Understanding Resilience of Vision-Based Navigation

Joshua Chiu

CPEN 499

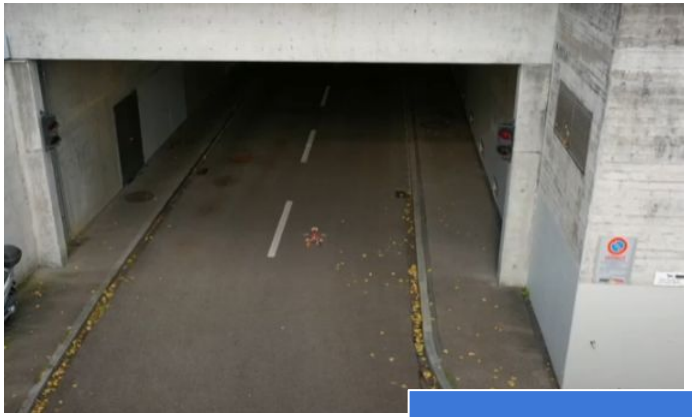
Drones in Real World

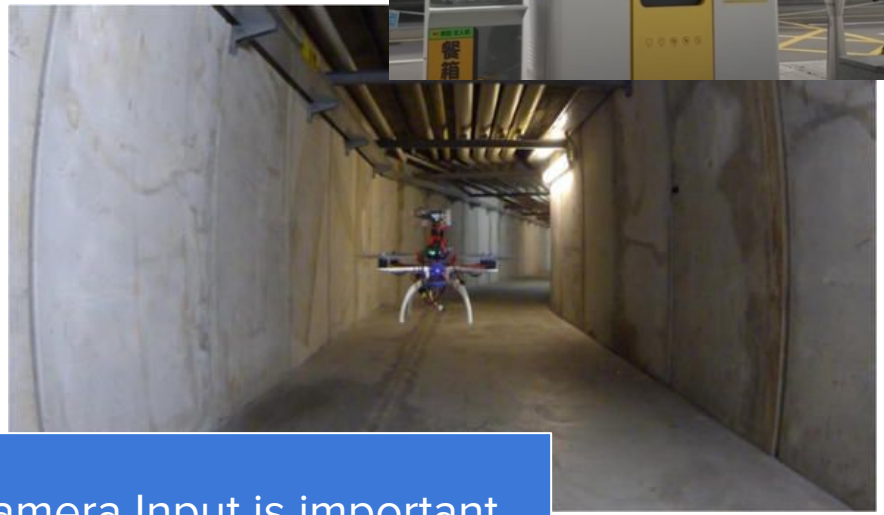
- Zipline: Delivering blood by drone (Rwanda)
- Meituan: Delivering takeout meals (China)
- Wing: Delivering Groceries (USA)
- Geodis: Warehouse Inventory (USA)

Drone are increasingly used in industrial use cases

What if... no GPS?

- Indoor Environments
- Low GPS Reception around Tall Buildings
- Interference from Power Lines





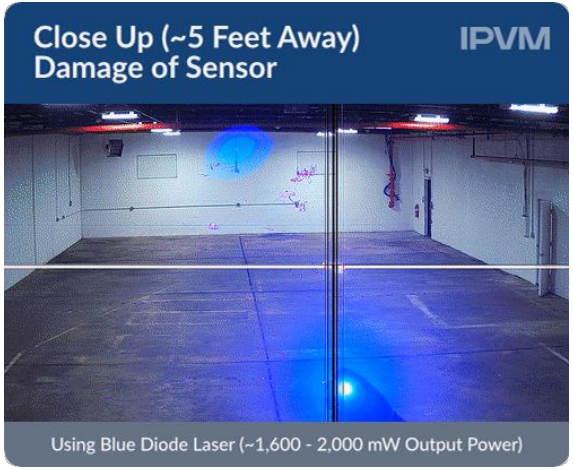
Correctness of Camera Input is important

Effects of Laser Interference

Cause temporary blindness or permanent sensor damage

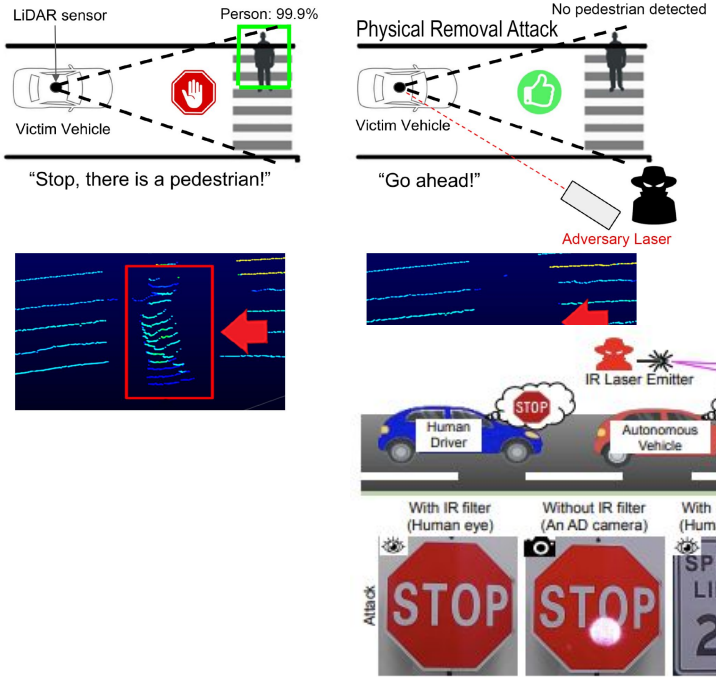
Lasers interference can be malicious or inadvertent

- light shows
- autonomous lidar
- laser structure scanners
- malicious intent



Existing Work

- Attacking LiDAR with Lasers
- Attacking Traffic Sign Recognition

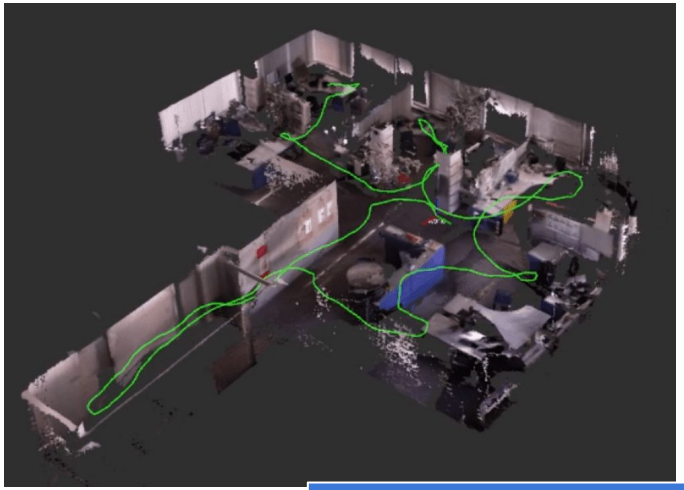


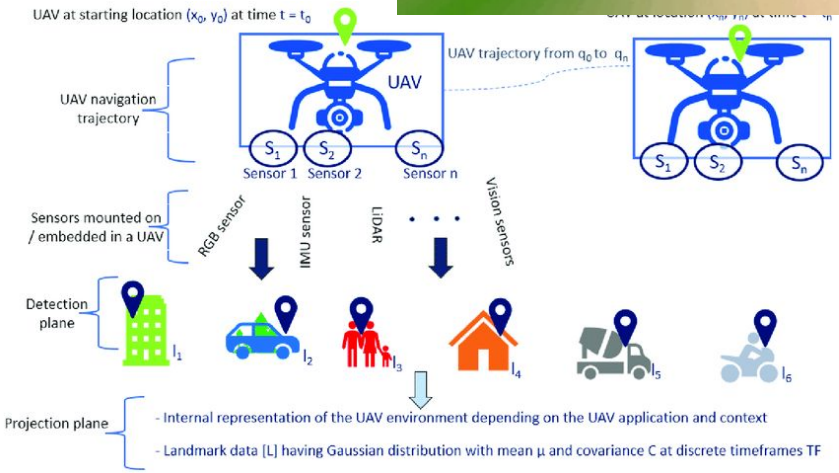
Our Distinction

- Attacking Positioning Algorithm
- Using Lasers to affect cameras

Vision Algorithms

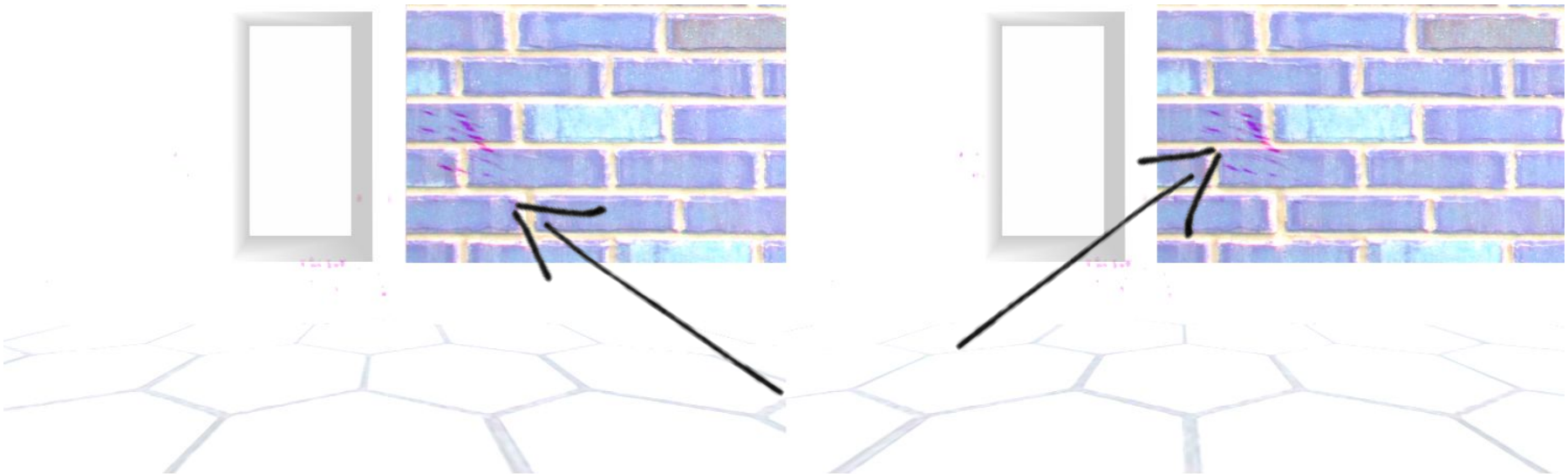
- Visual Odometry (Egomotion, Corner tracking)
- Vision Inertial Odometry (Sensor Fusion with IMU)





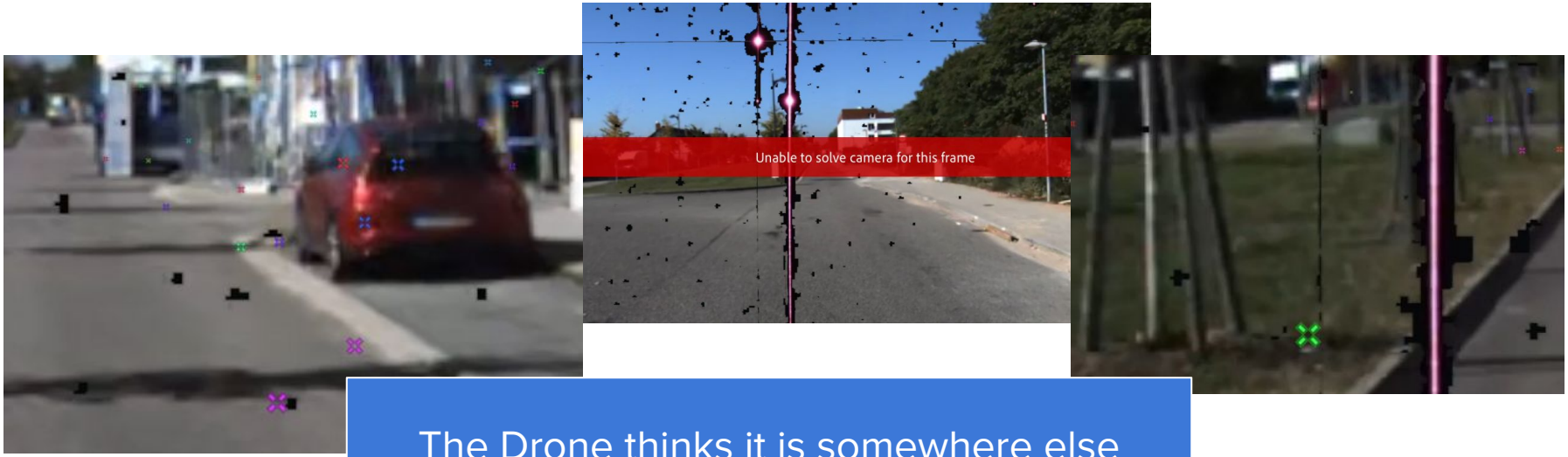
These algorithms need a high quality and clear image

An Intuition



Feature Points: Erroneous Tracking

- Incorrect landmarks are tracked
- Pose and trajectory calculated incorrectly
- Error exists between ground truth and estimation



The Drone thinks it is somewhere else

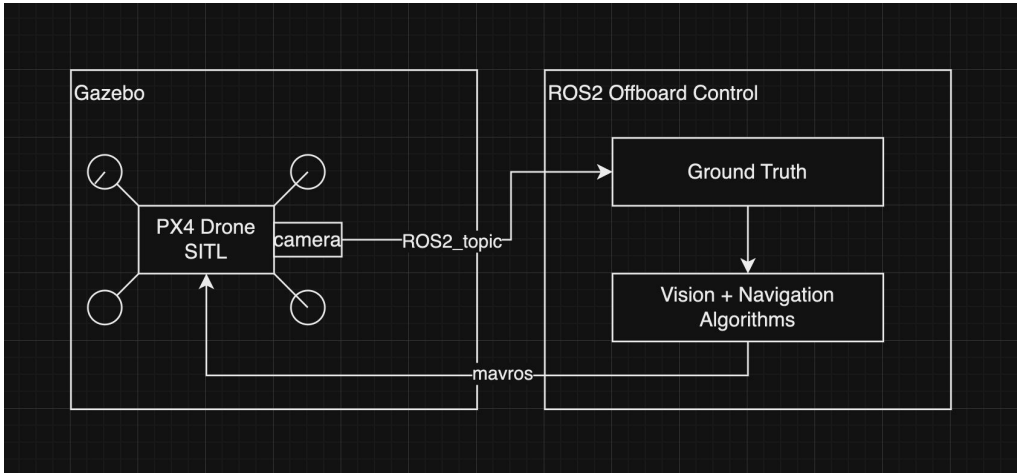
Testing Plan and Method

Simulation

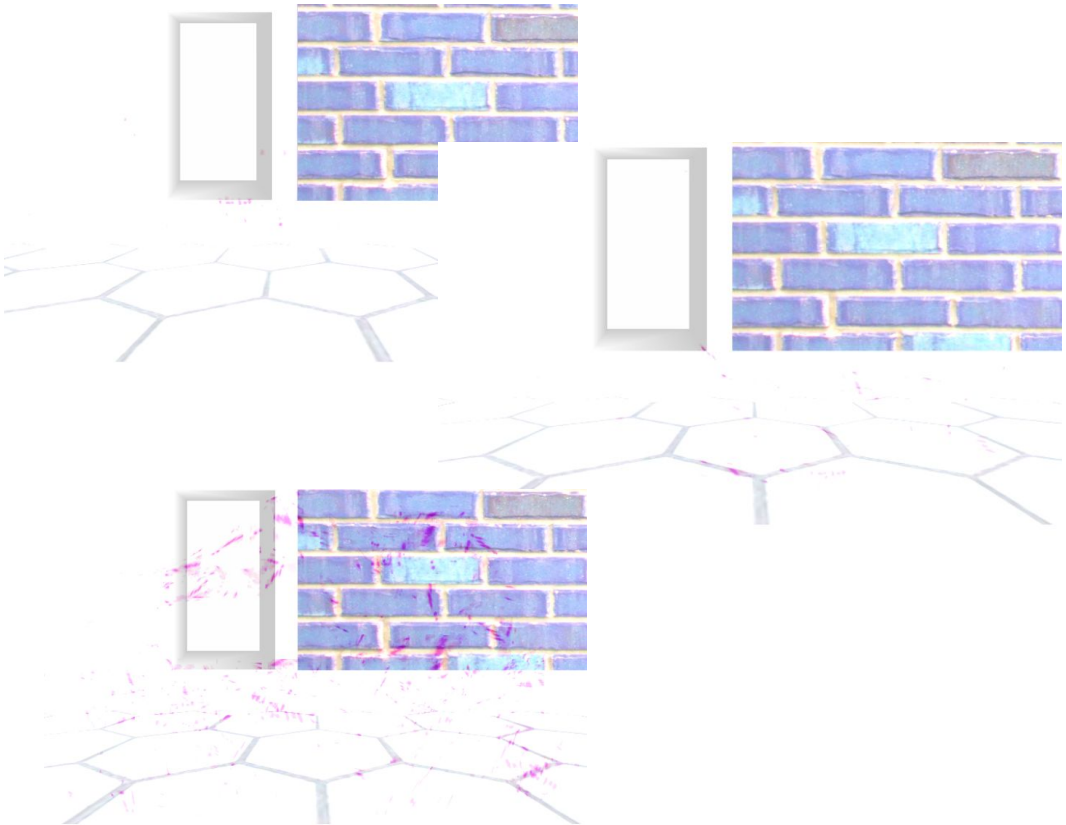
- Build vehicle
- Test control algorithms

Real life replication

- Show the system reacting (adversely) to damage and interference

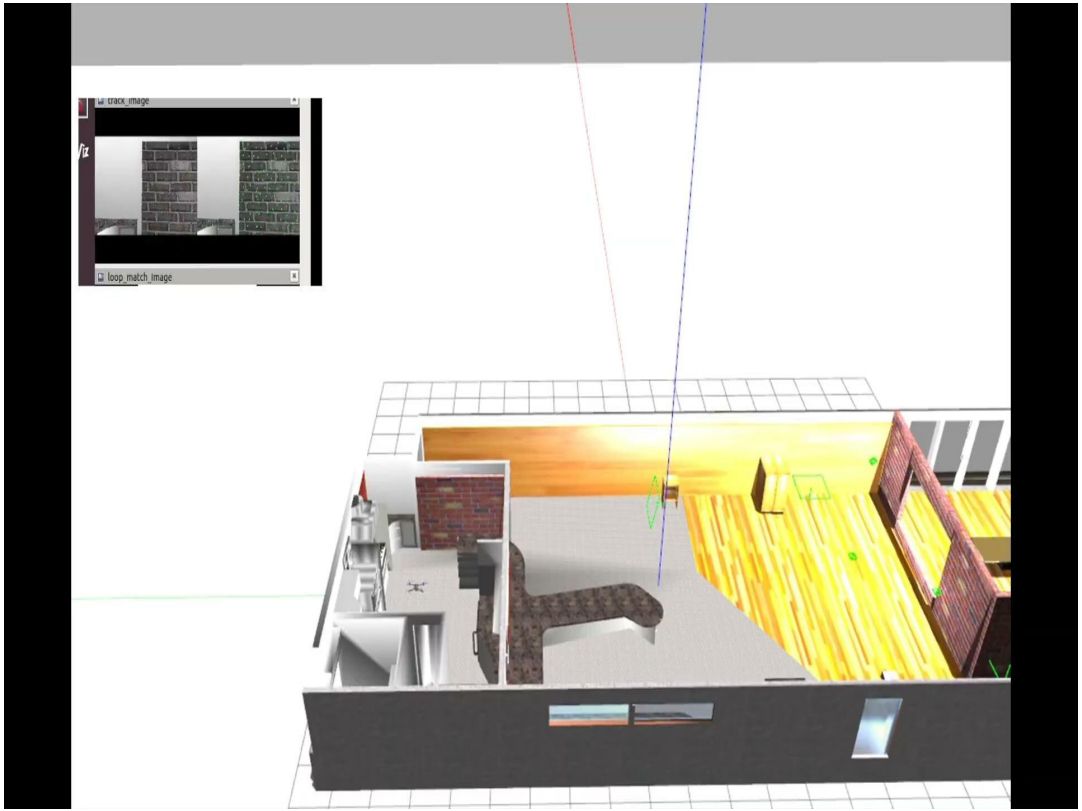


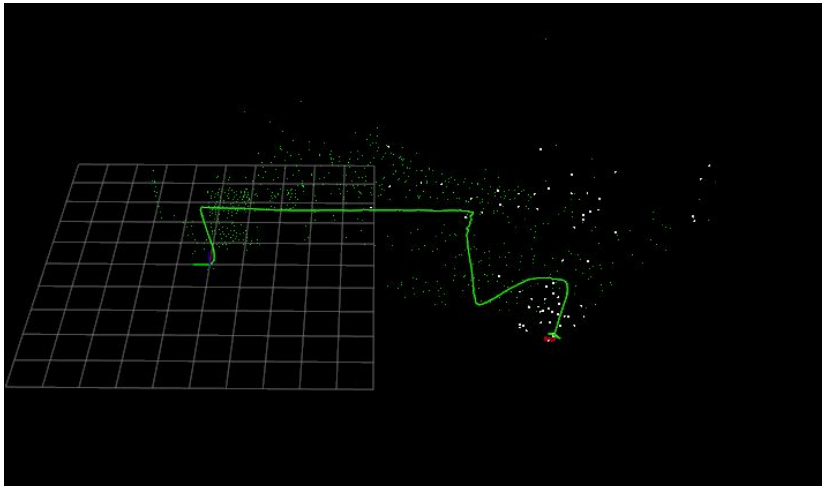
Defining Low, Medium, High



Damage	Percent of Sensor Damaged
None	0%
Low	< 1%
Medium	< 10%
Severe	10%+

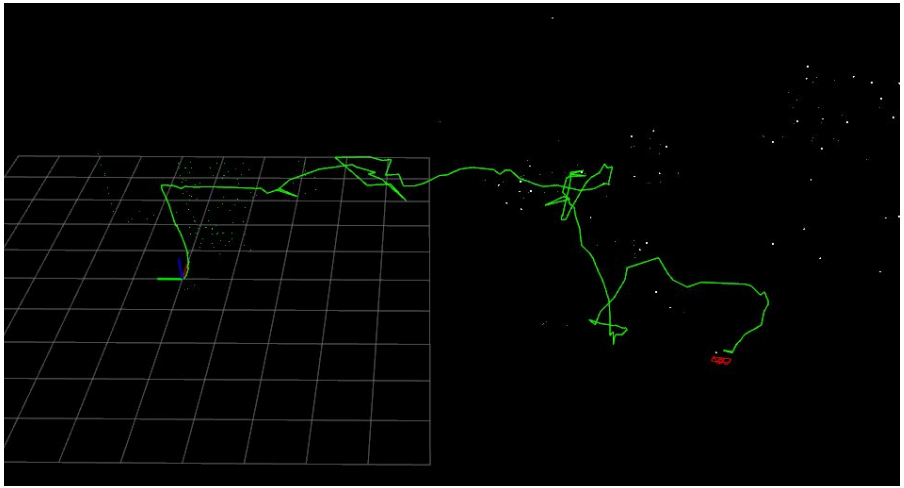
Video: Before and After





Normal (Perfect) Trajectory

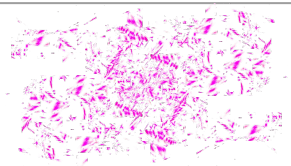
Able to accurately detect and calculate its position and fly to each of the waypoints



Attack Trajectory

Struggle to detect and calculate its position to mitigate the noise and fly to each of the waypoints

Evaluation: Successful Arrivals

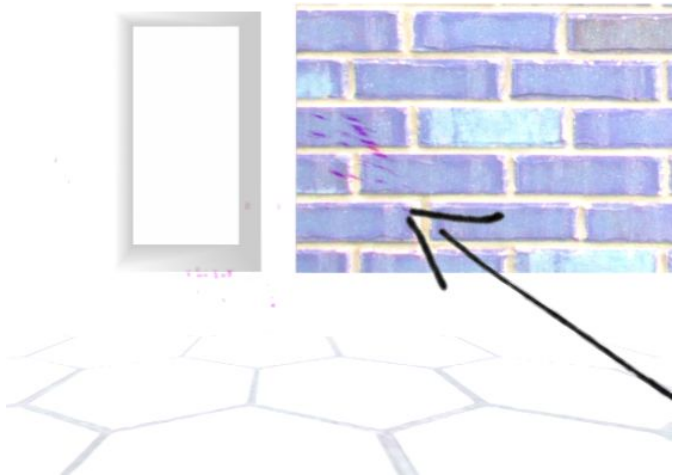
Damage	Sample Overlay	Successful Arrival Rate
None		99.8%
Low		95.2%
Medium		61.0%
Severe		0.9%

Evaluated on 1000 runs of the path for 1m of arrival waypoint

Extending the Attack: Hijack Forward Control

Laser damage on the left side of sensor

- Left side stationary, right side moving
- Thinks vehicle is turning left
- **Corrects with right deviation**



Replication in simulator

- Reliability about 3 out of 4 times to deviate 1 meter along a 10 meter straight path

Summary

- Vision Navigation requires accurate feature points representation
- Lasers are everywhere and can interfere with a camera sensor
- The resiliency of VO to interference from lasers is weak
- Laser artifacts on cameras can easily affect flight paths

Learning and Takeaways

- How to tell a story, the different types of narratives
- Effectively communicate to different audiences
- Project planning and management

Closing

Joshua Chiu

joshchiu@student.ubc.ca
joshuachiu.com

With thanks to the DSS team at UBC, Pritam Dash and Dr. Karthik Pattabiraman

University of British Columbia

Closing

Joshua Chiu

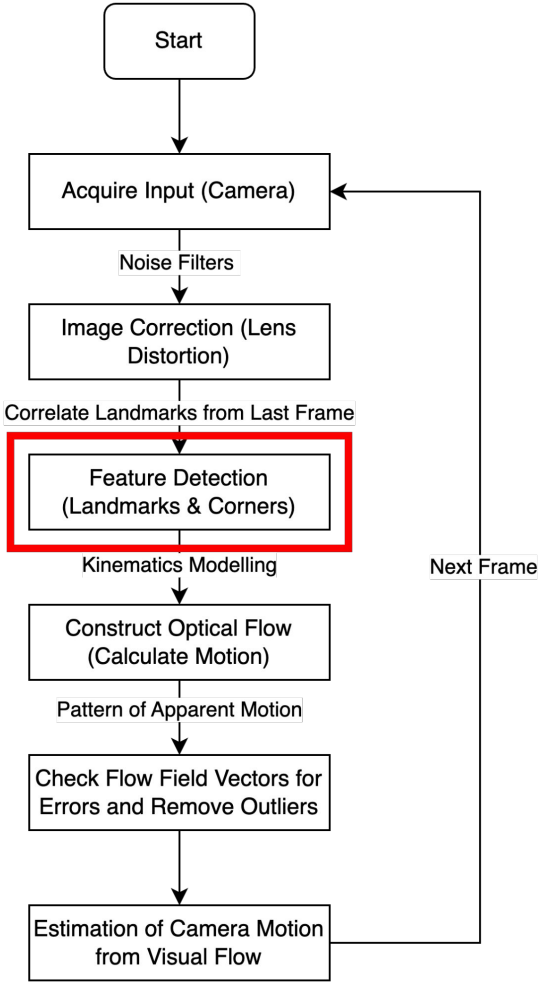
joshchiu@student.ubc.ca
joshua.chiu@student.ethz.ch
joshuachiu.com

With thanks to the ROVIO team at ETHz, DSS team at UBC, Pritam Dash and Dr. Karthik Pattabiraman

University of British Columbia
Eidgenössische Technische Hochschule Zürich

Appendix: The Attack

- Introduce bad input
- Observe effects on feature detection
- Observe effects on navigation



Background

Unmanned aerial vehicles are getting (more) popular

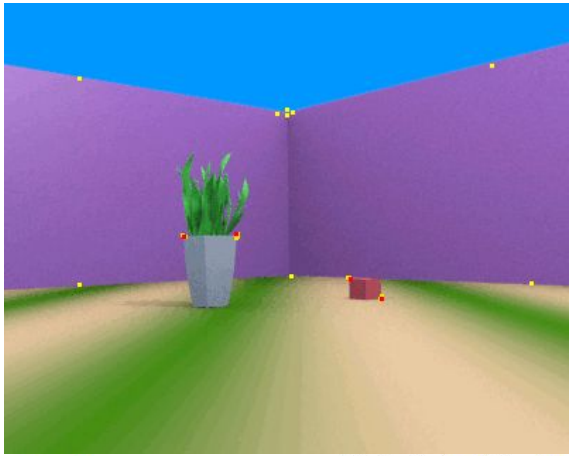
- Drones are used in Urban Delivery
- Safety Issues in fault handling
  - Can’t just stop
- Lasers already an existing problem for pilots

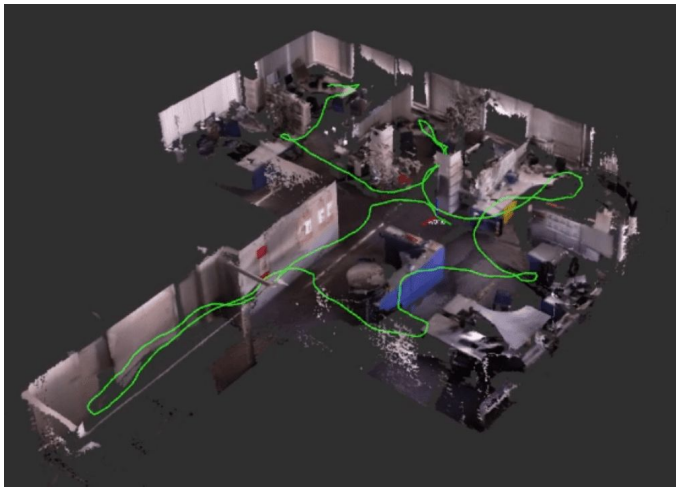
Urban Navigation Challenges

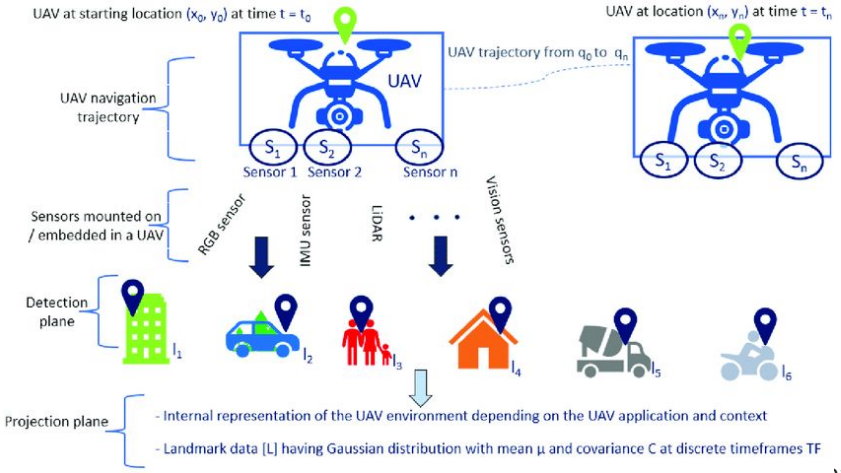
- GPS is unavailable, weak or inaccurate here
- Rely on positioning by other means, primarily cameras
- Susceptible to obstruction and damage

Vision Algorithms

- Visual Odometry (Egomotion, Corner tracking)
- Vision Inertial Odometry (Sensor Fusion with IMU)







Can laser interference be used to maliciously attack vision algorithms?

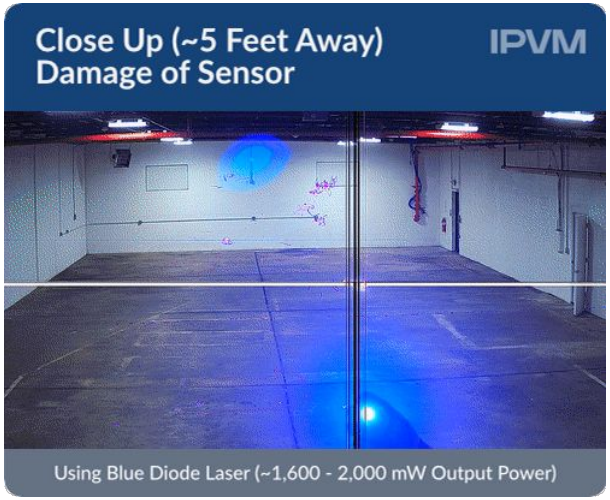
Reasoning and Justification

Laser (from light shows, autonomous lidar, mobile laser scanners, malicious intent, etc.)

1. Laser can cause temporary or permanent damage on most camera sensor

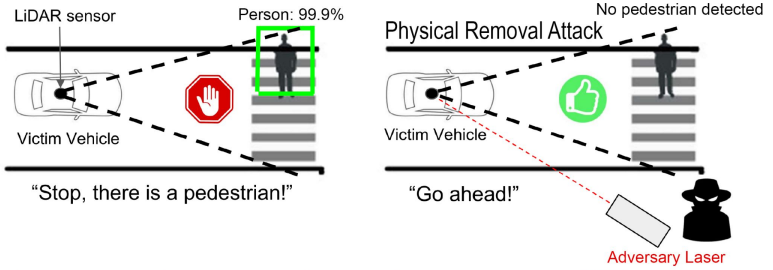
2. Vision navigation algorithms can falsely use these attributes as landmarks (corners)

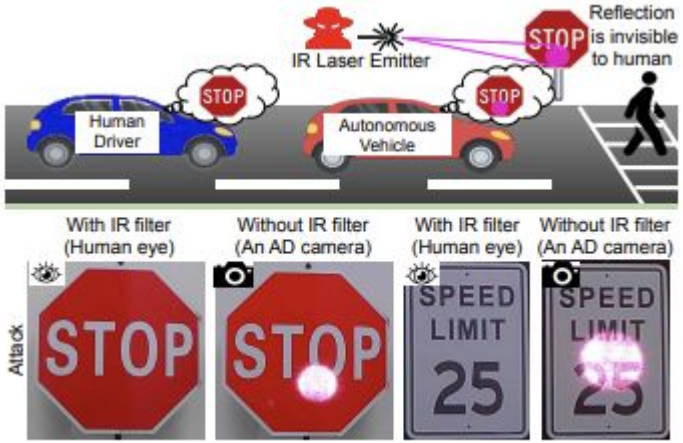
3. Lost of navigation **can** cause unexpected behaviour, shutdown or emergency landing



Existing Work

- Attacking LiDAR with Lasers
- Attacking Traffic Sign Recognition
- Vision Navigation (Egomotion)
- Sensor Input Spoofing



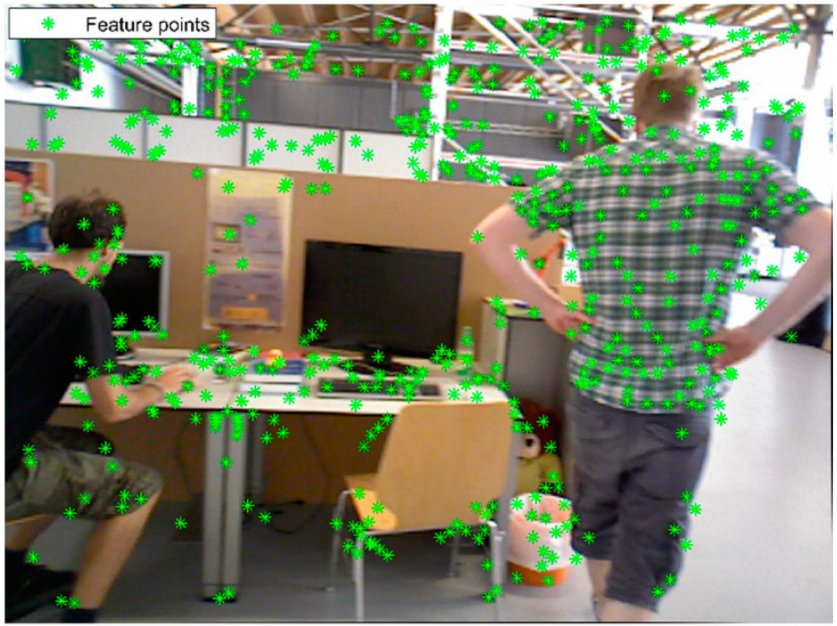


Real Examples

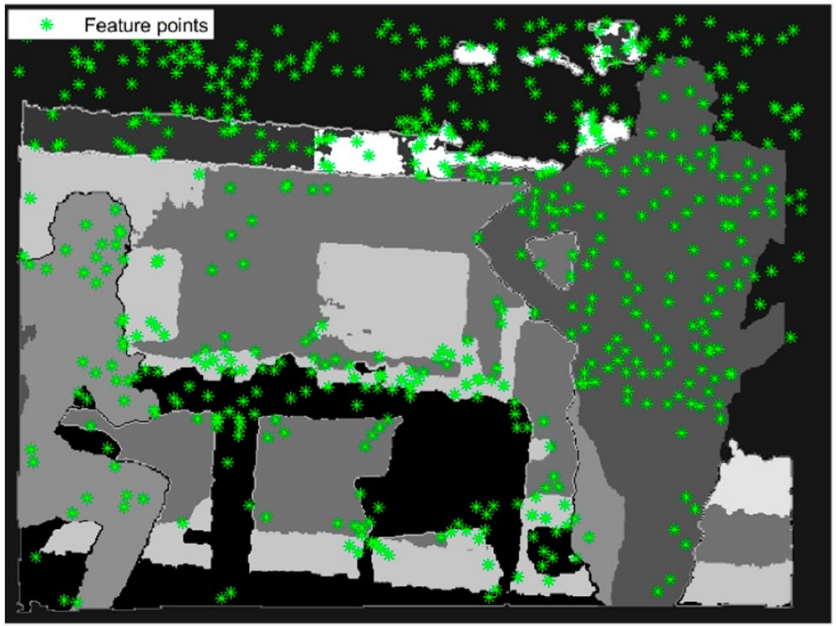
Real Examples

Attacking VO/VIO/SLAM

Feature Point and Corner Algorithms



(a)

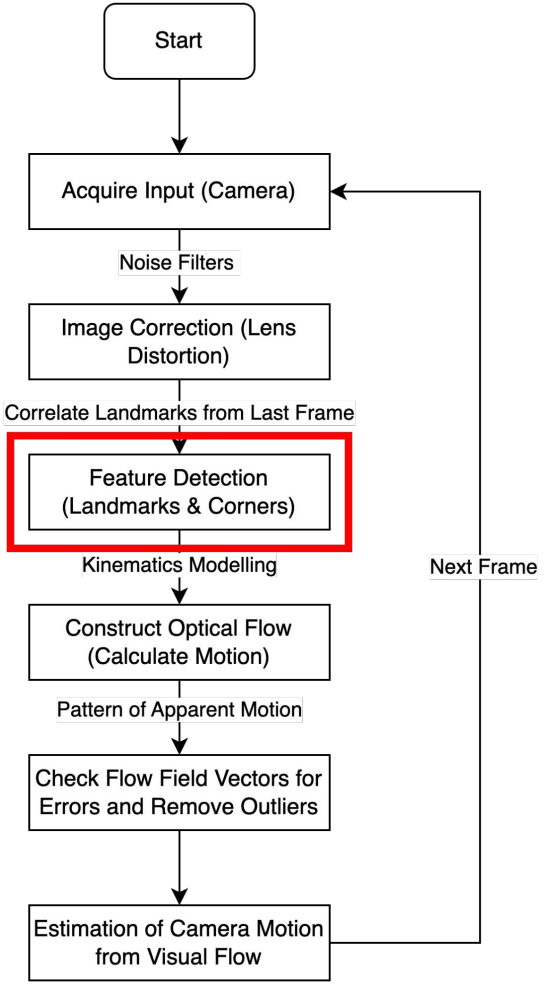


(b)

Attacking VO/VIO/SLAM

Using a known landmark detection algorithms

1. Construct a bad image input
2. Observe effects on feature detection
3. Observe effects on navigation navigation algorithm



Testing Plan and Method

Now - February

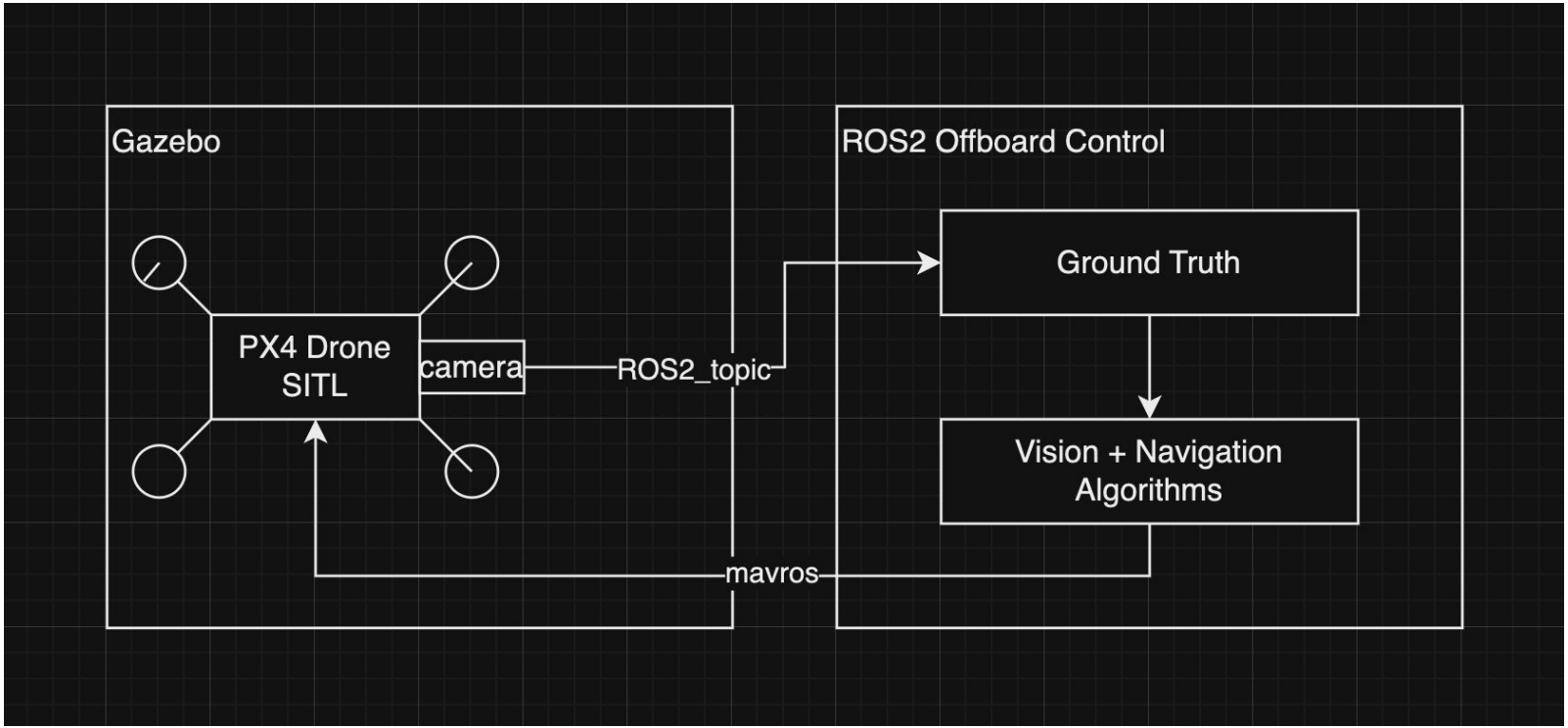
Simulation

- Build environment and vehicle
- Create ground truth
- Implement control algorithms

Real life replication (if time allows)

- Show the system reacting (adversely) to damage or interference

Testing Plan and Method



Summary

Visual is crucial

Correctness of camera is crucial

Resiliency of VIO to interference to lasers

Contact info