Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control

Qi Alfred Chen, Yucheng Yin, Yiheng Feng, Z. Morley Mao, Henry X. Liu

Presented by Sezana Fahmida

Outline

- Introduction
- Background
- Threat Model
- Analysis Overview
- Data Spoofing Strategies
- Congestion Attack Analysis
- Exploit Construction
- Evaluation
- Defense Strategy

Introduction

- Connected Vehicle (CV) technologies to transform the transportation system
- Vehicles and infrastructures are connected through wireless
- USDOT launched CV pilot program in September,2016
- Under testing in three cities including NYC
- Aims to reduce traffic congestion
- Opens new doors for cyber attack!

Connected Vehicles

Introduction

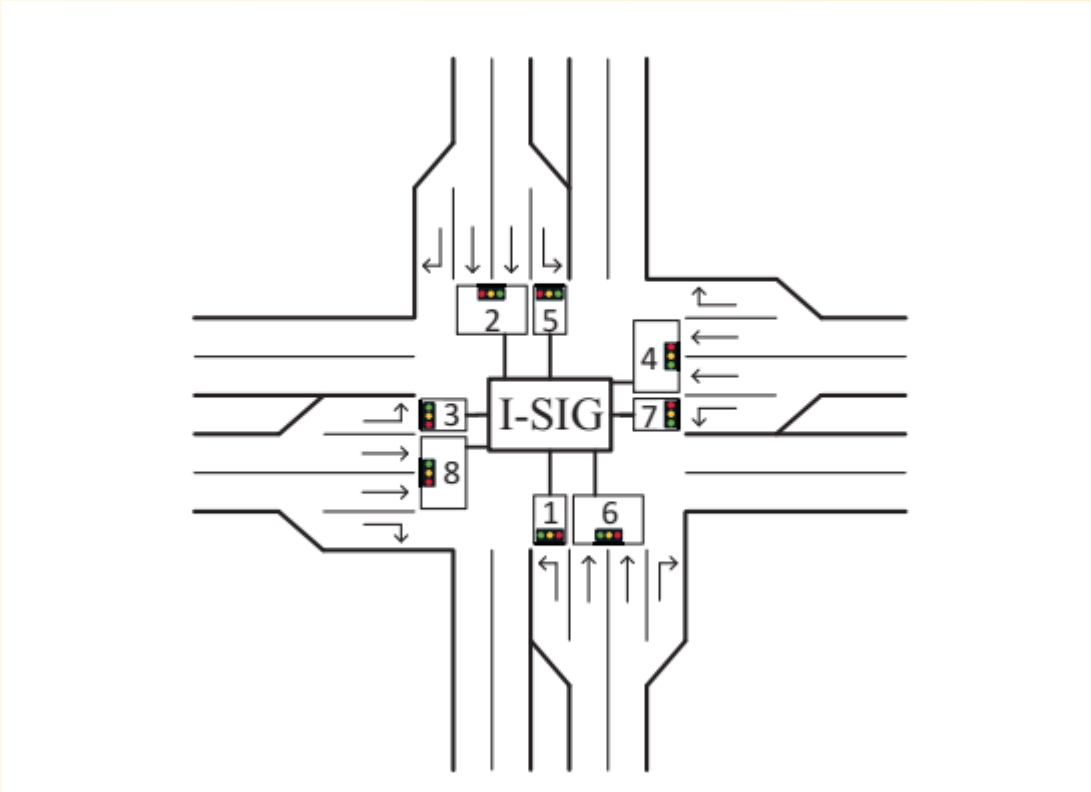
- This paper : Security analysis on CV-based transportation systems
- Target system: Intelligent Traffic Signal System (I-SIG)
- Used for traffic signal control
- Fully implemented and tested on real road intersections
- Achieved 26.6% reduction in total vehicle delay
- Authors aim : identification of fundamental security challenges
- Main focus on problems in signal control algorithm
- Design and implementation choices

Background

- CV technologies
- DSRC: Dedicated Short Range Communications protocol
- Dedicated Band allocated by FCC
- Vehicle to Vehicle (V2V) or Vehicle to Infrastructure(V2I) communications
- OBU (On Board Unit) & RSU (Road Side Unit)
- Vehicles use OBUs to broadcast basic safety messages (BSM)
- Equipped vehicles : with OBU
- Unequipped vehicles: without OBU
- Security and Credential management system (SCMS)

Background

- The I-SIG system
- Real time vehicle data leveraged for better traffic control
- Traffic Signals: Phases
- Operates on RSU



Background

- Configured with min and max green light time (t_{gmin}, t_{gmax},t_y,t_r)
- Signal Plan: setting t_g and phase sequence
- t_{gmin} <=t_g<= t_{gmax}
- 2 phase sequneces Ring 1 and 2
- Phases in same ring conflict
- Planned sequentially
- Broken down to stages
- Phases in former stage conflict with latter stage
- Stages are planned as a whole

Background

- Delay time : time to pass the intersection – free flow travel time
- Goal is to reduce the delay time for all vehicles
- Controlled Optimization of Phases (COP)
- Input : Estimated Arrival Time (to reach the stop bar)
- Uses DP to calculate optimal signal plan
- Releasing time based on queue length
- Delay= releasing time – arrival time
- If no vehicle, skips the phase

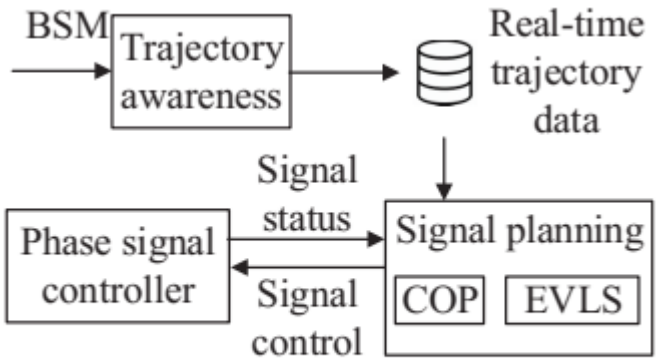


Fig. 4: The I-SIG system design.

Background

- Original Design: Unlimited stages to serve all vehicles
- I-SIG uses only two stages
- Only applies planned signal duration for the first stage, can not change order
- Can change duration and order of phases in second stage
- Limit in planning stages due to timing and resource constraints
- Finds plans with least unserved vehicles and chooses one with least delay

Background

- COP works if equipped devices >95%
- Need at least 25-30years to achieve 95% CV
- Transition Period: EVLS algorithm
- Estimation of Location and Speed
- Data from equipped devices used to estimate data for unequipped devices

Threat Model

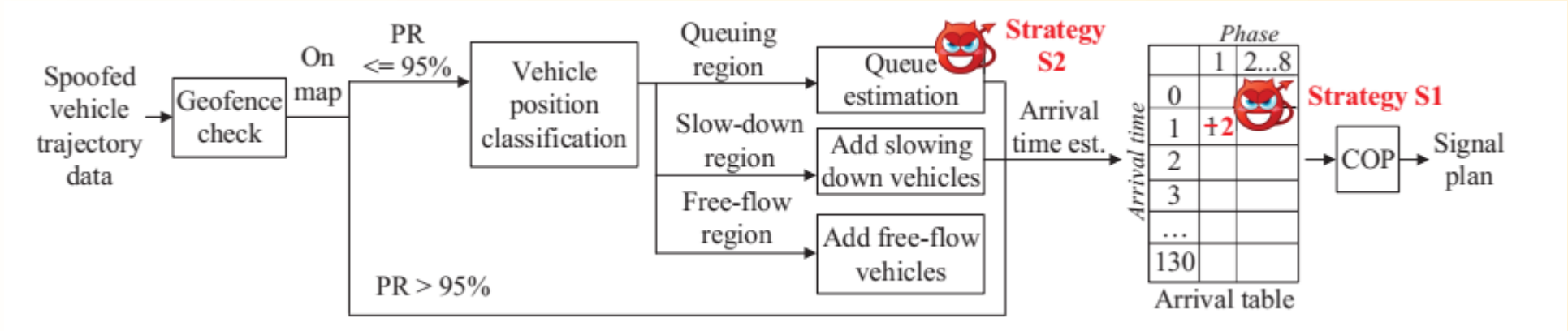
- Attack from vehicle side devices
- Malicious BSM messages with spoofed data
- Assumption : BSM messages are signed but data is spoofed
- Only one attack vehicle present in intersection
- Limited computation power for the attacker
- Signal control algorithm choices, configurations and intersection maps are known to the attacker
- Can receive BSM messages and can execute COP and EVLS

Analysis methodology

- Attack goal: Create congestion
- Data spoofing strategy identification
- Vulnerability Analysis for each attack goal
- Cause analysis and practical exploit construction
- Evaluation using simulations with real world intersection settings

Data spoofing strategy

- Attack input Data flow



Arrival Table

- 2D array (the estimated arrival time and phases)
- Element (i,j)-> number of vehicles for arrival time i at phase j
- First row : vehicles with zero arrival time
- COP uses arrival table to change the compute optimal total delay
- Attack goal: Change value in arrival table by spoofing

Transition Period

- Percentage of equipped vehicles -> PR
- PR <95% : transition period
- EVLS algorithm used to estimate unequipped devices
- three regions: (1) queuing region, including vehicles waiting in the queue with zero speed,
- slowdown region : vehicles slowing down because of the front vehicles
- free-flow region, vehicles away from the queue
- Estimates the number of vehicles in queue by dividing the length of the queuing region by the sum of the vehicle length and headway in queue

Spoofing Strategies

- Arrival Time and phase spoofing for both full deployment and transition periods
  - Set location and speed in BSM messages to increase value (i,j) in arrival table
- Queue length manipulation for the transition period only
  - Set the location of the farthest stopped vehicle by a BSM message

Congestion Attack Analysis

- Using standard configuration value and generic intersection VISSIM used to generate vehicles
- Snapshots are after running I-SIG
- PR levels 25%, 50% and 75% is used
- All data spoofing options are tried
- For each data spoofing trial, a new vehicle trajectory data entry with spoofed data is added to the traffic snapshot as attack input
- Attack effectiveness measured by total delay of all vehicles in the snapshot

Congestion Attack Analysis

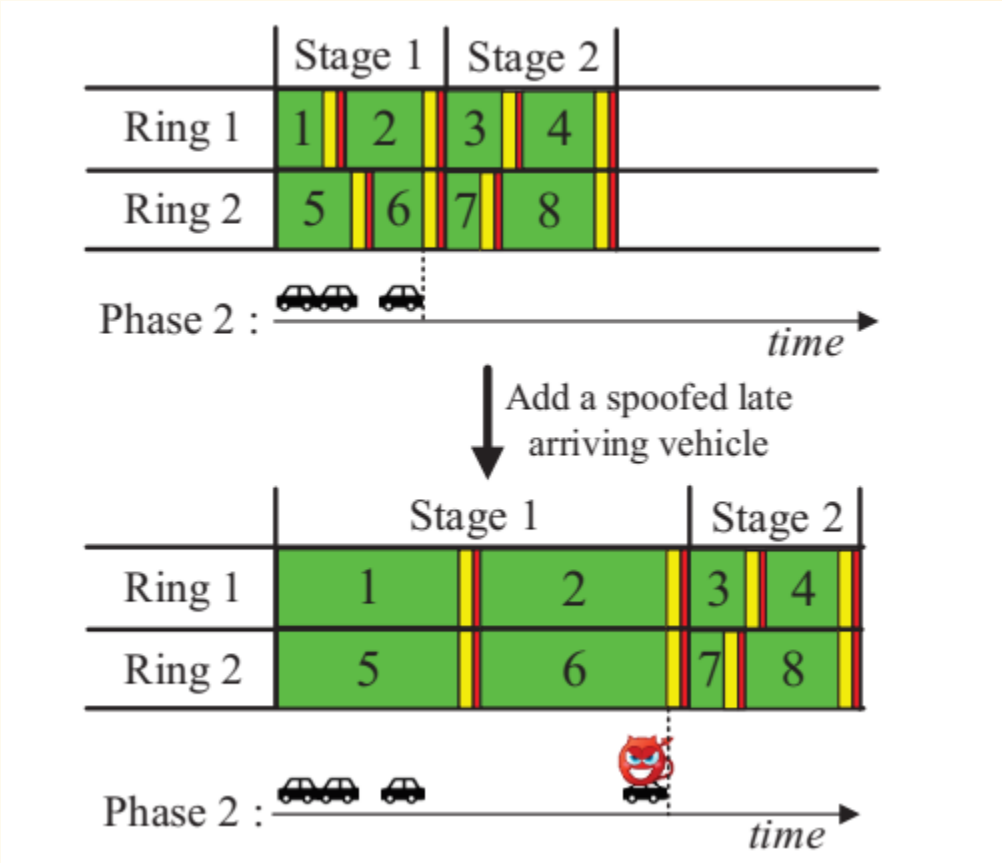
CV deployment	Full deployment		Transition period											
	100% PR		75% PR				50% PR				25% PR			
COP config.	2-S	5-S	2-S		5-S		2-S		5-S		2-S		5-S	
Strategy	S1	S1	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2
Vulnerability analysis (exhaustively try all data spoofing options)														
Success %	99.9%	96.4%	99.1%	98.3%	83.2%	96.8%	99.4%	99.2%	83.0%	97.4%	99.9%	98.9%	82.0%	91.6%
Ave. delay	1078.7	162.7	982.2	536.3	167.3	533.9	1001.3	536.2	206.6	569.6	1009.2	531.1	295.8	616.7
inc. (s) & %	68.1%	11.5%	60.2%	32.7%	10.6%	33.5%	61.4%	33.0%	12.5%	34.6%	60.6%	32.4%	17.0%	34.3%
Practical exploit (strategically try data spoofing options due to attack decision time limits in practice)														
Ave. trial #	3.8	13.3	3.8	N/A	N/A	14.7	3.8	N/A	N/A	23.9	3.6	N/A	N/A	28.8
Success %	99.8%	84.7%	99.1%	N/A	N/A	95.6%	99.4%	N/A	N/A	96.6%	99.8%	N/A	N/A	91.5%
Ave. delay	1077.4	119.8	1057.1	N/A	N/A	595.3	1061.0	N/A	N/A	591.7	1008.98	N/A	N/A	609.6
inc. (s) & %	68.0%	9.3%	60.0%	N/A	N/A	35.4%	61.2%	N/A	N/A	35.1%	60.6%	N/A	N/A	33.9%

Congestion Attack Analysis

- Full deployment period
- Strategy 1 (increasing arrival table entry value) increases total delay for 99.9% snapshots with 68.1% delay increase
- Cause: last vehicle advantage
- Most successful attack trial added a spoofed vehicle with very late arrival time
- Results in higher green light end time for requested phase
- Causes delay for all phases after it!!

Congestion Attack Analysis

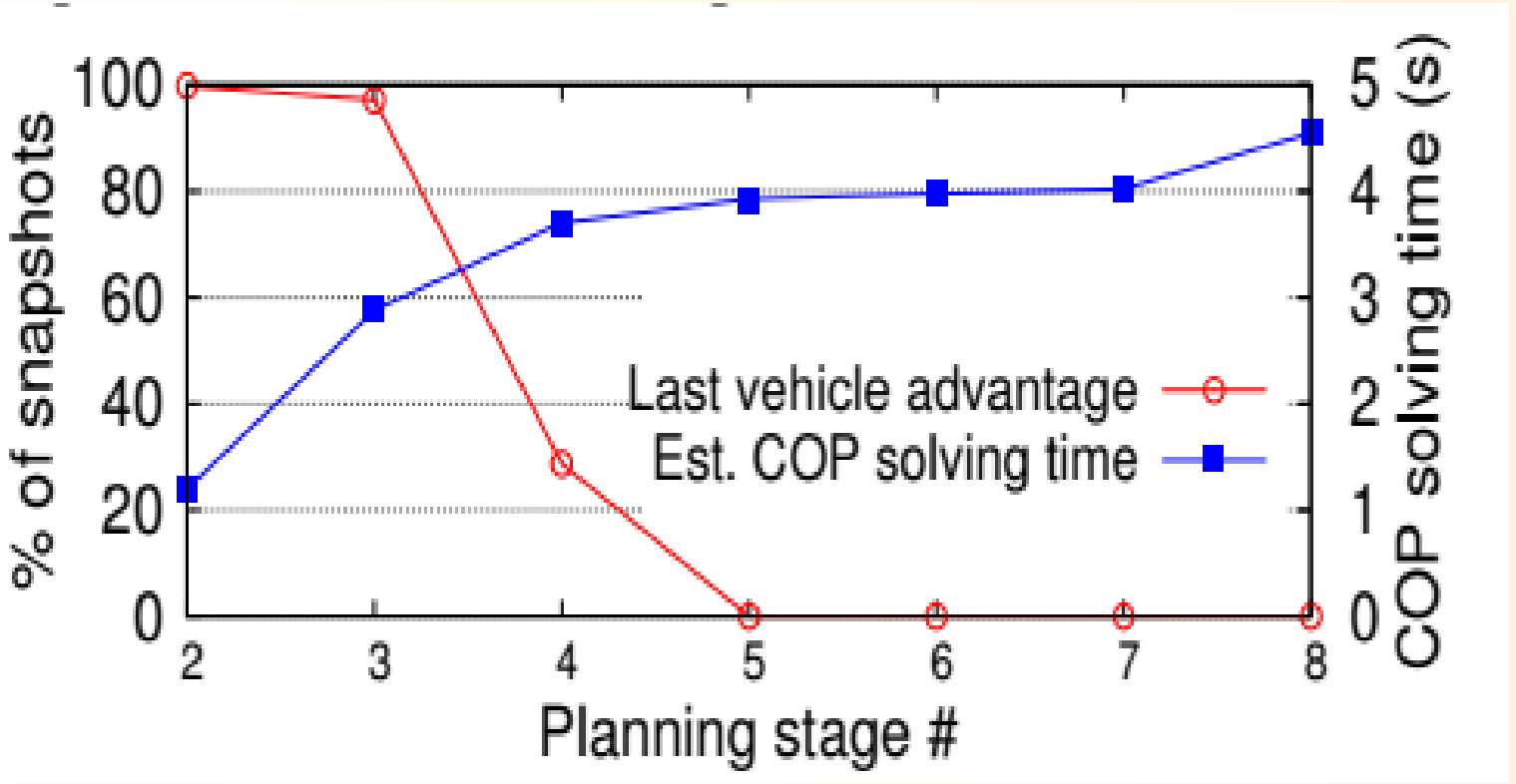
- Last vehicle advantage



Congestion Attack Analysis

- COP should just give up serving this very late vehicle
- Root cause lies in planning stage limitation
- In two stage planning, each phase can only be planned once
- COP tries to serve all vehicles at once, resulting in late vehicle advantage
- Trade off between security and deployability.
- Planning has to finish within 5-7 seconds
- RSU devices have limited computation power
- Adding more stages increases planning time

Congestion Attack Analysis



Congestion Attack Analysis

- Same attack strategy with Five-stage Planning is less effective
- Attacks cause 11.5% delay
- two types of effective spoofing trials
- Open a skipped phase
- Extend the green light end time.
- set the spoofed vehicle arrival time to a few seconds after the original green light end time for a phase
- COP extends the green light time to serve this vehicle (<4seconds)

Congestion Attack Analysis

- Transition Period
- Both S1 and S2 are tried
- Two stage planning: Late vehicle advantage is seen
- Five stage planning S2 dominates
- Best attack trial: for a certain phase, add the most non-existing unequipped vehicles.
- i.e., adding a farthest stopped vehicle using S2

Exploit Construction

- Real-time attack requirement
- Enumerating all data spoofing attacks takes time (>8minutes)
- Attack decision has to be made faster
- Budget-based attack decision
- When phase in the current stage turns yellow, attacker waits for 1 second & triggers the decision process
- $t_y + t_r$ is 6 seconds
- Decision time is 5 seconds

Exploit Construction

- Budget based data spoofing trial strategies
- E1: Congestion Attack for two stage planning
  - Late vehicle advantage
- E2: Congestion Attack for five stage planning in Full deployment
  - Opens skipped phases
  - Increase green light time
- Congestion Attack for five stage planning in Transition Period
  - Non-existing queuing of unequipped vehicles

Evaluation

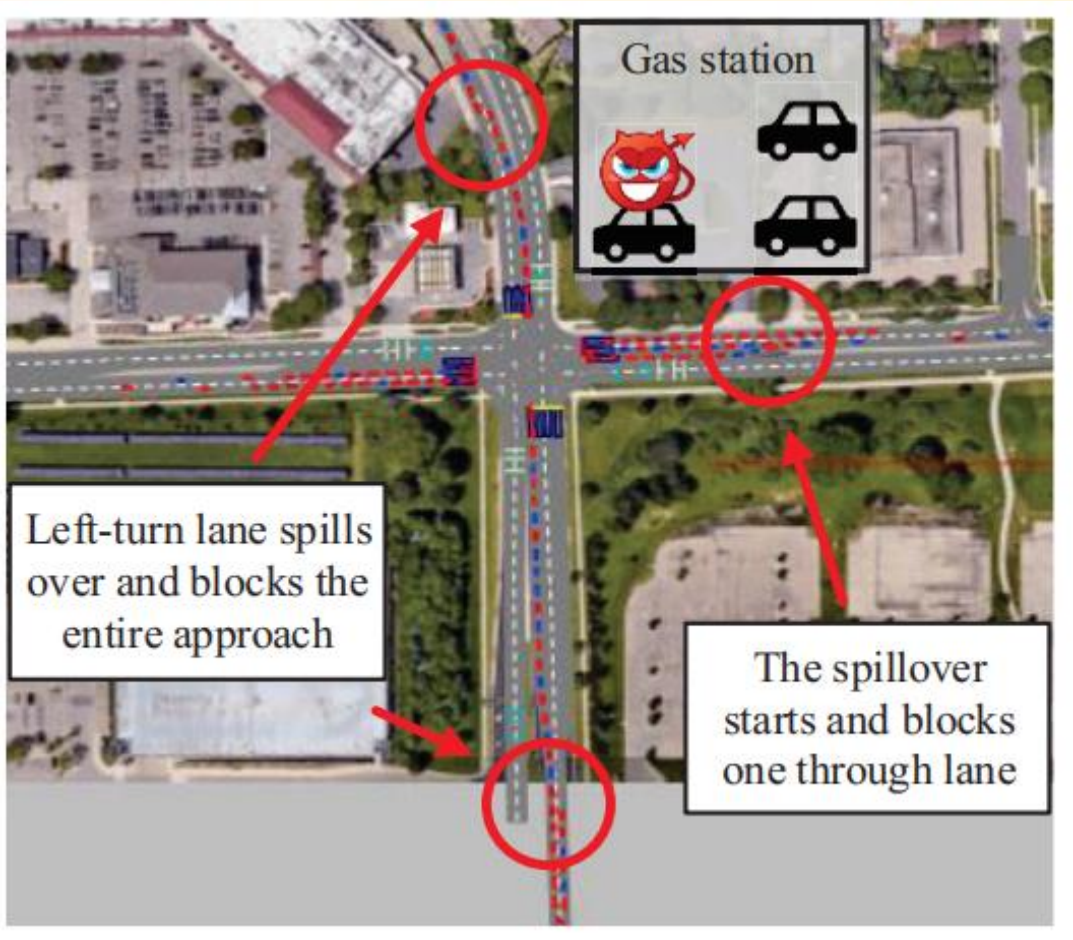
- E1 achieves 46.2% delay increase
- E2 is less effective as it is dependent on traffic conditions
- E3 is most effective (193.3% delay increase)

CV deployment	Full deployment		Transition period					
	100% PR		75% PR		50% PR		25% PR	
COP config.	2-S	5-S	2-S	5-S	2-S	5-S	2-S	5-S
Exploit	E1	E2	E1	E3	E1	E3	E1	E3
Ave. delay inc. (s) & %	68435.4	4695.9	64008.0	187746.0	66797.4	197410.0	56618.0	146685.0
	66.7%	4.8%	61.7%	181.6%	64.2%	193.3%	46.2%	133.2%

Evaluation

- The lane blocking effect
- In five stage planning continuous attack accumulates attack effect
- Delayed planning of attack vehicles causes more delays
- Can block entire approach
- Queues in the left-turn lane start to spill over to the through lanes and block the through lane.
- Through lane to start queuing after the spilled-over left-turn vehicles
- COP assigns minimum green light to left turn lane to clear the thorough lane

Evaluation


Gas station
Left-turn lane spills over and blocks the entire approach
The spillover starts and blocks one through lane

Defense Strategies

- Robust algorithm design for the transition period
- Performance improvement for RSUs
- Data spoofing detection using infrastructure-controlled sensors

THANK YOU!!!