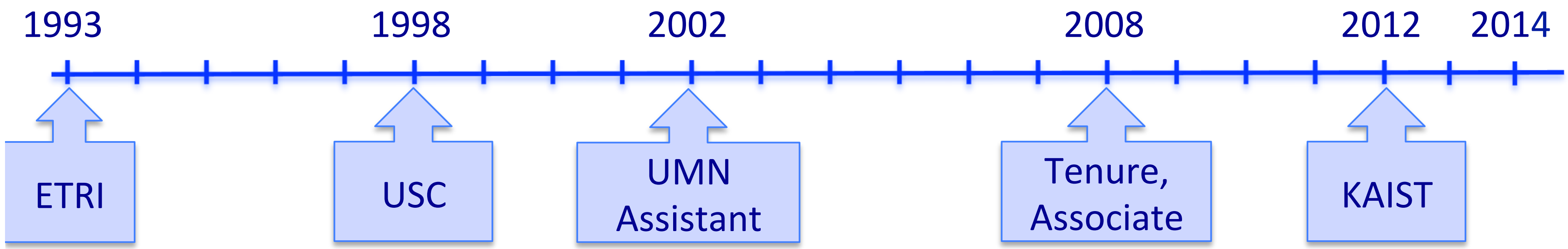

# Hacking Sensors

Yongdae Kim

SysSec@KAIST




- KAIST chair Professor at EE, KAIST (2012. 9 ~)
- CNS Group leader at EE, KAIST (2013. 3 ~)
- Affiliated professor at GSIS, KAIST (2012. 9 ~)

- 20 year career in security research
  - Applied cryptography, Group key agreement, Storage, P2P, Mobile/Sensor/ Ad-hoc/cellular Networks, Social networks, Internet, Anonymity, censorship, Medical devices, smart meters, Embedded devices, cyber Physical Systems

- Mostly publishing Attack Papers in Academic conferences
  - Shutting down eMule, BitTorrent, 802.11ac, Internet, Botnet
  - cellular Networks: Location tracking, Free 3G/VoLTE communication
  - Stopping Pacemaker, Shutting down Drones

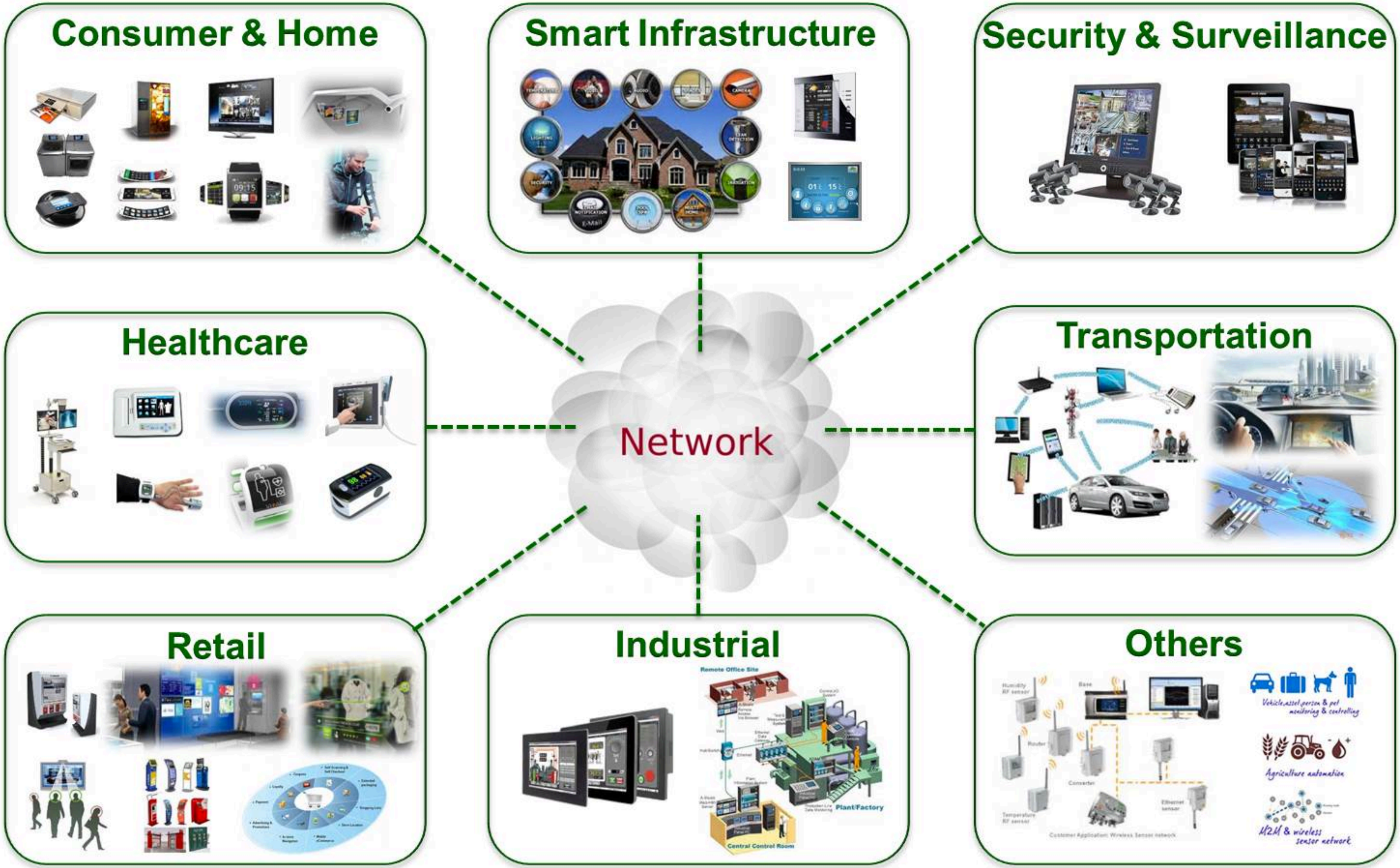
## Professor

## Cellular/Mobile Security

1 Professor
9 Ph.D. students
9 MS students
1 Researcher
(Total 20 people)

## Embedded/OS/Web Security

## Physical Security

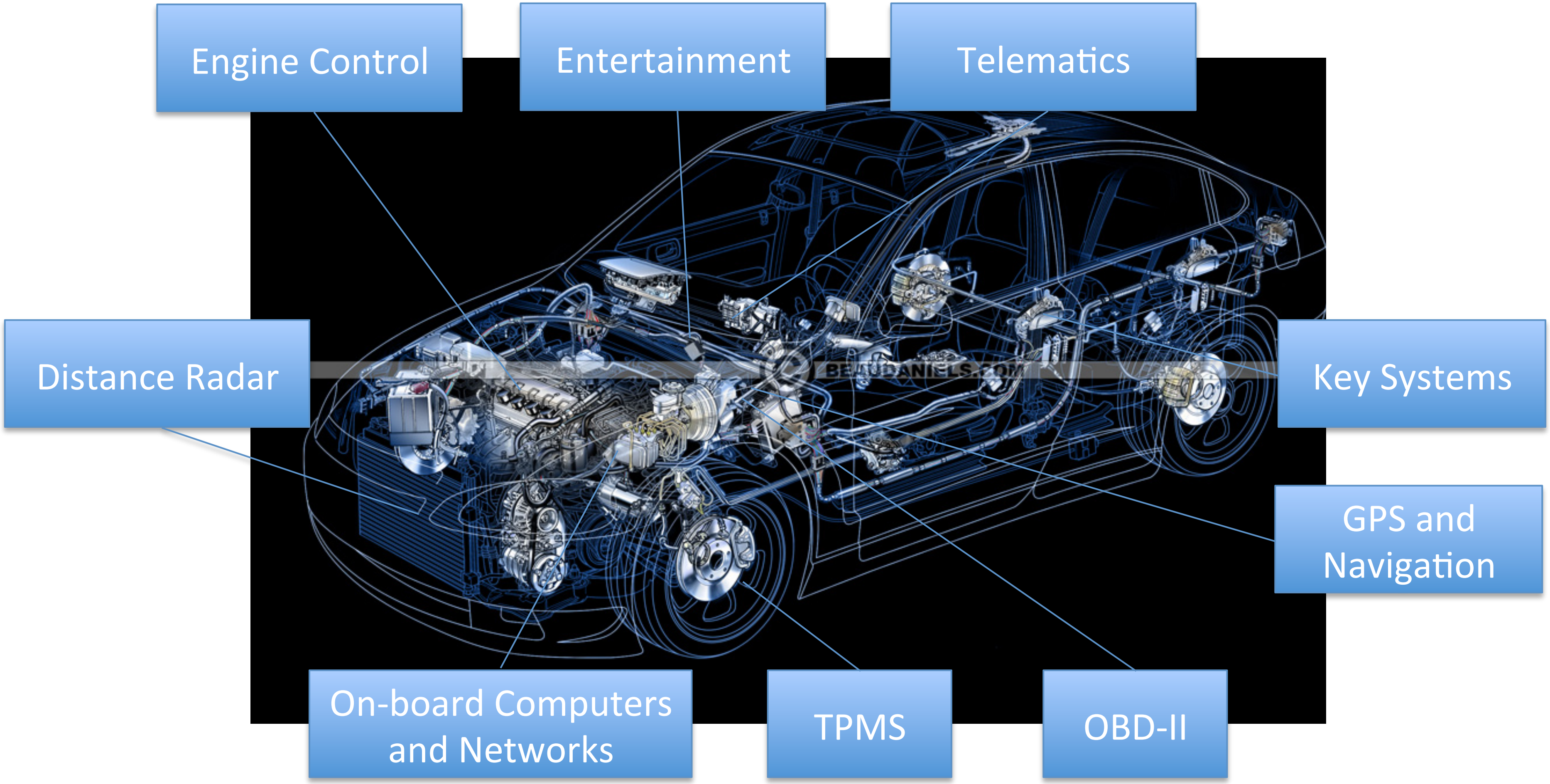

Consumer & Home
Smart Infrastructure
Security & Surveillance
Healthcare
Network
Transportation
Retail
Industrial
Others

# Typical IoT vulnerabilities

- ❑ Unsigned/unencrypted Software update
- ❑ Unsigned/unencrypted Management/web interface
- ❑ Secret keys in binary
- ❑ Unprotected hardware debugging
- ❑ Massive kernel
- ❑ No user permission
- ❑ (almost) No code review
- ❑ Hidden weak backdoor
- ❑ (almost) No logging and editable logs
- ❑ Timely patching
- ❑ Buffer/Stack/Integer overflow
- ❑ CSRF, XSS, …
- ❑ Exploitable security solutions
- ❑ No or weak software obfuscation
- ❑ Non-standard crypto primitives

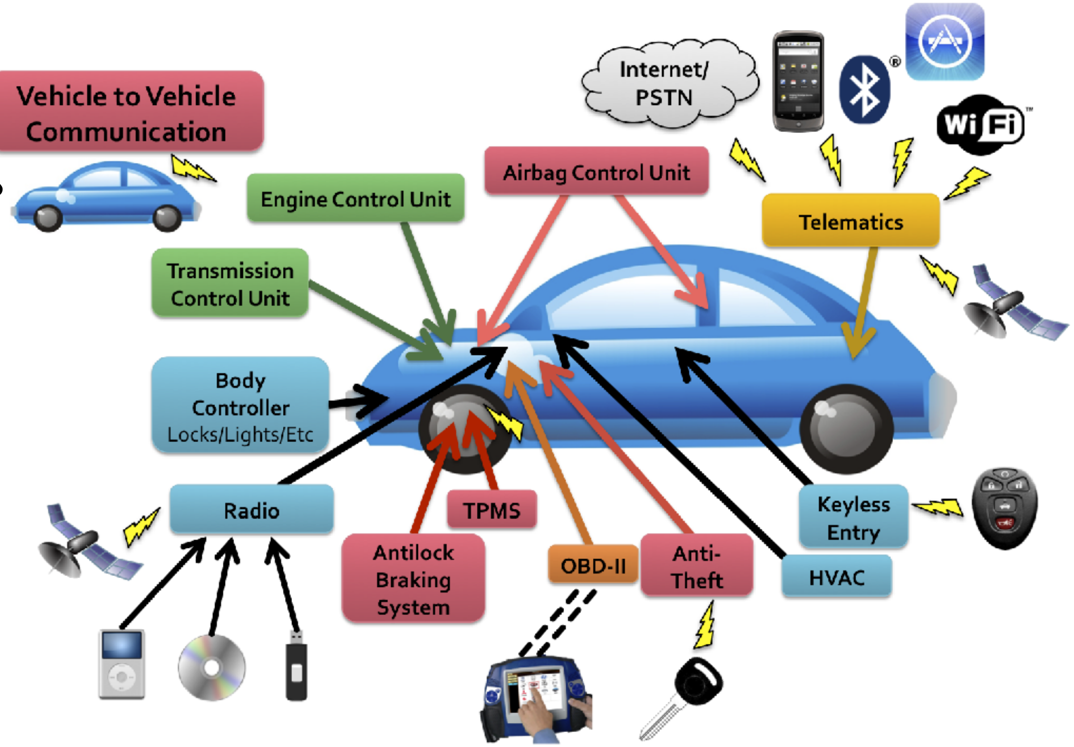
# Good Old Days

# Now and after



# Attack Surface

- Indirect physical access:
  - OBD-II (PassThru)*
  - Audio system*
- Short-range wireless access
  - Bluetooth*
  - Remote Keyless Entery
  - Tire Pressure (TPMS)?
  - Wifi
- Long-range wireless access
  - GPS
  - Satellite Radio
  - Digital Radio
  - Remote Telematics Systems*

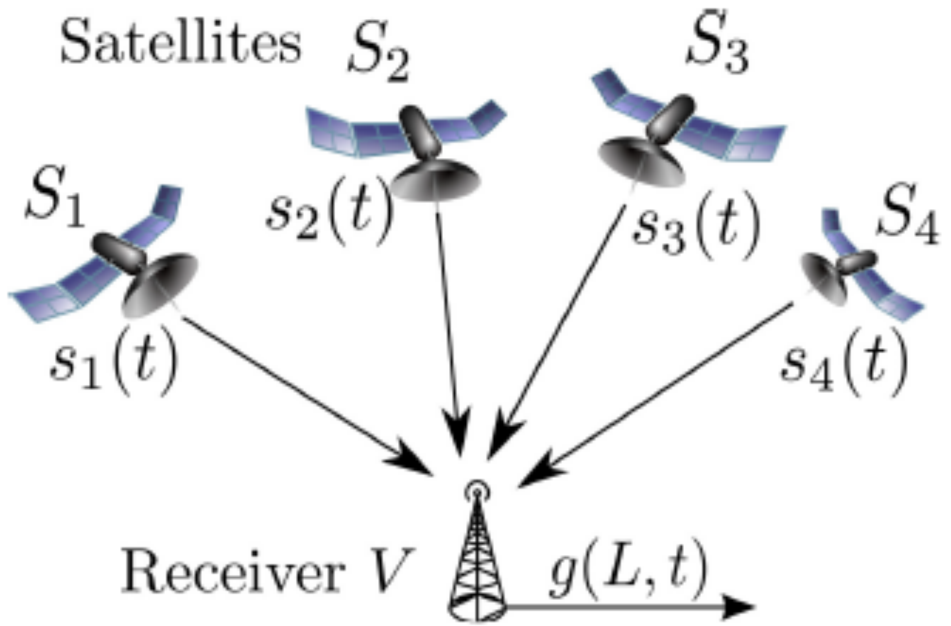


# Navigation Systems

- Korean Navigation systems in 2013
  - Android 2.3 (current version: 4.3)
  - Wifi
  - Browser
  - Blackbox
  - Mic

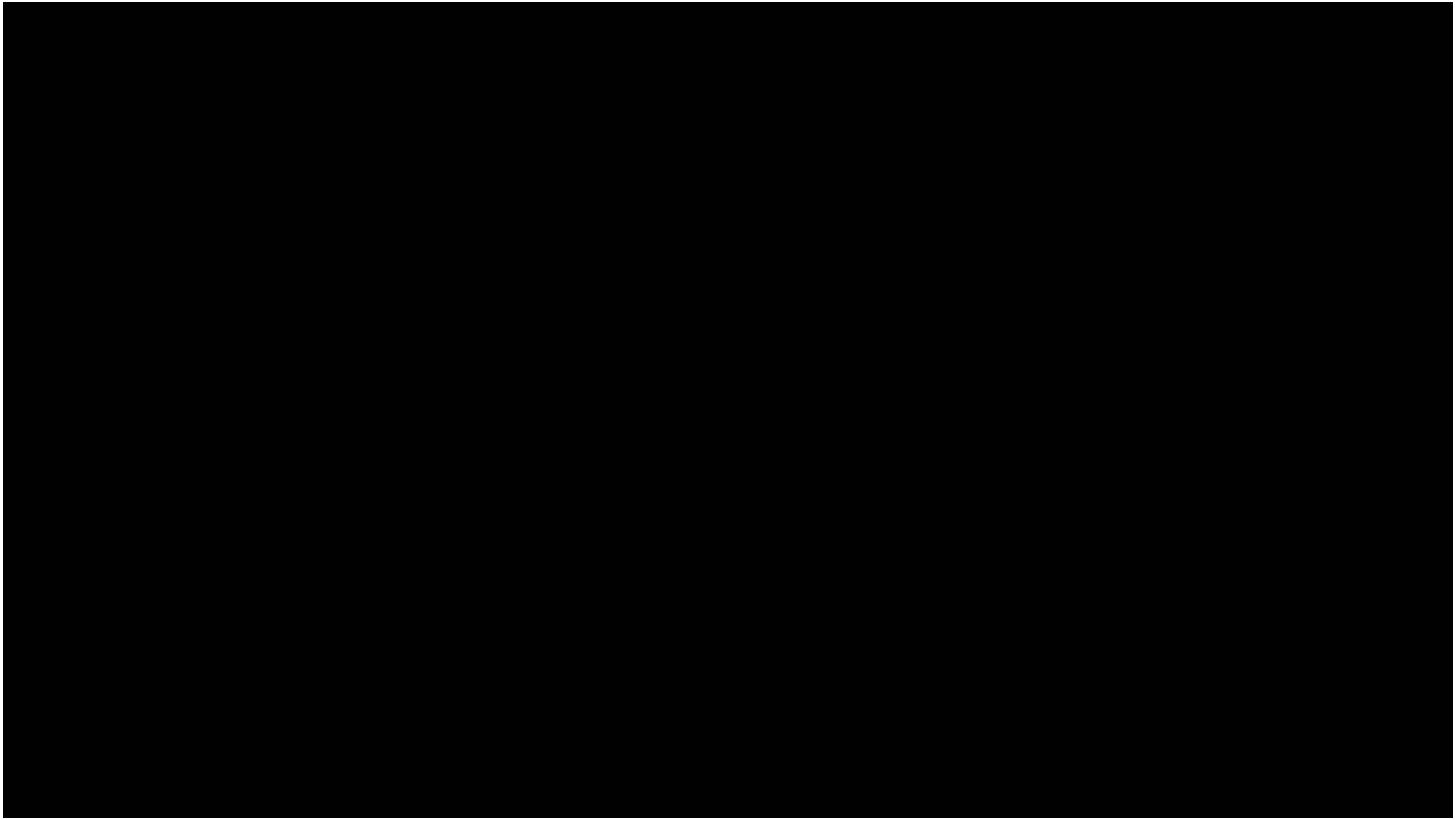
# Navigator Hacking

# GPS

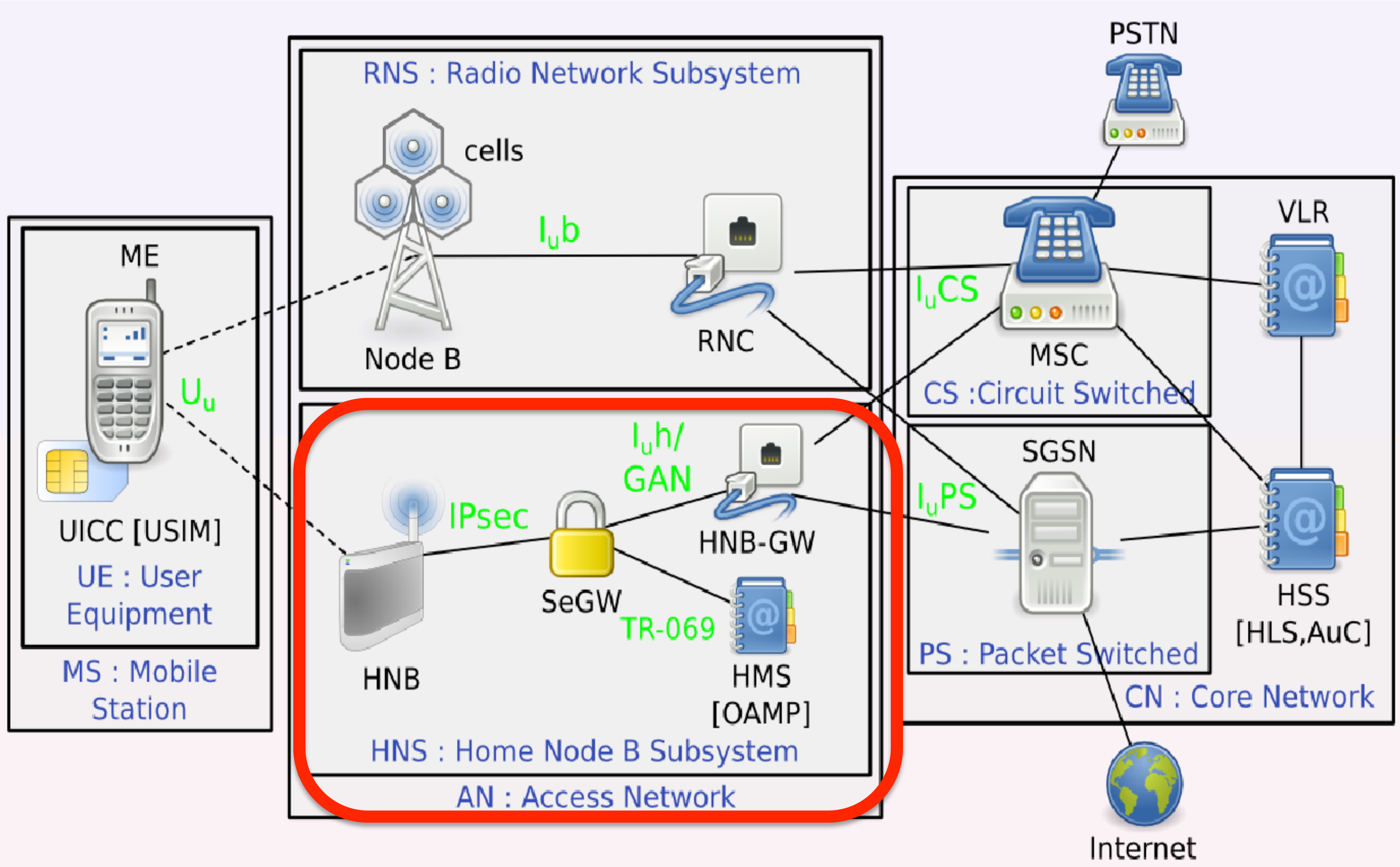


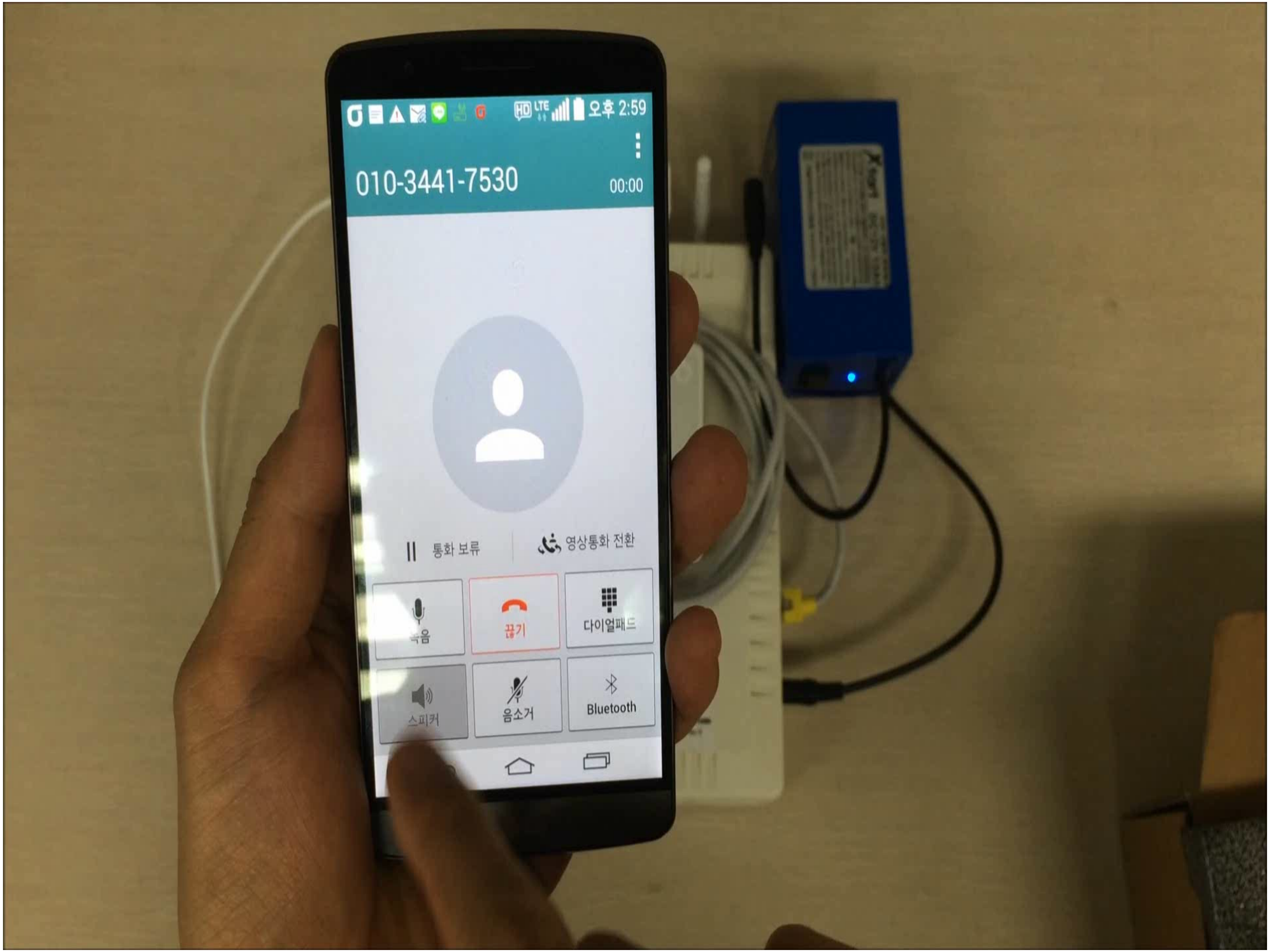

- $(x-x_{Si})^2+(y-y_{Si})^2+(z-z_{Si})^2=(R_i-\Delta)^2$
  - (x, y, z): v's coordinate
  - $\Delta$: error caused by time off-set

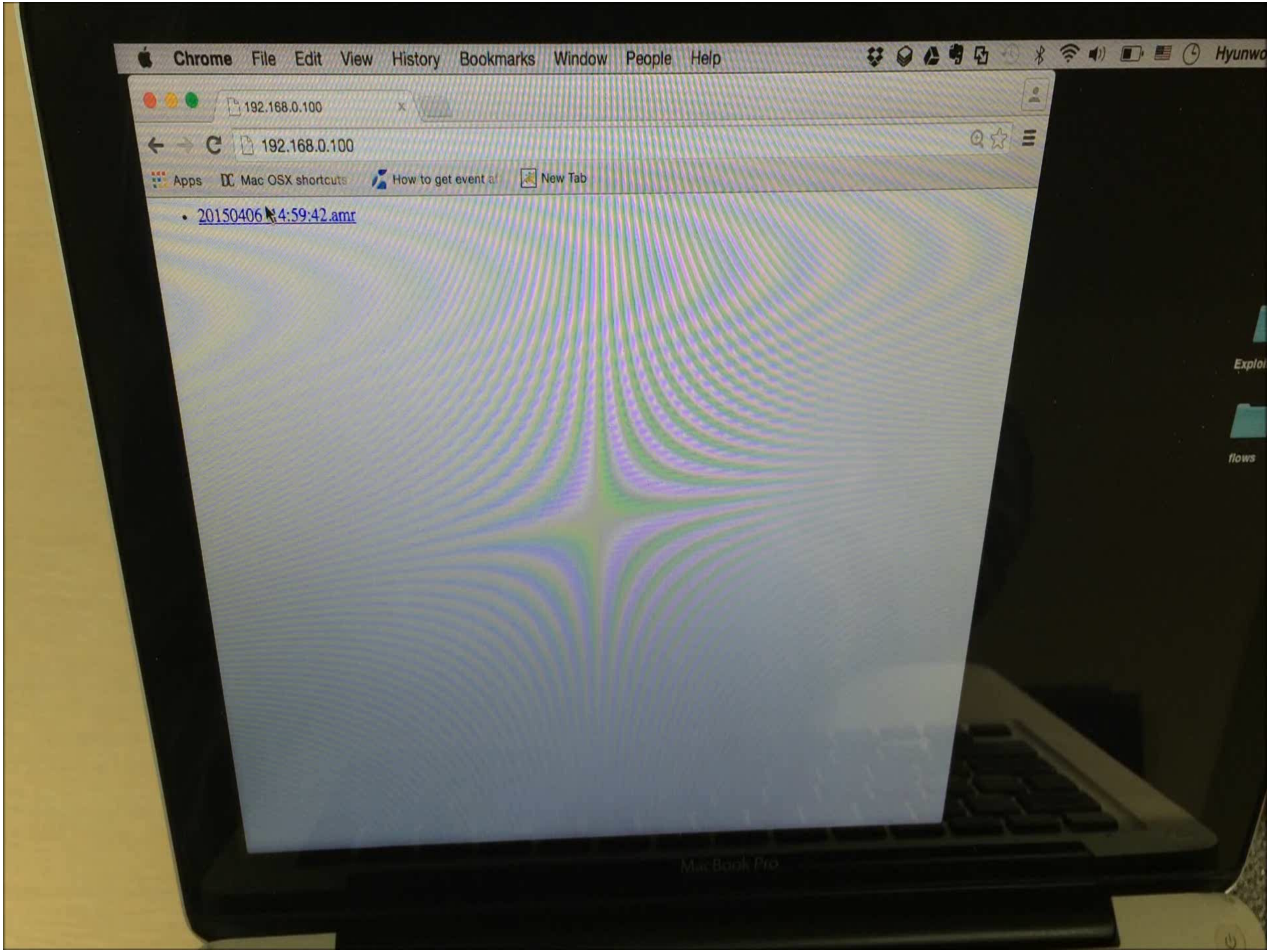
# GPS

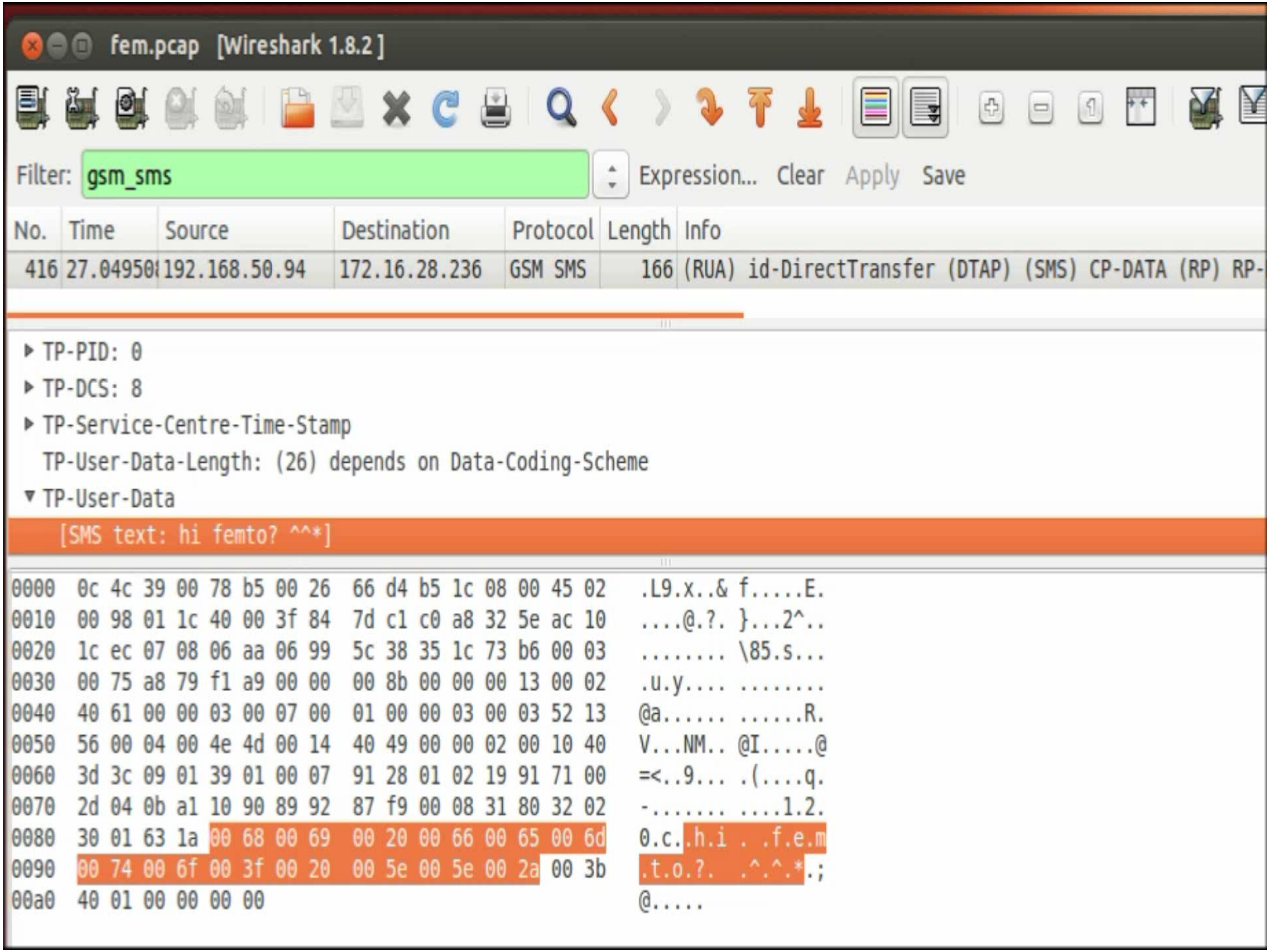


# Femtocell Architecture

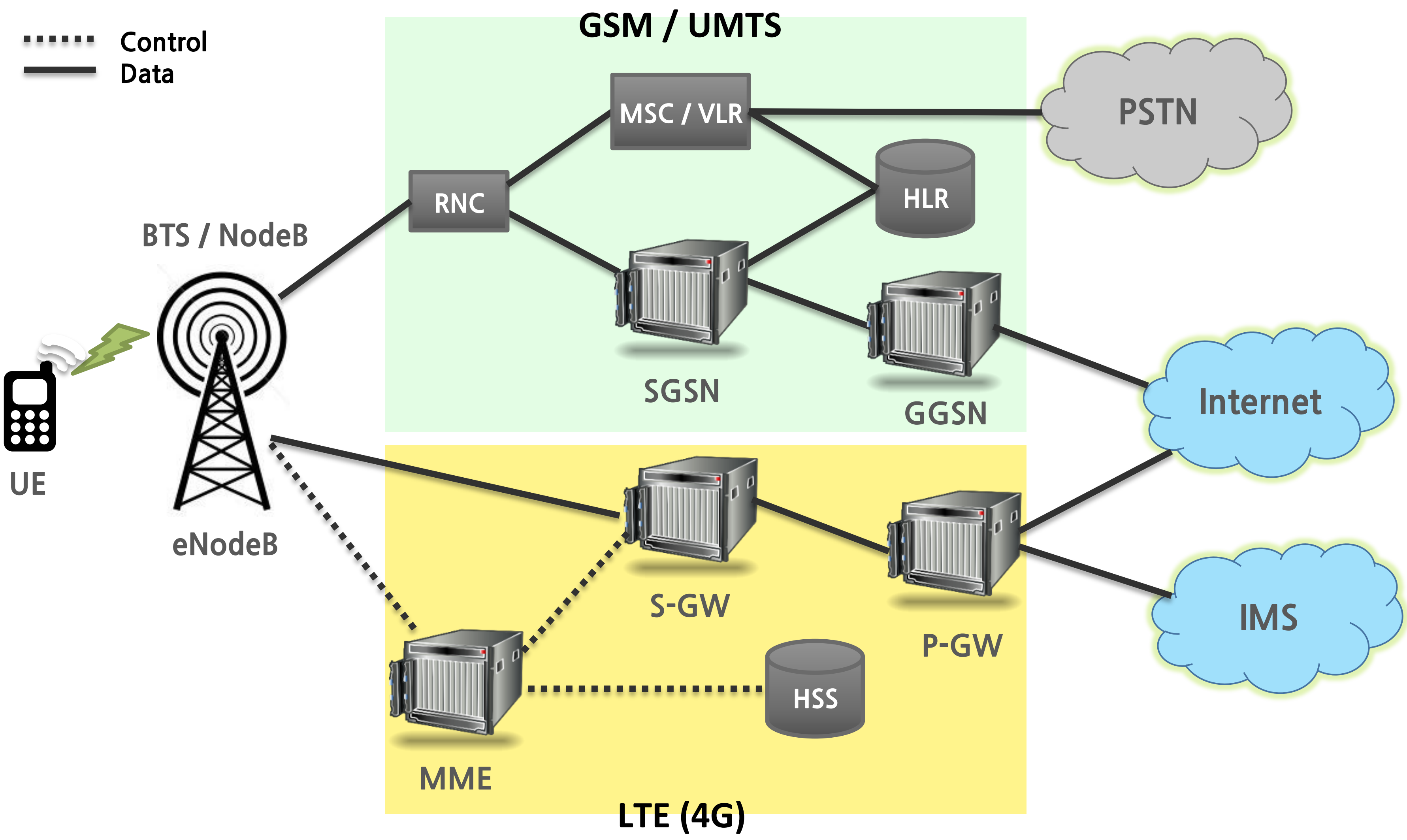



오후 2:59
010-3441-7530
00:00
통화 보류
영상통화 전환
끊기
다이얼패드
스피커
음소거
Bluetooth


Chrome File Edit View History Bookmarks Window People Help
192.168.0.100
192.168.0.100
Apps
Mac OSX shortcuts
How to get event a
New Tab
20150406 14:59:42.amr
flows


fem.pcap [Wireshark 1.8.2]
Filter: gsm_sms
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
416 27.04950 192.168.50.94 172.16.28.236 GSM SMS 166 (RUA) id-DirectTransfer (DTAP) (SMS) CP-DATA (RP) RP-
TP-PID: 0
TP-DCS: 8
TP-Service-Centre-Time-Stamp
TP-User-Data-Length: (26) depends on Data-Coding-Scheme
TP-User-Data
[SMS text: hi femto? ^^*]
0000 0c 4c 39 00 78 b5 00 26 66 d4 b5 1c 08 00 45 02 .L9.x..& f.....E.
0010 00 98 01 1c 40 00 3f 84 7d c1 c0 a8 32 5e ac 10 ....@.?. }...2^..
0020 1c ec 07 08 06 aa 06 99 5c 38 35 1c 73 b6 00 03 ........ \85.s...
0030 00 75 a8 79 f1 a9 00 00 00 8b 00 00 00 13 00 02 .u.y.... ........
0040 40 61 00 00 03 00 07 00 01 00 00 03 00 03 52 13 @a...... ......R.
0050 56 00 04 00 4e 4d 00 14 40 49 00 00 02 00 10 40 V...NM.. @I.....@
0060 3d 3c 09 01 39 01 00 07 91 28 01 02 19 91 71 00 =<..9... .(....q.
0070 2d 04 0b a1 10 90 89 92 87 f9 00 08 31 80 32 02 -....... ....1.2.
0080 30 01 63 1a 00 68 00 69 00 20 00 66 00 65 00 6d 0.c..h.i . .f.e.m
0090 00 74 00 6f 00 3f 00 20 00 5e 00 5e 00 2a 00 3b .t.o.?. .^.^.*.;
00a0 40 01 00 00 00 00 @.....

# CellNet Fundamental Problem?



# No Authentication/Session Management

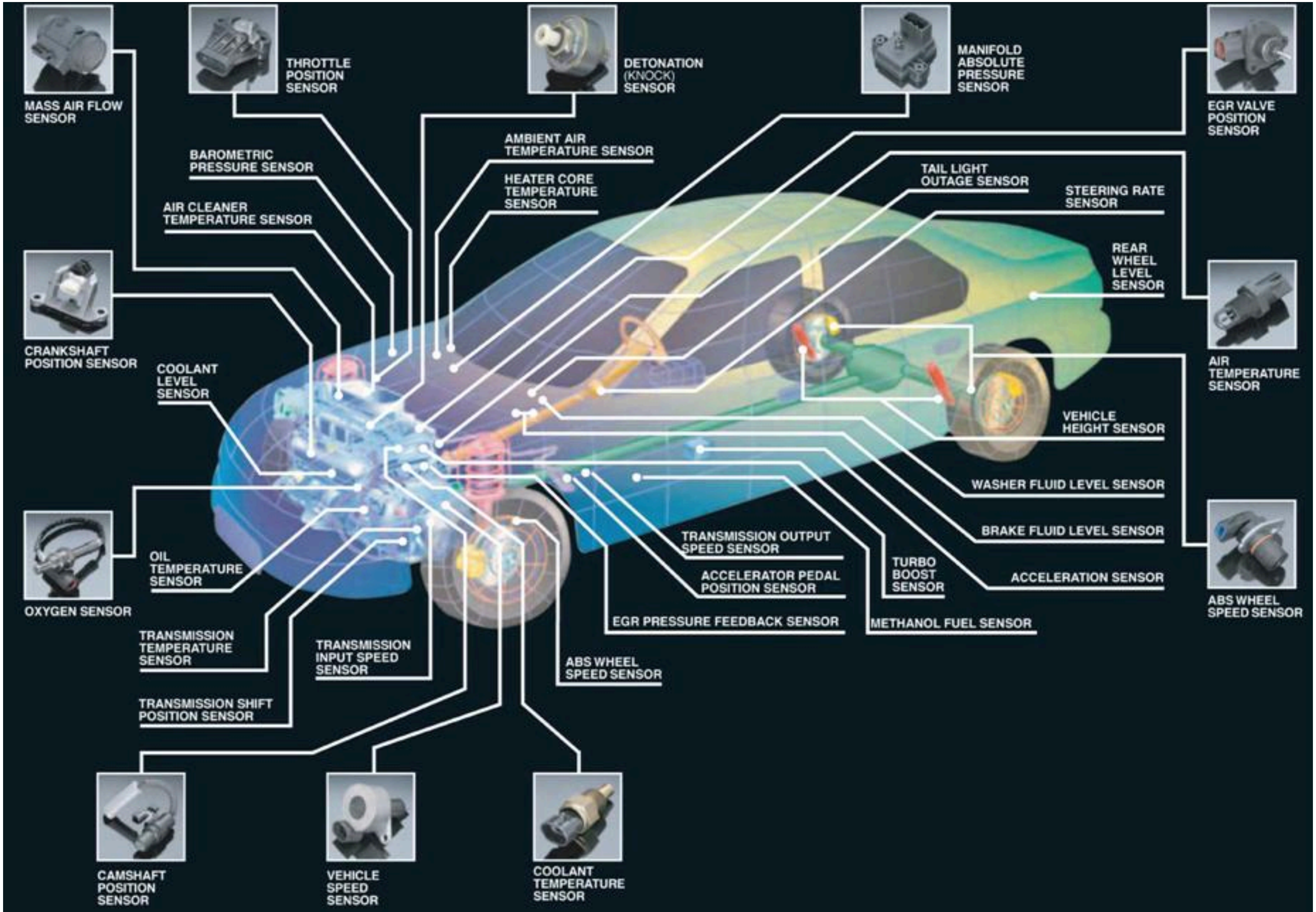
- No authentication
  - Make a call with a fake number
- No session management

  * In a normal call, one user can call to only one person

  - Send multiple INVITE messages
    - Several call sessions are established
    - For each call session, high-cost bearer is established
  - Even one sender can deplete resources of the core network

| Weak Point | Vulnerability | US-1 | US-2 | KR-1 | KR-2 | KR-3 | Possible Attack |
|---|---|---|---|---|---|---|---|
| IMS | No Authentication | X | X | O | O | X | Caller Spoofing |
| | No Session Management | O | O | O | X | O | Denial of Service on core Network |


vim (vim)
..dia tunneling (zsh)
adb (adb)
do_phishing = True
send_GangnamStyle = True
caller_ip = "[redacted].100.196"
caller_phone_no = "[redacted]0606"
to_whom = "[redacted]7183"
NORMAL BR: master | sip_client_spoof.py <os | utf-8 | python 11% LN 67:1
CALLEE
11:26 PM
YouTube
Phone
Messages
Contacts
Internet
Apps
CALLER
Phone
TALK
ATTACKER
31% 11:26 PM
Tap to add current location
11:26 PM
Tue, Sep 29
Welcome to Smart Notice!
Getting started... Please wait.
Google


MASS AIR FLOW SENSOR
THROTTLE POSITION SENSOR
DETONATION (KNOCK) SENSOR
MANIFOLD ABSOLUTE PRESSURE SENSOR
EGR VALVE POSITION SENSOR
AMBIENT AIR TEMPERATURE SENSOR
BAROMETRIC PRESSURE SENSOR
HEATER CORE TEMPERATURE SENSOR
TAIL LIGHT OUTAGE SENSOR
STEERING RATE SENSOR
AIR CLEANER TEMPERATURE SENSOR
REAR WHEEL LEVEL SENSOR
CRANKSHAFT POSITION SENSOR
COOLANT LEVEL SENSOR
AIR TEMPERATURE SENSOR
VEHICLE HEIGHT SENSOR
WASHER FLUID LEVEL SENSOR
BRAKE FLUID LEVEL SENSOR
OXYGEN SENSOR
OIL TEMPERATURE SENSOR
TRANSMISSION OUTPUT SPEED SENSOR
ACCELERATOR PEDAL POSITION SENSOR
TURBO BOOST SENSOR
ACCELERATION SENSOR
ABS WHEEL SPEED SENSOR
EGR PRESSURE FEEDBACK SENSOR
METHANOL FUEL SENSOR
TRANSMISSION TEMPERATURE SENSOR
TRANSMISSION INPUT SPEED SENSOR
ABS WHEEL SPEED SENSOR
TRANSMISSION SHIFT POSITION SENSOR
CAMSHAFT POSITION SENSOR
VEHICLE SPEED SENSOR
COOLANT TEMPERATURE SENSOR

# Sensors

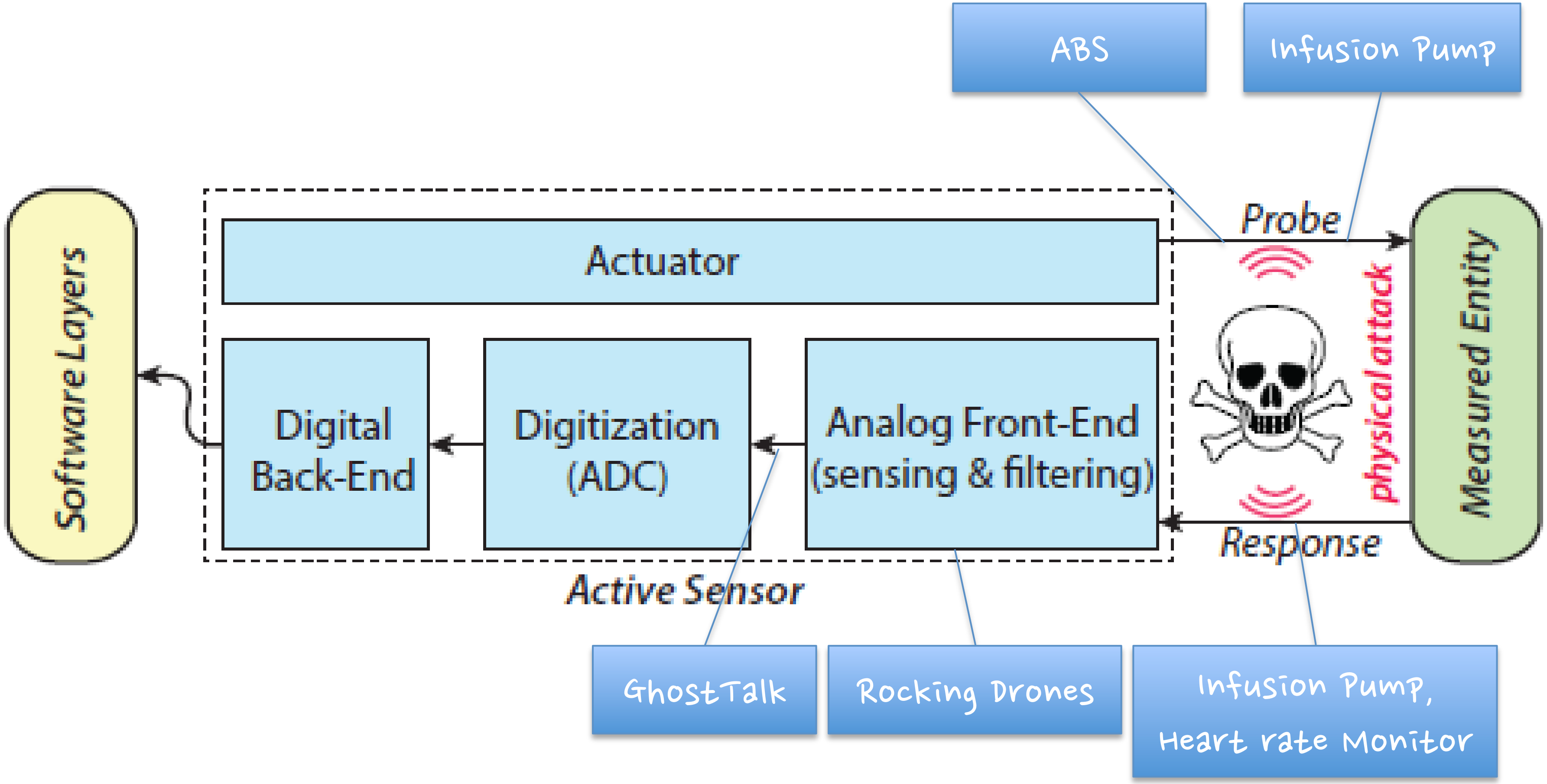
## Passive Sensors

- Measure ambient energy
- Do not make any output
- e.g. thermometer, barometer, gyroscope, accelerometer, pressure meter, etc.

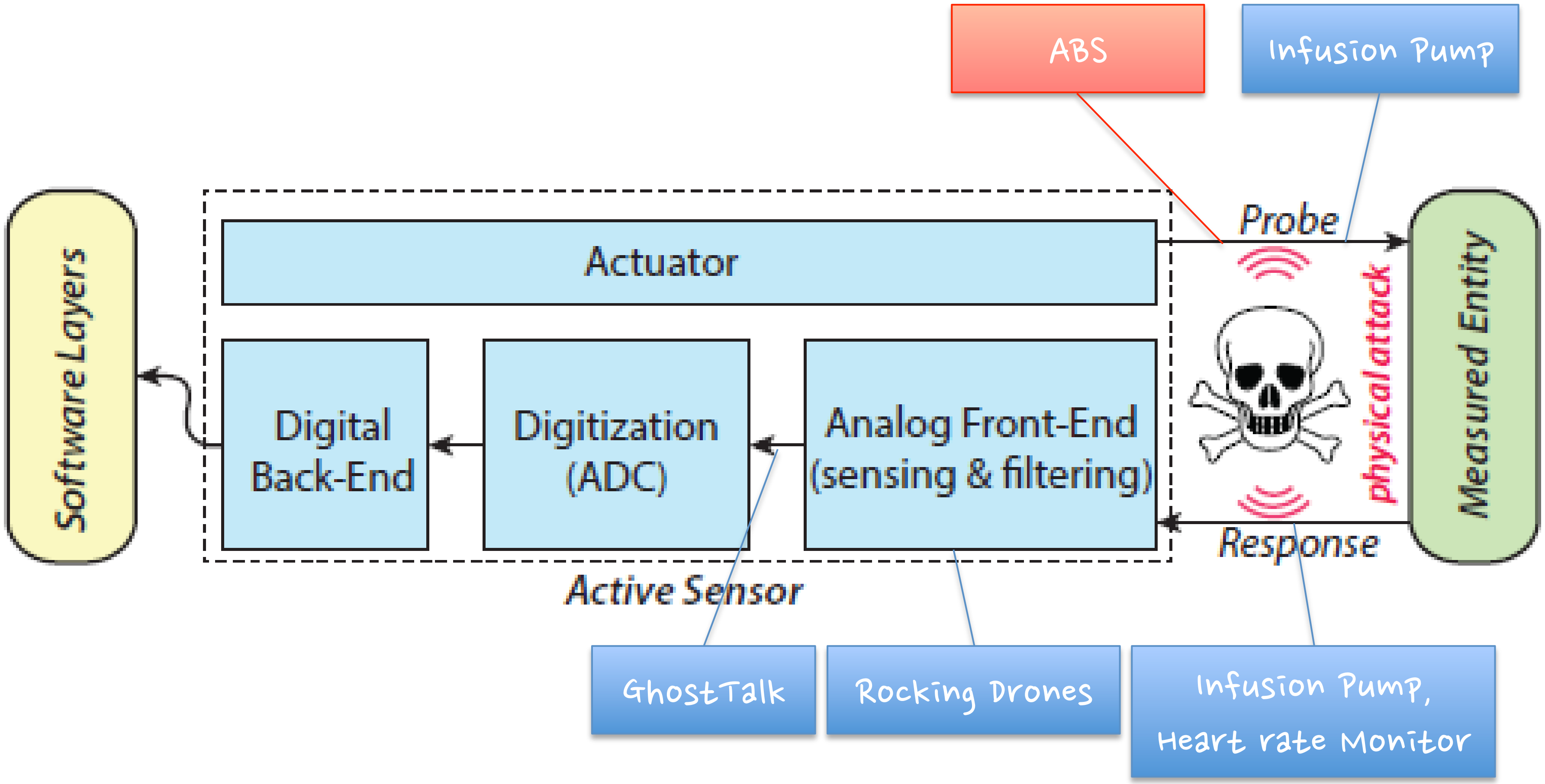
## Active Sensors

- Measure echoes
- Exert self-generated energy to the measured entity
- e.g. ultrasound sonar, radar, LiDAR, optical/magnetic encoder, etc.

# Typical Sensor Architecture

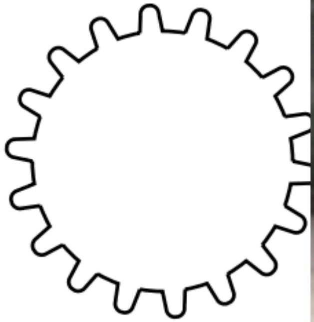


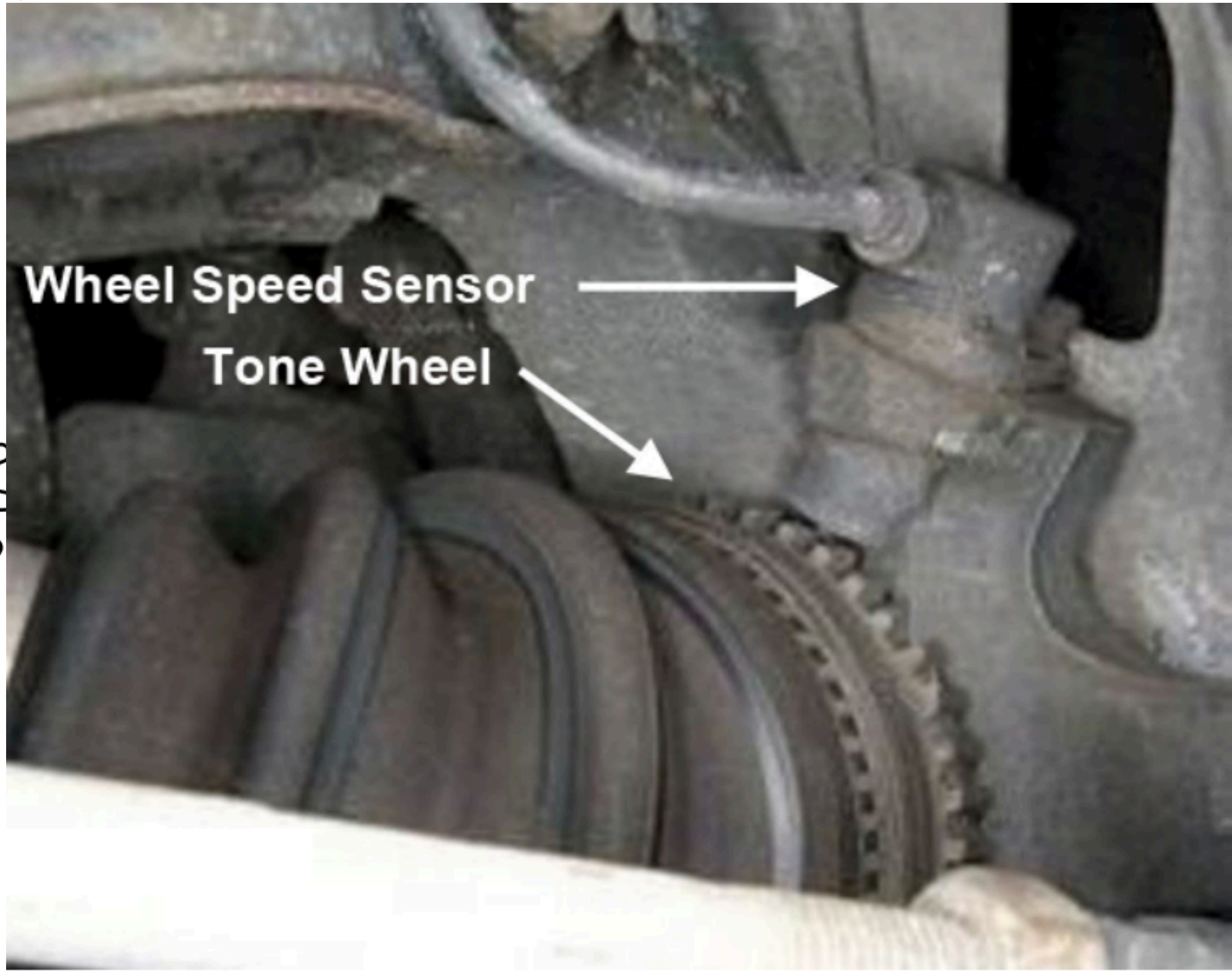
# Typical Sensor Architecture



# ABS

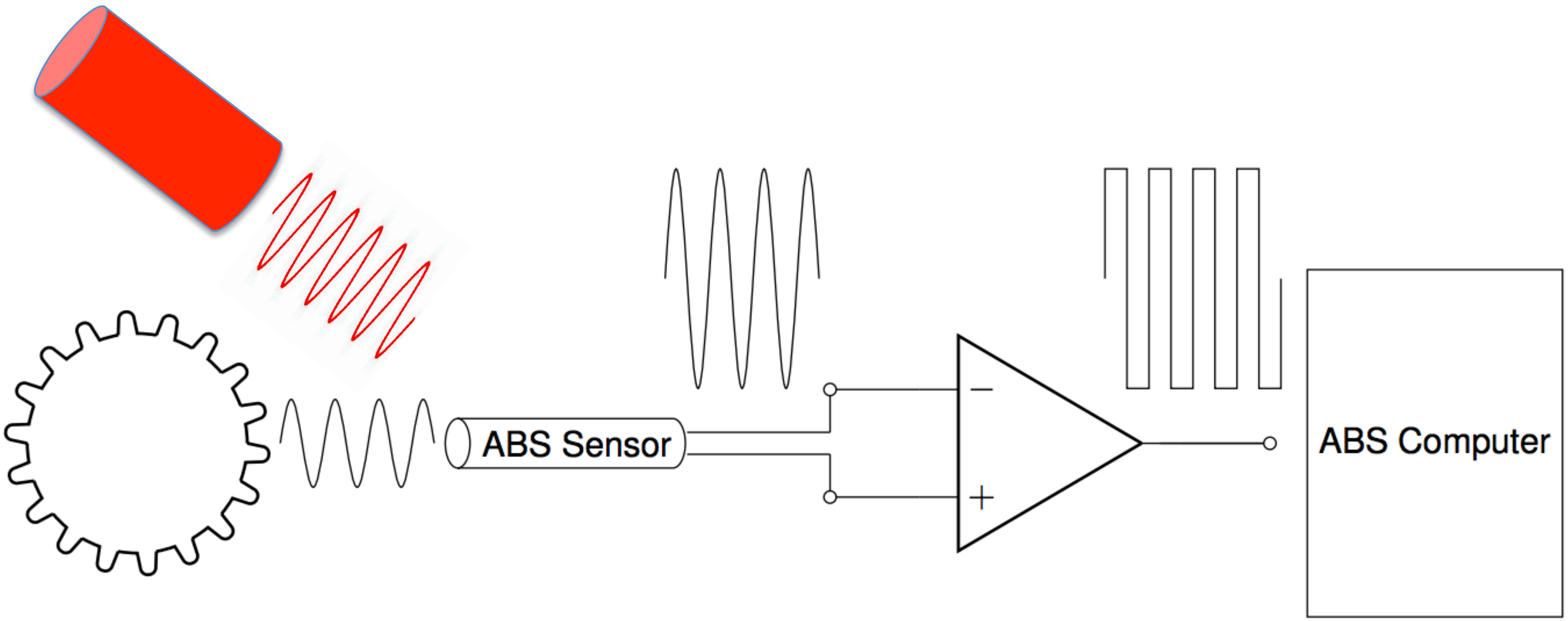
Yasser Shoukry, Paul Martin, Paulo Tabuada, and Mani Srivastava. 2013.
Non-invasive





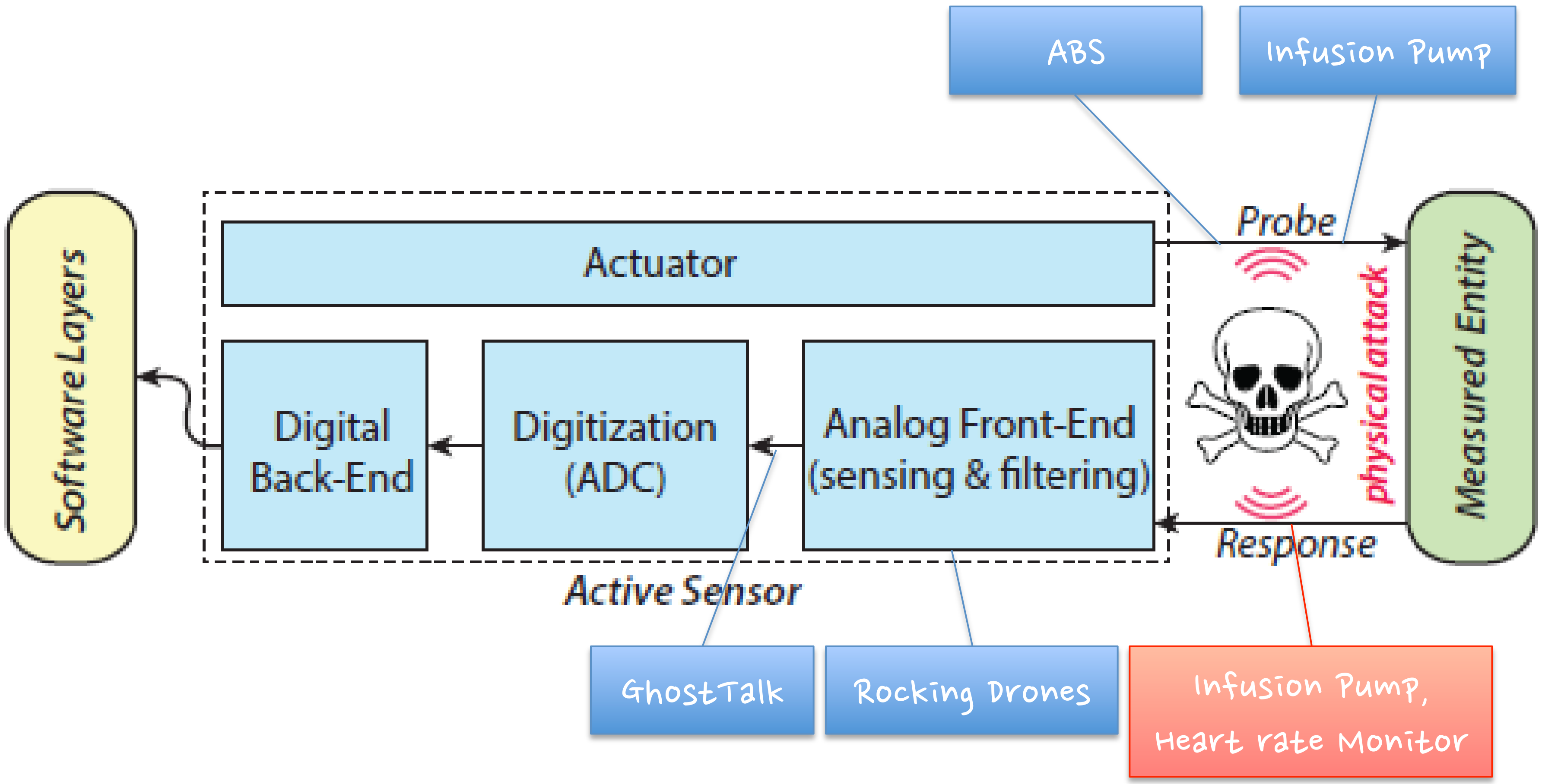

S Computer

# ABS Attack



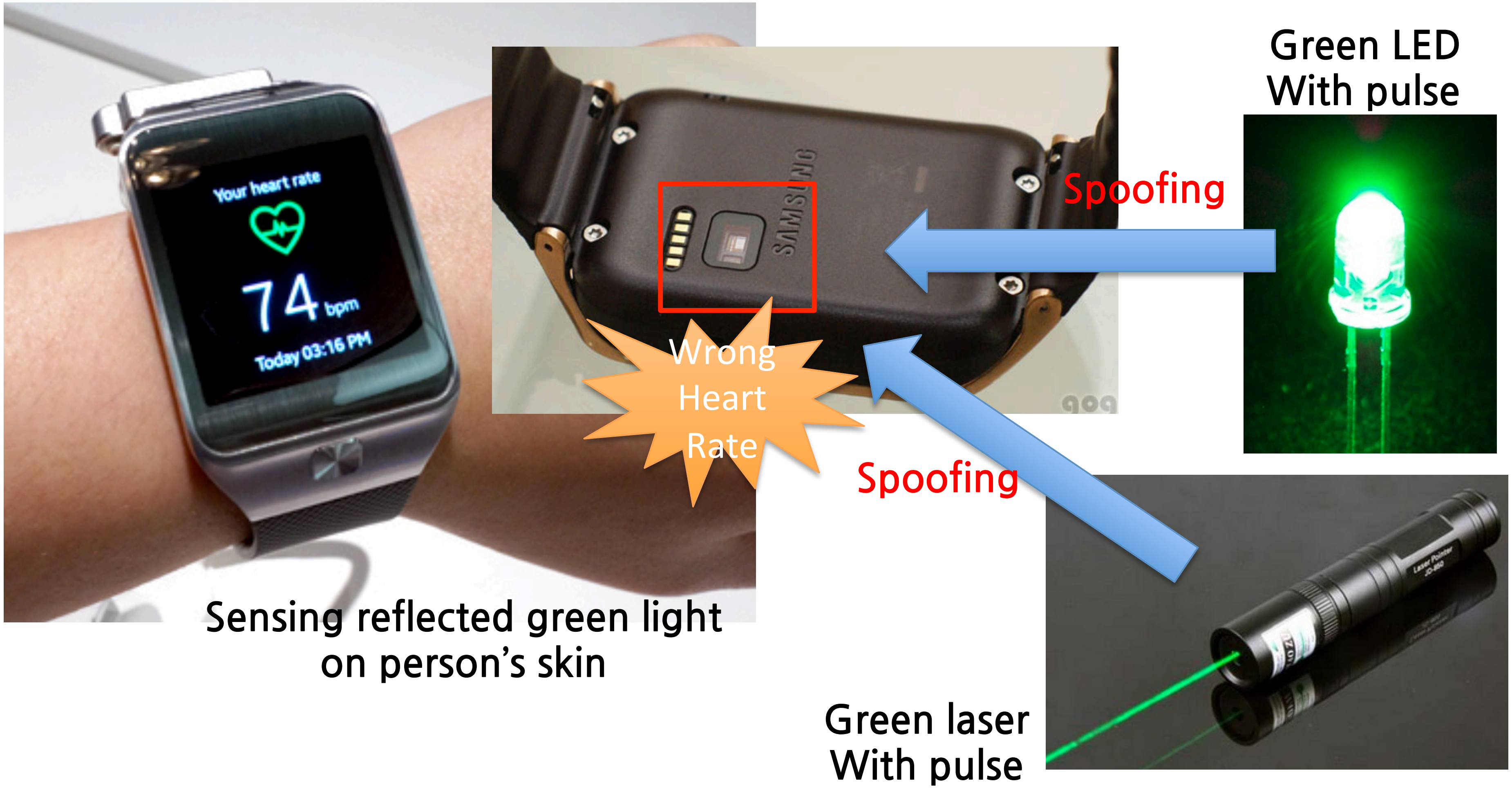

Basic speed sensor operation for ABS systems

# Typical Sensor Architecture



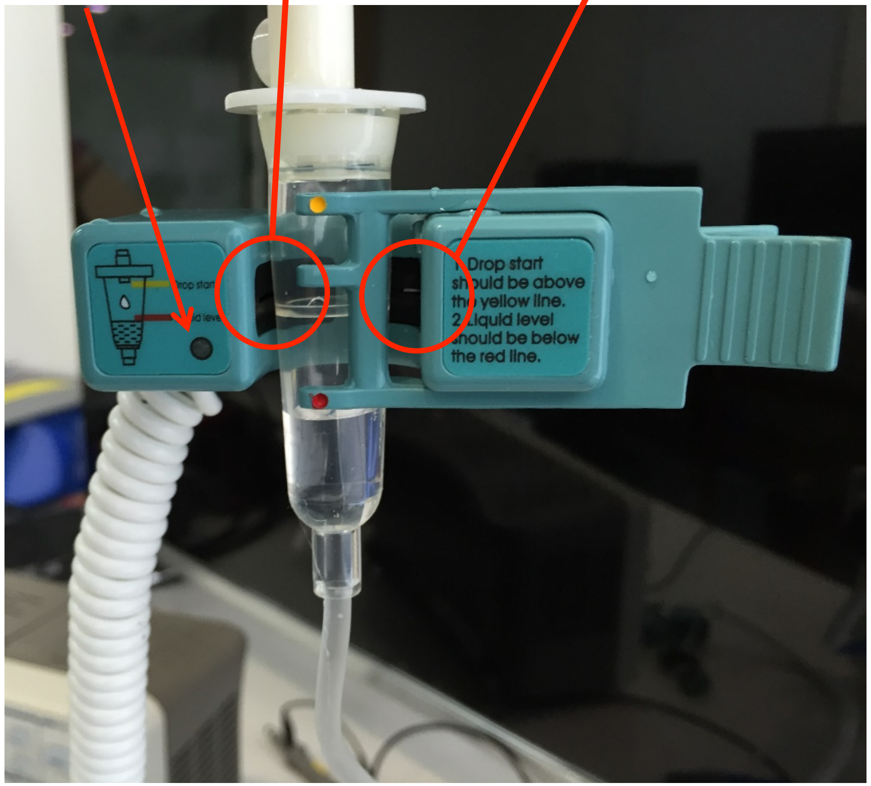
# Heart Rate Sensor Spoofing

- Heart rate sensor using green light (Galaxy gear)

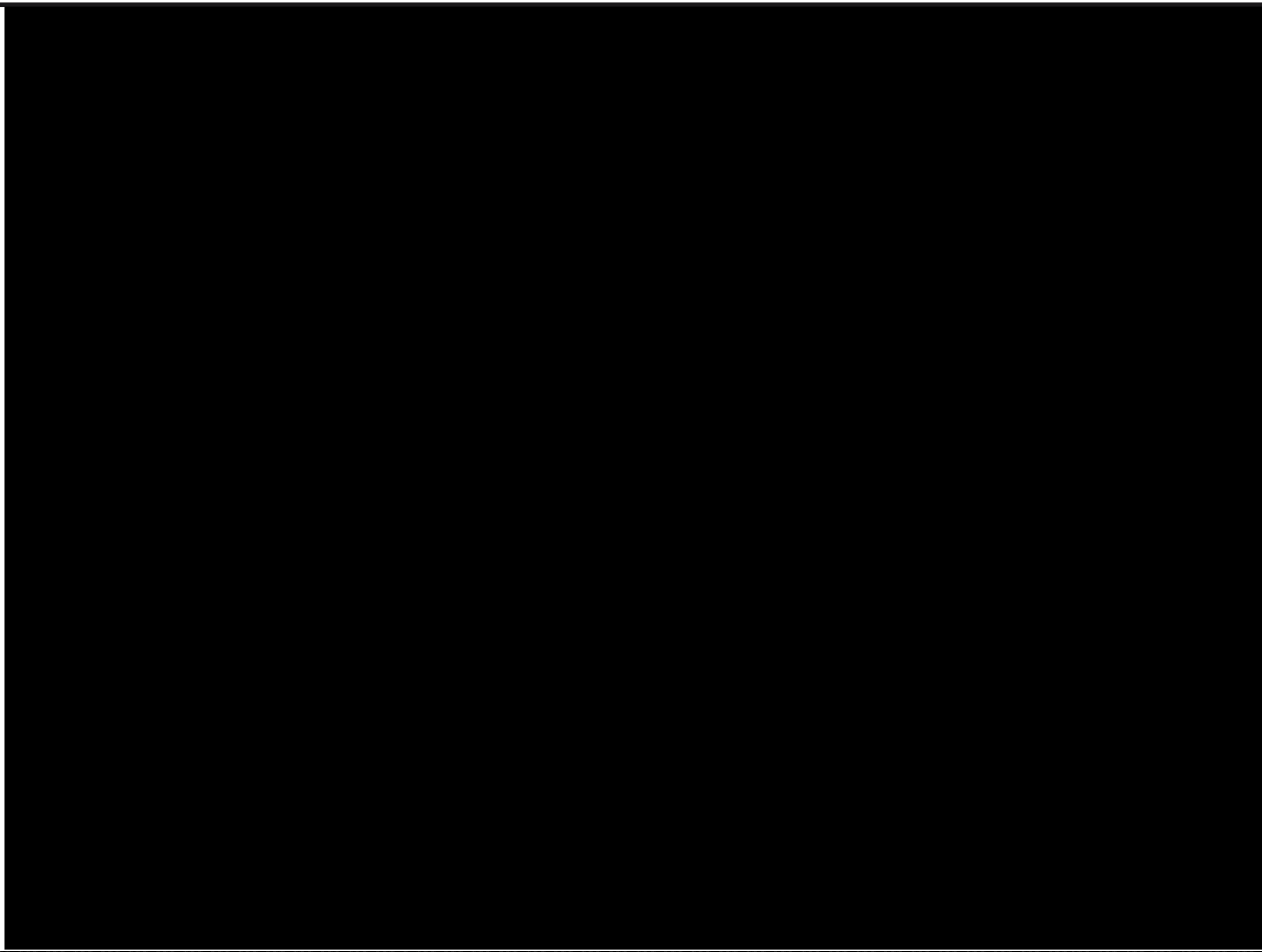


# Heart Rate Sensor Spoofing

# Infusion Pump

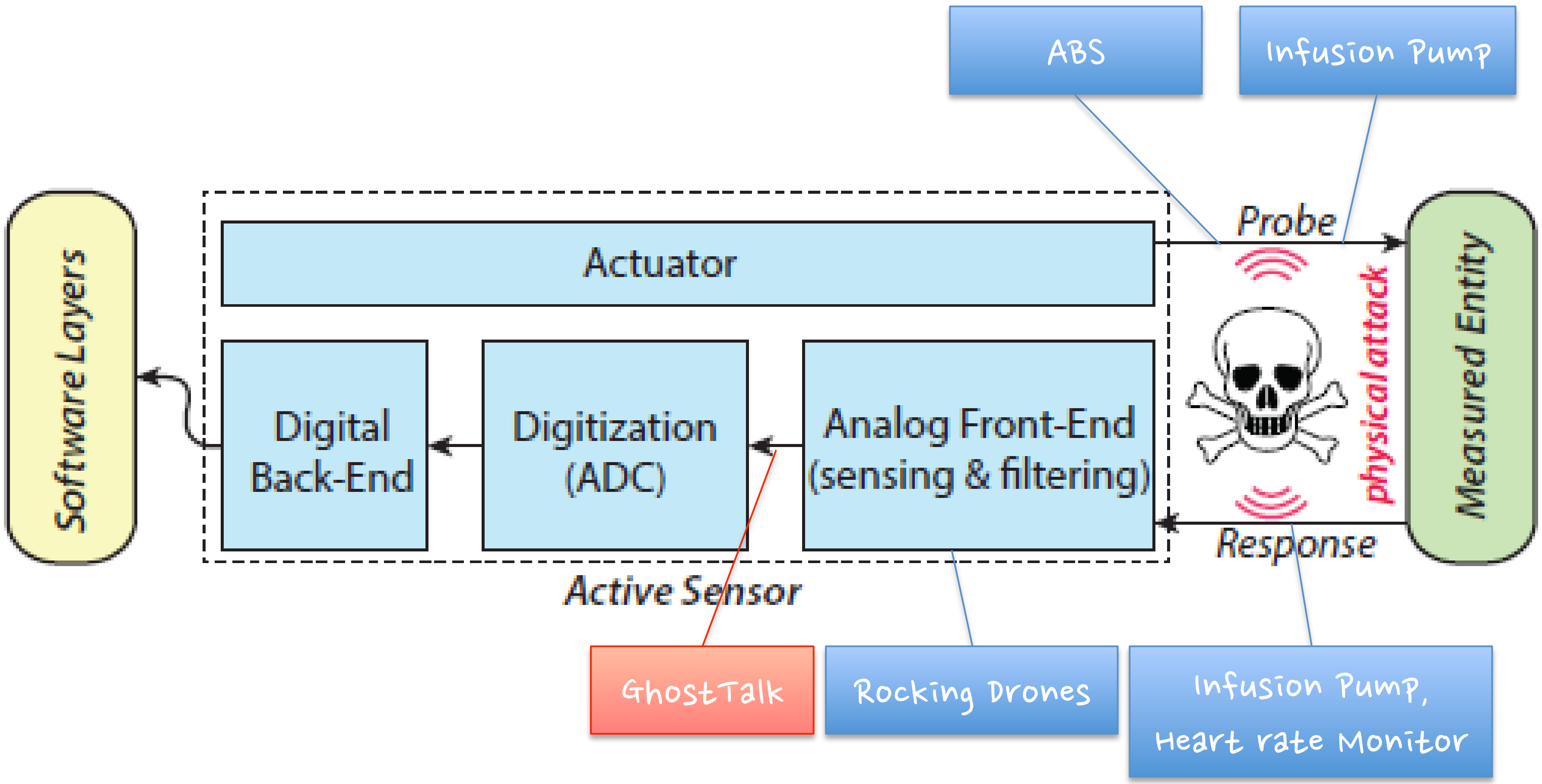



# Infusion Pump Demo 1



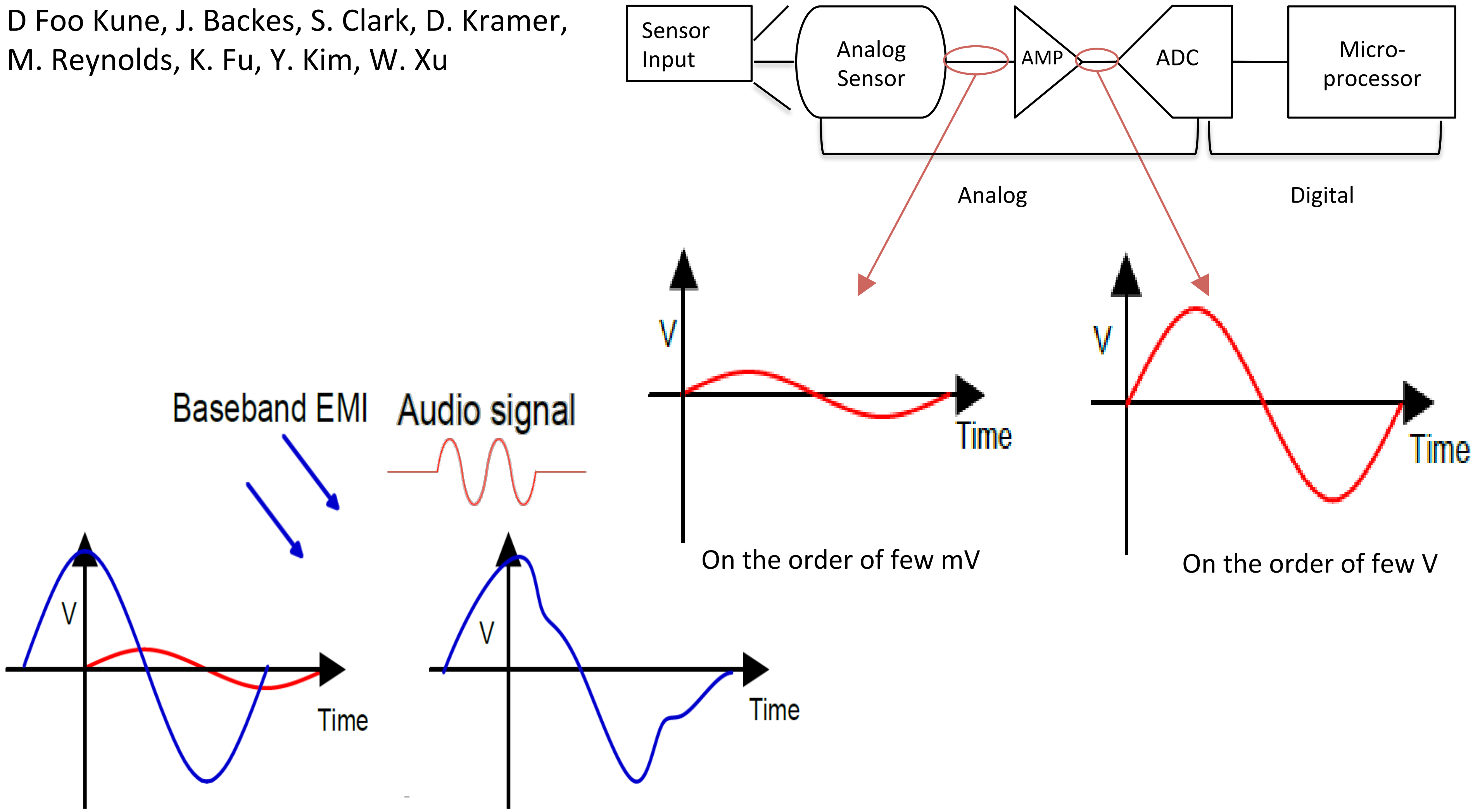
# Infusion Pump Demo 2

# Typical Sensor Architecture

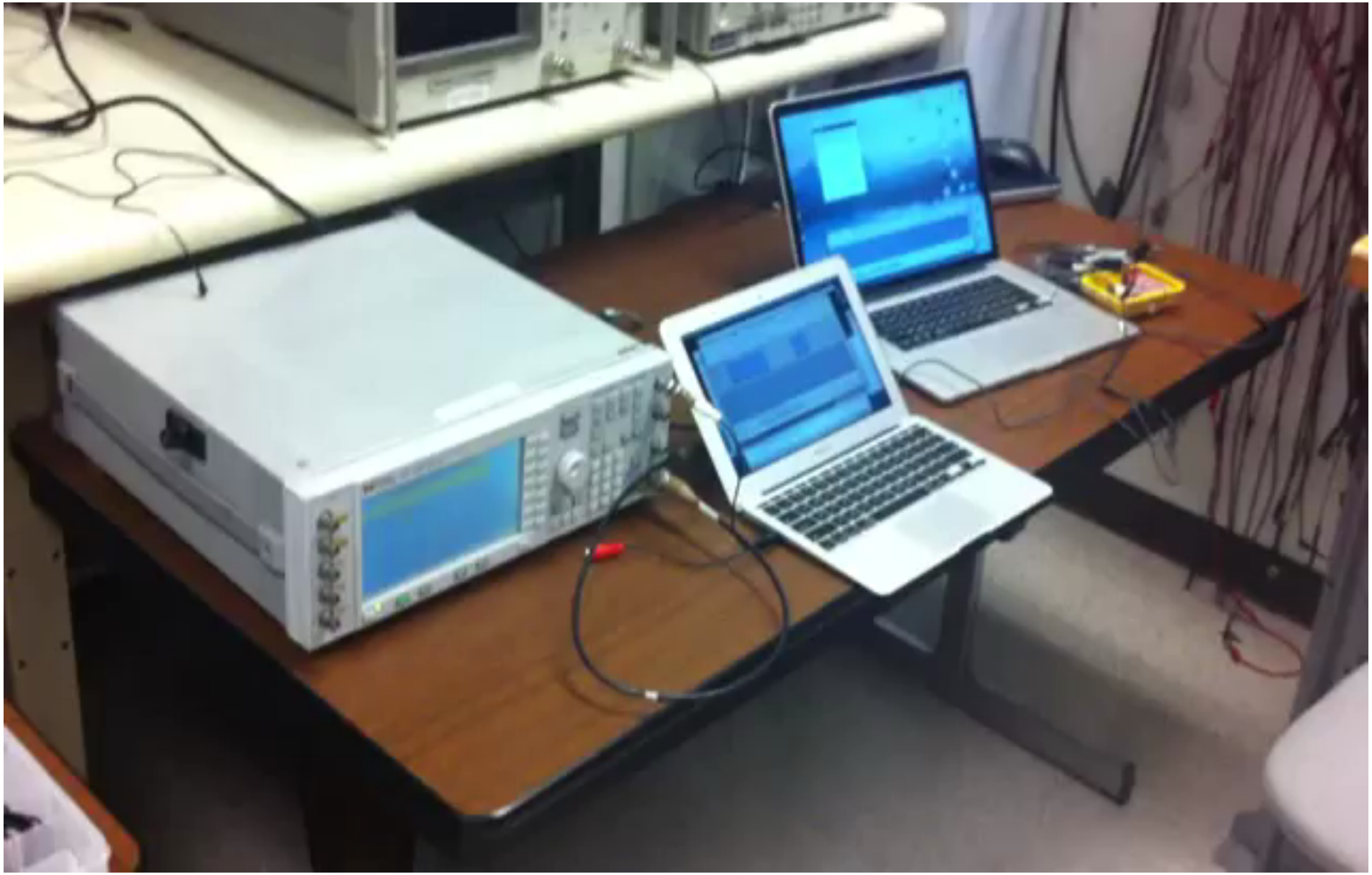


# Signal Injection using EMI [oakland13]

D Foo Kune, J. Backes, S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, W. Xu



# Signal Injection using EMI [Oakland13]



# Application to medical devices

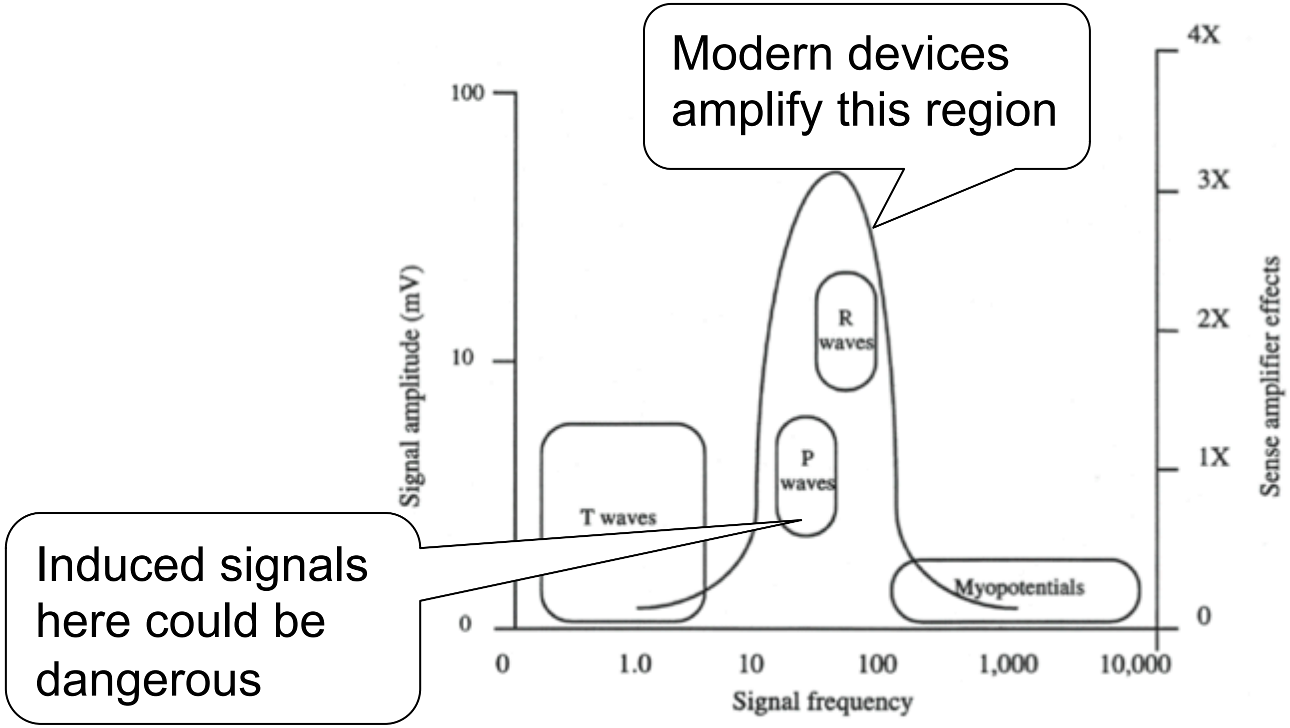


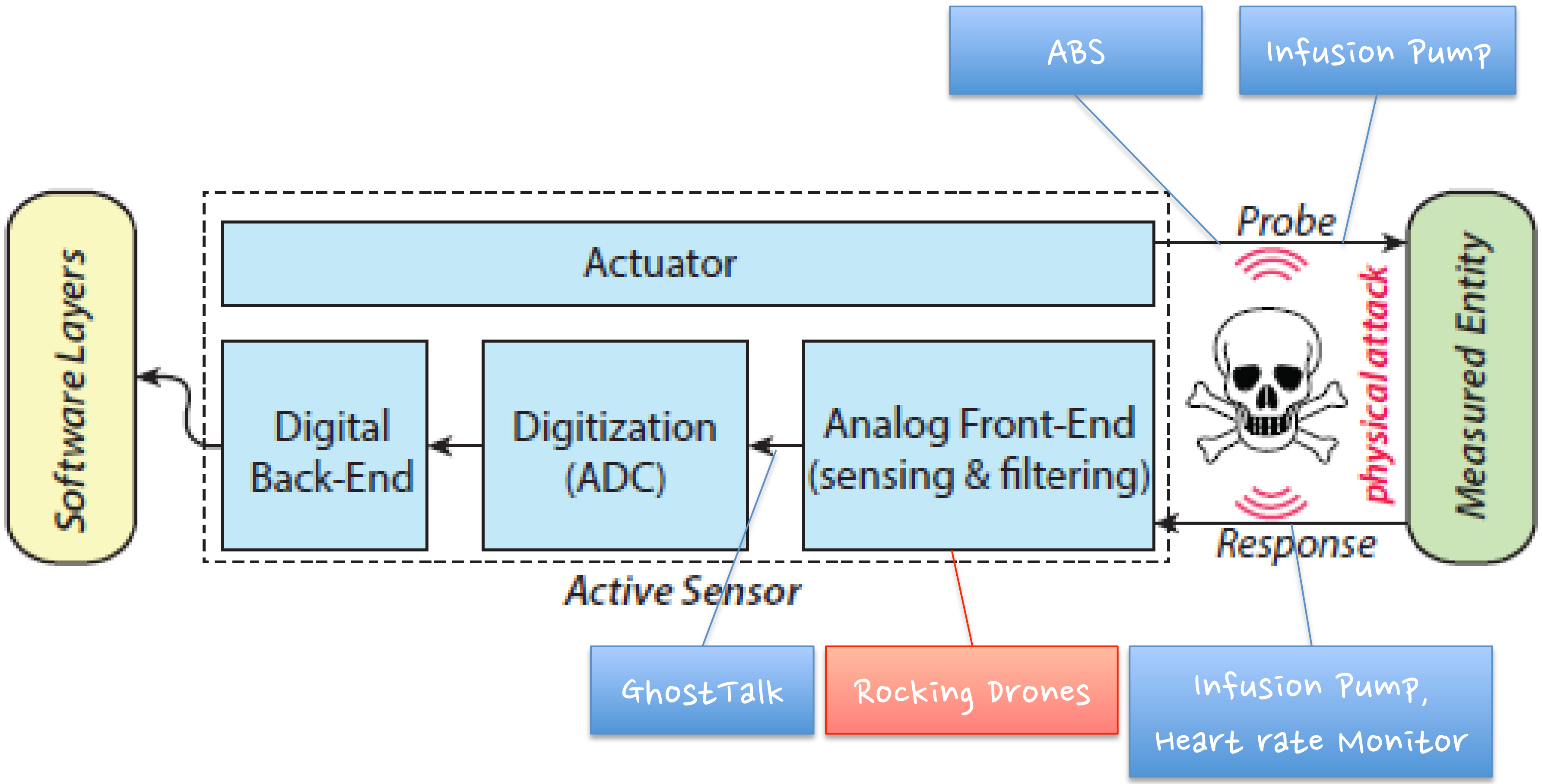

**Fig 17.1** Signal amplitude and frequency from various sources. Modern sense amplifiers employ bell-shaped response curves that amplify signals within the 10–100 Hz range while attenuating signals below and above these frequencies. In this way signals from ventricular depolarization (R waves) and atrial depolarization (P waves) can be amplified and the effects from spurious signals, such as T waves and myopotentials, can be minimized.

# Standard Lead Design

# Results

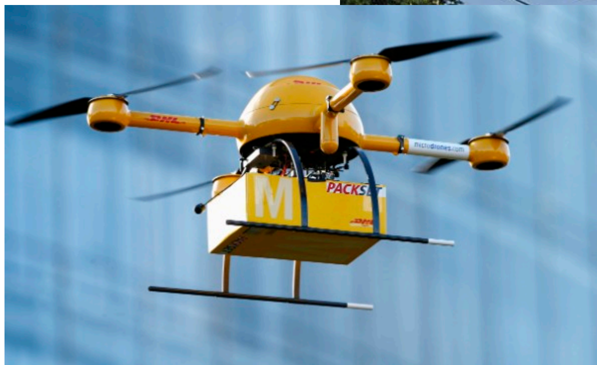
| Device | Open air | Saline | SynDaver |
|---|---|---|---|
| Medtronic Adapta | 1.36m | 0.03m | Unknown |
| Medtronic Insync Sentry | 1.57m | 0.05m | 0.08m |
| Boston Scientific ICD | No response | Unknown | Unknown |
| St. Jude ICD | 0.76m | Unknown | Unknown |

# Typical Sensor Architecture



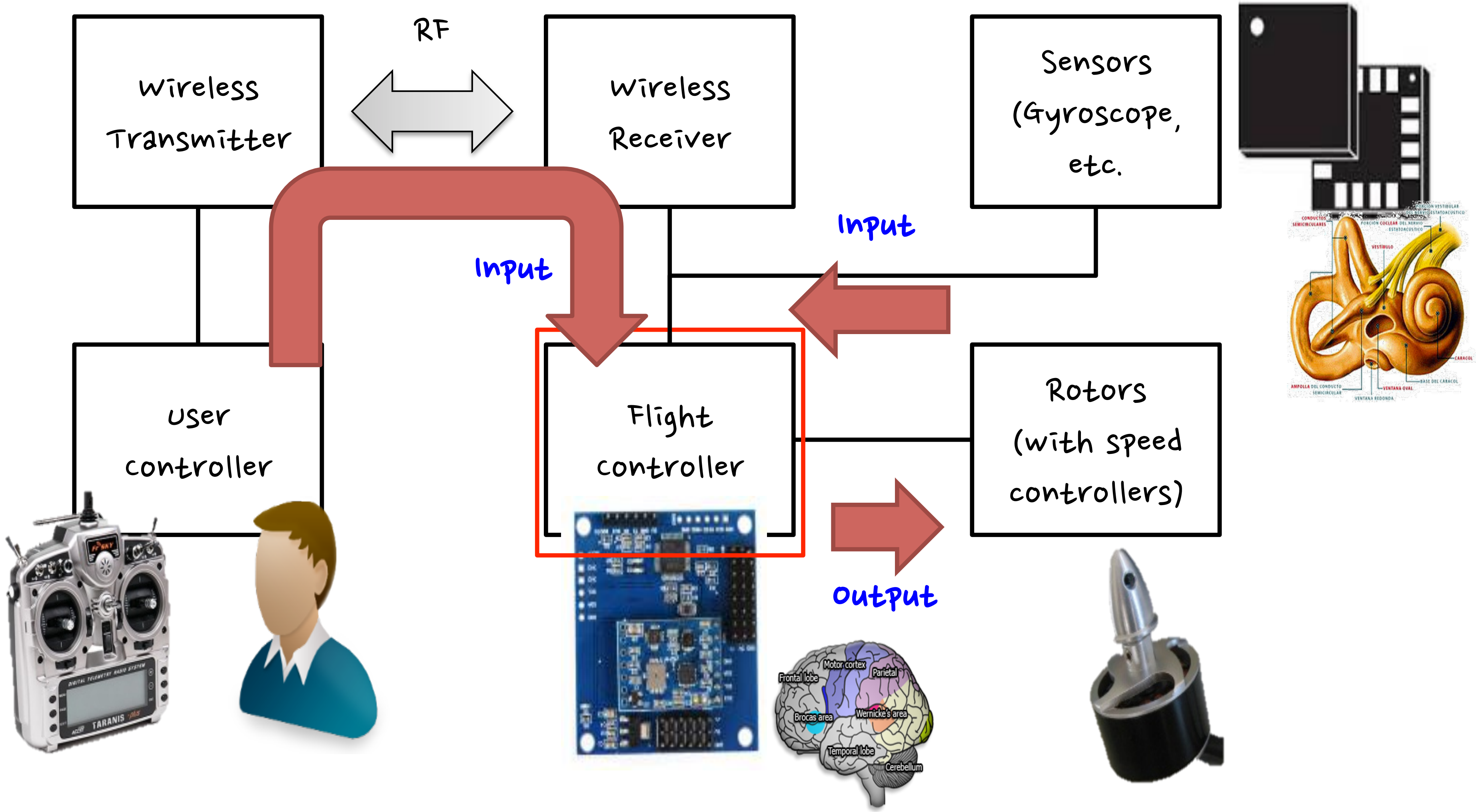
# Drones (Multicopters)

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



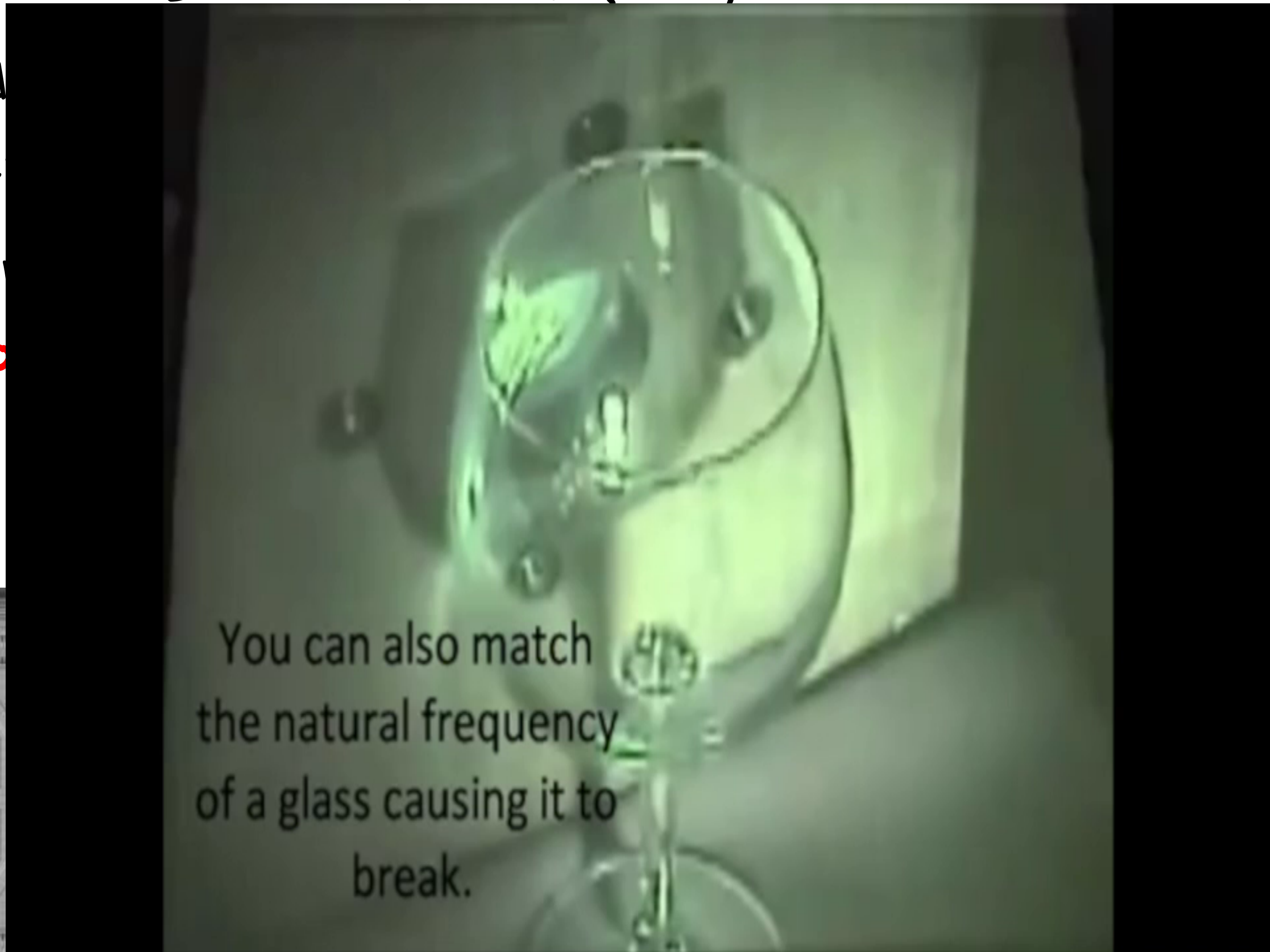
# Drone controlling

Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, Y. Kim,
Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors, Usenix Sec 2015



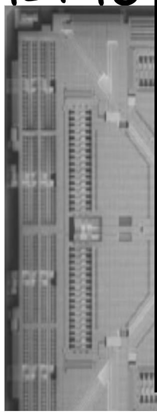
# Gyroscope on Drone

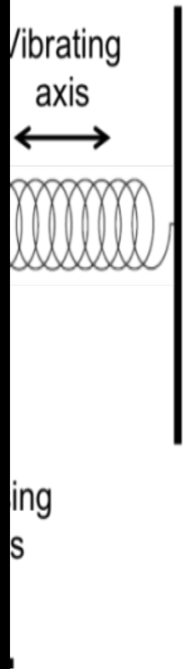
- Inertial Measurement Unit (IMU)
  - A d
    orie
  - usi
    gyro




…S gyro.>

- MEMS





# Resonance in MEMS Gyroscope

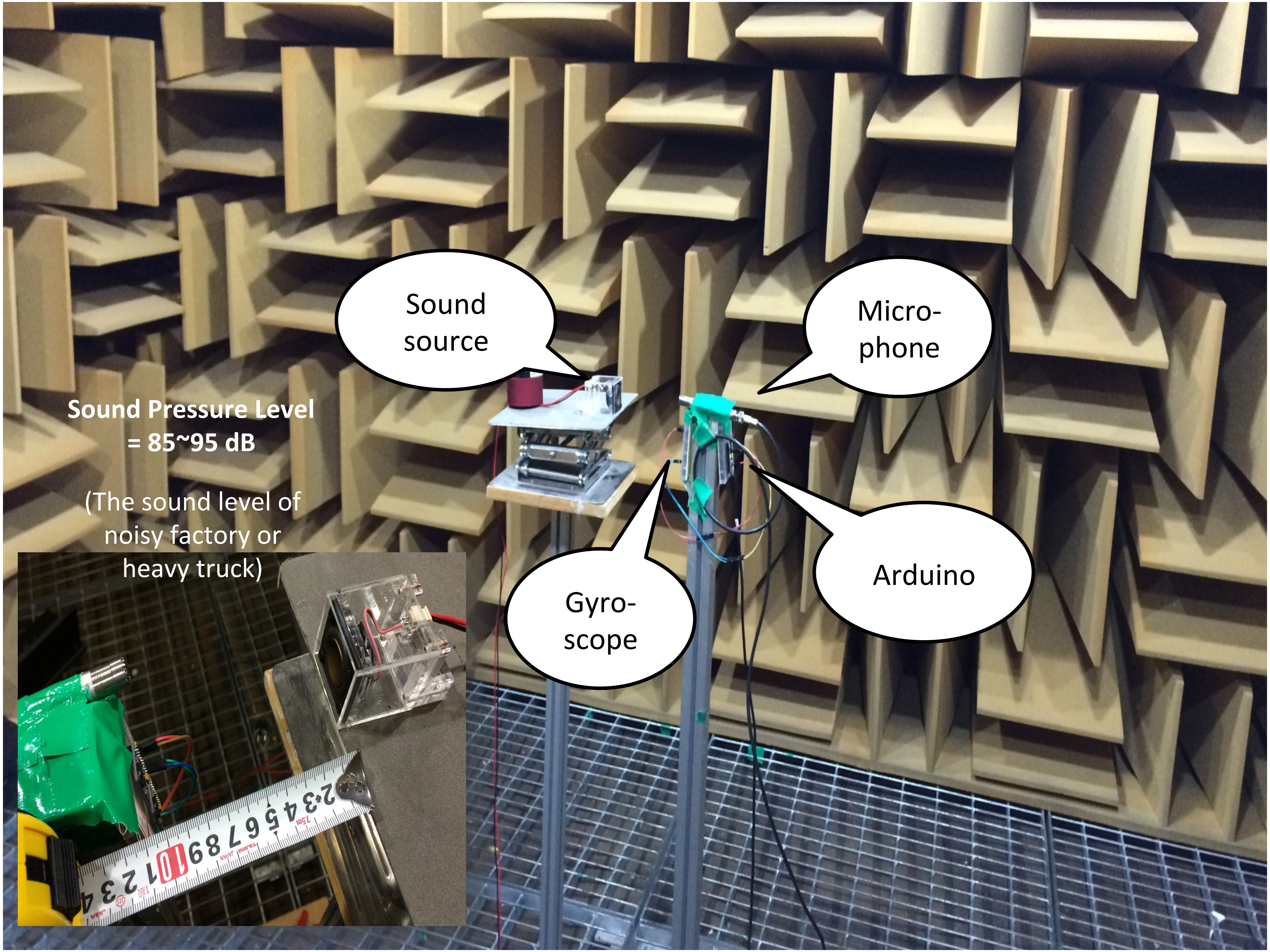
- Mechanical resonance by sound noise
  - Known fact in the MEMS comm
  - Degrades MEMS Gyro's accuracy
  - With (resonant) frequencies of

**L3GD20**

**Features**

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

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


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

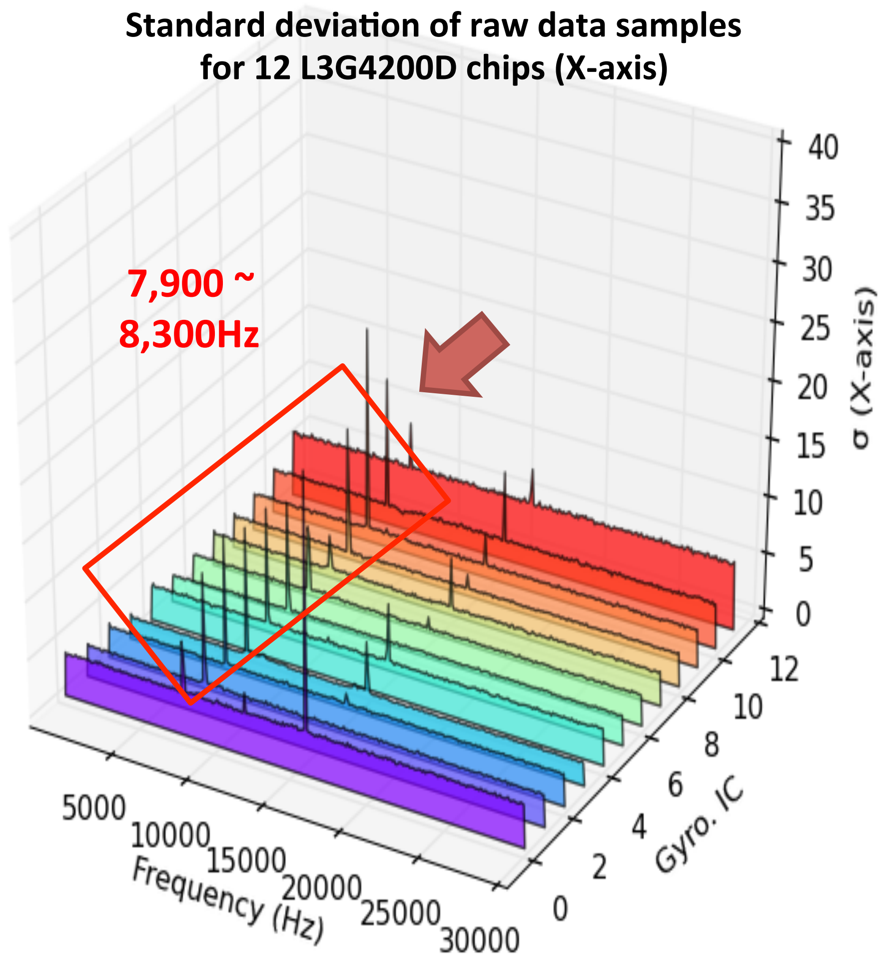
# Experimental Results (1/3)

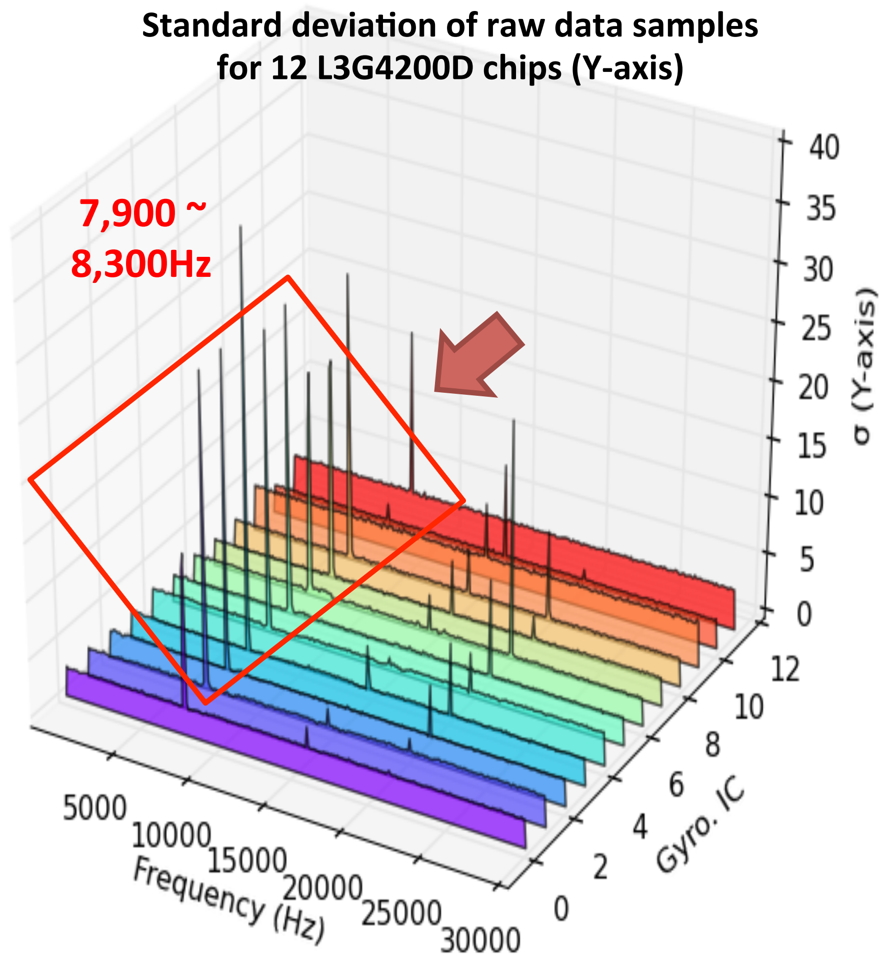
- Found the resonant frequencies of 7 MEMS gyroscopes

| 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)<br>27 ~ 33 kHz (Y)<br>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)

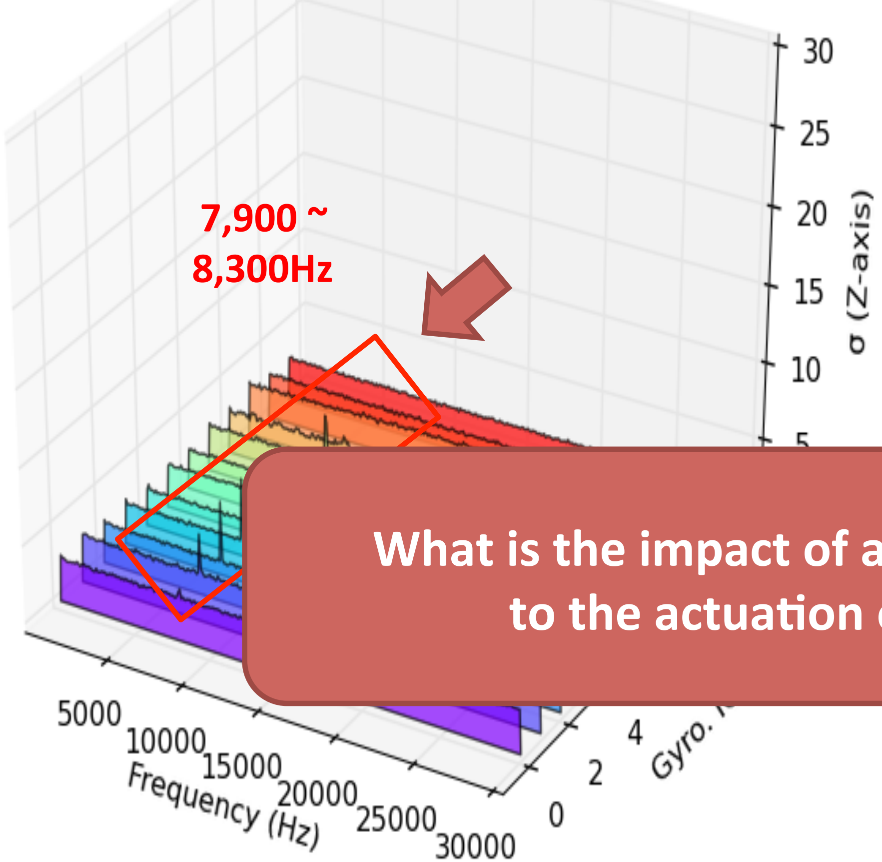


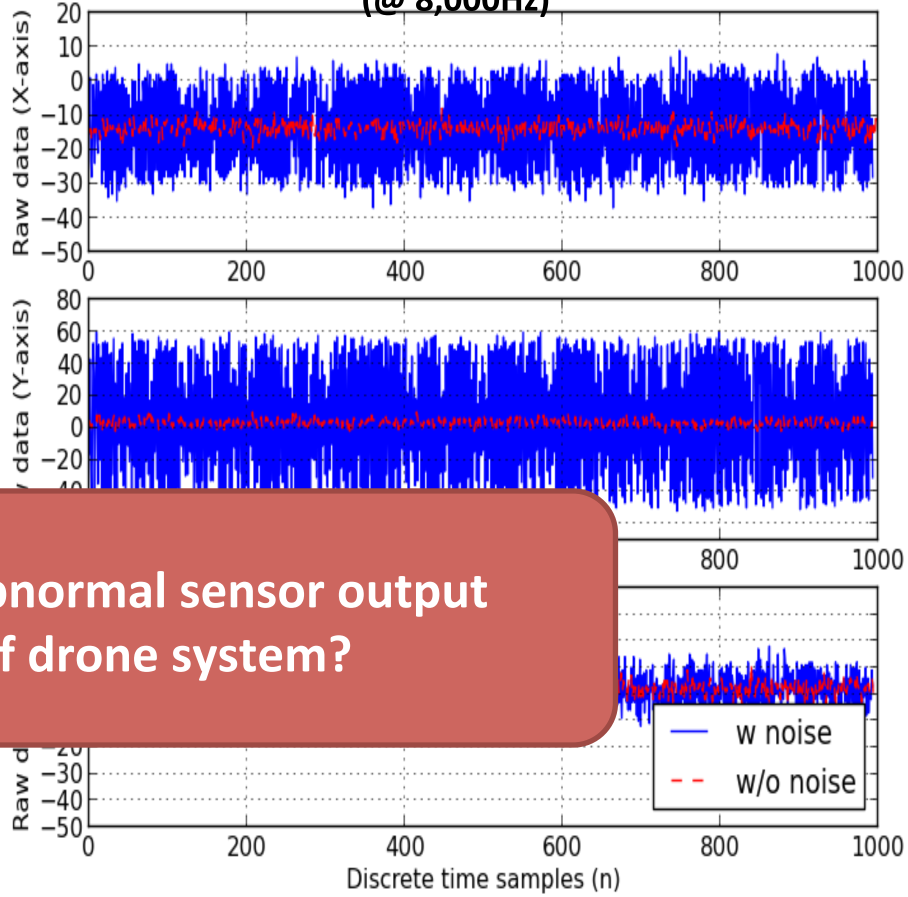
# Experimental Results (3/3)

- 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 (@ 8,000Hz)




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



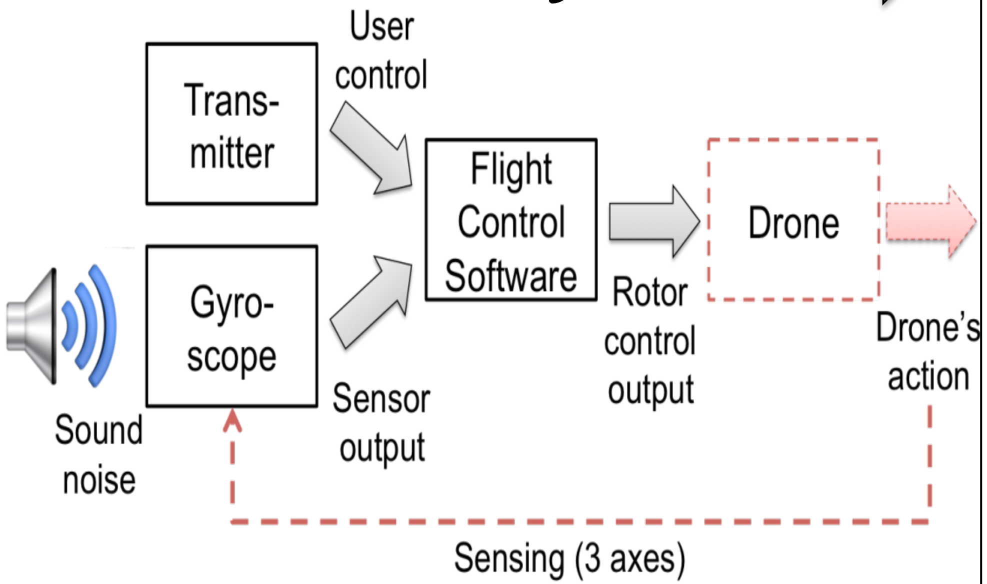
SysSec System Security Lab

# Software A

- Two open-source firmware pro
  - Multiwii project
  - ArduPilot project

Proportional-Integral
-Derivative control

- Rotor control algorit




**for** *axis* **do**

$P = txCtrl[axis] - \boxed{gyro[axis]} \times G_P[axis];$

$error = txCtrl[axis]/G_P[axis] - gyro[axis];$

$error_{accumulated} = error_{accumulated} + error;$

$I = error_{accumulated} \times G_I[axis];$

$\boxed{delta = gyro[axis] - gyro_{last}[axis];}$

$delta_{sum} =$ sum of the last three delta values;

$D = delta_{sum} \times G_D[axis];$

$\boxed{PIDCtrl[axis] = P + I - D;}$

**end**

**for** *rotor* **do**

**for** *axis* **do**

$\boxed{rotorCtrl[rotor] = txCtrl[throttle] + PIDCtrl[axis];}$

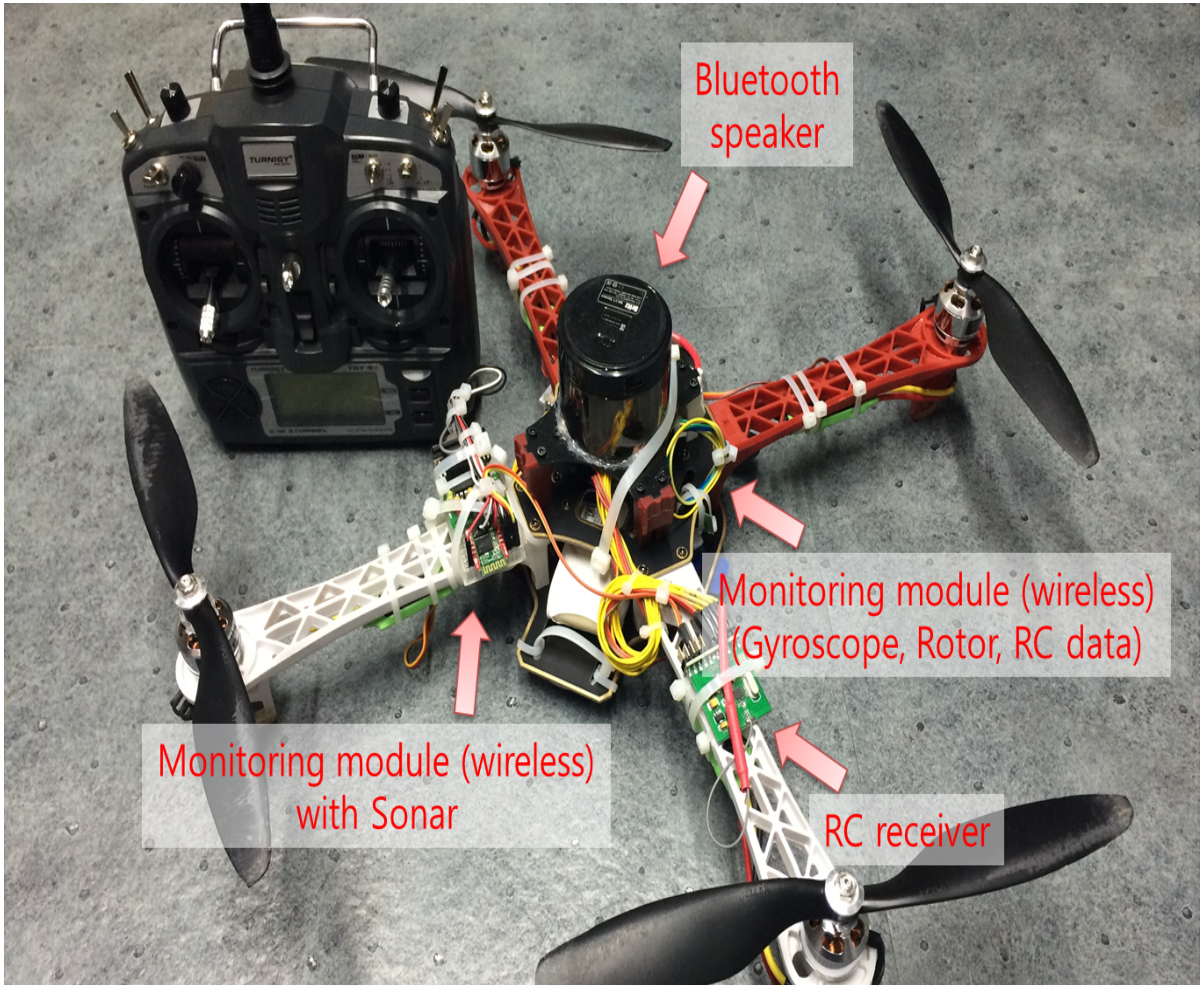
**end**

limit $rotorCtrl[rotor]$ within the pre-defined $\boxed{\text{MIN (1,150)}}$ and $\boxed{\text{MAX (1,850)}}$ values;

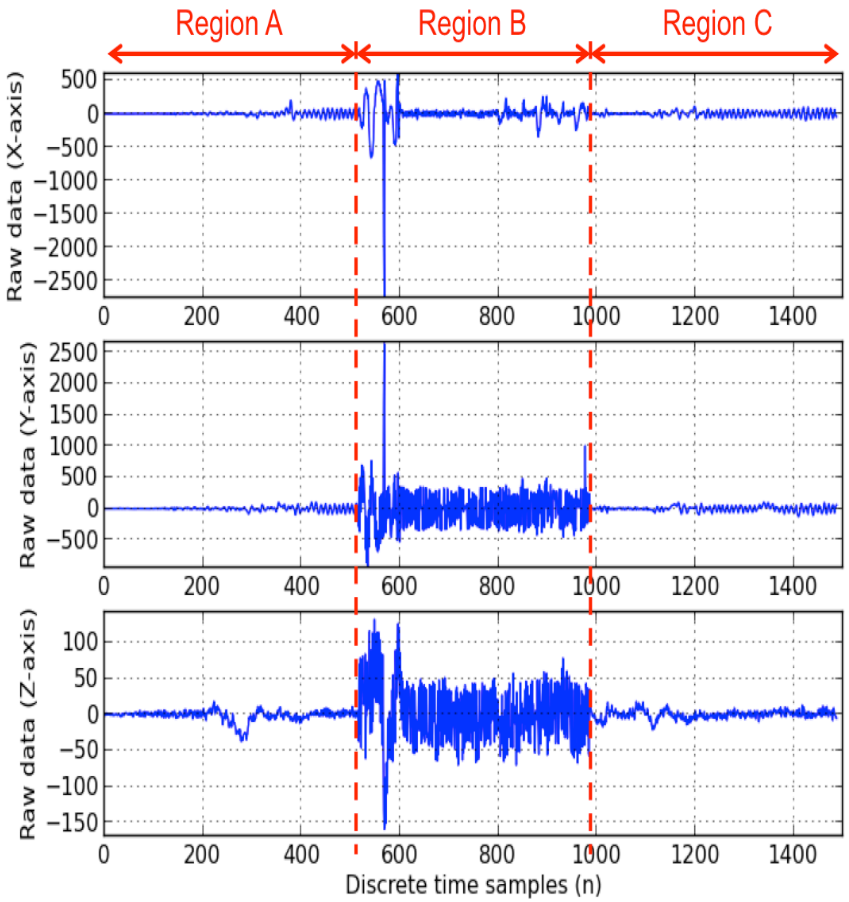
**end**

actuate rotors;

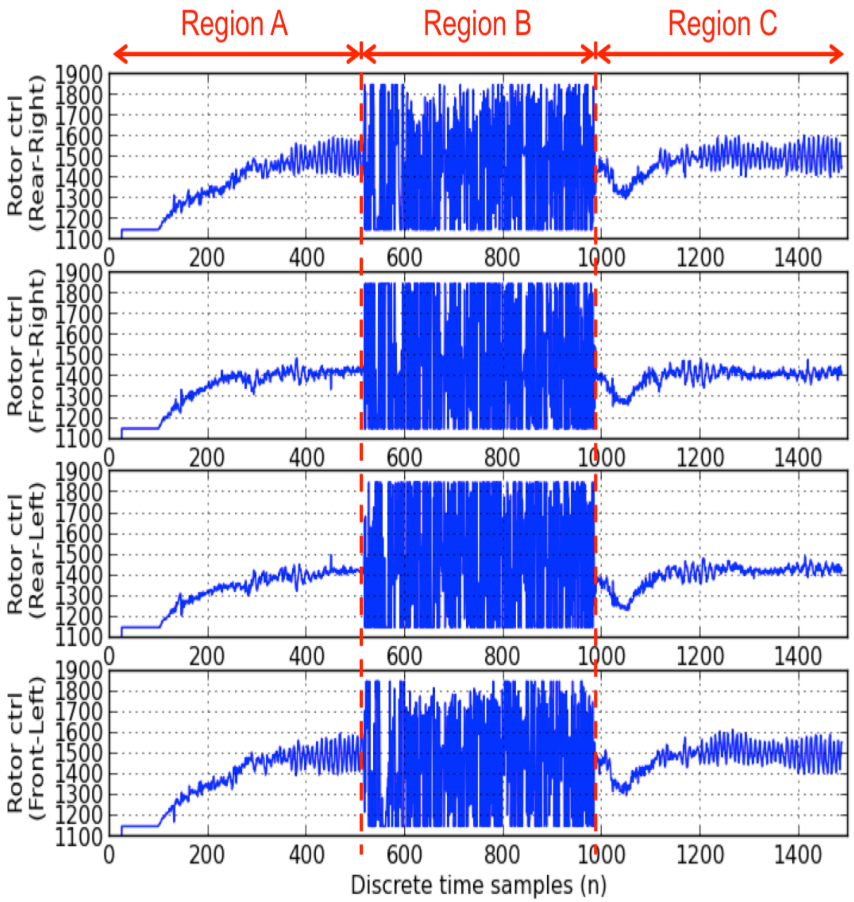
# Attack Demo


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

# Attack Demo




Raw data samples of the gyroscope




Rotor control data samples

# Typical vulnerabilities

- Unsigned/unencrypted Software update
- Unsigned/unencrypted Management/web interface
- Secret keys in binary
- Unprotected hardware debugging
- Massive kernel
- No user permission
- (almost) No code review
- Hidden weak backdoor
- (almost) No logging and editable logs
- Timely patching
- Buffer/Stack/Integer overflow
- CSRF, XSS, …
- Exploitable security solutions
- No or weak software obfuscation
- Non-standard crypto primitives

# Conclusion

- Sensing is one of the most important components of IoT
  - Driverless cars, Drone, Medical devices, SCADA systems, …
- Sensor security has been out of concern
- Time to look at security of sensors
- And it is a lot of fun, but requiring EE knowledge!

# 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"