Autonomous Vehicle Platoons Robust Against Communication and Sensor Failure

Platoons of autonomous vehicles controlled by a centralized adaptive cruise control are vulnerable to disruptions in communications between cars, and unreliable sensing information of the vehicles around them. By building methods to simulate a centralized command during communication loss, and to establish safety margins based on still-reliable sensor information during a sensor failure, a platoon of vehicles can guarantee safety in even emergency situations while suffering communication and sensor loss.

Technology ID
BDP 8498

Category
Hardware/Other
Software/Machine Learning
Software/Other
Selection of Available Technologies

Authors
Santosh Devasia

View online page

What is the Problem?

Platoons of constantly spaced autonomous vehicles promise increases in fuel efficiency, closer inter-car spacing, and improved traffic efficiency over human drivers. With a centralized control method in charge of all platoon vehicles, the single-file line can remain stable even if a single vehicle is forced to swerve or stop. This has the potential to revolutionize the trucking industry, where one human driver can lead an entire platoon of vehicles. However, this scheme is vulnerable to disruptions in communications, and is heavily reliant on accurate sensor information.

If centralized communication fails, errors in car position grow over time as cars become only aware of their neighbors through on-car sensors. If the data from those sensors is inaccurate, which can happen from extreme lighting, inclement weather, or even intentional attacks, the errors from the decentralized control scheme can lead to serious safety concerns and vehicle collisions.

There is therefore an unmet need of improving the method of handling communication delays in autonomous vehicle platoons and equipping that method to guarantee safety in a worst-case combination of loss of centralized communication and unreliable sensor data.

What is the Solution?

This technology combines the centralized control algorithm of a platoon with a decentralized method in each individual car based on past data. This type of delayed self-reinforcement (DSR) control mimics an ideal centralized command, based on sensor data. When communication is delayed or lost, this mimicked centralized command is followed in place of a decentralized computation based on only the vehicle's neighbors. This leads to improved performance with large delays or loss of communication.

For disruptions in sensor data, an occlusion-aware algorithm detects the disruption in the sensor. All other available sensors are then used to fill in the gaps. For instance, in the case of a malfunctioning long-range sensor, the short range sensor's inability to detect the car in front shows that the next car is far enough to be out of range of the short range sensor. This type of "negative" information can be used to generate a safety limit for the speed of the car, guaranteeing safety even with the disruption of both communications and sensing.

What is the Competitive Advantage?

The DSR-based control scheme decreases the error in vehicle position by 80% compared with a method based only off of detecting nearest neighbors. In addition, in the case of disruption, the DSR-based method decreases the time it takes for the cars to reach consensus again is decreased by 95%.

The implementation of occlusion-aware algorithms to establish safety margins for vehicles experiencing sensing issues successfully guarantees safety in high-fidelity simulations, even in a worst-case combination of communications loss and an emergency braking. This approach is capable of working even for long disruptions in sensor reliability.

Together, these technologies increase the safety and reliability of autonomous vehicle platoons by building robustness against two vulnerable points of centralized control.

Patent Information:

WO2023244950A1

WO2023043684A1

References

1. Yudong Lin, Anuj Tiwari, Brian Fabien, Santosh Devasia(2023-03) , https://doi.org/10.1109/TITS.2022.3224635, https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6979, 24, 3370–3382