Berkeley
UNIVERSITY OF CALIFORNIA

Security Analysis of Freeway Systems:

A Distributed Control Approach

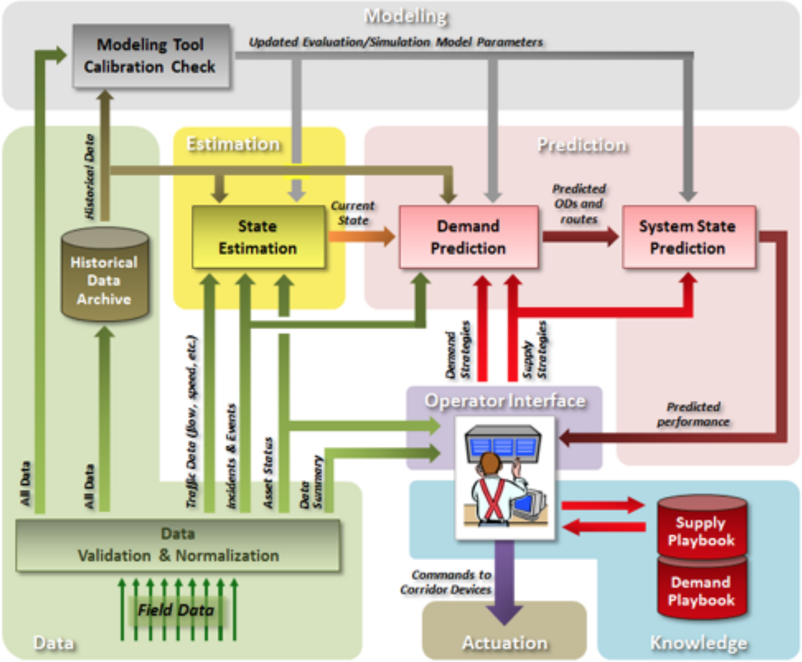
Jack Reilly - Dissertation Talk


4:20
Google
Maps
Play Store

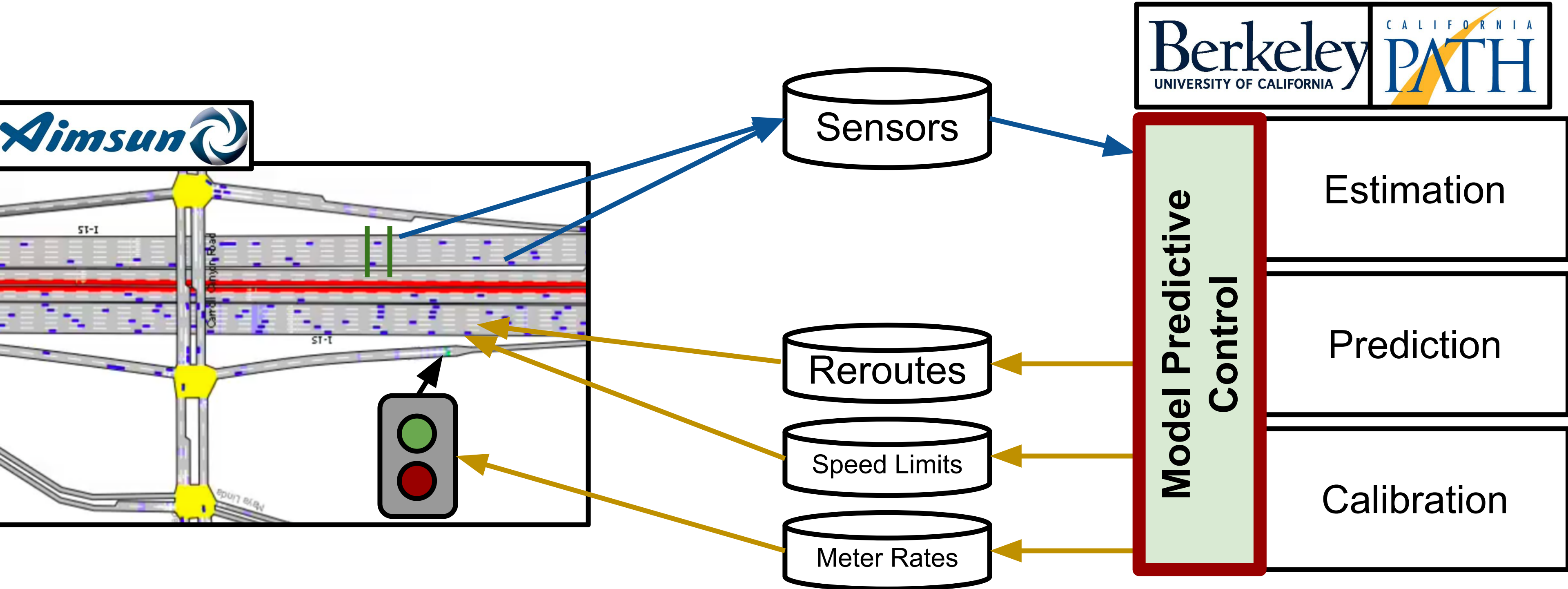
Connected Corridors

"Reduce congestion and improve travel time reliability along fifty corridors throughout the state of California"

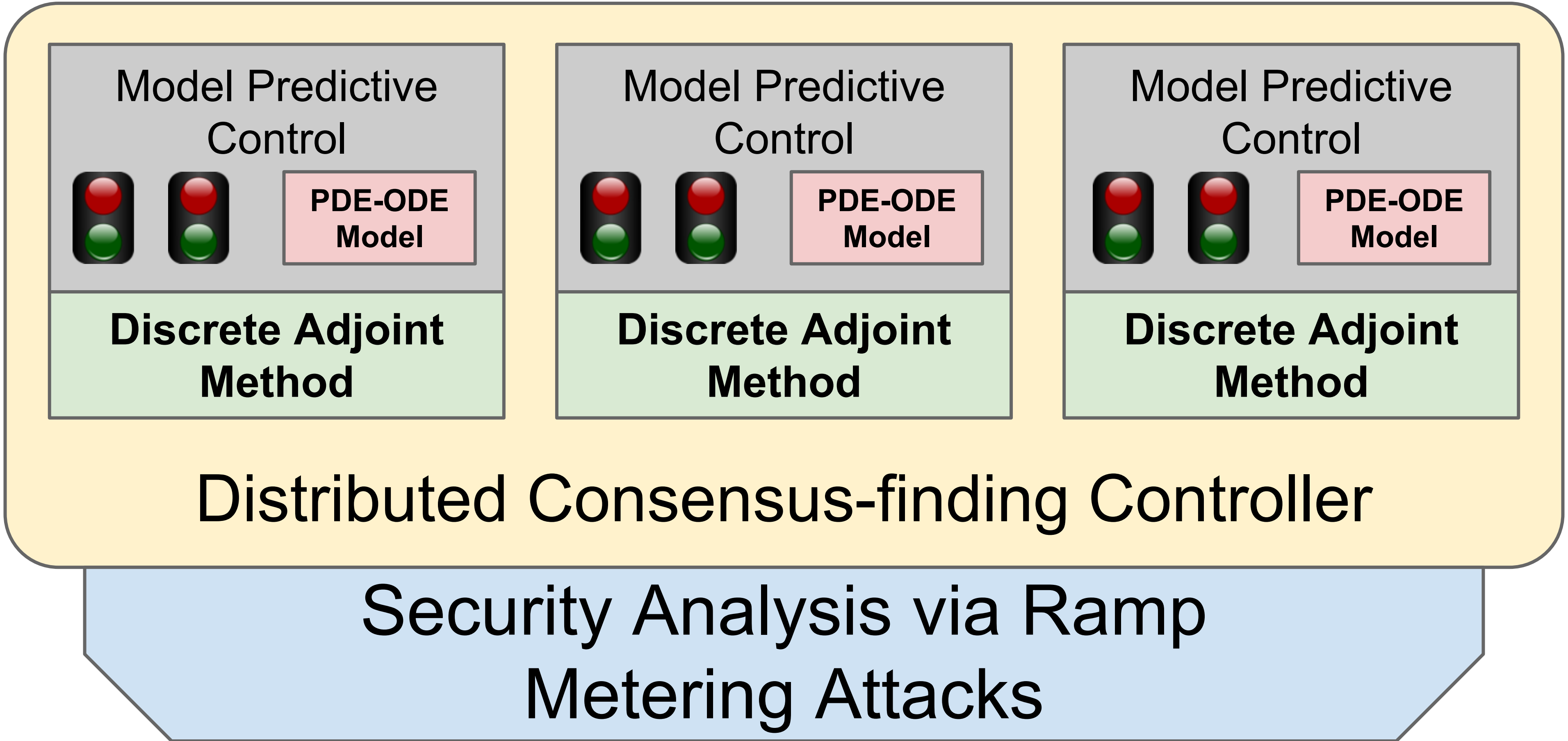
- Mission Statement



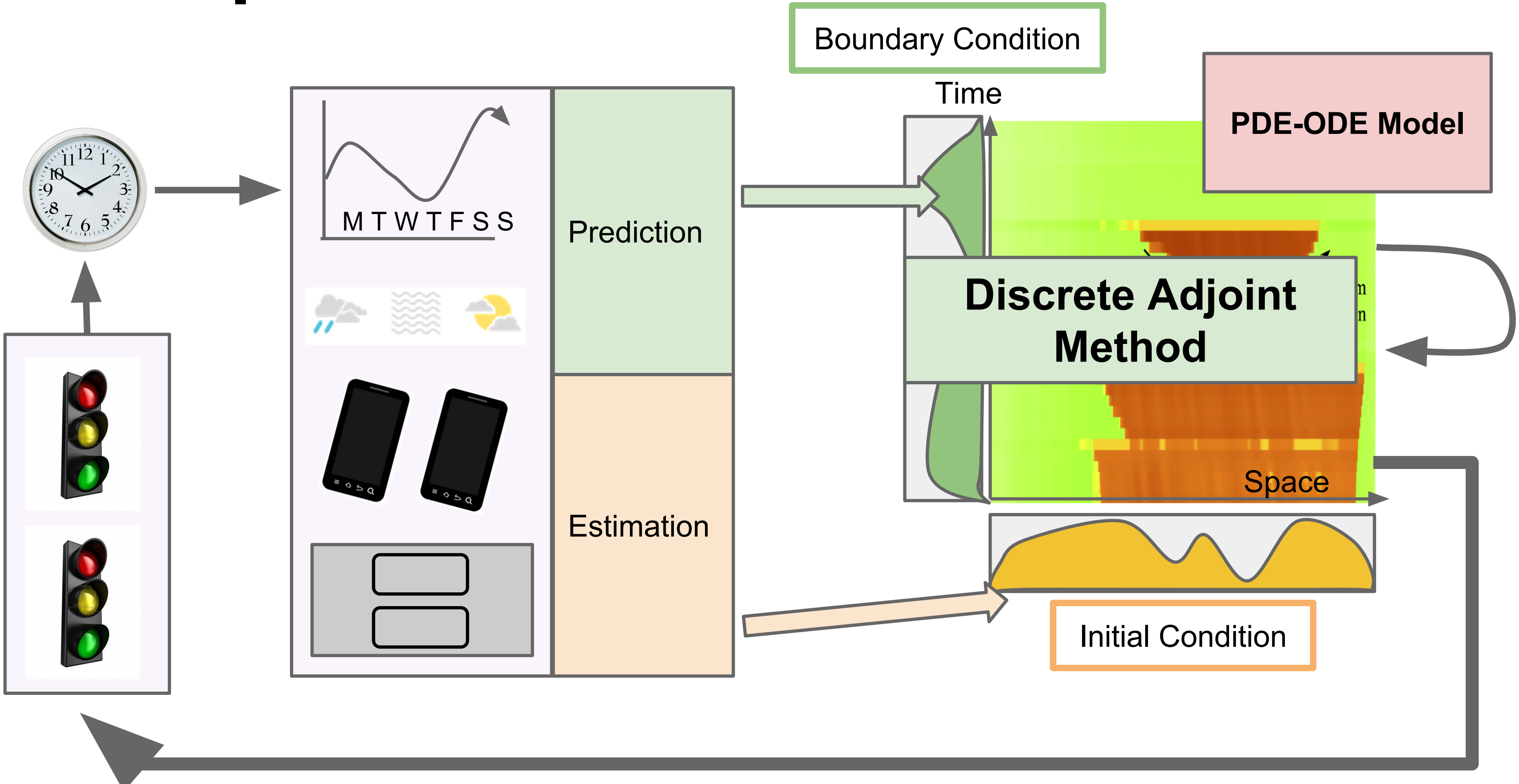
CC System Architecture



Overview


Model Predictive Control
PDE-ODE Model
Discrete Adjoint Method
Model Predictive Control
PDE-ODE Model
Discrete Adjoint Method
Model Predictive Control
PDE-ODE Model
Discrete Adjoint Method
Distributed Consensus-finding Controller
Security Analysis via Ramp Metering Attacks

Model predictive control

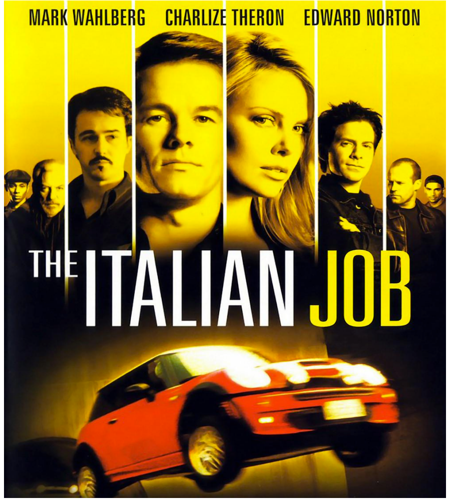


Model Predictive Control: Ramp Metering

Distributed Consensus-finding Controller

Recent traffic system compromises

The *Italian Job* (2003)



Recent traffic system compromises

The *Italian Job* (2003)

The "real" *Italian Job* (2007)

Los Angeles Times | LOCAL | SPORTS | ENTERTAINMENT | NATION | WORLD | BUSINESS | OPINION | LIFESTYLE | MORE

YOU ARE HERE: LAT Home → Collections → Los Angeles

Key signals targeted, officials say

Two accused of hacking into L.A.'s traffic light system plead not guilty. They allegedly chose intersections they knew would cause major jams.

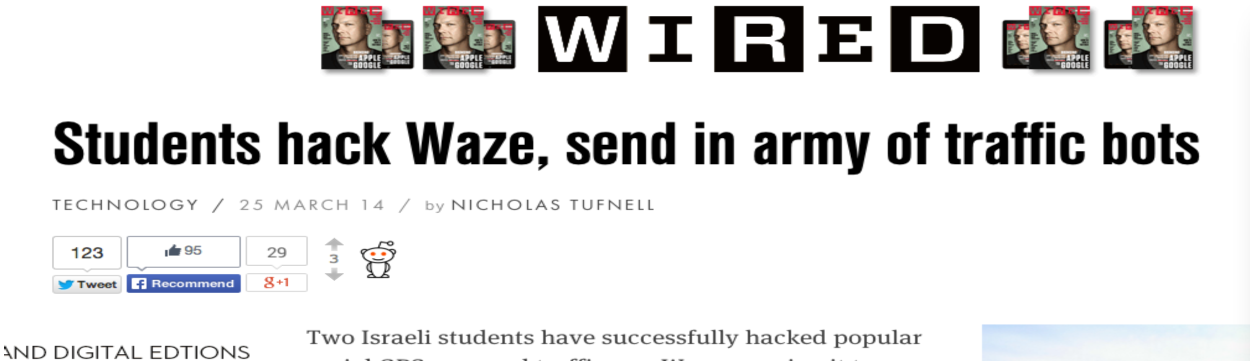
January 09, 2007 | Sharon Bernstein and Andrew Blankstein | Times Staff Writers

Recent traffic system compromises

The *Italian Job* (2003)

The “real” *Italian Job* (2007)

Waze / Google hacked (2014)


WIRED

Students hack Waze, send in army of traffic bots

TECHNOLOGY / 25 MARCH 14 / by NICHOLAS TUFNELL

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

AND DIGITAL EDTIONS

Two Israeli students have successfully hacked popular

Recent traffic system compromises

The *Italian Job* (2003)

The “real” *Italian Job* (2007)

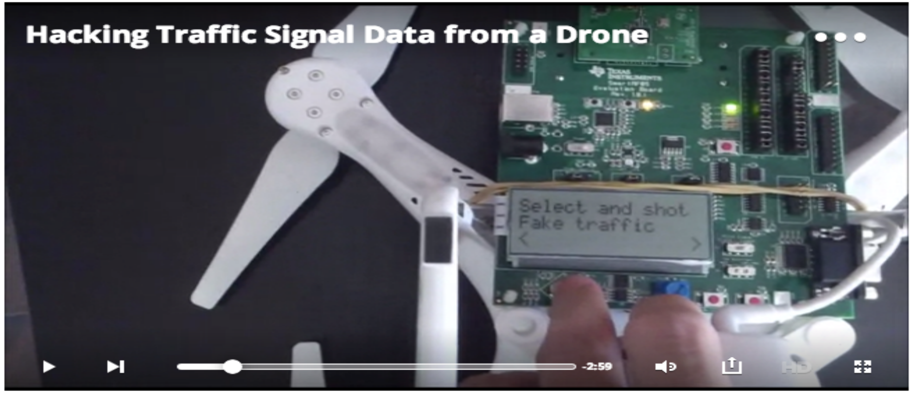
Waze / Google hacked (2014)

Sensys Attack (2014)

Recent traffic system compromises

Security Analysis via Ramp Metering Attacks

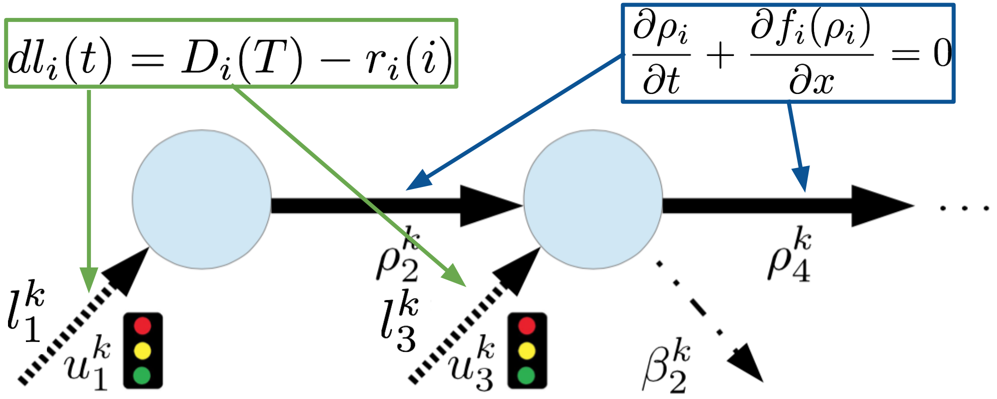
- The
- The “real” *Italian Job* (2007)
- Waze / Google hacked (2014)
- Sensys Attack (2014)



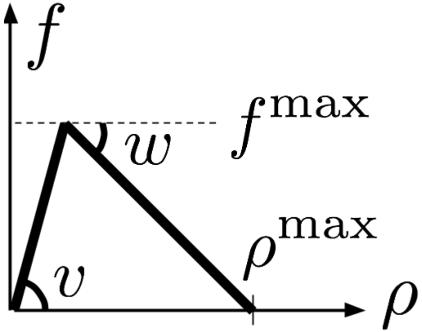
Overview

- Motivation: *Connected Corridors*
- **PDE model for optimal control applications**
- Discrete adjoint framework for ramp-metering
- Distributed control for large-scale systems.
- Security analysis via *ramp-metering attacks*

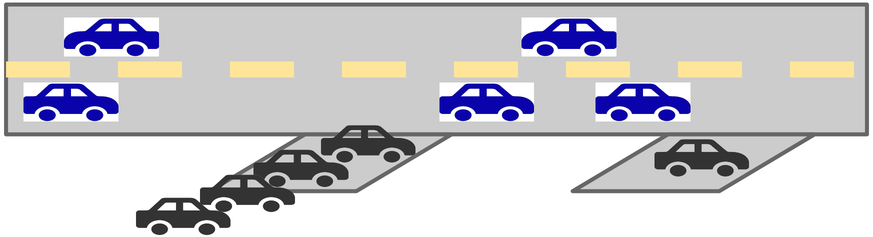
Our model: LWR Network Overview



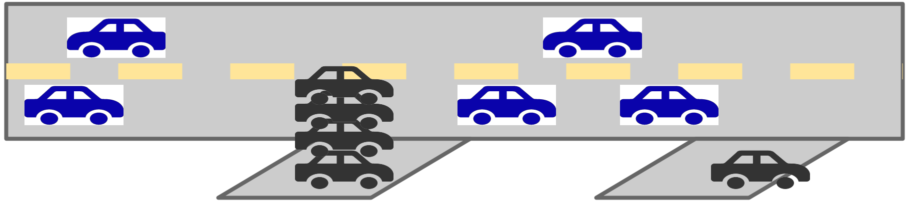
ρ	Vehicle Density
f	Flow Rate
l	Queue Length
u	Metering Rate
β	Turning Rate
v	Free Flow Vel.
w	Cong. Speed
D	Ramp Demand



Weak Boundary Conditions: **PDE**



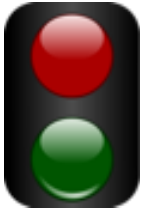
Strong Boundary Conditions: **ODE**



Delle Monache, M. L., Reilly, J., Samaranayake, S., Krichene, W., Goatin, P., & Bayen, A. M. (2014). A PDE-ODE model for a junction with ramp buffer. *SIAM Journal on Applied Mathematics*, *74*(1), 22–39.

Freeway Control Applications

Ramp Metering



$$\min_{u_i(t)} J(u) \text{ s.t. } r_i(t) = u_i(t)\tilde{r}_i(t)$$

Variable Speed Limit

$$\min_{v_i(t)} J(v) \text{ s.t. } \delta_i(t) = \min(v_i(t)\rho_i(t), f_i^{\max})$$

Optimal Re-routing

$$\min_{\beta_i(t)} J(\beta) \text{ s.t. } f_i^{\text{off}}(t) = \beta_i(t) f_i(t)$$

Reilly, J., Samaranayake, S., Delle Monache, M. L., Krichene, W., Goatin, P., & Bayen, A. M. (2014). Adjoint-based optimization on a network of discretized scalar conservation law PDEs with applications to coordinated ramp metering. *Journal of Optimization Theory and Applications (under Review)*.

Delle Monache, M. L., Reilly, J., Samaranayake, S., Krichene, W., Goatin, P., & Bayen, A. M. (2014). A PDE-ODE model for a junction with ramp buffer. *SIAM Journal on Applied Mathematics*, *74*(1), 22–39.

Samaranayake, S., Reilly, J., Krichene, W., Delle Monache, M. L., Goatin, P., & Bayen, A. M. (2014). Multi-commodity real-time dynamic traffic assignment with horizontal queuing. *Transportation Science (under review)*

Overview

- Motivation: *Connected Corridors*
- PDE model for optimal control applications
- **Discrete adjoint framework for ramp-metering**
- Distributed control for large-scale systems.
- Security analysis via *ramp-metering attacks*

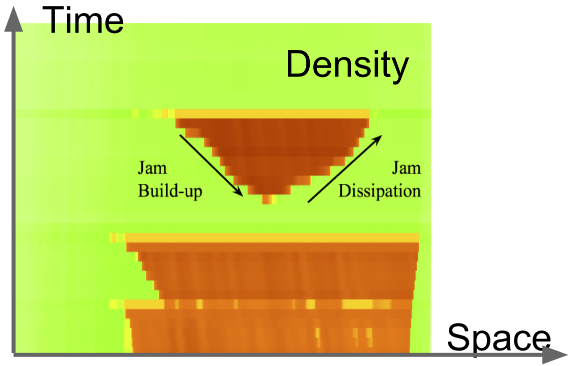
Discretizing via Godunov's Method

$$\min_u J(\rho, u)$$

CONTINUOUS

$$\frac{\partial \rho_i}{\partial t} + \frac{\partial f_i(\rho_i)}{\partial x} = 0$$

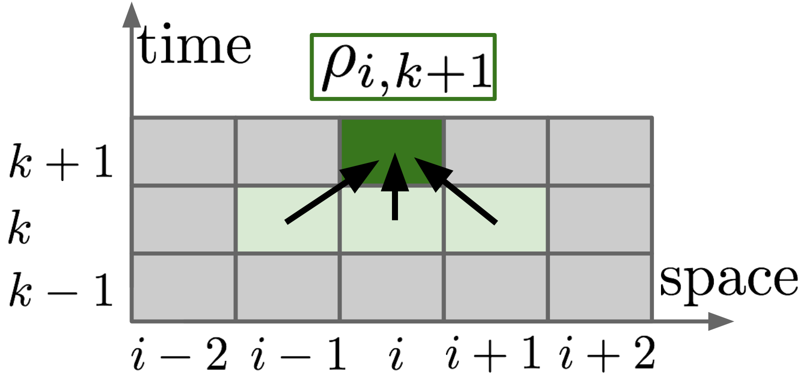
$$dl_i(t) = D_i(T) - r_i(i)$$



DISCRETE

$$H(\rho, u) = 0$$

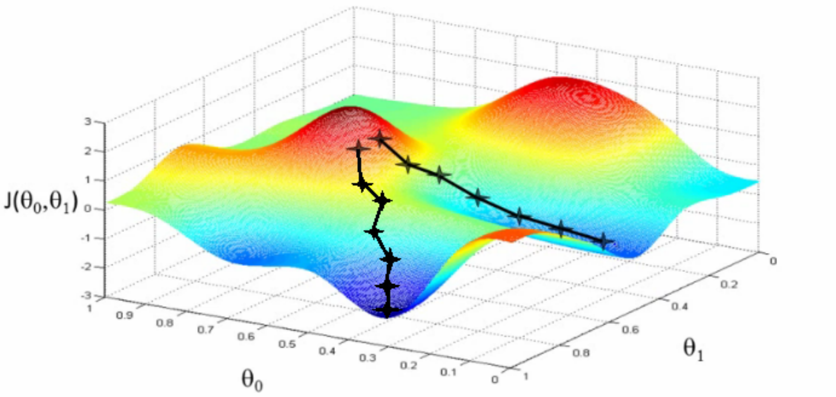
$$H_{i,k+1} = \rho_{i,k+1} - g_i(\rho_{i\pm,k}, u_k)$$

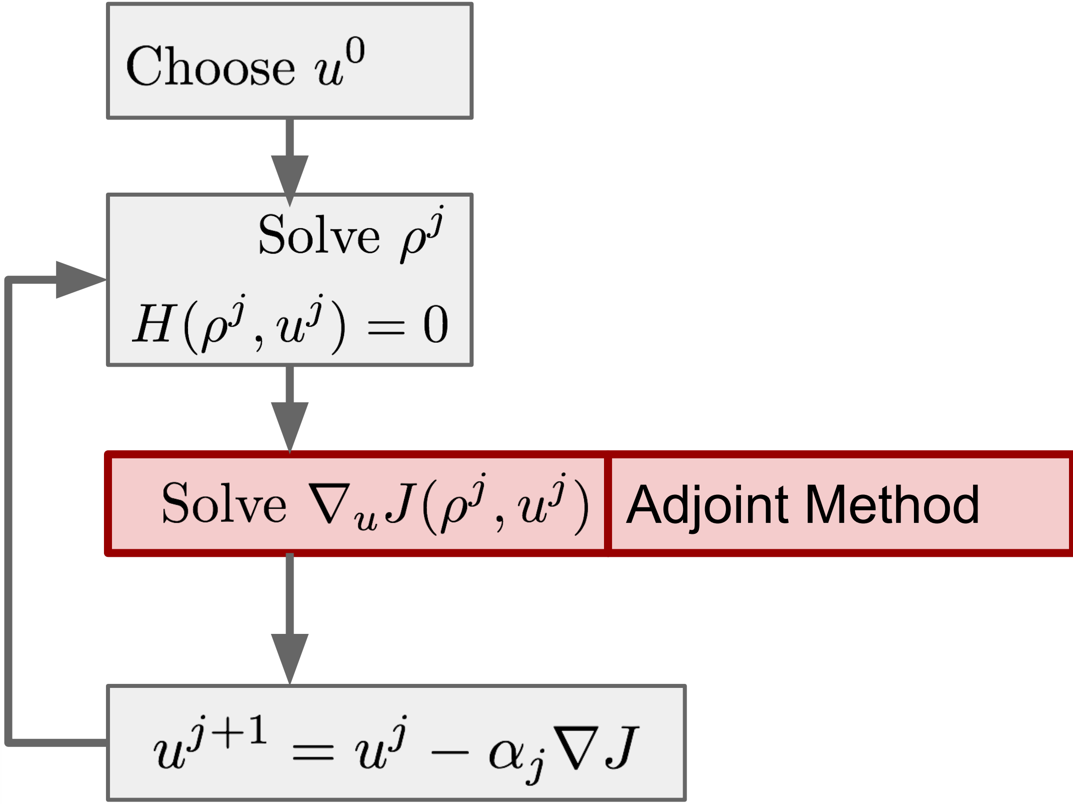


Optimizing Control Via Gradient Descent

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

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





Adjoint Formulation

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

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

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

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

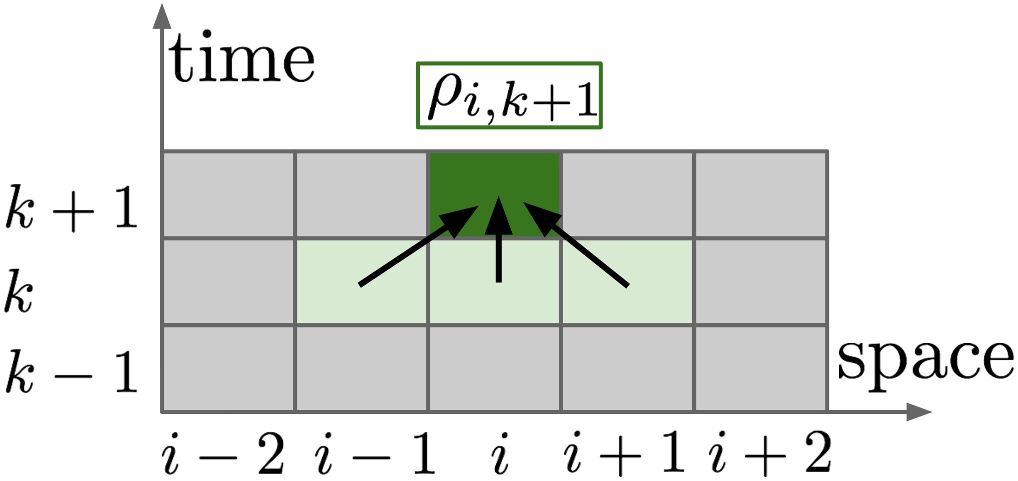
$$\nabla_u J =$$

$$J_u + \lambda^T H_u$$ ⟹ λ : Adjoint Variable

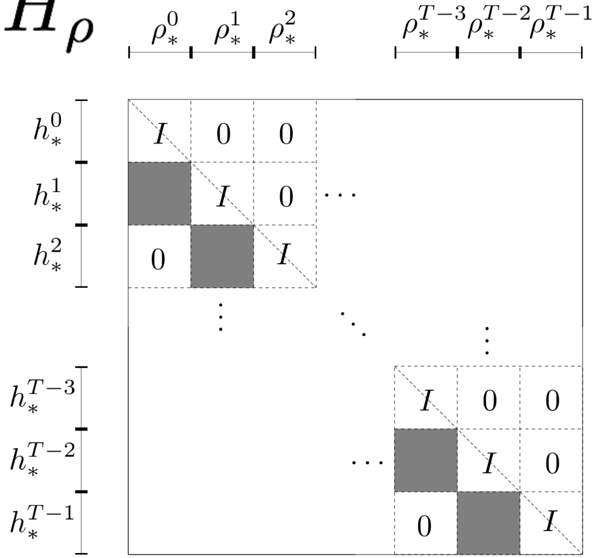
$$H_\rho^T \lambda = -J_\rho^T$$ ⟹ Discrete Adjoint Eqn.

Exploiting Sparsity of System Coupling

$$\nabla_u J =$$
$$J_u + \lambda^T H_u$$
$$H_\rho^T \lambda = -J_\rho^T$$

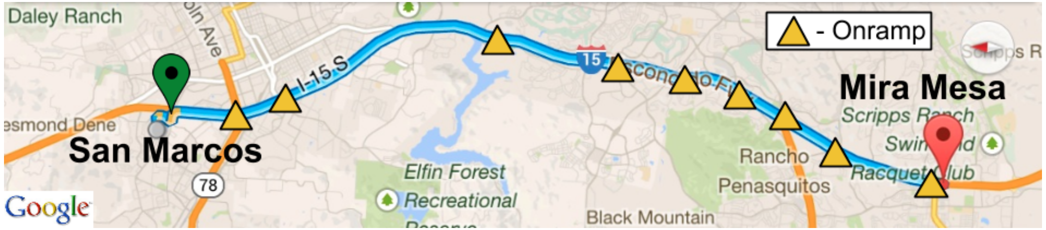


Sparsity of H_ρ

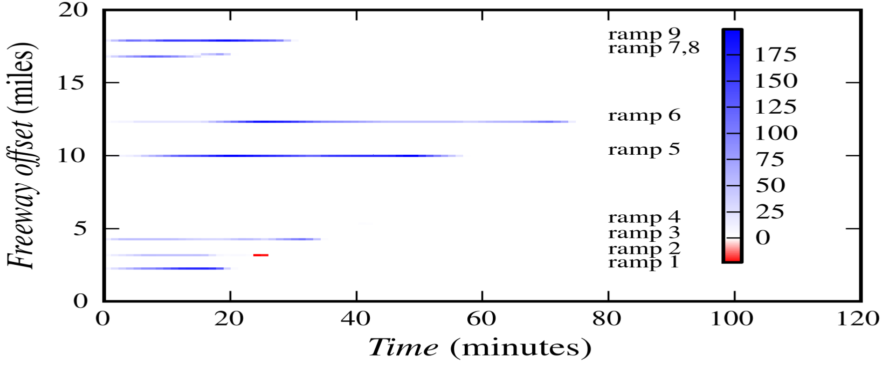


- Lower Triangular
- Sparse
- Linear Complexity

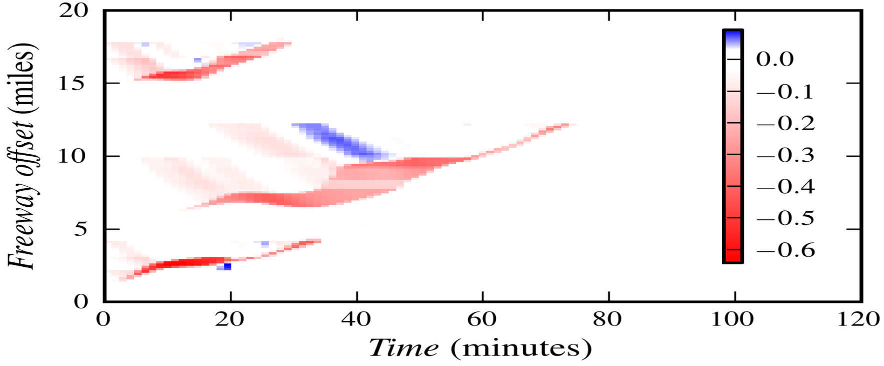
I15 FW (San Diego) Simulations.



Increase in Onramp Queue Lengths



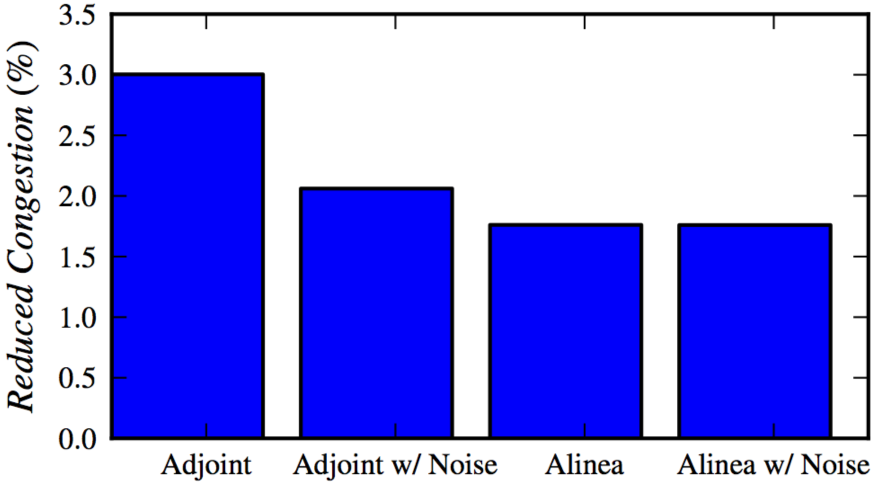
Decrease in Mainline Vehicle Density



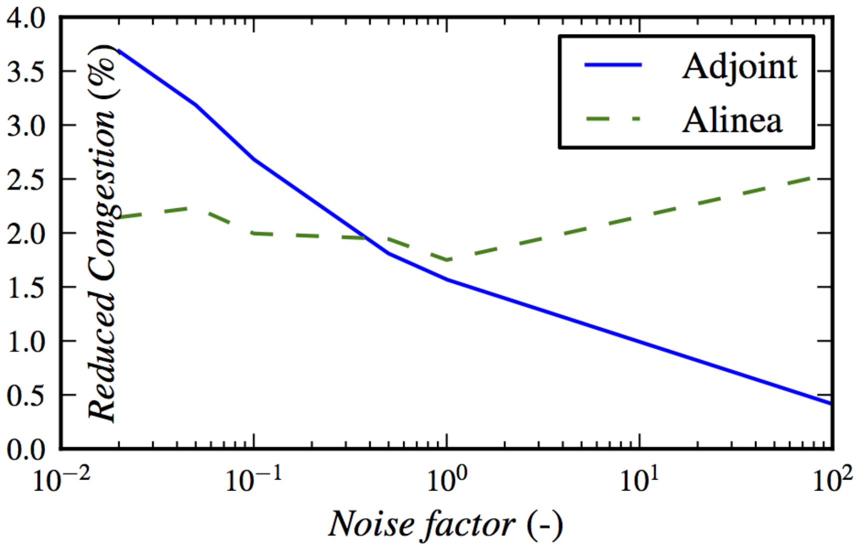
Reilly, J., Samaranayake, S., Delle Monache, M. L., Krichene, W., Goatin, P., & Bayen, A. M. (2014). Adjoint-based optimization on a network of discretized scalar conservation law PDEs with applications to coordinated ramp metering. *Journal of Optimization Theory and Applications (under Review)*.

I15 MPC Robustness Results

Percentage Reduction in Congestion

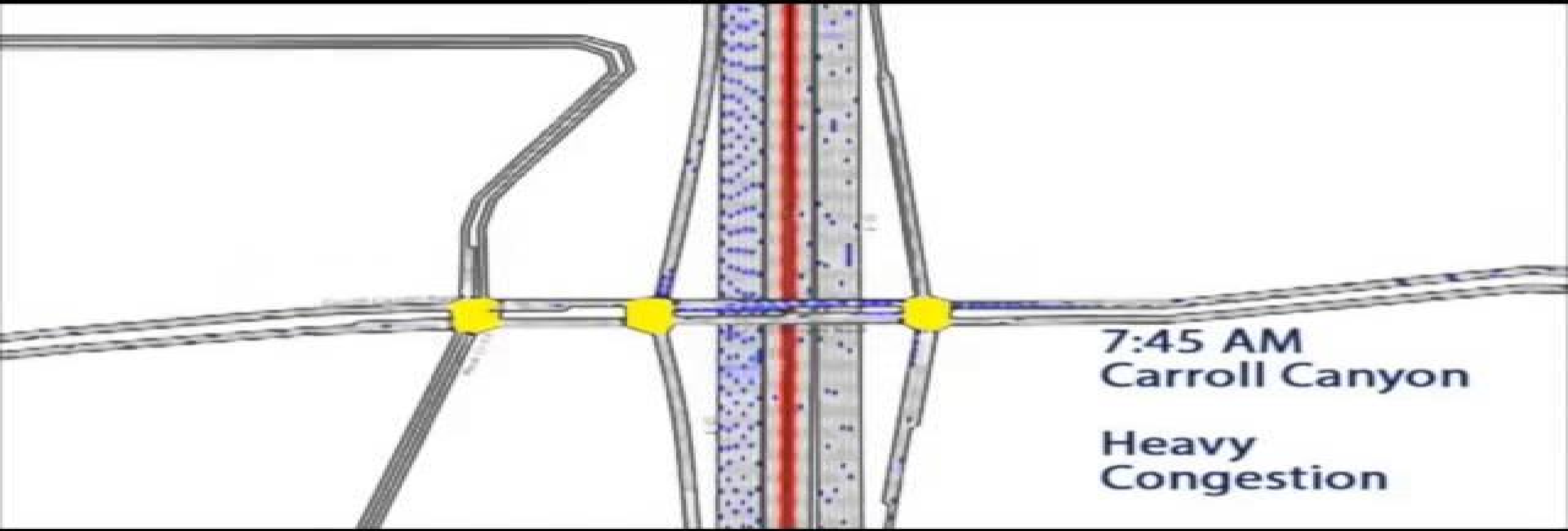


Robustness of Controller to Noise

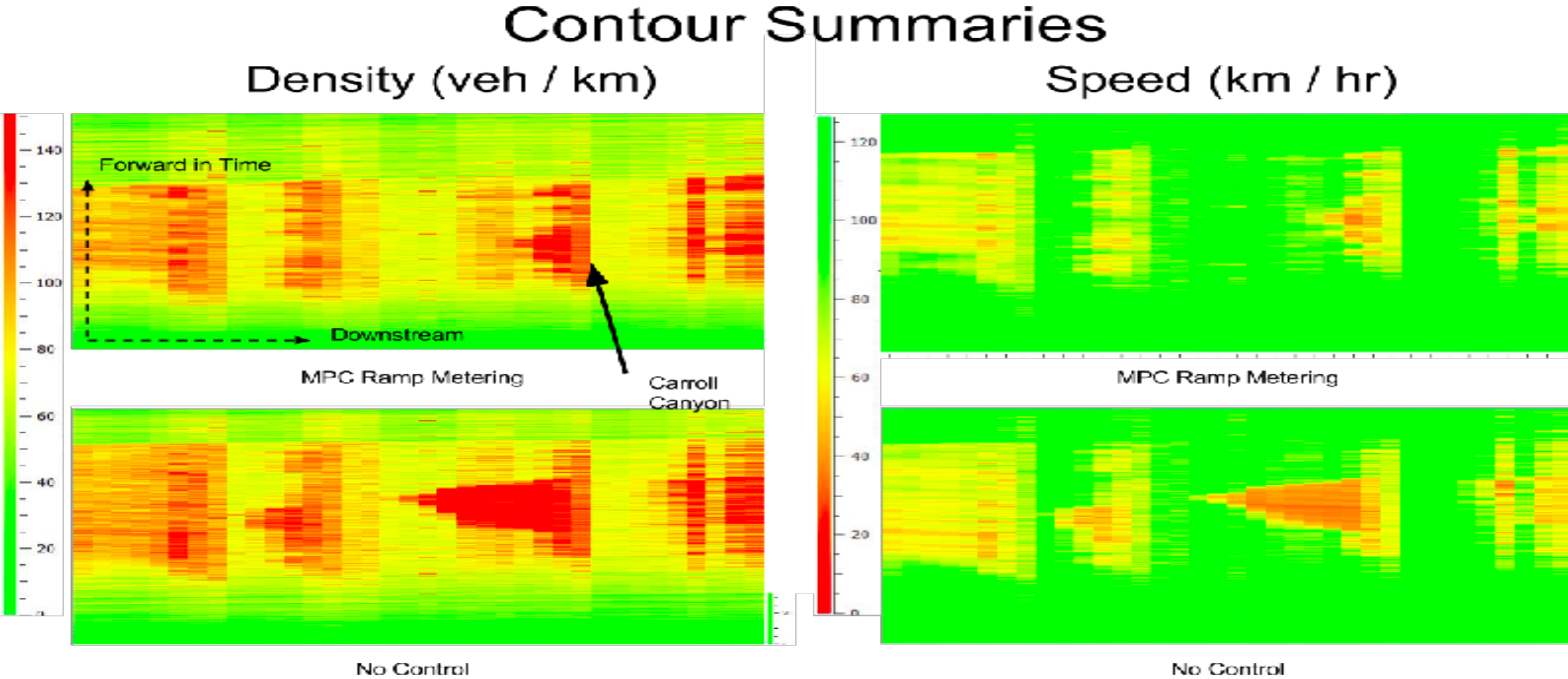


Reilly, J., Samaranayake, S., Delle Monache, M. L., Krichene, W., Goatin, P., & Bayen, A. M. (2014). Adjoint-based optimization on a network of discretized scalar conservation law PDEs with applications to coordinated ramp metering. *Journal of Optimization Theory and Applications (under Review)*.

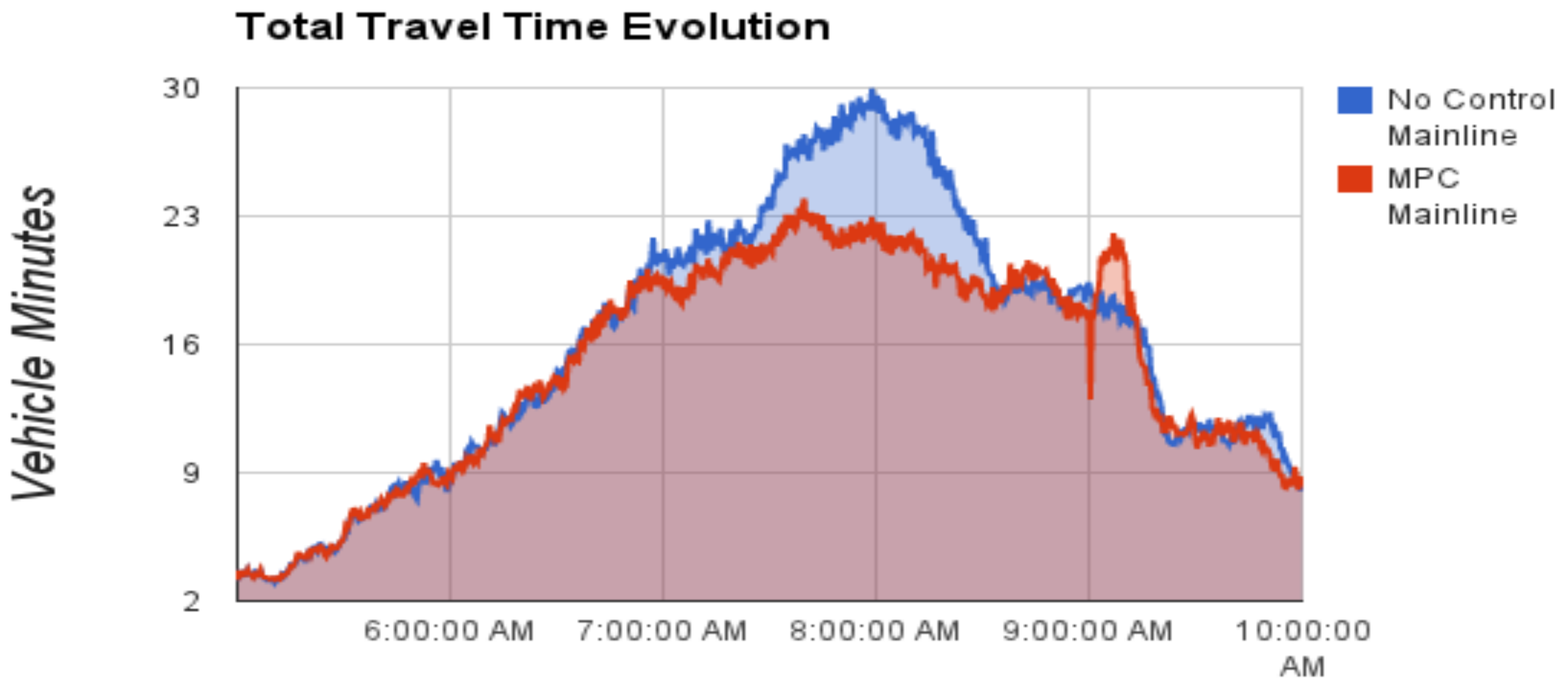
Aimsun Micro-Simulation



Aimsun I15 Space-time Summary



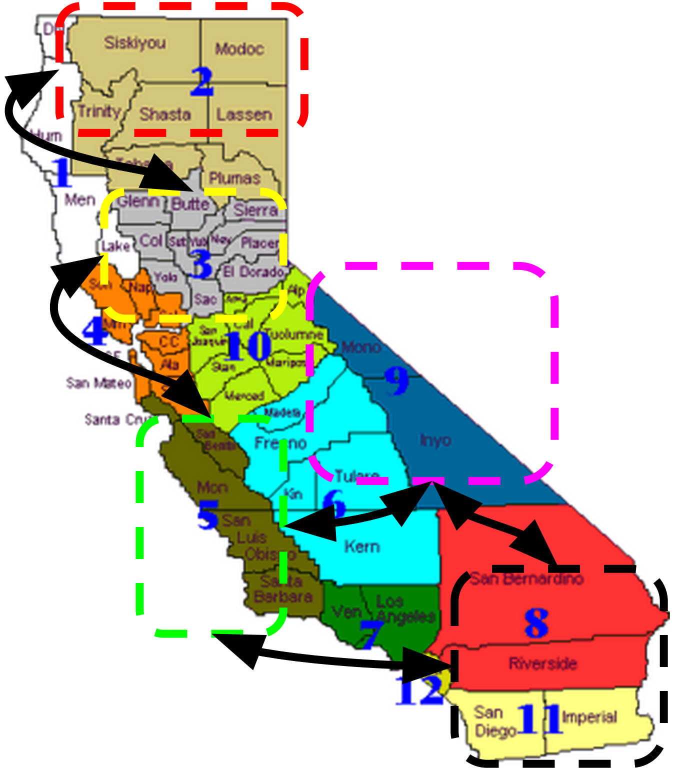
Mainline Travel Time Decrease



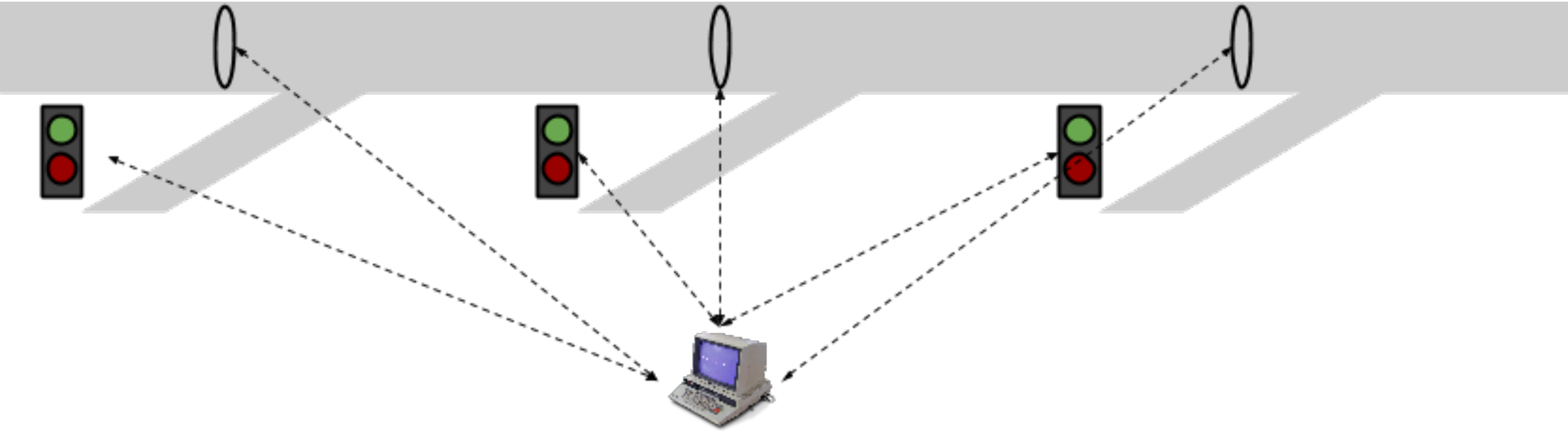
Overview

- Motivation: *Connected Corridors*
- PDE model for optimal control applications
- Discrete adjoint framework for ramp-metering
- **Distributed control for large-scale systems.**
- Security analysis via *ramp-metering attacks*

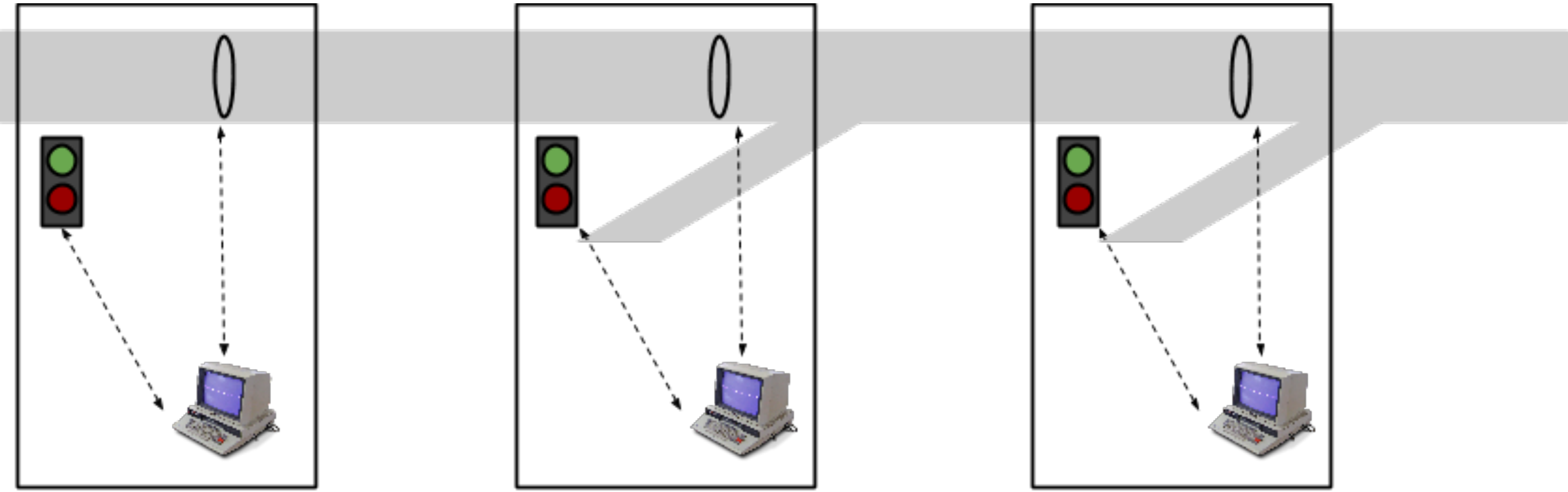
Distributed Control Architectures



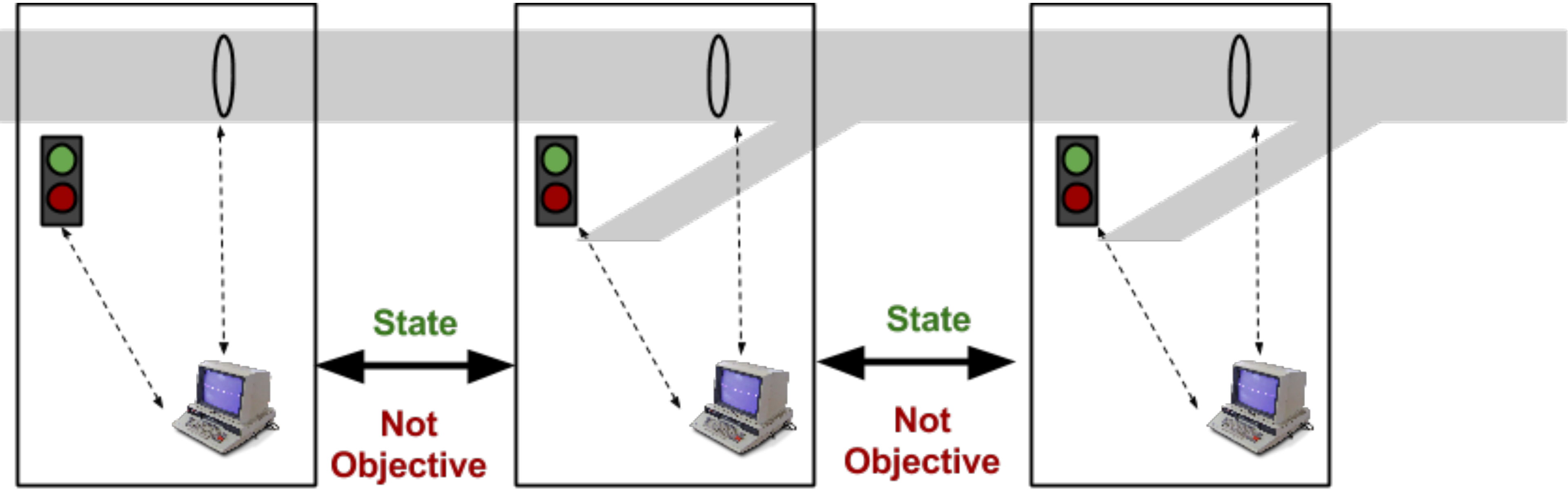
Existing approaches: Centralized



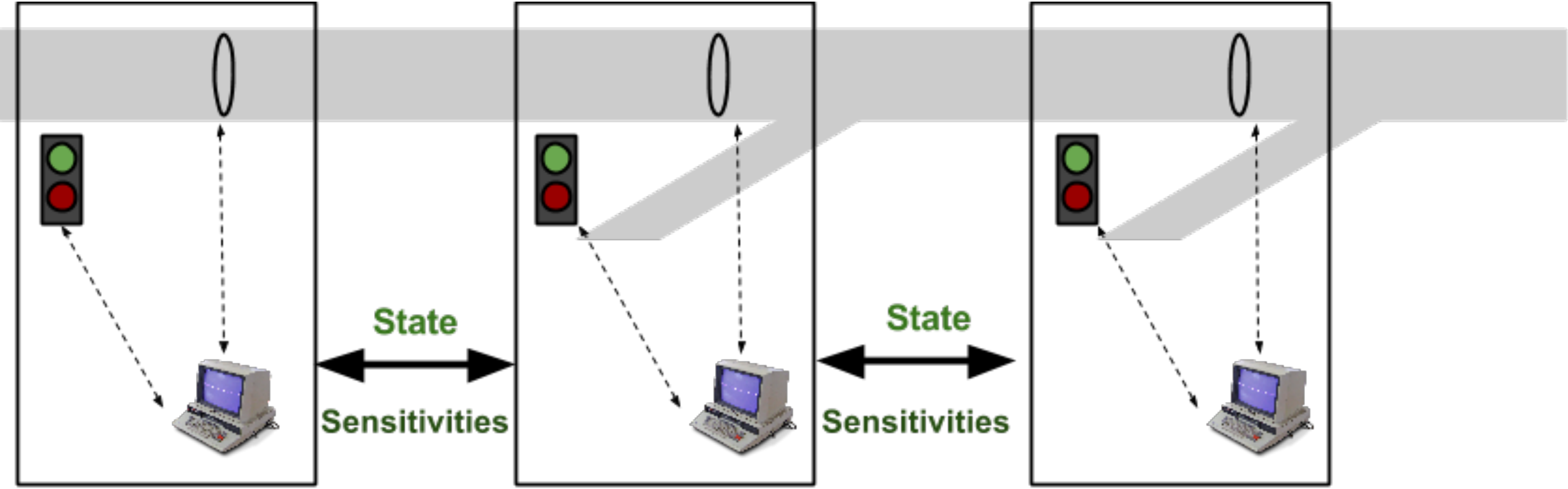
Existing approaches: Local



Existing approaches: Communicative

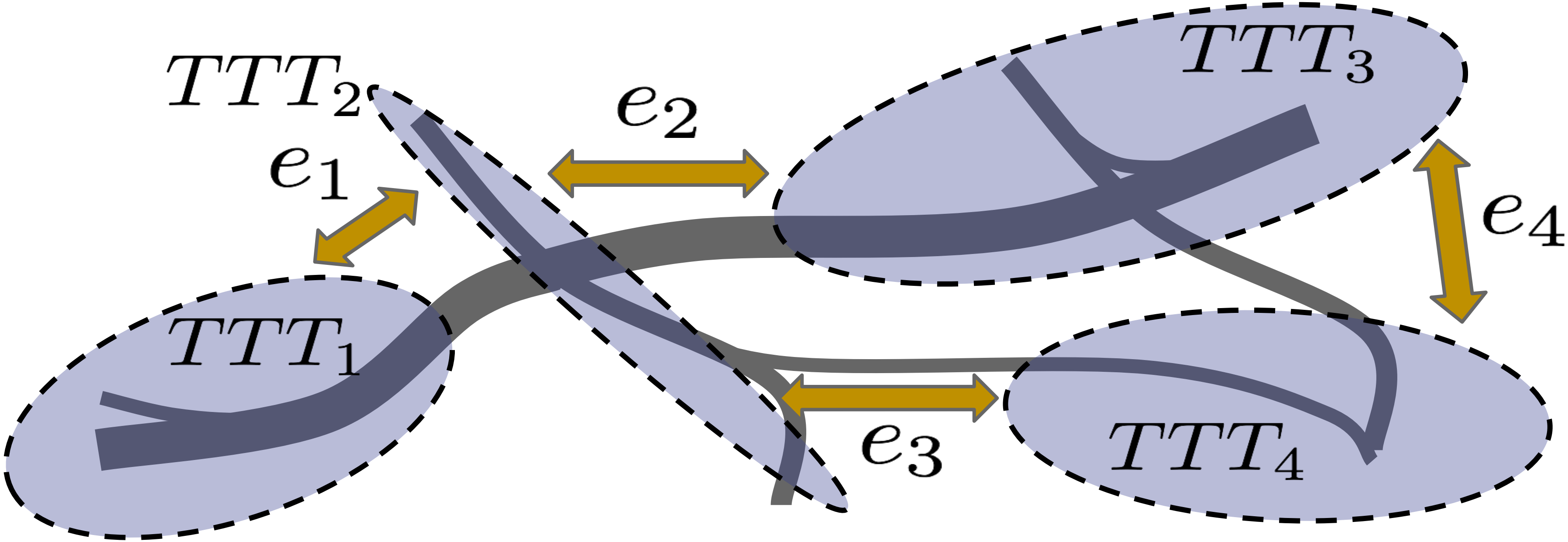


Our approach: <u>Consensus Sensitivity</u>



Multi-agent Consensus Optimization: HOW IT WORKS

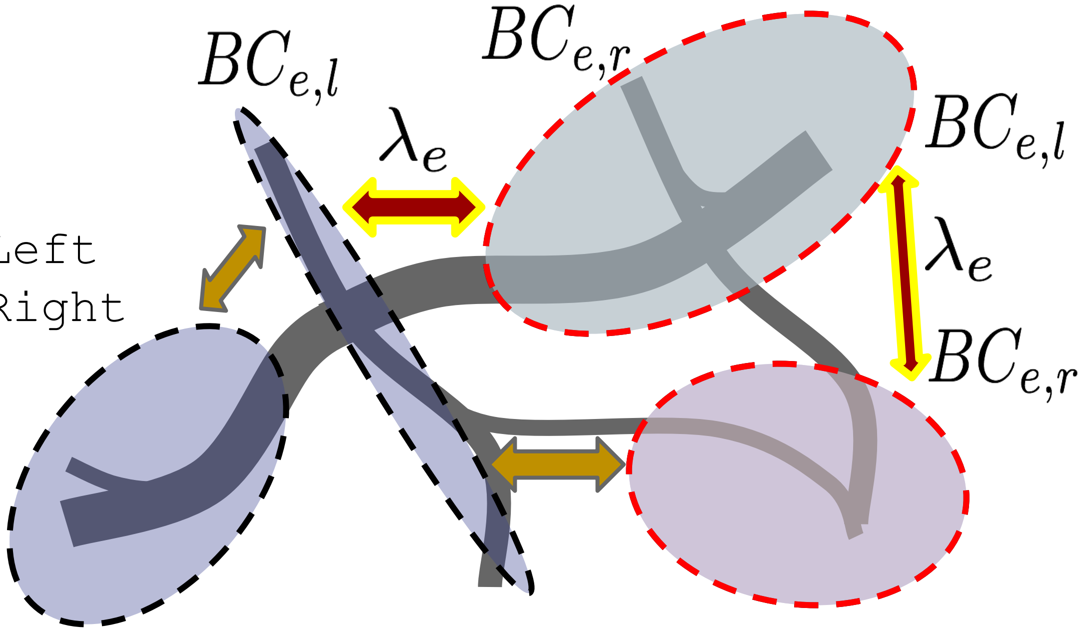
$$\max_{\lambda_{e\in E}} \min J = TTT = \sum_i TTT_i + \sum_e \lambda_e^T (BC_{e,l} - BC_{e,r})$$



Asynchronous ADMM Algorithm

$$\min_{\substack{\max \\ \lambda_{e \in E}}} J = TTT = \sum_i TTT_i + \sum_e \lambda_e^T (BC_{e,l} - BC_{e,r})$$

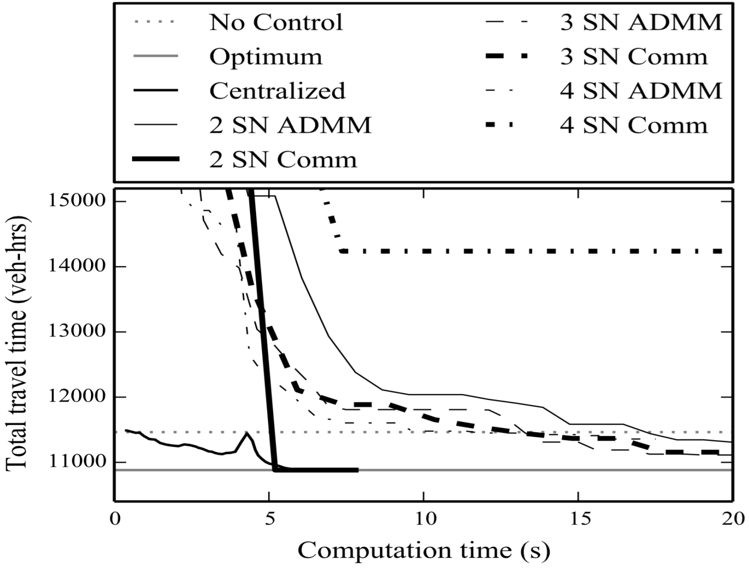
```
def A-ADMM(J_i, E):
    While Not Converged:
        Choose e from E
        Minimize J_i: i = e-Left
        Minimize J_i: i = e-Right
        Exchange BC's
        Maximize e-λ
    return optimal_control
```



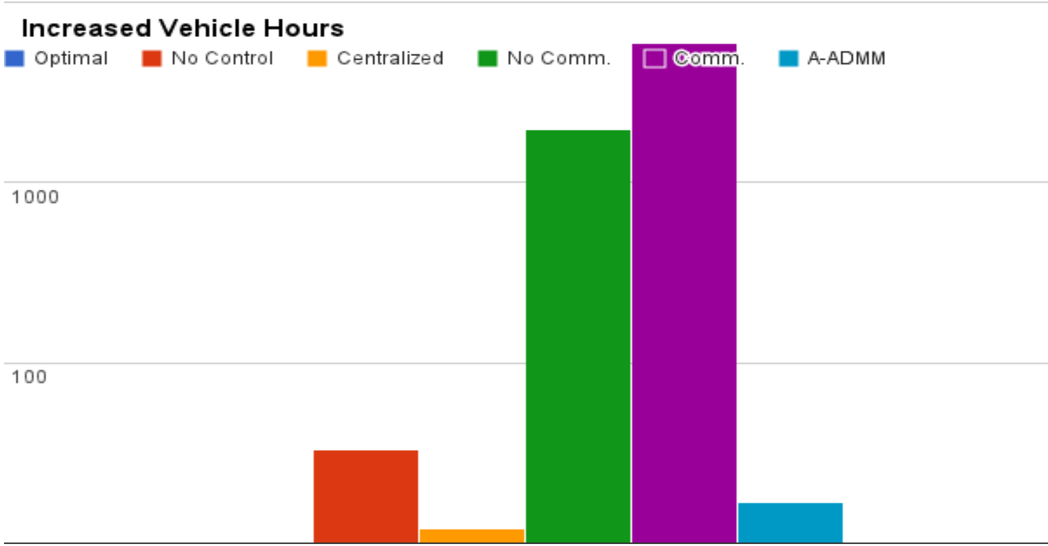
Reilly, J., & Bayen, A. M. (2014). Distributed Optimization for Shared State Systems: Applications to Decentralized Freeway Control via Subnetwork Splitting. *IEEE Transactions on Intelligent Transportation Systems (under Review)*.

I15 Experiment: Metering + VSL

Convergence Time vs. Number of Agents



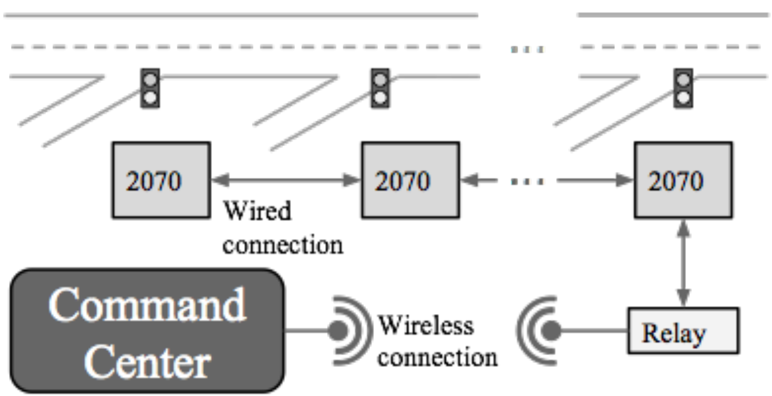
MPC Travel Time Above Theoretical Optimum

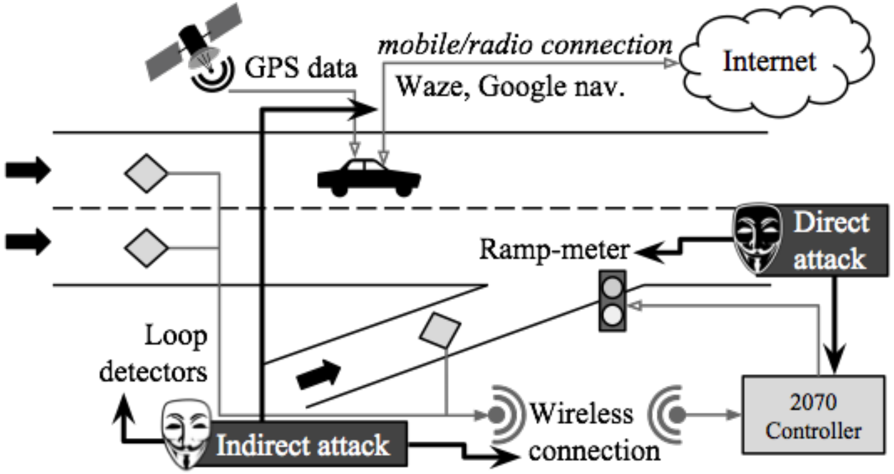


Overview

- Motivation: *Connected Corridors*
- PDE model for optimal control applications
- Discrete adjoint framework for ramp-metering
- Distributed control for large-scale systems.
- **Security analysis via *ramp-metering attacks***

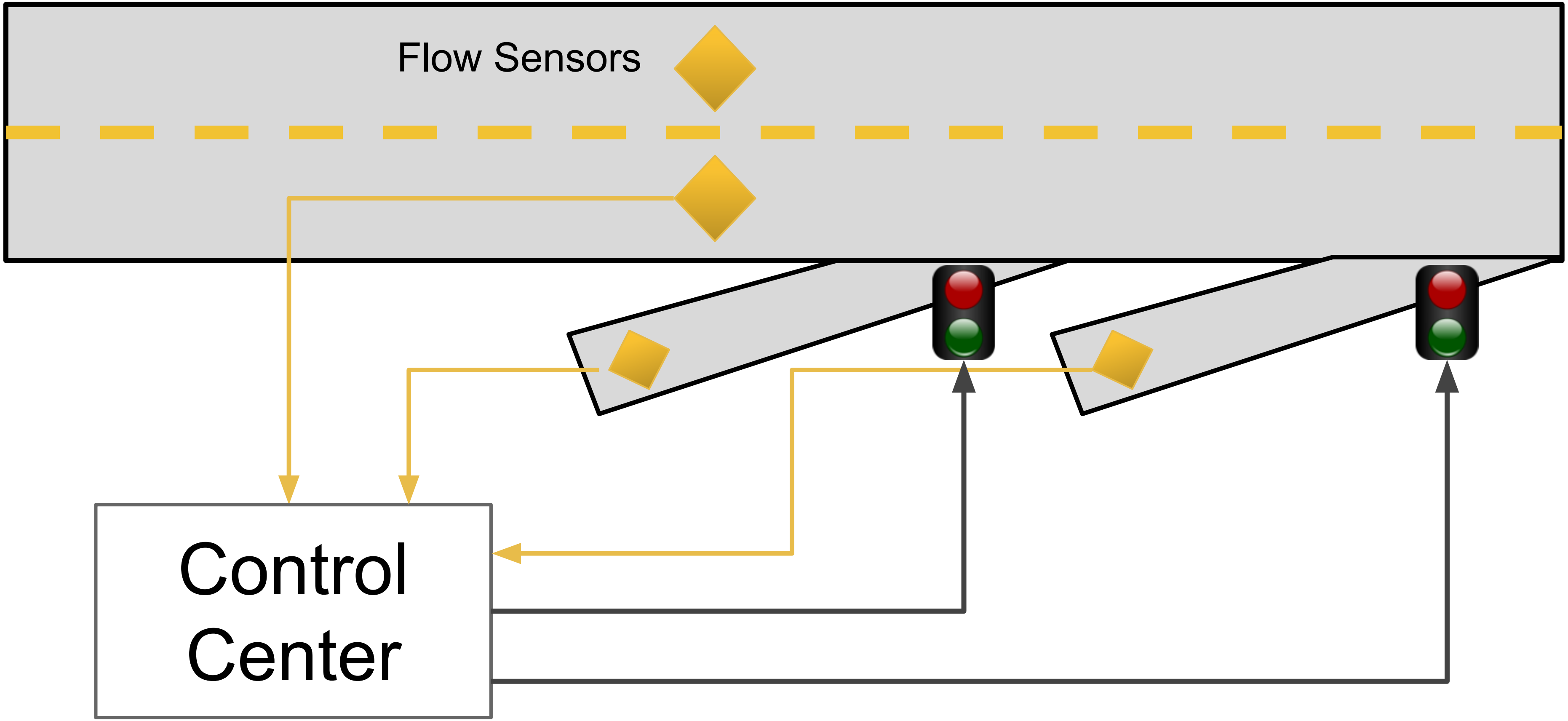
Traffic System Vulnerabilities



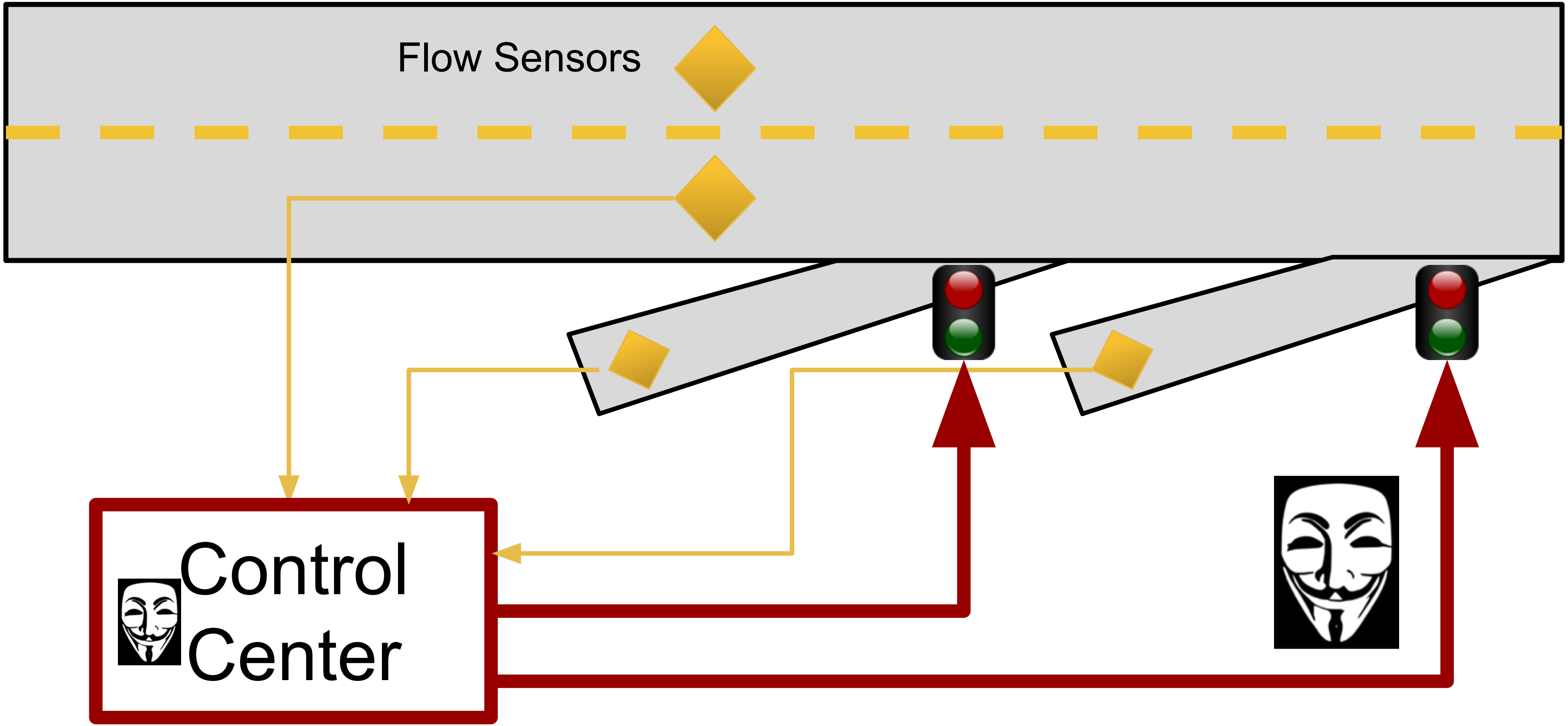


Attack Description	Access	Control	Complexity	Cost
copper theft/clipping wires	physical	low	low	low
replacing a single sensor/actuator	physical	low	low	low
attacking a single sensor/actuator	locality	low	medium	low
replacing a single control box	physical	medium	medium	medium
replacing a set of sensors/actuator	physical	medium	medium	medium
attacking a set of sensors/actuator	locality	low	medium	low
replacing a corridor of control boxes	physical	high	medium	medium
attacking a corridor of control boxes	network	high	high	medium
attacking the control center	network	high	high	high
spoofing GPS data	network	medium	high	medium
attacking navigation software	network	medium	medium	medium

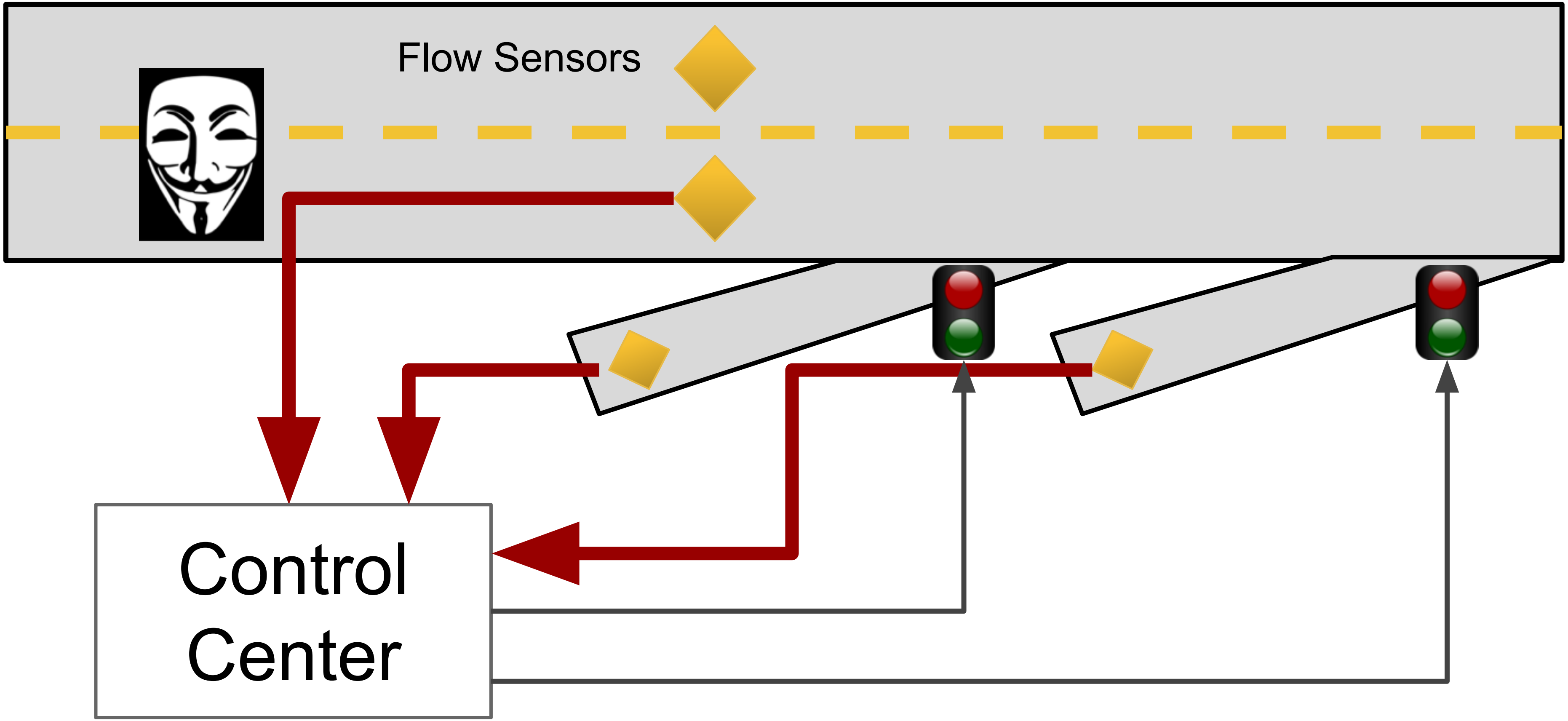
Security of Freeway Systems



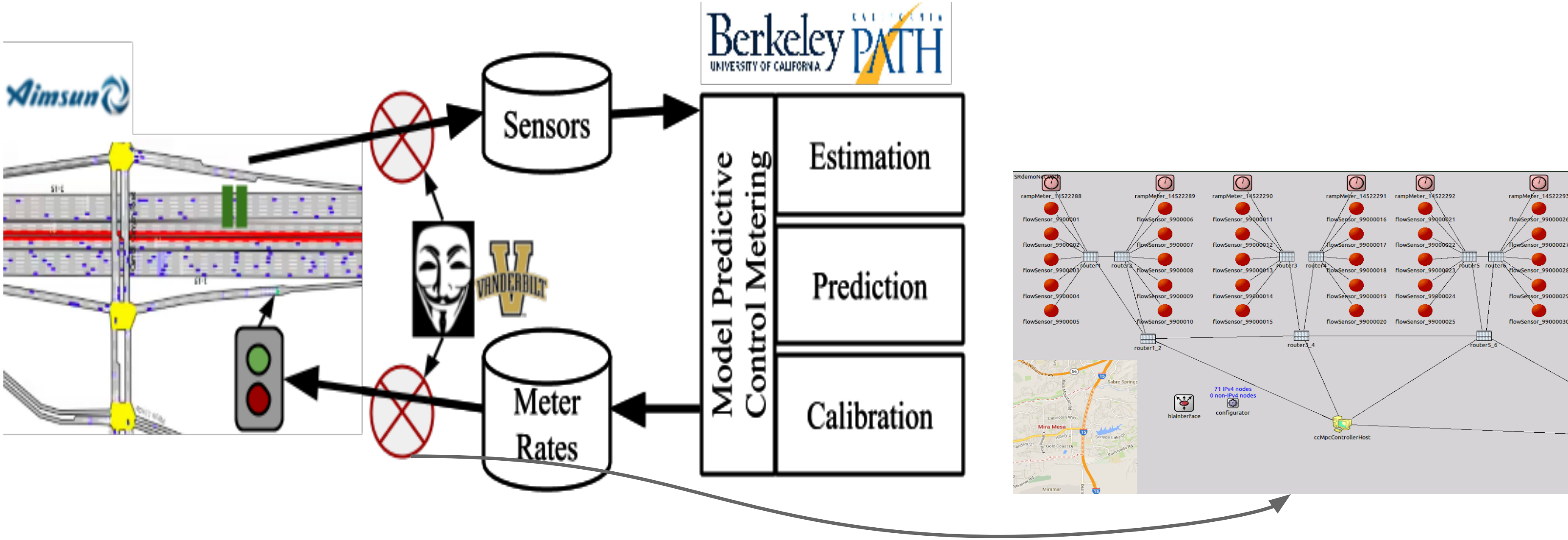
Direct Control



Indirect Control



SmartRoads project



SmartRoads

C2WindTunnel

Reilly, J., Martin, S., Payer, M., Song, D., & Bayen, A. M. (2014). On Cybersecurity of Freeway Control Systems: Analysis of Coordinated Ramp Metering Attacks. *Transportation Research Part B - Methodological (under Review)*.

Indirect Control: Sensor Spoofing

Direct Control: High-level Objectives

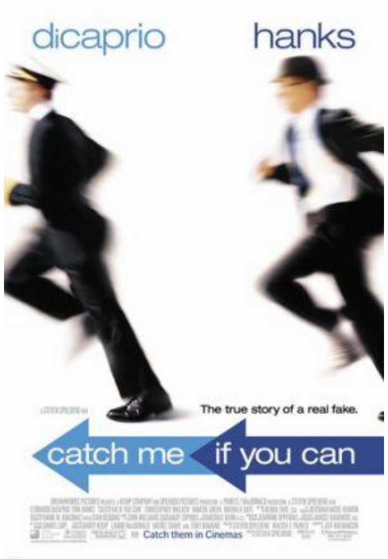
f_1 — Maximize Congestion Behind Leo.

f_2 — Maximize Hanks' Travel Time

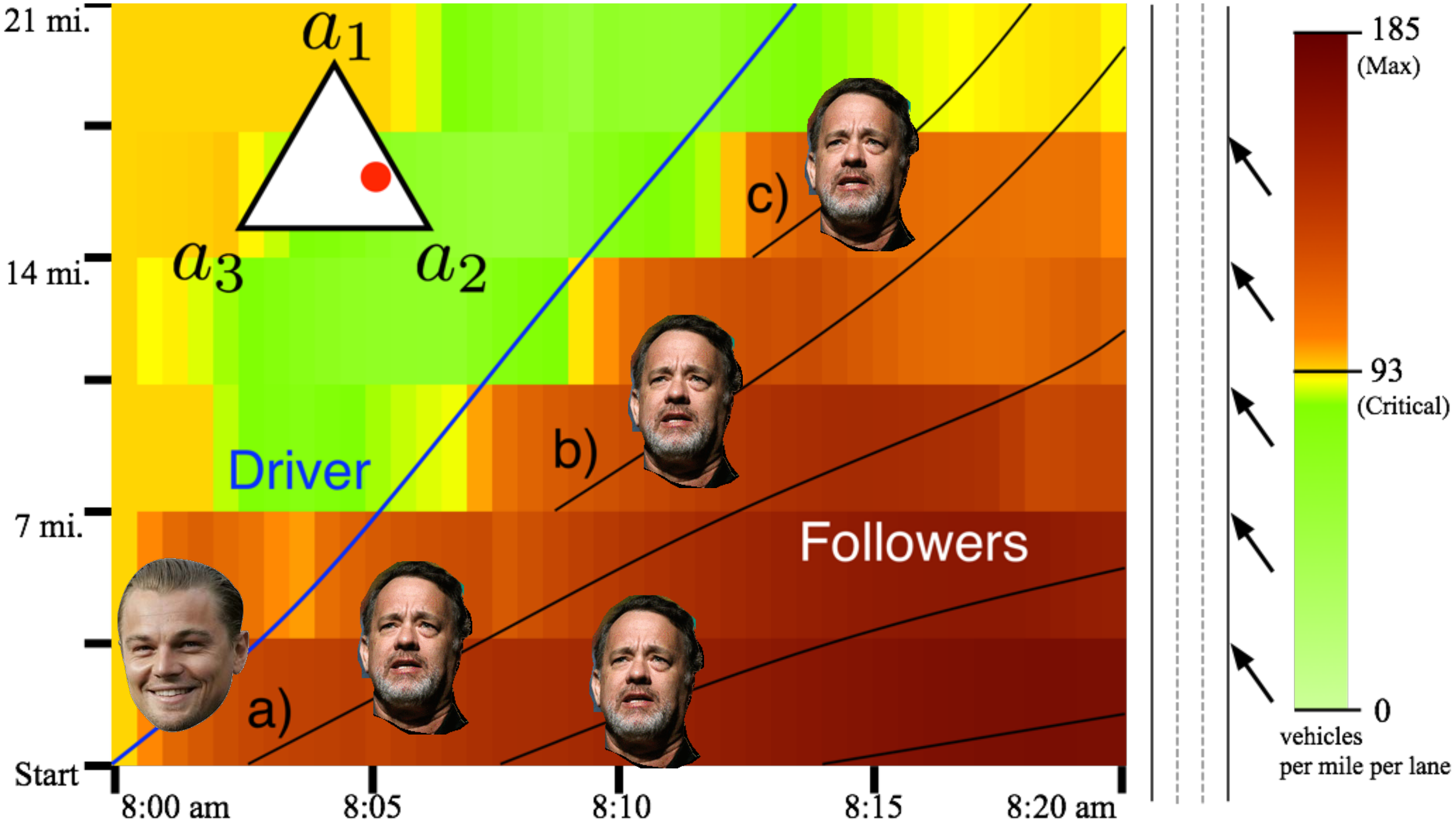
f_3 — Minimize Detection (Min TTT)

f_4 — Minimize Leo's Travel Time.

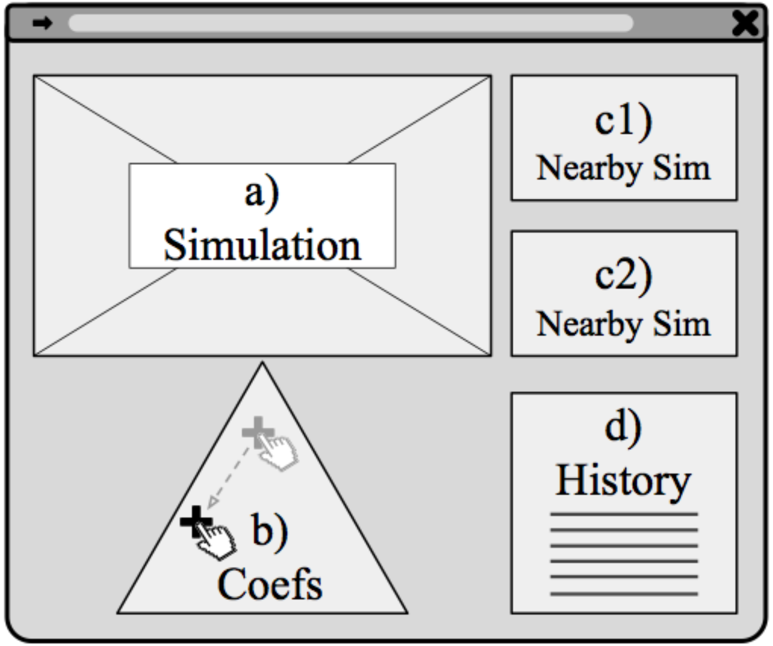
$$\sum_i a_i f_i$$



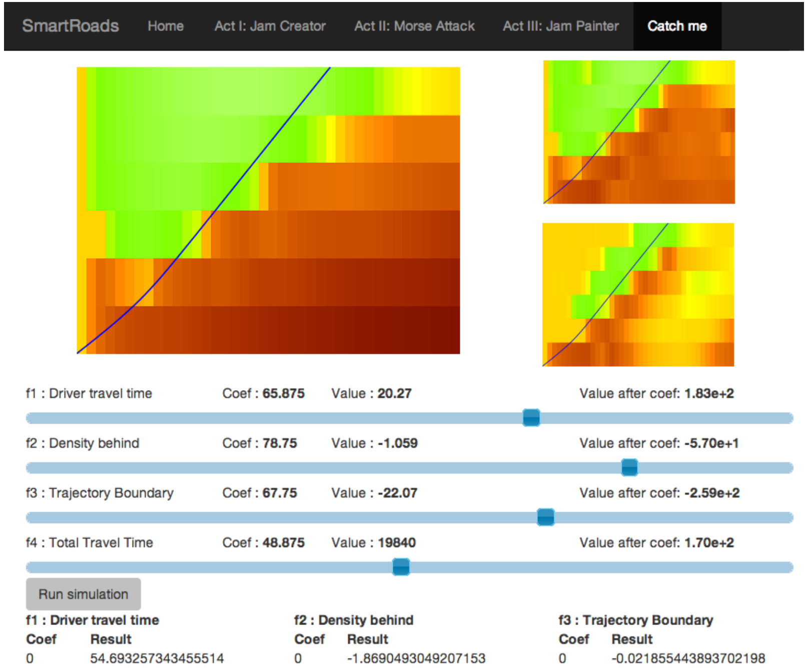
CATCH ME IF YOU CAN



Achieving high-level objectives via Multi-objective Optimization

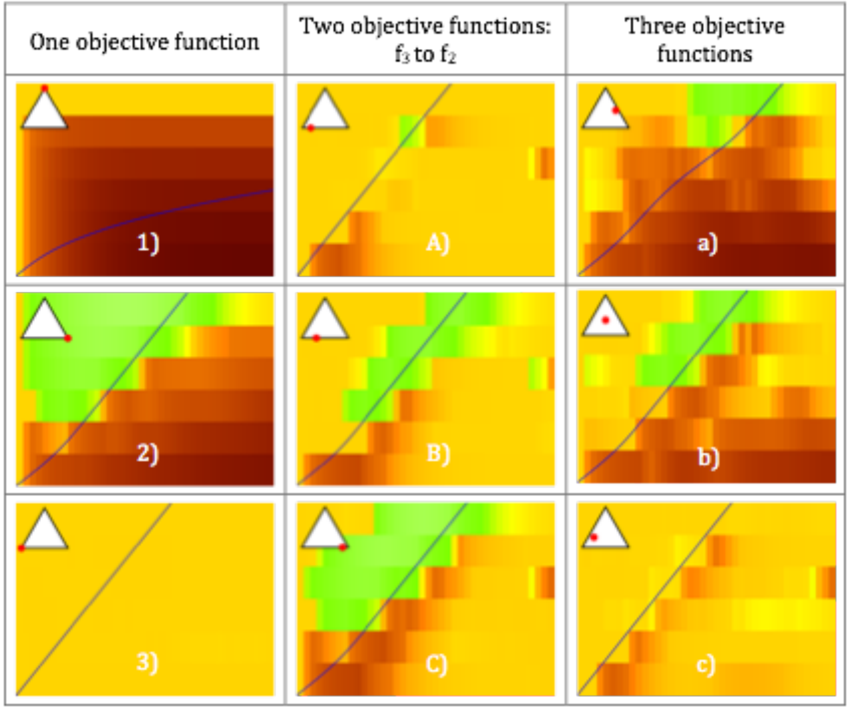


UI Diagram

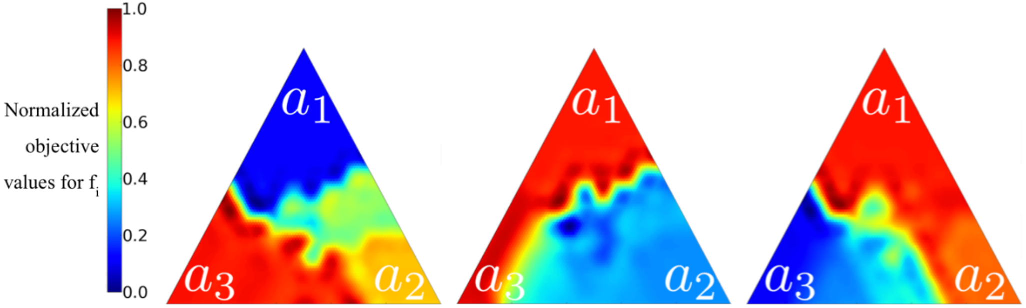


Actual Slider Implementation

Interactive vs. A Posteriori Optimization



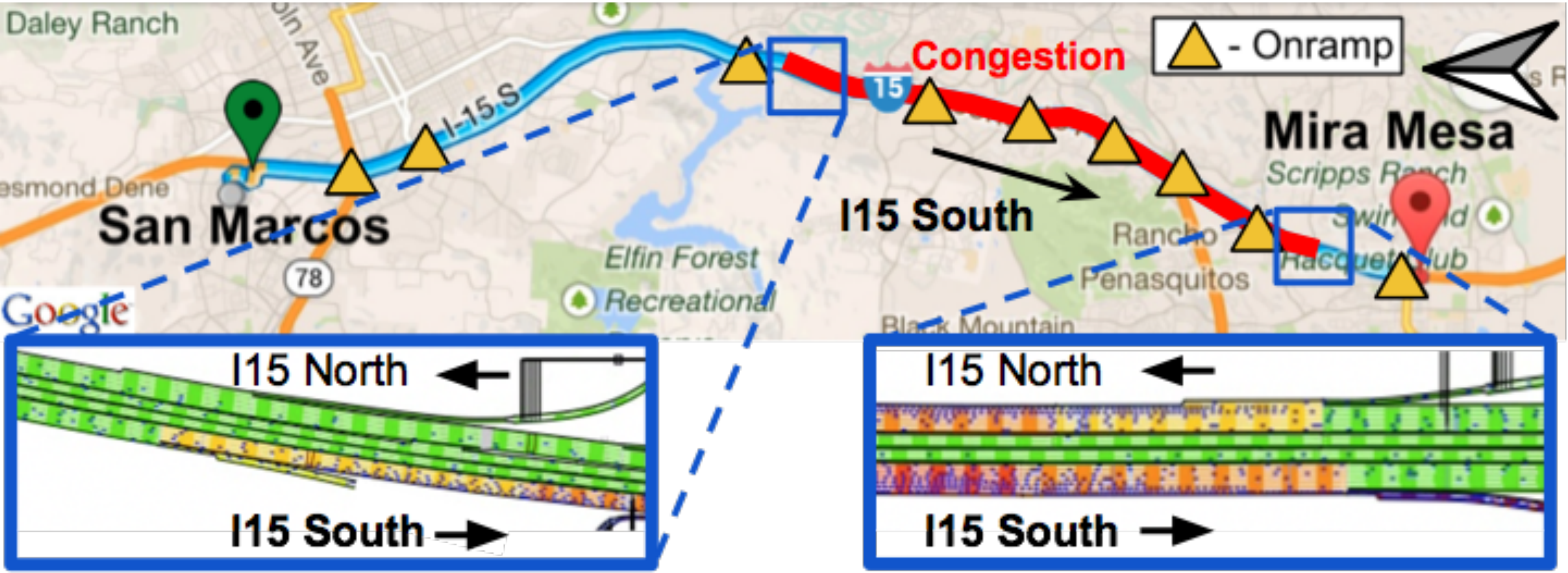
Interactive



(b) Scaled values of f_1 (c) Scaled values of f_2 (d) Scaled values of f_3

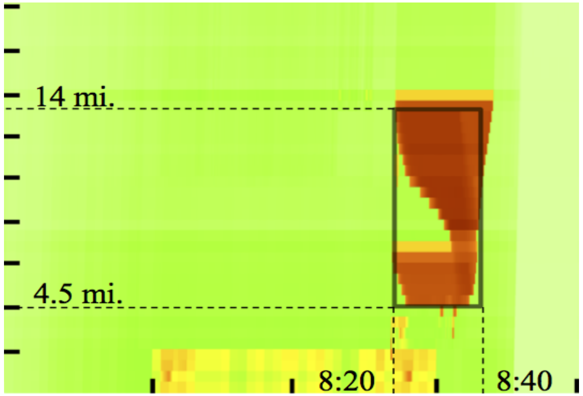
A posteriori

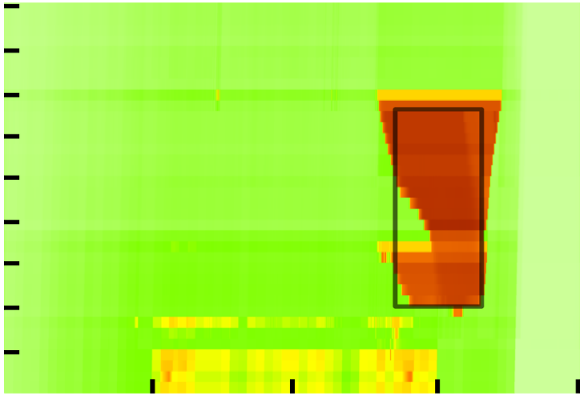
Box Objective on I15 Freeway

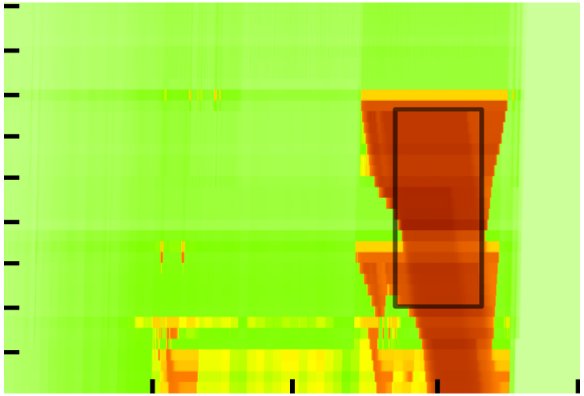


Box Objective

$$J = (1-\alpha)TTT_{\text{out of box}} - \alpha TTT_{\text{in box}}$$

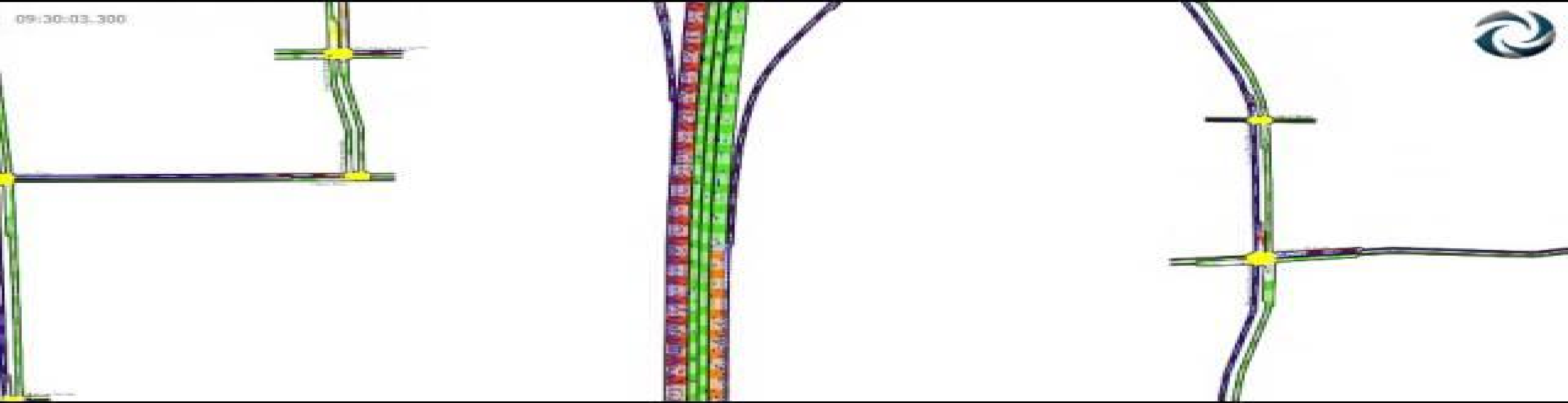




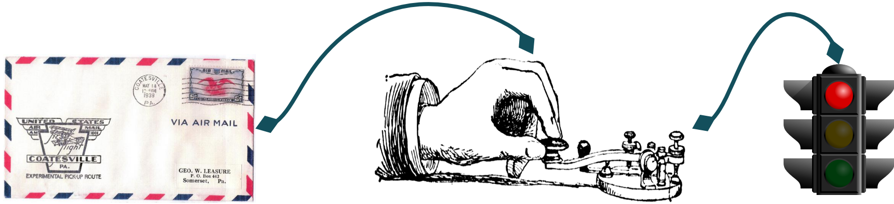


$\alpha = .3$ $\alpha = .5$ $\alpha = .9$

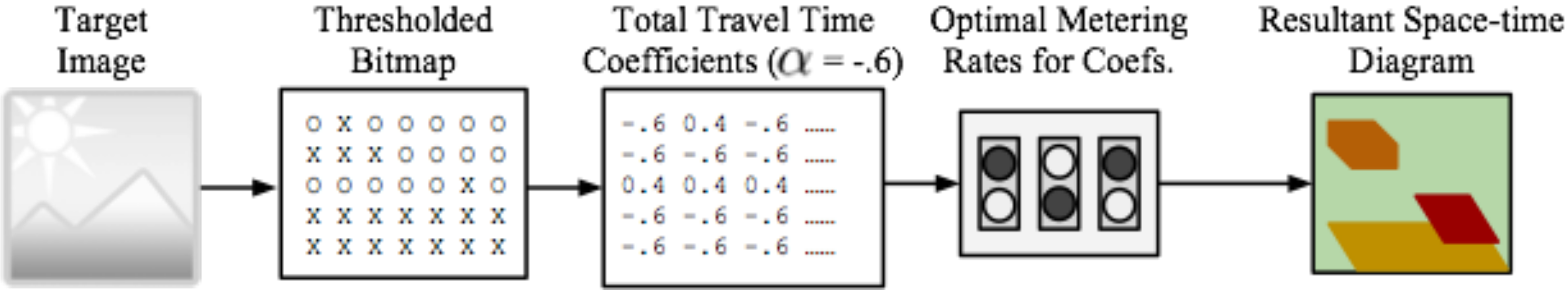
SmartRoads Box Objective



Morse Code Attack



Freeway Painter

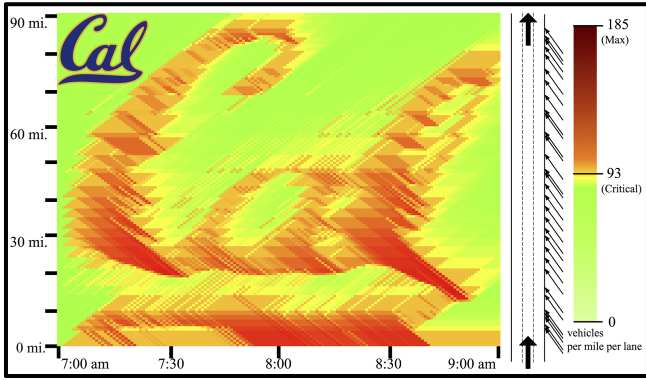


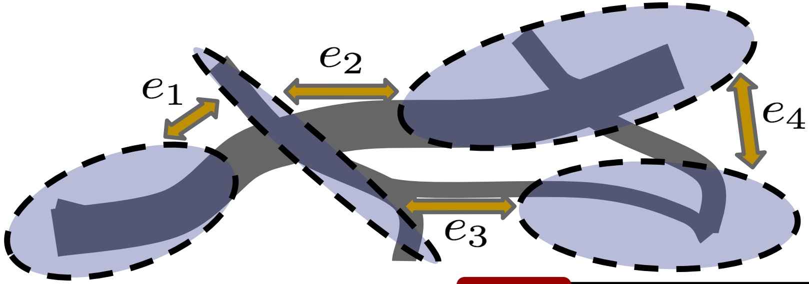
Conclusions

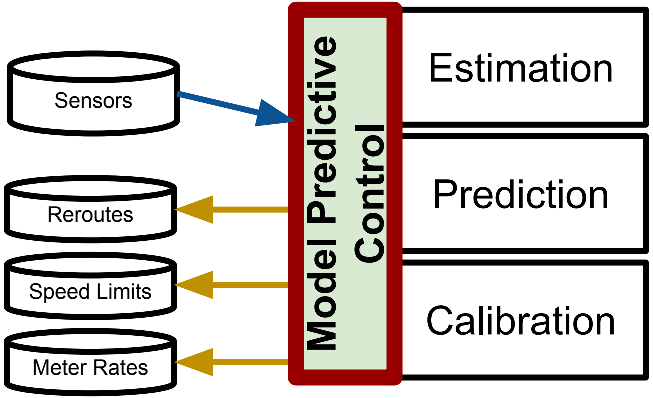
Real-world application and robustness

General and extensible framework

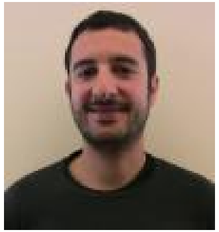
Improves w/ estimation and prediction advances.

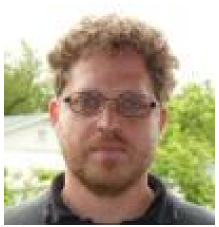






Acknowledgments





Thank you for listening! Questions?