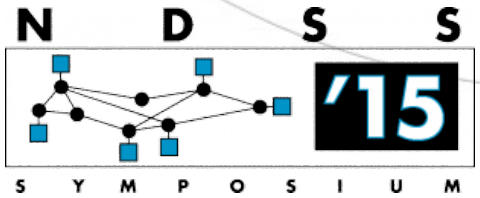
Congestion Attacks to Autonomous Vehicles Using Vehicular Botnets

Mevlut Turker Garip, Mehmet Emre Gursoy, Peter Reiher, Mario Gerla

Department of Computer Science
University of California Los Angeles



2015 NDSS SENT Workshop

Outline

- Introduction
- Problem Statement
- Congestion Attack
- Evaluation
- Conclusion

Introduction

- Extreme traffic in big cities
- Building roads not solution
- Load balancing
- Google Maps Traffic
- WAZE

VANETs

- Vehicular Ad hoc Network (VANET) is a wireless ad hoc network where each node is a vehicle
- Inter-vehicular communications are used for traffic safety and other applications to provide a better traffic experience
- By the standards of DSRC and 802.11p, vehicles broadcast their speed, location, angle, etc., to other vehicles
  - Proactive driving and collision avoidance

VANET Solutions

- State-of-the-art congestion avoidance mechanism: Computer-Assisted Traveling Environment (CATE)
- Dijkstra algorithm where roads are edges and travel times on the roads are link costs
- Big Dijkstra tables stored in each car, high computation cost of reconstructing Dijkstra table
- High network overhead due to broadcasting congestion info
- Does not scale, introduced further optimizations for our experiments

VANET Solutions
Our Optimizations

- Congestion request/response packets instead of constant broadcasting
- Installation of pre-calculated routes from any point to another point on the map
- Congestion measurement database to store congestion info learned

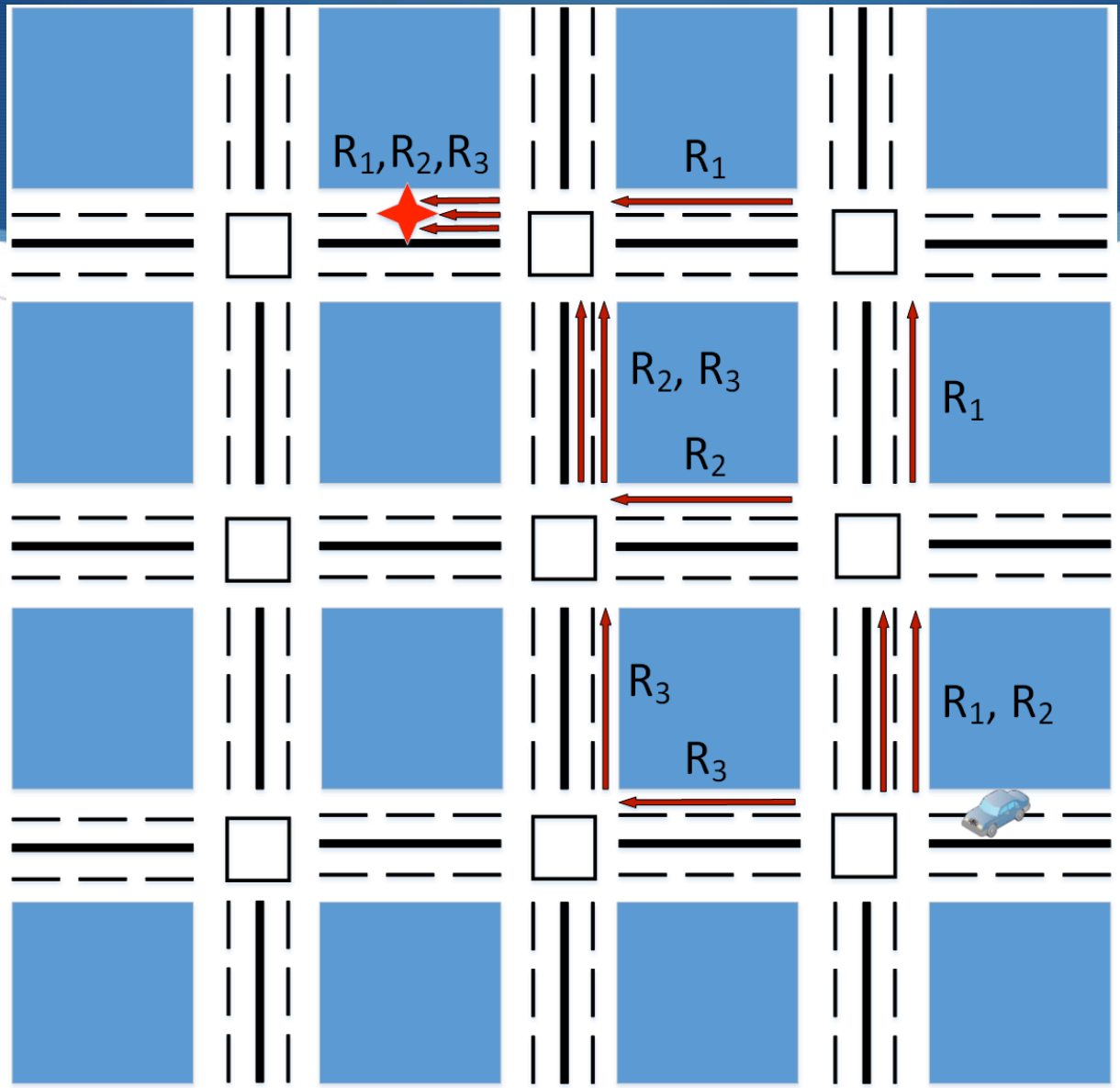
Packet Types

- Basic Safety Messages: each vehicle will listen to these packets from the cars on the same road and average the speeds heard including the speed of its own.
  - At the end of the road, this total average of speeds will be inserted to the car's congestion info database
- Congestion Request message will be sent when a car approaches to the end of a road to decide on the next turn
- Congestion Response message include the congestion measurements belonging to the interesting roads requested

Congestion Information Database

- Database of congestion measurements created by the car itself or learned from others
- Upon congestion request message, measurements for the roads that are asked in the message will be sent if exists
- Maintenance of this database and insertion/update procedures are explained in our paper in more detail

Congestion Attack



Vulnerabilities

- Common vulnerabilities in all of the proposed congestion avoidance mechanisms in the literature
- They completely trust and forward congestion information without trying to detect outliers and implausible information
- Checking incorrect information uses the assumption of "honest majority"
- Vehicular botnets are possible due to the vulnerabilities in autonomous cars (Examples are cited in the paper)

Vehicular Botnets

- To the best of our knowledge, our paper is the first that demonstrated a botnet attack in the realm of VANETs
- Current security solutions in the literature cannot cope with vehicular botnets (explained in the paper)
- Botnets enables various types of attacks to be performed on VANETs
- We chose congestion attack as the first demonstration of its potential power

Congestion Attack

- It is a representation of a much broader set of attacks that can be performed by vehicular botnets spreading bogus information
- It demonstrates the global impact of vehicular botnets on traffic conditions by the domino effect on the congestion levels
- It is like a DDoS attack to the roads which can be used for economic and political incentives
  - Fort Lee lane closure scandal against New Jersey Governor Chris Christie
  - delaying police arrival to a robbery scene, blocking emergency vehicle access to an area targeted by a terrorist attack, increasing congestion around a specific store to favor its competitor

Congestion Attack Compromised Cars

- Cars with a legitimate owner, which are compromised by attackers using the vulnerabilities in automated vehicles
- They optimize their routes with congestion avoidance mechanism just like any other car
- Cannot perform any suspicious action that might alert their owners
- They advertise malicious congestion data without their owners' knowledge

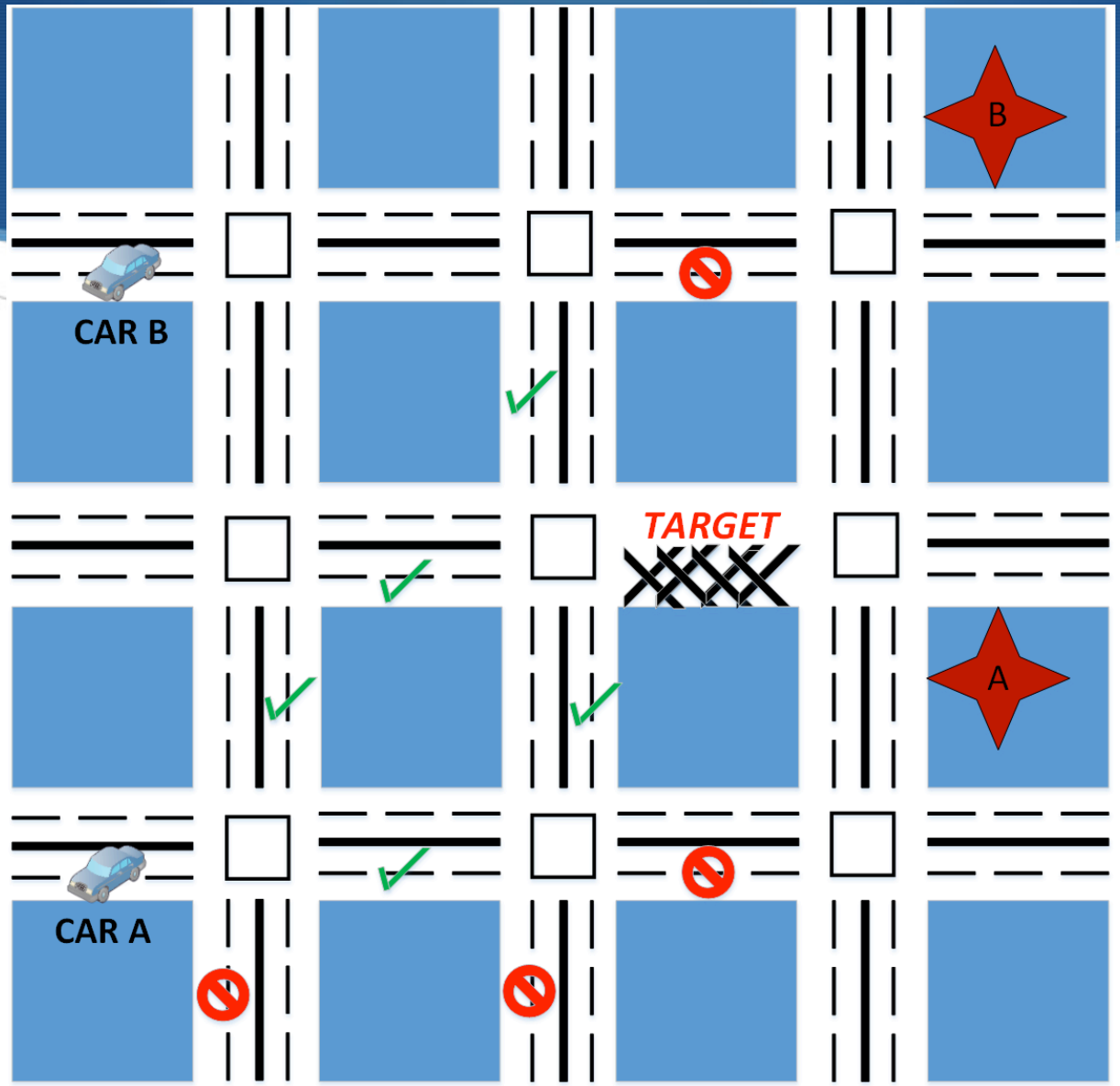
Congestion Attack
Parked Bot Cars

- Cars owned by the attacker, spread all around the map
- Parked in random places, mostly inactive until they are needed
- They advertise malicious congestion information if they are close to targeted road, if not, they stay inactive until needed
- When they sense there are uncovered areas in the targeted region, they become active and move there to cover those areas
- Significantly fresh measurements, complete knowledge of the map

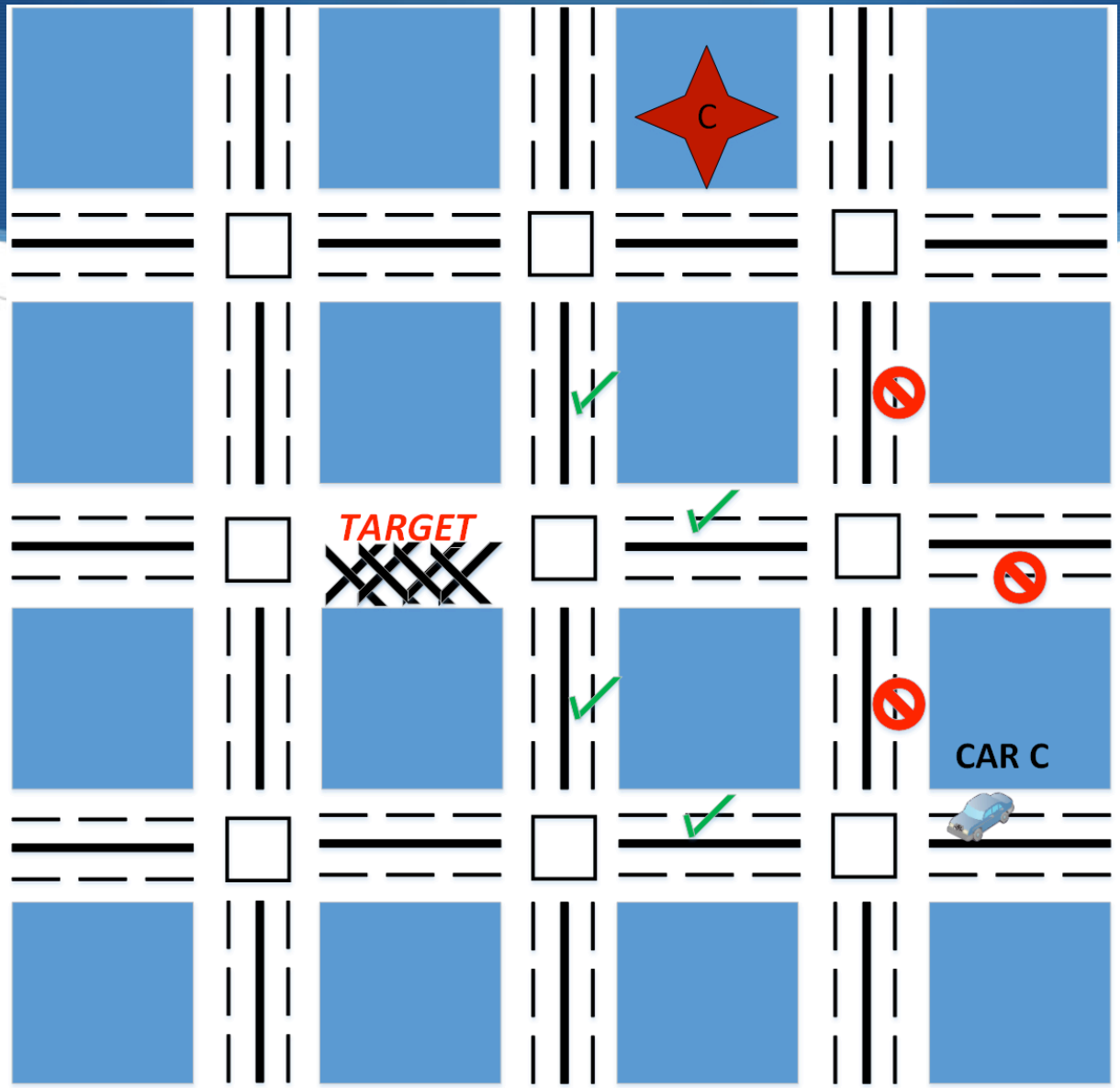
Congestion Attack Uninfected Cars

- They honestly follow the congestion avoidance mechanism
- They share the congestion measurements created by themselves and learned from others without malicious alteration
- They will "honestly" disseminate the bogus information learned from bot cars that will disseminate it to uncovered areas by bots

Congestion Attack



Congestion Attack



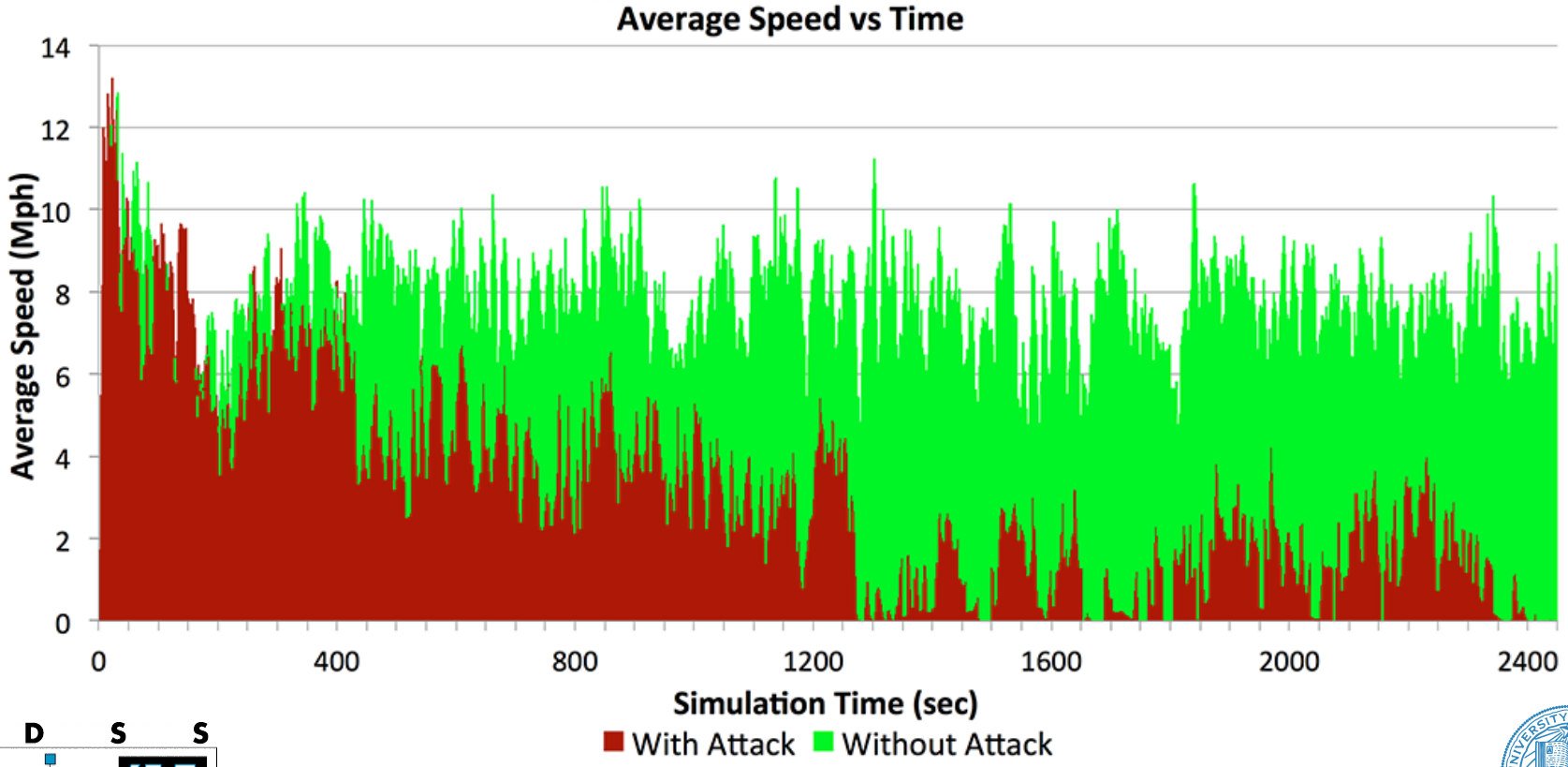
Maintaining Congestion

- Cars currently do not share partial measurements of a road
- Even if they did, once a victim get in the communication range to hear it directly from the cars in the targeted area, it is too late
- There will be many uninfected cars, which are not on the congested road, that will still disseminate our malicious congestion information
  - Does not forward congestion victim's warning signals due to timestamps
  - Help us build some majority with its help

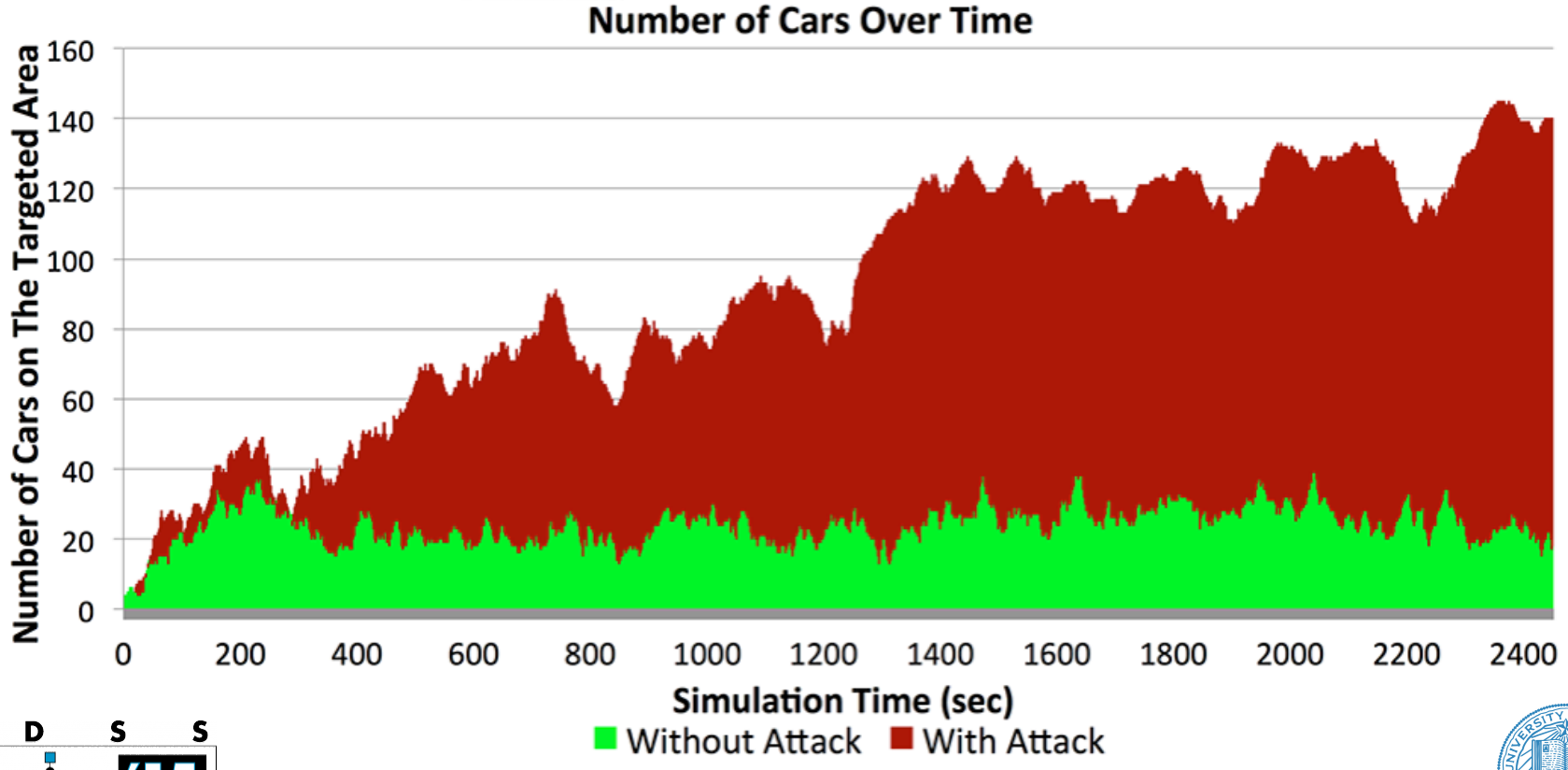
Evaluation

- Did not have an infrastructure to experiment on real autonomous vehicles in a big enough map
- Experimented in Veins (SUMO <-> OMNeT++)
- SUMO simulates the realistic mobility patterns of vehicles
- OMNeT++ simulates the inter-vehicular communication
- Congestion avoidance and botnet software implemented in Veins

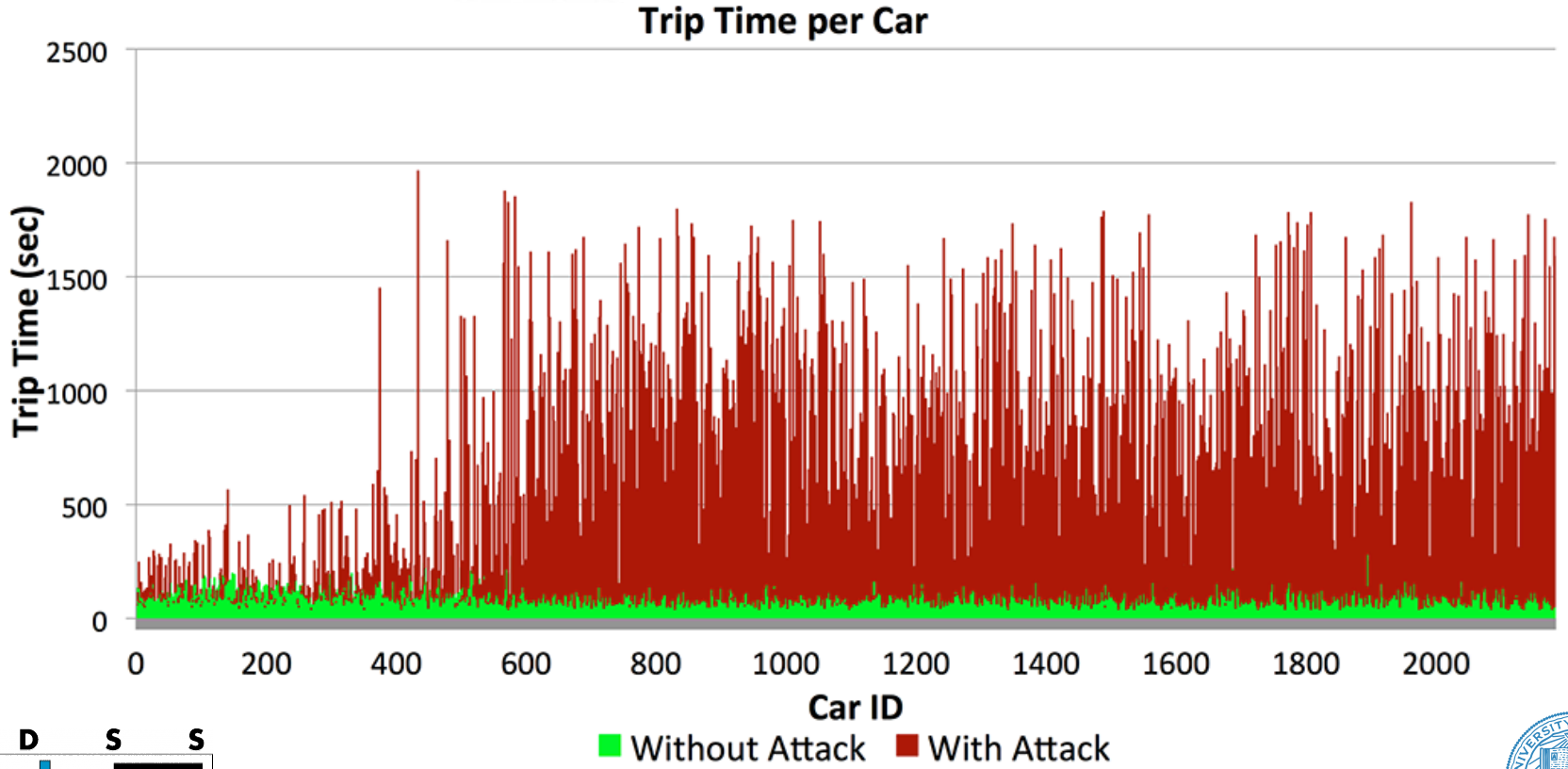
Evaluation
Average Speed on the Targeted Road



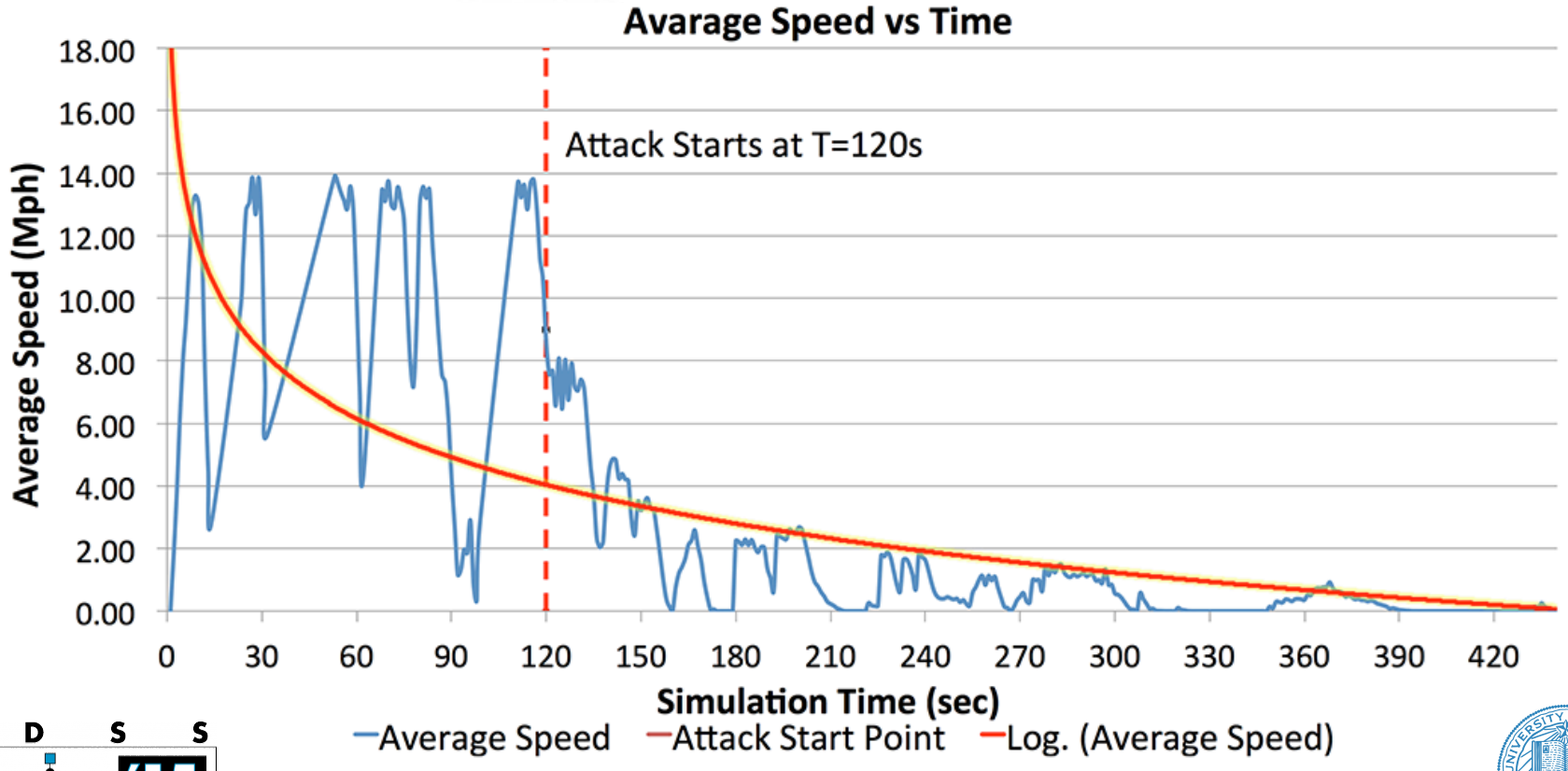
Evaluation
Number of Cars on the Targeted Road



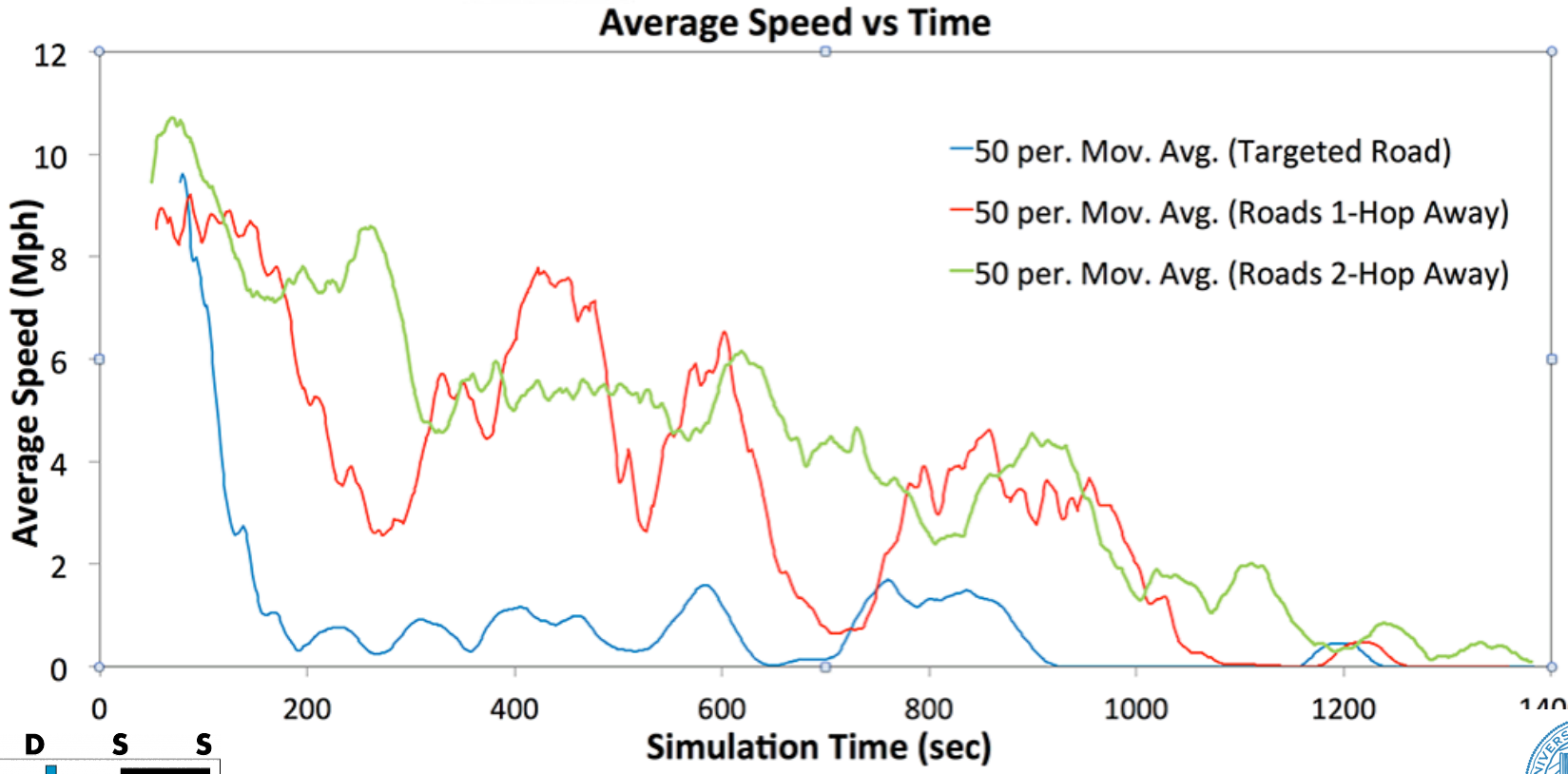
Evaluation
Trip Times for Individual Cars



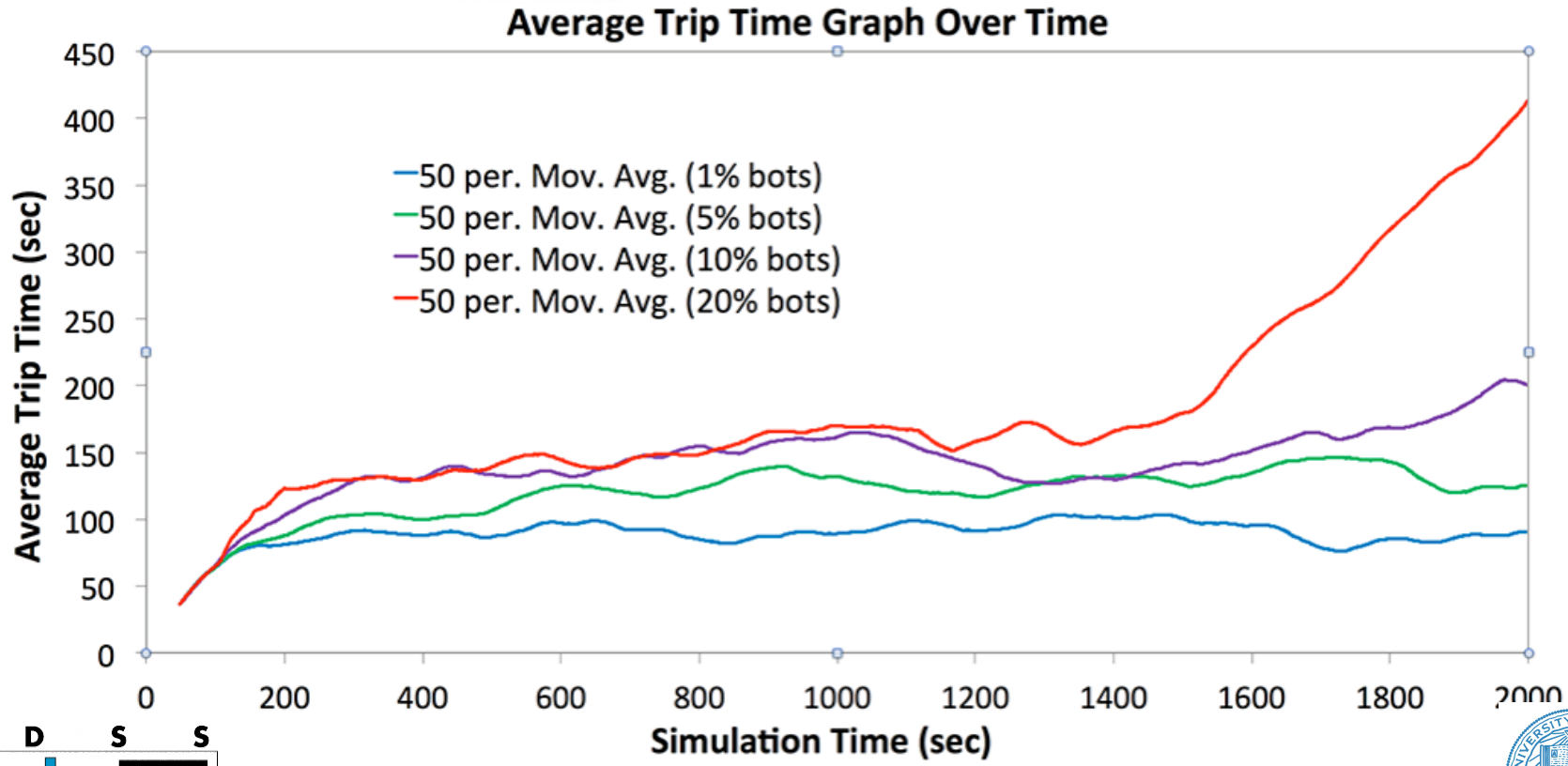
Evaluation
Speed of the Attack



Evaluation
Domino Effect



Evaluation
Changing Bot Percentages



Conclusion

- First that demonstrates vehicular botnets
- Current security solutions cannot cope with it
- Can cause congestion any targeted road
- Has a global effect on traffic congestion levels
- Targeted road becomes unusable quickly
- New security proposals should not overlook these botnets

Thank You

Q & A