

Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels

Joonha Jang*, **Mangi Cho***, Jaehoon Kim, Dongkwan Kim, and Yongdae Kim

Syssec@KAIST

Drone



Military

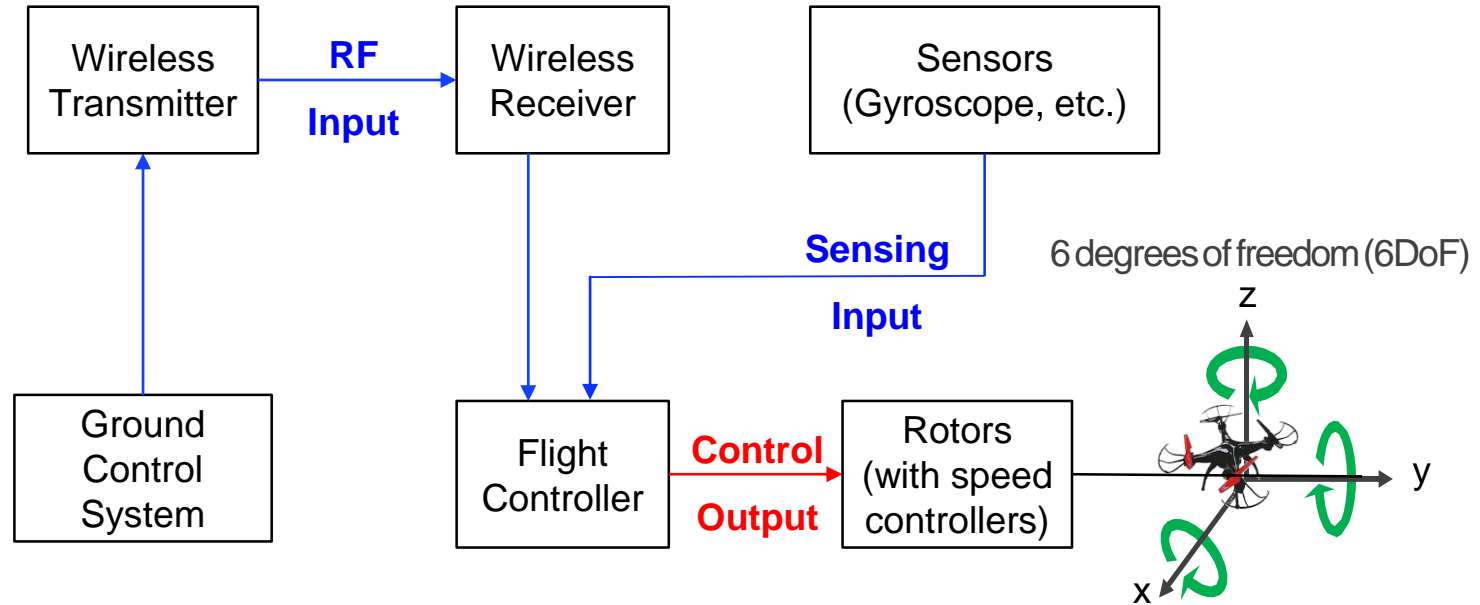
Transport

Reconnaissance

Delivery

Fire fighting

Drone system



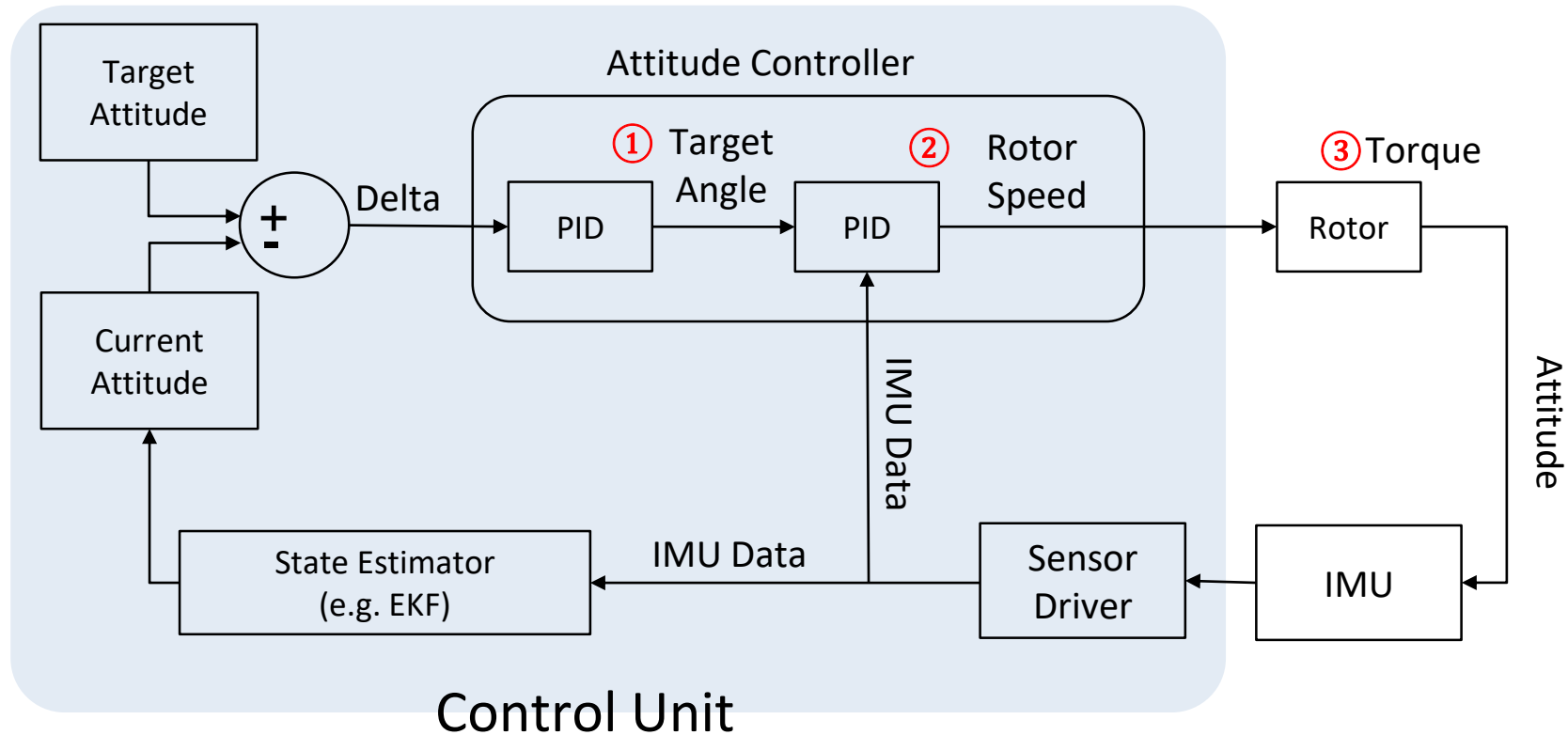
Drone Neutralization Technologies

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	

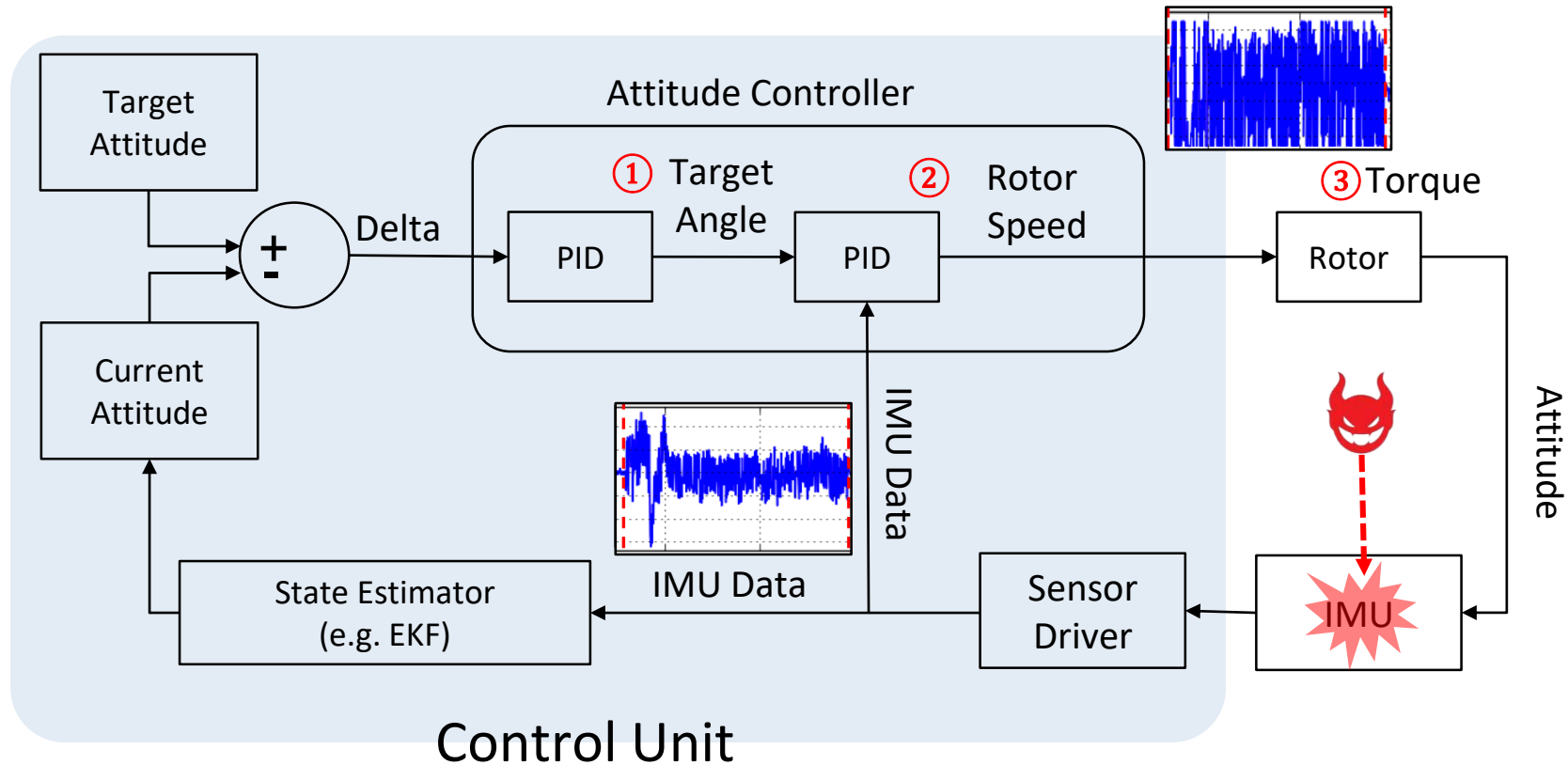
Previous Work: Rocking Drone [Usenix'15]

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	

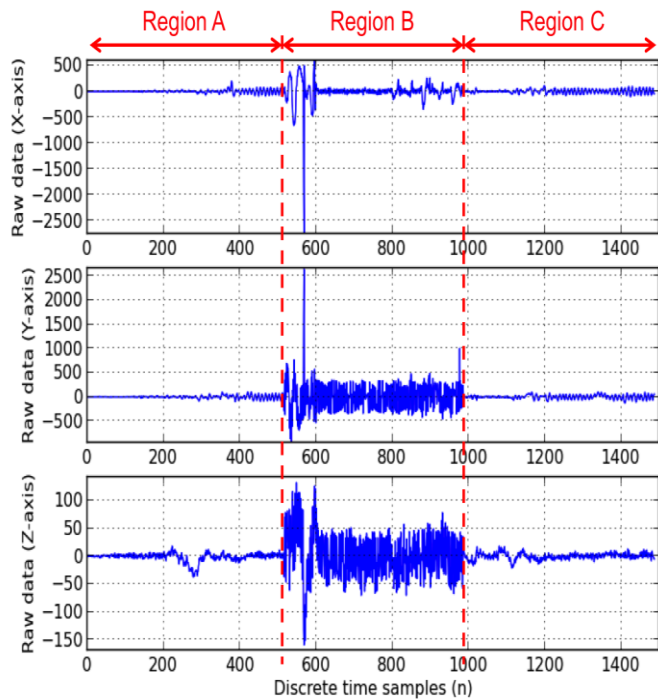
How Drone Control Works



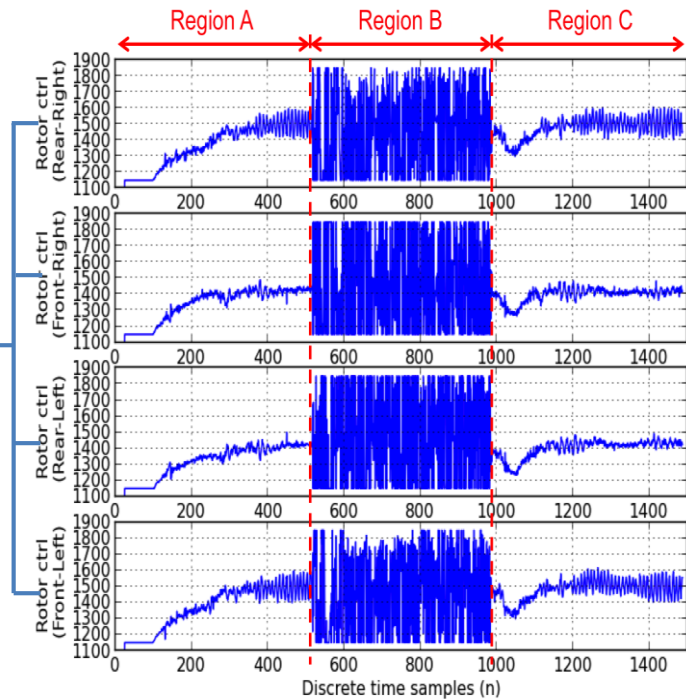
How Rocking Drone Control Works



Rocking Drone Attack Results



PID- Controller



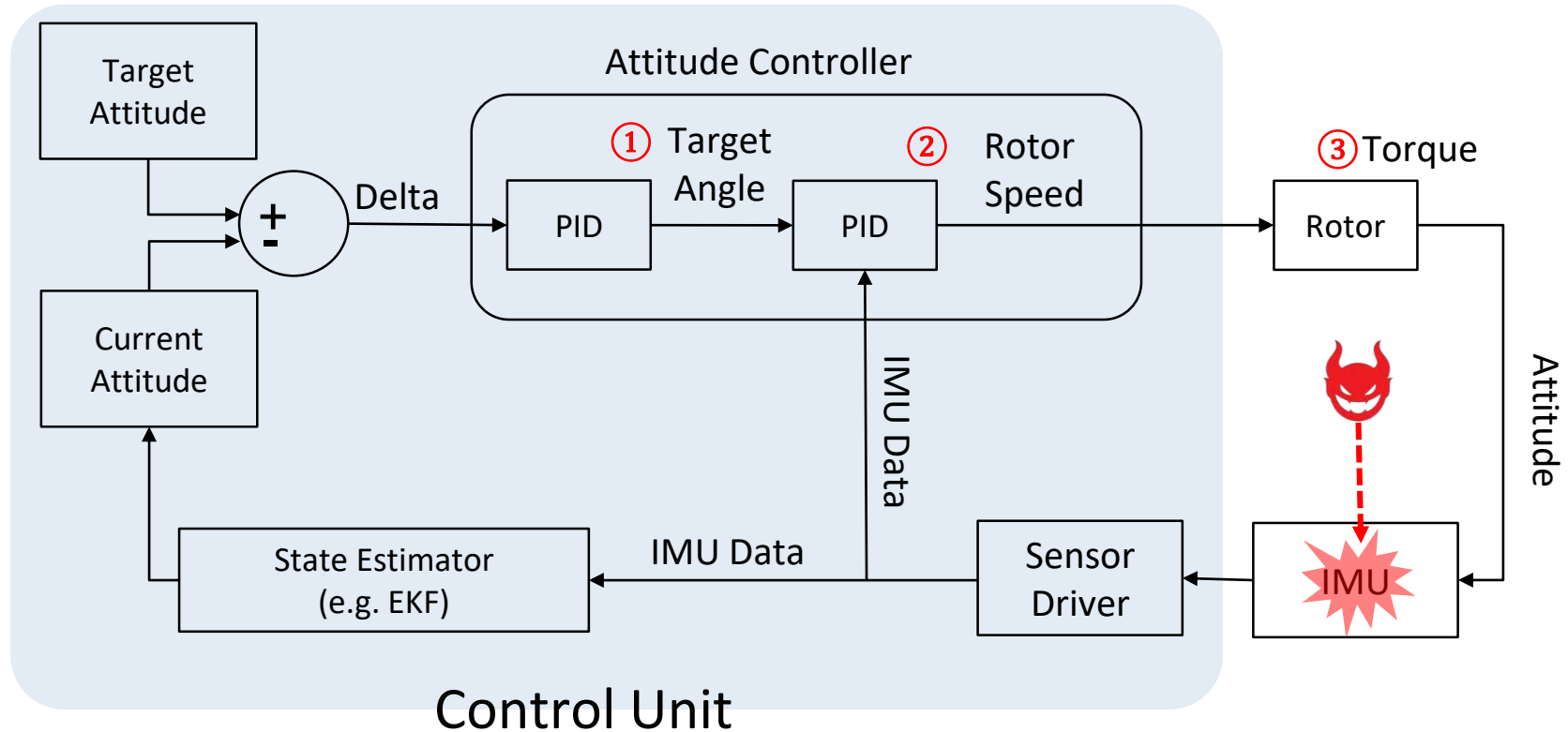
Raw data samples of the gyroscope

Rotor control data samples

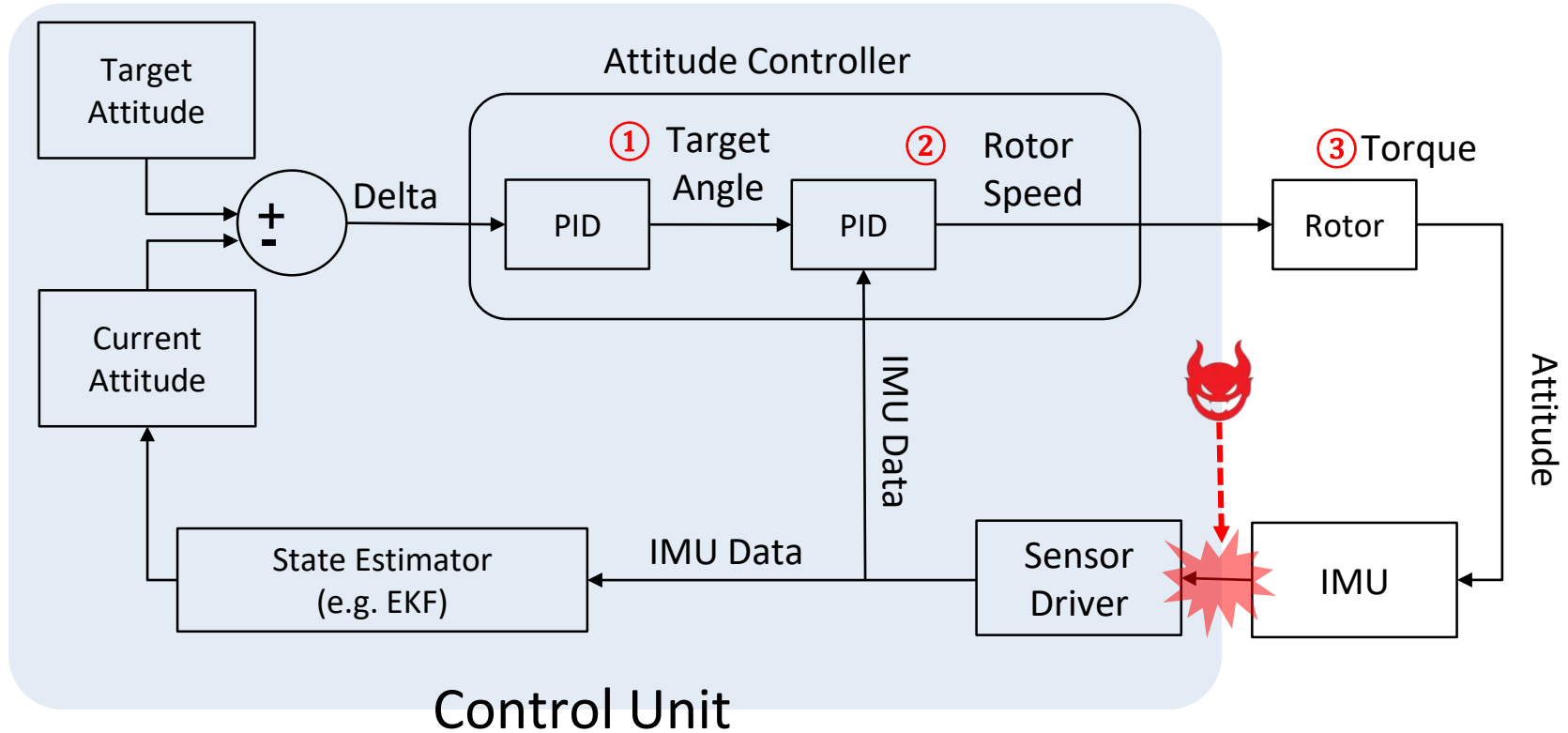
Paralyzing Drones with EMI Attack

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	

Rocking Drone: Control System Perspective



Paralyzing Drone: Control System Perspective



Q1. Distorting Communication Channel?

**Disrupting
Original Signal**

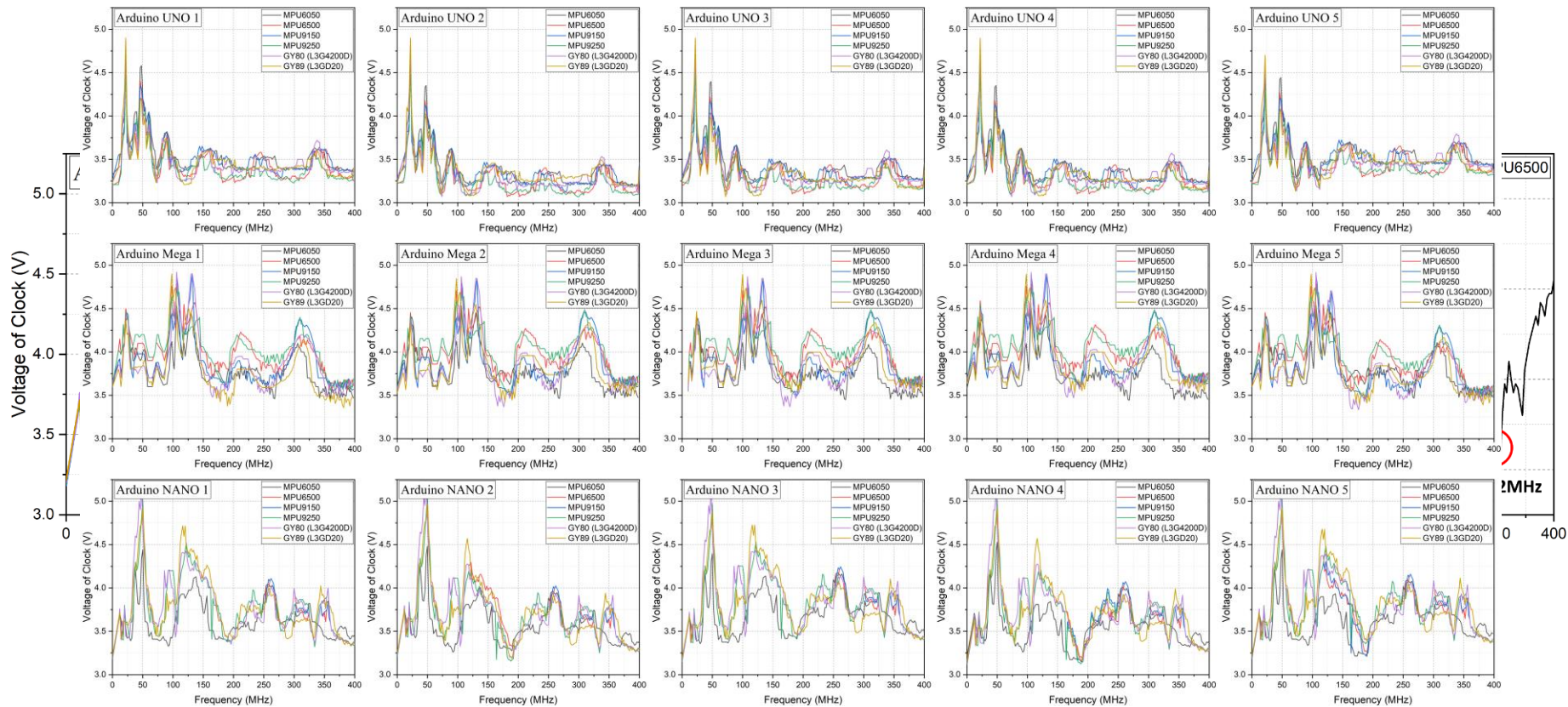
Q2. Remote disturbance possible?

**Experiments With
EM Injection**

Q3. Remote injection possible for drone?

**EM injection experiment
On hovering Drone**

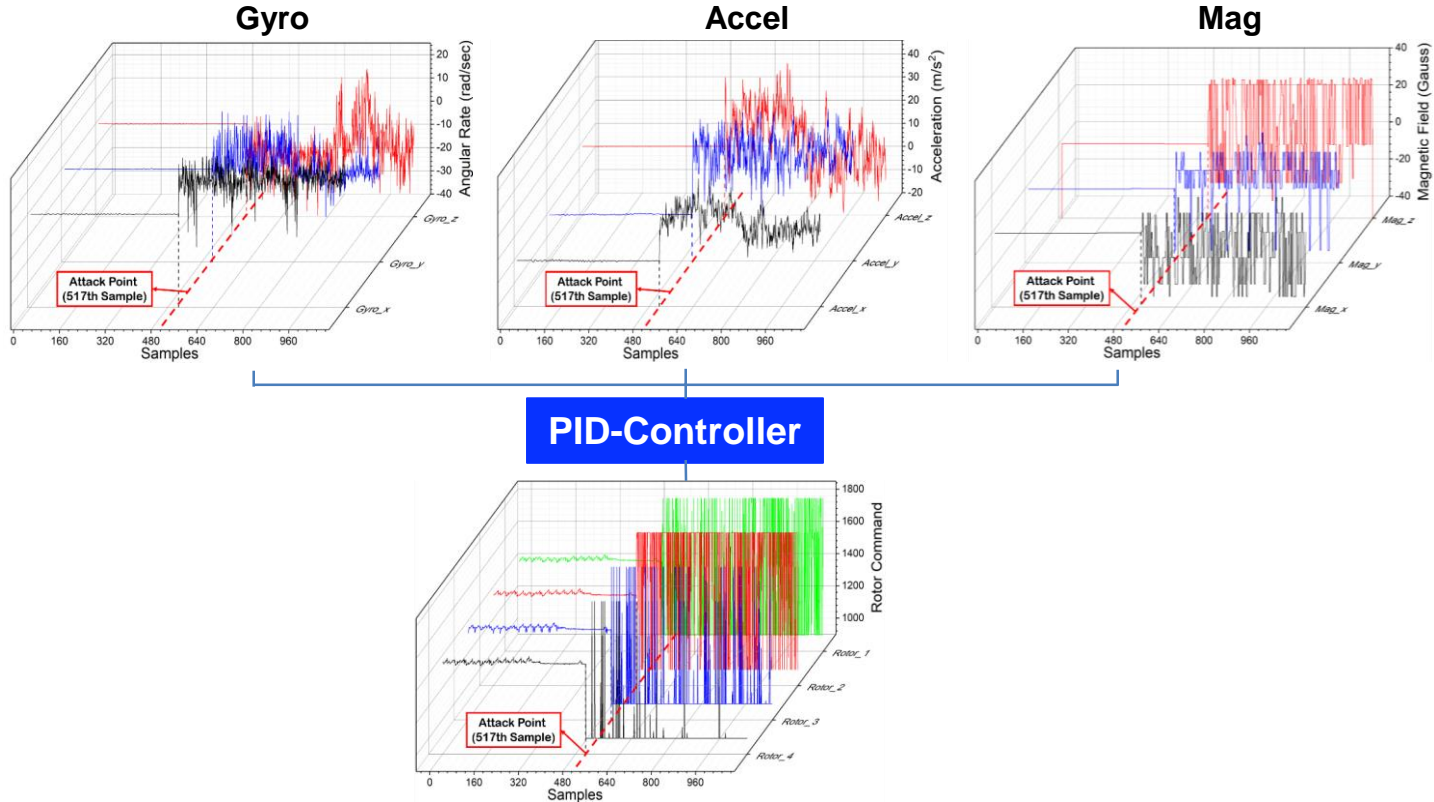
Q4. Attack Frequency?



Q4. Attack Frequency?

Targeted EMI injection Experiment

Q5. Response time?



Q6. POE & Shielding?

**Shielding Evaluation
IMU & Wire**

Conclusion

- ❖ Advantages of Paralyzing Drones
 - The attack frequency is determined by the main board → Swarming
 - Very narrow frequency → lesser collateral damage, lesser power
 - Within a single sampling time → no time for detect and recovery

- ❖ Future work (commercialize)
 - Analysis of countermeasures
 - Analysis with more drones
 - Analysis for more efficient and effective EMI injection

Thank you!

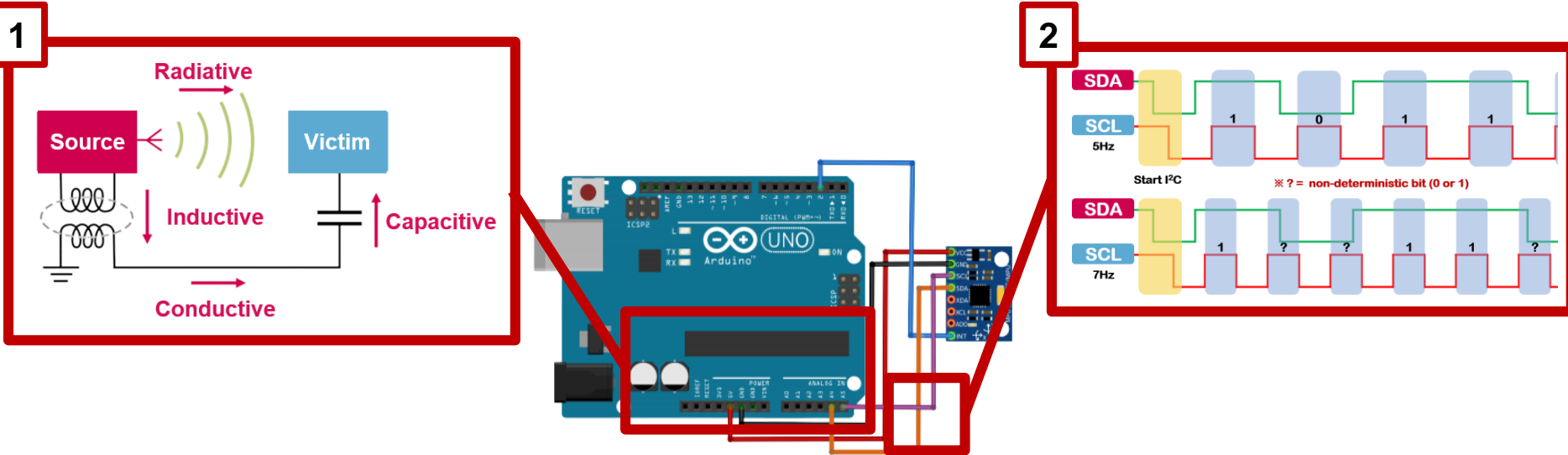
Joonha Jang (cyber040946@kaist.ac.kr)

Mangi Cho (mgcho0608@kaist.ac.kr)

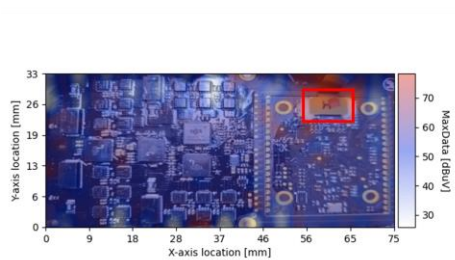
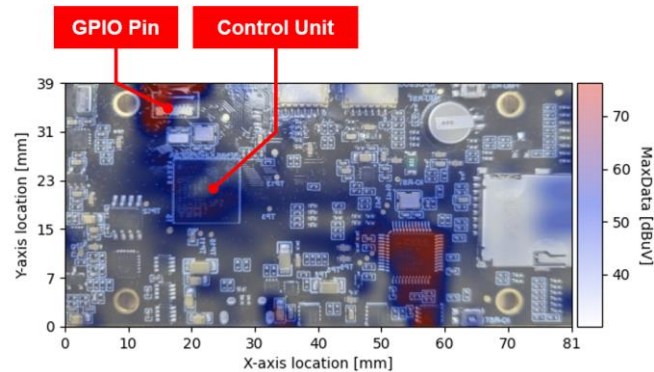
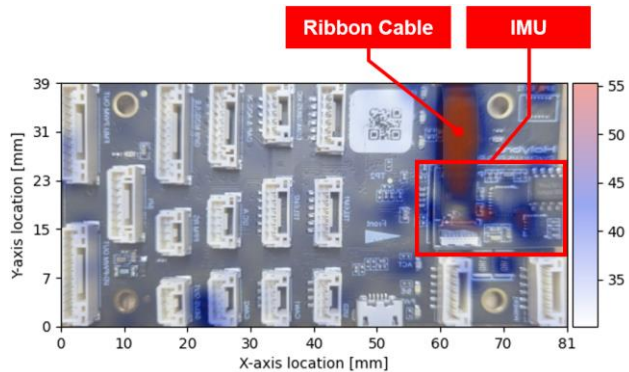
<https://sites.google.com/view/paralyzing-drones-via-emi>

How is this Working

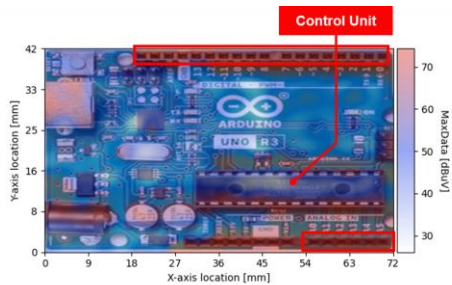
1. Back door EMI coupling(Radiative) on Control unit
2. Signal distortion in the digital signal of the communication channels between the IMU and control unit.



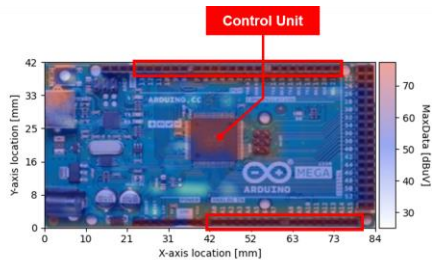
POE (Point of Entry)



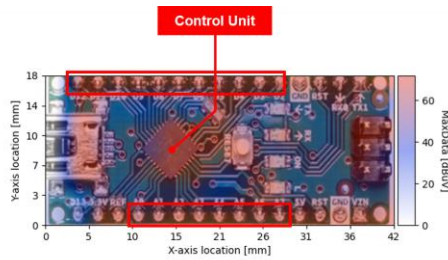
DJI Mavic Pro



Arduino UNO

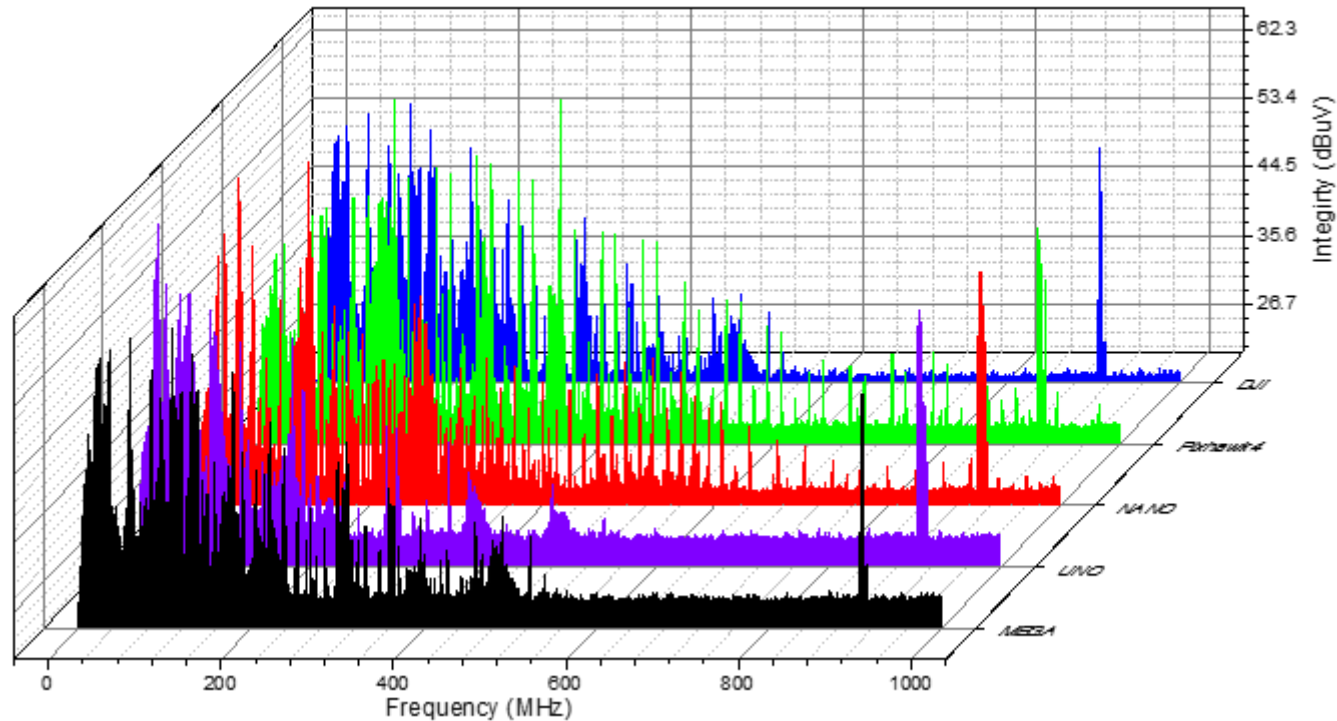


Arduino Mega

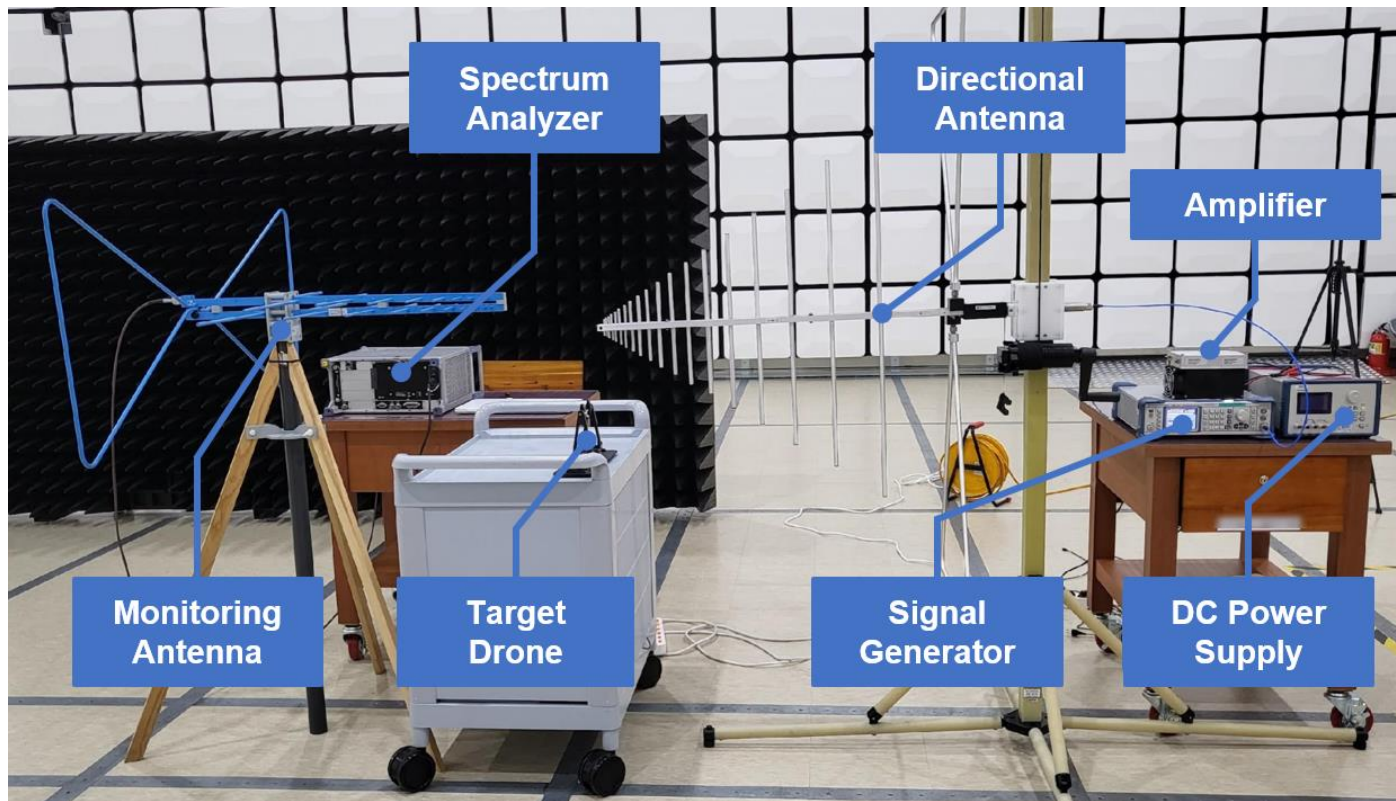


Arduino NANO

POE (Point of Entry)



Experiment Setup



Q6. Countermeasure?

