Insider Vs. Outsider Threats to Autonomous Vehicle Platooning

Soodeh Dadras and Prof. Chris Winstead

Department of Electrical and Computer Engineering, Utah State University
Executive Summary

❖ Autonomous Vehicle platooning
  ➢ Platooning Pros and challenges
  ➢ Platooning research questions

❖ Security in Platooning
  ➢ Security of Vehicular Network
  ➢ Security of Control Systems

❖ Security of Control system in platoon
  ➢ Platoon Model
  ➢ Insider and Outsider Attacks Design
  ➢ Consequences of the attacks and comparison

❖ Conclusion
Outline

- Introduction
- Security of Vehicle Platooning
- Insider and Outsider Attacks
- Results
- Conclusion
Autonomous Vehicle Platooning

- **Autonomous Vehicle:**
  The car that drives itself.

- **Platooning:**
  Group of Autonomous vehicles travelling together with relatively small spacing to improve capacity of highways and to minimize the relative velocity of the vehicles.
Platoon and Level of Automation

HUMAN DRIVER MONITORS DRIVING ENVIRONMENT

- No Automation
- Driver Assistance
- Partial Automation
- Conditional Automation

AUTOMATED DRIVING SYSTEM MONITORS DRIVING ENVIRONMENT

- High Automation
- Full Automation

Platoon
**AUTOMATION LEVELS OF AUTONOMOUS CARS**

**LEVEL 0**
There are no autonomous features.

**LEVEL 1**
These cars can handle one task at a time, like automatic braking.

**LEVEL 2**
These cars would have at least two automated functions.

**LEVEL 3**
These cars handle “dynamic driving tasks” but might still need intervention.

**LEVEL 4**
These cars are officially driverless in certain environments.

**LEVEL 5**
These cars can operate entirely on their own without any driver presence.

**SOURCE:** SAE International

**BUSINESS INSIDER**
Platooning Pros and Challenges

Pros:
- Safety
- Operational Efficiency (Increase highway capacity)
- Driving Comfort
- Transit time Efficiency

Challenges:
- Computer failure
- Degrading performance in case of interception
- Increase in crashes involving pedestrians
Platooning Research Challenges:

- Reliability
- System Security
Outline

• Introduction

● Security of Vehicle Platooning
  • Insider and Outsider Attacks
  • Results

• Conclusion
Attractive Targets:

Oakland 2010

CHES 2013

BlackHat 2015, 2016
Examples of attack on vehicular network

<table>
<thead>
<tr>
<th>Security issues</th>
<th>Attacks[1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Jamming attack; DoS attack.</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Eavesdropping attack; Man in the middle attack.</td>
</tr>
<tr>
<td>Authentication</td>
<td>GPS spoofing; Impersonation attack; Masquerading attack; Message tampering.</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>Replay attack; Message modification attack.</td>
</tr>
</tbody>
</table>
## Examples of attack on Platoon Control Systems

<table>
<thead>
<tr>
<th>Security issue</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control algorithm modification</td>
<td>Destabilizing attack[2]; High-speed collision induction attack[3]; Traffic flow instability attack[6,7].</td>
</tr>
<tr>
<td>Sensor reading tampering</td>
<td>False data injection[5]; Efficiency-motivated attack[4].</td>
</tr>
</tbody>
</table>
Configuration of Autonomous Vehicles

Human-machine Interface

- Camera
- Radar
- Lidar
- GPS
- IMU
- Ultrasonic sensor
- Wireless comm.

Multi-sensor data fusion

Mission Planner

Behavior Planner

Path Planner

Upper-Level Controller

Lower-Level Controller

Vehicle System

Driver Behavior & Interaction

Performance Index
- Safety
- Fuel Economy
- Ride Comfort
- Smoothness
- Emission
Cooperative Adaptive Cruise Control

Upper level controller
The upper level controller determines the desired acceleration of automated vehicle based on measured range, range rate, speed, and acceleration. **We only study longitudinal control not lateral control in this work.**

Lower level controller
The lower level controller manipulates the engine and brake actuators to track the desired acceleration, which is estimated in the upper level controller with the feedback acceleration information.
**Platoon Model**

Each vehicle receives measurement through its sensors. **No communication is considered between vehicles.**

\[ x_i, \text{ car } i\text{'s position} \]
\[ v_i, \text{ car } i\text{'s velocity} \]
\[ \sigma_{\text{ref}}, \text{ desired separation} \]

\[ u_i = k_p(x_{i+1} - x_i - \sigma_{\text{ref}}) + k_p(x_{i-1} - x_i + \sigma_{\text{ref}}) + k_d(v_{i+1} - v_i) + k_d(v_{i-1} - v_i) \]

with \( k_p \) position gain and,
with \( k_d \) velocity gain
Platoon Performance
Outline

• Introduction
• Security of Vehicle Platooning
  • Insider and Outsider Attacks
• Results
• Conclusion
Who Is the Attacker?

A single actor in control of a vehicle who attempt to disrupt the platoon.

- **Outsider**: Has NO prior knowledge of control law and only modify its motion.
- **Insider**: Modifying the control law and its motion.
Attacks Objectives

Disrupting system performance and cause collisions
Outline

• Introduction
• Security of Vehicle Platooning
• Insider and Outsider Attacks
• Results
• Future Works
Outsider Attack Results

Let’s consider desired spacing between each vehicle is $\delta_{\text{ref}} = d(m)$ and $d > 0$. Then attacker can cause collision if $\text{spacing} \geq -d$.

Attacker is at the end of 5-vehicle platoon.
Insider Attack Results

Attacker is at the end of 5-vehicle platoon.
Outline

• Introduction

• Security of Vehicle Platooning

• Insider and Outsider Attacks

• Results

• Conclusion
Conclusion

The results clearly indicate that:
Both insider and outsider attackers can cause collisions.

But,
Insider attacker performs more powerful attack that results in catastrophic collisions.
Bibliography


Thank you
Backup slides
Level 0 _ No Automation **System capability:** None. • **Driver involvement:** The human at the wheel steers, brakes, accelerates, and negotiates traffic. • **Examples:** A 1967 Porsche 911, a 2018 Kia Rio.

Level 1 _ Driver Assistance **System capability:** Under certain conditions, the car controls either the steering or the vehicle speed, but not both simultaneously. • **Driver involvement:** The driver performs all other aspects of driving and has full responsibility for monitoring the road and taking over if the assistance system fails to act appropriately. • **Example:** Adaptive cruise control.

Level 2 _ Partial Automation **System capability:** The car can steer, accelerate, and brake in certain circumstances. • **Driver involvement:** Tactical maneuvers such as responding to traffic signals or changing lanes largely fall to the driver, as does scanning for hazards. The driver may have to keep a hand on the wheel as a proxy for paying attention. • **Examples:** Audi Traffic Jam Assist, Cadillac Super Cruise, Mercedes-Benz Driver Assistance Systems, Tesla Autopilot, Volvo Pilot Assist.

Level 3 _ Conditional Automation **System capability:** In the right conditions, the car can manage most aspects of driving, including monitoring the environment. The system prompts the driver to intervene when it encounters a scenario it can’t navigate. • **Driver involvement:** The driver must be available to take over at any time. • **Example:** Audi Traffic Jam Pilot.
**Level 4 _ High Automation** *System capability:* The car can operate without human input or oversight but only under select conditions defined by factors such as road type or geographic area. • *Driver involvement:* In a shared car restricted to a defined area, there may not be any. But in a privately owned Level 4 car, the driver might manage all driving duties on surface streets then become a passenger as the car enters a highway. • *Example:* Google’s now-defunct Firefly pod-car prototype, which had neither pedals nor a steering wheel and was restricted to a top speed of 25 mph.

**Level 5 _ Full Automation** *System capability:* The driverless car can operate on any road and in any conditions a human driver could negotiate. • *Driver involvement:* Entering a destination. • *Example:* None yet, but Waymo—formerly Google’s driverless-car project—is now using a fleet of 600 Chrysler Pacifica hybrids to develop its Level 5 tech for production.
Driver

- **Eyes On, Hands On**
  - Driver is continuously exercising longitudinal AND lateral control.

- **Eyes On, Hands Off**
  - Driver is continuously exercising longitudinal OR lateral control.

- **Temporary Hands Off**
  - Driver has to monitor the system at all times; must always be in a position to resume control.

Vehicle

- **Eyes Off, Hands Off**
  - Driver does not have to monitor the system at all times; must always be in a position to resume control.

- **Non-Monitoring Driving**
  - Driver is not required during defined use case.

**Level**

- **Level 0**
  - Lateral or longitudinal control is accomplished by the system.

- **Level 1**
  - System has longitudinal and lateral control in a specific use case.

- **Level 2**
  - System has longitudinal AND lateral control in a specific use case. System recognizes the performance limits and requests driver to resume control within a sufficient time margin.

- **Level 3**
  - System can cope with all situations automatically in a defined use case.

- **Level 4**
  - System can cope with all situations automatically during the entire journey. No driver required.

**Vehicle Role**

- **Driver Only**
- **Assisted**
- **Partial Automation**
- **Conditional Automation**
- **High Automation**
- **Full Automation**
Security Issues in Platoon

1-Security in Vehicular network

- Availability
- Confidentiality
- Data integrity
- Authentication
- Non-repudiation
Vehicle Model

Each vehicle in platoon:
Point Mass Model obeying Newton’s laws
(Double Integrator system)

\[ x : \text{position}; \]
\[ \dot{x} = v : \text{velocity}; \]
\[ \ddot{x} = \dot{v} = a : \text{acceleration}; \]
\[ m = \text{mass}; \]
\[ F = u = ma : \text{control input}. \]
Platooning Control Policy

Inter-vehicle spacing Policies:

- Constant Spacing Policy (CSP),
- Variable Time Gap (VTG),
- Constant Time Gap (CTG).
Platoon Information Flow

- **Follower-predecessor:**

  Vehicle States: \( x_1, v_1 \quad x_2, v_2 \quad x_3, v_3 \quad \ldots \quad x_n, v_n \)

  Cars: 1 \( \rightarrow \) 2 \( \rightarrow \) 3 \( \ldots \) \( \rightarrow \) \( n \)

  Direction of travel

  Vehicle \#n: Leader
## Platoon Control laws

### Control algorithm

<table>
<thead>
<tr>
<th>Control algorithm</th>
<th>Policy</th>
<th>Inter-veh-comm</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\ddot{x}<em>i = k_p (x</em>{i+1} - x_i - \sigma_{\text{ref}}) + k_p (x_{i-1} - x_i + \sigma_{\text{ref}}) + k_d (\ddot{x}_{i+1} - \ddot{x}<em>i) + k_d (\dot{x}</em>{i-1} - \dot{x}_i)$</td>
<td>CSP</td>
<td>No</td>
</tr>
<tr>
<td>$\ddot{x}<em>i = k_p (x</em>{i+1} - x_i - h \dot{x}<em>i) + k_d (\dot{x}</em>{i+1} - \dot{x}_i)$</td>
<td>CTG</td>
<td>No</td>
</tr>
</tbody>
</table>
Platoon Model

State Space representation (absolute coordinate 2n states and error (2n-2) states for n vehicles)

\[ x = Ax + Bu \]
\[ \dot{y} = Cx + Du \]

Absolute coordinate states \( x_i \) and \( v_i \)

Error coordinate

\[ z_i = x_i - x_{i+1}; \]
\[ y_i = v_i - v_{i+1} \]