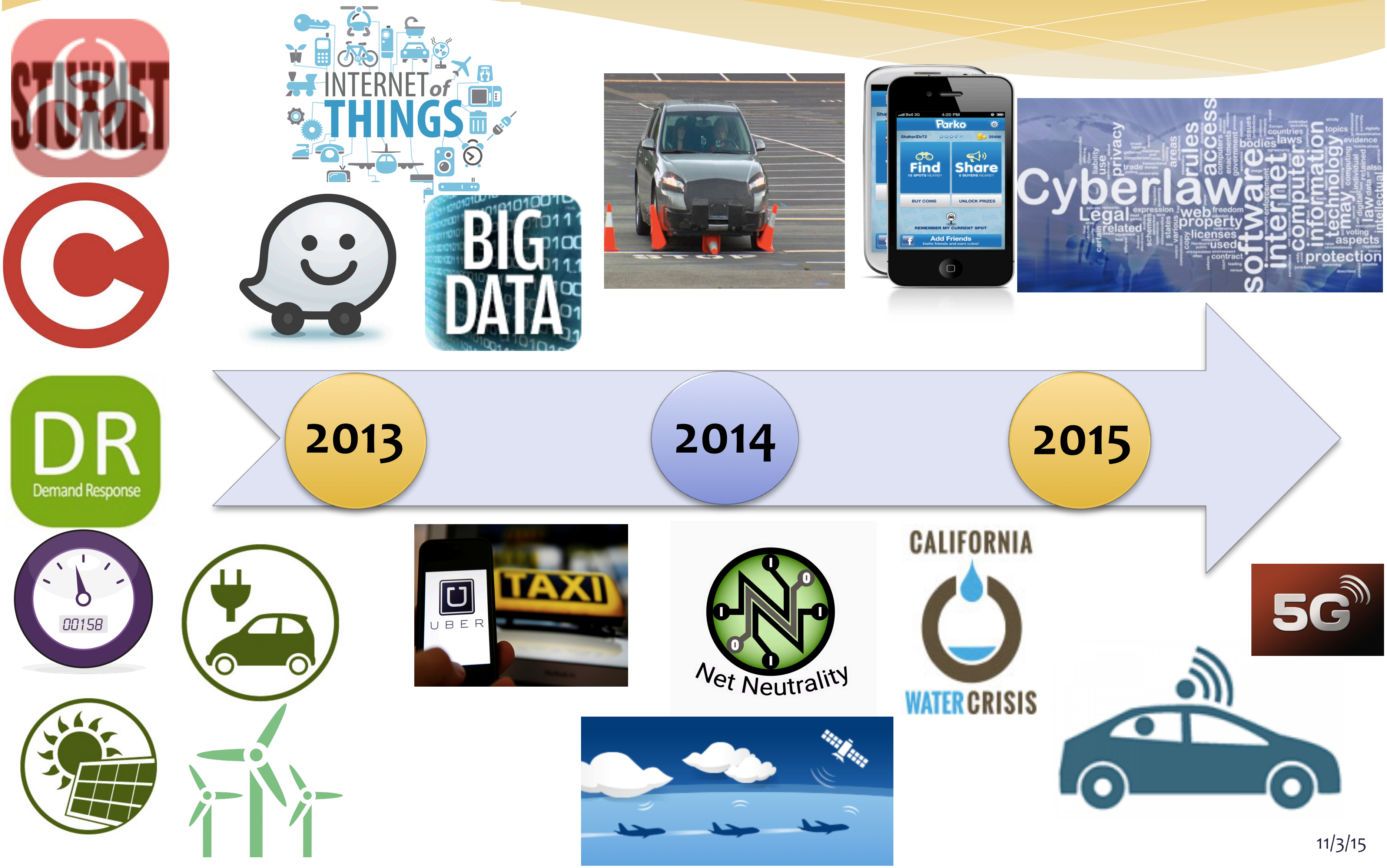
FORCES Scientific Agenda

Saurabh Amin
MIT

Annual Review, November 4-5, 2015

CPSs continue to be on [rapid] ascent!



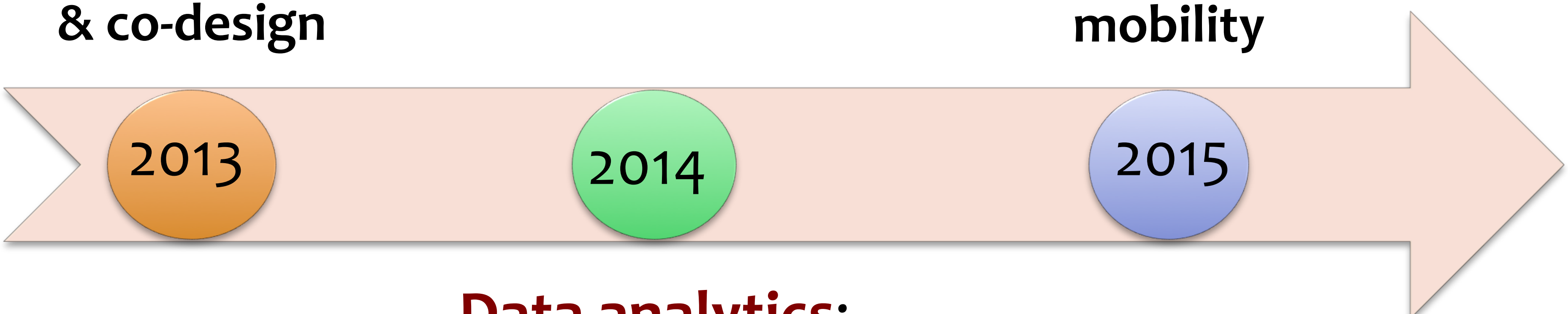
FORCES: Timeline and refinement of agenda

RC+EI

Integration & co-design

New Services & Markets:

Data, energy, mobility



Data analytics:

Humans + CPS

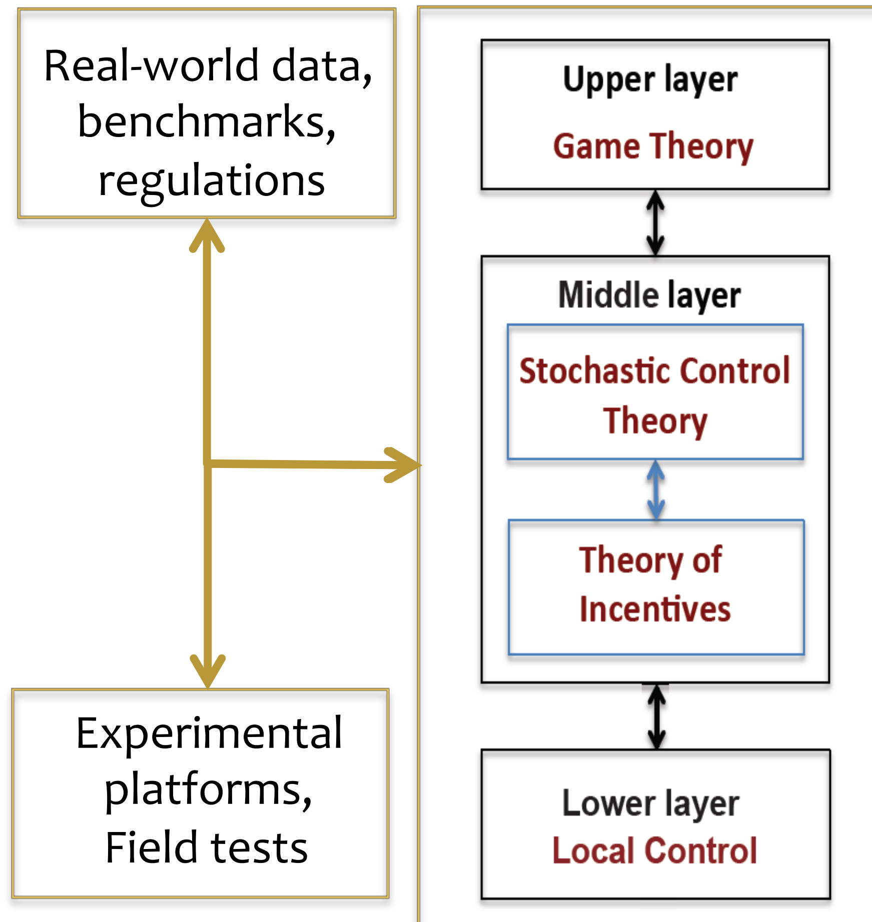
Privacy & security

Incentive regulation

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FORCES Technical Approach

1) **Network Games**
   * How the collection of CPS agents deal with strategic entities?
   * Security-Reliability failure models
2) **Incentives & Mechanism design**
   * How strategic entities contribute to CPS efficiency while protecting their individual objectives?
   * Joint stochastic control and incentive theoretic design coupled with outcome of network game
3) **Resilient diagnostics & control**
   * Security & privacy preserving control
   * Resilience to cyber-physical failures and network level attacks



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Outline

1) **Network games**
   * Security (attacker-defender) games
   * Congestion games, routing, and learning
   * Incomplete information games of CPS entities
2) **Incentives and Mechanism design**
   * Data, energy, mobility services: new markets, regulation, pricing
   * Security and privacy constraints (in addition to efficiency)
   * Imperfect competition and asymmetric (private) information
3) **Resilient diagnostics and control algorithms**
   * Data-driven, stochastic hybrid models of operational modes
   * Fast approximation algorithms for diagnostics and estimation
   * Network control and demand management under uncertain supply and/or security failures

Cross-industry CPS infrastructure

* CPS infrastructures differ across several dimensions
  * Requirements, characteristics, properties
* Resilience a cross-cutting need
  * But details vary across industries
* How can we characterize cyber-physical infrastructures?
  * Capture commonalities as well as differences

* **Tariq Samad: "Abstractions are important, but solutions must be informed by the problem domain"**
* **Challenge posed by David Corman in 2014: "Pick one abstraction and illustrate problem-domain inspired solutions on it."**

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Part I: Network Games & Resilient Control

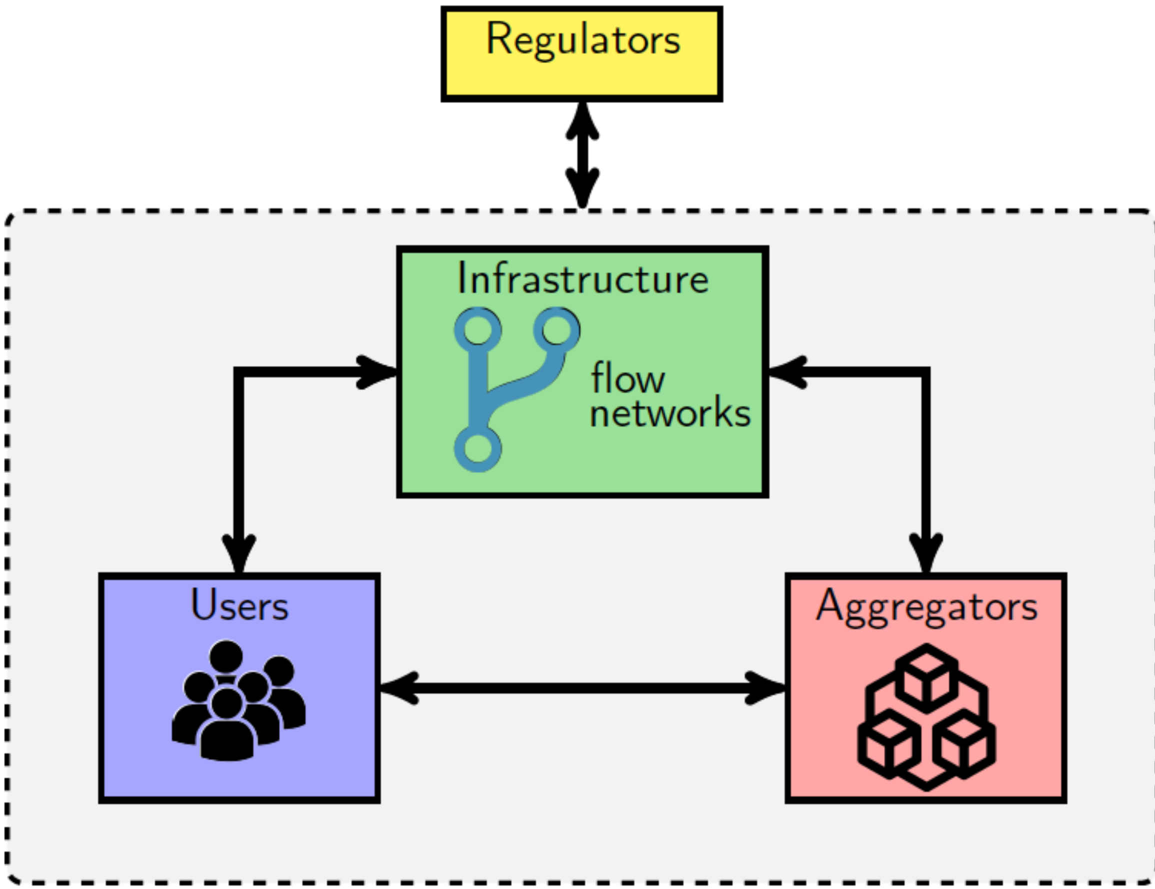
* Infrastructure networks: traffic, water, electricity distribution

* **Physical**: nonlinearities and constraints (operational & safety)
* **Cyber**: sensing and communication network architectures
* **Multiple entities**:
  * Users (commuters / customers)
  * Network operators (defender) and regulators
  * Malicious agents: adversarial flows, disruptions (node or link)
  * New service providers: data/information, energy, mobility

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Networked environment

Ratliff, Dong, Sastry

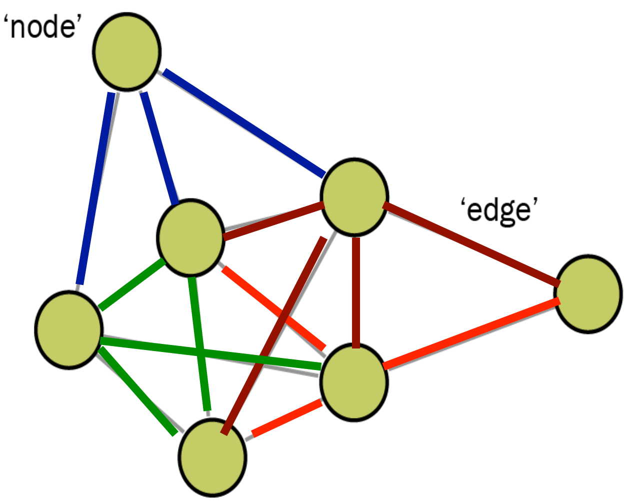


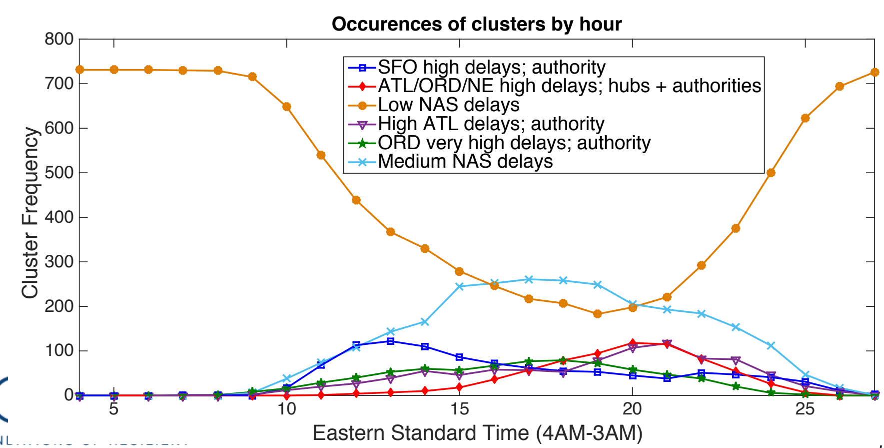
FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Dynamic network structure estimation under stochastic delays

Balakrishnan, Gopalakrishnan, Badrinath

* Structure estimation of air traffic "delay networks"
* Edges weights model departure delays on OD pairs
* Clustering based on network centrality metrics and weights (delays)
* Stochastic switched systems models of delay propagation through air traffic networks
* Basic input to resiliency improving control algorithms

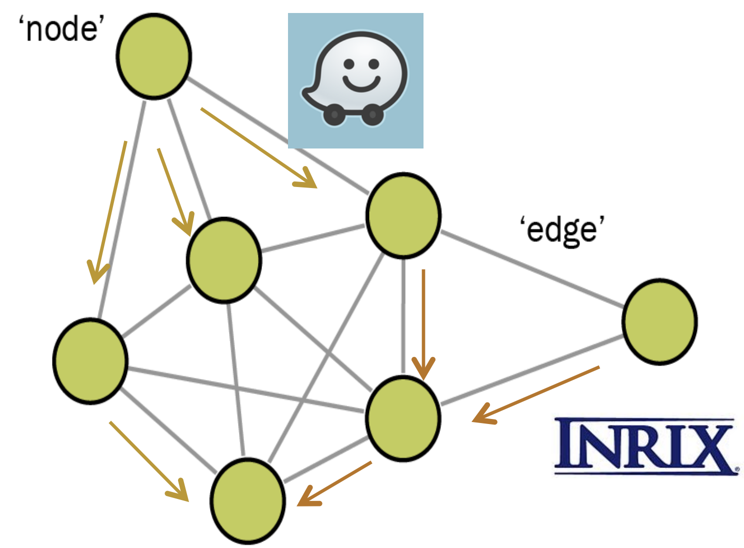


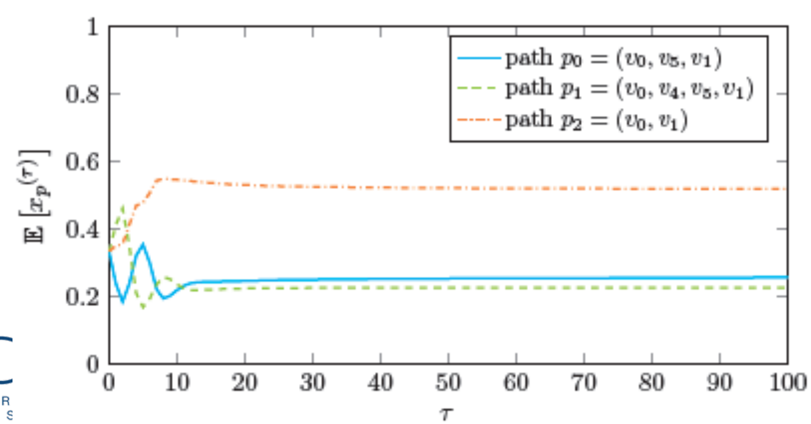


Routing games: learning with noisy information

- N-player routing games with multiple information providers
- Make choice ---> Drive ---> Evaluate outcome ---> Learn
- For a class of convex potential games, showed convergence in:
  - Approximate replicator dynamics
  - Distributed mirror descent
  - Distributed stochastic mirror descent
- Deep connections with machine learning, specifically online learning
- Extensions to Nash-Stakelberg games

Krichene and Bayen

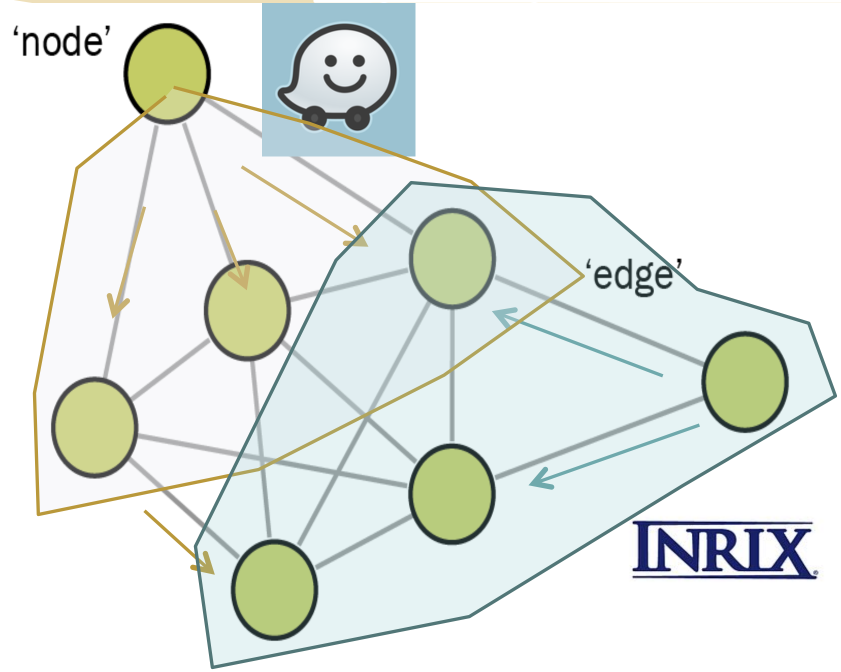


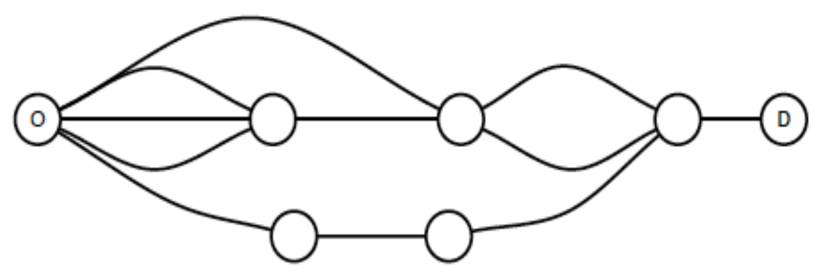


Network routing with heterogeneous information

Ozdaglar, et al.

* Effect of providing more information about possible routes to a subset of users
* Users choose lowest-cost path, but information set of one subgroup is "expanded"
* *Informational Braess paradox*: providing info about additional edges increases travel time!
* Paradox does not occur if and only if graph is series-parallel



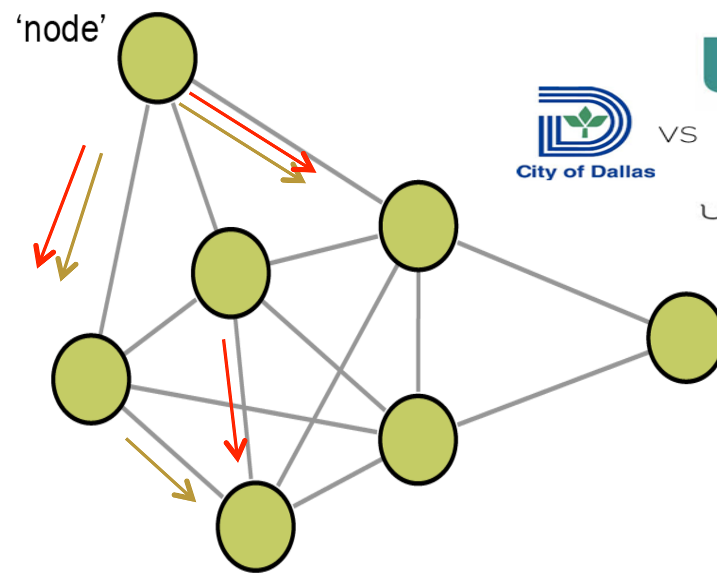


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

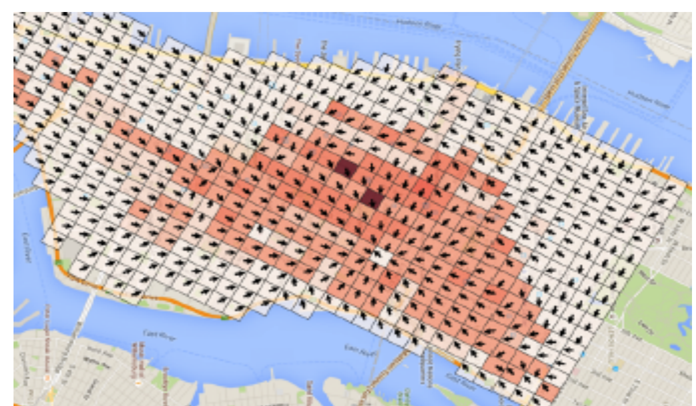
Network routing with strategic non-cooperative atomic flows

Yuan, Thai, Bayen

- Strategic competition between Mobility-as-a-Service systems in transportation networks
- Scenario: One entity becomes malicious by artificially limiting supply and increasing demand
- Effects of strategic and malicious behavior interpreted as DoS by "Zombies" (in addition to customers and balancers)
- Jackson queuing network + non-cooperative game model
- Outcome: Penalty to deter such attack and adjustment of cancellation charges



City of Dallas VS lyft UBER

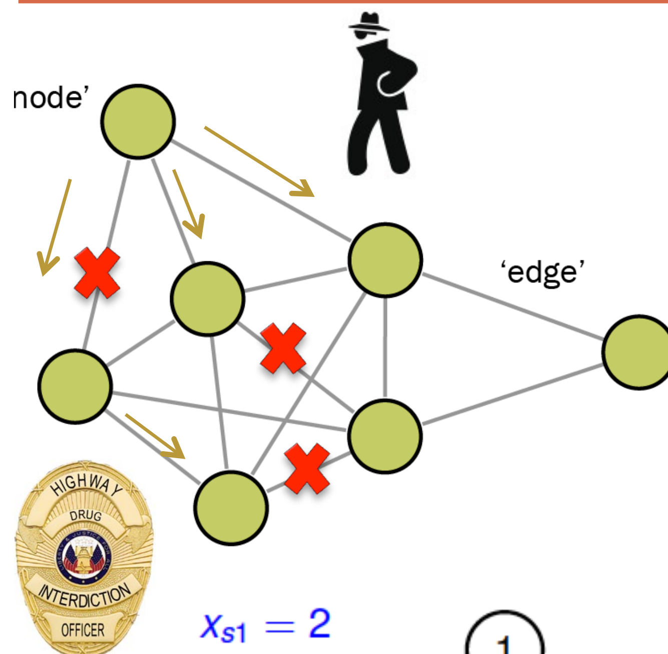


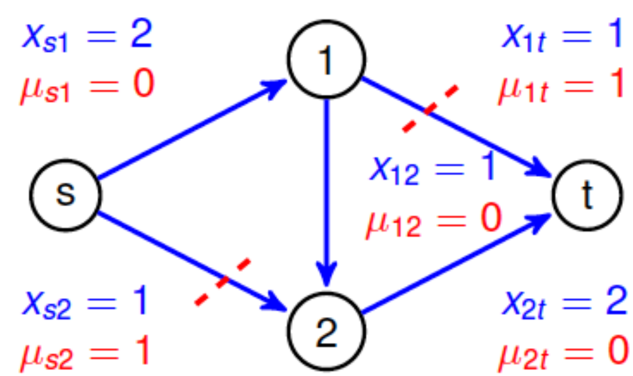
CES
F RESILIENT
AL SYSTEMS

Network flow routing under adversarial link disruptions

Dahan, Amin

- Simultaneous non-zero sum game
- Player 1: disrupt multiple edges and face cost of attack
- Player 2: strategically choose flow but no-rerouting after disruption and face cost of transportation
- Outcomes: structural insights on NE; extension of network flow problems (specifically, max-flow min-cost and min-cuts); measure of network vulnerability under strategic attacks



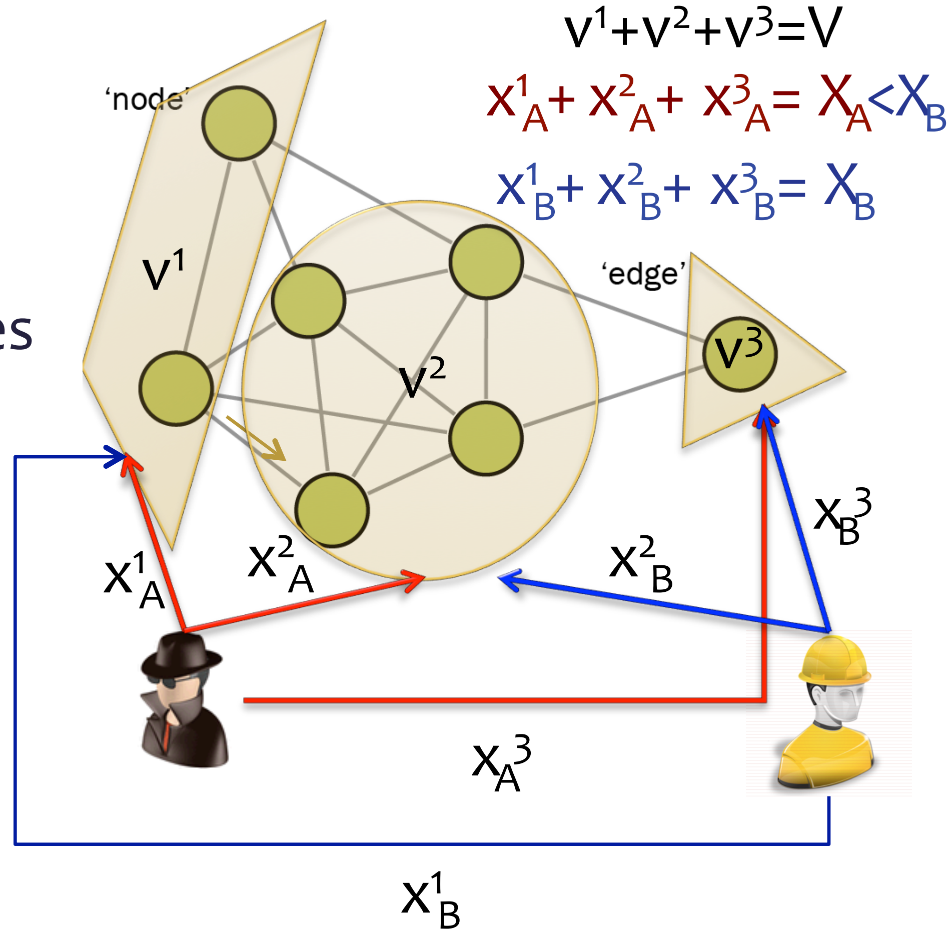


Initial flow and attack.

Network defense in multi-battlefield conflicts

- Blotto games: General resource allocation in strategic settings and multi-battlefield conflicts
- Constant-sum, non-finite game with discontinuous payoffs
- Nash Eq. only in mixed strategies
- Contributions: Asymmetric players and heterogeneous battlefields
- Possibility to add extra fields and form alliances (coalitions with transfer of resources)

Schwartz, Loisseau, Sastry

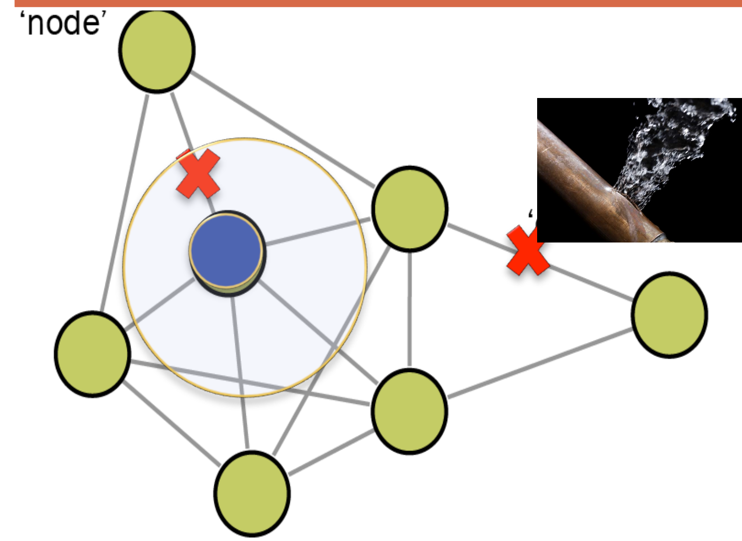


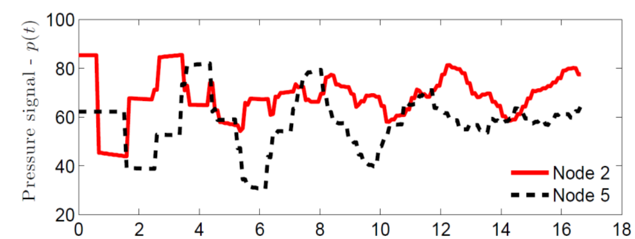
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Network sensing under random link disruptions

Abbas, Sela, Kousoukos, Amin

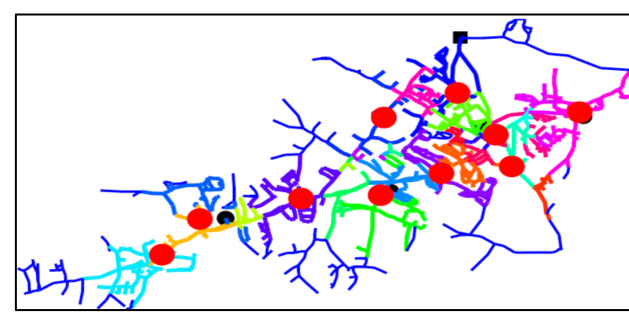
* Detection and localization of link failures (pipe leaks & bursts)
* Sensor network design to maximize detec./local. with minimum number of sensors
* Outcomes: Minimum set and test cover formulations; efficient greedy algorithms for submodular opt.
* Heterogeneous network design with multi-level sensors





Abbas, Laszka, Kousoukos

* Scheduling IDS on resource-constrained nodes
* New graph labeling approach to achieve desired tradeoffs between diagnostic performance and network lifetime

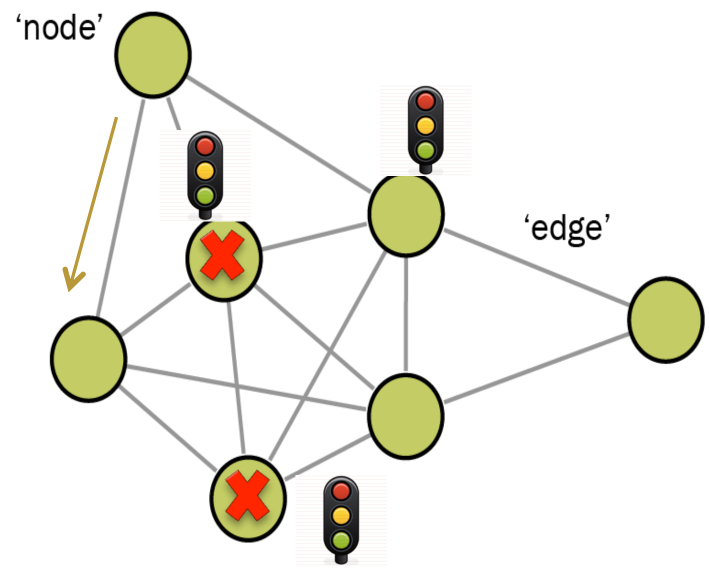


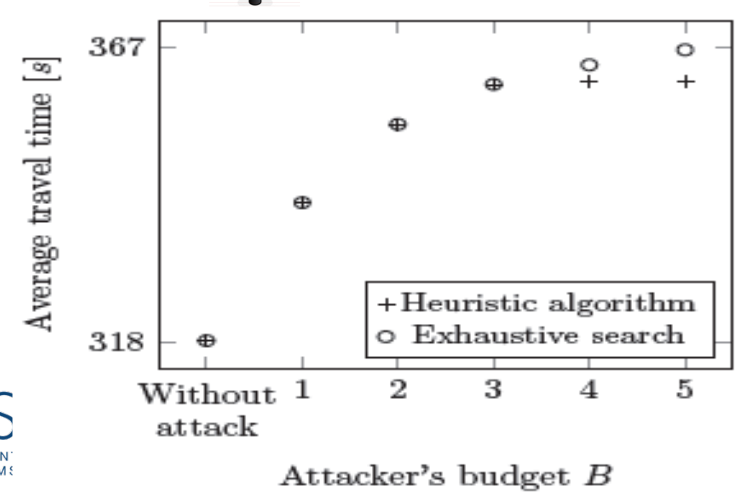
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Network sensing under strategic node disruptions

Laszka, Potteriger, Vorobeychik, Kousoukos, Amin

* Resilience of transportation networks under traffic signal compromises
* Effects: adversarial congestion and network-wide jams
* Vulnerability analysis: find critical intersections when resource constrained attacker tampers signals (coordinated attack) to maximize network congestion
* Greedy algo. for macroscopic model
* Evaluation: calibrated micro-simulation of real-world networks
* Similar ideas apply to resilient observation selection in Gaussian processes

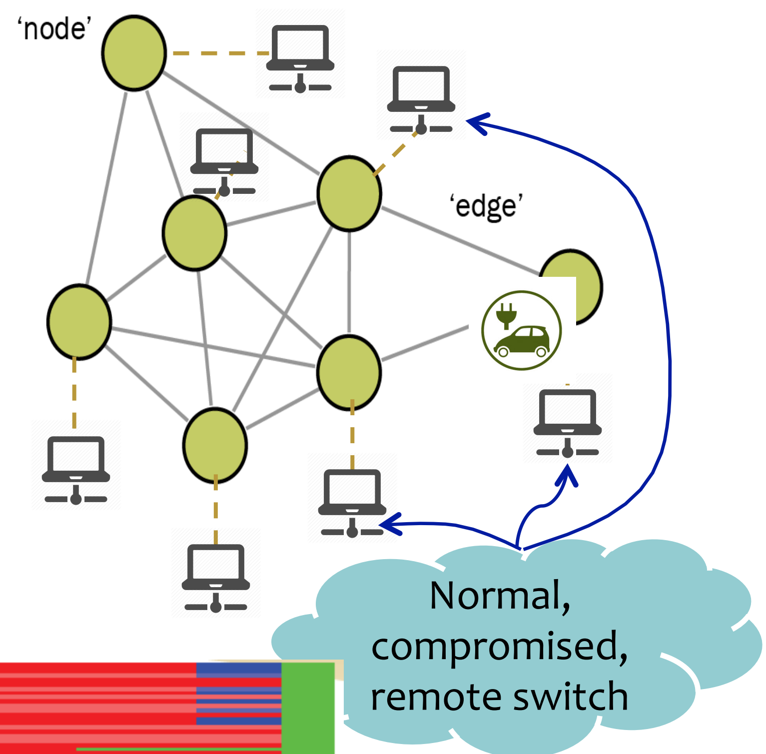


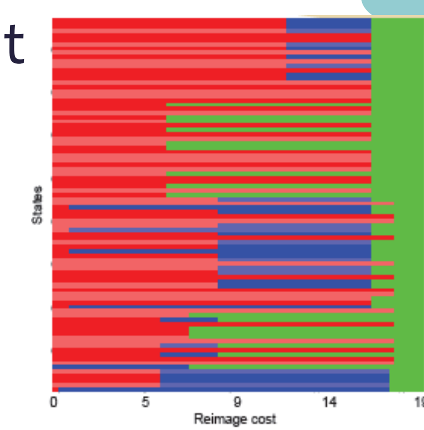


Network supervisory control with progressive attacks

Rasouli, Miehling, Teneketzis

* Supervisor control approach
* Defender: dynamic defense, imperfect information, and state-dependent cost for security actions
* Models progressive attacks (in both time and scale of the network)
* Outcome: Dynamic programming with numerical results for determining optimal (minimax) defense policy within a restricted class of policies at each time period
* Applicable to supervisory minimax control of CPS with dynamic state evolution and progressive attacks



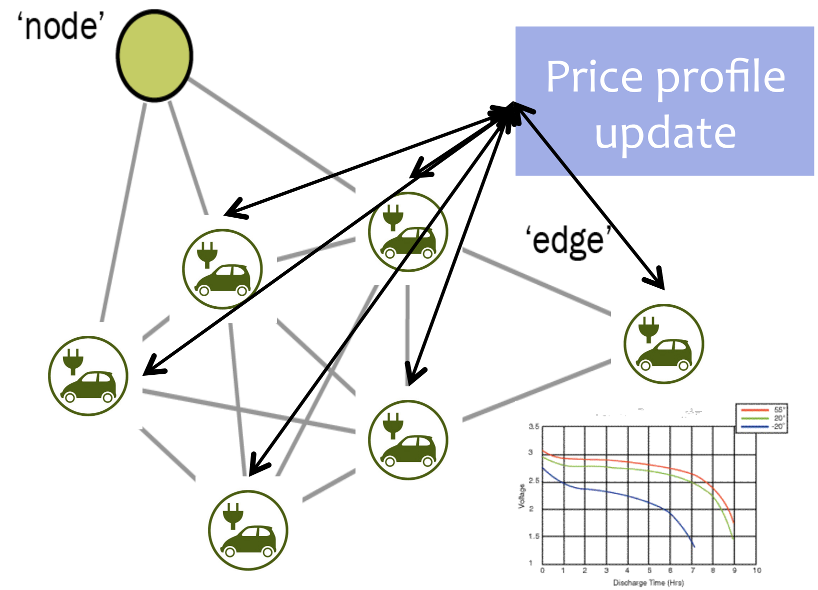


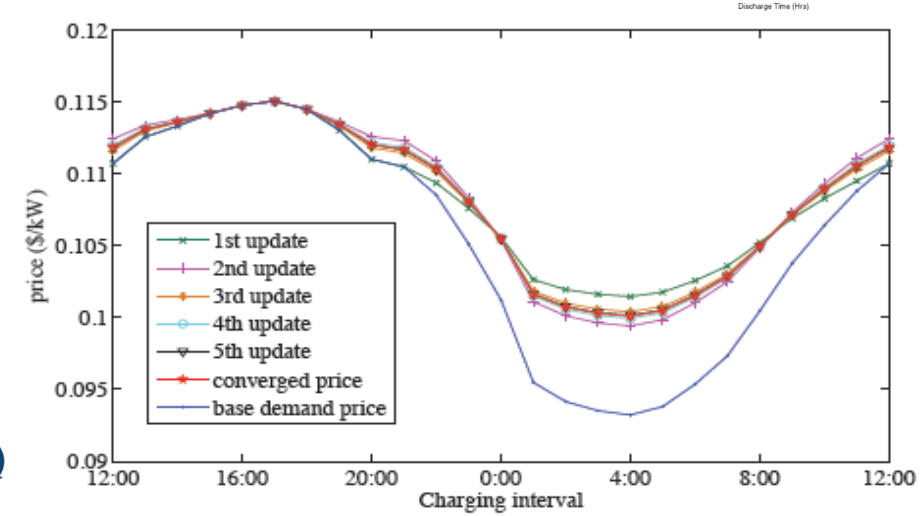
Optimal defense policy

Decentralized control to achieve tradeoff between network performance vs node reliability

Ma and Hiskens

- Responsive load control of networks with PEVs
- Trade-offs between: energy price, distribution network effects, and battery degradation (node reliability)
- Contribution: design of individual cost function and price update mechanism to achieve socially optimal (centralized) solution

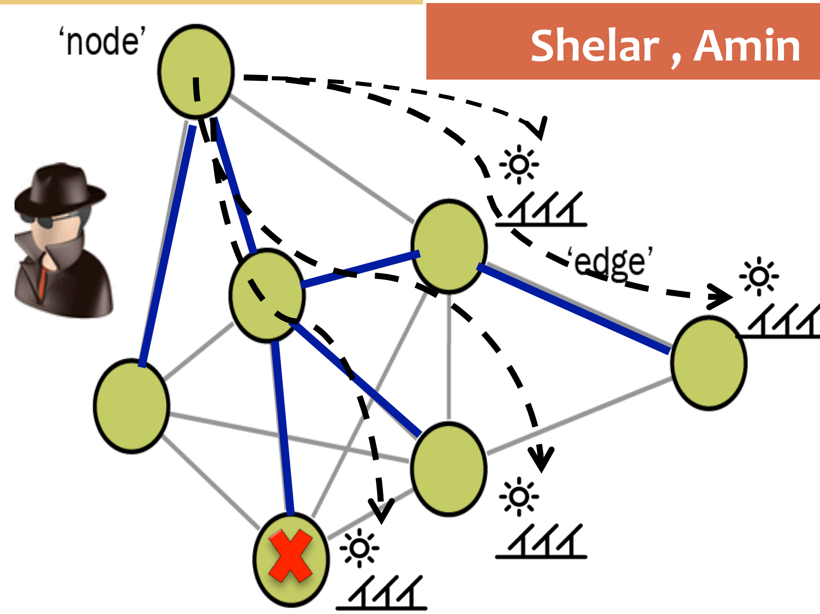


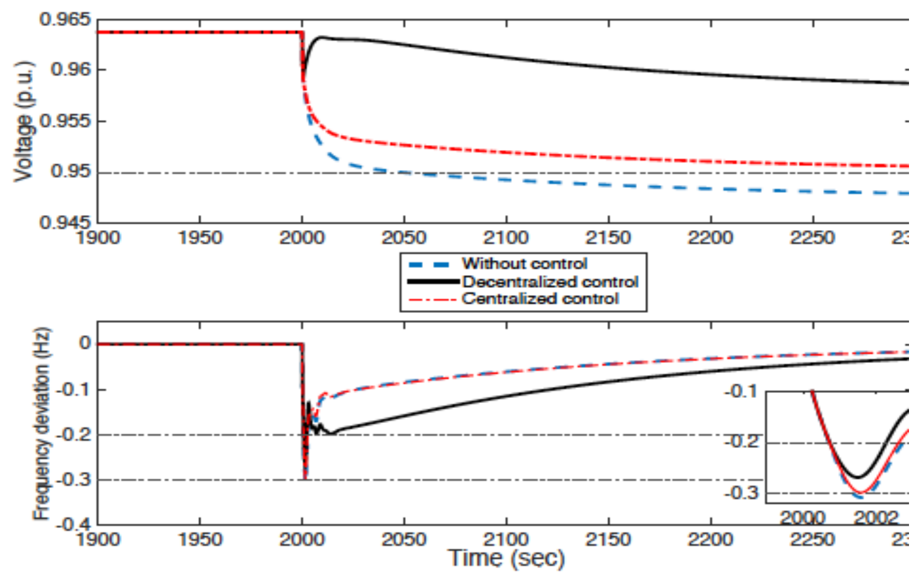


Network control under strategic DER node disruptions

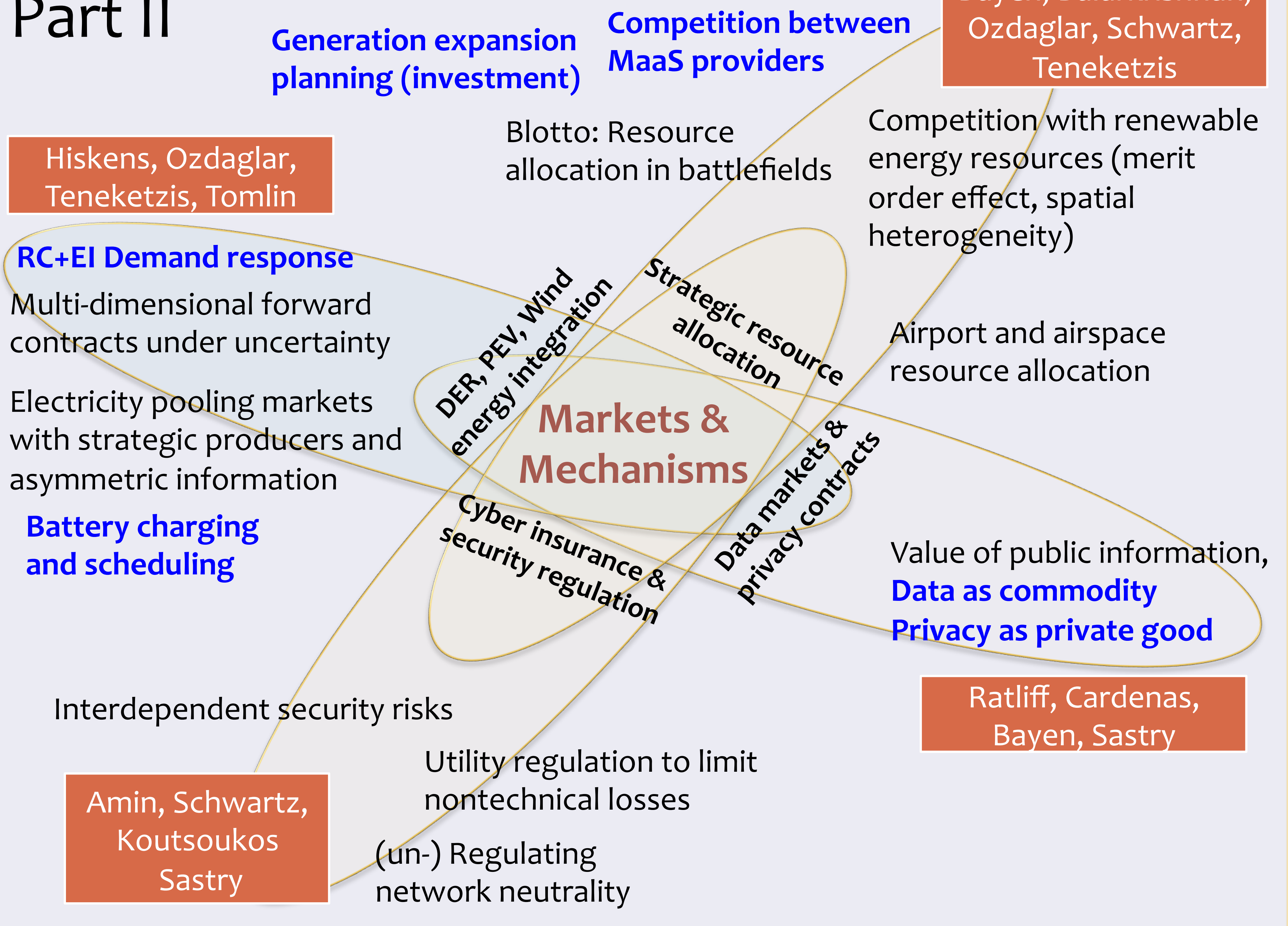
Shelar , Amin

- Vulnerability assessment of electricity networks to disruptions of Distributed Energy Resources (DERs)
- Design decentralized defender (network operator) strategies
- Outcomes: Interdiction model; Structural results on worst case attacks that maximize voltage deviations and / or freq. deviation
- Efficient (greedy) technique for solving interdiction problems with nonlinear power flow constraints
- Distributed control strategies





Part II



Generation expansion planning (investment)
Competition between MaaS providers
Bayen, Balarkrishnan, Ozdaglar, Schwartz, Teneketzis
Blotto: Resource allocation in battlefields
Competition with renewable energy resources (merit order effect, spatial heterogeneity)
Hiskens, Ozdaglar, Teneketzis, Tomlin
RC+EI Demand response
Multi-dimensional forward contracts under uncertainty
Electricity pooling markets with strategic producers and asymmetric information
Battery charging and scheduling
DER, PEV, Wind energy integration
Strategic resource allocation
Airport and airspace resource allocation
Markets & Mechanisms
Data markets & privacy contracts
Cyber insurance & security regulation
Value of public information,
Data as commodity
Privacy as private good
Ratliff, Cardenas, Bayen, Sastry
Interdependent security risks
Utility regulation to limit nontechnical losses
(un-) Regulating network neutrality
Amin, Schwartz, Koutsoukos Sastry

Part III: Modeling and Experimentation

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Analytics-driven resurgence of Stochastic Hybrid Systems

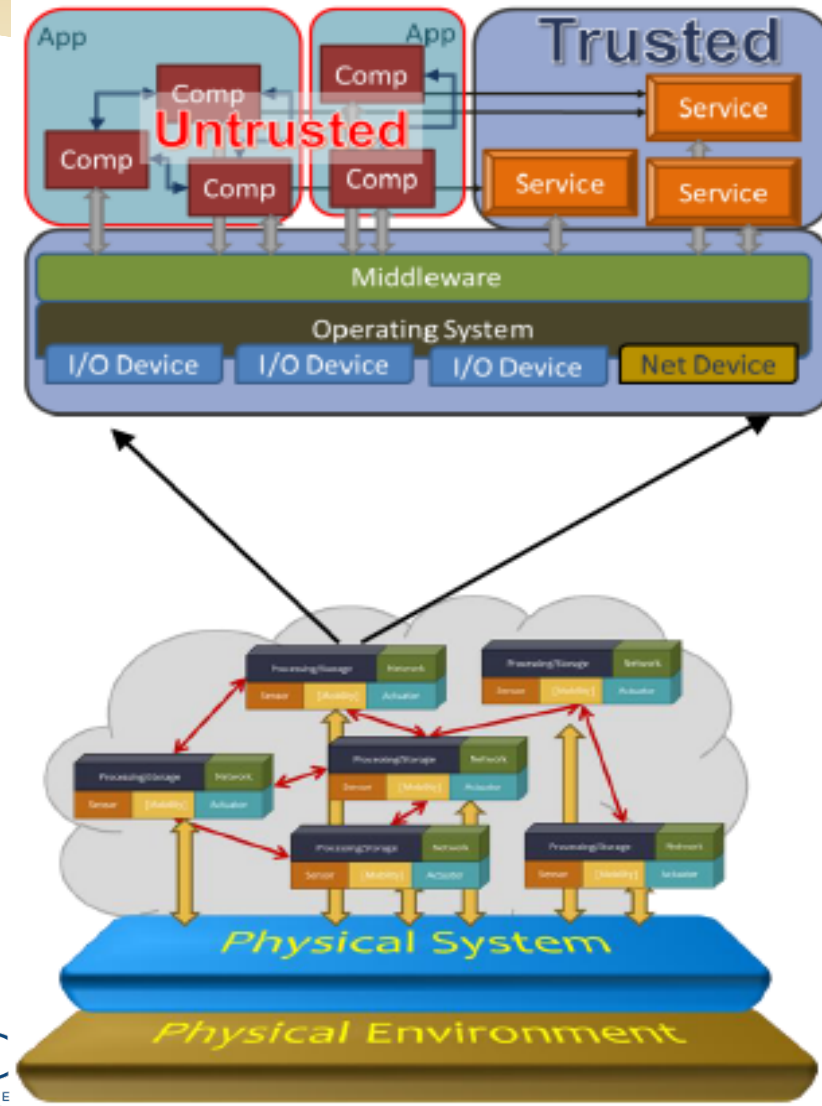
* **Modeling, state estimation, inferences, and control**
* Random incidents, i.e., state dependent transitions and capacity fluctuations in freeway networks (PDMPs): **Jin and Amin**
* Non-intrusive load monitoring and utility learning (HMM and variants): **Ratliff, Dong, Sastry**
* Modeling of aircraft engine performance (Bayesian multiple linear regression): **Chati, and Balakrishnan**
* Secure state estimation under adversarial attacks (Kalman filters and switching variants): **Chang, Hu, and Tomlin**
* Quantifying user engagement in DR programs (nonparametric regression): **Balandat, Zhou, and Tomlin**
* Ensemble control of hysteretic loads (nonlinear hybrid systems): **Hiskens**
* Delay propagation in air-traffic networks (SHS models): **Balakrishnan, Gopalakrihnan**

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Evaluating Resilience

Karsai et al.

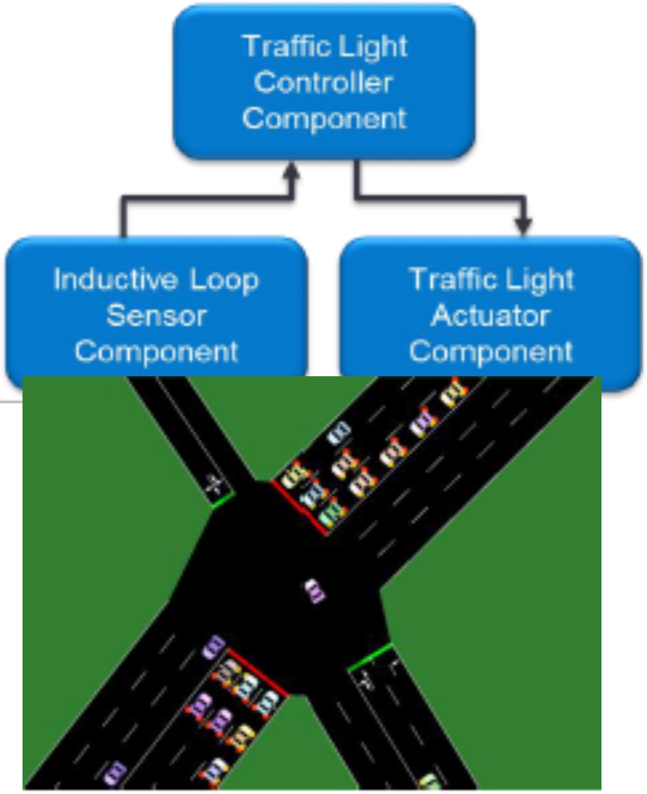
* Resilience: system-level property
* Software platform with core abstractions and services
  * Trusted platform
  * Untrusted appln. & components
* Management of cyber-physical interactions and integrations
* Key questions: modeling of resilient architectures in CPS, secure software, and assurances for resilience

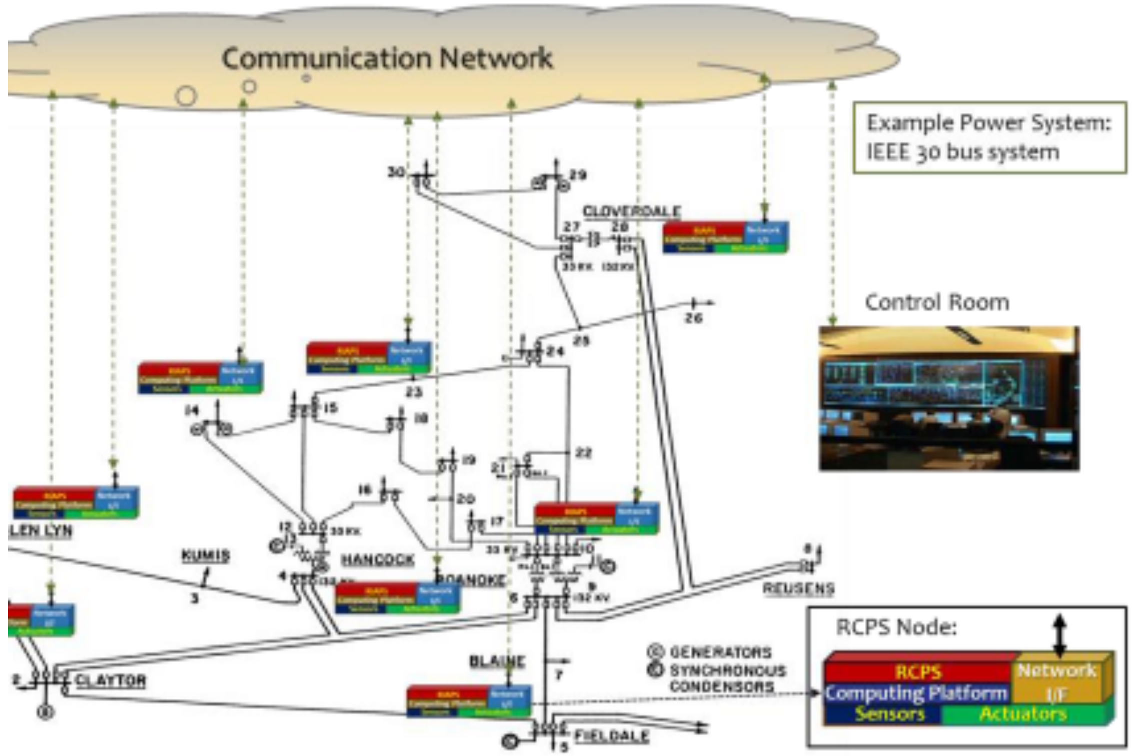


FORC
FOUNDATIONS OF RE
CYBER-PHYSICAL SY

CPS architectures for monitoring & control

Karsai et al.



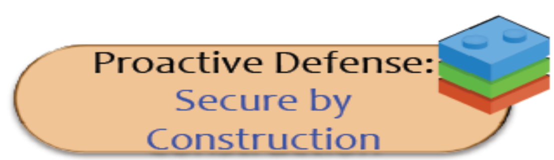


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Security & Privacy Solutions: IoT to CPS

Song, et al.

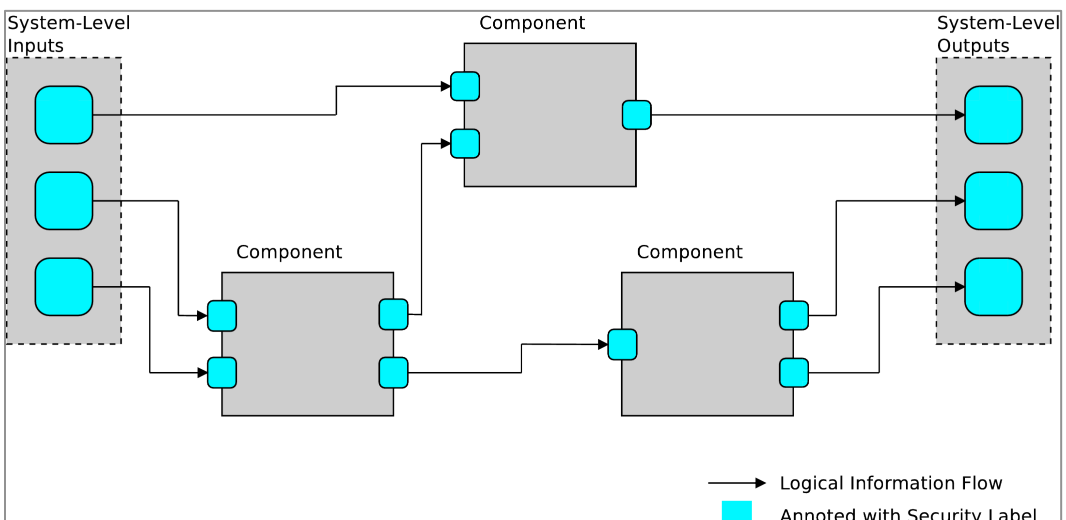
* Traditional vulnerabilities & new attacks
* Security analysis tools (state consistency attacks, privacy leaks)
* New tools and security concepts
  * Define security properties and enforce certain minimum specs
  * Move from a posteriori bug finding to secure by construction
  * New solutions for program hardening: Compact control-flow integrity; code pointer integrity
* New ideas for secure collaborative analytics:
  * Attach security policies to data
  * Enforce learned security policies



Embedding security requirements in system-level design process

Sztipanovits

* Behavior and information flow models ---> Security requirements ---> mapping and co-design tool suite development
* Main focus:
  * Integrity attacks: manipulation of CPS data
  * Confidentiality: data leakage to unauthorized entities
* Dencentralized label model for information flow control: extension to system-level information flow modeling languages



Thank you!

and look forward to exciting talks and discussions