



## Cyber-Security of Networked Control Systems

Karl Henrik Johansson  
 ACCESS Linnaeus Center  
 Royal Institute of Technology, Sweden

Joint work with Henrik Sandberg, André Teixeira, Kin C. Sou



Workshop on Cooperative Estimation and Control over Networks  
 Academy of Mathematics and Systems Science, CAS, Beijing, Jul 3, 2012



ROYAL INSTITUTE  
OF TECHNOLOGY

## ACCESS Linnaeus Center

- ACCESS was established at KTH from an Excellence Grant from the Swedish Research Council
- Developed into **one of Europe's largest university research centers** in networked systems
  - 36 faculty, 20 postdocs, >100 PhD students
  - Basic funding from VR on 1.3 MEUR per year
  - Total research budget 2010 over 12 MEUR
- Graduate school with **>40 graduated PhD's**
- **Faculty renewal** and mobility programs
- Extensive international and industrial collaborations
- External communication and dissemination



2



## Recent Cyber-Attacks on Control Systems

**The Washington Post**

**U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say**

By Ellen Nakashima, Greg Miller and Julie Tate, Published: June 19

The United States and Israel jointly developed a sophisticated computer virus nicknamed Flame that collected intelligence in preparation for cyber-sabotage aimed at slowing Iran's ability to develop a nuclear weapon, according to Western officials with knowledge of the effort.

The [mainline sites of malware](#) secretly mapped and monitored Iran's computer networks, sending back a steady stream of intelligence to prepare for a cyberwarfare campaign, according to the officials.

The effort, involving the National Security Agency, is believed to have caused malfunctions in Iran's nuclear energy program.

**BBC NEWS TECHNOLOGY**

29 June 2012 Last updated at 10:54 GMT

**Researchers use spoofing to 'hack' into a flying drone**

American researchers took control of a flying drone by tracking into its GPS system (E644) data from the US Homeland Security (DHS).

as at Austin team used techniques where the drone is hijacked from hackers for the one minutes.

may have been used to rone in Iran in 2011.

Drones are mostly used for military operations

---

**The Register**

Hardware Software Music & Media Networks Security Cloud Public Sector Business Jobs

Operating Systems Applications Developer Microbite

Hacker jailed for revenge sewage attacks  
Job rejection caused a bit of a stink

By Tony Smith • Get more from this author

Posted in Software, 31st October 2011 15:55 GMT

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

**CBS NEWS**

11/9/2009

**Cyber War: Sabotaging the System**

60 Minutes: Former Chief of National Intelligence Says U.S. Unprepared for Cyber Attacks

(CBS) Nothing has ever changed the world as quickly as the Internet has. Less than a decade ago, "60 Minutes" went to the Pentagon to do a story on something called information warfare, or cyber war as some people called it. It involved using computers and the Internet as weapons.

Much of it was still theory, but we were told that before too long it might be possible for a hacker with a computer to disable critical infrastructure in a major city and disrupt essential services, to steal millions of dollars from banks all over the world, infiltrate defense systems, extort millions from public companies, and even sabotage our weapons systems.

---

**Bits**

Hacker jailed for revenge sewage attacks  
Job rejection caused a bit of a stink

By Tony Smith • Get more from this author

Posted in Software, 31st October 2011 15:55 GMT

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

**Malware Hits Computerized Industrial Equipment**

The technology industry is being rattled by a quiet and sophisticated malicious software program that has infiltrated factory computers.

The malware, known as Stuxnet, was discovered by VirusBlokAda, a Belarusian computer security company in July, at least several months after its creation.

Security experts say Stuxnet attacked the software in specialized industrial control equipment made by Siemens by exploiting a previously unknown hole in the Windows operating system.

The malware is the first such attack on critical industrial infrastructure that sits at the foundation of modern economies.

## Cyber-Security of Networked Control Systems

- Networked control systems are to a growing extent based on **open communication and software technology**
- Leads to **increased vulnerability** to cyber-threats with many potential points of attacks

- How to model attacks?
- How to measure vulnerability?
- How to compute consequences?
- How to design secure control systems

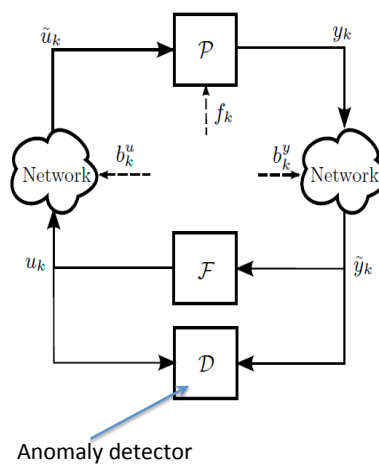
- Traditional computer and information security do not provide answers these questions
- Need for a theory for secure control systems

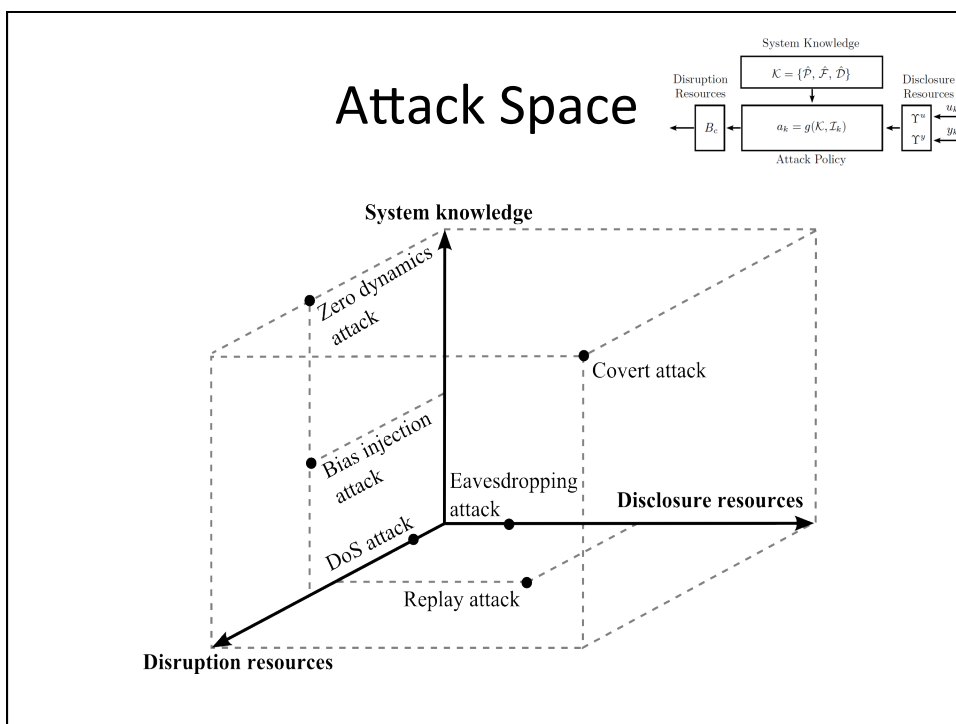
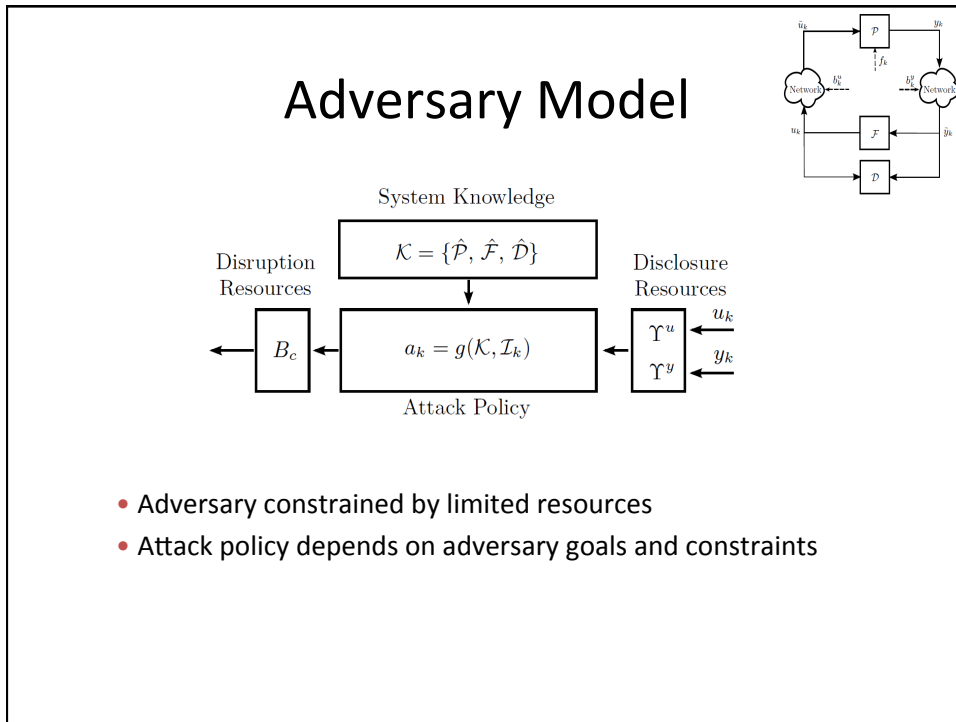
The diagram illustrates a networked control system. At the top, three actuators (a1, a2, a3) and four sensors (s1, s2, s3, s4) are connected to a central 'Physical Plant' block. The Physical Plant is connected to a 'Communication Network' cloud. Below the network are three 'Distributed Controllers' (C1, C2, C3). Red arrows indicate potential attack points on the communication links between the actuators/sensors and the network, and between the network and the controllers.

## Outline

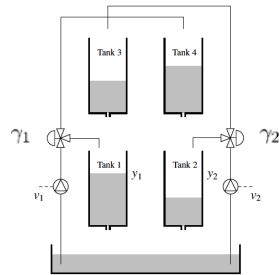
- Introduction
- Attack model for control systems
- Attack on power network state estimator
- Stealthy minimum-effort attacks
- Security index
- Conclusions
- Biography

## Networked Control System under Attack



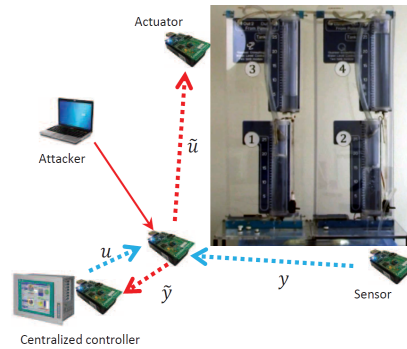


## Experimental Set-Up



$$\frac{dx}{dt} = \begin{bmatrix} -\frac{1}{T_1} & 0 & \frac{A_3}{A_1} \gamma_3 & 0 \\ 0 & -\frac{1}{T_2} & 0 & \frac{A_4}{A_2} \gamma_4 \\ 0 & 0 & -\frac{1}{T_3} & 0 \\ 0 & 0 & 0 & -\frac{1}{T_4} \end{bmatrix} x + \begin{bmatrix} \frac{\gamma_1 k_1}{A_1} & 0 \\ 0 & \frac{\gamma_2 k_2}{A_2} \\ 0 & \frac{(1-\gamma_2)k_2}{A_3} \\ \frac{(1-\gamma_1)k_1}{A_4} & 0 \end{bmatrix} u$$

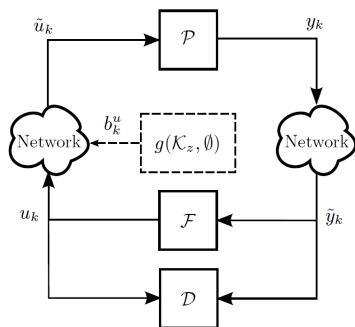
$$y = \begin{bmatrix} k_c & 0 & 0 & 0 \\ 0 & k_c & 0 & 0 \end{bmatrix} x$$



Quadruple-tank process has non-minimum-phase zero if  $0 < \gamma_1 + \gamma_2 < 1$

[J, 2000]

## Zero Dynamics Attack



- Zero dynamics are characterized by:

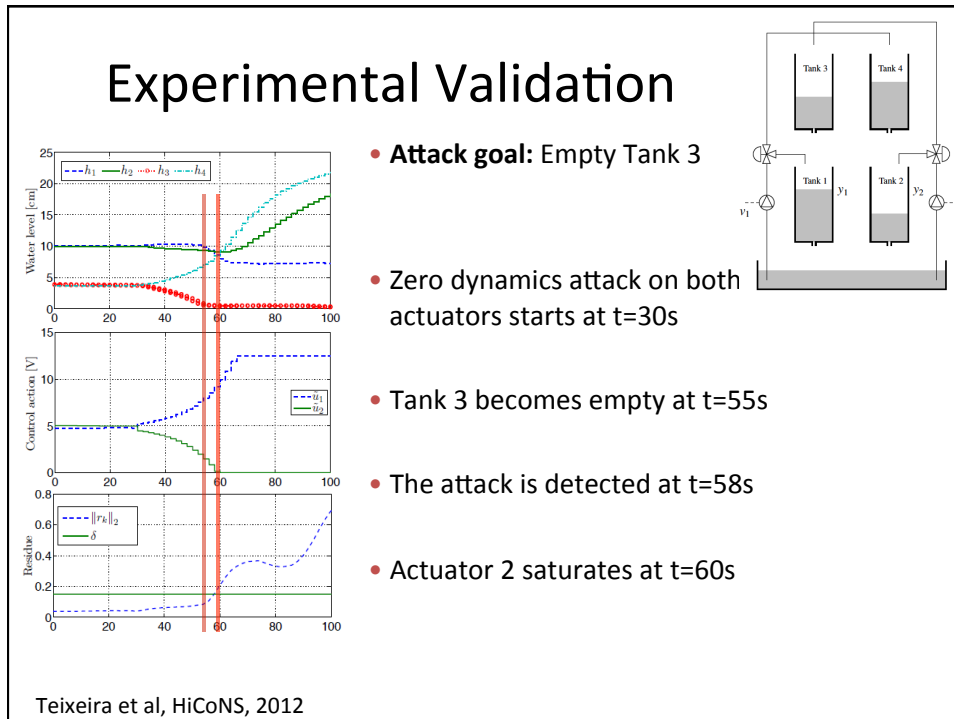
$$\begin{bmatrix} \nu I - A & -B \\ C & 0 \end{bmatrix} \begin{bmatrix} x_0 \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

- Suggests attack on actuators with policy:

$$a_k = g\nu^k$$

- If the zero is unstable, then the plant state can be moved by this attack without detection

- Requires system knowledge (zero dynamics) but no disclosure resources



## Outline

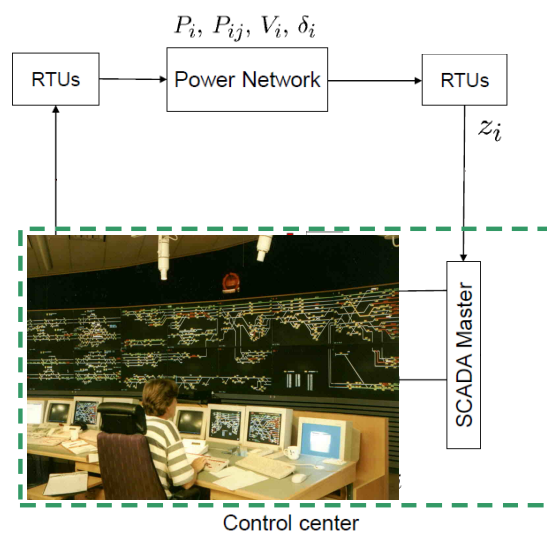
- Introduction
- Attack model for control systems
- Attack on power network state estimator
- Stealthy minimum-effort attacks
- Security index
- Conclusions
- Biography

## Motivation

- Northeast blackout Aug 14, 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 systems with similar consequences pose a substantial threat

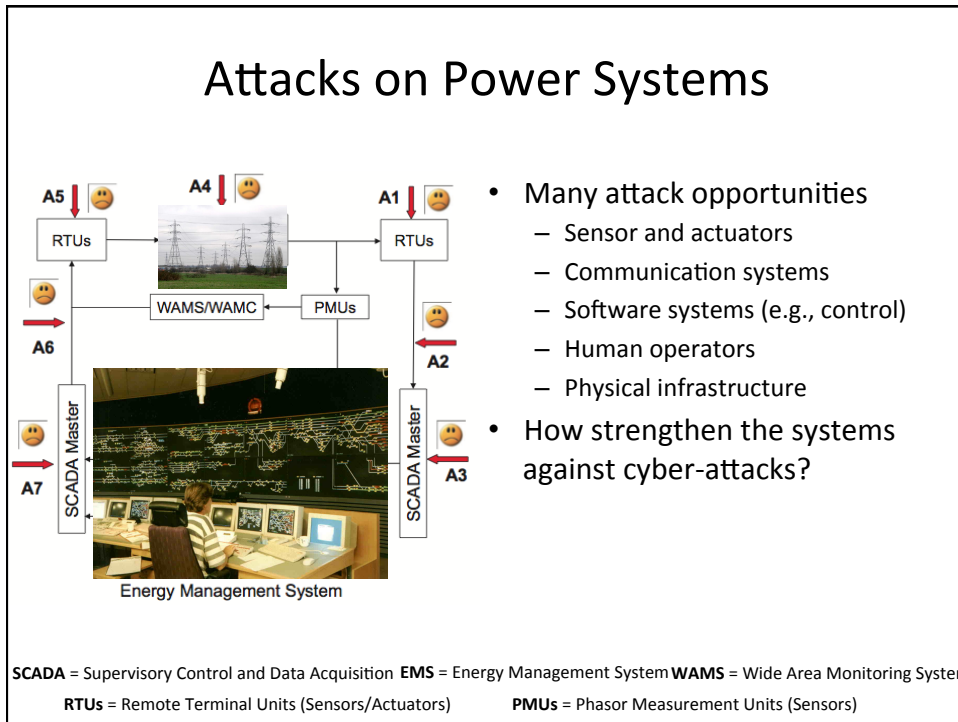


## SCADA/EMS Systems



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

## Attacks on Power Systems



## (Static) Power Network Model

- Local states at bus  $i$ :

- $\theta_i$  – phase angle
- $V_i$  – voltage magnitude

- Active and reactive power injections:

$$P_i = V_i \sum_{j \in N_i} V_j (G_{ij} \cos \theta_{ij} + B_{ij} \sin \theta_{ij})$$

$$Q_i = V_i \sum_{j \in N_i} V_j (G_{ij} \sin \theta_{ij} - B_{ij} \cos \theta_{ij})$$

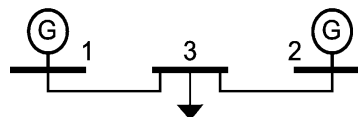
- Active and reactive power flows:

$$P_{ij} = V_i^2 (g_{si} + g_{ij}) - V_i V_j (g_{ij} \cos \theta_{ij} + b_{ij} \sin \theta_{ij})$$

$$Q_{ij} = -V_i^2 (b_{si} + b_{ij}) - V_i V_j (g_{ij} \sin \theta_{ij} - b_{ij} \cos \theta_{ij})$$

where

$$\theta_{ij} = \theta_i - \theta_j$$



- Measurement model:

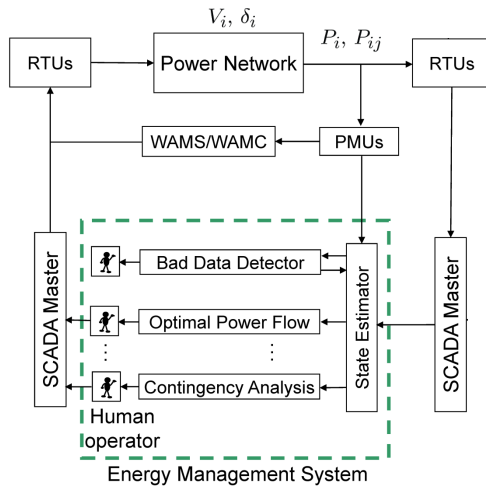
$$z = h(x) + \epsilon$$

- $x \in \mathbb{R}^n$  : network states
- $z \in \mathbb{R}^m$  : power flow measurements
- $\epsilon$  : measurement noise

Static model because the power grid time constant  $\sim 10$  ms is beyond existing measurement technology. Typical sampling time  $\sim 1$  s.



## Energy Management System for Power Networks



- SCADA-EMS provides power network state information to
  - Identify faulty equipment
  - Optimize power flows
  - Analyze reliability (contingency)
  - Etc
- Large system with slow sampling
  - 100-1 000's of RTUs sampled in sec's
  - 10K-40K measurements
- Decisions taken by human operators

**Remark**

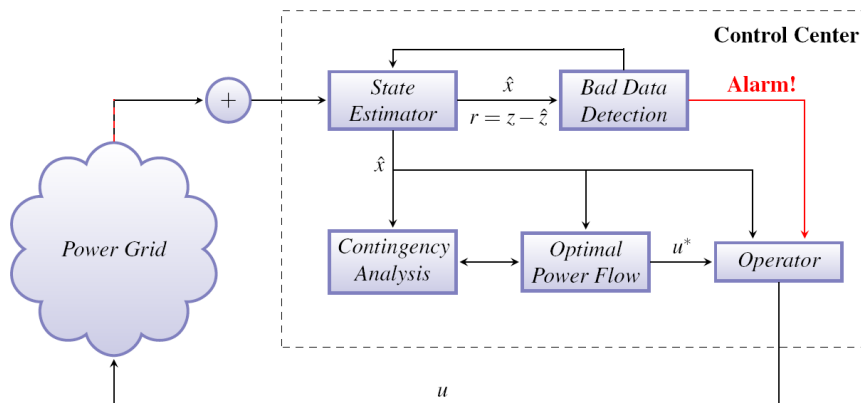
New WAMCs based on high-rate PMUs are better protected but constitute only a small portion of the overall network

WAMC = Wide Area Monitoring and Control System

RTUs = Remote Terminal Units (Sensors/Actuators)

PMUs = Phasor Measurement Units (Sensors)

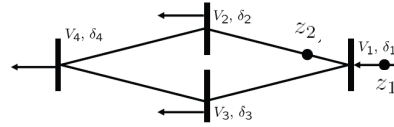
## Energy Management System



- 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

## State Estimator

- 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  $\hat{\delta}_i$  (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):

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z \quad H := \left. \frac{\partial h(x)}{\partial x} \right|_{x=\hat{x}}$$

E.g., [Schweppe and Wildes, 1970; Abur and Exposito, 2004]

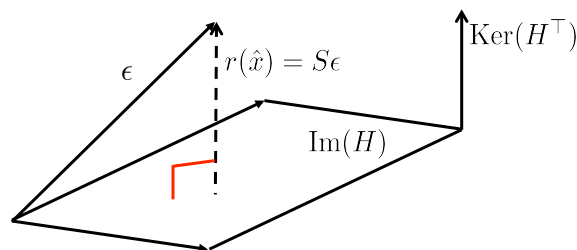
## Bad Data Detector

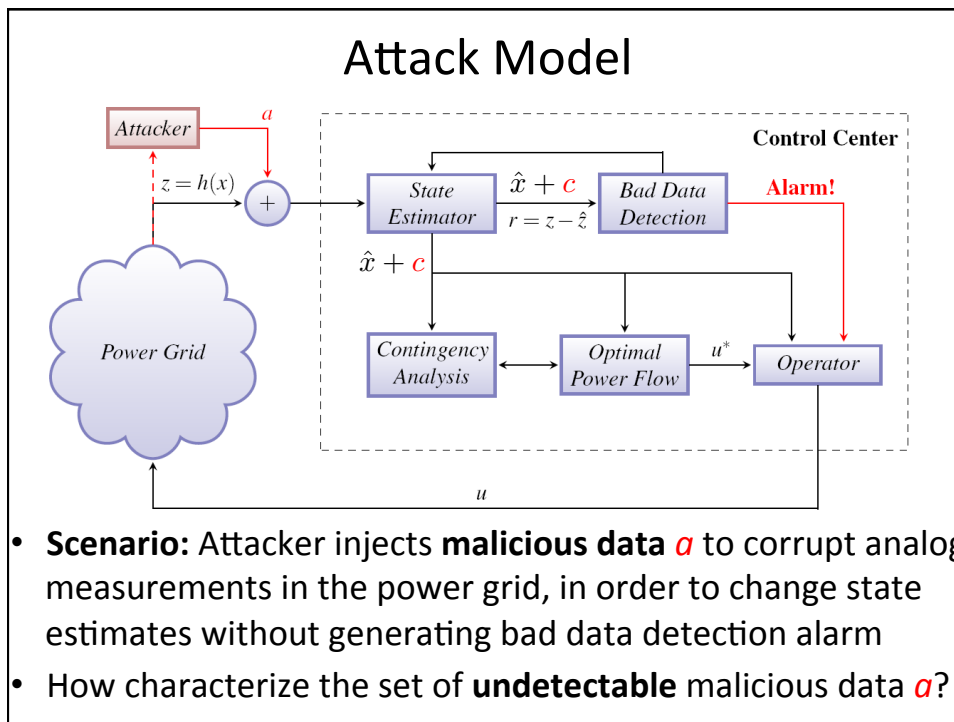
$$H = \left. \frac{\partial h(x)}{\partial x} \right|_{x=\hat{x}}$$

- Today's BDD is based on measurement residual  $r(\hat{x}) = z - h(\hat{x})$

$$\|W r(\hat{x})\|_p \underset{H_1}{\overset{H_0}{\leq}} \tau$$

- For the Gauss-Newton method:  $r(\hat{x}) \approx (I - H(H^T H)^{-1} H^T) \epsilon = S \epsilon$
- Note that  $S = \mathbf{P}_{\text{Ker}(H^T)}$  is the orthogonal projection onto  $\text{Ker}(H^T)$
- Can be exploited by an attacker

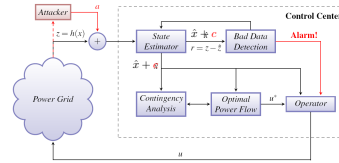




## Outline

- Introduction
- Attack model for control systems
- Attack on power network state estimator
- **Stealthy minimum-effort attacks**
- Security index
- Conclusions
- Biography

## Bad-Data Detection and Stealthy Attacks



- Bad-data detection trigger alarm when residual  $r$  is large

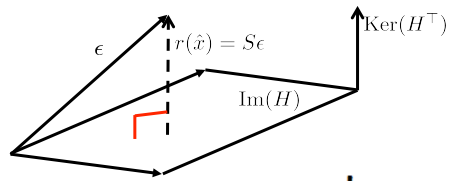
$$r := z - \hat{z} = z - H\hat{x} = z - H(H^T R^{-1} H)^{-1} H^T R^{-1} z$$

- Characterization of undetectable malicious data  $a$

$$z_a := z + a$$

$$a = Hc \in \text{Im}(H)$$

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



- The attacker has a lot of freedom in the choice of  $a$ !
- Attacker likely to seek sparse solutions  $a$ , i.e., manipulate only few measurements

[Liu et al., 2009]

## Stealthy Minimum-Effort Attack

- Attack single measurement  $z_k$

$$\min_a \|a\|_2$$

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

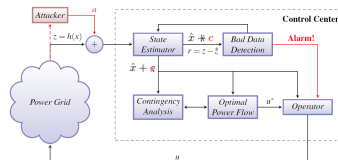
- $\mathcal{U} = \text{Im}(H)$
- $\mathcal{G}_k = \{a \in \mathbb{R}^m : a_k = 1\}$
- $\mathcal{C} = \mathbb{R}^m$

- Optimal attack

$$a^* = K_k^{-1} K e_k$$

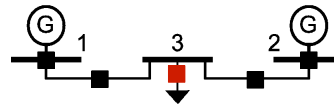
$$K = H H^\dagger$$

- $a^*$  is typically not sparse, so many sensors need to be corrupted
- Consider **0-norm** instead of 2-norm



## Stealthy Minimum-Effort Attack

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



- $P_3$  is the target measurement
- A few possible attacks:
  - ~~$\{P_3\}, \{P_3, \star\}$~~  not stealthy
  - $\{P_1, P_{13}, P_3\}$  minimum effort
  - $\{P_2, P_{23}, P_3\}$  effort
  - $\{P_1, P_{13}, P_3, P_{23}, P_2\}$

## Security Index $\rho_k$

- Security index for measurement k:  $\rho_k = \|a^*\|_0$

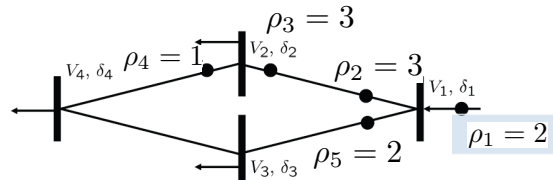
- $a^*$  is the optimal solution of

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

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

- $\rho_k$  is the minimum number of measurements to manipulate for a successful attack

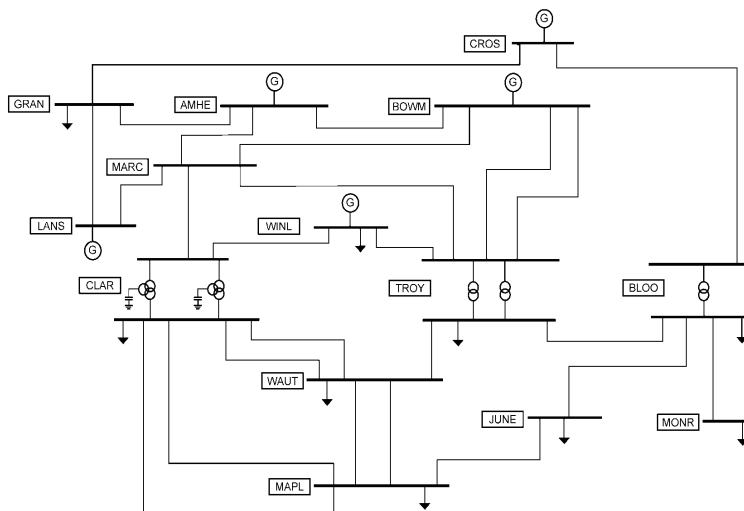
## Example



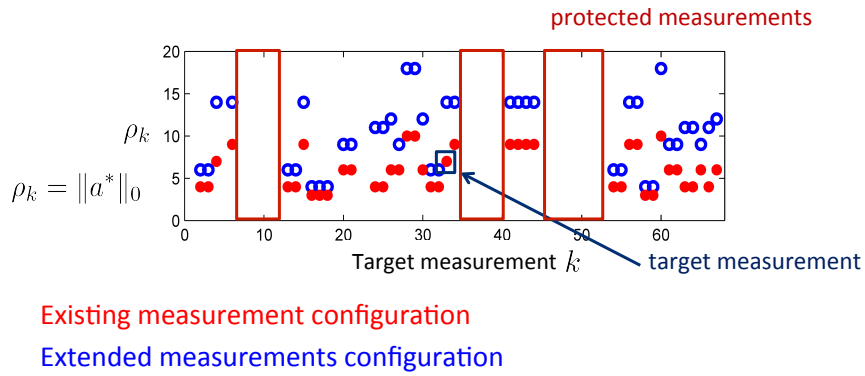
- Sparse attack corresponding to  $\rho_k$ :
 
$$(a_1 \ a_2 \ a_3 \ a_4 \ a_5) = \begin{pmatrix} 1 & 1 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$
- Compare with the “hat matrix”:
 
$$\begin{pmatrix} \hat{z}_1 \\ \hat{z}_2 \\ \hat{z}_3 \\ \hat{z}_4 \\ \hat{z}_5 \end{pmatrix} = \begin{pmatrix} 0.60 & 0.20 & -0.20 & 0 & 0.40 \\ 0.20 & 0.40 & -0.40 & 0 & -0.20 \\ -0.20 & -0.40 & 0.40 & 0 & 0.20 \\ 0 & 0 & 0 & 1.00 & 0 \\ 0.40 & -0.20 & 0.20 & 0 & 0.60 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \end{pmatrix}$$

$$= H(H^T R^{-1} H)^{-1} H R^{-1}$$
- Hat matrix misleading for judging sparsity of attacks!

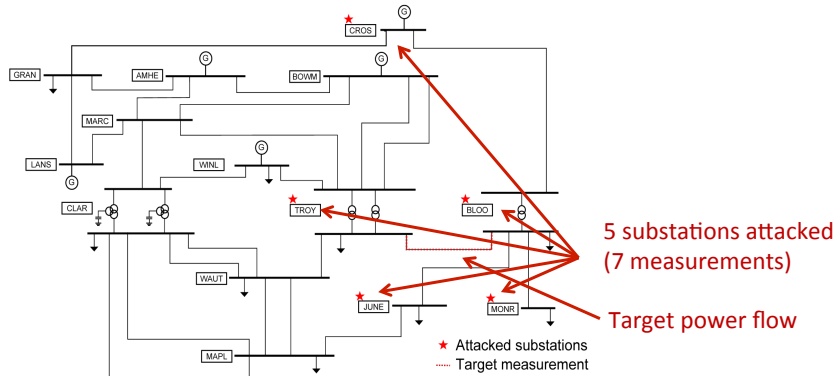
## VIKING 40-bus Benchmark



## VIKING Benchmark: Security Index

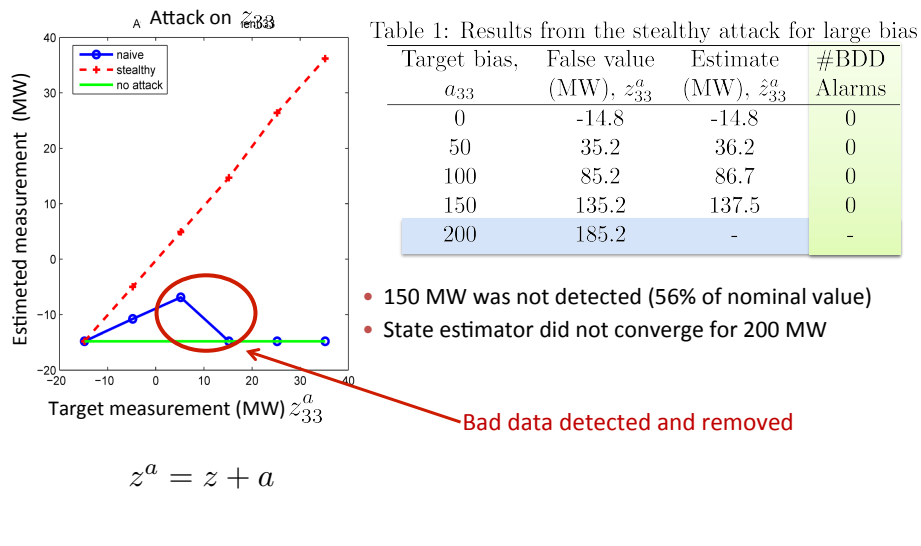


## VIKING Benchmark: Experimental Results



- Target measurement: flow between TROY and BLOO,  $z_{33}$
- Nonlinear models are used by the state estimator and bad data detector
- Attacker knows the linear DC model accurately

## VIKING Benchmark: Experimental Results



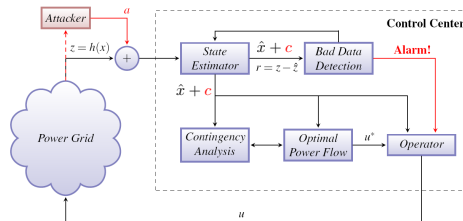
## Outline

- Introduction
- Attack model for control systems
- Attack on power network state estimator
- Stealthy minimum-effort attacks
- Security index
- Conclusions
- Biography



## Conclusions

- **Cyber-attack models** for networked control systems
- Undetectable false-data attack against power systems state estimator possible, both in theory and practice
- New **security index**  $\rho_k$  to estimate vulnerabilities
- Suggests locations of counter measures
- Many open problems in secure networked control theory



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

## Bibliography

- A. Giani, S. Sastry, K. H. Johansson, and H. Sandberg. The VIKING project: an initiative on resilient control of power networks. In Proc. 2nd Int. Symp. on Resilient Control Systems, pages 31–35, Idaho Falls, ID, USA, August 2009.
- H. Sandberg, A. Teixeira, and K. H. Johansson, "On Security Indices for State Estimators in Power Networks". In First Workshop on Secure Control Systems, Stockholm, Sweden, 2010.
- A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked Control Systems under Cyber Attacks with Applications to Power Networks". In American Control Conference, Baltimore, MD, USA, 2010.
- 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, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry, "Cyber Security Analysis of State Estimators in Electric Power Systems". In Proceedings of the 49th Conference on Decision and Control, Atlanta, GA, USA, 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.
- O. Vuković, K. C. Sou, G. Dán, H. Sandberg, "Network-layer Protection Schemes against Stealth Attacks on State Estimators in Power Systems", in Proceedings of IEEE International Conference of Smart Grid Communications, 2011.
- K. C. Sou, H. Sandberg, and K. H. Johansson. Electric power network security analysis via minimum cut relaxation. In *Proceedings of the 50th IEEE Conference on Decision and Control*, December 2011.
- A. Teixeira, "Toward Secure and Reliable Networked Control Systems", Licentiate Thesis, KTH, Sweden, 2011.
- A. Teixeira, H. Sandberg, G. Dán, and K. H. Johansson. "Optimal Power Flow: Closing the Loop over Corrupted Data". American Control Conference, 2012. Submitted.

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

## Bibliography (cont'd)

- F. C. Schweppe and J. Wildes. Power system static-state estimation, part I: Exact model. *IEEE Transactions on Power Apparatus and Systems*, 89(1):120–125, January 1970.
- F. F. Wu. Power system state estimation: a survey. *Int. J. Elec. Power and Energy Systems*, April 1990.
- M. Shahidehpour, F. Tinney, and Y. Fu. Impact of security on power systems operation. *Proceedings of the IEEE*, 93(11):2013–2025, nov 2005a.
- Y. Liu, M. K. Reiter, and P. Ning. False data injection attacks against state estimation in electric power grids. In *Proc. 16th ACM Conf. on Computer and Communications Security*, pages 21–32, New York, NY, USA, 2009.
- L. Jia, R. J. Thomas, and L. Tong. Malicious data attack on real-time electricity market. In *Proc. of IEEE ICASSP*, May 2011.
- O. Kosut, L. Jia, R. Thomas, and L. Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *Proc. of IEEE SmartGridComm*, October 2010.
- L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. In *First IEEE International Conference on Smart Grid Communications*, Oct. 2010
  
- A. Abur and A.G. Exposito. *Power System State Estimation: Theory and Implementation*. Marcel-Dekker, 2004.
- A. Monticelli. *State Estimation in Electric Power Systems: A Generalized Approach*. Kluwer Academic Publishers, 1999.
- P. Kundur. *Power System Stability and Control*. McGraw-Hill Professional, 1994.
- E. A. Blood, *From Static to Dynamic Electric Power Network State Estimation: The Role of Bus Component Dynamics*, PhD Thesis, ECE, CMU, 2011