Autonomous Vehicle Security

Tong Ray Huang, David Pham, Christopher DiPalma, Sammy Wong
Professor Alfred Qi Chen
Department of Electrical Engineering and Computer Science

Background

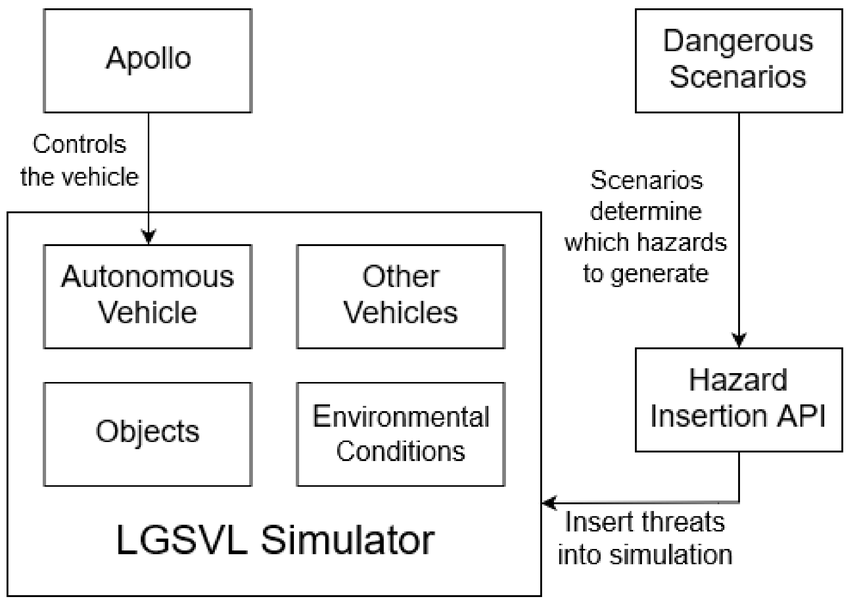
The future is moving towards automated vehicles and networks connecting people on the road are being developed. The focus has been on building the mechanics of the autonomous vehicle but not on protecting the various sensors and networks that make the car autonomous.

Objective

The objective of this project is to develop a simulation environment that emulates security threats made to an autonomous vehicle. The application will reflect various attacks meant to confuse sensors on the car and indicate the degree of success in stopping the threat through a virtual scenario.

Project Components

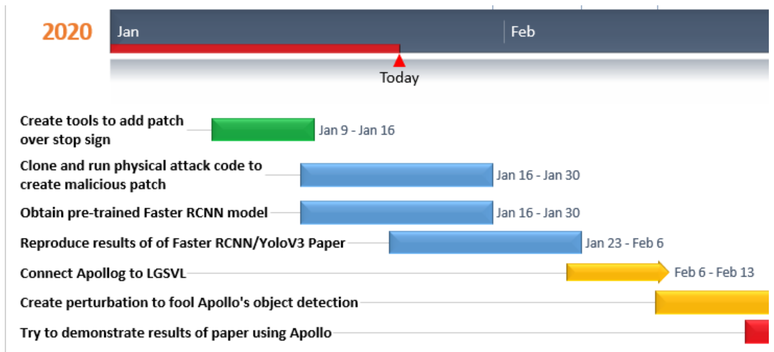
- Unity Real-Time Development Platform
- Baidu Apollo Self-Driving Software
- LGSVL Physical-World Simulator



Progress Updates

- Changed patch over stop sign to a perturbed 2D sprite
- Trying to fool Faster R-CNN object detection model

Timeline



References

Jia, Yunhan Jack, et al. “Towards Secure and Safe Appified Automated Vehicles.” *Towards Secure and Safe Appified Automated Vehicles*, 27 Mar. 2017, www.ics.uci.edu/~alfchen/jack_iv17.pdf.

Toews, Rob. “The Biggest Threat Facing Connected Autonomous Vehicles is Cybersecurity.” *TechCrunch*, TechCrunch, 25 Aug. 2016, techcrunch.com/2016/08/25/the-biggest-threat-facing-connected-autonomous-vehicles-is-cybersecurity/.

Cao, Yulong, et al. “Adversarial Sensor Attack on LiDAR-Based Perception in Autonomous Driving.” *Adversarial Sensor Attack on LiDAR-Based Perception in Autonomous Driving*, www.ics.uci.edu/~alchen/yulong_ccs119.pdf

THE HENRY SAMUELI SCHOOL OF ENGINEERING
UNIVERSITY of CALIFORNIA • IRVINE