SEVENTH FRAMEWORK PROGRAMME

VIKING

KTH VETENSKAP OCH KONST

ROYAL INSTITUTE OF TECHNOLOGY

Cyber-physical Models of Power System State Estimation Security

György Dán

School of Electrical Engineering

KTH, Royal Institute of Technology

Stockholm, Sweden

Joint work with: Ognjen Vuković, Henrik Sandberg, Kin Cheong Sou, André Teixeira, Karl-Henrik Johansson, Gunnar Karlsson

ACCESS

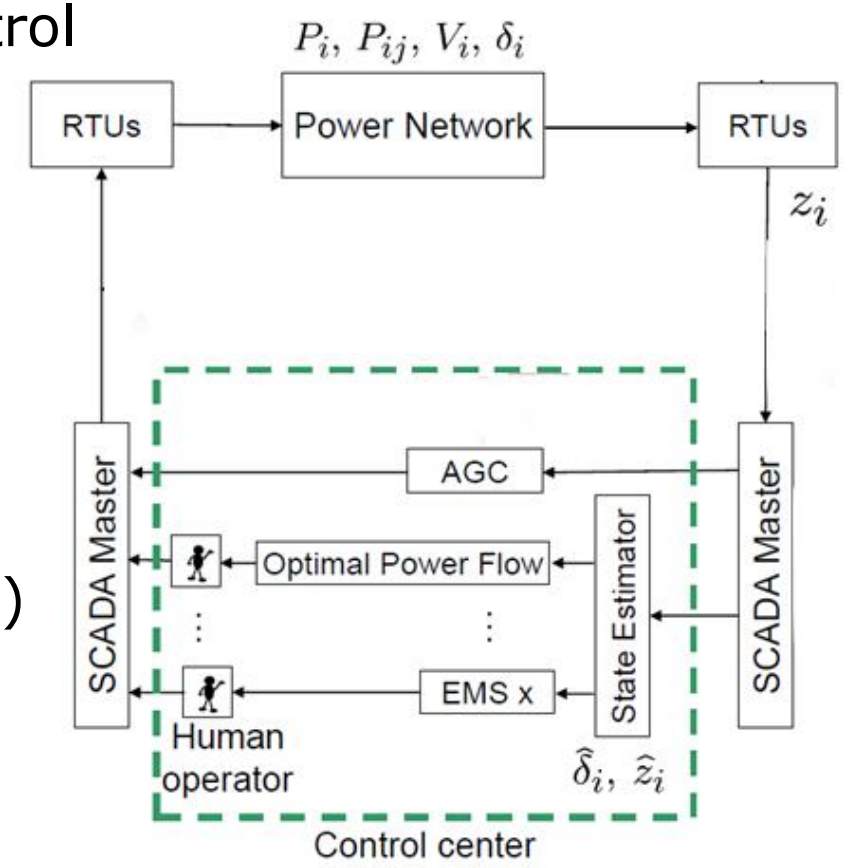
TCIPG Seminar Series

7 December 2012

Supervisory Control and Data Acquistion (SCADA)

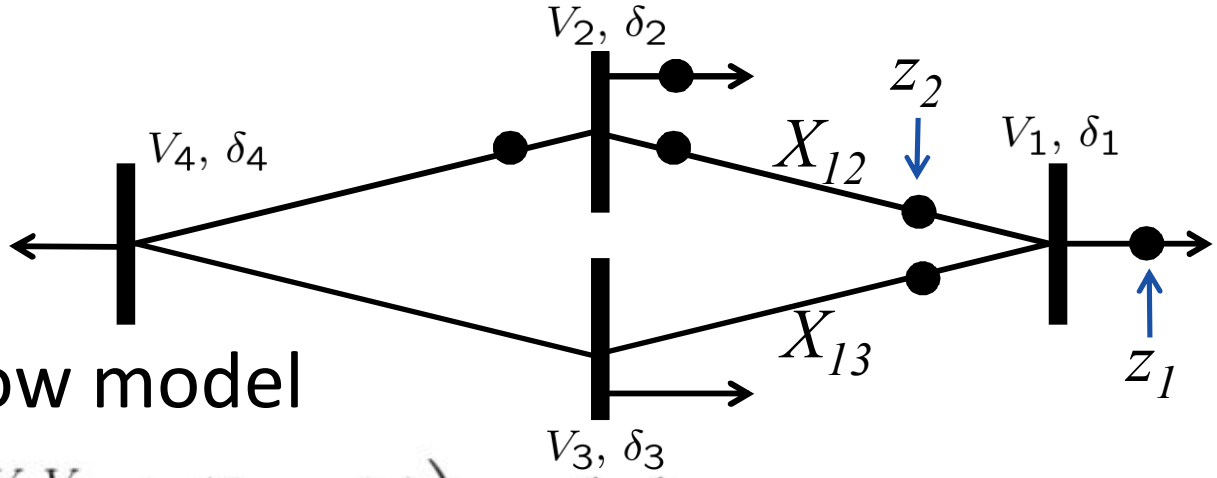
- Computerized monitoring and control
  - Real-time data acquisition
    - Metering
      - Voltage, current, power
    - Status information
      - Breakers
  - Control

- Energy Management System (EMS)
  - Short circuit calculation
  - Contingency analysis
  - Optimal power flow
  - ...
  - *State estimation*



A. Teixeira et al, ``Optimal Power Flow: Closing the Loop over Corrupted Data,'' *in Proc. of American Control Conference (ACC), Jun. 2012*
L. Xie et al, "False Data Injection Attacks in Electricity Markets," *in Proc. of IEEE SmartGridComm, Oct. 2010*

Model-based State Estimation



- Steady-state power flow model

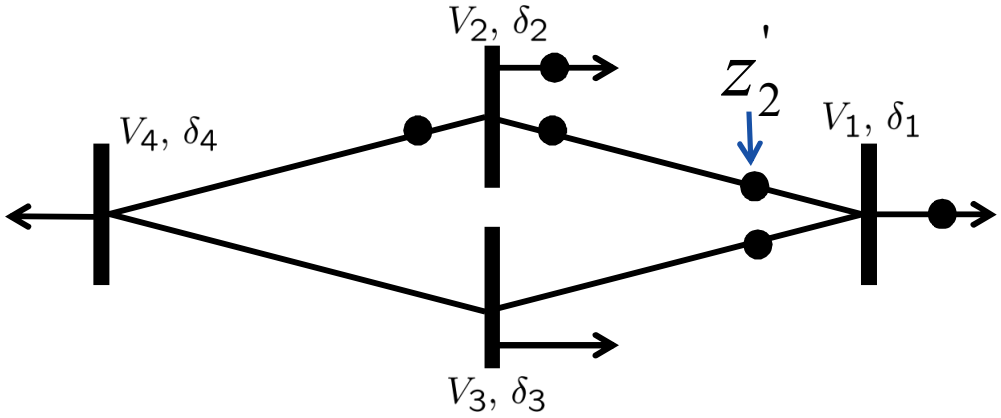
$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} \frac{V_1 V_2}{X_{12}} \sin(\delta_1 - \delta_2) + \frac{V_1 V_3}{X_{13}} \sin(\delta_1 - \delta_3) \\ \frac{V_1 V_2}{X_{12}} \sin(\delta_1 - \delta_2) \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = h(x) + e \in \mathbb{R}^m$$

- Estimation of phase angles δ_i,($\hat{x}$ vector) based on (z)
  - Weighted Least Squares (WLS) estimation
  - *Gauss-Newton* algorithm

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

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

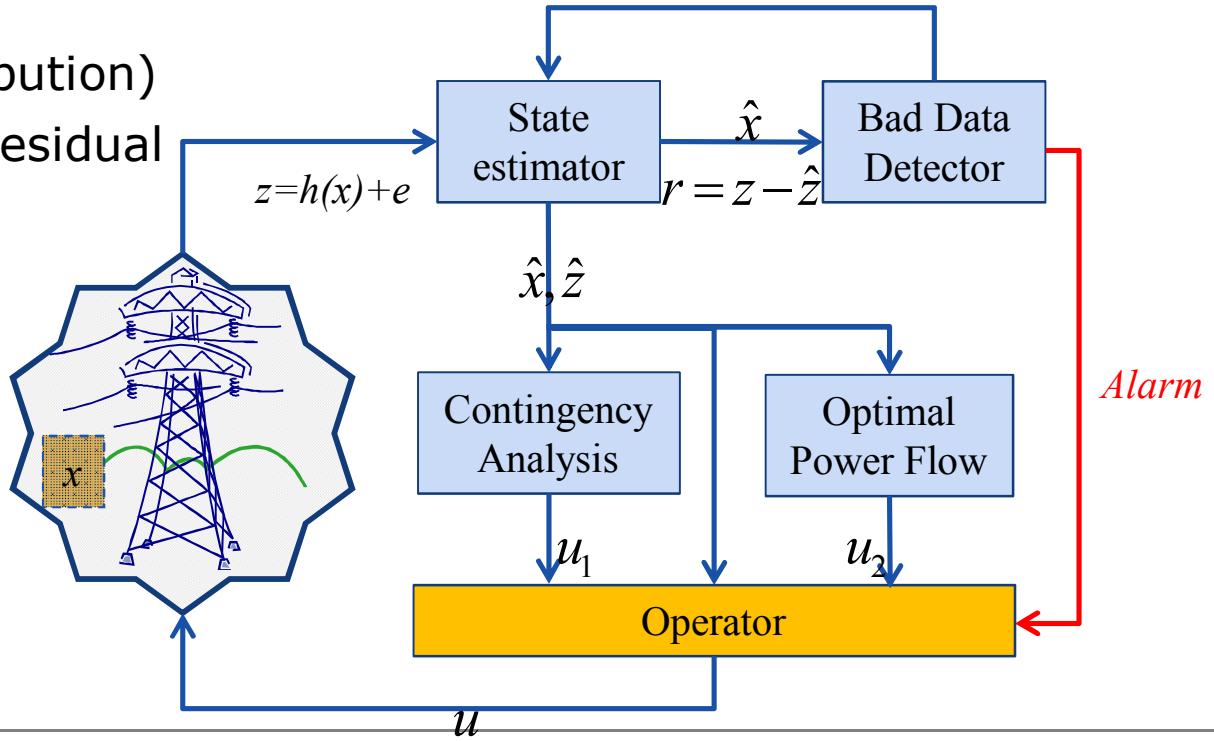
Bad Data Detector (BDD)



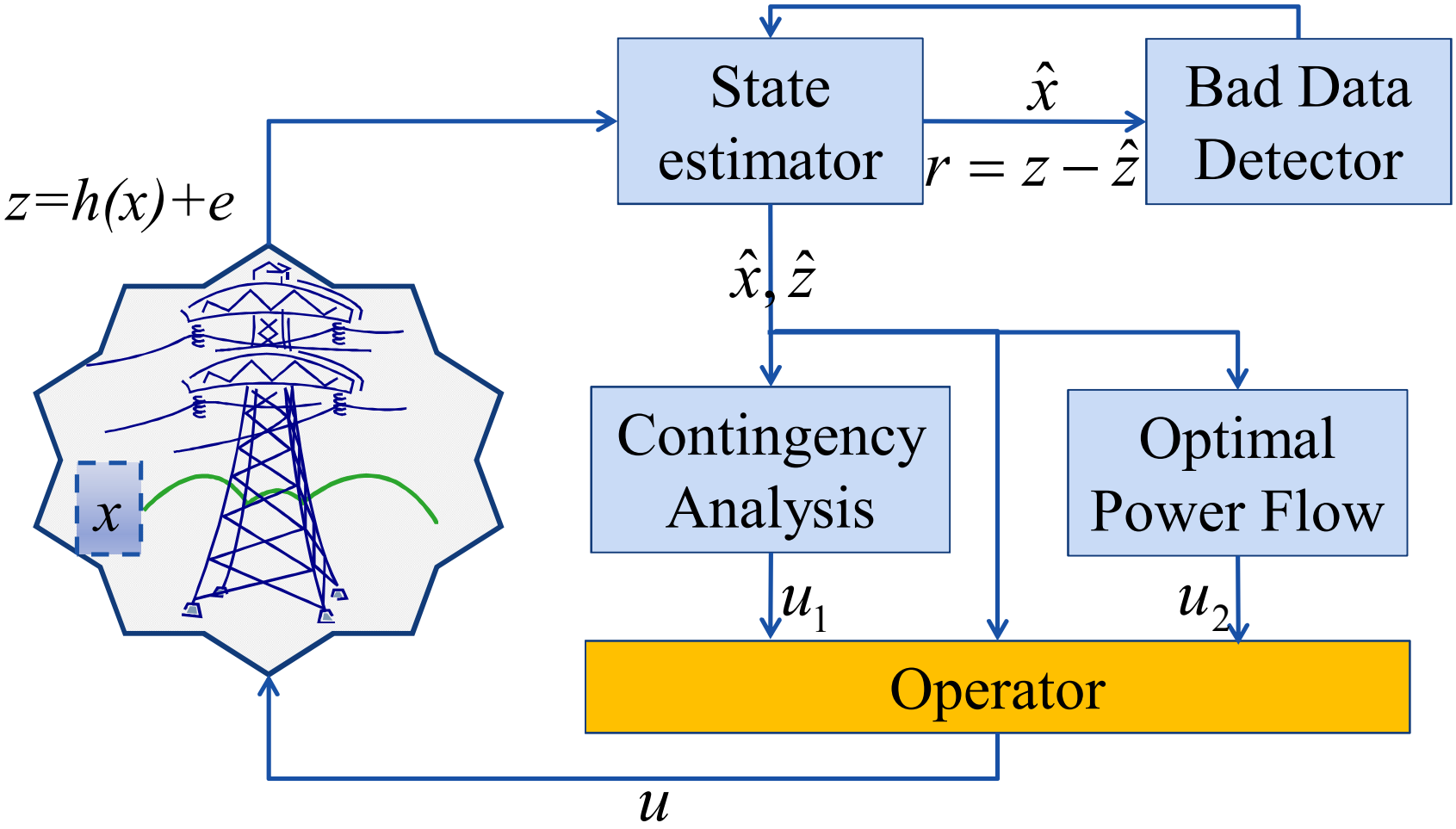
- Measurement residual

$$r := z - \hat{z} = h(x) + e - h(\hat{x})$$

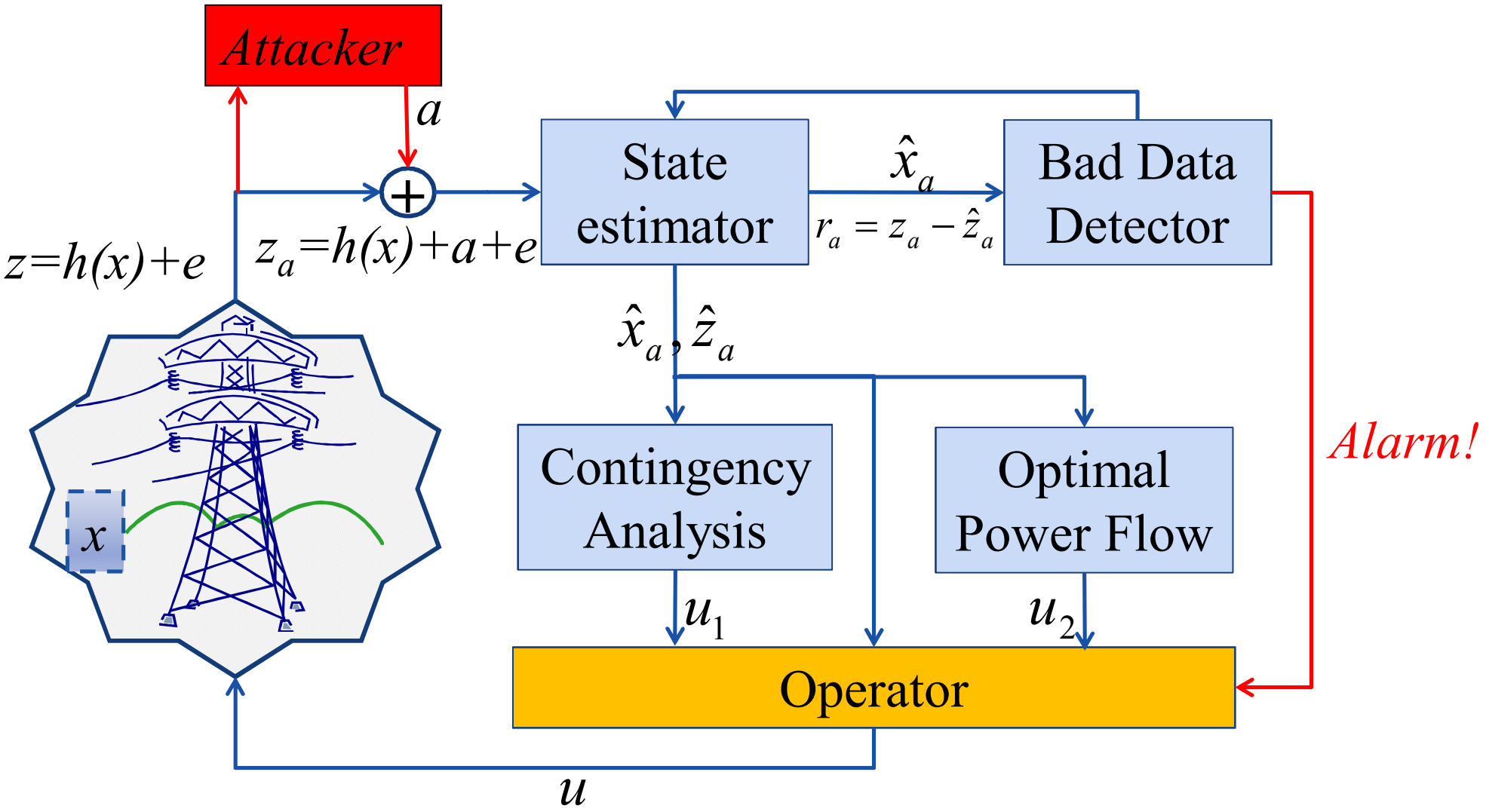
- Hypothesis testing
  - H0: Random measurement noise
  - Various methods
    - χ^2 test (Normal distribution)
    - Maximum normalized residual
- BDD alarm



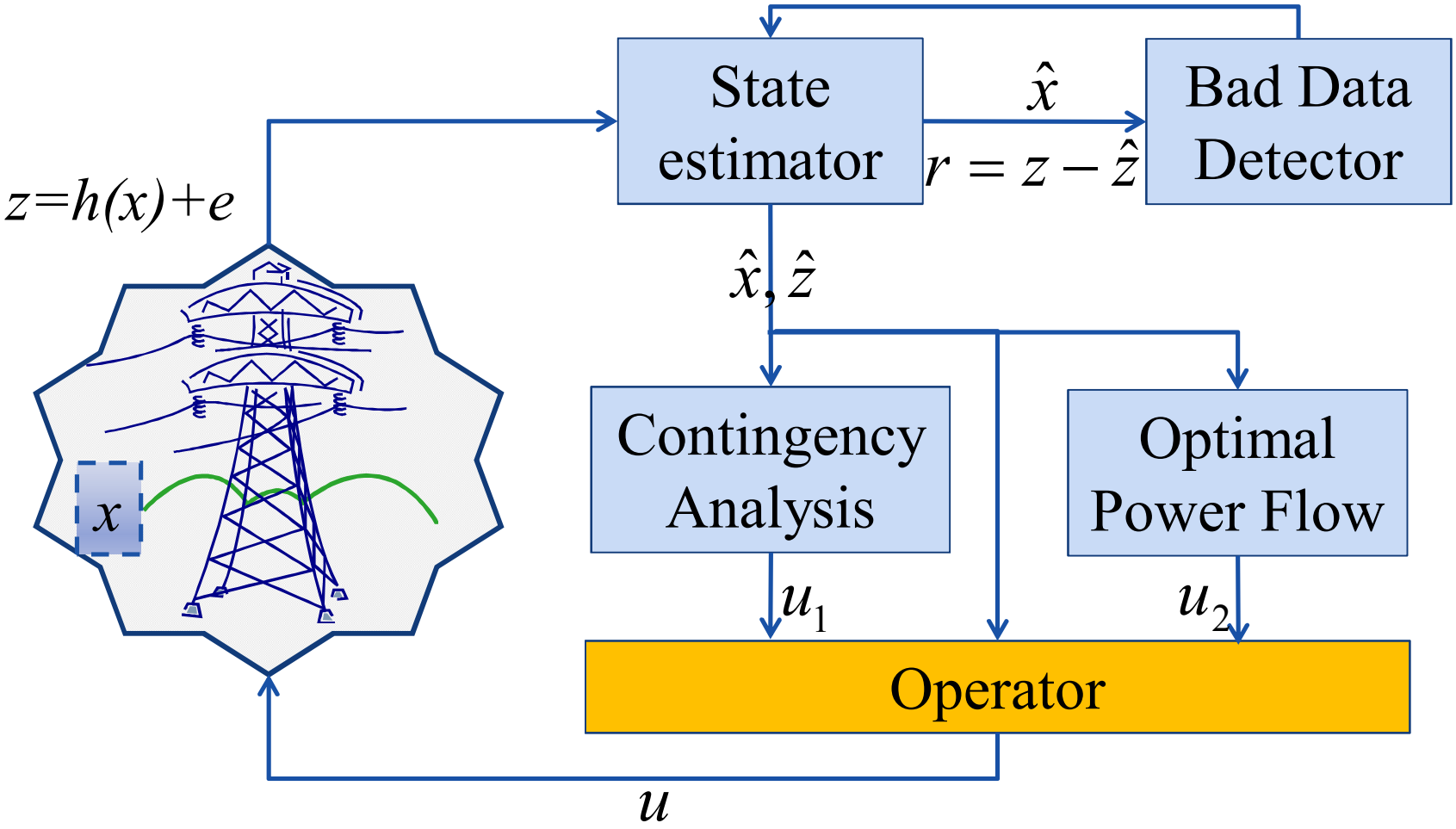
State Estimator and BDD



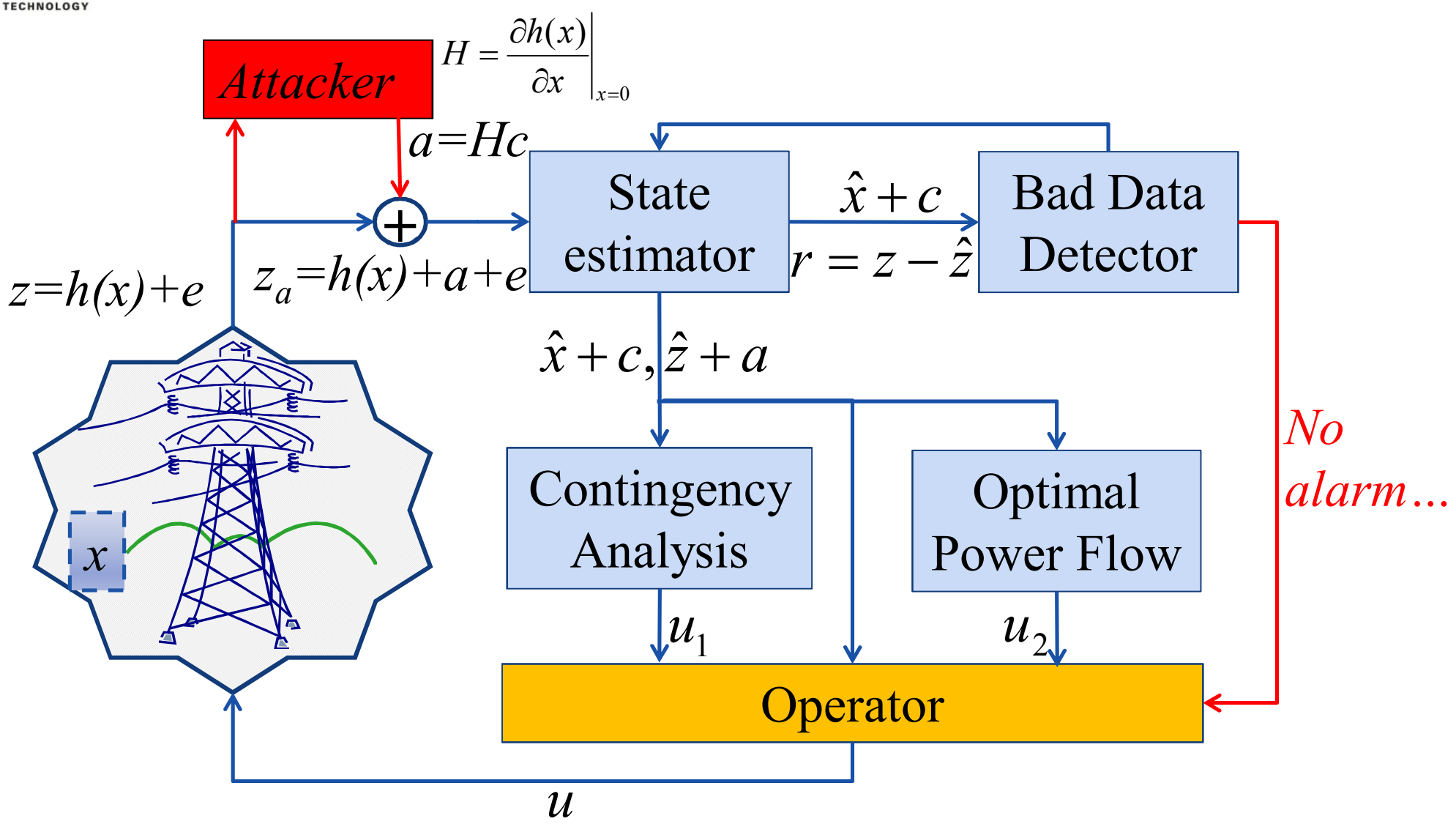
Naïve Attack on the State Estimator



State Estimator and BDD



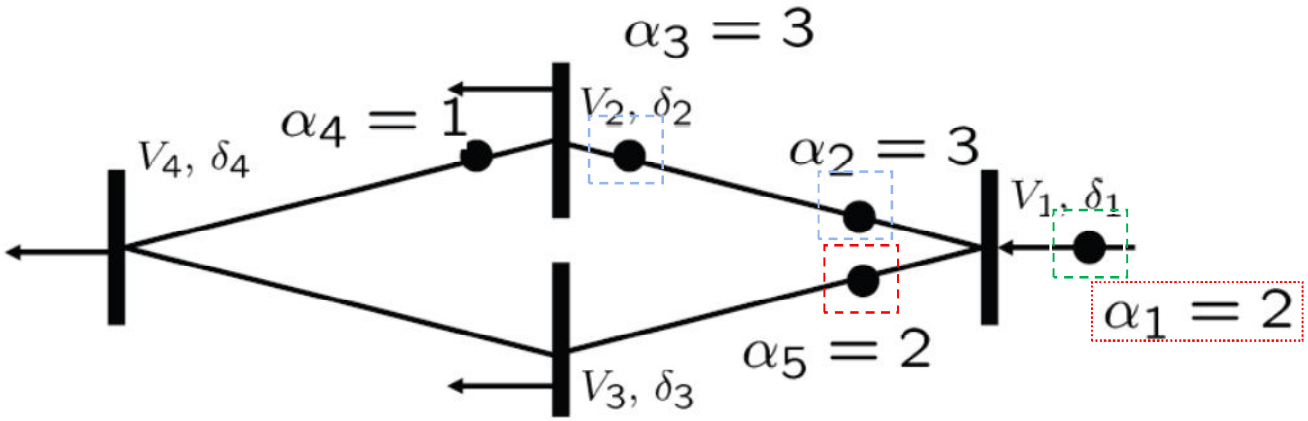
Stealth Attack on the State Estimator



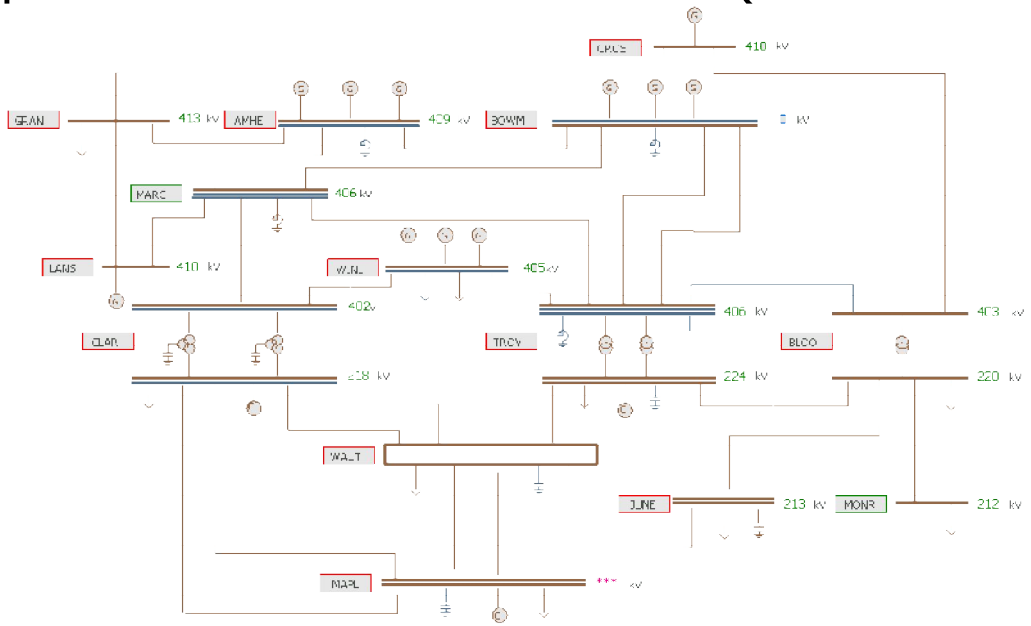
Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM CCS*, 2009, pp. 21–32.

Two Examples

- Simple network



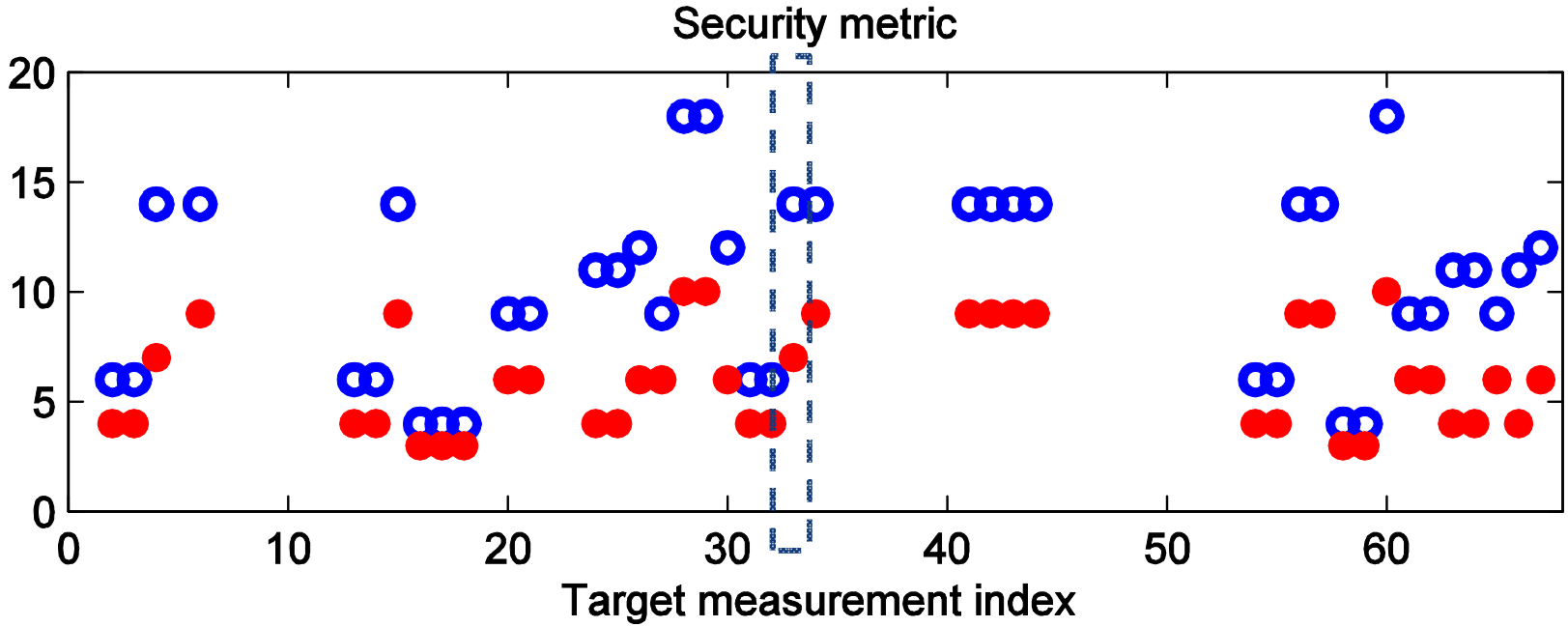
- 40 bus training network
  - Real and pseudo measurement data (66 measurement points)



Minimum Effort Stealth Attacks

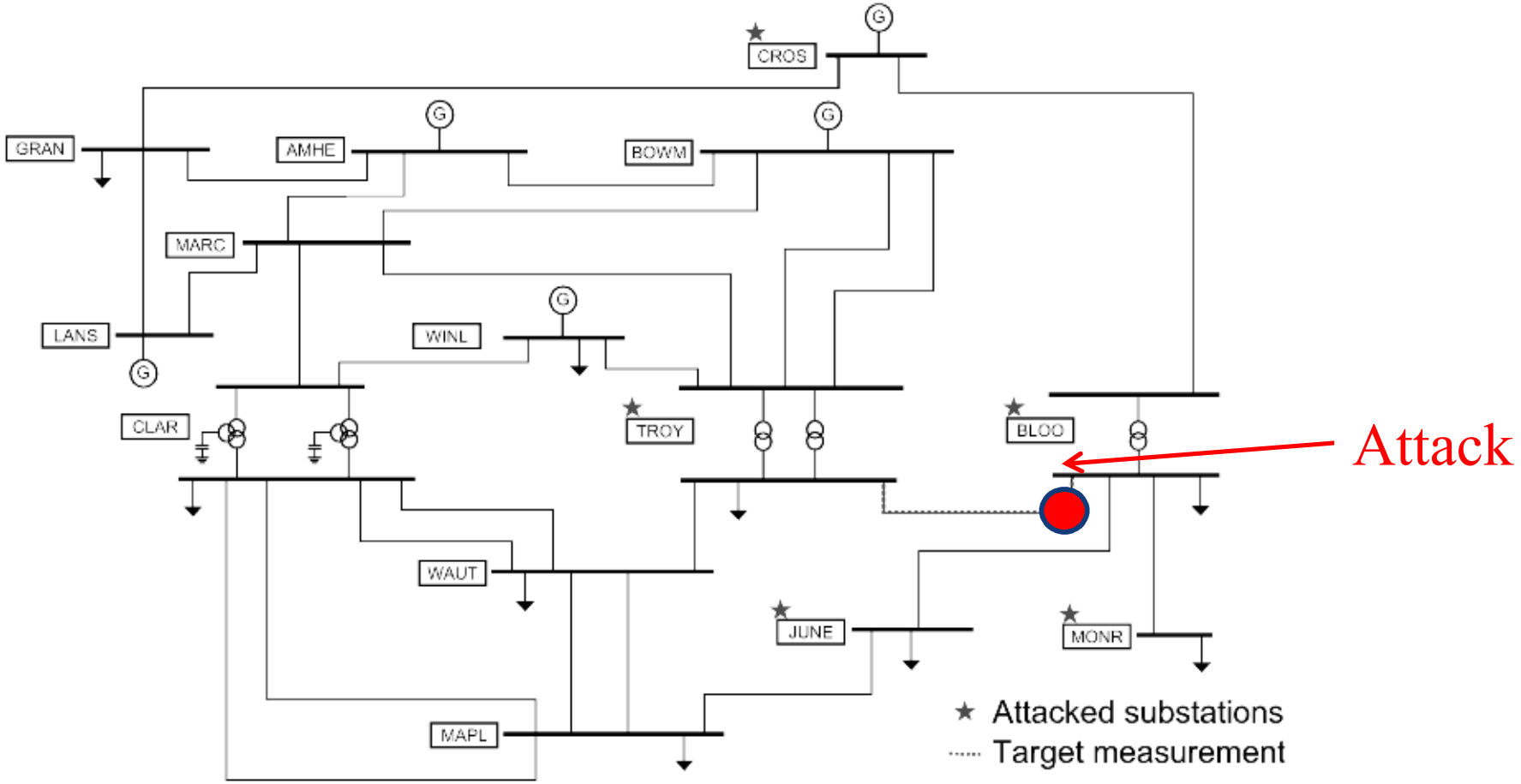
40 bus training network

- o: maximum metering redundancy
- •: actual metering redundancy



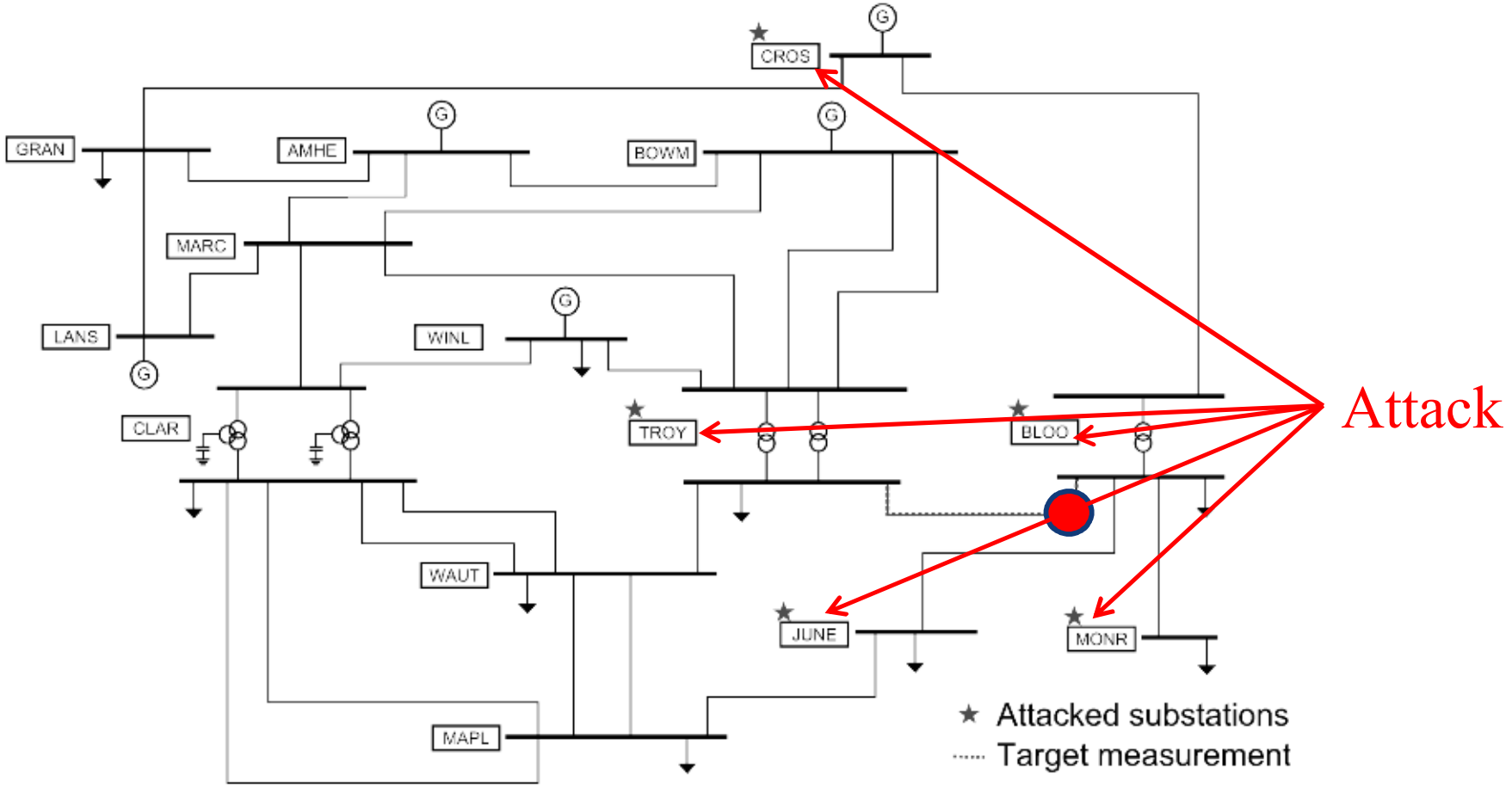
- Based on linear approximation
- Pseudo measurements unchanged

Specific Attack: „Naive”



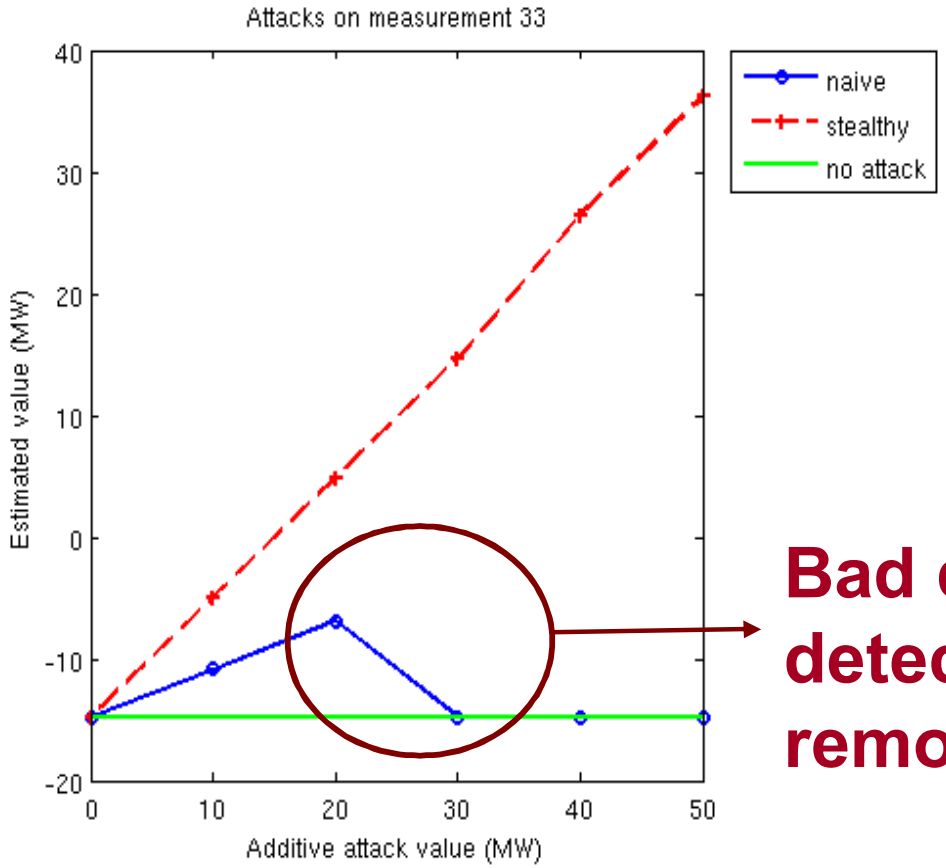
- Attack of transmission line (measurement 33)
- Manipulation of 1 measurement value at BLOO

Specific Attack: „Stealth”



- Attack of transmission line (measurement 33)
- Manipulation of 7 measurements at 5 substations

Experiment: „Stealthy" vs „Naive" Attack



Bad data detected & removed

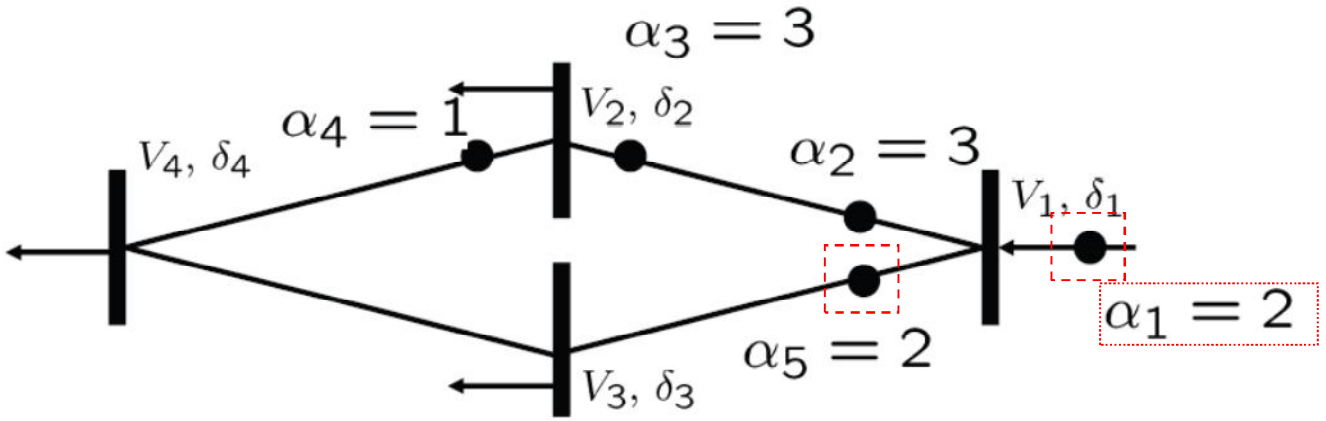
Target bias (MW)	Estimated value (MW)	# BDD Alarms
0	-14.8	0
50	36.2	0
100	86.7	0
150	137.5	0
200	Non convergent	-

- SCADA/EMS system
- Complete state estimator (active and reactive power)
- Attacked data written to SCADA database

Transmission line nom. rat.: 260 MVA

Teixeira et al, "A Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator," *in Proc. of IFAC World Congress, Aug. 2011*

Protection against „Stealth" Attacks



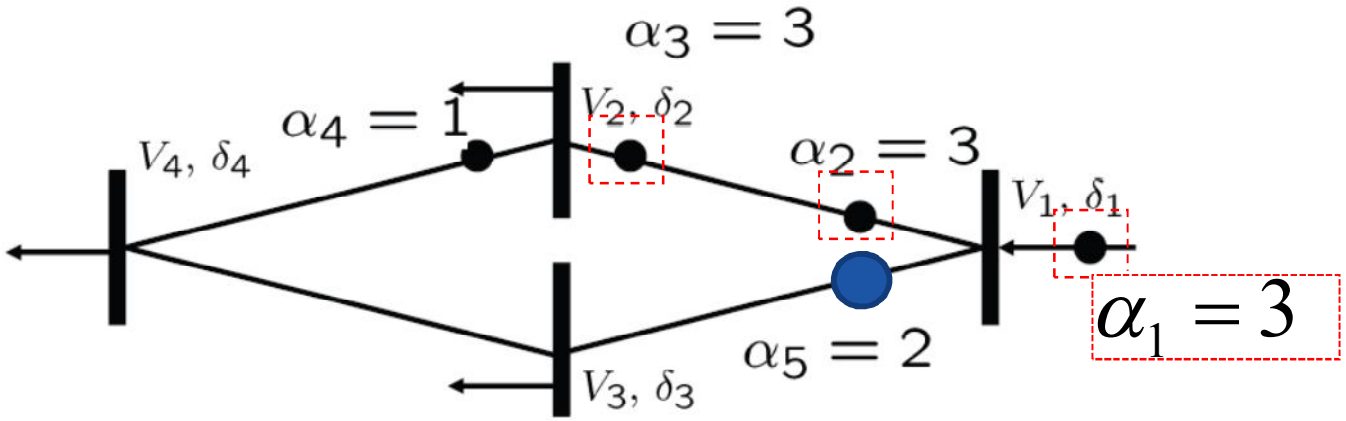
- Calculate the effort needed for attack
- Increase the effort needed for attack
  - Maximize attack cost for budget π

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

  - Make attacks impossible
    - Protection of at least *n* measurements

Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM CCS*, 2009, pp. 21–32.
R. Bobba et al, "Detecting false data injection attacks on DC state estimation," *in Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, 2010.*
G. Dán, H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," in Proc. of IEEE SmartGridComm, Oct. 2010

Protection against „Stealth” Attacks



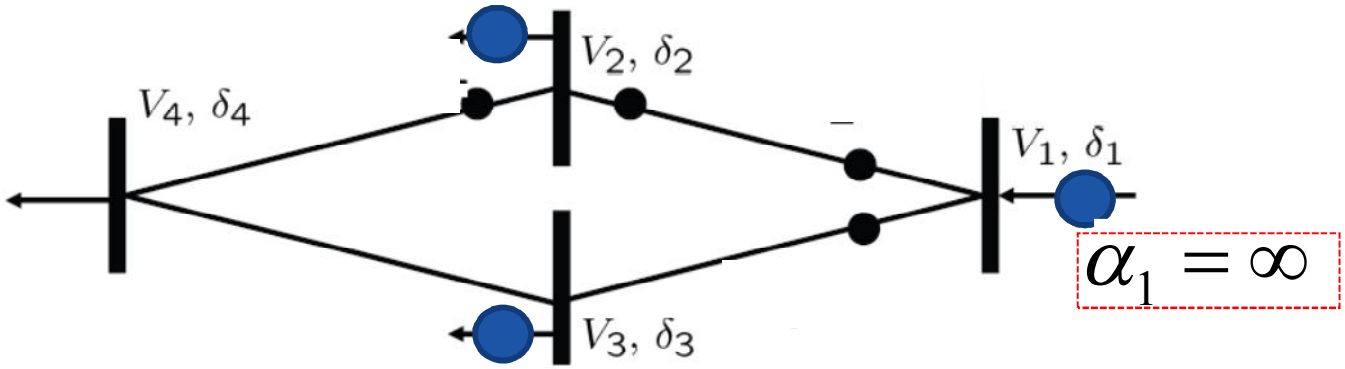
- Calculate the effort needed for attack
- Increase the effort needed for attack
  - Maximize attack cost for budget π

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

  - Make attacks impossible
    - Protection of at least *n* measurements

Y. Liu, P. Ning, and M. Reiter, “False data injection attacks against state estimation in electric power grids,” in *Proc. ACM CCS*, 2009, pp. 21–32.
R. Bobba et al, “Detecting false data injection attacks on DC state estimation,” *in Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, 2010.*
G. Dán, H. Sandberg, “Stealth Attacks and Protection Schemes for State Estimators in Power Systems,” in Proc. of IEEE SmartGridComm, Oct. 2010

Protection against „Stealth” Attacks



- Calculate the effort needed for attack
- Increase the effort needed for attack
  - Maximize attack cost for budget π

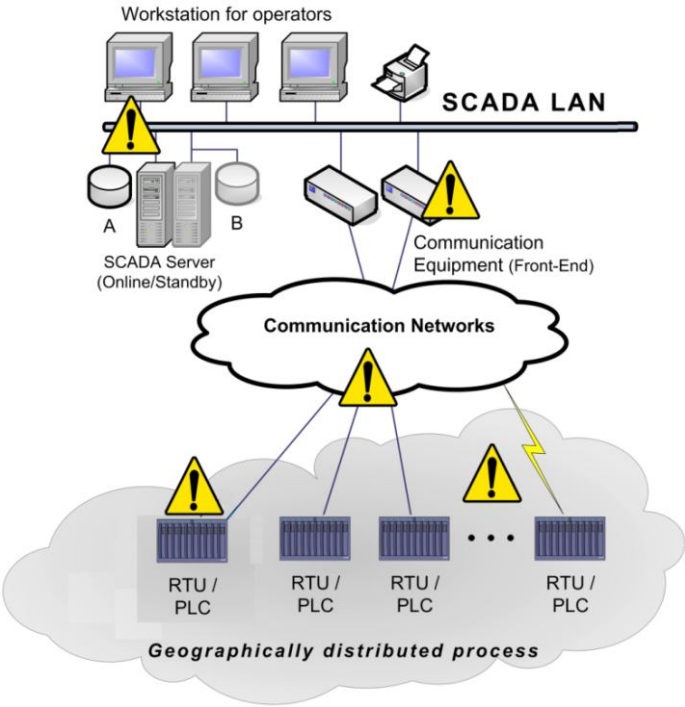
$$\mathrm{P}^{MM} = \arg \max_{\mathrm{P}:C_M(P)\leq\pi} \min_k \alpha_k$$

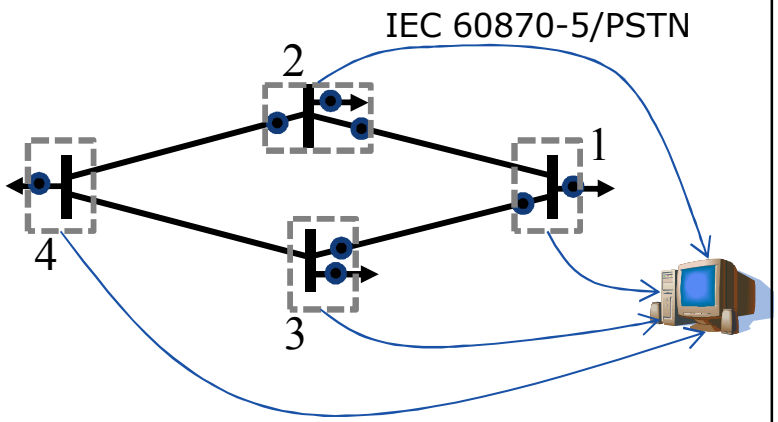
  - Make attacks impossible
    - Protection of at least *n* measurements
- Effort?

Y. Liu, P. Ning, and M. Reiter, “False data injection attacks against state estimation in electric power grids,” in *Proc. ACM CCS*, 2009, pp. 21–32.
R. Bobba et al, “Detecting false data injection attacks on DC state estimation,” *in Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, 2010.*
G. Dán, H. Sandberg, “Stealth Attacks and Protection Schemes for State Estimators in Power Systems,” in Proc. of IEEE SmartGridComm, Oct. 2010

SCADA Attack Surface and Costs

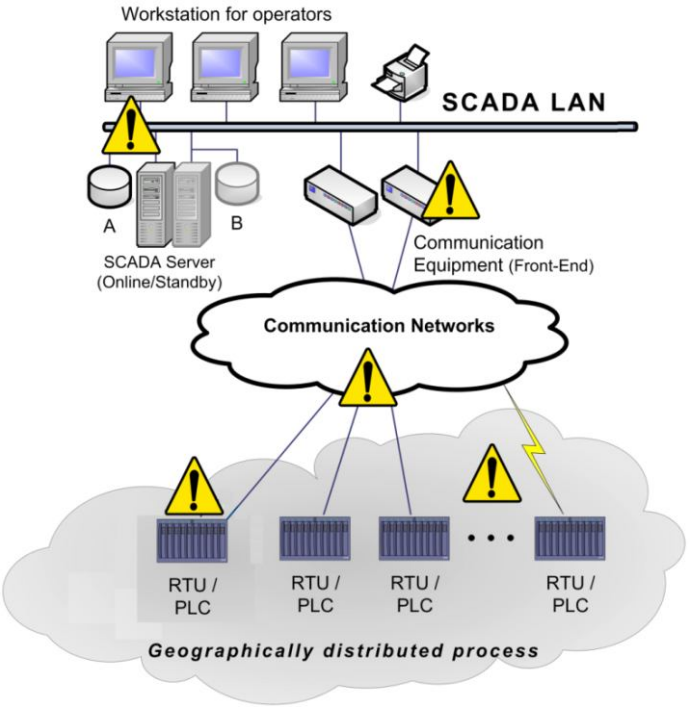
- Attack cost
  - Number of attacked infrastructure components
- Protection cost
  - Number of protected infrastructure components
    - Equipment upgrades
  - Key management
  - Performance implications
- Heterogeneous infrastructure
  - Point-to-point links (PSTN, leased line)
  - Multi-hop links (OPGW)

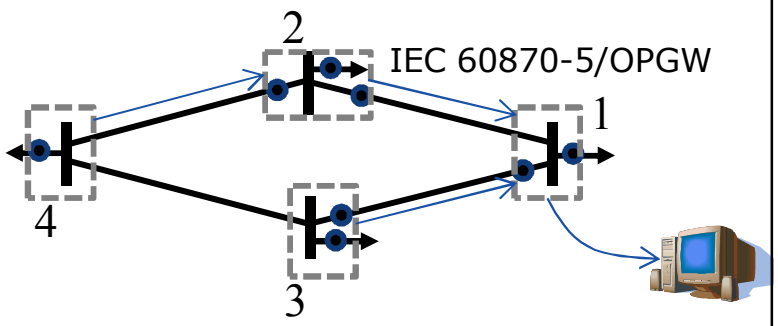




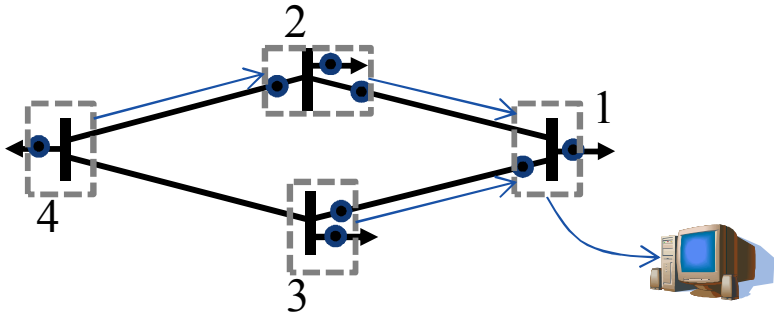
SCADA Attack Surface and Costs

- Attack cost
  - Number of attacked infrastructure components
- Protection cost
  - Number of protected infrastructure components
    - Equipment upgrades
  - Key management
  - Performance implications
- Heterogeneous infrastructure
  - Point-to-point links (PSTN, leased line)
  - Multi-hop links (OPGW)





Cyber-Physical Infrastructure Model



- $n+1$ buses
- Set of measurements M
- Set of substations S
  - Control center s_c
  - Measurement $m \in M$ taken at substation $S(m)$
- Communication system: undirected graph $G(S, E)$
- Set of established routes for substation $s \in S$

$$R_s = \{r_s^1, r_s^2, ..., r_s^{R(s)}\}, \quad r_s^i \subseteq S, \; s \in r_s^i, s_c \in r_s^i$$

  - $|R(s)| = 1$, all measurement data are sent over a single route to s_c
  - $|R(s)| > 1$, all data are split equally over $|R(s)|$ routes to s_c

O.Vuković et al., ``Network-aware Mitigation of Data Integrity Attacks on Power System State Estimation,'' *IEEE Journal on Selected Areas in Communications (JSAC), vol. 30, no. 6, July 2012*

Mitigation Schemes

- Bump-in-the-wire (BITW) authentication
  - $E \subset S$ set of substations that use BITW authentication
  - $\sigma_E(r_s^i)$ set of substations where data is susceptible to attack

$$s \in E,\ \sigma_E(r_s^i) = \{s\}$$

$$s \notin E,\ \sigma_E(r_s^i) = r_s^i$$

- Physical protection
  - Guards or video surveillance
  - $P \subseteq S,\ s_c \in P$

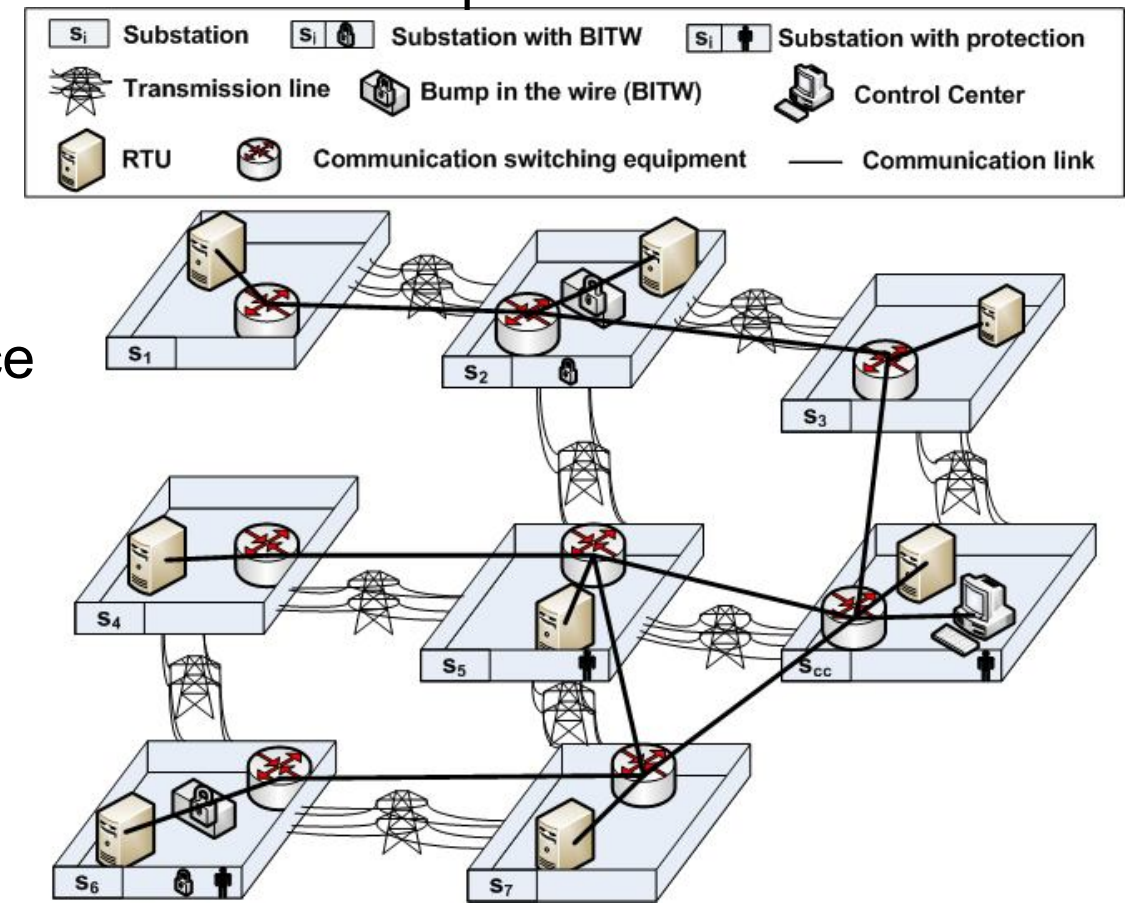
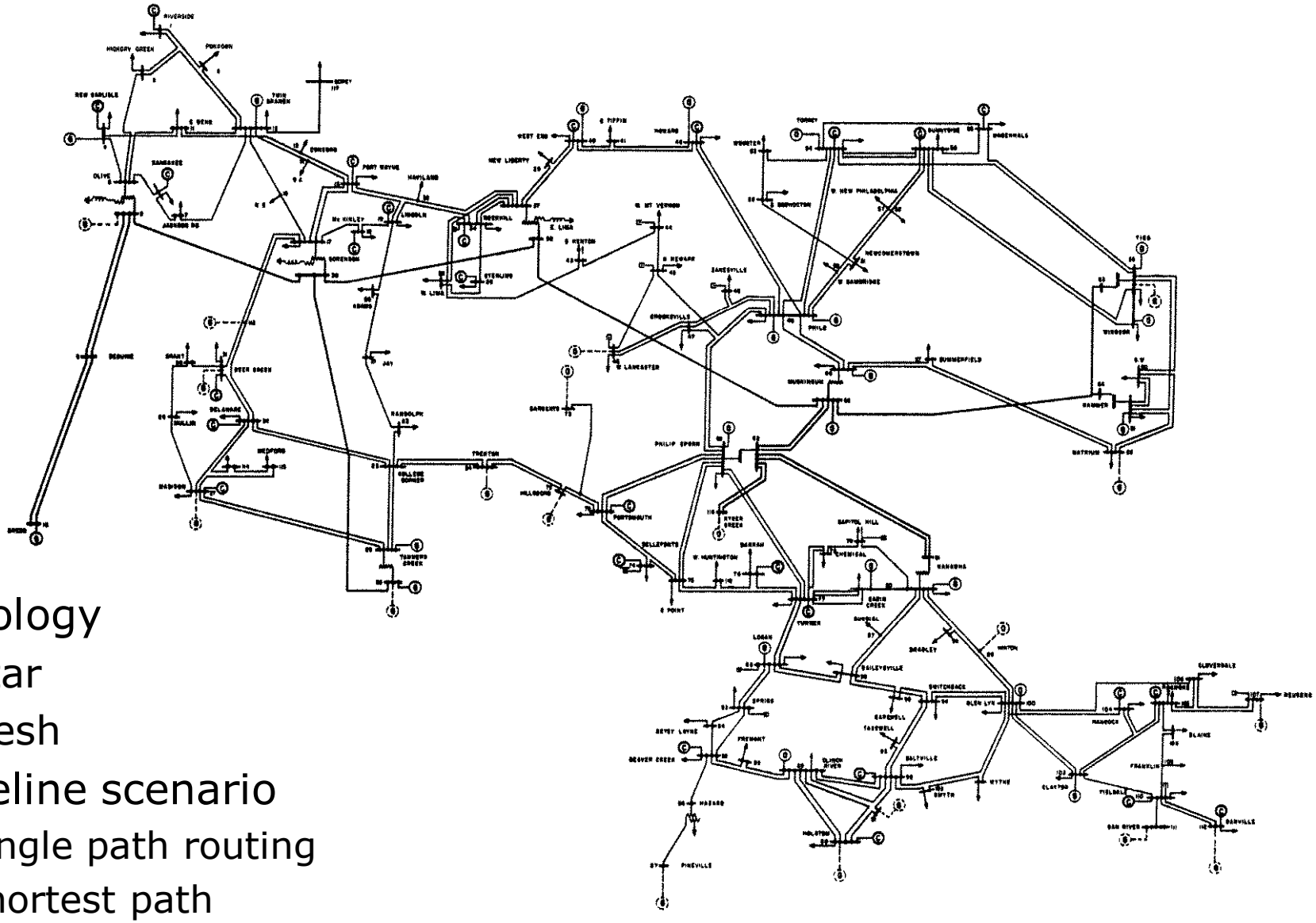


Illustration: IEEE 118 Bus Network



- Topology
  - Star
  - Mesh
- Baseline scenario
  - Single path routing
  - Shortest path

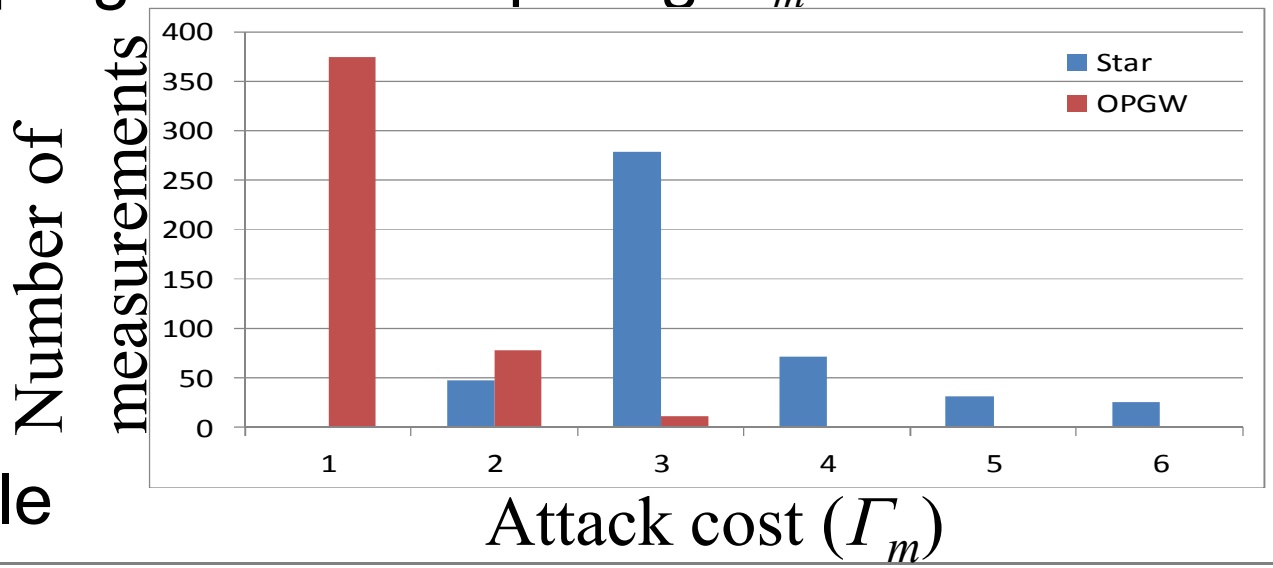
Security Metrics: Measurement Attack Cost

- Γ_m - minimum number of substations to be attacked in order to perform a stealth attack against measurement m

$$\Gamma_m = \min_{\omega \subseteq S; \omega \cap P = 0} |\omega| \quad \text{s.t. } \exists a, c \;\; a = Hc, \;\; a(m) = 1 \;\; \text{and}$$

$$a(m') \neq 0 \Rightarrow \omega \bigcap \sigma_E(r^i_{S(m')}) \neq 0, \forall r^i_{S(m')} \in R_{S(m')}$$

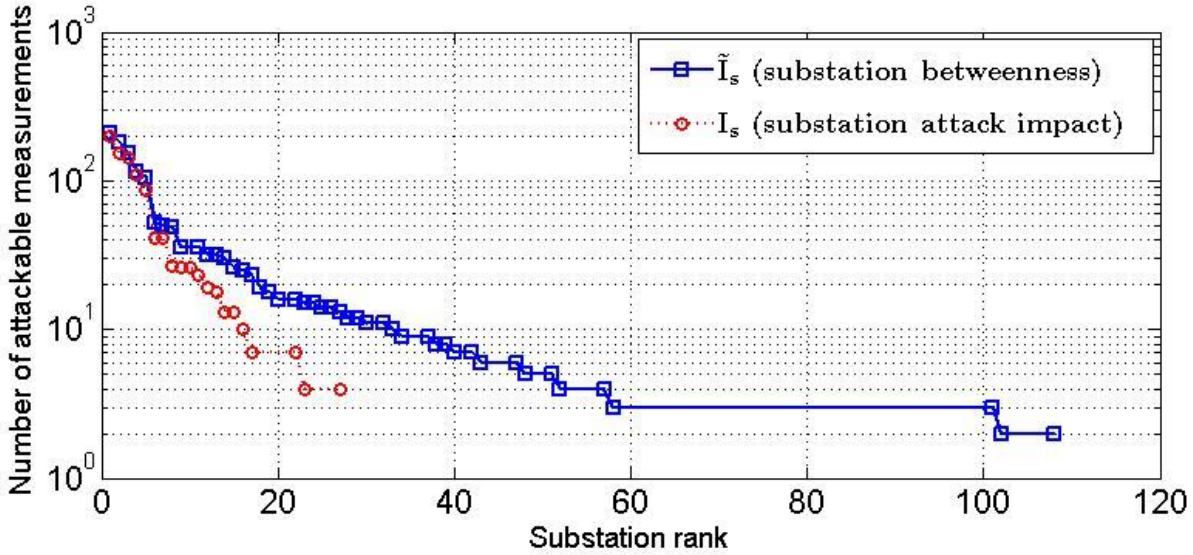
- Mixed Integer Linear program for computing Γ_m



- OPGW more vulnerable

Security Metrics: Substation Attack Impact

- I_s - number of measurements that can be stealthily attacked at substation s $\quad \forall s \in P \;\; I_s = 0$
- Efficient (O(M³)) algorithm for computing I_s
- Comparison with (substation) betweenness centrality
  - Single shortest-path routing, $|R_s| = 1 \; \forall s, E = \emptyset, P = \{s_c\}$



- Attack impact up to 40% of measurements

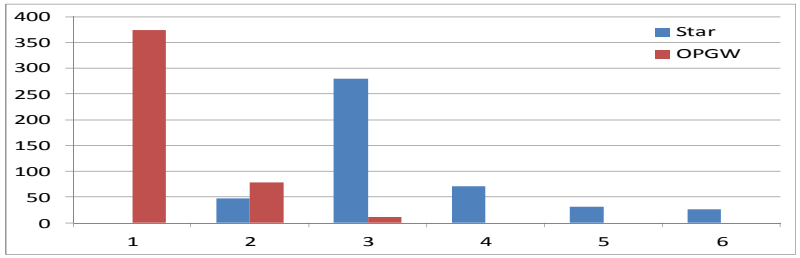
Mitigation Against Attacks

- Improve the most vulnerable part of the system
  - Minimize $\max_{\forall s \in S} I_s$ or maximize $\min_{\forall m \in M} \Gamma_m$
- Multi-objective optimization problem
  - Objective γ : minimize number of measurements with attack cost γ

$$\min\left|\{m \mid \Gamma_m = \gamma\}\right|$$

  - Objectives are ordered, objective γ has priority over objective $\gamma' > \gamma$
  - Lexicographical minimization

$$\underset{P,E,R}{\text{lexmin}}\ w(P,E,R), \quad \mathrm{w}_\gamma = \left|\{m \mid \Gamma_m = \gamma\}\right|$$



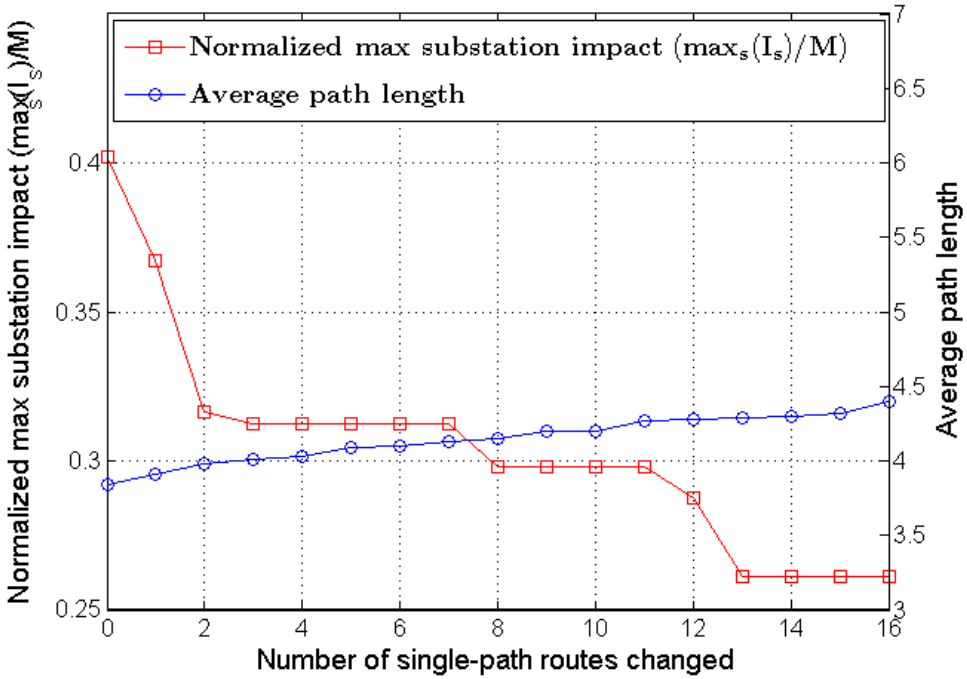
Algorithm for Mitigation

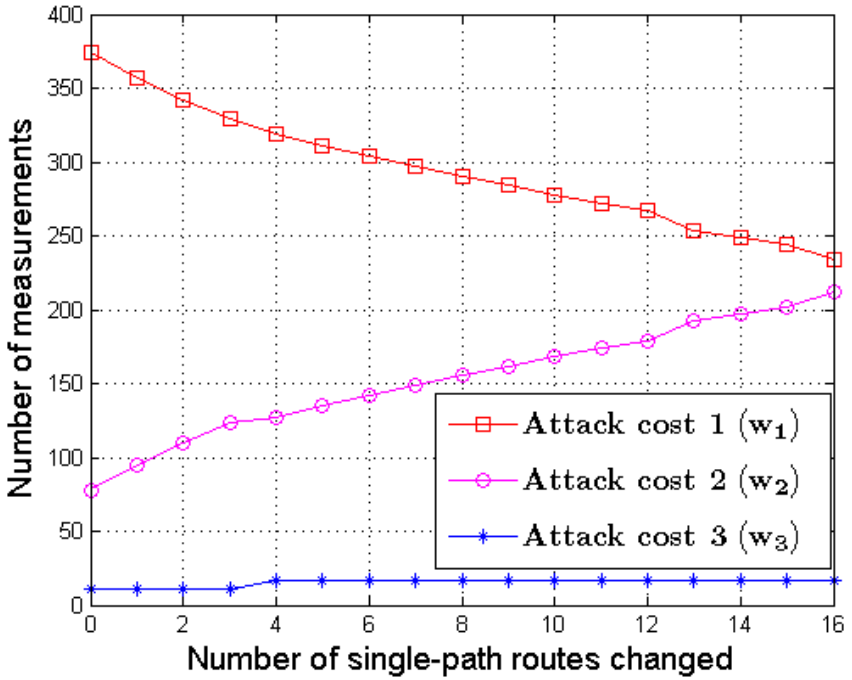
- Critical Substation First algorithm
  - Iterative algorithm
  - In each iteration
    - Identify *critical* substations
    - For every *critical* substation create alternate mitigation schemes
    - Calculate $\Gamma_m^{'}$ assuming the alternate mitigation schemes
    - Apply the mitigation scheme that improves Γ_m the most
- Mitigation schemes
  - Modified single-path routing
  - Multi-path routing
  - Data authentication (Tamper-proof and BITW)
  - Protection

O.Vuković et al., ``Network-aware Mitigation of Data Integrity Attacks on Power System State Estimation,'' *IEEE Journal on Selected Areas in Communications (JSAC), vol. 30, no. 6, July 2012*

Numerical Results

- Modified single-path routing – simple but efficient

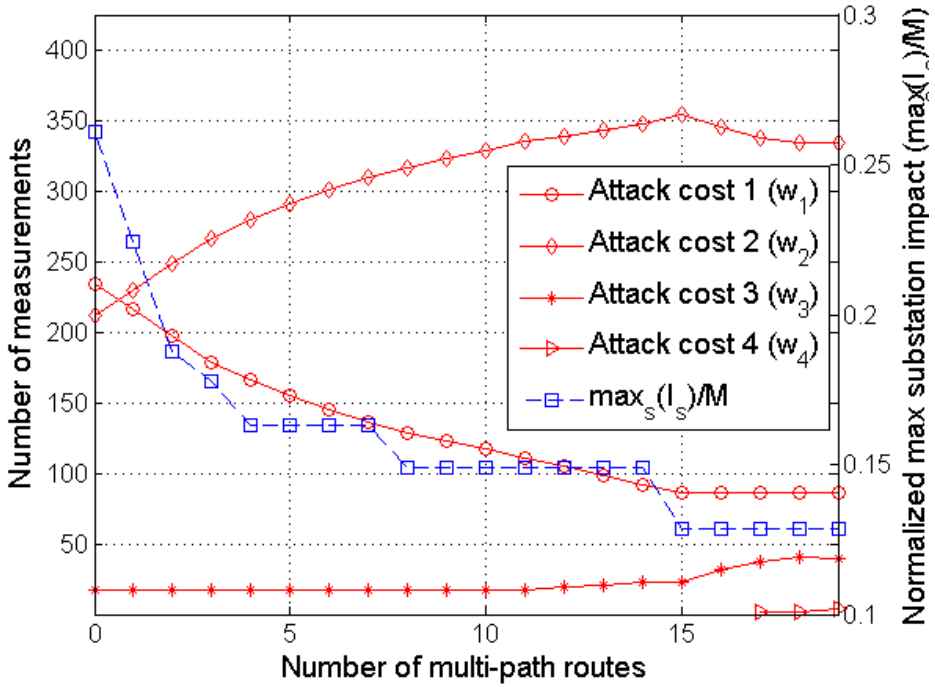




- 40% decrease of the maximum attack impact
- Increased attack cost for 50% of measurements

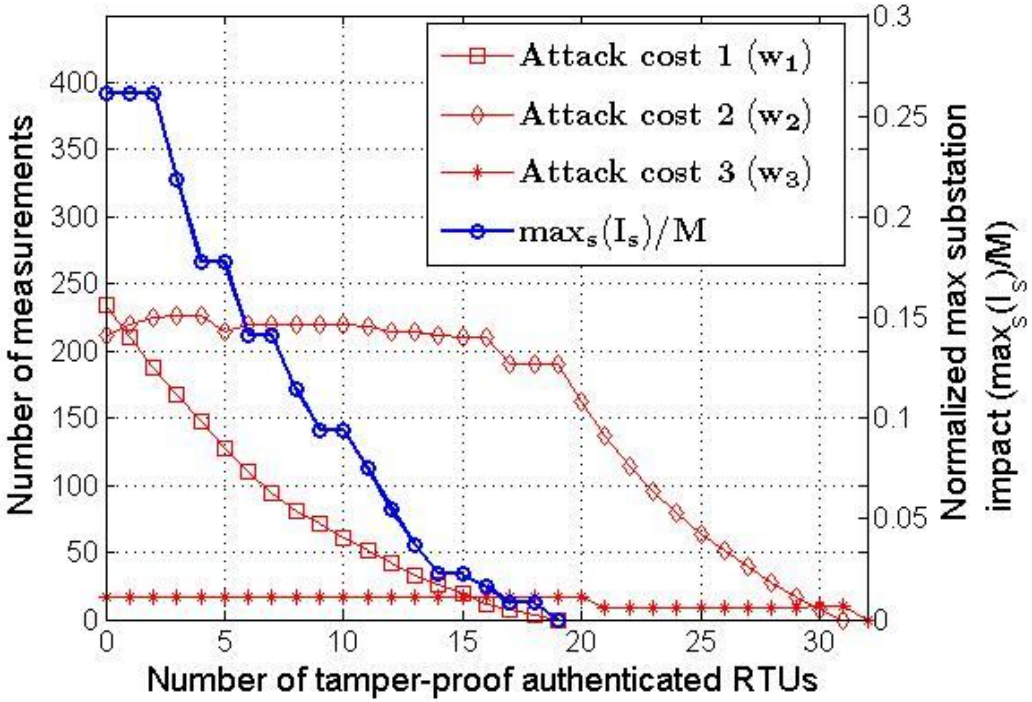
Numerical Results

❑ Multi-path routing



- $\Gamma_m \geq 2$ for most measurements
- Decreases $\max_{\forall s \in S} I_s$ by 50%

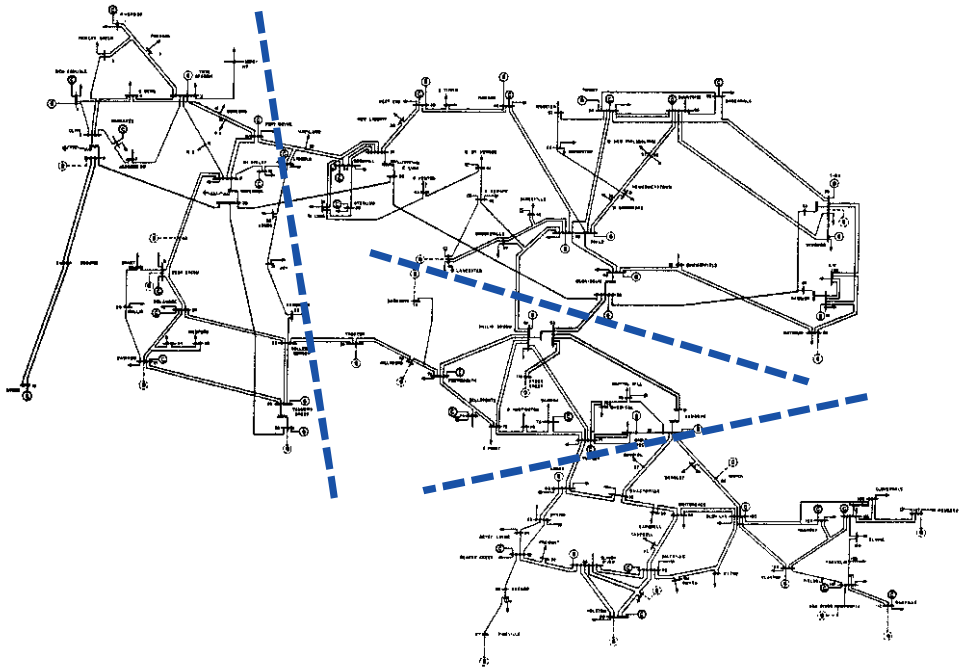
❑ Authentication



- $\Gamma_m > 1, \forall m$
- Dominating set to mitigate attacks (<< *n*) !!!

Multi-area State-Estimation

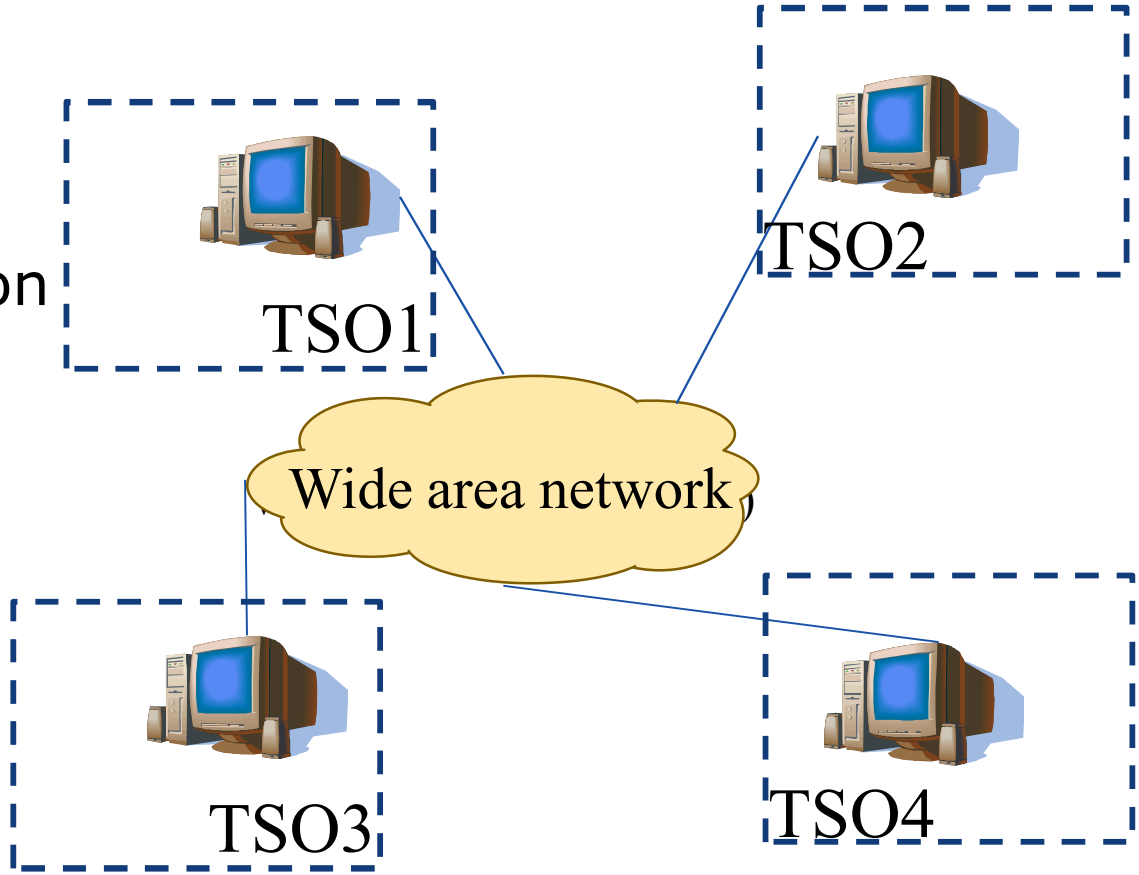
- Interconnected systems
  - No central authority
- Distributed state estimation
  - Protect sensitive data
  - Fully distributed
  - Inter CC communication
    - ICCP over TCP/IP
- Data integrity attack
  - Compromise CC
  - Manipulate data to disturb estimation
    - Avoid or delay convergence



O.Vuković , G. Dán `` On the Security of Distributed Power System State Estimation under Targeted Attacks,'' *ACM Symposium on Applied Computing, Mar. 2013*

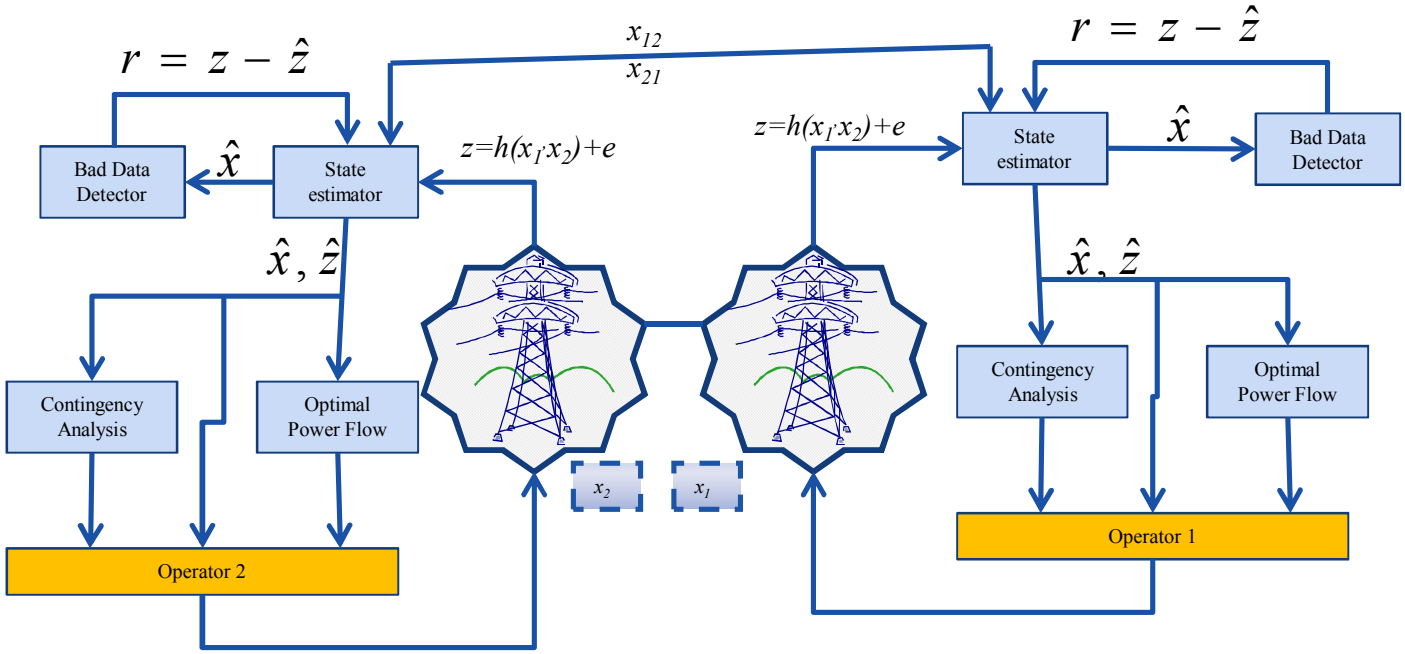
Multi-area State-Estimation

- Interconnected systems
  - No central authority
- Distributed state estimation
  - Protect sensitive data
  - Fully distributed
  - Inter CC communication
    - ICCP over TCP/IP
- Data integrity attack
  - Compromise CC
  - Manipulate data to disturb estimation
    - Avoid or delay convergence



O.Vuković , G. Dán `` On the Security of Distributed Power System State Estimation under Targeted Attacks,'' *ACM Symposium on Applied Computing, Mar. 2013*

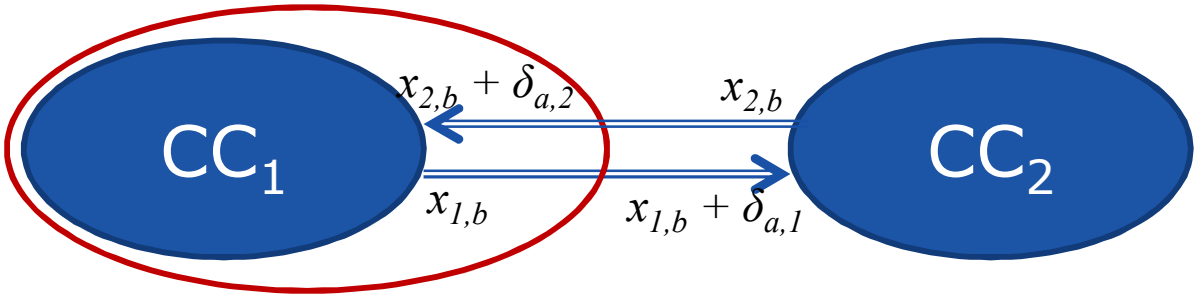
Distributed State Estimation



- Periodic exchange of border state variables
  - Several algorithms available
- Convergence to consistent state estimate
- Iterative algorithm

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

Border Bus Phase Angle Attack



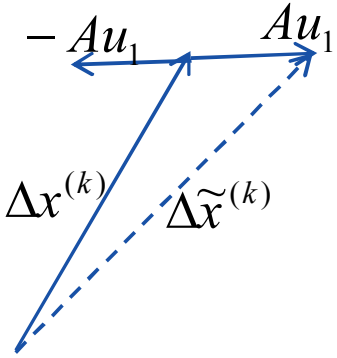
- Iteration under attack

$$x^{(k+1)} = x^{(k)} + \Delta\tilde{x}^{(k)} \neq x^{(k)} + \Delta x^{(k)}$$

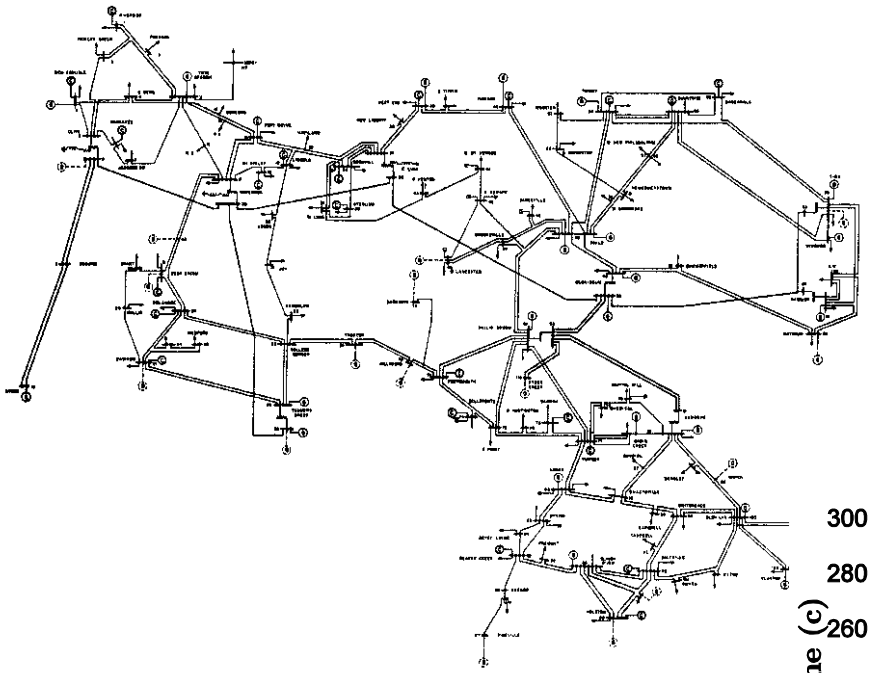
- Attacker chooses $\delta_{a,2}$ to maximize $\| \Delta\tilde{x}^{(k)} \|$
  - Under constraint on $||\delta_{a,2}||$
- First singular vector attack (model/state-aware)

$$\Delta\tilde{x}^{(k)} \approx \Delta x^{(k)} - \underbrace{[H^{(k)T} W^{-1} H^{(k)}]^{-1} H^{(k)T} W^{-1} H_b^{(k)}}_{A} \delta_a$$

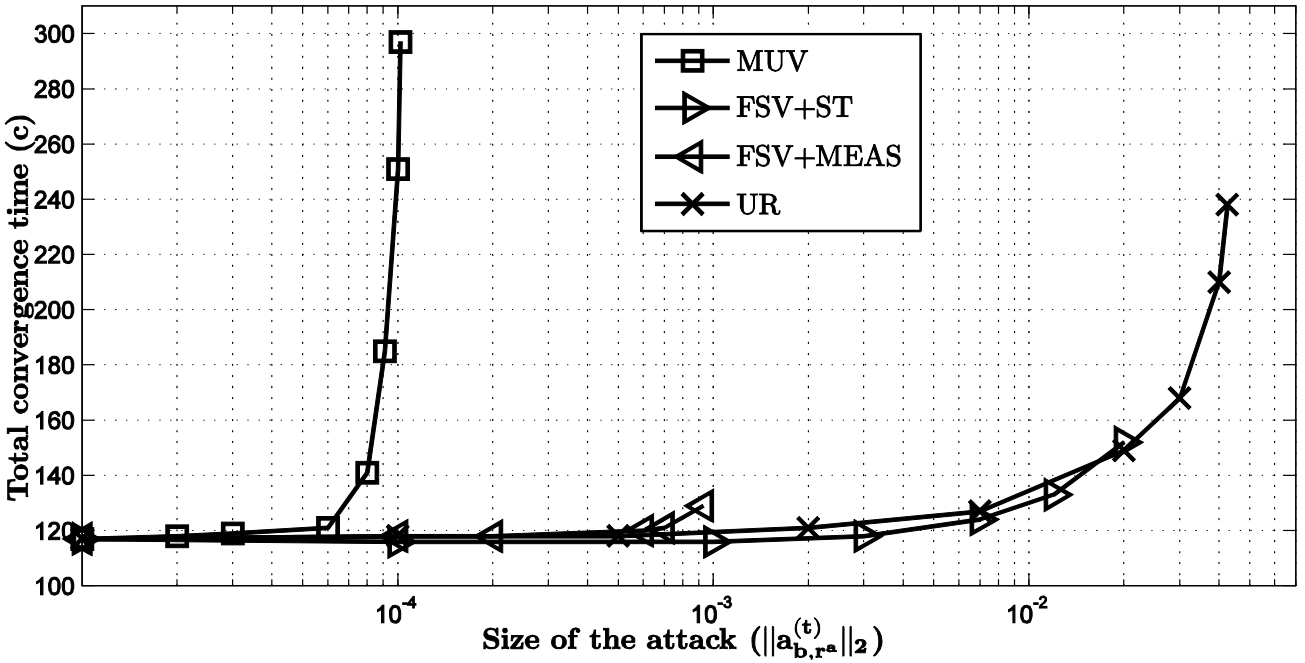
  - $\delta_a = u_1$ (First singular vector of A)
- Attacker needs information
  - H matrix and system state
  - Power flow measurements – direction ($\pm$)



Attack Impact: Convergence Time

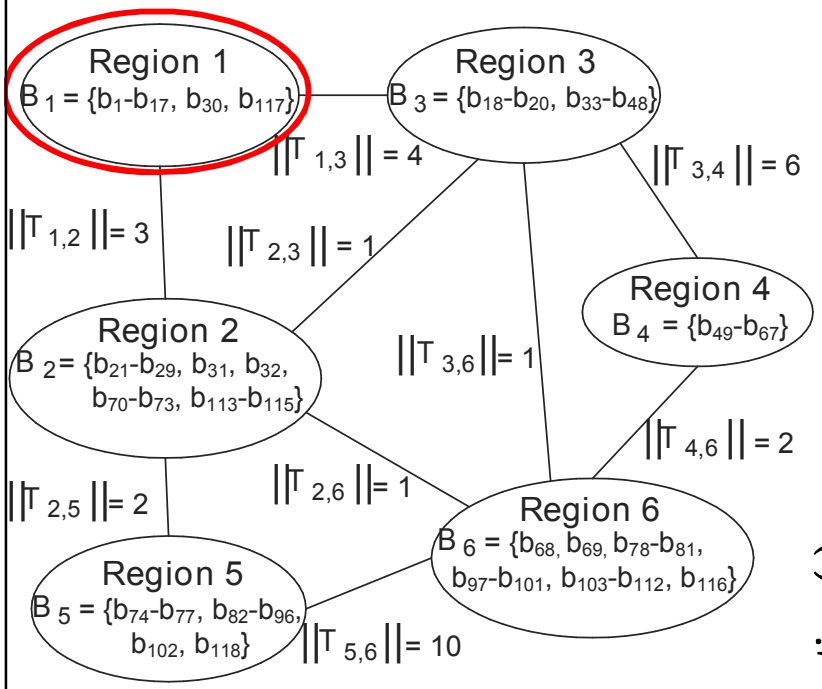


- IEEE 118 bus system 6 regions
- Attacker compromises Area 1
- Attack strategies
  - MUV: Maximum update every iteration
  - FSV: First singular vector
  - UR: Uniform rotation

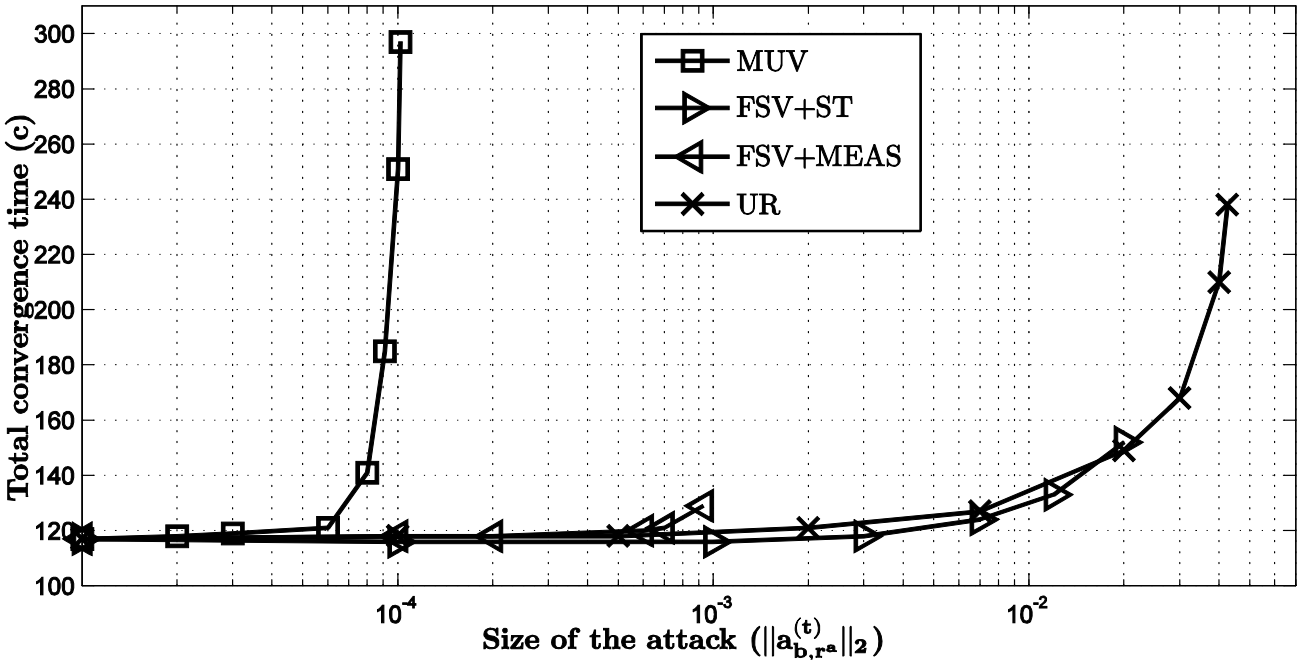


- Attack strategy crucial
- Field measurement data important for powerful attack (FSV+MEAS)

Attack Impact: Convergence Time

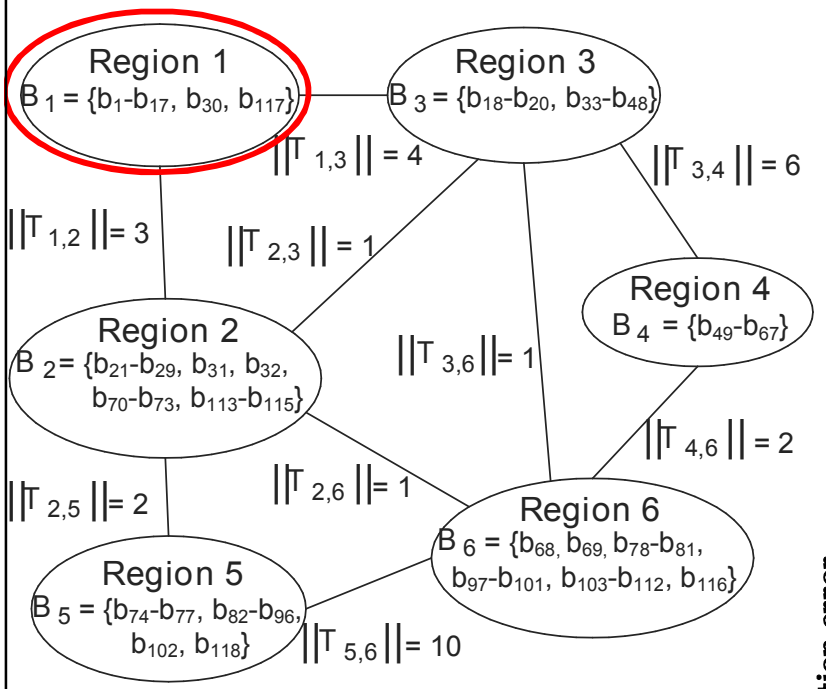


- IEEE 118 bus system 6 regions
- Attacker compromises Area 1
- Attack strategies
  - MUV: Maximum update every iteration
  - FSV: First singular vector
  - UR: Uniform rotation

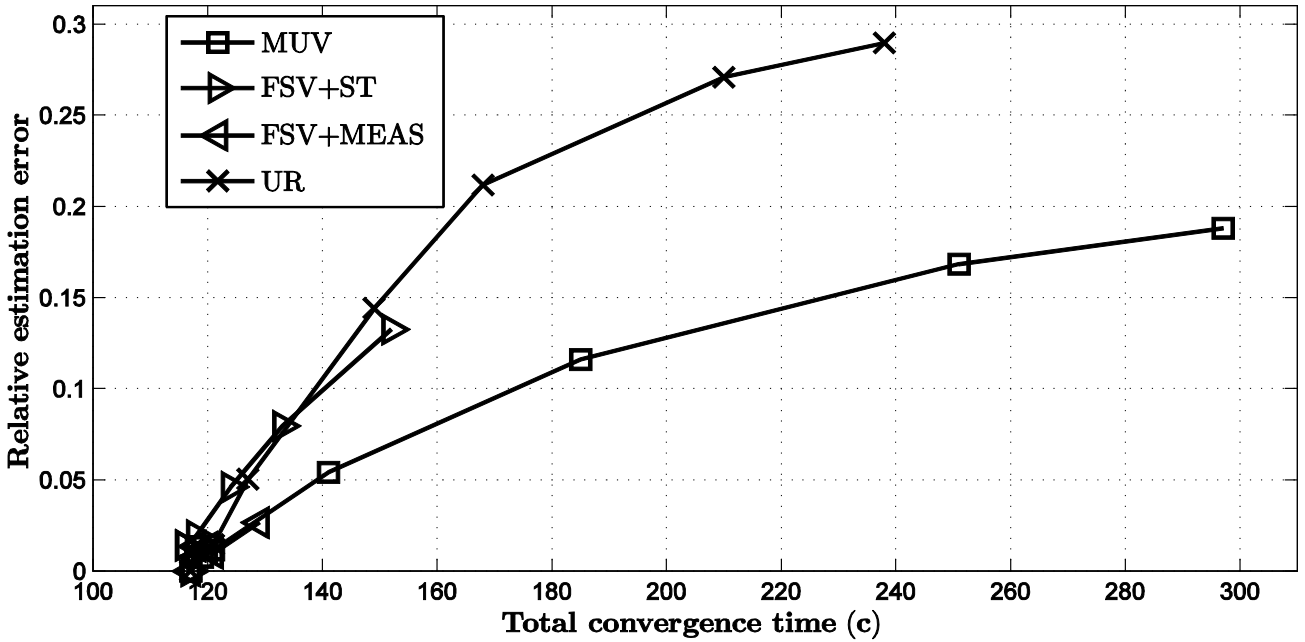


- Attack strategy crucial
- Field measurement data important for powerful attack (FSV+MEAS)

Attack Impact: Estimation Error



- IEEE 118 bus system 6 regions
- Attacker compromises Area 1
- Attack strategies
  - MUV: Maximum update every iteration
  - FSV: First singular vector
  - UR: Uniform rotation



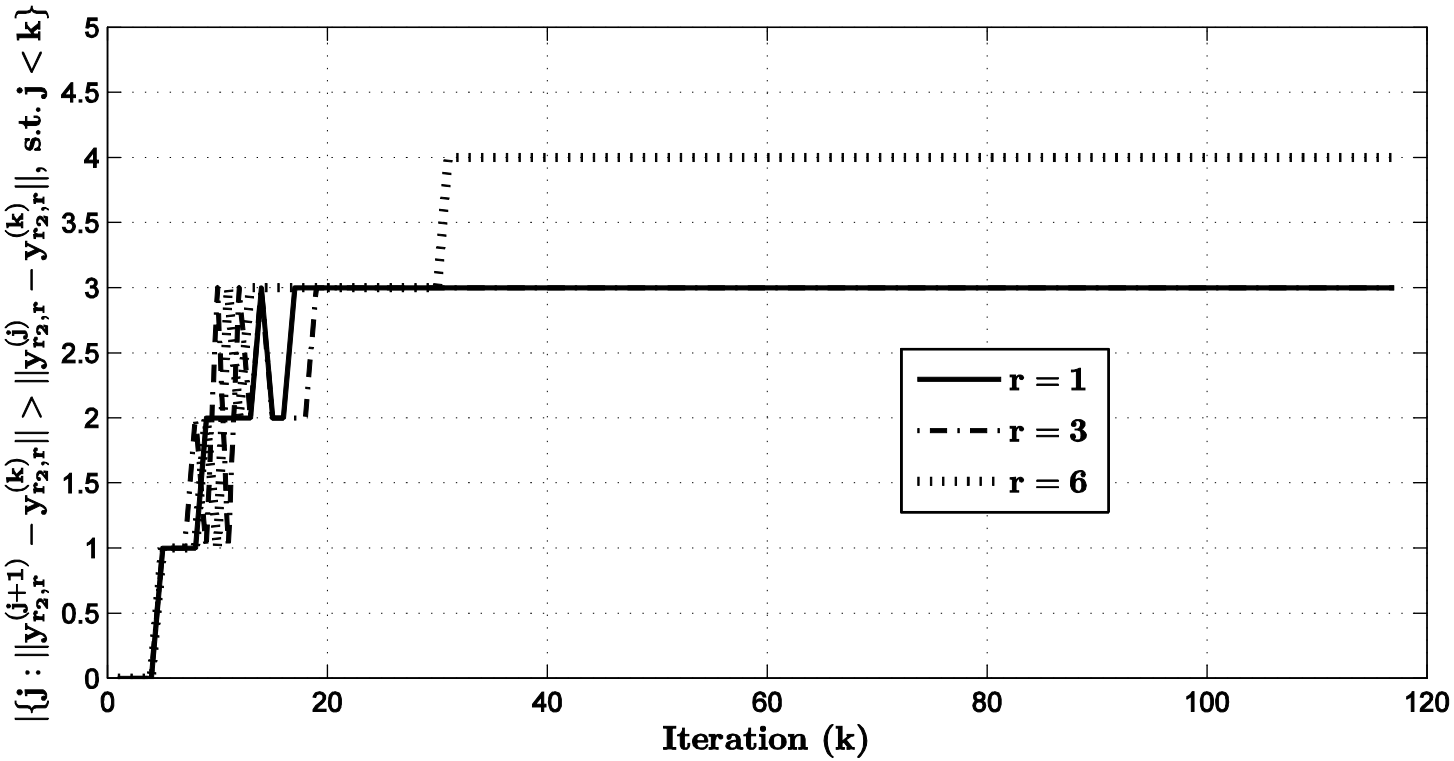
- Up to 30% estimation error on most loaded transmission lines

Attack Detection

- Expected behavior of non-expansive mapping
  - For large k and $k'<k$

$$\| x^{(k'+1)} - x^{(k)} \|_\infty \leq \| x^{(k')} - x^{(k)} \|_\infty$$

- Example: No attack

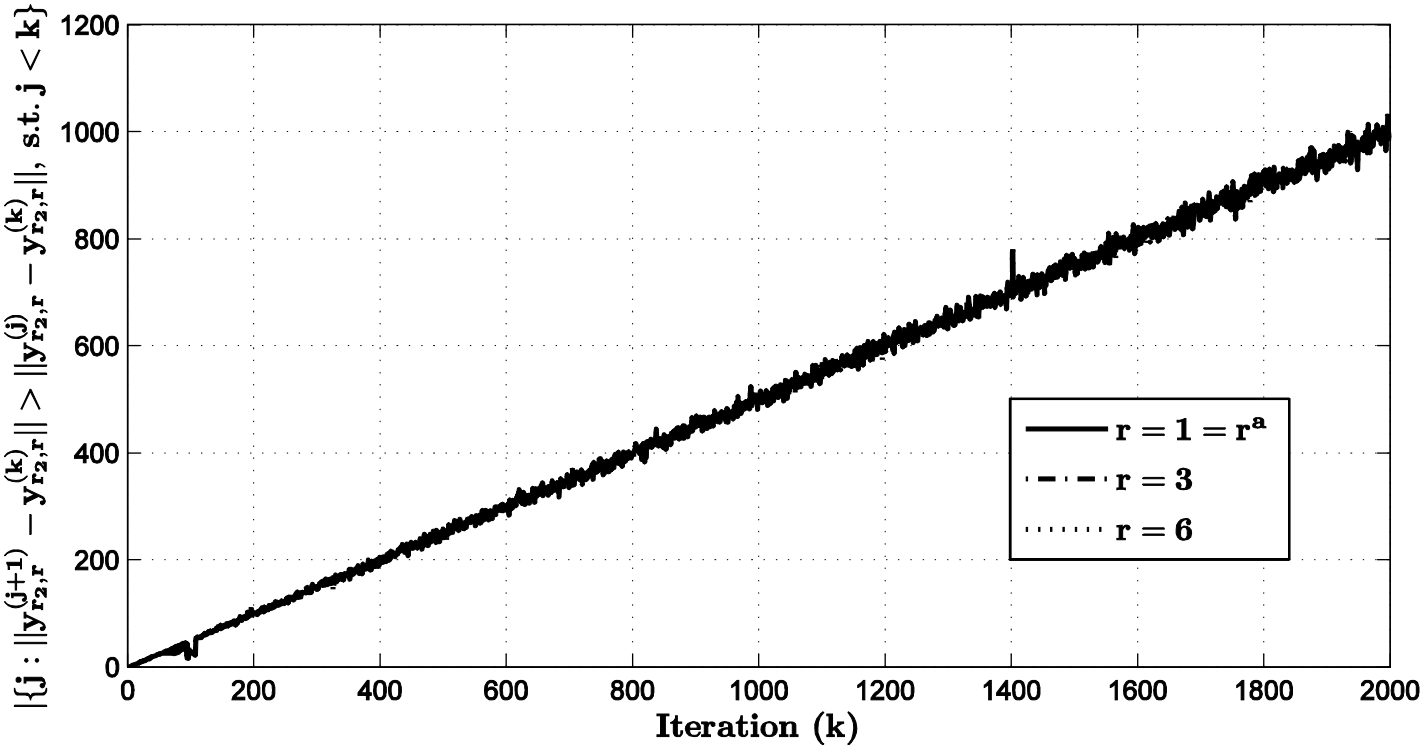


Attack Detection

- Expected behavior of non-expansive mapping
  - For large k and $k'<k$

$$\| x^{(k'+1)} - x^{(k)} \|_\infty \leq \| x^{(k')} - x^{(k)} \|_\infty$$

- Example: FSV attack no convergence



ROYAL INSTITUTE OF TECHNOLOGY

Summary

- SCADA/EMS state estimator BDD can be fooled
  - Based on linear approximation
  - Potentially in reality too
- Cyber-attack vulnerability and cost model
  - Communication topology matters
  - Algorithm for cost-effective mitigation
- Distributed state estimator vulnerable
  - Confidentiality for measurement data important
  - Detection possible
  - Localization and mitigation?

References

- G. Dán, H. Sandberg, „Stealth Attacks and Protection Schemes for State Estimators in Power Systems ", *in Proc. of IEEE SmartGridComm, Oct. 2010*
- A. Teixeira, G. Dán, H. Sandberg, K.H. Johansson, "A Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator", *in Proc. of IFAC World Congress, Aug. 2011*
- O. Vuković, K.C. Sou, G. Dán, H. Sandberg, "Network-layer Protection Schemes against Stealth Attacks on State Estimators in Power Systems", *in Proc. of IEEE SmartGridComm, Oct. 2011*
- *G. Dán, K.C. Sou, H. Sandberg,* "Power System State Estimation Security: Attacks and Protection Schemes", in Smart Grid Communications and Networking (eds. Poor, Hossain, Han), Cambridge University Press, 2012.
- André Teixeira, Henrik Sandberg, György Dán and Karl-Henrik Johansson, "Optimal Power Flow: Closing the Loop over Corrupted Data,'' *in Proc. of American Control Conference (ACC), Jun. 2012*
- O. Vuković, K.C. Sou, G. Dán, H. Sandberg, "Network-layer Protection Schemes against Stealth Attacks on State Estimators in Power Systems", IEEE Journal on Selected Areas in Communications (JSAC), Jul. 2012
- György Dán, Henrik Sandberg, Gunnar Björkman, Mathias Ekstedt, "Challenges in Power System Information Security,'' IEEE Security & Privacy Magazine, vol. 10, no. 4, Jul.-Aug. 2012
- O. Vuković, G. Dán, "On the Security of Distributed Power System State Estimation under Targeted Attacks," *in Proc. of ACM Symposium on Applied Computing (SAC), Mar. 2013*

SEVENTH FRAMEWORK PROGRAMME

VIKING

KTH VETENSKAP OCH KONST

ROYAL INSTITUTE OF TECHNOLOGY

Cyber-physical Models of Power System State Estimation Security

György Dán

School of Electrical Engineering

KTH, Royal Institute of Technology

Stockholm, Sweden

Joint work with: Ognjen Vuković, Henrik Sandberg, Kin Cheong Sou, André Teixeira, Karl-Henrik Johansson, Gunnar Karlsson

ACCESS

TCIPG Seminar Series

7 December 2012