THE UNIVERSITY OF BRITISH COLUMBIA

# Out of Control: Stealthy Attacks on Robotic Vehicles Protected by Control-Based Techniques

Pritam Dash, Mehdi Karimi, and Karthik Pattabiraman

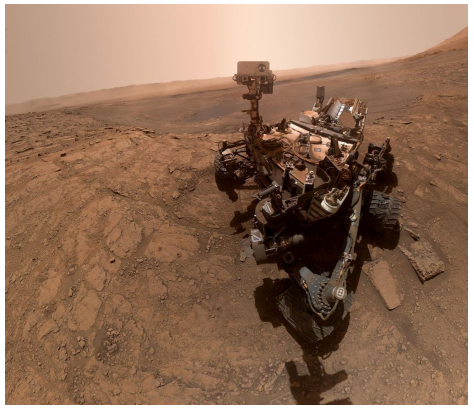
University of British Columbia, Vancouver, Canada

ACSAC 2019

# Robotic Vehicle (RV) in Industrial Sector

- Autonomous UAVs and Rovers.
  - Delivery
  - Warehouse Management
  - Surveillance
  - Cinematography


Autonomous RVs are increasingly becoming popular.
RV missions are time critical.



# Motivation

- GPS spoofing [ION GNSS'12], Optical spoofing [CCS'11]
- Acoustic noise injection in MEMS gyroscope [Usenix'15], MEMS accelerometer [Euro S&P'17]

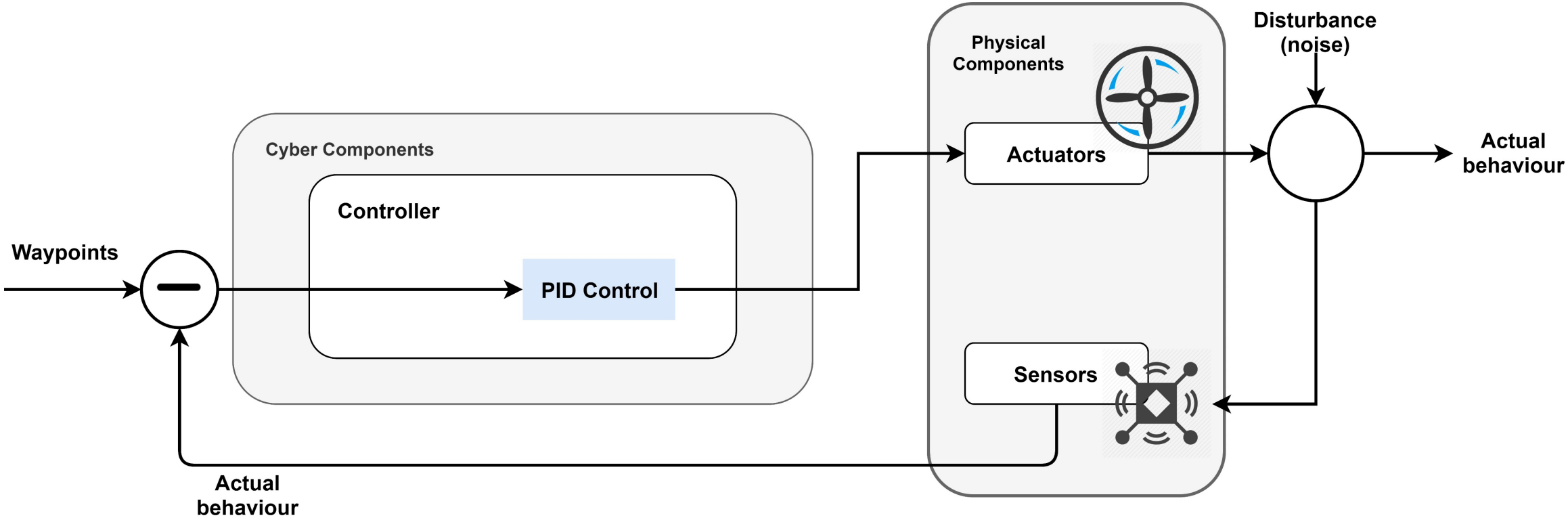
**Major Saudi Arabia oil facilities hit by drone strikes Sep 2019**

**Gatwick drone attack theories - who is behind the airport sabotage?**

Can an attacker remain stealthy and trigger adversarial actions?

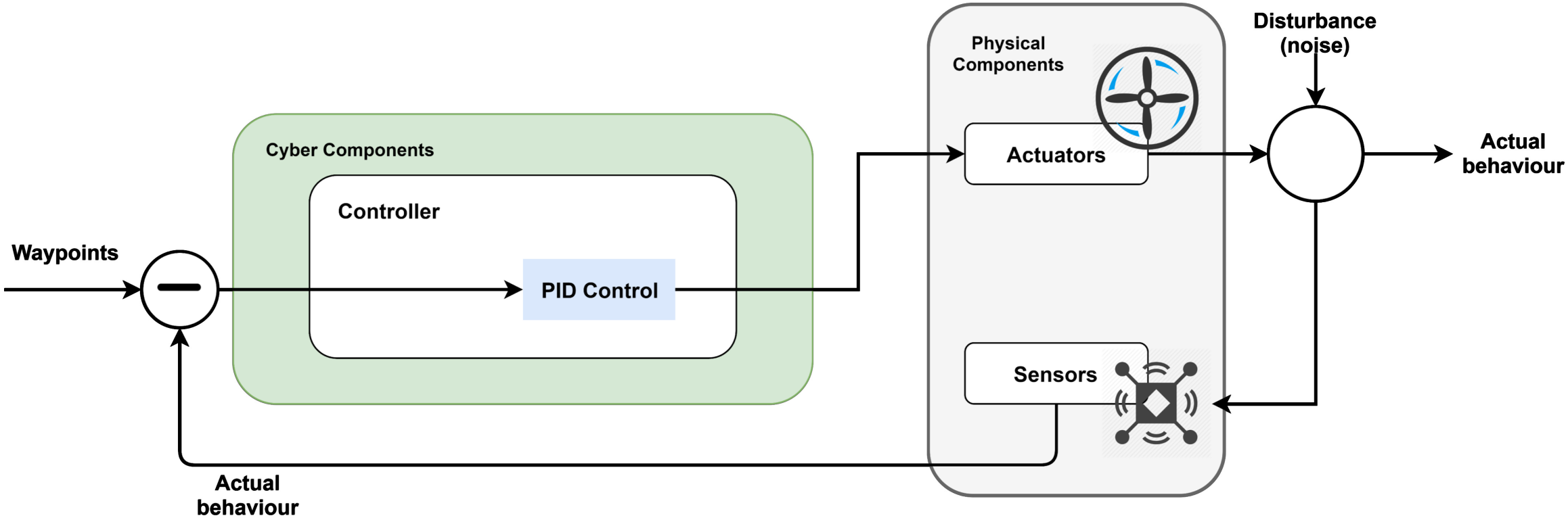
# Robotic Vehicle System

- Cyber component
- Physical component



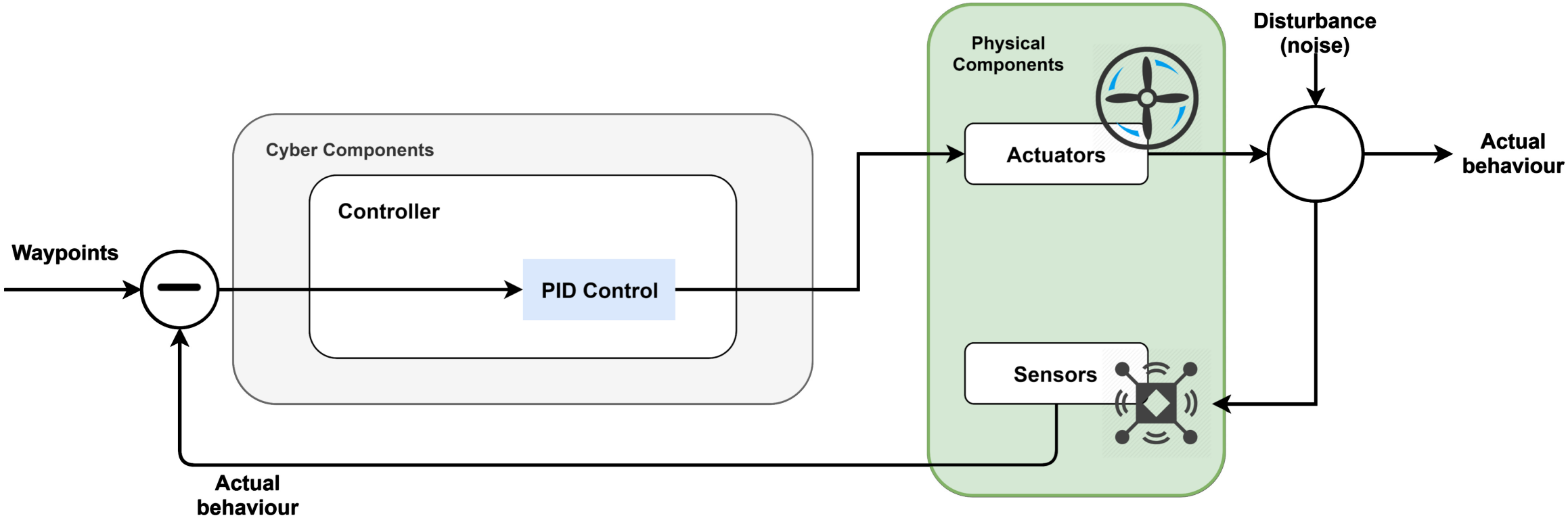
# Robotic Vehicle System

- Cyber component
- Physical component



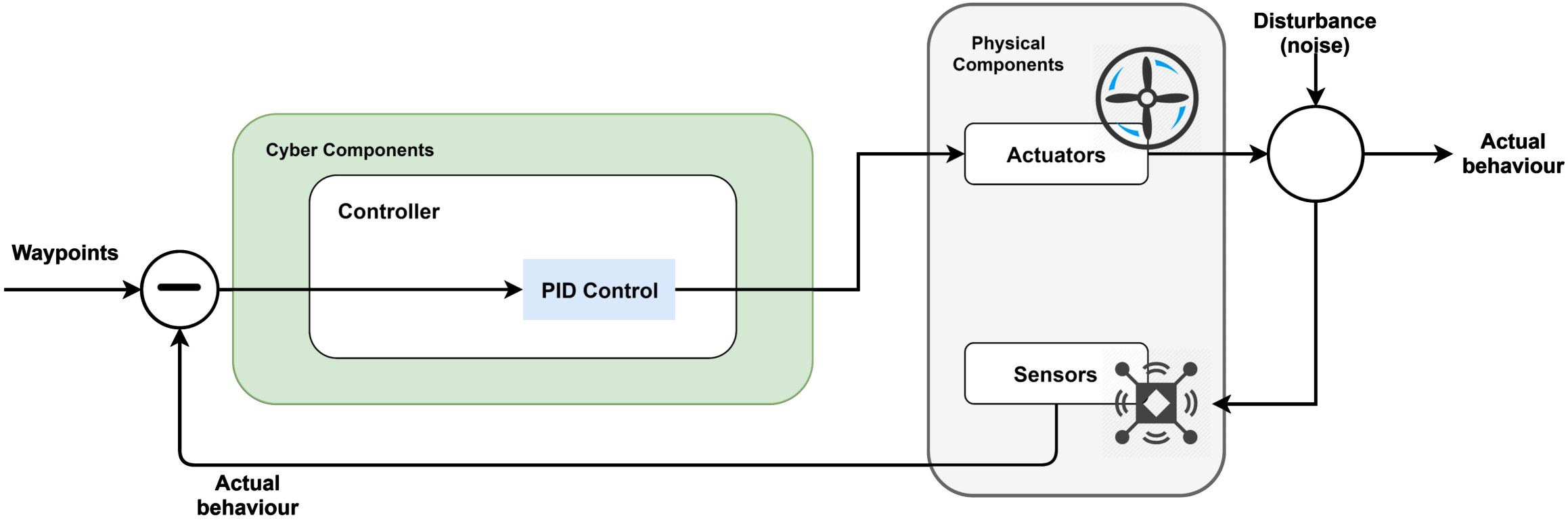
# Robotic Vehicle System

- Cyber component
- Physical component



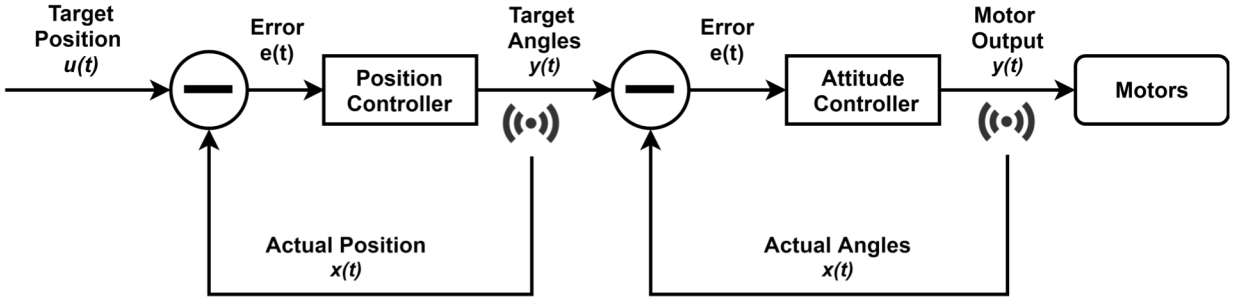
# Robotic Vehicle System

- Cyber component
- Physical component

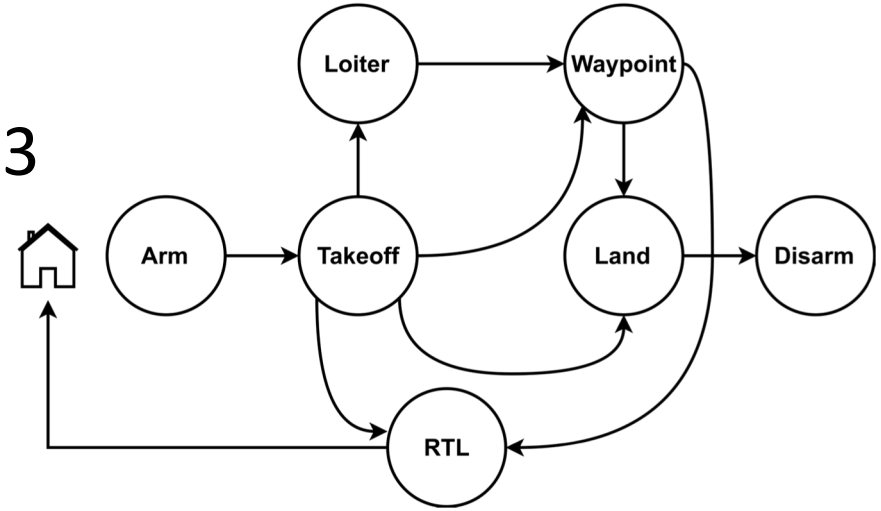


# Autonomous Control in RVs

- Control algorithms
  - Position Controller
  - Attitude Controller



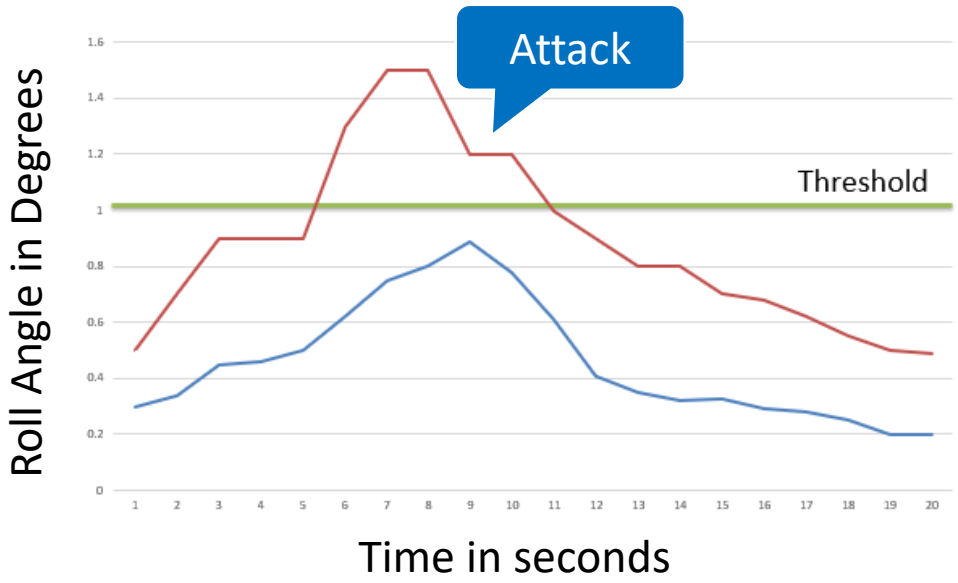

- Modes of Operation
  - A typical drone mission → at least 3 modes.



# Control-based Attack Detection Techniques

- Control Invariants (CI) [CCS'18]
  - State Space Model to predict target angles.


- Extended Kalman Filter (EKF)
  - Residual analysis → sensor or actuator attacks



# Limitations in Control-based Detection

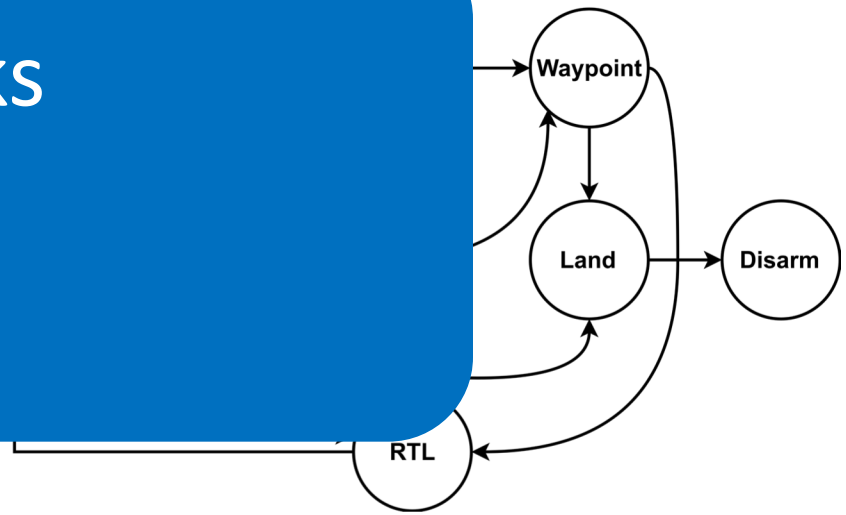
- Fixed threshold
  - Large threshold to reduce False Positives (FP).
    - Environmental factors – friction, wind
    - Sensor faults.
- Fixed Monito
- Often fail to
  - Takeoff
  - Waypoi

## Stealthy Attacks

False Data Injection

Artificial Delay

Switch Mode Attack



# Attack Model

137.49, -139.22

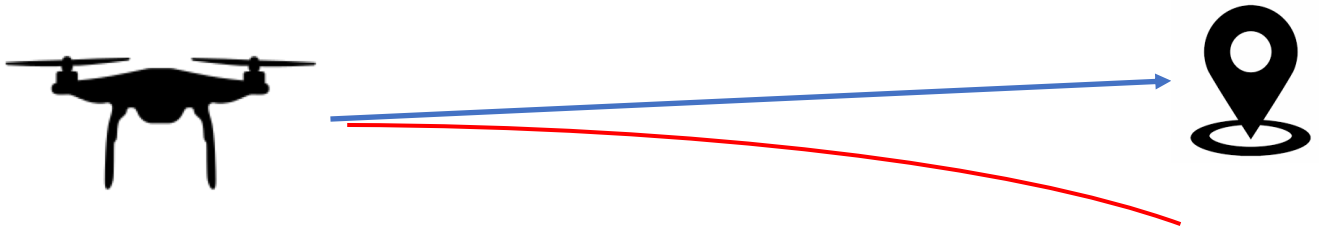
137.50, -140.40

137.50, -139.40

- Cannot tamper with the firmware.
- Cannot have root access to the RV system.
- Does not know the physical properties and detailed specifications of the RV.

# Attack 1: False Data Injection Attack

- Tampering sensor measurements
  - Inject false data → sensor
  - Acoustic noise



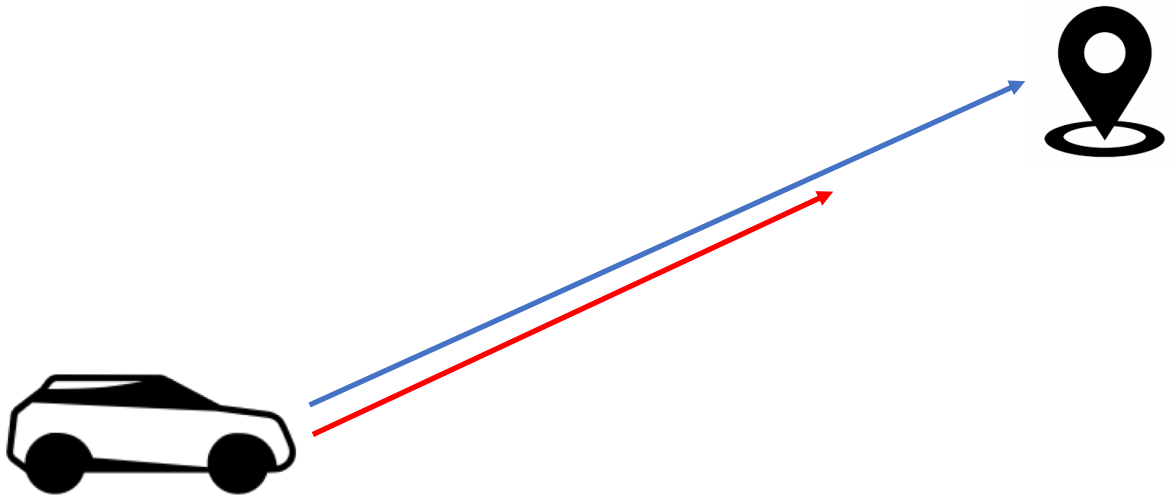
- False Data Injection
  - Delivery at a wrong location
  - Misplacements in warehouse


- [Usenix'15] Son et. al. Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

# Attack 2: Artificial Delay Attack

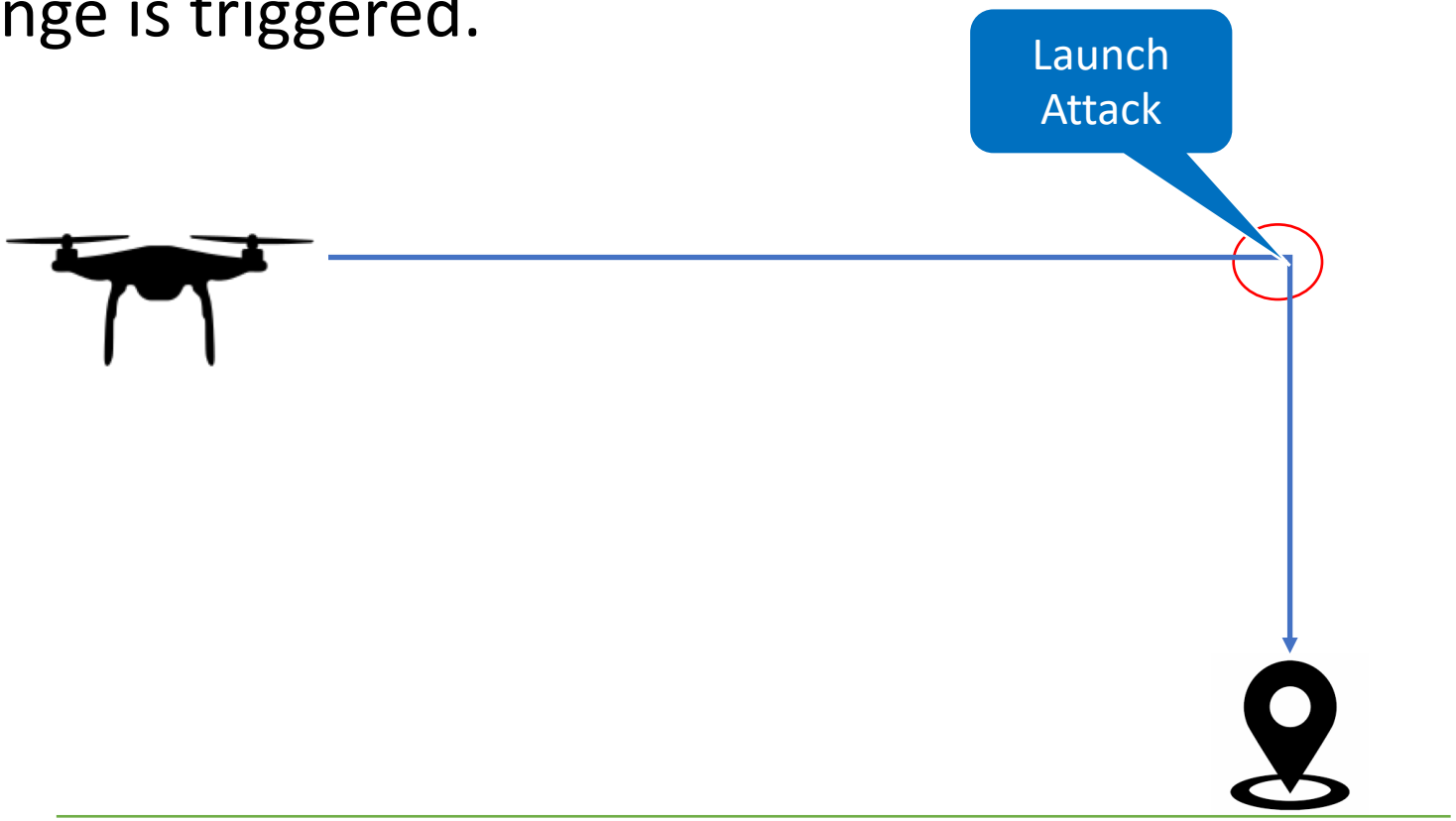
- Delay system operations
  - Mode changes
  - Motor commands

- Artificial delay attack
  - Delay receiving commands
  - Delays RV mission



# Attack 3: Switch Mode Attack

- Initiated when a mode change is triggered.
  - Steady-state flight → Land
  - Takeoff → Waypoint
- Switch mode attack
  - Gain elevation instead of landing
  - Potential crash

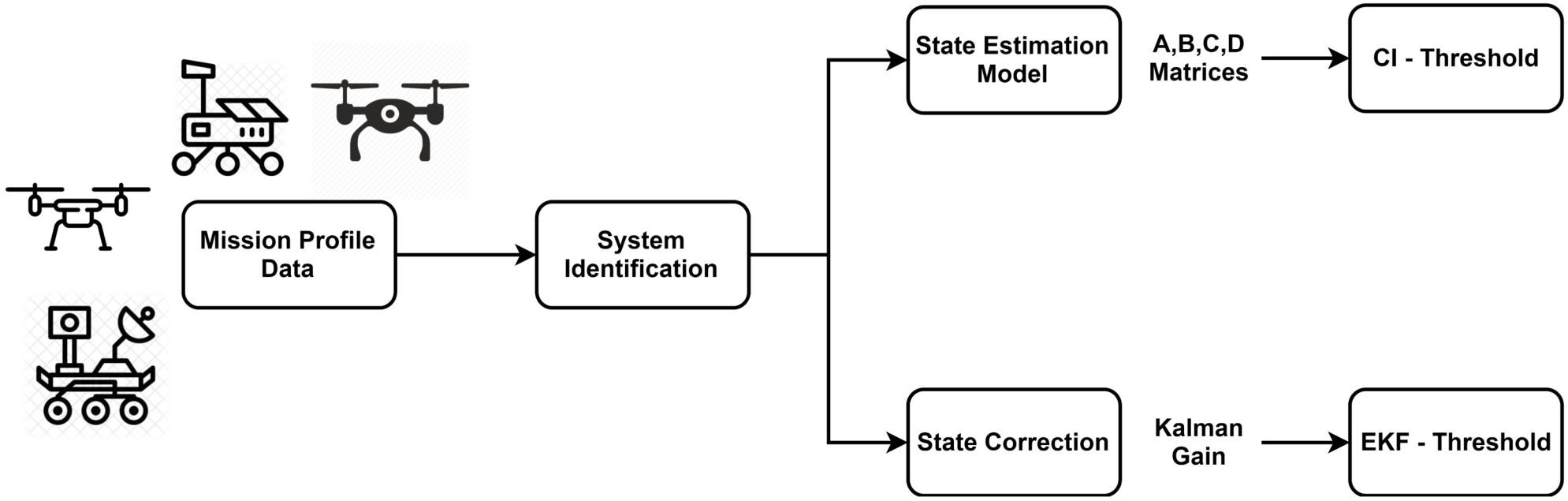


# Our Approach to Stealthy Attacks

- Challenges
  - Deriving the Detection threshold employed by CI and EKF.
    - Stealthy sensor tampering attacks – FDI, SM
  - Deriving the Monitoring window employed by control based IDS.
    - Artificial delays in control flow.

# State Estimation Model

- Collect mission profile data either from real RVs or simulations.
  - RVs autonomous flight control
  - Various mission trajectories.




https://www.mathworks.com/help/ident/gs/about-system-identification.html

# Triggering Stealthy Attacks at Runtime

- Controlled acoustic noise.
- Malicious libraries and wrapp
  - Exploiting dynamic linking feat
- Tampering gyroscopic sensor
- Running resource intensive op
- Tampering motor thrust outp


[DSN'16] Alemzadeh et. al. Targeted Attacks on Teleoperated Surgical Robots: Dynamic Model-Based Detection and Mitigation.

# Results and Evaluation

RQ1 How much effort does the attacker need to expend to derive the state estimation model?

RQ2 What are the impacts of the stealthy attacks on the subject RVs?

RQ3 How effective are the attacks in achieving the attacker's objectives?

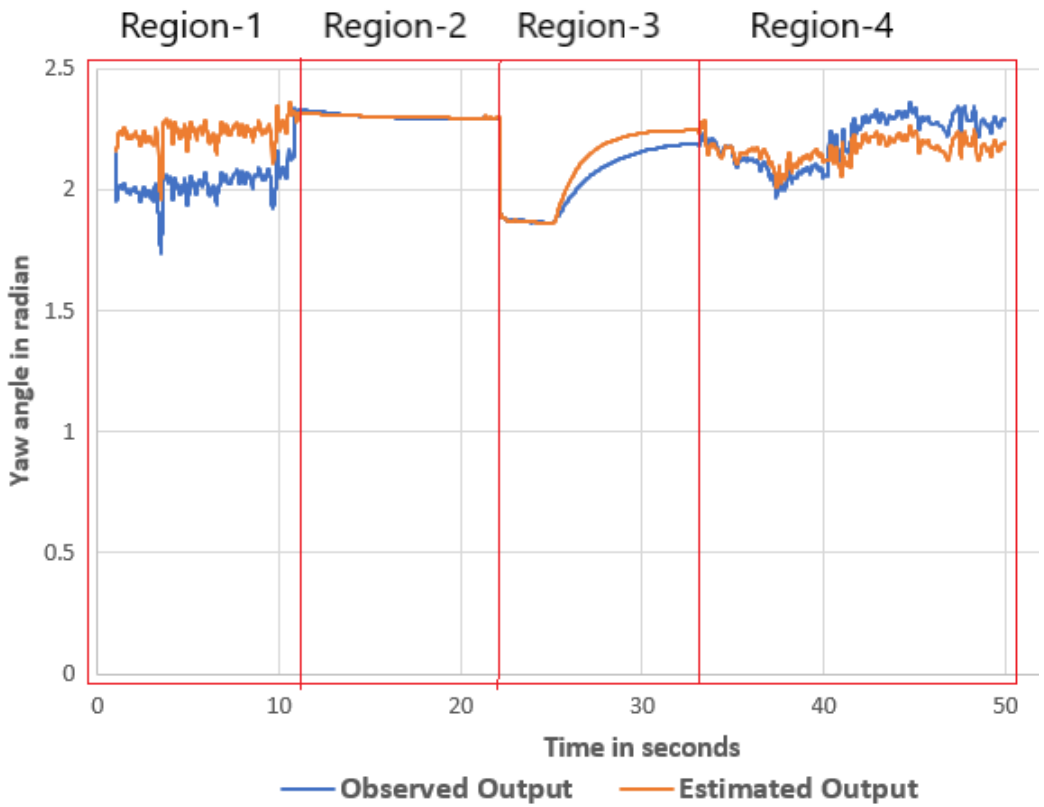

- ArduPilot - http://ardupilot.org/
- Pixhawk - https://pixhawk.org/
- Aion R1 Rover - https://www.aionrobotics.com/r1

# RQ1: Attacker's Effort

- Attacker's effort in deriving the state estimation model.

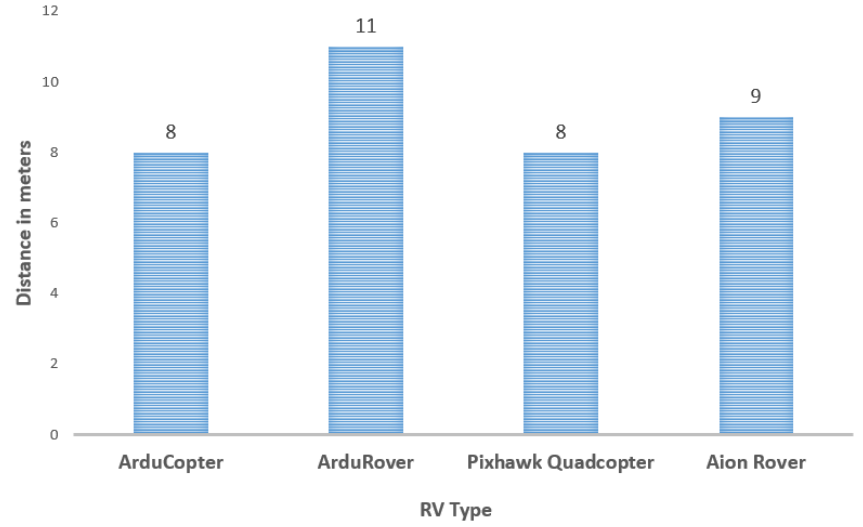
- Two Phases
  - Model extraction phase
    - 15 missions each subject RV.
  - Model testing phase
    - 5 missions each subject RV.

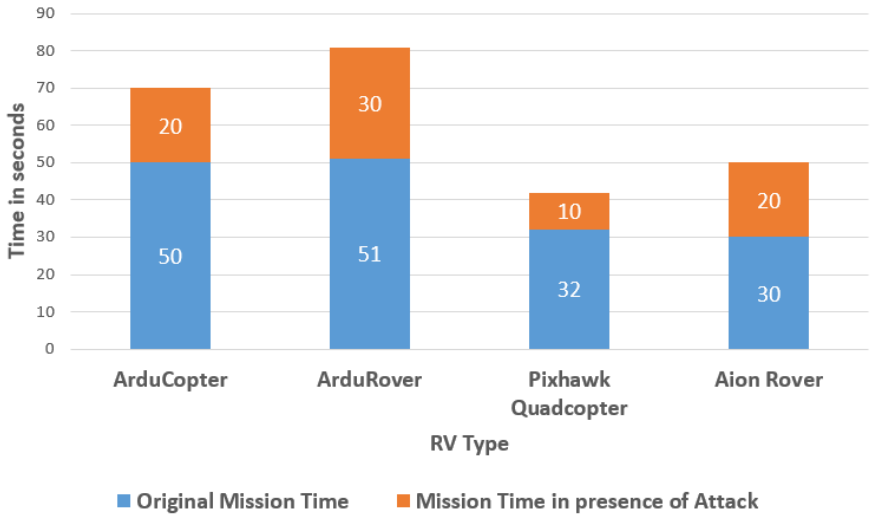
- Convergence
  - 5-7 missions for all the subject RVs.



# R2Q: Impacts of Stealthy Attacks

- False data injection attack
  - Deviates RV from its trajectory.
- Artificial delay attacks
  - Delays mission time
    - Drones → At least 25%
    - Rovers → At least 30%
- Switch mode attack (applicable to drone
  - Crash landing
  - Land at wrong locations.



# RQ3: Stealthy Attacks in Industrial Scenarios

- Delivery drones
  - Typical mission duration 30 mins.
  - Distance covered 1 – 20 KM
- False data injection
  - deviation more than 100 meters.
- Artificial delay
  - increase mission time by 25-30%.
- Switch mode
  - Ignore commands.
  - crash landing.

# How to Detect Stealthy Attacks?

- Large detection threshold enables stealthy attacks.
  - Improved system modelling → accurate estimations.
  - Smaller Thresholds, smaller monitoring windows.
- Inability to model the mode change states.
  - Modelling the Non-linear and Dynamic behavior during RV mission.

- Improved noise filtering techniques
  - Prevent sensor manipulation
  - Increase the production cost

# Summary

- Vulnerabilities in control theory based attack detection techniques.
- Demonstrate three types of stealthy attacks on RV simulator and real RV systems.
  - Attacks deviate a RVs by more than 100 meters, increases duration of RV mission by 25-30%, even result in crashes.
- Demonstrate techniques to automate the attacks on a class of RVs.


Pritam Dash

pdash@ece.ubc.ca

Artifacts: https://github.com/DependableSystemsLab/stealthy-attacks