angles δ_i (in vector \hat{x}):

$$\hat{x}^{k+1} = \hat{x}^k + (H_k^T R^{-1} H_k)^{-1} H_k^T R^{-1} (z - h(\hat{x}^k))$$

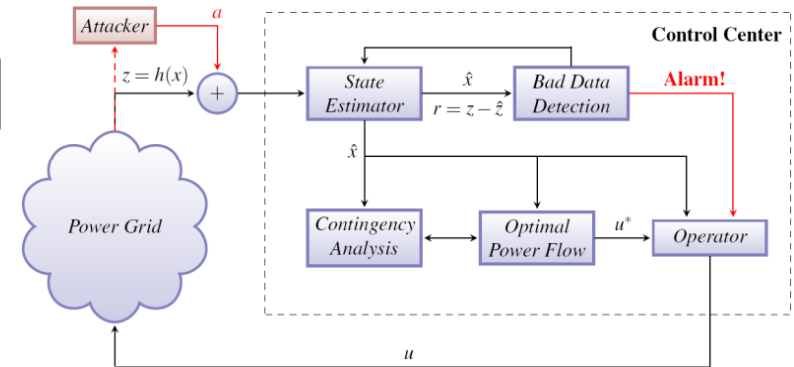
$$H_k := \frac{\partial h}{\partial x}(\hat{x}_k) \quad R := \mathbf{E} e e^T$$

- Linear DC approximation (\approx ML-estimate):

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z$$

$$H := \left. \frac{\partial h(x)}{\partial x} \right|_{x=0}$$

Bad-Data Detection and Undetectable Attacks



- Bad-Data Detection triggers when residual r is large

$$r := z - \hat{z} = z - H\hat{x} = z - H(H^T R^{-1} H)^{-1} H^T R^{-1} z$$

- Characterization of undetectable malicious data a

$$z_a := z + a$$

$$a = Hc \in \mathcal{R}(H)$$

$$r = z - \hat{z} = z_a - \hat{z}_a$$

- The attacker has a lot of freedom in the choice of a !
- Attacker likely to seek sparse solutions a !

Security Index α_k

- Assume attacker wants to make undetectable attack against measurement k

$$\alpha_k := \min_c \|a\|_0 \quad (\text{sparsest possible attack})$$

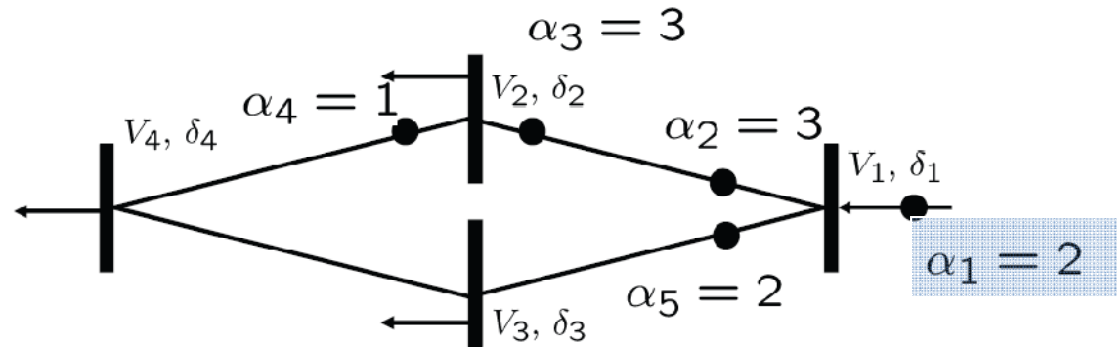
$$a = Hc \quad (\text{undetectable attack})$$

$$a_k = 1 \quad (\text{targets measurement } k)$$

$$(\|a\|_0 := \#\{a_i; a_i \neq 0\})$$

- Estimates complexity of “least-effort undetectable attack” on measurement k
- Example:** $\alpha_1=2 \Rightarrow$ undetectable attack against measurement 1 involves *at least two* measurements
- Non-convex optimization problem. How solve efficiently?

Example of the Index α_k



- Sparse attack corresponding to α_k :

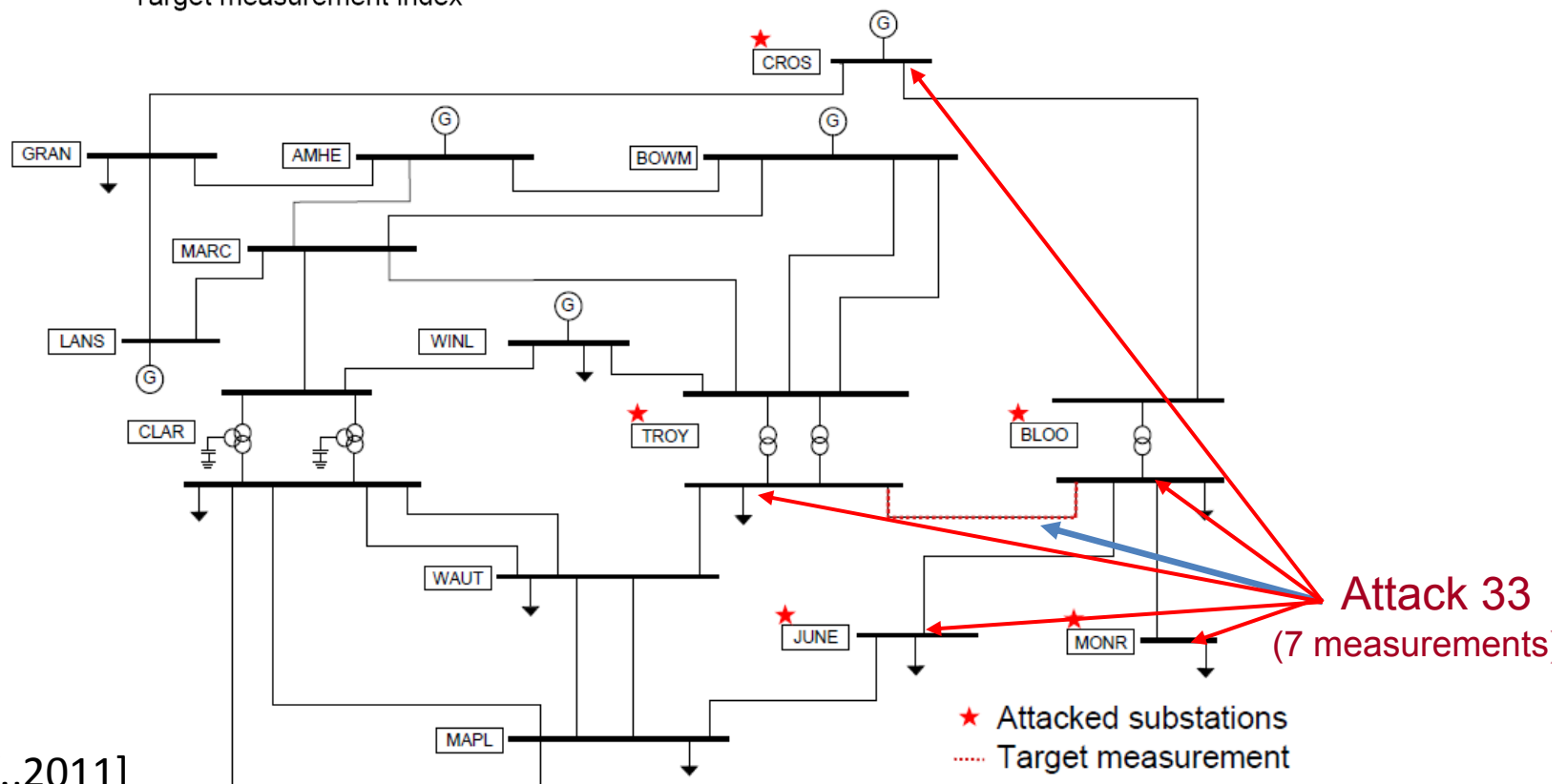
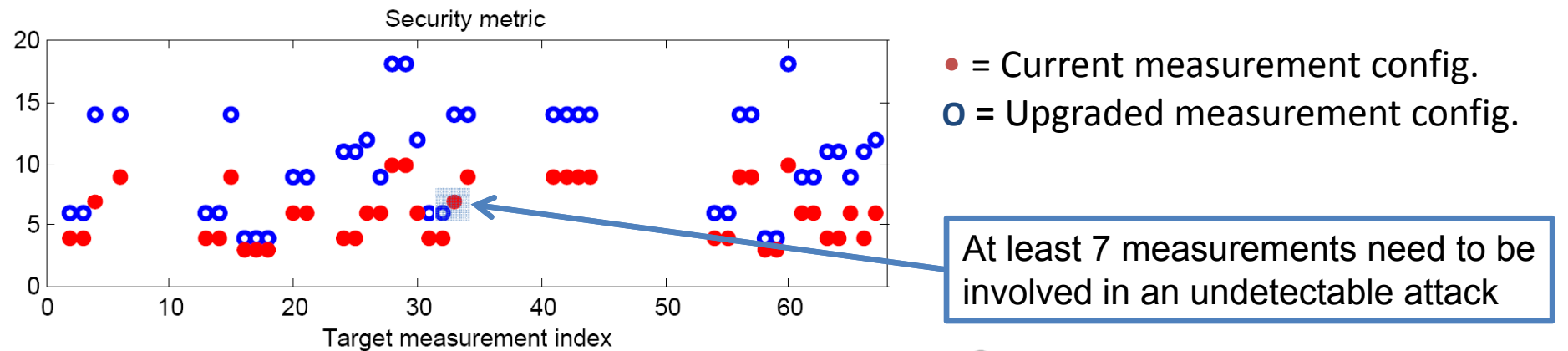
$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- Compare with the “hat matrix”:

$$\begin{pmatrix} \hat{z}_1 \\ \hat{z}_2 \\ \hat{z}_3 \\ \hat{z}_4 \\ \hat{z}_5 \end{pmatrix} = \underbrace{\begin{pmatrix} 0.60 & 0.20 & -0.20 & 0 & 0.40 \\ 0.20 & 0.40 & -0.40 & 0 & -0.20 \\ -0.20 & -0.40 & 0.40 & 0 & 0.20 \\ 0 & 0 & 0 & 1.00 & 0 \\ 0.40 & -0.20 & 0.20 & 0 & 0.60 \end{pmatrix}}_{=H(H^T R^{-1} H)^{-1} H R^{-1}} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \end{pmatrix}$$

- Hat matrix misleading for judging sparsity of attacks!

Security Metric α_k for 40-bus Network



Efficient Computations of Security Metric

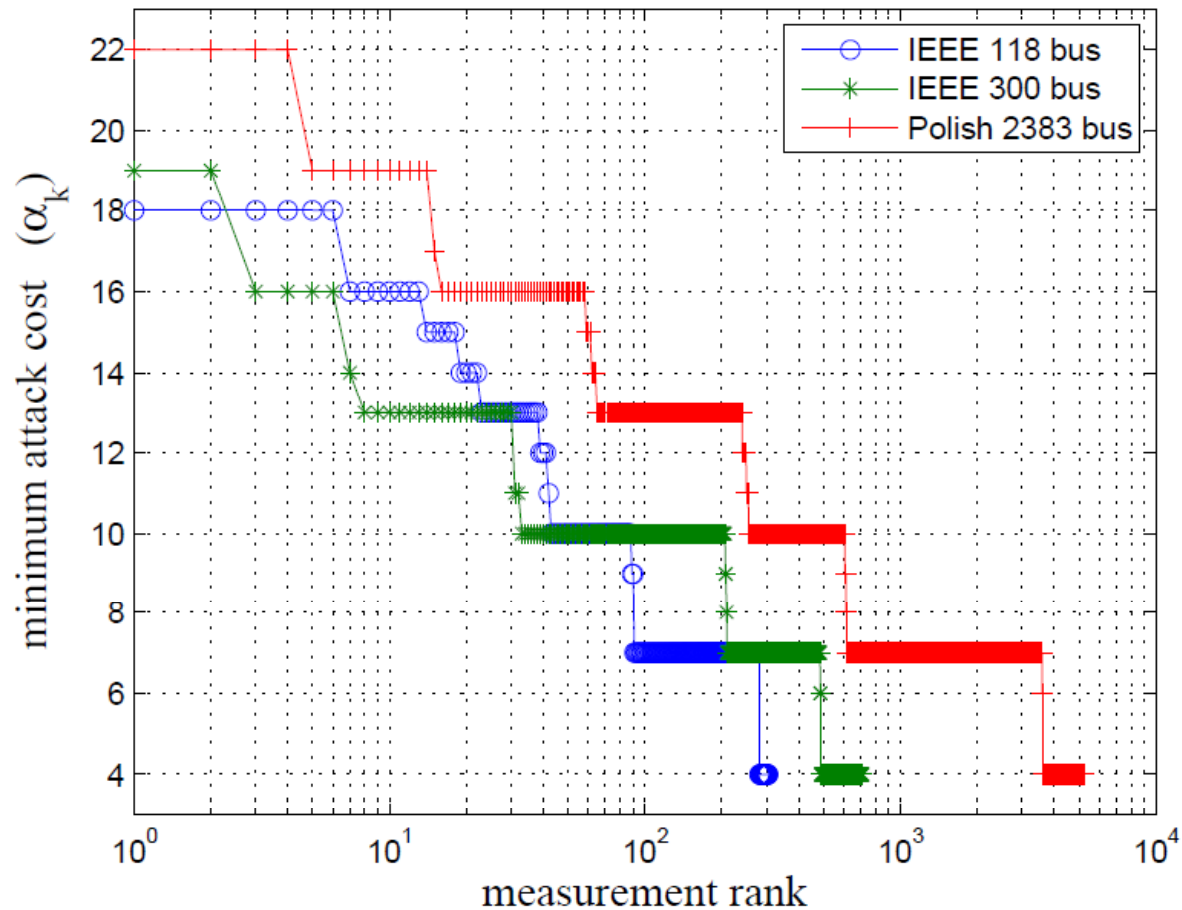
$$\alpha_k := \min_{\Delta\delta} \|H\Delta\delta\|_0$$

subject to $H(k,:) \Delta\delta = 1$

- Mixed integer linear program (MILP)
- Combinatorial optimization problem. **Expensive!**
- Typical convex heuristics: LASSO ($\|\cdot\|_0 \rightarrow \|\cdot\|_1$)
- Exploit structure in H instead:

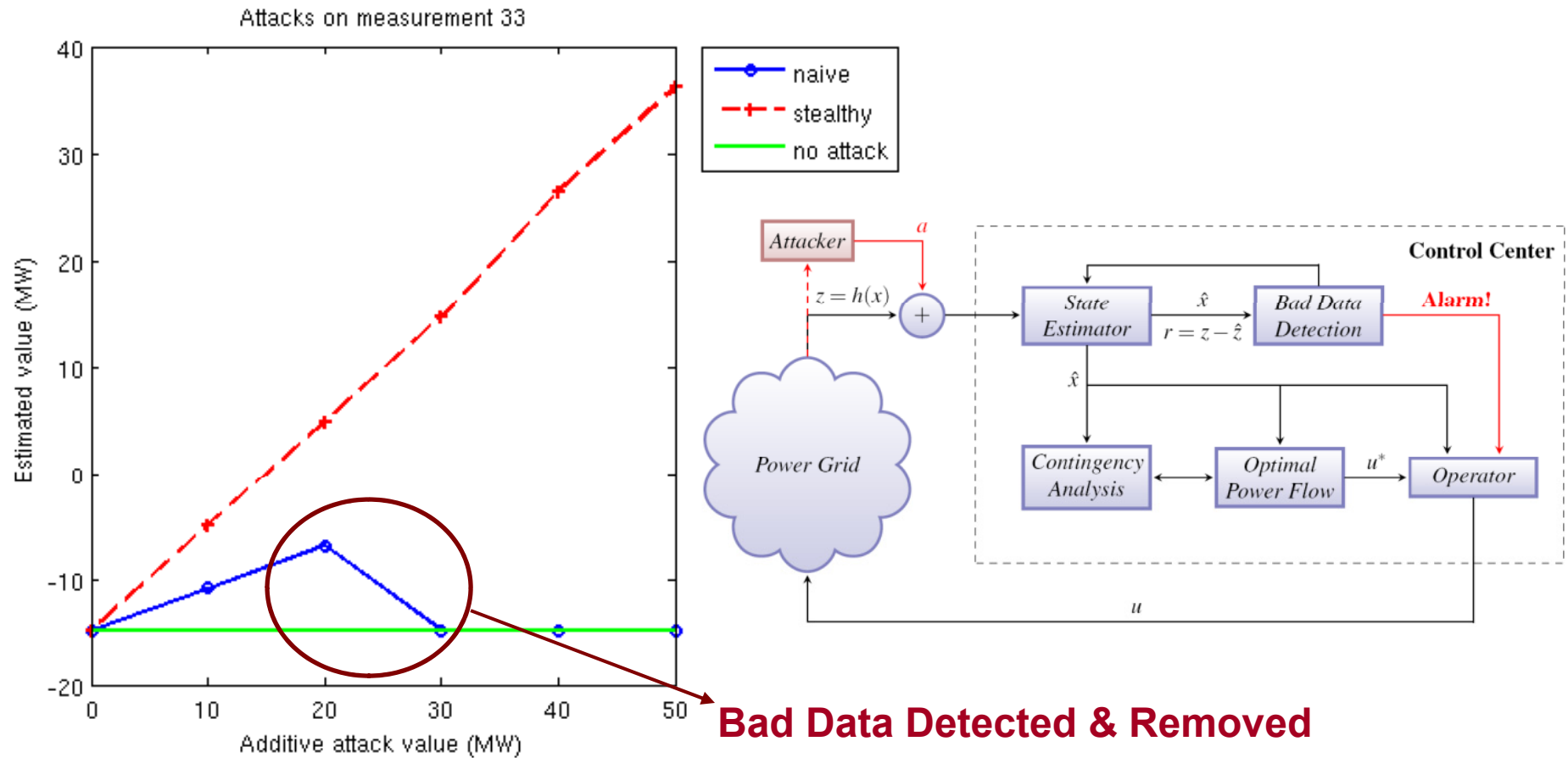
$$H = \begin{bmatrix} ADA^T \\ DA^T \\ -DA^T \end{bmatrix}, A = \text{arc-to-node incidence matrix}, D = \text{pos. diag. matrix}$$

Large-Scale Examples

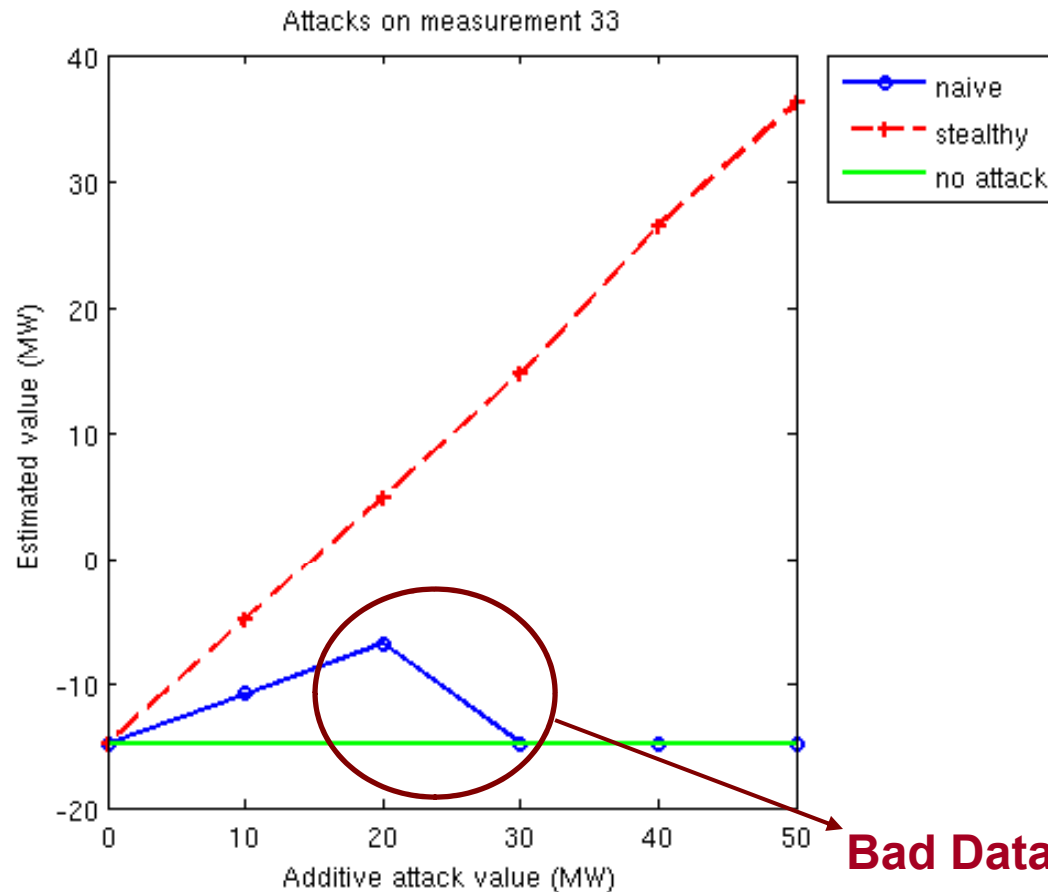


- **IEEE 300-bus:** Exact 6700 sec, LASSO 42.5 sec, MIN-CUT 0.044 sec
- **Polish 2383-bus:** Exact ≈ 5.7 days, MIN-CUT 30 sec

Experiments on KTH SCADA/EMS Testbed



Experiments on KTH SCADA/EMS Testbed



False value (MW)	Estimated value (MW)	# BDD Alarms
-14.8	-14.8	0
35.2	36.2	0
85.2	86.7	0
135.2	137.5	0
185.2	Non convergent	-

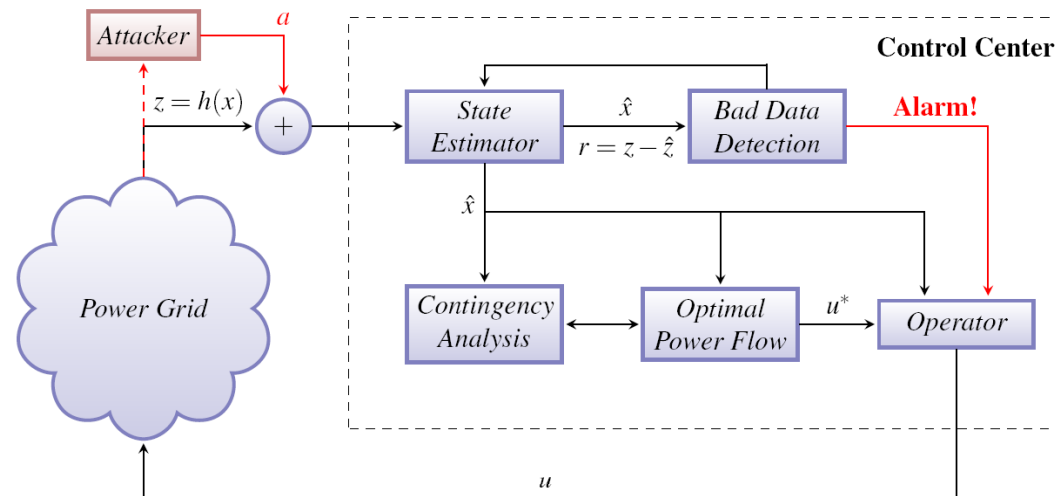
Bad Data Detected & Removed

- Attacks of 150 MW ($\approx 55\%$ of nominal value) pass undetected in a real system!

[Teixeira *et al.*, 2011]

Conclusions

- Undetectable false-data attack against power systems state estimator possible, both in theory and practice
- New security metric α_k to estimate vulnerabilities
- Suggests locations of encryption devices and other counter measures



<http://www.ee.kth.se/~kallej>

Summary so Far

- *Multiple interacting bad data* is hard to detect. What if attacker exploits this well-known fact?
- Security index α_k identifies measurements that are relatively “easy” to attack (it locates weak spots)
- Analysis of the hat matrix can be misleading for judging the sparsity of possible attacks
- How do we compute \mathbb{R}_k , and can we use it for protection and mitigation?

Graph Interpretation

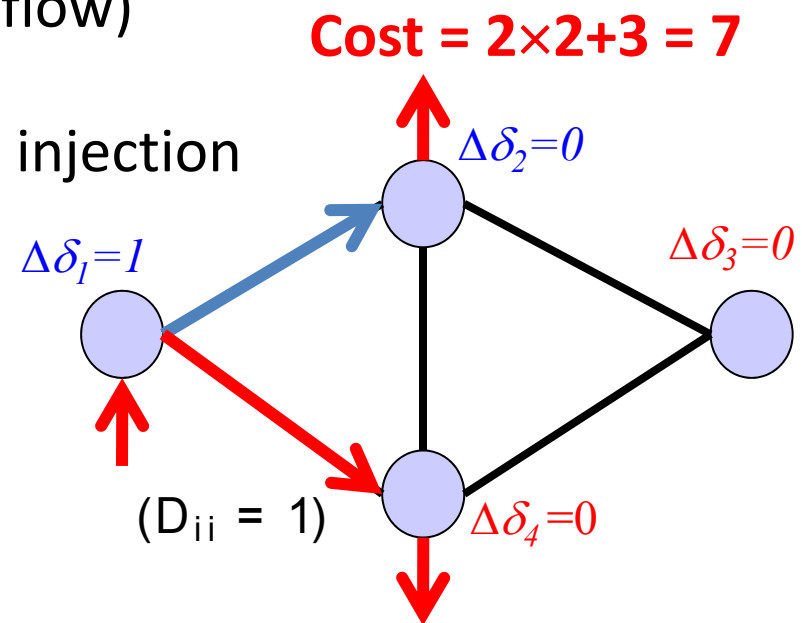
$\Delta\delta$ phase angles

$H\Delta\delta$ injections and flows induced by phase angles

$$\begin{aligned} \|H\Delta\delta\|_0 &= 2 \|DA^T \Delta\delta\|_0 \quad 2 \times (\# \text{ arc with flow}) \\ \text{cost} &+ \|ADA^T \Delta\delta\|_0 \quad \# \text{ node with injection} \end{aligned}$$

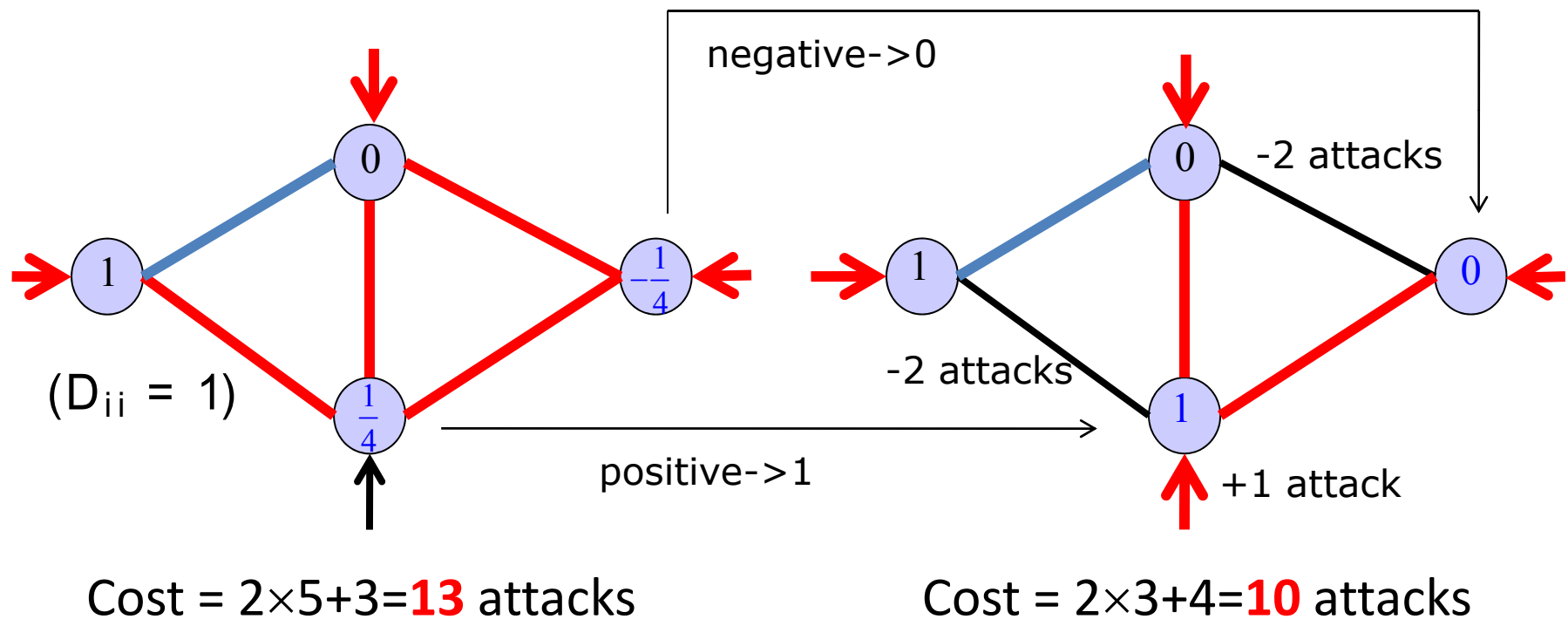
$$H(k,:) \Delta\delta = 1 \quad \text{Fix two phase angles}$$

$$\|H\Delta\delta\|_0 \rightarrow \min \quad \text{Determine the rest to minimize cost}$$



Optimal Solution is Binary Vector

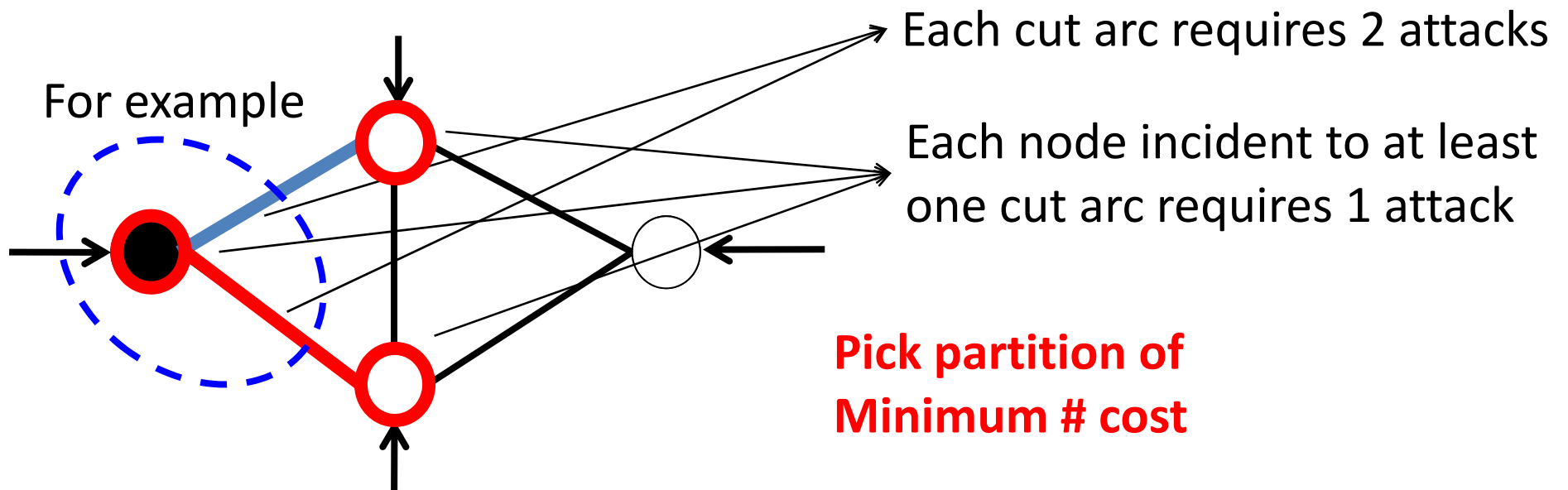
Can always construct no worse 0-1 feasible solution



Reformulation as Graph Partitioning

Optimal $\Delta\delta_i$ are either 0 or 1, for all i

➡ Consider only partitioning of nodes

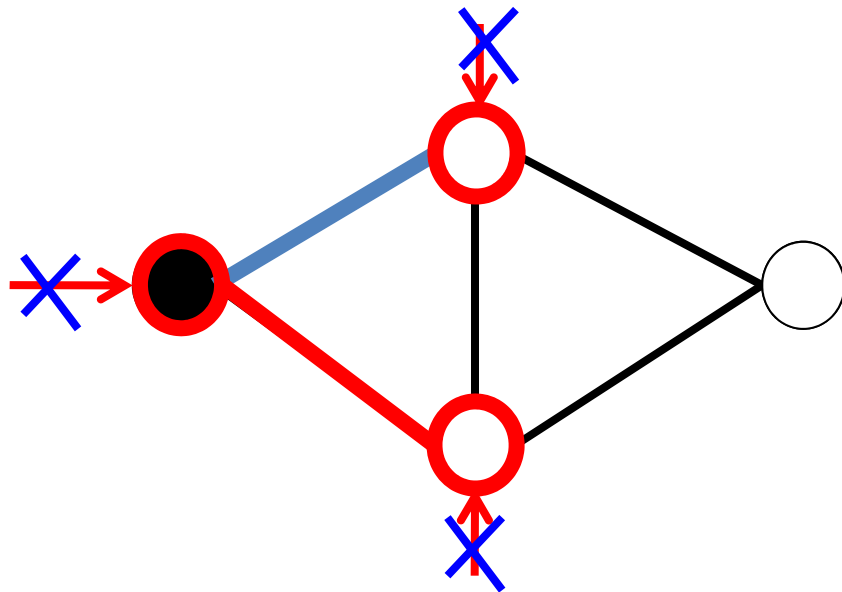


MIN-CUT Relaxation

Min cost partitioning difficult; **Relaxation**: ignore injection cost

$$\|H\Delta\delta\|_0 = 2\|DA^T\Delta\delta\|_0 + \|ADA^T\Delta\delta\|_0$$

$2\times(\# \text{ cut arcs})$ ~~$\# \text{ node with injection}$~~

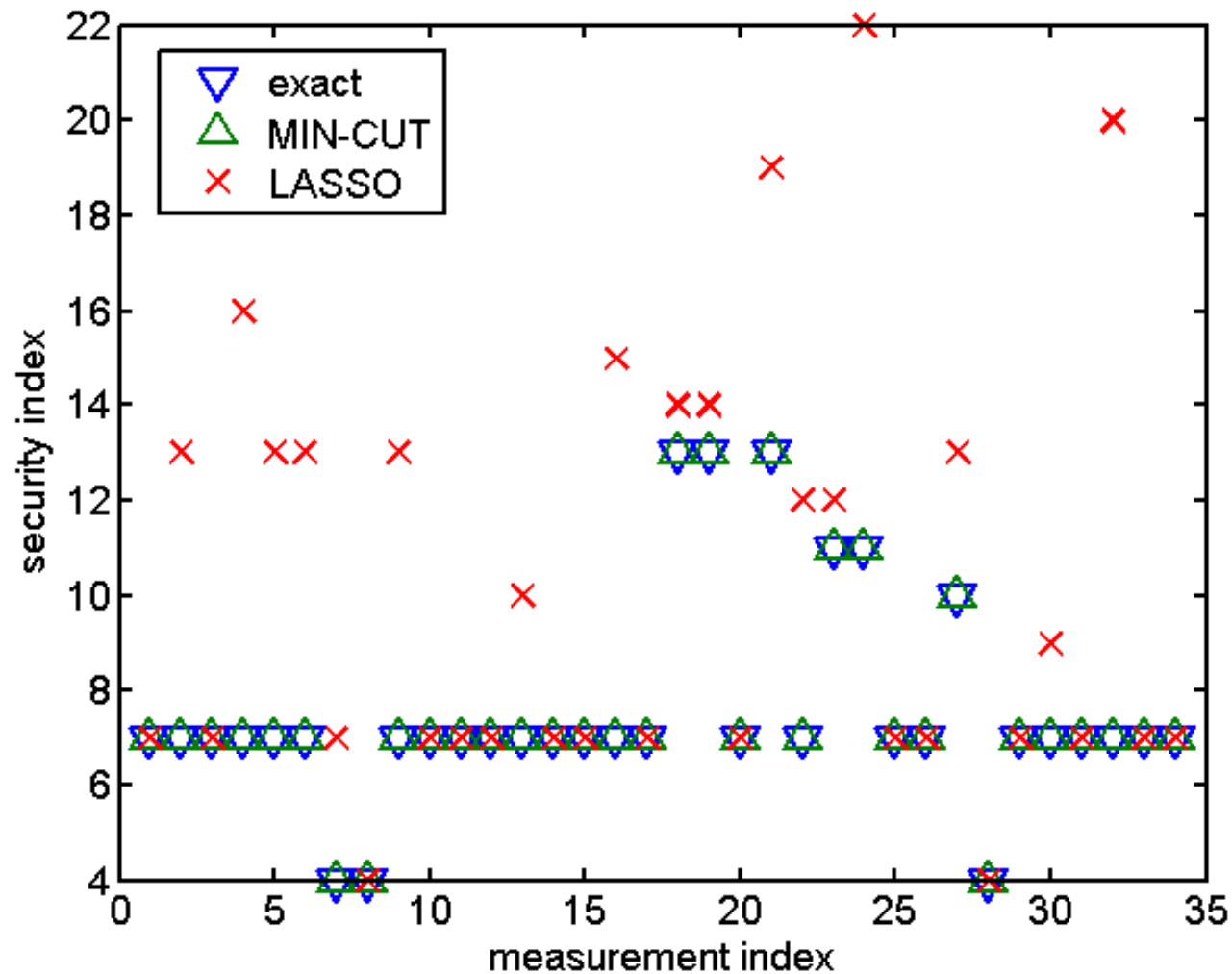


Partitioning with minimum
#of cut arcs

MIN-CUT problem

Enumerate **ALL** MIN-CUT
partitions for best relaxation!

IEEE 14-bus Security Indices



MIN-CUT incurs no error, LASSO is very bad here

Outline

- On state estimation, bad-data detection, and stealth attacks in power systems
- A security index
 - Definition and experimental validation
 - Computation
 - **Protection and mitigation strategies**
- Conclusions

Protection Against Stealth Attacks

- Set of protected measurements P
 - Cost of protection $C_M(P)$

- Protection goals
 - Perfect protection

$$\min_P C_M(P) \quad s.t. \quad \alpha_k = \infty \quad \forall k$$

- Limited budget $C_M(P) \leq \pi$

- *Max-min*
 - *Max-ave*

Protection with Limited Budget π

- Maximize minimum attack cost \mathbb{R}_k

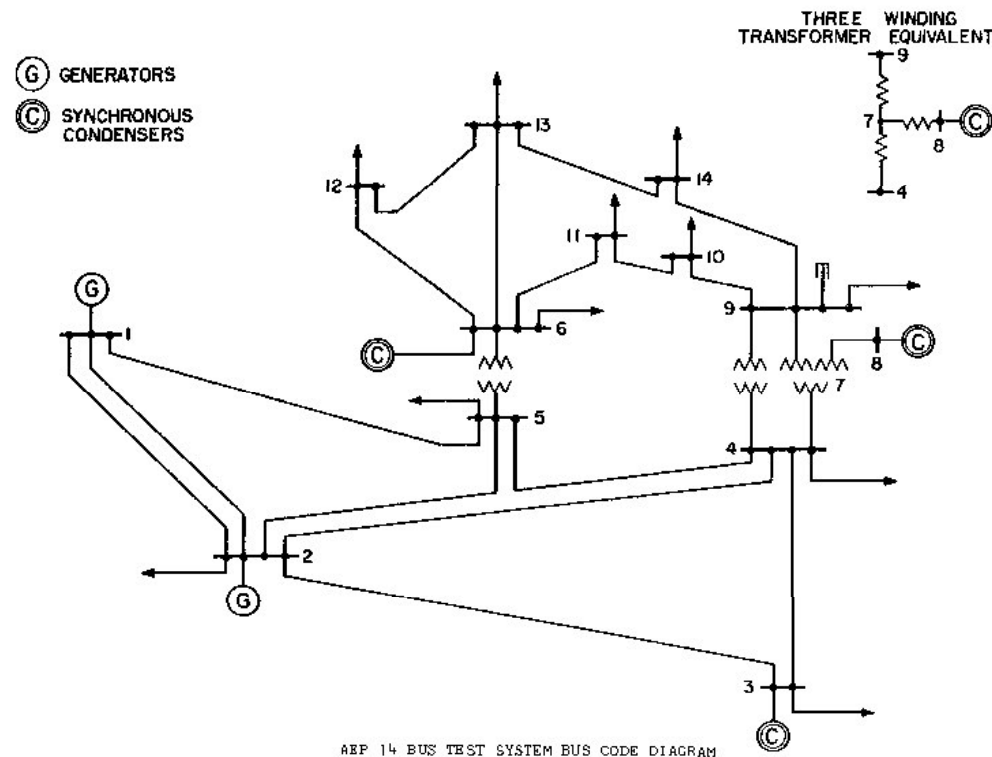
$$P^{MM} = \arg \max_{P: C_M(P) \leq \pi} \min_k \alpha_k$$

- Greedy iterative algorithm (MSM)

- $P = \emptyset$
- Iterate until $C_M(P) = \pi$
 - Calculate α_k given P ($k=1, \dots, M$)
 - Find most frequently appearing meters in minimal attacks corresponding to $\min_k \mathbb{R}_k$ and put in M_j
 - Set $P = P \cup M_j$

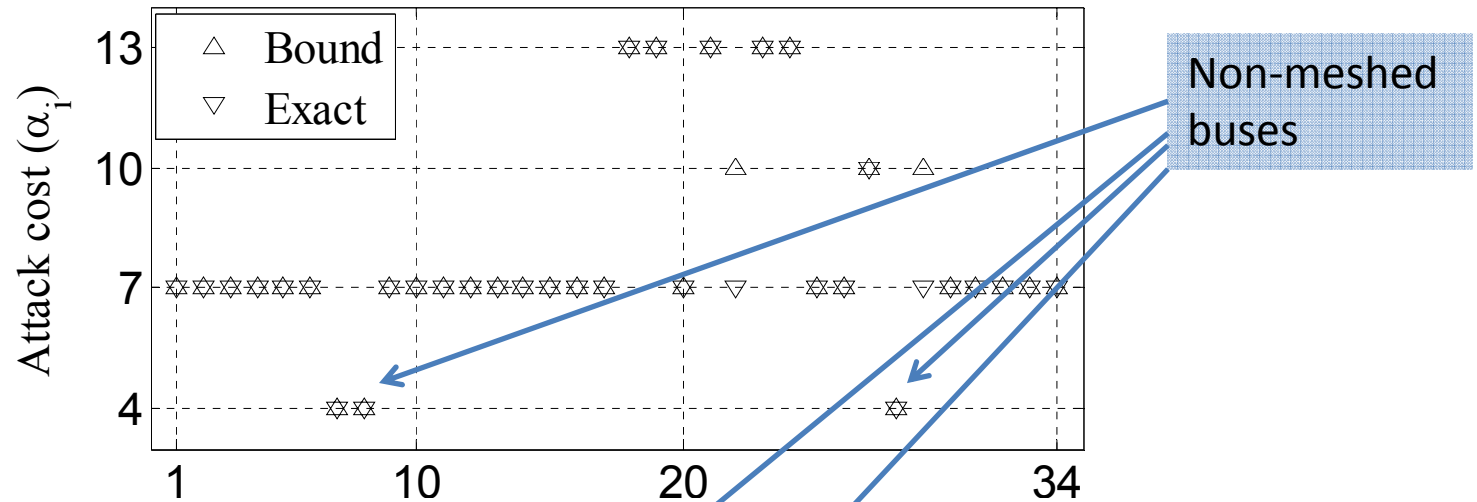
Numerical Results

- IEEE 14-bus and 118-bus networks
- Meters on every load and transmission line
 - 54 and 490 measurements

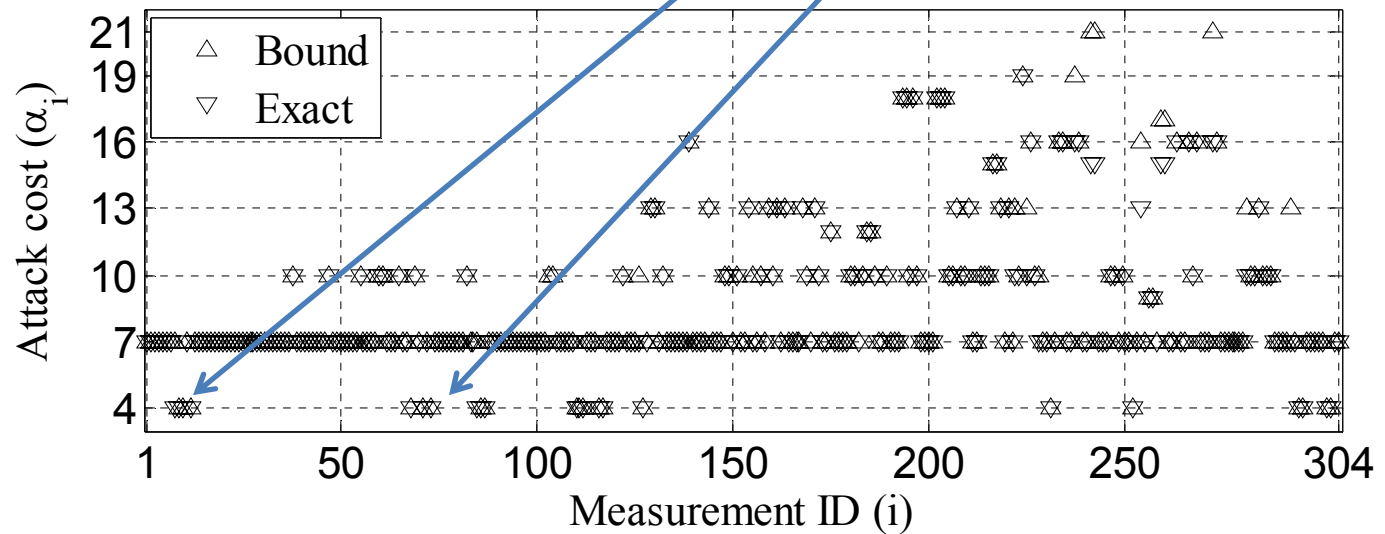


Minimal Attacks - No Protection

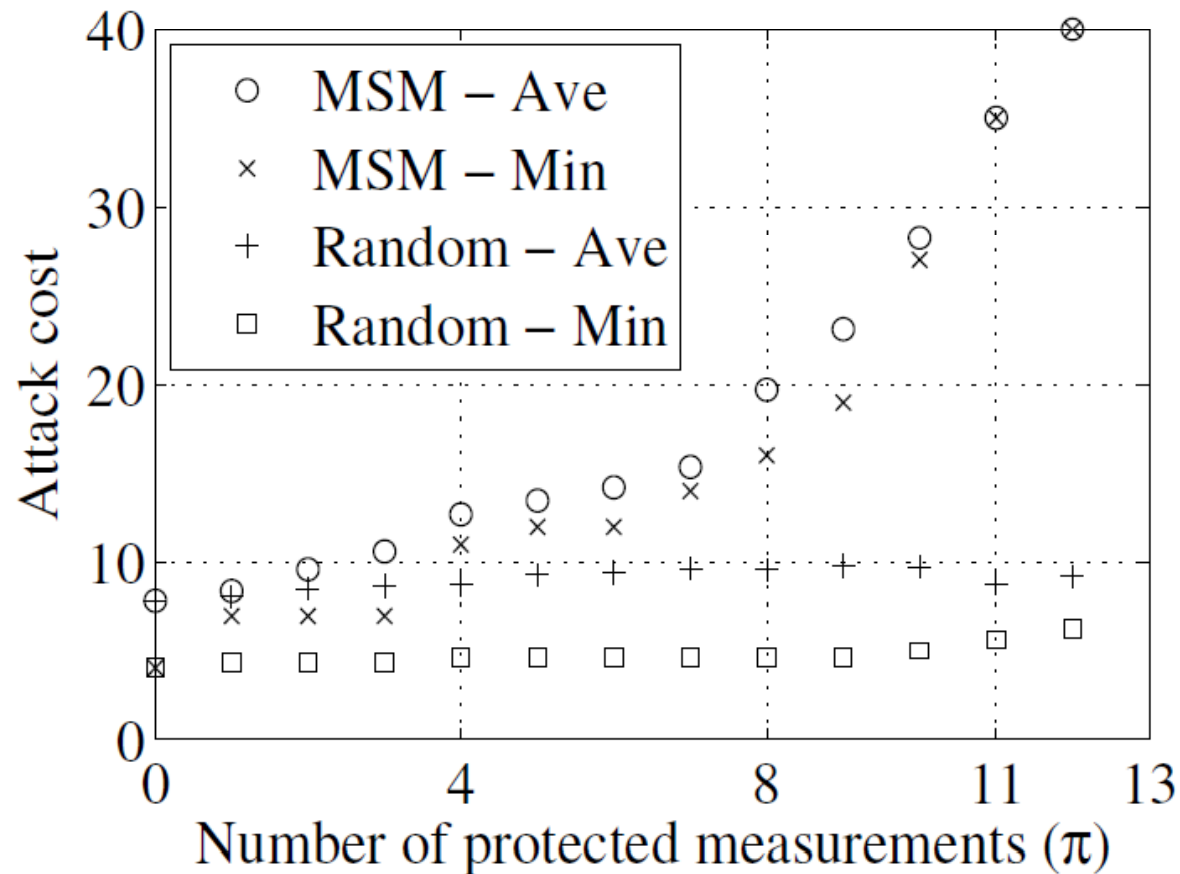
IEEE-14



IEEE-118



Incremental Protection (IEEE 14-bus)

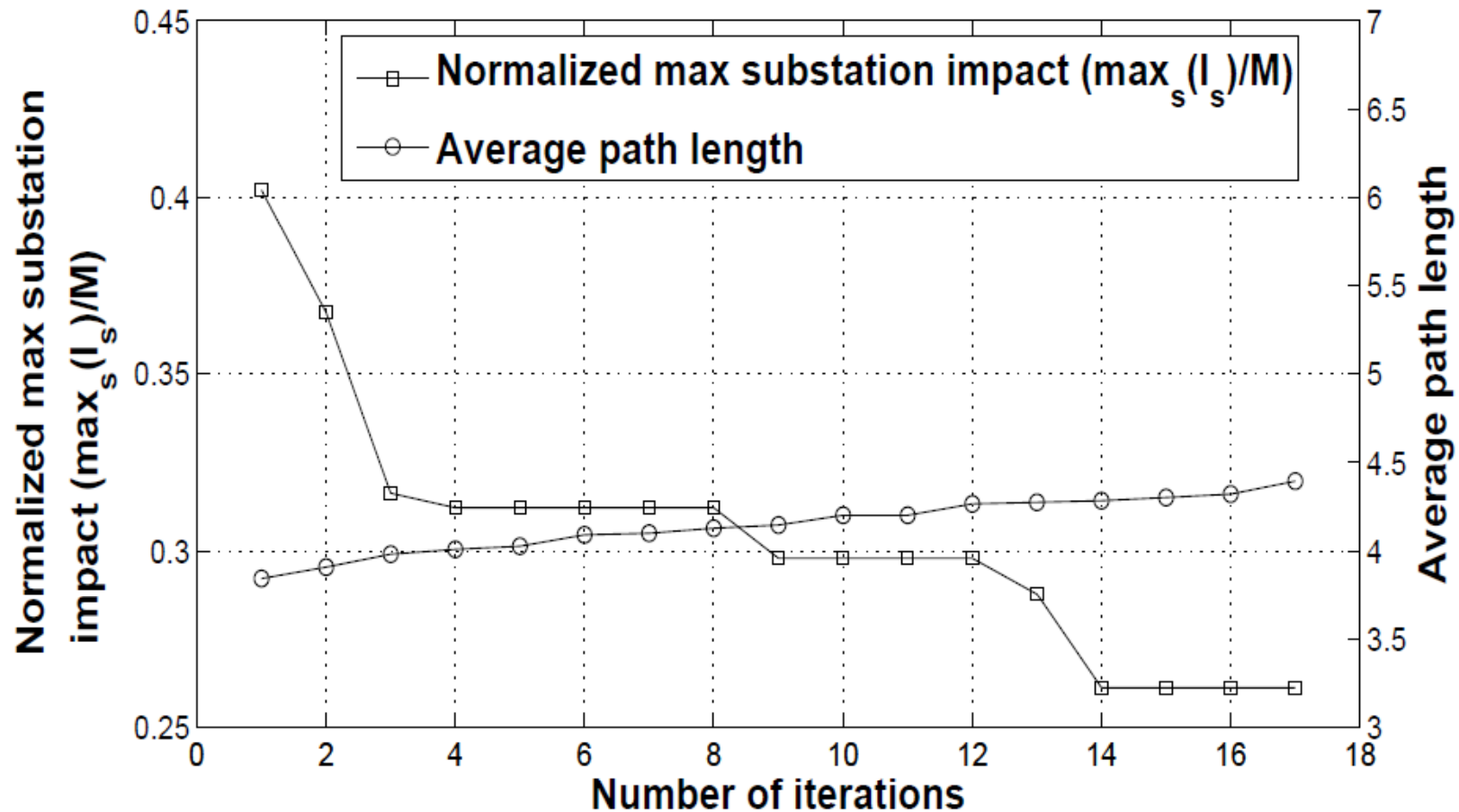


- Increase protection budget $\pi=0,1,\dots,n$
- Perfect protection for $\pi=n=13$
 - Incremental deployment efficient (compare with random deployment)

Impact of the Network Layer

- Optical ground wire topology along transmission lines
- Attack targets
 - Substation switching equipment
- Security metrics
 - Substation attack impact (I_s)
 - # measurements exposed by substation
 - Measurement attack cost (Γ_m)
 - # substations needed to attack measurement
- Mitigation
 - Routing – single and multipath
 - Encryption – tamper proofness
 - Physical protection, surveillance

Reroute Physically Correlated Measurements (IEEE 118-bus)



[Dán, Sou, and Sandberg, 2011]