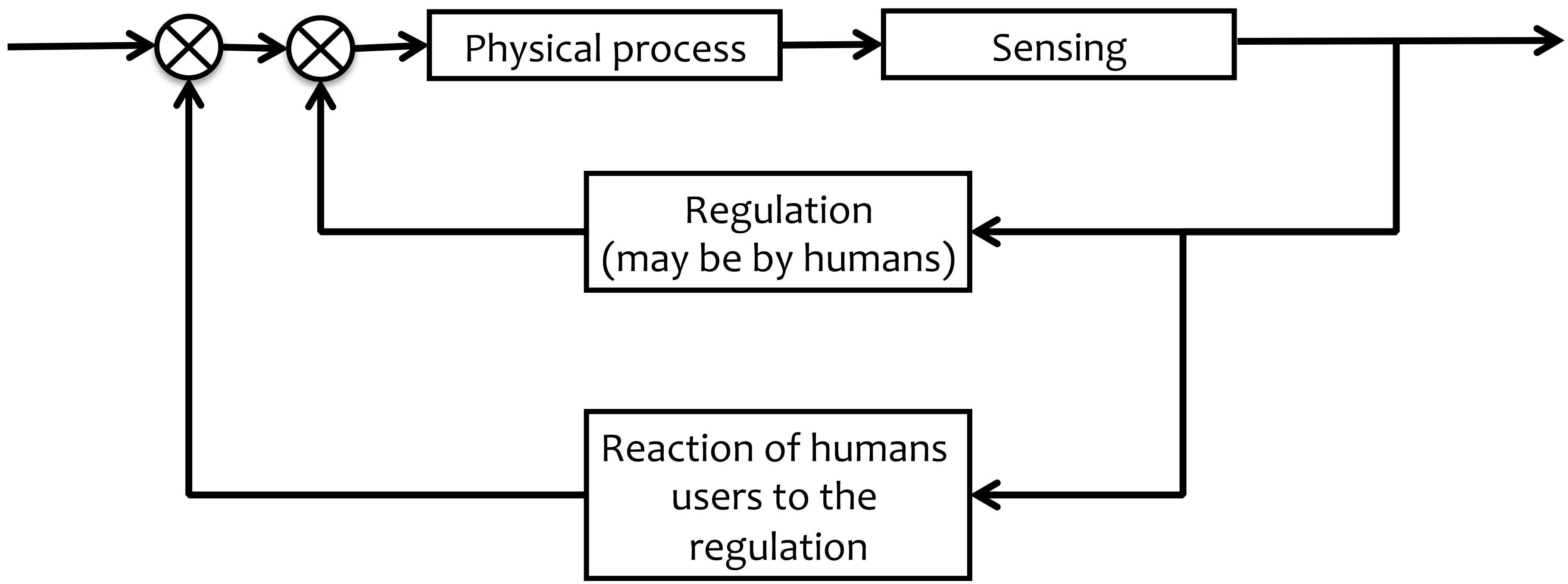
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Resilience and robustness of networks: from games to security

Alex Bayen, EECS / CEE
with Walid Krichene, Jack Reilly, Jerome Thai

Berkeley UNIVERSITY OF CALIFORNIA
Massachusetts Institute of Technology
NSF
MICHIGAN
VANDERBILT UNIVERSITY

Talk outline



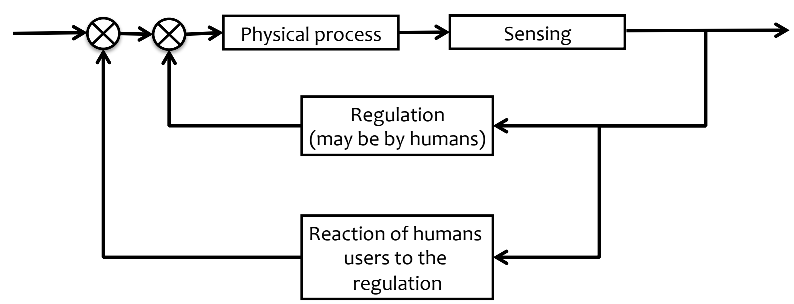
FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Talk outline

1) CPS-sensing: using the physics for network state estimation
   - Background: Mobile Millennium Connected Corridors
   - Godunov scheme based HS sensing

2) CPS-regulatory later: adjoint-based network control
   - Optimal control of flow networks
   - Vulnerability of networks to attacks

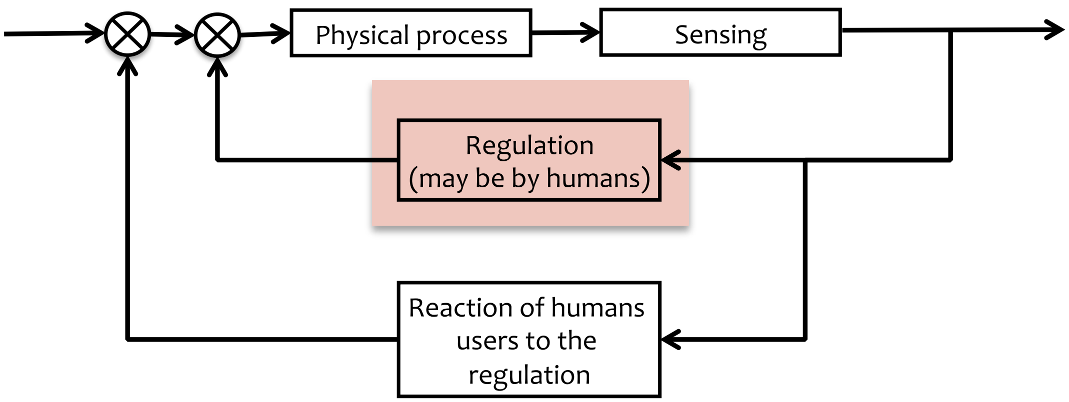
3) h-CPS: reaction of embedded humans
   - Static Nash-Stackelberg games
   - Dynamic repeated games

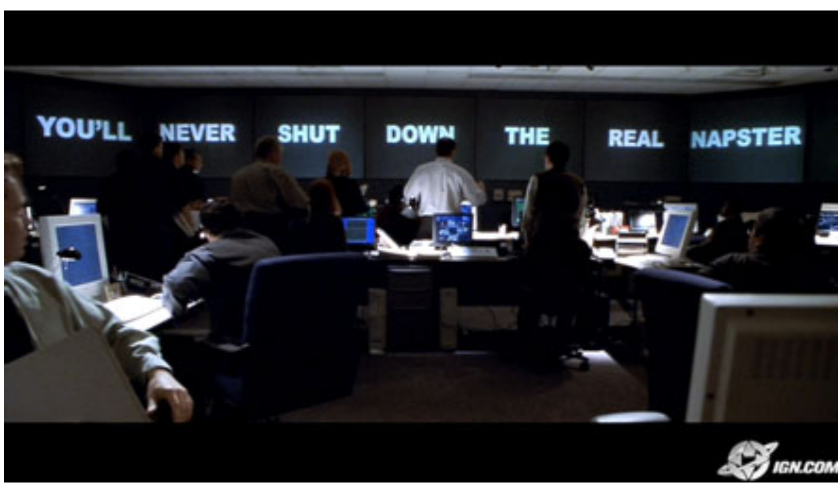


FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Roughly one attack a month on the traffic management infrastructure

The *Italian Job* (2003)



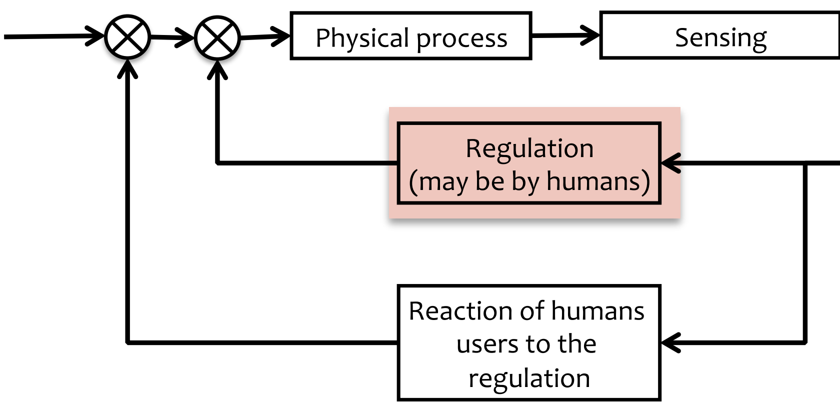


Roughly one attack a month on the traffic management infrastructure

The *Italian Job* (2003)

The "real" *Italian Job* (2007)

NC DOT signs hacked (2014)



MEMBERS: Register | Login

WWAY NewsChannel 3 abc Celebrating 50 YEARS 1964-2014

LIVE. LOCAL. INTE

SOUTHEASTERN NORTH CAROLINA'S #

Home News Weather Sports Videos Community Features Programming Abo

FBI investigating hacked NCDOT digital road signs

Submitted by WWAY on Sat, 05/31/2014 - 9:55am.

READ MORE: News New Hanover County News Crime Cybercrime FBI Hacking N.C. NCDOT Transportation

Like 17 Tweet 5 Share 6

WILMINGTON, NC (WWAY) -- The North Carolina Department of Transportation says the FBI is looking into a group that hacked into at least five digital road signs yesterday, including one in New Hanover County.

The DOT says it is also evaluation the security measures in place for its digital road signs after a group changed the intended transportation-related messages on the signs to an advertisement for its Twitter account. According to a news released, the DOT corrected the messages as soon as it discovered the hackings.

The DOT says the hacked message boards are on Carolina Beach Road in New Hanover county, I-40 and I-240 in Asheville, US 421 in Winston-Salem and I-77 near the North Carolina/Virginia state line.

riously," NCDOT Chief Information Officer David Ulmer said in

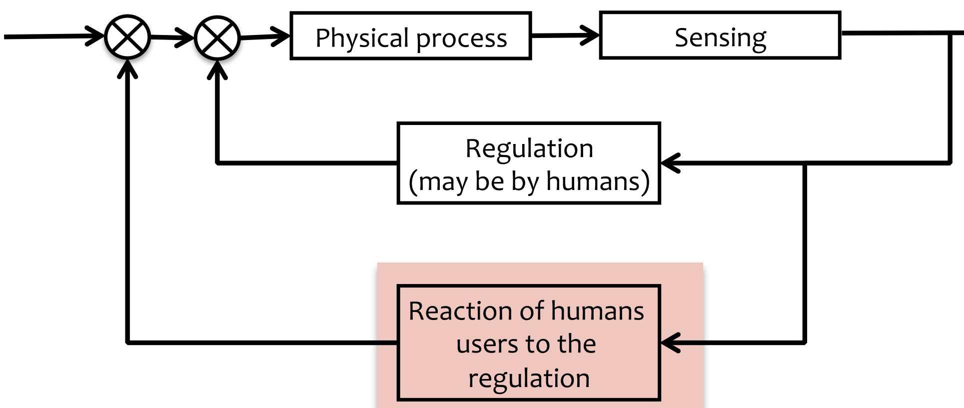
Roughly one attack a month on the traffic management infrastructure

The *Italian Job* (2003)

The "real" *Italian Job* (2007)

NC DOT signs hacked (2014)

Snail operations (2014)



ACTUALITÉS | SPORTS | MA VILLE | CULTURE & LOISIRS | VIDÉOS | PHOTOS | YOU | LA PARISIENNE

Toute l'actualité, 15 juin 2014, mis à jour à 20h47

Rechercher sur le site OK

Le Parisien

À SUIVRE La question du jour | Grève SNCF | France - Honduras | Frondeurs du PS | Irak

À LA UNE | SOCIÉTÉ | FAITS DIVERS | POLITIQUE | COUPE DU MONDE | ECONOMIE | AUTO | INTERNATIONAL

Actualité > **Transports**

Manifestation des taxis ce matin : attention aux opérations escargot !

Publié le 12.01.2014

Recommander 79 personnes recommandent ça. Soyez le premier parmi vos amis. Tweeter 56 g+1 Share

Roughly one attack a month on the traffic management infrastructure

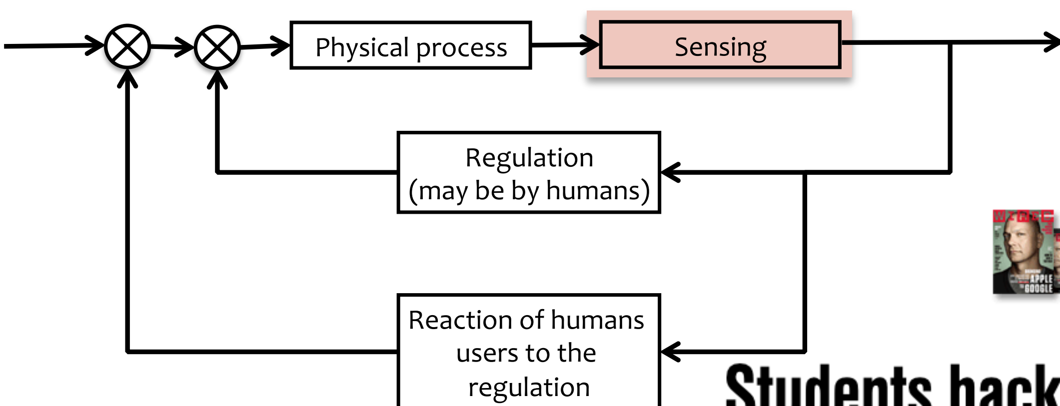
The *Italian Job* (2003)

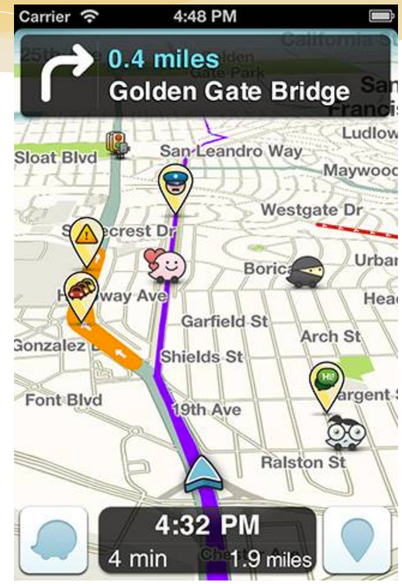
The “real” *Italian Job* (2007)

NC DOT signs hacked (2014)

Snail operations (2014)

Waze / Google hacked (2014)





Students hack Waze, send in army of traffic bots

TECHNOLOGY / 25 MARCH 14 / by NICHOLAS TUFNELL

123 Tweet | 95 Recommend | 29 g+1 | 3

Two Israeli students have successfully hacked popular

AND DIGITAL EDTIONS

Roughly one attack a month on the traffic management infrastructure

The *Italian Job* (2003)

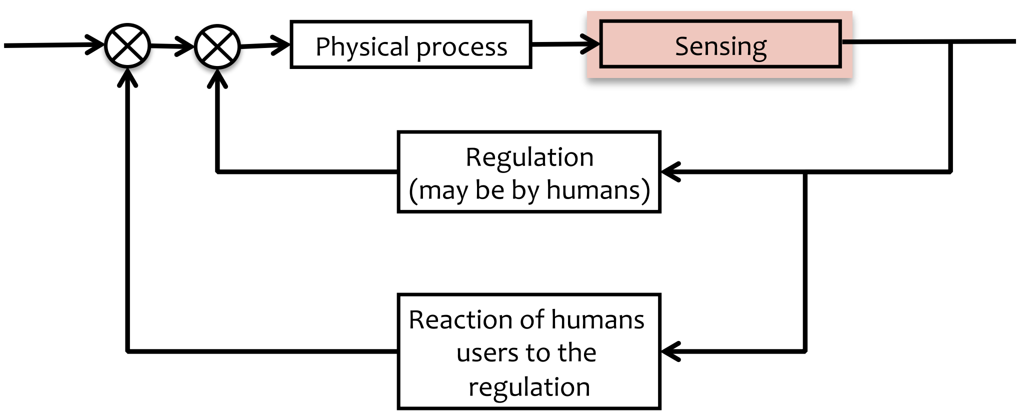
The "real" *Italian Job* (2007)

NC DOT signs hacked (2014)

Snail operations (2014)

Waze / Google hacked (2014)

Sensys Attack (2014)



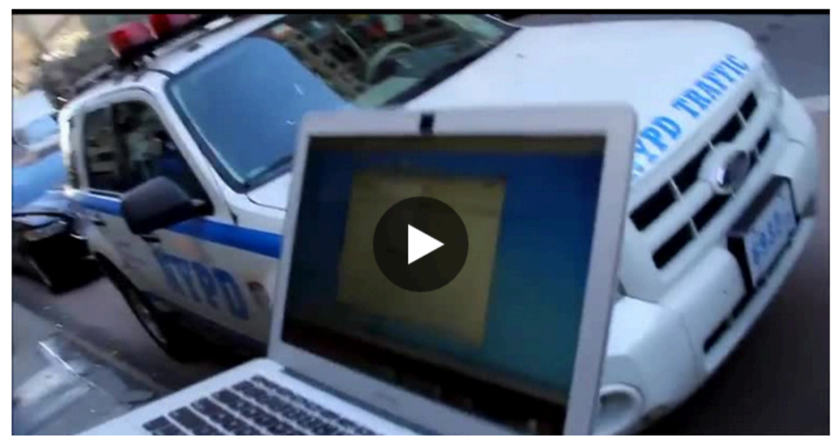

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION

THREAT LEVEL | cybersecurity | hack and cracks

Hackers Can Mess With Traffic Lights to Jam Roads and Reroute Cars

BY KIM ZETTER 04.30.14 | 6:30 AM | PERMALINK

Share 851 Tweet 883 +1 192 Share 314 Pin it



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Roughly one attack a month on the traffic management infrastructure

The *Italian Job* (2003)

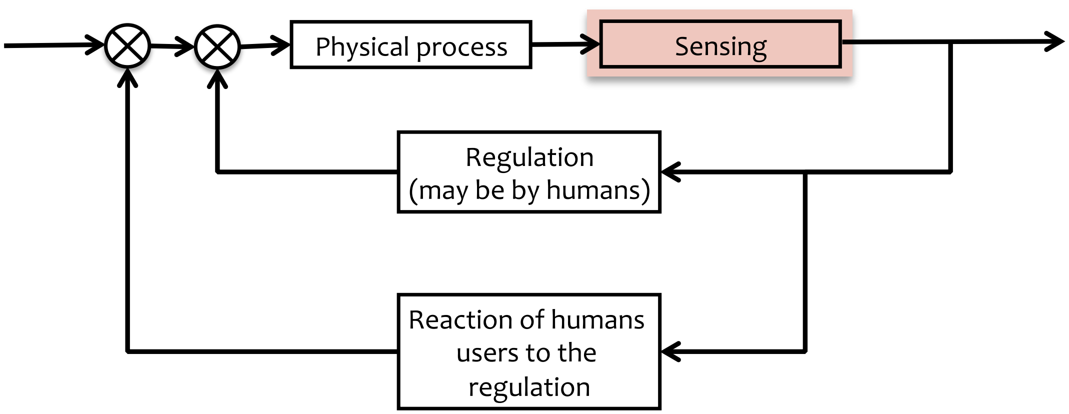
The “real” *Italian Job* (2007)

NC DOT signs hacked (2014)

Snail operations (2014)

Waze / Google hacked (2014)

Sensys Attack (2014)



Cesar Cerrudo in downtown New York City, conducting field test of vulnerable traffic sensors. Photo: Courtesy of Cesar Cerrudo

Roughly one attack a month on the traffic management infrastructure

The *Italian Job* (2003)

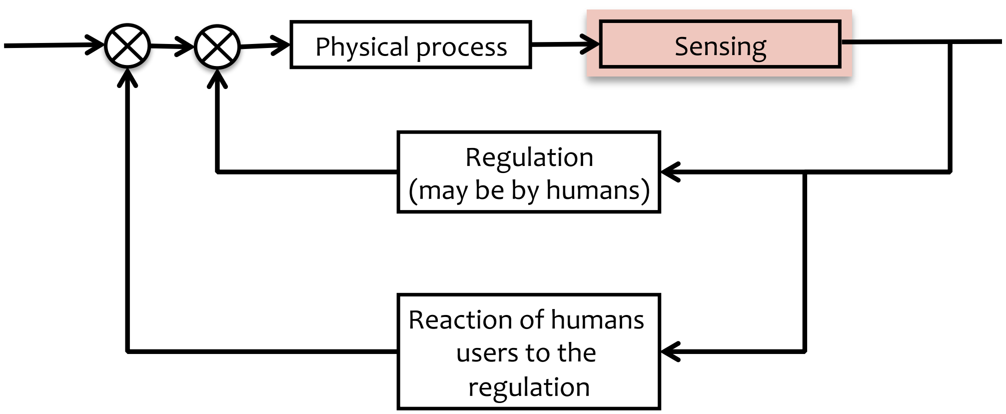
The "real" *Italian Job* (2007)

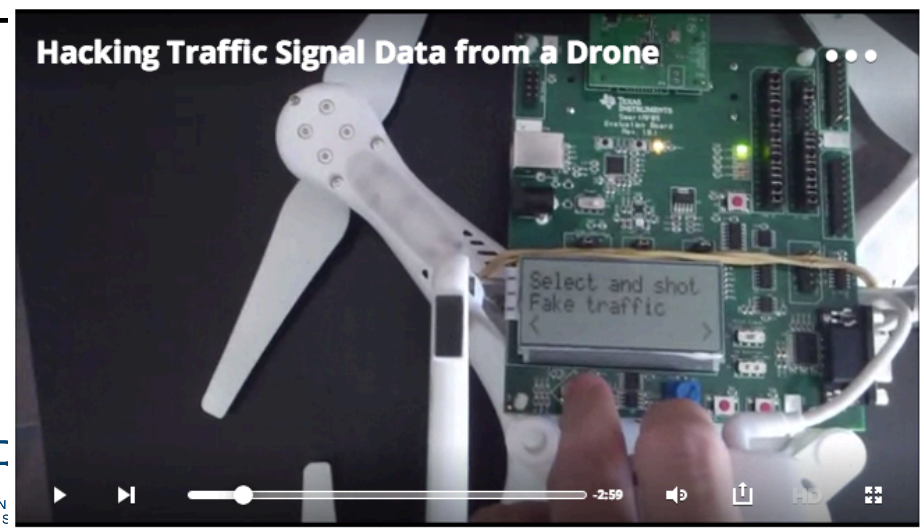
NC DOT signs hacked (2014)

Snail operations (2014)

Waze / Google hacked (2014)

Sensys Attack (2014)



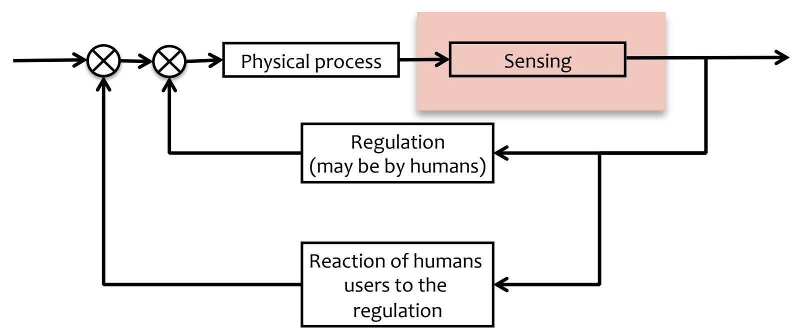


Talk outline

1) CPS-sensing: using the physics for network state estimation
   - Background: Mobile Millennium Connected Corridors
   - Godunov scheme based HS sensing

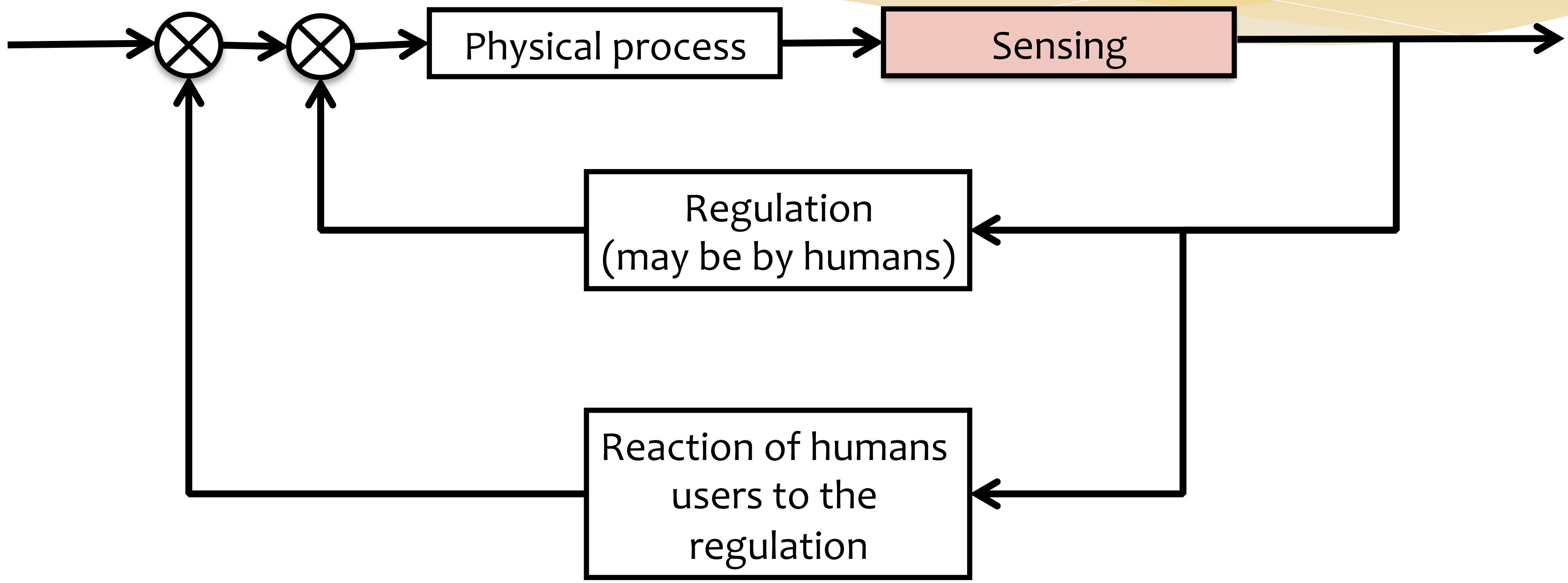
2) CPS-regulatory later: adjoint-based network control
   - Optimal control of flow networks
   - Vulnerability of networks to attacks

3) h-CPS: reaction of embedded humans
   - Static Nash-Stackelberg games
   - Dynamic repeated games



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

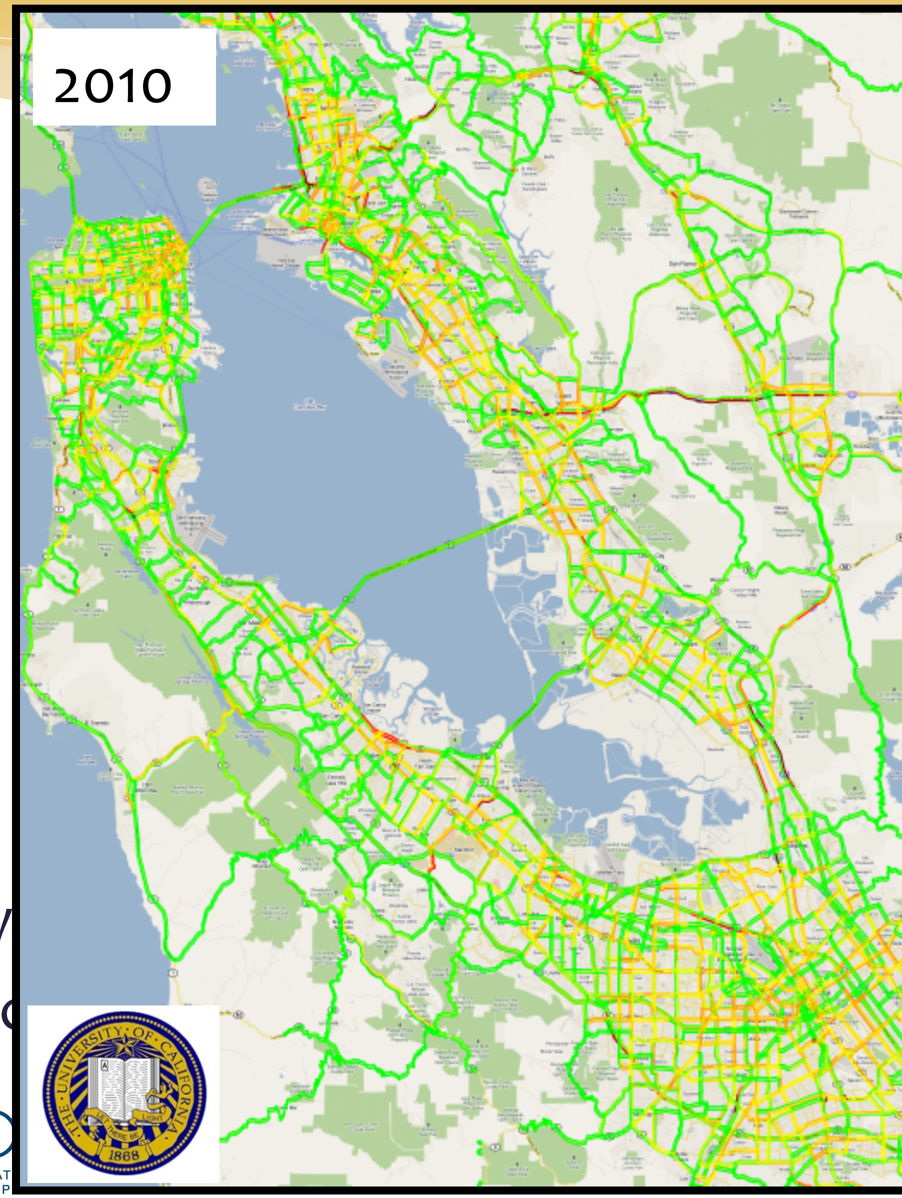
CPS sensing: using the physics for networks state estimation



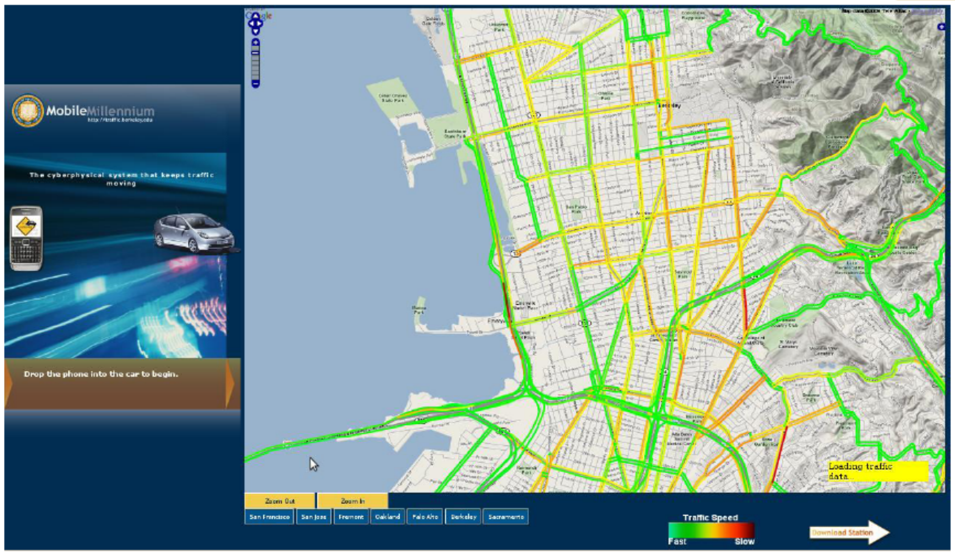
Questions:

1) Can the “physics” in the CPS system be used for estimation?
2) How can this help with resilience (attack detection)

General context: big data (data fusion)



Estimation algorithms capable of detecting spoofed data incompatible with physics

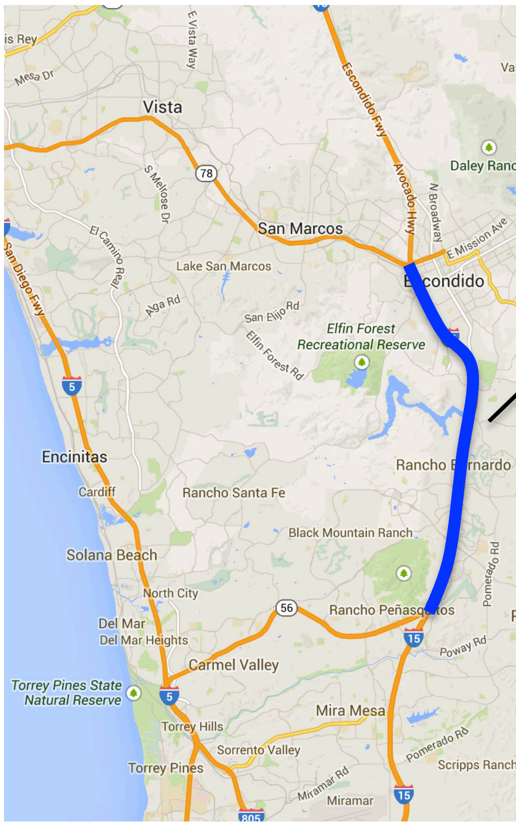


An early instantiation of participatory sensing

- Consortium: NSF, US DOT, Caltrans, Nokia, NAVTEQ, + 10 others
- Initially, 5000 downloads of the FIRST Nokia traffic app worldwide
- Today: gathers about 60 million data points / day from dozen of sources (smartphones, taxis, fleets, static sensors, public feeds)
- Provides real-time nowcast (soon forecast) of highway and arterial traffic, provide routing and data fusion tools.

Hybrid Systems decomposition of flow models for data anomaly detection

Algebraic work based on the discretization of PDEs

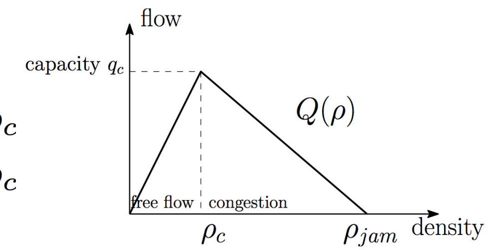


LWR PDE:

$$\frac{\partial \rho(x,t)}{\partial t} + \frac{\partial Q(\rho(x,t))}{\partial x} = 0$$

Fundamental diagram:

$$Q(\rho) = \begin{cases} v_f \rho & \text{if } \rho \leq \rho_c \\ -\omega_f\left(\rho - \rho_{\text{jam}}\right) & \text{if } \rho > \rho_c \end{cases}$$



Discretization into n cells using the Godunov scheme:

$$\rho_i^{t+1} = \rho_i^t - \frac{\Delta t}{\Delta x}\left(G(\rho_i^t, \rho_{i+1}^t) - G(\rho_{i-1}^t, \rho_i^t)\right)$$

Since Q(ρ) is piecewise affine (PWA), the Godunov scheme is PWA.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

A novel way to estimate the traffic state based on Hybrid systems

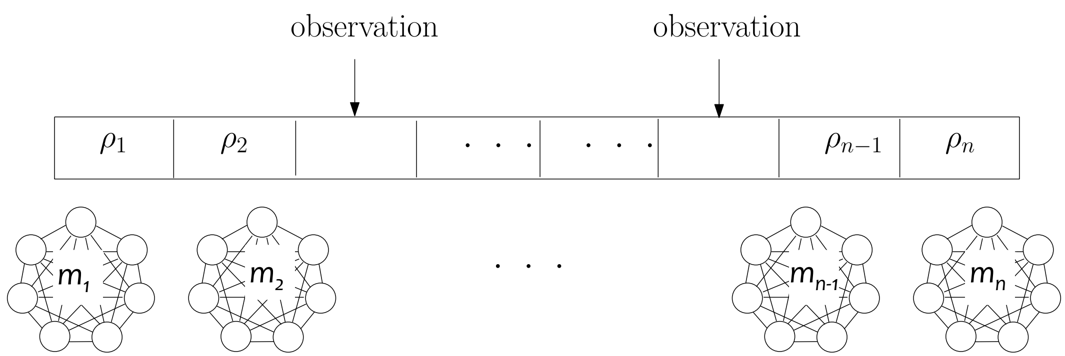
Explicit formulation as a switched linear system:

For mode vector: $\boldsymbol{m} = (m_1, \cdots, m_n)$:

$$\boldsymbol{\rho}^{t+1} = A_{\boldsymbol{m}}\boldsymbol{\rho}^t + b_{\boldsymbol{m}} + c^t \quad \text{if} \quad \boldsymbol{\rho}^t \in \mathrm{Dom}(\boldsymbol{m})$$

$$A_{\boldsymbol{m}} = \begin{pmatrix} 0 & \cdots & 0 \\ L_{m_1} & & \\ & \ddots & \\ & & L_{m_n} \\ 0 & \cdots & 0 \end{pmatrix}, \quad b_{\boldsymbol{m}} = \begin{pmatrix} 0 \\ w_{m_1} \\ \vdots \\ w_{m_n} \\ 0 \end{pmatrix}, \quad c^t = \begin{pmatrix} u^t \\ 0 \\ \vdots \\ 0 \\ d^t \end{pmatrix}$$

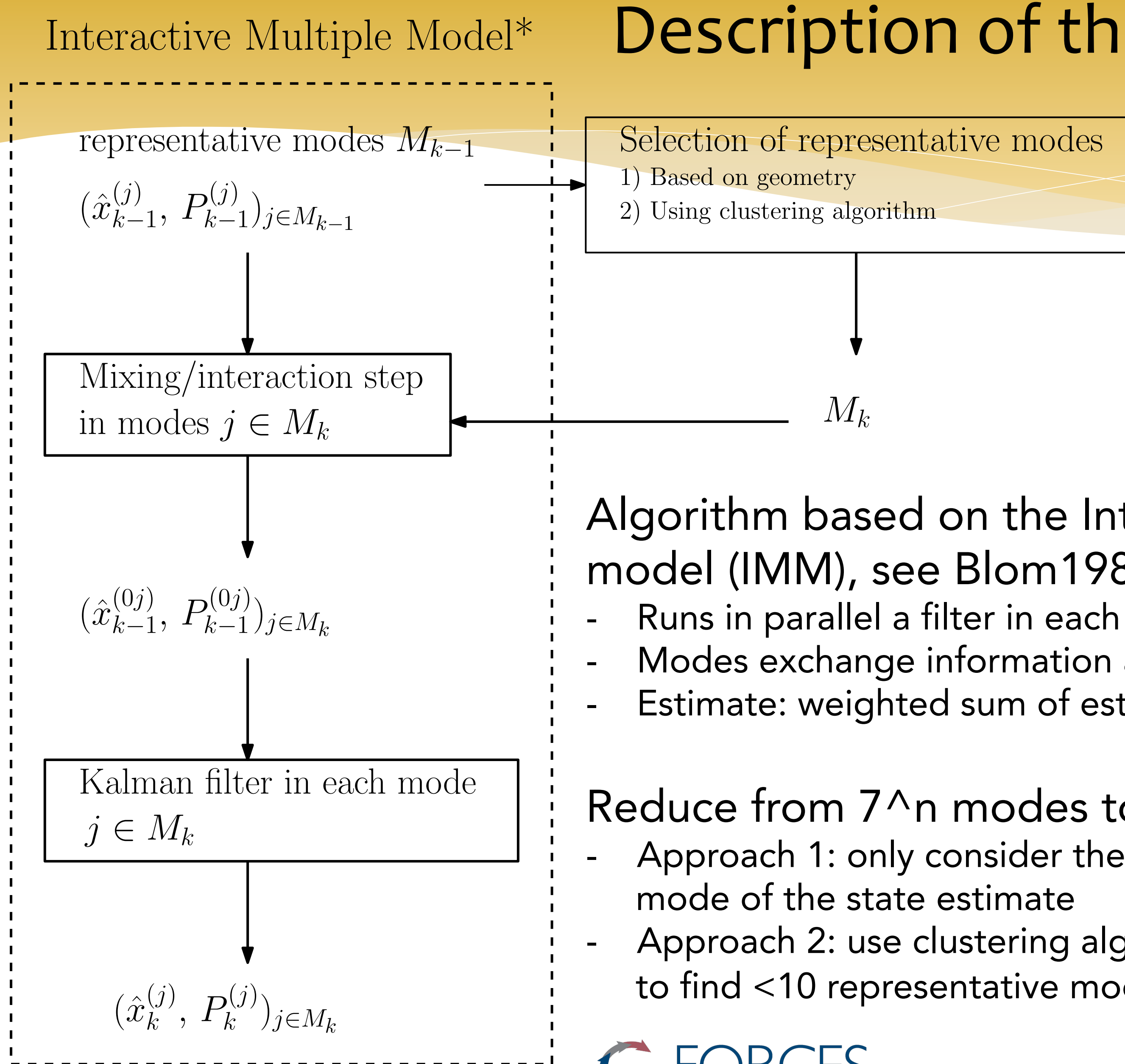
Each cell switches b/w 7 modes: ~ 7^n modes!



Design of a hybrid estimation algorithm for multicellular hybrid systems

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Description of the Algorithm



Algorithm based on the Interaction Multiple model (IMM), see Blom1988

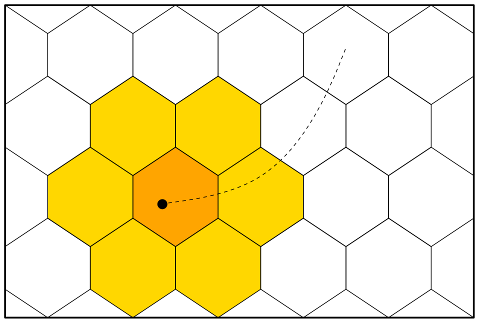
- Runs in parallel a filter in each mode at each step
- Modes exchange information at each step
- Estimate: weighted sum of estimates in each mode

Reduce from 7^n modes to <10 modes

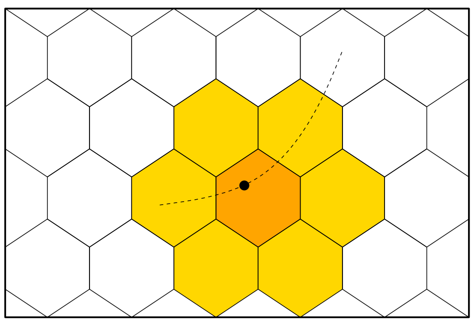
- Approach 1: only consider the modes adjacent to mode of the state estimate
- Approach 2: use clustering algorithm on historical data to find <10 representative modes

Description of the Algorithm

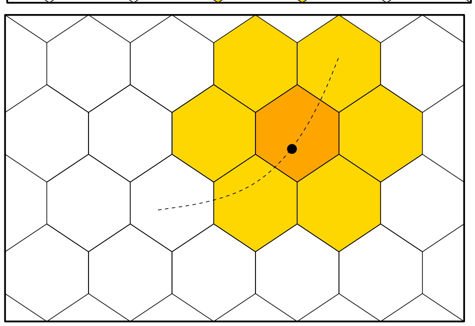
Approach 1: only consider the modes adjacent to the mode of the state estimates



The state space Is partitioned into the domains of each mode

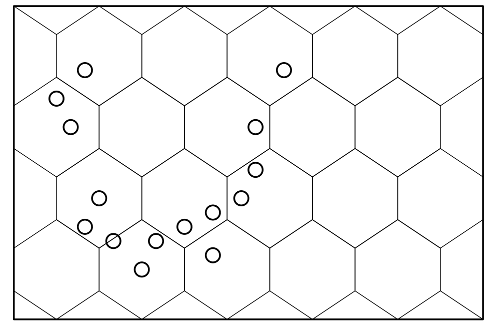


The state estimate switches between different modes (which domain Is in orange)

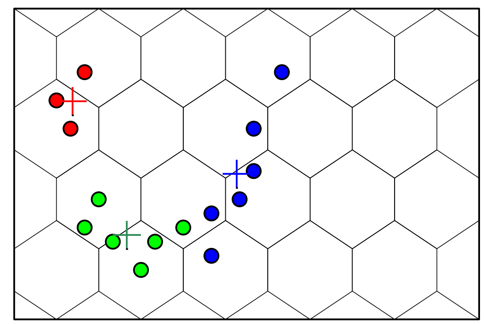


We only keep the mode of the state estimate and the adjacent modes (in yellow)

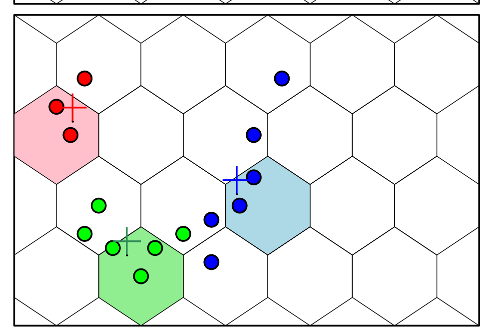
Approach 2: apply clustering algorithm to historical data



Observations (in the state space)



Obtain K clusters and their centroid



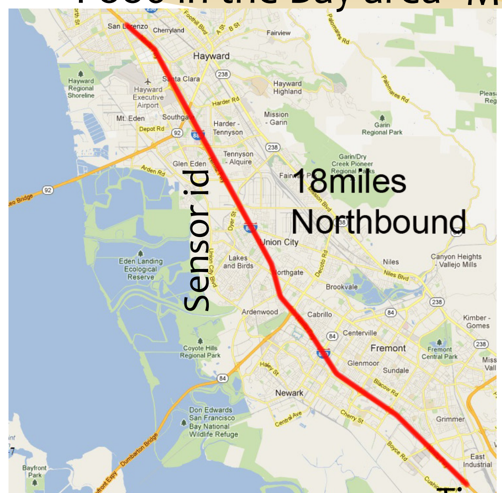
The representative modes are the modes of each centroid

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

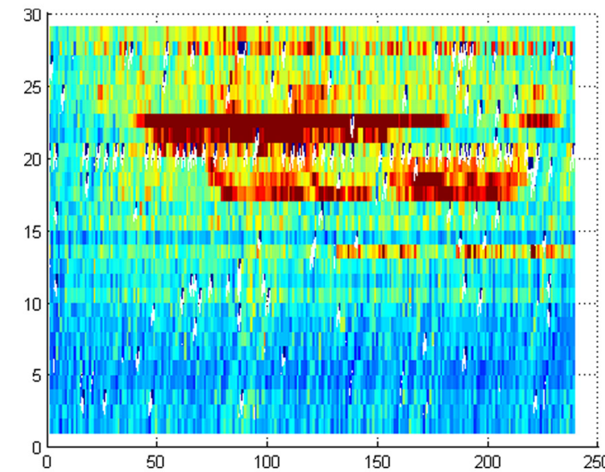
Numerical results

- Comparison between the EnKF and the IMM with reduced number of modes (R-IMM)
- They provide similar estimate
- R-IMM is much faster

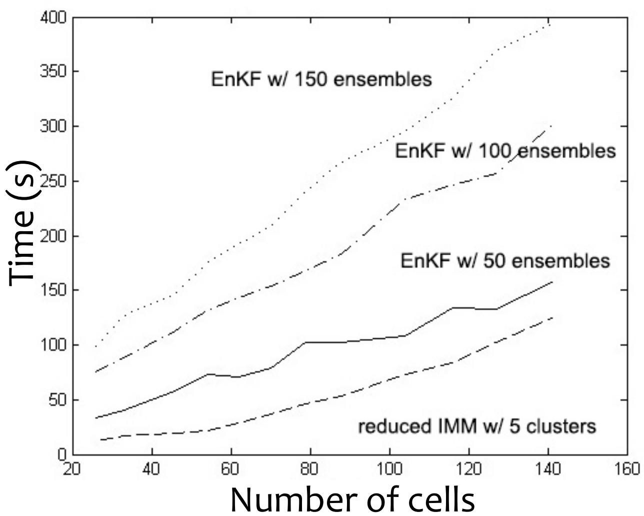
I-880 in the Bay area



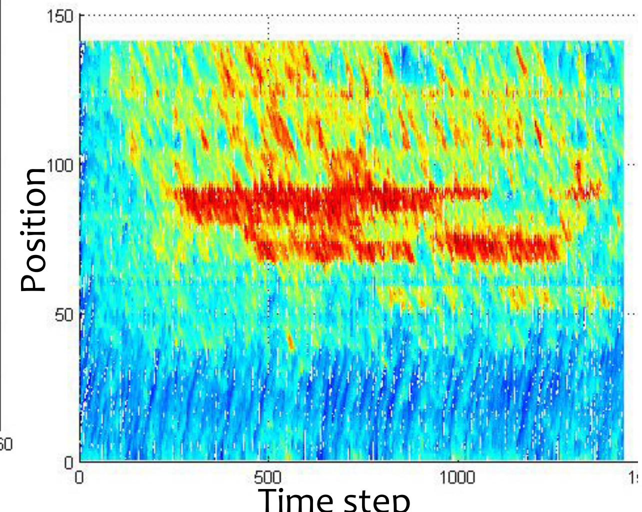
Measurements from 29 loop detectors



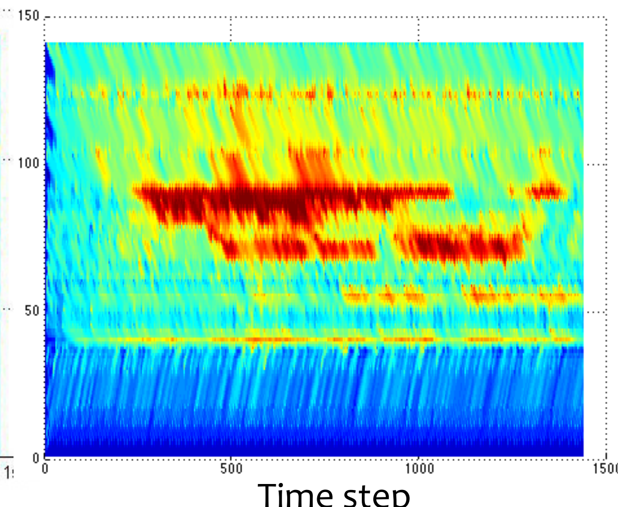
CPU times: EnKF vs. reduced-IMM



EnKF estimate



R-IMM estimate (w/ 5 clusters)

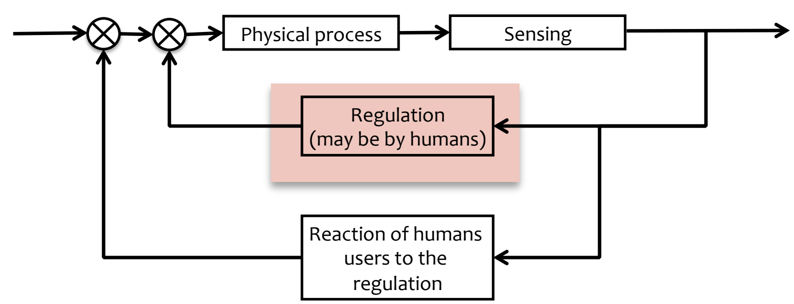


Talk outline

1) CPS-sensing: using the physics for network state estimation
   - Background: Mobile Millennium Connected Corridors
   - Godunov scheme based HS sensing

2) CPS-regulatory later: adjoint-based network control
   - Optimal control of flow networks
   - Vulnerability of networks to attacks

3) h-CPS: reaction of embedded humans
   - Static Nash-Stackelberg games
   - Dynamic repeated games

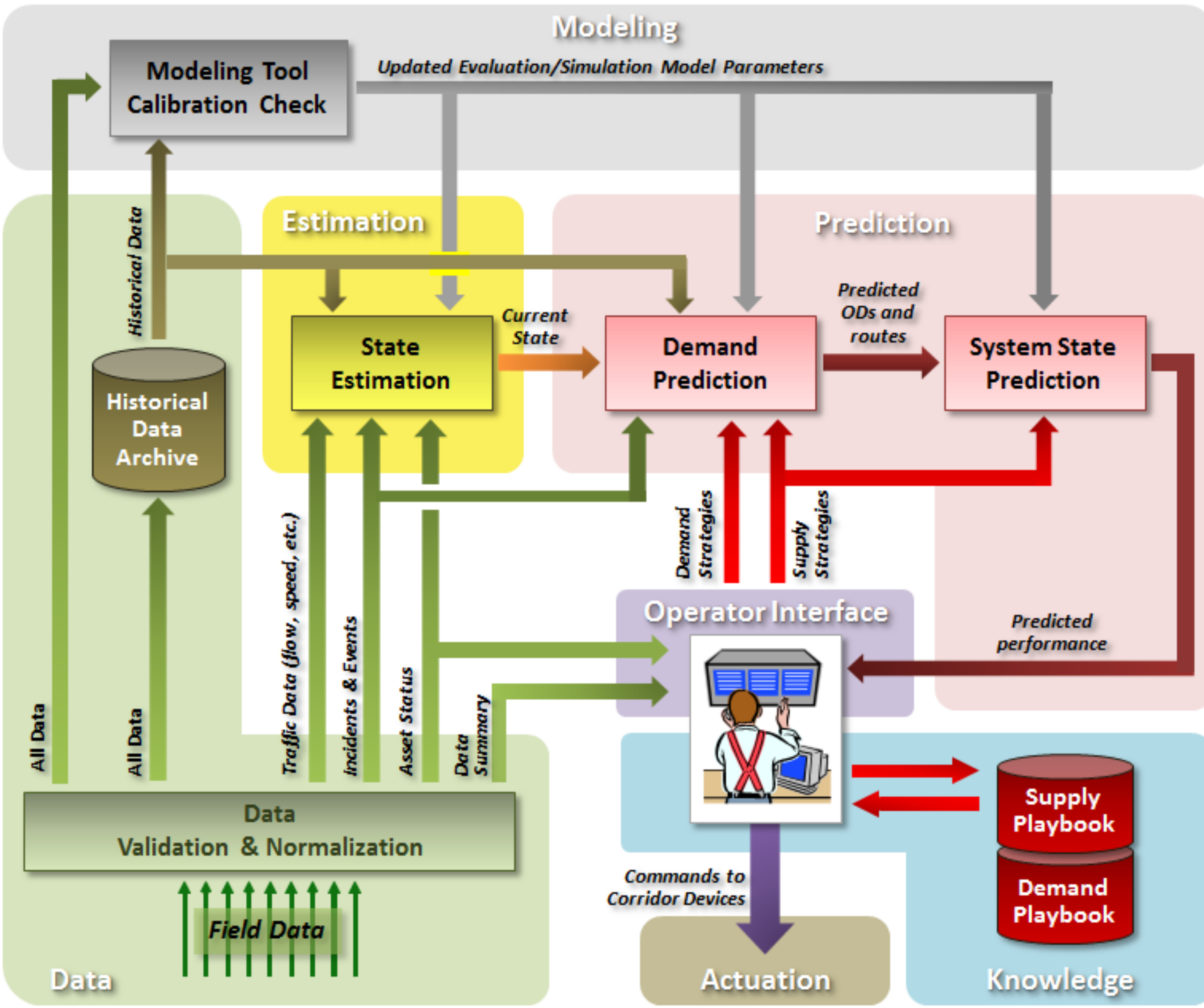


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Coordinated network control using adjoint-based optimization

- Increasing amounts of freeway **data** and **sensing** available**.**
  - Informative for real-time traffic prediction and control.
- Metering (lights) in practice:
  - Use overly-simple models.
  - No prediction.
  - Local/isolated control.
- **REAL-TIME, Coordinated, Predictive** metering schemes feasible using **Adjoint Methods** within optimal control.

Coordinated network control using adjoint-based optimization



Finite-horizon Optimal Control Problem (MPC)

$$\min_{\mathbf{u}\in U} \underbrace{\sum_{t=1}^{T-1}\sum_{i=1}^{N} f\left(u_{i,t},\rho_{i,t}\right)}_{\text{Running Cost}} + \underbrace{\sum_{i=1}^{N} f_T\left(u_{i,T},\rho_{i,T}\right)}_{\text{Terminal Cost}}$$

subject to system dynamics:

$$\rho_{i,0} = \rho_i^0$$

$$\rho_{i,t+1} = \rho_{i,t} + \frac{\Delta t}{\Delta x}\left(G\left(\rho_{i-1,t},\rho_{i-1,t},u_{i,t}\right) - G\left(\rho_{i,t},\rho_{i+1,t},u_{i,t}\right)\right)$$

$$\forall i \in [1,N], \forall t \in [1,T]$$

$$\min_{\mathbf{u}\in U} J\left(\mathbf{u},\rho\right)$$

$$\text{s.t.} \quad H\left(\mathbf{u},\rho\right) = 0$$

* Non-linear
* Non-smooth
* Non-convex

* Performing gradient descent w/ finite-differences **infeasible for large networks!**

Adjoint Formulation

$$\min_{\mathbf{u}\in U} J(\mathbf{u},\rho)$$
$$\text{s.t.} \quad H(\mathbf{u},\rho) = 0$$

Compute gradient: $\nabla_{\mathbf{u}} J = \frac{\partial J}{\partial \mathbf{u}} + \frac{\partial J}{\partial \rho}\frac{d\rho}{d\mathbf{u}}$

Easy

Hard

Eliminate $\frac{d\rho}{d\mathbf{u}}$ using system dynamics: $\nabla_{\mathbf{u}} H = \frac{\partial H}{\partial \mathbf{u}} + \frac{\partial H}{\partial \rho}\frac{d\rho}{d\mathbf{u}} = 0$

$$\nabla_{\mathbf{u}} J =$$
$$J_u + J_\rho \rho_u + \lambda^T \left[H_\rho + H_u\right] =$$
$$\left(J_\rho + \lambda^T H_\rho\right)\rho_u + \left(J_u + \lambda^T H_u\right)$$

⟺

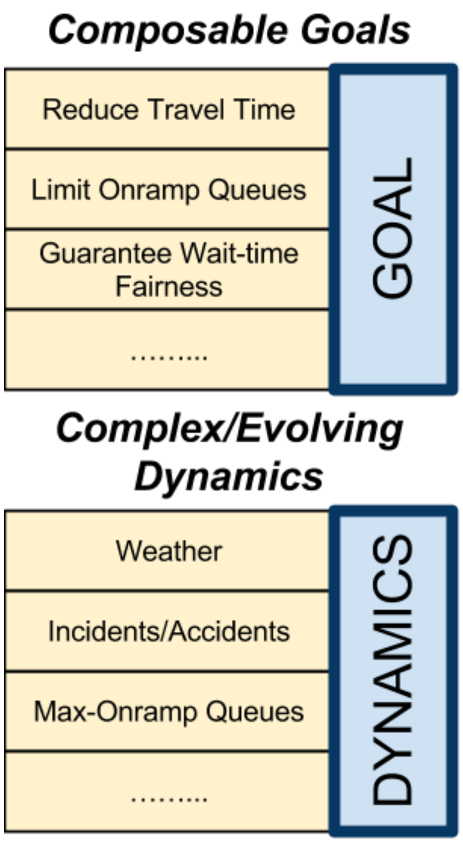
$$\nabla_{\mathbf{u}} J =$$
$$J_u + \lambda^T H_u$$
$$\text{s.t.} \quad H_\rho^T \lambda = -H_u^T$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Finding Optimal Control Policy

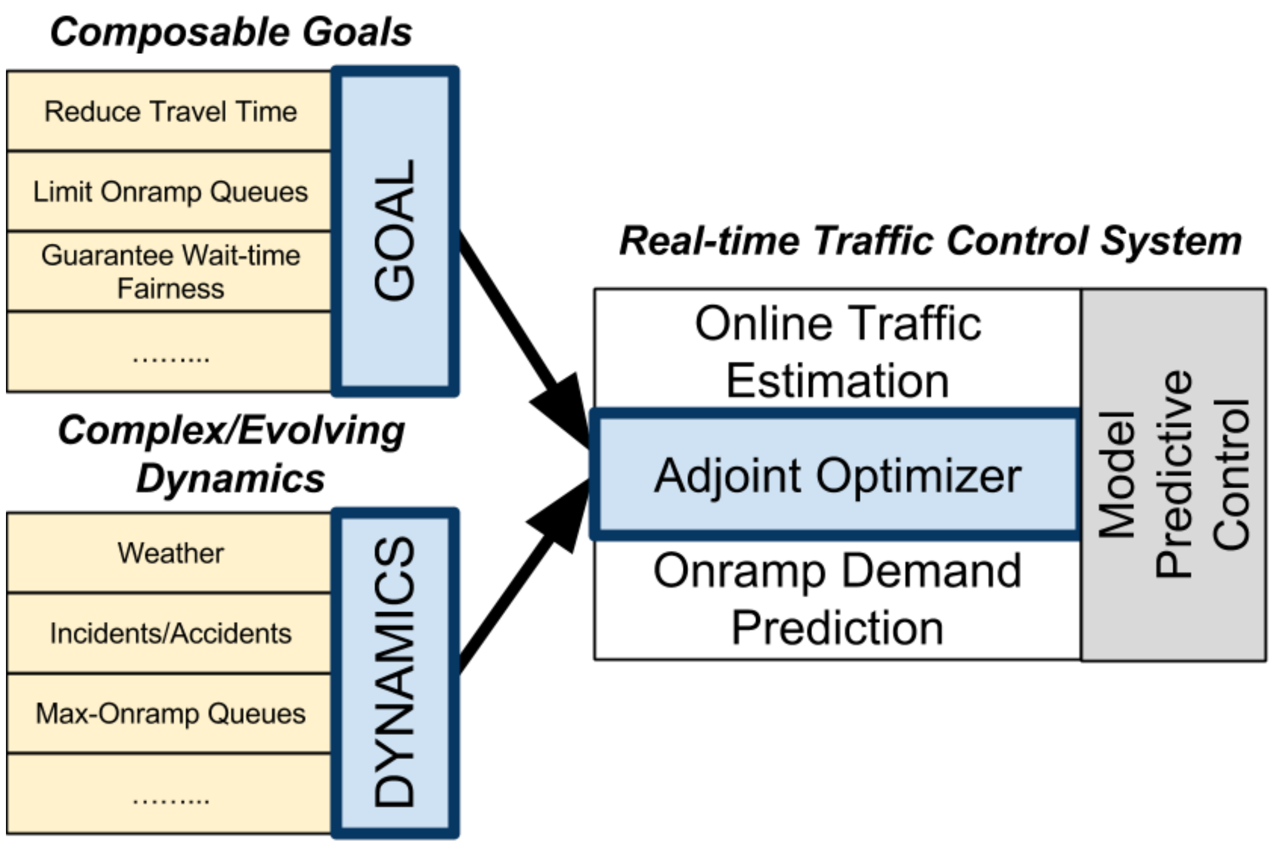
- First-order gradient methods.
  - Given u^0, find gradient $\nabla_u J(u^0, x(u^0))$
  - Take step in direction of gradient:
- **Finite-differences infeasible** for **large** physical systems in practice, e.g. freeway networks.
- **Adjoint Method:** Exploiting knowledge of system dynamics in gradient computation: $u^{i+1} = u^i - \alpha \nabla_u J(u^0, x(u^0))$
- Tractable for sparse networks.
  - **Linear** computation time in:
    - **Size of network**
    - **Time horizon**

Coordinated Freeway Control using **Adjoint** Methods



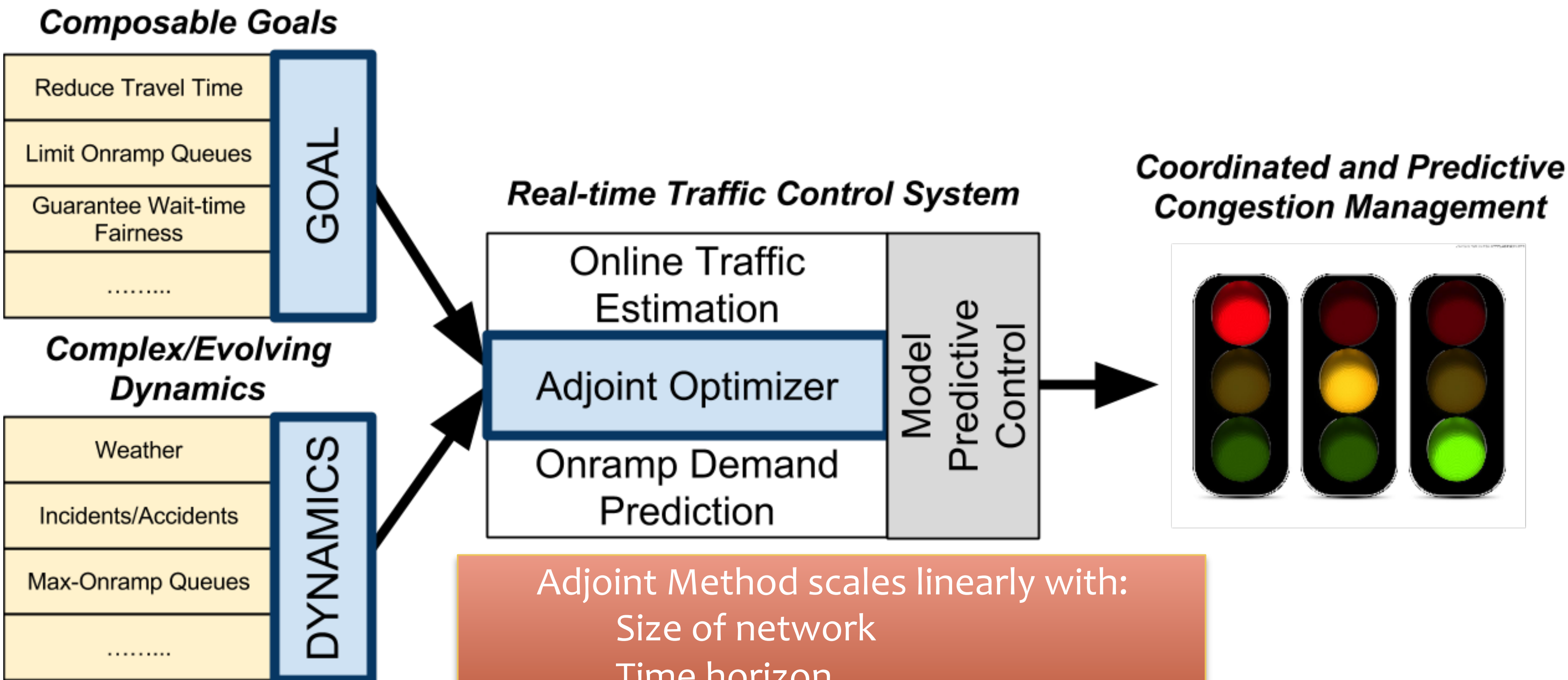
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Coordinated Freeway Control using **Adjoint** Methods



FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Coordinated Freeway Control using **Adjoint** Methods

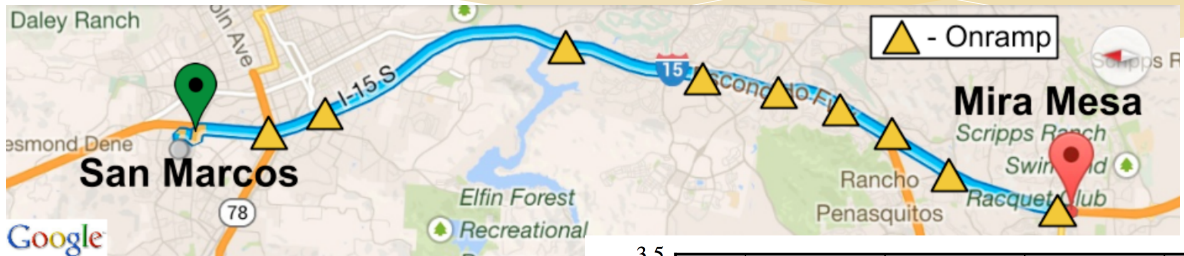


Adjoint Method scales linearly with:
Size of network
Time horizon

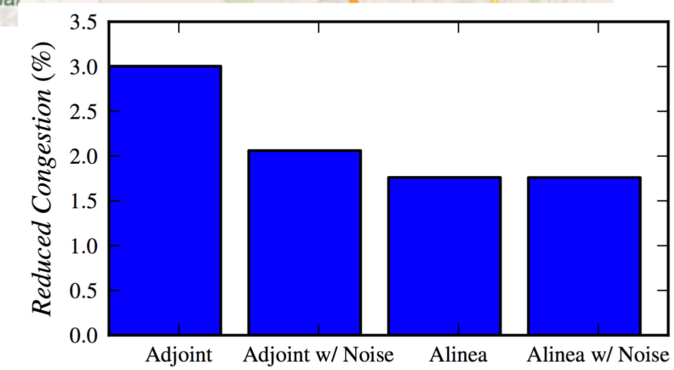
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

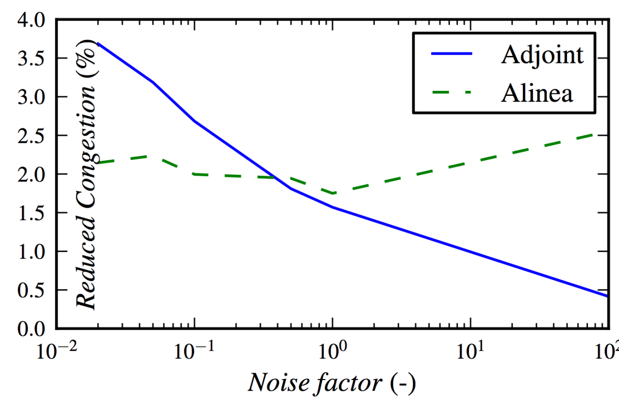
Adjoint Control on I15 Freeway Simulation

* San Diego I15 Freeway Simulation.



* Overall **reduction** of total travel time over existing feedback-based methods.
* **Robustness** to sensor/prediction noise and model errors.



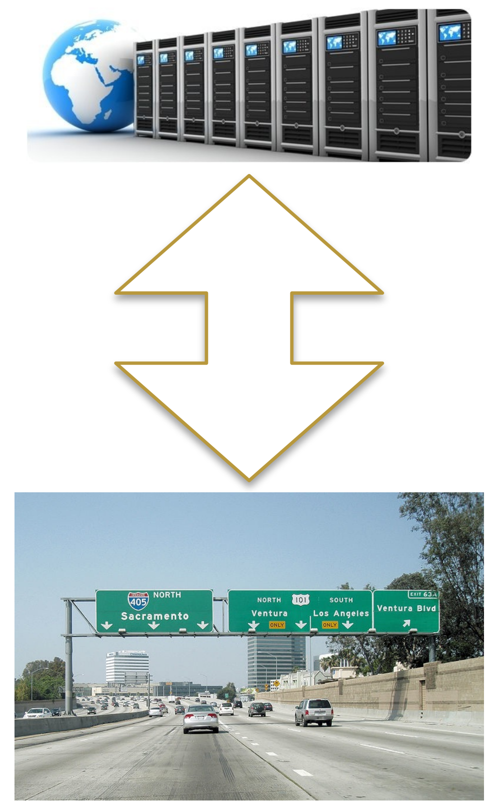


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

I15 MPC Demonstration on Micro-Simulator

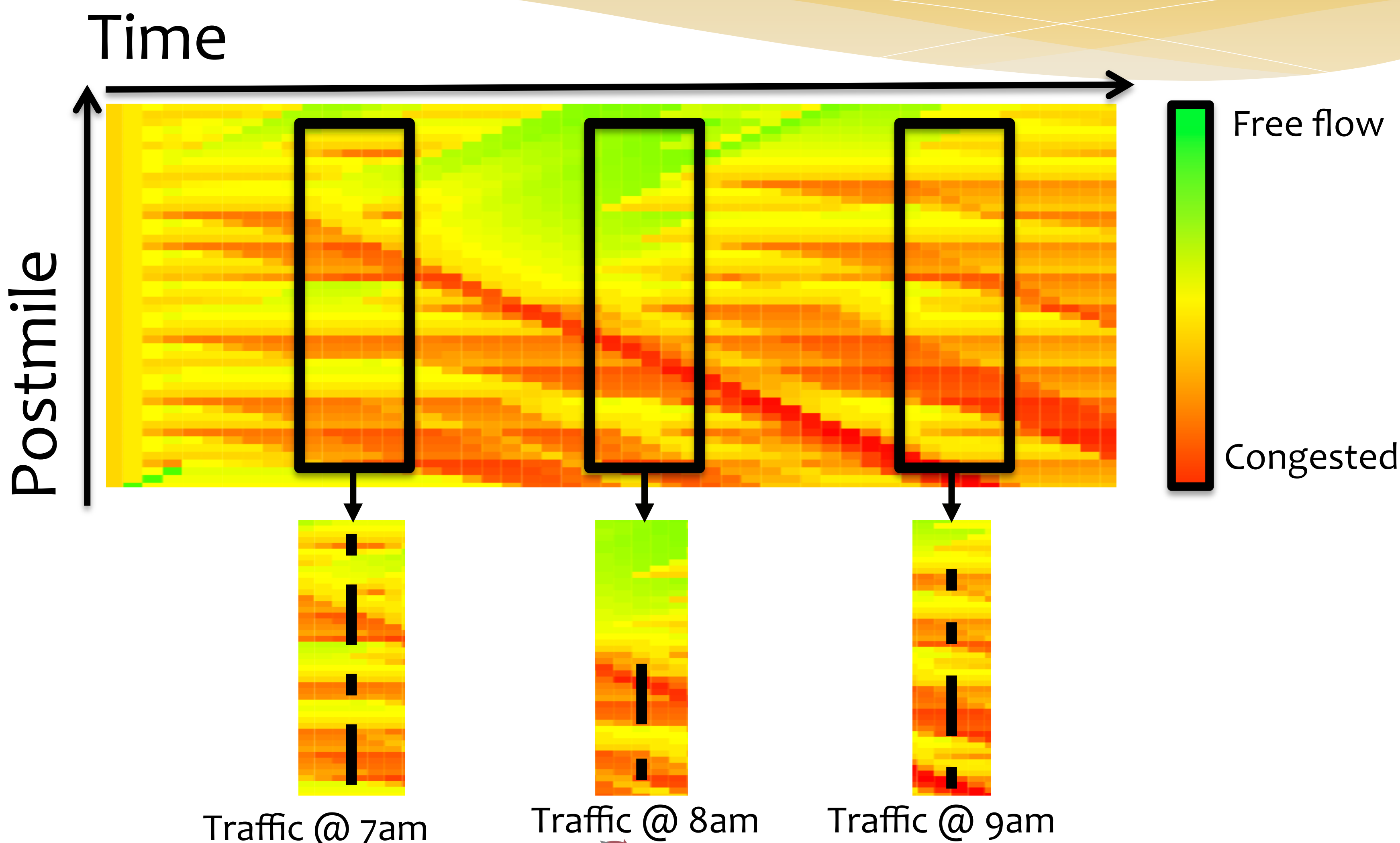
SmartRoads: Cyber-physical Security on Traffic Networks

- Traffic management has two components:
  - **Physical** sensors and traffic lights
  - **Virtual** control and estimation algorithms
- **Compromise** of cyber traffic systems has been demonstrated in the field
- Potential attack vectors numerous:
  - Broadcasting fake accident reports
  - Compromise of **metering light network.**
- **Resiliency to attack** through fault detection and modeling/sensing discrepancies.



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

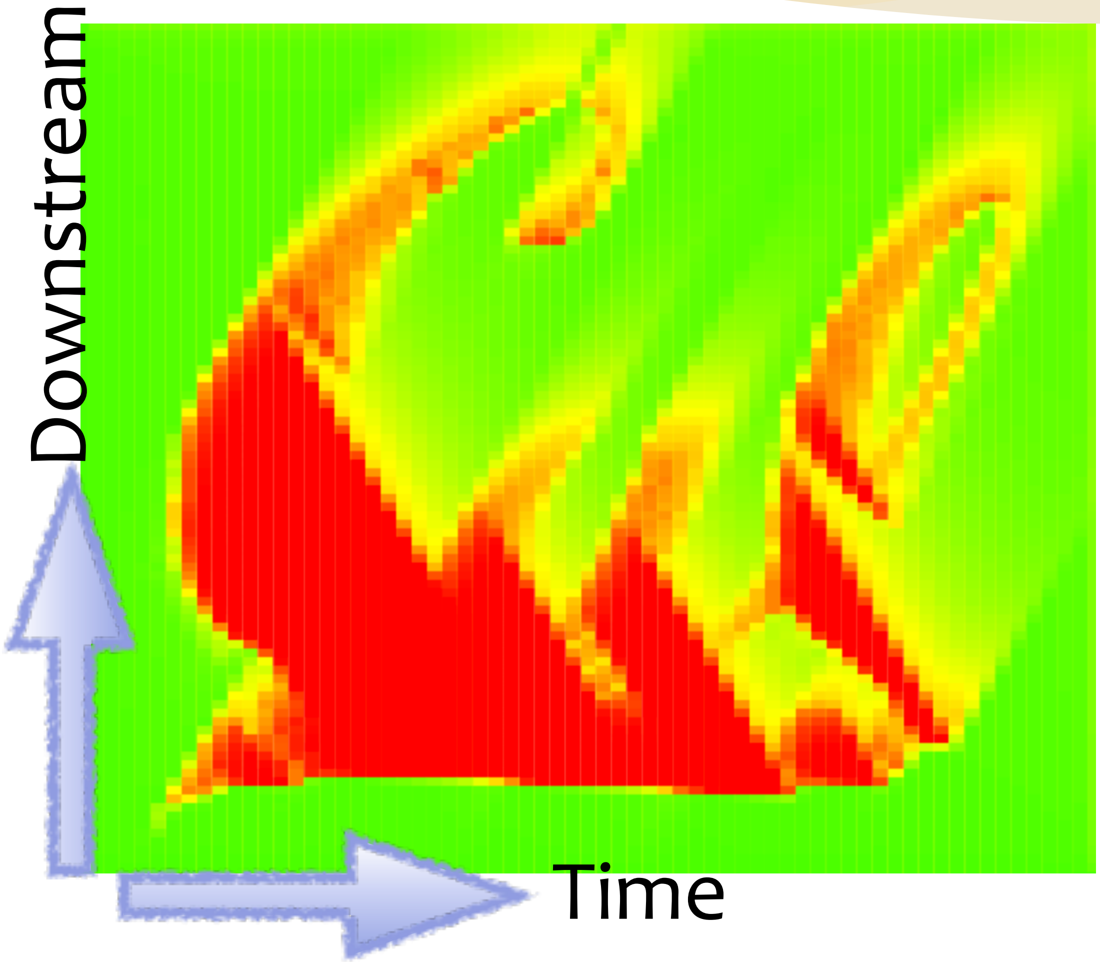
Precise Freeway [control/attack] exploiting adjoint metering control



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Morse Code Attack on the Freeway

Cal Bears Hacking Lights in Palo Alto…

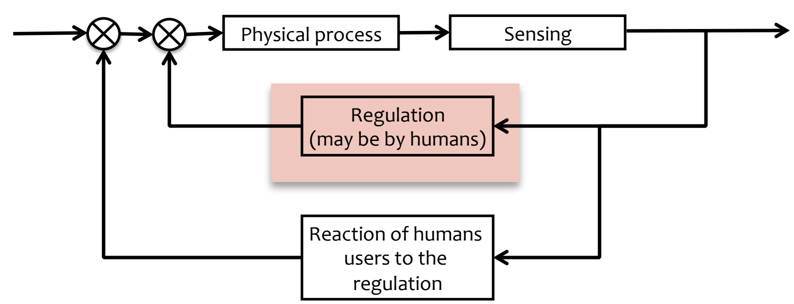


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Talk outline

1) CPS-sensing: using the physics for network state estimation
   - Background: Mobile Millennium Connected Corridors
   - Godunov scheme based HS sensing

2) CPS-regulatory later: adjoint-based network control
   - Optimal control of flow networks
   - Vulnerability of networks to attacks

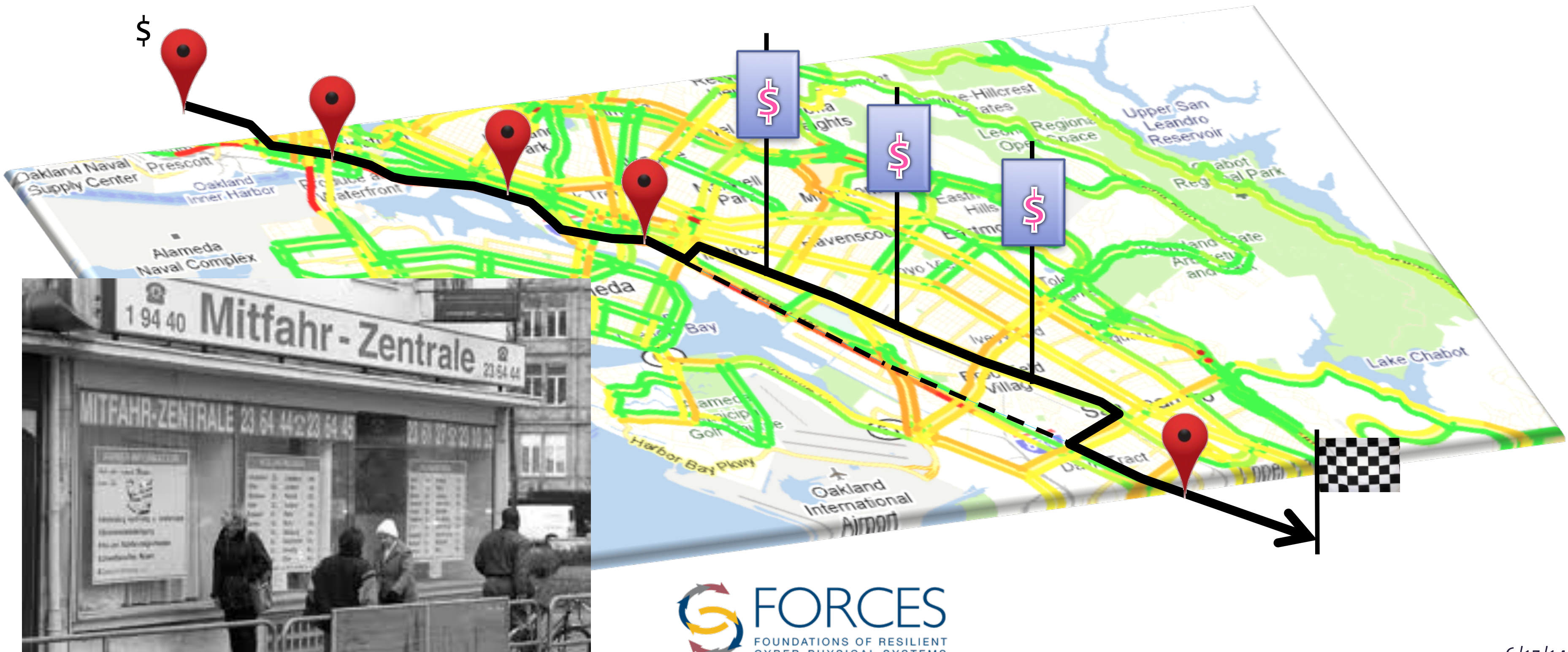


3) h-CPS: reaction of embedded humans
   - Static Nash-Stackelberg games
   - Dynamic repeated games

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Routing games

What happens is one subset of the population changes its behavior (for the good or for the bad), when everybody else in the system is proceeding normally?



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Routing games

Motivation:

- Model route choices of drivers (or routers in a communication network).
- Design routing which is aware of strategic response of selfish drivers.
- One-shot game.
    - Quantify efficiency of network.
    - Design incentives.
- Online-learning framework.
    - Model strategy dynamics.

Routing games

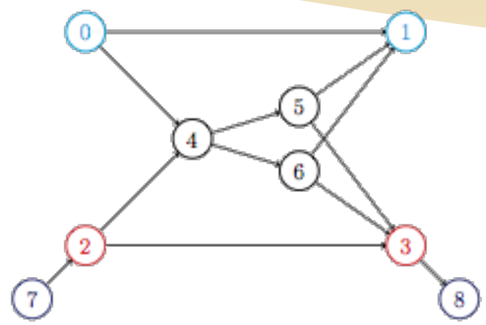


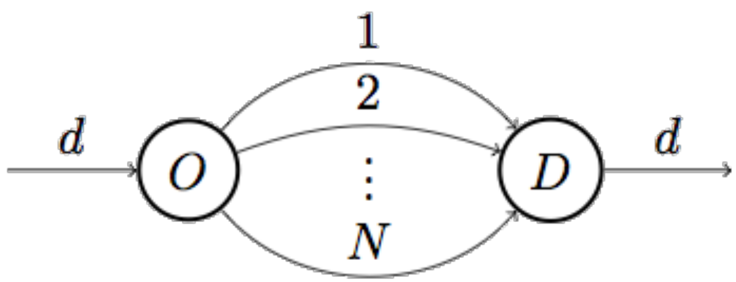
Figure : Example network

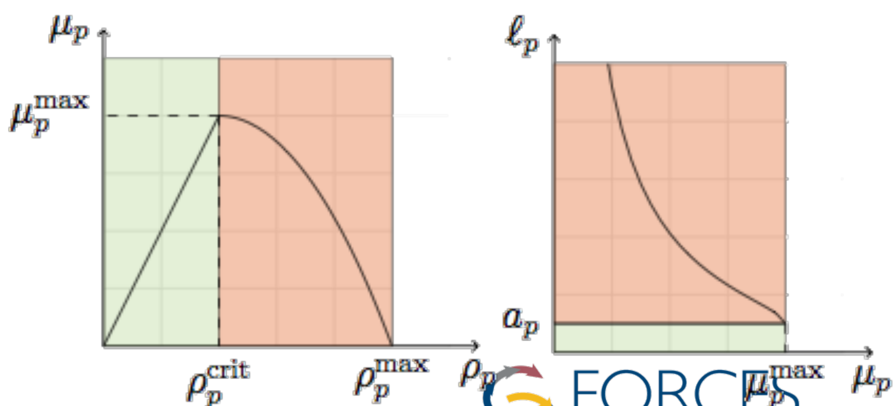
- Graph (V, E)
- Source-sink pairs, (s_k, t_k): paths $\mathcal{P}_k$
- Players choose a distribution over paths π
- Population distribution $\mu^k \in \Delta^{\mathcal{P}_k}$, $\mu^k = \int_{\mathcal{X}_k} \pi(x) dm(x)$
- μ determines edge loads $\phi = M\mu$ (linear function)
- Congestion on edge e: $c_e : \phi_e \mapsto c_e(\phi_e)$, increasing
- Players want to minimize personal latency $\ell_p^k(\mu) = \sum_{e \in p} c_e(\phi_e)$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Stackelberg routing with horizontal queues

- Parallel network, N edges (paths)
- Cost of path p: latency $\ell_p(\mu_p, m_p)$. Depends on
  - total flow μ_p on link p
  - congestion state $m_p \in \{0, 1\}$





FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Characterization of Nash equilibria

Nash equilibrium

(μ, m) is a Nash equilibrium if

$$p \in \text{supp}(\mu) \Rightarrow \forall p',\ \ell_p(\mu_p, m_p) \leq \ell_p(\mu_{p'}, m_{p'})$$

- can be computed in $O(N^2)$ time

Example:

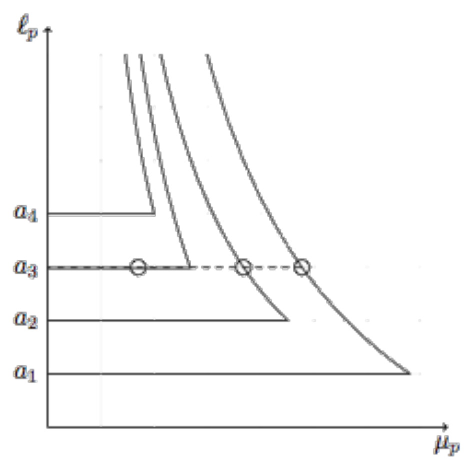


Figure : Nash equilibrium with support $\{1, 2, 3\}$

Non-compliant First strategy

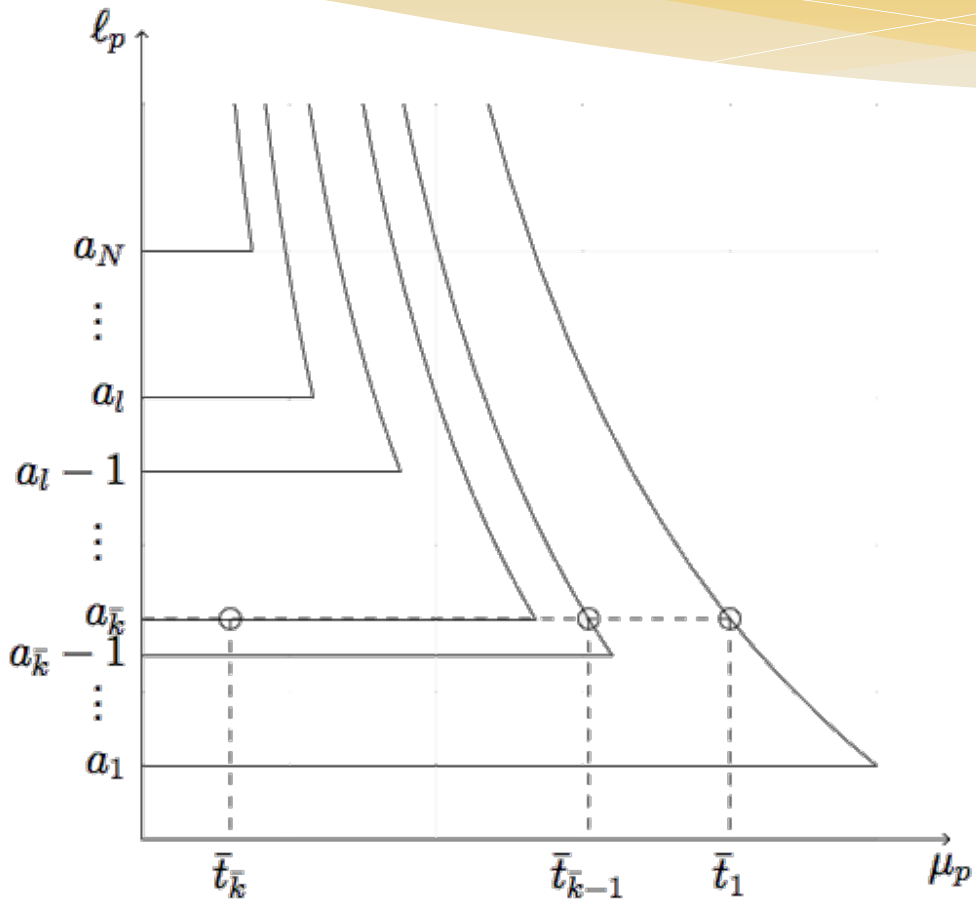


Figure : Non-compliant first strategy $\bar{s}$

Non-compliant First strategy

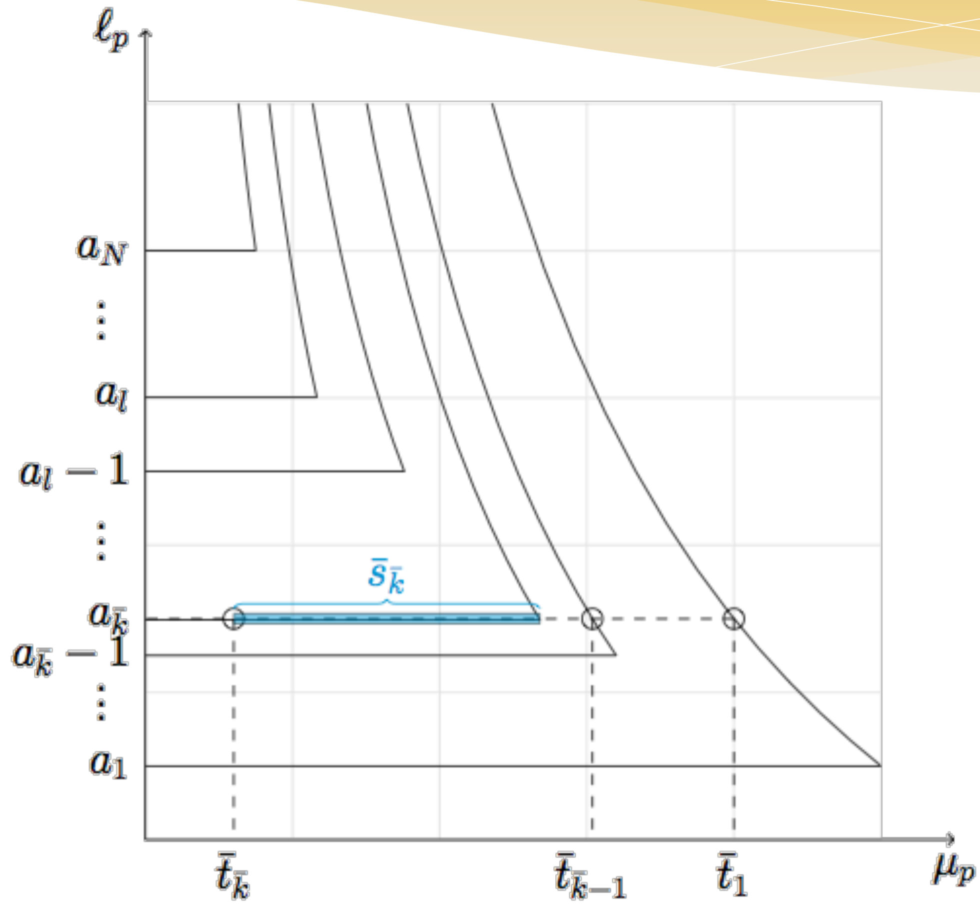


Figure : Non-compliant first strategy $\bar{s}$

Non-compliant First strategy

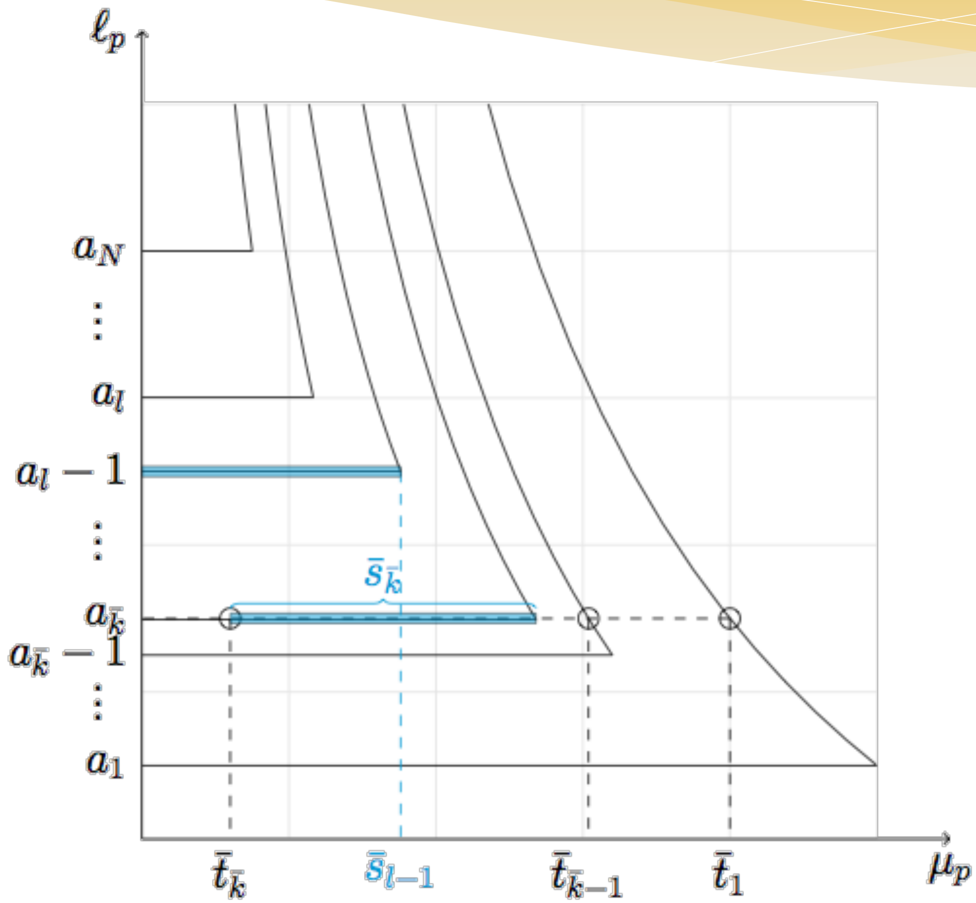


Figure : Non-compliant first strategy $\bar{s}$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Non-compliant First strategy

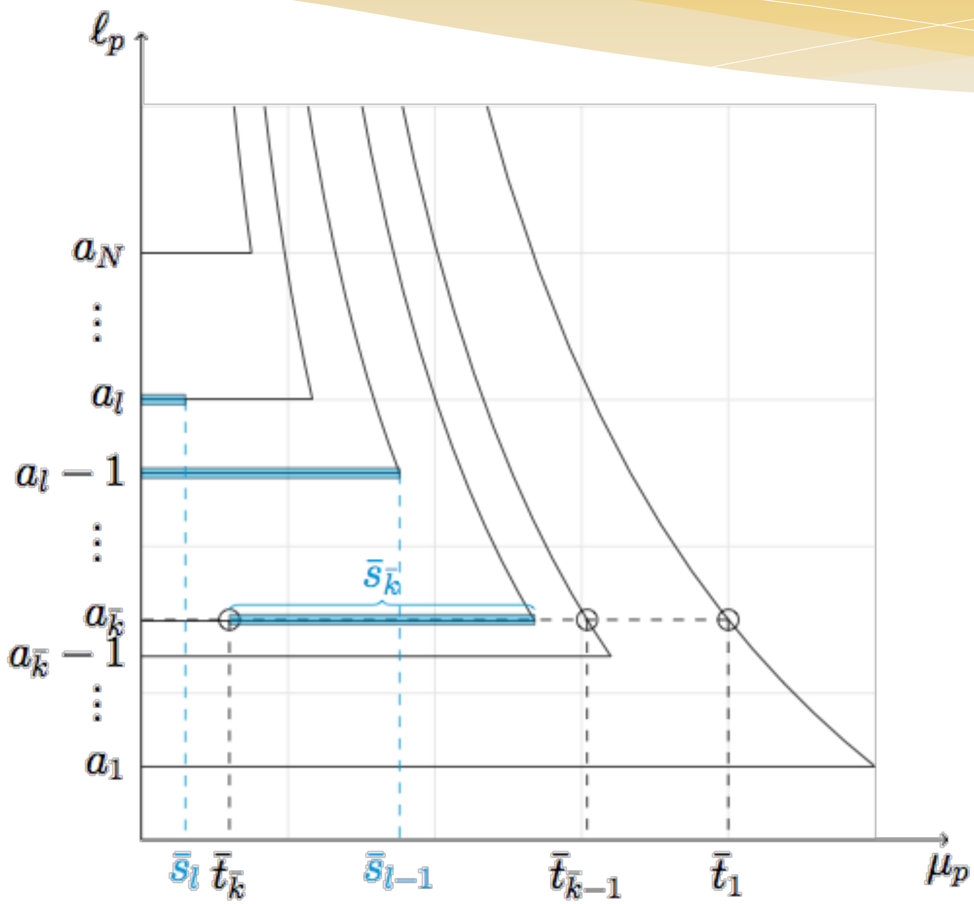


Figure : Non-compliant first strategy $\bar{s}$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Non-compliant First strategy

- Can be computed in P time

Theorem

The NCF strategy $\bar{s}$ is optimal.

Krichene et. al (2013).

Price of stability

Definition: Price of stability

$$\text{POS}(d, \alpha) = \frac{C(\text{Stack}(d, \alpha))}{C(\text{SO}(d))}$$

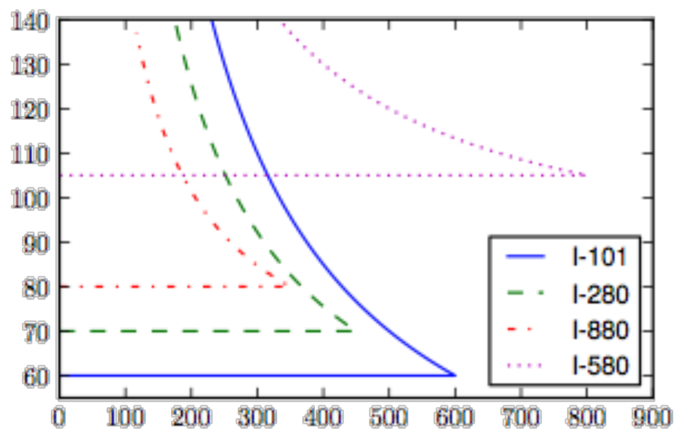


Figure : Latency functions on an example highway network.

Price of stability

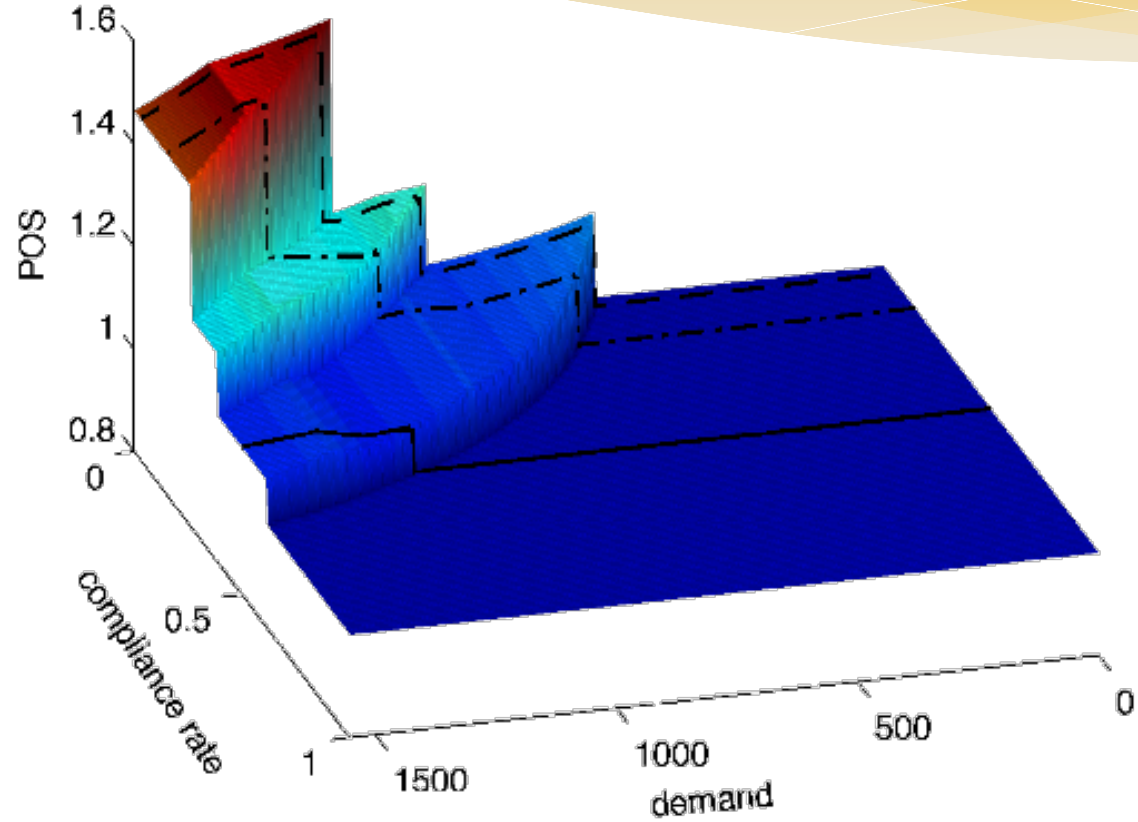


Figure : Price of stability as a function of compliance rate α and demand r. Iso-α lines are plotted for $\alpha = 0.03$ (dashed), $\alpha = 0.15$ (dot-dashed), and $\alpha = 0.5$ (solid).

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Stackelberg routing: summary

Summary

- Introduced new class of latency functions for traffic networks
- Showed NCF is optimal. Can compute it in P time.
- Necessary and sufficient conditions for optimality

Can use this analysis

- Predict performance of network under different loads.
- To guide incentive design (what fraction of population we need to incentivize).

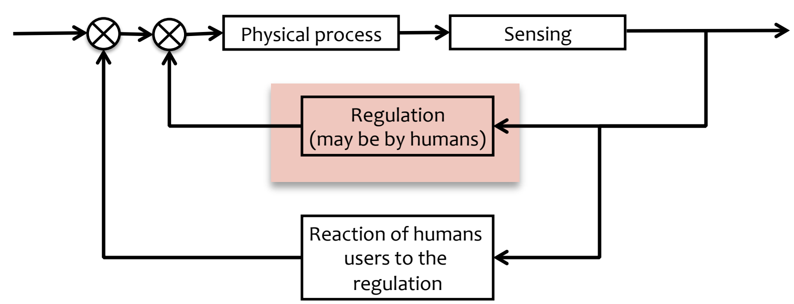
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Talk outline

1) CPS-sensing: using the physics for network state estimation
   - Background: Mobile Millennium Connected Corridors
   - Godunov scheme based HS sensing

2) CPS-regulatory later: adjoint-based network control
   - Optimal control of flow networks
   - Vulnerability of networks to attacks

3) h-CPS: reaction of embedded humans
   - Static Nash-Stackelberg games
   - Dynamic repeated games



FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

An online learning model

A learning model for routing

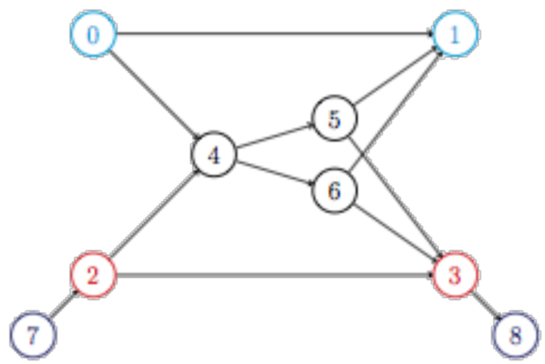


Figure : Example network

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

How to compute Nash equilibria

Nash equilibrium

μ is a Nash equilibrium if for all k, for all $p \in \mathcal{P}_k$ with positive mass, $\ell_p^k(\mu)$ is minimal on $\mathcal{P}_k$

$$\ell_p^k(\mu) \leq \ell_{p'}^k(\mu) \; \forall p' \in \mathcal{P}_k$$

- How to compute Nash equilibria? Convex formulation

Potential function

μ is a Nash equilibrium iff it minimizes a potential function

$$\min_{\mu \in \Delta^{\mathcal{P}_1} \times \cdots \times \Delta^{\mathcal{P}_K}, \phi = M\mu} \sum_e \int_0^{\phi_e} c_e(u) du$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The learning model

- How do players find a Nash equilibrium?
  Ideally: distributed, and has minimal information requirements.
- Player dynamics: given $\pi^{k(t)}$, $\ell^k(\mu^{(t)})$, choose $\pi^{k(t+1)}$

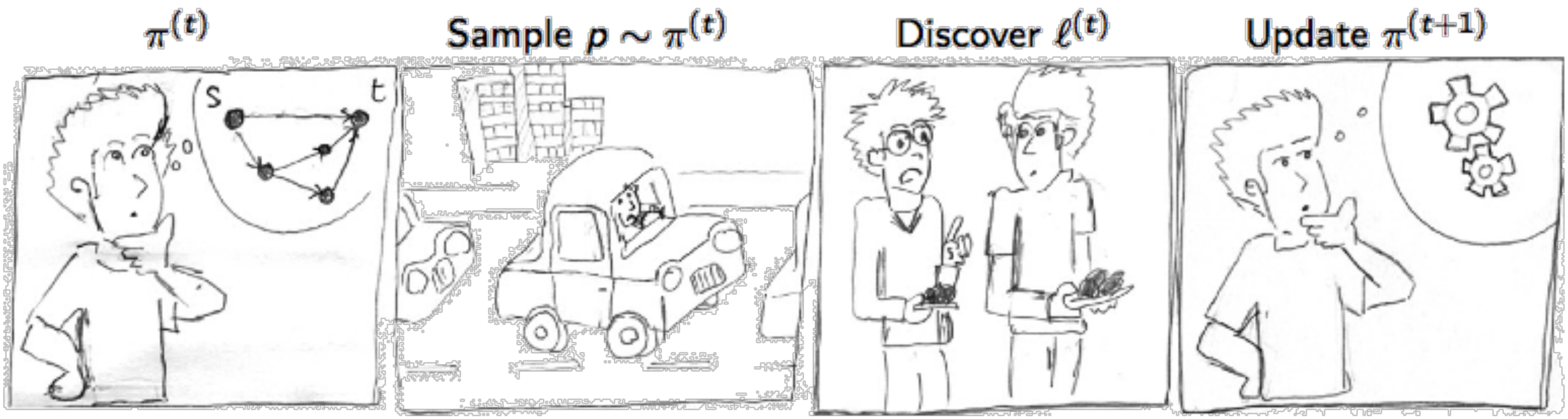
Hedge algorithm

- Update the distribution according to observed loss

$$\pi_p^{k(t+1)} \propto \pi_p^{k(t)} e^{-\eta_t \ell_p^{k(t)}}$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The learning model



A bound on discounted regret

- Assume losses are in [0, 1].
- Expected loss is $\langle \pi^{(t)}, \ell^k(\mu^{(t)}) \rangle$
- Discounted regret

$$\bar{r}^{k(T)} = \frac{\sum_{t \le T} \eta_t \langle \pi^{k(t)}, \ell^k(\mu^{(t)}) \rangle - \min_p \sum_{t \le T} \eta_t \ell_p^k(\mu^{(t)})}{\sum_{t \le T} \eta_t}$$

Fact: Regret bound

Under Hedge with learning rates η_t,

$$\bar{r}^{(T)} \le \frac{\ln \pi_{\min}^{(0)} + c \sum_{t \le T} \eta_t^2}{\sum_{t \le T} \eta_t}$$

Convergence of no-regret learning

Convergence of averages to Nash equilibria

If an update has vanishing regret, then $\bar{\mu}^{(T)} = \sum_{t \le T} \eta_t \mu^{(t)} / \sum_{t \le T} \eta_t$ converges

$$\lim_{T \to \infty} d\left(\bar{\mu}^{(T)}, \mathcal{N}\right) = 0$$

Proof: show

$$V(\bar{\mu}^{(T)}) - V(\mu^*) \le \sum_k \bar{r}^{k(T)}$$

Corollary

A dense subsequence of $(\mu^{(t)})_t$ converges.

Krichene et al. (2014)

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Strong convergence

- Have $\bar{\mu}^{(t)} \to \mathcal{N}$.
- For some classes of algorithms, can show $\mu^{(t)} \to \mathcal{N}$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Strong convergence results

Approximate REP algorithm

$$\pi_p^{(t+1)} - \pi_p^{(t)} = \eta_t \pi_p^{(t)} \left(\left\langle \ell^k(\mu^{(t)}), \pi^{(t)} \right\rangle - \ell_p^k(\mu^{(t)}) \right) + \eta_t U_p^{k(t+1)}$$

$(U^{(t)})_{t \geq 1}$ perturbations that satisfy for all $T > 0$,

$$\lim_{\tau_1 \to \infty} \max_{\tau_2 : \sum_{t=\tau_1}^{\tau_2} \eta_t < T} \left\| \sum_{t=\tau_1}^{\tau_2} \eta_t U^{(t+1)} \right\| = 0$$

Theorem (Krichene et al., ICML 2014)

Under any no-regret algorithm which is AREP, $\mu^{(t)} \to \mathcal{N}$.

Theorem

If edge latencies are Lipschitz, then under any Mirror Descent algorithm with $\eta_t \downarrow 0$ and $\sum_t \eta_t = \infty$

$$\mu^{(t)} \to \mathcal{N}$$

Online learning: summary

- Convergence of $\bar{\mu}^{(t)}$ under no-regret updates.
- Convergence of a dense subsequence $(\mu^{(t)})_{t \in \mathcal{T}}$ under no-regret updates.
- Convergence of $\mu^{(t)}$ under no-regret AREP updates.
- Convergence of $\mu^{(t)}$ under any Mirror Descent with $\eta_t \downarrow 0$ and $\sum_t \eta_t = \infty$.

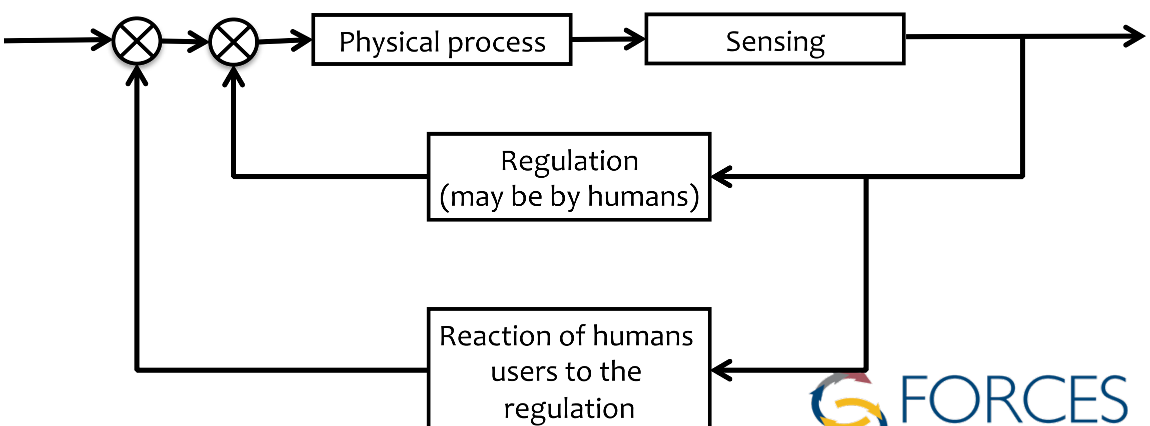
We have a model for route choice dynamics

- Can apply optimal control, e.g. partial route control, tolling.
- Currently exploring robustness of convergence.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Conclusions

* Vulnerabilities exist at all levels of the network: sensing, regulation, reaction of humans.
* Optimal control schemes can be turned into attack schemes for the three levels
* Next steps: assessments of the vulnerability (resilience) and mitigation models
* End step: economic incentives assessments (pricing)



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS