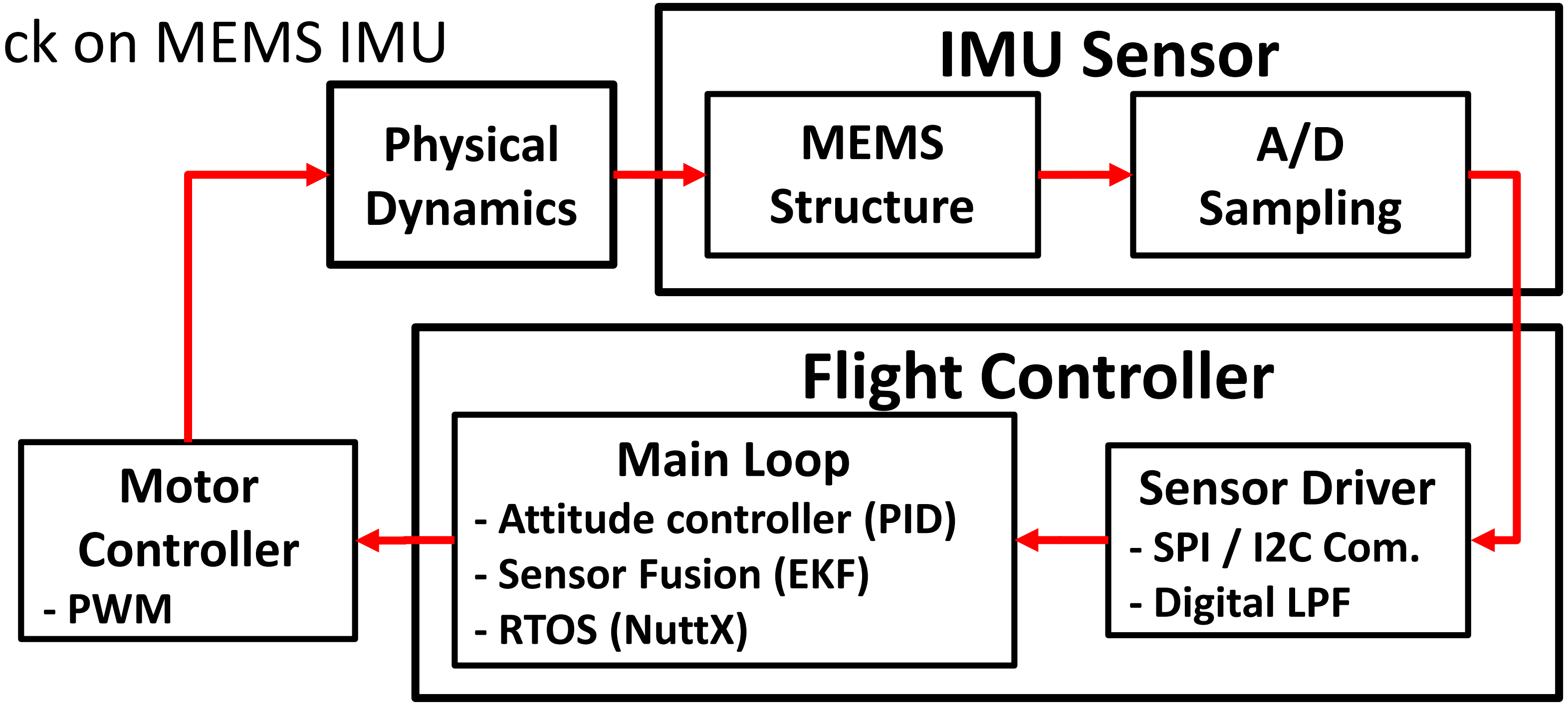
Un-Rocking Drones: Foundations of Acoustic Injection Attacks and Recovery Thereof

Jinseob Jeong*, Dongkwan Kim, Joonha Jang, Juhwan Noh, Changhun Song, and Yongdae Kim

KAIST Syssec

Drone System

- Sensing and actuation, safety critical system
  - Sensor values are propagated to the actuator.
  - Failure of the drone causes safety issues.
- Rocking Drone [Son'15]
  - Acoustic injection attack on MEMS IMU



Rocking Drone [Usenix Sec’15]

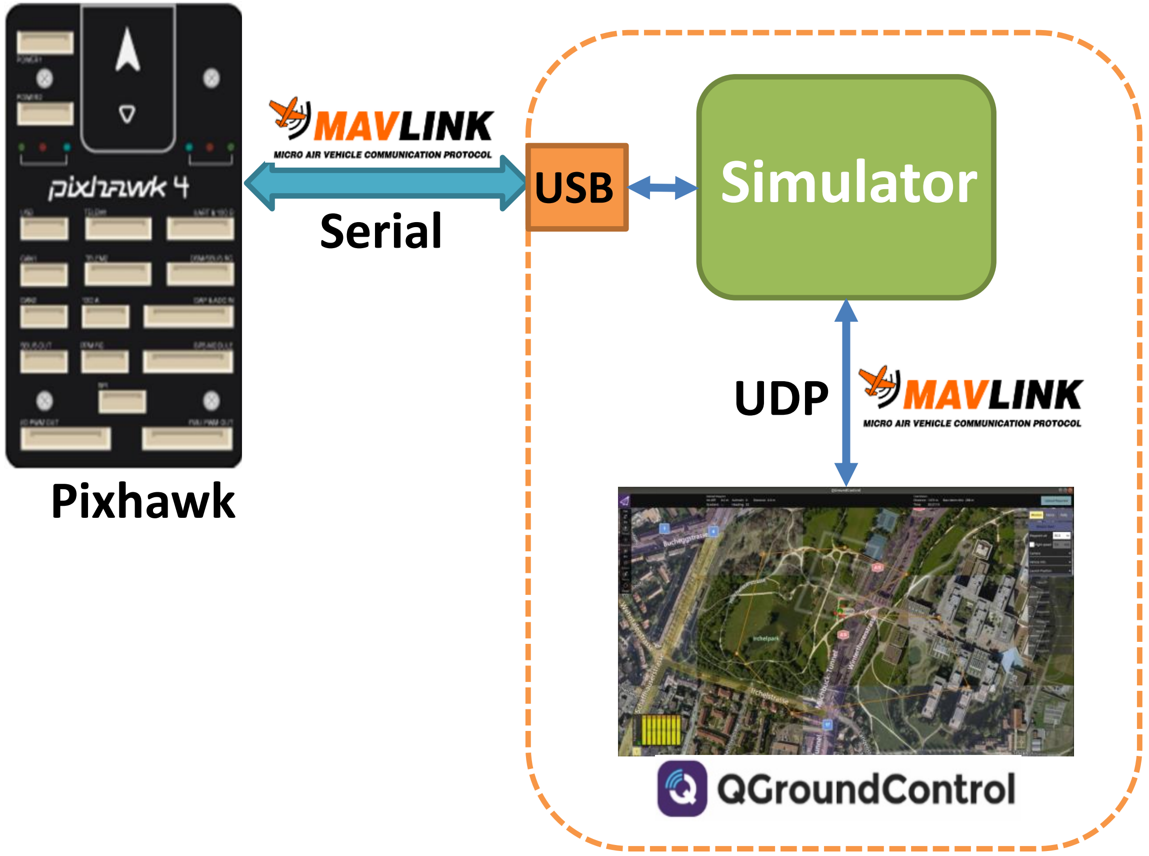
Rocking Drone with SITL

*SITL : Software-In-The-Loop

Acoustic Injection Testbed

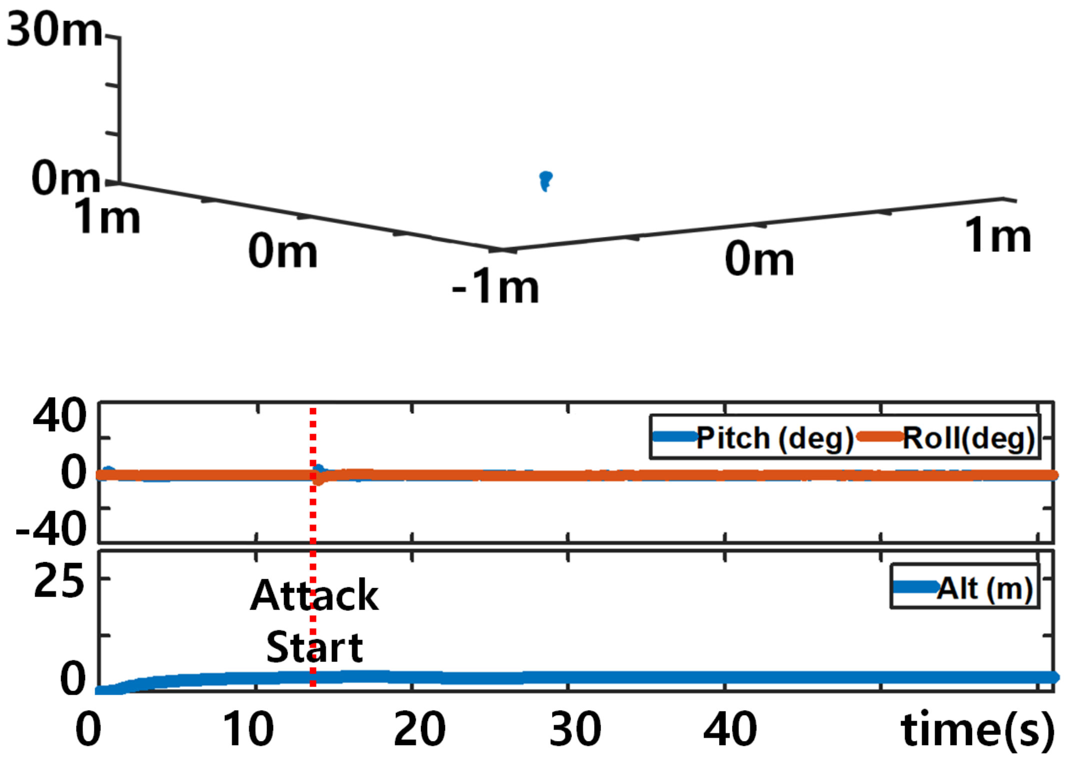
- Test modes
  - Software-In-The-Loop (SITL)
  - Hardware-In-The-Loop (HITL)
  - Real drone test

HITL configuration

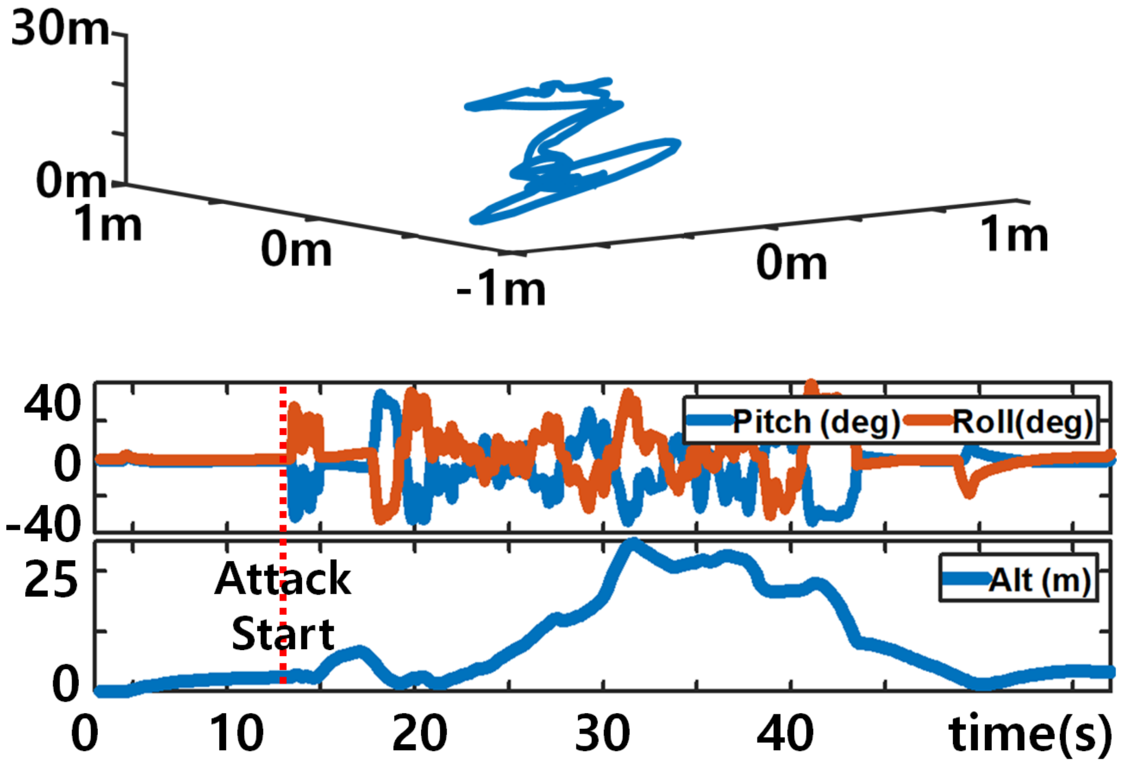


Host Computer

SITL and HITL Experiments

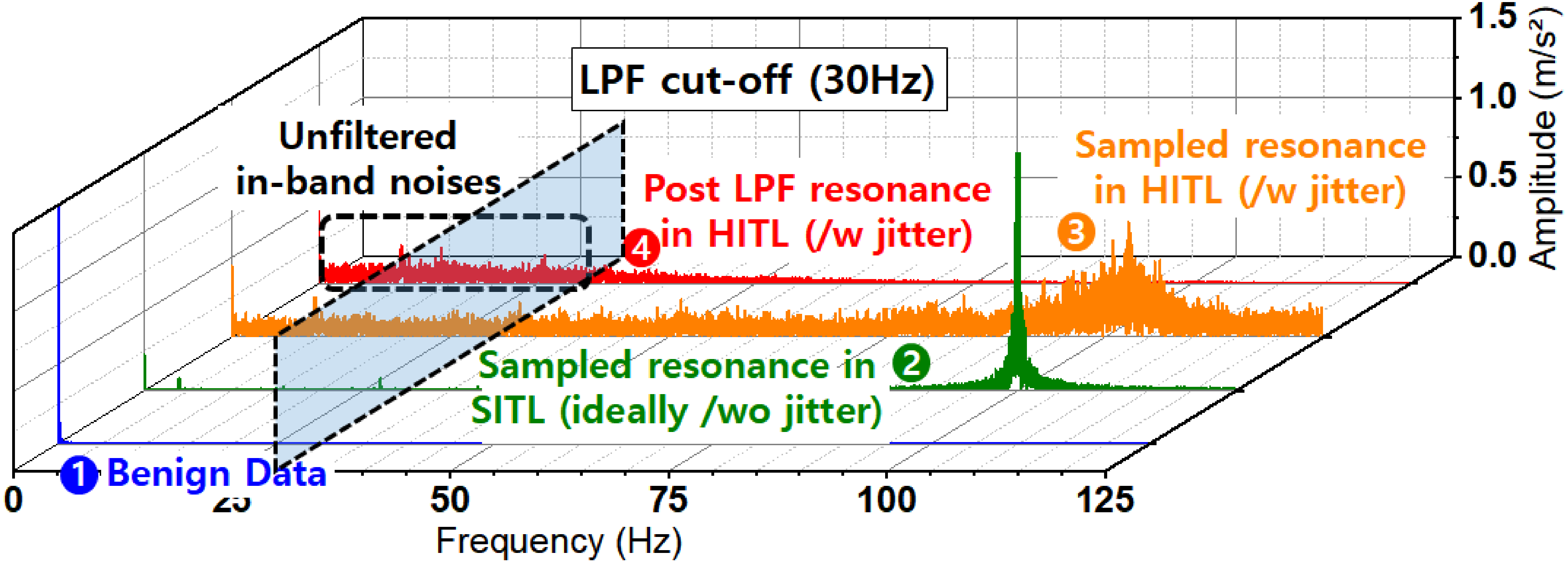


SITL



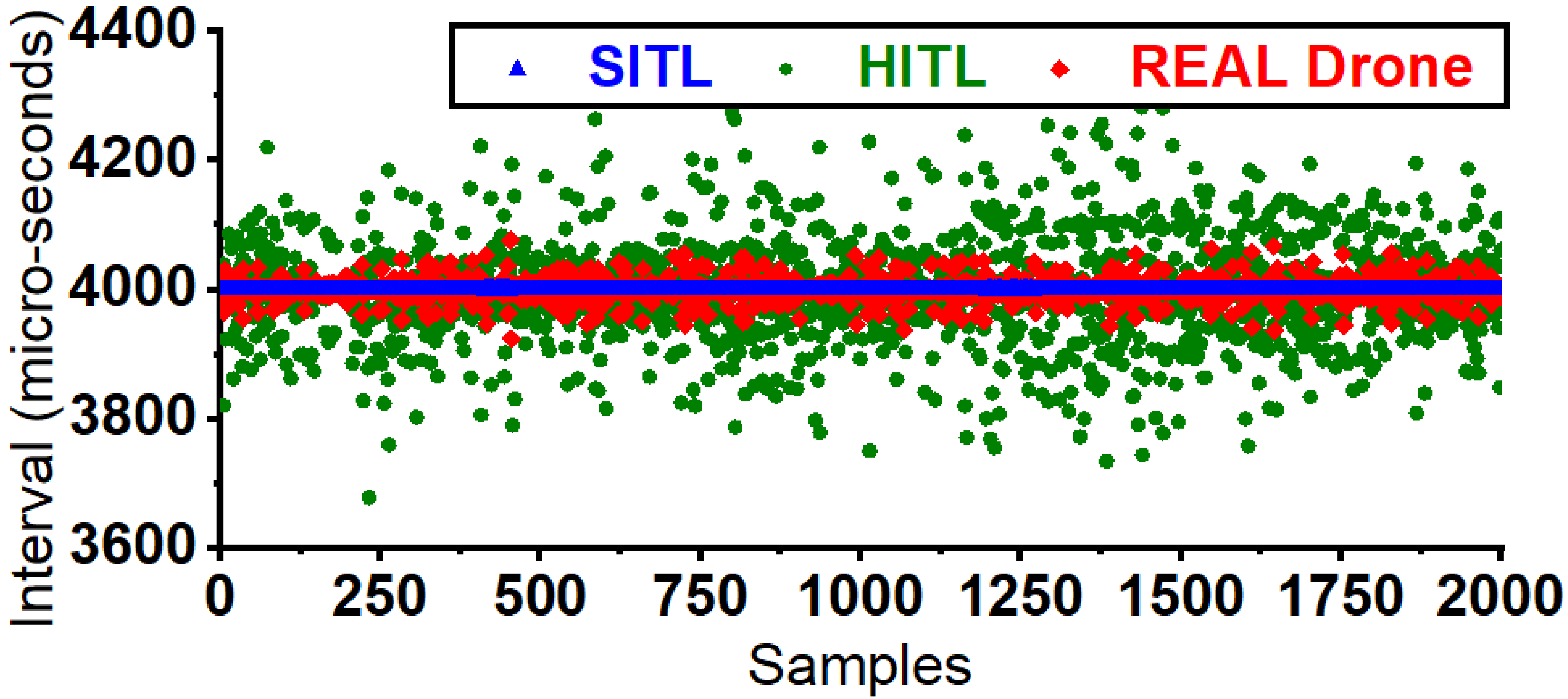
HITL

SITL/HITL Frequency Domain Analysis



SYSSEC KAIST

Sampling Jitter as a Critical Factor



❖ Sampling jitter exists due to hardware imperfection.
  – Even with sampling jitters, drone fly normally in benign cases.

Effects of Sampling Jitter in Drones (SITL/HITL)

SYSSEC KAIST

UnRocker
IMU Sensor Recovery

Possible Mitigations

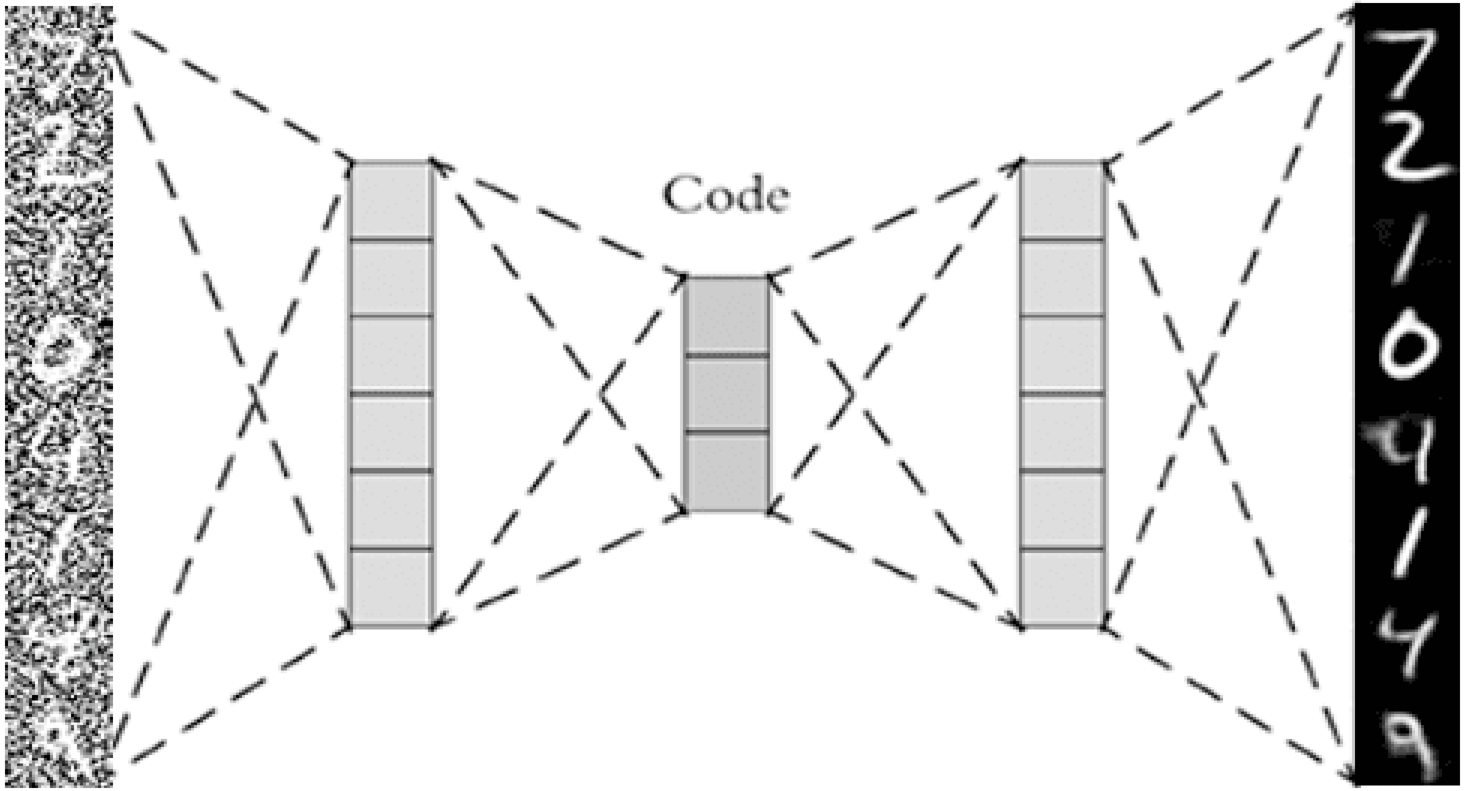
- Simple filtering approaches
  - Mechanical shielding [Son’15] ➔ Heating problem
  - Circuit parameter changing [Son’15] ➔ Unintended resonance
  - Sampling randomization [Trippel’17] ➔ Increased DoS effect

- State estimation based attack detection [Choi‘18, Quinonez’20]
  ➔ Only detection without recovery

- Partial gyro sensor value recovery from accelerometer [Choi ’20]
  - They can recover the gyroscope for only a few seconds.

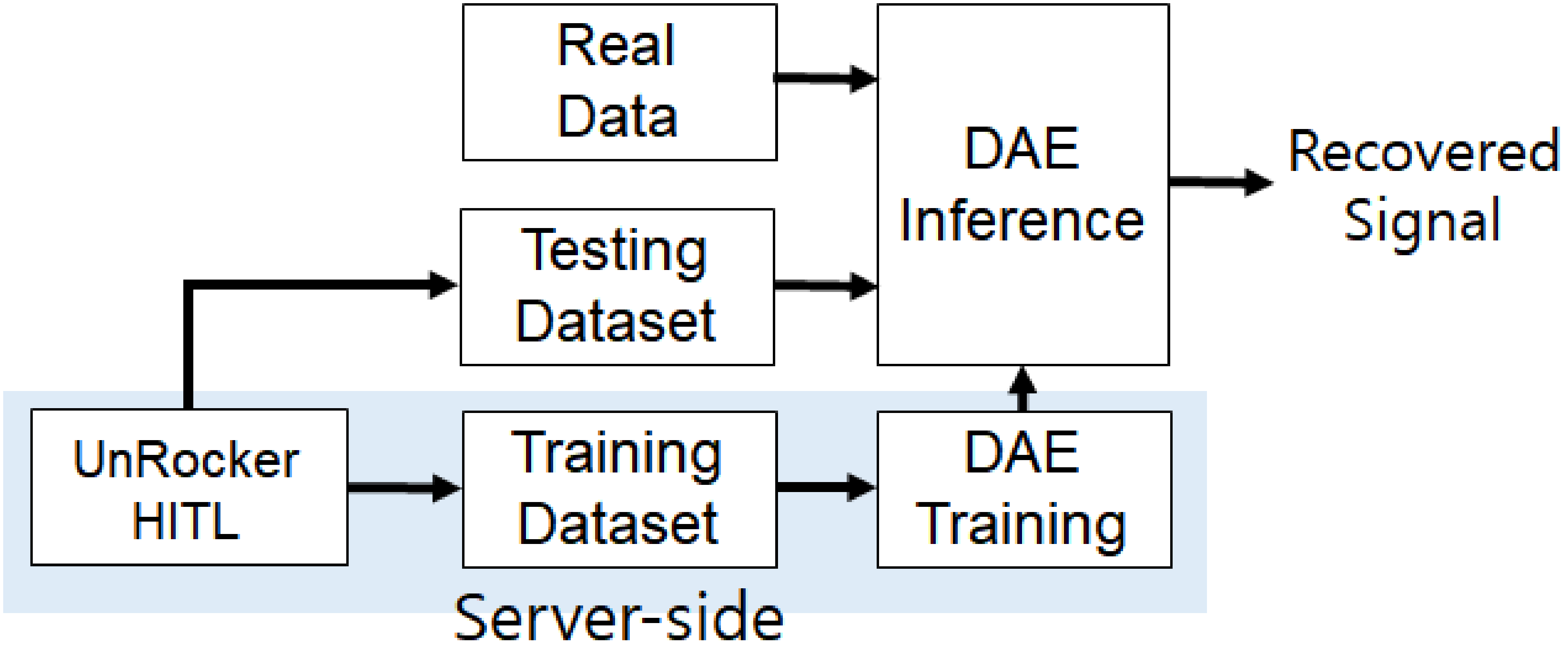
Main idea: Denoising Autoencoder (DAE)

- DAE is has been used for noise reduction applications.
  - Medical imaging, industrial process, Radar, …
  - 1-D CNN DAE



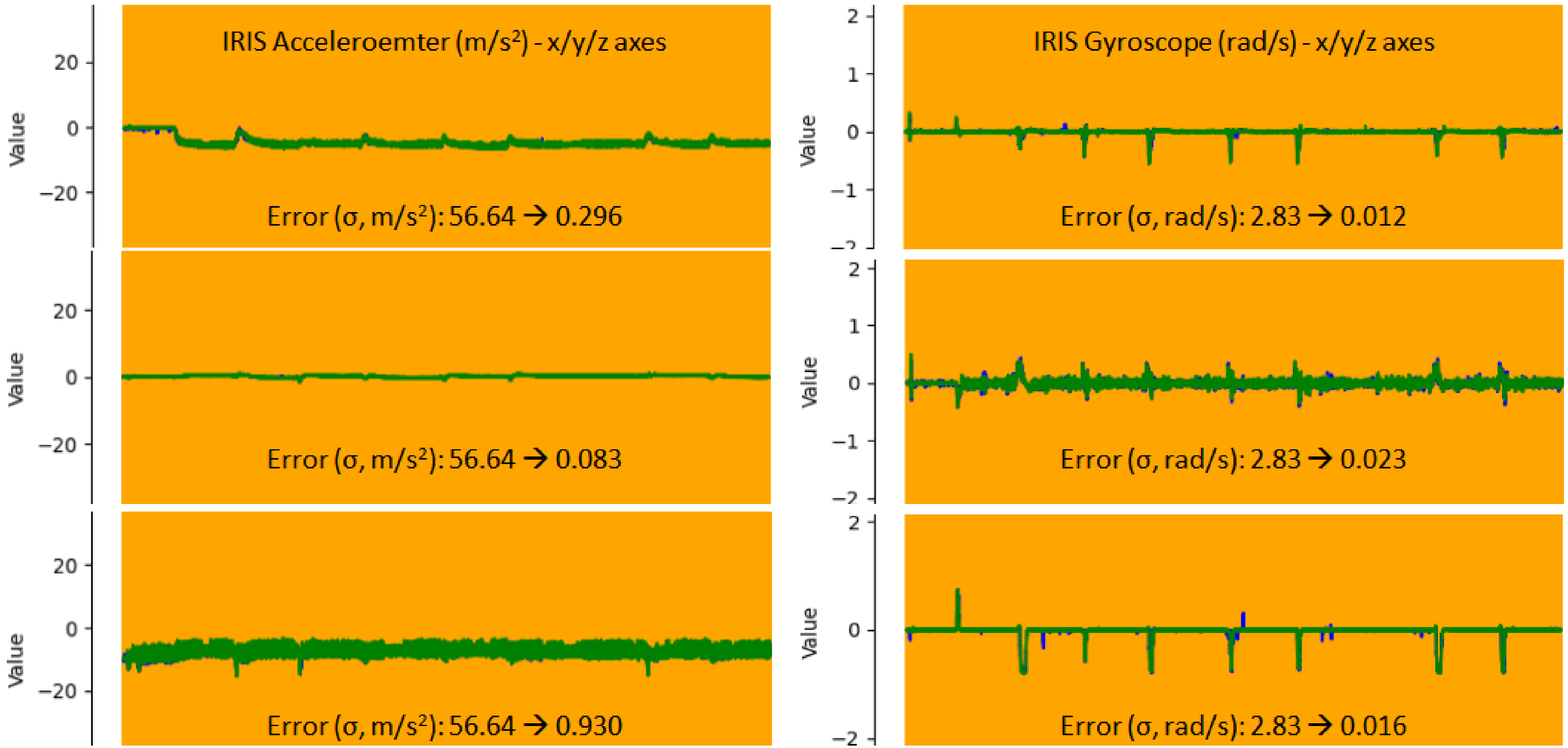
SYSSEC KAIST

UnRocker for IMU Sensor Recovery



UnRocker Evaluation with Testing Dataset

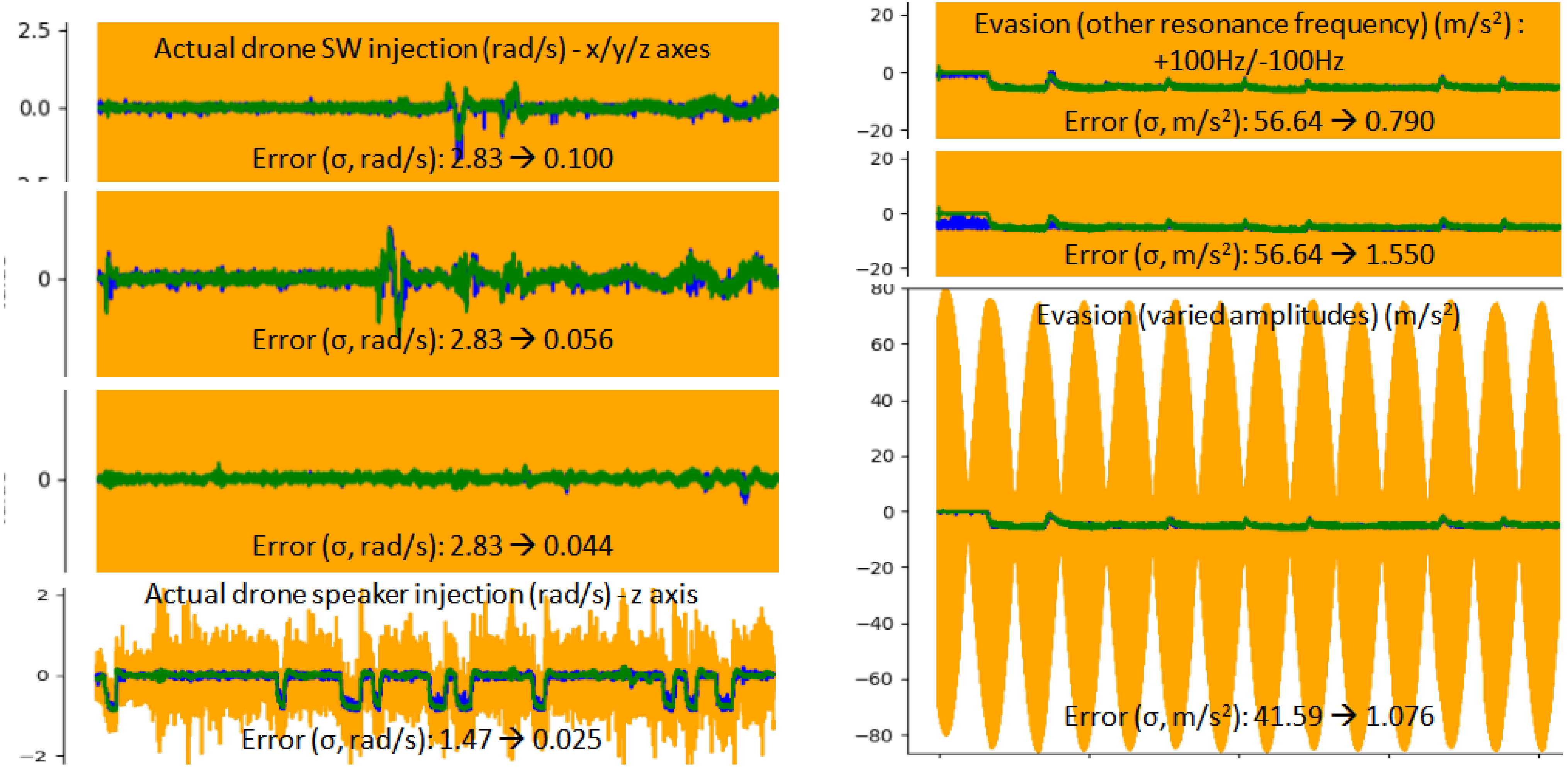
❖ Recovery Results (orange: compromised, blue: recovered, green: benign)



SYSSEC KAIST

UnRocker Evaluation with Other Datasets

❖ Domain Adaptation (orange: compromised, blue: recovered, green: benign)



Conclusion

- “**Rocking Drone**” was crashed not only because of the “resonation of the gyroscope”, but also because of the “**sampling jitter**.”
- **UnRocker**: a novel DAE based sensor recovery approach.
- Open-sourced: https://github.com/jinseobjeong/UnRocker

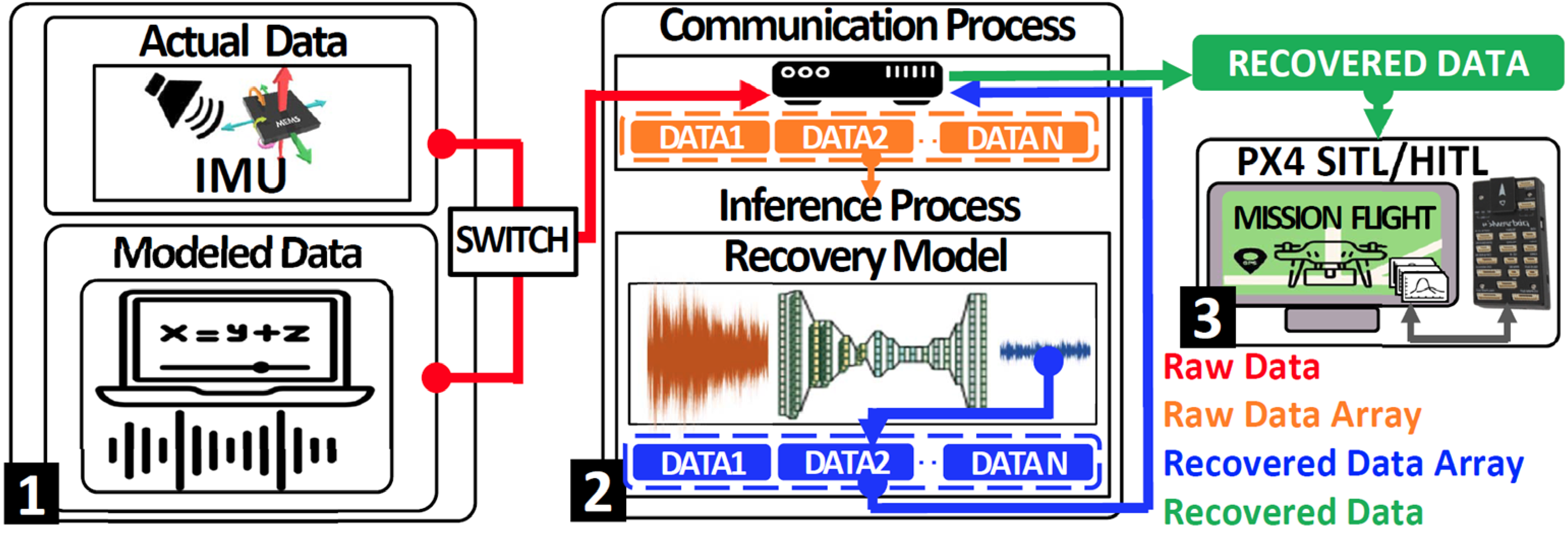
Thank You

Please contact

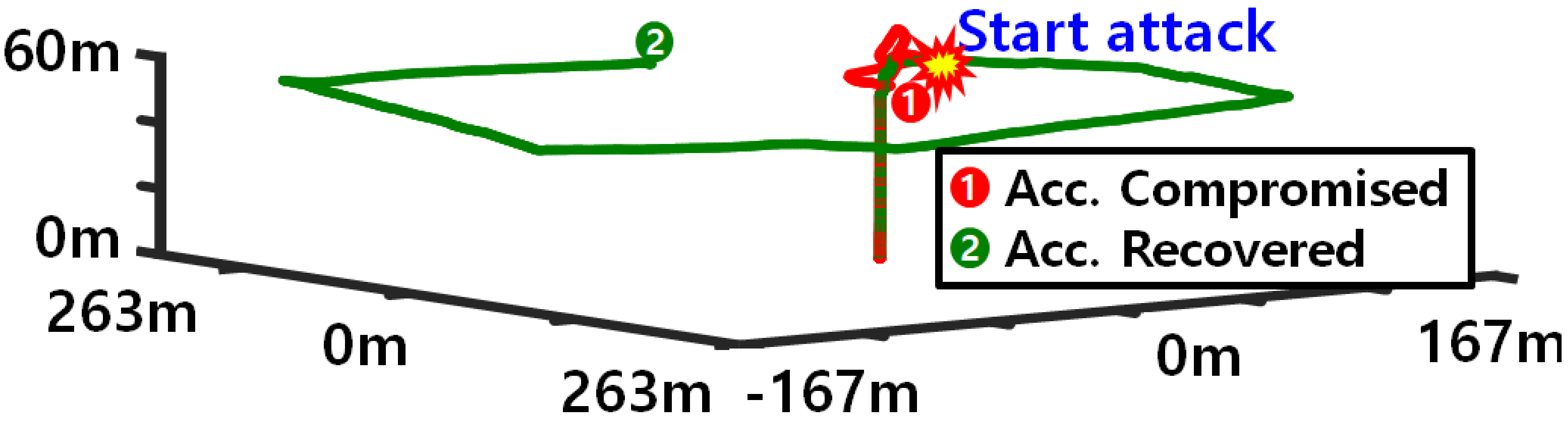
Jinseob Jeong (jeongjin-sub@kaist.ac.kr)

If you have any comments

Towards Real-Time Recovery

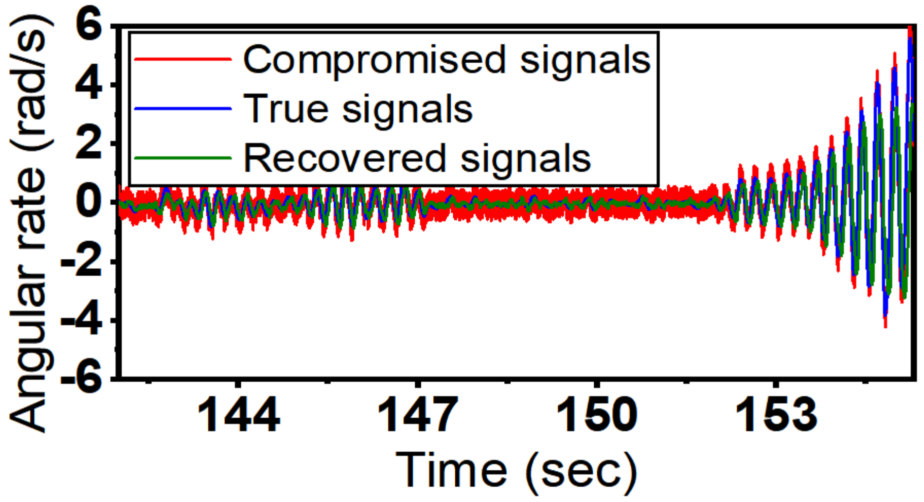


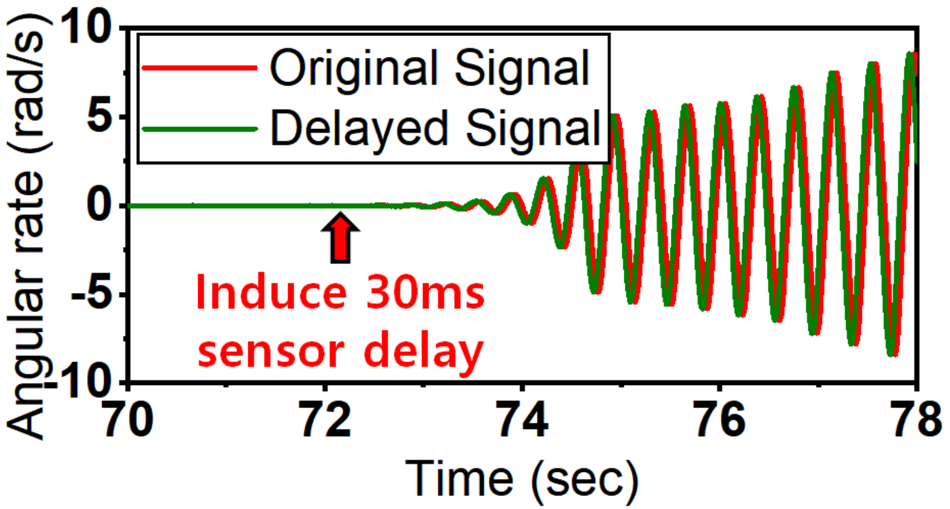
Real-Time Recovery

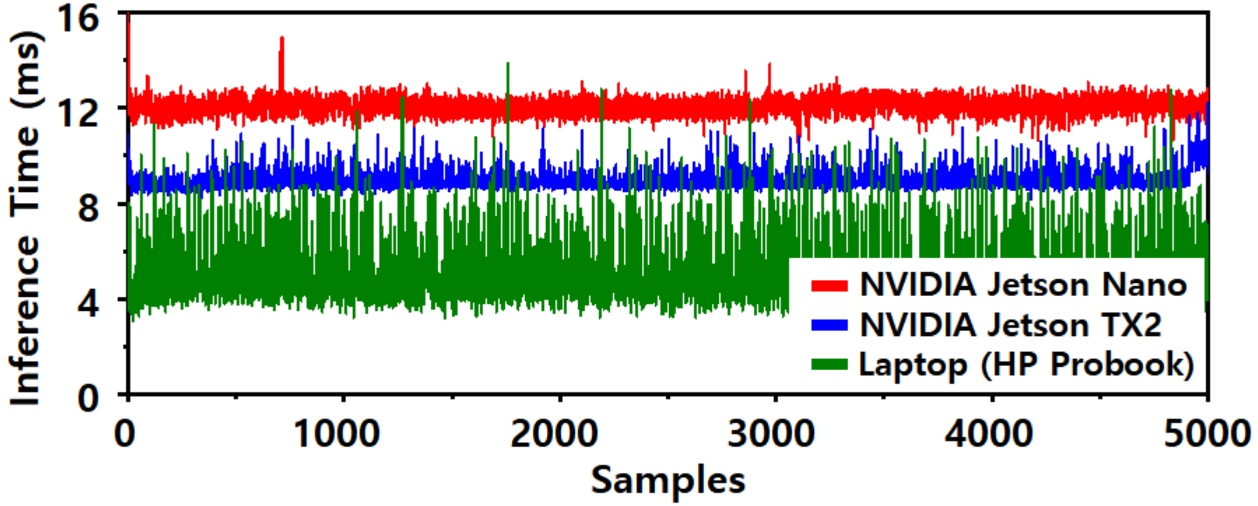


SYSSEC KAIST

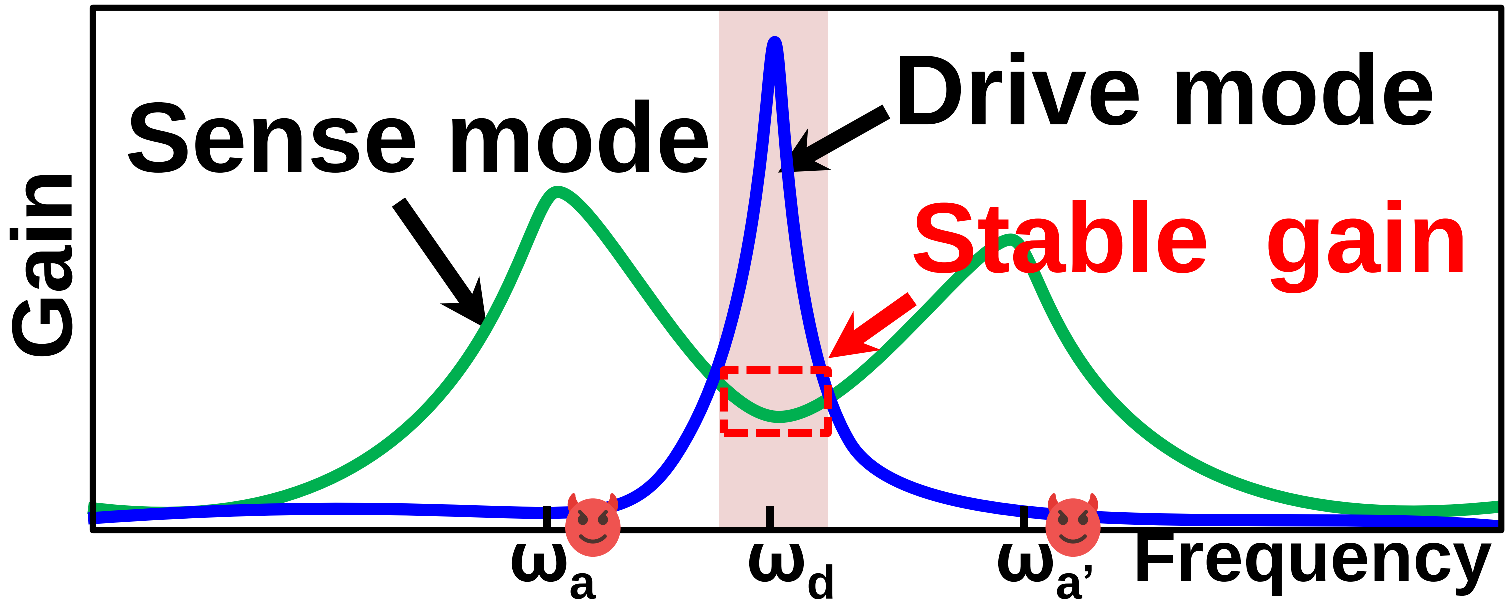
Real-Time Recovery

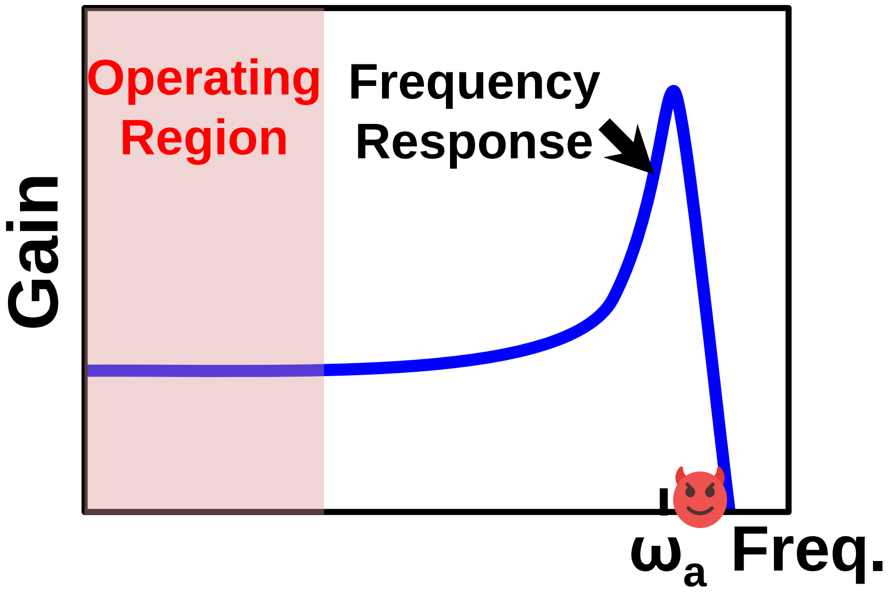






Mechanical Gain and the Threat Model





- ❖ MEMS IMUs have peak response outside the operating region.
- ❖ We assume a strong attacker that targets the peak response to maximize the implication of the attack.

Modeling of the Resonating MEMS signals

- Modeling of Resonating MEMS Accelerometer
  - 『 $\hat{s}_{acc}(t) = s_{acc}(t) + A_e \cdot \cos(2\pi F_{ac}\, t+\Phi)$ 』 (Previously modeled by Trippel et. al. in EuroS&P '17)
  - The false signal is directly related to the injected acoustic frequency.
- Modeling of Resonating MEMS Gyroscope
  - The impact of acoustic injection is decomposed into 2-orthogonal directions.
  - The potential output signal of compromised MEMS gyroscope signal is

$$\hat{\Omega}(t) = \Omega(t) + \Omega(t)\left(\frac{A_d}{S} cos\left(2\pi(f_{ac} - f_d)t + \phi\right)\right) + \left(\frac{A_s}{S} cos\left(2\pi(f_{ac} - f_d)t + \phi\prime\right)\right)$$

False angular rate from acoustic induced dr iving direction (negligible)

False angular rate from acoustic induced s ensing direction

  - Then the relative gain of driving directional to the sensing directional impact is

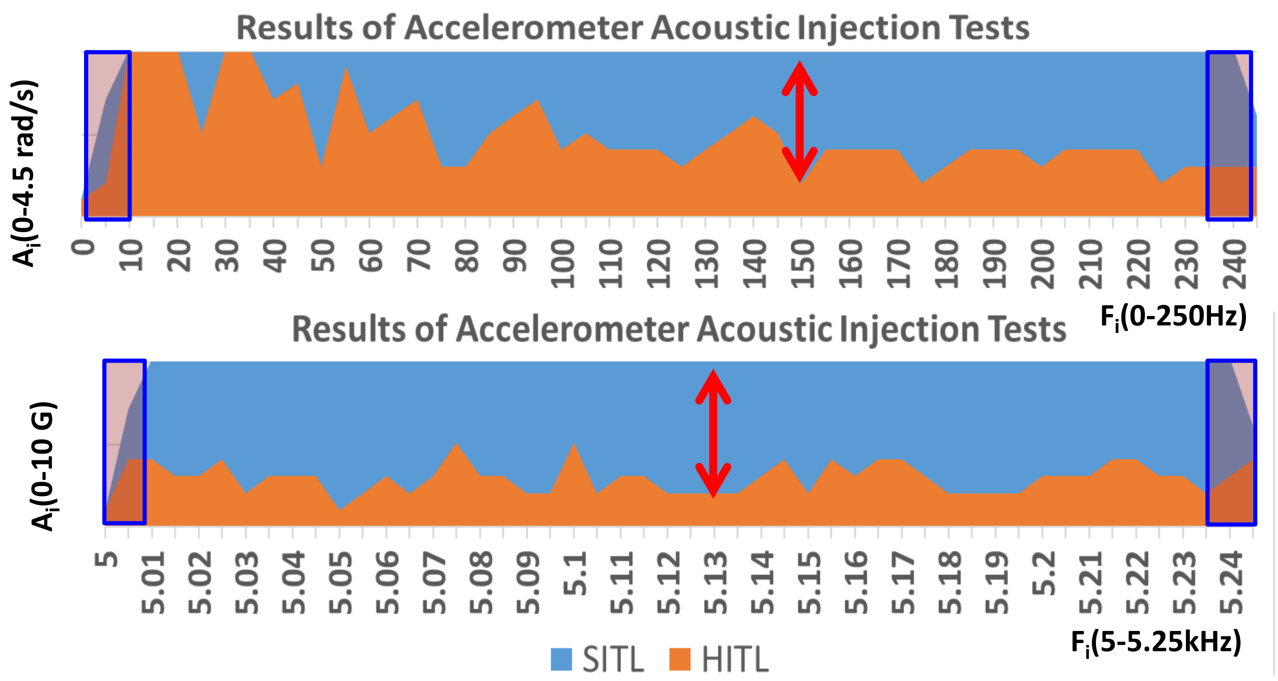
$$G_{rel} = \frac{A_d \cdot \Omega}{A_s} = \frac{4\pi \cdot m \cdot f_{ac} \cdot x_d \cdot \Omega}{k_s \cdot x_s} = 3.3 \times 10^{-5} \approx 0$$

  - In short, $\hat{\Omega}_{gyro}(t) \approx \Omega_{gyro}(t) + A_i \cdot cos(2\pi F_i t + \phi)\left(A_i = \frac{A_s}{S}, F_i = |f_{ac} - f_d|\right)$

SYSSEC KAIST

Acoustic Injection Tests with our Testbed

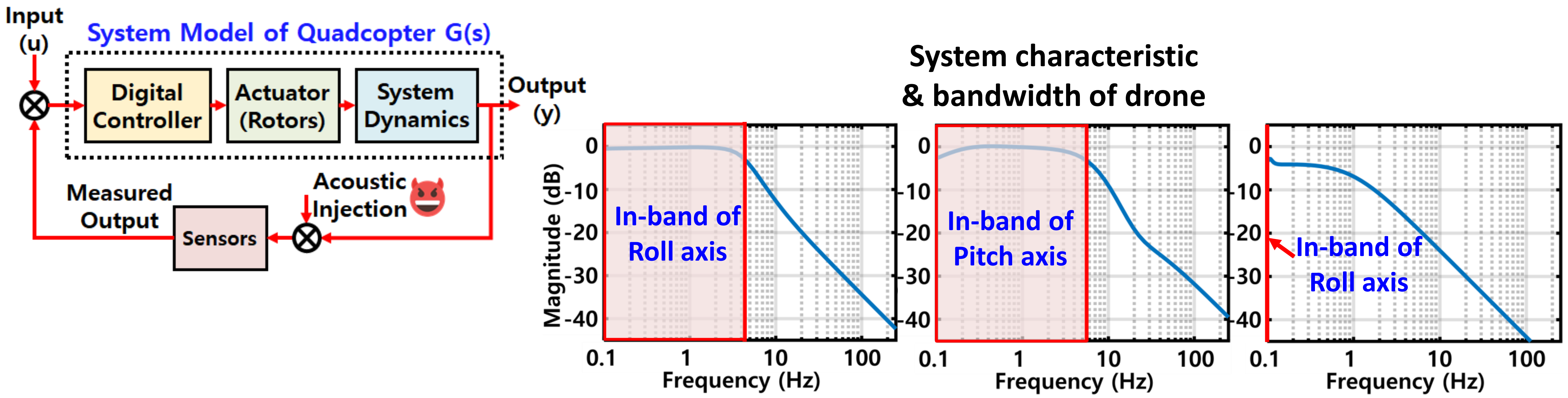
- Acoustic injection for several frequencies and amplitudes
  - SITL tests show the robustness of control logic. (Except for in-band frequencies (0-5Hz))
  - There are gaps between the SITL and HITL tests, which means that certain practical hardware operations breach the inherent resilience.



*Drone succeeded its flight in colored region

Inherent Robustness of the Drone

- Resonance signal is high-frequency.
  - It is sampled, filtered, and then it affects the drone system.

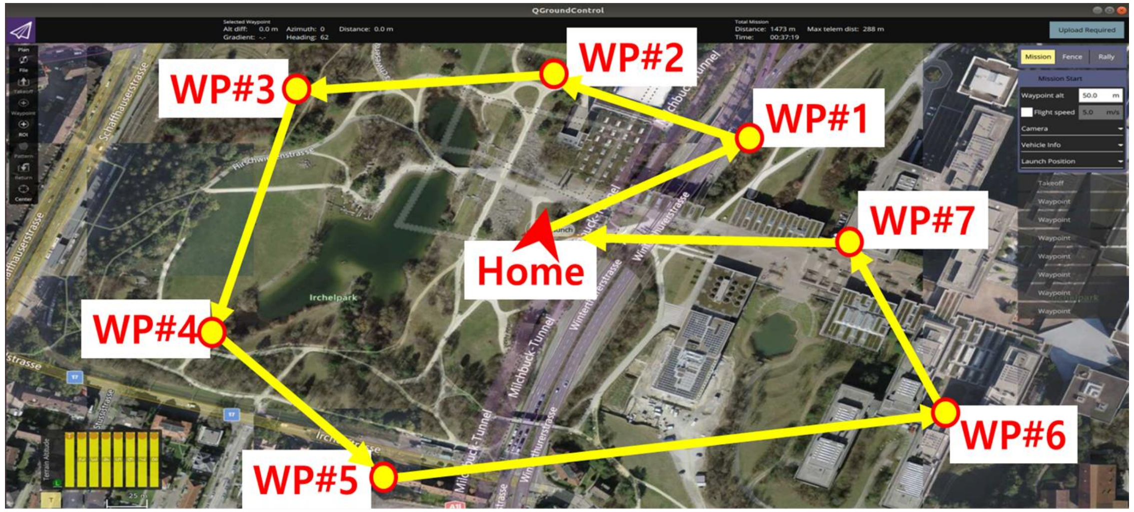


- The robust control logic can prevent drone crashes in ideal (SITL) experiments
  - Basically, low-pass filter (LPF) removes high frequency signals.
  - The bandwidth of the drone system was 4.32, 5.37, and 0.005Hz (roll/pitch/yaw).
  - The narrow 'in-band' frequency leads to no response to the 'out-band' signals.

Implementation and Dataset Collection

- Implementation of UnRocker
  - DAE model, Dataset Generator, Model Training and Online Inference

- Dataset Collection
  - Gyroscope: Induced frequency F_i = 206Hz, A_i = 0, 1, 2, 3, 4 rad/s
  - Accelerometer: Induced frequency F_i = 1.83kHz, A_i = 0, 20, 40, 60, 80 m/s^2
  - Mission summary : 7 waypoints, 1330m distance, 25~100m altitudes, 6 min flight time
  - Etc : 2 drones (Iris, Solo), 4:1:1 (train/val/test)
  - Total dataset : 32.4M pairs (2-drones × 2-sensors × 3-axes × 5-amps × 6-times × 6-min × 250-Hz)

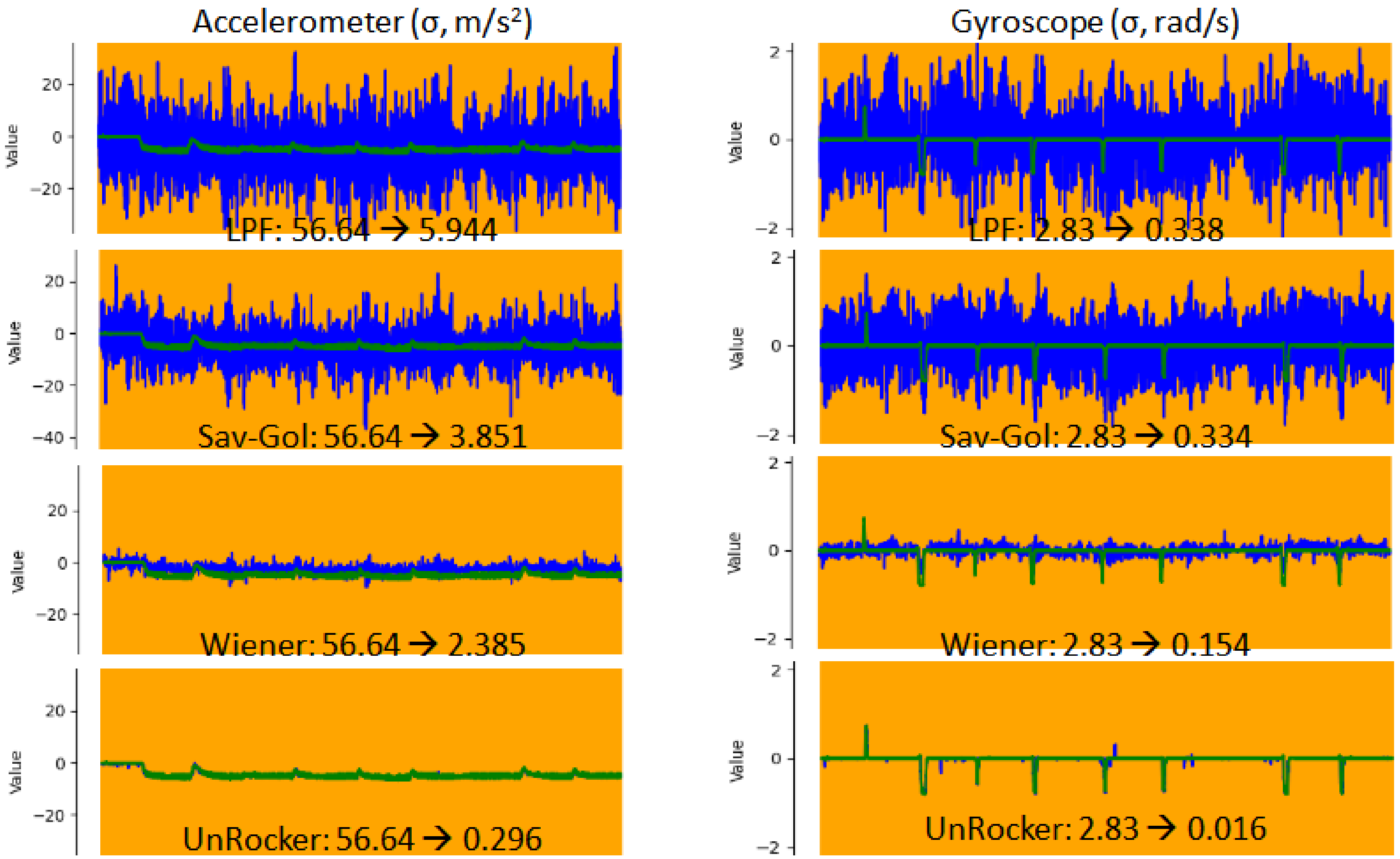


< Sample mission in our experiments >

SYSSEC KAIST

Limitations of Existing Heuristic Filters

❖ Heuristic filters failed to mitigate acoustic injection attacks.



Mitigating Acoustic Attack Using Savzitky-Golay Filter for Gyroscope

SYSSEC KAIST

Acoustic Injection Attack Examples