FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Traffic Jams on Demand:
Precision Attacks on Freeways using Optimal Control Techniques.

Jack Reilly

Sébastien Martin

Berkeley UNIVERSITY OF CALIFORNIA

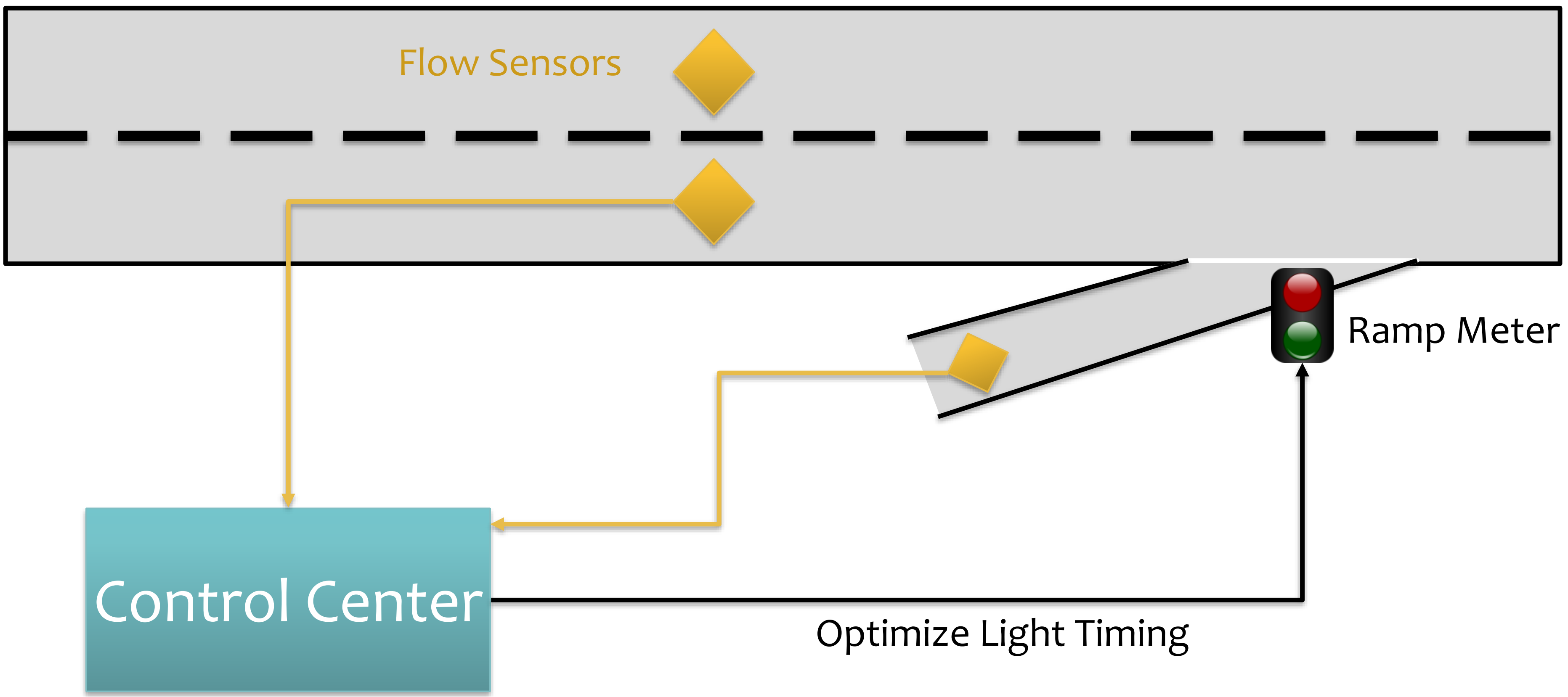
Massachusetts Institute of Technology

NSF

MICHIGAN

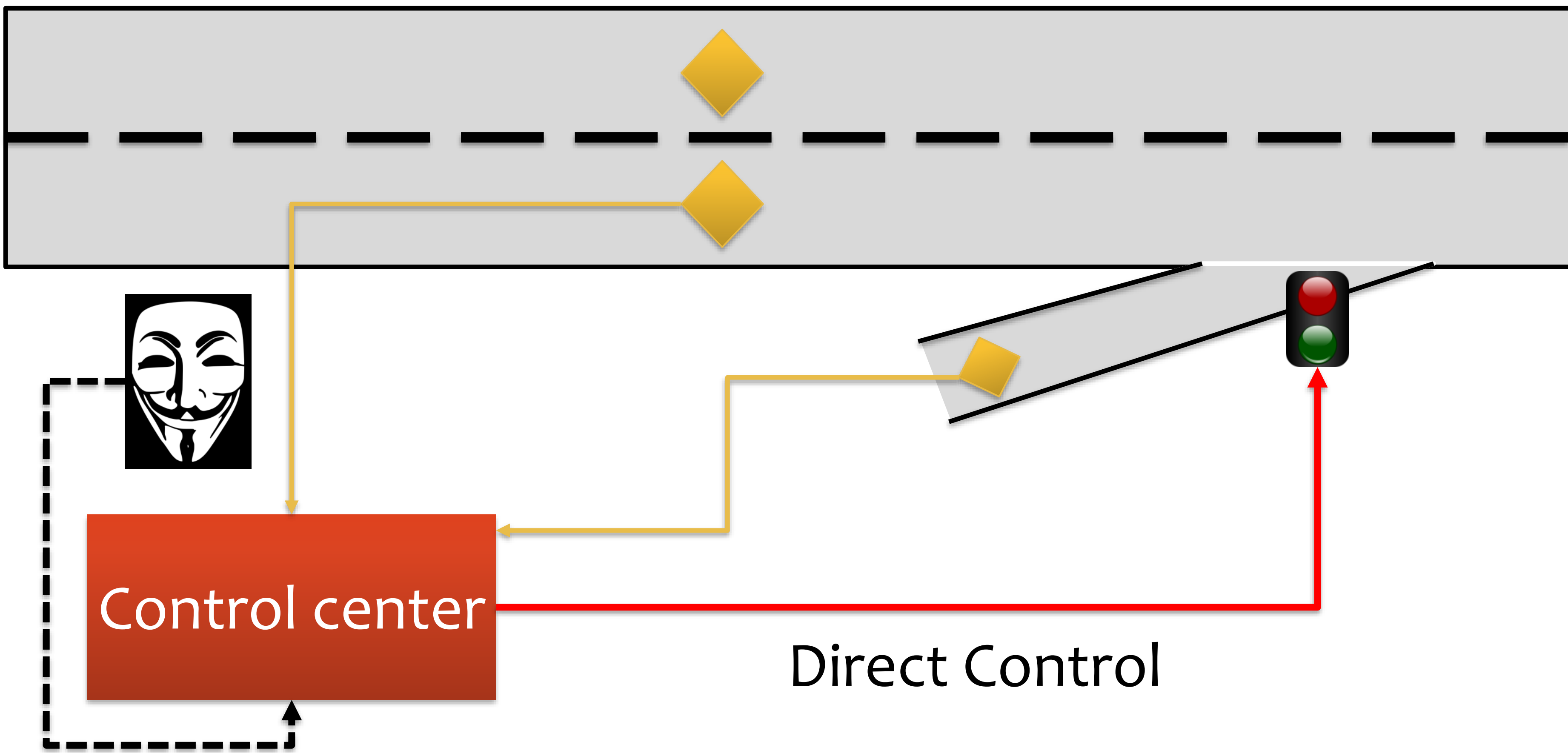
VANDERBILT UNIVERSITY

Freeway Traffic systems



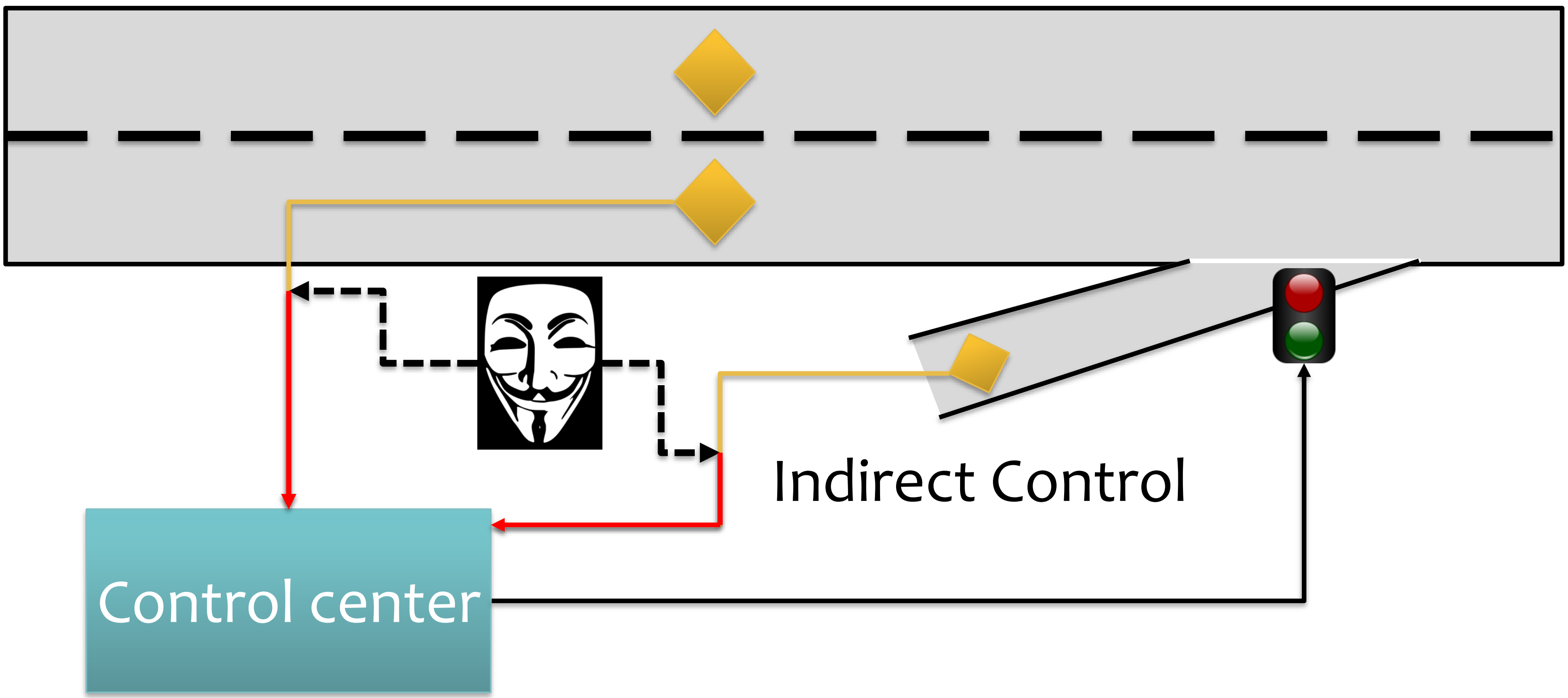
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Compromise : complete takeover



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Compromise : spoofing the sensors

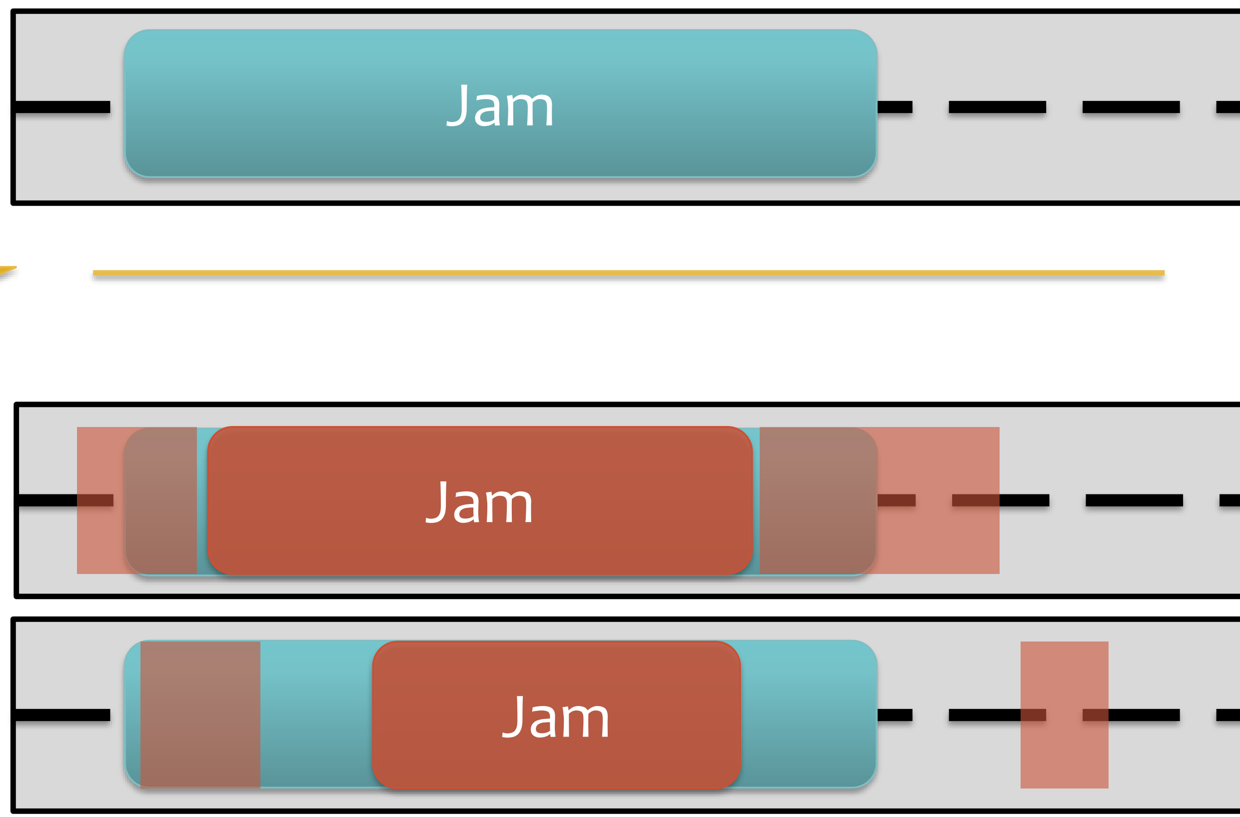


FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Compromise : spoofing the sensors

Closest Reachable states

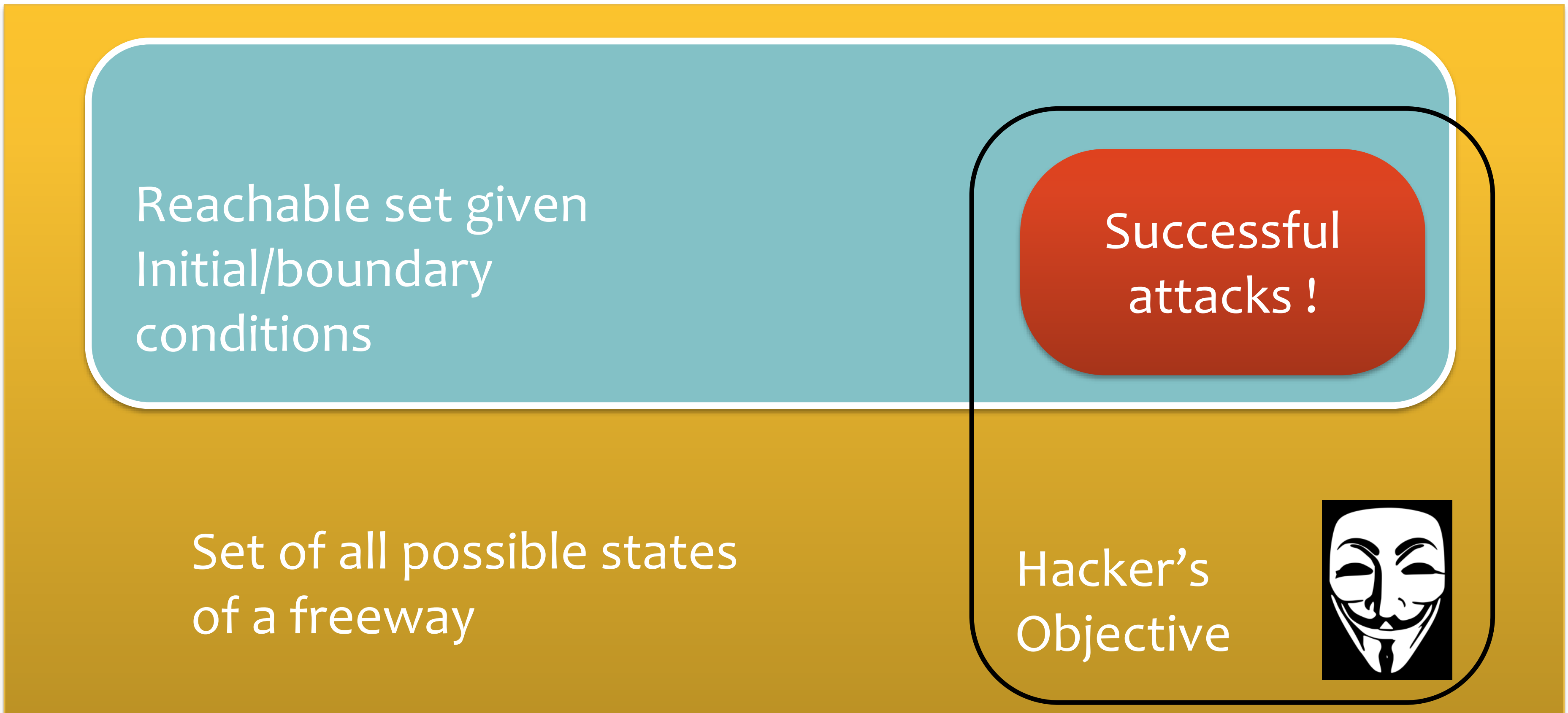
Attacker’s optimal objective



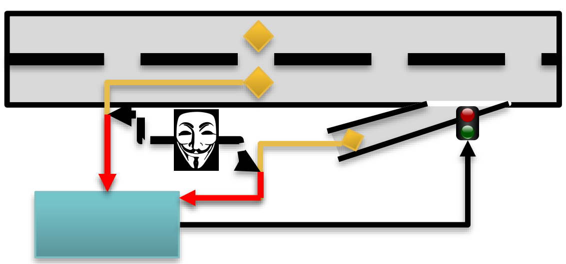
- Direct Control
- Sensor Spoofing Only

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

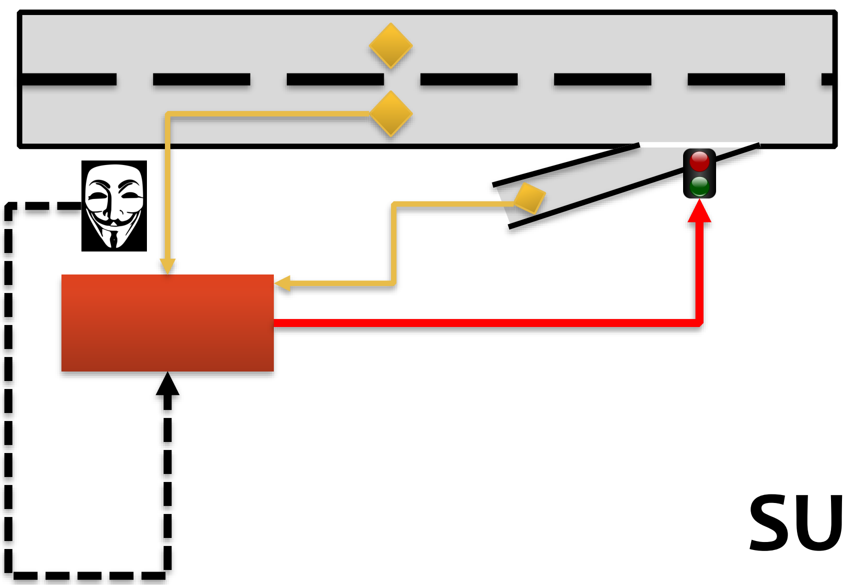
Reachable sets



Sensor Spoofing Attack: Micro-Simulation



Direct Attack: Optimal Control Method



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

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

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

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

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

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

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 $k \leftarrow k+1$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Take-Over-The-Freeway Attack Demo!

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS