Cyber-Physical Systems: Some Food for Thought

Ness B. Shroff

Electrical and Computer Engineering & Computer Science and Engineering

E-mail: shroff.11@osu.edu

THE OHIO STATE UNIVERSITY

What is CPS?

- By NSF:
  - "*…engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components*." --- [nsf14542.pdf, pp. 1]
- Some Defining Characteristics
  - Cyber-physical coupling
    - Every PHY component with Cyber capability
    - Networked at large and even extreme scales (nano vs. galacial)
  - Systems of systems
    - Complex & cross-cutting spatial-temporal constraints
  - New interactions between communication/computing/control
    - High degree of automation for large # of non-tech-savvy people

Domains of CPS

Energy Systems

Transportation systems

Agricultural Systems

Manufacturing Systems

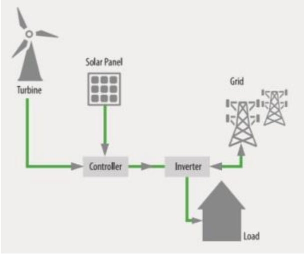
Buildings Systems

Medical Systems

Credit: Google images

Cross-Disciplinary

- PHY Modeling and Hybrid Systems Design
  - Require deep understanding of application domain
  - Human interface and interact with the systems



- Communications and Networking
  - Real-time sensing, tracking, and adaptation
  - Distributed control and computation

- Data Analytics
  - Machine learning
  - Prediction and optimization

- Safety and Security
  - PHY limits, cyber holes, privacy …
  - Greater flexibility ➔ greater vulenerability

Important Challenges

- **Modeling**
  - Accurate and tractable computational abstractions for system
  - Composition and interaction of Cyber and PHY components
- **Algorithm Design**
  - Low Complexity, self-adaptive
  - Distributed vs. centralized
  - Incomplete/imperfect state knowledge (due to size, costs….)
- **Performance Optimization**
  - Optimality, stability , convergence speed
  - Delay, robustness (safety), scalability
  - Security, privacy?

Modeling CPS: Respect PHY Laws

Different levels of complexity in modeling power systems

- DC Flow Models (Kirchhoff's Law)
  - Based on "sin(θ)~= θ if θ small" (i.e., ignore nonlinearity & reactive power)
  - Analytically easy to work with (due to linearity, convexity…)
  - Good for day-ahead & long-term planning (e.g., electricity market)
- AC Flow Model
  - Doesn't ignore nonlinearity, capture active/reactive powers
  - Noncovex, notoriously hard to work with (OPF open over 50 yrs)
  - Needed for more accurate steady-state analysis in shorter time-scale
- Transient Models
  - Power system dynamics (still being actively researched)
  - Hard to work with, stability is main concern
  - Needed for tasks (e.g., UFLS) at fast time-scale (e.g., 10^-1 secs)

Important Challenges

- **Modeling**
  - Accurate and tractable computational abstractions for PHY and Human
  - Composition and interaction of Cyber and PHY components
- **Algorithm Design**
  - Low Complexity, self-adaptive
  - Distributed vs. centralized
  - Incomplete/imperfect state knowledge (due to size, costs….)
- **Performance Optimization**
  - Optimality, stability , convergence speed
  - Delay, robustness (safety), scalability
  - Security, privacy?

Important Challenges

- **Modeling**
  - Accurate and tractable computational abstractions for PHY and Human
  - Composition and interaction of Cyber and PHY components
- **Algorithm Design**
  - Low Complexity, self-adaptive
  - Distributed vs. centralized
  - Incomplete/imperfect state knowledge (due to size, costs….)
- **Performance Optimization**
  - Optimality, stability , convergence speed
  - Delay, robustness (safety), scalability
  - Security, privacy

Complex Interactions

- In a variety of CPS systems, there can be complex, sometimes **unexpected** interactions that must be carefully modeled, analyzed, and designed for.
- Discuss examples in:
  - Green Buildings
  - Sensor Networks with Renewable Energy
  - Smart Grid
  - Electric Grid …

Green Buildings

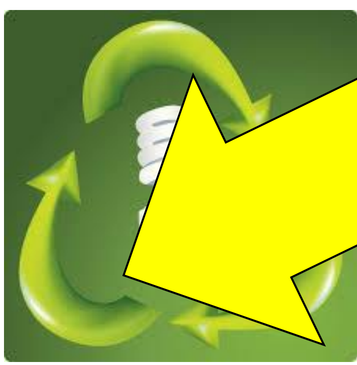
There could be unintended/surprising coupling effects
E.g., in “green”buildings:

Producing less heat

…ore energy
…human
…omfort

…gs

Green? Maybe Not!



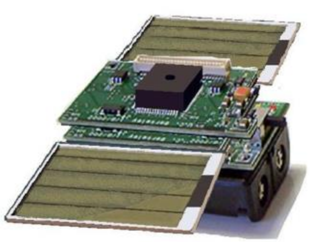
Energy-Efficient Lighting

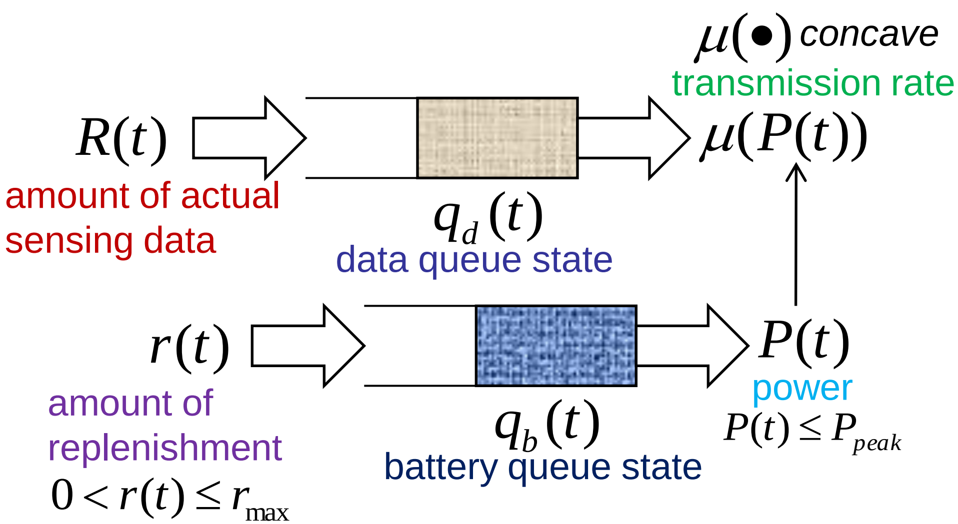
HVAC Systems

A deeper understanding and domain knowledge is critical in designing for CPS

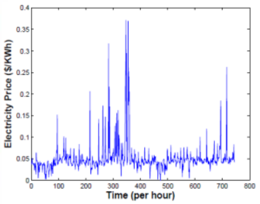
Systems with Renewable Energy

- Sensor networks w/ renewable energy.
  - Traditional approaches of energy management (e.g., keeping batteries full) can leads to poor performance
  - Need to find right balance between [Mao,Koksal,Shroff,TAC12]:
    - —Energy conservation: Missed recharging opportunities b/c battery full ➔ data loss or reduced capacity
    - —Over-aggressive use of energy leading to potential loss of connectivity/coverage





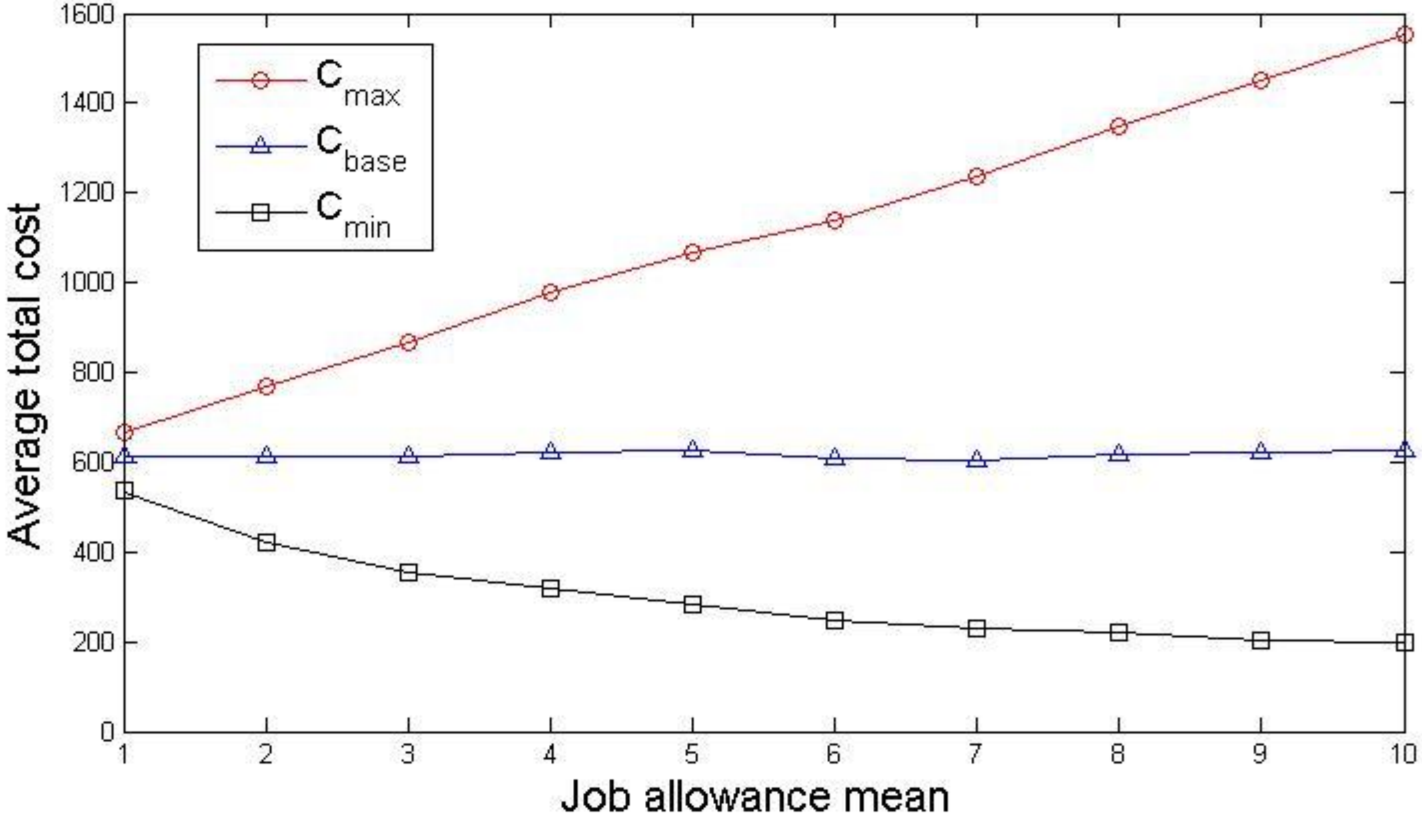
Smart Grid



- Smart Grid: Random demands meet uncertain supply
  - Distributed renewable supplies of energy

> - **Individual actions may cause instability**
> - **Greater vulnerability to stealthy attacks**

Flexibility results in greater vulnerability



- A stealthy adversary can intercept/modify control messages
  - Stealth: It may modify only a fraction of msgs, and always ensure feasibility
  - Damage can be quite significant (e.g., increased power cost)

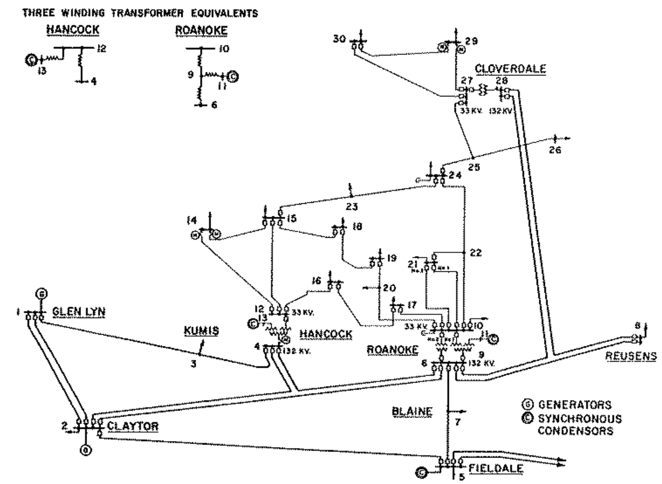
Electric Grid: Blackout

- US-Canada 2003 Blackout
  - 2nd largest in history, 55m people affected, cost $10 billions
- Causes [US-Canada Pwr Sys Ourage Task Force ‘04]:
  - A combination of many physical-computer-human errors
  - Timeline: 8/14/2003, 12:15pm—16:05 (nearly 4 hours)
  - Key **Cyber-failure**: MISO’s centralized contingency analysis failed to converge in **4 hrs** due to erroneous Topo. Info. by communications problems

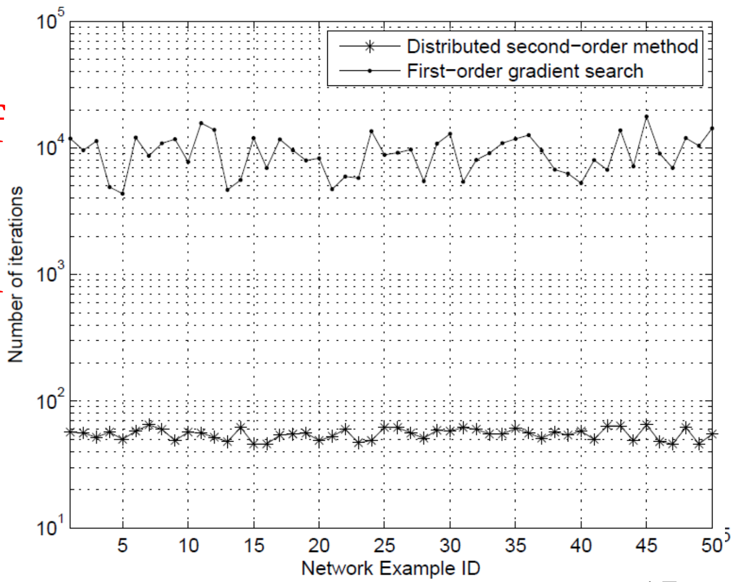
Centralized vs. distributed?
Convergence speed?

Fast Distributed Contingency Analysis

- A Second-order Distributed Approach [Liu,Xia,Shroff,Sherail Sigmetrics'14]
  - RST-Based Reformulation under DC
  - Interior-point + 2nd-order framework
  - Distributed design by exploiting RST



- Features
  - **Quad. rate of convergence**: $O(\log_2 \log_2(K/\varepsilon))$ (small constant for all ε of practical interests)
  - All iterates feasible (guarantees safety even terminated prematurely)
  - Enable use of many efficient distributed spanning tree algs. (Exactly goal of CPS!)



Summary

- Many opportunities
  - Many enabling technologies: communications & networking, massively parallel cloud computing, real-time sensing & tracking…
  - Leverage existing knowledge/tools: Distributed control; stochastic optimization; large-system dynamics, decision processes, approx. algo …
- Many challenges:
  - Tailored design: For specific 'CPS application' needs
    - Deep understanding, hardly 'one size fits all' solutions
  - Speed and Low-latency: Fast control algorithms, low delay data collection…
  - Cascading failures in cyber-physical systems: Failure of Cyber systems could cause failure/instability in PHY systems & vice versa...
  - Performance vs security: Greater controllability/elasticity also exposes vulnerability…

Thank you

Backup Slides