IMUFUZZER:
Resilience-based Discovery of Signal Injection Attacks on Robotic Aerial Vehicles

Sudharssan Mohan*, Kyeongseok Yang‡, Zelun Kong*, Yonghwi Kwon†, Junghwan Rhee§,
Tyler Summers*, Hongjun Choi¶, Heejo Lee‡, Chung Hwan Kim*

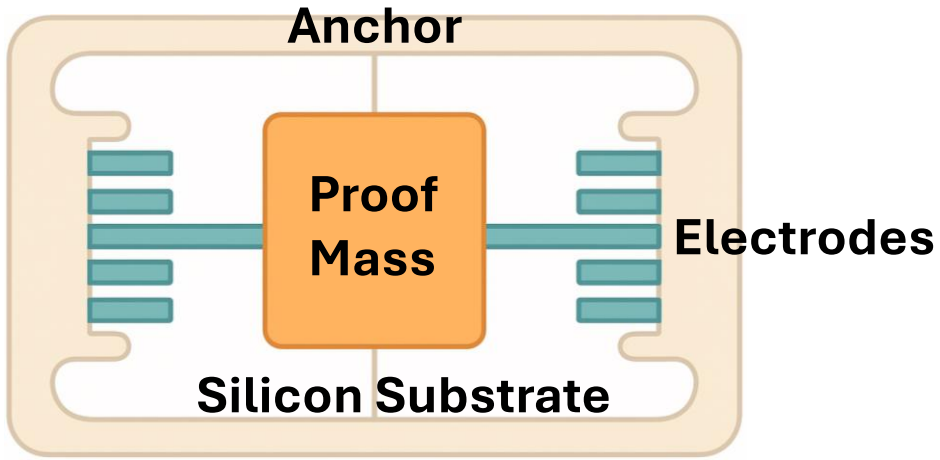
*University of Texas at Dallas, ‡Korea University, †University of Maryland,
§University of Central Oklahoma, ¶DGIST

MEMS IMU Sensors

- **IMU Sensors –** Accelerometers and Gyrocopes.

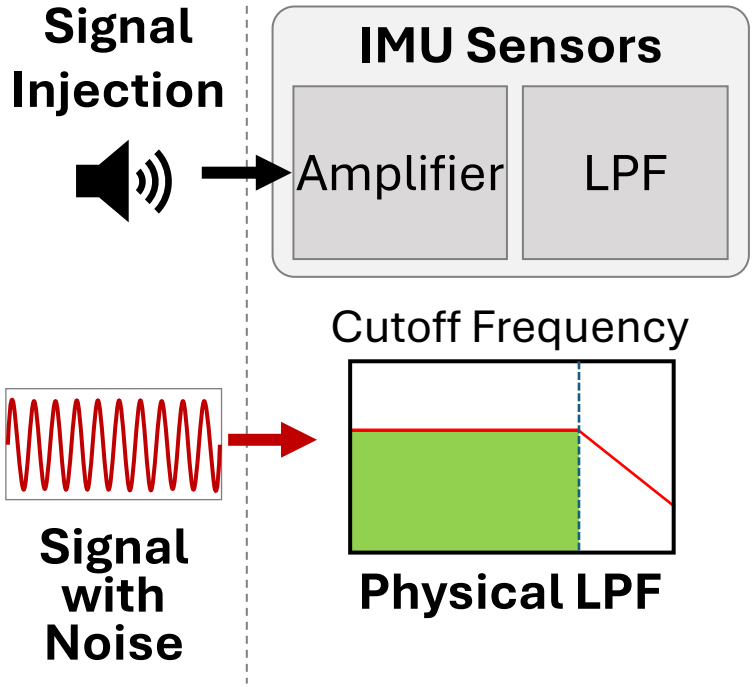
Sensor	Measures
Accelerometer	Speed/Acceleration
Gyroscope	Roll, Pitch & Yaw

- **MEMS Sensors –** Micro-electro-mechanical systems.



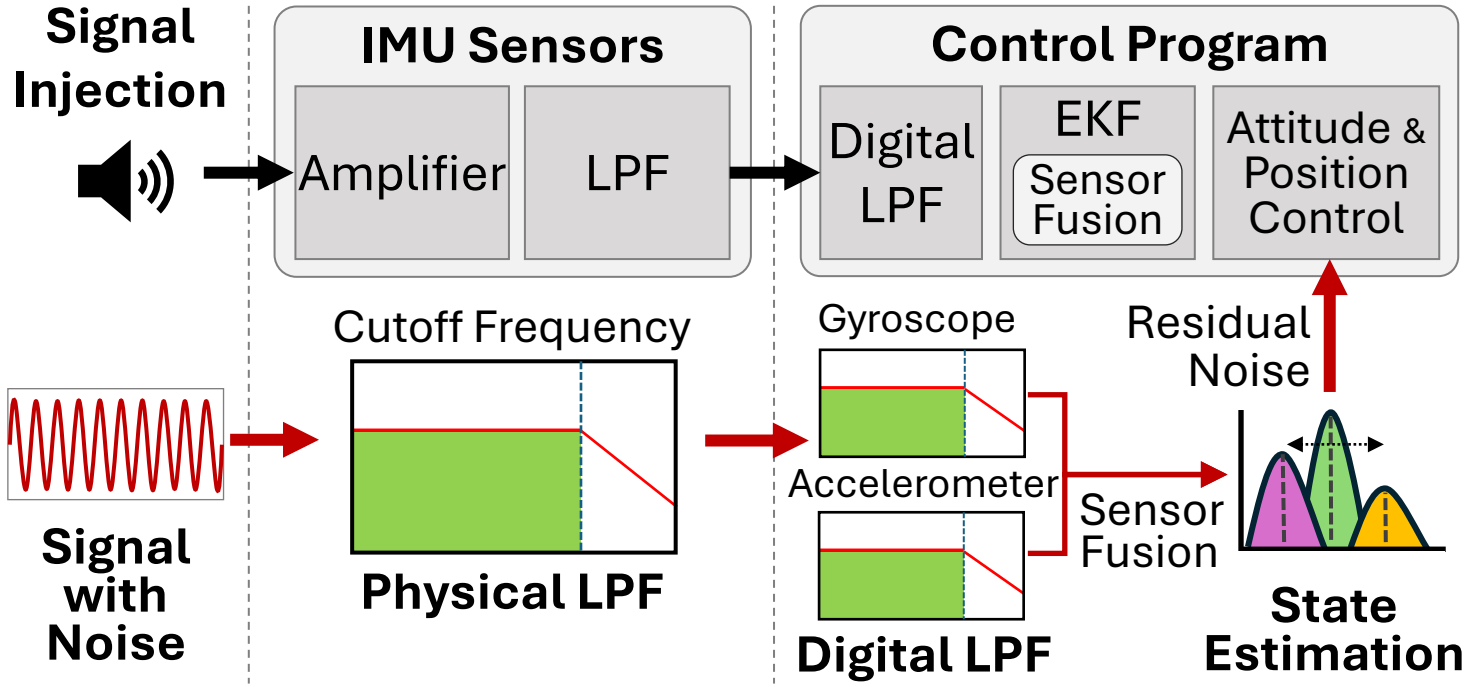
Signal Injection Attacks

- Sensor spoofing with acoustic signals [USENIX Sec'15, EuroS&P'17, USENIX Sec.'18].



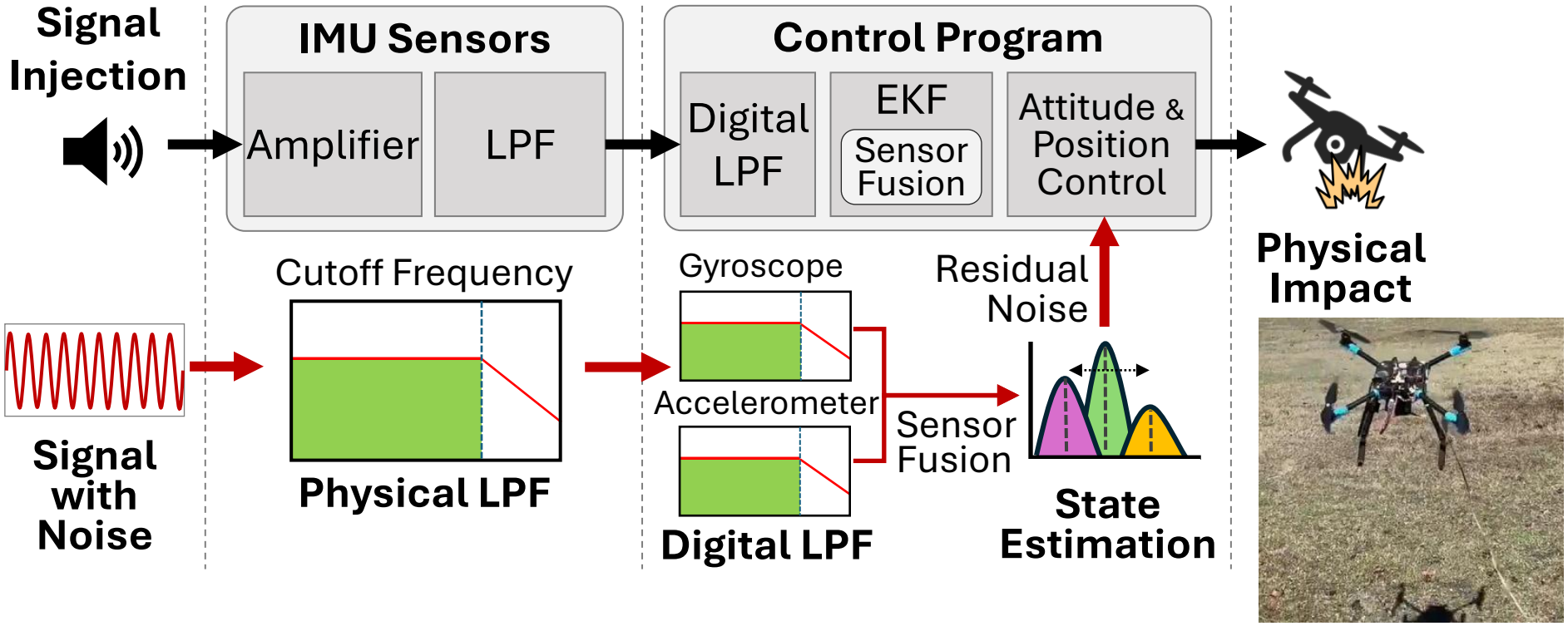
Signal Injection Attacks

- Sensor spoofing with acoustic signals [USENIX Sec'15, EuroS&P'17, USENIX Sec.'18].

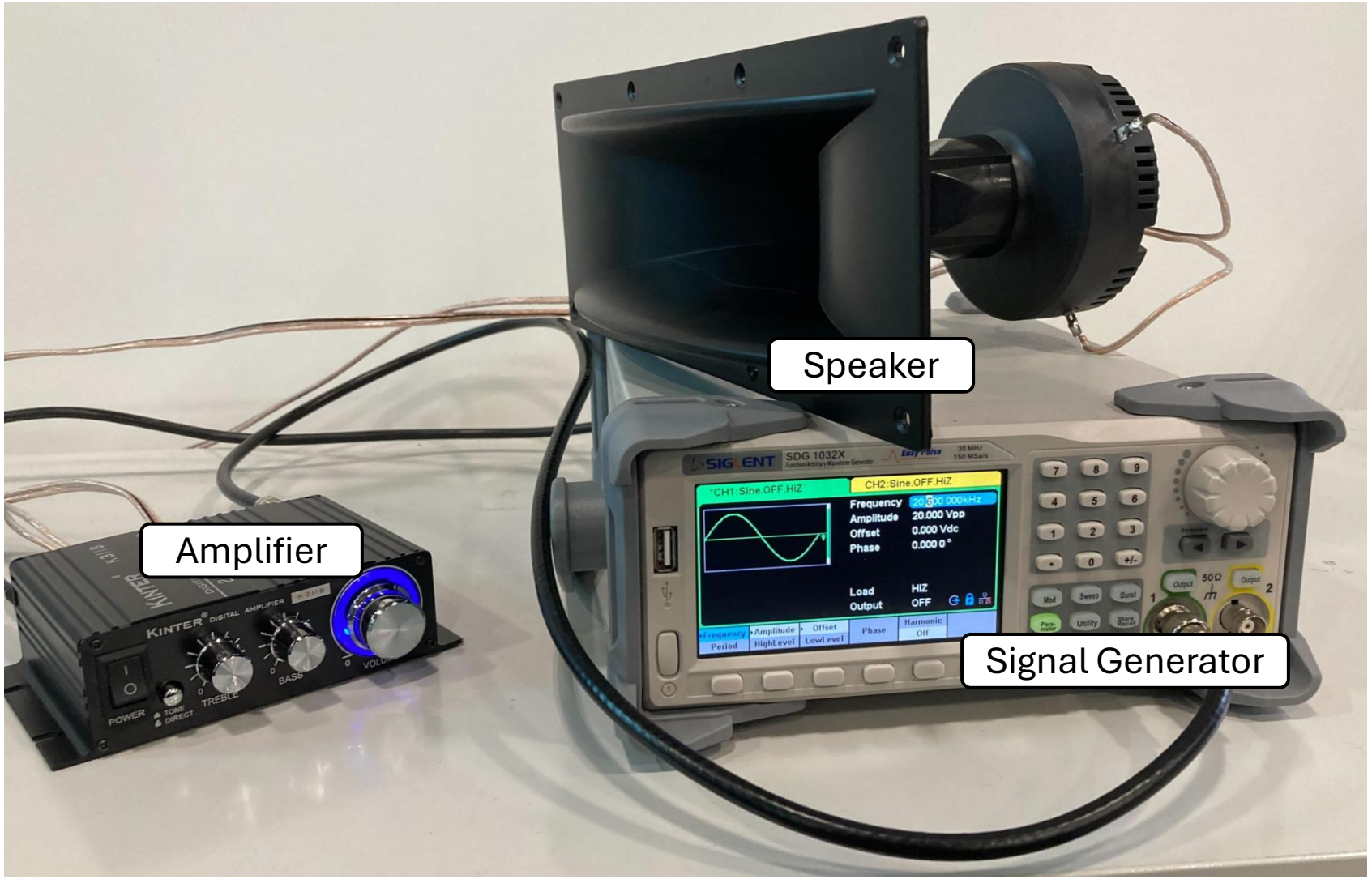


Signal Injection Attacks

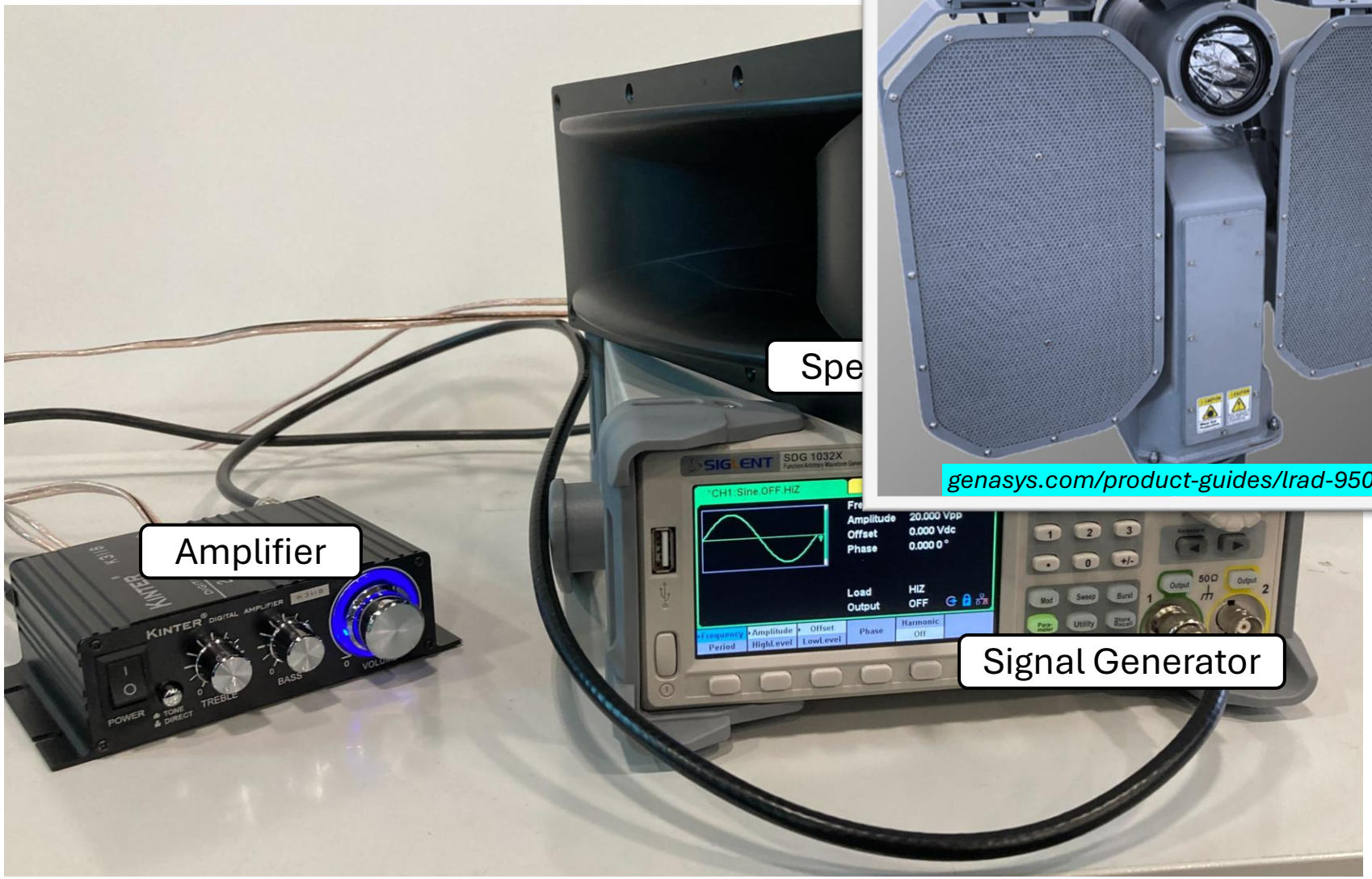
- Sensor spoofing with acoustic signals [USENIX Sec'15, EuroS&P'17, USENIX Sec.'18].



Attack Setup



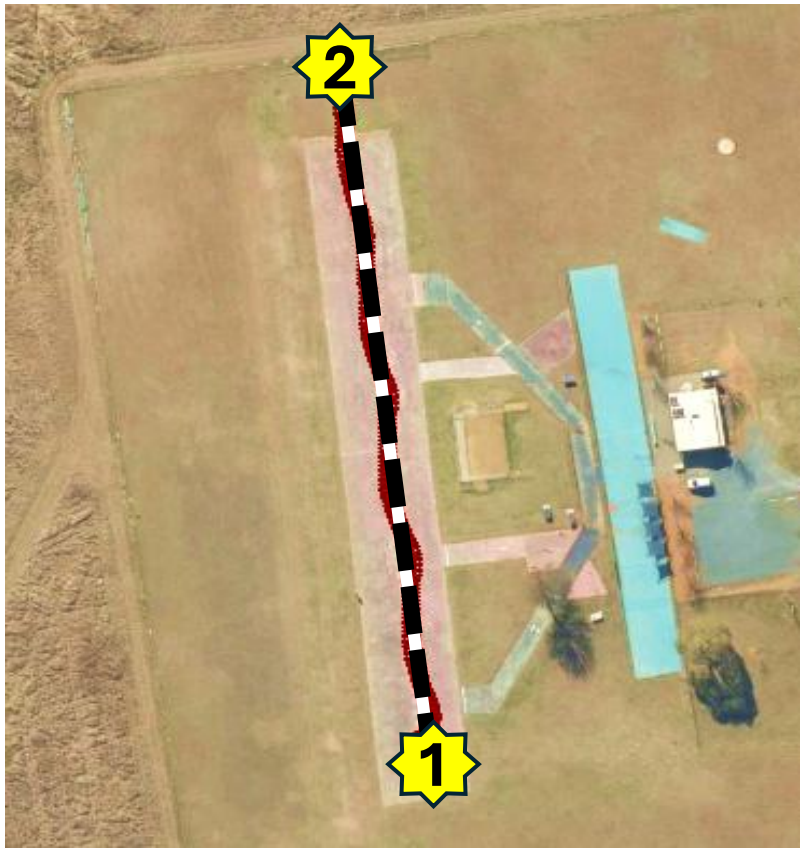
Attack Setup

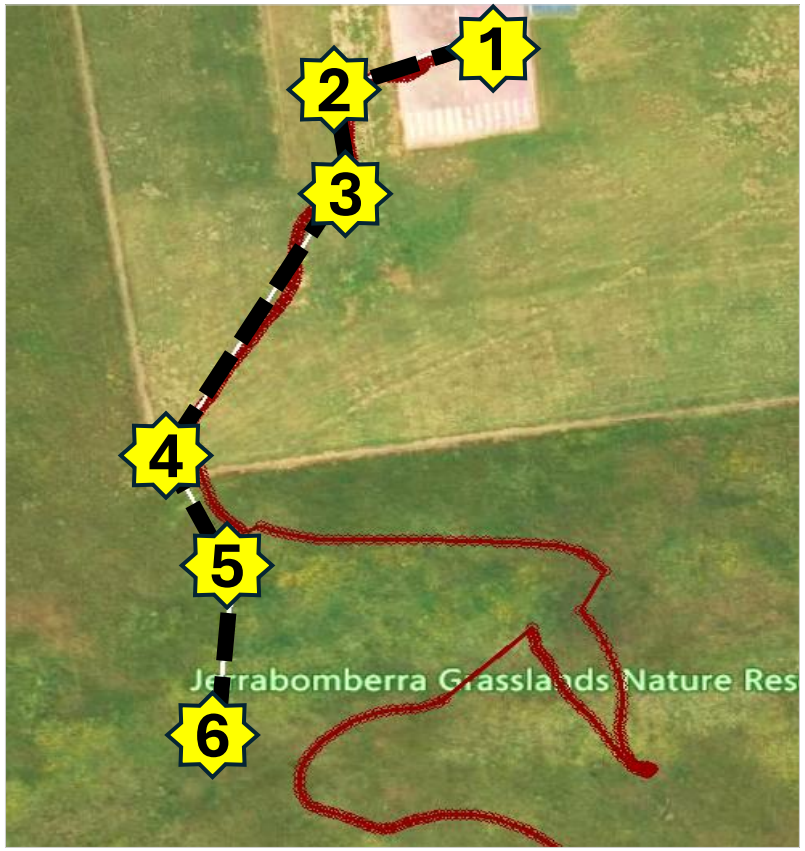


Do The Same Attacks Work In All Cases?

Do The Same Attacks Work In All Cases?

No. Same Attacks ≠ Same Impacts.

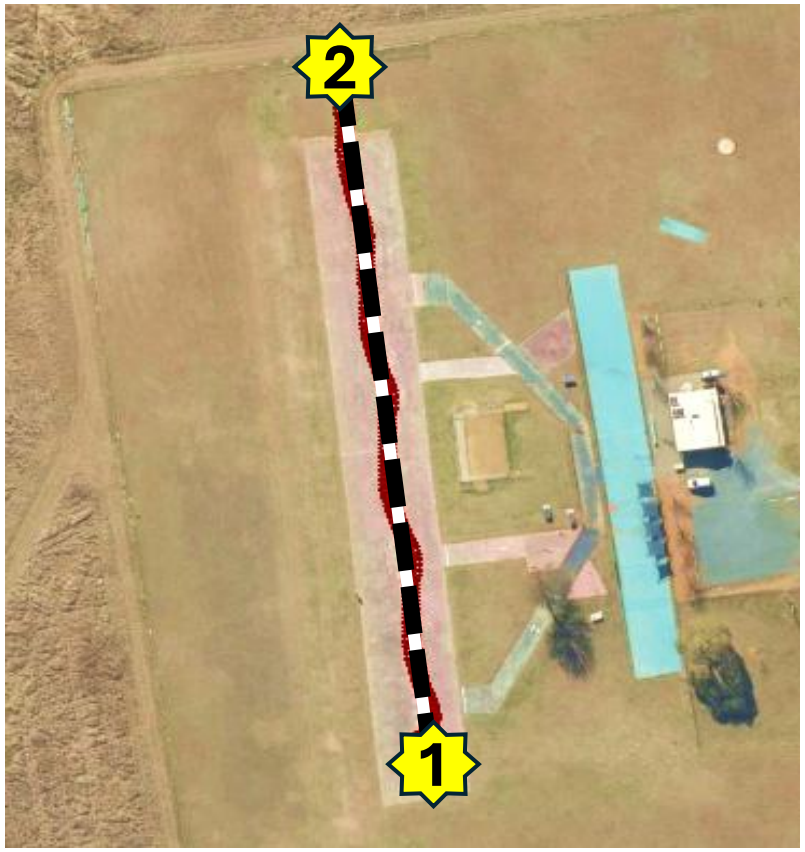


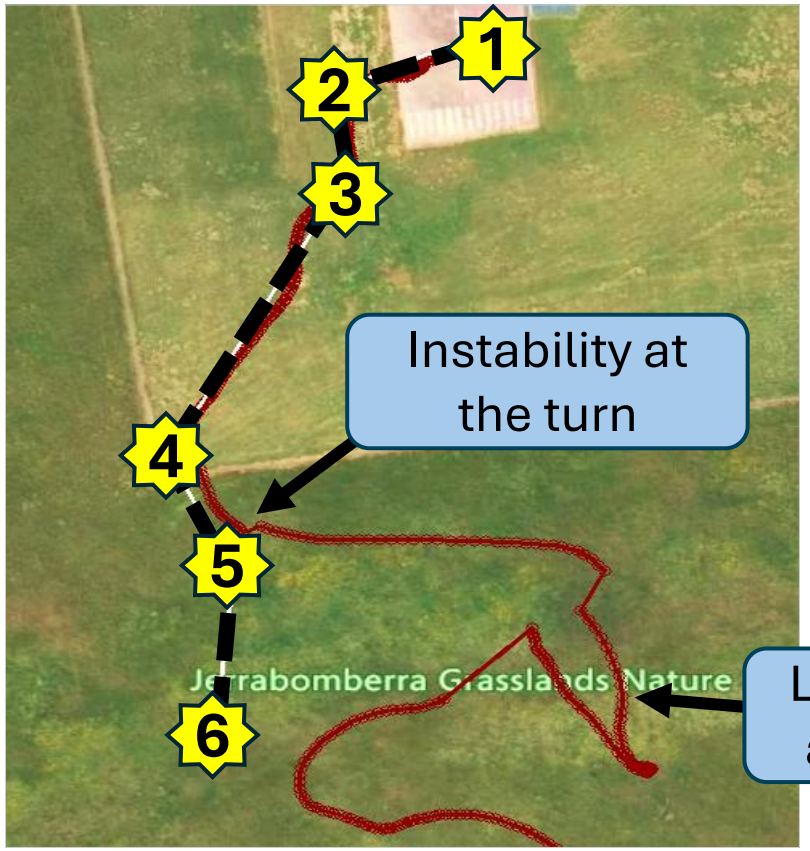


Actual Path
Mission Path
Waypoints

Do The Same Attacks Work In All Cases?

No. Same Attacks ≠ Same Impacts.





Actual Path
Mission Path
Waypoints

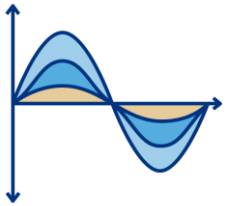
Change in physical states triggers crash!

IMUFUZZER's Approach

- We present ***IMUFUZZER***:

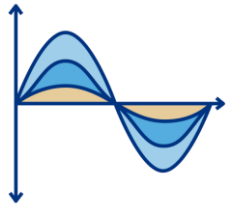
IMUFUZZER's Approach

- We present ***IMUFUZZER***:
  - **Sensor fuzzing** to discover signal injection attacks.

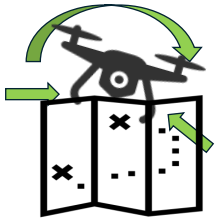


IMUFUZZER's Approach

- We present ***IMUFUZZER***:
  - **Sensor fuzzing** to discover signal injection attacks.

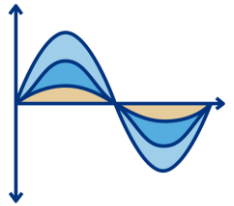


  - Explore **physical states** to find **hidden attacks**.

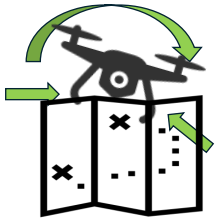


IMUFUZZER's Approach

- We present ***IMUFUZZER***:
  - **Sensor fuzzing** to discover signal injection attacks.



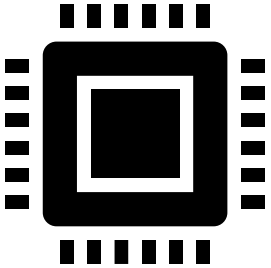
  - Explore **physical states** to find **hidden attacks**.



  - **Control-aware feedback** for efficient sensor fuzzing.

Inputs To Fuzzer

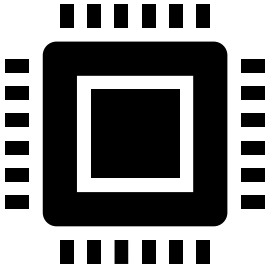
Inputs To Fuzzer



Sensor Profile

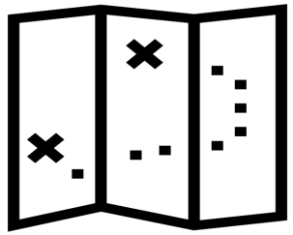
Derived from real-world
IMU sensors

Inputs To Fuzzer



Sensor Profile

Derived from real-world IMU sensors



Seed Mission

1. Waypoints
2. Distances
3. Angles

Sensor Input Generator

- Injects sine waves with varying **amplitude & frequency.**

$$A * sin(2\pi Ft + \phi)$$

Sensor Input Generator

- Injects sine waves with varying **amplitude & frequency.**

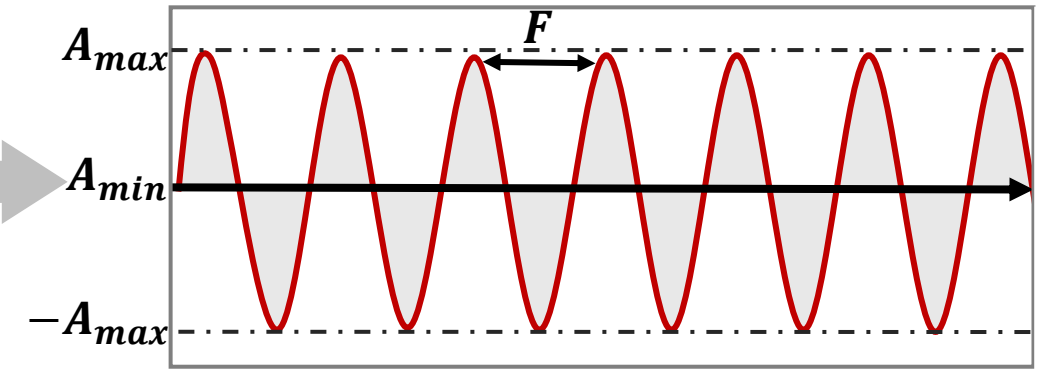
$$A * sin(2\pi Ft + \phi)$$

Sensor Type [Accel/Gyro]

Amp. = [A_{min}, A_{max}]

Freq. = [0, 50]kHz

Sensor Profile



Generated Sensor Signal

Mission Mutation

- Generates diverse 3D mission paths.

Dist. = [0,30]m.

XY-Ang.= [0,360]°

Z-Ang.= [-90,+90]°

Mission Mutator

Mission Mutation

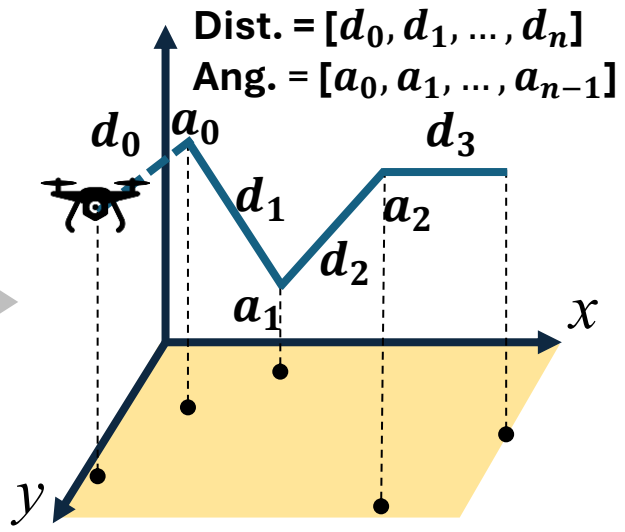
- Generates diverse 3D mission paths.

Dist. = [0,30]m.

XY-Ang.= [0,360]°

Z-Ang.= [-90,+90]°

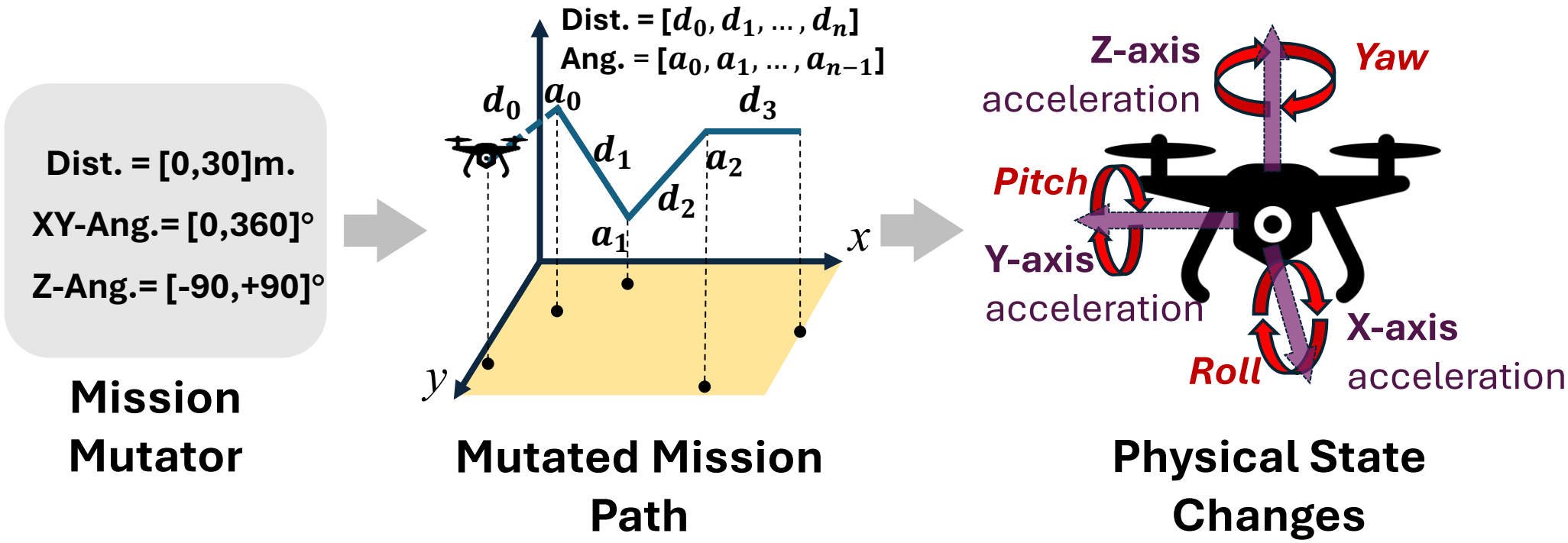
Mission Mutator



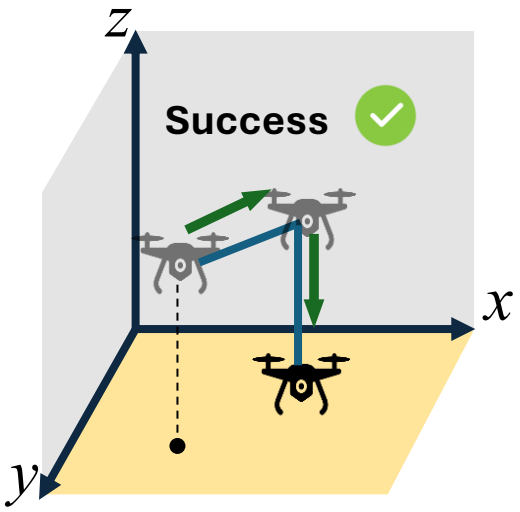
Mutated Mission Path

Mission Mutation

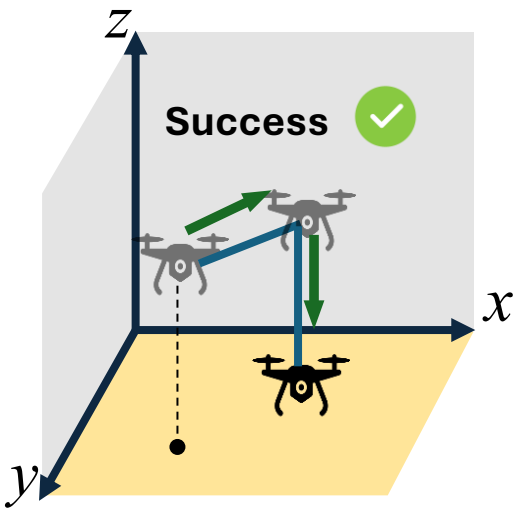
- Generates diverse 3D mission paths.

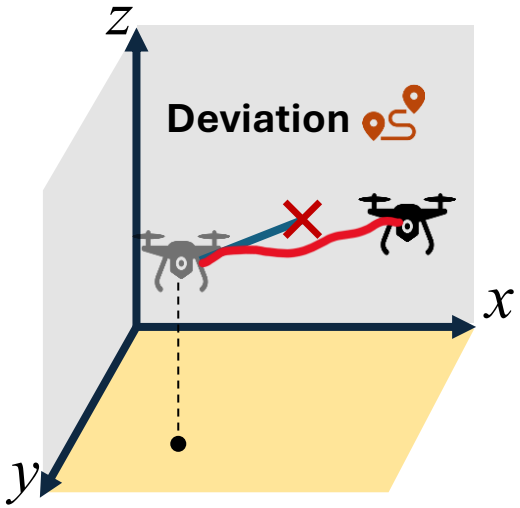


Mission Failure Detection

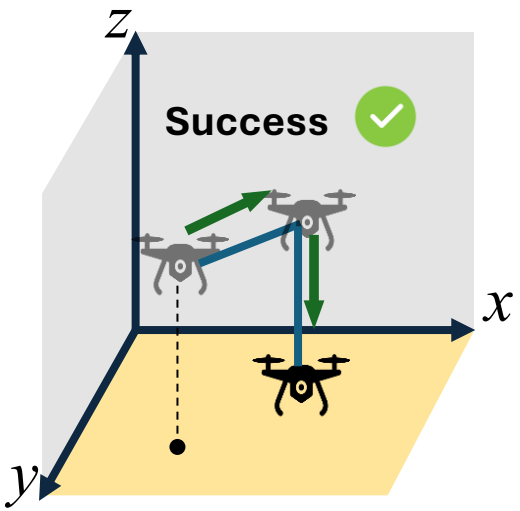


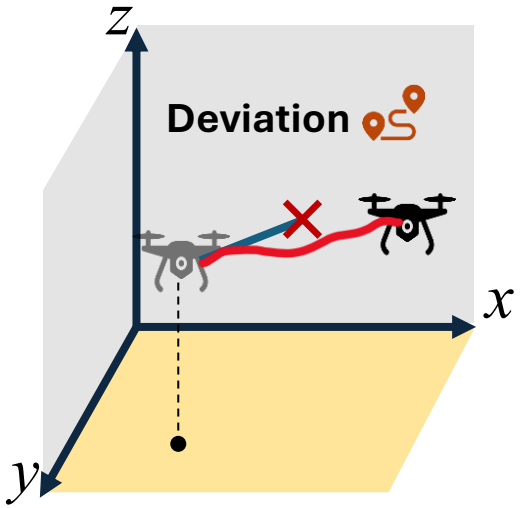
Mission Failure Detection

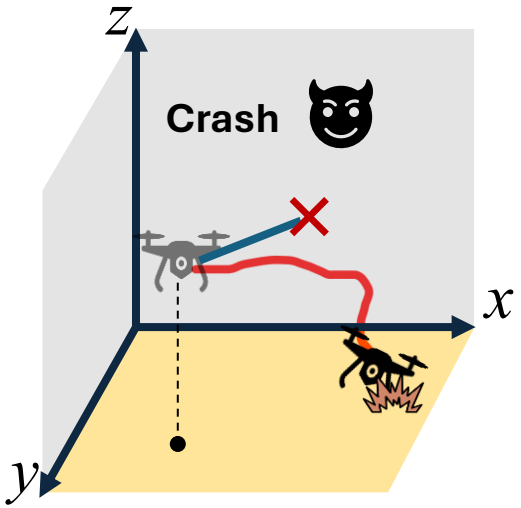




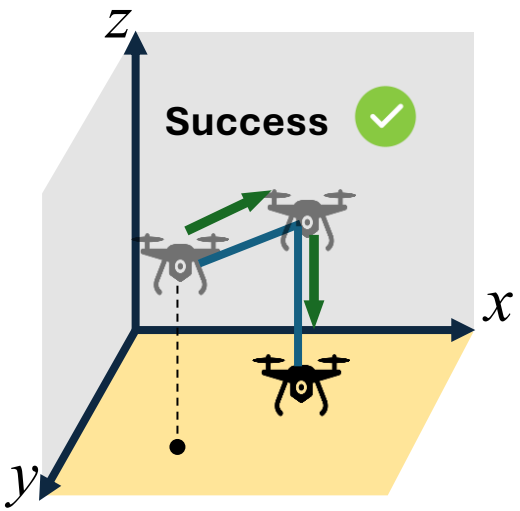
Mission Failure Detection

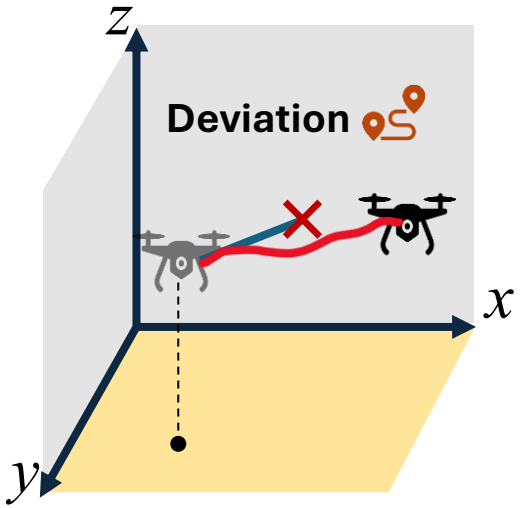


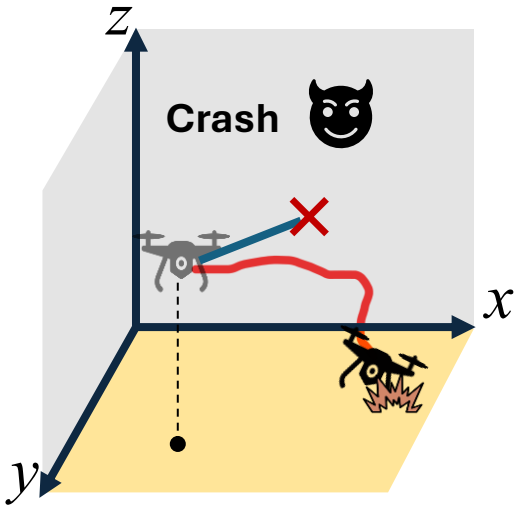


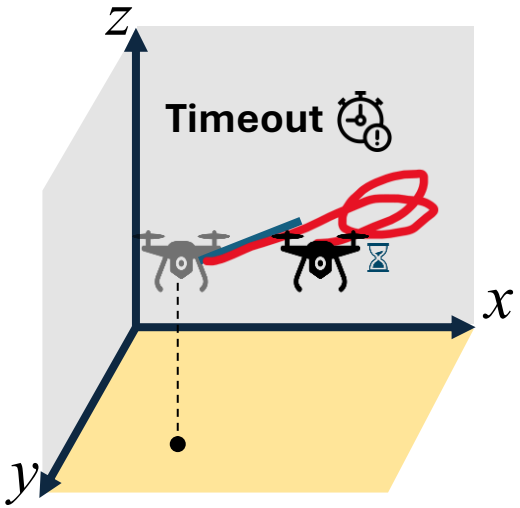


Mission Failure Detection

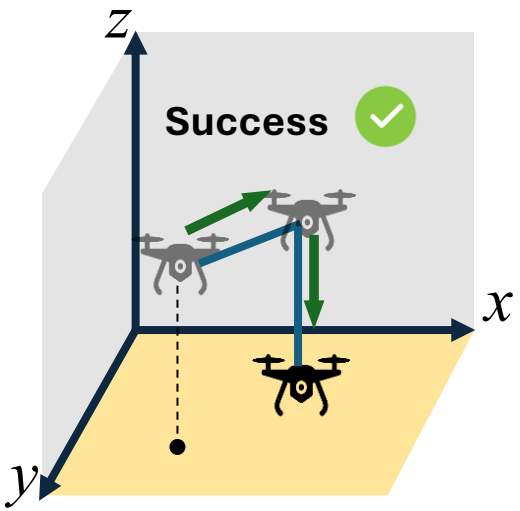


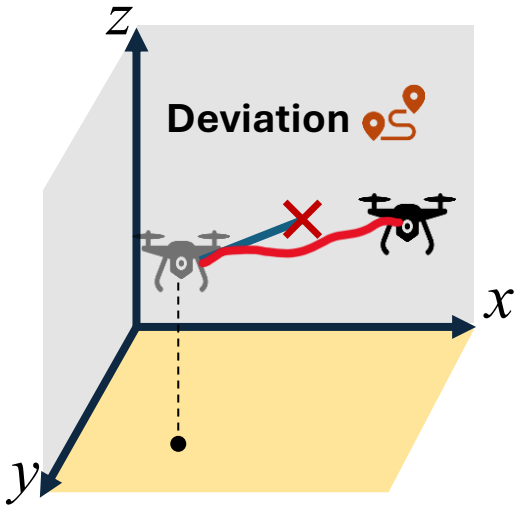


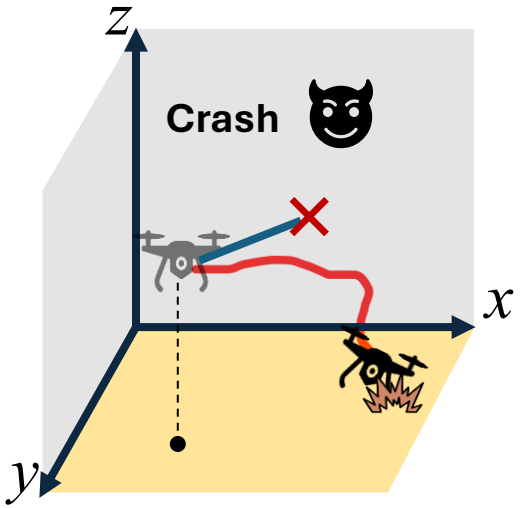


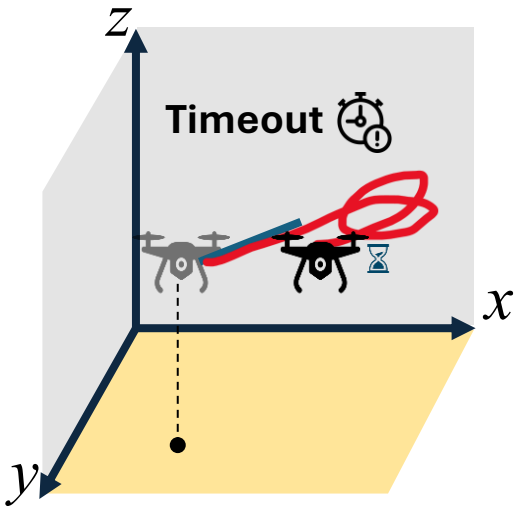


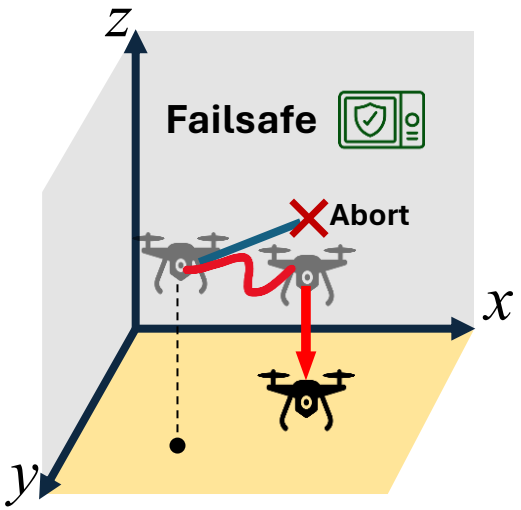
Mission Failure Detection





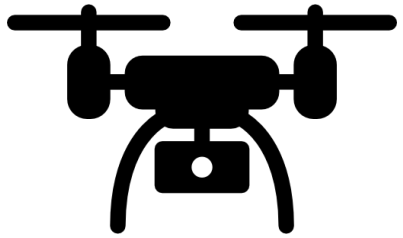






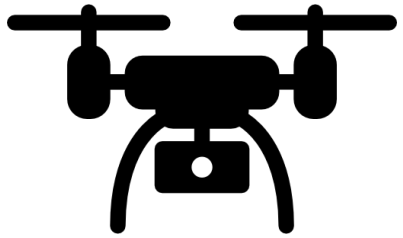
What Feedback Metric Should We Use?

What Feedback Metric Should We Use?



Mission Success ≠ Stable Flight

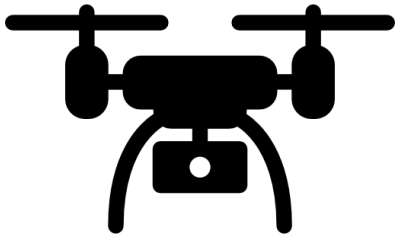
What Feedback Metric Should We Use?



Mission Success ≠ Stable Flight

Code Coverage ≠ More Attacks

What Feedback Metric Should We Use?



Mission Success ≠ Stable Flight

Code Coverage ≠ More Attacks

Feedback Metric: Resilience Score

Resilience Score

- Quantifies RAV **stability and performance**.

- Having lower ρ → weaker RAV resilience (system destabilized).

Resilience Score

- Quantifies RAV **stability and performance**.

- Having lower ρ → weaker RAV resilience (system destabilized).

Computed by monitoring **internal controller states**:

1. Acceleration
2. Angular Velocity
3. Position

Evaluation

- ArduCopter v4.5.0

- Physical drone experiments with Pixhawk4 board.

Sensor Profiles Used by IMUFuzzer

Sensor Profiles Used by IMUFuzzer

6 real-world IMU sensor profiles

Sensor Profiles Used by IMUFuzzer

6 real-world IMU sensor profiles

Find a **valid range** of displacements for each IMU under test.

	Sensor	Amp. (V)	Freq. (KHz)	Displacement	
				Min	Max
Accel.	AXDL345	10.3	3.8	-134.0	53.2
	MPU-6050	9.5	5.3	-80.0	80.0
	MPU-9250	4.2	20.6	-22.2	-4.3
Gyro.	L3G4200D	8	8.1	-105.1	105.3
	MPU-6050	3.2	26.86	-270.4	260.3
	MPU-9250	3.2	27.3	-232.6	247.1

Attacks Discovered

23 unique attacks across accelerometers and gyroscopes

- Each case had:
  - distinct **flight path**.
  - distinct **acoustic signal.**
- *19 cases* resulted in the RAV *crashing*.
- *4 cases* made the RAV suffer significant *deviation*.

Statefulness of Attacks

#	Attk. ID	Signal Injection		
		Amp.	Freq. (kHz)	Sensor Profile
1	A1	19.75-29.75	20	AXDL345
2	A2	19.25-29.50	16	AXDL345
3	A3	9.25-11.00	40	MPU-6050
4	A4	13.25-19.25	28	MPU-6050
5	A5	18.5-23.50	11.2	MPU-6050
6	A6	20.25-28.25	16	AXDL345
7	A7	10.00-26.75	40	MPU-6050
8	A8	17.50-19.50	24	MPU-6050
9	A9	4.25-8.50	52	AXDL345
10	A10	15.00-22.50	28	AXDL345
11	A11	2.75-8.00	44	AXDL345
12	A12	14.00-29.50	47.2	AXDL345
13	G1	13.50-30.00	35.4	MPU-6050
14	G2	7.25-30.00	48	L3G4200D
15	G3	9.00-29.00	48	MPU-6050
16	G4	7.25-30.00	40	L3G4200D
17	G5	20.25-29.75	23.8	L3G4200D
18	G6	11.00-17.00	6.4	MPU-9250
19	G7	27.25-29.75	15.8	MPU-9250
20	G8	22.50-28.75	47.8	MPU-6050
21	G9	17.50-29.75	23.9	MPU-9250
22	G10	22.25-30.00	8.3	MPU-6050
23	G11	17.00-18.50	29.8	MPU-9250

Statefulness of Attacks

Only **7 attacks** worked in **all flight scenarios.**

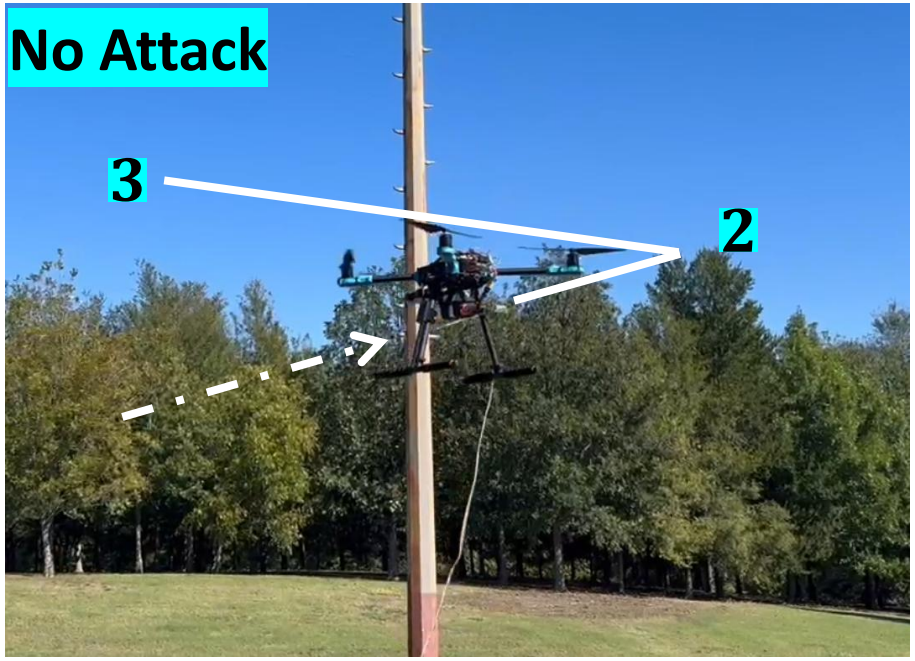
Other **16 attacks** required **specific physical states.**

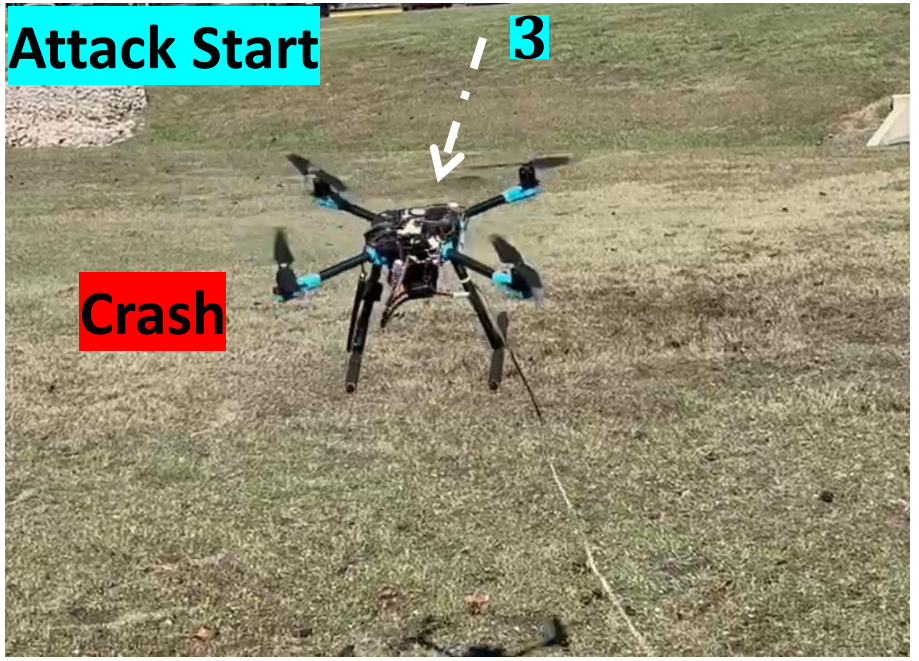
#	Attk. ID	Signal Injection		
		Amp.	Freq. (kHz)	Sensor Profile
1	A1	19.75-29.75	20	AXDL345
2	A2	19.25-29.50	16	AXDL345
3	A3	9.25-11.00	40	MPU-6050
4	A4	13.25-19.25	28	MPU-6050
5	A5	18.5-23.50	11.2	MPU-6050
6	A6	20.25-28.25	16	AXDL345
7	**A7**	**10.00-26.75**	**40**	**MPU-6050**
8	**A8**	**17.50-19.50**	**24**	**MPU-6050**
9	**A9**	**4.25-8.50**	**52**	**AXDL345**
10	**A10**	**15.00-22.50**	**28**	**AXDL345**
11	A11	2.75-8.00	44	AXDL345
12	A12	14.00-29.50	47.2	AXDL345
13	**G1**	**13.50-30.00**	**35.4**	**MPU-6050**
14	G2	7.25-30.00	48	L3G4200D
15	G3	9.00-29.00	48	MPU-6050
16	G4	7.25-30.00	40	L3G4200D
17	G5	20.25-29.75	23.8	L3G4200D
18	**G6**	**11.00-17.00**	**6.4**	**MPU-9250**
19	G7	27.25-29.75	15.8	MPU-9250
20	G8	22.50-28.75	47.8	MPU-6050
21	G9	17.50-29.75	23.9	MPU-9250
22	**G10**	**22.25-30.00**	**8.3**	**MPU-6050**
23	G11	17.00-18.50	29.8	MPU-9250

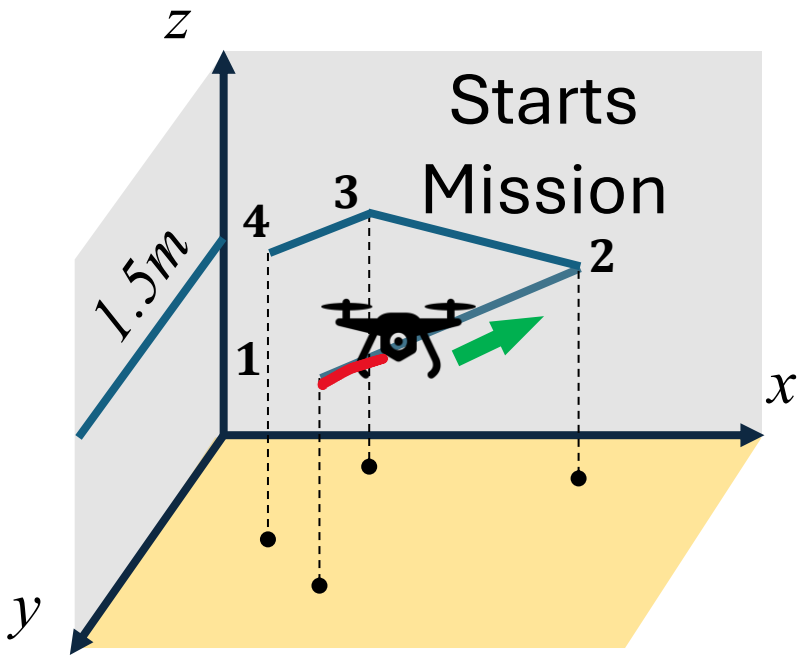
Real-world Experiments

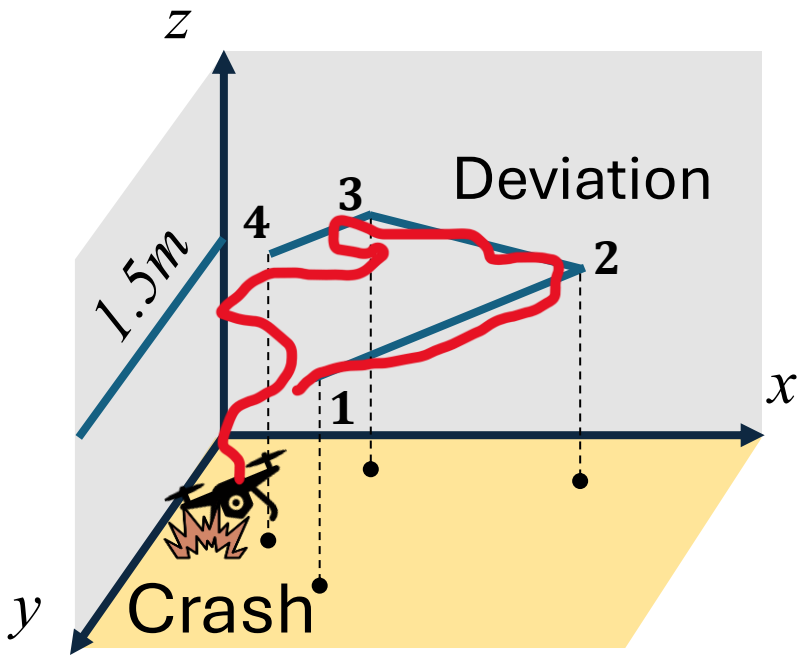
- Physical Experiments:
  - Pixhawk4 drone with Ardupilot v4.5.
  - Mission with varied physical states.

- Inject signal at **27.4 kHz** into an **ICM-20689 gyroscope**.


No Attack
3
2

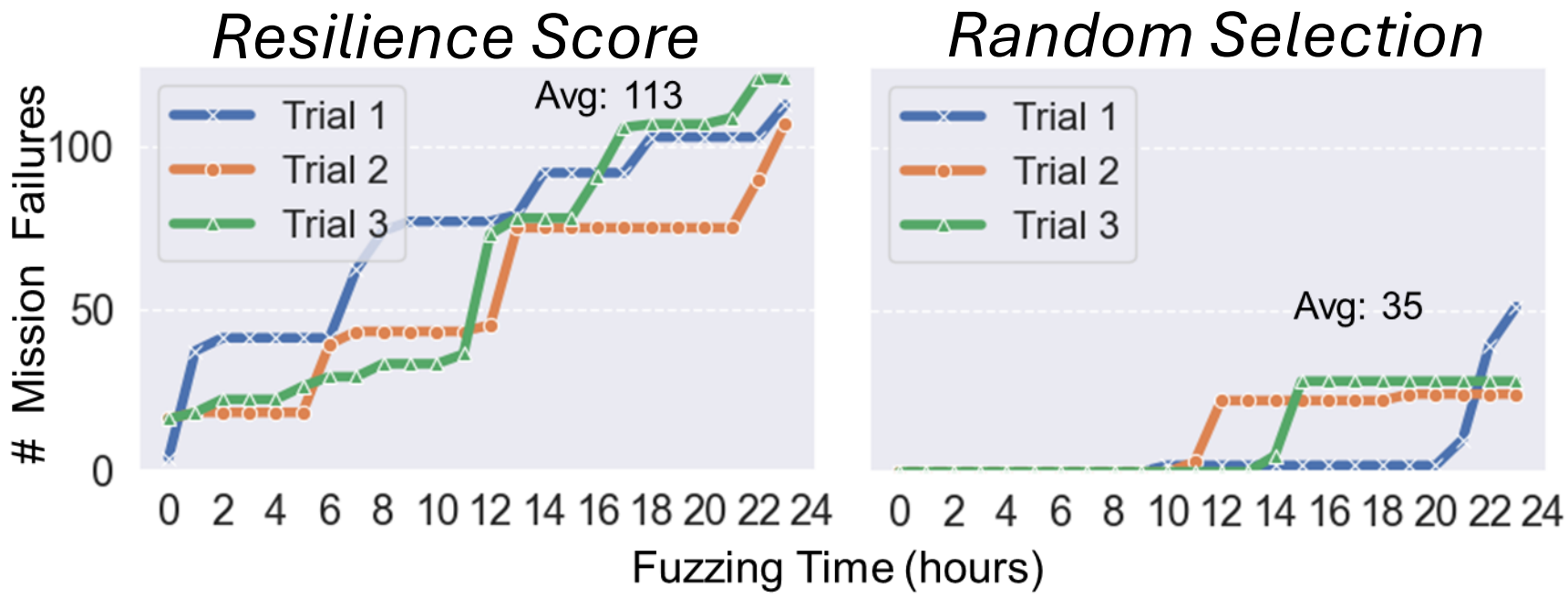

Attack Start
3
Crash


z
Starts
Mission
3
4
2
1.5m
1
x
y


z
Deviation
3
4
2
1.5m
1
x
y
Crash

Effectiveness of Resilience Feedback

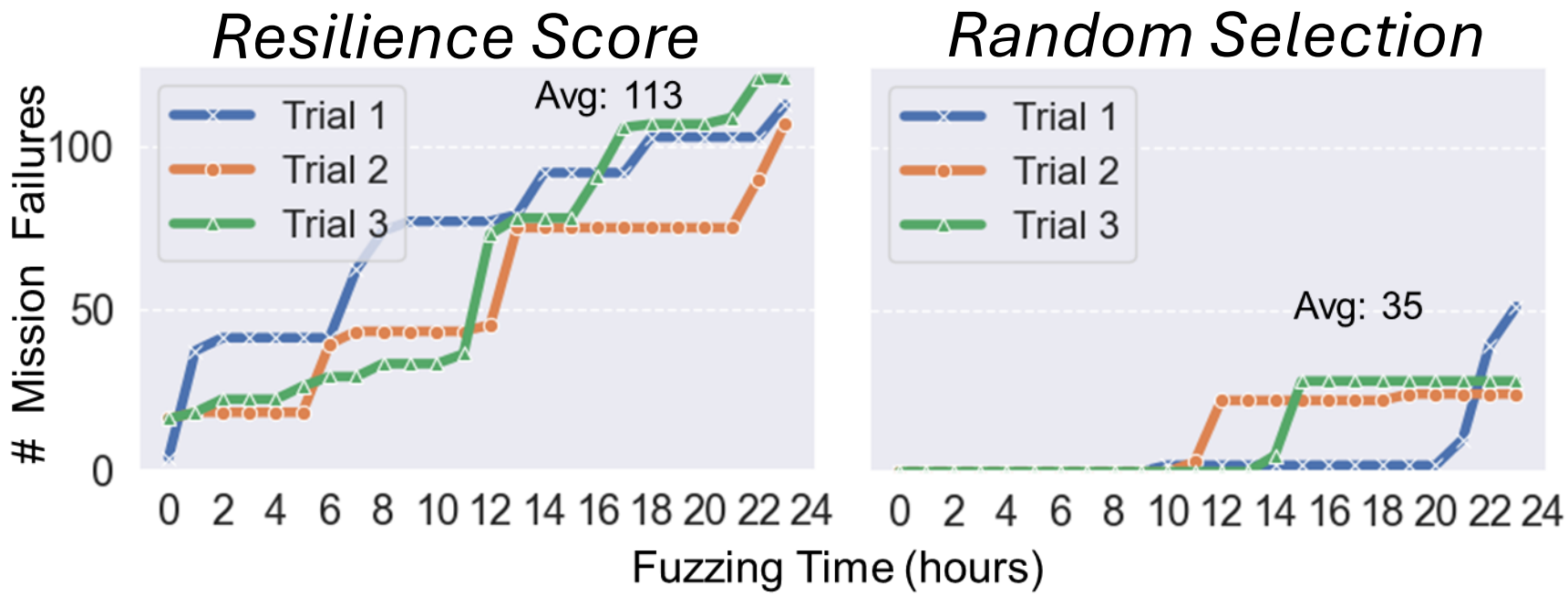
- Fuzzing with and without resilience score feedback.



Effectiveness of Resilience Feedback

- Fuzzing with and without resilience score feedback.

2.2x additional mission failures than randomized selection



IMUFUZZER Summary

- **Sensor fuzzing** framework to find acoustic injection attacks.
- **Acoustic signals** + **mission mutation** + **resilience feedback** for effective exploration.
- **23 unique attacks** with **6 real-world IMU profiles**.
- We **open-sourced** our code, data and videos.

IMUFUZZER Summary

- **Sensor fuzzing** framework to find acoustic injection attacks.
- **Acoustic signals** + **mission mutation** + **resilience feedback** for effective exploration.
- **23 unique attacks** with **6 real-world IMU profiles**.
- We **open-sourced** our code, data and videos.

Join us at the poster session!

Q&A

Contact: **Sudharssan Mohan**

sudharssan.mohan@utdallas.edu