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

SysSec Lab.

- System Security Lab. @ KAIST, Korea
  - Prof. Yongdae Kim
  - Electrical Engineering & Information Security

- Research areas: Hacking Emerging Technologies such as IoT, Drone, Blockchain, Medical device, Automobiles, Critical Infra, Cellular, …
  - Software vulnerability (hacking)
  - Physical cyber system security (sensor, hardware Trojan, …)
  - Wireless communication security (Bluetooth, Zigbee, …)
  - Mobile network security (privacy, abuse, …)

Yongdae Kim

FOLLOW

Professor of Electrical Engineering, KAIST, Korea
Verified email at kaist.ac.kr - Homepage

Security Distributed Systems Networks Privacy

Cited by		VIEW ALL
	All	Since 2018
Citations	9625	3620
h-index	52	33
i10-index	103	69

Drones in Ukraine War

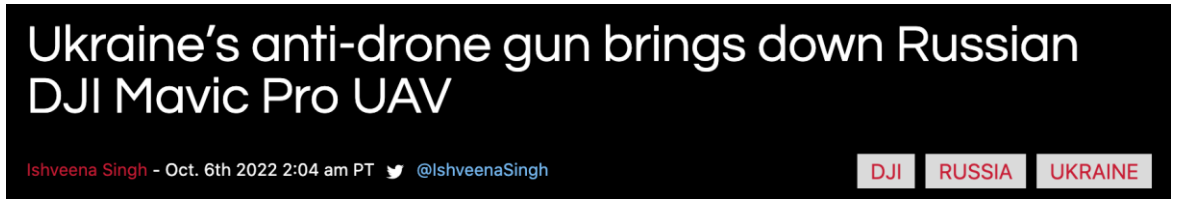
Chinese drone firm DJI pauses operations in Russia and Ukraine 04/2022

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

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

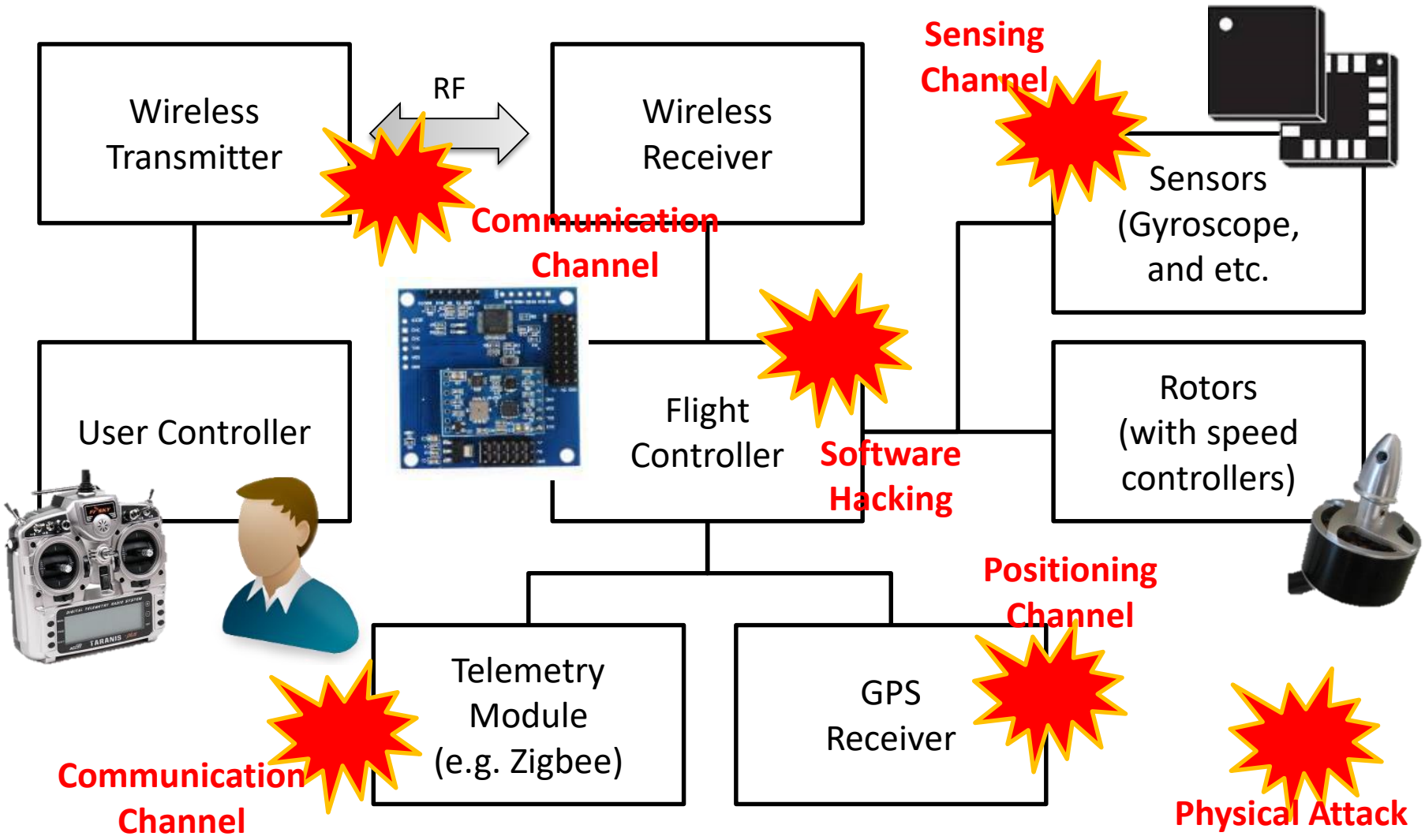
MAY 13, 2022 JARON SCHNEIDER

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

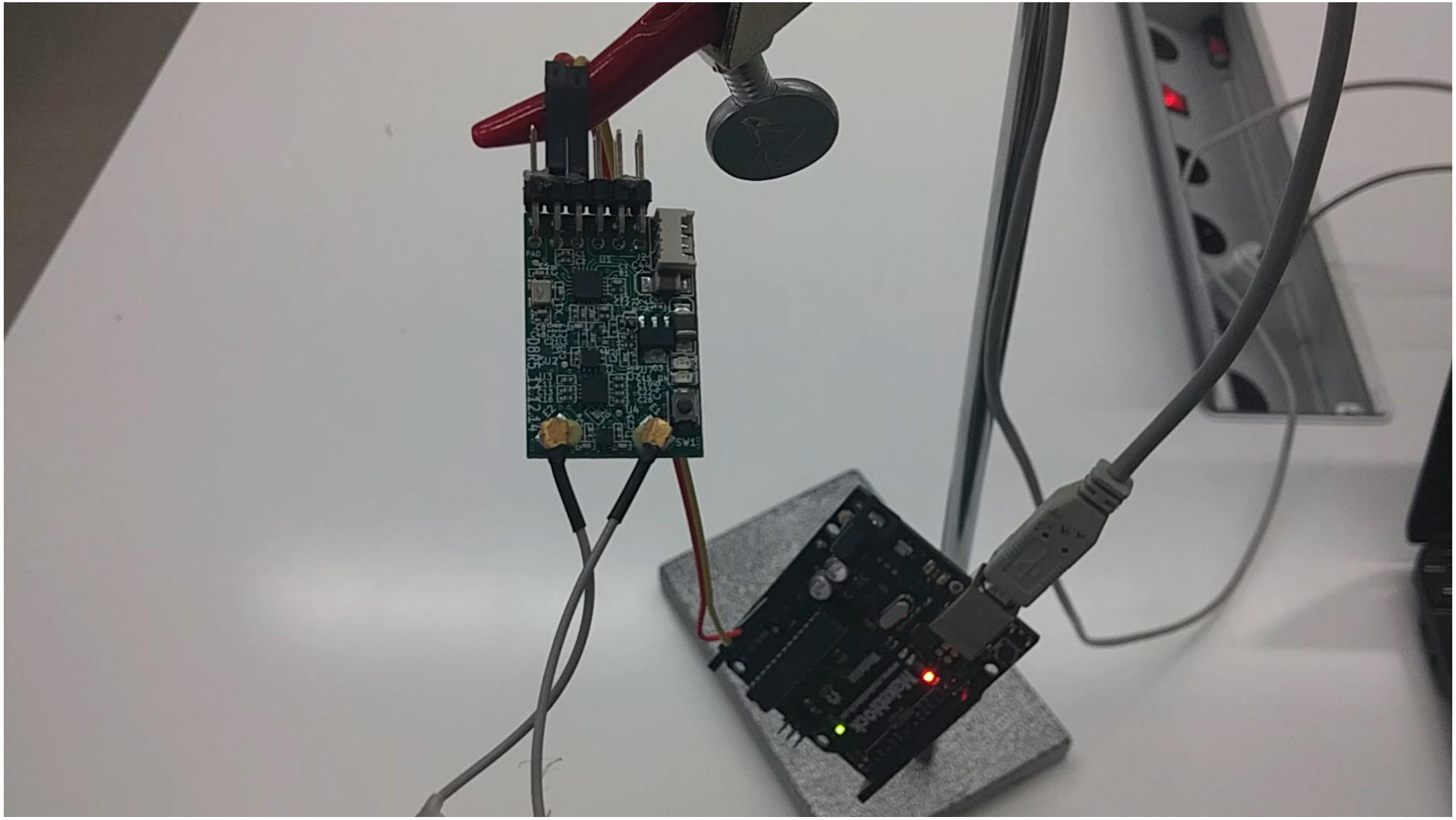
Drone Controller

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

Transmitter

Receiver

Reactive jamming test



Positioning Channel

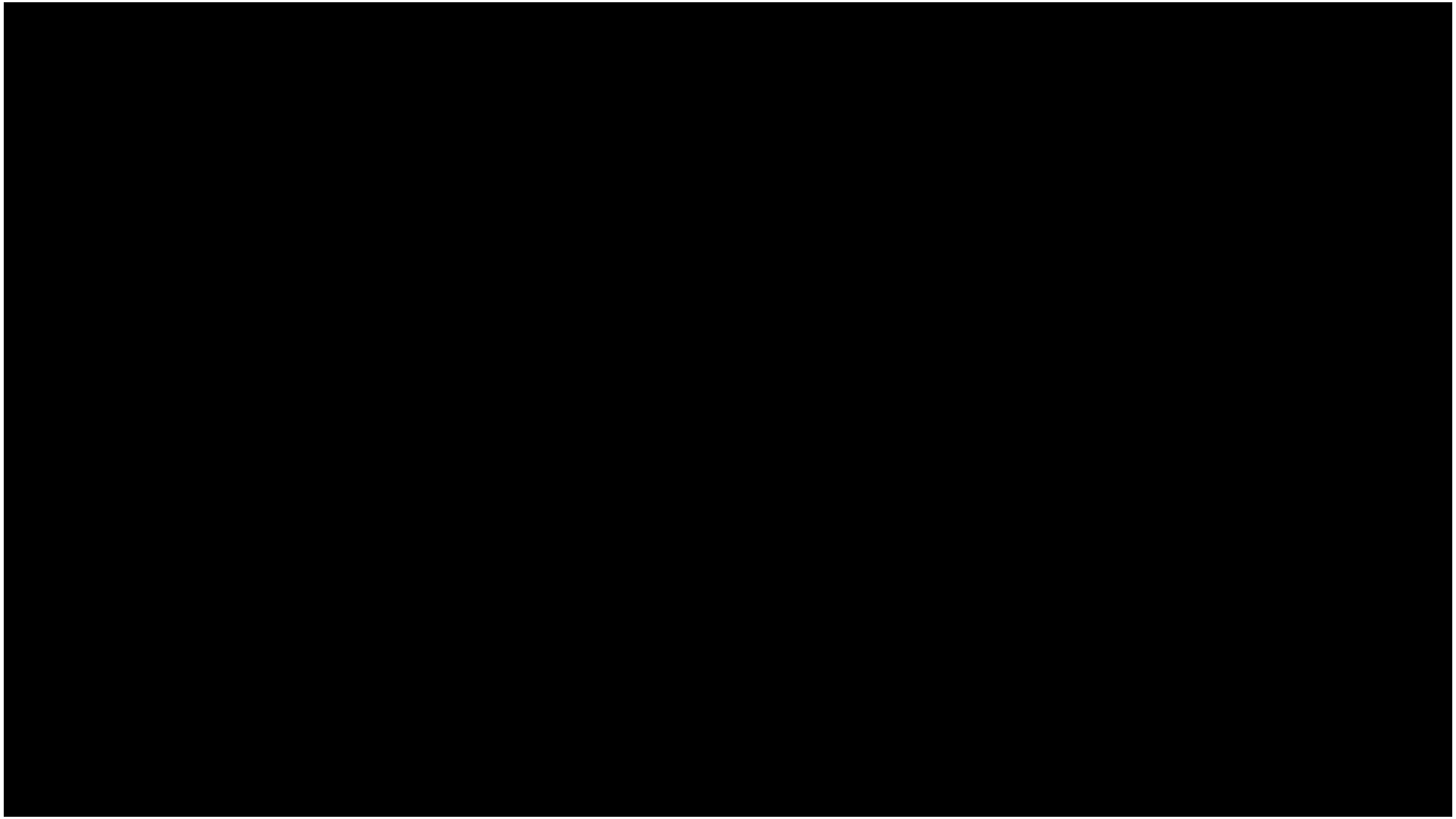
GNSS (GPS) Spoofing and Jamming

- 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)

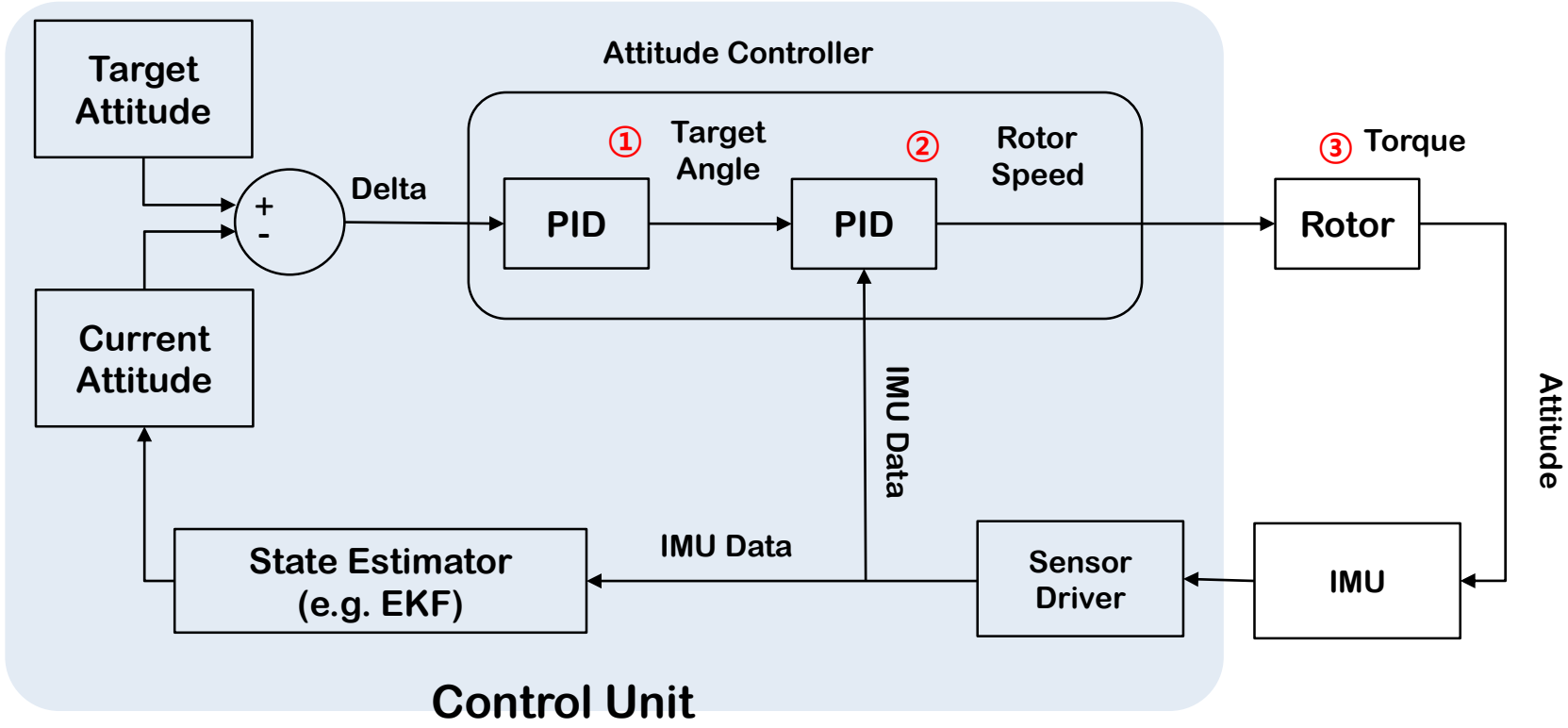
Hard GPS spoofing + Failsafe Bypass



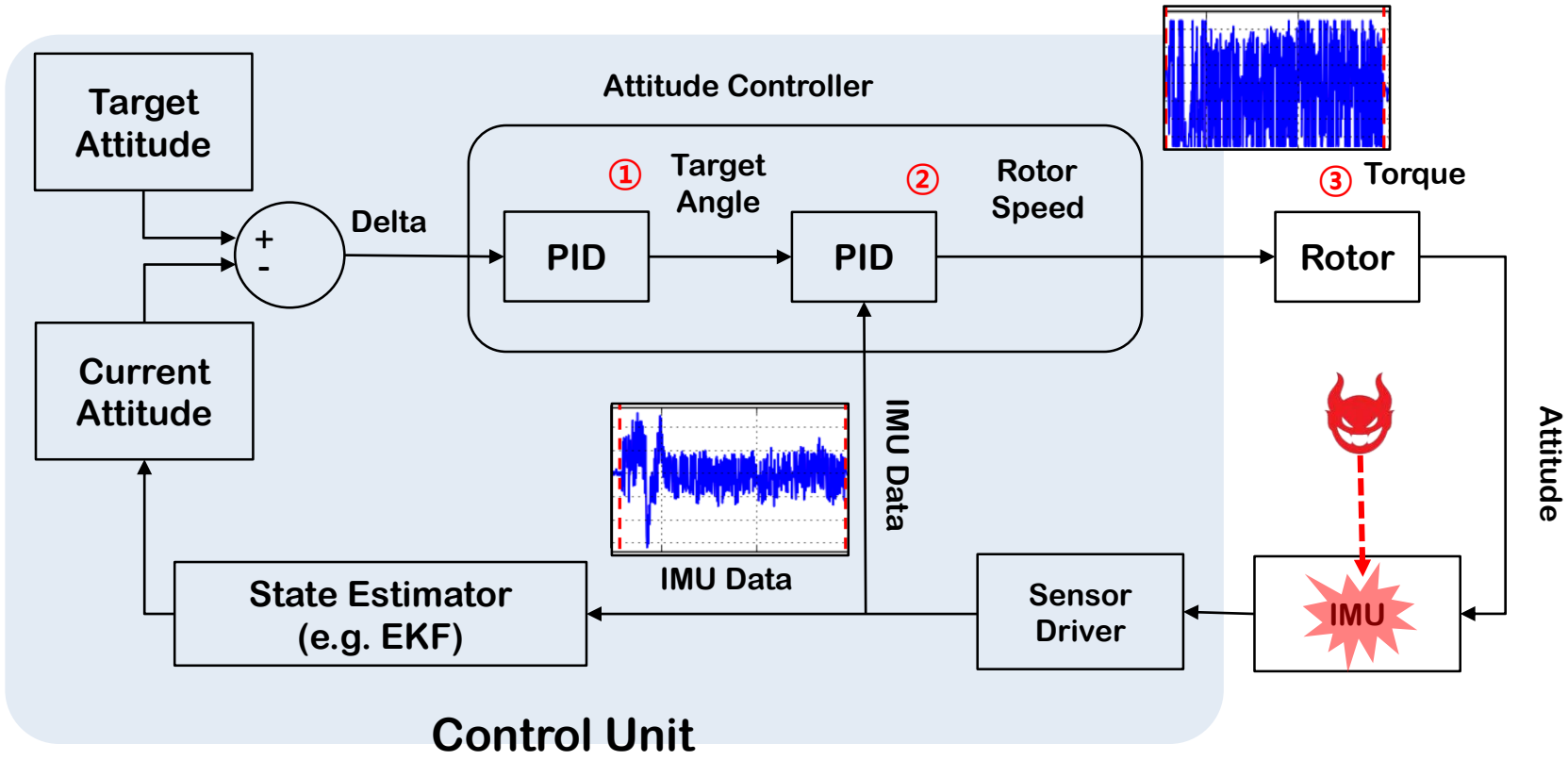
Soft GPS Spoofing

Sensing Channel

How Drone Control Works

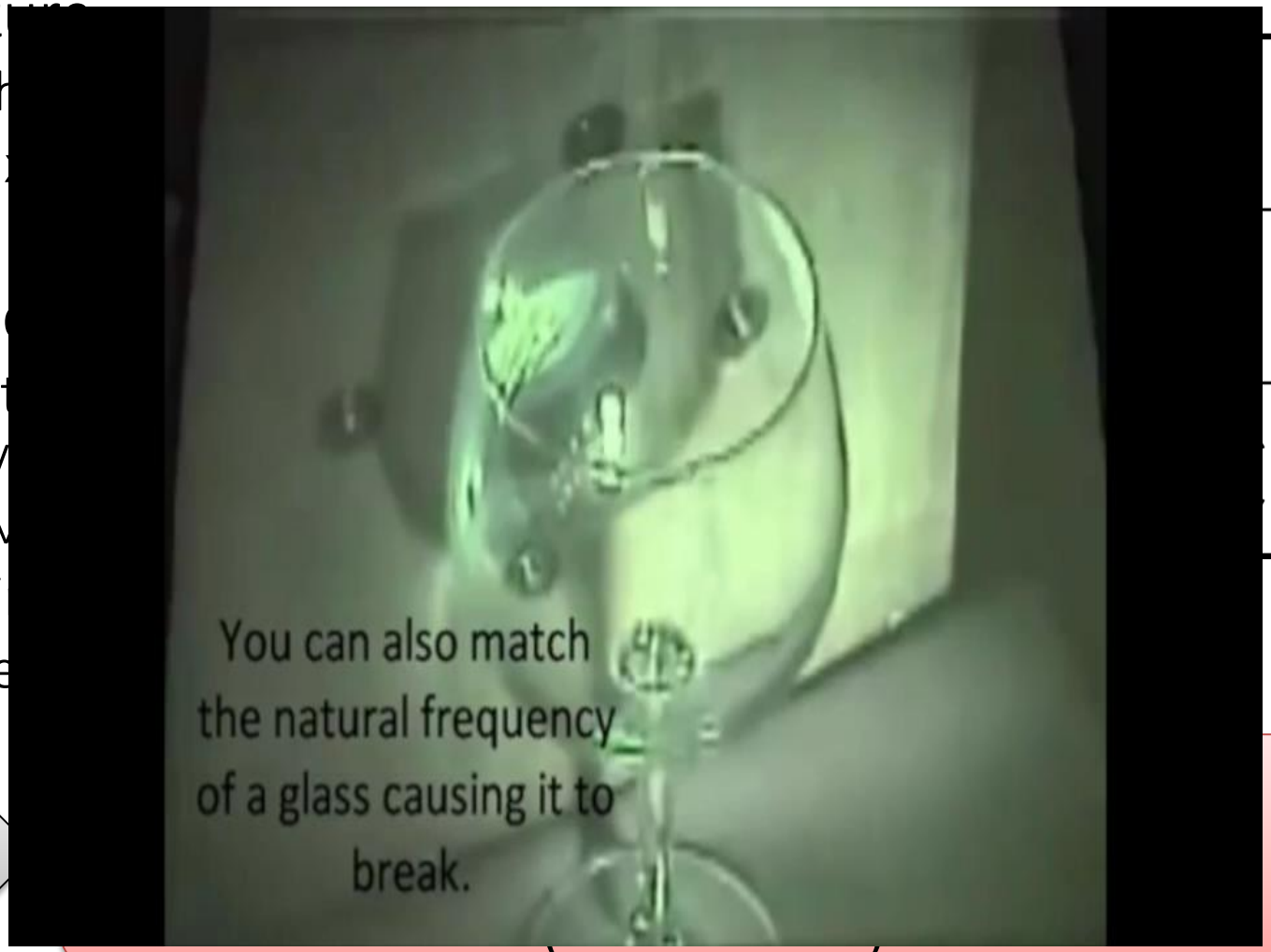


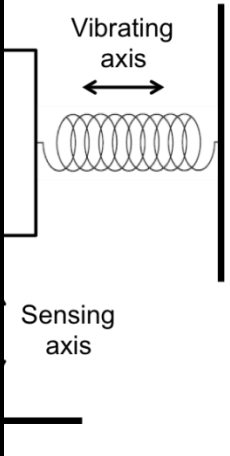
How Rocking Drone Control Works



MEMS Gyro. & Sound Noise

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

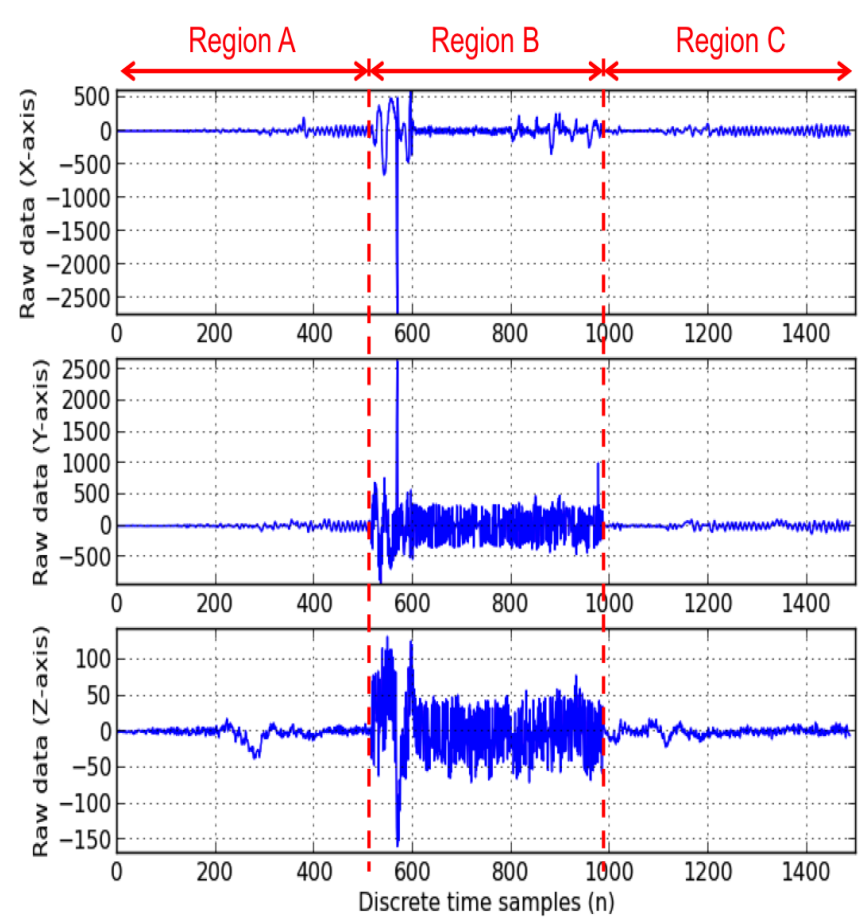




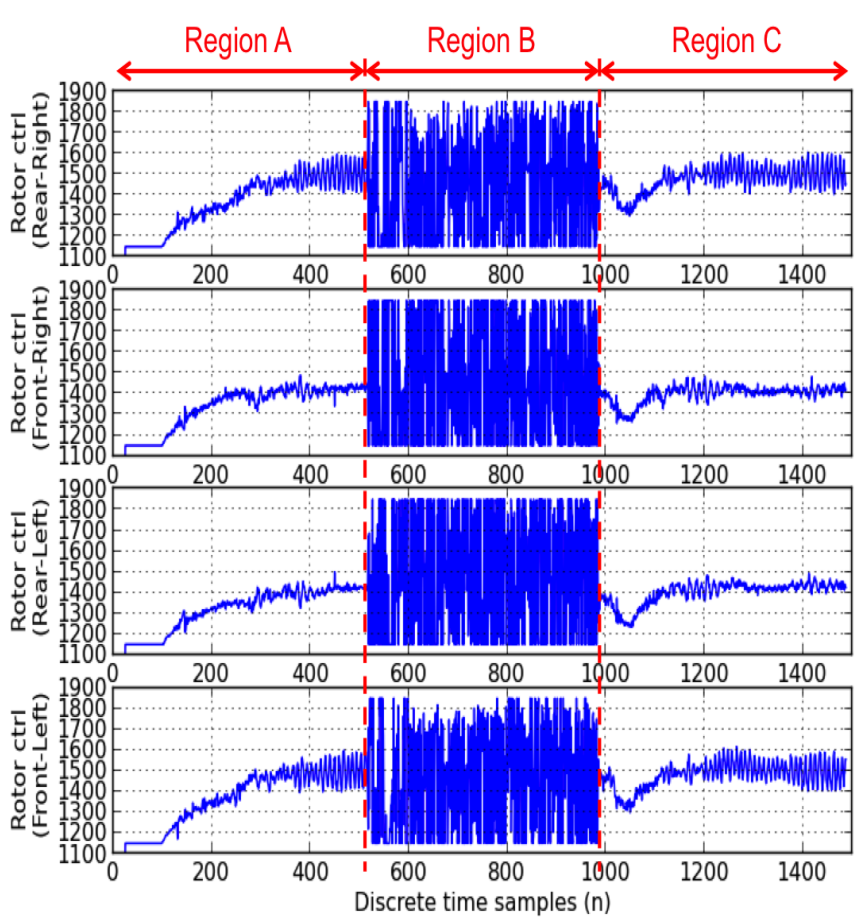
structure>

Rocking Drone Experiments

Test Results



Raw data samples of the gyroscope



Rotor control data samples

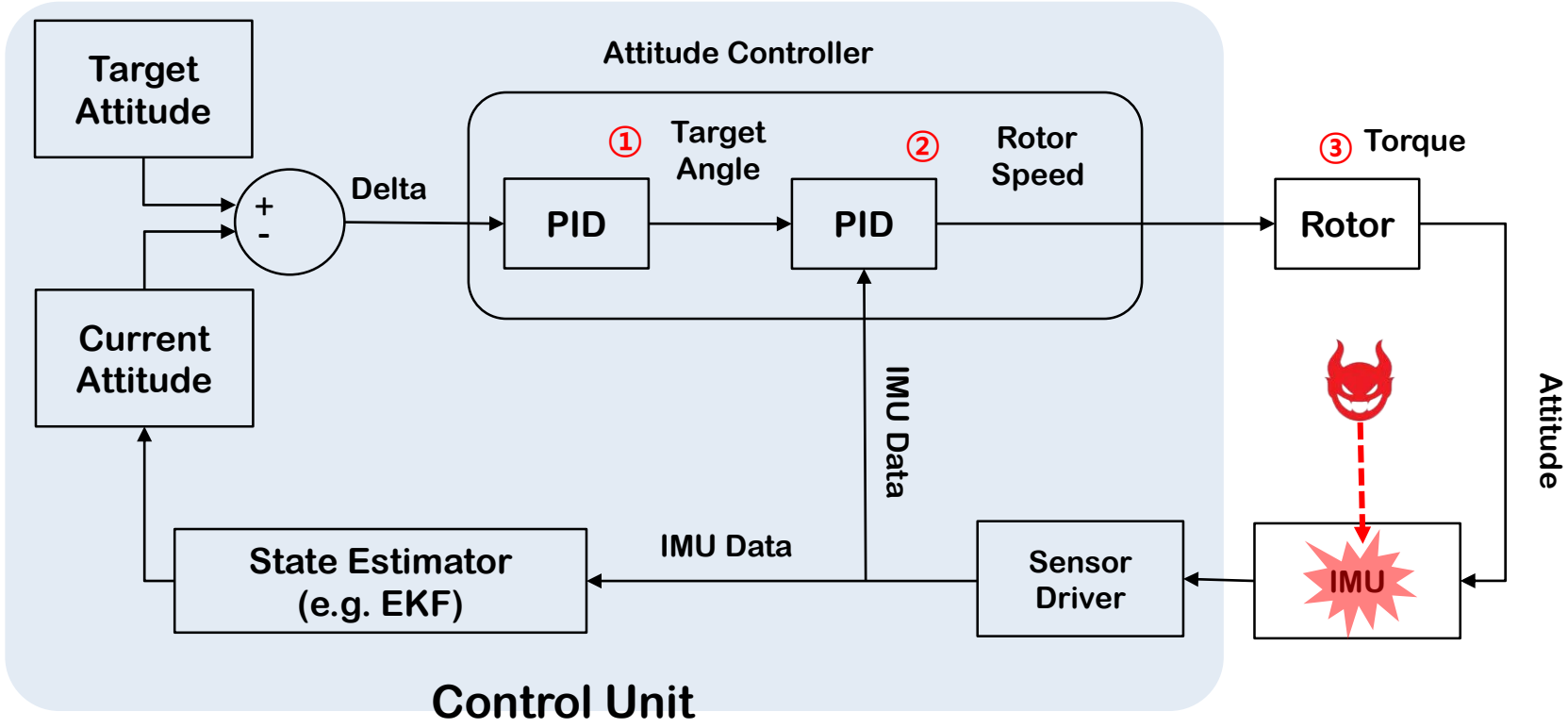
Remote Experiments

Anti-Drone Technologies

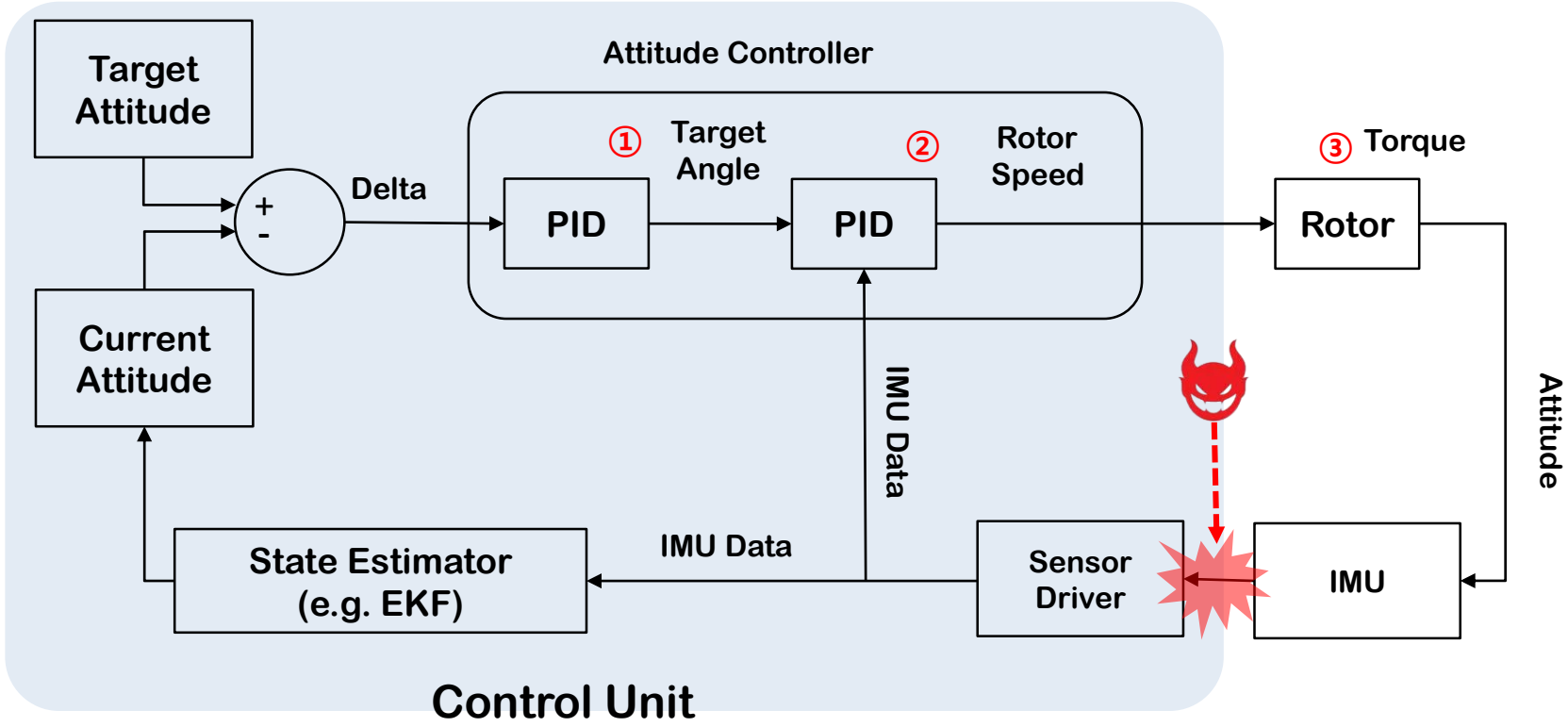
Type	Technology	Strength	Weakness	Response Time
Physical	Machine Gun,	Cost	Accuracy, Collateral damage	≈ 0
	Net, Colliding Drone	Cost	Accuracy, Reload	<10 sec
	Sound	Swarm attack	Distance, Power, Bypass, Aiming	<10 sec
	High-power laser	Accuracy, Distance	Response time, Cost, Swarm	>10 sec
Electro-magnetic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

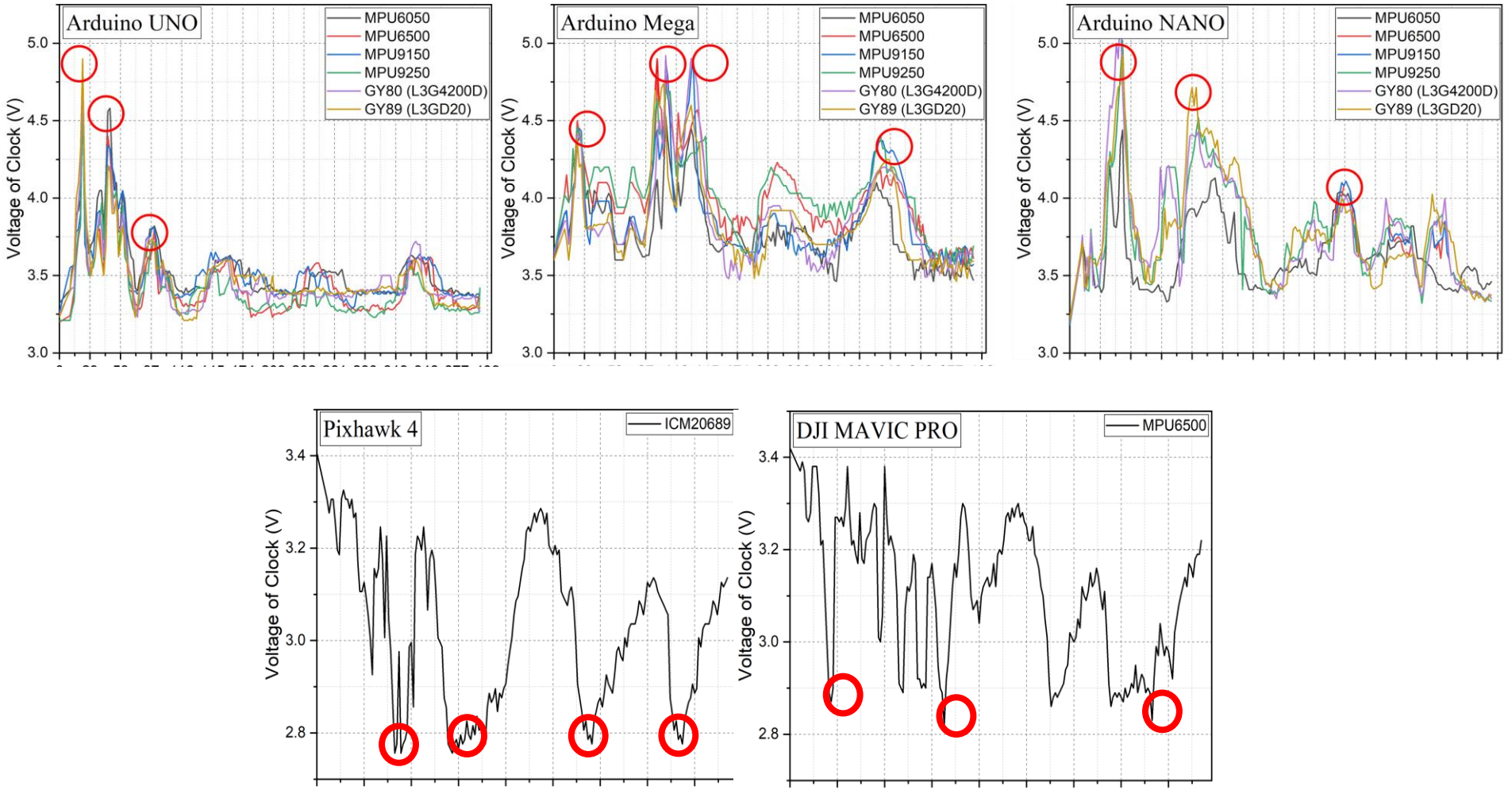


Paralyzing Drone: Control System



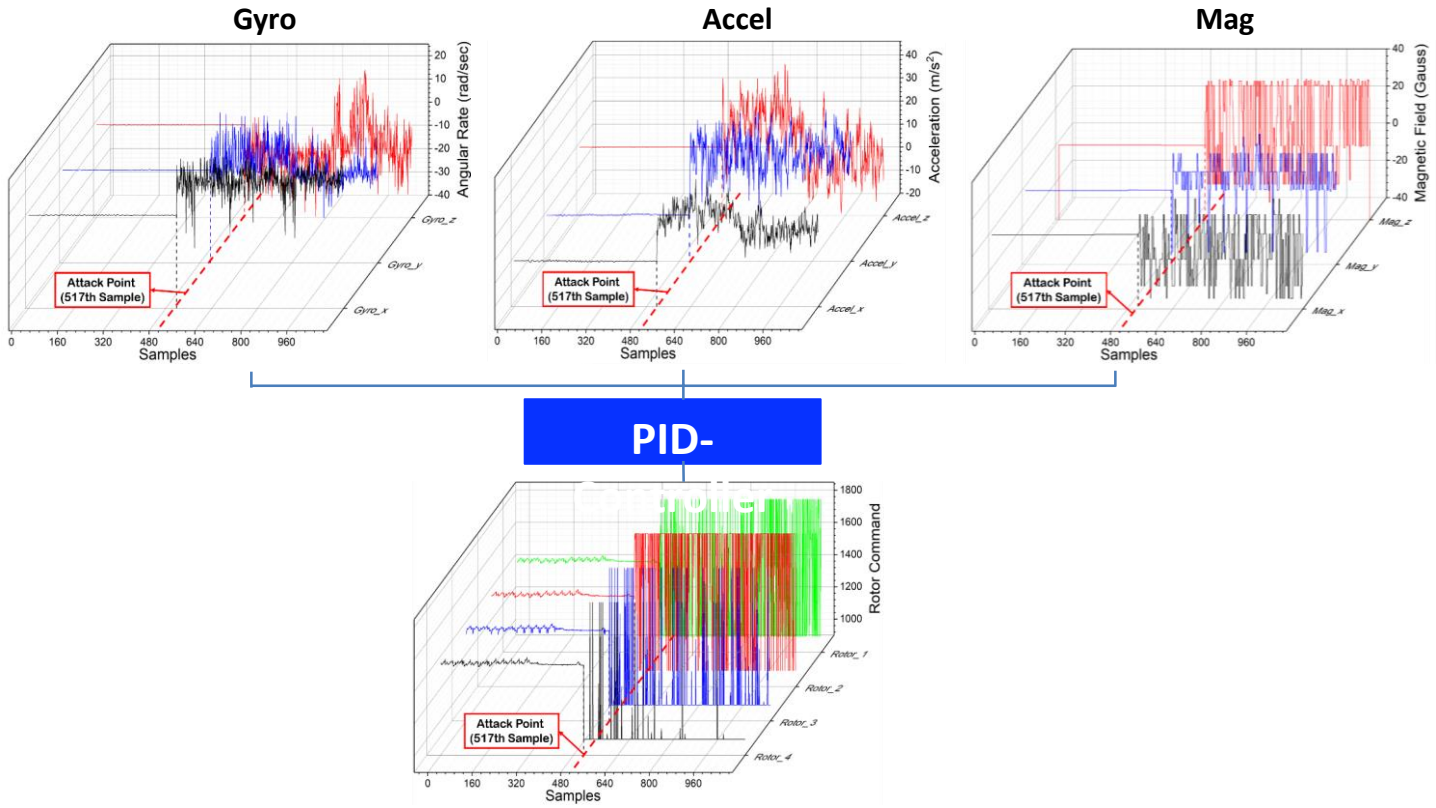
Paralyzing Drone: Experiments

Finding Attack Frequencies

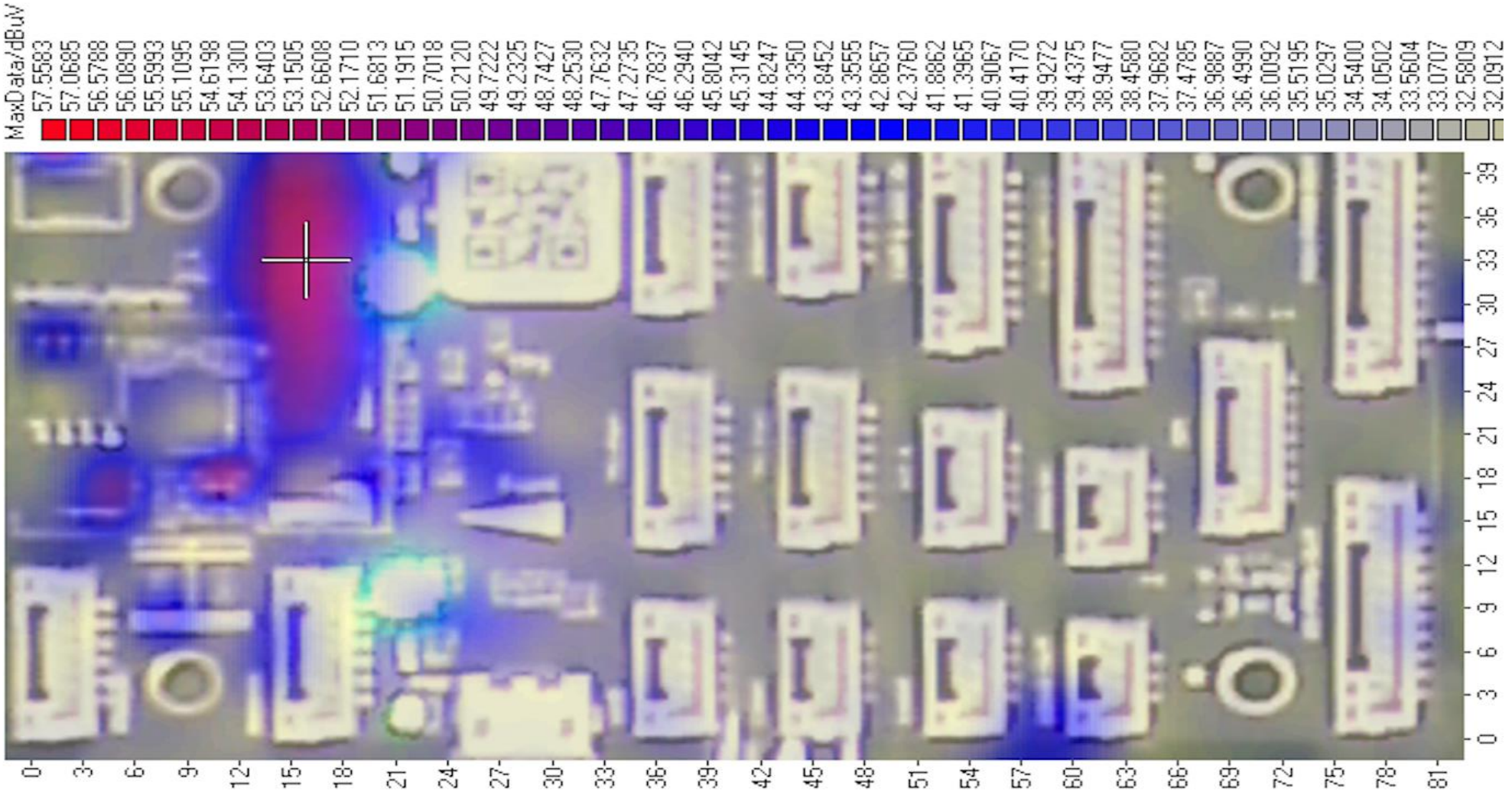


Paralyzing Drone: Targeted Injection

Paralyzing Drone: Response Time



EM Leakage Measurement



Paralyzing Drone

- Attack frequency depends on mainboard ➔ Swarming drone
- Narrow attack frequency ➔ Minimize collateral damage, energy-efficient
- Immediate response ➔ Impossible to detect and response

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.

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