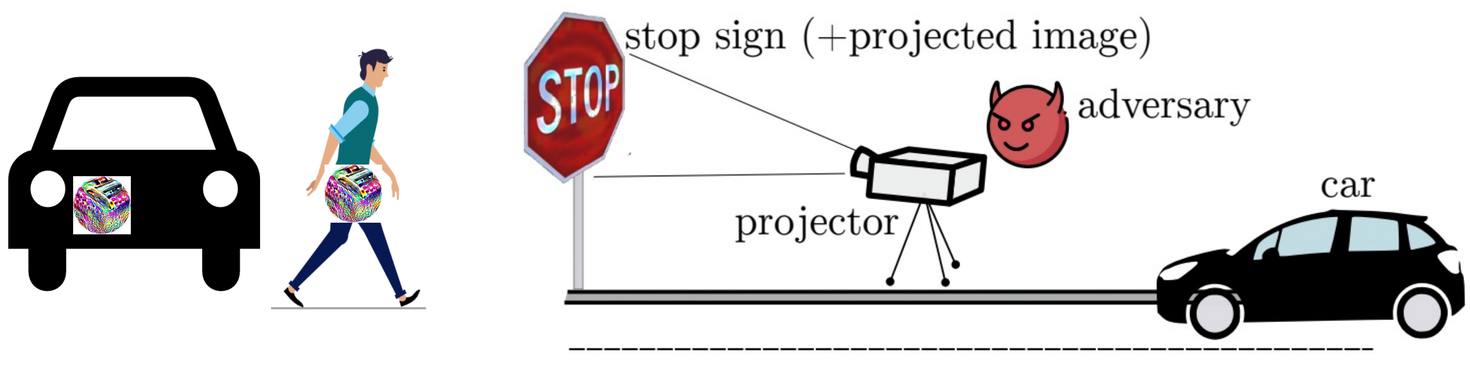
CPS: Medium: Robust Sensing and Learning for Autonomous Driving Against Perceptual Illusion

Qiben Yan, Sijia Liu, Xiaoming Liu, Michigan State University
Wenjing Lou, Thomas Hou, Virginia Tech

https://seit.egr.msu.edu/research/cps2023.html

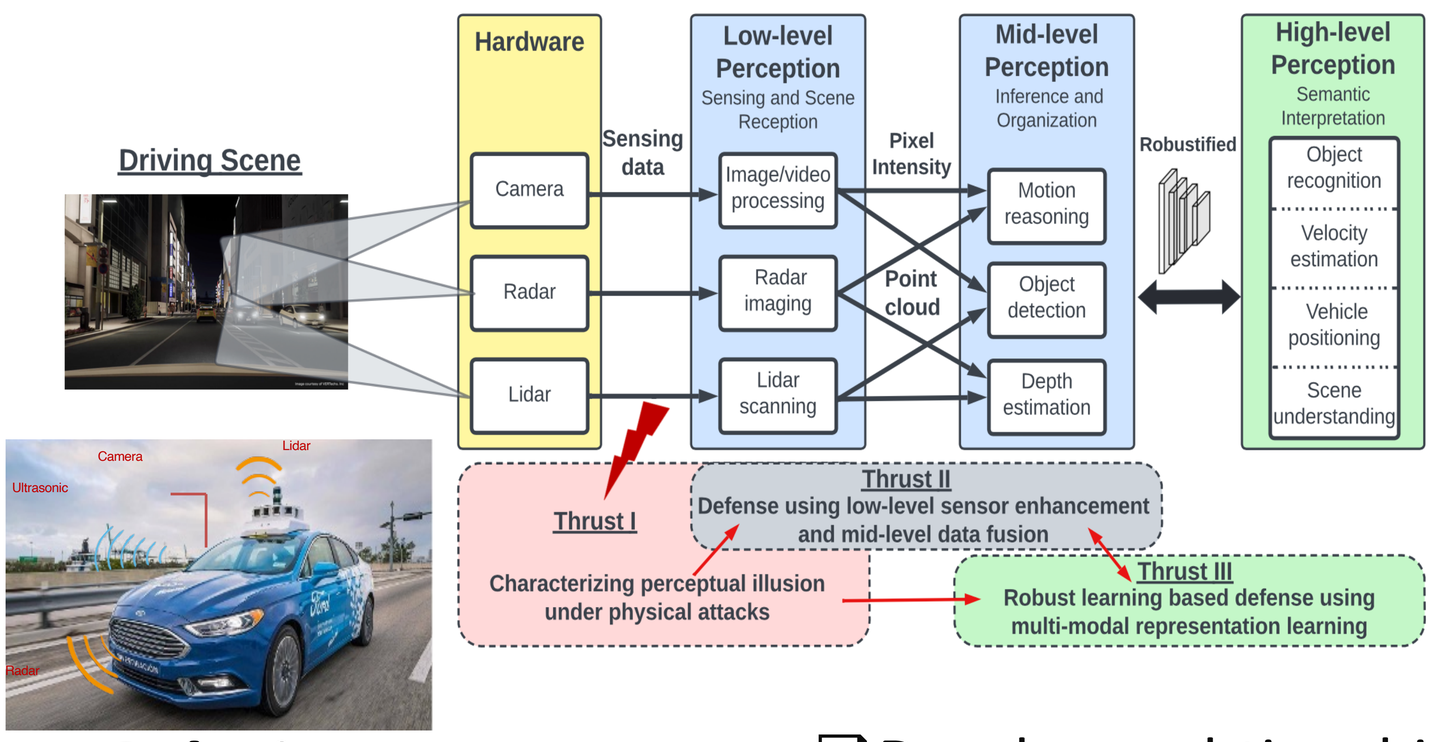
• Introduction:

- ❑ Perceptual illusions deceive autonomous vehicles into misinterpreting its surroundings
- ❑ Lack of comprehensive datasets and frameworks to study and characterize the impact of these attacks
- ❑ Lack of defense against perceptual illusion attacks that exploit physical channels



• Scientific Impact:

- ❑ The project's advanced defense strategies and threat modeling methodologies offer a template for enhancing security across various CPS systems
- ❑ The protocols for real-world validation and benchmarking of defense mechanisms can inform best practices across CPS research



• Solution:

- ❑ Incorporate neuroscience to understand the causes of perceptual illusion that could be rooted in both the sensors at low-level and perception models at mid- and high-level
- ❑ Collect perceptual illusion datasets for vehicles
- ❑ Develop real-time high-resolution radar sensing technology and mid-level data fusion to enhance the robustness of each sensing modality
- ❑ Build multi-sensor representation learning to achieve robust high-level perception in an adversarial environment

• Broad Impact

- ❑ Developed multiple course modules
- ❑ Involved undergraduate students in CPS research
- ❑ Created open-source projects for attack and defense

MICHIGAN STATE UNIVERSITY
VIRGINIA TECH
Award ID#:CNS-2235231