FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Vulnerability of Fixed-Time Control of Signalized Intersections to Cyber-Tampering

Amin Ghafouri, Waseem Abbas, Yevgeniy Vorobeychik, and Xenofon Koutsoukos
Institute for Software Integrated Systems
Vanderbilt University

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

Sensor Vulnerabilities in Transportation Networks

- 200,000 vulnerable traffic control sensors in important cities around the world such as New York, San Francisco, London, and Melbourne
- Traffic signal control
  - Feedback control such as max-pressure
  - Periodic cycle such as fixed-time control
- 90 percent of all traffic signals in the US follow fixed-time control policy.

A. Ghafouri, W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Vulnerability of fixed-time control of signalized intersections to cyber-tampering." Submitted to the 9th International Symposium on Resilient Control Systems (ISRCS), Chicago, Illinois, 2016.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Fixed-Time Control

- Deterministic vehicle flows subject to 1) conservation constraints, 2) constraints on saturation flows, and 3) simultaneous turn movements.

Total duration

$$\min \sum_{S \in \mathbb{S}} \lambda_S$$

$$\text{s.t.} \quad \sum_{S \in \mathbb{S}} \lambda_S c(i,j) S(i,j) \geq f(i,j), \text{all } (i,j)$$

$$\lambda_S \geq 0 \text{ all } S \in \mathbb{S}$$

Sensor attack on flow measurement

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Attacker Model

1. **Network accumulation:** destabilizing the overall network as much as possible
2. **Lane accumulation:** causing worst-case accumulation on some target lanes
3. **Risk-averse target accumulation:** reaching a target accumulation by making the minimum perturbation

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Attacker Model

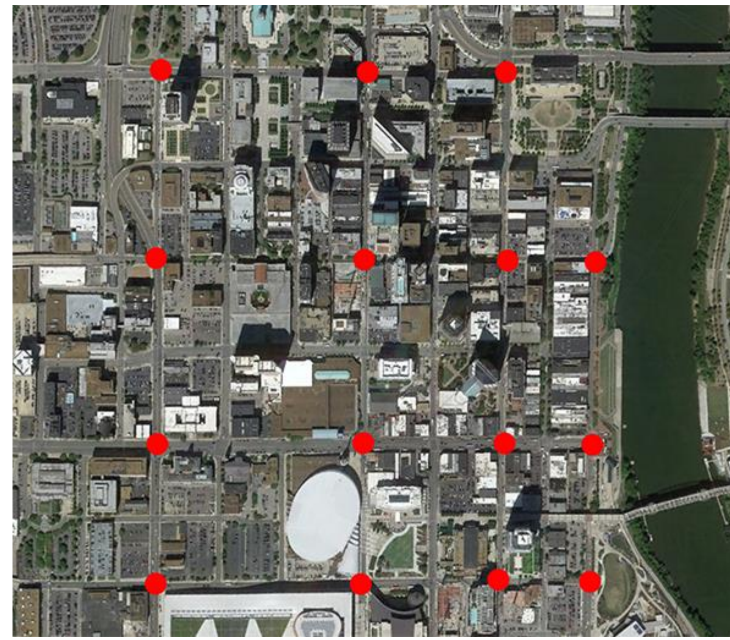
- All attacker problems are Bilevel Mixed Integer Quadratic Programs (BMIQP).
- Solution using branch-and-bound and cutting planes. GUROBI OPTIMIZATION
- Metrics: $\mathrm{NV} = \dfrac{\text{Accumulation Rate}}{\text{Total Flow}}$ and $\mathrm{LV} = \dfrac{\text{Lane Accumulation Rate}}{\text{Lane Total Flow}}$

Total accumulation rate	$\max_{\tilde{Q},\tilde{F}} \quad \sum_{ij} \max(0, (f_{ij} - \sum_{S} \tilde{\lambda}_S c_{ij} S_{ij}))$
Fixed-Time sub-problem	$\text{s.t.} \quad \tilde{\lambda}_S \in \mathrm{FT}(\tilde{F})$
Feasibility constraint	$\sum \tilde{\lambda}_S < 1$
Flow conservation	$\sum_h \tilde{f}(h,i) = \sum_j \tilde{f}(i,j)$
Attacker's budget	$\lvert\tilde{Q}\rvert \leq B$
	$\tilde{f}(i,j) \geq 0, \ \text{all } (i,j)$

Worst-case Network Accumulation

Case Study – Nashville Downtown

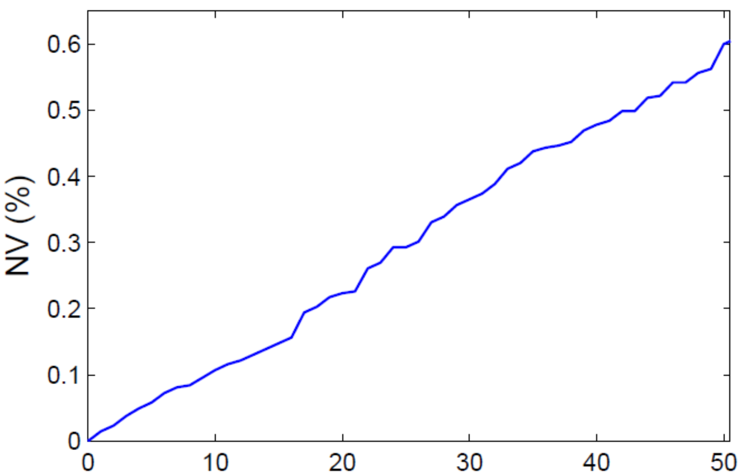
- Real traffic history data provided by Tennessee Department Of Transportation (TDOT)
- Area between 1st Ave, 8th Ave, Demonbreun St, and Charlotte Ave.
- 15 intersections (12 four-way and 3 three-way), and 104 phases
- Total demand approximately 15000 vehicles per hour



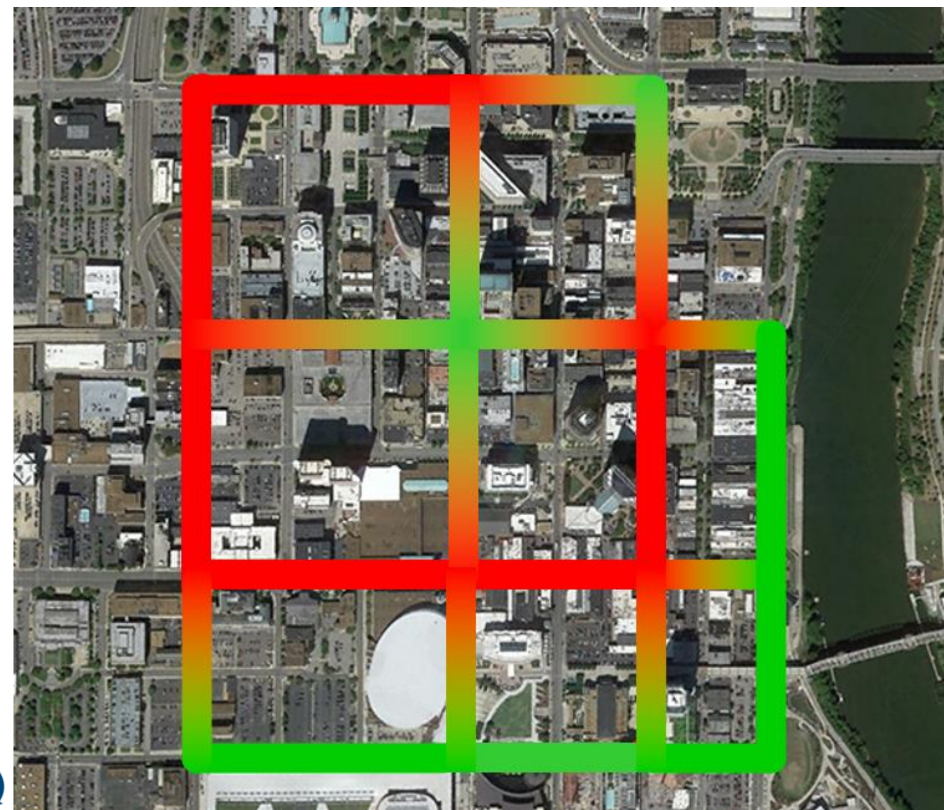
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Worst-Case Network Accumulation

1. Accumulation of 4000 vehicles per hour by compromising 20% of sensors (~21 sensors)



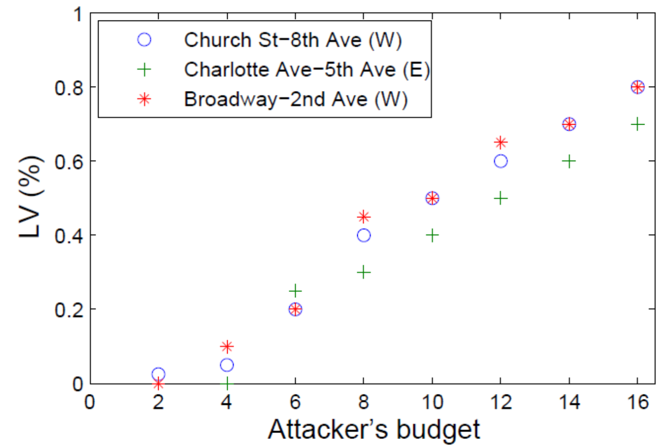
Sensor measurement	Frequency
Charlotte Ave-8th Ave (WE)	98%
Broadway-8th Ave (NW)	97%
Charlotte Ave-8th Ave (SE)	95%
Demonbreun St-8th Ave (NE)	95%
Charlotte Ave-5th Ave (WE)	94%
Charlotte Ave-3rd Ave (NE)	94%
Broadway-8th Ave (WE)	91%
Broadway-5th Ave (WE)	83%

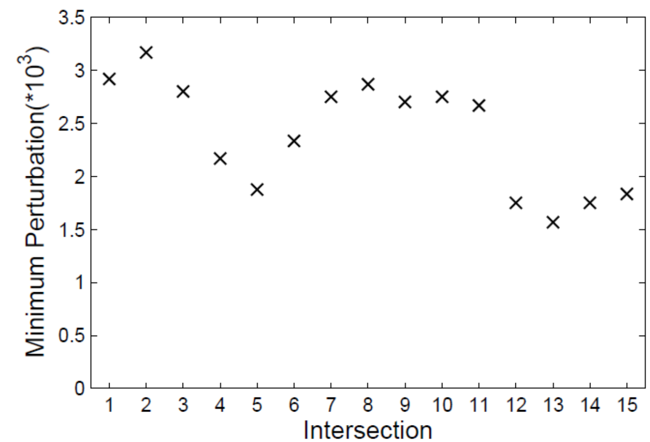


Worst-Case Lane Accumulation and Risk-Averse Target Accumulation

2. **Lane accumulation:** easier to cause a disastrous congestions on Broadway-2nd Ave.

3. **Risk-averse target accumulation:**
   - highest perturbation: Charlotte Ave-5th Ave
   - lowest perturbation: Demonbreun St-3rd Ave and

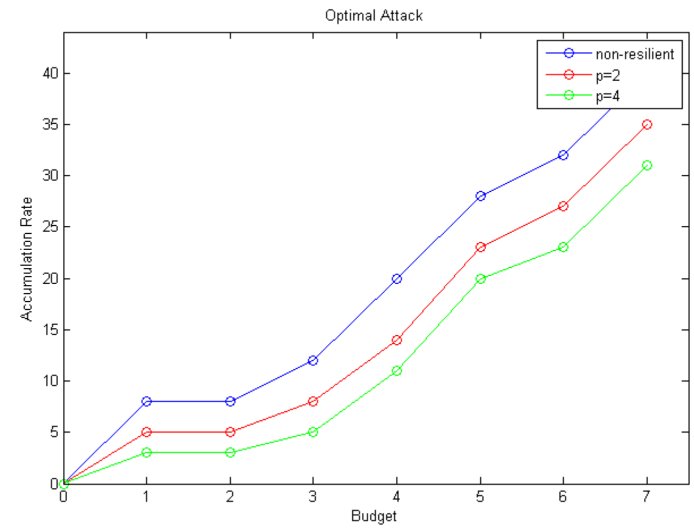




FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Ongoing Work

1. Resilient Fixed-time Control
   - Worst-case attack is mitigated by %20 if cycle length is quadrupled.
2. Analysis of Max-Pressure Control
3. Implementation
   - Vulnerability analysis incorporating real-time user data provided by Transit-Hub
   - Transit-Hub: public transit route finder app powered by real-time data from the Nashville MTA



Nashville MTA

Available on the App Store

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Thank you for your attention!

Questions?