Analyzing Traffic Control System Compromises: Coordinated Ramp Metering Attacks

Jack Reilly Sebastien Martin Mathias Payer Alexandre M. Bayen

MOTIVATION: Real World Attacks

Figure: Waze GPS Spoofing

- Launch many Android emulators.
- Spoof GPS readings to create virtual **"jam"**.

Figure: Sensys Vehicle Counter

- Insecure **wireless** comm. between sensor & receiver.
- **Drone** broadcasts fake readings.

Freeway Control System Vulnerabilities

Figure: Local Control

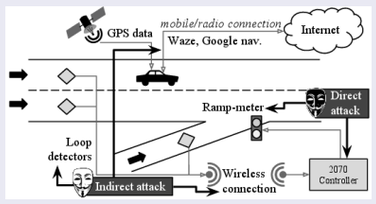
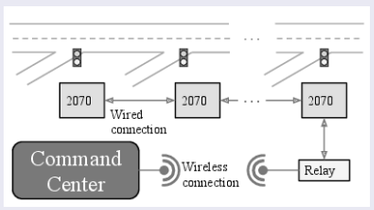
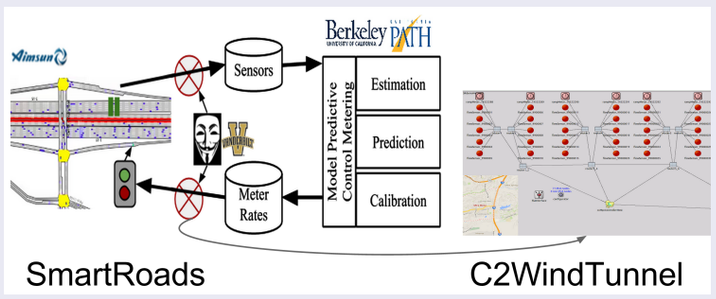


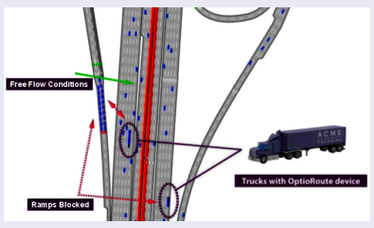
Figure: Global Control



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

SmartRoads Project: VIP Lane Attack





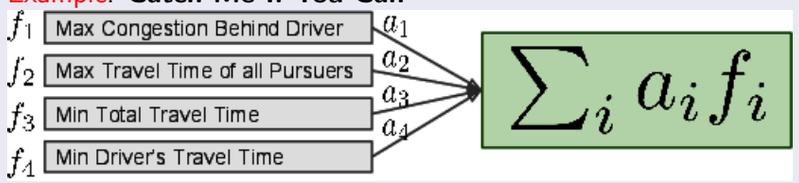
- **VIP Lane**: Intercept loop detector readings to allow trucks to travel quickly from upstream entrance.
- Implement attack on **SmartRoads** system using microsimulation and comm. modeling.

METHODOLOGY: Designing Ramp Metering Attacks

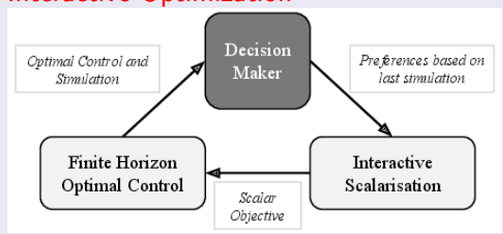
High-level, Multi-goal Objectives

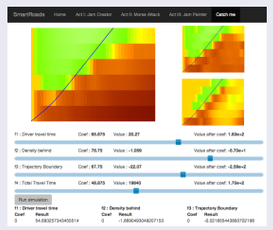
- Difficult to mathematically express high-level goals
- Construct objective using **scalarization** of multiple goals.
- Use **interactive optimization** to explore **Pareto space**.

Example: Catch Me If You Can



Interactive Optimization





Adjoint-based Optimal Control

Problem Statement

$$\min_{u \in U} f(\rho, u)$$
$$\text{subject to: } H(\rho, u) = 0$$

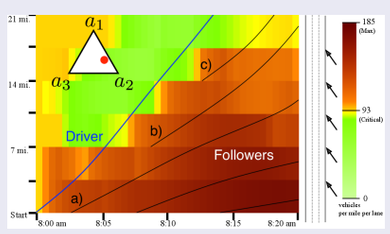
- $u(i,t)$ metering rate for ramp i, time t.
- $\rho(i,t)$ traffic density cell/ramp i, time i.

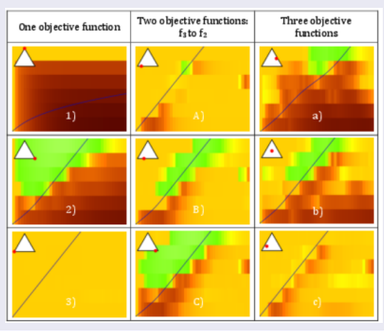
Solution: Gradient Descent via Discrete Adjoint

- Finite differences infeasible.
- **Adjoint** gives **linear** complexity w.r.t. network size.

$$\nabla_u f = \frac{\partial f}{\partial u} + \lambda^T \frac{\partial H}{\partial u}$$
$$\text{subject to: } \frac{\partial H}{\partial \rho}^T \lambda = \frac{\partial f}{\partial x}$$

Catch Me If You Can Results

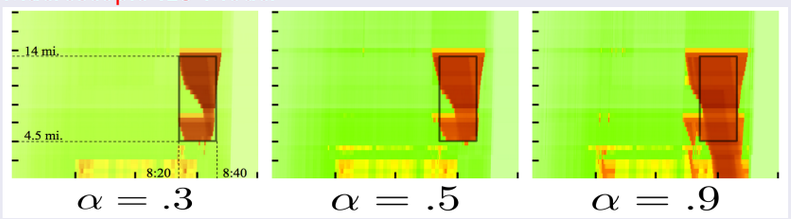




NUMERICAL RESULTS: I15 Freeway Box Objective

- Create congestion in predetermined range of **time** and **space**.
- $f = (1-\alpha) TTT_{\text{out of box}} - \alpha TTT_{\text{in box}}$

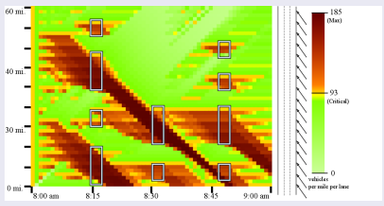
Macroscopic I15 Model

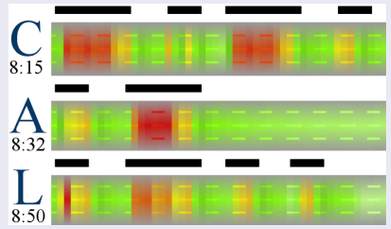


Interactive optimization discovers α balance parameter.

Extending Box Objective

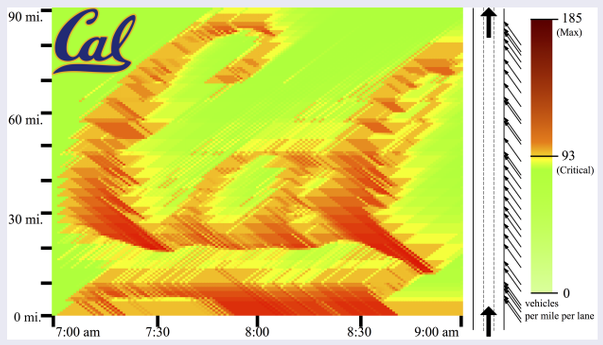
Morse Code

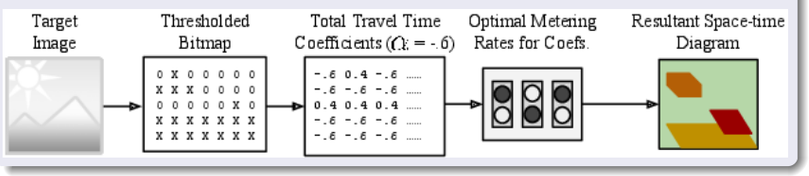




"Inkjet Printer"

- Input: Any digital image file.
- Output: Metering rates which reproduces image in congestion patterns.





CONCLUSIONS

- **Direct** (metering lights) and **indirect** (loop detectors) control a potential security threat.
- Sophisticated objectives achievable using few control points.
- Efficient optimal control techniques enable real-time deployment of attack techniques.
- Interactive optimization useful for **management** and **calibration**.