ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Cyber-Security of SCADA Systems

Göran Andersson
Power System Laboratory
ETH Zürich

Joint work with: Peyman Mohajerin Esfahani, Maria Vrakopoulou, Kostas Margellos, John Lygeros, André Teixeira, György Dàn, Henrik Sandberg, and Karl H. Johansson

Research supported by the European Commission under the **VIKING** project, FP7-ICT-SEC-2007-1

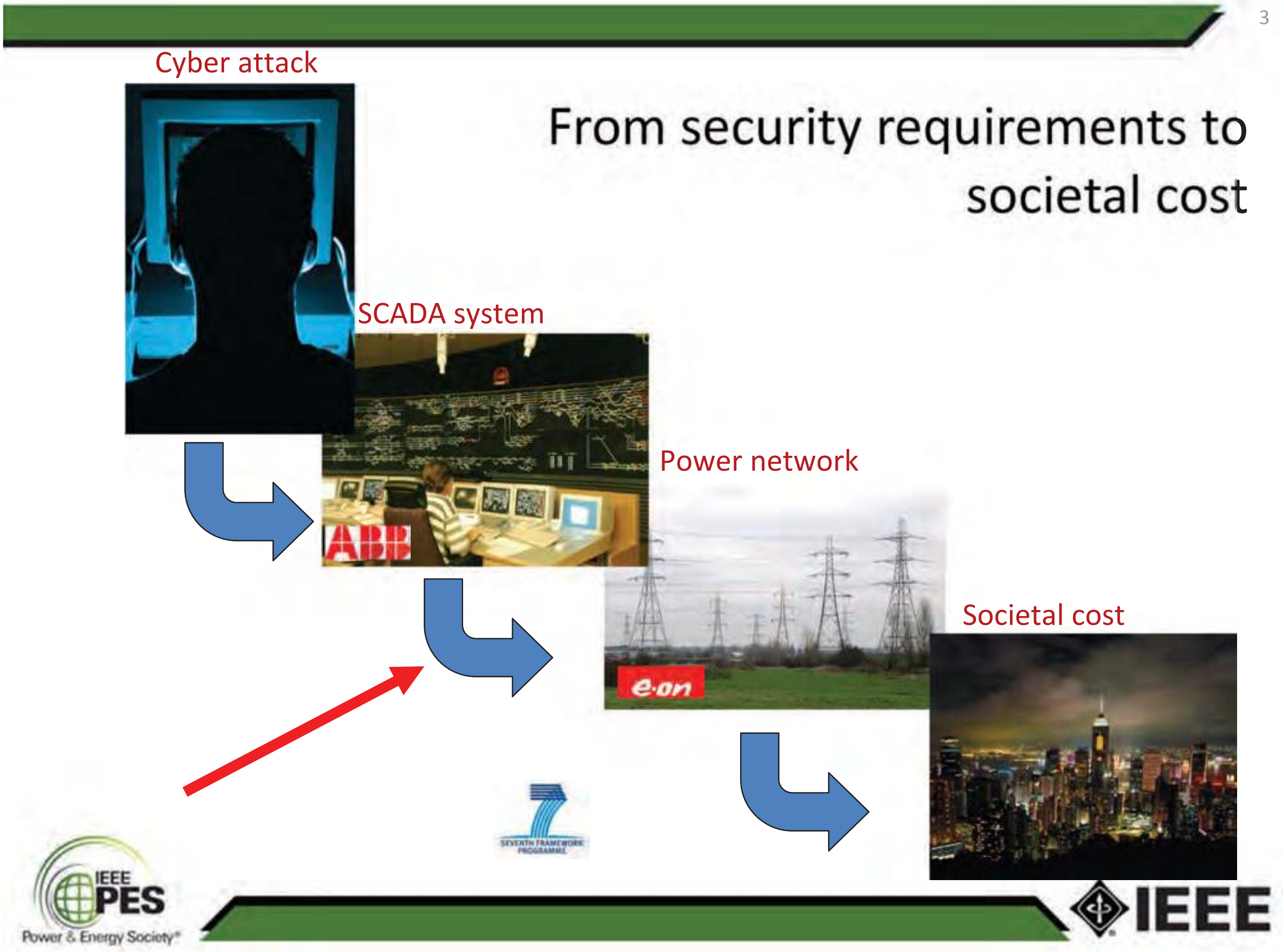
VIKING Projekt

VIKING

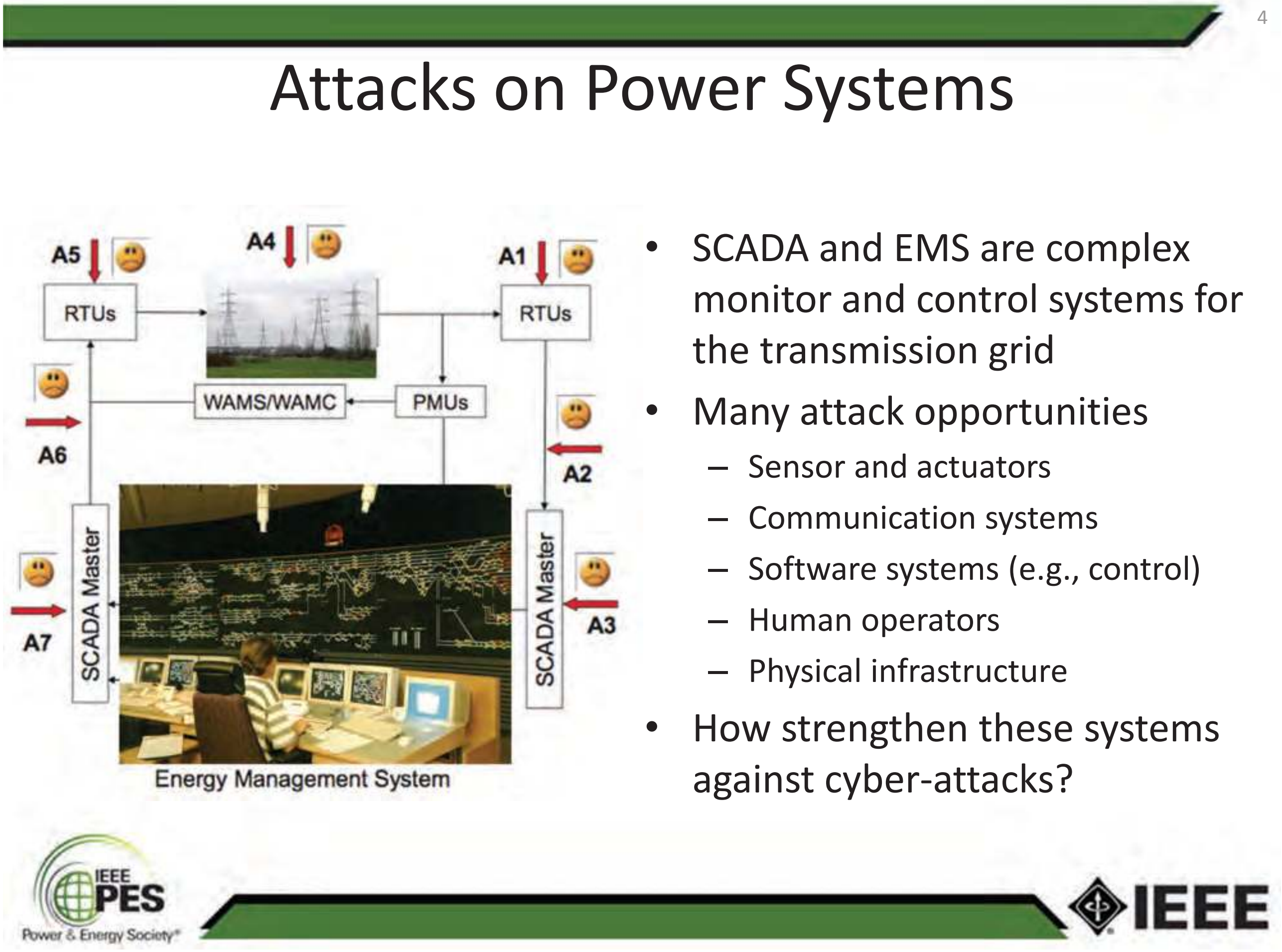
http://www.vikingproject.eu

The main objectives of VIKING are:

- To investigate the vulnerability of SCADA systems and the cost of cyber attacks on society
- To propose and test strategies and technologies to mitigate these weaknesses
- To increase the awareness for the importance of critical infrastructures and the need to protect them



From security requirements to societal cost



Attacks on Power Systems

- SCADA and EMS are complex monitor and control systems for the transmission grid
- Many attack opportunities
  - Sensor and actuators
  - Communication systems
  - Software systems (e.g., control)
  - Human operators
  - Physical infrastructure
- How strengthen these systems against cyber-attacks?

In this Presentation

- Attack on the Automatic Generation Control (AGC)
- Cyber security of State Estimators

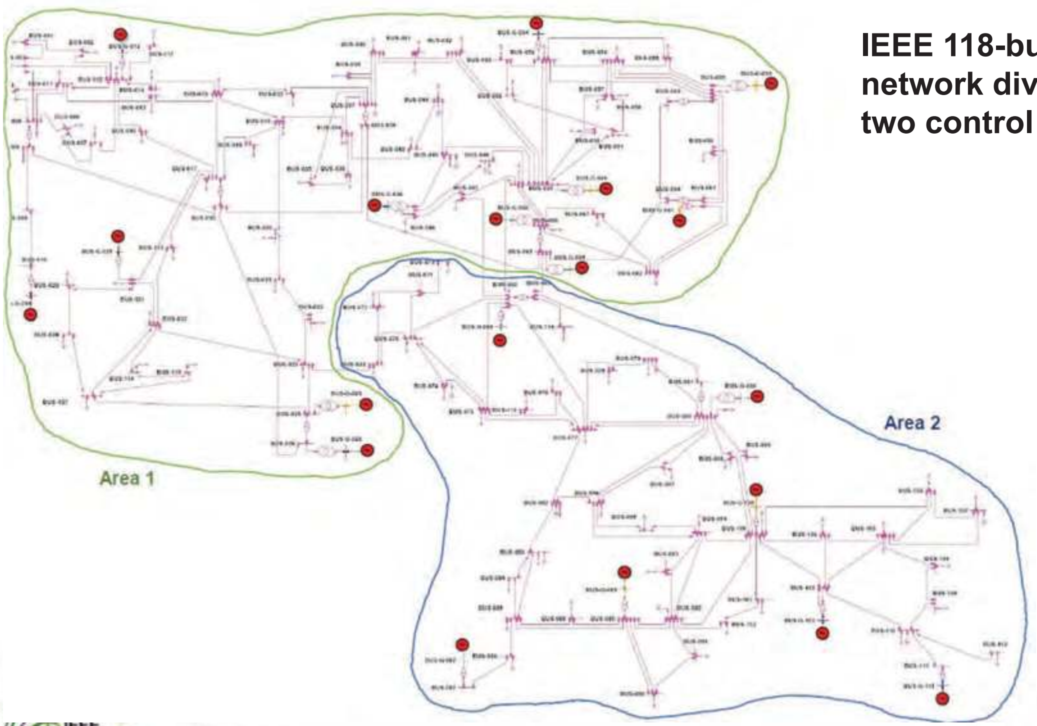
Which signals could be manipulated by a cyber-attack?

- Genetaror set points (**AGC**, etc)
- Load tap changers
- Status of switches
- Configuration changes (macros)

The AGC is one of very few automatically closed loop controllers of the SCADA system. (The only one?)

Can we find an attack signal that is able to lead our nominal state in unsafe operation?

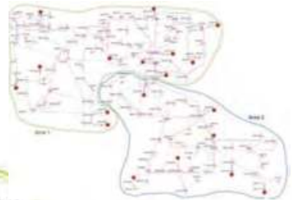
Test system: Two-Area Power Network

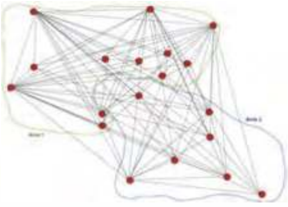


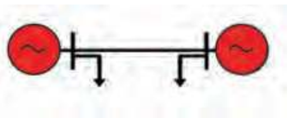
IEEE 118-bus network divided in two control areas

Two-Area Power System modeling

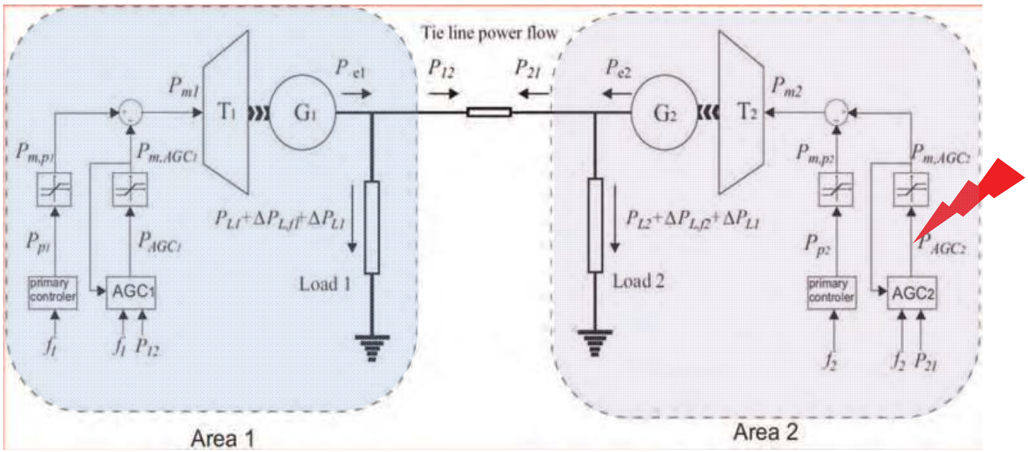
‘Full’ model	Multimachine classical model	Two machine frequency model
• **567** dynamic states • 236 algebraic states	• **59** dynamic states • no algebraic states	• **7** dynamic states • no algebraic states
• voltage + frequency dynamics	• frequency dynamics	• frequency dynamics
• AVR, PSS, governor, AGC	• Governor, AGC • Node elimination	• Governor, AGC • Center of H aggregation







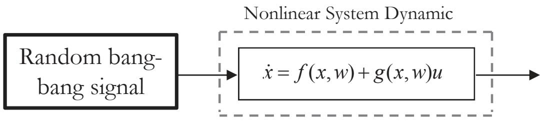
Two machine frequency model



- What can attacker do with access to AGC signal in one area?
- Can he cause frequency or power exchange range violations ?
  → Load shedding or generator tripping

Synthesizing an Attack Signal

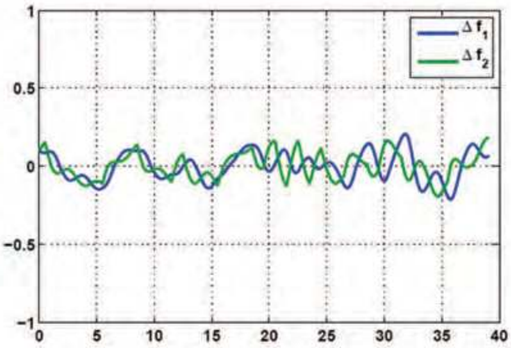
a) Random switching signal

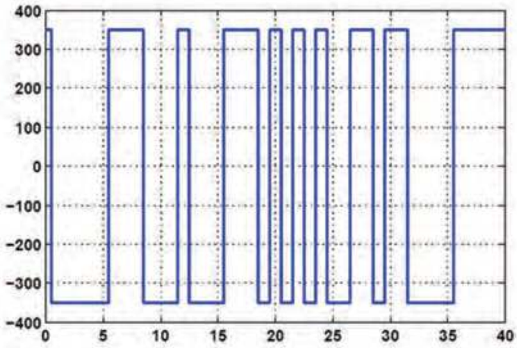


Nonlinear System Dynamic

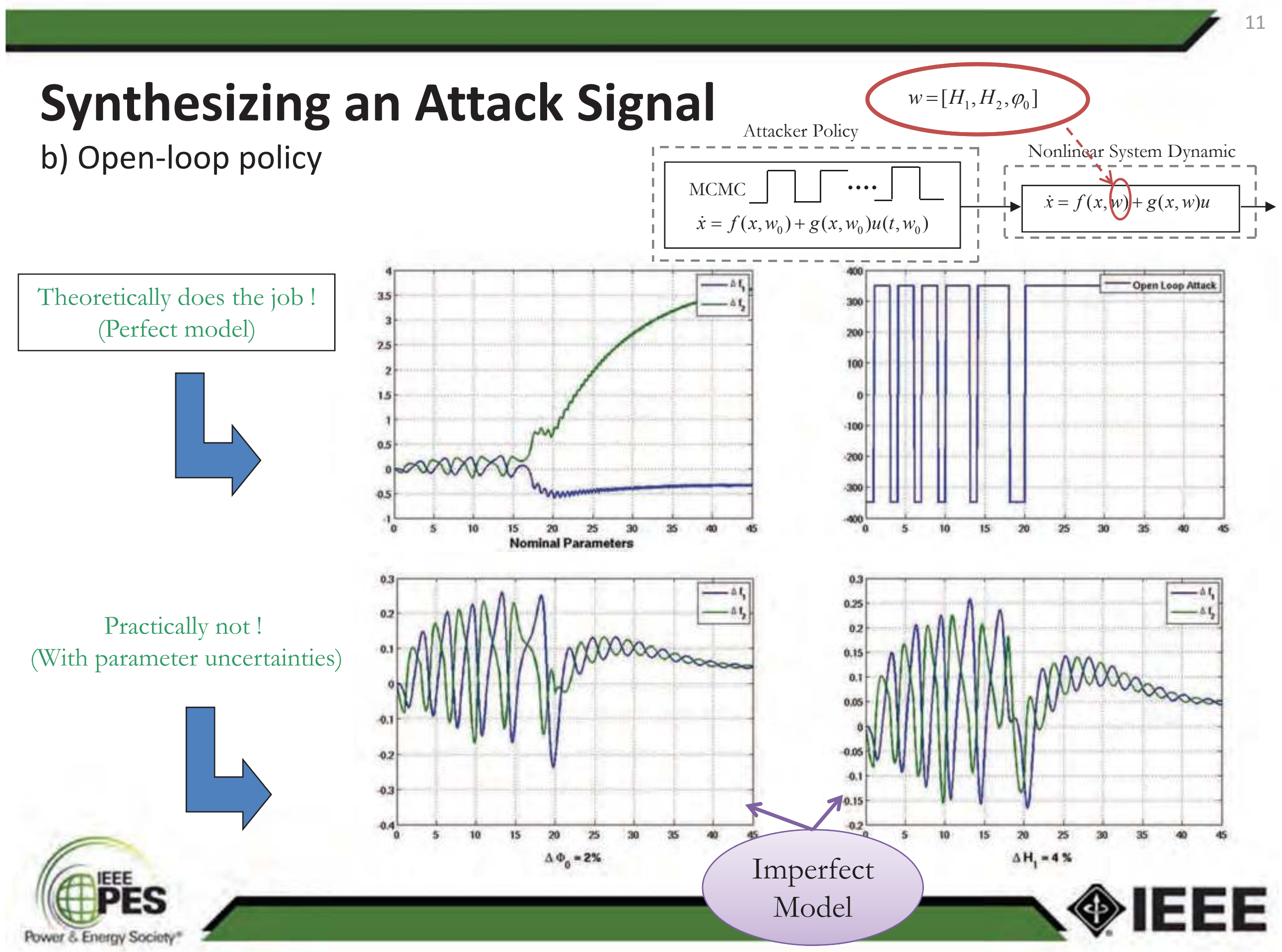
Random bang-bang signal

$\dot{x} = f(x,w) + g(x,w)u$





- ➢ Naïve attacker cannot violate frequency constraints !
- ➢ More intelligent policy is needed …



Synthesizing an Attack Signal

b) Open-loop policy

$w = [H_1, H_2, \varphi_0]$

Attacker Policy

MCMC

$\dot{x} = f(x, w_0) + g(x, w_0)u(t, w_0)$

Nonlinear System Dynamic

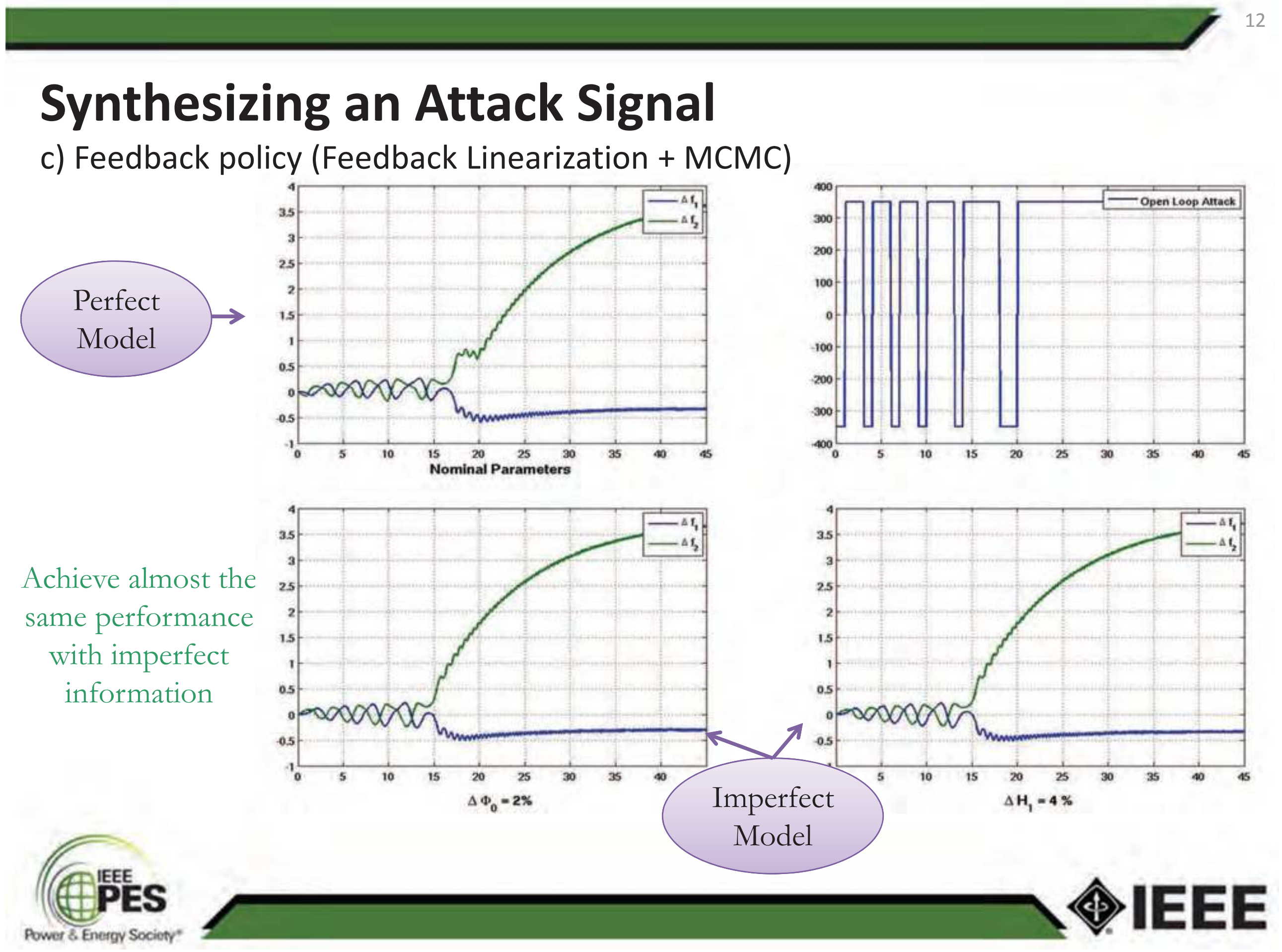
$\dot{x} = f(x, w) + g(x, w)u$

Theoretically does the job !
(Perfect model)

Practically not !
(With parameter uncertainties)

Imperfect
Model

Δf_1
Δf_2
Nominal Parameters
Open Loop Attack
$\Delta \Phi_0 = 2\%$
$\Delta H_1 = 4\%$



Synthesizing an Attack Signal

c) Feedback policy (Feedback Linearization + MCMC)

Perfect
Model

Achieve almost the
same performance
with imperfect
information

Imperfect
Model

Δf_1
Δf_2
Nominal Parameters
Open Loop Attack
$\Delta \Phi_0 = 2\%$
$\Delta H_1 = 4\%$

Outline

- Can attacker cause problems by manipulating AGC?

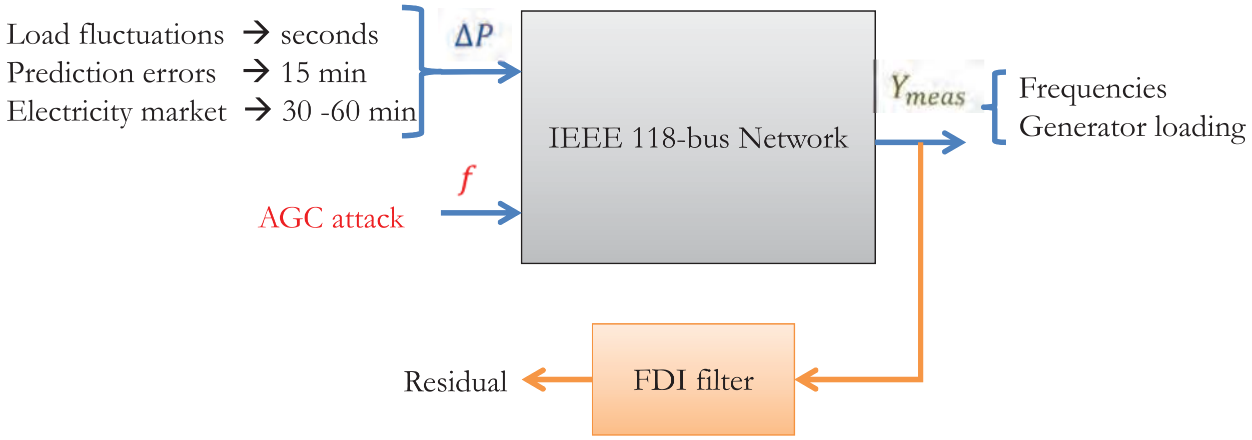
  Yes he can!

- How?

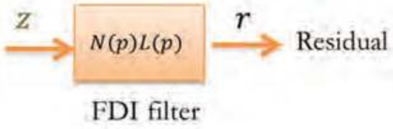
  With a fairly sophisticated feedback controller

- What can we do about it?

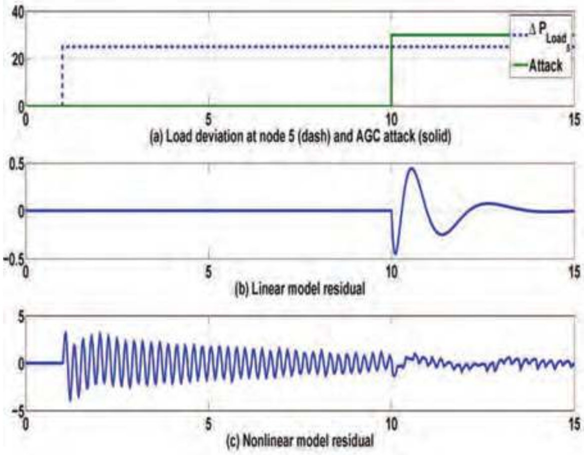
Fault Detection and Isolation (FDI) Problem



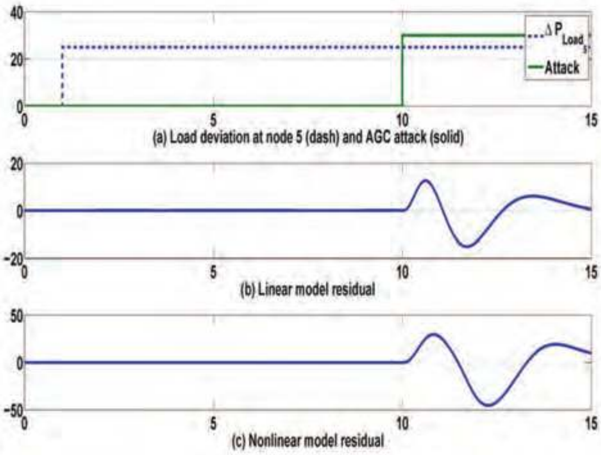
Simulation Results on Multimachine Classical Model



LP formulation

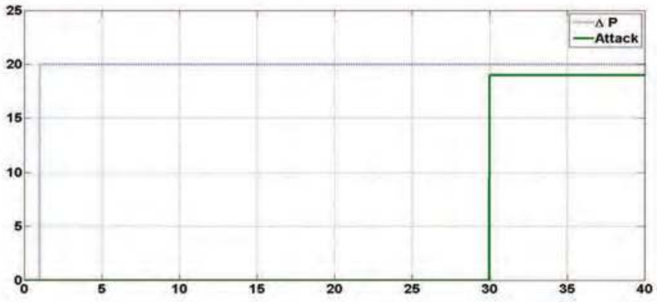


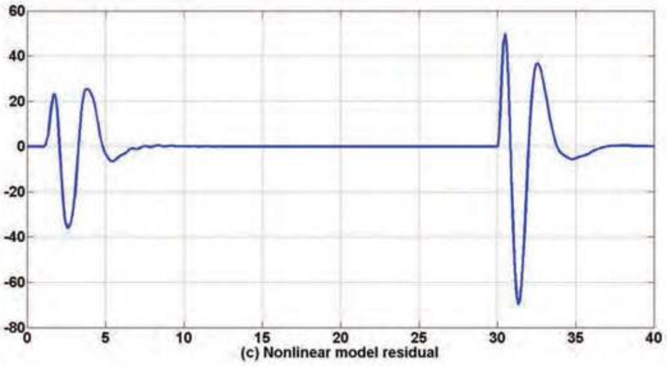
QP formulation



- ➢ Linearization based seems more sensitive in ideal setup, but not robust with respect to nonlinear terms
- ➢ Filter based on family of excitation signals is robust to load deviations at all nodes in the network

Simulation Results on Full Model



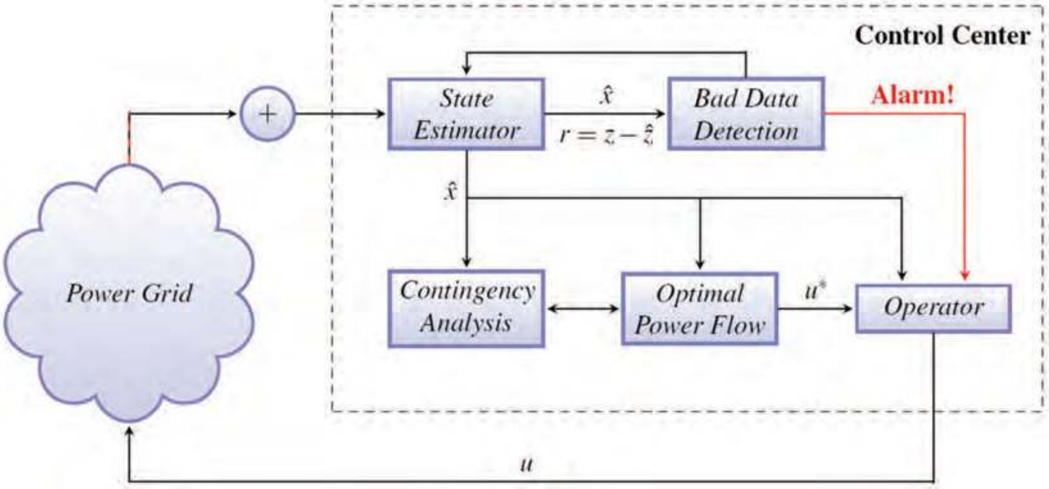


Despite of some obvious uncertainties, the filter works fairly well

In this Presentation

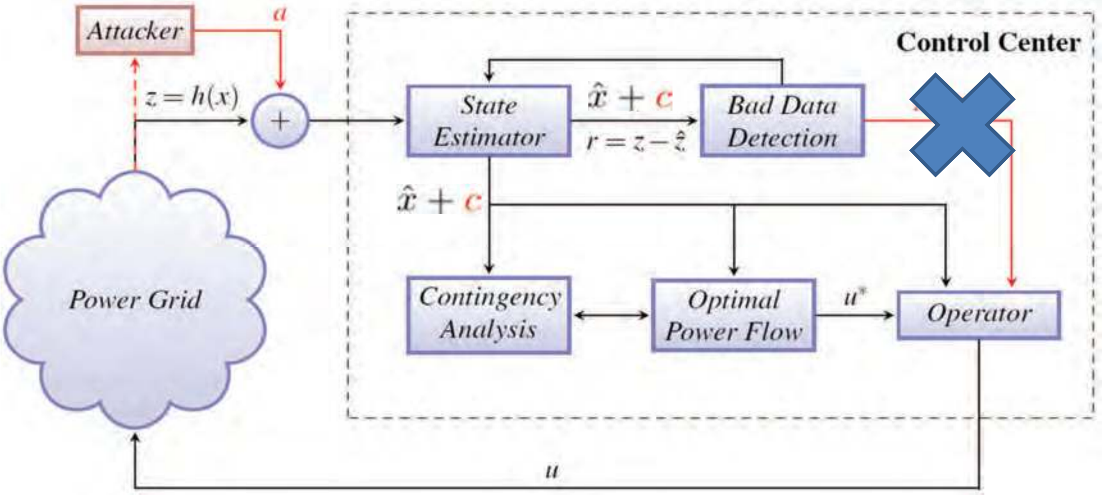
- Attack on the Automatic Generation Control (AGC)
- Cyber security of State Estimators

Energy Management System



- The **state estimator** has a crucial role in the EMS
- If the **bad data detector** identifies a faulty sensor, the corresponding measurement is removed from the state estimator
- Bad data detection is typically done under the assumption of **uncorrelated faults**, which does not hold for intelligent attacks

Attack Model

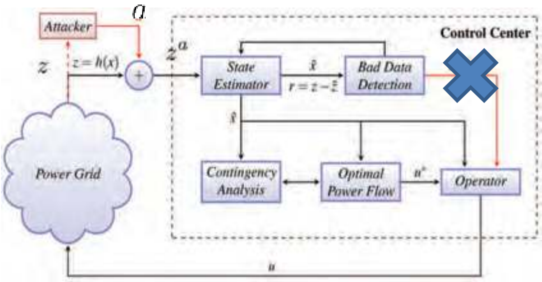


- **Scenario:** Attacker injects **malicious data** *a* to corrupt analog measurements in the power grid, in order to change state estimates without generating bad data detection alarm
- How characterize the set of **undetectable** malicious data *a*?

Minimum Effort Attack

$$\min_{a} \|a\|_p$$

$$\text{s.t.}\ \ a \in \mathcal{U} \cap \mathcal{G} \cap \mathcal{C}$$



- $\mathcal{U}$: set of stealthy attacks
- $\mathcal{G}$: set of attack goals, e.g., ”corrupt measurement k”
- $\mathcal{C}$: set of other constraints, e.g., sparsity, convergence

Security Index ρ_k

- Security index for measurement k: $\rho_k = \|a^*\|_0$
  - a^* is the optimal solution of

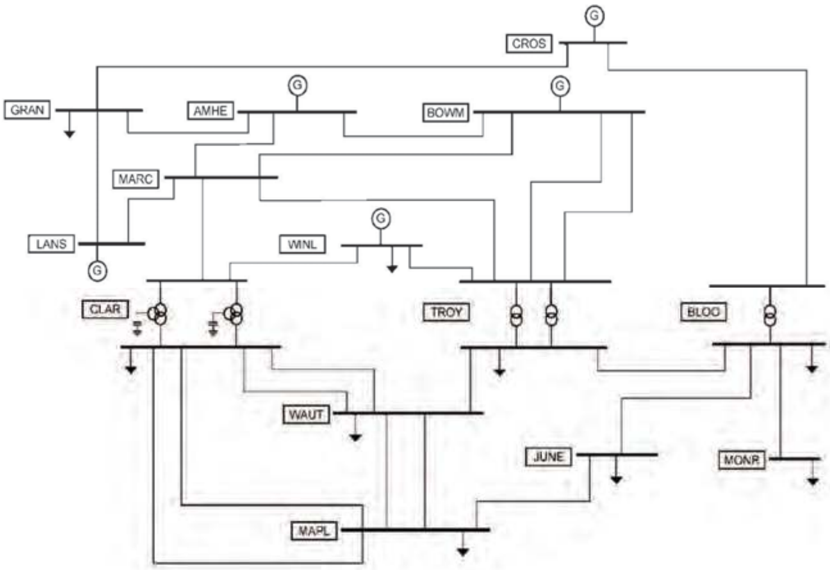
$$\min_a \|a\|_0$$
$$\text{s.t. } a \in \mathcal{U} \cap \mathcal{G}_k \cap \mathcal{C}$$

- $\mathcal{U} = \mathrm{Im}(H)$	Stealthy
- $\mathcal{G}_k = \{a \in \mathbb{R}^m : a_k = 1\}$	Corrupted
- $\mathcal{C} = \{a \in \mathbb{R}^m : a_i = 0 \quad \forall i \in \mathcal{P}\}$	Protected

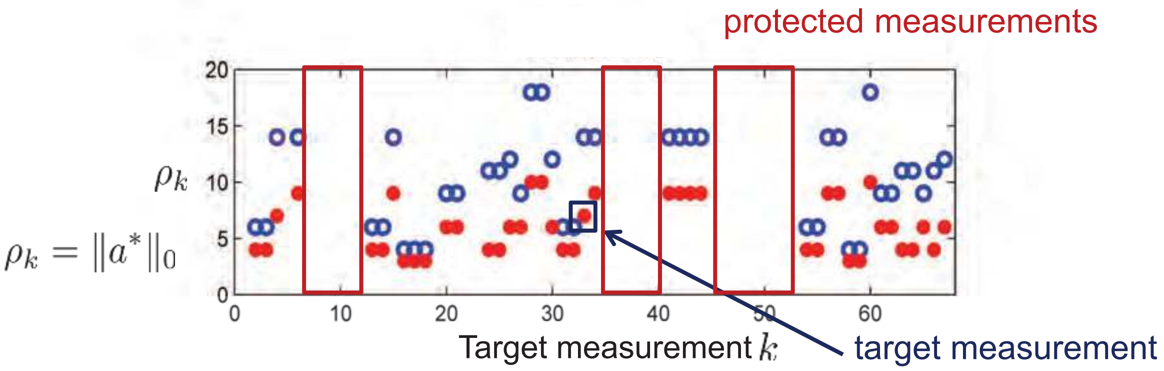
- ρ_k is the minimum number of measurements to manipulate for a successful attack

---

VIKING 40-bus Benchmark (IEEE 39-bus)



VIKING Benchmark: Security Index



protected measurements

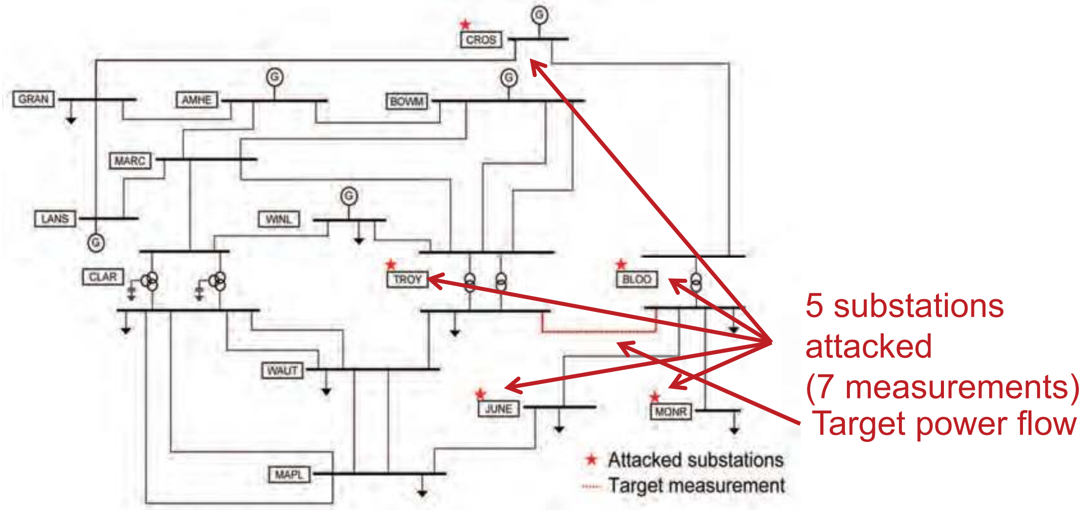
$\rho_k = \|a^*\|_0$

target measurement

Existing measurement configuration

Extended measurements configuration

VIKING Benchmark: Experimental Results



5 substations attacked
(7 measurements)
Target power flow

- Target measurement: flow between TROY and BLOO, z_{33}
- Nonlinear models are used by the SE and BDD
- Attacker knows the linear DC model accurately

VIKING Benchmark: Experimental Results

Attack on z_{33}

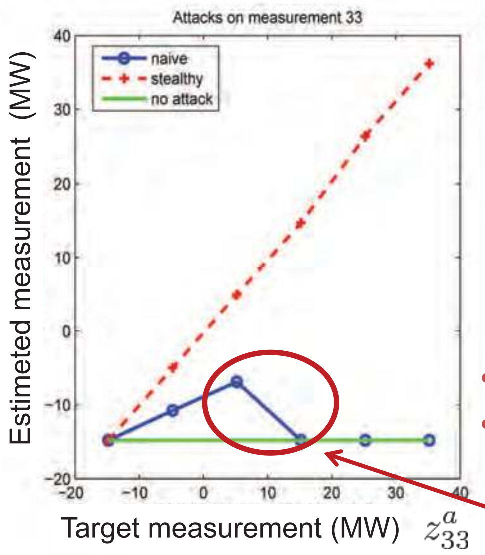


Table 1: Results from the stealthy attack for large bias

Target bias, a_{33}	False value (MW), z^a_{33}	Estimate (MW), $\hat{z}^a_{33}$	#BDD Alarms
0	-14.8	-14.8	0
50	35.2	36.2	0
100	85.2	86.7	0
150	135.2	137.5	0
200	185.2	-	-

- 150 MW was not detected (56% of nominal value)
- State estimator did not converge for 200 MW

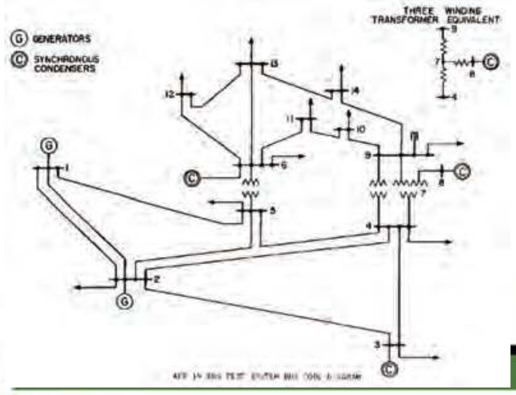
Bad data detected and removed

$$z^a = z + a$$

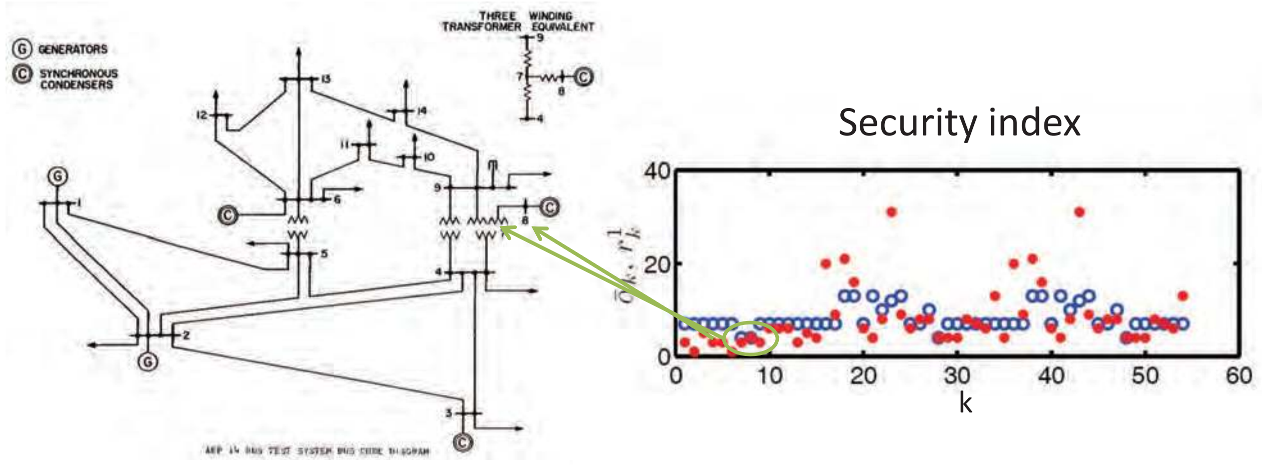
Protected Device Allocation

Protection against false-data deception attacks:

- Introduce protected measurements, immune to false data deception attacks (e.g, encryption)
- Where to allocate protected measurements to improve security the most?
- Improve ρ_k as much as possible, given limited number of protected measurements



Example: IEEE 14-bus Network

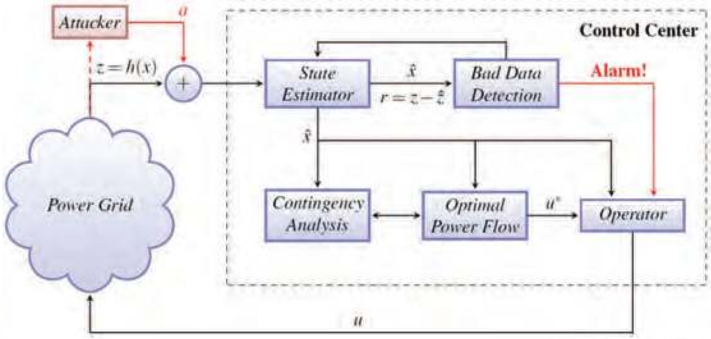


- Introduce protected device at the measurement with the smallest security index. Iterate.
- Allocate new secure measurements

Conclusions (SE attacks)

- Undetectable false-data attack against power systems state estimator possible, both in theory and practice
- New security index ρ_k to estimate vulnerabilities
- Suggests locations of encryption devices and other counter measures
- Experimental evaluation on real SCADA software

Nordic grid



Bibliography

- P. M. Esfahani, M. Vrakopoulou, G. Margellos, J. Lygeros, G. Andersson, "A Robust Policy for Automatic Generation Control Cyber Attack in Two Area Power Network", In Proceedings of the 49th Conference on Decision and Control, Atlanta, GA, USA, 2010
- P. M. Esfahani, M. Vrakopoulou, J. Lygeros, G. Andersson, " A Tractable Nonlinear Fault Detection An Isolation Technique with Application to Cyber-Physical Security in Power Systems", Submitted to ACC 2012
- G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in Proceedings of IEEE International Conference of Smart Grid Communications, 2010.
- A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator". In 18th IFAC World Congress, Milan, Italy, 2011.

Thank you!

?