SRS STUDENT RESEARCH SYMPOSIUM

Insider Vs. Outsider Threats to Autonomous Vehicle Platooning

Soodeh Dadras and Prof. Chris Winstead

Department of Electrical and Computer Engineering,
Utah State University

UtahState University

4/12/2018

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:

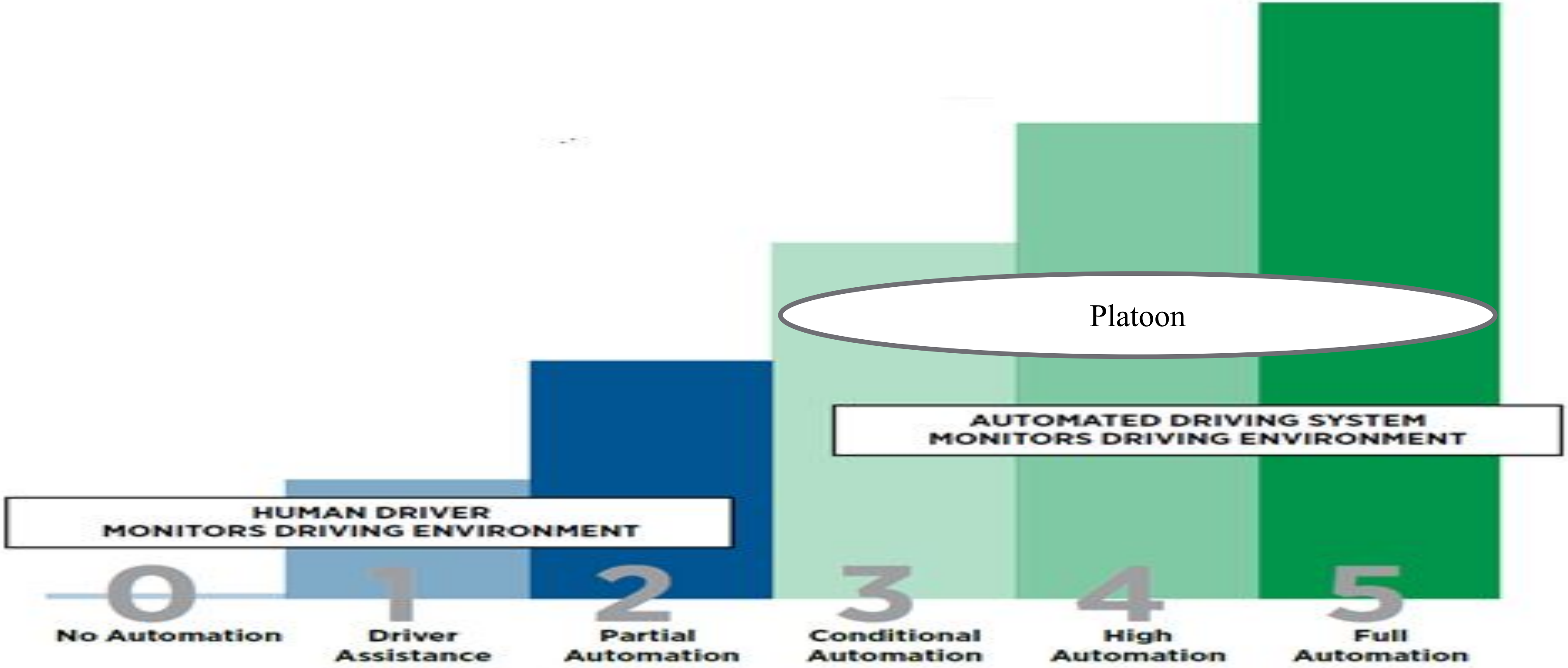
The car that drives itself.

- 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.

Image Source: https://www.fhwa.dot.gov/advanced-research/pubs/12033/004.cfm

Platoon and Level of Automation



AUTOMATION LEVELS OF AUTONOMOUS CARS

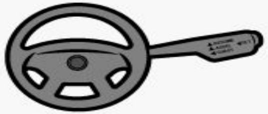
LEVEL 0

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:

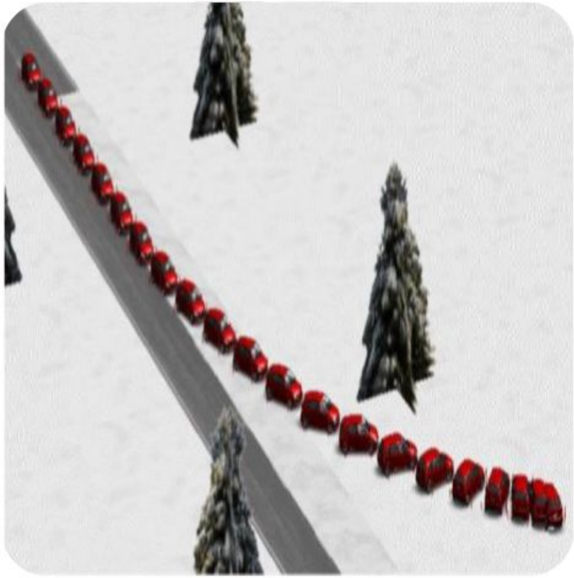
- Reliability
- System Security

Outline

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

Attractive Targets:

Oakland 2010



CHES 2013

BlackHat 2015, 2016

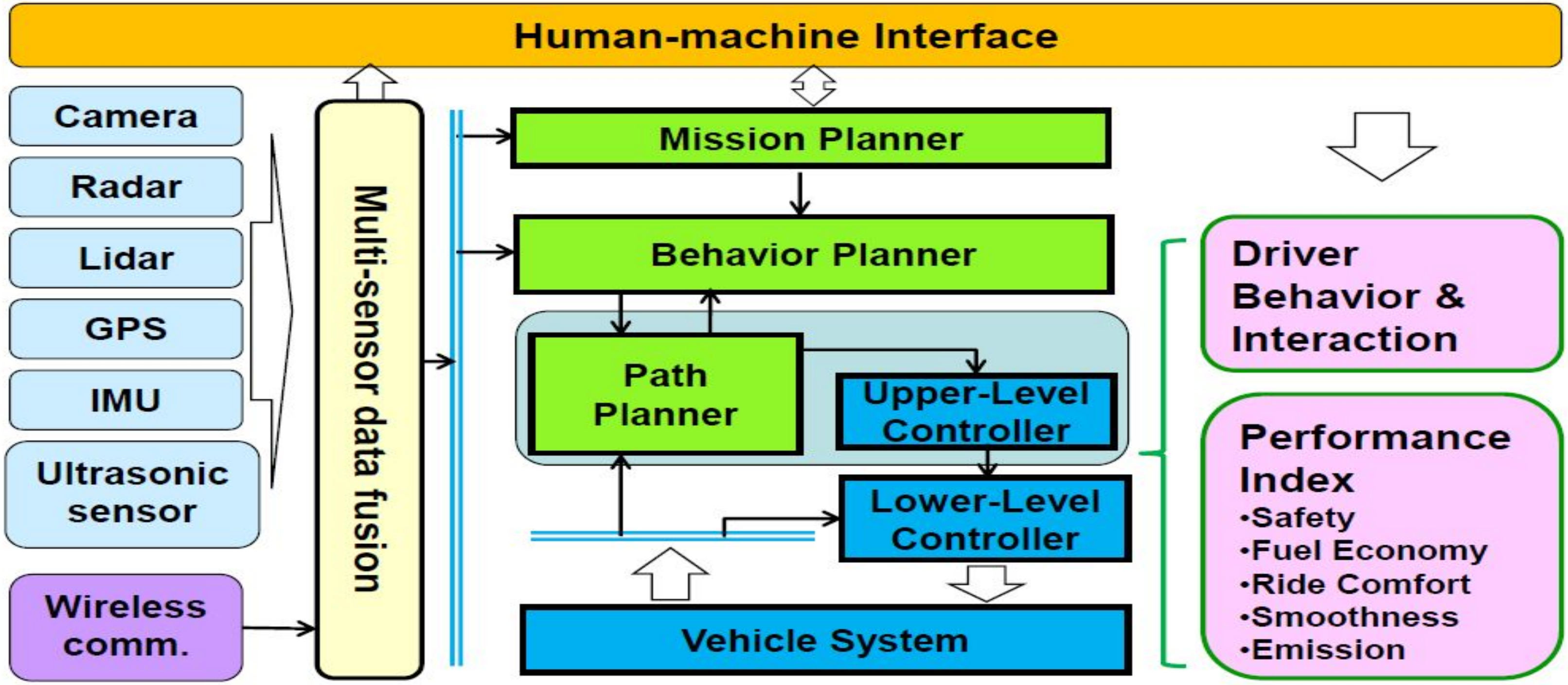
Examples of attack on vehicular network

Security issues	Attacks[1]
Availability	Jamming attack; DoS attack.
Confidentiality	Eavesdropping attack; Man in the middle attack.
Authentication	GPS spoofing; Impersonation attack; Masquerading attack; Message tampering.
Data Integrity	Replay attack; Message modification attack.

Examples of attack on Platoon Control Systems

Security issue	Attacks
Control algorithm modification	Destabilizing attack[2]; High-speed collision induction attack[3]; Traffic flow instability attack[6,7].
Sensor reading tampering	False data injection[5]; Efficiency-motivated attack[4]

Configuration of Autonomous Vehicles



Cooperative Adaptive Cruise Control

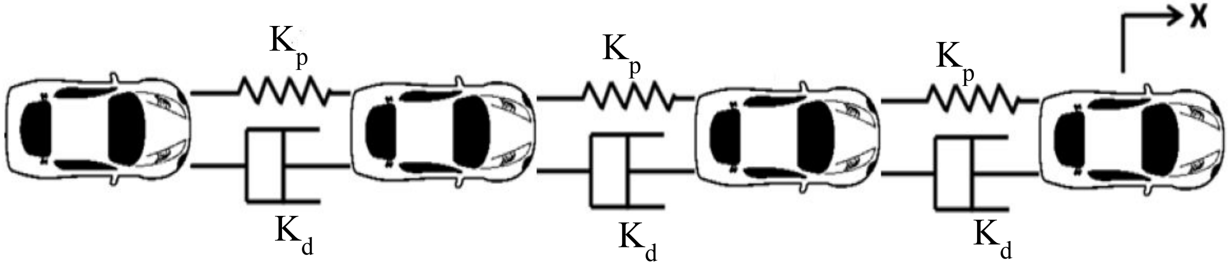
Upper level controller

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



x_i, car i's position

v_i, car i's velocity

σ_{ref}, desired separation

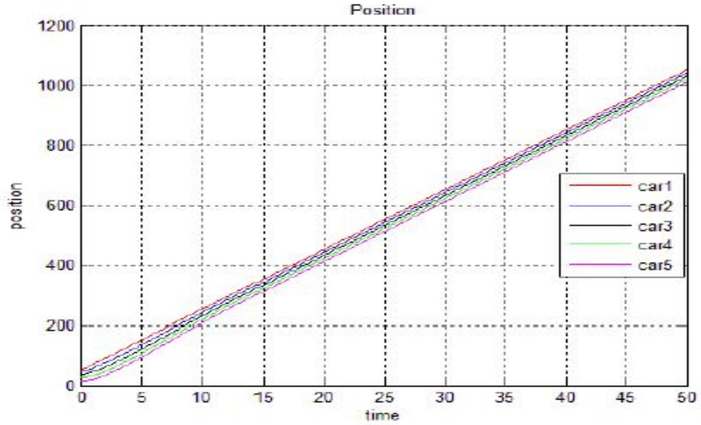
$$u_i = k_p(x_{i+1} - x_i - \sigma_{\text{ref}}) + k_p(x_{i-1} - x_i + \sigma_{\text{ref}}) + k_d(v_{i+1} - v_i) + k_d(v_{i-1} - v_i)$$

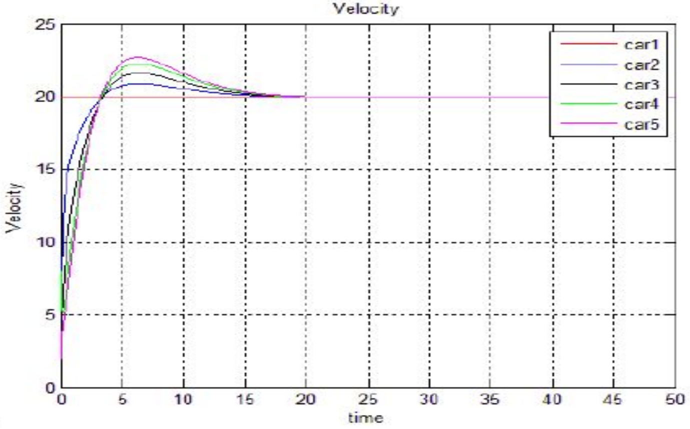
with k_p position gain and,

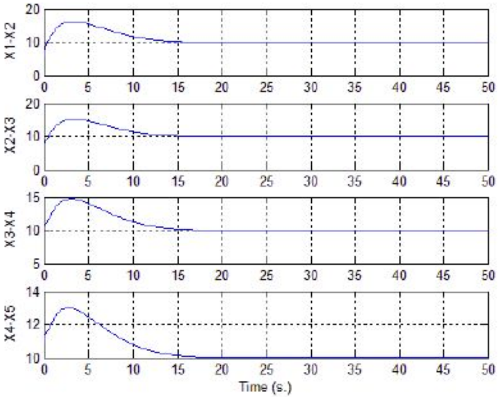
with k_d velocity gain

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

Platoon Performance







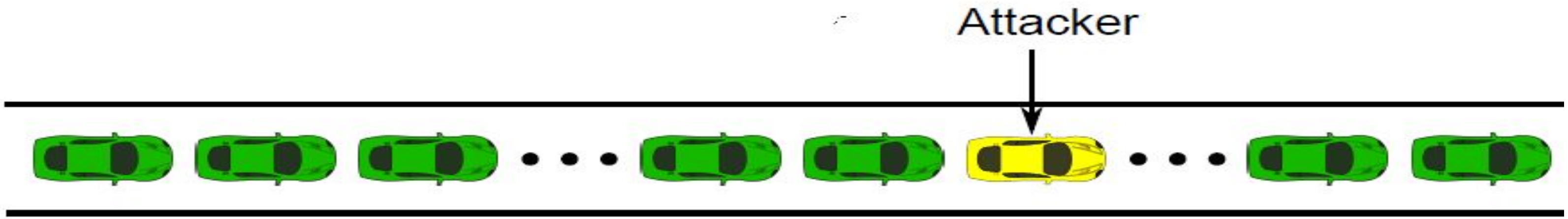
Outline

- 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.



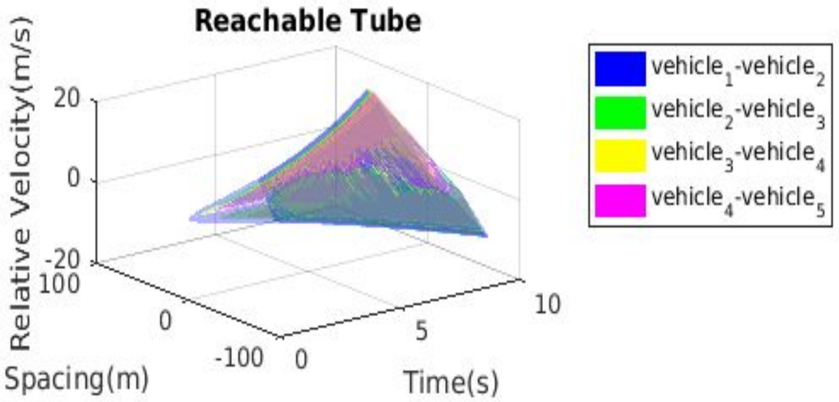
Attacks Objectives

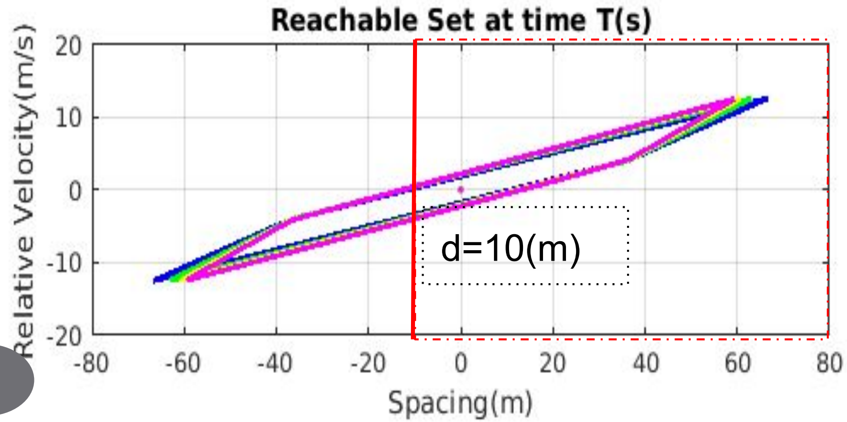
Disrupting system performance and cause collisions

Outline

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

Outsider Attack Results

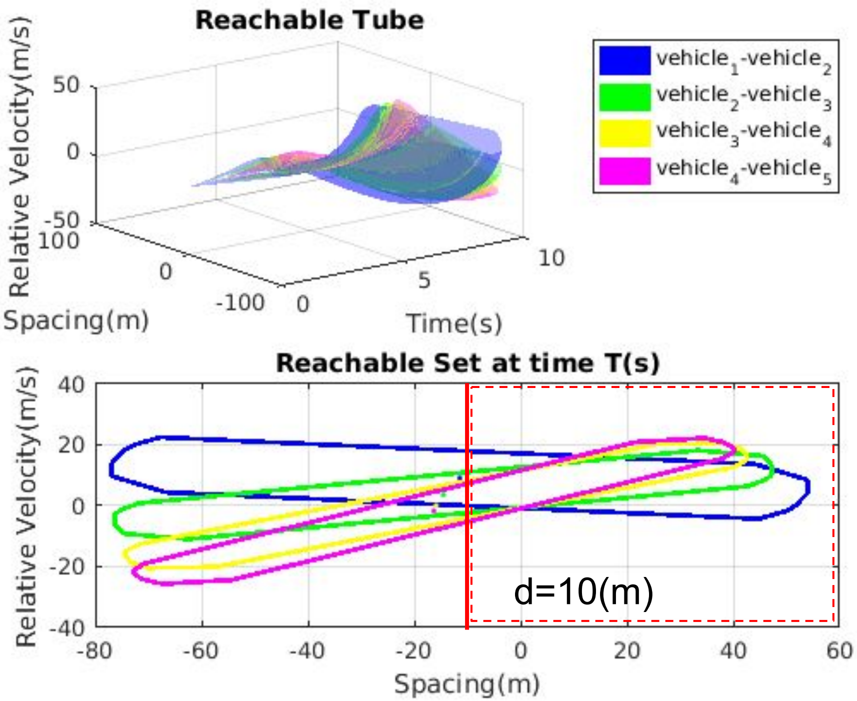




Let's consider desired spacing between each vehicle is $\boldsymbol{\delta}$-ref =d(m) and d>0. Then attacker can cause collision if spacing>=-d.

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

[1] Azees, M., Vijayakumar, P., & Deborah, L. J. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. IET Intelligent Transport Systems, 10(6), 379-388.

[2] Dadras, S., Gerdes, R. M., & Sharma, R. (2015, April). Vehicular platooning in an adversarial environment. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (pp. 167-178). ACM.

[3] DeBruhl, B., Weerakkody, S., Sinopoli, B., & Tague, P. (2015, June). Is your commute driving you crazy?: a study of misbehavior in vehicular platoons. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (p. 22). ACM.

[4] Gerdes, R. M., Winstead, C., & Heaslip, K. (2013, December). CPS: an efficiency-motivated attack against autonomous vehicular transportation. In Proceedings of the 29th Annual Computer Security Applications Conference (pp. 99-108). ACM.

[5] Biswas, B. (2015). Analysis of false data injection in vehicle platooning. Utah State University.

[6] Dunn, D. D. (2015). Attacker-induced traffic flow instability in a stream of automated vehicles. Utah State University.

[7] Dunn, Daniel D., et al. "Regular: Attacker-Induced Traffic Flow Instability in a Stream of Semi-Automated Vehicles." *Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on*. IEEE, 2017.

[8] Yanakiev, D., & Kanellakopoulos, I. (1996, July). A simplified framework for string stability analysis in AHS. In Proceedings of the 13th IFAC World Congress (Vol. 182, pp. 177-182).

Bibliography

[10] Eyre, J., D. Yanakiev, and I. Kanellakopoulos. "A Simplified Framework for String Stability Analysis of Automated Vehicles∗." *Vehicle System Dynamics* 30.5 (1998): 375-405.

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.

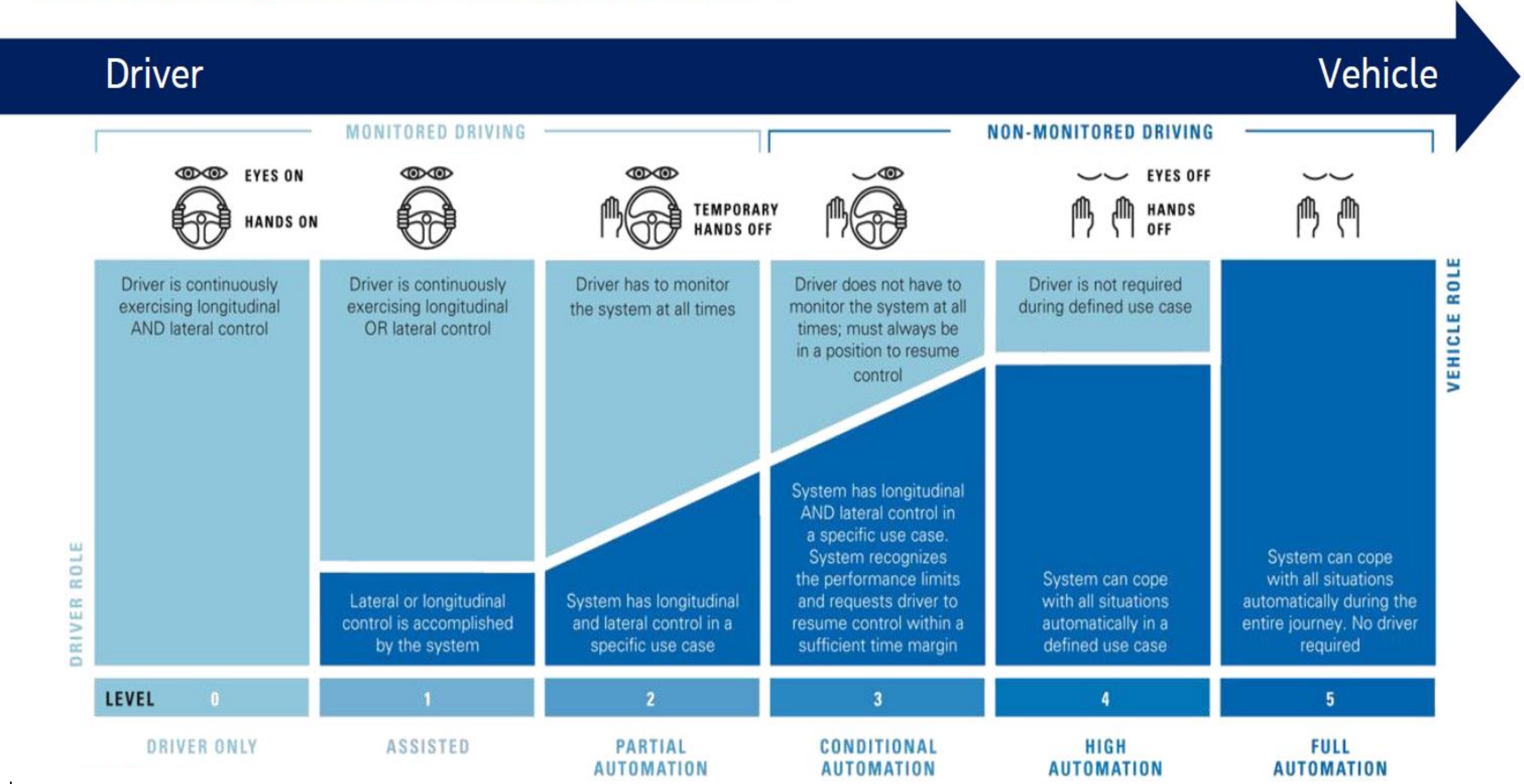
Level 2 _ Partial Automation ***System capability:*** The car can steer, accelerate, and brake in certain circumstances. • ***Driver involvement:*** Tactical maneuvers such as responding to traffic signals or changing lanes largely fall to the driver, as does scanning for hazards. The driver may have 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,

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.


Computer Vision
Sensor Fusion
Localization
Path Planning
Control



Driver
Vehicle
MONITORED DRIVING
NON-MONITORED DRIVING
EYES ON
HANDS ON
TEMPORARY HANDS OFF
EYES OFF
HANDS OFF
Driver is continuously exercising longitudinal AND lateral control
Driver is continuously exercising longitudinal OR lateral control
Lateral or longitudinal control is accomplished by the system
Driver has to monitor the system at all times
System has longitudinal and lateral control in a specific use case
Driver does not have to monitor the system at all times; must always be in a position to resume control
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
Driver is not required during defined use case
System can cope with all situations automatically in a defined use case
System can cope with all situations automatically during the entire journey. No driver required
VEHICLE ROLE
DRIVER ROLE
LEVEL 0
1
2
3
4
5
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)

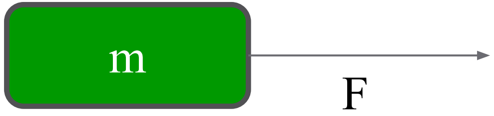
$x: position;$

$\dot{x} = v: velocity;$

$\ddot{x} = \dot{v} = a: acceleration;$

$m = mass;$

$F = u = ma: control\ input.$



$$\begin{cases} \dot{x} = v, \\ \dot{v} = u. \end{cases}$$

Platooning Control Policy

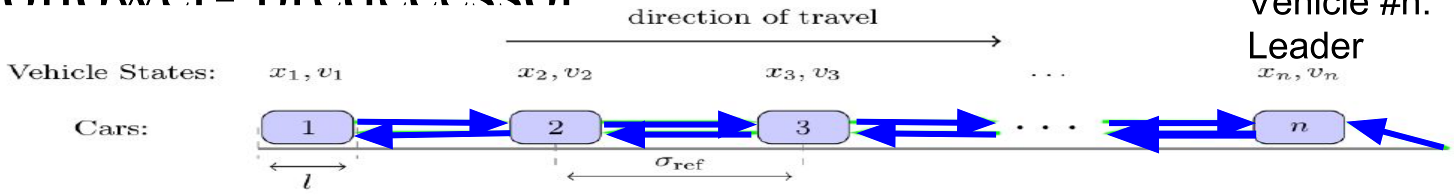
Inter-vehicle spacing Policies:

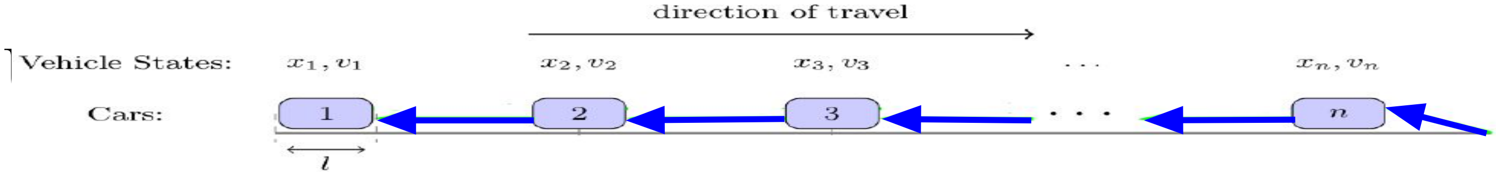
- Constant Spacing Policy (CSP),
- Variable Time Gap (VTG),
- Constant Time Gap (CTG).

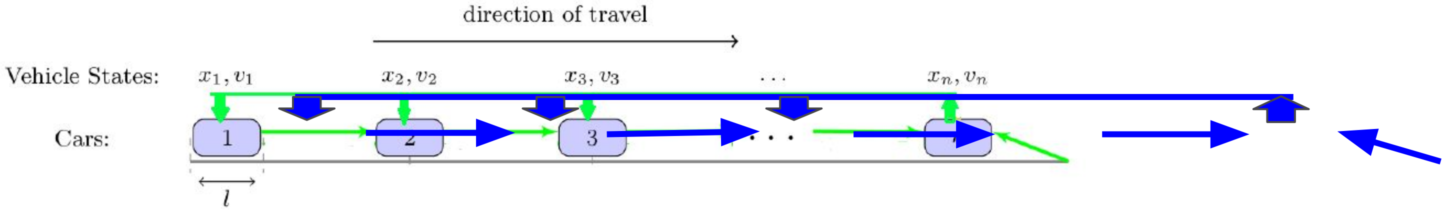
Platoon Information Flow

- Follower- predecessor:

Vehicle #n: Leader



- 

- 

Platoon Control laws

Control algorithm	Policy	Inter-veh-comm
$\ddot{x}_i = k_p(x_{i+1} - x_i - \sigma_{ref}) + k_p(x_{i-1} - x_i + \sigma_{ref}) + k_d(\dot{x}_{i+1} - \dot{x}_i) + k_d(\dot{x}_{i-1} - \dot{x}_i)$	CSP	No
$\ddot{x}_i = k_p(x_{i+1} - x_i - h\dot{x}_i) + k_d(\dot{x}_{i+1} - \dot{x}_i)$	CTG	No

Platoon Model

State Space representation (absolute coordinate 2n states and error (2n-2) states [illegible] hicles)

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

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ -k_p & -k_d & k_p & k_d & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ k_p & k_d & -2k_p & -2k_d & k_p & k_d & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \cdots & 0 & 0 & 0 & k_p & k_d & -k_p & -k_d \end{bmatrix}$$

Absolute coordinate states x_i and v_i

Error coordinate

$z_i = x_i - x_{i+1}$;

$y_i = v_i - v_{i+1}$

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ -2k_p & -2k_d & k_p & k_d & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \cdots & 0 \\ k_p & k_d & -2k_p & -2k_d & k_p & k_d & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & \cdots & 0 & 0 & 0 & k_p & k_d & -2k_p & -2k_d \end{bmatrix}$$