Acknowledgments

• André Teixeira (KTH)
• György Dán (KTH)
• Karl Henrik Johansson (KTH)

• Kin Cheong Sou (Chalmers)
• Iman Shames (Univ. Melbourne)

• Julien M. Hendrickx (UC Louvain)
• Raphael M. Jungers (UC Louvain)
Outline

• Background and motivation

• Quantifying security using sparse optimization

• Quantifying security using game theory

• Summary
Networked control systems
• are being **integrated with business/corporate networks**
• have many potential points of **cyber-physical attack**

Need tools and strategies to understand and mitigate attacks:
- Which threats should we care about?
- What impact can we expect from attacks?
- Which resources should we protect (more)?

• **Need for quantification!**
Outline

- Background and motivation
- Quantifying security using sparse optimization
- Quantifying security using game theory
- Summary
Power System Monitoring

Practically motivated problem...

How much security does the Bad Data Detector provide?

[Giani et al., IEEE ISRCS, 2009]
[Mohajerin Esfahani et al., CDC, 2010]
• **Attack policy:** Induce bias in power measurements without alarms
• **Model knowledge:** Steady-state model of power system
• **Disruption resources:** Small number of measurement channels

Can we quantify how hard such attacks would be?
Steady-State Power System Model

States ($\theta$)
= bus voltage phase angles
(flow conservation)
bus injection

Measurements ($y$)
= line power flow & bus injection

“DC power flow model”:
$$ y = H \theta $$

measurement matrix

12/17/2014
Sandberg: "Quantifying Security in Cyber-Physical Systems"
Structure of Measurement Matrix $H$

$$H = \begin{bmatrix} 
DA^T \\
-DAT^T \\
ADAT^T 
\end{bmatrix}$$

- $A$ - directed incidence matrix of graph corresponding to power network topology
- $D$ - nonsingular diagonal matrix containing reciprocals of reactance of transmission lines

- More measurements than states. Redundancy!
State Estimation by Least Squares

State estimator (LS)

\[ y = H \theta \]

\[ \Rightarrow \hat{\theta} = (H^T H)^{-1} H^T y \]

What if the measurements were **wrong**?

\[ \tilde{y} = y + \Delta y \quad \text{random measurement noise} \]

\[ \tilde{\theta} = \hat{\theta} + \Delta \theta \quad \text{intentional data attack} \]
Stealthy Additive Deception Attack

Measurements subject to **attack**:
\[ \tilde{y} = y + \Delta y \]

Is there a state explaining the received measurements?

Attack is **constrained**; otherwise will be **detected** by Bad Data Detection algorithm

**Stealth attack**: \[ \Delta y = H \Delta \theta \]
Quantification: Security Index

Stealth attack $\Delta y = H \Delta \theta$

In general, $e_k \notin \text{span}(H)$

Minimum # of meters attacked, targeting the $k^{th}$ measurement:

$$\min_{\Delta \theta} \|H \Delta \theta\|_0$$

s.t. $H(k, :) \Delta \theta = 1$

Minimum objective value = security index

[Sandberg et al., CPSWEEK, 2010]

See also [Kosut et al., IEEE TSG, 2011]
A Security Metric for 40-bus Network

At least 7 measurements involved in a stealth attack against measurement 33.
The Goal: Quantify Security to Aid Allocation of Protection

Security level
- dangerous
- moderate
- safe
Security index problem

\[ \min_{\Delta \theta} \| H \Delta \theta \|_0 \]

s.t. \( H(k,:) \Delta \theta = 1 \)

**How to solve?**

Closely related to compressed sensing and computation of \textit{cospark} of \( H \) [Tillmann and Pfetsch, IEEE TIT, 2013]. Problem known to be \textbf{NP-hard} for arbitrary \( H \).
Wish List

• Can we find solutions as **accurately** as MILP, and **faster** than LASSO?
  - Arbitrary $H$: **No!** (Problem NP-hard)
  - $H$ with the special physical and measurement structure: **Yes!** (Min cut polynomial time algorithm next)

• Can we find methods giving more **problem insight**, and ideas for **assigning protection**?
  - **Yes**, exploit graph interpretation of solution
Theorem: Optimal $\Delta \theta_i$ can be restricted to 0 or 1, for all $i$

Proof: Restriction can never increase number of flows, given the structure of $H$
Reformulation as Node Partitioning

\[
\min_{\Delta \theta} \|H \Delta \theta\|_0
\]
\[
\text{s.t. } H(k,:) \Delta \theta = 1
\]
\[
\Delta \theta_i \in \{0, 1\}
\]

Security index problem:
Pick partition of minimum # of flows and incident nodes

Flow between partitions

Each line with flow requires 2 attacks
Each node incident requires 1 attack

\(\Delta \theta_1 = 1\) \(\Delta \theta_2 = 0\) \(\Delta \theta_3 = 0\) or 1? \(\Delta \theta_4 = 0\) or 1?

target  additional
Partition nodes into two sets (black and white) such that source is black and sink is white (“a cut”)

Find partitions with the smallest number of edges from source set to sink set (“a min cut”)

Problem solvable in $O(|V||E| + |V|^2 \log|V|)$ operations
Security index problem

Generalized Min Cut problem

$$\begin{align*}
\min_{\Delta \theta} & \|H \Delta \theta\|_0 \\
\text{s.t.} & \quad H(k,:) \Delta \theta = 1
\end{align*}$$

How to solve generalized Min Cut?
Standard Min Cut on Appended Graph

Generalized Min Cut = Standard Min Cut on appended graph

generalized min cut  \iff  standard min cut appended graph

\[ |V| \text{ nodes} \]
\[ |E| \text{ edges} \]

\[ p_s = 2 \]
\[ p_1 = 0 \]
\[ p_2 = 4 \]
\[ p_3 = 4 \]
\[ p_t = 0 \]

Nodes \leq 3|V|
Edges \leq 3|E| + 2|V|

[Hendrickx et al., TAC, 2014]
Security index problem

$$\min_{\Delta \theta} \| H \Delta \theta \|_0$$

s.t. \( H(k,:) \Delta \theta = 1 \)

\textbf{Standard Min Cut problem on an appended graph}

\[ \text{maxflow, mincut} = \text{max}_\text{flow}(A, \text{source}, \text{sink}); \]

\textbf{Generalized Min Cut problem}

Practical implications?

[Sou et al., CDC, 2011]
[Hendrickx et al., TAC, 2014]
IEEE 14 Bus Benchmark Test Result

Security indices for all measurements

Solve time: MILP 1.1s; LASSO 0.6s; Min Cut 0.02s
Min Cut solution is **exact**

Solve time comparison:

<table>
<thead>
<tr>
<th>Method/Case</th>
<th>118 bus</th>
<th>300 bus</th>
<th>2383 bus</th>
</tr>
</thead>
<tbody>
<tr>
<td>MILP</td>
<td>763 sec</td>
<td>6708 sec</td>
<td>About 5.7 days</td>
</tr>
<tr>
<td>Min Cut</td>
<td>0.3 sec</td>
<td>1 sec</td>
<td>31 sec</td>
</tr>
</tbody>
</table>
Wish List

• Can we find solutions as **accurately** as MILP, and **faster** than LASSO?
  - Arbitrary $H$: No! (Problem NP-hard)
  - $H$ with the special physical and measurement structure: Yes! (Min cut polynomial time algorithm next.)

• Can we find methods giving more **problem insight**, and ideas for **assigning protection**?
  - Yes, exploit graph interpretation of solution
  - Securing sensors that are frequently cut gives indirect protection to many sensors!
    [Vukovic et al., JSAC, 2012]
Outline

• Background and motivation

• Quantifying security using sparse optimization

• Quantifying security using game theory

• Summary
Stealth Attack on Distribution System
Volt/VAR Control

- **Operator’s goal:** Switch capacitors $C^1$ and $C^3$ to make voltage levels as low as possible, but within safety limits.

- The voltage measurements $v_2$ and $v_5$ are stealth attacked (*i.e.*, bias consistent with physical model)

- **Adversary’s goal:** Make voltage levels unnecessarily high, but within safety limits (to avoid detection)

[Teixeira et al., ACC, 2014]
Operator vs. Adversary Game

**True voltage levels**

**Observed voltage levels** ($|a| = 0.5$)

**MP** = Mixed operator strategy

**BRP** = Pure operator strategy
Summary

• How to **quantify security** in CPS? Standard control metrics \( (\mathcal{H}_2, \mathcal{H}_\infty, \ldots) \) not necessarily the relevant ones

• Security metric using sparse optimization (exactly computable using min cut)

\[
\min_{\Delta \theta} \|H \Delta \theta\|_0 \\
\text{s.t. } H(k, :) \Delta \theta = 1
\]

• Game theory to quantify and limit possible damage of stealth attacks

• Many exciting opportunities in security for CPS!
Related References

• **Security metrics and sparse optimization:**

• **Game example:**