Vulnerability of Transportation Networks to Traffic-Signal Tampering

Aron Laszka[1]

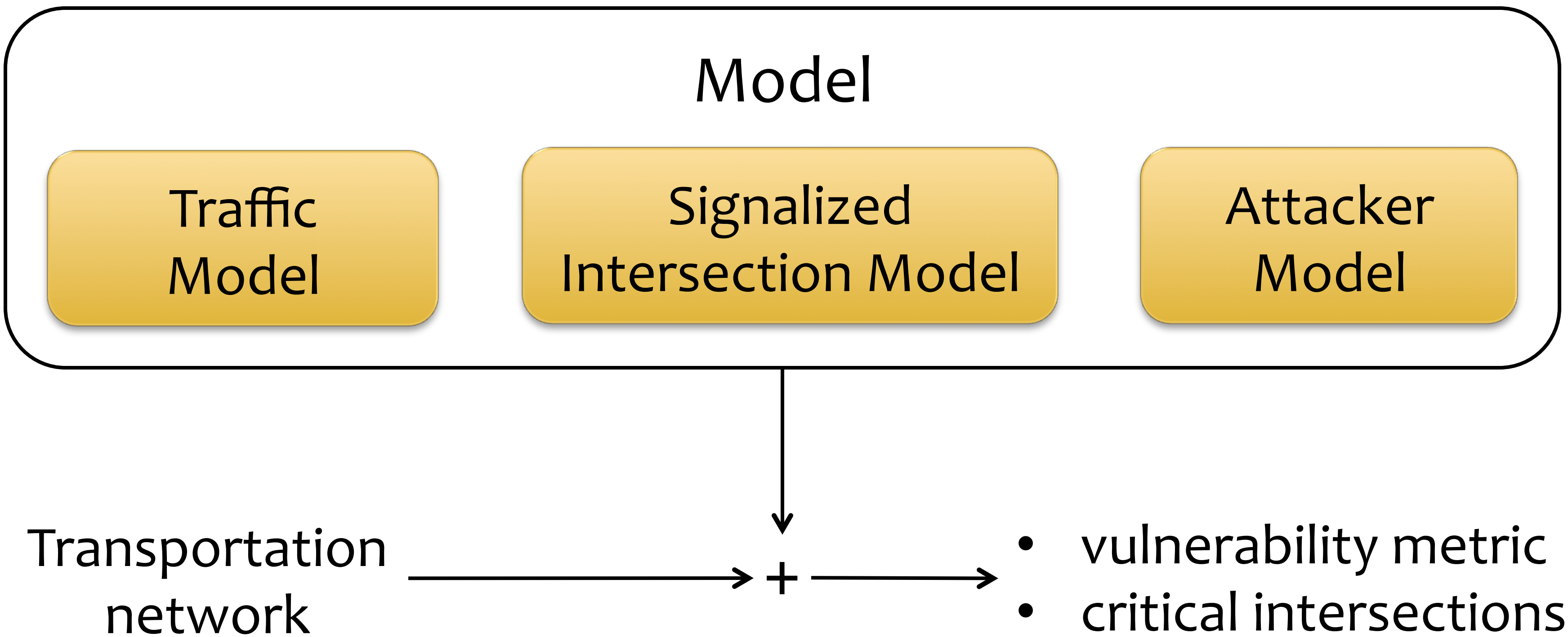
in collaboration with Bradley Potteiger[2], Yevgeniy Vorobeychik[2], Saurabh Amin[3], and Xenofon Koutsoukos[2]

[1]UC Berkeley [2]Vanderbilt University [3]MIT

Traffic Signals

* In the beginning…
  * standalone hardware devices running on fixed schedules
  * vulnerable only to attacks based on direct physical access
* Nowadays
  * networked devices controlled by software solutions
  * vulnerable to attacks through wireless interfaces or even the Internet
  * hardware-based failsafes prevent unsafe configurations, but an attack may cause disastrous traffic congestions

Evaluating the Vulnerability of Transportation Networks



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Traffic and Signalized Intersection Models

* Traffic model: Daganzo's cell transmission model
  - well-known and simple approach for modeling traffic flow consistent with the hydrodynamic model
  - discrete: time is divided into intervals, while roads are divided into cells (i.e., road segments)
  - traffic flow is limited by the capacity and the congestion level of the successor cell
* Signalized intersections
  - modeled using cells with multiple predecessors
  - traffic signal schedule: defines the inflow proportions of the cell

Attacker Model

* Action space
  * budget limit B: the attacker can compromise at most B intersections
  * tampering: the attacker can change the schedule (i.e., inflow proportions) of the compromised intersections
  * failsafes: the attacker can select only valid schedules (i.e., the inflow proportions must add up to one)
* Goal
  * worst-case: the attacker minimizes the network's utility by maximizing its congestion
* We measure congestion as the total travel time of the vehicles

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Vulnerability and Critical Intersections

* Vulnerability of a transportations network:

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

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

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

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Computational Complexity

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

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

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Heuristic Algorithm

- Selecting the set of intersections to attack: **greedy algorithm**
- Choosing a schedule for each selected intersection: **iterate over extreme configurations**

Algorithm 1 Polynomial-Time Heuristic Algorithm for Finding an Attack

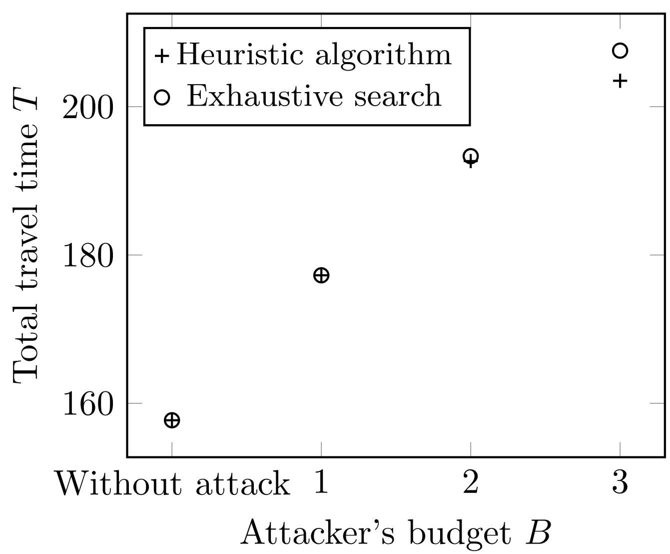
$\mathcal{A} \leftarrow (\emptyset, \emptyset)$
for $b = 1, \ldots, B$ **do**
  for $s \in \mathcal{S}$ **do**
    for $k \in \Gamma^{-1}(s)$ **do**
      $\mathcal{A}' \leftarrow \mathcal{A} \cup (\{s\}, \{\hat{p}_{ks} = 1, \forall j \neq k : \hat{p}_{js} = 0\})$
      if $T(\mathcal{A}') \geq T(\mathcal{A}^*)$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

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

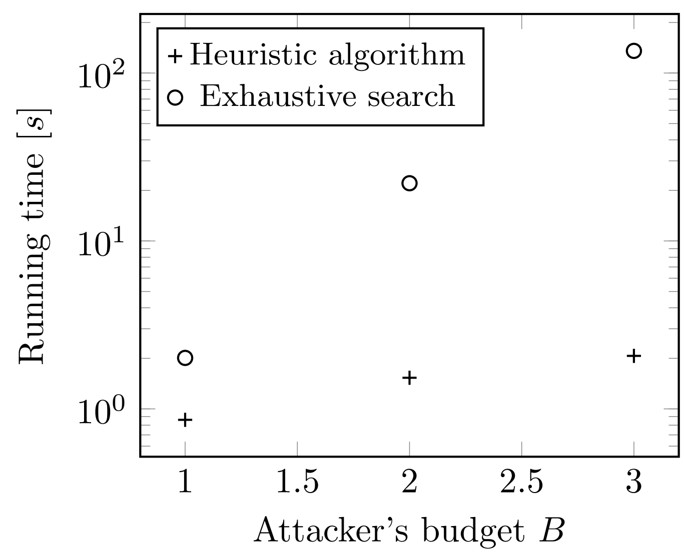
Numerical Results

* Grid model with Random Edges (GRE)
  * 250 random networks resembling real-world road networks
  * performed an exhaustive search and the proposed heuristic on each

Impact of Attacks



Running Time



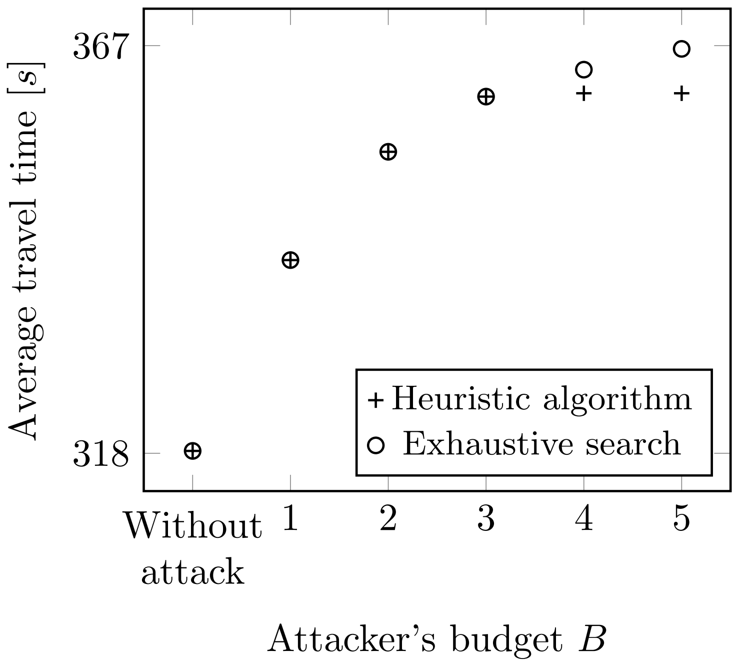
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Micro-Model Based Simulations

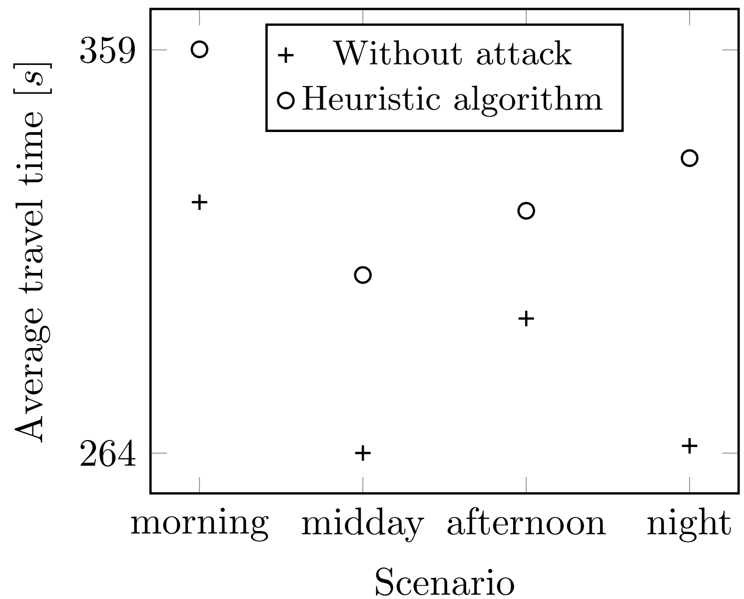
- SUMO simulator
  - widely-used microscopic traffic simulator
- Transportation network
  - Vanderbilt campus
  - from OpenStreetMap
- Traffic scenarios
  - morning commute
  - midday
  - afternoon commute
  - nighttime

Simulation Results

Comparison of Algorithms in the Morning Scenario



Comparison of Various Scenarios



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Conclusion & Future Work

* We proposed an approach and algorithm for evaluating the vulnerability of transportation networks
* We evaluated our approach and algorithm using a large number of random networks and a real-world road netwok
* Future work
  - configuring traffic signals in a resilient way, so that travel time remains low even if some of the signals are compromised
  - characterizing what makes a traffic signal an attractive target using graph-theoretic metrics, characteristics of the traffic flowing through the intersection, and centrality metrics

Thank you for your attention!

Questions?