Dropping Drones from the Sky: Requirements, Pros and Cons

2023 HACKTHEON SEJONG

Yongdae Kim

SysSec@KAIST

joint work with many of my students and collaborators

KAIST

Syssec

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

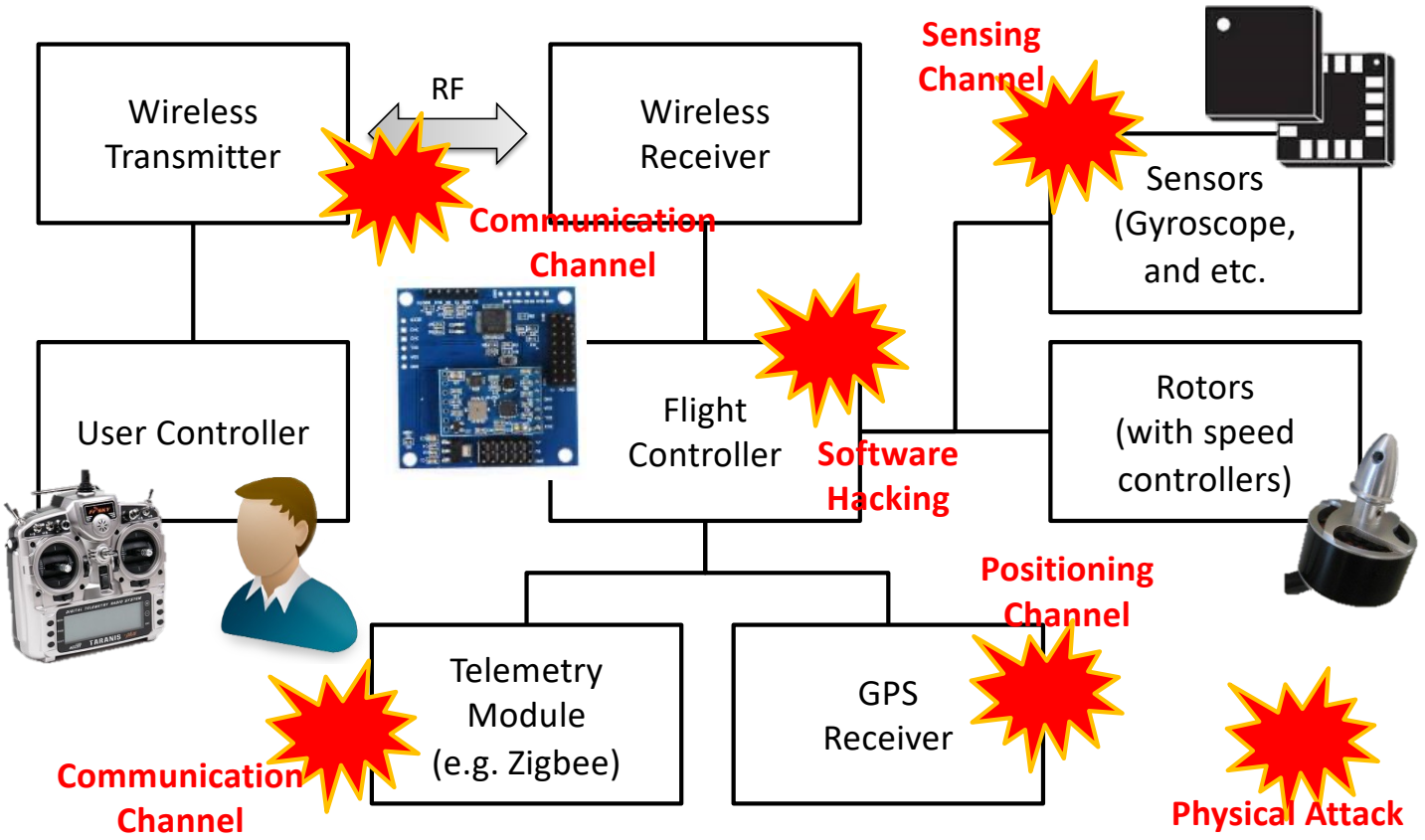
Ukrainians Say Russia is Still Tracking Their Drones with DJI AeroScope 05/2022

MAY 13, 2022 JARON SCHNEIDER

07/2022

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

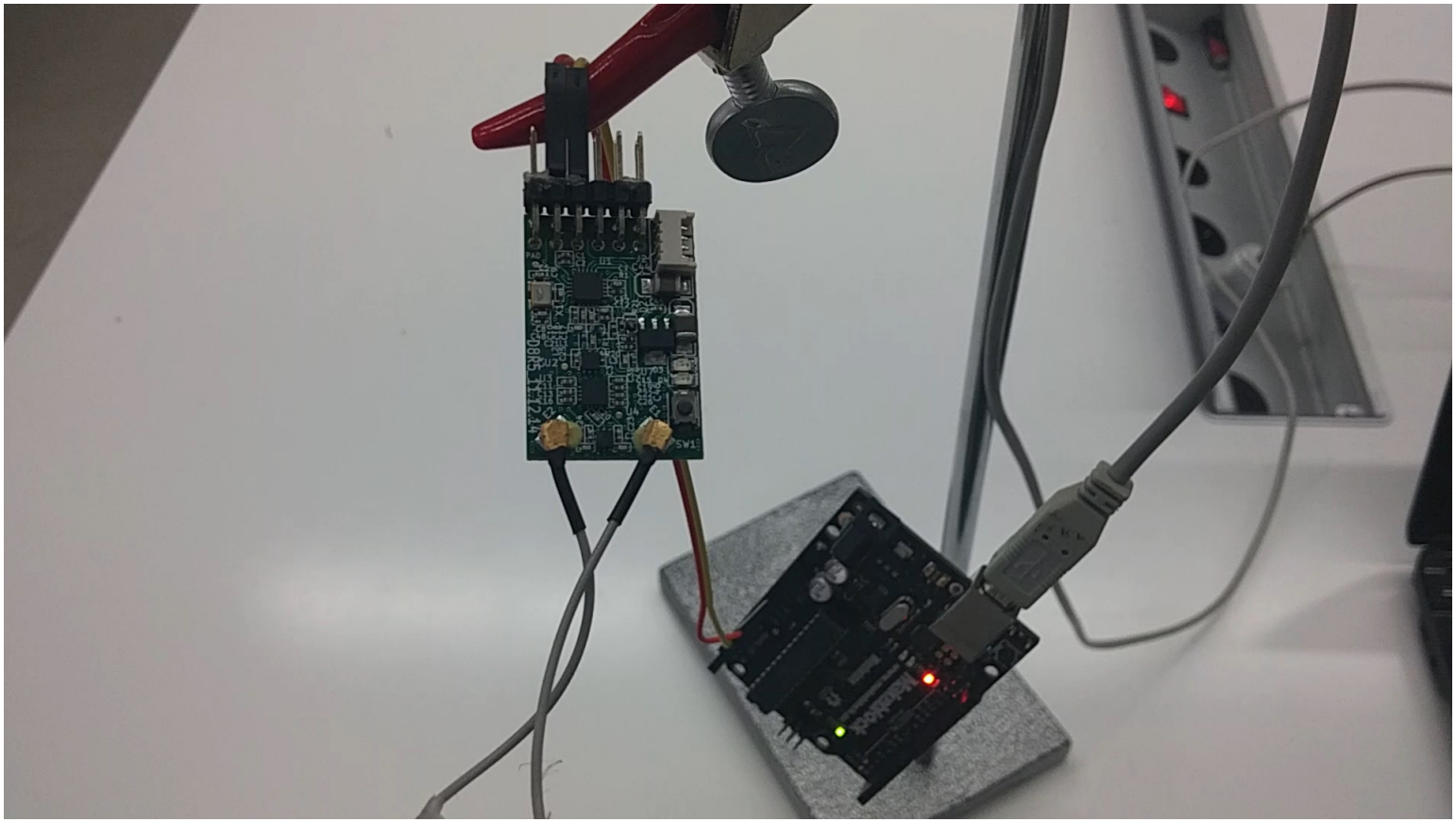
Type	Technology	Strength	Weakness	Response Time
Physical	Machine Gun	Cost	Accuracy, Collateral damage	≈ 0
	Net, Colliding Drone	Cost	Accuracy, Reload	<10 sec
	Sound	Swarm attack	Distance, Power, Bypass, Aiming	<10 sec
	High-power laser	Accuracy, Distance	Response time, Cost, Swarm	>10 sec
Electro-magnetic	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

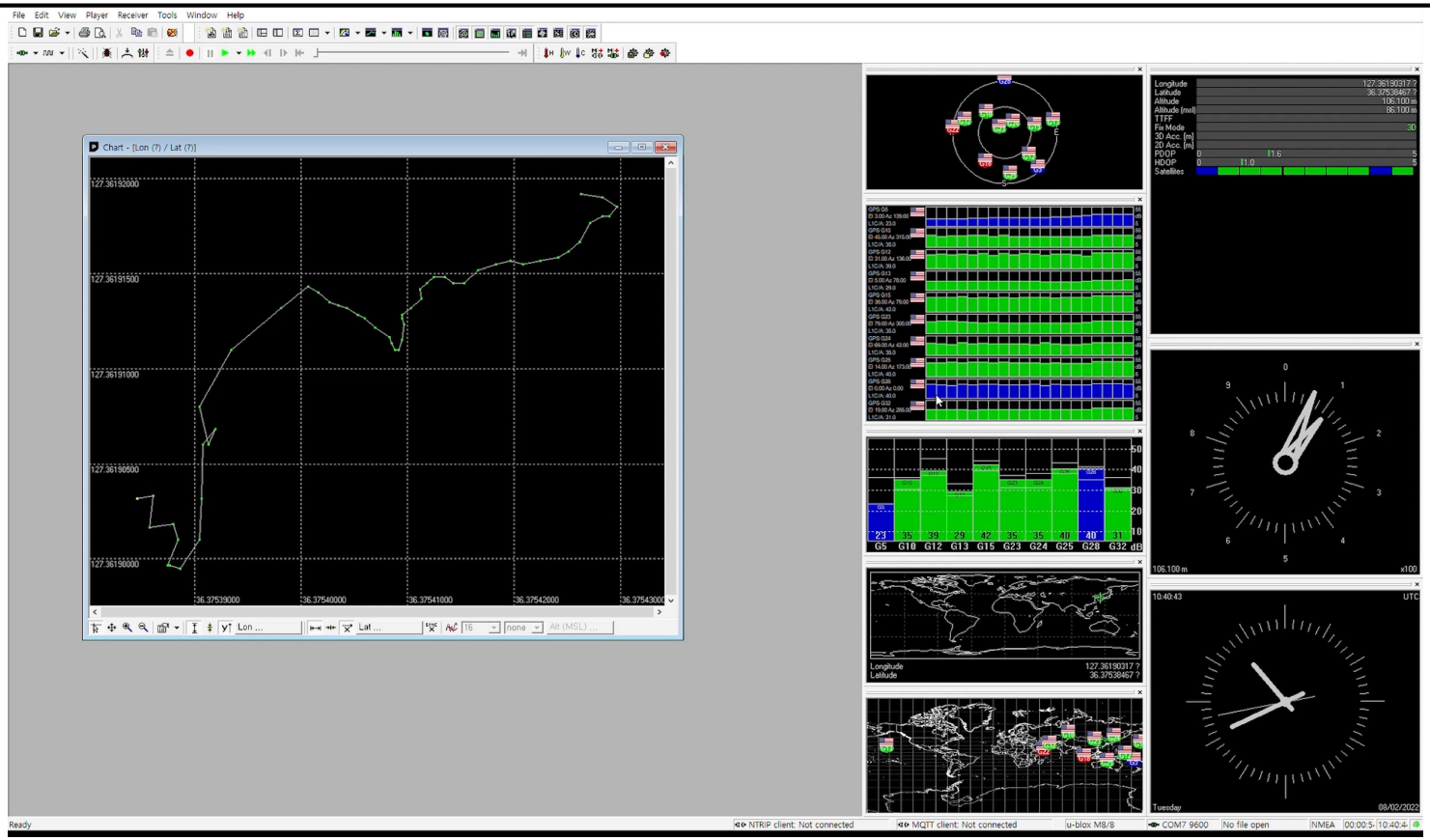
- No authentication and encryption for commercial GPS (GNSS)
- GNSS is used for localization and time synchronization
- Signal from satellite is weak.

- 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

Soft GPS Spoofing (Receiver)

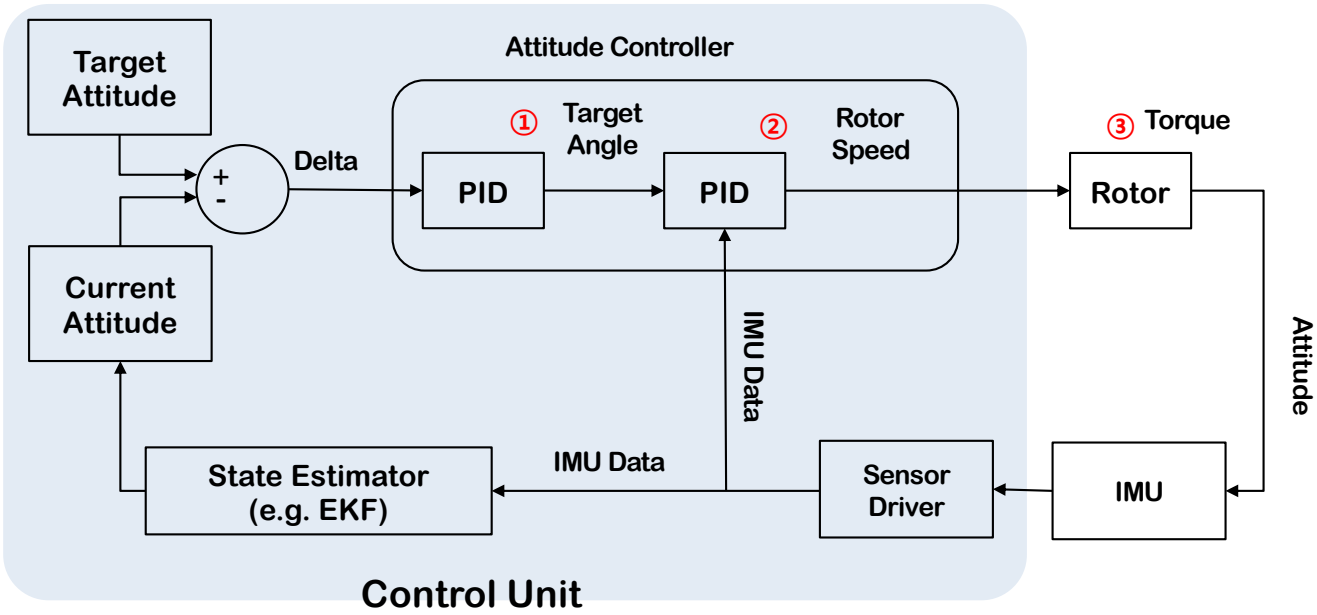


SysSec
System Security Lab

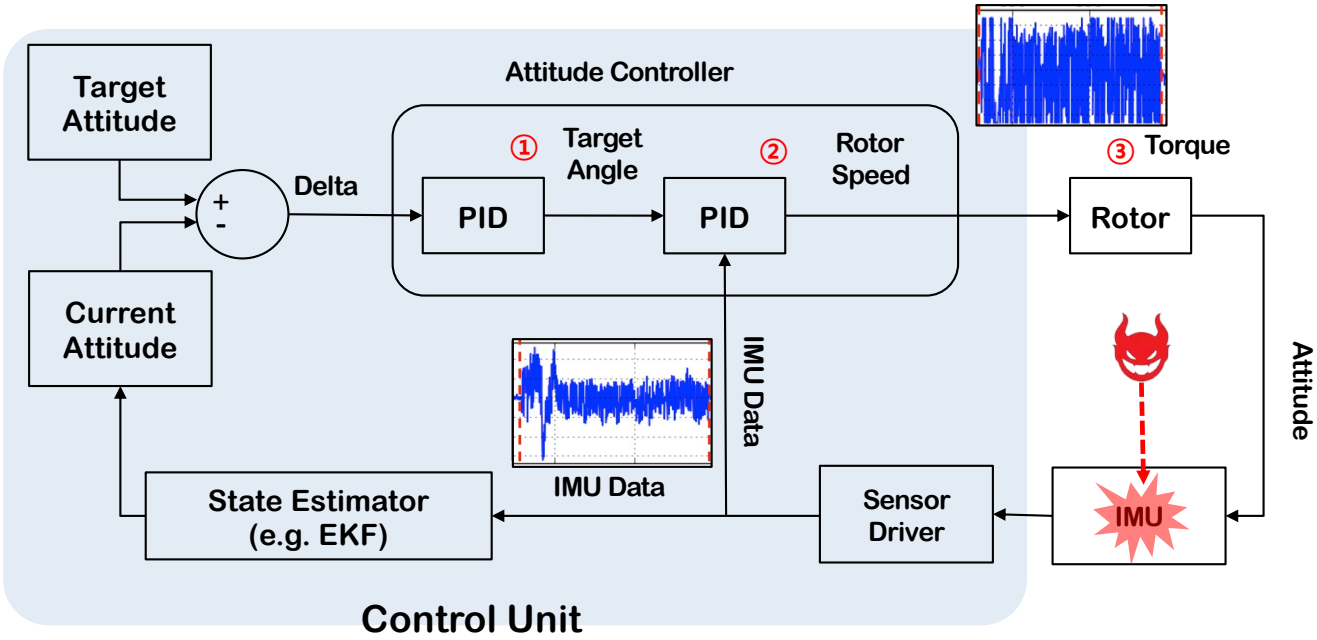
Soft GPS Spoofing

Sensing Channel

How Drone Control Works

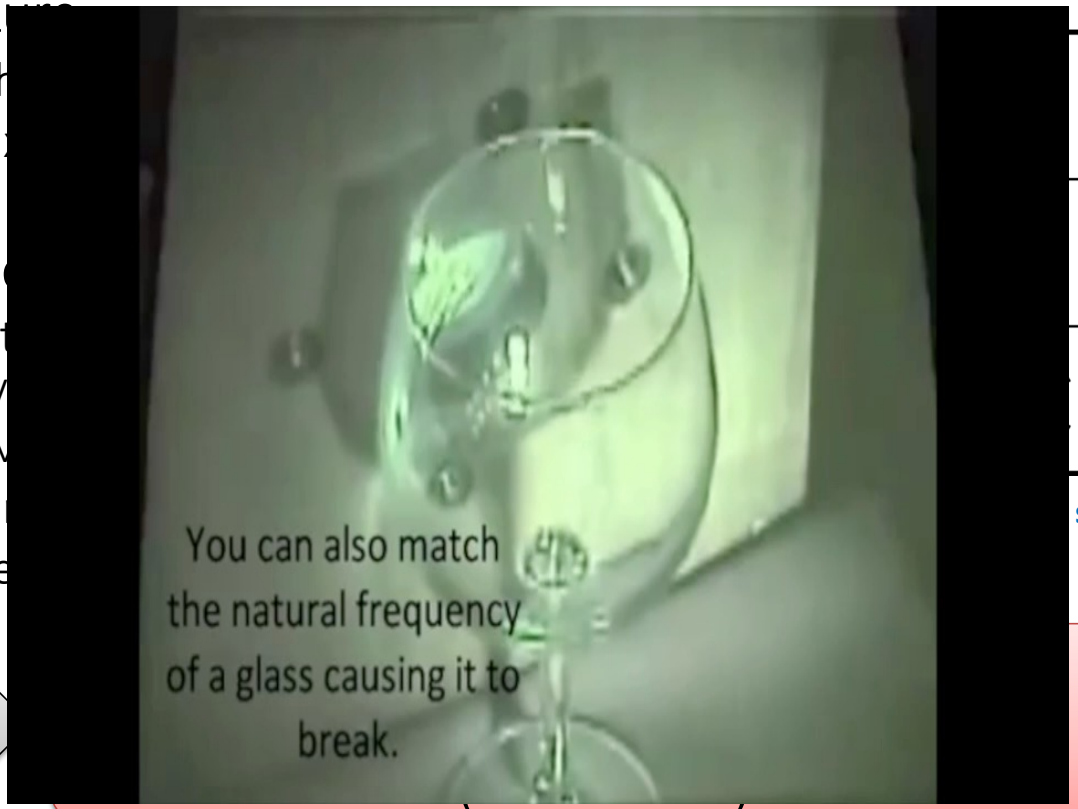


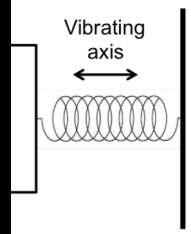
How Rocking Drone Control Works



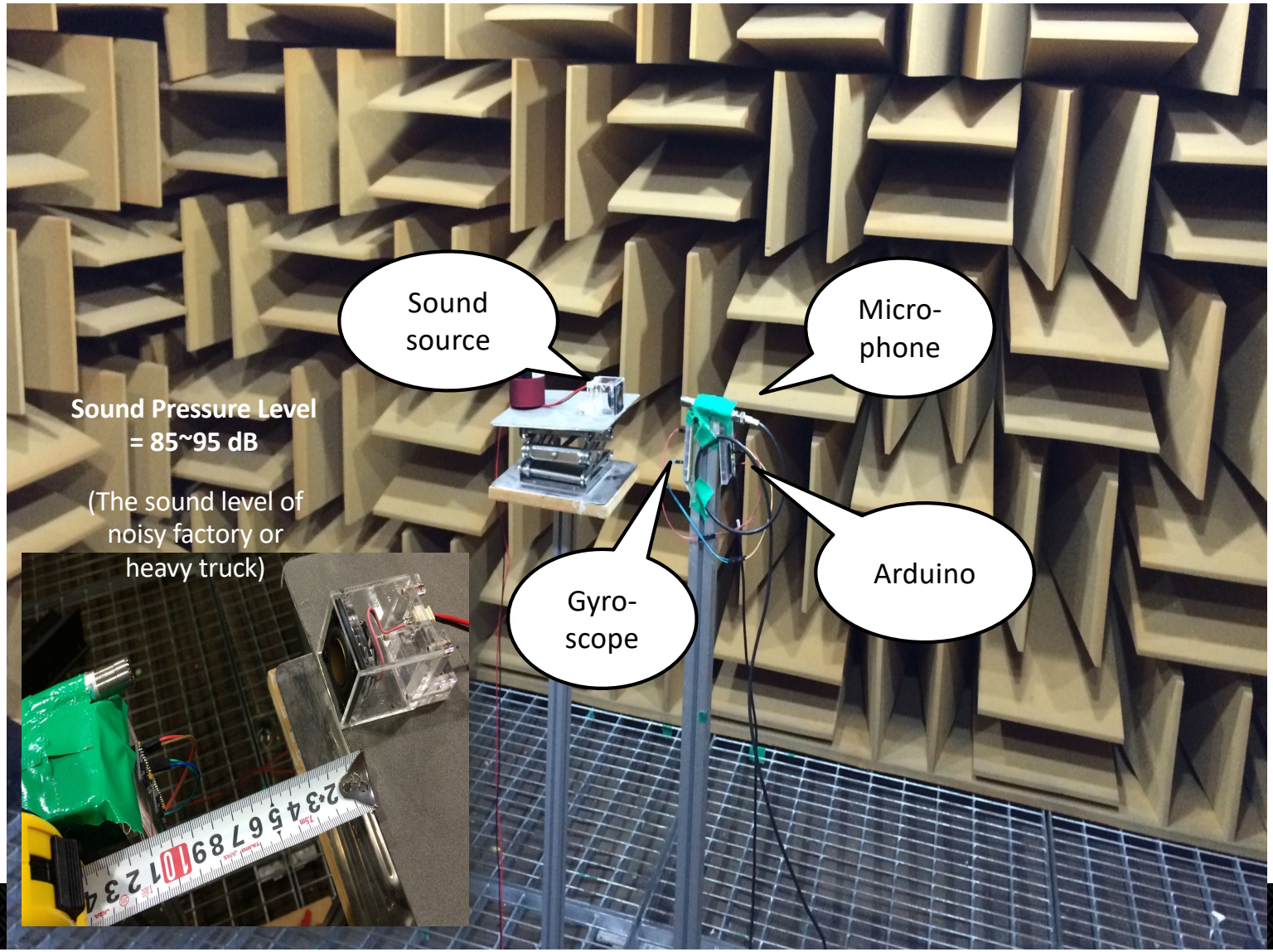
MEMS Gyro. & Sound Noise

- MEMS struct
  - Based on th
  - Vibrating a
- Sound noise
  - Known fact
    community
  - Degrades M
  - With certai
  - May induce





structure>

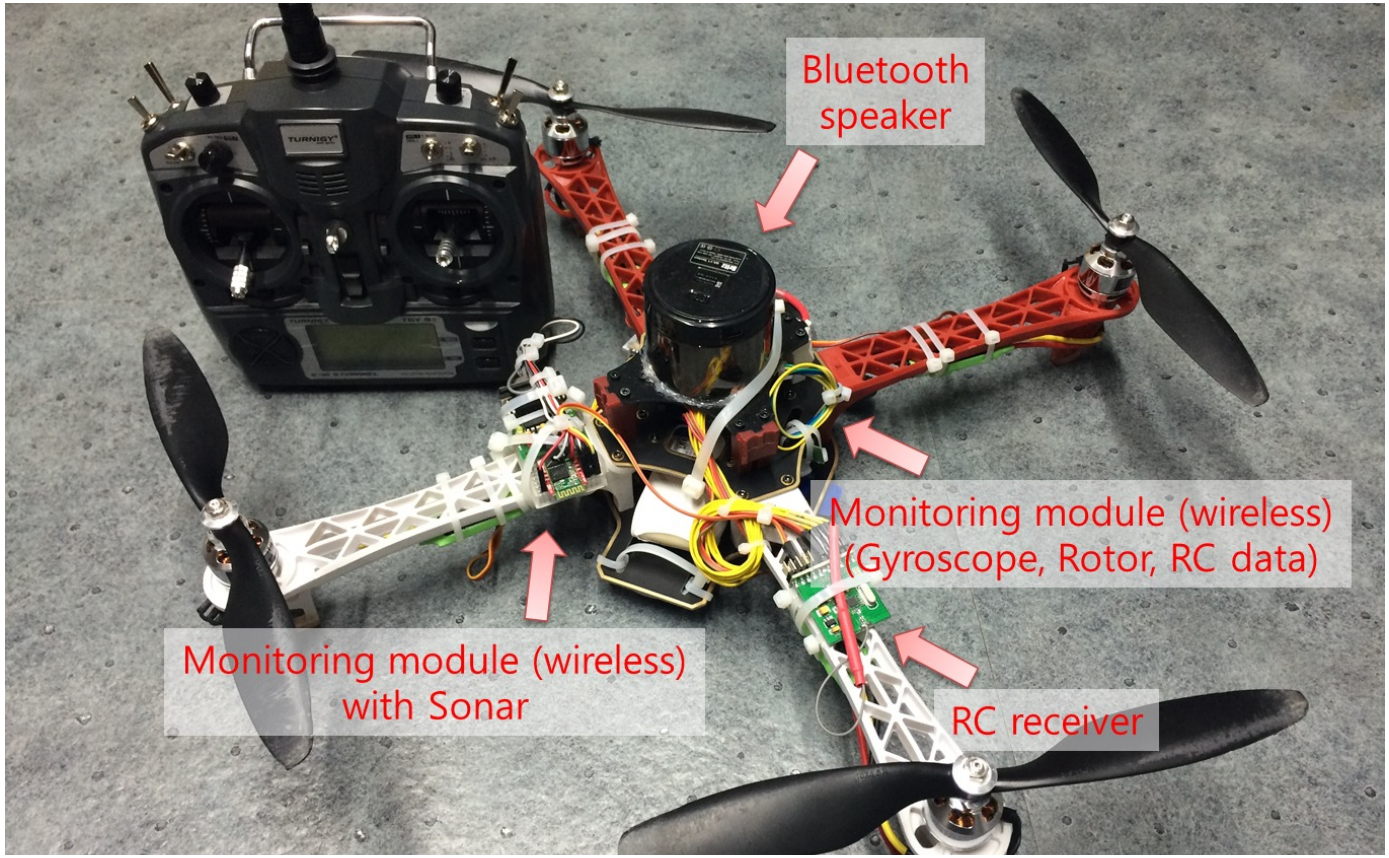

Sound source
Micro-phone
Arduino
Gyro-scope
Sound Pressure Level = 85~95 dB
(The sound level of noisy factory or heavy truck)

Experimental Results

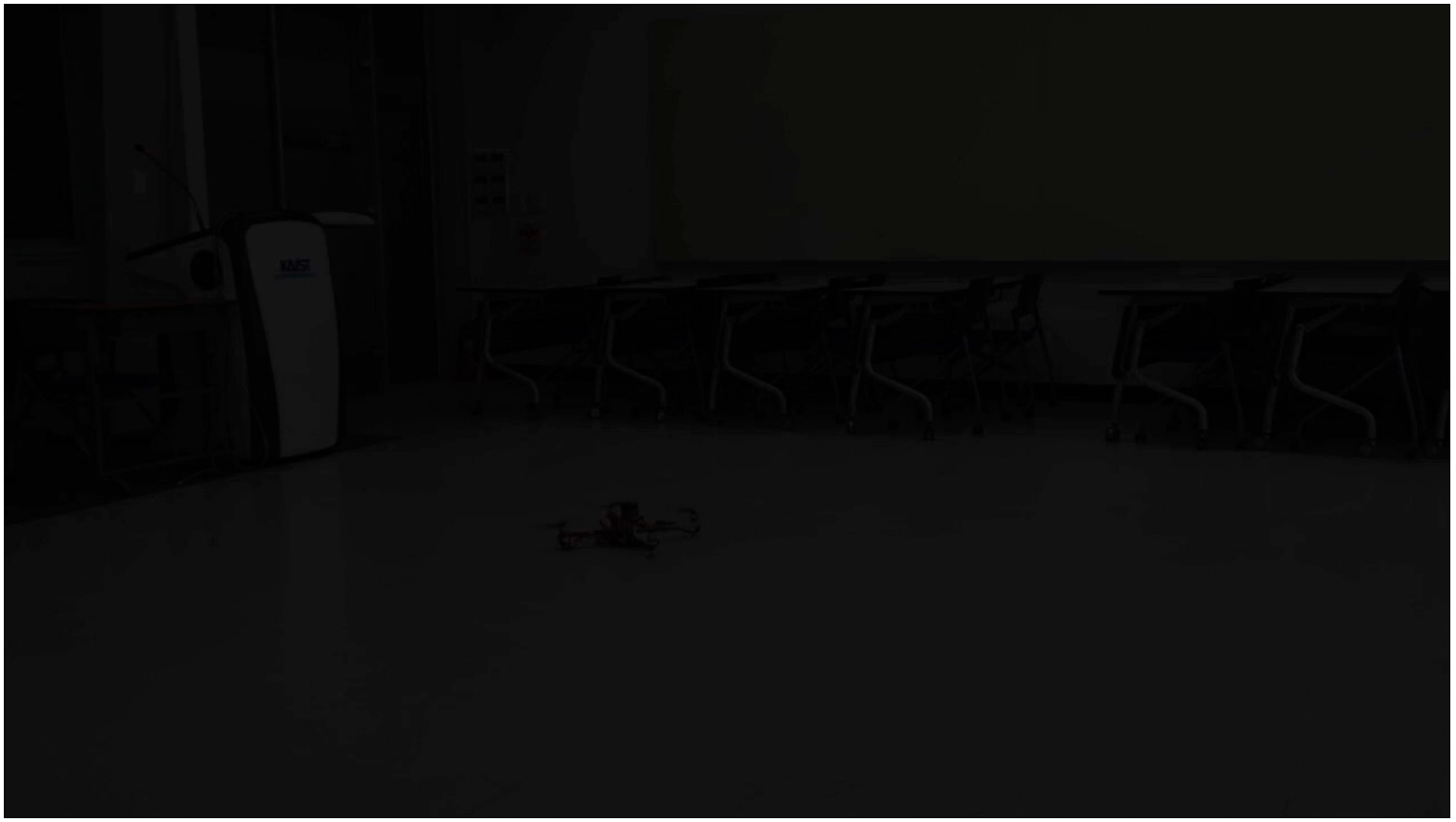
- ❖ Found the resonant frequencies of **7 MEMS gyroscopes**
- ❖ Not found for 8 MEMS gyroscopes

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)

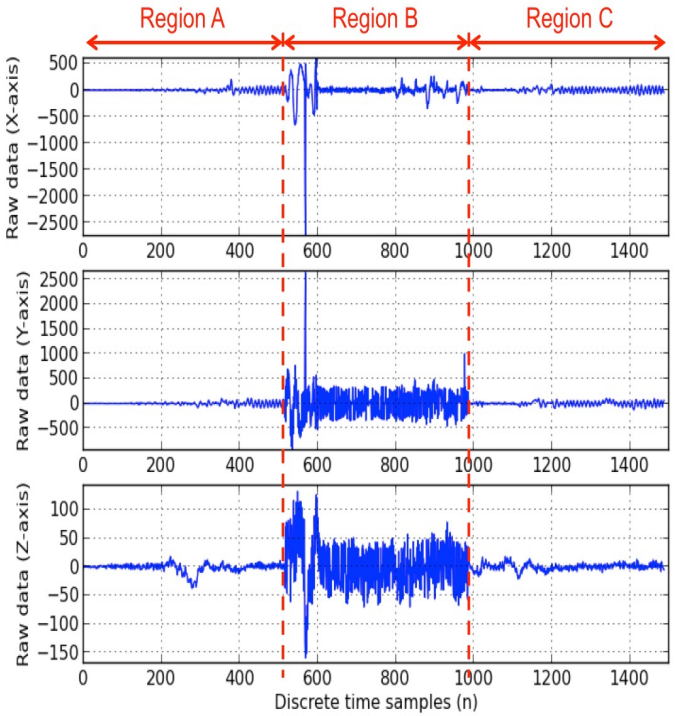
Attack Demo


Bluetooth speaker
Monitoring module (wireless) (Gyroscope, Rotor, RC data)
Monitoring module (wireless) with Sonar
RC receiver

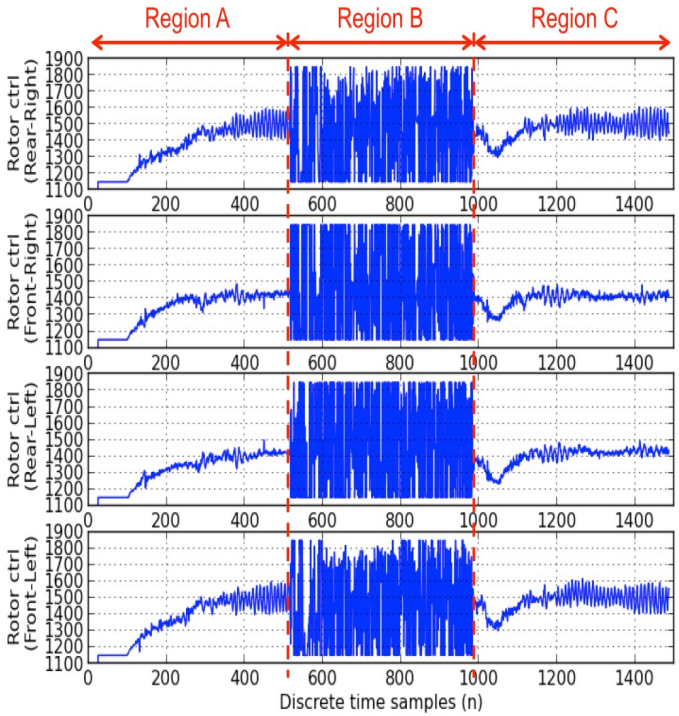
Rocking Drone Experiments



Test Results



Raw data samples of the gyroscope



Rotor control data samples

Remote Experiments

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

<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

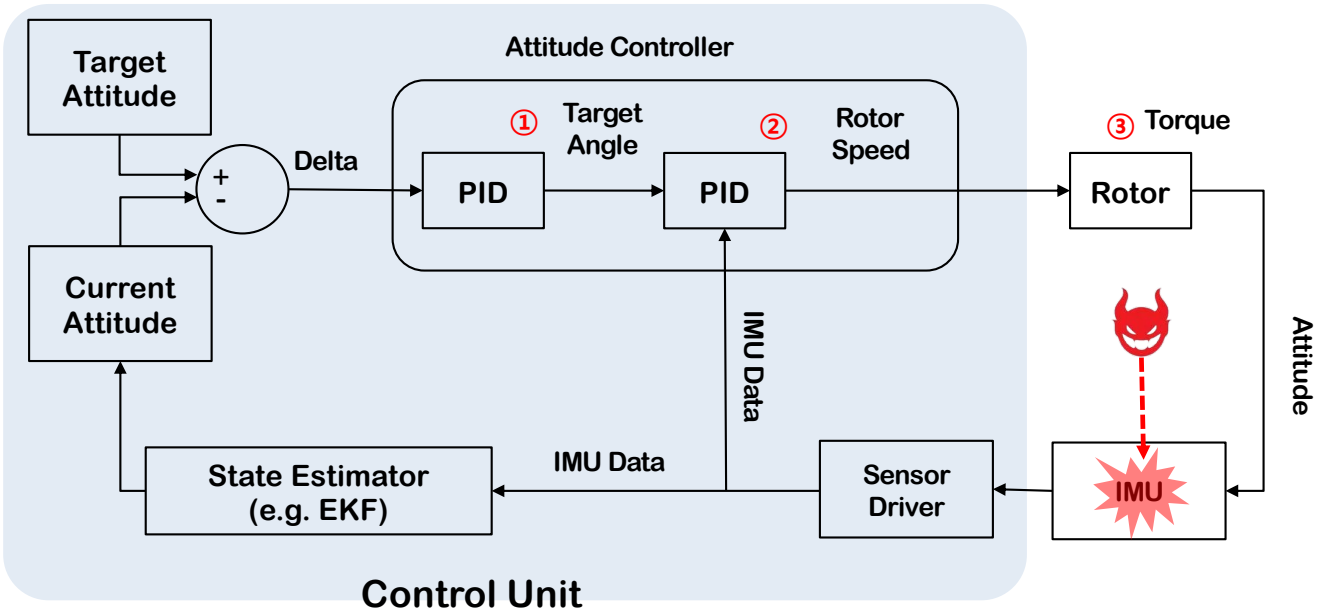
(http://www.lradx.com/wp-content/uploads/2015/05/LRAD_Datasheet_450XL.pdf)

Anti-Drone Technologies

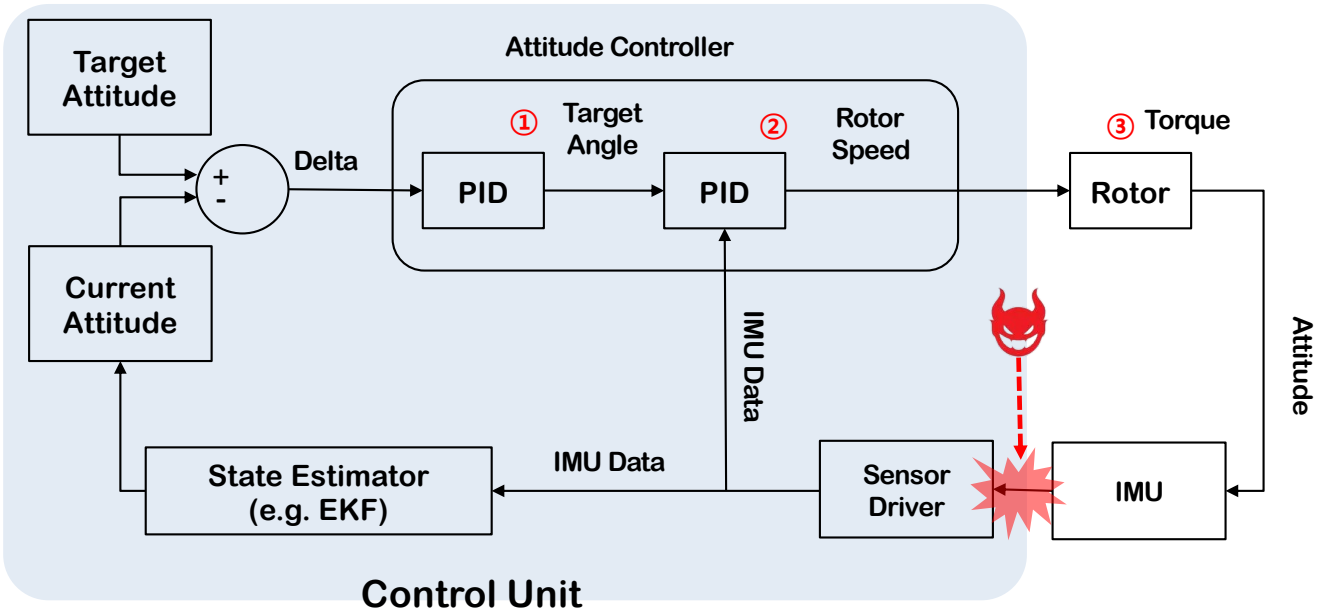
Type	Technology	Strength	Weakness	Response Time
Physical	Machine Gun,	Cost	Accuracy, Collateral damage	≈ 0
	Net, Colliding Drone	Cost	Accuracy, Reload	<10 sec
	Sound	Swarm attack	Distance, Power, Bypass, Aiming	<10 sec
	High-power laser	Accuracy, Distance	Response time, Cost, Swarm	>10 sec
Electro-magnetic	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

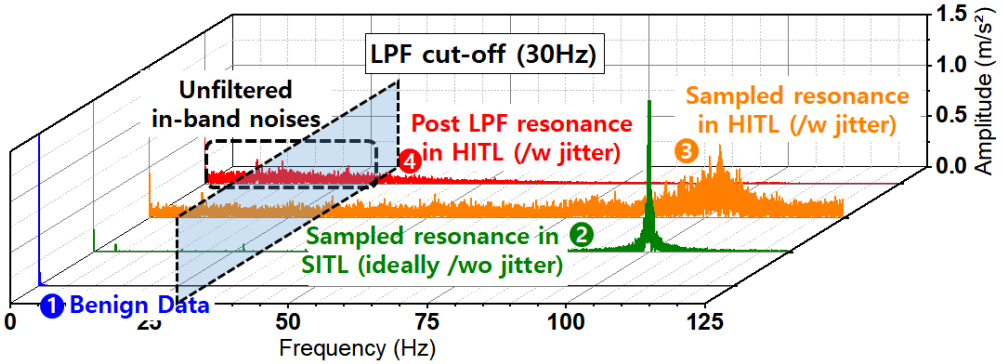
- Arms race in Ukraine: anti-drone vs. counter-anti-drone

- What attacks should be in scope?
- RL under adversarial environment?

- “Perception and identification” is also very important.

Best Questions

- Seunghyun Lee: Would this be mitigated with a low-pass filter in between the MEMS gyroscope output and flight control software?
  - Un-Rocking Drones: Foundations of Acoustic Injection Attacks and Recovery Thereof, Jinseob Jeong et al, NDSS'23



- Dongok Kim: will it be possible to adopt a visual sensor attack targeting the visual sensor of an autonomous driving system?
- Suhwhan Jeong: Can other components of drones could be affected due to their resonant frequency?

Good Questions

- Using Bluetooth seems too expensive as an attack vector?
- Could an attacker aim sound noise at a target drone?
- Are there other benefits when the attack frequency is ‘audible’?
- Is there any software based defense method for this attack?
- Are other MEMS sensors like accelerometers and barometers also vulnerable?
- Can this attack affect other sensors causing a critical problem?
- How did real-world drones overcome this attack?
- Are there any alternatives than MEMS gyroscopes?
- Is the attack more powerful than attacks using EMI injection?
- Is an attack possible even for a fibre optic gyroscope?
- Even with physical isolation, is this attack still possible?
- Will it self-attack due to the noise generated by their propellers during operation?

Questions?

- Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google "Yongdae Kim"

Ministry of Science and ICT
IITP Institute of Information & Communications Technology Planning & Evaluation
경찰청 KOREAN NATIONAL POLICE AGENCY
SAMSUNG