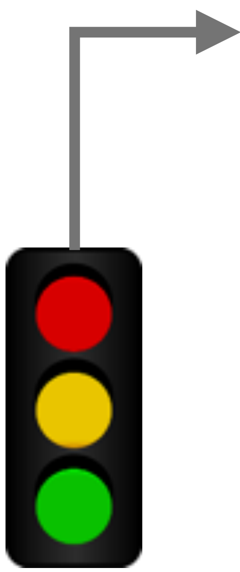
Vulnerability of Transportation Networks to Traffic-Signal Tampering

Aron Laszka[1], Bradley Potteiger[2], Yevgeniy Vorobeychik[2], Saurabh Amin[3], Xenofon Koutsoukos[2]

[1]University of California, Berkeley
[2]Vanderbilt University
[3]Massachusetts Institute of Technology

Evolution of Transportation Networks

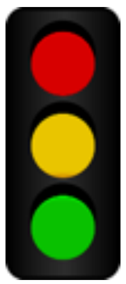


Evolution of Transportation Networks

Intelligent Transportation

- reducing wasted time and environmental impact, increasing road safety, etc.

Evolution of Traffic Control

	**Traditional**	**Intelligent**
Traffic control devices	standalone hardware	**complex networked systems of sensors and controllers**
Traffic signal timing	configured at the time of deployment	**adapt to local or global traffic situation**
Traffic flow	varies freely with traffic demand	**optimized to minimize, e.g., wasted time and environmental impact**
Vulnerabilities	direct attacks based on physical access	**attacks through wireless interfaces or remote attacks over the Internet**

Vulnerabilities in Traffic Signals

Case study by University of Michigan [1]

- In cooperation with a road agency located in Michigan, which operates around a hundred traffic signals
- Intersections are part of the same network, but operate individually
- Major weaknesses:
  - wireless communication is **unencrypted**
  - controllers are vulnerable to **known exploits**
  - devices use **default usernames** and **passwords**

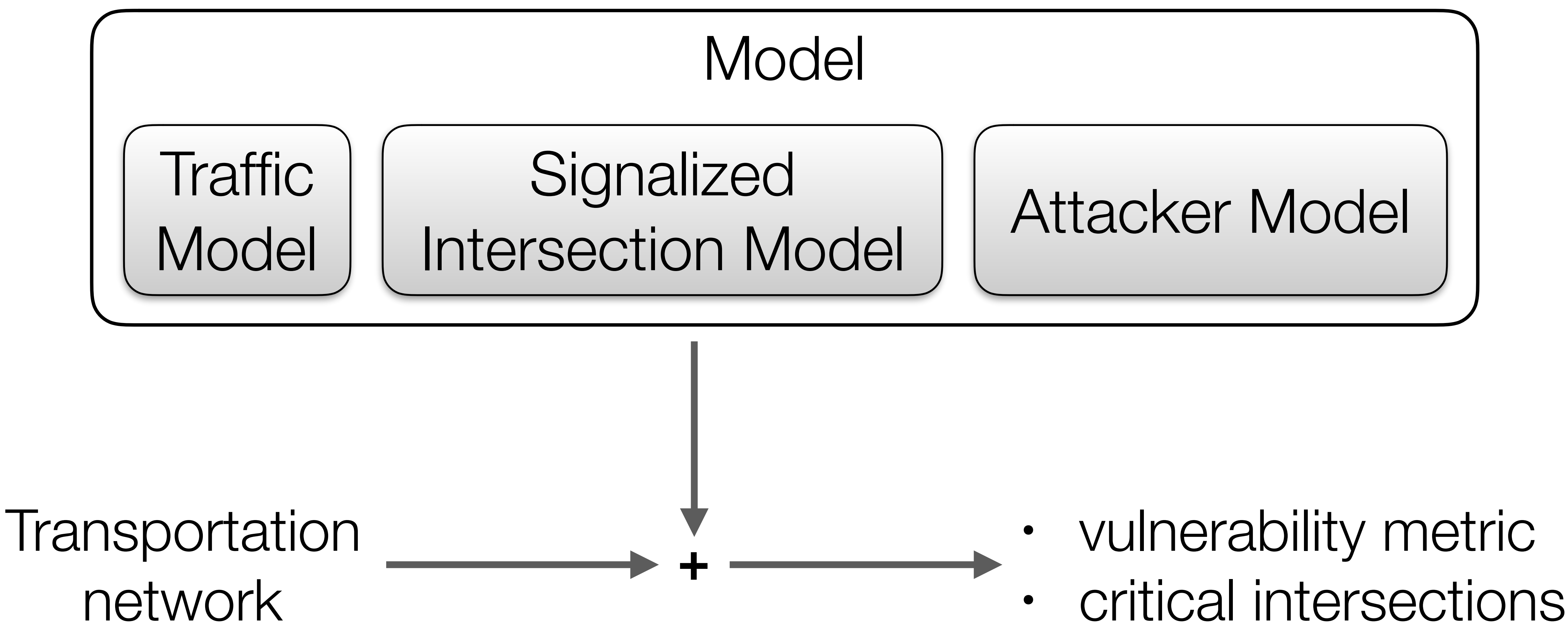
[1] Ghena et al., "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," *Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT)*, August 2014.

Attacks Based on Traffic Signal Tampering

- Due to hardware-based failsafes, these vulnerabilities cannot be used directly to cause traffic accidents
- However, they may be used to cause **disastrous traffic congestions**, which can effectively cripple a transportation network

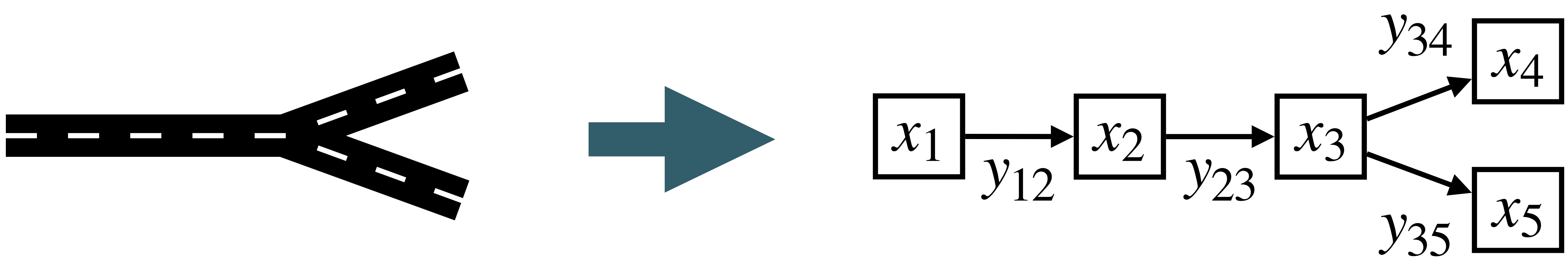
How vulnerable are transportation networks to such attacks?

Vulnerability Assessment

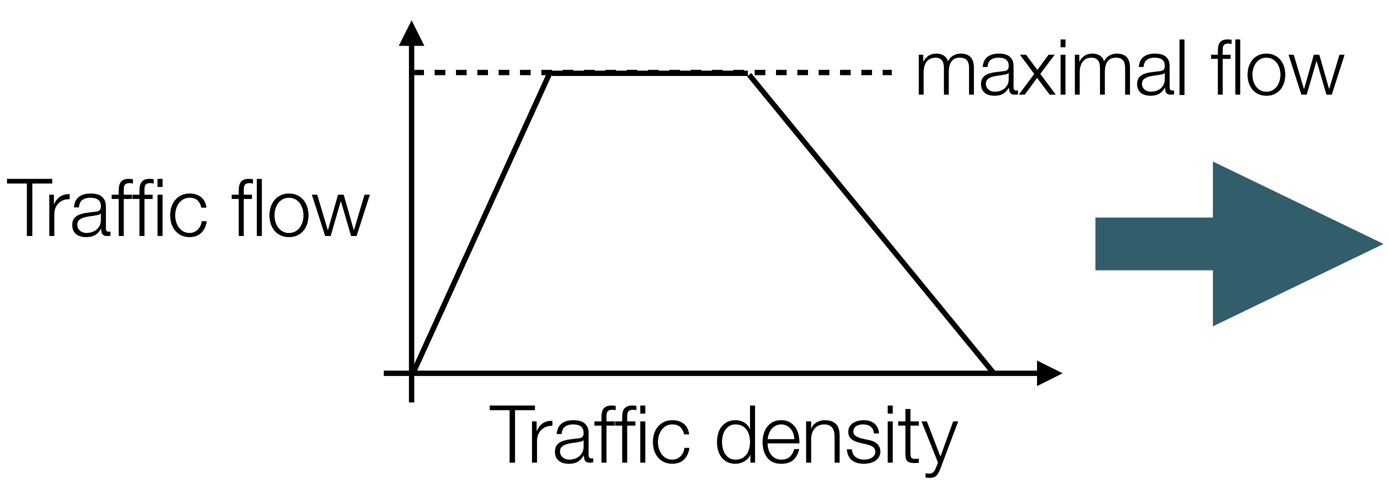


1. Traffic Model: Daganzo’s Cell Transmission Model

- Well-known and simple approach for modeling traffic flow
- Discrete: **time** is divided into **intervals**,
  while **roads** are divided into **cells**



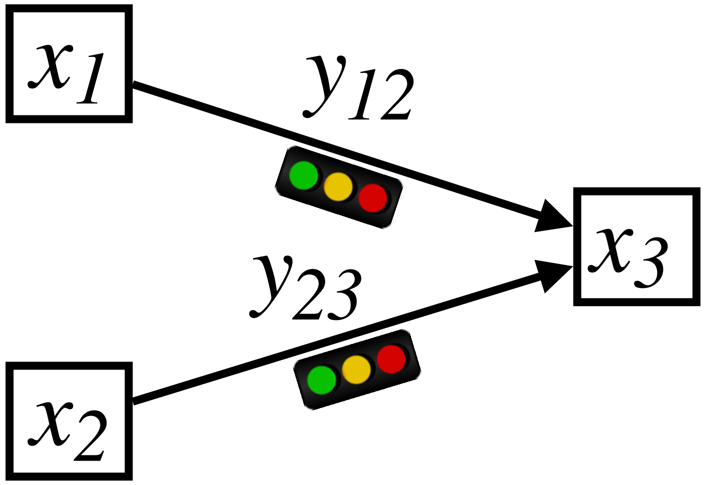
- Traffic flow is limited by the capacity and the congestion level of the successor cell



$$y_{ij} = \min(x_i, Q, \delta(N - x_j))$$

2. Signalized Intersection Model

- Intersection:
  cell with multiple predecessors



- Signalized intersection:
  inflow proportions are controlled by the signal schedule

$$y_{ij} \leq \boldsymbol{p_{ij}} \times \min(Q, \delta(N - x_j))$$

$$\Sigma_i \, p_{ij} = 1$$

3. Attacker Model

- Action space
  - **budget limit**: attacker can compromise at most B intersections
  - **tampering**: attacker can change the schedule (i.e., inflow proportions p_{ij}) of every compromised intersection j
  - **failsafes**: the attacker can select only valid schedules (i.e., the inflow proportions must add up to one: $\sum_i p_{ij} = 1$)
- Goal
  - **worst-case**:
    attacker minimizes the network's utility by maximizing its congestion
- We quantify congestion as the **total travel time** T of the vehicles that enter the transportation network

Vulnerability and Critical Intersections

Vulnerability of a transportation network:

$$\frac{T(\mathcal{A}) - T}{T}$$

- T: total travel time without attack
- $T(\mathcal{A})$: total travel time resulting from a worst-case attack

Critical intersections:
an intersection is **critical** if it is an element of a worst-case attack

Computational Complexity

Theorem: Given a transportation network, an attacker budget B, and a threshold travel time T^*, determining whether there exists an attack $\mathcal{A}$ satisfying the budget constraint such that $T(\mathcal{A}) > T^*$ is NP-hard.

- We cannot hope to find polynomial-time algorithms for evaluating the vulnerability of a transportation networks against signal-tampering attacks

Heuristic Algorithm for Finding an Attack

- Combination of two principles:
  - *outer search:* **greedy heuristic** for selecting the set of intersections to target
  - *inner search:* for each new intersection j, exhaustive search over **extreme configurations** (i.e., $p_{ij}=1$ for some i)

Algorithm 1 Polynomial-Time Heuristic Algorithm for Finding an Attack

$\mathcal{A} \leftarrow (\emptyset, \emptyset)$
for $b = 1, \ldots, B$ **do**
  for $s \in \mathcal{S}$ **do**
    for $k \in \Gamma^{-1}(s)$ **do**
      $\mathcal{A}' \leftarrow \mathcal{A} \cup (\{s\}, \{\hat{p}_{ks} = 1, \forall j \neq k : \hat{p}_{js} = 0\})$
      if $T(\mathcal{A}') \geq T(\mathcal{A}^*)$ **then**
        $\mathcal{A}^* \leftarrow \mathcal{A}'$
      end if
    end for
  end for
  $\mathcal{A} \leftarrow \mathcal{A}^*$
end for
Output $\mathcal{A}$

- Running time: polynomial in the size of the input

Numerical Evaluation

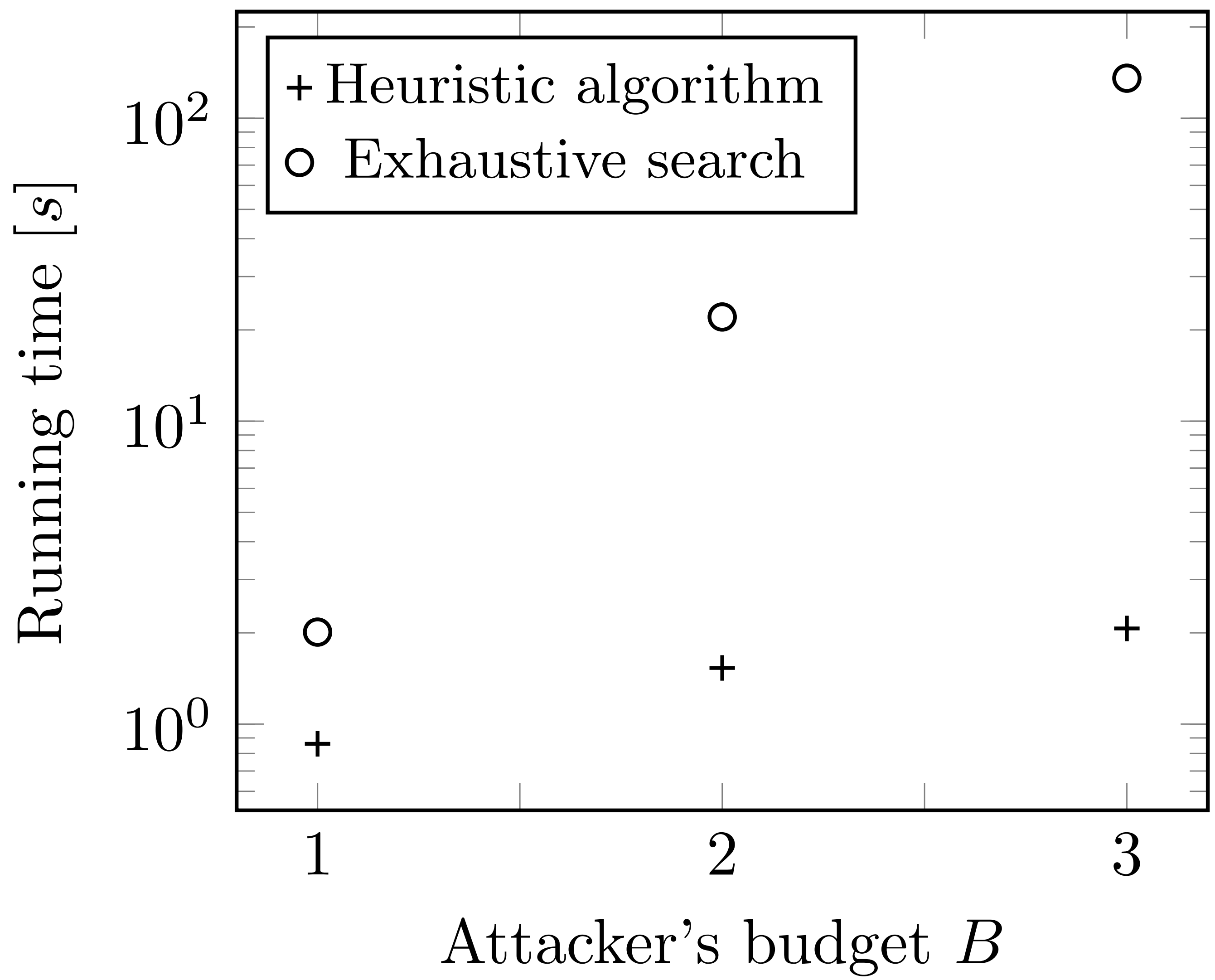
- Random road networks:
  Grid model with Random Edges (GRE) [2]
  - grid with **randomly** chosen horizontal/vertical edges **removed** and diagonal edges **added**
  - resulting networks are **very similar** to **real-world** road networks with respect to various metrics (e.g., road density, shortest-paths)
- Generated 300 random networks
  - resembling either European or US cities
- Performed an **exhaustive search** and the **heuristic algorithm** on each network

Los Angeles

Helsinki

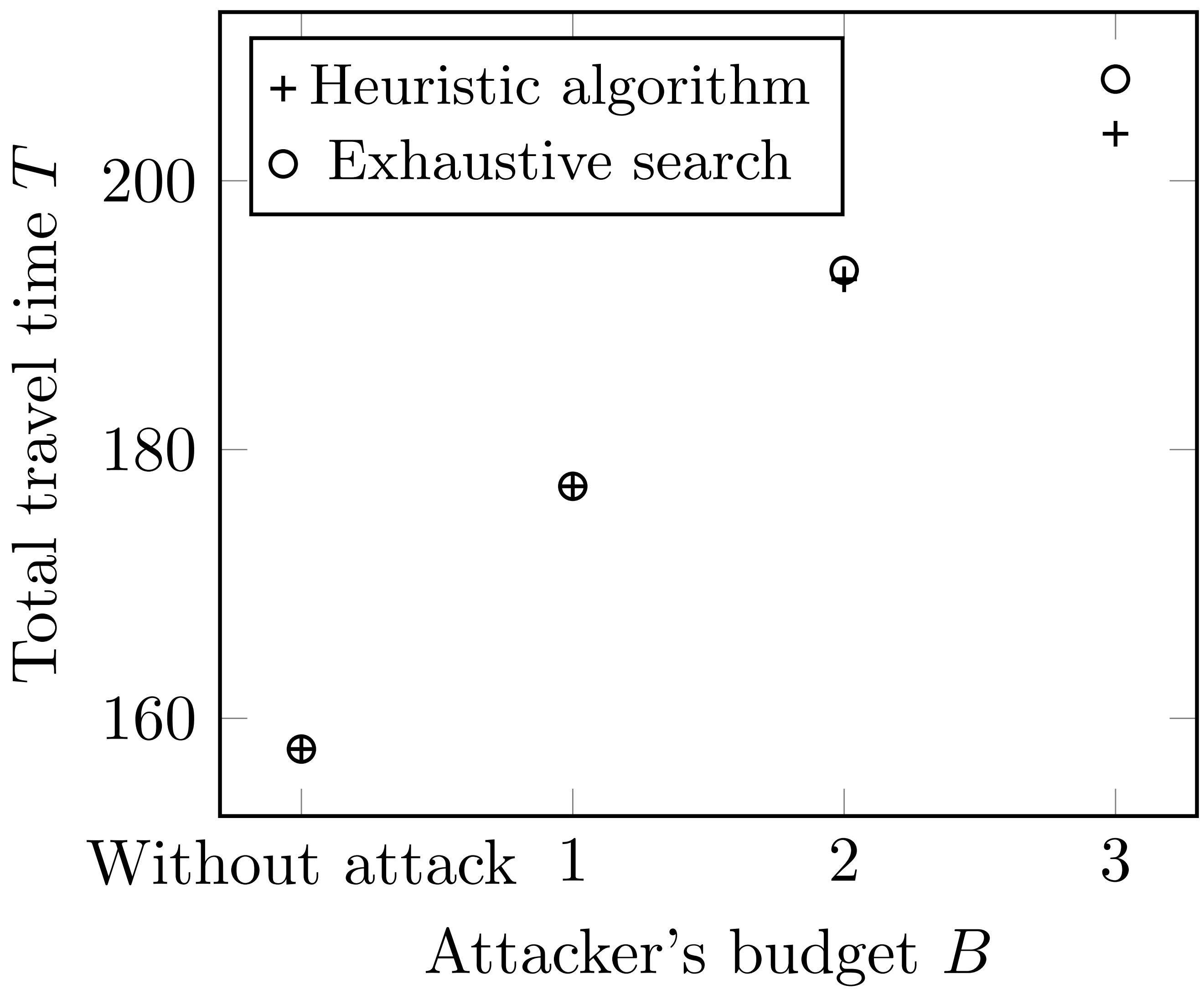
[2] W. Peng, G. Dong, K. Yang, J. Su, and J. Wu. “A random road network model for mobility modeling in mobile delay-tolerant networks.” *Proceedings of the 8th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, pages 140–146. IEEE, 2012.

Running Times



as expected, the running time of
exhaustive search **grows exponentially**

Travel Times

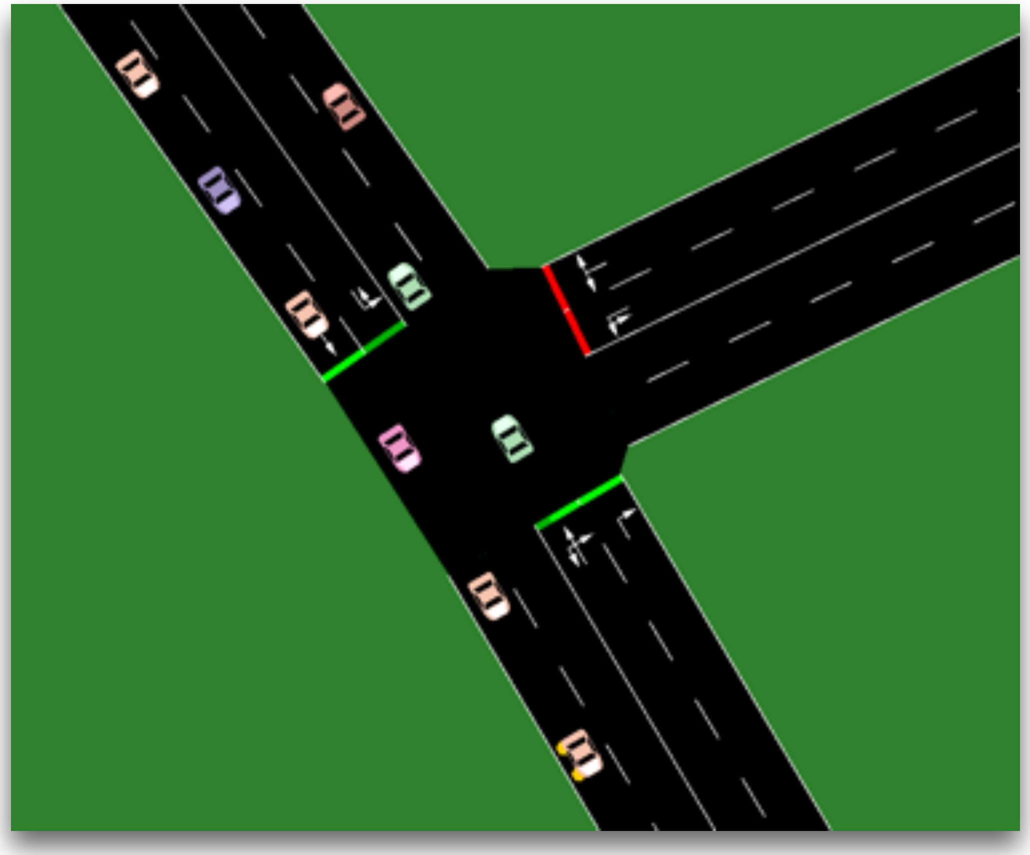


less than **3.4%** difference in every case

Micro-Model Based Simulations

How well does the algorithm perform in a micro model?

- SUMO simulator
  (Simulation of Urban MObility)
  - widely-used microscopic simulator
  - *traffic demand:*
    placing individual vehicles on the road network and setting their trajectories
  - *traffic light schedule:*
    modeled explicitly by SUMO



- Total travel time $T(\mathcal{A})$: total travel time output by SUMO

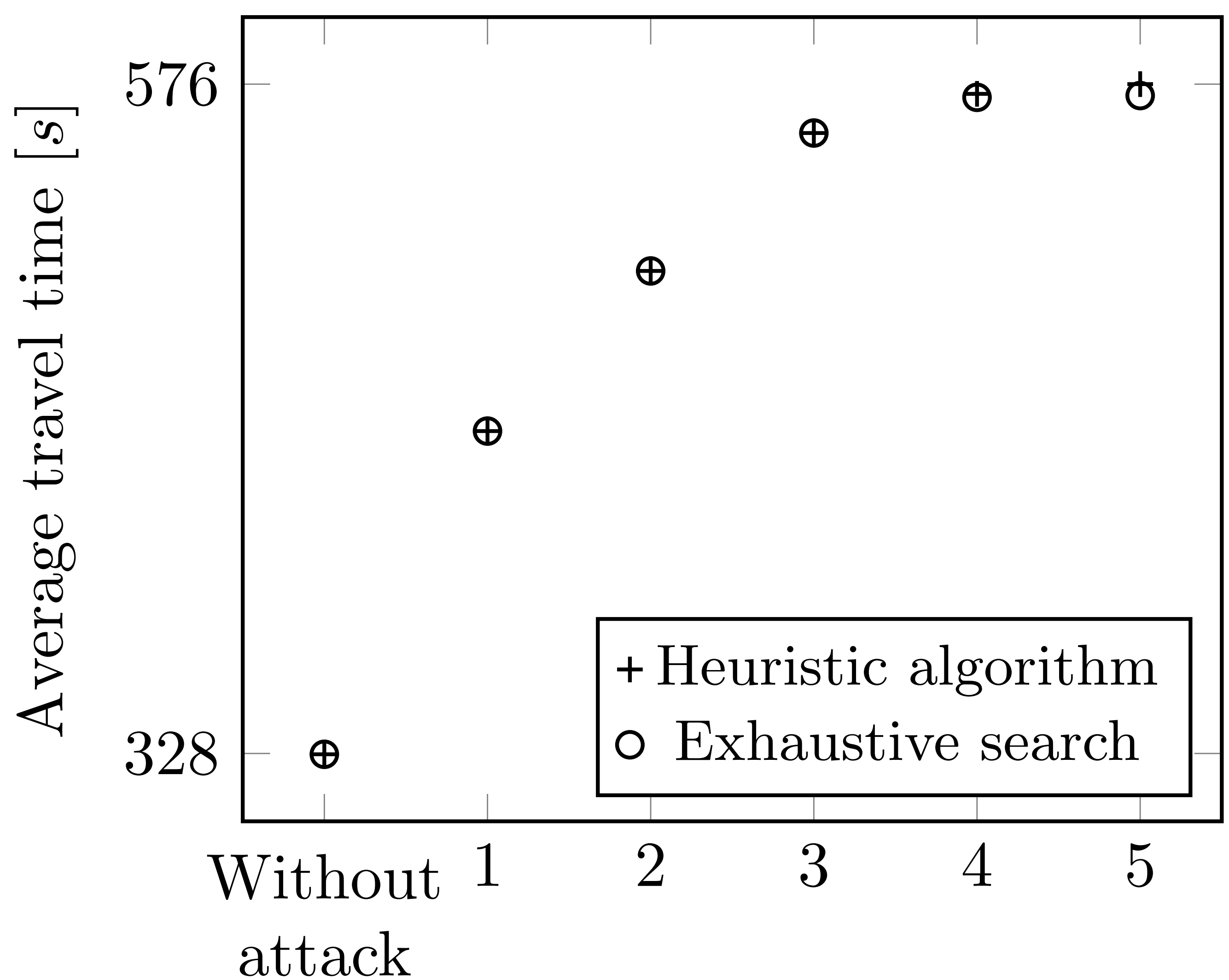
Example Transportation Network

- Transportation network
  - area around Vanderbilt University campus
  - from OpenStreetMap
- Traffic scenarios
  1. morning commute
  2. midday
  3. afternoon commute
  4. nighttime

(all data available on the first author's homepage)

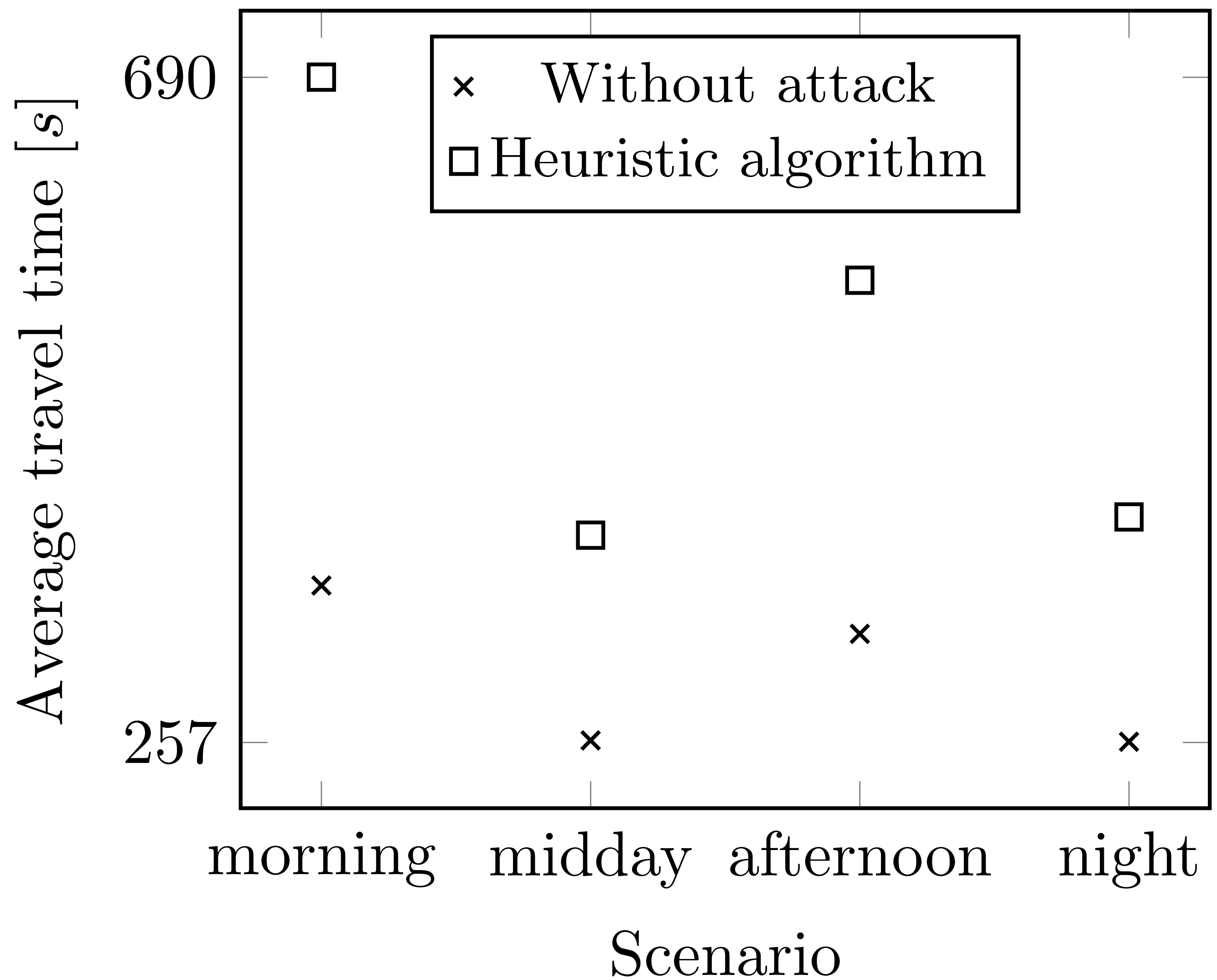
Targetable intersections
marked by **red disks**

Travel Times in the Afternoon Scenario



less than **0.8%** difference in every case

Comparison of Scenarios



vulnerability varies between
51% (midday scenario) and **92%** (morning scenario)

Ongoing Work: Resilient Traffic Signal Configuration

- **Resilient configuration:**
  even if some of the traffic signals are compromised and reconfigured, the default configuration of the remaining signals ensures acceptable traffic flow

- Tradeoff:

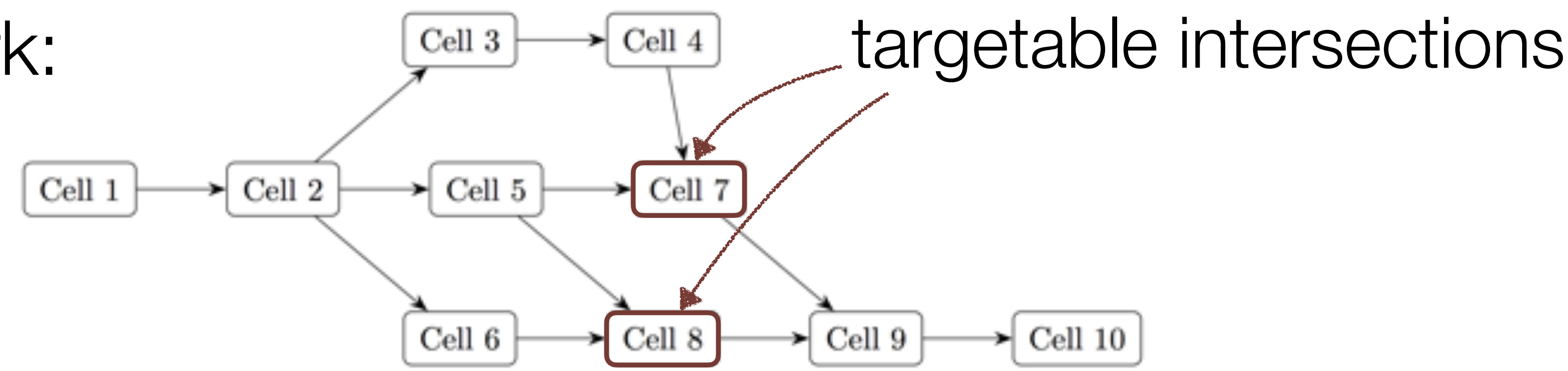
  resilience ↔ efficiency

  travel time after attack ↔ travel time without attack

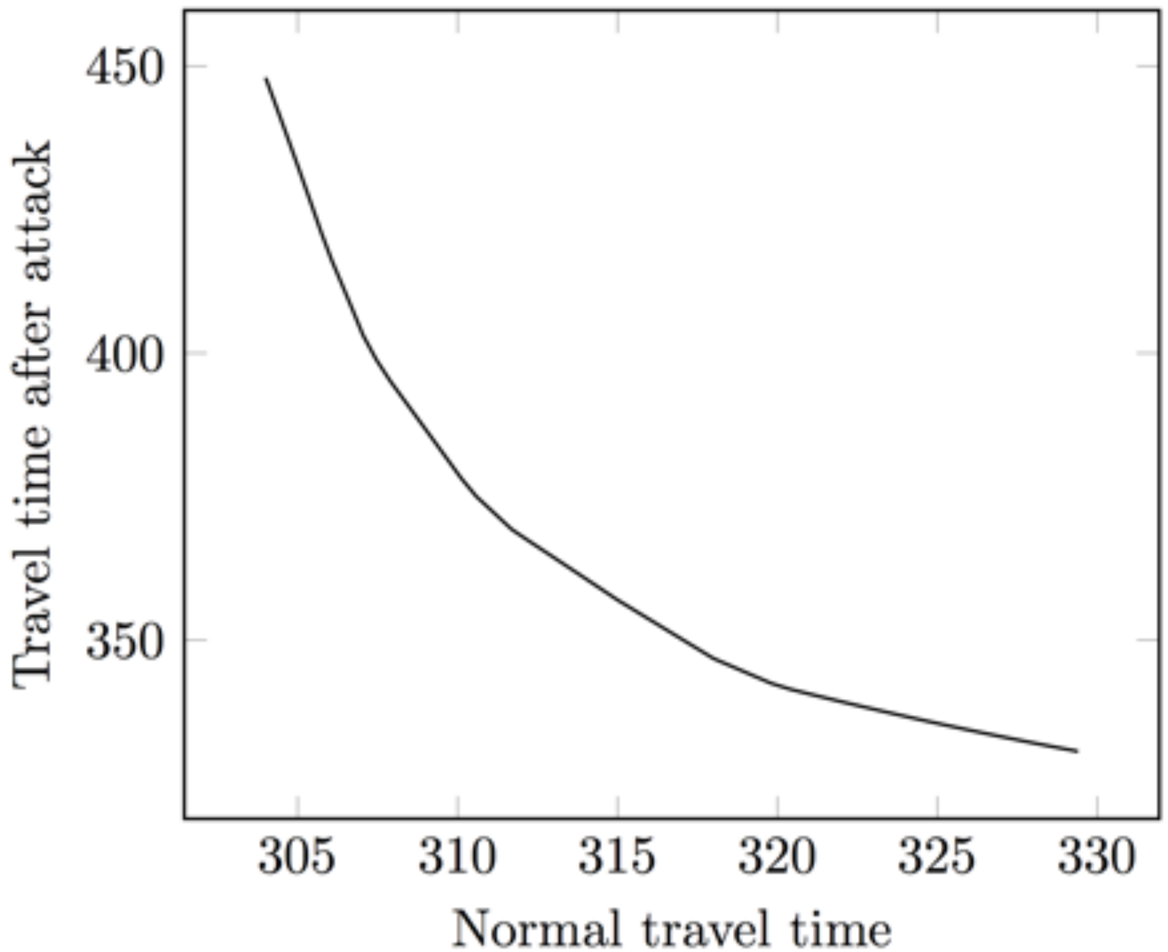
Can we increase resilience
without a significant sacrifice of efficiency?

Numerical Example

- Example network:

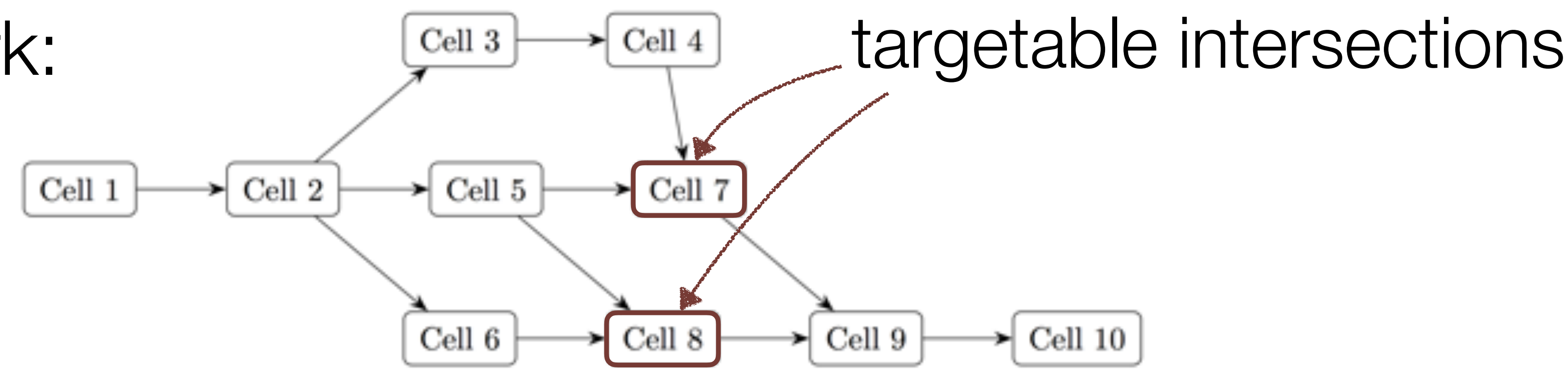


- Pareto optimal configurations:

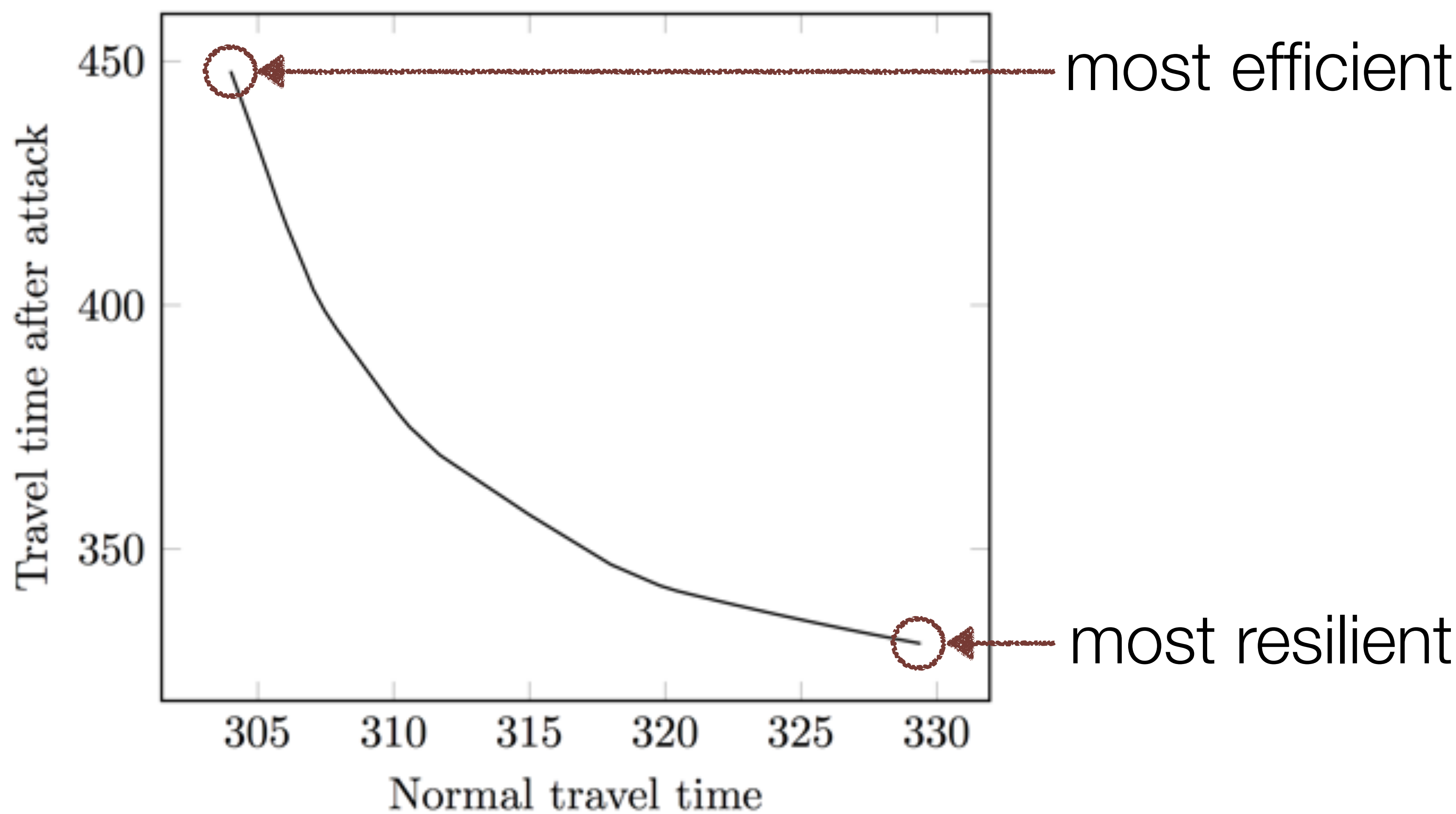


Numerical Example

- Example network:

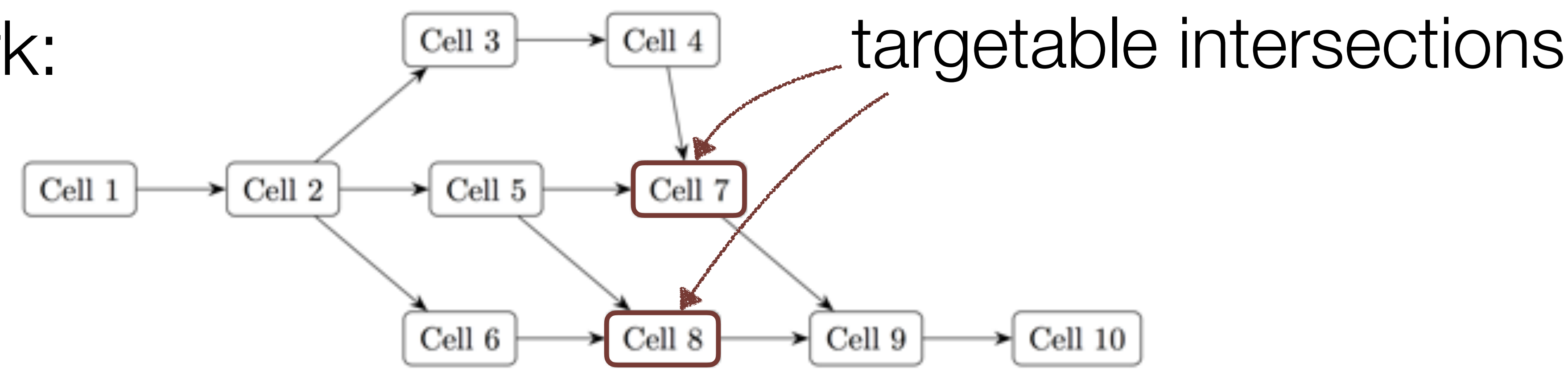


- Pareto optimal configurations:

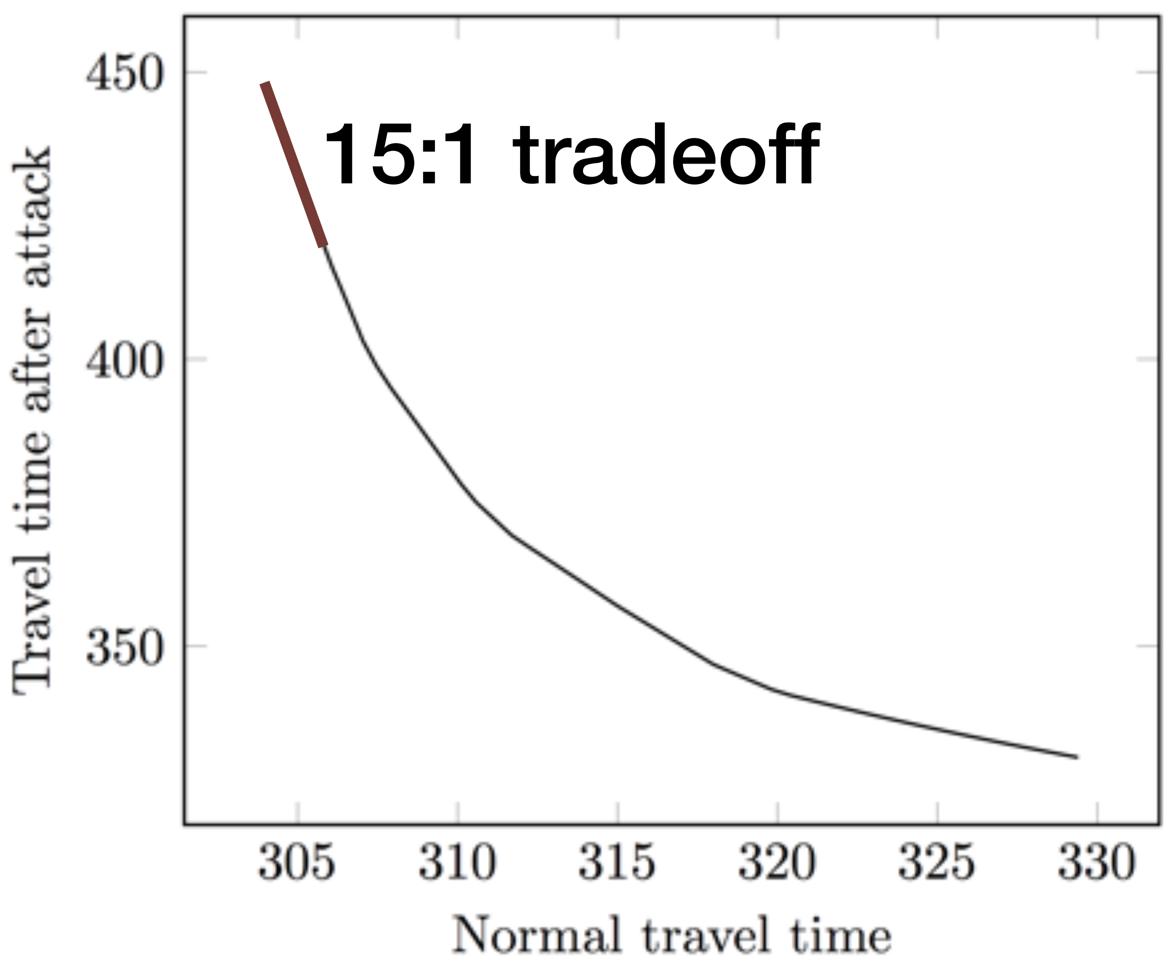


Numerical Example

- Example network:



- Pareto optimal configurations:



Conclusion & Future Work

- Approach and algorithm for evaluating the vulnerability of transportation networks
- Evaluation based on a large number of random networks and a real-world road network
- Future work: what makes a traffic signal critical?
    - what metrics are related to vulnerability and criticality
      (e.g., characteristics of the traffic flowing through the intersection, graph-theoretic metrics, such as centrality)

Thank you for your attention!

Questions?