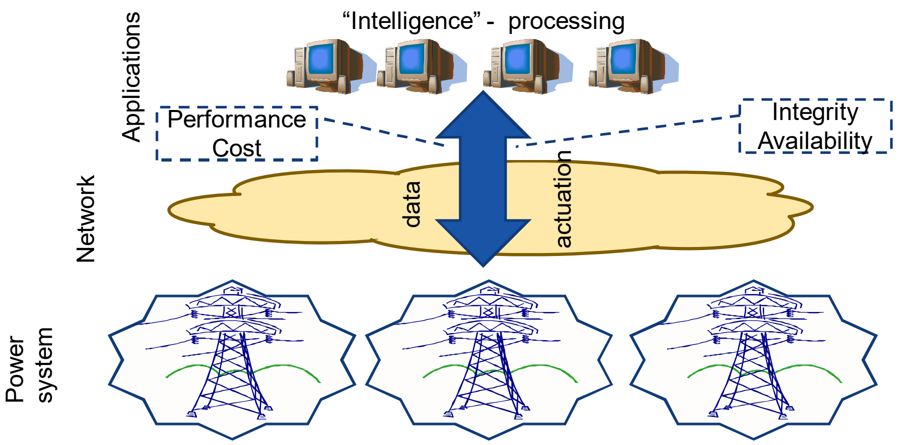
Fully Distributed Power System State Estimation Security: Attacks and Mitigation

György Dán
KTH/EES/Communication Networks

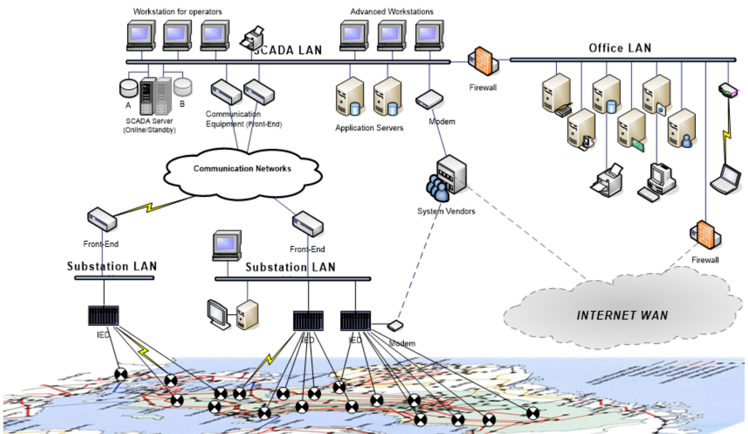
Joint work with: Ognjen Vuković, Henrik Sandberg, Kin Cheong Sou, André Teixeira, Karl-Henrik Johansson, Gunnar Karlsson

GeorgiaTech 2015-11-06

Cyber-Physical Infrastructure



SCADA/EMS Architecture



G. Björkman, ABB

SCADA/EMS Applications

Monitoring

- Status & Analog Retrieval (SAR)
- Network Model Builder (NMB)
- Scheduler Function (SF)
- State Estimation (SE)
- Network Sensitivity (NS)

Analysis

- Dispatcher Power Flow (DPF)
- Security Analysis (SA)
- Short Circuit Analysis (SCA)

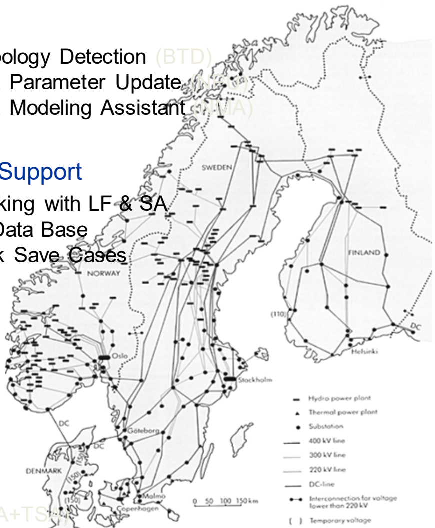
Operations Enhancement

- Optimal Power Flow (OPF)
- Security Constrained Dispatch (SCD)
- Voltage Stability Analysis (VSA)
- Thermal Security Analysis (TSA)
- Available Transmission Capacity (ATC=VSA+TSA)
- Equipment Outage Scheduler (EOS)

- Bad Topology Detection (BTD)
- Network Parameter Update
- Network Modeling Assistant (NMA)

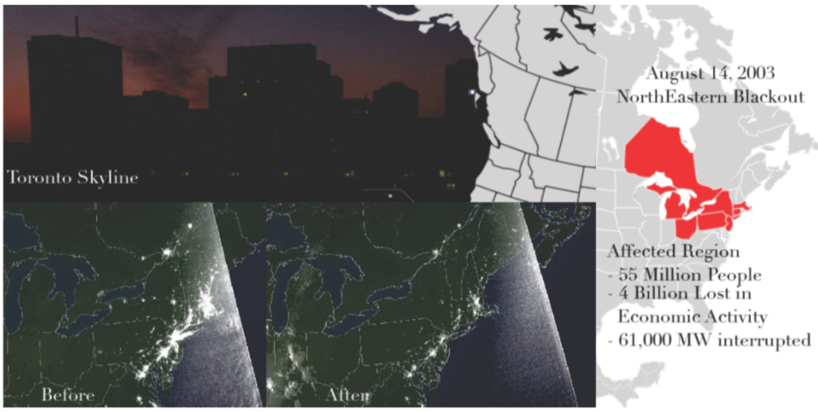
Decision Support

- Interlocking with LF & SA
- Study Data Base
- Network Save Cases



G. Björkman, ABB

North-east American Blackout Aug. 14



Other Black-outs:
WECC 1996 Break-up, European Blackout (4-Nov.-2006), London (28-Aug.-2003), Italy (28-Sep.-2003), Denmark/Sweden (23-Sep.-03), . . .

G. Björkman, ABB

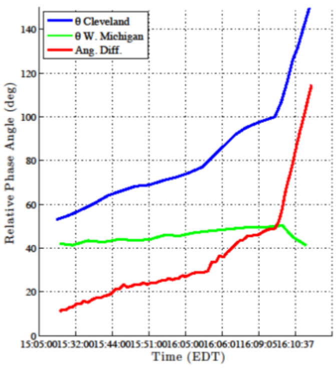
North-east American Blackout Aug. 14 Causes

- Physical Cause:

1. FirstEnergy Corporation's failure to trim trees in part of its OH service area.
2. A generation plant in OH went off-line during high demand, stressing HV lines which came in contact with "overgrown trees", and went out of service.

- Informational Cause:

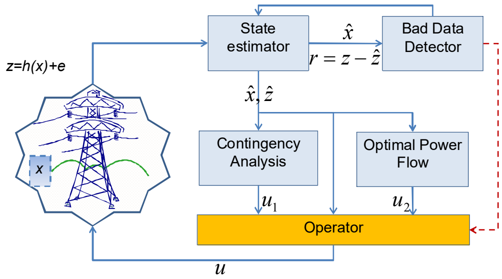
1.
2.
3. The failure deprived them of alerts for monitoring important changes in system state. (Lack of early warnings)
4. Back-up server failures slowed the screen refresh rate of the operators' consoles from 1-3 seconds to 59 seconds per screen. (Lack of dynamic visibility)
5. The loss of alarms led operators to dismiss a call from American Electric Power about the tripping and re-closure of a 345 kV shared line in northeast Ohio. (Lack of corrective measures)



U.S. - Canada Power System outage Task Force Final Report on the August, 14, 2003 Blackout

G. Björkman, ABB

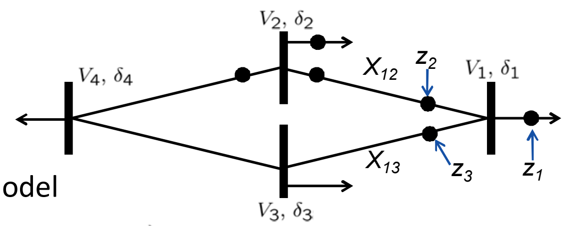
Power System State Estimation



State estimation
- Input: noisy measurements of *P*,*Q*
- Output: state estimate $\widehat{x}$

Bad data detection
- Input
  - Noisy measurements of *P*,*Q*
  - Estimated power flows $\hat{P}$,$\hat{Q}$
- Output
  - Outlier measurements
  - Alarm

Model-based State Estimation



Steady-state power flow model

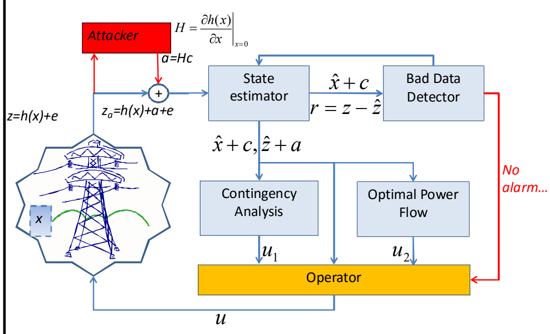
$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} \frac{V_1 V_2}{X_{12}} \sin(\delta_1 - \delta_2) + \frac{V_1 V_3}{X_{13}} \sin(\delta_1 - \delta_3) \\ \frac{V_1 V_2}{X_{12}} \sin(\delta_1 - \delta_2) \end{pmatrix} + \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = h(x) + e \in \mathbb{R}^m$$

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

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

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

State Estimation Security

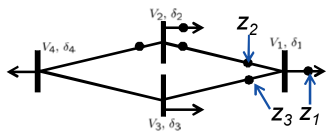


Goal of attacker

- Mislead power application/operator
- SCADA state estimator/BDD

Attack model

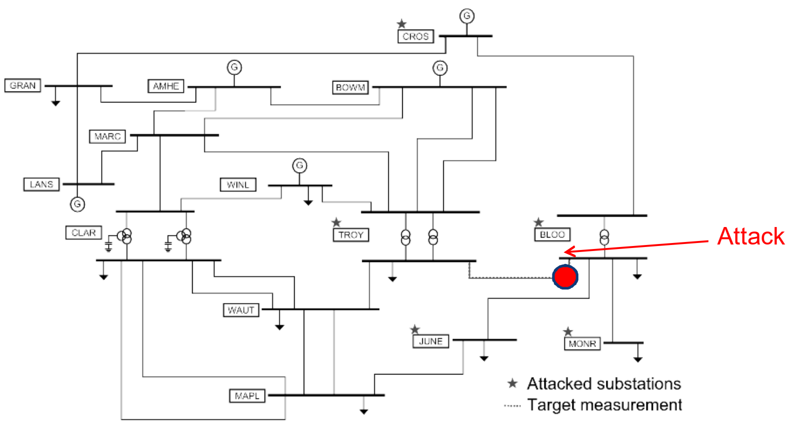
- False data injection
- Compromise measurements



Liu et al., " False data injection attacks against state estimation in electric power grids," in Proc. of ACM CCS 2009

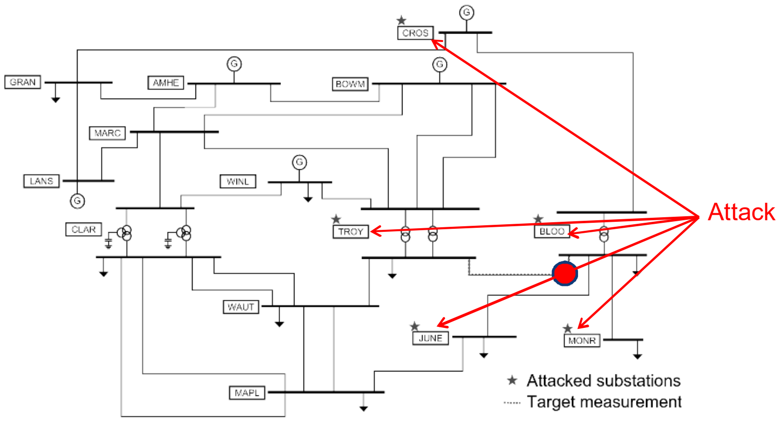
Dán et al., "Stealth attacks and protection schemes for state estimators in power systems," in Proc. of IEEE SmartGridComm, 2010

Example: „Naive” FDI attack



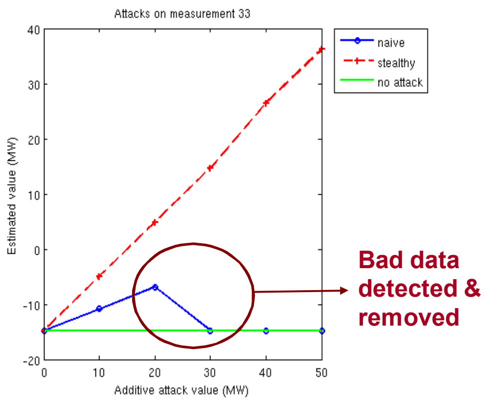
- Attack of transmission line (measurement 33)
- Manipulation of 1 measurement value at 1 substation

Example: „Stealthy” FDI attack



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

Experiment: „Stealthy” vs „Naive” Attack



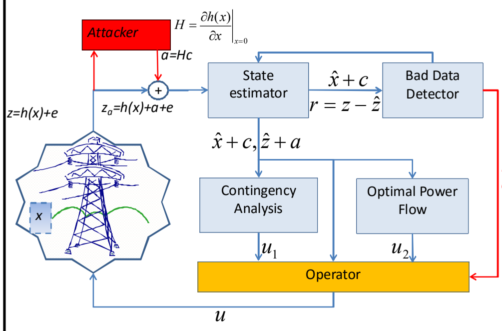
Target bias (MW)	Estimated value (MW)	# BDD Alarms
0	-14.8	0
50	36.2	0
100	86.7	0
150	137.5	0
200	Non convergent	-

Transmission line nom. rat.: 260 MVA

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

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*

State Estimation Security



Liu et al., " False data injection attacks against state estimation in electric power grids," in Proc. of ACM CCS 2009

Dán et al., "Stealth attacks and protection schemes for state estimators in power systems," in Proc. of IEEE SmartGridComm, 2010

Goal of attacker

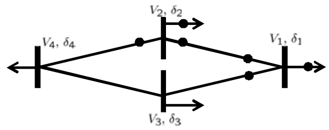
- Mislead power application/operator
- SCADA state estimator/BDD

Attack model

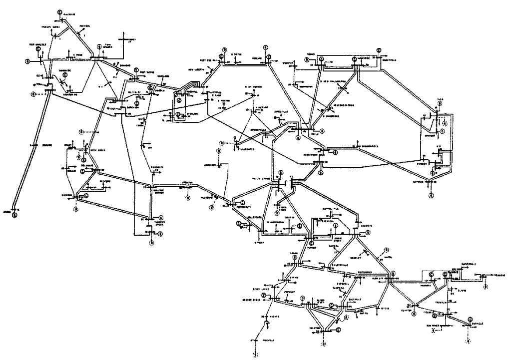
- False data injection
- Compromise measurements

Compute security metrics

- Least cost attack
- Least cost targeted attack



State Estimation Security vs. Network Topology



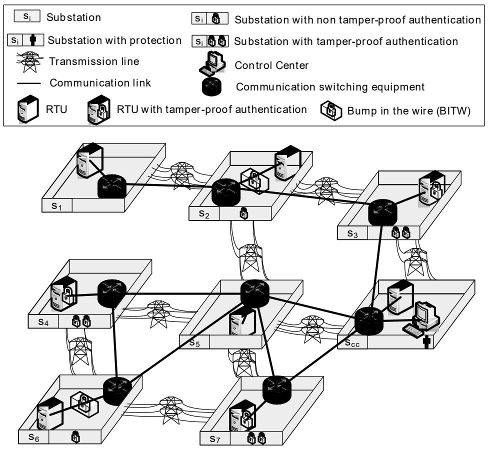
Goal of attacker

- Mislead power application/operator
- SCADA state estimator/BDD

Attack model

- False data injection
- Compromise communication infrastructure (routers)

State Estimation Security vs. Network Topology



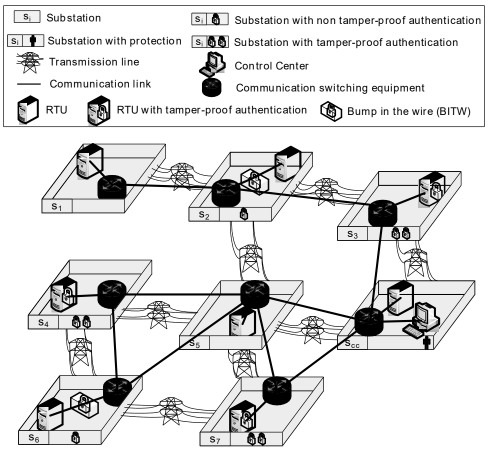
Goal of attacker

- Mislead power application/operator
- SCADA state estimator/BDD

Attack model

- False data injection
- Compromise communication infrastructure (routers)

State Estimation Security vs. Network Topology



Vuković et al., "Network-layer Protection Schemes against Stealth Attacks on State Estimators in Power Systems", *in Proc. of IEEE SmartGridComm, Oct. 2011*

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

Goal of attacker

- Mislead power application/operator
- SCADA state estimator/BDD

Attack model

- False data injection
- Compromise communication infrastructure (routers)

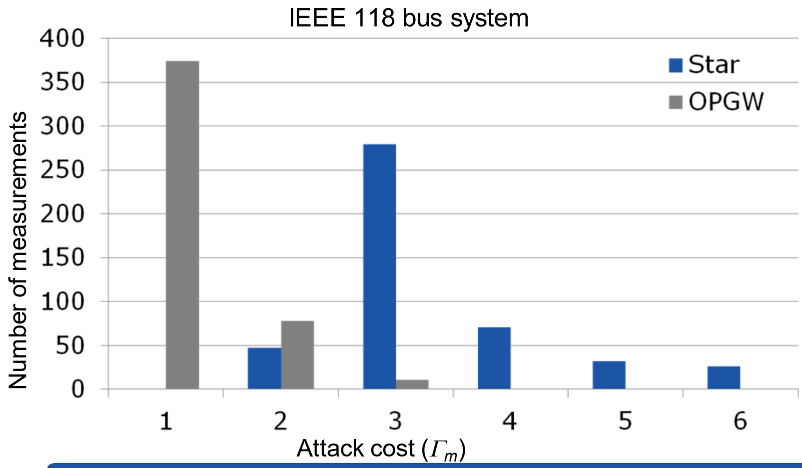
Network-aware security metrics

- Least cost targeted attack
- Attack impact

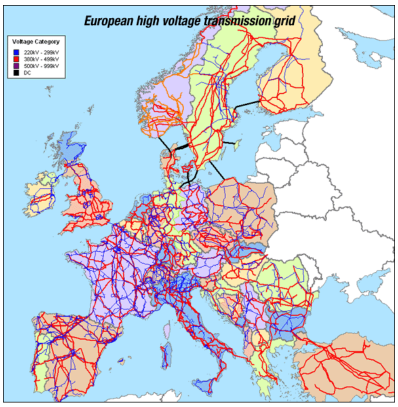
Mitigation

- Multipath, BITW, authentication

Measurement Attack Cost
Star vs. OPGW Topology



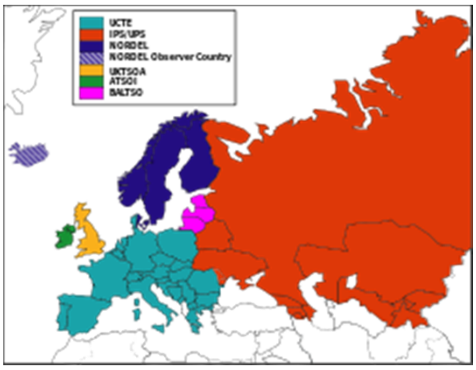
Networks of Transmission Systems



ENTSO-E
- 41 TSOs
- 34 countries
- 4+1 synchronous grids

European Network of Transmission System Operators for Electricity

Networks of Transmission Systems



ENTSO-E

- 41 TSOs
- 34 countries
- 4+1 synchronous grids

European Network of Transmission System Operators for Electricity

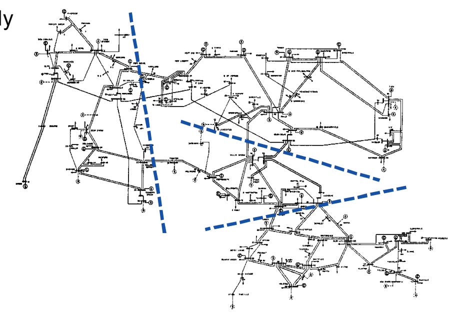
Multi-area State-Estimation

State estimation architectures

- Hierarchical
  - Local solutions coordinated centrally
- Fully distributed
  - Local solutions in consensus

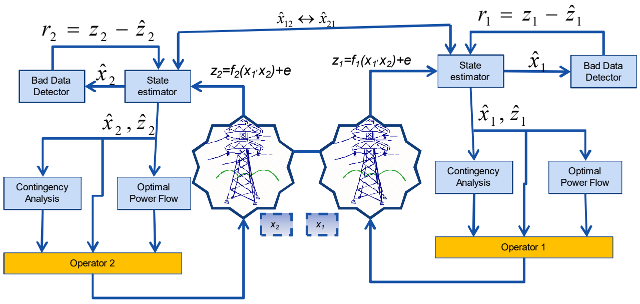
Inter CC communication

- ICCP over TCP/IP
- Confidentiality and integrity using TLS+IPSec



O.Vuković , G. Dán, `` Detection and Localization of Targeted Attacks on Fully Distributed Power System State Estimation," *in Proc. of IEEE SmartGridComm, Oct. 2013*
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 Problem

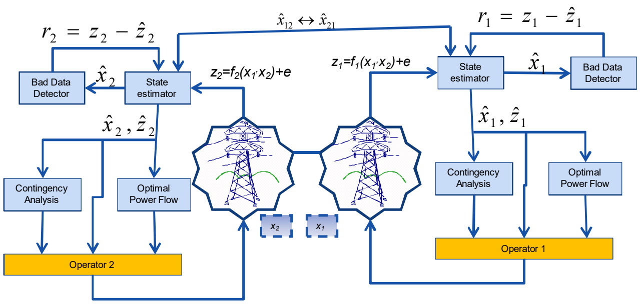


- Local minimization subject to agreement of estimates

$$\min_{x_r,\, r\in\mathcal{R}} \sum_{r\in\mathcal{R}} [z_r - f_r(x_r)]^T [W_r^{-1}][z_r - f_r(x_r)]$$

$$s.t. \quad x_{r,r'} = x_{r',r} \quad \forall r \in \mathcal{R} \; and \; \forall r' \in \mathcal{N}(r)$$

Simple Distributed State Estimation



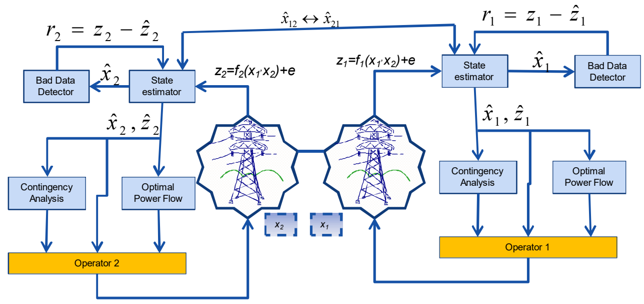
- Gauss-Newton including border state variables

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

  - Periodic exchange of border state variables
- Convergence time k^* $\quad \left\| x_r^{(k^*+1)} - x_r^{(k^*)} \right\|_\infty < \varepsilon \qquad \forall r \in \mathcal{R}$
  - Convergence?

M. Shahidehpour and Y. Wang, "Communication and Control in Electric Power Systems," John Wiley and Sons, 2003.

ADMM-based Distributed State Estimation



Consensus between neighboring regions

$$x_r^{(k+1)} = (H_r^{(k)T} W^{-1} H_r^{(k)} + cD_r)^{-1}(H_r^{(k)T} z_r + cD_r p_r^{(k)})$$

$$s_r^{(k+1)} = U_{x_r} \cdot \sum_{\forall r' \in \mathcal{N}(r)} Y_{r,r'} \cdot x_{r',r}^{(k+1)}$$

Average of border state variables

$$p_r^{(k+1)} = p_r^{(k)} + s_r^{(k+1)} - \frac{1}{2}(Y_{r,b} \cdot Y_{r,b}^T \cdot x_r^{(k)} - s_r^{(k)}),$$

Convergence time k^* $\quad \left\| x_r^{(k^*+1)} - x_r^{(k^*)} \right\|_\infty < \varepsilon \quad \forall r \in \mathcal{R}$

V. Kekatos and G. B. Giannakis, "Distributed robust power system state estimation," IEEE Transactions on Power Systems, vol. 28, no. 2, pp. 1617–1626, 2013

Distributed State Estimation Security

Attacker's goal

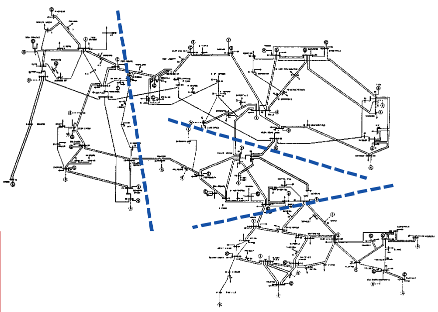
- Disable fully distributed state estimation

Attack model

- Compromise CC
  - Compromise communication (ICCP)
- False data injection

Important questions

- Can attack disturb DSE?
- Can attack be detected?
- Can compromised CC be localized?



O.Vuković , G. Dán, `` Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks,'' *IEEE JSAC, Jul. 2014*
O.Vuković , G. Dán `` On the Security of Distributed Power System State Estimation under Targeted Attacks,'' *ACM Symposium on Applied Computing, Mar. 2013*

Byzantine Approximate Agreement

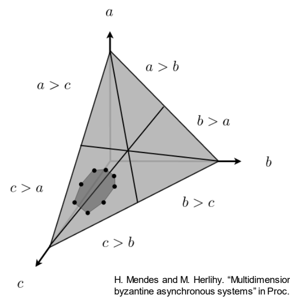
- Set $N = G \bigcup B$ of processes, each with input $x_n \in \Re^m$
- Have to produce output

$$y_n \in \Re^m, \quad \|y_n - y_{n'}\| < \varepsilon, \quad y_n \in Conv(\{x_{n'} \mid n' \in G\})$$

- Underlying topology
  - Complete
  - Non-complete

- Question

$$\max|B|$$



H. Mendes and M. Herlihy. "Multidimensional approximate agreement in byzantine asynchronous systems" in Proc. of ACM STOC, 2013

Distributed State Estimation Security

Attacker's goal

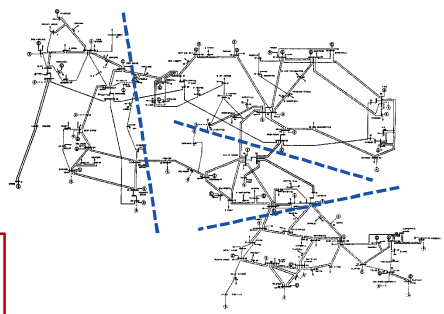
- Disable fully distributed state estimation

Attack model

- Compromise CC
  - Compromise communication (ICCP)
- False data injection

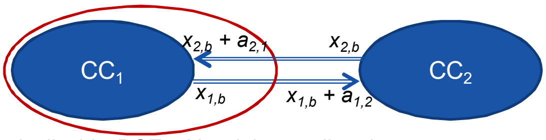
Important questions

- Can attack disturb DSE?
- Can attack be detected?
- Can compromised CC be localized?



O.Vuković , G. Dán, `` Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks,'' *IEEE JSAC, Jul. 2014*
O.Vuković , G. Dán `` On the Security of Distributed Power System State Estimation under Targeted Attacks,'' *ACM Symposium on Applied Computing, Mar. 2013*

Border Bus Phase Angle Attack Model



Goal: disable DSE with minimum disturbance

$$\min_{a^{(k)}_{b,r^a},k=1,\ldots} \beta \quad \text{s.t. } k^* = \infty \text{ and } \beta = ||a^{(k)}_{b,r^a}||_2; \forall k.$$

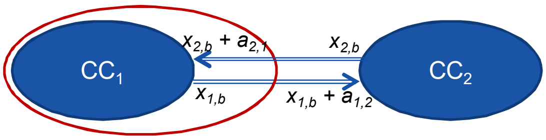
Greedy approximation of optimal attack strategy

- DSE iteration under attack

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

- Greedy *Maximum Update Vector* strategy
  - Choose $a_{1,2}$ to maximize $\| \Delta\tilde{x}^{(k)} \|$
  - Under constraint $\beta = ||a_{1,2}||$

First Singular Vector Attack

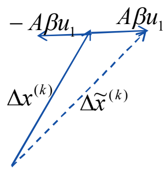


First Singular Vector attack (model/state-aware)

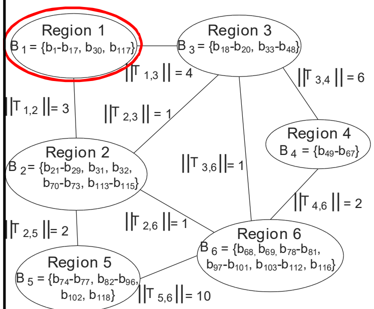
$$x^{(k+1)} = x^{(k)} + \Delta\tilde{x}^{(k)} \neq x^{(k)} + \Delta x^{(k)}$$

$$\Delta\tilde{x}^{(k)} \approx \Delta x^{(k)} - \underbrace{[H^{(k)T}W^{-1}H^{(k)}]^{-1}H^{(k)T}W^{-1}H_b^{(k)}}_{A} a_{1,2}$$

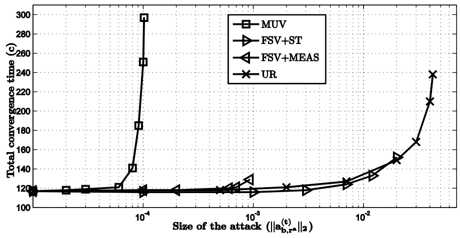
- $a_{1,2} = \beta\, u_1$ (First singular vector of A)
- Attacker needs information
  - H matrix and system state
  - Power flow measurements → direction (±)



Attack Impact: Convergence Time

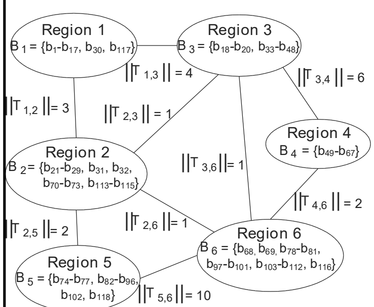


- IEEE 118 bus system 6 regions
- Attacker compromises Area 1
- Attack strategies
  - MUV: Maximum update every iteration
  - FSV: First singular vector
  - UR: Uniform rotation

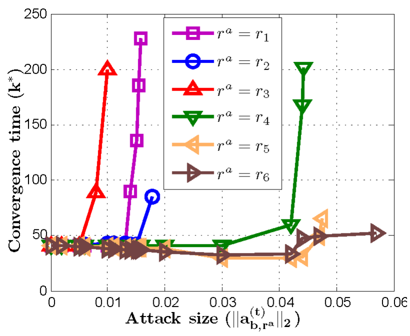


- Attack strategy crucial
- Field measurement data important for powerful attack (FSV+MEAS)

Attack Impact: Convergence Time



- IEEE 118 bus system 6 regions
- Attack strategy
  - FSV: First singular vector



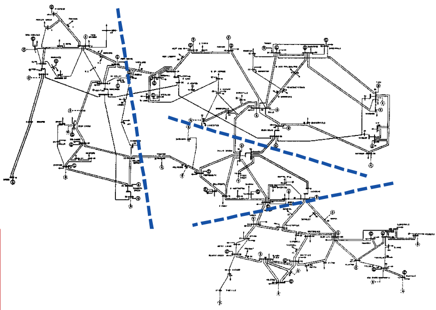
- Limited importance of attack location

Distributed State Estimation Security

Attacker's goal
- Disable fully distributed state estimation

Attack model
- Compromise CC
  - Compromise communication (ICCP)
- False data injection

Important questions
- Can attack disturb DSE? YES
- Can attack be detected?
- Can compromised CC be localized?



O.Vuković , G. Dán, `` Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks,'' *IEEE JSAC, Jul. 2014*
O.Vuković , G. Dán `` On the Security of Distributed Power System State Estimation under Targeted Attacks,'' *ACM Symposium on Applied Computing, Mar. 2013*

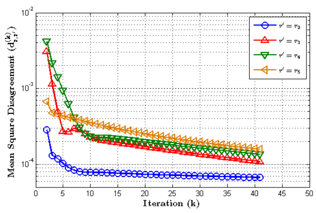
Attack Detection

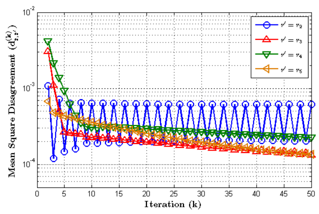
- Mean squared disagreement (MSD)

$$d_{r,r'}^{(k)} = \left\| \frac{x_{r,r'}^{(k)} - x_{r',r}^{(k)}}{2} \right\|_2^2 / \left| x_{r,r'}^{(k)} \right|$$

  - Observation: If ADMM converges w/o attack then $d_{r,r'}^{(k)} \to 0$
- Detection rule: If $\sup\{ d_{r,r'}^{(k')} : k' > k\} > 0$ and $\forall t \geq 0$

$$\sup\{ d_{r,r'}^{(k')} : k' > k\} \leq \sup\{ d_{r,r'}^{(k')} : k' > k + t\}$$



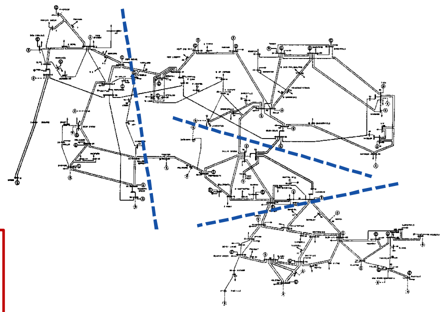


Distributed State Estimation Security

Attacker's goal
- Disable fully distributed state estimation

Attack model
- Compromise CC
  - Compromise communication (ICCP)
- False data injection

Important questions
- Can attack disturb DSE? YES
- Can attack be detected? YES
- Can compromised CC be localized?



O.Vuković , G. Dán, `` Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks,'' *IEEE JSAC, Jul. 2014*
O.Vuković , G. Dán `` On the Security of Distributed Power System State Estimation under Targeted Attacks,'' *ACM Symposium on Applied Computing, Mar. 2013*

Attack Localization

- Smoothed MSD

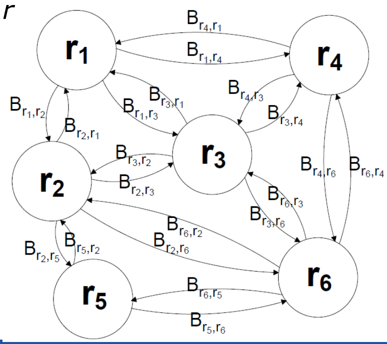
$$\tilde{d}^{(k)}_{r,r'} = \alpha_k \cdot d^{(k)}_{r,r'} + (1-\alpha_k)\cdot d^{(k-1)}_{r,r'}, \quad \alpha_k \in (0,1), \sum_k \alpha_k = \infty$$

- Belief of attack location of region r

$$B^{(k)}_{r,r'} = \frac{\tilde{d}^{(k)}_{r,r'}}{\sum_{\forall r' \in N(r)} \tilde{d}^{(k)}_{r,r'}}$$

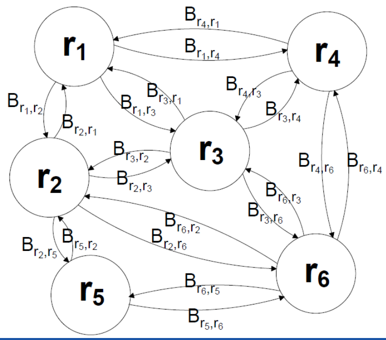
- Properties
  - Symmetry $\tilde{d}^{(k)}_{r,r'} = \tilde{d}^{(k)}_{r',r}$
  - Non-negativity

$$B^{(k)}_{r,r'} > 0 \Leftrightarrow B^{(k)}_{r',r} > 0$$



Attack Localization: Token Passing

- Token passing-based localization
  - Central observer
  - Token
    - Forwarded to r' w.p. $B^{(k)}_{r,r'}$
- Probability of compromise in r
  - Empirical frequency of visiting region r
- Candidate for attacked region
  - Most visited region

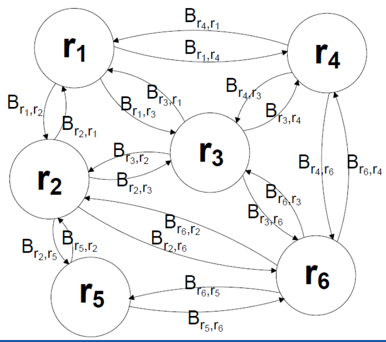


Attack Localization: Belief Consensus Algorithm

1. Flood $\tilde{d}^{(k)}_{r,r'}$
2. Compute $B^{(k)}_{r,r'}$
3. Construct $B^{(k)} = (B^{(k)}_{r,r'})$
4. Compute $\pi^{(k)} = \pi^{(k)} B^{(k)}$
5. If $\left\|\pi^{(k)} - \pi^{(k-1)}\right\|_\infty < \varepsilon^L \Rightarrow k^L = k$

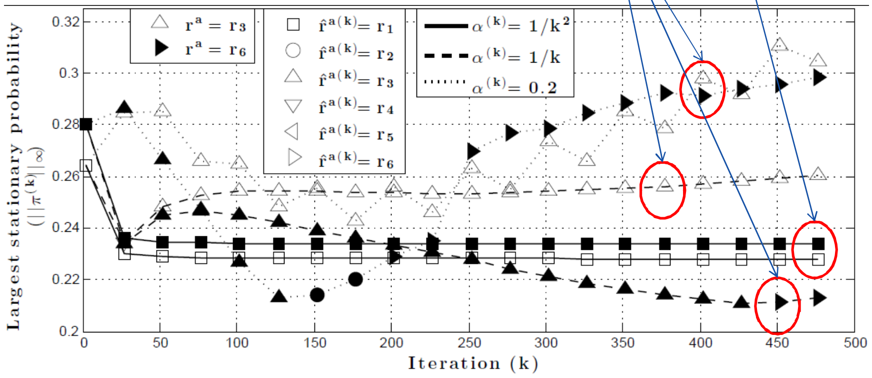
$$r^{a(k^L)} = \operatorname*{argmax}_r \pi^{(k^L)}$$

- Results:
  - If G contains 3-clique and the DSE does not converge $\Rightarrow \pi^{(k)}$ exists and is unique
  - If $\alpha_k \to 0$ and $x^{(k)}$ asymptotically periodic $\Rightarrow \pi^{(k)} \to \pi^*$



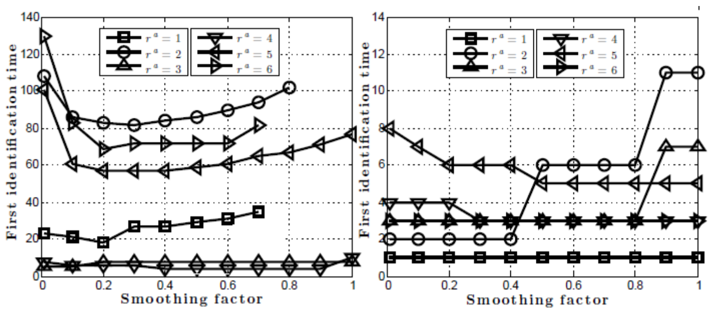
Attack Localization: Example

- Attack in r_3 and r_6
- Different smoothing factors



Attack Localization: Example

- Attack in each *individual* region

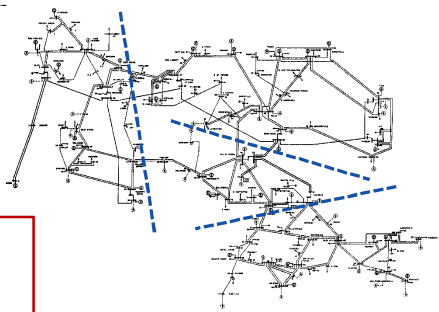


- Small constant smoothing factor ⇒ fast localization
  - No guarantee on convergence
- Large attack magnitude faster to localize

Distributed State Estimation Security

Attacker's goal
- Disable fully distributed state estimatio

Attack model
- Compromise CC
  - Compromise communication (ICC
- False data injection



Important questions
- Can attack disturb DSE? YES
- Can attack be detected? YES
- Can compromised CC be localized? YES

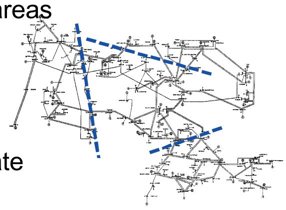
O.Vuković , G. Dán, `` Detection and Localization of Targeted Attacks on Fully Distributed Power System State Estimation,'' *in Proc. of IEEE SmartGridComm, Oct. 2013*
O.Vuković , G. Dán `` On the Security of Distributed Power System State Estimation under Targeted Attacks,'' *ACM Symposium on Applied Computing, Mar. 2013*

Conclusion

Power system state estimation
- Centralized: FDI attack on integrity
  - Network-aware attack cost/mitigation
- Distributed: FDI attack on availability
  - First singular vector attack

DSE attack detection algorithm
- Observation of disagreement between areas

Distributed localization algorithm
- Based on consensus of beliefs



Open questions
- Chaotic behavior of attacked system state
- Improve localization performance
  - Algorithmic vs. architectural/system solution

References

G. Dán and 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 and 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 and H. Sandberg, ``Network-layer protection schemes against stealth attacks on state estimators in power systems,'' *in Proc. of IEEE SmartGridComm, Oct 2011*

O. Vuković, K. C. Sou, G. Dán and H. Sandberg, ``Network-aware Mitigation of Data Integrity Attacks on Power System State Estimation,'' IEEE JSAC, vol. 30, no. 6, July 2012

G. Dán, H. Sandberg, G. Björkman, M. Ekstedt, ``Challenges in Power System Information Security,'' *IEEE Security & Privacy Magazine, Jul. 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, Mar. 2013*

O.Vuković , G. Dán, ``Detection and Localization of Targeted Attacks on Fully Distributed Power System State Estimation," *in Proc. of IEEE SmartGridComm, Oct. 2013*

O.Vuković , G. Dán ``Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks," IEEE JSAC, Jul 2014

A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba, A. Valdes, ``Security of Smart Distribution Grids: Data Integrity Attacks on Integrated Volt/VAR Control and Countermeasures," *in Proc. of American Control Conference (ACC), Jun. 2014.*

N. M. Torrisi, O. Vuković, G. Dán, S. Hagdahl, ``Peekaboo: A Gray Hole Attack on Encrypted SCADA Communication using Traffic Analysis," *in Proc. of IEEE SmartGridComm, Nov. 2014*

H. Sandberg, G. Dán, R. Thobaben, ``Differentially Private State Estimation in Distribution Networks with Smart Meters," in Proc. of IEEE Conference on Decision and Control (CDC), Dec 2015, to appear

Fully Distributed Power System State Estimation Security: Attacks and Mitigation

György Dán

KTH/EES/Communication Networks

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

GeorgiaTech 2015-11-06