



Dropping Drones from the Sky: Requirements, Pros and Cons

Yongdae Kim

SysSec@KAIST

joint work with many of my students and collaborators



Drones in Ukraine War

Chinese drone firm DJI pauses operations in Russia and Ukraine 04/2022

DJI ADMITS DRONE AEROSCOPE SIGNALS ARE NOT ACTUALLY ENCRYPTED 05/2022

Ukrainians Say Russia is Still Tracking Their Drones with DJI AeroScope 05/2022

🕒 MAY 13, 2022 👤 JARON SCHNEIDER

Drone Wars: Ukraine's Homegrown Response To 'Deadly' Chinese Detection Tech

July 14, 2022 11:35 GMT

07/2022

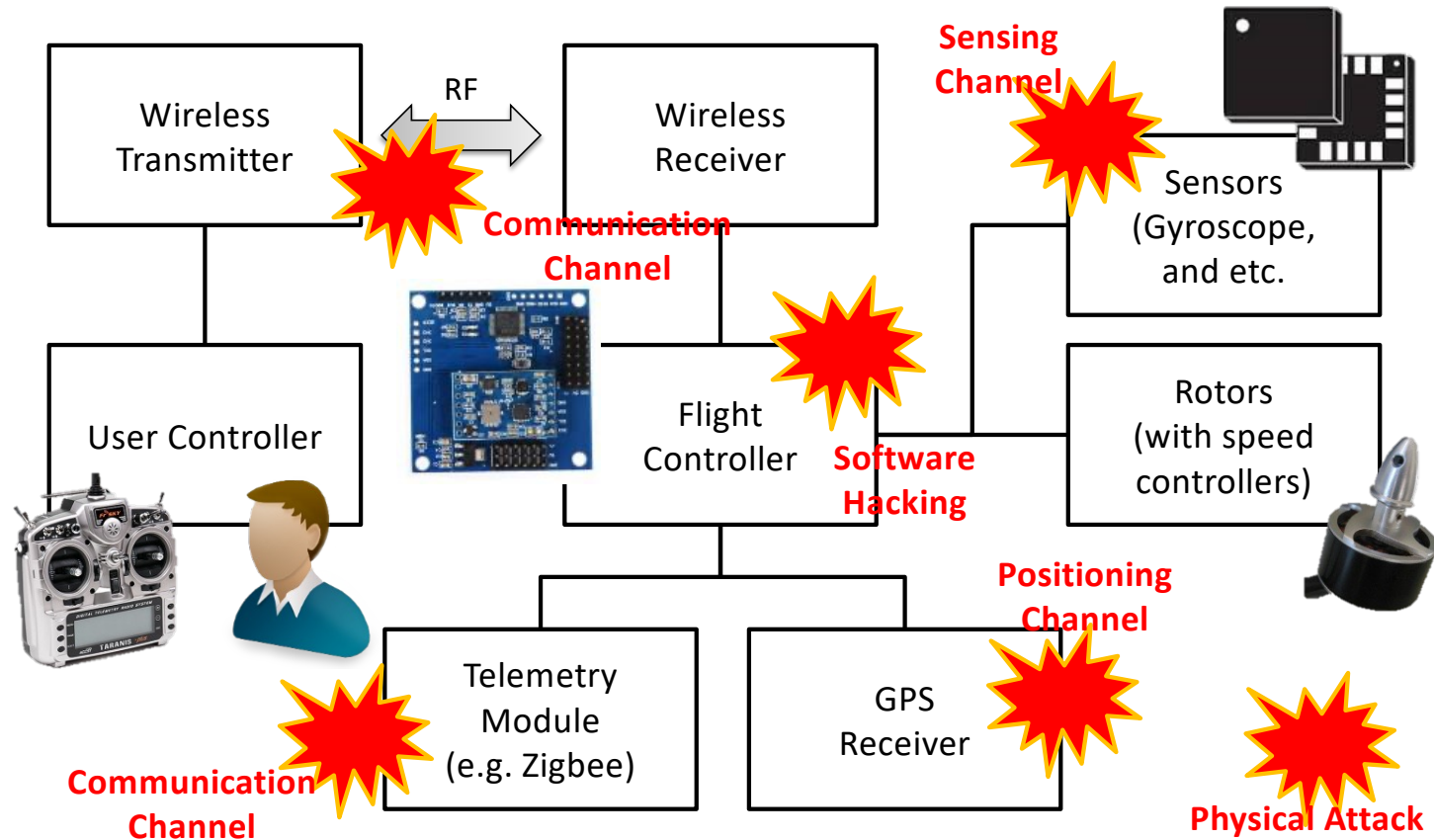
Ukraine's anti-drone gun brings down Russian DJI Mavic Pro UAV

Ishveena Singh - Oct. 6th 2022 2:04 am PT 🐦 @IshveenaSingh

DJI RUSSIA UKRAINE

10/2022

Drone Systems and Attack Vectors



Requirements for Anti-Drone

Low
Power

Long
Distance

Accuracy

Hard to
Bypass

Direction
Control

Minimize
Collateral
Damage

Near Zero
Response
Time

Handling
Swarming
Drones

Drone Neutralization Technologies

Type	Technology	Strength	Weakness	Response Time
Physical	Machine Gun	Cost	Accuracy, Collateral damage	≈ 0
	Net, Colliding Drone	Cost	Accuracy, Reload	<10 sec
	Sound	Swarm attack	Distance, Power, Bypass, Aiming	<10 sec
	High-power laser	Accuracy, Distance	Response time, Cost, Swarm	>10 sec
Electro-magnetic	RF jamming	Cost, Distance	Collateral damage, Response time, Bypass	>10 sec
	GNSS jamming	Cost, Distance	Collateral damage, Response time, Bypass	>10 sec
	High-power EM	Swarm, Distance	Cost, Collateral damage	≈ 0
	Targeted EM	Power, Swarm, Distance	Cost	≈ 0
Hijacking	GNSS spoofing	Hijacking, Distance	Collateral damage, Response time	<10 sec
	Software hijacking	Cost	Need vulnerability	

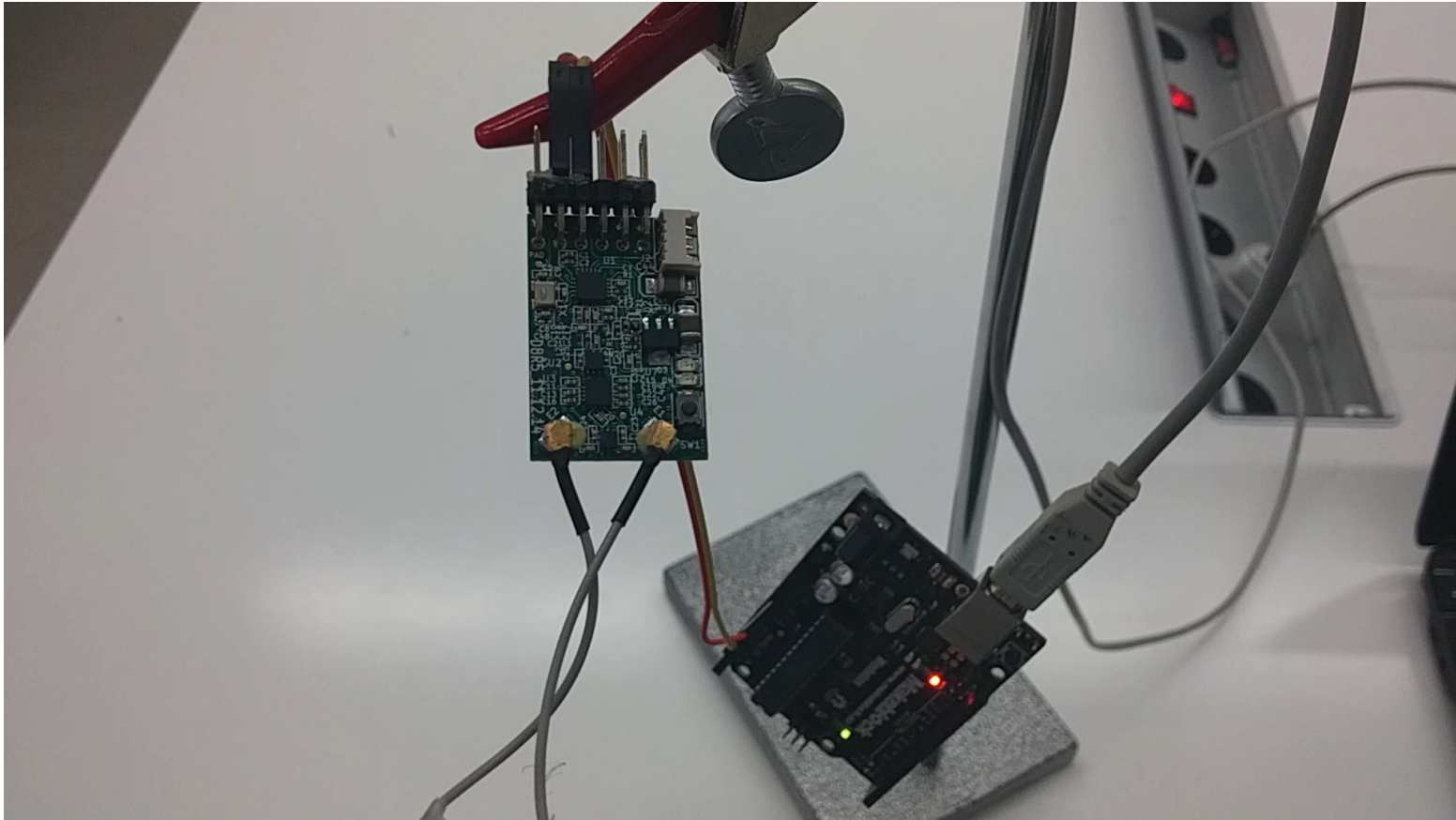
Communication

Drone Controller

- ❖ Just a RC controller
- ❖ Frequency: 2.4GHz
- ❖ Modulation: FHSS (Freq. Hopping Spread Spectrum)
 - Channel rapidly switches pseudo-randomly



Reactive jamming test



Positioning Channel

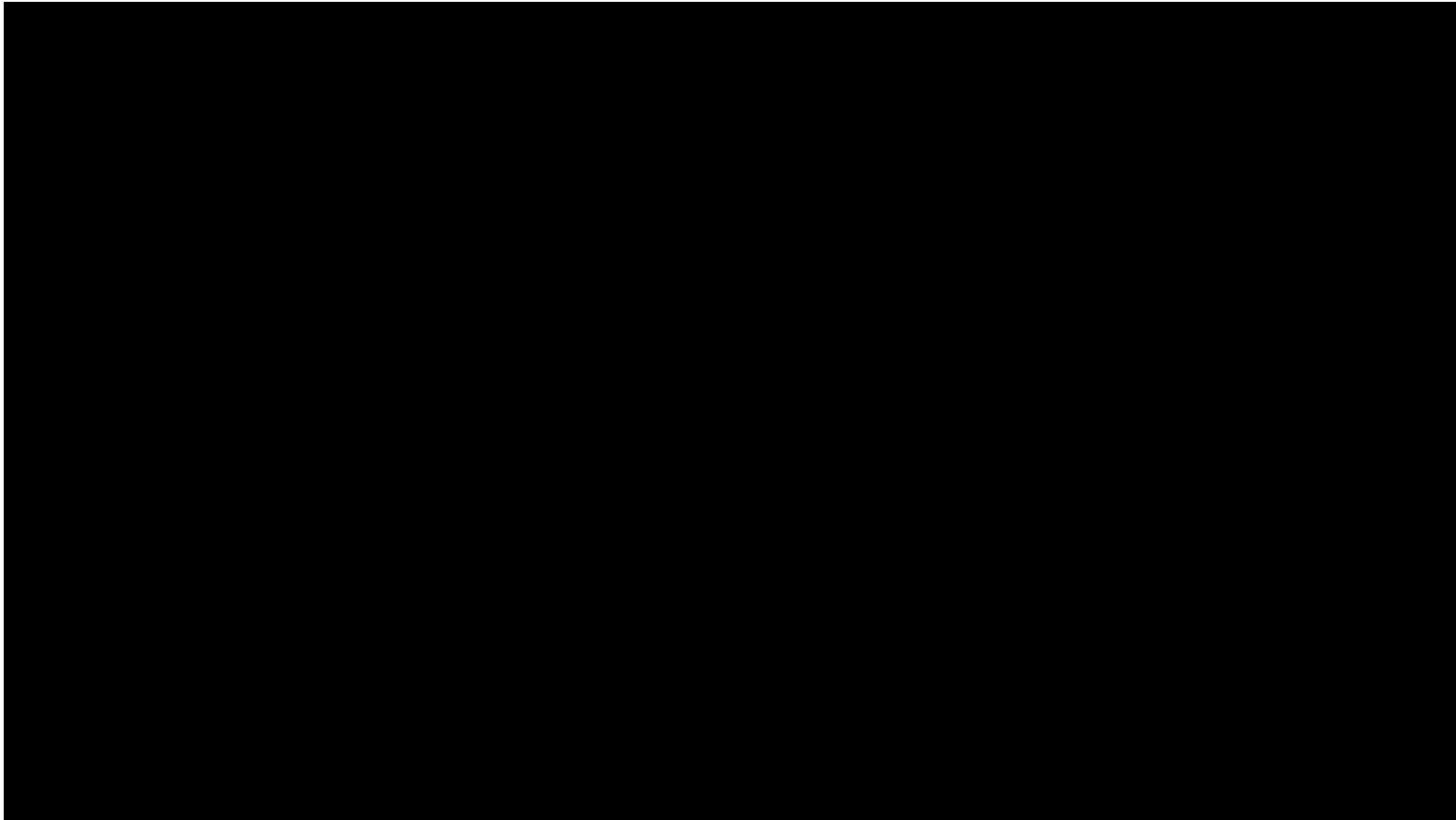
GNSS (GPS) Spoofing and Jamming

- ❖ No authentication and encryption for commercial GPS (GNSS)
- ❖ GNSS is used for localization and time synchronization
- ❖ Signal from satellite is weak.

- ❖ GNSS jamming causes loss of lock (wrong position or time)
- ❖ GNSS spoofing may cause much serious problems.

- ❖ Consideration for GNSS spoofing?
 - Fail-safe mode design
 - Hard vs. Soft spoofing (or seamless takeover)

Hard GPS spoofing + Failsafe Bypass



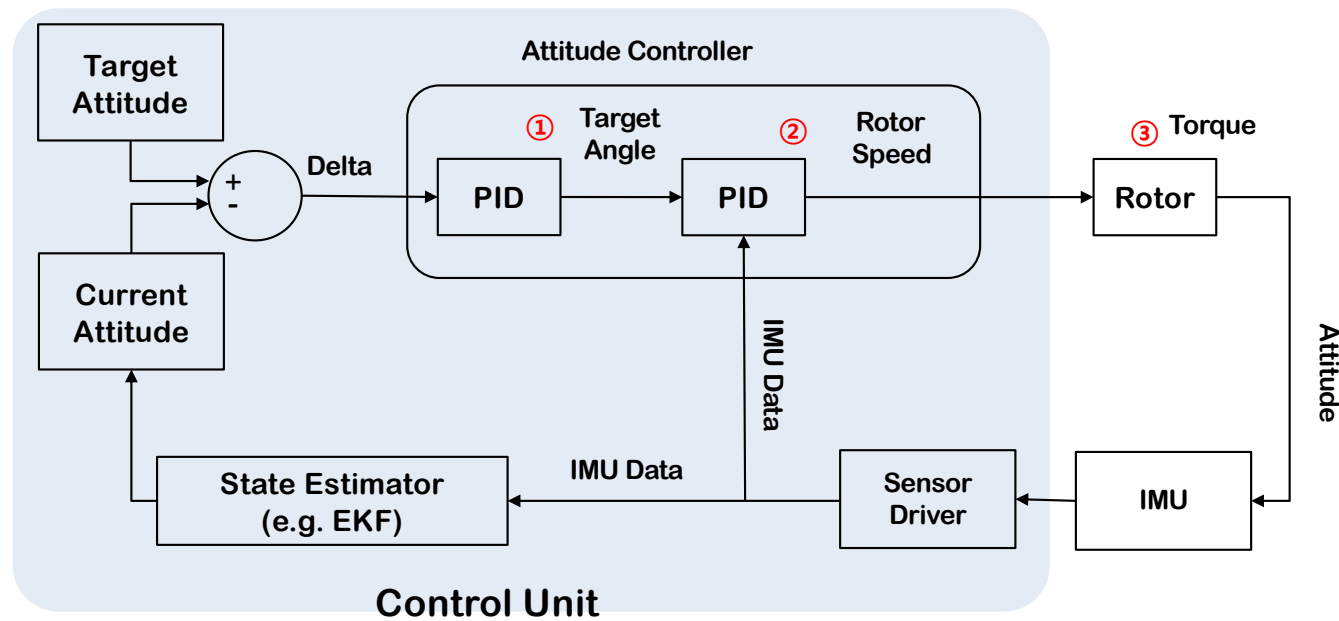
Tractor Beam: Safe-hijacking of Consumer Drones with Adaptive GPS Spoofing, ACM TOPS'19


Soft GPS Spoofing



Sensing Channel

How Drone Control Works





USENIX Security Symposium 2015

Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

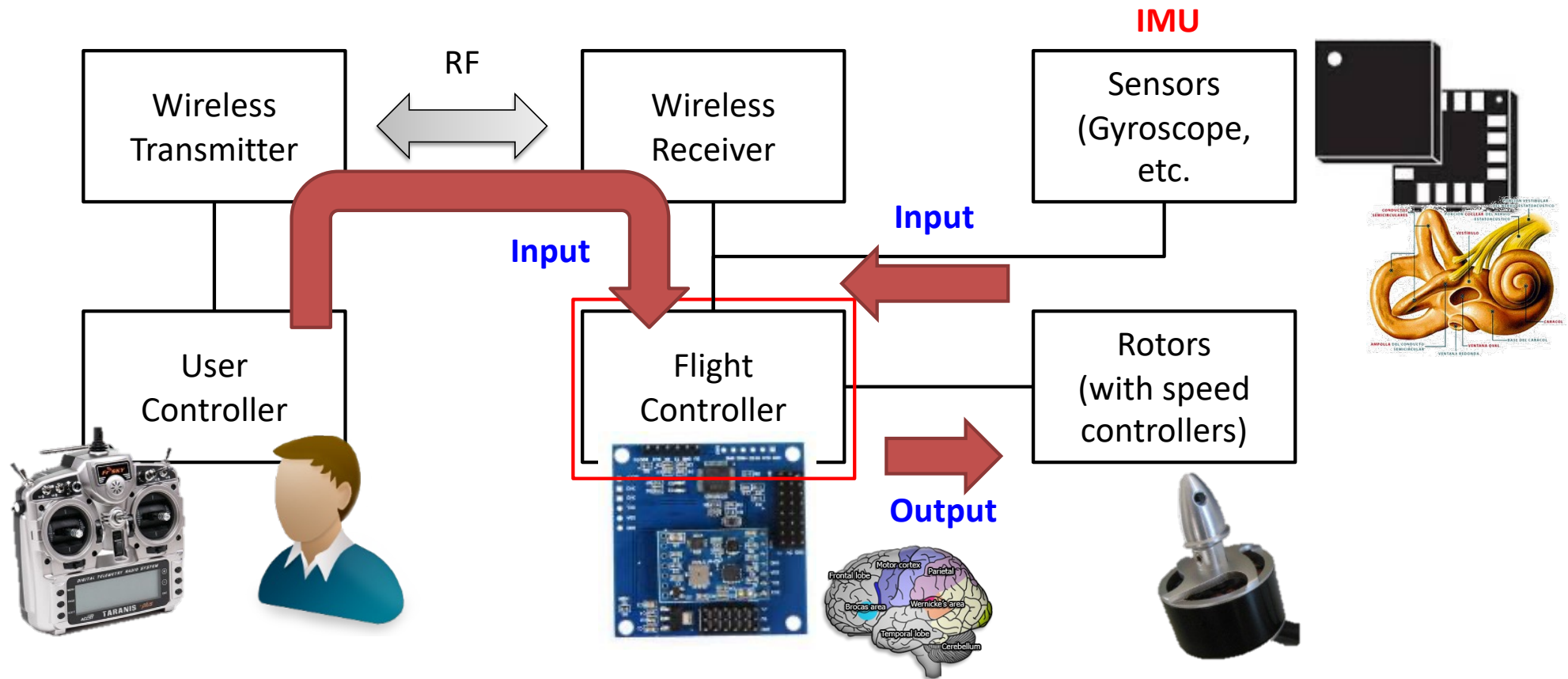
2015. 08. 14.

Yunmok Son, Hocheol Shin, Dongkwan Kim, Youngseok Park,
Juhwan Noh, Kibum Choi, Jungwoo Choi, and **Yongdae Kim**
Electrical Engineering at KAIST
System Security Lab.

KAIST

Drone System

* IMU: Inertial Measurement Unit



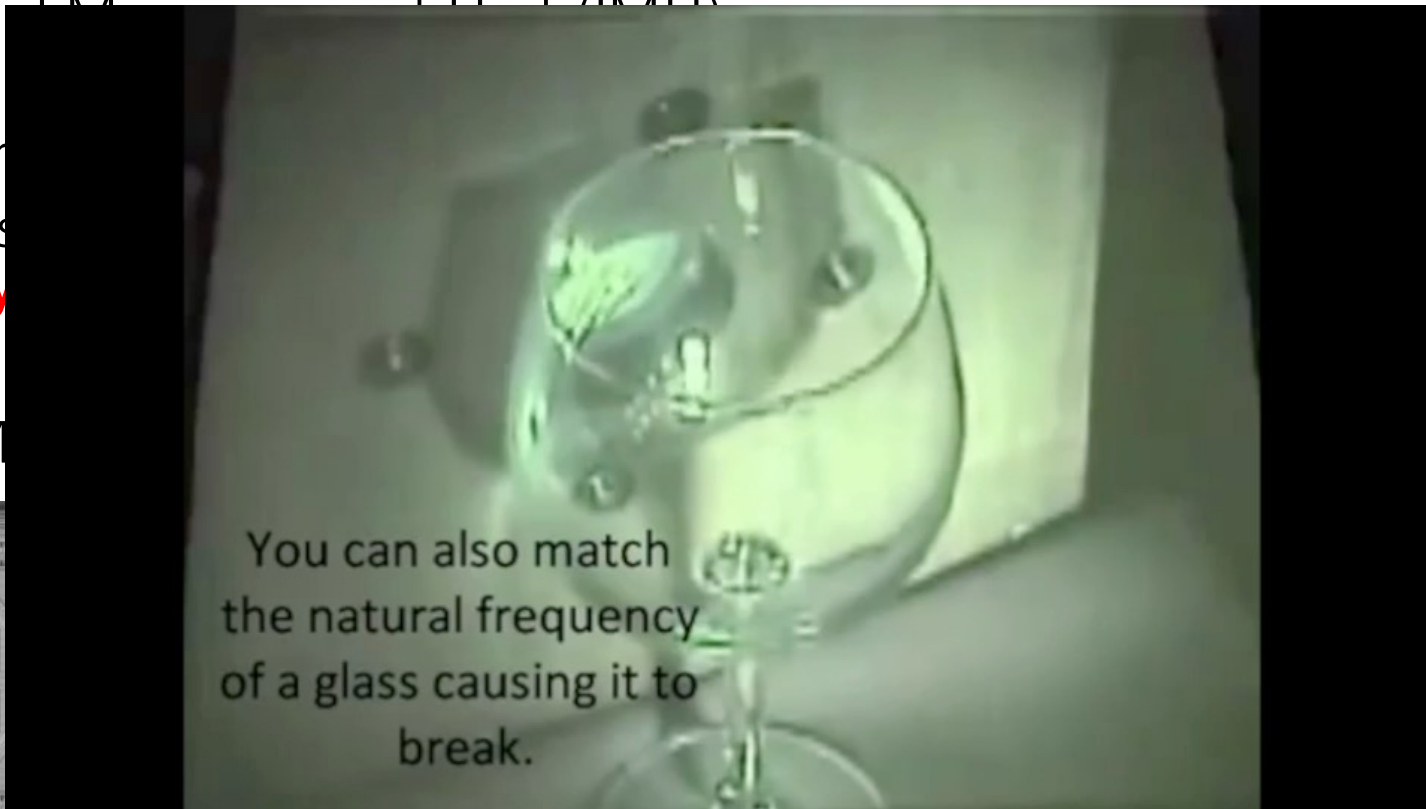
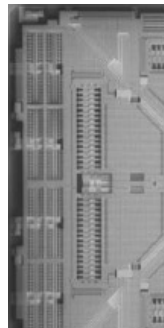
Gyroscope on Drone

* MEMS: Micro-Electro-Mechanical Systems

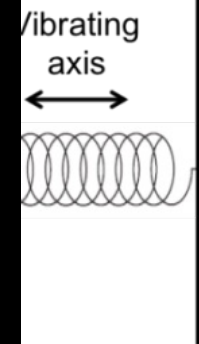
❖ Inertial Measurement Unit (IMU)

- Accelerometer
- Gyroscope

❖ MEMS



1S gyro.>



ing
s

(<https://www.youtube.com/watch?v=joS6kfjuKQo>, <https://www.youtube.com/watch?t=45&v=sH7XSX10QkM>)

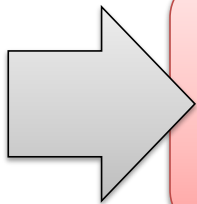
Resonance in MEMS Gyroscope

- ❖ Mechanical resonance by sound noise
 - Known fact in the MEMS community
 - Degrades MEMS Gyro's accuracy
 - With (resonant) frequencies of sound

L3GD20

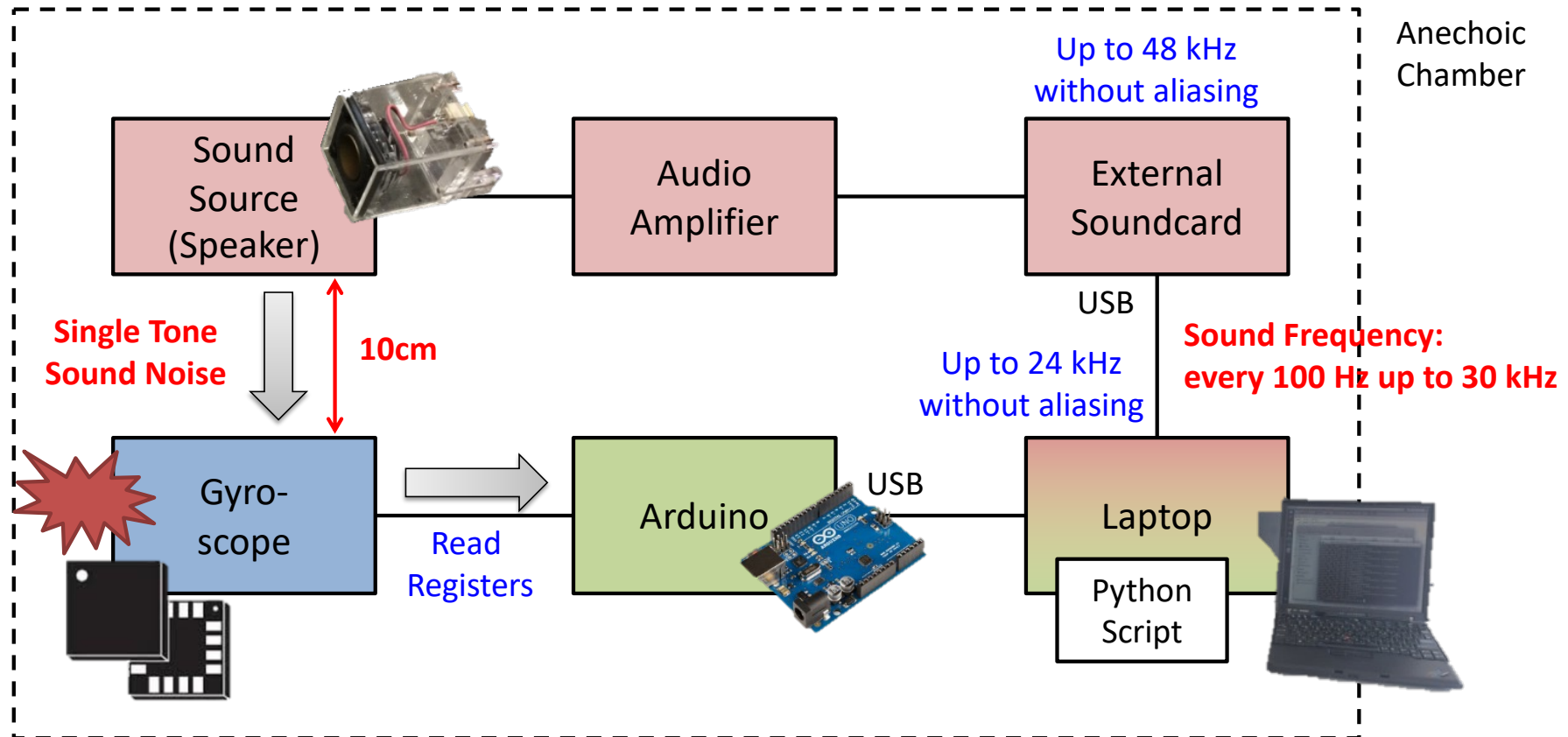
Features

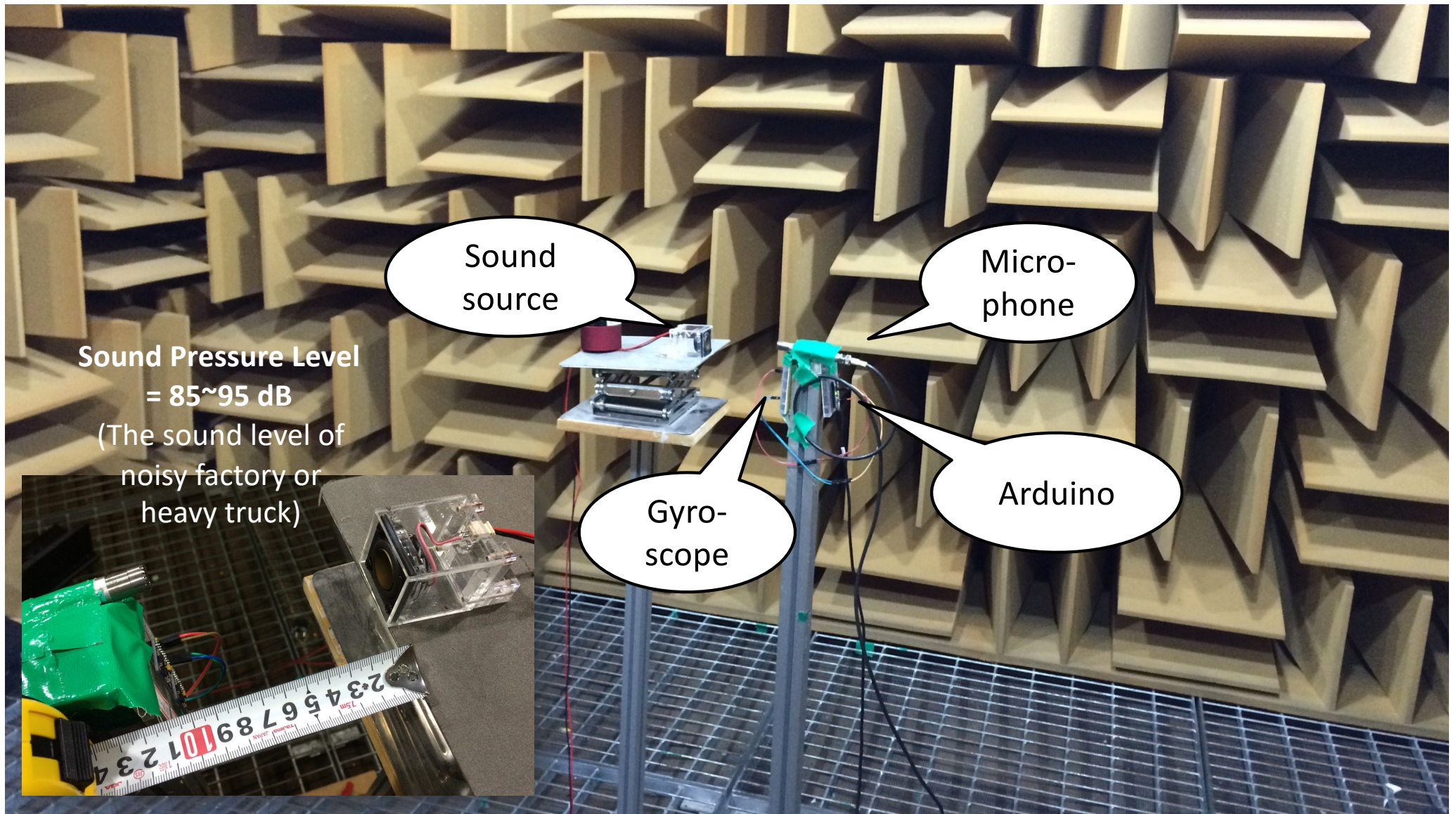
- Three selectable full scales ($\pm 250/500/2000$ dps)
- 20+ kHz resonant frequency over the audio bandwidth



MEMS Gyro. with a high resonant frequency
to reduce the sound noise effect (above 20kHz)

Experiment Setup





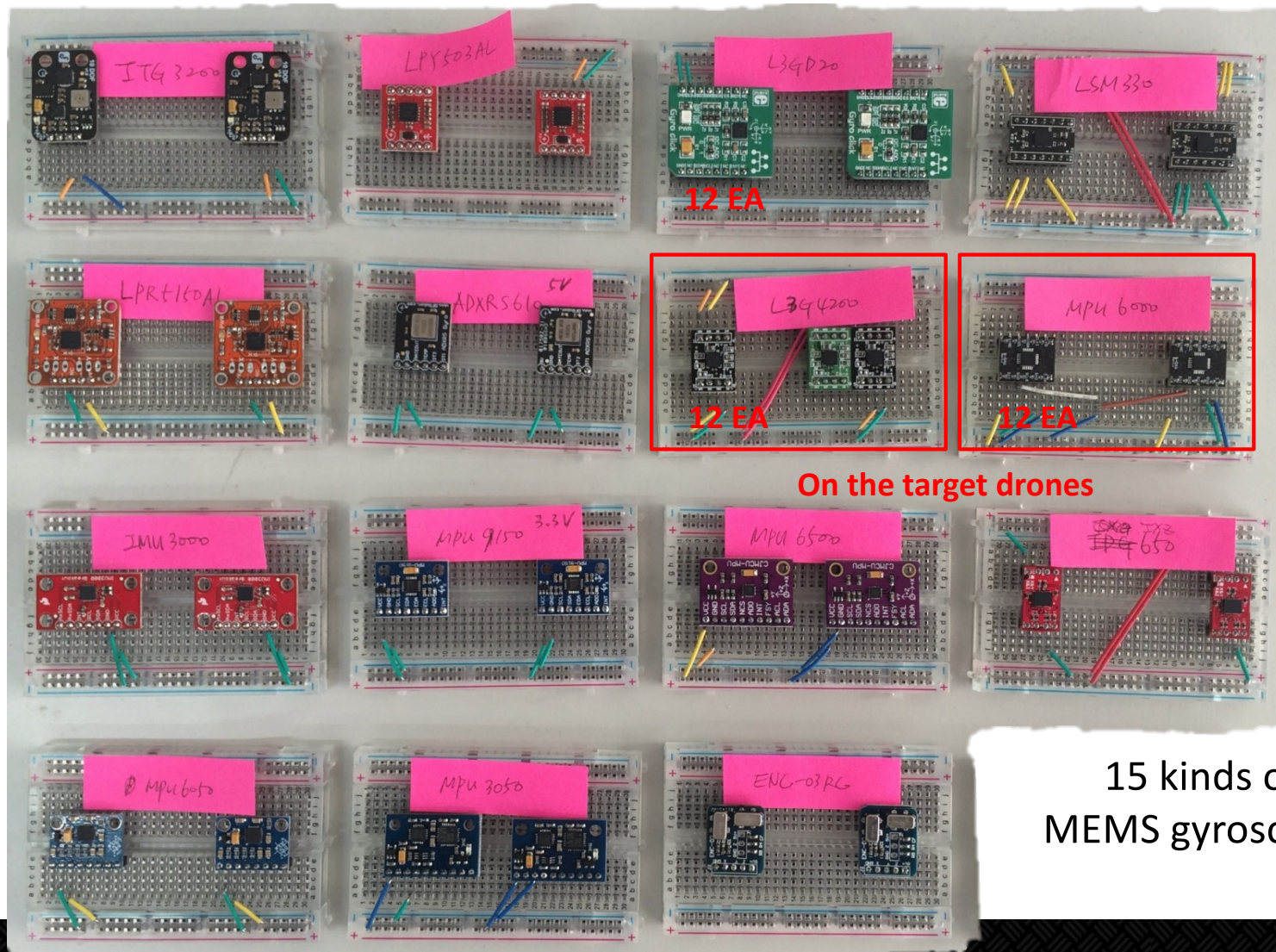
Sound
source

Micro-
phone

Sound Pressure Level
= 85~95 dB
(The sound level of
noisy factory or
heavy truck)

Gyro-
scope

Arduino



15 kinds of
MEMS gyroscopes

Experimental Results (1/3)

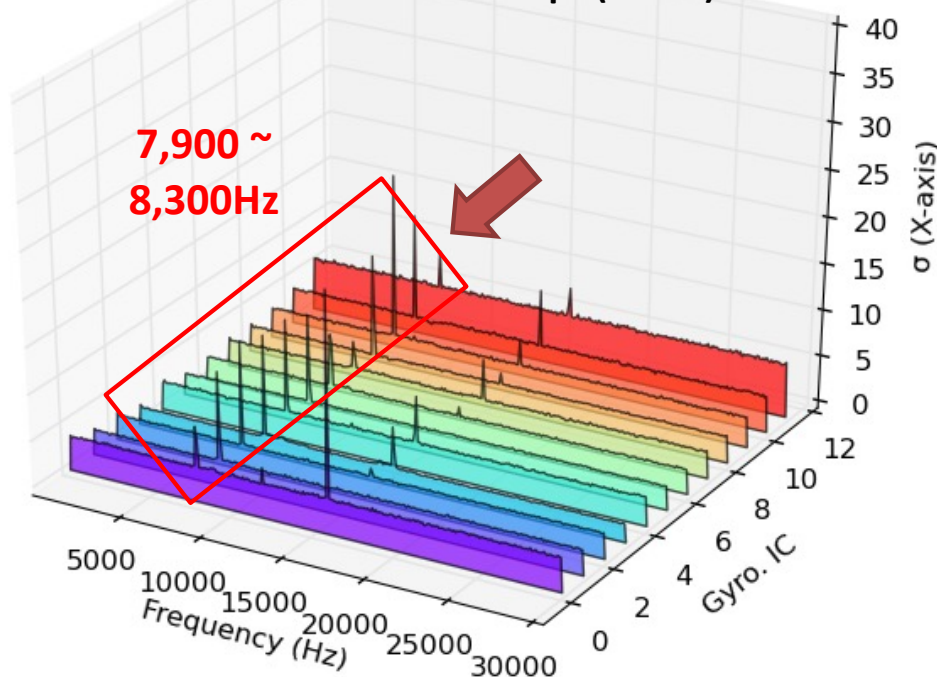
- ❖ Found the resonant frequencies of **7 MEMS gyroscopes**
- ❖ Not found for 8 MEMS gyroscopes

Sensor	Vender	Supporting Axis	Resonant freq. in the datasheet (axis)	Resonant freq. in our experiment (axis)
L3G4200D	STMicro.	X, Y, Z	No detailed information	7,900 ~ 8,300 Hz (X, Y, Z)
L3GD20	STMicro.	X, Y, Z		19,700 ~ 20,400Hz (X, Y, Z)
LSM330	STMicro.	X, Y, Z		19,900 ~ 20,000 Hz (X, Y, Z)
MPU6000	InvenSense	X, Y, Z	30 ~ 36 kHz (X) 27 ~ 33 kHz (Y) 24 ~ 30 kHz (Z)	26,200 ~ 27,400 Hz (Z)
MPU6050	InvenSense	X, Y, Z		25,800 ~ 27,700 Hz (Z)
MPU9150	InvenSense	X, Y, Z		27,400 ~ 28,600 Hz (Z)
MPU6500	InvenSense	X, Y, Z	25 ~ 29 kHz (X, Y, Z)	26,500 ~ 27,900 Hz (X, Y, Z)

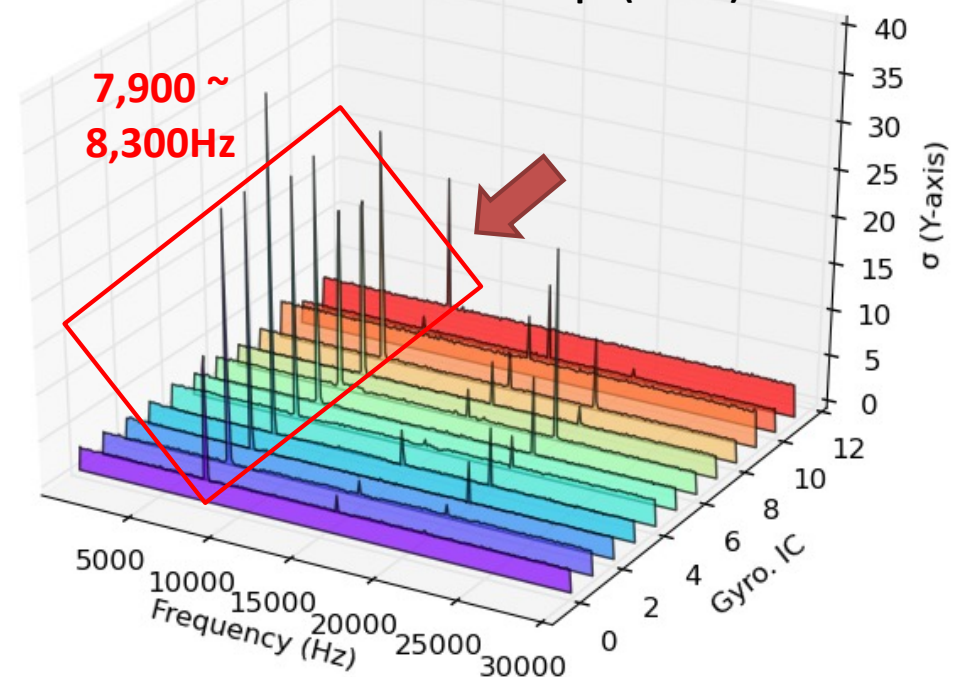
Experimental Results (2/3)

- ❖ Unexpected output by sound noise (for L3G4200D)

Standard deviation of raw data samples
for 12 L3G4200D chips (X-axis)



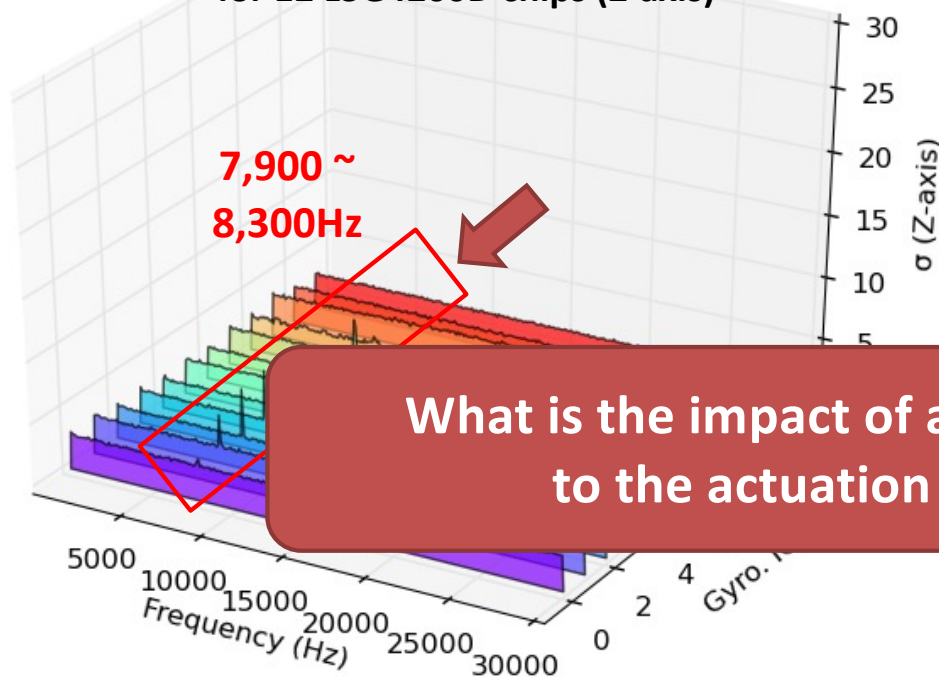
Standard deviation of raw data samples
for 12 L3G4200D chips (Y-axis)



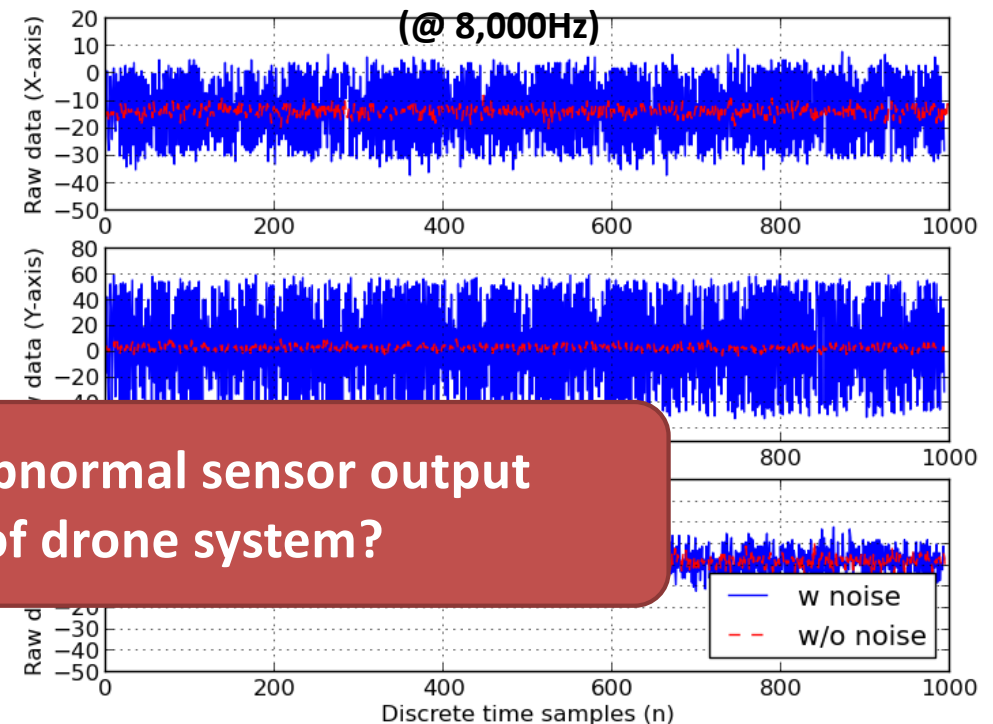
Experimental Results (3/3)

- ❖ Unexpected output by sound noise (for L3G4200D)

Standard deviation of raw data samples
for 12 L3G4200D chips (Z-axis)




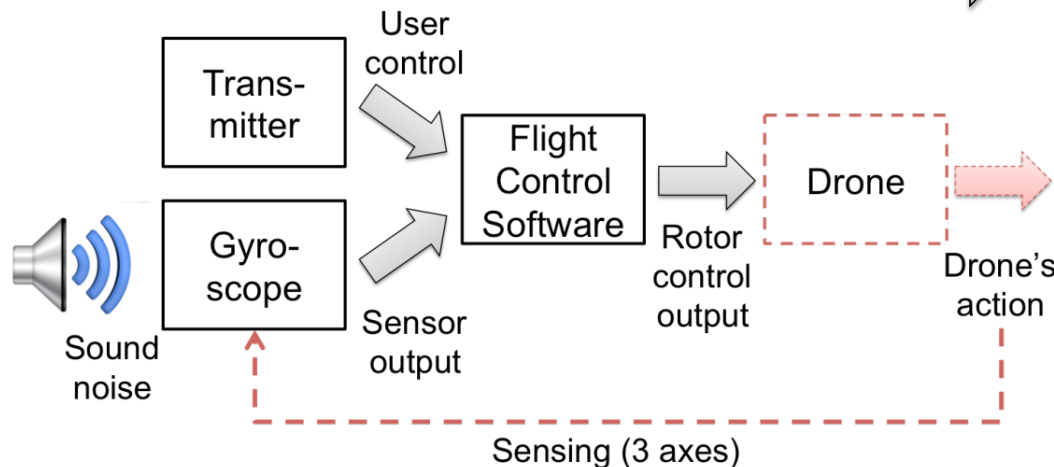
Raw data samples of one L3G4200D chip



What is the impact of abnormal sensor output
to the actuation of drone system?

Software Analysis

- ❖ Two open-source firmware programs
 - Multiwii project
 - ArduPilot project
- ❖ Rotor control algorithm 



for *axis* **do**

```

     $P = txCtrl[axis] - gyro[axis] \times G_P[axis];$ 
     $error = txCtrl[axis] / G_P[axis] - gyro[axis];$ 
     $error_{accumulated} = error_{accumulated} + error;$ 
     $I = error_{accumulated} \times G_I[axis];$ 
     $delta = gyro[axis] - gyro_{last}[axis];$ 
     $delta_{sum} = \text{sum of the last three delta values};$ 
     $D = delta_{sum} \times G_D[axis];$ 
     $PIDCtrl[axis] = P + I - D;$ 

```

end

for *rotor* **do**

for *axis* **do**

```

     $rotorCtrl[rotor] =$ 
     $txCtrl[throttle] + PIDCtrl[axis];$ 

```

end

limit $rotorCtrl[rotor]$ within the pre-defined
 MIN (1,150) and MAX (1,850) values;

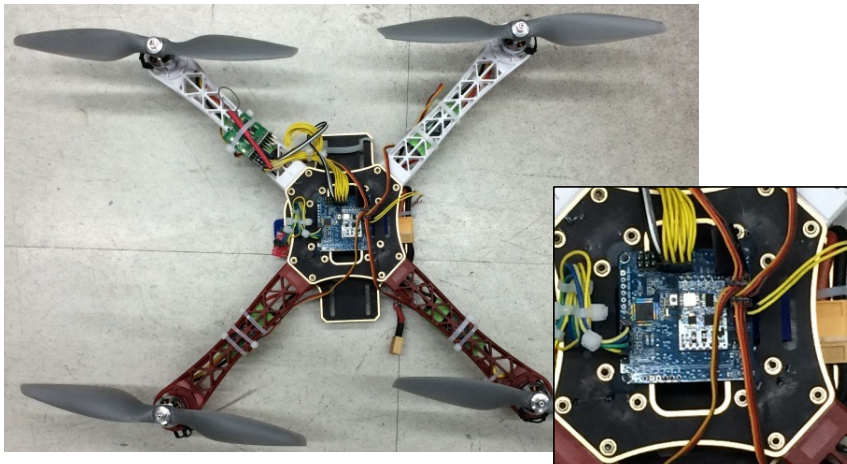
end

actuate rotors;

Target Drones

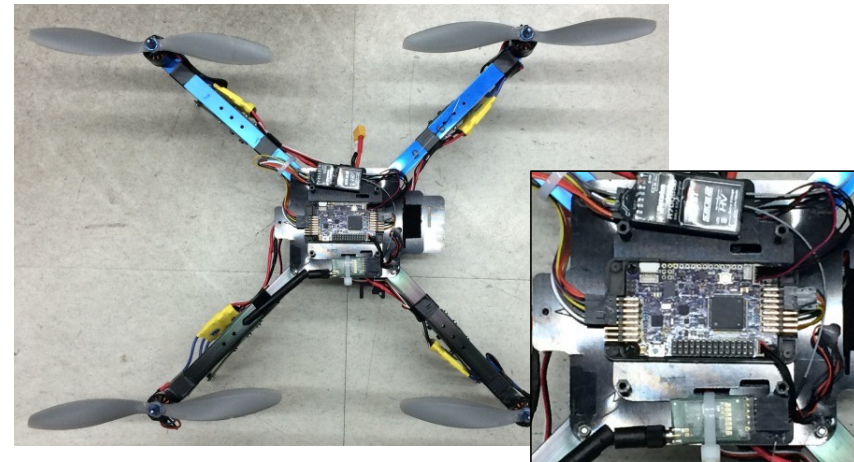
❖ Target drone A (DIY drone)

- Gyroscope: L3G4200D
- Resonant freq.: 8,200 Hz
- Firmware: Multiwii (Audible sound range)

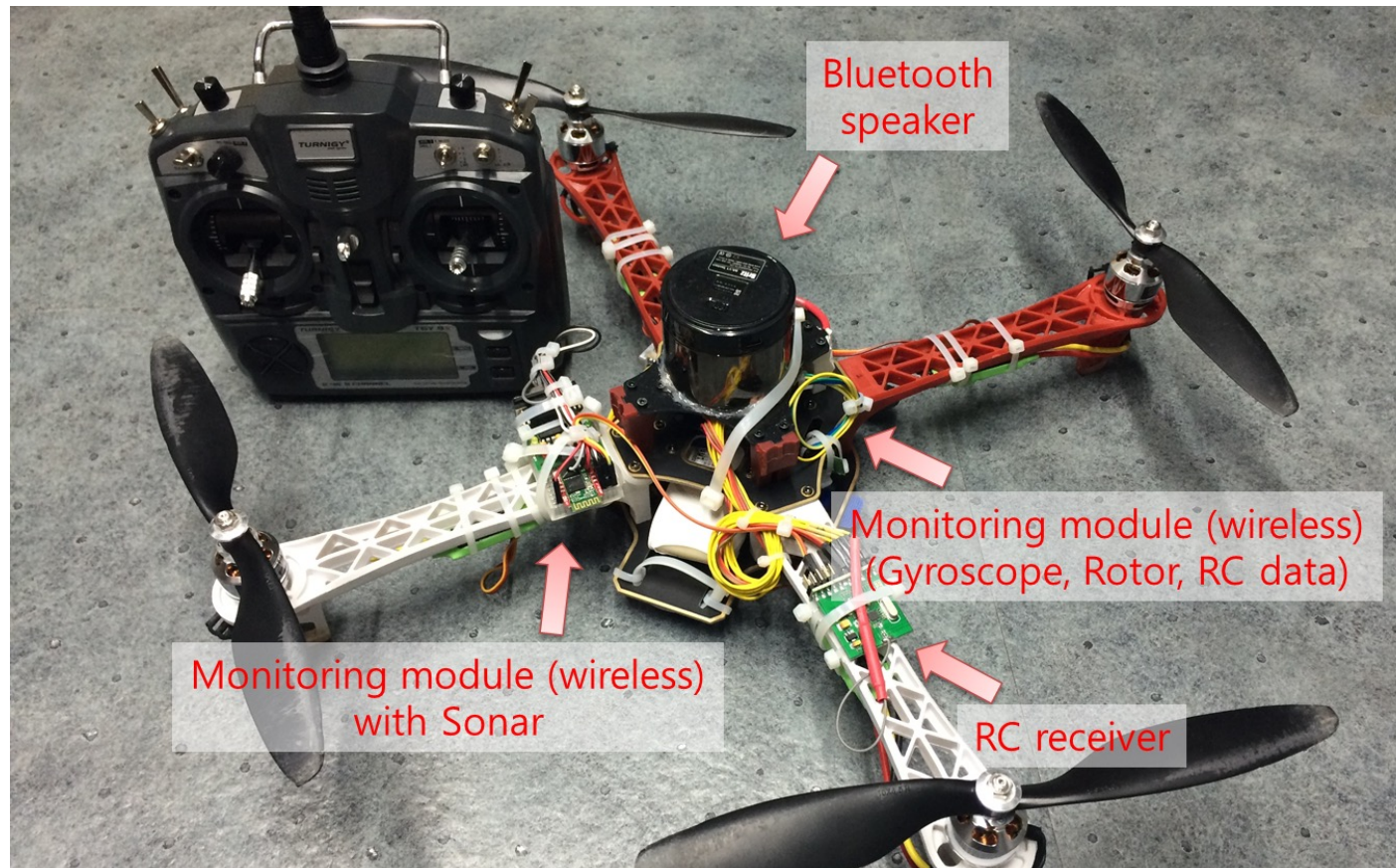


❖ Target drone B (DIY drone)

- Gyroscope: MPU6000
- Resonant freq.: 26,200 Hz
- Firmware: ArduPilot (Ultra sound range)

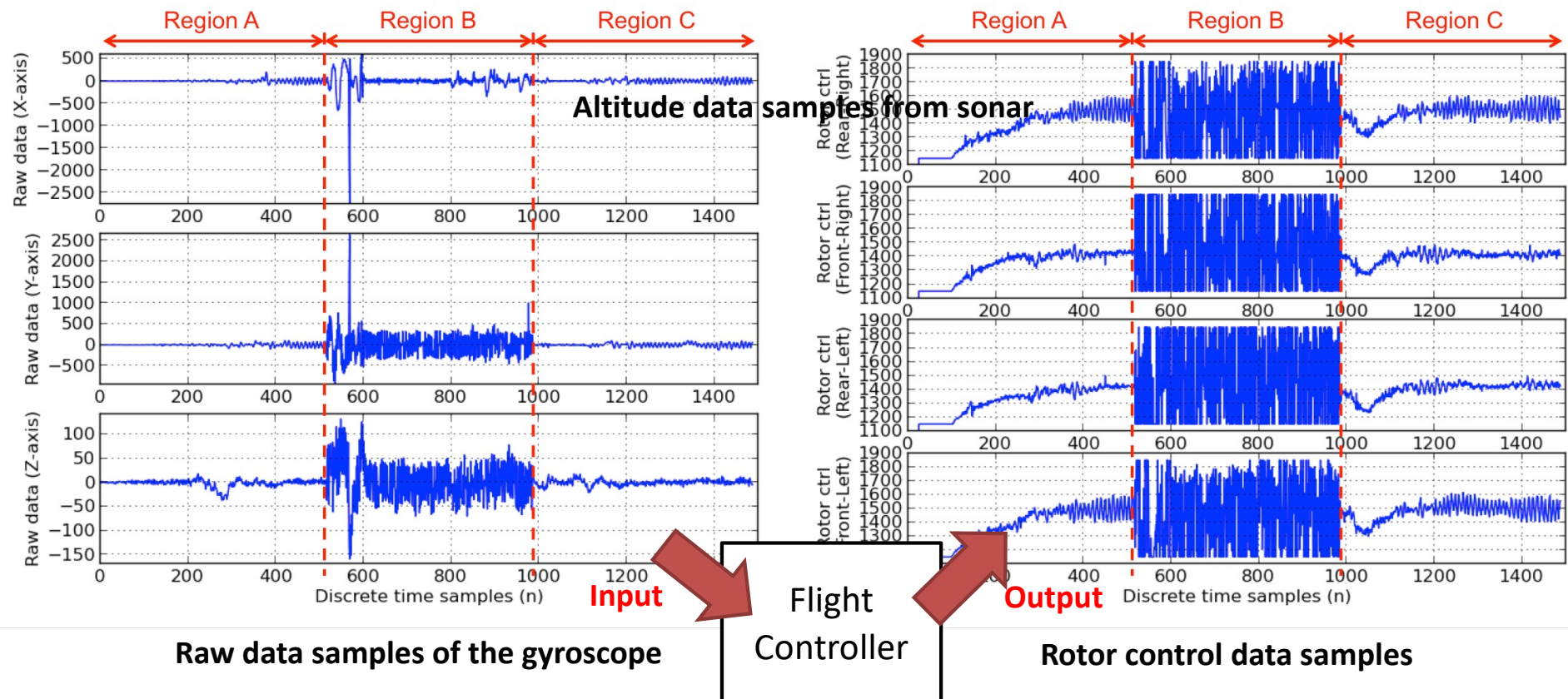


Attack DEMO





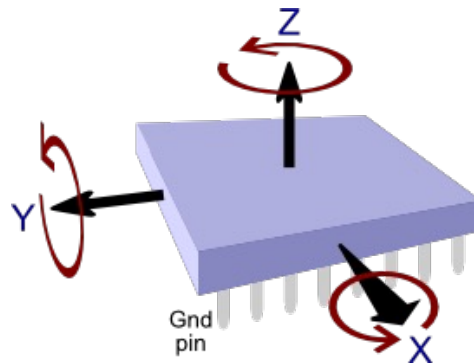
Attack DEMO (Target drone A)



Attack Results

❖ Result of attacking two target drones

	Target Drone A	Target Drone B
Resonant Freq. (Gyro.)	8,200 Hz (L3G4200D)	26,200 Hz (MPU6000)
Affected Axes	X, Y, Z	Z
Attack Result	Fall down	-



- X- and Y-axis = vertical rotation (more critical effect on stability)
- Z-axis = horizontal orientation

Attack Distance

- ❖ The minimum sound pressure level in our experiments
 - About 108.5 dB SPL (at 10cm)
- ❖ Theoretically, 37.58m using a sound source that can generate 140 dB SPL at 1m

$$SPL = SPL_{ref} - 20\log\left(\frac{d}{d_{ref}}\right)$$



<450XL of LRAD Corporation>

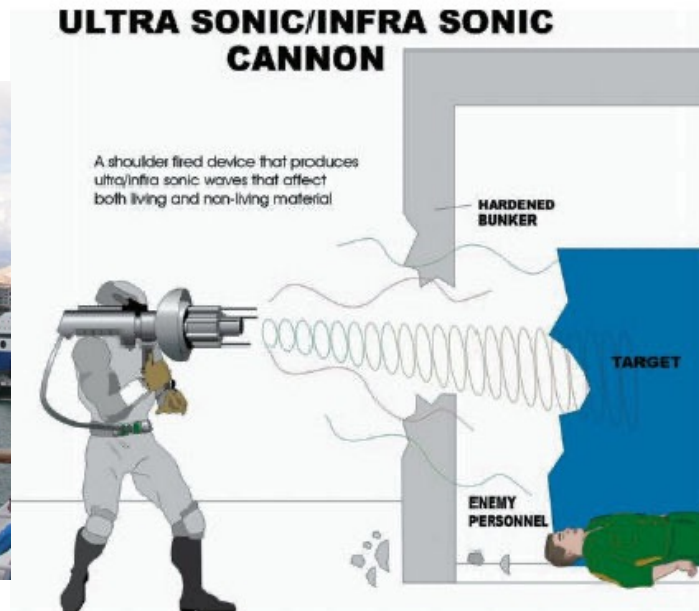
ACOUSTIC PERFORMANCE

Maximum Continuous Output	146dB SPL @ 1 meter, A-weighted
Sound Projection	+/- 15° at 1 kHz/-3dB
Communications Range	Highly intelligible voice messages over

(http://www.lradx.com/wp-content/uploads/2015/05/LRAD_Datasheet_450XL.pdf)

Attack Scenarios

- ❖ Drone to Drone Attack
- ❖ Sonic Weapons
- ❖ Sonic Wall/Zone





Limitations (2/2)

- ❖ No accumulated effect or damage



Simple sonic wall
(3m-by-2m, 25 speakers)

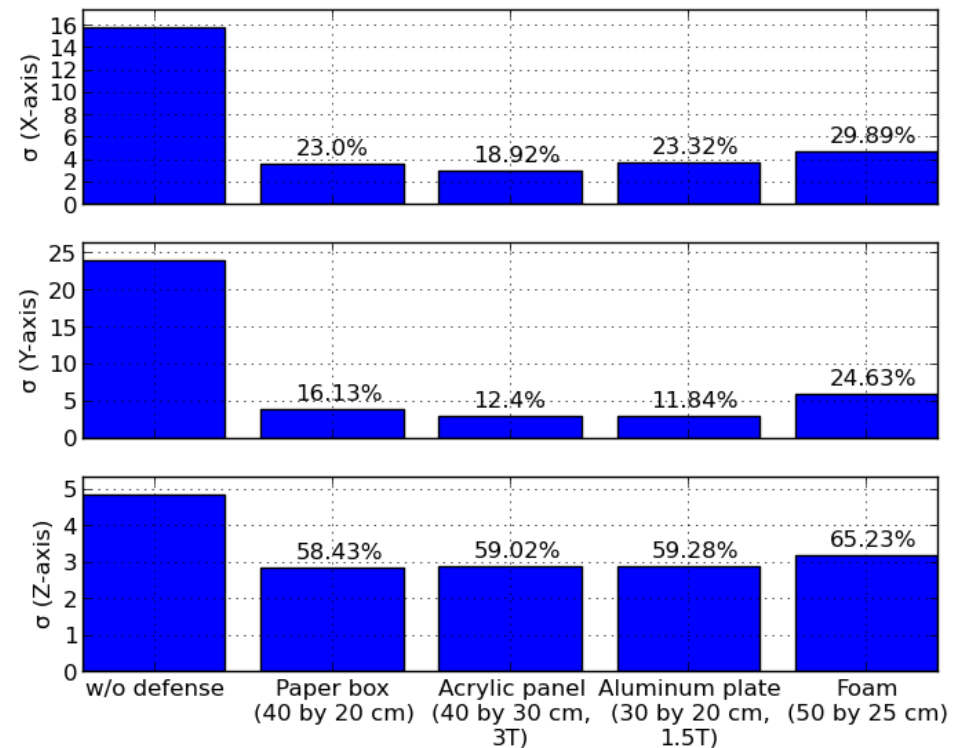


Countermeasure

- ❖ Physical isolation
 - Shielding from sound
 - Using four materials
 - Paper box
 - Acrylic panel
 - Aluminum plate
 - Foam



Standard deviation of raw data samples for one L3G4200D chip (averaged for 10 identical tests)



Conclusion

- ❖ A case study for a threat caused by sensor input
 - Finding mechanical resonant frequencies from 7 kinds of MEMS gyro.
 - Analyzing the effect of this resonance on the firmware of drones

Sensor output should not be fully trusted.

(Not only by natural errors, but also by attackers)

- ❖ Future work
 - Developing a software based defense (without hardware modifications)
 - Against sensing channel attacks for drones or embedded devices

Directed Acoustic Energy (Sandia Lab)

- ❖ Assessing the Vulnerability of Unmanned Aircraft Systems to Directed Acoustic Energy. Sandia National Lab
- 1. detonated/deflagrated explosive charges of various sizes
- 2. accurately measured impulse pressure and pulse duration
- 3. determined what magnitude of acoustic insult to the IMU disrupts flight and for how long and
- 4. determined if the air blast/shock wave on aircraft/propellers disrupts flight

DARPA Fire

- ❖ Faithful Integrated Reverse-Engineering and Exploitation (FIRE)
- ❖ Anticipated Funding Available for Award: \$70M
- ❖ cyber-physical vulnerabilities (CPV) arises from the composition of hardware, software, and physical components where each component may not be vulnerable in-and-of itself
- ❖ Driven by the proliferation of low-cost COTS components
- ❖ Innovative CPS vulnerability analysis tools and techniques

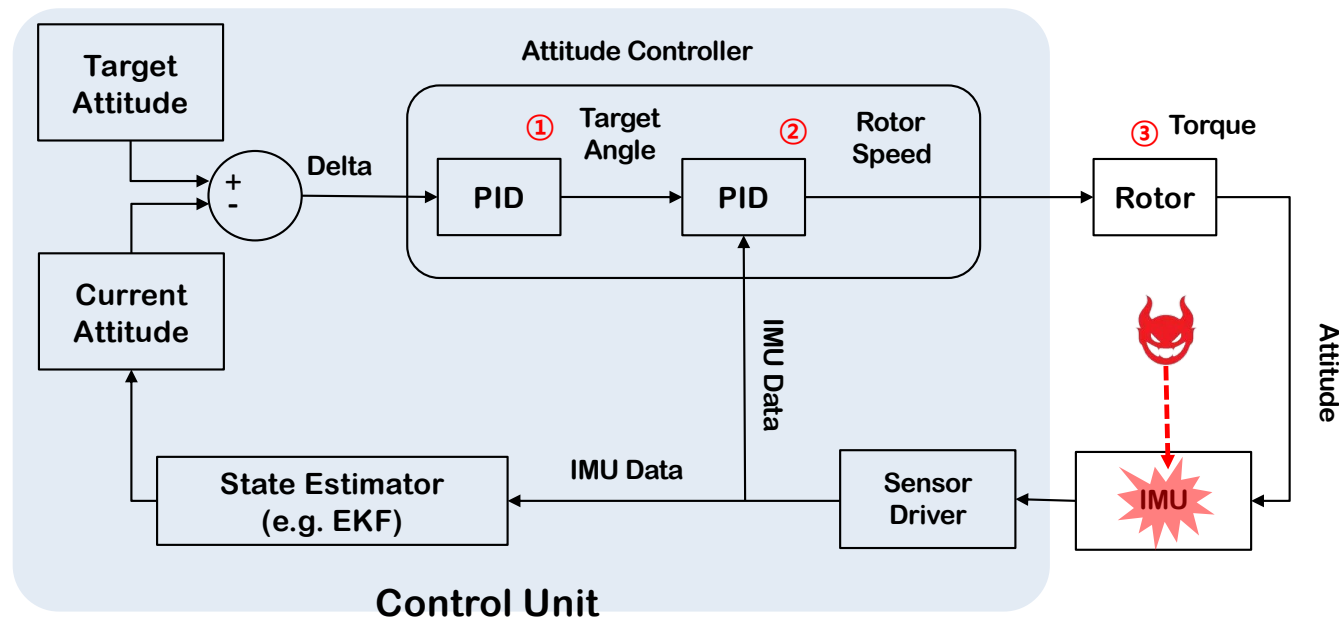
Anti-Drone Technologies

Type	Technology	Strength	Weakness	Response Time
Physical	Machine Gun,	Cost	Accuracy, Collateral damage	≈ 0
	Net, Colliding Drone	Cost	Accuracy, Reload	<10 sec
	Sound	Swarm attack	Distance, Power, Bypass, Aiming	<10 sec
	High-power laser	Accuracy, Distance	Response time, Cost, Swarm	>10 sec
Electro-magnetic	RF jamming	Cost, Distance	Collateral damage, Response time, Bypass	>10 sec
	GNSS jamming	Cost, Distance	Collateral damage, Response time, Bypass	>10 sec
	High-power EM	Swarm, Distance	Cost, Collateral damage	≈ 0
	Targeted EM	Power, Swarm, Distance	Cost	≈ 0
Hijacking	GNSS spoofing	Hijacking, Distance	Collateral damage, Response time	<10 sec
	Software hijacking	Cost	Need vulnerability	

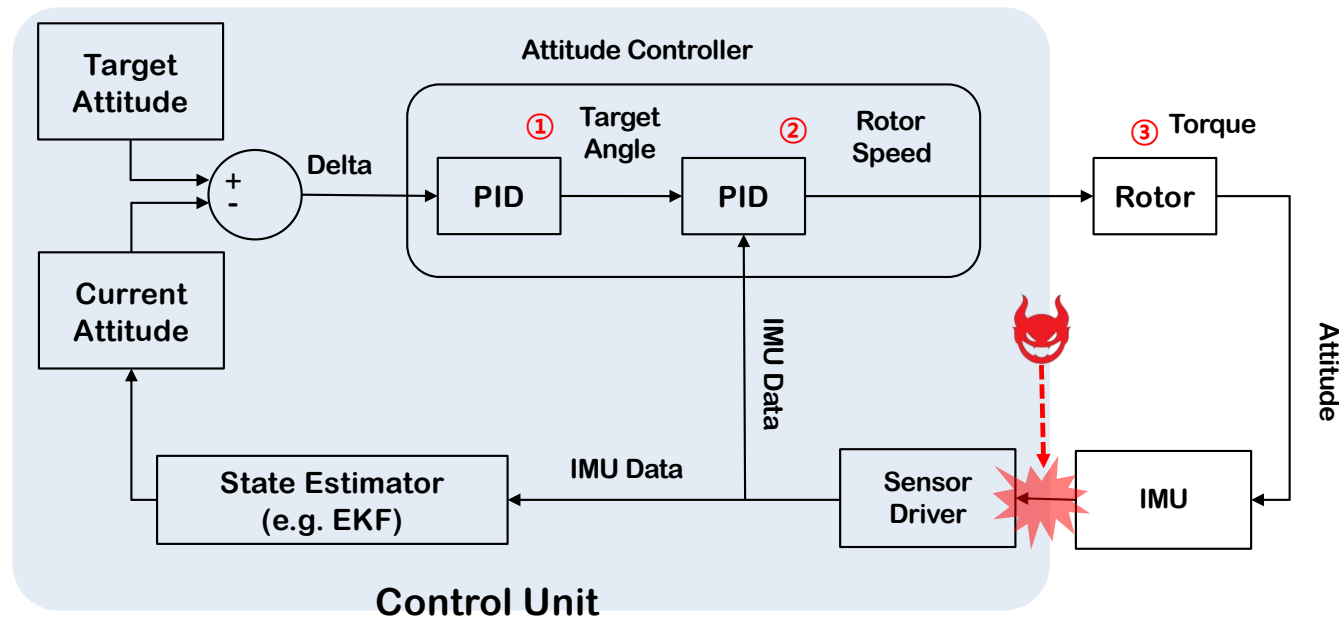
THOR US Military



Rocking Drone: Control System



Paralyzing Drone: Control System



Conclusion

- ❖ Arms race in Ukraine: anti-drone vs. counter-anti-drone
- ❖ What attacks should be in scope?
- ❖ RL under adversarial environment?
- ❖ “Perception and identification” is also very important.

Good questions

- ❖ Can this attack affect other sensors with resonant frequencies?
- ❖ Can you detect anomalies in advance?
- ❖ Multi-frequency or inaudible frequency attack?
- ❖ Defense strategy against drone-related military threats?
- ❖ Could the system be manipulated to create a false perception of stability, potentially leading to dangerous situations?
- ❖ Could this type of acoustic vulnerability extend beyond drones to other autonomous systems?
- ❖ Comparison of different approaches? Most popular anti-drone system?
- ❖ is it possible to identify the type of gyroscope just by examining the exterior?
- ❖ if the attacker can compromise the speaker, why can't they also compromise the drone control system?
- ❖ Could attackers exploit antenna resonance frequencies to achieve similar disruption?
- ❖ gyroscope data isn't reliable enough to be used for drones since it tends to drift over time
- ❖ Wouldn't making the resonant frequency not existent?
- ❖ Could the range/effectiveness be extended using directional speakers or arrays?
- ❖ Why MEMS?

Best questions

- ❖ Munim: Are there software-based defense without requiring hardware modifications?
- ❖ Donghyun: are there other methods that could effectively increase the attack range while maintaining maximum stealthiness?
- ❖ Younghyo: Would fail-safe modes be useful in this attack scenario, or would they be ineffective because rotor control is completely disrupted?