A Control-Theoretic and Data-Driven Approach to Securing Cyber-Physical Systems and Networks

Fabio Pasqualetti

Department of Mechanical Engineering
University of California, Riverside

2nd Annual CROSS Research Symposium & 9th UCSC Systems Oktoberfest
October 4-5, 2017, Santa Cruz, CA

Cyber-Physical Systems

- Power generation, transportation, distribution networks
- Water, oil, gas and mass transportation systems
- Sensor networks and multi-agent systems
- Process control and industrial automation systems
  (metallurgical process plants, oil refining, chemical plants, pharmaceutical manufacturing ... ubiquitous SCADA/PLC systems)

Security of these systems is critically important

Documented Security Incidents

Stuxnet worm (Iran, 2010)
New York Times 15jan2011: replay attack as if “out of the movies.”
  - records normal operations and plays them back to operators
  - spins centrifuges at damaging speeds

Cars vulnerable to cyber attacks
Hackers take control of cars: start/stop the engine, shut off the lights, hit the brakes...

Smart cities: security of automated cars, roads, and intersections?

Cyber-Physical systems are prone to failures and attacks against their physical, communication, and computational layers

Emerging Threats for Cyber-Physical Systems

- State / Actuator attack
- Data Substitution Attack
- Consensus attack

- Tamper with control and dynamic
- Compromise commands and reference signals
- Tamper with distributed computation

Pacific Northwest National Laboratory Report Reveals Dramatic Increase in Cyber Threats and Sabotage on Critical Infrastructures and Key Resources
June 2012 – US Dept of Energy

Some current headlines
- Cockrell School Researchers Demonstrate First Successful “Spoofing” of UAVs
- Obama: Cyber attack serious threat to economy, national security
- Pacific Northwest National Laboratory Report Reveals Dramatic Increase in Cyber Threats and Sabotage on Critical Infrastructures and Key Resources
- June 2012 – US Dept of Energy

Features
- Power generation, transportation, distribution networks
- Water, oil, gas and mass transportation systems
- Sensor networks and multi-agent systems
- Process control and industrial automation systems
  (metallurgical process plants, oil refining, chemical plants, pharmaceutical manufacturing ... ubiquitous SCADA/PLC systems)

Summary:
- This is the president of the United States of America outlining his thoughts on the threat of a cyber attack.
- He believes legislation will help the U.S. fight “the cyber threat to our nation,” which he calls “one of the most serious economic and national security challenges we face.”
- Fortunately, last month’s scenario was just a simulation—an exercise to test how well federal, state and local governments and the private sector can work together in a crisis. But it was a sobering reminder that the cyber threat to our nation is one of the most serious economic and national security challenges we face.
Cyber-physical security complements cyber security

Cyber security
- does not verify “data compatible with physics/dynamics”
- is ineffective against direct attacks on the physics/dynamics
- is never foolproof (e.g., insider attacks)

Cyber-physical security extends fault tolerance
- fault detection considers accidental/generic failures
- cyber-physical security models worst-case attacks

An Example of Cyber-Physical Attack

Physical dynamics: classical generator model & DC load flow
Measurements: angle and frequency of generator $g_1$
Attack: modify real power injections at buses $b_4$ & $b_5$

The attack affects the second and third generators while remaining undetected from measurements at the first generator

A. H. Mohsenian-Rad and A. Leon-Garcia “Distributed internet-based load altering attacks against smart power grids” IEEE Transactions on Smart Grid, 2011
Modeling Stuxnet as Unknown Inputs

System dynamics:
\[ E\dot{x}(t) = Ax(t) + Bu_3(t) \]
\[ y(t) = Cx(t) + Du_1(t) + Du_2(t) \]

Undetectable Attacks

The attack \( u \) is undetectable if its effect on measurements is
undistinguishable from the effect of some nominal operating condition

\[ y(x_1, 0, t) = y(x_2, u, t) \]

Detectability of Attacks

Equivalent characterizations of undetectable attacks:

- **Vulnerability**: undetectable attack \( y(x_1, 0, t) = y(x_2, u, t) \)
- **System theory**: intruder/monitor system has invariant zeros
- **Graph theory**: \# attack signals > size of input-output linking

Attack \((Bu(t), Du(t))\) is not detectable by measurements \( y(t) \) & destabilizes the system

By linearity, an undetectable attack is such that \( y(x_2 - x_1, u, t) = 0 \).
\[ \Leftrightarrow \text{invariant zeros for system} \]
\[ E\dot{x}(t) = Ax(t) + Bu(t) \]
\[ y(t) = Cx(t) + Du(t) \]
\[ \Leftrightarrow \text{nontrivial solution to} \]
\[ [sE - A -B] \begin{bmatrix} x_0 \\ u_0 \end{bmatrix} = 0 \]
Detectability of Attacks

Equivalent characterizations of undetectable attacks:

- **Vulnerability:** undetectable attack $y(x_1, 0, t) = y(x_2, u, t)$
- **System theory:** intruder/monitor system has invariant zeros
- **Graph theory #** attack signals > size of input-output linking

An Example of Undetectable Attack

- Physical dynamics: classical generator model & DC load flow
- Measurements: angle and frequency of generator $g_1$
- Attack: modified real power injections at buses $b_4$ & $b_5$

The attack through $b_4$ and $b_5$ excites only zero dynamics for the measurements at the first generator

(Many) Other Results, and Research Directions #1

Analysis of vulnerabilities and detection schemes:


Secure estimation in the presence of attacks:


Design of remedial actions:


(Many) Other Results, and Research Directions #2

Typical assumptions:

- Simple system dynamics, often linear and time-invariant
- Global system knowledge by attacker and defender
- Infinite computational power by attacker and defender (small data)

Our ongoing work:

- Large volume of data
- Scarcie system knowledge
- Richer class of dynamics
- Detailed system knowledge
Cloud-Connected Multi-Agent Networks

- Local, ad-hoc communication among nearby agents
- Cloud-based communication among far-away agents
- Cloud-based computation and contextual awareness
- Yet... additional vulnerabilities, more involved dynamics ...

Dynamics of Cloud-Connected Multi-Agent Networks

LTI for agents dynamics + impulsive updates for cloud interactions:

\[
\begin{align*}
\dot{x}(t) &= A_c x(t) + B_c u(t) \\
y(t) &= C_c x(t)
\end{align*}
\]
for \( t \in \mathbb{R}_{\geq 0} \setminus T \)

\[
\begin{align*}
x(t) &= A_i x(t^-) + B_i u(t) \\
y(t) &= C_i x(t^-)
\end{align*}
\]
for \( t \in T \)

- Unknown cloud interactions at \( T = \{\tau_1, \tau_2, \ldots\} \); \( \tau_k - \tau_{k-1} \geq \tau_{\text{min}} \)
- Attacks as unknown inputs to continuous and impulsive updates
  - malware injection into the cloud, authentication attack, man-in-the-middle attack, ...
- Monitor has access to measurements and dynamics matrices

Attack Detectability and Conditions #1

Geometric characterization of undetectable attacks:

1. **Attack undetectability**: \( y(x_0, 0, 0, T, t) = y(x_0, B_c, B_i, u, T, t) \)
2. **Output-nulling equivalence**: \( y(\tilde{x}_0, B_c, B_i, u, T, t) = 0 \)
3. **Existence of undetectable attacks**: There exist undetectable attacks \( (B_c, B_i, u) \) if and only if there exists a subspace \( \mathcal{V} \) satisfying

\[
\begin{align*}
\mathcal{V} &\subseteq \text{Ker}(C_c) \cap \text{Ker}(C_i) \\
A_c \mathcal{V} &\subseteq \mathcal{V} + \text{Im}(B_c) \\
A_i \mathcal{V} &\subseteq \mathcal{V} + \text{Im}(B_i) + \mathcal{R}_c
\end{align*}
\]

where \( \mathcal{R}_c \) is the output-nulling reachable subspace of \( (A_c, B_c, C_c) \)

Attack Detectability and Conditions #2

Geometric characterization of undetectable attacks:

1. **Attack undetectability**: \( y(x_0, 0, 0, T, t) = y(x_0, B_c, B_i, u, T, t) \)
2. **Output-nulling equivalence**: \( y(\tilde{x}_0, B_c, B_i, u, T, t) = 0 \)
3. **Existence of undetectable attacks**: There exist undetectable attacks \( (B_c, B_i, u) \) if and only if there exists a subspace \( \mathcal{V} \) satisfying

\[
\begin{align*}
\mathcal{V} &\subseteq \text{Ker}(C_c) \cap \text{Ker}(C_i) \\
A_c \mathcal{V} &\subseteq \mathcal{V} + \text{Im}(B_c) \\
A_i \mathcal{V} &\subseteq \mathcal{V} + \text{Im}(B_i) + \mathcal{R}_c
\end{align*}
\]

where \( \mathcal{R}_c \) is the output-nulling reachable subspace of \( (A_c, B_c, C_c) \)

Because \( y = 0 \), the state trajectory must be contained in the null space of the output matrices \( x \in \mathcal{V} \iff (1) + (2) \)
Attack Detectability and Conditions #3

Geometric characterization of undetectable attacks:

- **Attack undetectability:** \( y(\bar{x}_0, 0, 0, T, t) = y(x_0, B_c, B_i, u, T, t) \)
- **Output-nulling equivalence:** \( y(\bar{x}_0, B_c, B_i, u, T, t) = 0 \)
- **Existence of undetectable attacks:** There exist undetectable attacks \((B_c, B_i, u)\) if and only if there exists a subspace \( V \) satisfying
  \[
  V \subseteq \text{Ker}(C_c) \cap \text{Ker}(C_i) \quad (1)
  
  A_c V \subseteq V + \text{Im}(B_c) \quad (2)
  
  A_i V \subseteq V + \text{Im}(B_i) + R_c \quad (3)
  \]
  where \( R_c \) is the output-nulling reachable subspace of \((A_c, B_c, C_c)\)

After the impulsive update, the state needs to return to the stealthy subspace \( V \) while ensuring \( y = 0 \iff (3) \)

An Undetectable Attack Strategy

- \( \bar{x}(\tau_k) \)
- \( \bar{x}(\tau_k + \tau_{\text{min}}) \)
- \( \text{Ker}(C_i) \)
- \( \text{Ker}(C_c) \)
- \( \bar{x}(\tau_k -) \)
- \( \bar{x}(\tau_{k+1}) \)

\[
\begin{align*}
  u(t) = \begin{cases}
    F_c \bar{x}(t) + u_g(t) & \text{for } t \in (\tau_k, \tau_k + \tau_{\text{min}}) \\
    F_c \bar{x}(\tau_k) & \text{for } t \in [\tau_k + \tau_{\text{min}}, \tau_{k+1}) \\
    F_i \bar{x}(\tau_k -) & \text{for } t = \tau_{k+1}
  \end{cases}
\end{align*}
\]

- attack strategy \( u \) combines closed-loop and open-loop inputs
- attack strategy is not unique; different behaviors can be obtained
- \( \bar{x} \) is an auxiliary variable simulated by attacker

An Illustrative Example #1

\[
\begin{bmatrix}
  \dot{x}_c(t) \\
  \dot{x}_i(t)
\end{bmatrix} =
\begin{bmatrix}
  A_{cc} & A_{ci} \\
  0 & 0
\end{bmatrix}
\begin{bmatrix}
  x_c(t) \\
  x_i(t)
\end{bmatrix}
\]

\[
\begin{bmatrix}
  x_c(t) \\
  x_i(t)
\end{bmatrix} =
\begin{bmatrix}
  I & 0 \\
  A_{ic} & A_{ii}
\end{bmatrix}
\begin{bmatrix}
  x_c(\tau_k -) \\
  x_d(\tau_k -)
\end{bmatrix}
\]

- Man-in-the-middle + malware injection attack
- Agents 1, 3, 5 compromised
- Cloud anchor 2 compromised
- Local monitor with relative distance agents 2-3 and 4-5

\[
C_c =
\begin{bmatrix}
  0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 1 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

\[
C_i =
\begin{bmatrix}
  1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\]

\[
B_c =
\begin{bmatrix}
  1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}^T
\]

\[
B_i =
\begin{bmatrix}
  0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{bmatrix}^T
\]

An Illustrative Example #2

- Nominal system
- Attacked system
- System output
Summary and Future Work

Control-theoretic methods for cyber-physical security:

1. Control-theoretic security is complementary to cyber security
2. Algebraic and graphical conditions for detectability of attacks
3. Framework for security in cloud-connected multi-agent networks


Students: Alessandra Duz, Rajasekhar Anguluri, Vaibhav Katewa