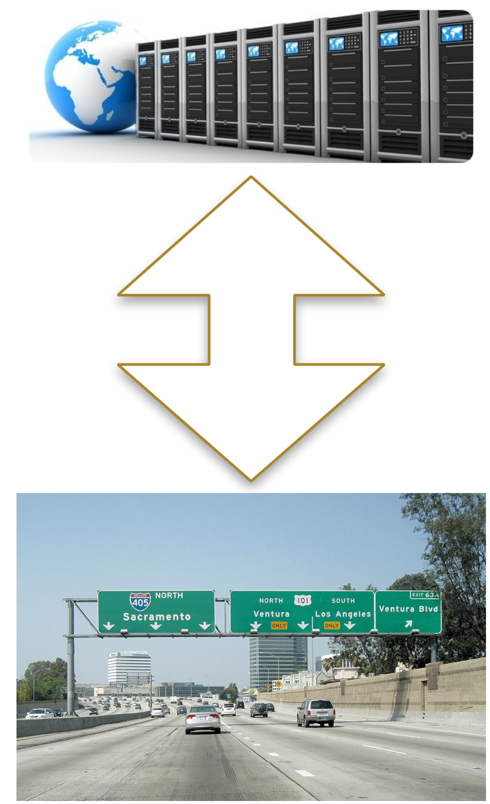
Traffic Control Systems Security: Coordinated Ramp Metering Attacks

Jack Reilly
Work with Professor Alexandre Bayen
Sebastien Martin
Mathias Payer

Overview of Talk

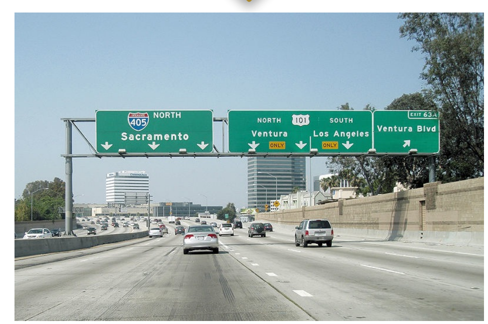
- Traffic Control Infrastructure
  - Actual Attack Examples
- SmartRoads: Traffic/Cybersecurity Testbed
- Coordinated Ramp Metering Attacks
  - Optimal Control
  - Multi-objective Optimization
- **Attack Examples**
  - Aiding a fleeing vehicle
  - Creating precise congestion patterns



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

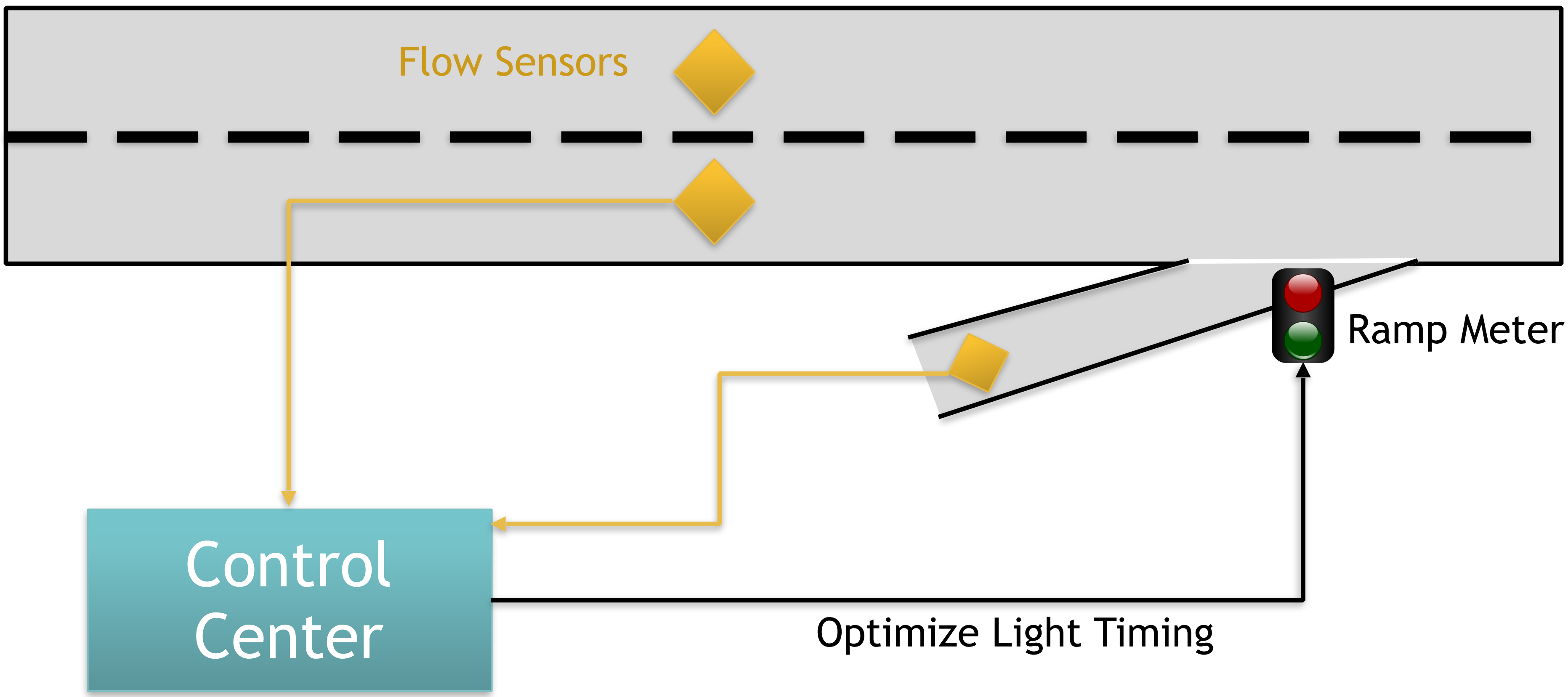
SmartRoads: Cyber-physical Security on Traffic Networks

- 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 wild.
- Potential attack vectors numerous:
  - Broadcasting fake accident reports
  - Compromise of **<u>metering light network.</u>**
- **<u>Resiliency to attack</u>** through fault detection and modeling/sensing discrepancies.



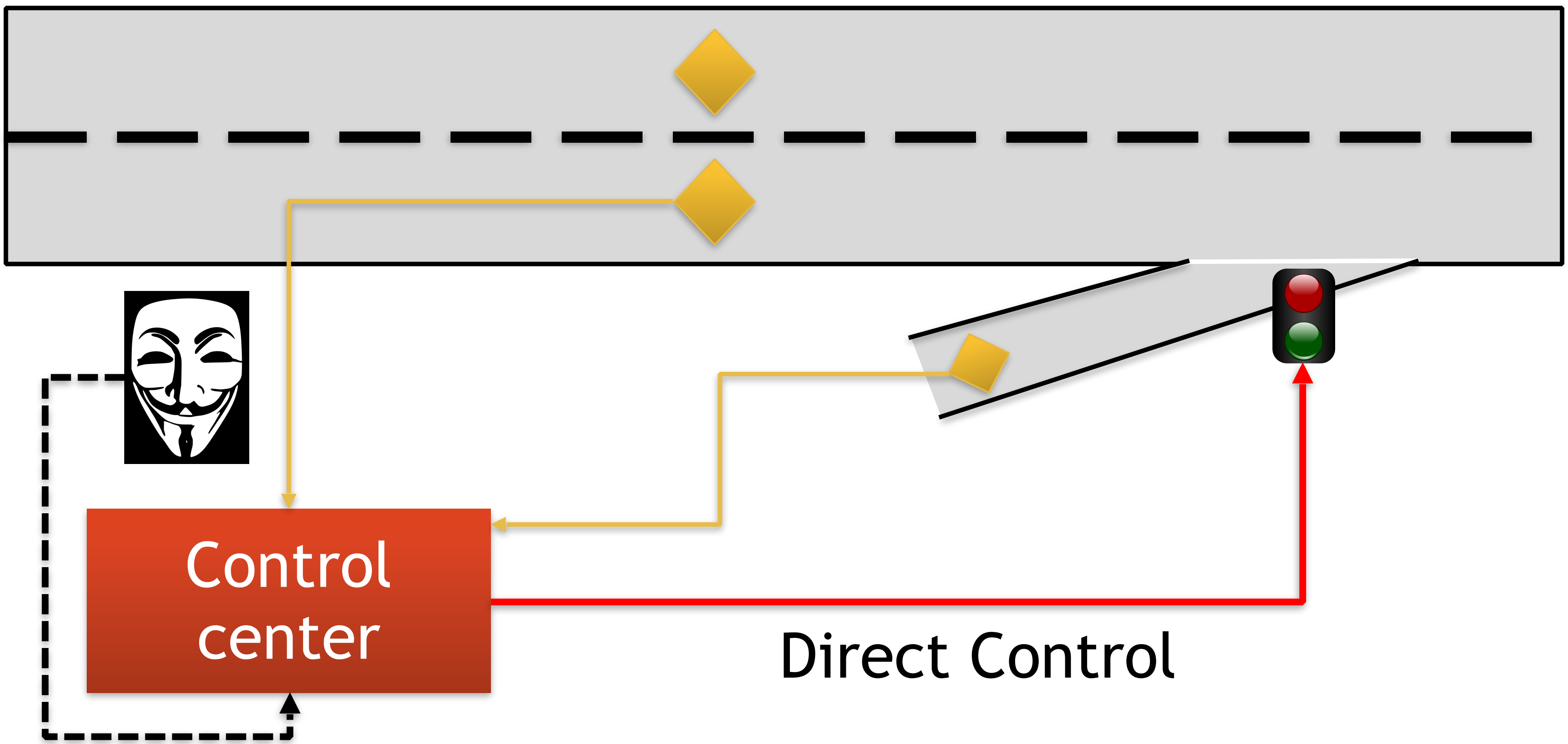
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Freeway Traffic systems

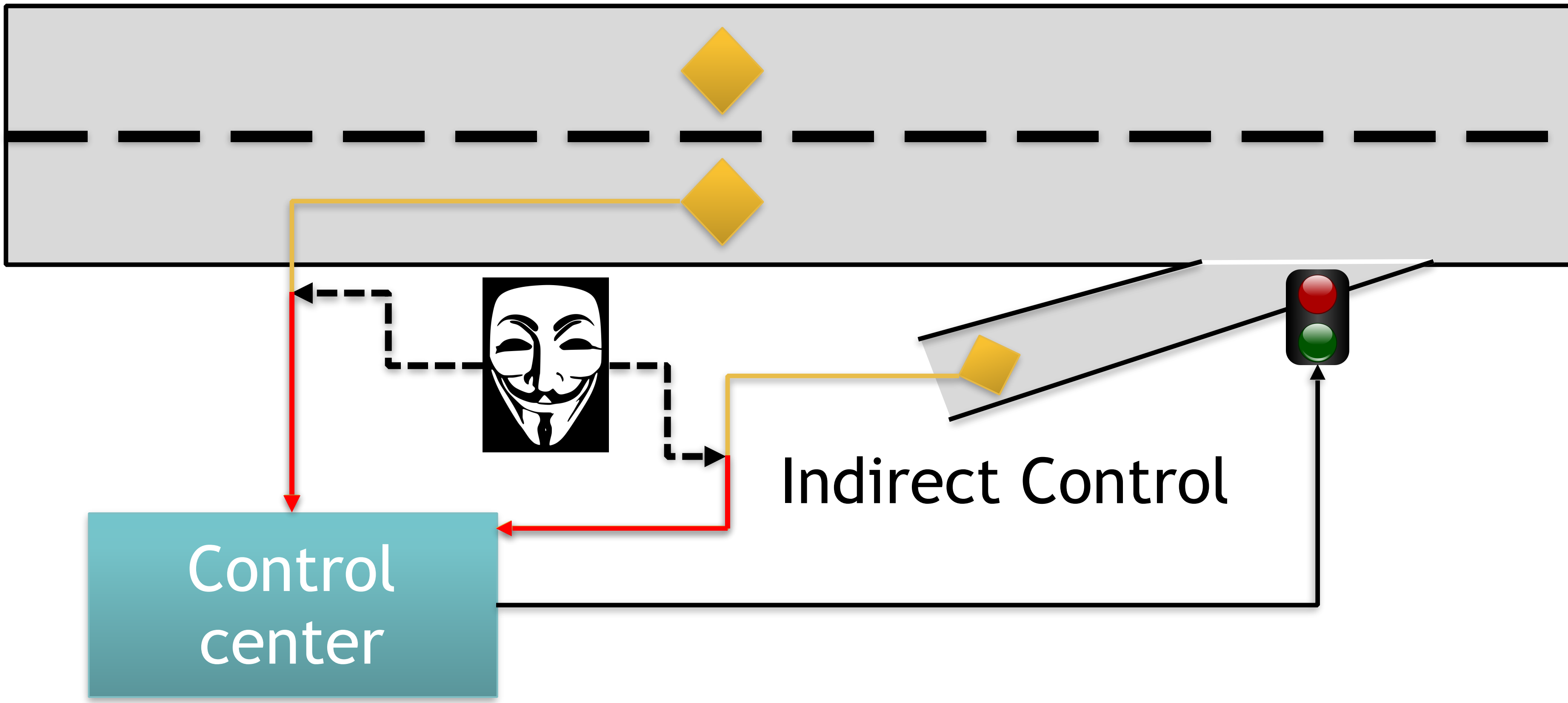


Berkeley
UNIVERSITY OF CALIFORNIA

Compromise : complete takeover

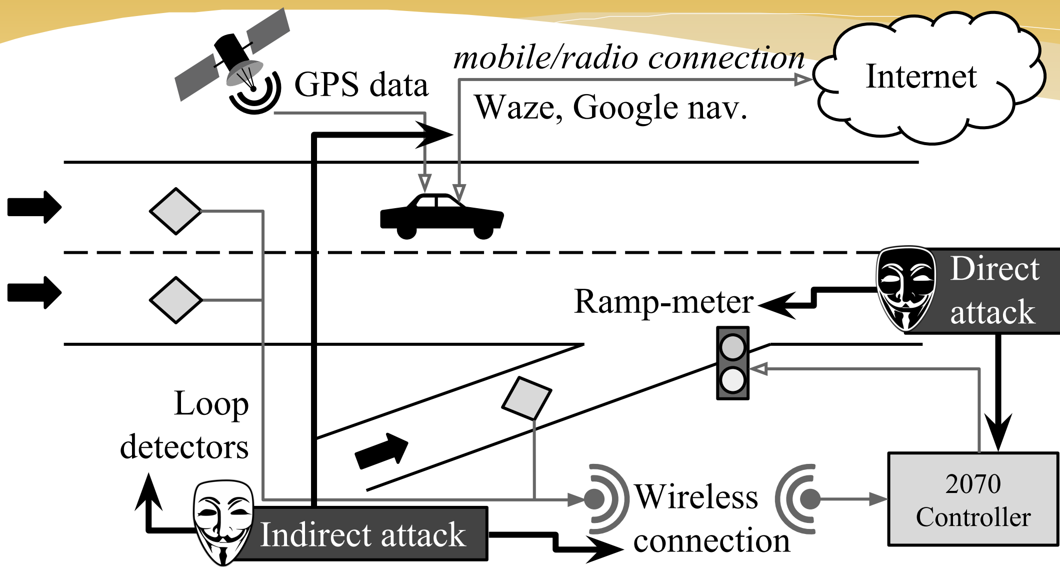


Compromise : spoofing the sensors

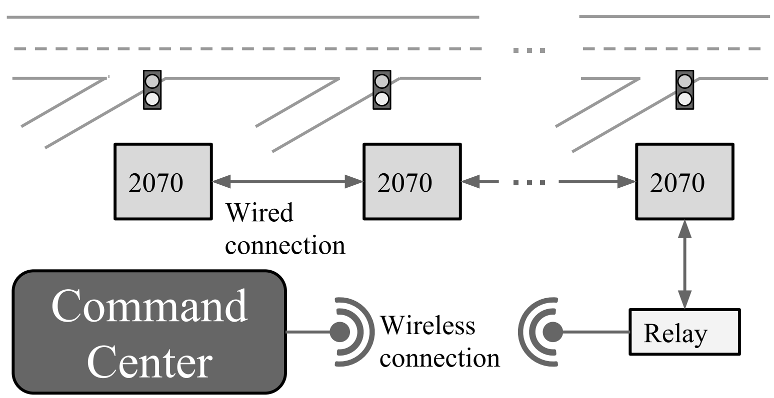


Berkeley
UNIVERSITY OF CALIFORNIA

Vulnerability Points



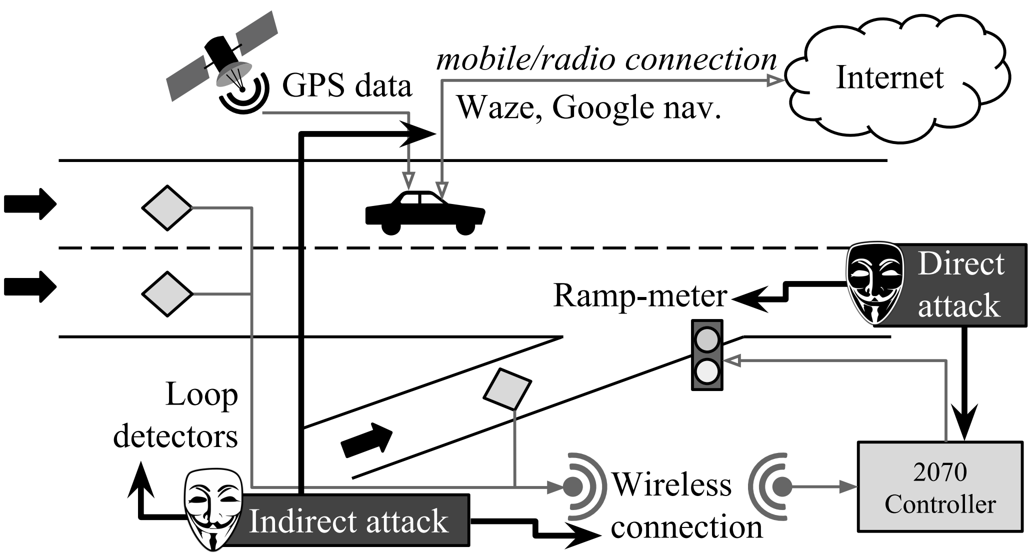
Local Architecture

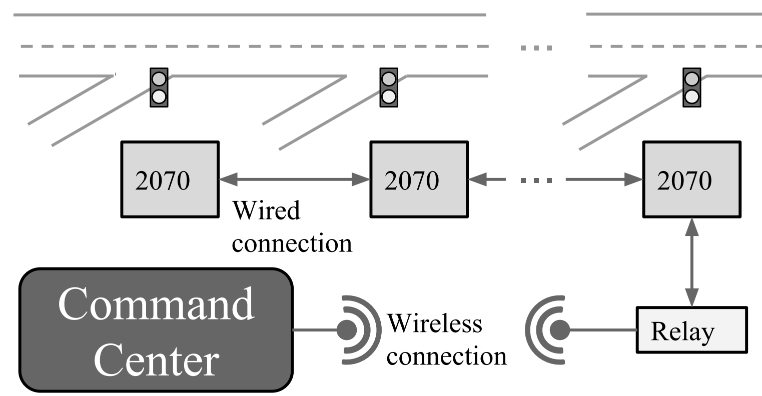


Networked Meters

Vulnerability Points Taxonomy

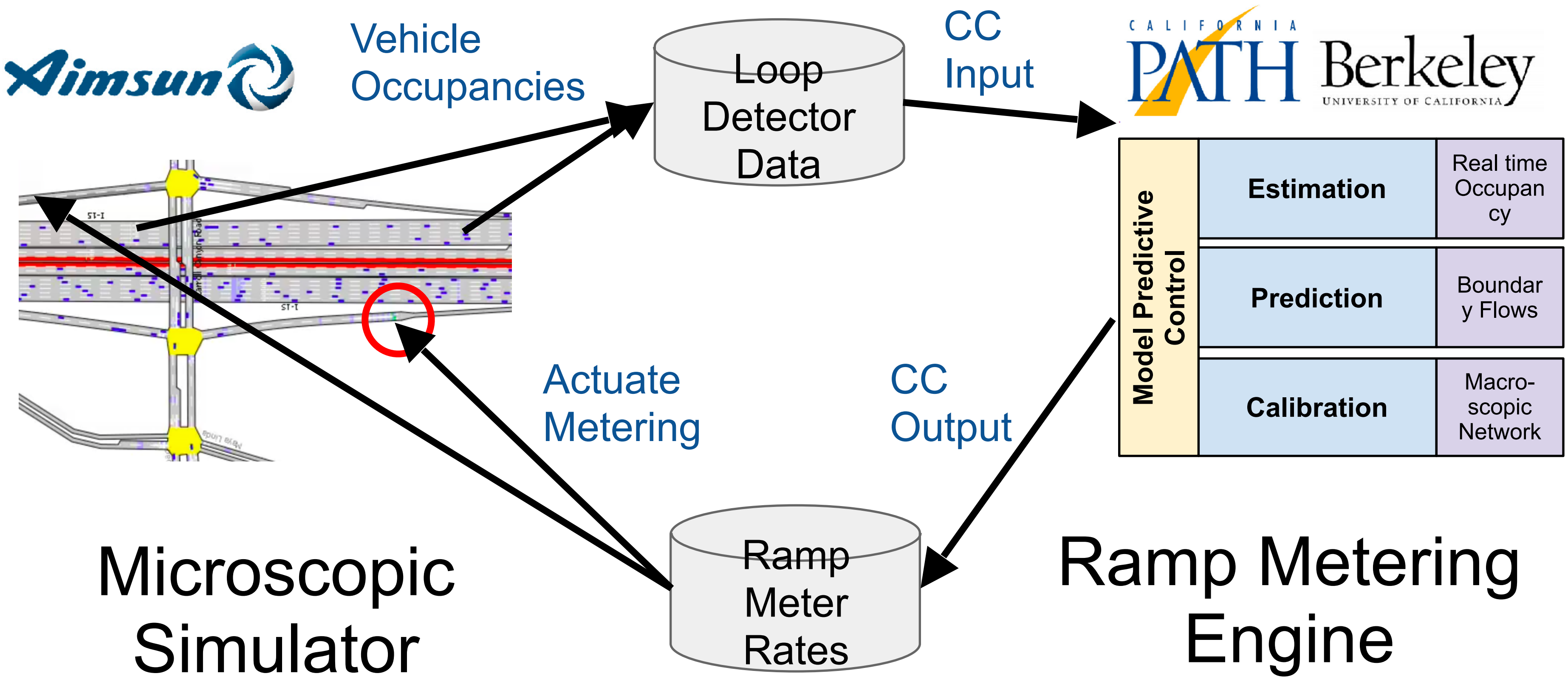
Attack Description	Access	Control	Complexity	Cost
copper theft/clipping wires	physical	low	low	low
replacing a single sensor/actuator	physical	low	low	low
attacking a single sensor/actuator	locality	low	medium	low
replacing a single control box	physical	medium	medium	medium
replacing a set of sensors/actuator	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



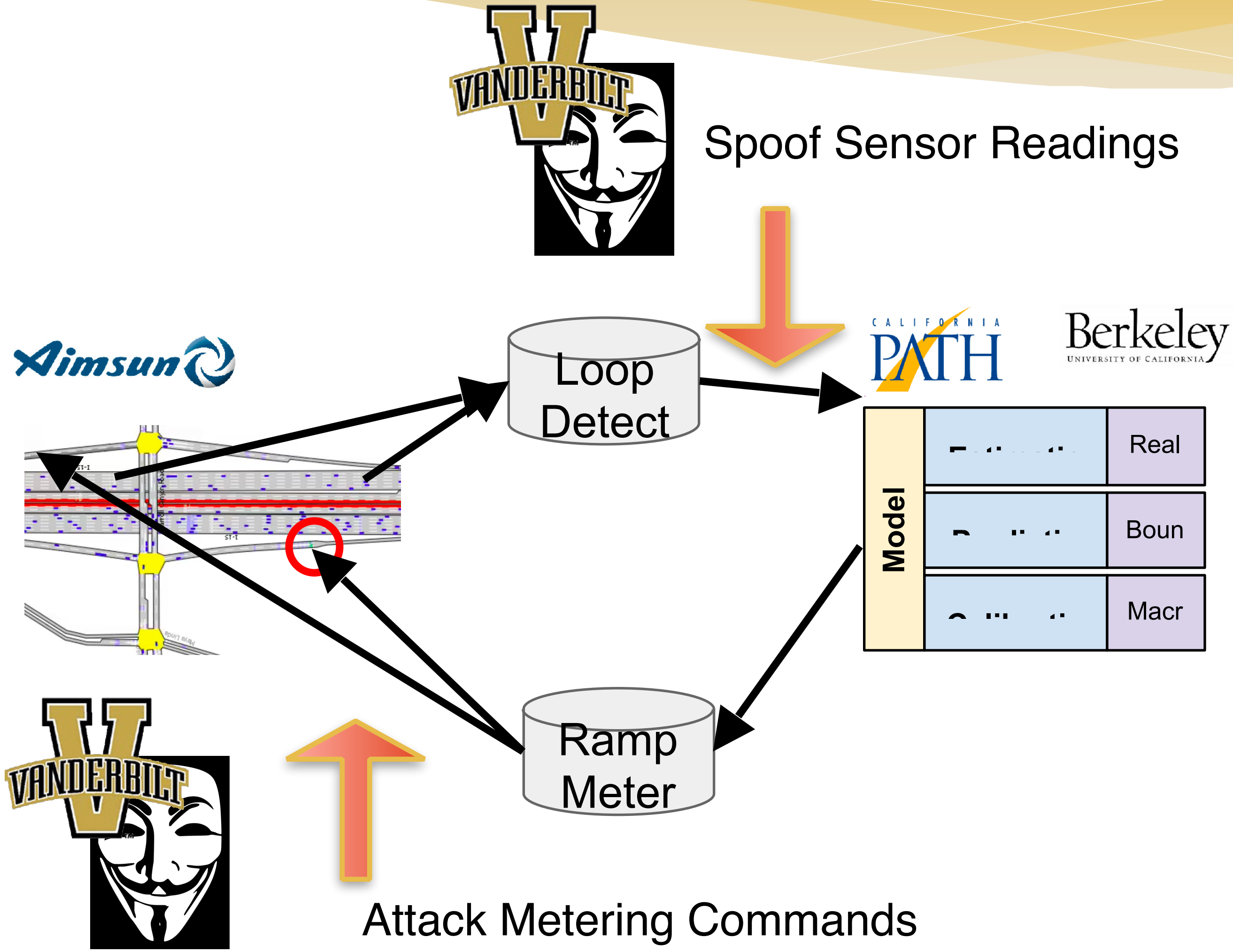


Berkeley
UNIVERSITY OF CALIFORNIA

SmartRoads Architecture

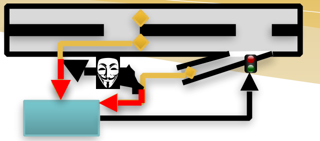


SmartRoads Architecture



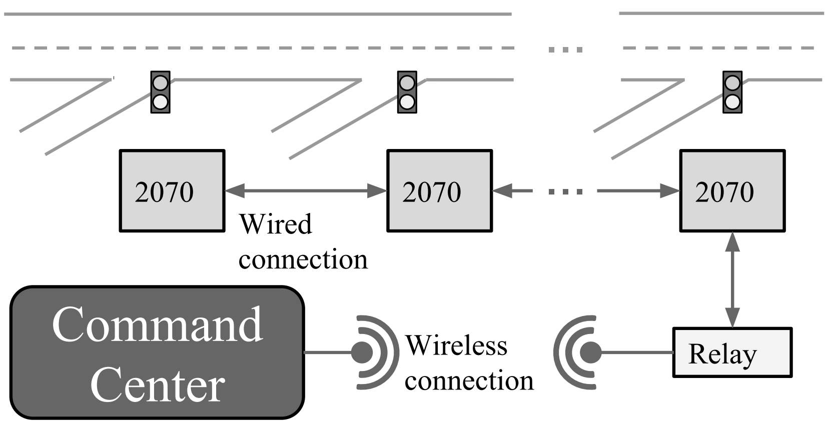
Berkeley
UNIVERSITY OF CALIFORNIA

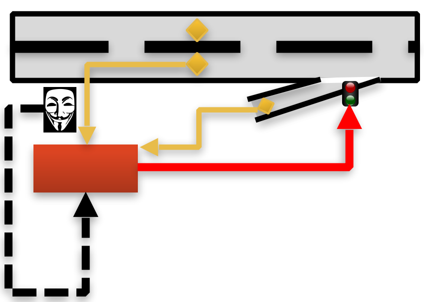
SmartAmerica Scenario



Berkeley
UNIVERSITY OF CALIFORNIA

Coordinated Ramp Metering Attacks





MAXIMIZE Attack Objective

Create Jam between Exits 4-6

+

Achieve Free-flow Otherwise
(Stealthy Attack, avoid detection)

+

Limit Onramp Queue Sizes

SUBJECT TO Traffic Dynamics

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

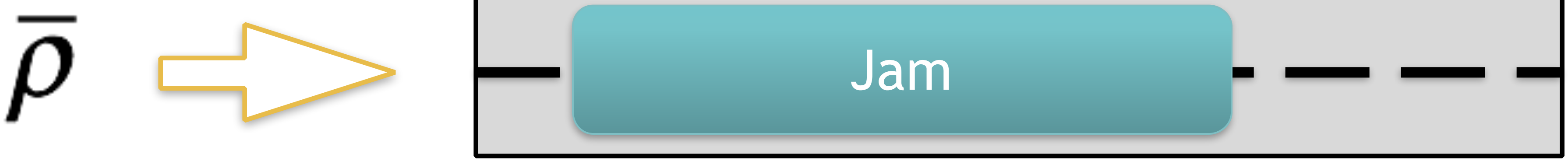
Berkeley
UNIVERSITY OF CALIFORNIA

Finite Horizon Optimal Control Formulation

- Discretize continuous PDE dynamics (Godunov's method)

$$H_{i,t} = \rho_{i,t} - \rho_{i,t-1} + \frac{\Delta t}{\Delta x}\left(f^{\text{in}}{}_{i,t-1} - f^{\text{out}}{}_{i,t-1}\right) = 0$$

- **Objective:** State tracking $\min_{u \in U} J = \sum_i \sum_t \| \rho_{i,t} - \bar{\rho}_{i,t} \|$



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

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

Berkeley
UNIVERSITY OF CALIFORNIA

Finite-horizon Optimal Control Problem

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

subject to system dynamics:

$$\begin{aligned}\rho_{i,0} =& \rho_i^0\\ \rho_{i,t+1} =& \rho_{i,t} + \frac{\triangle t}{\triangle x}\left(G\left(\rho_{i-1,t},\rho_{i-1,t},u_{i,t}\right) - \right.\\ & \left. G\left(\rho_{i,t},\rho_{i+1,t},u_{i,t}\right)\right)\\ & \forall i \in [1,N], \forall t \in [1,T]\end{aligned}$$

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

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

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

* Performing gradient descent w/ finite-differences i<u>**nfeasible for large networks!**</u>

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

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

Coordinated Freeway Control using **Adjoint** Methods

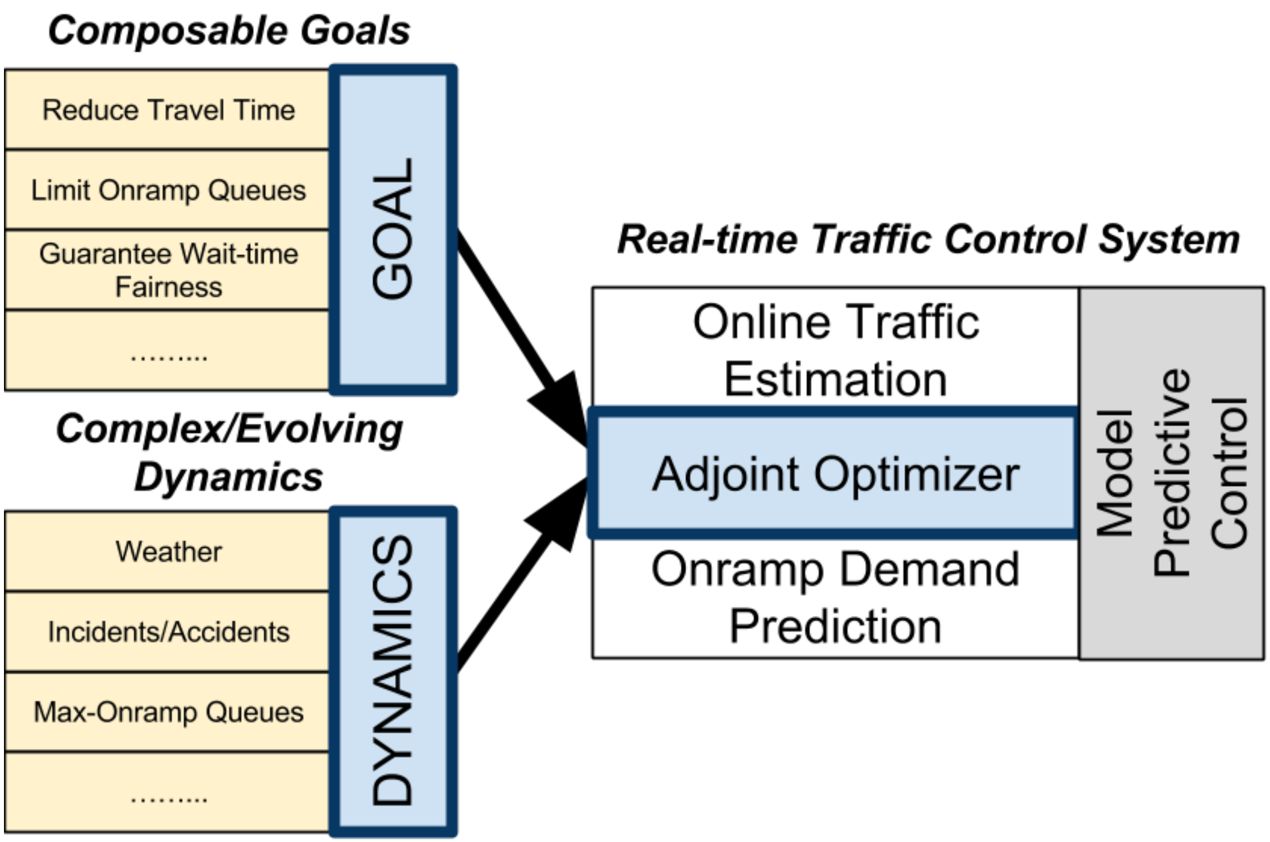
Composable Goals

	GOAL
Reduce Travel Time	
Limit Onramp Queues	
Guarantee Wait-time Fairness	
………	

Complex/Evolving Dynamics

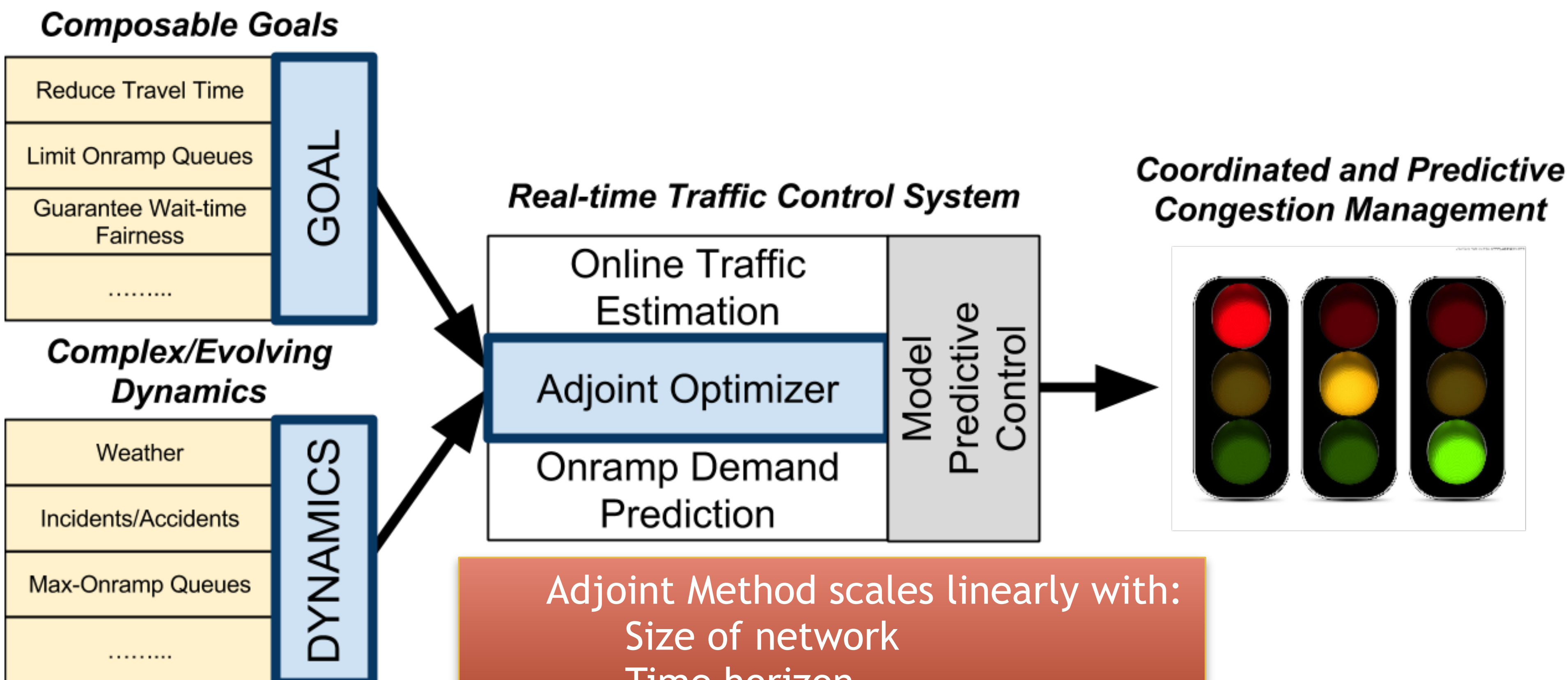
	DYNAMICS
Weather	
Incidents/Accidents	
Max-Onramp Queues	
………	

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

Gradient Descent

* Compute gradient of constrained problem via ***adjoint***

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

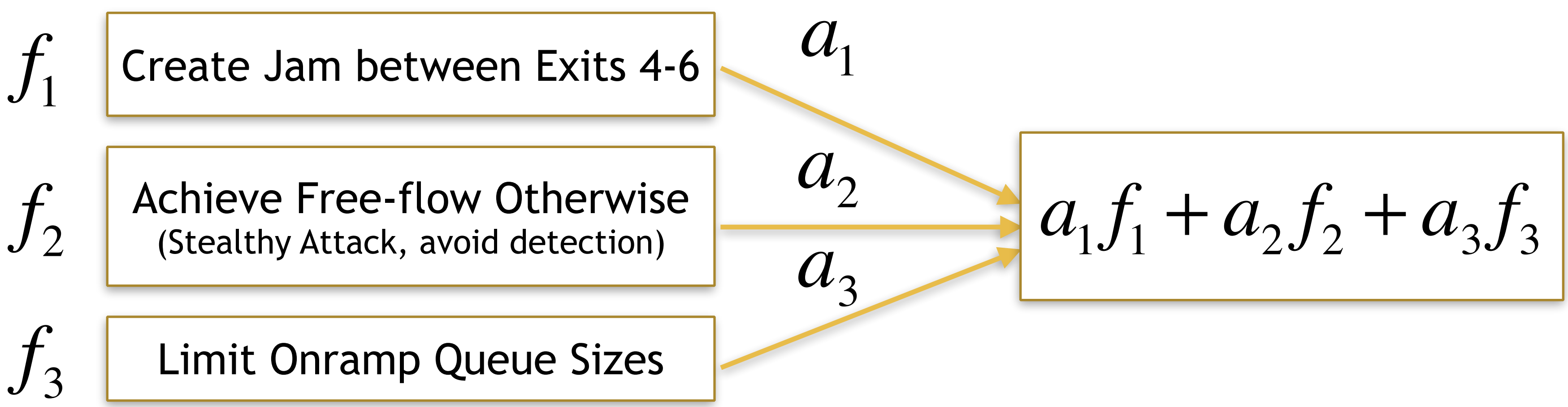
$$\nabla_{\mathbf{u}} J = J_u + \lambda^T H_u$$
$$\text{s.t. } H_\rho^T \lambda = -H_u^T$$

* Embed within gradient descent loop:
  * 1) Compute new state $\rho^k : H(\rho^k, u^k) = 0$ *[forward sim]*
  * 2) Compute gradient $\nabla_u J(\rho^k, u^k)$
  * 3) Update $u^{k+1} = f(u^1, \ldots, u^k, \nabla_u J^k)$ *[e.g. L-BFGS]*
  * 4) Loop $k \leftarrow k+1$

Berkeley
UNIVERSITY OF CALIFORNIA

Multi-objective Optimization for Attacks

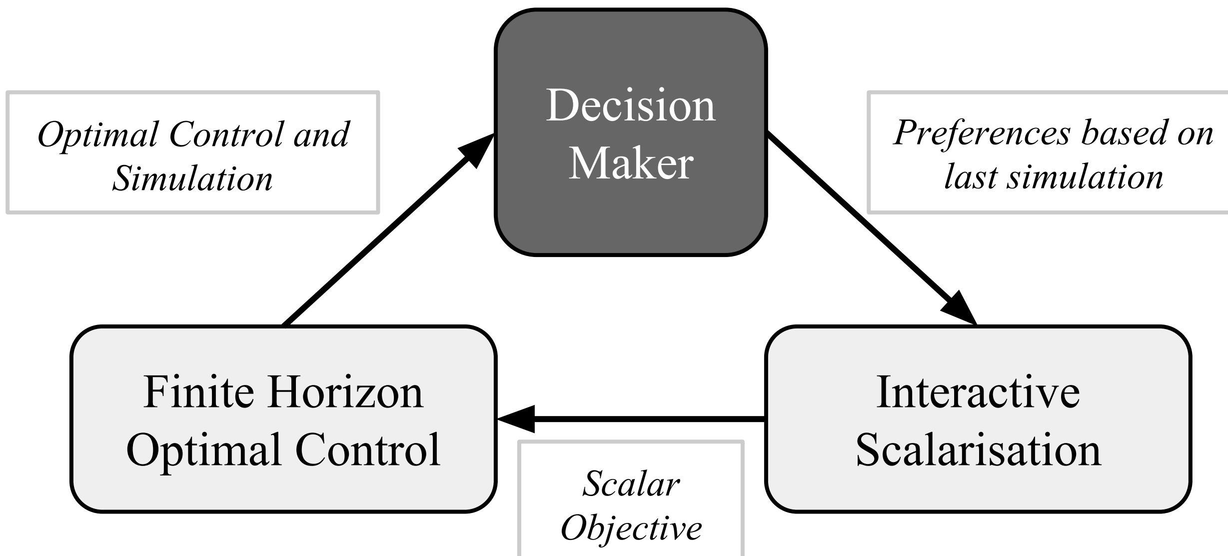
- **Goal:** Achieve success on many conflicting goals simultaneously
- **Solution:** Scalarization
  - Objective -> linear combination of sub-objectives.



Berkeley
UNIVERSITY OF CALIFORNIA

Interactive Optimization

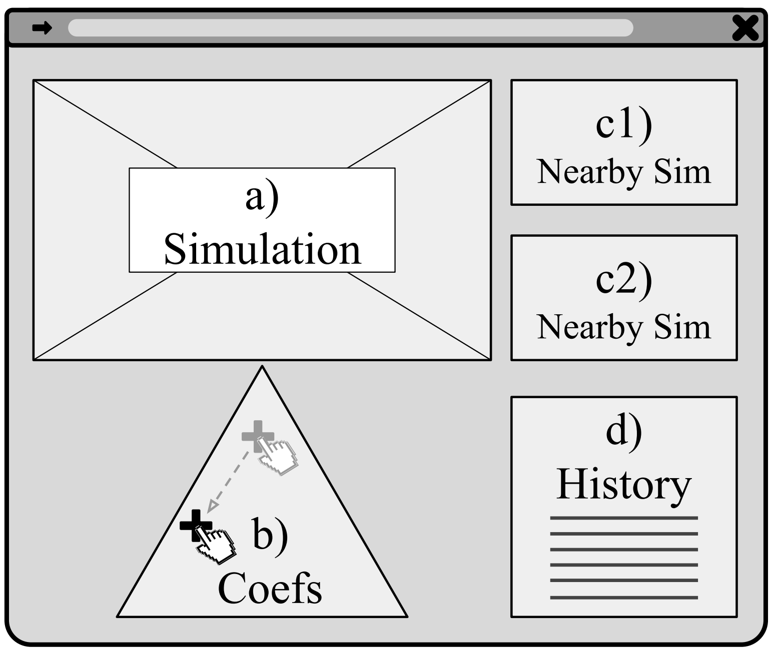
* Use human expertise to find proper a_i coefficients **during** exploration

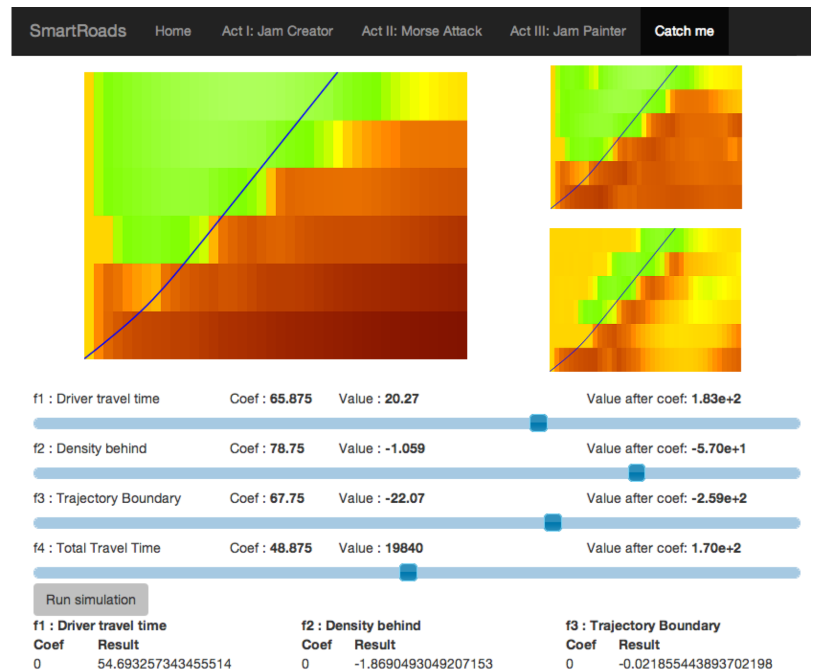


Berkeley
UNIVERSITY OF CALIFORNIA

Interactive Optimization

* Use human expertise to find proper a_i coefficients



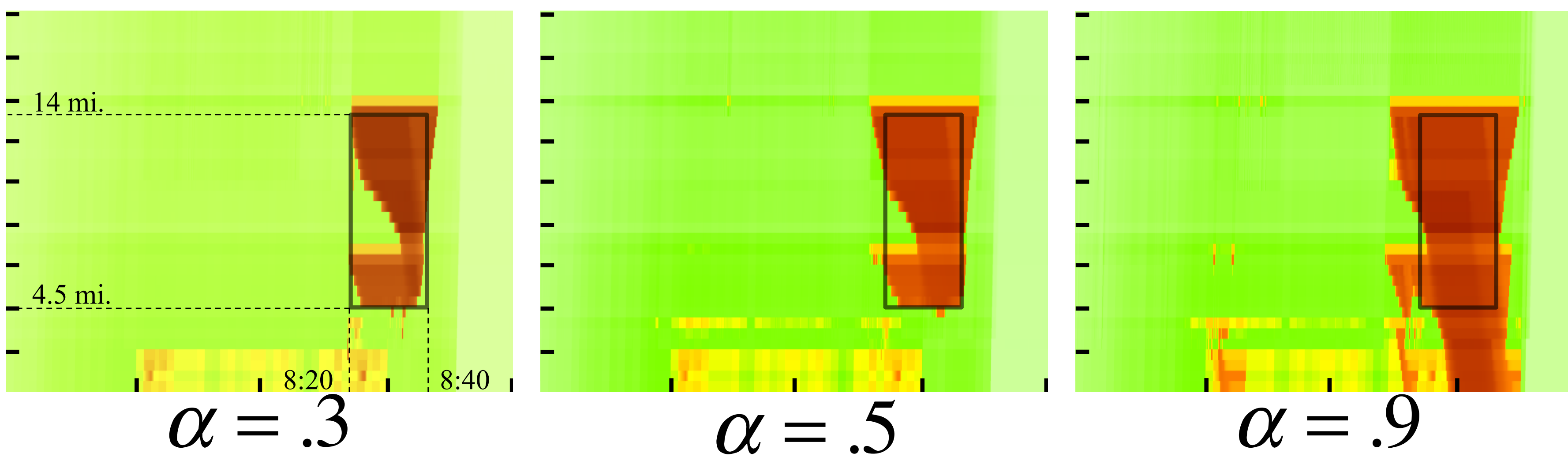


Berkeley
UNIVERSITY OF CALIFORNIA

Box Attack Sim: I15 Freeway in San Diego

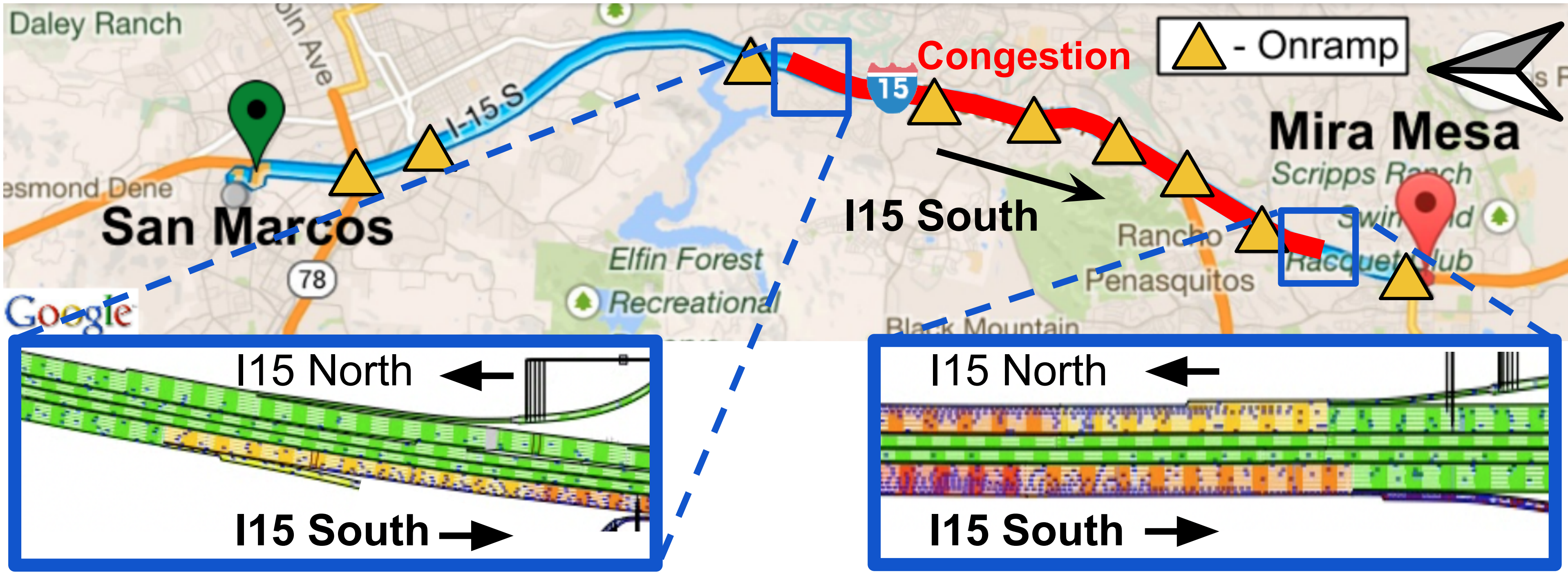
- Create isolated, precise jam over predetermined time.
- **Balance** between maximizing jam in "box" and minimizing free-flow outside box.

$$f = \alpha f_{\text{jam box}} + (1-\alpha) f_{\text{clear outside box}}$$



Berkeley
UNIVERSITY OF CALIFORNIA

Box Attack Sim: I15 Freeway in San Diego

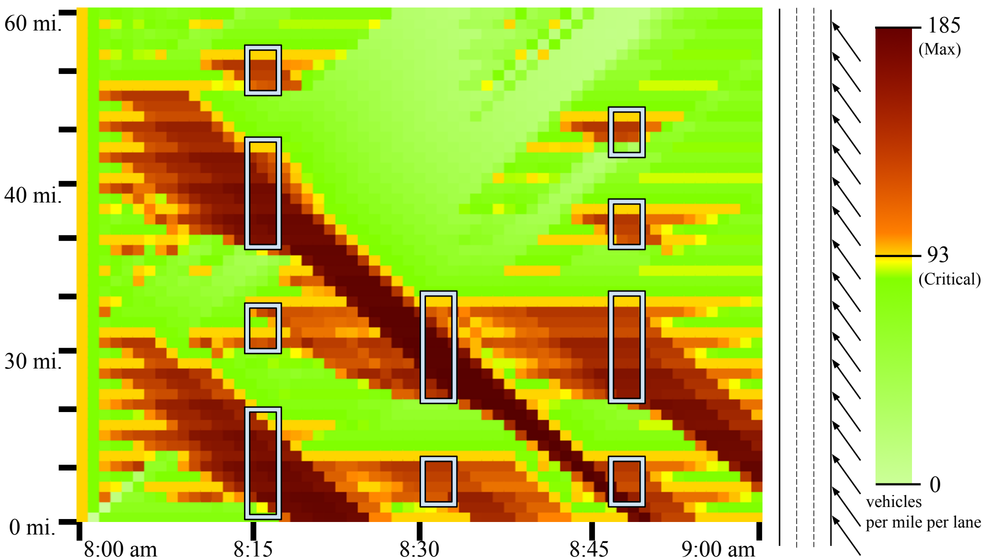


Berkeley
UNIVERSITY OF CALIFORNIA

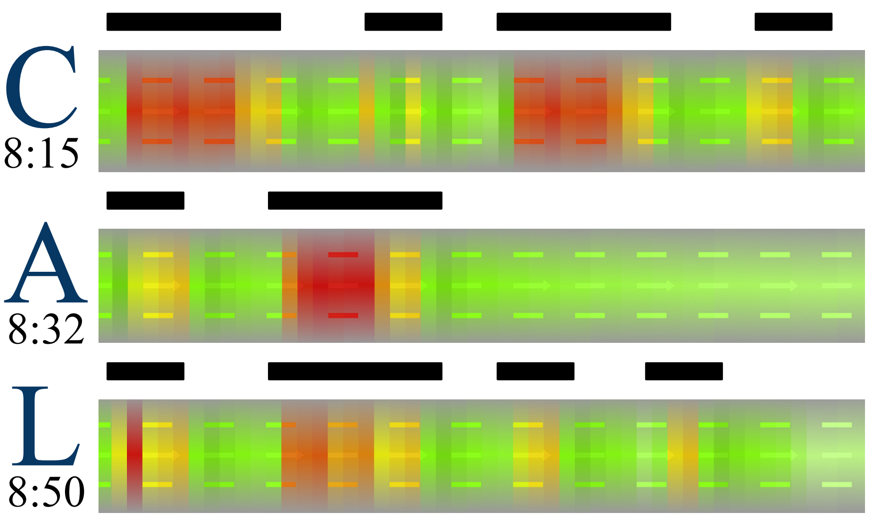
Box Attack Sim: I15 Freeway in San Diego

Morse Code Attack on the Freeway

- Use Box Objective is “building block” for more sophisticated attacks
- Example: Write Morse code on freeway with traffic jams



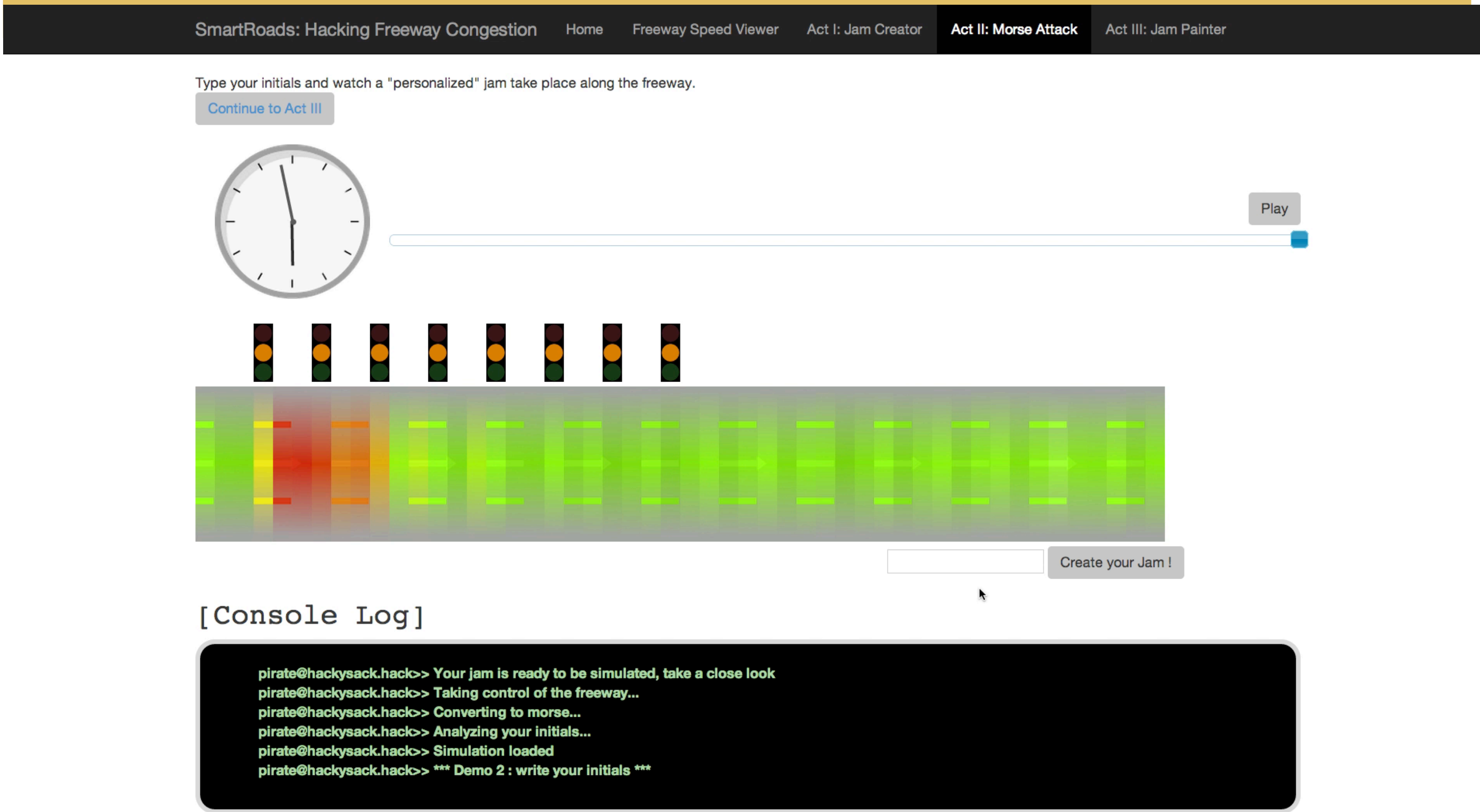
Space-time Diagram



Time Slices along Freeway

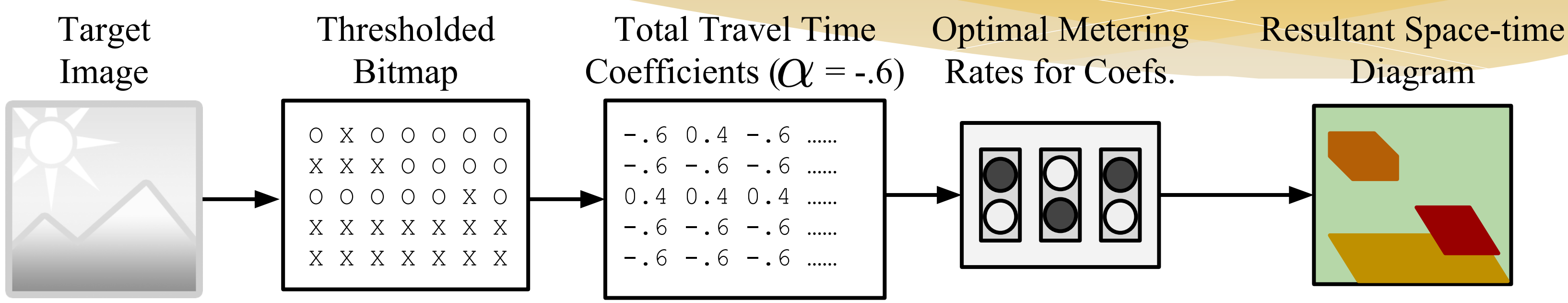
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Morse Code Attack on the Freeway



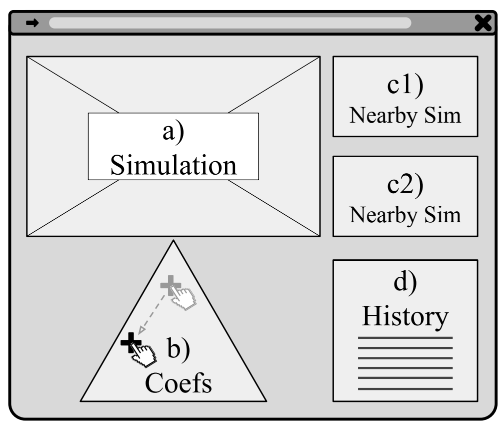
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Drawing Cal On the Freeway



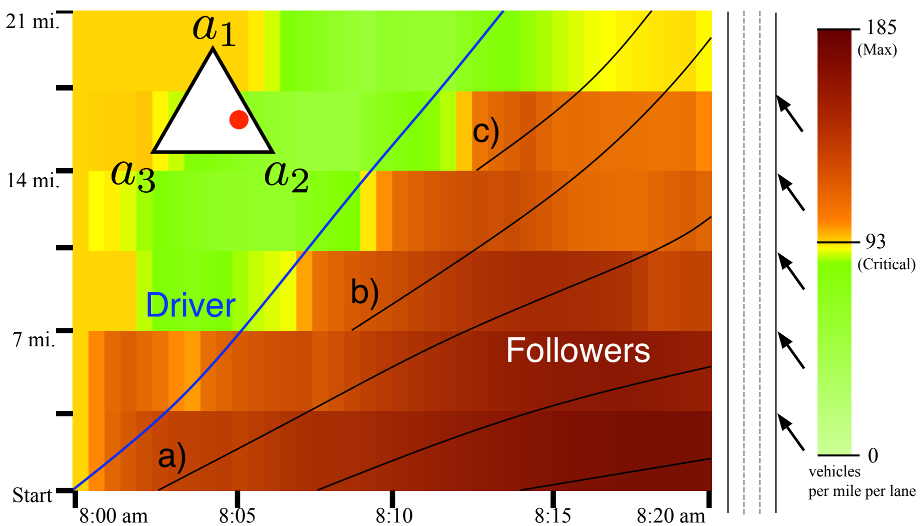
Attack Example: *CATCH ME IF YOU CAN*

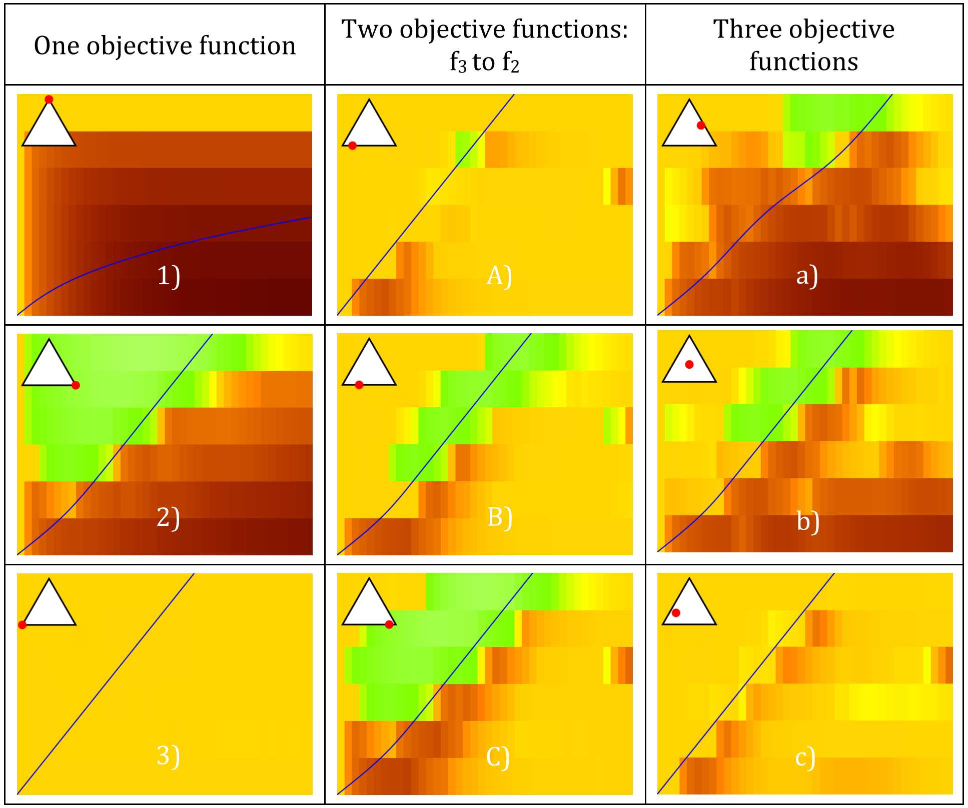
* Attacker wishes to escape vehicles chasing him.
* Three objectives:
  * f_1 Maximize congestion behind driver
  * f_2 Maximize speed change **directly** behind driver trajectory
  * f_3 Minimize travel time otherwise (avoid suspicion)



Berkeley
UNIVERSITY OF CALIFORNIA

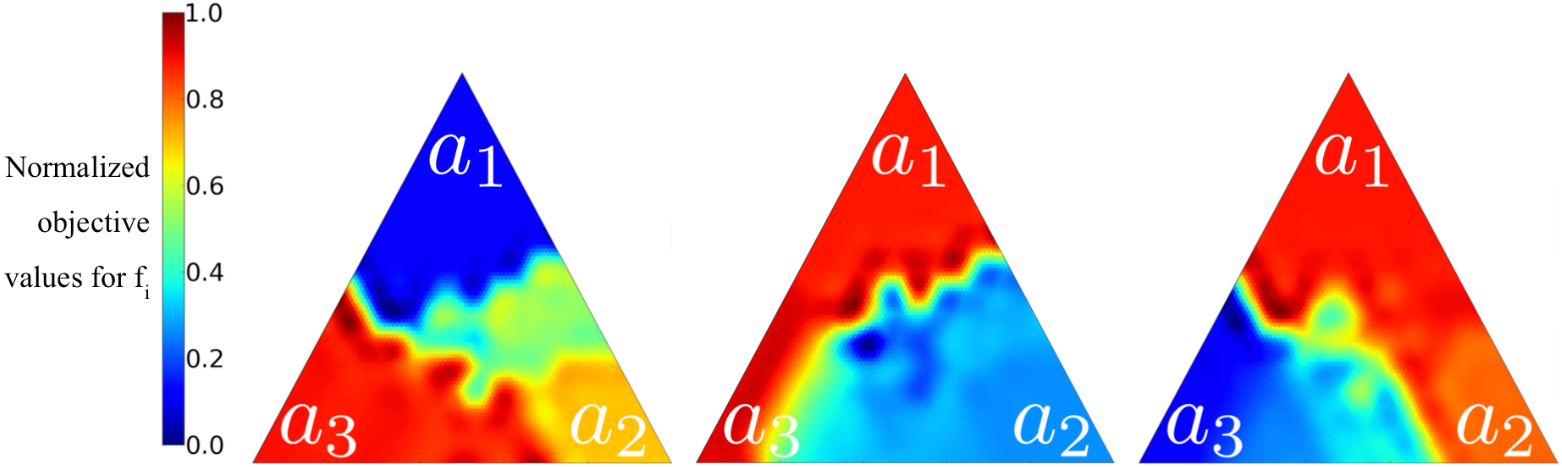
Attack Example: *CATCH ME IF YOU CAN*





A posteriori Optimization

- Explore a_i space, creating a "representative" subset of Pareto solutions



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

Open Questions

* Risk To Reward Ratio
  * How costly to society are the attacks?
  * How costly is the <u>implementation</u> of the attacks?
* Connected Vehicles/Infrastructure Security
  * What vulnerabilities exist when vehicles are in the loop?
* **Prevention**
  * How can we leverage knowledge traffic dynamics to prevent attacks?

Berkeley
UNIVERSITY OF CALIFORNIA

Publications

- Reilly, J., Martin, S., Payer, M., & Bayen, A. M. (2014). On Cybersecurity of Freeway Control Systems: Analysis of Coordinated Ramp Metering Attacks. Transportation Research Part B Methodological, (In Review)
- Reilly, J., Krichene, W., Delle Monache, M. L., Samaranayake, S., 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).
- Reilly, J., & Bayen, A. M. (2014). Distributed Optimization for Shared State Systems: Applications to Decentralized Freeway Control via Subnetwork Splitting. Journal of Computational Physics (In Preparation).
- 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.

Berkeley
UNIVERSITY OF CALIFORNIA

Thank you for listening!

Questions?