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
The 2003 northeast blackout


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

Pre-blackout events

Grid events
- Bloomington-Denos Creek line (trip) at 12:15pm
- Stuart-Atlanta line (trip) at 02:02pm

MISO/FirstEnergy
- MISO SE gives unusually large error at 01:00pm
- SE fixed but 5-min interval SE turned off (human error)
- 5-min interval SE turned on, but fails to solve at 02:42pm
- MISO SE recovers 2 min before cascade failure at 04:04pm

Pre-blackout events

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”

Power system and vulnerabilities

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

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

(System vulnerabilities)

RTU: Remote terminal unit
A: Analog data (power flows, injections)
D: Digital data (line breaker states)
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:
  - Digital: $\mathbf{s} \rightarrow \mathcal{G}$
  - Analog: $\mathbf{z} = h(\mathbf{x}; \mathcal{G}) + \mathbf{e}$
State estimation and bad data detection

- **State estimation:**
  \[ D: \quad s \rightarrow \hat{G} \]
  \[ A: \quad \hat{x} \triangleq \operatorname{arg\,min}_x (z - h(x; \hat{G}))^T \Sigma^{-1} (z - h(x; \hat{G})) \]

- **Bad data test:**
  \[ \|z - h(\hat{x}; \hat{G})\|_\Sigma^{-1}^2 \geq \tau \quad \text{Fail} \]
  \[ \|z - h(\hat{x}; \hat{G})\|_\Sigma^{-1}^2 < \tau \quad \text{Pass} \]
Network observability

Locally observable at $x_0$:

Locally unobservable at $x_0$:

$$z = Hx$$

$$H \cong \nabla h(x_0, g)$$
Observability: algebraic condition

- Local linearized model:

\[ \begin{align*}
  z &= Hx + e, \\
  H &\equiv \nabla h(x_0, g)
\end{align*} \]

**Theorem**

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

- Attack model:
  \[ \bar{Z}_t = h(x_t, g) + a, \quad a \in A. \]
- Unobservable attack: there exists \( \bar{x}_t \) such that
  \[ \bar{Z}_t = h(\bar{x}_t, g) \]
Unobservable attack

- Attack model:
  \[ \tilde{z}_t = h(x_t, \mathcal{G}) + a, \quad a \in \mathcal{A}. \]

- Unobservable attack: there exists \( \tilde{x}_t \) such that
  \[ \tilde{z}_t = h(\tilde{x}_t, \mathcal{G}) \]

- Liu, Ning, Reiter (2009)

  \[ z = Hx + a \]
  \[ = Hx + H\Delta x = H\tilde{x} \]
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 $\tilde{H}$ is singular.
Observability: graph theoretic condition

Theorem (Krumpholz et al., TPAS’1980)

A network is **observable** if and only if
\[ \exists \text{ a spanning tree with an } \text{assigned meter} \]
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 $S_T$ of attacked meters into $\{S_A, S_F\}$.
  - $S_A$: adversary meters
  - $S_F$: framed meters

- Data framing attack:
  By controlling $S_A$, the adversary makes the control center identify $S_F$ as bad and exclude them from state estimation.

Framing attack via QCQP

\[
\begin{align*}
\text{maximize} & \quad \mathbb{E}\{\sum_{i \in S_T} (r_i^N)^2\} = \|Ra\|_2^2 \\
\text{subject to} & \quad \|a\|_2 = 1, \ a \in A \\
& \quad \tilde{a} \in \text{Col}(\tilde{U})
\end{align*}
\]

maximize residue at framed meters

find best direction to align attack vector

ensure strong attack

Protection against topology attack

- Find a spanning tree $T = (V, E_T)$
- Find a vertex set $B$ such that $B$ and $T$ cover $G$
- Protect flow meters on $T$ and injection meters on $B$

**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.

Protection against topology attack

30% of meters need to be protected

Corollary

Any state or topology attack is detectable IFF

the set of PMU-assigned buses is a vertex cover of $G_0$. 

---

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)

<table>
<thead>
<tr>
<th></th>
<th># secure PMUs</th>
<th>(# secure PMUs) / (# all buses)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE 14</td>
<td>8</td>
<td>57%</td>
</tr>
<tr>
<td>IEEE 118</td>
<td>61</td>
<td>52%</td>
</tr>
<tr>
<td>IEEE 300</td>
<td>140</td>
<td>47%</td>
</tr>
</tbody>
</table>

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

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.

Framing attack with unknown network parameters

Framing attack with unknown network parameters and partial measurements

Conclusions

- Perfect security does not exist.
  - 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