Anti Drone 기술

- 현재와 미래 -

Yongdae Kim

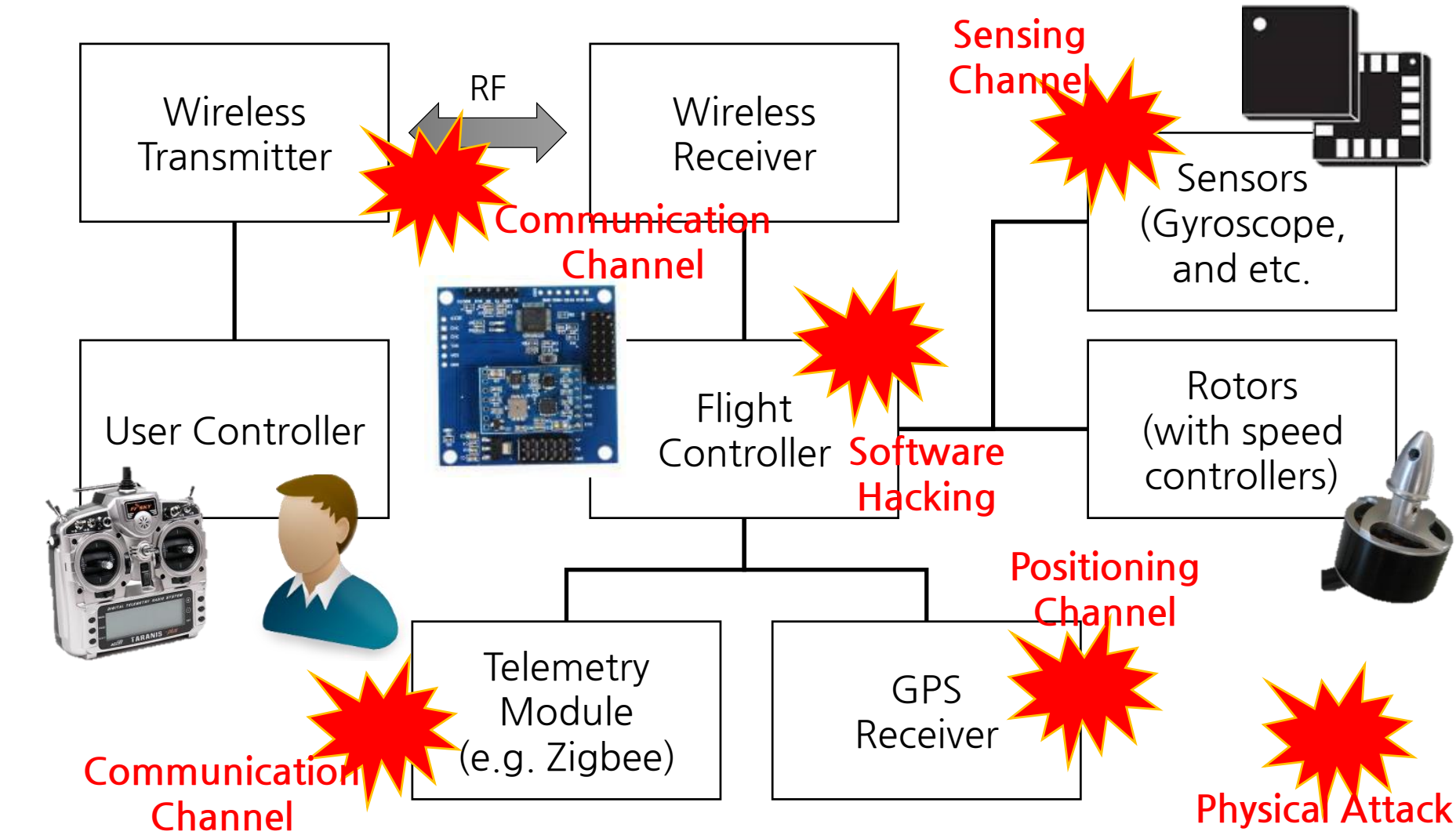
KAIST

Syssec Lab.

Drones (Multicoptors)

- Distribution delivery
- Search and rescue
- Aerial photography
- **Security and terrorism**
- Private hobby

Drone System & Attack Vectors



Motivation

Heathrow airport: Drone sighting halts departures

8 January 2019 Share

Gatwick drone shutdown

Departures at Heathrow were temporarily stopped after a drone was reported to have been sighted.

Flights from the west London airport resumed about an hour after police said a drone had been seen.

Update: 143 flights cancelled at Frankfurt Airport due to drone sighting

Archive photo shows a drone and an aeroplane. Photo: DPA

AFP/The Local
news@thelocal.de
@thelocalgermany

9 May 2019 | 08:34 CEST+02:00

Frankfurt airport was shut down for nearly an hour on Thursday morning as operators halted flights over a drone sighting, in the latest such incident affecting a busy European hub.

Attack

1. Communication Channel (Controller)

Typical Drone Controller

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

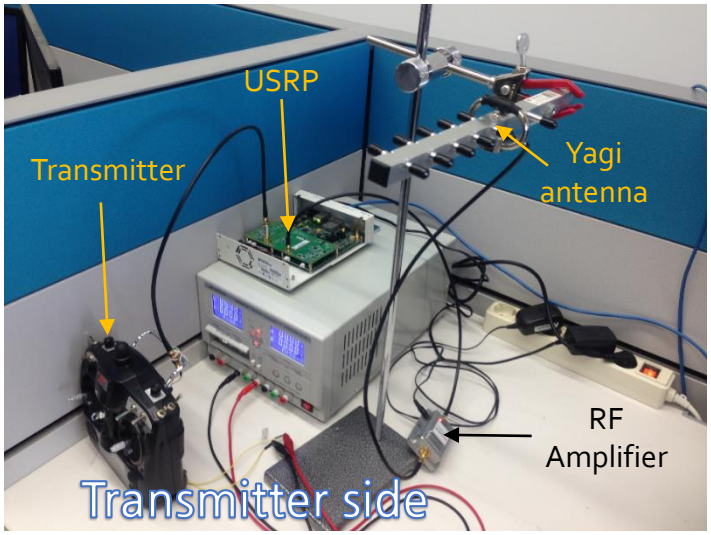
Transmitter

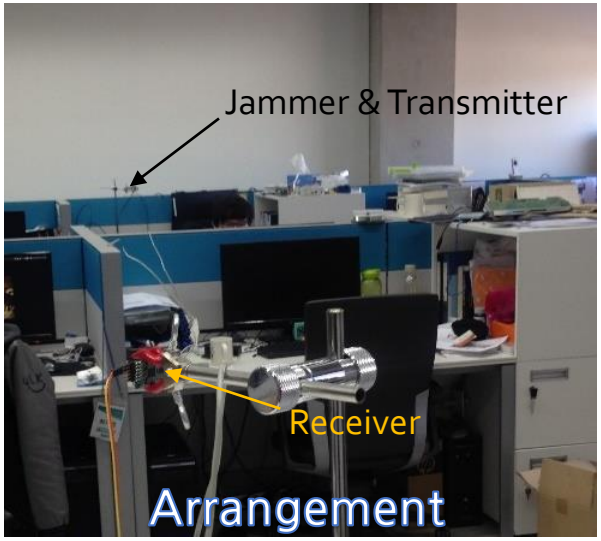
Receiver

Reactive Jamming

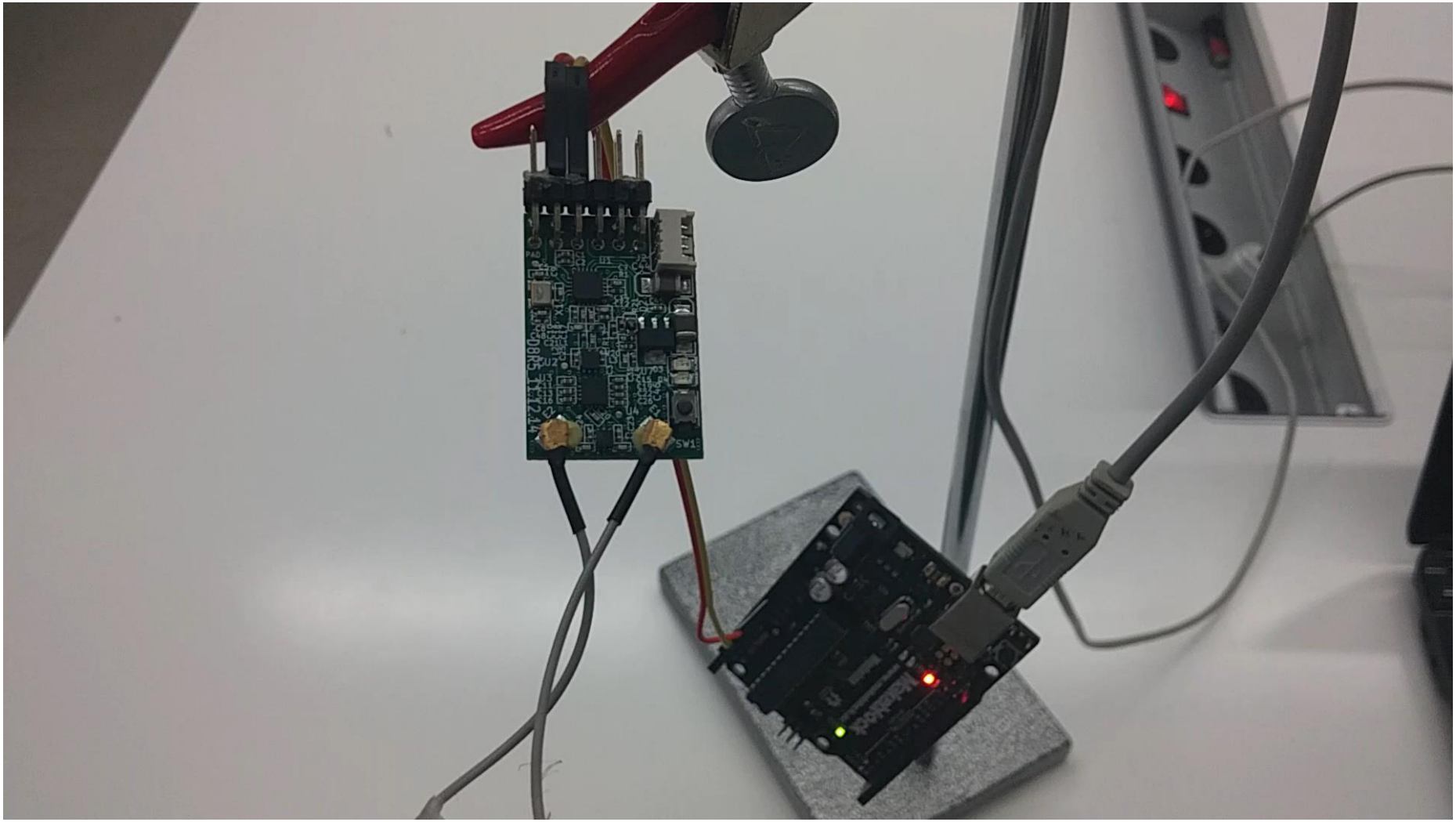
❖Jamming waveform

- Single sinusoidal signal
- Following to the extracted hopping sequence





Reactive jamming test



Attack

2. Communication Channel (Telematics)

Vulnerabilities in Telemetry

No authentication and encryption !!

- Telemetry connection
  - "3DR Radio" : setup telemetry
  - Open source firmware – ZigBee
  - Small size, Light weight

- Sniffing & spoofing attack
  - NO paring step - multiple connection
  - NO data encryption

Mission planner

Telemetry module
(Victim)

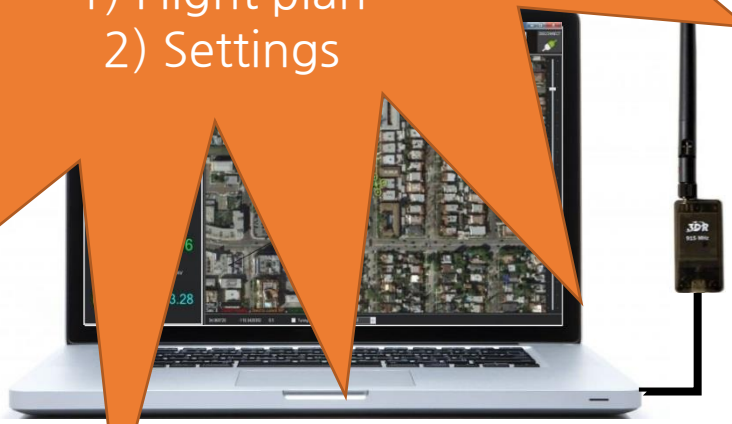
Connected

Attacker can acquire
1) Location
2) Fight plan
3) Settings

Attacker can modify
1) Flight plan
2) Settings

Connected

Multiple connection



Attacker

Telemetry moduel
(Attacker)

Attack

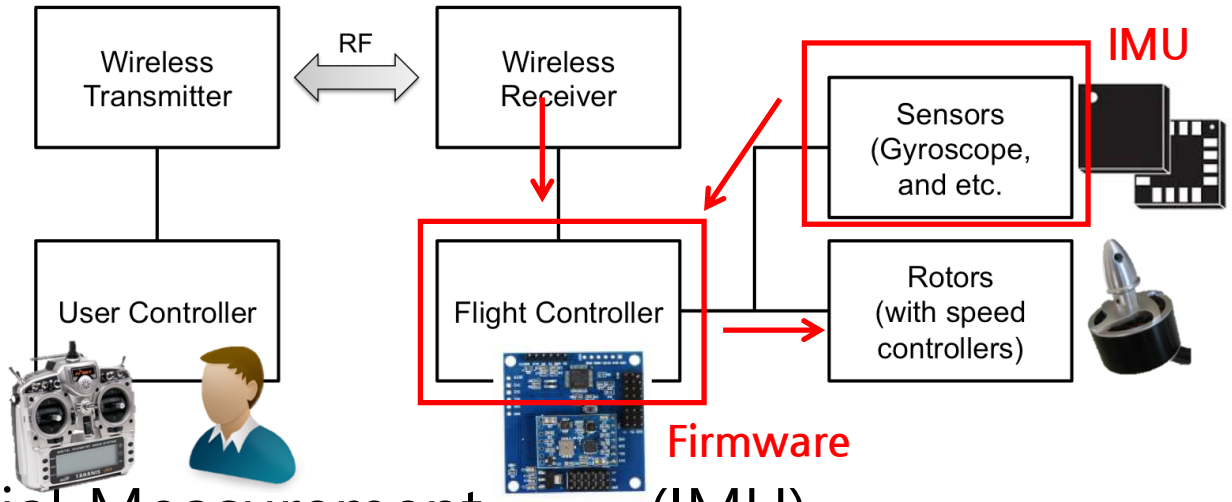
3. Positioning Channel (See at the end)

Attack

4. Sensing Channel

Inertial Measurement Unit (IMU)

Sensor input can be contaminated !!



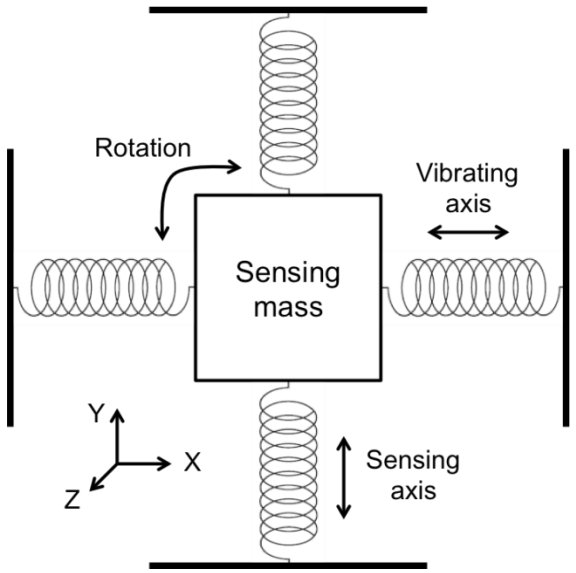
❖Inertial Measurement Unit (IMU)

- A device to measure velocity, orientation, or rotation
- MEMS **gyroscopes** and accelerometers

MEMS Gyro. & Sound Noise

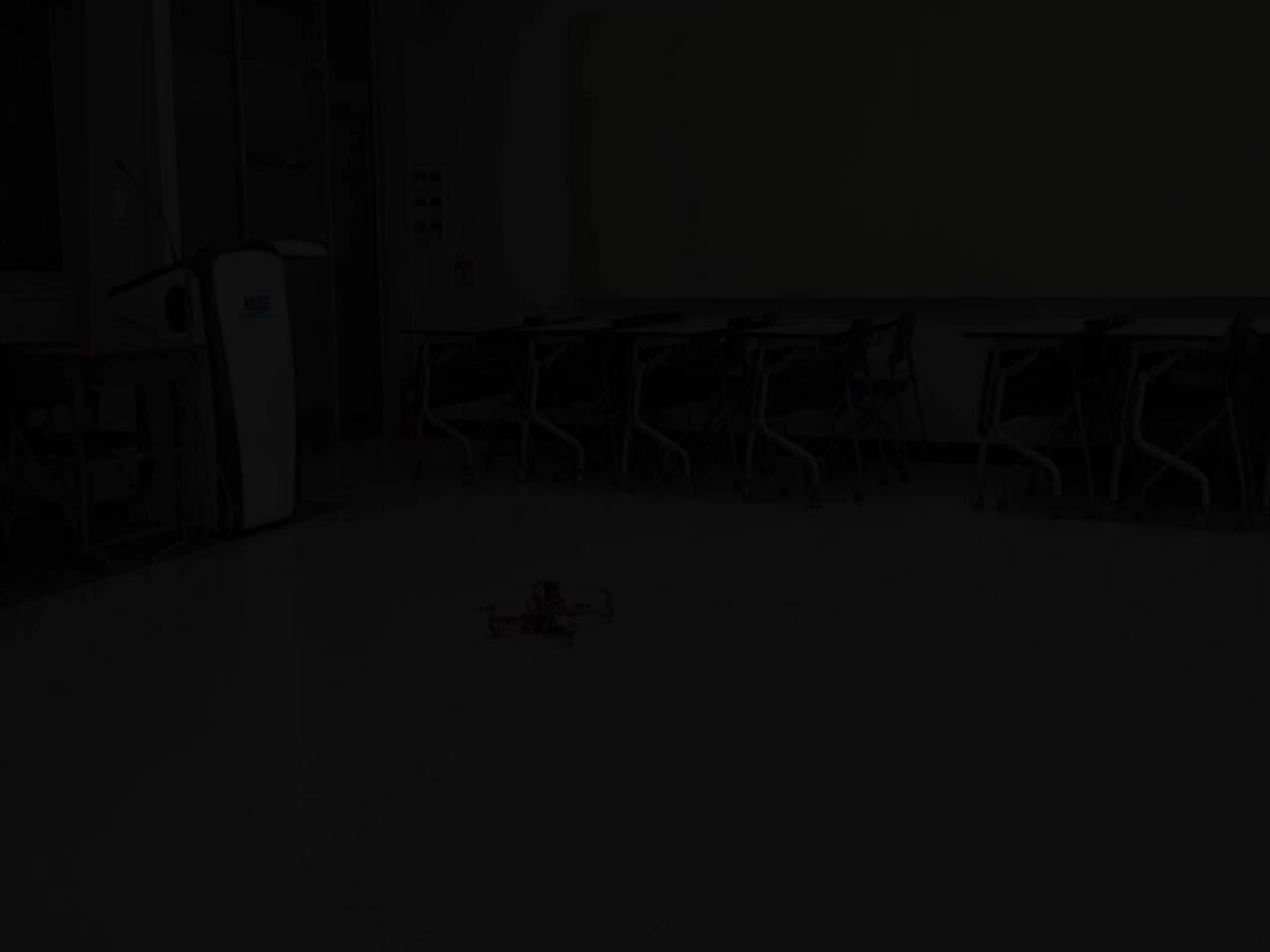
❖MEMS structure
- Based on the Coriolis effect
- Vibrating axis and sensing axis

❖Sound noise effect
- Known fact in the MEMS community
- Degrades MEMS Gyro's accuracy
- With certain (resonance) frequency
- May induce mechanical vibrations

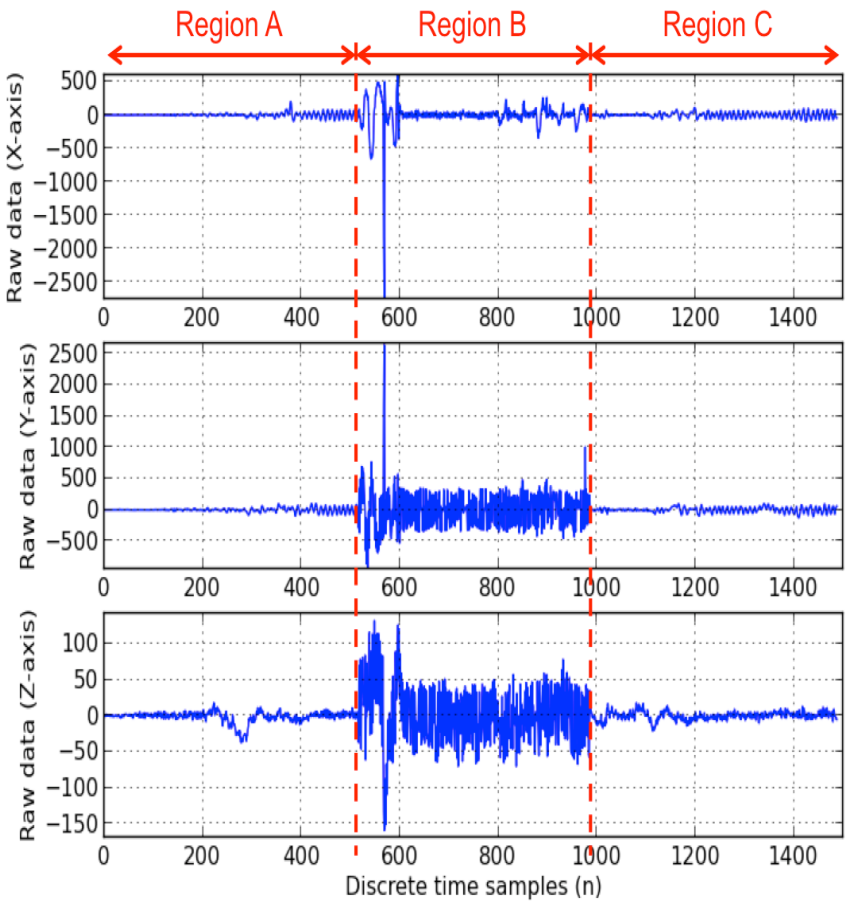


〈Basic MEMS structure〉

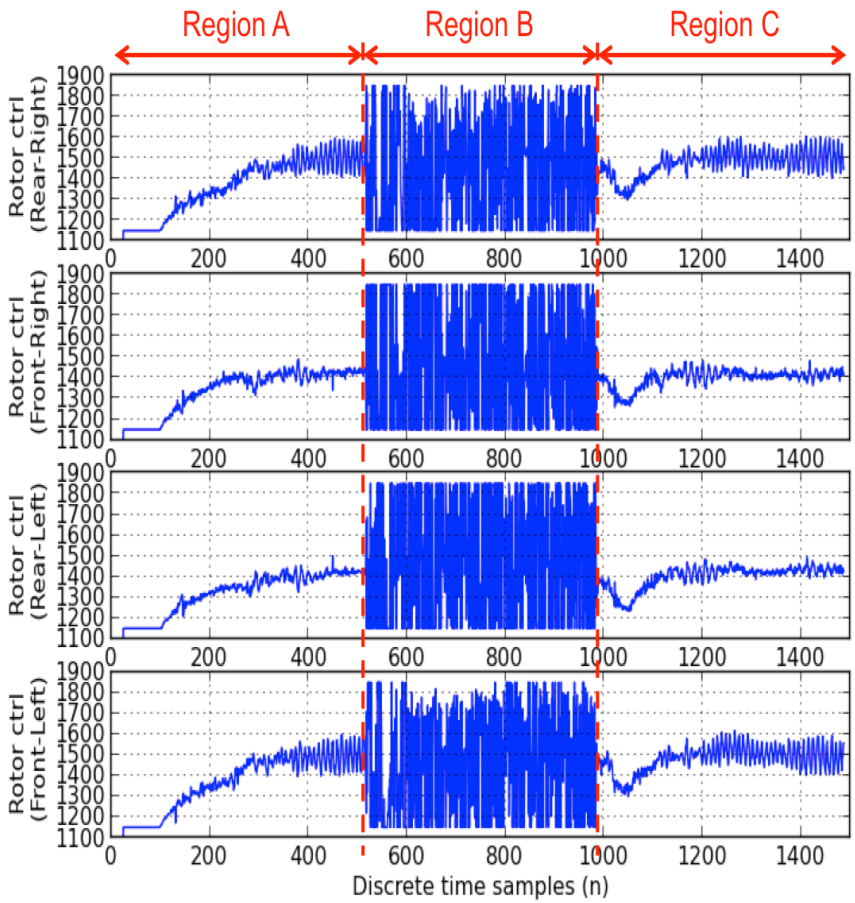
Gyro. with a high resonance frequency to reduce the sound noise effect (above 20kHz)



Attack Demo



Raw data samples of the gyroscope



Rotor control data samples


Long Range
Acoustic
Device
for police

Limitations (2/2)

❖No accumulated effect or damage

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

Attack

5. Software Hacking

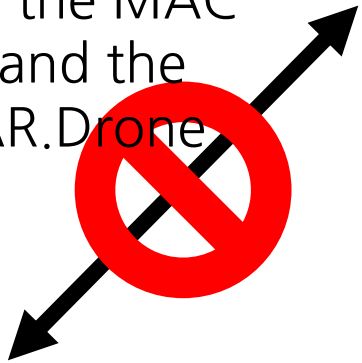
WiFi based Drones

- Using WiFi
  - Remote control with a smartphone or smartpad
  - Recording and sharing an HD video
  - E.g. AR.Drone (Parrot)

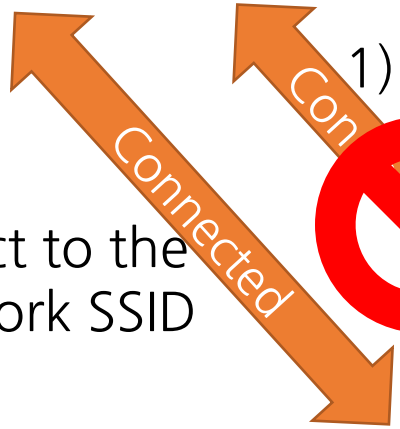
High accessibility, open services (FTP, Telnet), and no encryption !!

Hijacking

2) Change the MAC address and the SSID of AR.Drone



3) Connect to the new network SSID



1) Obtain a root-shell through Telnet

Attack

6. Physical Attack

Laser Attack

❖U.S. Navy Laser Test Takes Down Drone

https://www.youtube.com/watch?v=l5qKSKsfUPM

Drone Capturing using a Net

❖MP200 (French, Malou Tech)

Drone Interceptor MP200, A Defensive Drone Carrying a Net Designed to Intercept and Capture Malicious Drones

by Brian Heater at 9:57 am on February 11, 2015

http://laughingsquid.com/drone-interceptor-mp200-a-defensive-drone-carrying-a-net-designed-to-intercept-and-capture-malicious-drones/

Drone Capturing using a Net

❖Also at KAIST

홈 > 기획·테크 > 리뷰

KAIST, "드론 잡는 드론" 개발

그물을 이용해 적의 무인기 무력화시키는 방법

승인 2015.04.16 01:05:47

▲ 국내 KAIST가 개발한 그물을 이용해 적의 드론을 잡는 드론 시험 모습

http://www.irobotnews.com/news/articleView.html?idxno=4730

Finding Malicious UAV Operator

- T180-5TH-U (French, infotron)

T180-5TH DRONE HUNTING DRONE PROMISES TO FIND MALICIOUS UAV OPERATORS

April 18, 2015 · in News

ECA Group, a French company specializing on various kinds of robotics has developed innovative on-board technology for its IT180 drone. This technology can locate malicious drone operators in under a minute.

The T180-5TH-U is a mini UAV propelled by a thermic engine and is dedicated to survey missions. Thanks to its long endurance (120 min), its long range (10 km) and its multiple payloads, it offers very high performances in data collection and can be used for multiple missions.

http://www.dronethusiast.com/t180-5th-drone-hunting-drone-promises-to-find-malicious-uav-operators/
http://www.infotron.fr/OUR-PRODUCTS

Bumper Drone

❖유콘시스템

사회 주말뉴스 토.일

[주말뉴스 토] 드론 잡는 드론부터 공중 급유 드론까지…끝없는 드론의 진화

이현준 기자 ▾ 등록 2015.06.27 19:49

기사 공유하기 ▸ 가+ | −가

SysSec System Security Lab

Tractor Beam: Safe-hijacking of Consumer Drones with Adaptive GPS Spoofing

Juhwan Noh, Yujin Kwon, Yunmok Son,
Hocheol Shin, Dohyun Kim, Jaeyeong Choi, Yongdae Kim
System Security Lab. @ KAIST

ACM Transactions on Privacy and Security, Vol. 22, No. 2, Article 12

Existing anti-drone techniques

Shooting net
- Too short range

Radio jamming
- Should wait until the battery of the target drone is depleted

Laser attack
- Dangerous (collateral damage)
- the target drone should be in LOS

GPS spoofing on drones?

LORENZO FRANCESCHI-BICCHIERAI SECURITY 07.19.12 05:32 PM

GPS HIJACKING CATCHES FEDS, DRONE MAKERS OFF GUARD

The University of Texas Radionavigation Laboratory drone, an Adaptive Flight Hornet Mini.
PHOTO: COURTESY TODD HUMPHREYS

UPDATED 7/20/12, 11.30AM

On June 19, when University of Texas researchers successfully hijacked a drone by "spoofing" it – giving it bad GPS coordinates – they showed the Department of Homeland

EXCLUSIVE: Drones vulnerable to terrorist hijacking, researchers say

By John Roberts, | Fox News

GPS fail-safe mechanisms

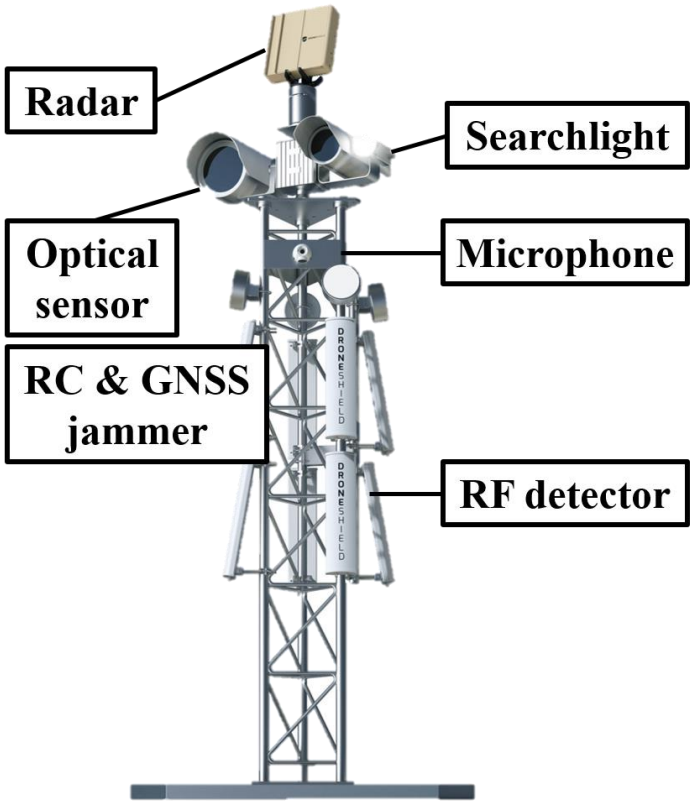
❖Three possible flight mode after GPS recovery

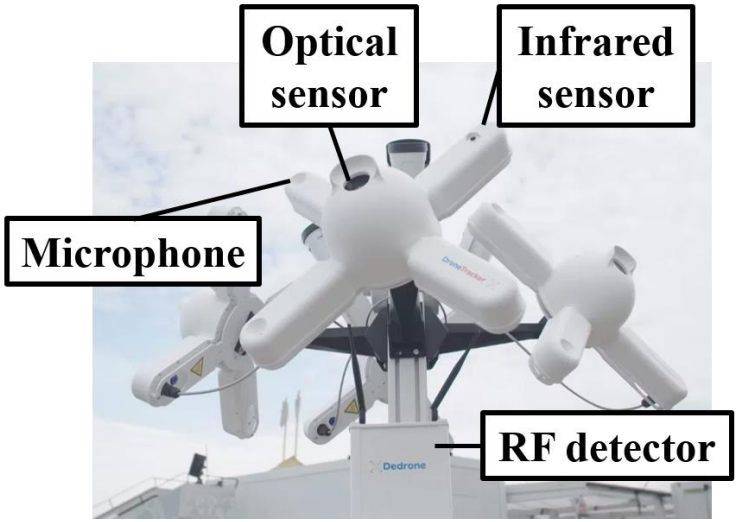
1. Positioning mode with GPS
2. Resuming autopilot
3. Maintaining the fail-safe mode

Fail-Safe Mechanism에 따른 드론의 분류

Drone type	GPS fail-safe flight mode	Behavior after GPS recovery	Belonging consumer drones
I	Positioning mode (non-GPS)	Positioning mode (GPS)	DJI Phantom 3 & Phantom 4
II		Autopilot (GPS)	Parrot Bebop 2
III		Continue fail-safe	3DR Solo
IV	Landing		-

Hijacking model





The strategy for Type III

- Should avoid activating the fail-safe
  - Conducting seamless GPS spoofing
  - Moving the spoofed location carefully according to the path following algorithm of the target drone

Drones and terrorism

WIRED SUBSCRIBE

BRIAN BARRETT SECURITY 08.04.18 10:51 PM

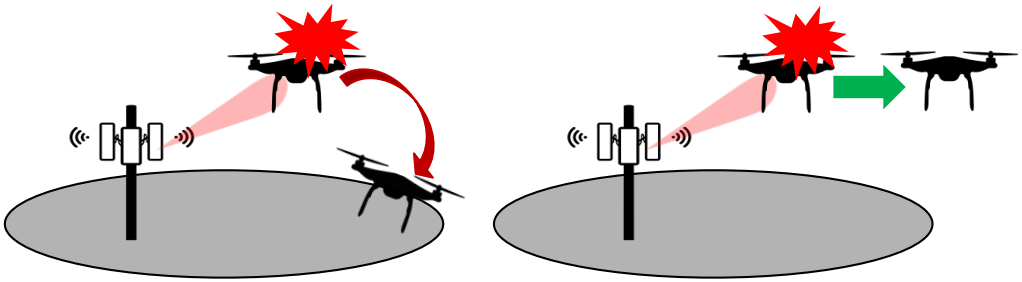
THE EXPLOSIVE-CARRYING DRONES IN VENEZUELA WON'T BE THE LAST

MIRAFLORES PALACE/REUTERS

ON SATURDAY, AS Venezuelan President Nicolas Maduro gave a speech in Caracas before a large military

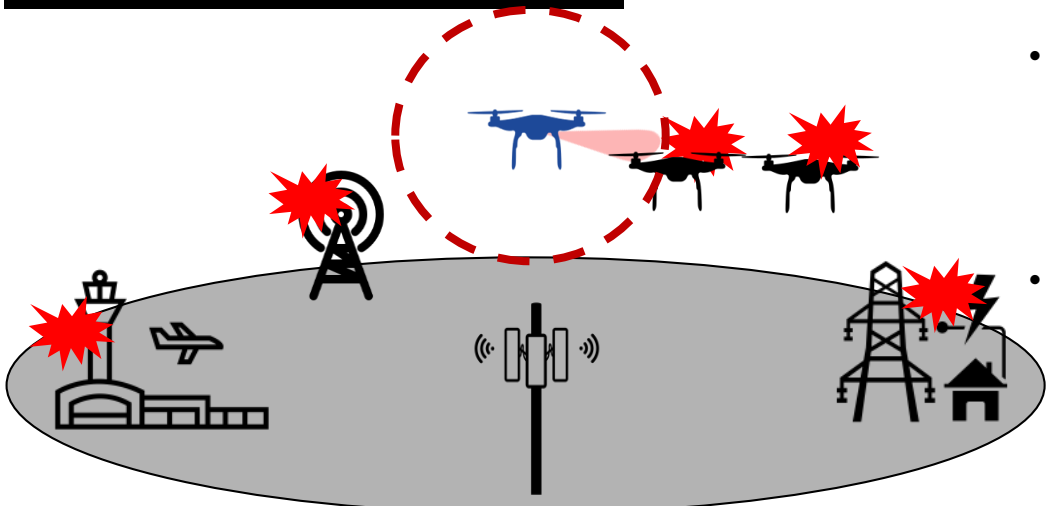
GPS Spoofing 안티드론의 미래

GPS 스푸핑 안티드론 기술의 우수



- 기존 안티드론 기술은 단순 드론 비행 무력화가 목적
- 무력화된 불법 드론이 보호 구역 내에 그대로 남아 있는 경우 부수적 피해가 발생할 수 있음
- GPS 스푸핑 안티드론 기술 활용시 드론을 보호 구역 밖으로 발견 즉시 견인 가능

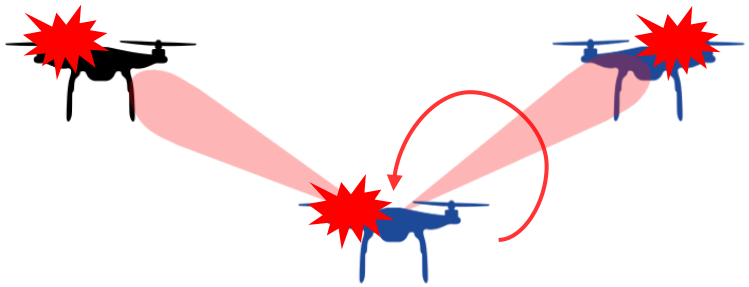
드론-드론 GPS 스푸핑의 필요성



- 그러나 GPS 스푸핑 신호가 이동통신망, 변전소, 공항 등 다른 기반시설에 영향을 주는 경우 막대한 피해 발생 가능
- 이러한 부수적 피해를 줄이기 위해서는 스푸핑 장비를 장착한 방호드론을 불법드론에 근접시키고 신호의 세기가 약한 스푸핑 신호를 생성하는 것이 필요

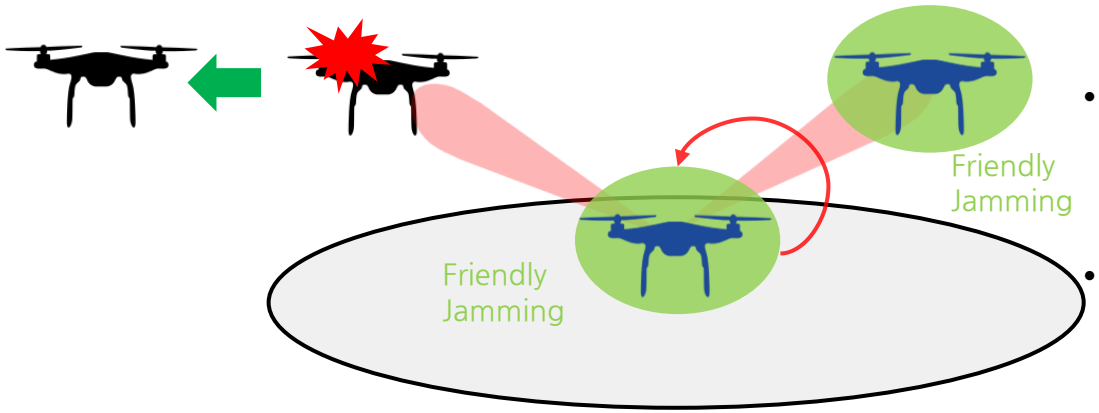
GPS Spoofing 안티드론의 미래

드론-드론 GPS 스푸핑의 문제점



- 방호드론도 위치 정보를 계산하는데 GPS 신호를 활용
- GPS 스푸핑 신호의 자체 간섭으로 인하여 스푸핑 신호를 생성하는 방호드론이 오작동할 수 있음
- 주변의 방호드론들도 GPS 스푸핑 신호에 영향을 받아 오작동 할 수 있음

Friendly Jamming을 이용한 자체 간섭 해결



- 자체 간섭을 해결하기 위해서 Friendly Jamming 기술을 활용
- 스푸핑 신호 생성시에 방호드론들 간에 신호를 공유하여 스푸핑 신호의 영향을 최소화
- 이에 반해 불법드론은 스푸핑 신호를 방어할 수단이 없기 때문에 구역 밖으로 견인 당하게 됨

만약 GPS 없이 비행을 한다면?

- 대안 1: 카메라 센서
- 대안 2: 라이다
- 대안 3: Gyroscope 만을 이용한 비행

3. Camera module blinded by laser injection

Lidar Exposure to Strong Light Source

Lidar Spoofing of Multiple Moving Fake Dots

Thank You!