MAN-IN-THE-MIDDLE ATTACK ON POWER GRID:

ATTACK MECHANISMS AND COUNTER MEASURES

Lang Tong

School of Electrical and Computer Engineering

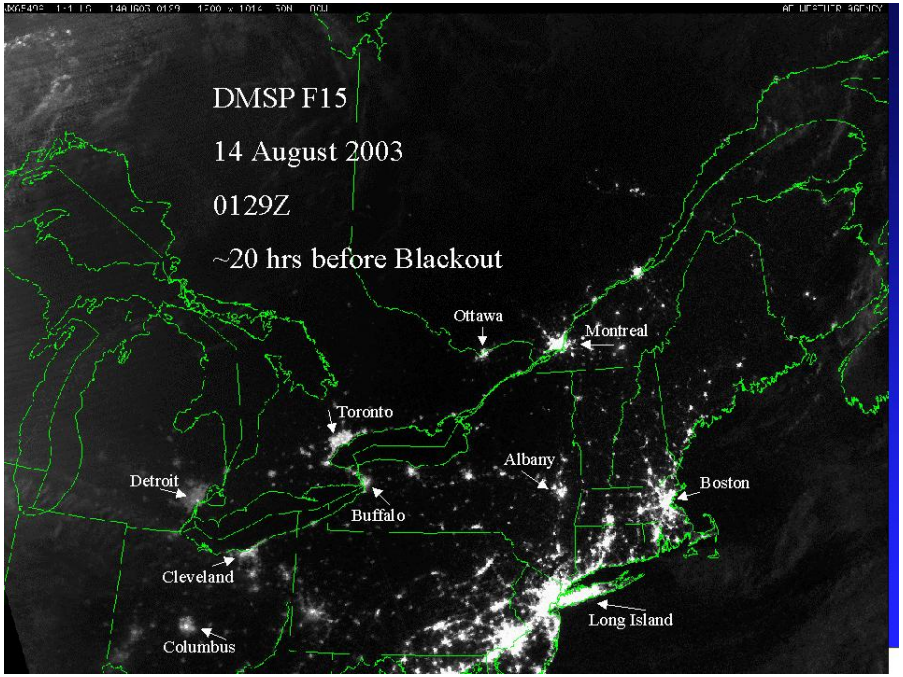
Cornell University, Ithaca, NY

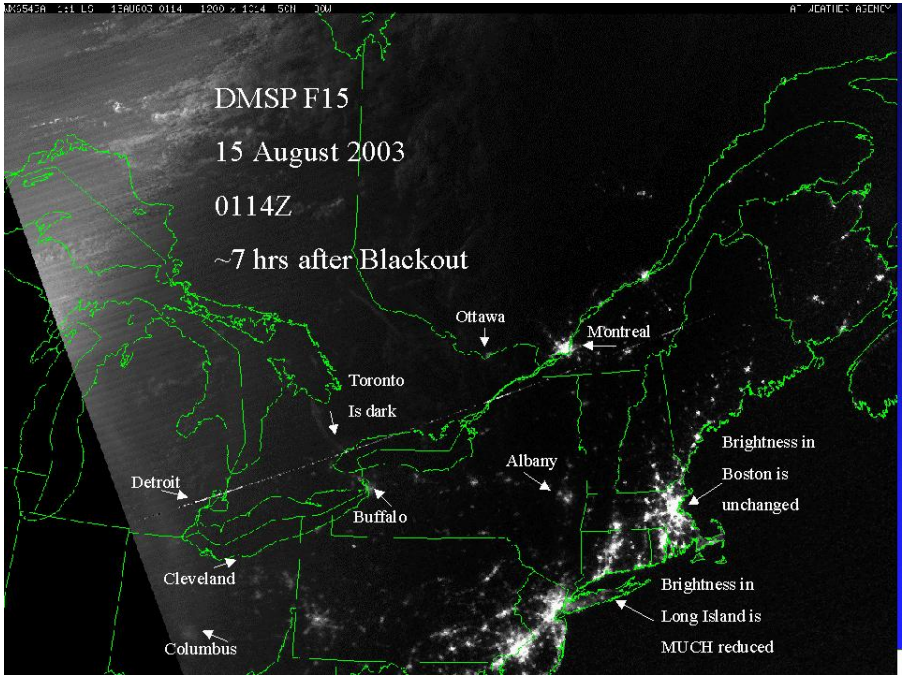
Joint work with Jinsub Kim and Robert J. Thomas

Presented at the PSERC Webinar, November 19, 2013

PSERC

The 2003 northeast blackout

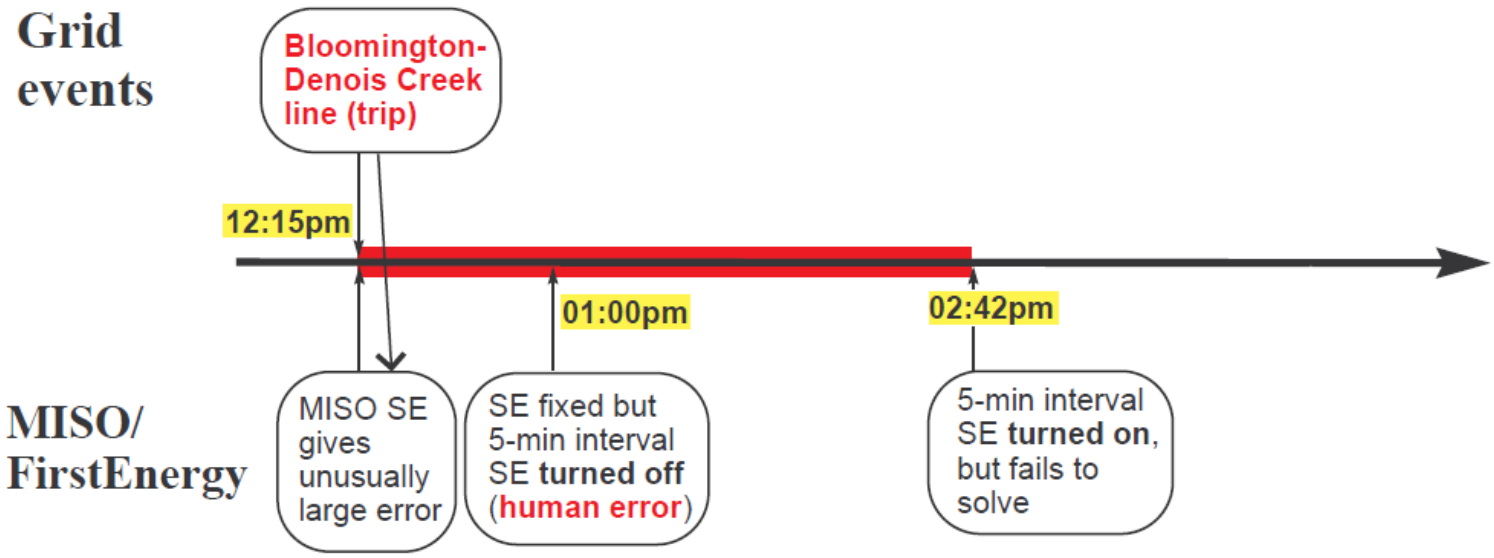




Source: http://www.noaanews.noaa.gov/stories/s2015.htm

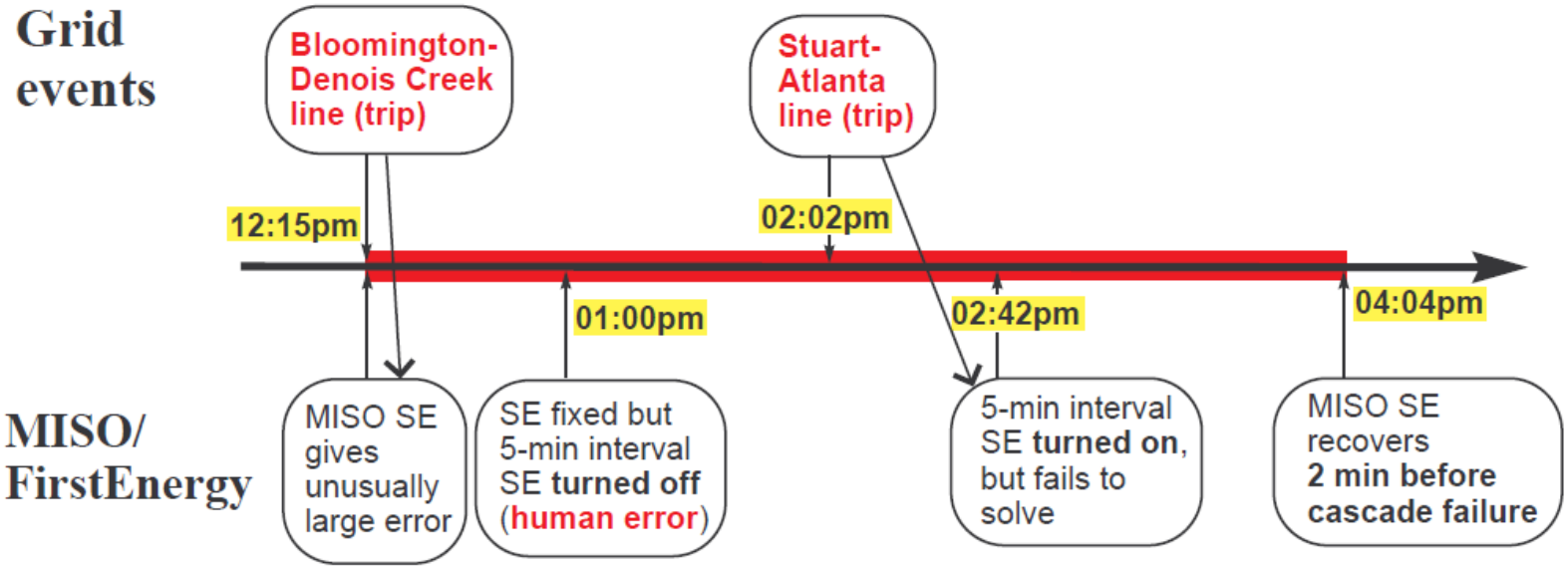
Acknowledgement: The speaker thanks Carl Hauser at WSU for pointing out the incorrect image used in the seminar.

Pre-blackout events



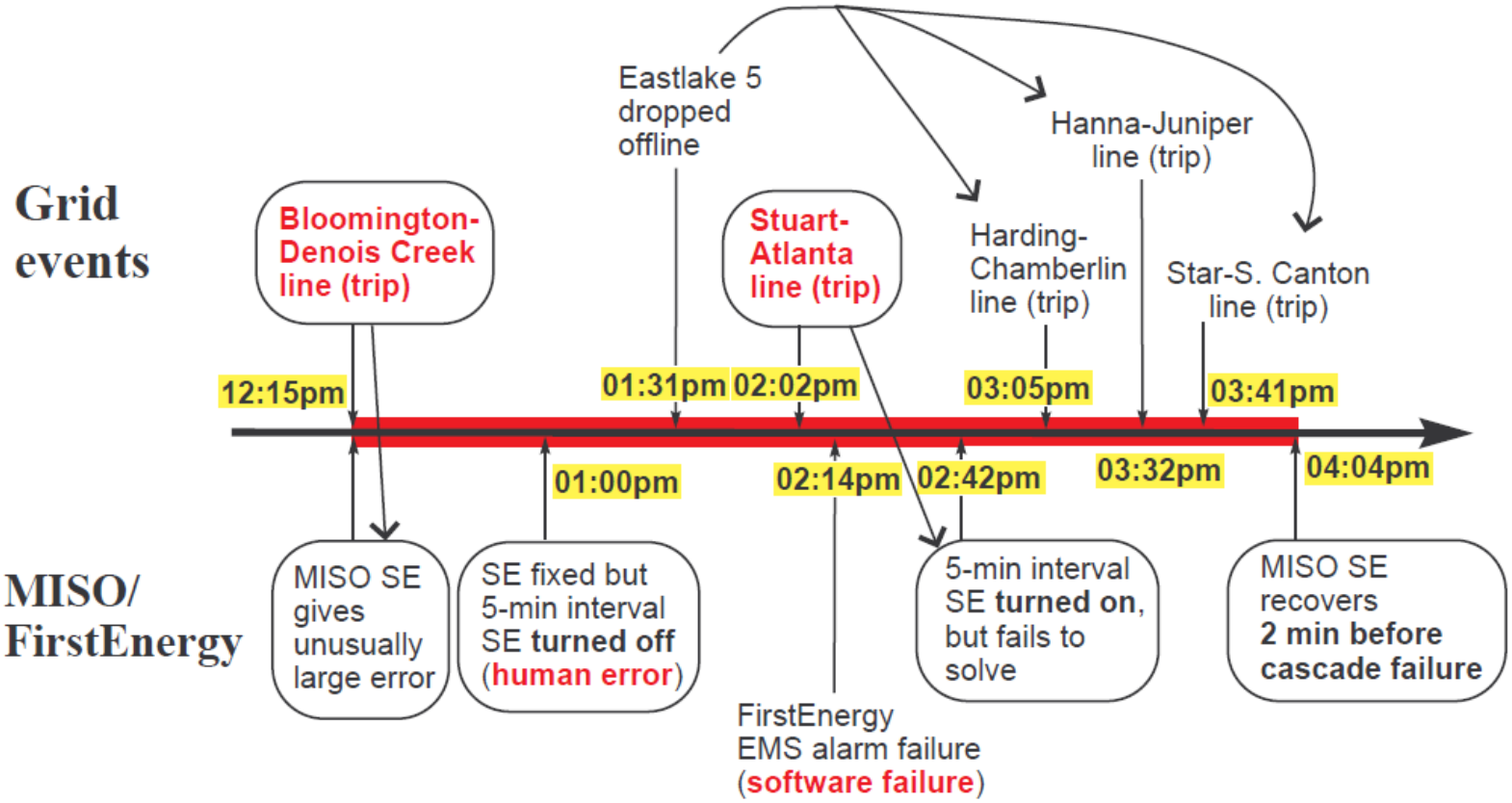
U.S.-Canada Power System Outage Task Force, "Final report on the August 14, 2003 blackout in the united states and Canada: causes and recommendations, April 2004"

Pre-blackout events



U.S.-Canada Power System Outage Task Force, "Final report on the August 14, 2003 blackout in the united states and Canada: causes and recommendations, April 2004"

Pre-blackout events



U.S.-Canada Power System Outage Task Force, "Final report on the August 14, 2003 blackout in the united states and Canada: causes and recommendations, April 2004"

On the security of the grid

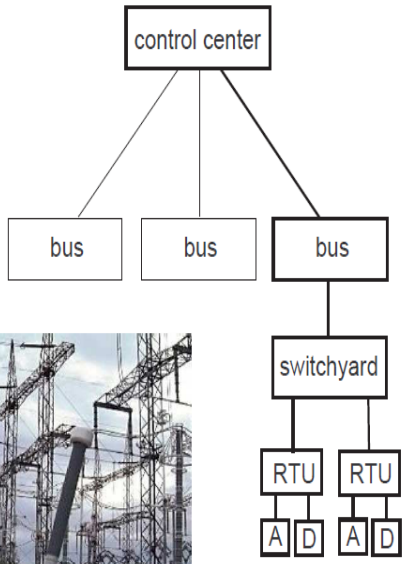
- "Most SCADA network protocols were designed with the original SCADA code base to be fast and are not designed to provide robust authentication and integrity checks"

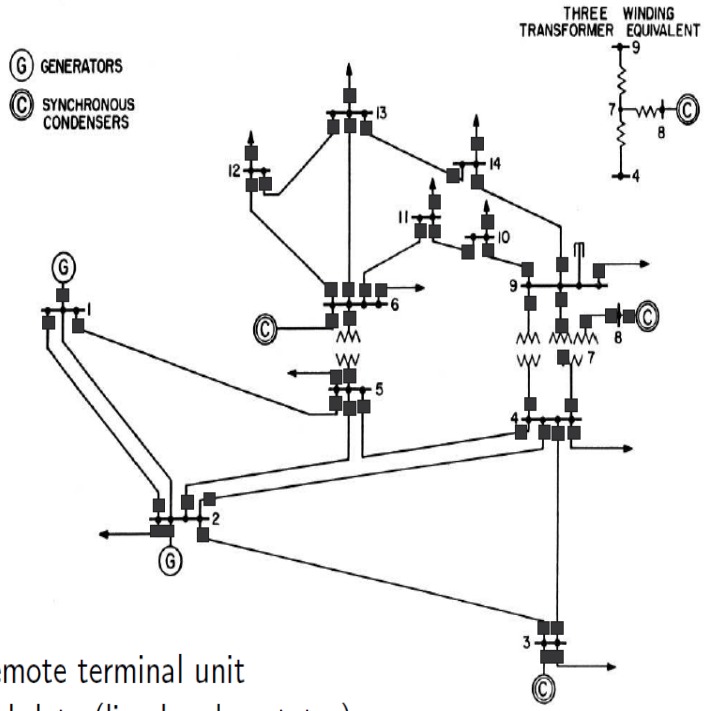
  INL, *Vulnerability Analysis of Energy Delivery Control Systems*, 2011

  "The risk of a "Trojan horse" or other deleterious program being intentionally embedded in the software of one or more of the control centers is real"

  NRC, *Terrorism and the Electric Power Delivery System*, 2012

Power system and vulnerabilities



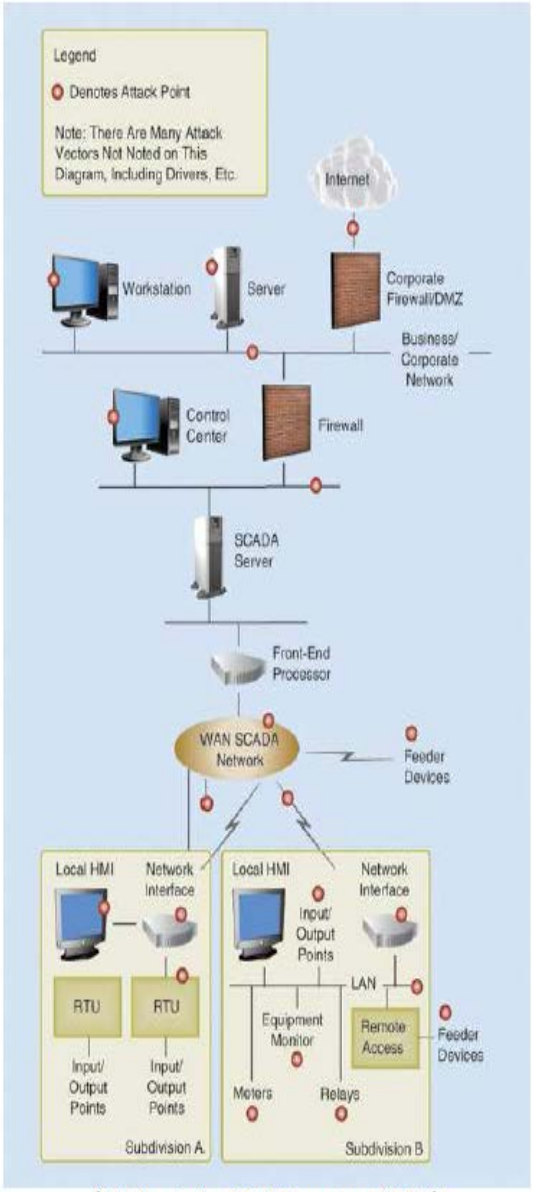


RTU: Remote terminal unit

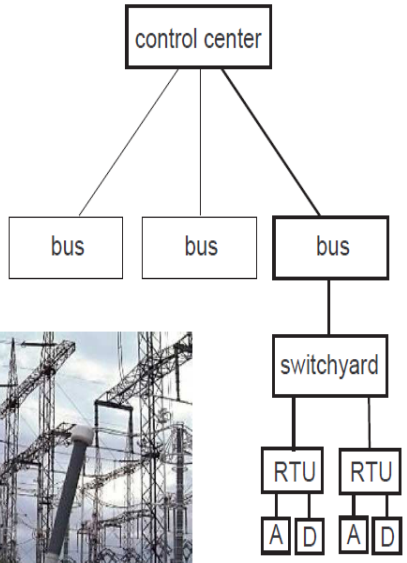
D: Digital data (line breaker states)

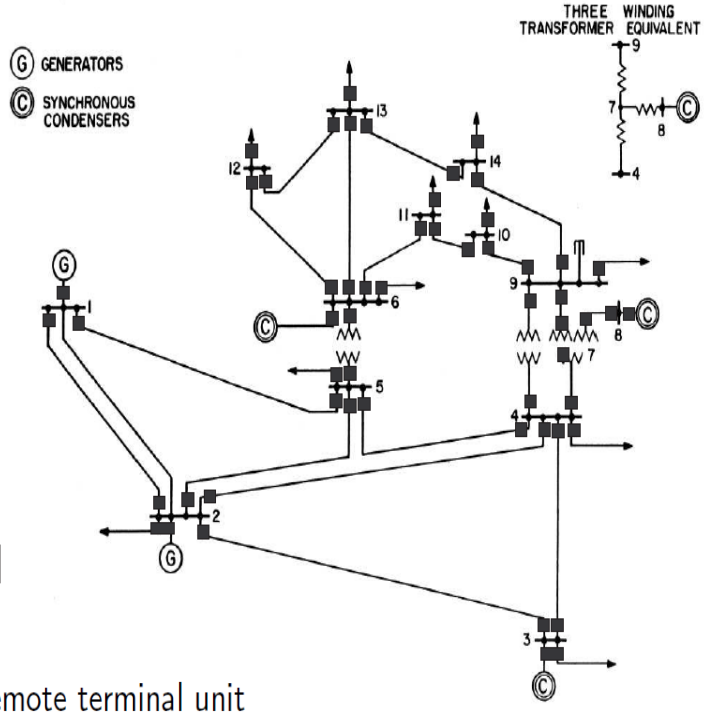
A: Analog data (power flows, injections)

Power system and vulnerabilities



(Hull *et al.*, PE Magazine'2012)





RTU: Remote terminal unit
D: Digital data (line breaker states)
A: Analog data (power flows, injections)

System vulnerabilities

- Backdoor attacks (Stuxnet)
- Man-in-the-middle attack
- Denial of service attacks

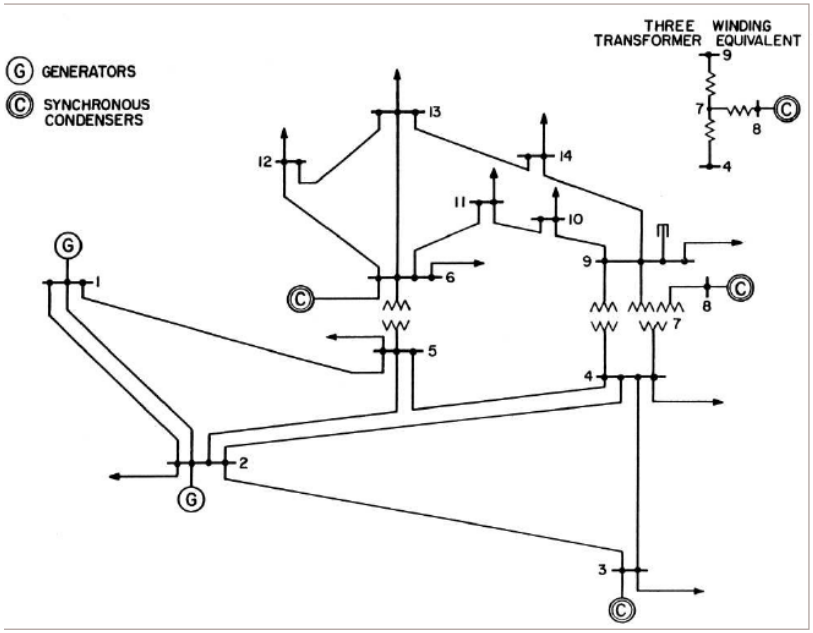
Outline

- System model and observability
- State attack: mechanisms and protection
- Topology attack: mechanisms and protection
- Data driven attack
- Summary and conclusions

Main theme:

- Develop graph and algebraic (matrix) techniques to characterize unobservable attacks
- Gain insights into cost-effective protection mechanisms.

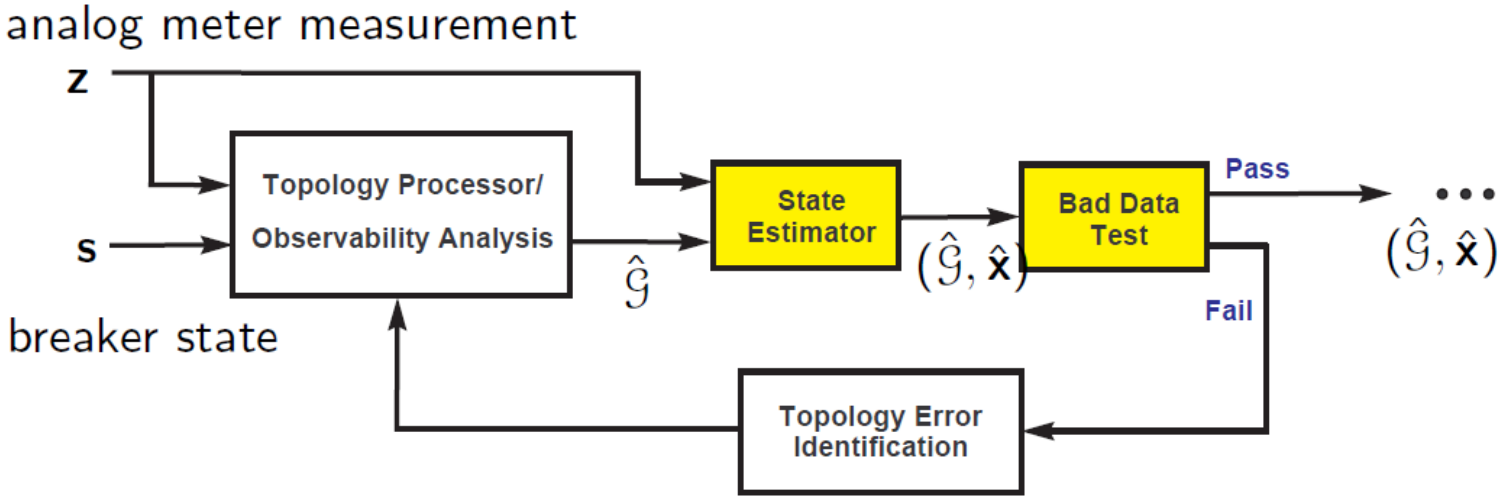
Power network and measurement model



- The topology graph: $\mathcal{G} = (\mathcal{V}, \mathcal{E})$.
  - $\mathcal{V}$: set of buses.
  - $\mathcal{E}$: set of transmission lines.
- System state: The vector of voltage phasors $\mathbf{x}$.
- Measurement:

$$\begin{cases} \text{Digital:} & \mathbf{s} \to \mathcal{G} \\ \text{Analog:} & \mathbf{z} = h(\mathbf{x}; \mathcal{G}) + \mathbf{e} \end{cases}$$

State estimation and bad data detection



- State estimation:

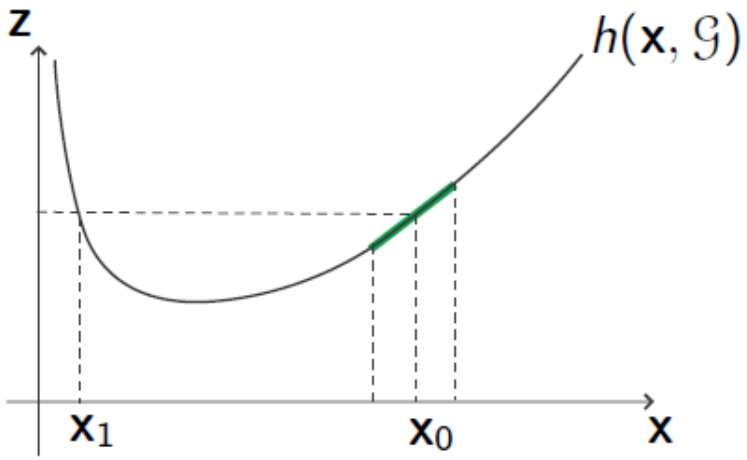
$$\mathbf{D}: \quad \mathbf{s} \rightarrow \hat{\mathcal{G}}$$
$$\mathbf{A}: \quad \hat{\mathbf{x}} \triangleq \arg\min_{\mathbf{x}} (\mathbf{z} - h(\mathbf{x}; \hat{\mathcal{G}}))^T \Sigma^{-1} (\mathbf{z} - h(\mathbf{x}; \hat{\mathcal{G}}))$$

- Bad data test:

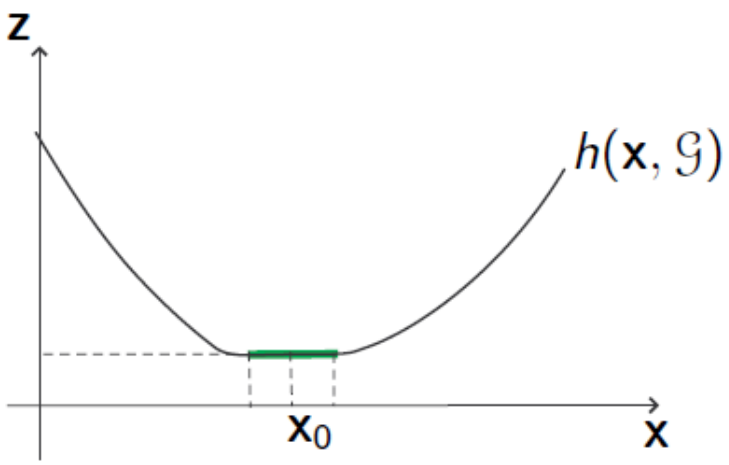
$$||\mathbf{z} - h(\hat{\mathbf{x}}; \hat{\mathcal{G}})||^2_{\Sigma^{-1}} \underset{\text{Pass}}{\overset{\text{Fail}}{\gtrless}} \tau$$

Network observability

- Locally observable at $\mathbf{x}_0$:



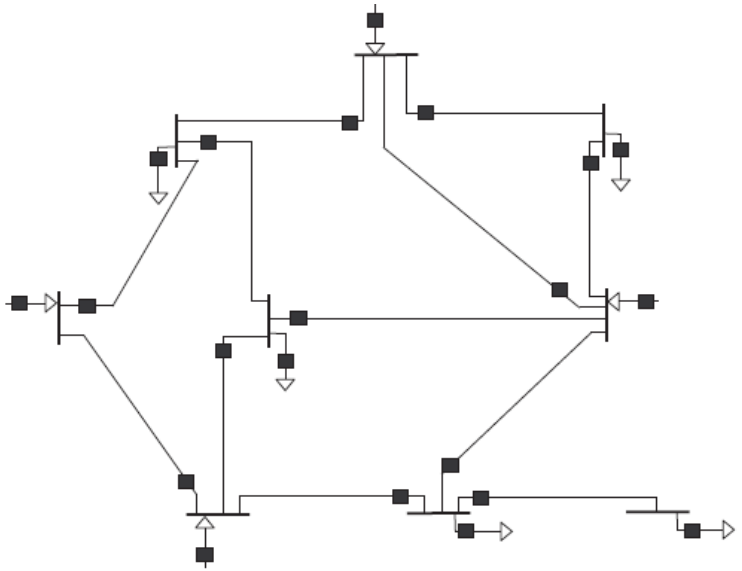
- Locally unobservable at $\mathbf{x}_0$:



$$\mathbf{z} = H\mathbf{x}$$

$$H \stackrel{\Delta}{=} \nabla h(\mathbf{x}_0, \mathcal{G})$$

Observability: algebraic condition



- Local linearized model:

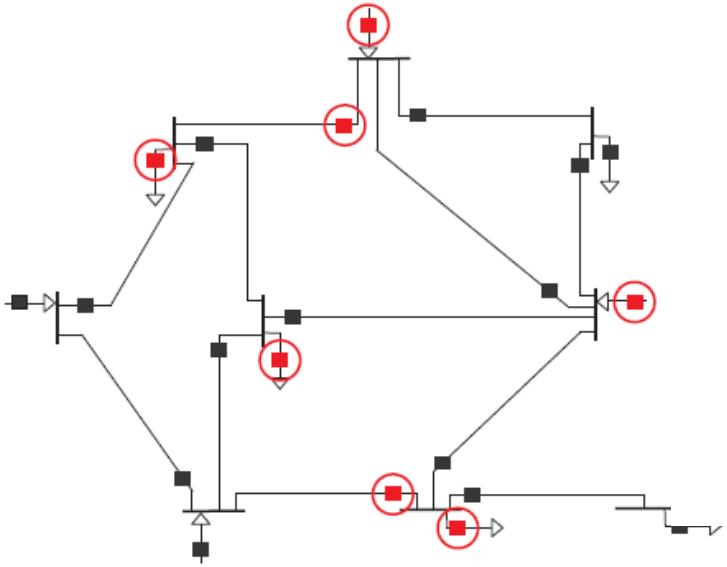
$$\mathbf{z} = H\mathbf{x} + \mathbf{e},$$

$$H \stackrel{\Delta}{=} \nabla h(\mathbf{x}_0, \mathcal{G})$$

Theorem

Network is (locally) observable if and only if H has full column rank.

Unobservable attack



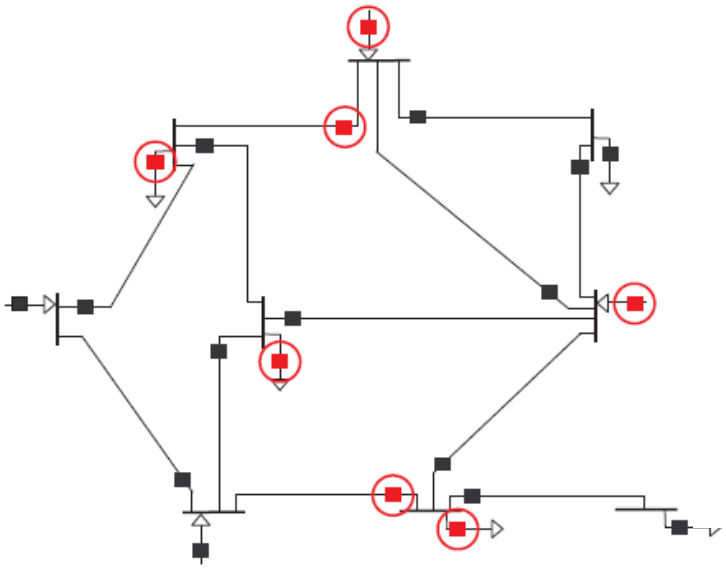
- Attack model:

$$\bar{\mathbf{z}}_t = h(\mathbf{x}_t, \mathcal{G}) + \mathbf{a}, \quad \mathbf{a} \in \mathcal{A}.$$

- Unobservable attack: there exists $\bar{\mathbf{x}}_t$ such that

$$\bar{\mathbf{z}}_t = h(\bar{\mathbf{x}}_t, \mathcal{G})$$

Unobservable attack



- Attack model:

$$\bar{\mathbf{z}}_t = h(\mathbf{x}_t, \mathcal{G}) + \mathbf{a}, \quad \mathbf{a} \in \mathcal{A}.$$

- Unobservable attack: there exists $\bar{\mathbf{x}}_t$ such that

$$\bar{\mathbf{z}}_t = h(\bar{\mathbf{x}}_t, \mathcal{G})$$

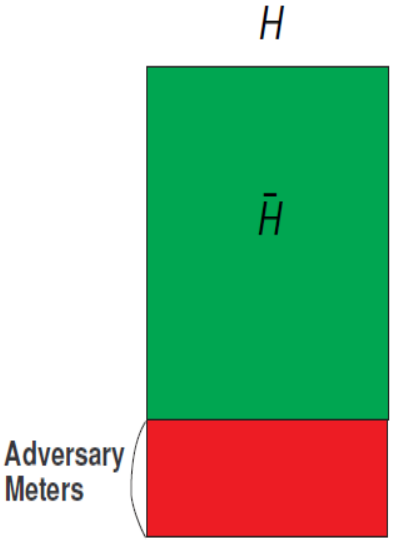
- Liu, Ning, Reiter (2009)

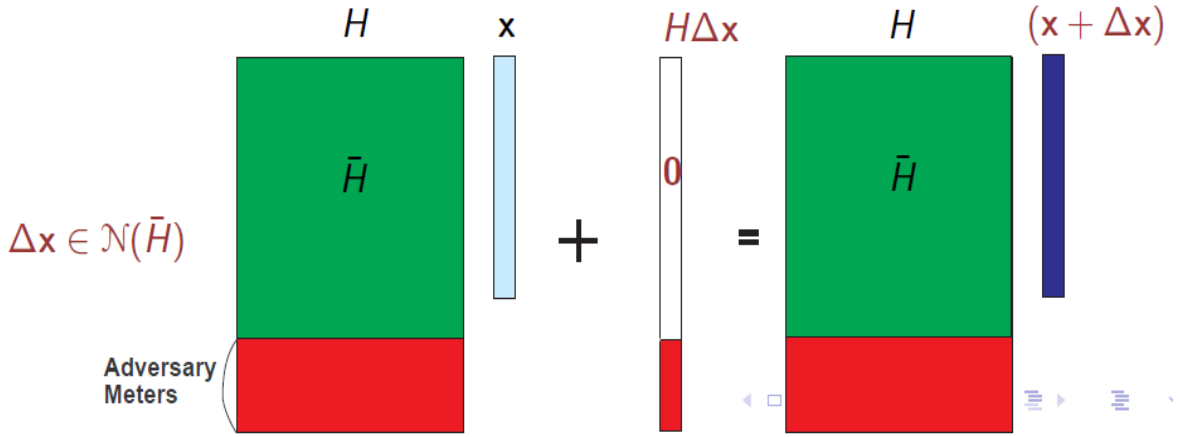
$$\begin{aligned} \mathbf{z} &= H\mathbf{x} + \mathbf{a} \\ &= H\mathbf{x} + H\Delta\mathbf{x} = H\bar{\mathbf{x}} \end{aligned}$$

Can attack make network unobservable?

Theorem (Kosut *et al.*, TSG'2011)

A unobservable attack exists if and only if removing attacked meters makes the network unobservable, i.e., the remaining measurement matrix $\bar{H}$ is singular.



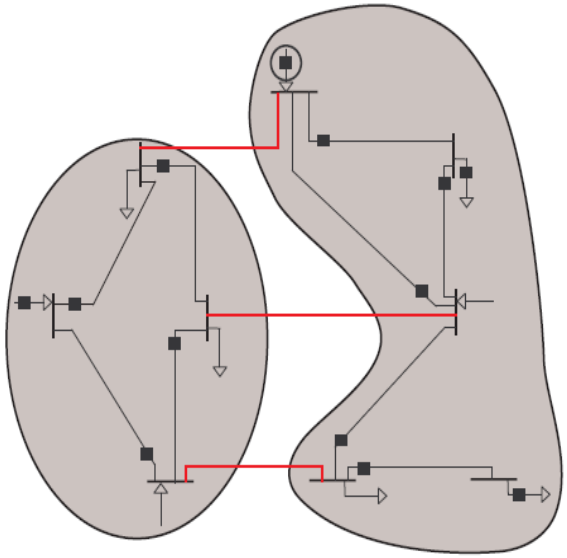


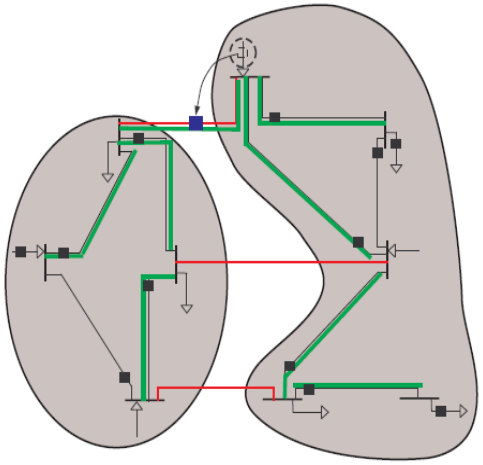
Observability : graph theoretic condition

Theorem (Krumpholz *et al.*, TPAS'1980)

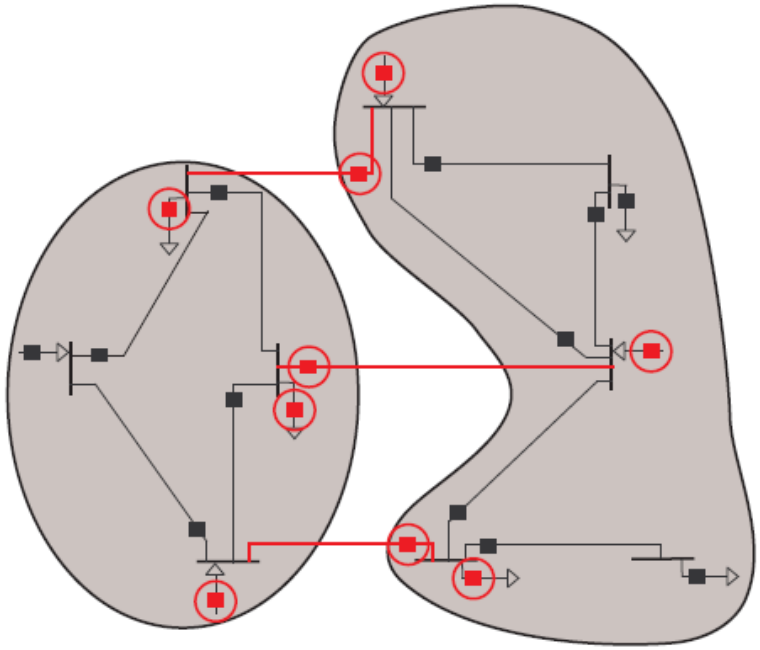
A network is observable if and only if
$\exists$ a spanning tree with an assigned meter on each edge.

Equivalently, the network is unobservable if and only if, for any assignment of injection meters, there exists a cut without meters.





Unobservable attack and protection

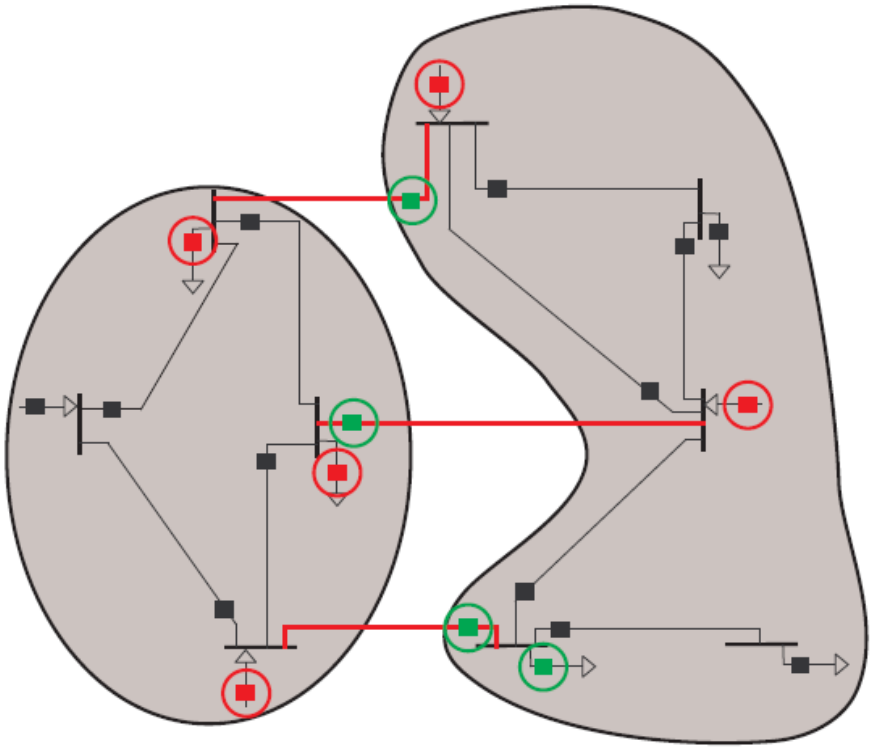


Theorem (Kosut *et al.*, TSG'2011)

An unobservable attack exists if and only if, after removing adversary controlled meters, for any assignment of injection meters to adjacent branches, there exists a cut without meters.

No unobservable attack exists if meters on a spanning tree are authenticated.

Framing attack



- Partition the set $\mathcal{S}_T$ of attacked meters into $\{\mathcal{S}_A, \mathcal{S}_F\}$.

  $\mathcal{S}_A$: adversary meters

  $\mathcal{S}_F$: framed meters

- Data framing attack:

  By controlling $\mathcal{S}_A$, the adversary makes the control center identify $\mathcal{S}_F$ as bad and exclude them from state estimation.

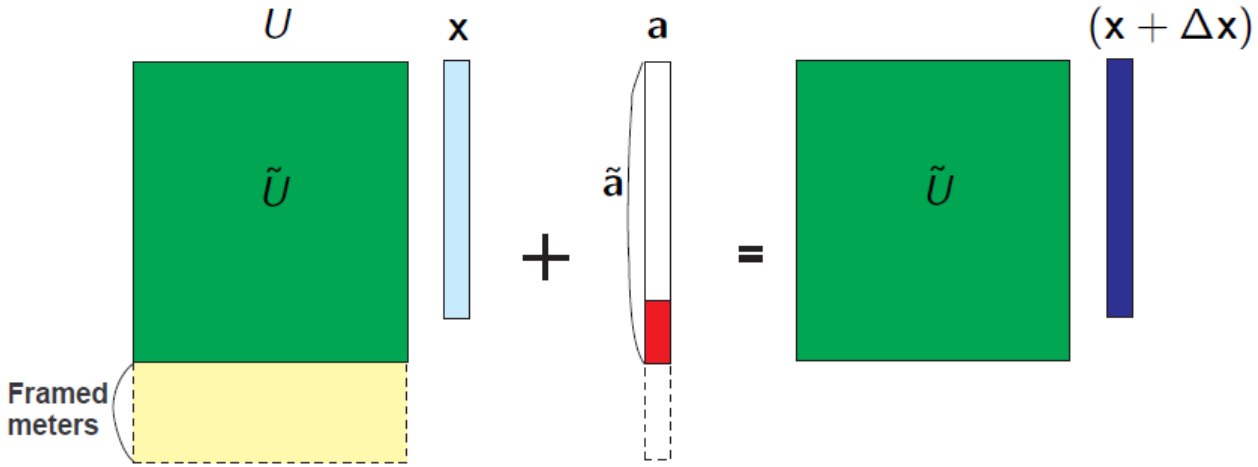
Jinsub Kim, Lang Tong, Robert J. Thomas, "Data framing attack on state estimation with unknown network parameters," Asilomar Conf. on Signals, Systems, and Computers, Nov., 2013.

Framing attack via QCQP

maximize $\mathbb{E}\{\sum_{i\in\mathcal{S}_T}(r_i^N)^2\} = \|R\mathbf{a}\|_2^2$ — maximize residue at framed meters

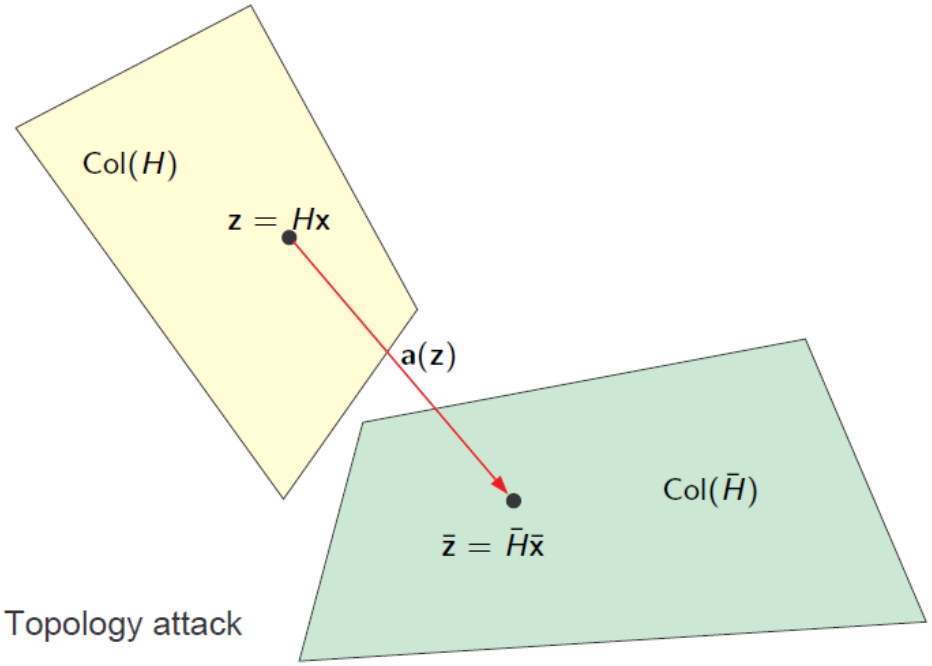
subject to $\|\mathbf{a}\|_2 = 1,\ \mathbf{a}\in\mathcal{A}$ — find best direction to align attack vector

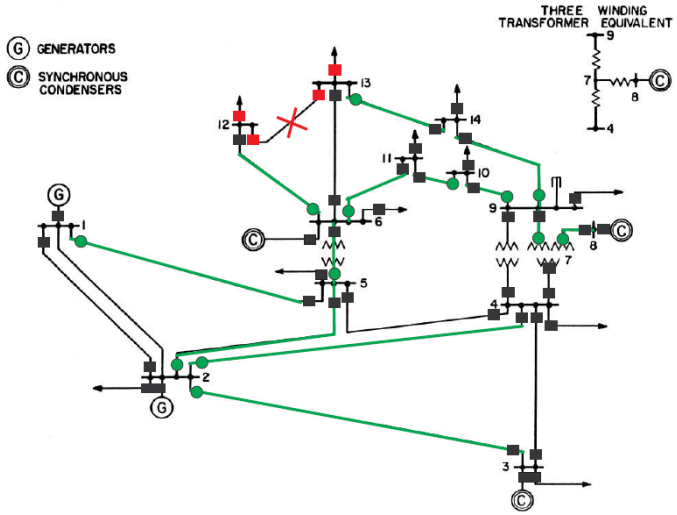
$\tilde{\mathbf{a}} \in \mathrm{Col}(\tilde{U})$ — ensure strong attack



Jinsub Kim, Lang Tong, Robert J. Thomas, "Data framing attack on state estimation with unknown network parameters," Asilomar Conf. on Signals, Systems, and Computers, Nov., 2013.

Topology attack

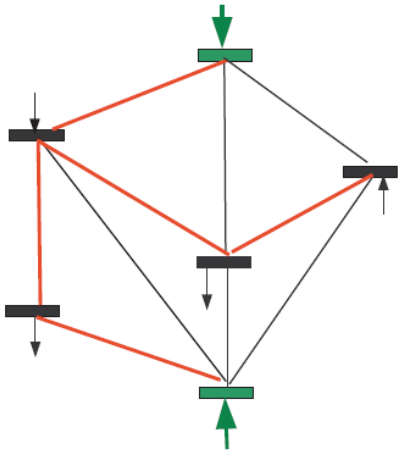




Jinsub Kim, Lang Tong, "On topology attack of a smart grid: undetectable attacks and countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, July, 2013.

Protection against topology attack

- Find a spanning tree $\mathcal{T} = (\mathcal{V}, \mathcal{E}_{\mathcal{T}})$
- Find a vertex set $\mathcal{B}$ such that $\mathcal{B}$ and $\mathcal{T}$ cover $\mathcal{G}$
- Protect flow meters on $\mathcal{T}$ and injection meters on $\mathcal{B}$



Theorem (Cover-up strategy)

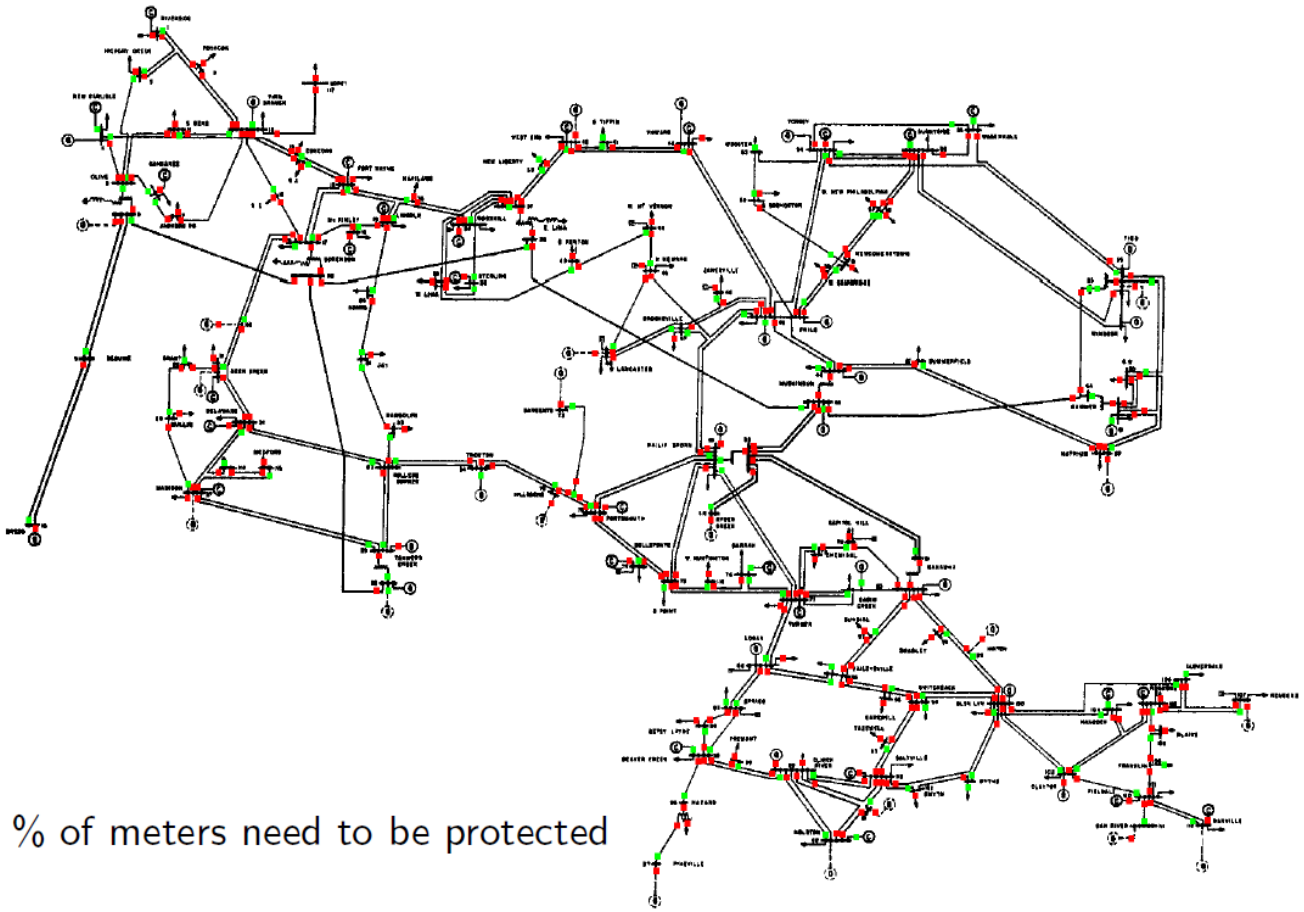
- *Any topology attack is detectable under cover-up protection.*

Remarks:

- Cover-up protection is sufficient for both state and topology attacks.
- The cover-up protection is tight for some networks.

Jinsub Kim, Lang Tong, "On topology attack of a smart grid: undetectable attacks and countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, July, 2013.

Protection against topology attack



30 % of meters need to be protected

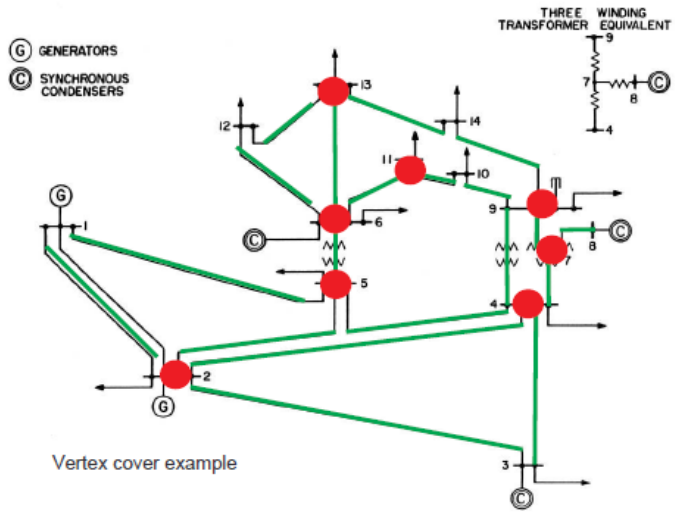
Jinsub Kim, Lang Tong, "On topology attack of a smart grid: undetectable attacks and countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, July, 2013.

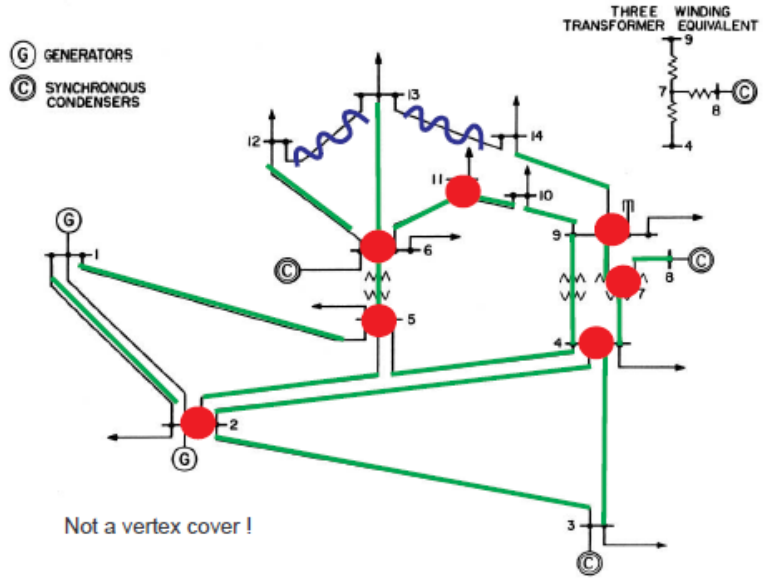
Protection against topology attack via PMU

Corollary

Any state or topology attack is detectable **IFF**

the set of PMU-assigned buses is a vertex cover of $\mathcal{G}_0$.





Jinsub Kim, Lang Tong, "On phasor measurement unit placement against state and topology attack," *IEEE SmartGridComm*, October, 2013.

Optimal PMU placement

- Minimizing the number of PMUs for protection corresponds to finding a minimum vertex cover: NP-complete.

- Polynomial-time approximation algorithms

  -*Greedy heuristic*: select the vertex with the highest degree first (effective for sparse network)

	# secure PMUs	$\left(\frac{\#\text{ secure PMUs}}{\#\text{ all buses}}\right)$
IEEE 14	8	57 %
IEEE 118	61	52 %
IEEE 300	140	47 %

∗ Protection against state attacks requires about a third of buses to have secure PMUs (Kim&Poor, TSG'2011)

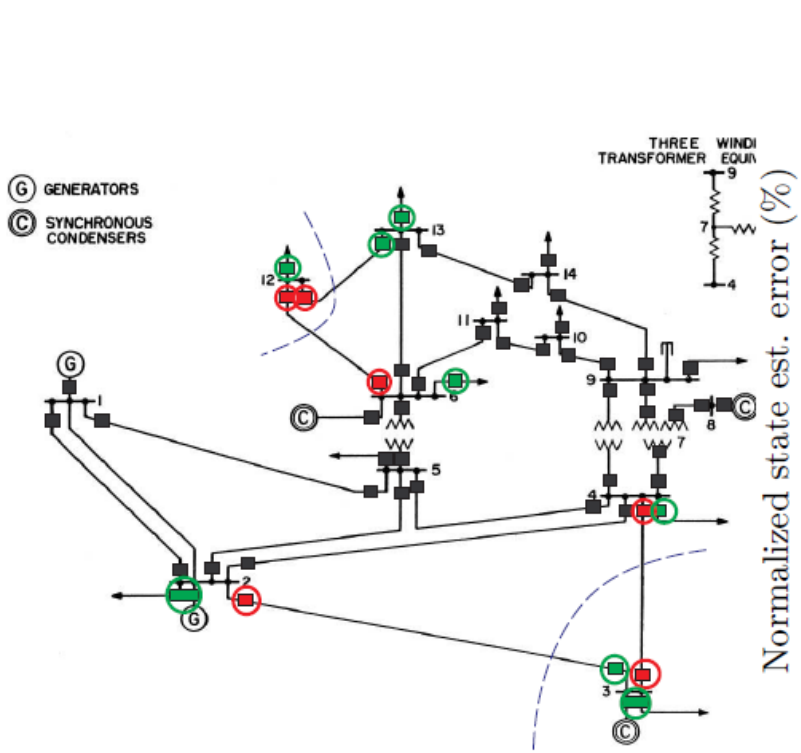
Jinsub Kim, Lang Tong, "On phasor measurement unit placement against state and topology attack," *IEEE SmartGridComm*, October, 2013.

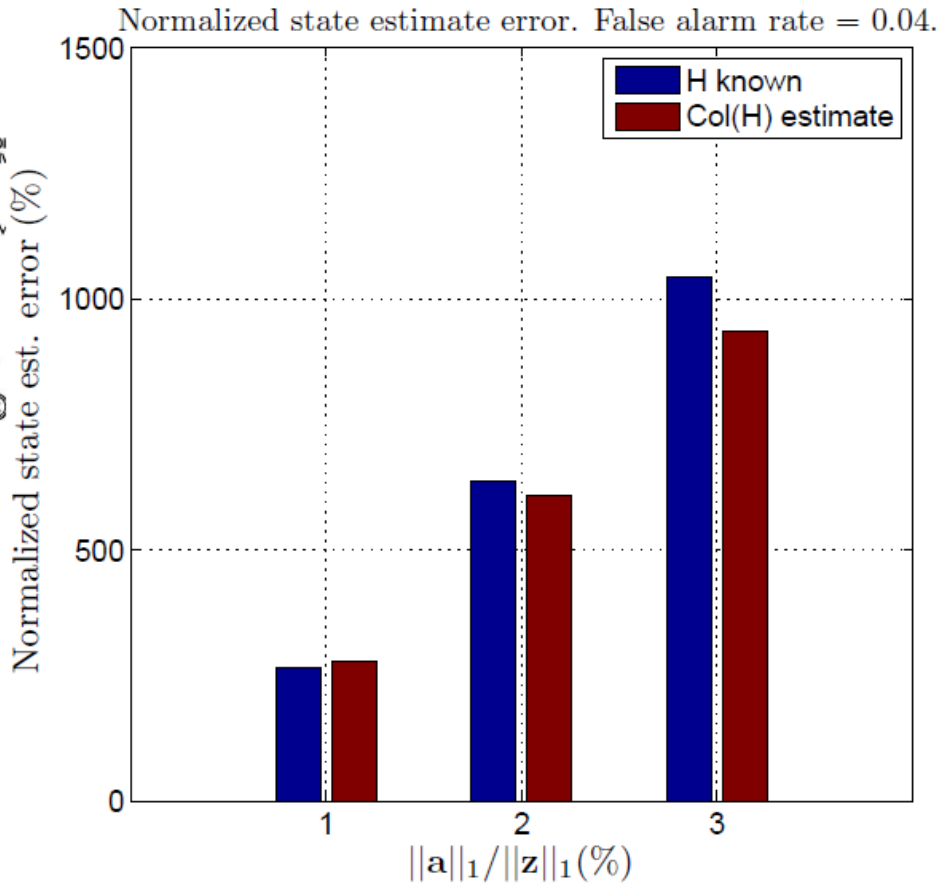
Data driven attacks

- Network topology and network parameters are difficult to obtain. But they may not be needed!
- Algebraic (rank) conditions for attacks can be used to construct data-driven attacks via subspace learning.
- Topology conditions can be used to construct attacks using only local measurements.

Jinsub Kim, Lang Tong, Robert J. Thomas, "Data framing attack on state estimation with unknown network parameters," Asilomar Conf. on Signals, Systems, and Computers, Nov., 2013.

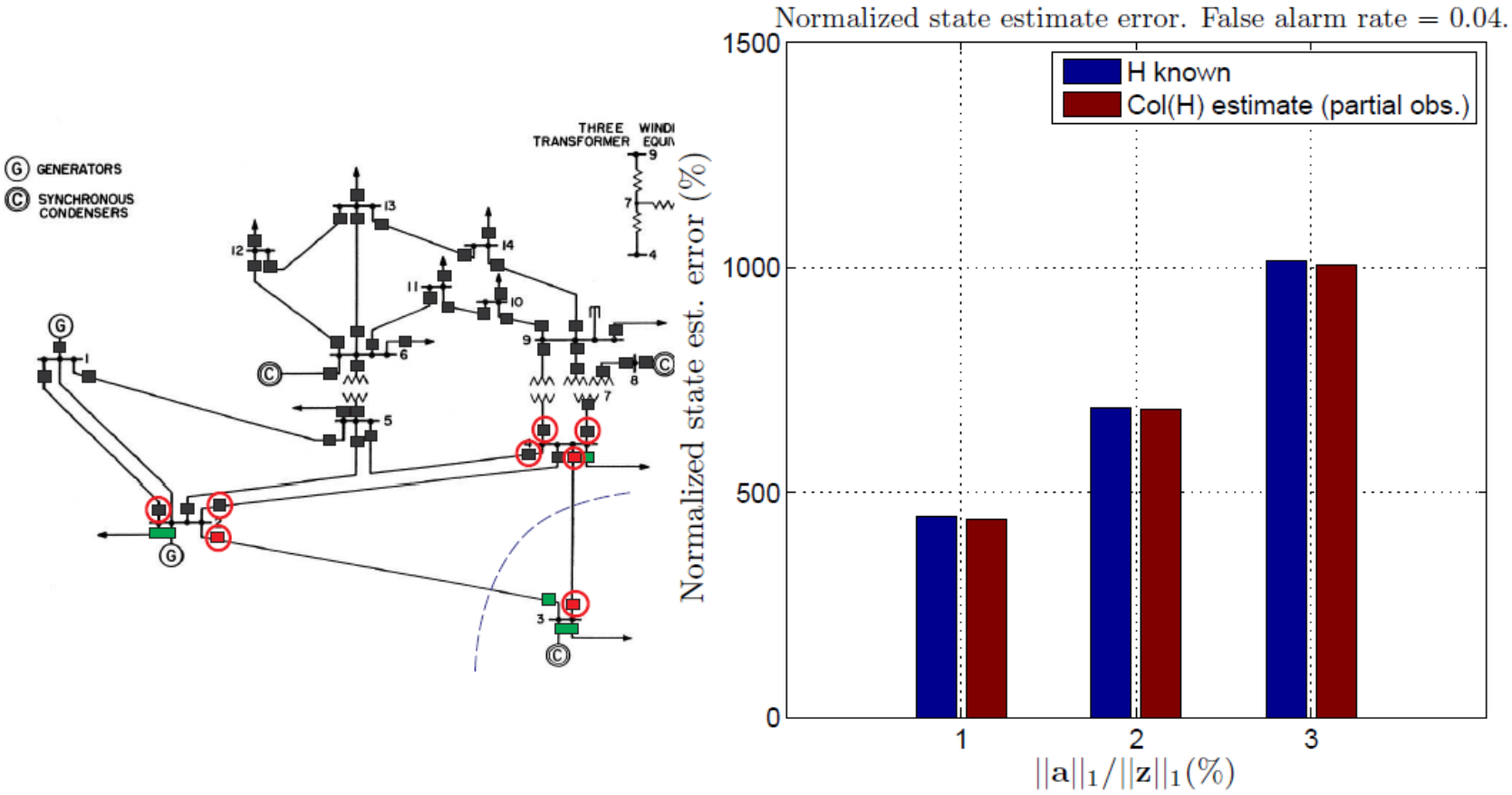
Framing attack with unknown network parameters





Jinsub Kim, Lang Tong, Robert J. Thomas, "Data framing attack on state estimation with unknown network parameters," Asilomar Conf. on Signals, Systems, and Computers, Nov., 2013.

Framing attack with unknown network parameters and partial measurements



Jinsub Kim, Lang Tong, Robert J. Thomas, "Data framing attack on state estimation with unknown network parameters," Asilomar Conf. on Signals, Systems, and Computers, Nov., 2013.

Conclusions

- Perfect security does not exists.
  - Cyber security (encryption and authentication) techniques need to be complemented by monitoring and security measures based on physical systems.
- Beyond state and topology attacks
  - Attack on real-time (dispatch and market) operations
  - Real-time contingency analysis (RTCA)
- Data driven approach to attacks and counter measures