USENIX Security Symposium 2015

Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors

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

2015. 08. 14.

usenix ASSOCIATION

SysSec SystemSecurityLab

Introduction

Drones use sensors to maintain their stability.

Sound in a specific frequency can cause malfunction the sensor.

When this happens, drones would drop from the sky.

Drones (Multi-coptors)

Aerial photography

Military

Transportation system

Distribution delivery

Fire fighting

Drone, A New Threat

Air terrorism using a weaponized drone

Teenager's video of gun-firing drone prompts investigations by aviation officials, police

Man detained outside White House for trying to fly drone

Watch the Pirate Party fly a drone in front of Germany' chancellor

TERRORISM

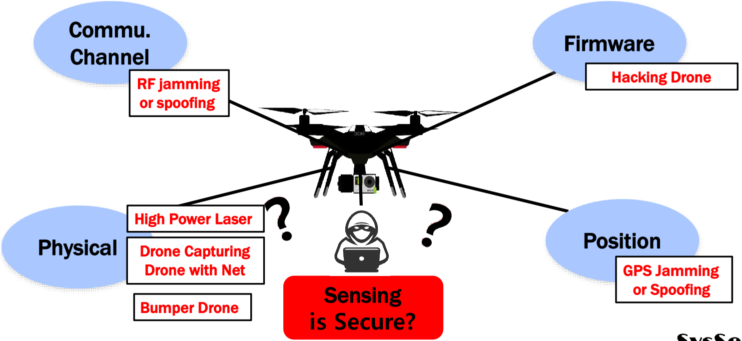
Drone used in attack on US electrical grid last year, report reveals

People

Important Place

Indiscriminate terrorism

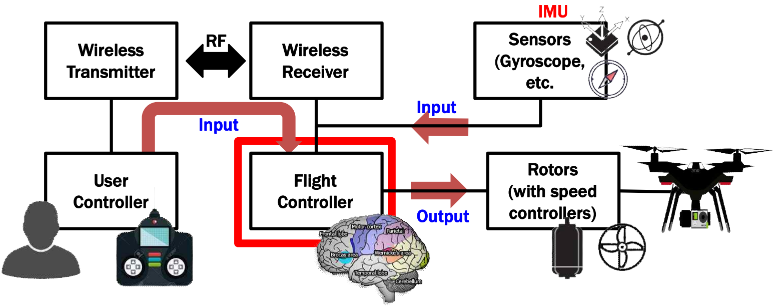
Drone Attack Vectors



SysSec
SystemSecurityLab

Drone Block Diagram

* IMU: Inertial Measurement Unit



Gyroscope on Drone

* MEMS: Micro-Electro-Mechanical Systems

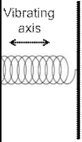
Inertial M

A dev
orien

Using
gyros

MEMS gy

MS gyro



Structure

SysSec
SystemSecurityLab

Resonance in MEMS Gyroscope

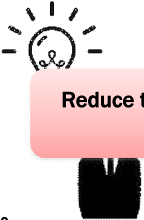
Mechanical resonance by sound noise

- Known fact in the MEMS community
- Degrades MEMS Gyro's accuracy
- With (resonant) frequencies of sound


L3GD20

Features

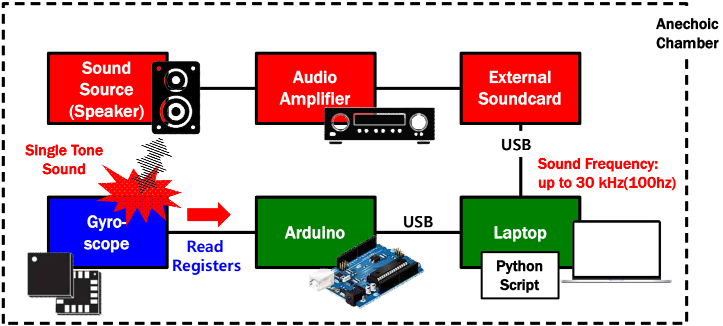
- Three selectable full scales (±250/500/2000 dps)
- 20+ kHz resonant frequency over the audio bandwidth



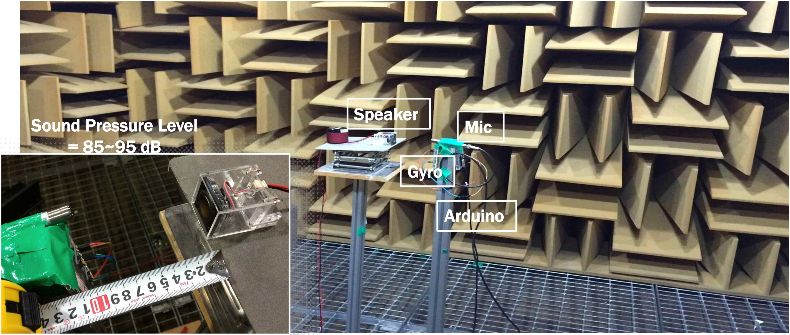
Reduce the sound noise effect (make resonant frequency higher than 20kHz)

SysSec
SystemSecurityLab

Experiment Setup



Anechoic Chamber



Experimental Results (1/3)

15 kinds of MEMS gyroscopes

Found the resonant frequencies of 7 MEMS gyroscopes

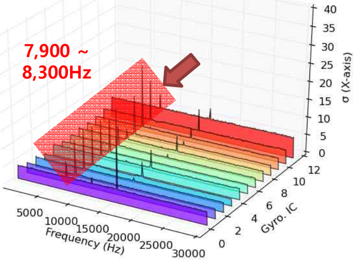
Not found for 8 MEMS gyroscopes in

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)

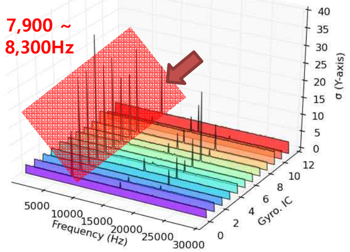
Experimental Results (2/3)

Unexpected output by sound noise (for L3G4200D)

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



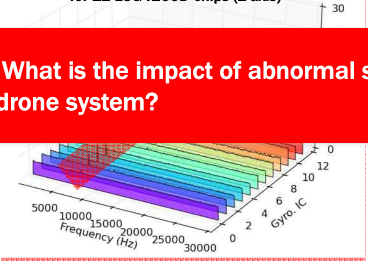
Standard deviation of raw data samples for 12 L3G4200D chips (Y-axis)



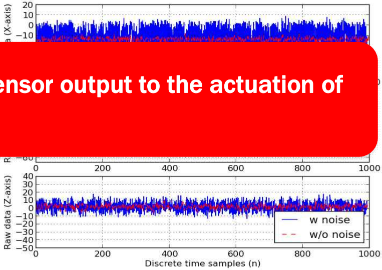
Experimental Results (3/3)

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



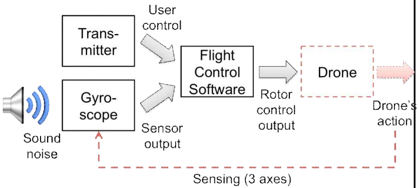
What is the impact of abnormal sensor output to the actuation of drone system?

Software Analysis

Two open-source firmware programs

- Multiwii project
- ArduPilot project

Rotor control algorithm



for *axis* **do**

- $P = txCtrl[axis] - gyro[axis] \times G_P[axis]$;
- $error = txCtrl[axis] / G_P[axis] - gyro[axis]$;
- $error_{accumulated} = error_{accumulated} + error$;
- $I = error_{accumulated} \times G_I[axis]$;
- $delta = gyro[axis] - gyro_{last}[axis]$;
- $delta_{sum}$ = 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;

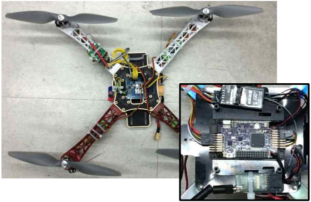
Target Drones

Target drone A (DIY drone)

Gyroscope: L3G4200D

Resonant freq.: 8,200 Hz

Firmware: Multiwii

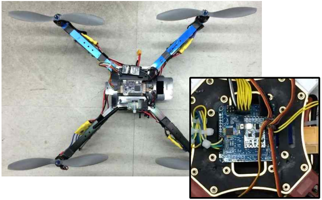


Target drone B (DIY drone)

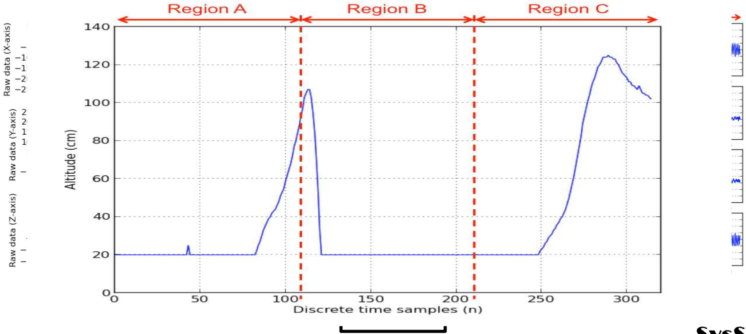
Gyroscope: MPU6000

Resonant freq.: 26,200 Hz

Firmware: ArduPilot



Attack DEMO (Target drone A)

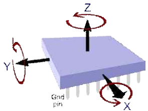


SysSec
SystemSecurityLab

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

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

LRAD 950RXL Long Range Acoustic Device

ACOUSTIC PERFORMANCE

Maximum Peak Output	156dB SPL @ 1 meter, C-weighted
Maximum Continuous Output	151db SPL @ 1 meter, A-weighted
Sound Projection	+/- 15° @ 1kHz/-3dB
Communication Ranges	Maximum range up to 3,000 meters in ideal conditions. Operational range up to 1,250 meters over 88dB of background noise. Ranges based on continuous output.

Attack Scenarios

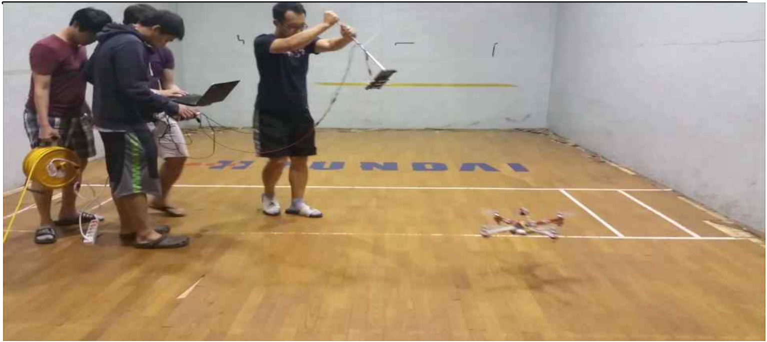
Drone to Drone Attack

Sonic Weapons

Sonic Wall/Zone

SysSec
SystemSecurityLab

Limitations (1/2)



Limitations (2/2)

No accumulated effect or damage

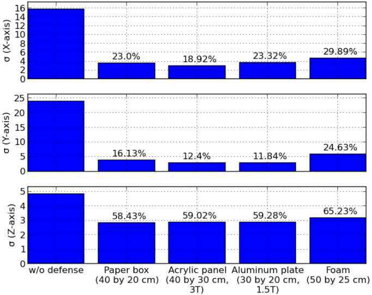
Simple sonic wall
(3m-by-2m, 25 speakers)

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)



SysSec
SystemSecurityLab

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
- Demonstrating to attack drones using sound noise in the real world
- Suggesting several attack scenarios and defenses

Future work

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

Conclusion

Stop entirely trust sensor.

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

Previous work

Resonant Frequencies of Gyroscopes:

Influence of acoustic noise on the dynamic performance of MEMS gyroscopes. In International Mechanical Engineering Congress and Exposition (2007), American Society of Mechanical Engineers.

Security Analysis of Commercial Drones:

AR.Drone: security threat analysis and exemplary attack to track persons. In Society of Photo-Optical Instrumentation Engineers Conference Series (2012).

Input Spoofing Attacks on Sensing Circuitry:

Ghost talk:mitigating EMI signal injection attacks against analog sensors. In IEEE Symposium on Security and Privacy (2013).

Following works

Sound attack on Accelerometers

"WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks"

Spoofing attack on IMU through a sound wave

"Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors"

Software based Defense:

"SAVIOR: Securing Autonomous Vehicles with Robust Physical Invariants"

Q&A

진영진

Q1. Are there other sensors that can be affected by mechanical resonance phenomena? Or is it limited to gyroscopes and accelerometers?

이태화

Q2. Defence techniques using hardware seem to be challenging to apply. Does software-based defence exist?

한상구

Q3. Can't we protect against gyroscope malfunction in the same way as fail safe mode? Are there more stealthy drone side channel attacks?

Thank you