On the Security of Distributed Power System State Estimation under Targeted Attacks

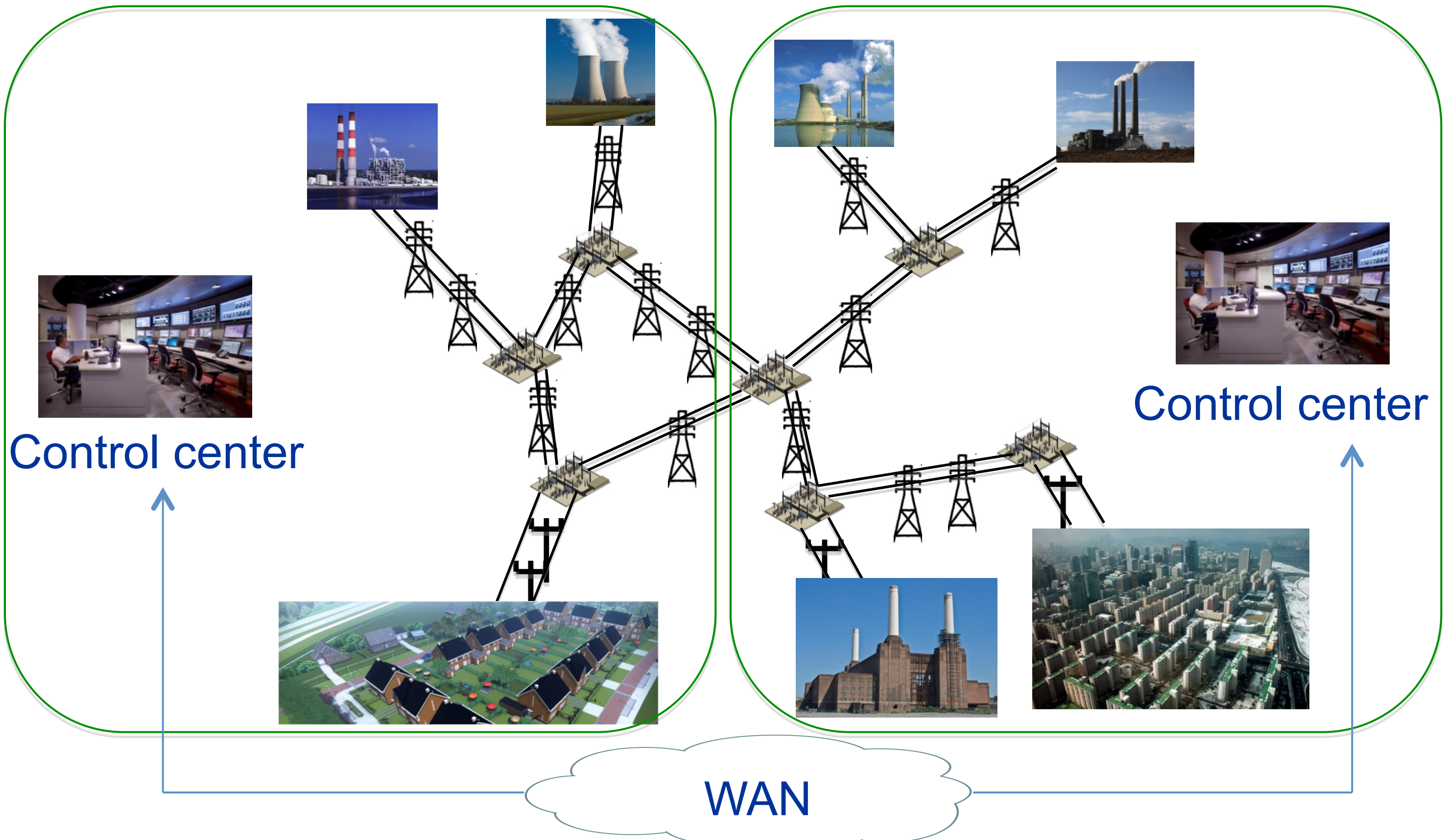
Ognjen Vuković, György Dán

School of Electrical Engineering, KTH Royal Institute of Technology
Stockholm, Sweden

ACM SAC
Coimbra, 19. March 2013

Power System Supervision and Control

- Supervisory Control and Data Acquisition (SCADA)
- Energy Management System (EMS)
  - State Estimation (SE) – a core EMS component
- Distributed Supervision and Control
  - Cooperation between operators; ICCP



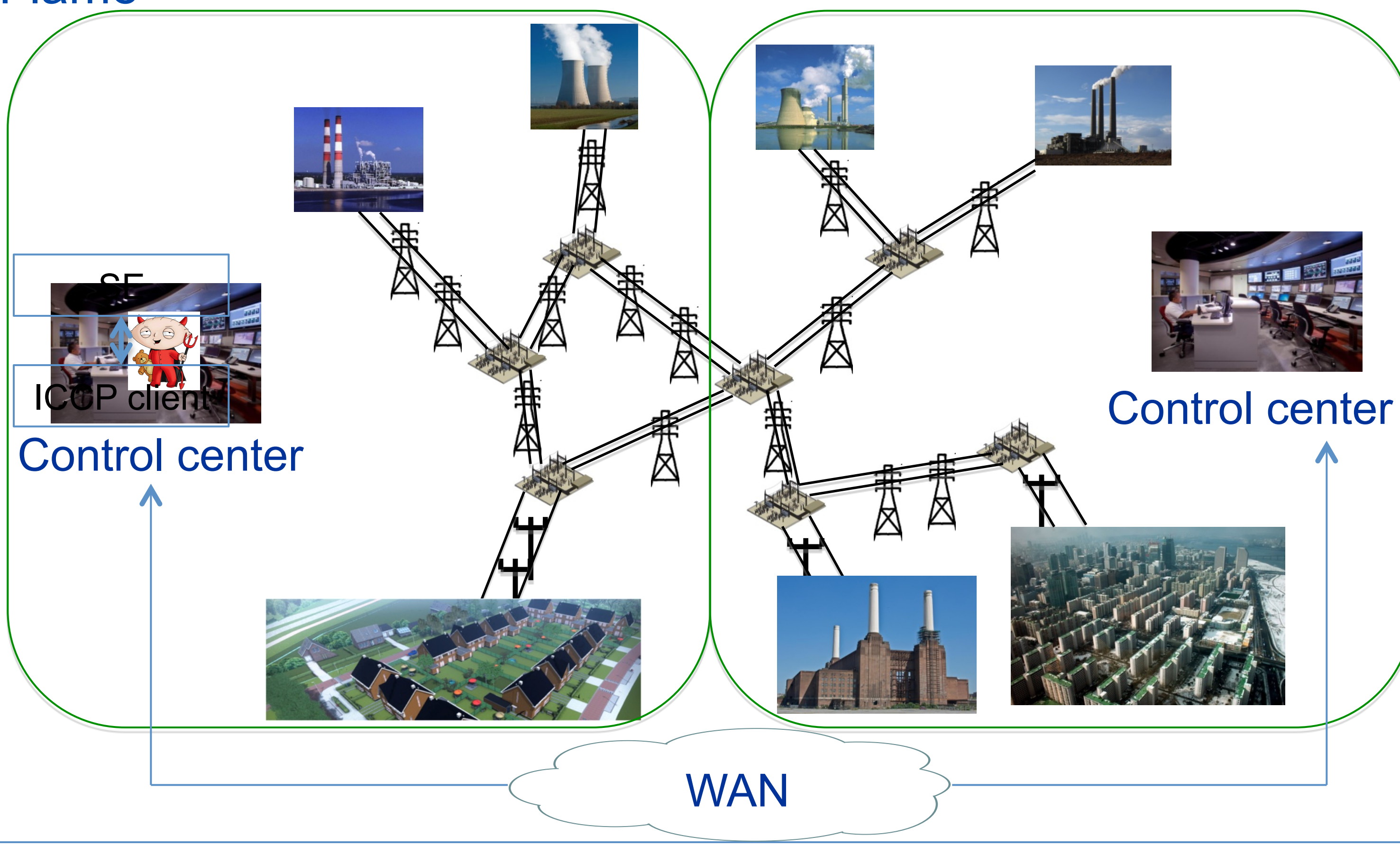
Distributed State Estimation (DSE)

- State Estimate of the Entire Interconnected System
  - Local state estimation + synchronization
- Security of Distributed State Estimation
  - Violation of the integrity of exchanged data
  - Stuxnet, Flame

Can the attack affect the DSE?

Detection?

Mitigation?

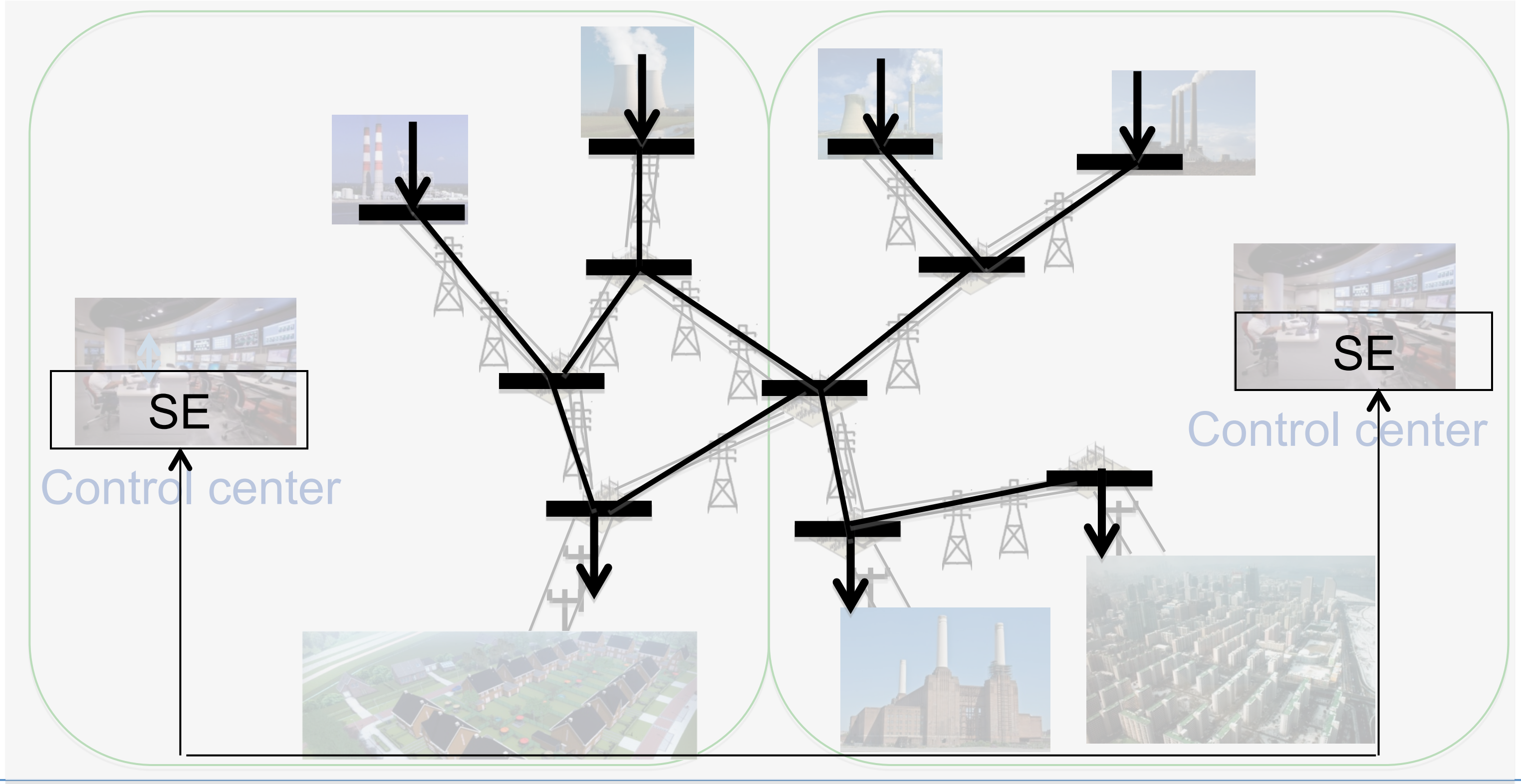


Outline

- Motivation
- System Model
- Attack Model and Strategies
- Attack Impact
- Detection and Mitigation
- Conclusion

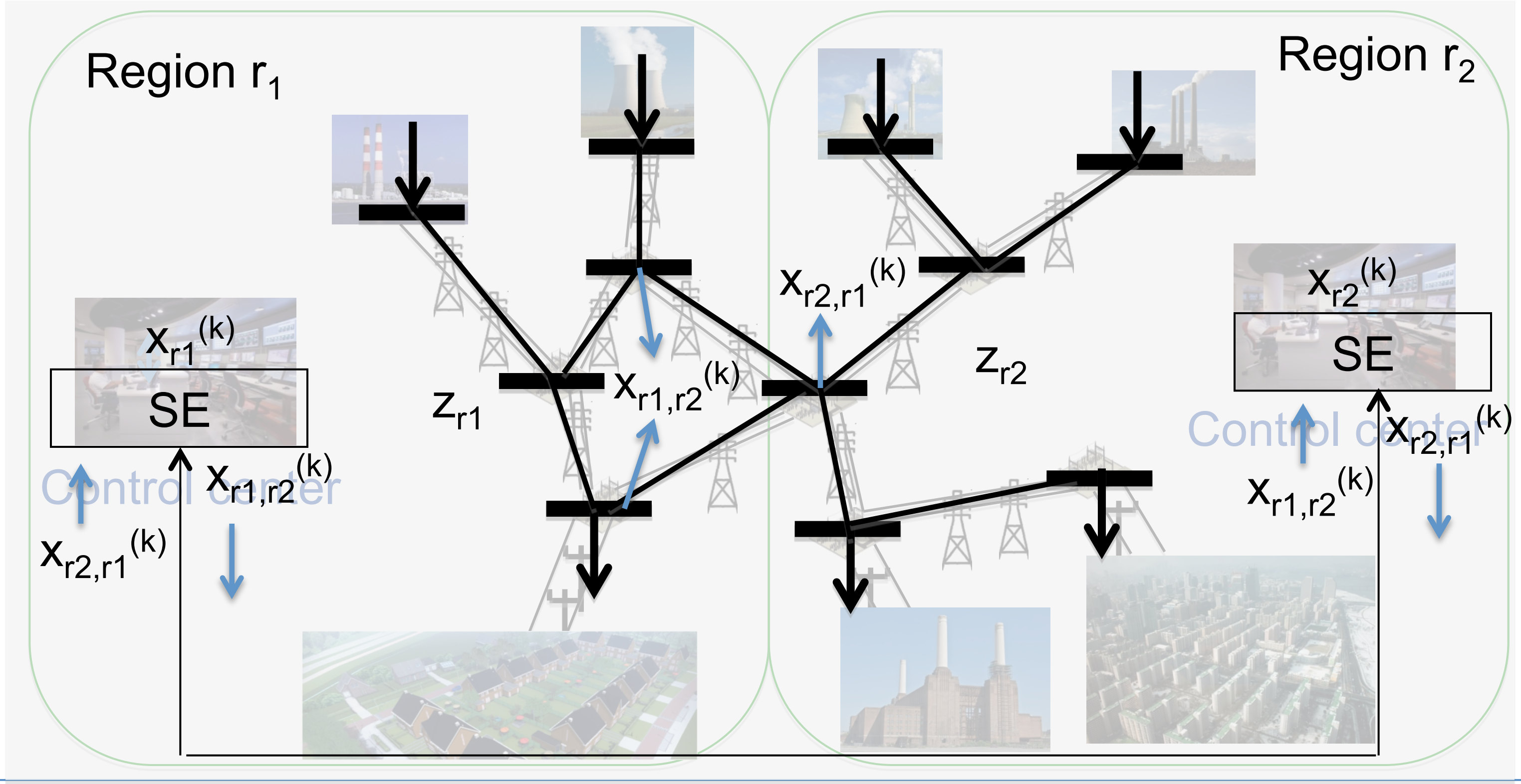
System Model

- Transmission Network: buses and branches
  - *Power injections and power flows* $P = [P_1 , P_2 , \ldots , P_M]^T$
- Measurements: $z = [z_1, z_2, \ldots, z_M]^T$, $z_i = P_i + e_i$
- State Vector x: bus voltage angles and magnitudes
  - $P = f(x^*)$, x^*: actual state of the system



System Model

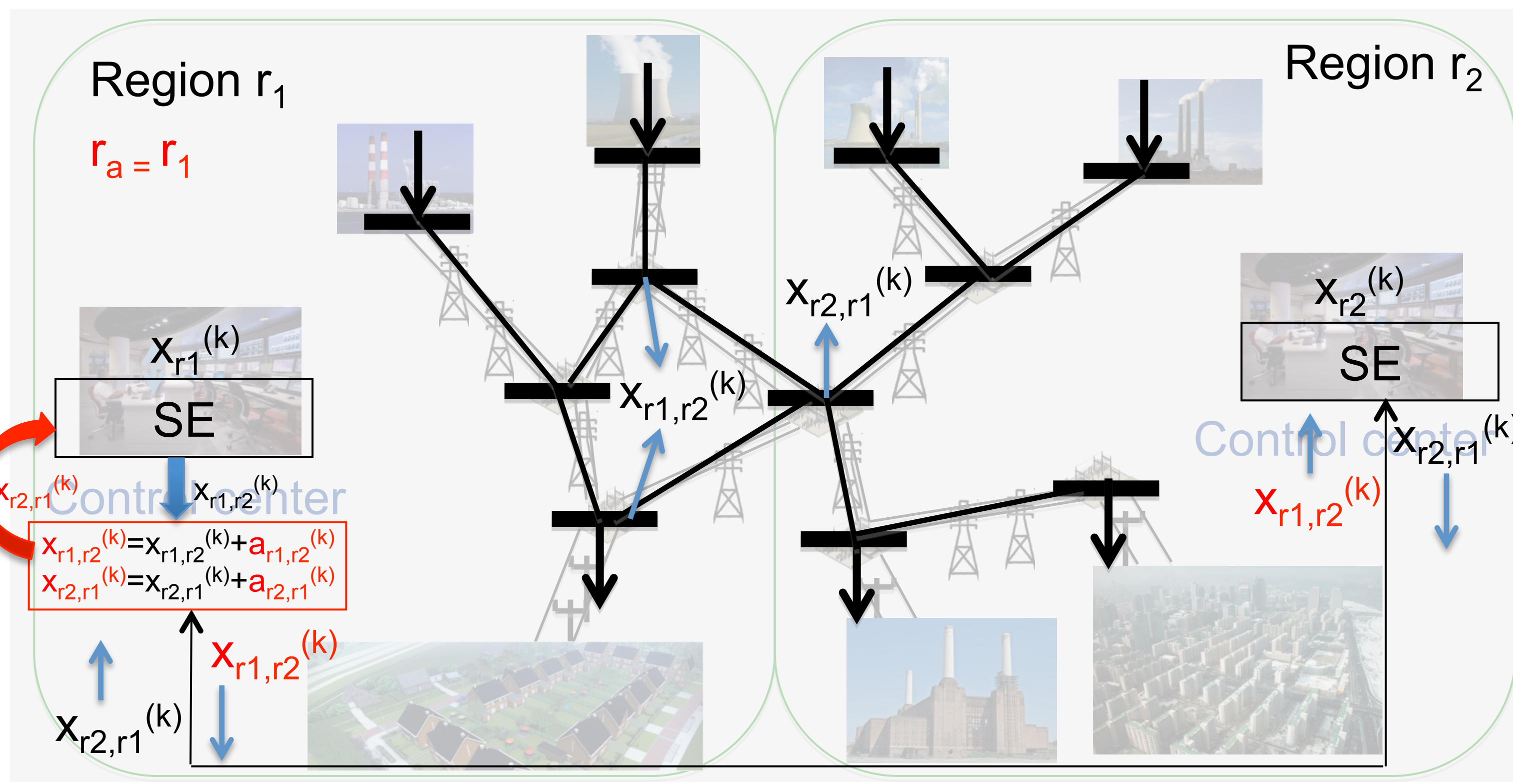
- State Estimation
  - Find x^*; Weighted Least Square estimation
  - Gauss-Newton algorithm: $x^{(k+1)} = x^{(k)} + \underbrace{[H^{(k)T} W^{-1} H^{(k)}]^{-1} H^{(k)T} W^{-1} [z - f(x^{(k)})]}_{\Delta x^{(k)}}$
- Distributed State Estimation
  - Local measurements z_r ; find x_r^*; send $x_{r,r'}^{(k)}$, use $x_{r',r}^{(k)}$ ($x_{b,r'}^{(k)}$) in k+1



Attack Model

- Attacked region r_a ; attack vector $a_{r,r_a}^{(k)}$ $(a_{b,r_a}^{(k)})$, attack size $\left\| a_{b,r_a}^{(k)} \right\|_2$
- Iterations under attack: $x_r^{(k+1)} = x_r^{(k)} + \Delta\tilde{x}_r^{(k)} \neq x_r^{(k)} + \Delta x_r^{(k)}$
- Attacker's objective: $\max\limits_{a_{r,r_a}^{(k)},\, k=1,\ldots} c \quad \text{s.t.} \left\| a_{r,r_a}^{(k)} \right\|_2 < \beta$

$$\boxed{\max_{a_{r,r_a}^{(k)},\, k=1,\ldots} \left\| \Delta\tilde{x}_r^{(k)} \right\|_2 \quad \text{s.t.} \left\| a_{r,r_a}^{(k)} \right\|_2 < \beta}$$



Attack Strategies

$$\max_{a_{r,r_a}^{(k)},\ k=1,\dots} \left\| \Delta\tilde{x}_r^{(k)} \right\|_2 \quad \text{s.t. } \left\| a_{r,r_a}^{(k)} \right\|_2 < \beta$$

First Singular Vector (FSV)

$$\Delta\tilde{x}_r^{(k)} = \Delta x_r^{(k)} - \underbrace{[H^{(k)T}W^{-1}H^{(k)}]^{-1}H^{(k)T}W^{-1}H_b^{(k)}}_{A} a_{r,r_a}^{(k)}$$

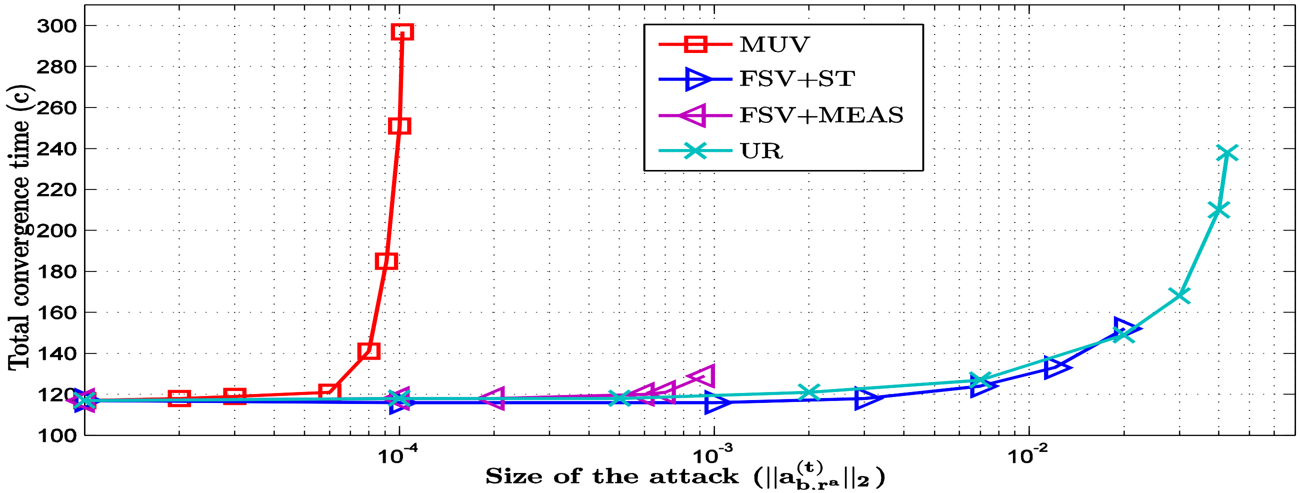
$a_{r,r_a}^{(k)} = u_1$, first singular vector of the matrix A

- Required knowledge of the system model (matrix *H*)
- Required knowledge of power flows/injections (sign($a_{r,ra}^{(k)}$))

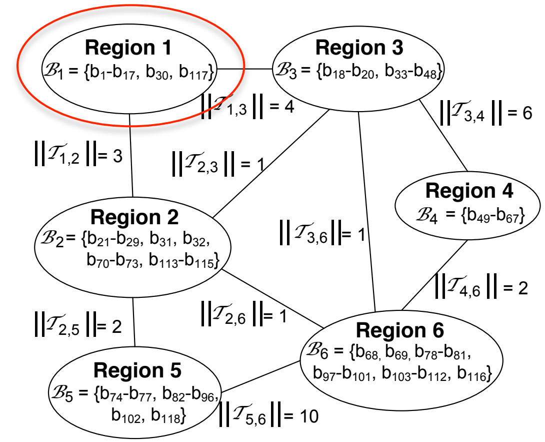
Other Strategies

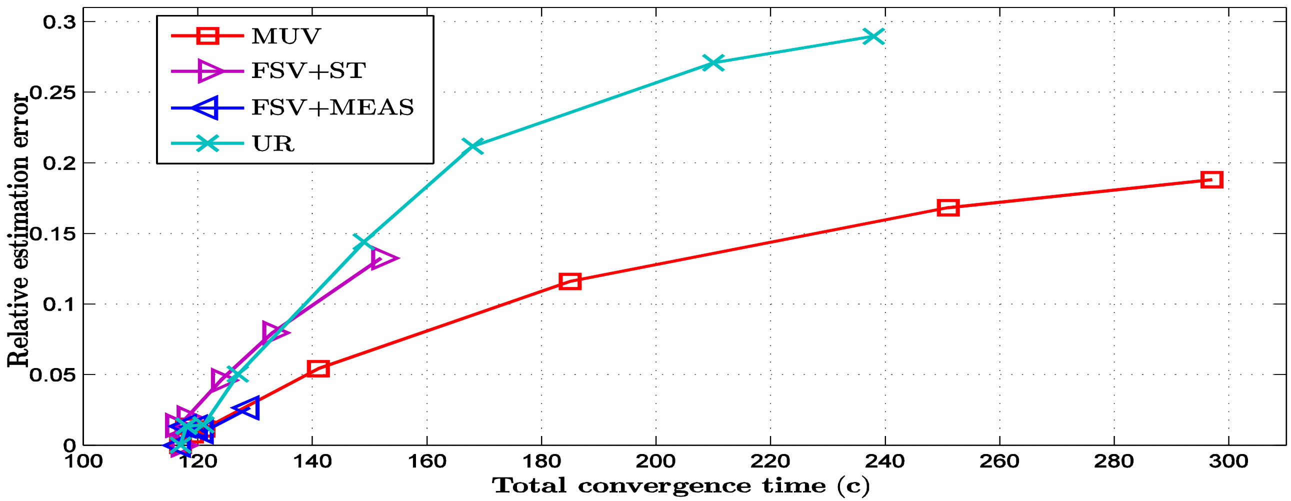
- Maximal Update Vector attack (MUV)
- Uniform Rotation Attack
- A couple more…

Attack Impact



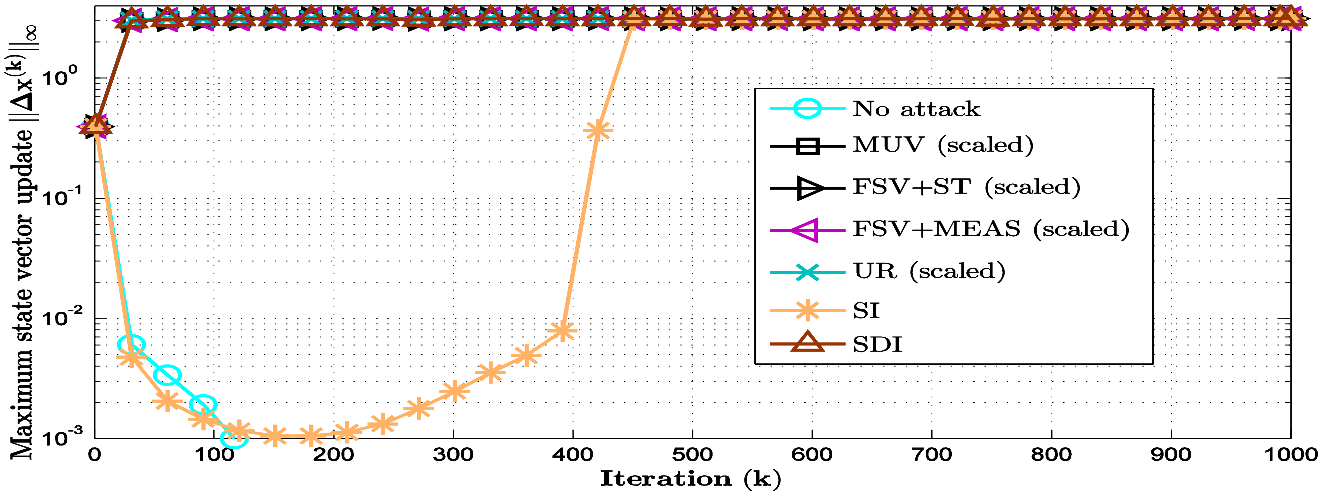
IEEE 118, 6 regions

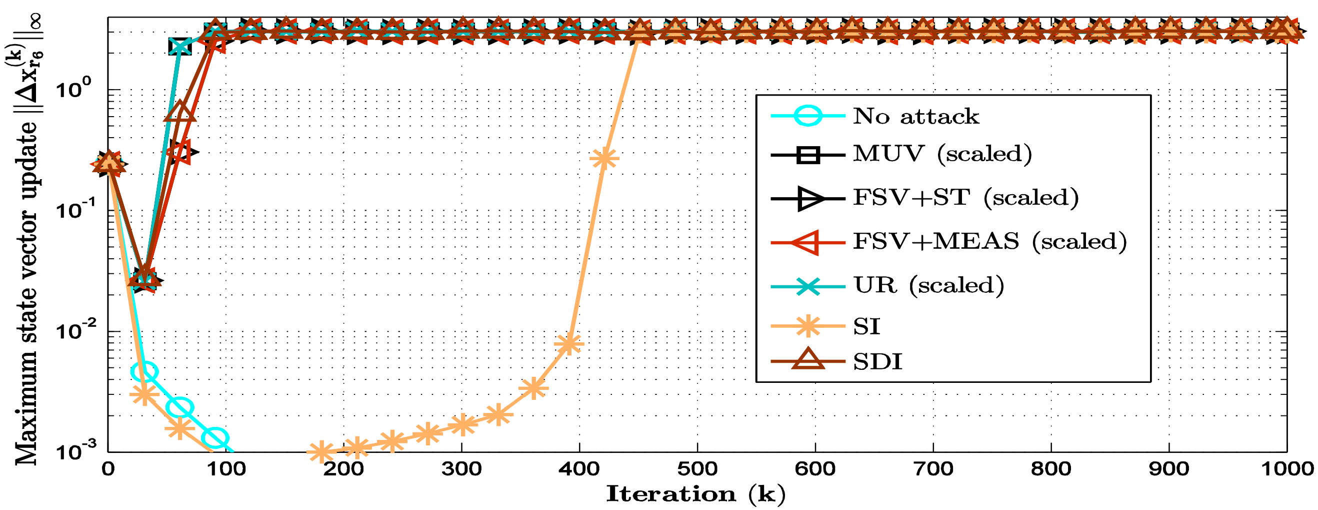




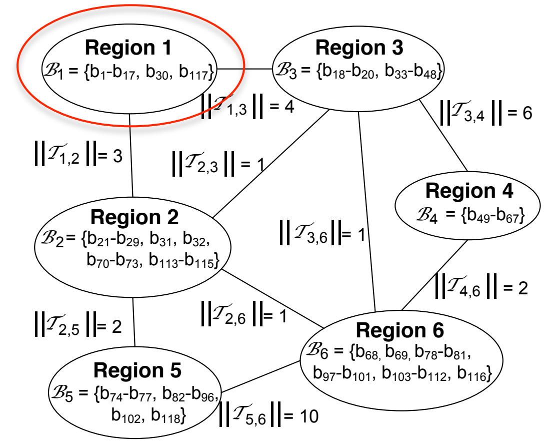
- ❑ Attack may significantly increase *c* and introduce high errors
- ❑ Attacks can prevent the convergence of DSE
- ❑ Protect *z*

Attack Impact





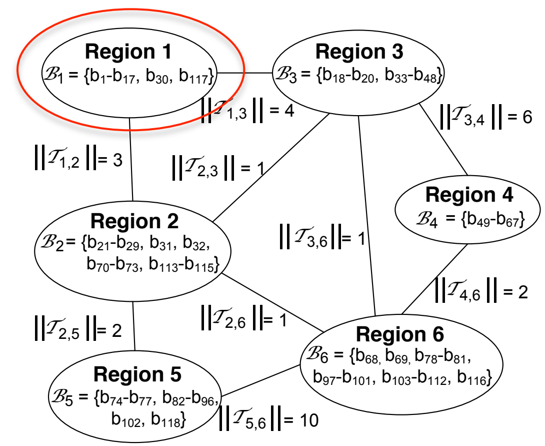
IEEE 118, 6 regions



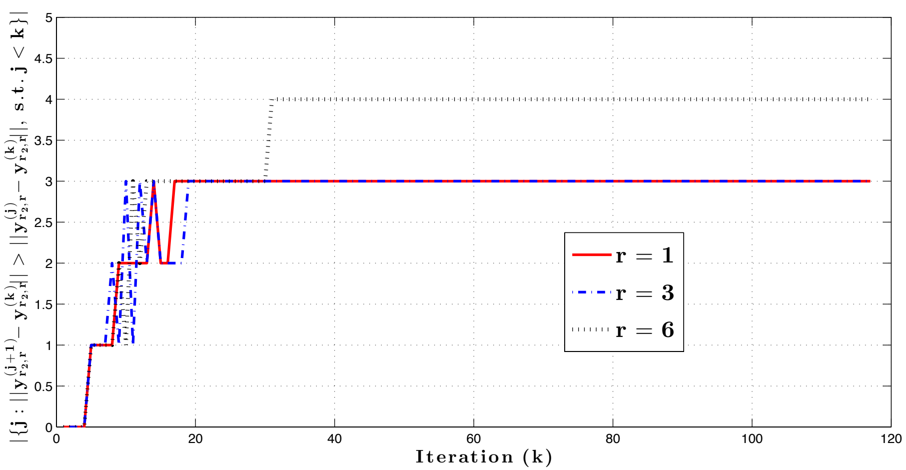
- ❑ All regions affected

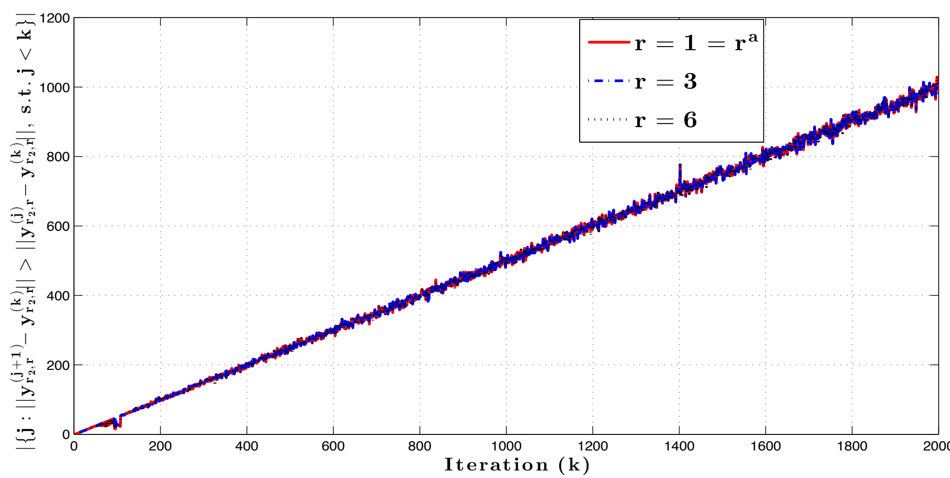
Detection and Mitigation

IEEE 118, 6 regions



- **Evolution of the state vector**
  - $x^{(k+1)} = g(x^{(k)})$, when converged $x^{(k^*+1)} \approx g(x^{(k^*+1)})$
  - If $||g(x)-x^*||_\infty \leq ||x-x^*||_\infty$ $(\forall x, \forall x^*)$, then $x(k)$ -> to a x^*
- **Detection based on the number of outliers**
  - $||x^{(k'+1)}-x^{(k)}||_\infty \leq ||x^{(k')}-x^{(k)}||_\infty$ for large k





- **The attack can be detected**
- **Mitigation: perform independent SE**

Conclusion

- Vulnerability of the DSE to attacks against exchanged data

- Multiple attack strategies
  - Even just one compromised CC can significantly disturb the DSE
  - Important to protect the confidentiality of measurements

- Detection and mitigation
  - Detection possible based on the number of outliers
  - A simple mitigation scheme

- *Localization and an improved mitigation scheme*

ACCESS
the future

On the Security of Distributed Power System State Estimation under Targeted Attacks

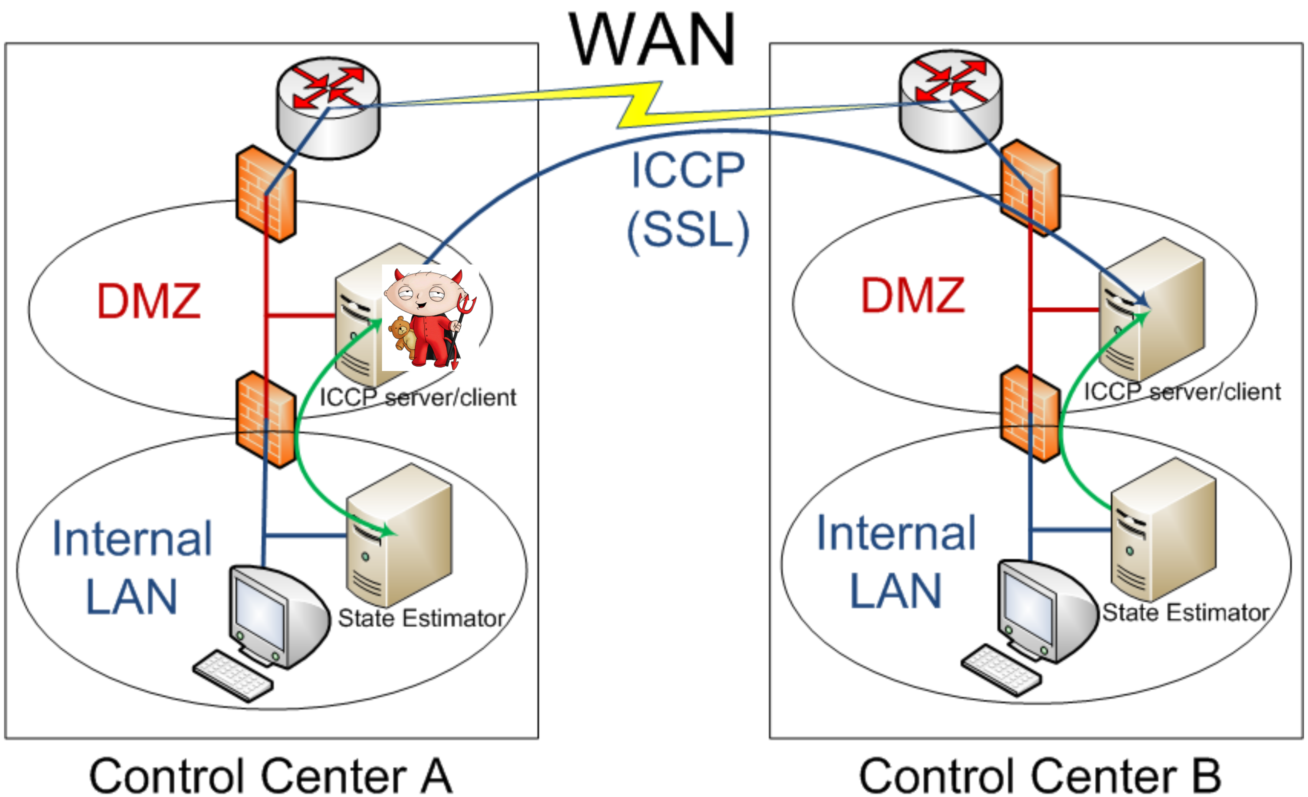
Ognjen Vuković, György Dán

School of Electrical Engineering, KTH Royal Institute of Technology
Stockholm, Sweden

ACM SAC
Coimbra, 19. March 2013

ICCP

- ICCP servers/clients are often in Demilitarized Zones (DMZ)



- Attacker corrupts ICCP server/client to modify the exchanged data