Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control

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

University of Michigan
Background: Connected Vehicle technology

- Wirelessly connect vehicles & infrastructure
- **Goal:** Dramatically improve mobility, safety, environmental impact, & public agency operations

**CV = Connected Vehicle**

**OBU = On-Board Unit**

**RSU = Road-Side Unit**
Background: Recent advances

- Will **soon** transform transportation systems today
- 2016.9, USDOT launched **CV Pilot Program**
  - National effort to deploy, test, & operationalize CV-based transportation systems
  - Launched in **3 sites**
Cybersecurity of CV-based transportation

• However, such dramatically increased connectivity also opens a new door for cyber attacks

• Highly important to understand potential security vulnerabilities & new security challenges
  – Need to ensure security & safety for vehicles, transportation infrastructure, drivers & pedestrians
  – Need to perform study now so that they can be proactively addressed before nationwide deployment
First security analysis of CV-based transp.

- **Target**: Intelligent Traffic Signal System (I-SIG)
  - Use real-time CV data for intelligent signal control
  - USDOT sponsored design & impl.
  - Fully implemented & tested in Anthem, AZ, & Palo Alto, CA
    - 26.6% reduction in total vehicle delay
  - Under deployment in NYC and Tampa, FL

*CV = Connected Vehicle, OBU = On-Board Unit, RSU = Road-Side Unit*
Threat model

- Malicious vehicle owners deliberately control the OBU to send spoofed data
  - OBU is compromised physically\(^1\), wirelessly\(^2\), or by malware\(^3\)
- Can only spoof data, e.g., location & speed
  - Can’t spoof identity due to USDOT’s vehicle certificate system

---

1 Koscher et al. @ IEEE S&P’10  
2 Checkoway et al. @ Usenix Security’11  
3 Mazloom et al. @ Usenix WOOT’16
Attack goal

• Create **traffic congestion**
  – Increase total delay of vehicles in the intersection
    • *Directly subvert the design goal of I-SIG*
  – **Damage**: City functions & individual (wasted fuel, time)
  – **Incentive**: Politically or financially
Analysis approach overview

Analysis of Attack input data flow

Source code
Traffic snapshots from simulator

Dynamic analysis
Spoofing option enum
Increased delay calc

Data spoofing strategies

Spoofing w/ top delay inc
Congestion creation vuln.

Real-time attack requirement (e.g., decision time ≤ 4 sec)

Exploit construction

Congestion creation exploit
Analysis result summary

Analysis of Attack input data flow

2 strategies

Data spoofing strategies

2 types of vuln.:
#1: Curse of transition period
#2: Last vehicle advantage

Dynamic analysis

Spoofing option enum → Increased delay calc

Real-time attack requirement (e.g., decision time ≤ 4 sec)

Exploit construction

Spoofing w/ top delay inc

Congestion creation vuln.

Source code

Traffic snapshots from simulator

Real-time attack requirement (e.g., decision time ≤ 4 sec)
Vuln #1: Curse of transition period

- I-SIG has 2 operation modes based on PR:
  - PR ≥ 95%, full deployment: Directly run an optimal signal planning algorithm
  - PR < 95%, transition: The optimal algorithm becomes ineffective, use an unequipped vehicle estimation algorithm as pre-step

PR ≥ 95%

Yes (full deployment period)

No (transition period)

Unequipped vehicle estimation

Optimal signal planning algorithm

Vulnerable

PR = Penetration Rate
Vulnerable queue estimation

- Find the queue estimation part highly vulnerable
  - Data from *one single attack vehicle* can add a queue with tens of “ghost” vehicles
  - Cause delay increased by 20-50%, sometimes even > 70%
An urgent & fundamental problem

- An **urgent** problem for the current design
  - Transition period is **unavoidable**, and **long** *(25-30 yrs est. by USDOT)*
  - First thing needs to be resolved for its deployment in practice

- **Fundament cause:** Lack a sufficiently robust signal control algorithm for the transition period
  - Low PR is **inherently more sensitive** to data spoofing
    - *Fundamentally more challenging to ensure robustness*
  - Need joint research effort in both transportation & security communities
Full deployment period is secure?

PR ≥ 95%

Yes (full deployment period)

No (transition period)

Unequipped vehicle estimation

Optimal signal planning algorithm

Vulnerable

PR = Penetration Rate
Vuln #2: Last vehicle advantage

• **Vulnerability**: Latest arriving vehicle determines signal plan
• **Attack**: Spoof to arrive as late as possible to increase the delay of queuing vehicles in other directions
• **Fundamental cause**: *Security vs deployability trade-off*
  – Limited decision time forces choice of a sub-optimal config.
  – Such sub-optimal config unexpectedly exposes such vuln.

Spoof to arrive as late as possible!
Attack video demo

• Demo time!
Defense discussion

• Robust algorithm design for the transition period
  – Inherently challenging, need joint research efforts in both transportation & security communities

• Speed-up control algorithm to avoid sub-optimal config.
  – E.g., offload computation to a nearby workstation or cloud

• Data spoofing detection using infrastructure-controlled sensors, e.g., camera
  – Cross check validity of driving data from OBUs

---

CV = Connected Vehicle  
OBU = On-Board Unit  
RSU = Road-Side Unit
Conclusion

• The **first security analysis** of a CV based transportation system, I-SIG
  – Discover new vulnerability & analyze causes
    • *Current control algorithm design & config. are highly vulnerable*
  – Construct & evaluate exploits to show the severity in practice
  – Propose defense directions based on the analysis insights

• Hope to inspire follow-up studies
  – E.g., other attack goals, other types of CV systems (*60+ open sourced*), defense solutions

• Reported to USDOT CV Pilot Program office & sites (NYC and Tampa)

[https://tinyurl.com/congestion-attack](https://tinyurl.com/congestion-attack)
• Questions?