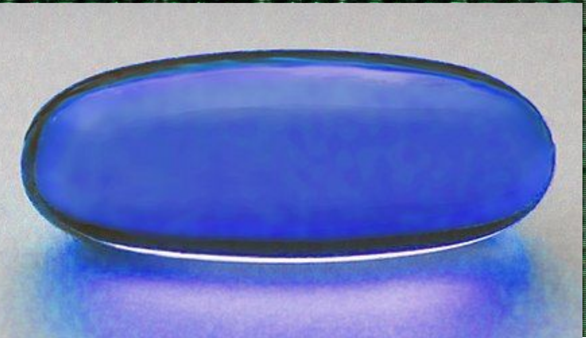
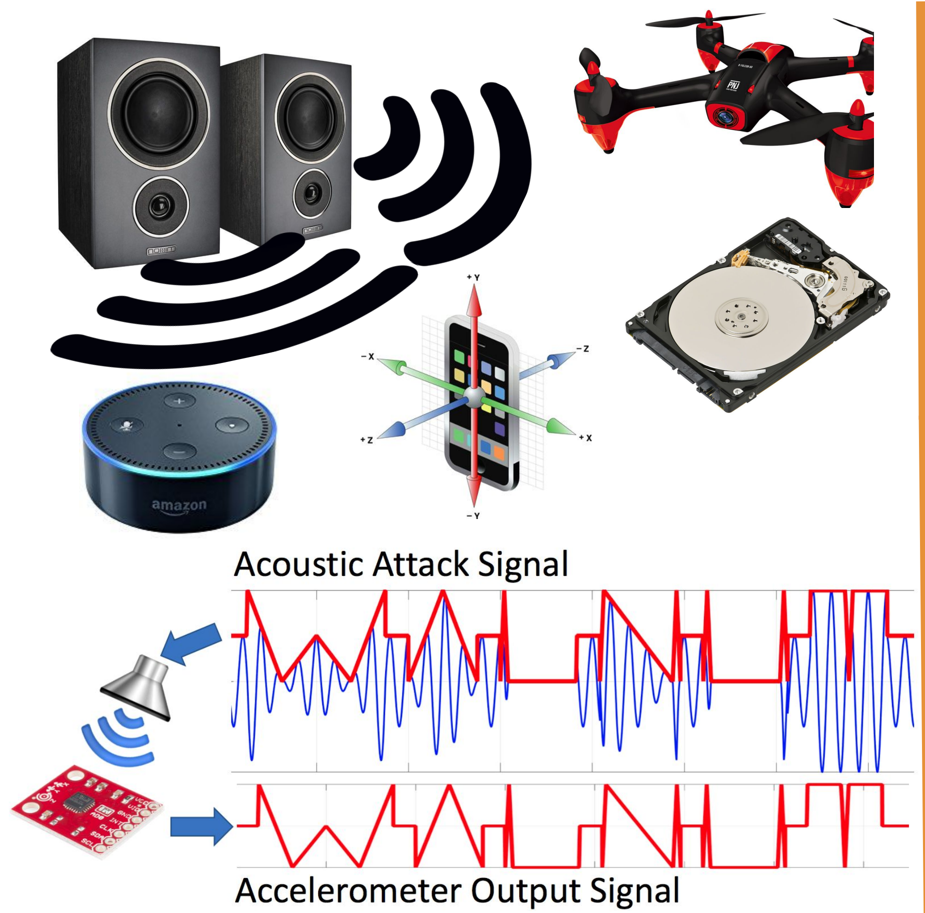
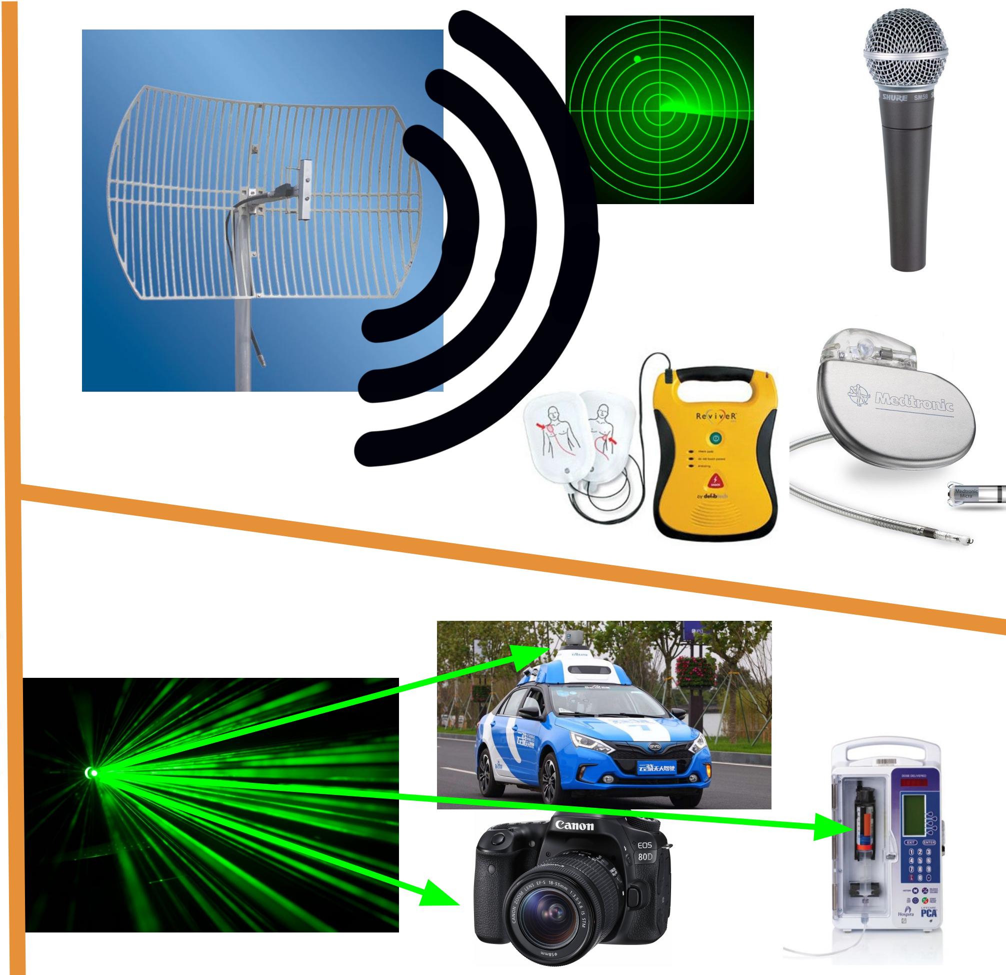
Taking the Red Pill: Designing Sensors that Recognize False Realities



Connor Bolton



https://spqr.eecs.umich.edu/walnut/



This is bad.

- Could control drone behavior

- Leaves little evidence

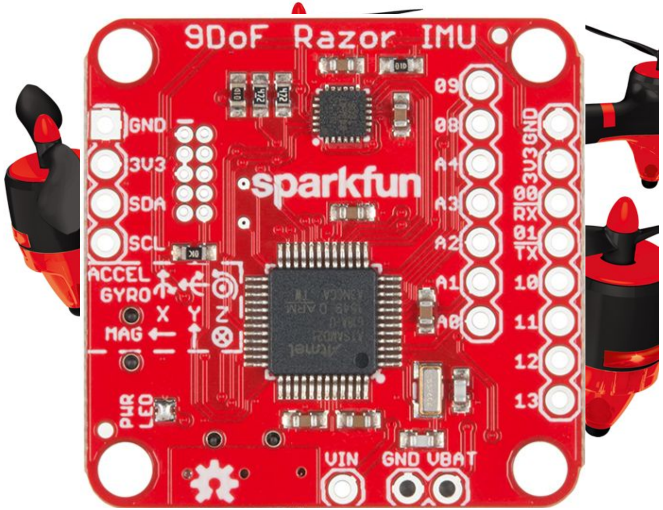
Current Defense Toolbox

- Ad-hoc
-
- M Learning

Not Enough

Need more tools!

Current Shortcomings



1. Accelerometer
2. Gyroscope
3. Magnetometer

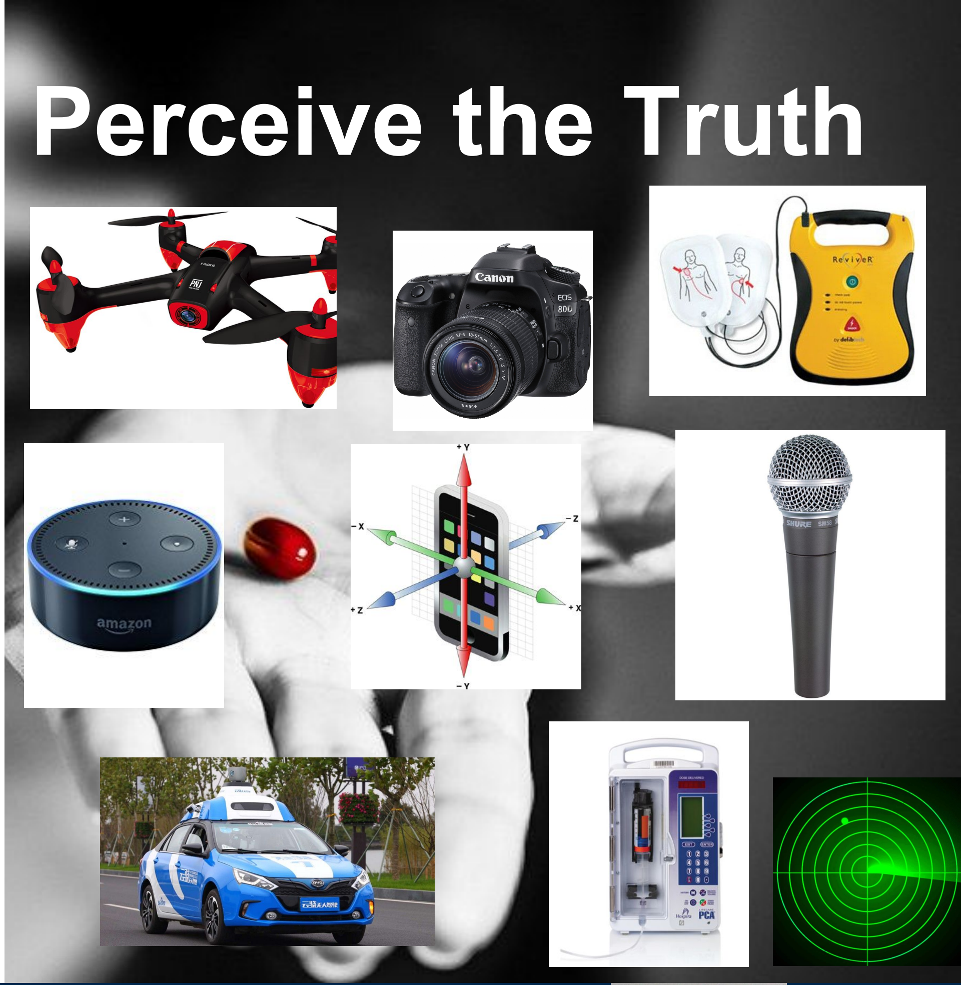
Ad-hoc: reactionary, $$

Sensor Fusion / Machine Learning

- Dependant on data
- Can’t deploy everywhere

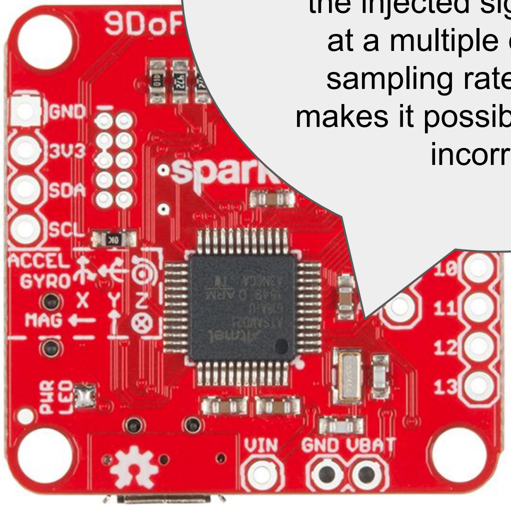
Stay Deceived

Perceive the Truth



New Defense Tools

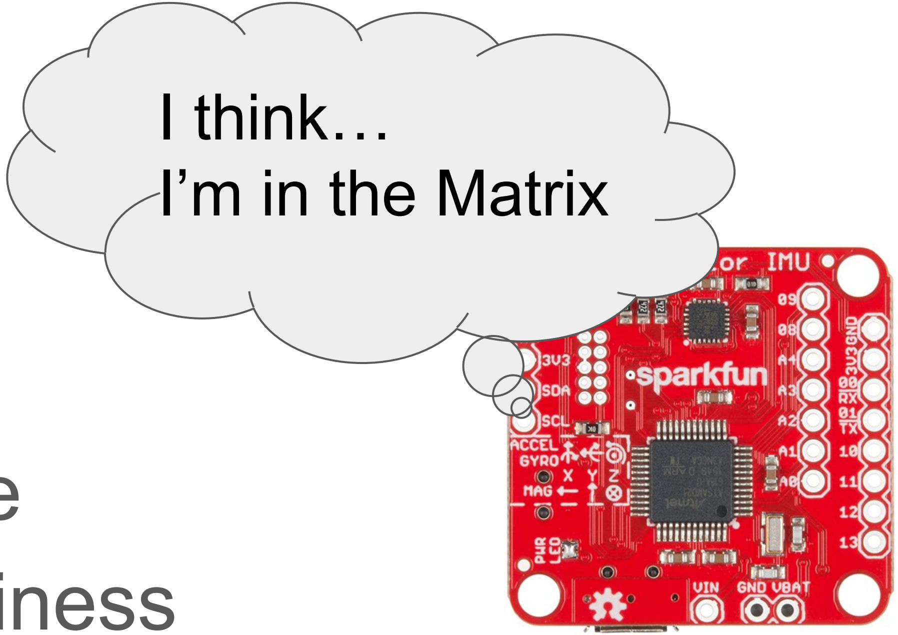
Add measures of trustworthiness



The physical masses are being vibrated violently at about 40 kHz, the low pass filter is not successfully filtering out this data, and the injected signal is about at a multiple of the ADC sampling rate. All of this makes it possible the data is incorrect.

Designing sensors to recognize false realities….

- Current defense tools
  - Ad-hoc defenses
  - Sensor fusion
  - Machine learning
- We need new tools
- One idea: could provide measures of trustworthiness



I think…
I’m in the Matrix