This Ain't Your Dose: Sensor Spoofing Attack on Medical Infusion Pump

Youngseok Park[1,2], Yunmok Son[2], Hocheol Shin[2], Dohyun Kim[2], and Yongdae Kim[2]

[1] NAVER Labs

[2] System Security Laboratory, KAIST

10th USENIX Workshop on Offensive Technologies (WOOT '16)

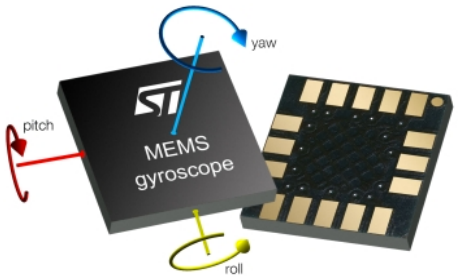
Aug.09.2016

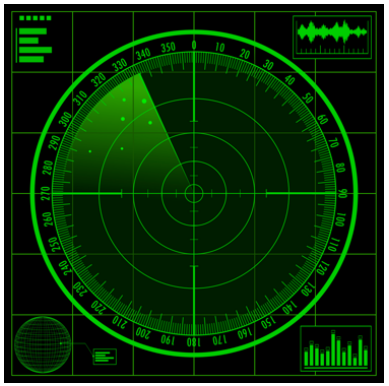
NAVER | L | A | B | S |

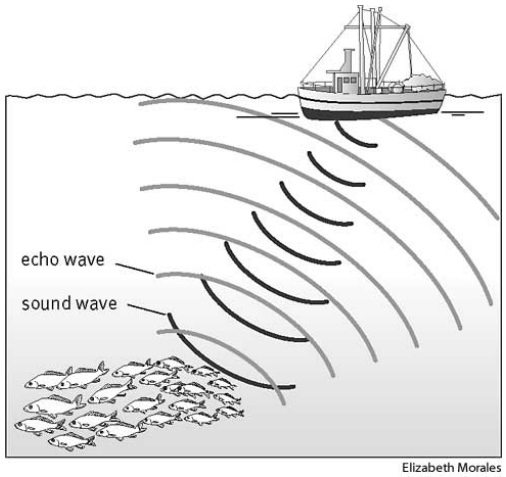
SysSec System Security Lab

Sensor

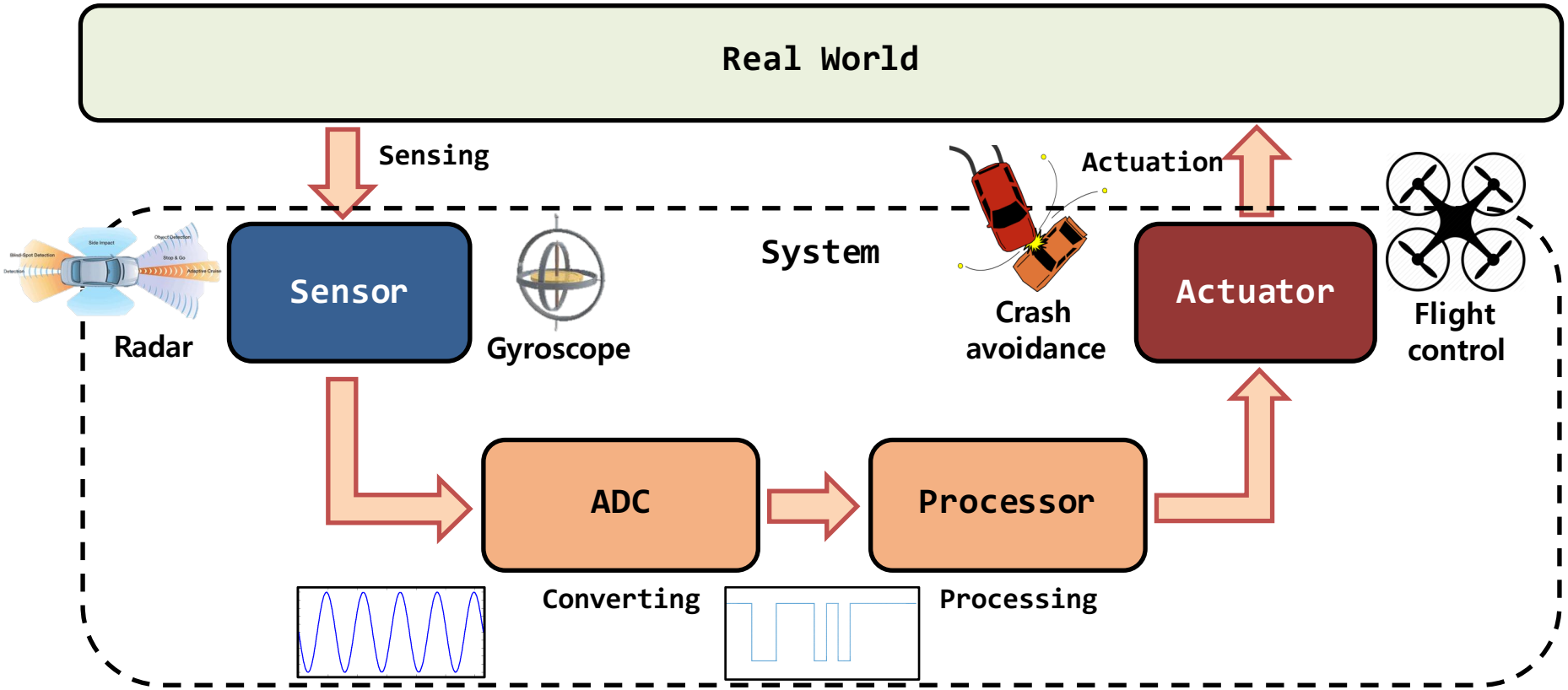
- ❖ Sensing changes in physical property and converting to electric signal
- ❖ Gyroscope, Accelerometer, Radar, Sonar, Infrared sensor, etc.





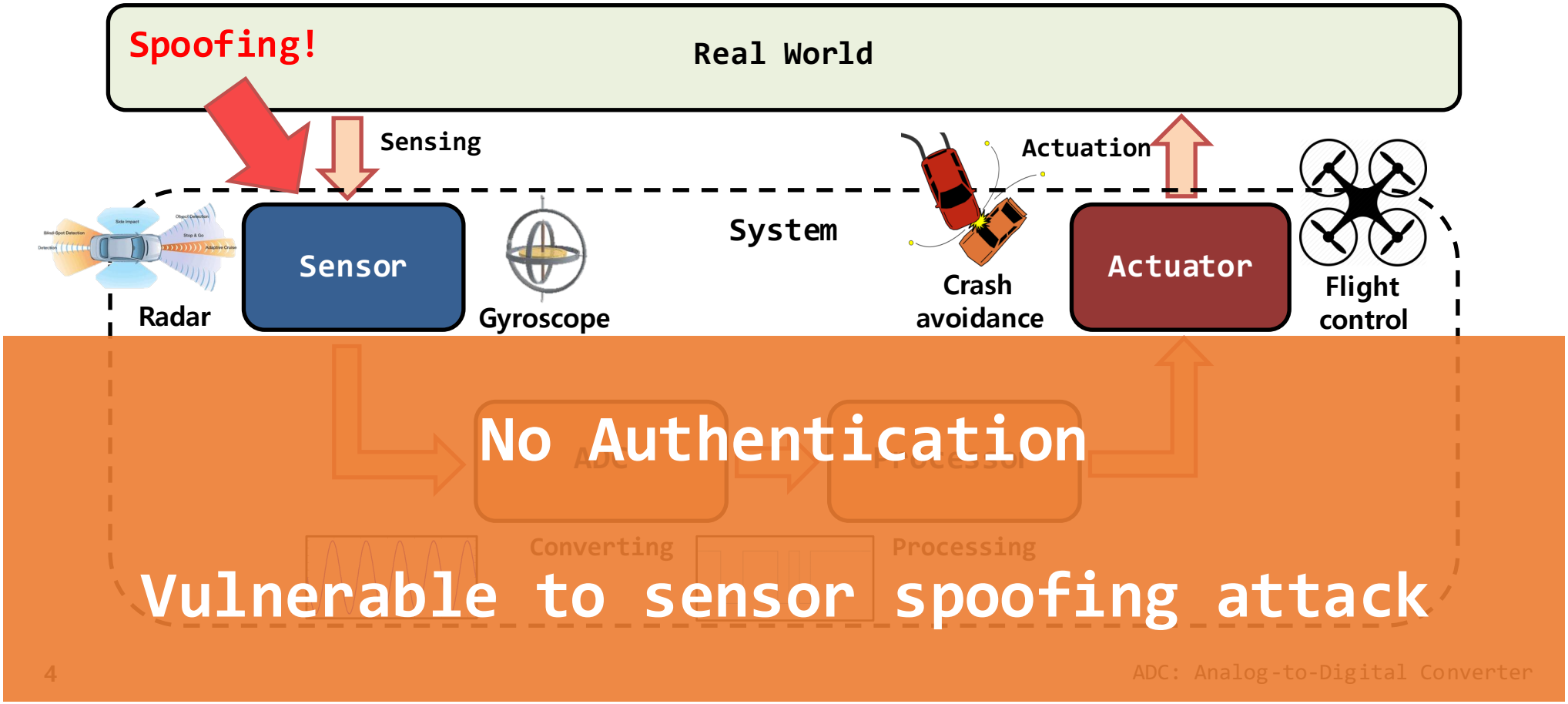


Sensing and Actuation System



ADC: Analog-to-Digital Converter

Sensing and Actuation System



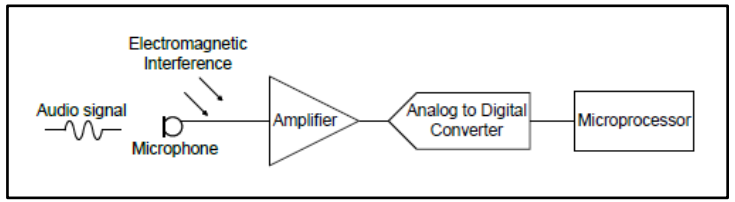
No Authentication

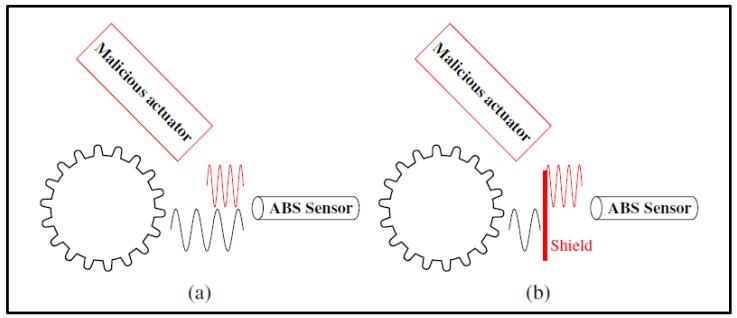
Vulnerable to sensor spoofing attack

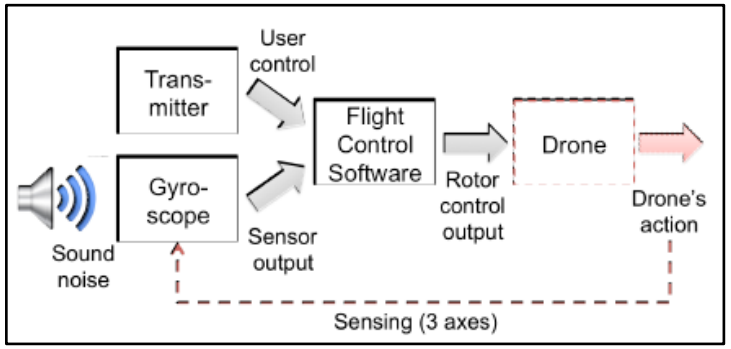
ADC: Analog-to-Digital Converter

Sensor Spoofing Attack

- Manipulating sensors with a malicious signal
- Previous works
  - Attacking Circuit using EMI: Injecting EMI into a wire of a defibrillator (S&P'13)
  - Canceling and injecting Active Sensor Signal: magnetic signal on ABS sensor (CHES'13)
  - Generating Resonance (DoS): Injecting sound noise into a gyroscope of a drone (SEC'15)





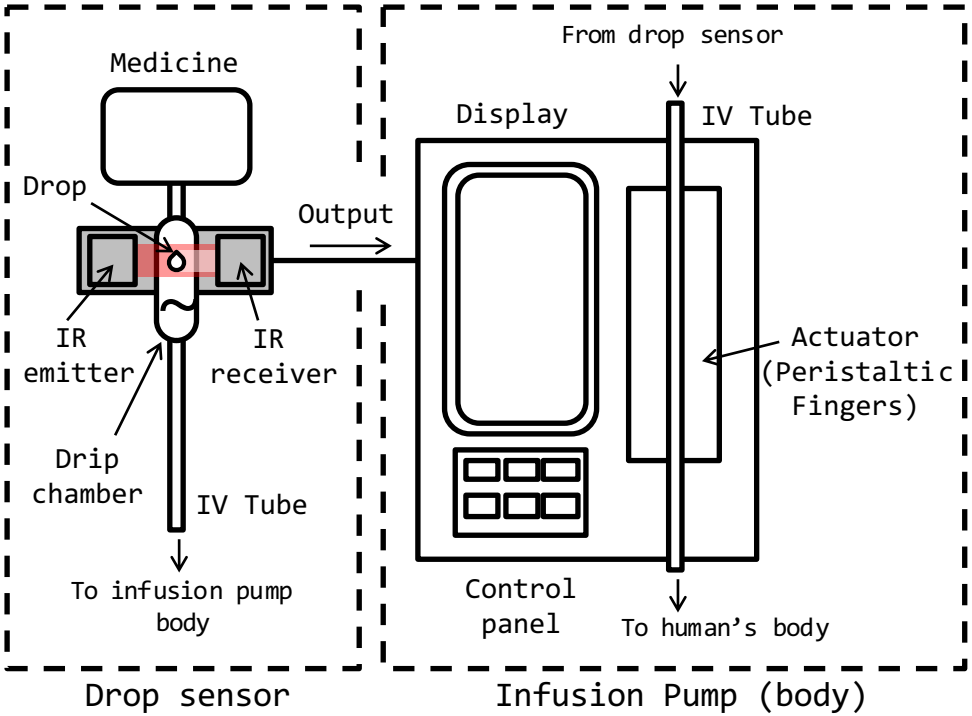


EMI: Electromagnetic Interference
ABS: Anti-lock Braking System

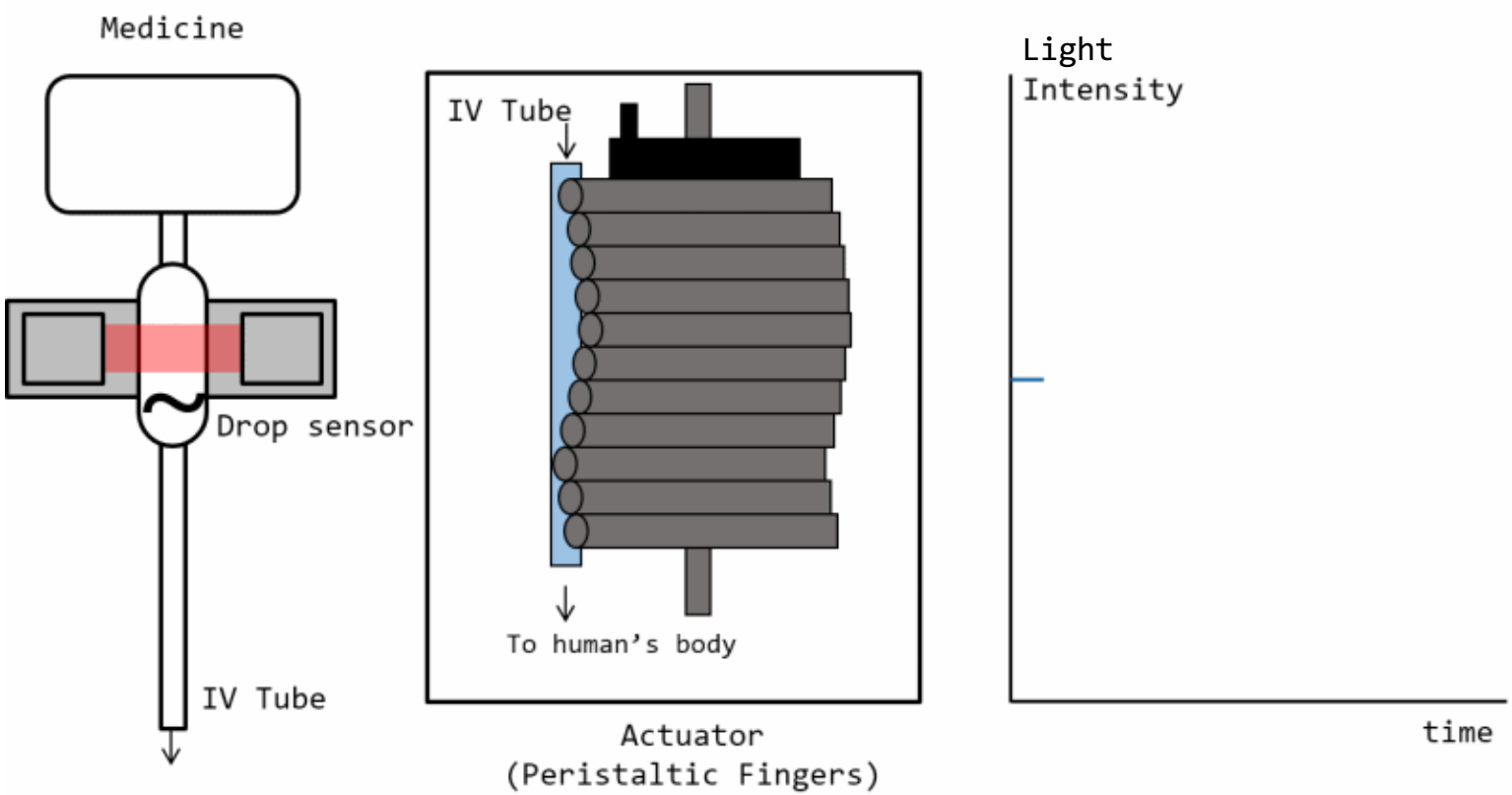
This Work:
Manipulating Sensing Values by Saturating Receiver

Target: Medical Infusion Pump

- ❖ Controlling infused volume of medicine to patients
- ❖ Sometimes using a drop sensor for accuracy



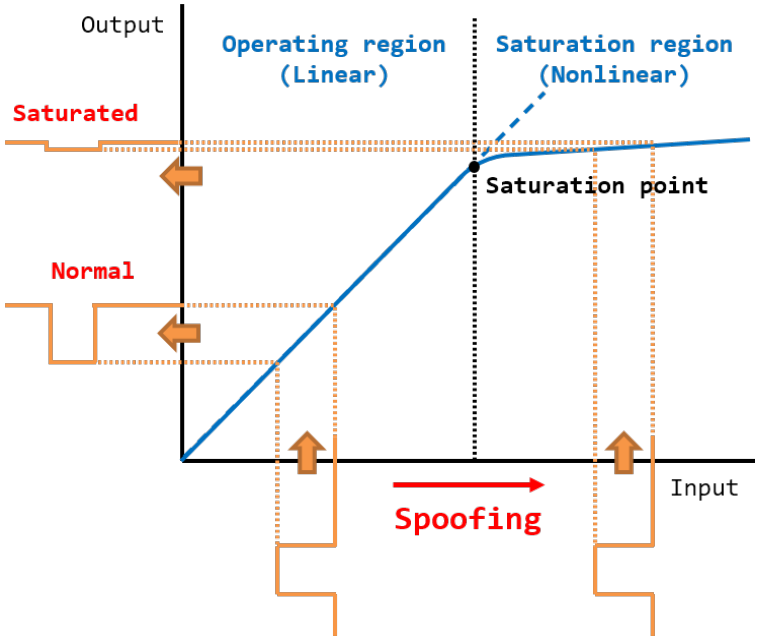
Infusion Pump Operation

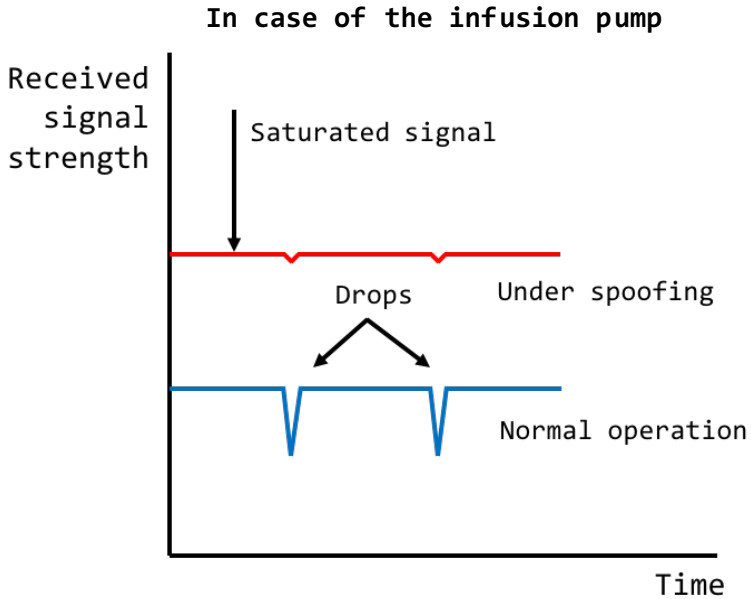


Sensor Saturation

❖ New type of sensor spoofing attack using **saturation**

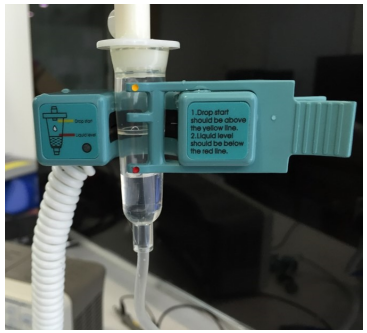
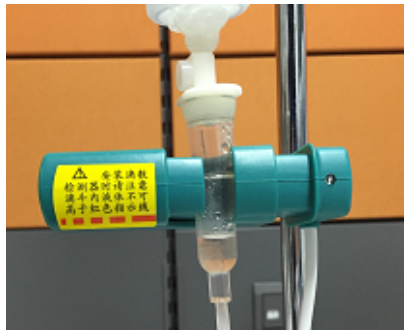
- Sensors have typical operating region
- Output is saturated when exceeding a saturation point
- Blinding sensors





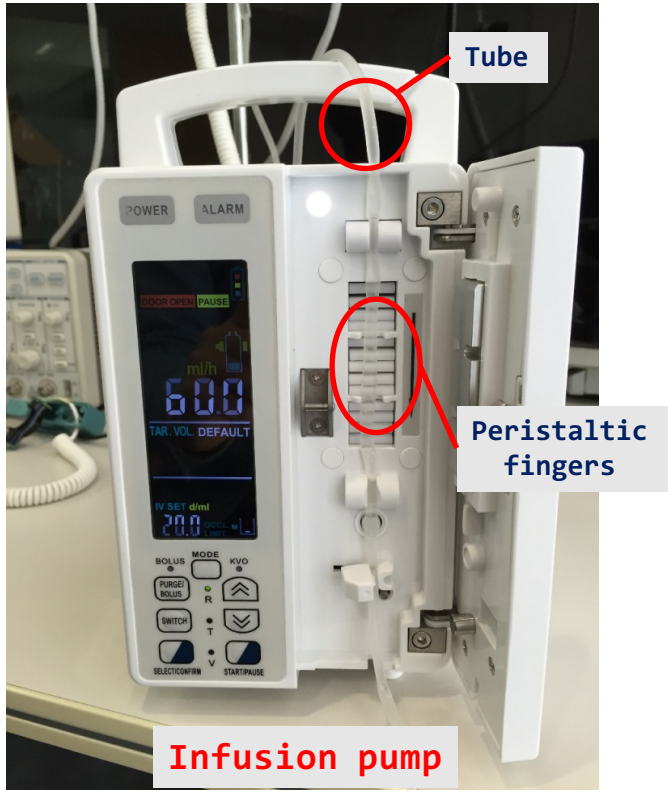
Medical Infusion Pump

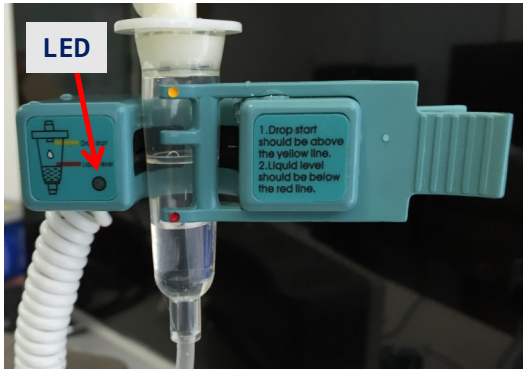
❖ Two infusion pumps with drop sensors

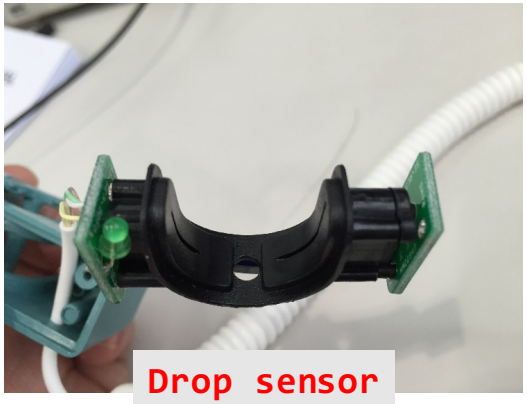
	Infusion pump	Drop sensor
JSB-1200 (Pump1)		
BYS-820 (Pump2)		

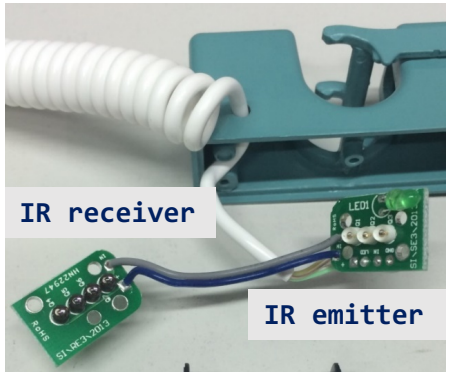
Hardware Analysis

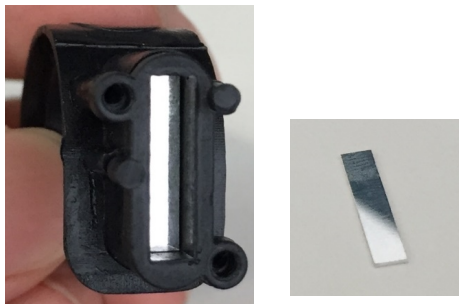
❖ Pump1 (JSB-1200)











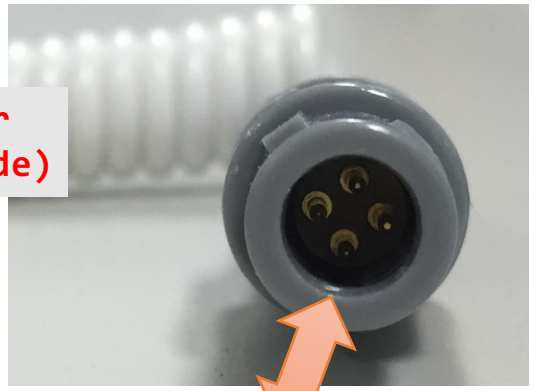
IR Filter

Hardware Analysis

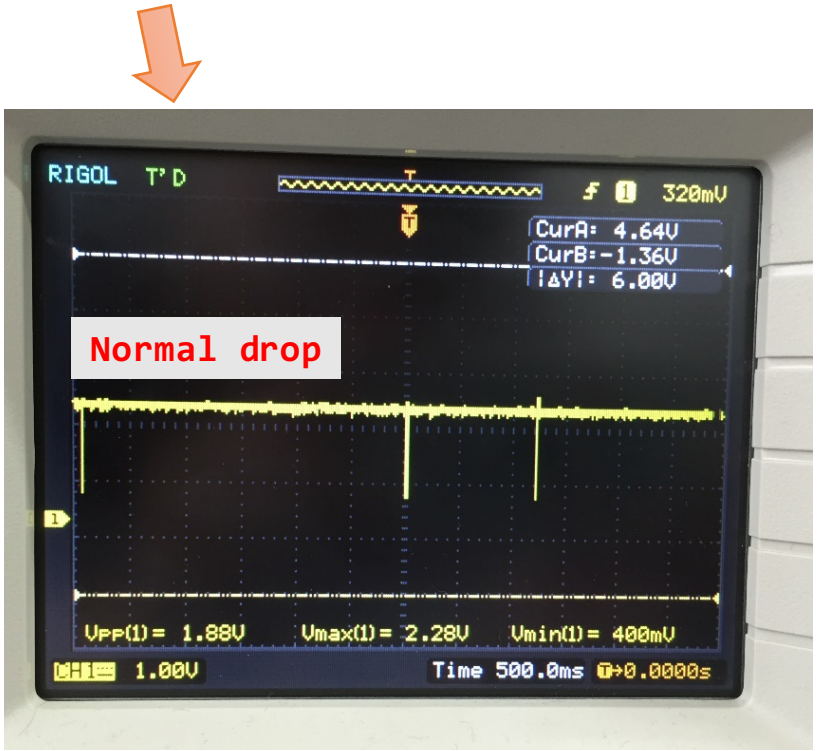
❖ Measuring signal with oscilloscope

- Connector = 4 pins: VCC, GND, LED, and **IN (signal)**

Connector (Device side)



Four pins (Sensor side)

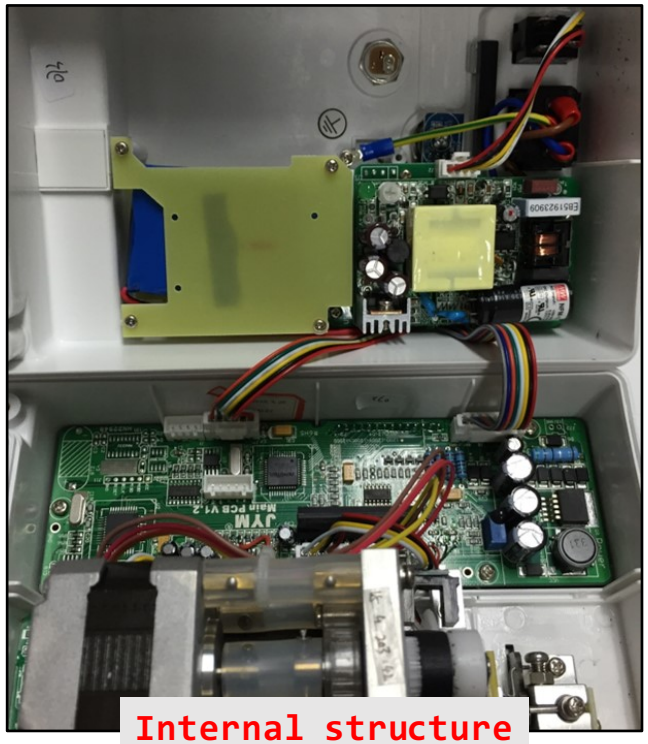


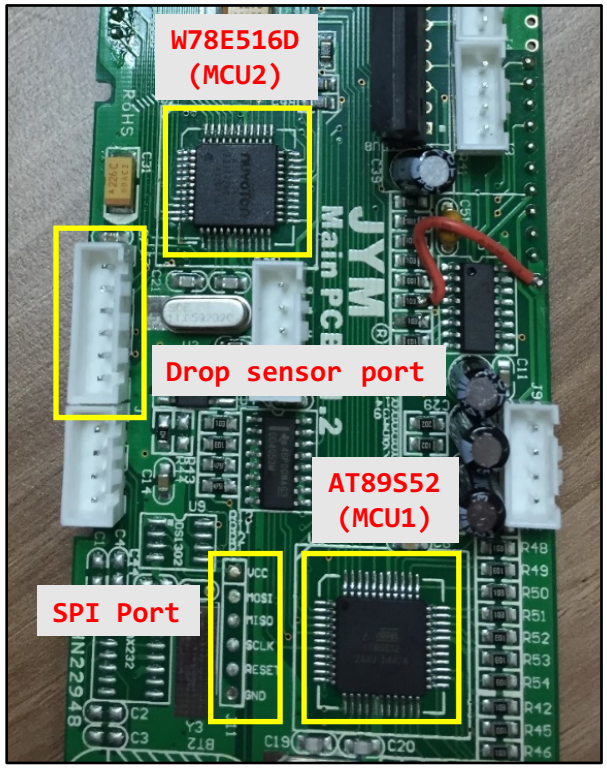
Simple Test (Saturation, w/o filter)

Simple Test (Saturation, w/o filter)

Hardware Analysis

❖ Mainboard (2 MCUs)

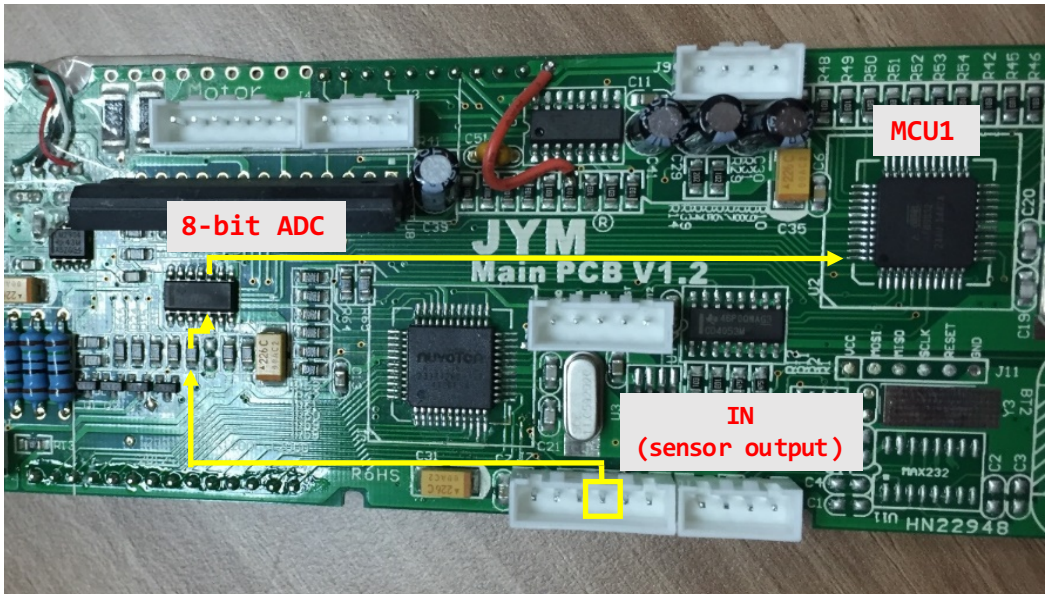


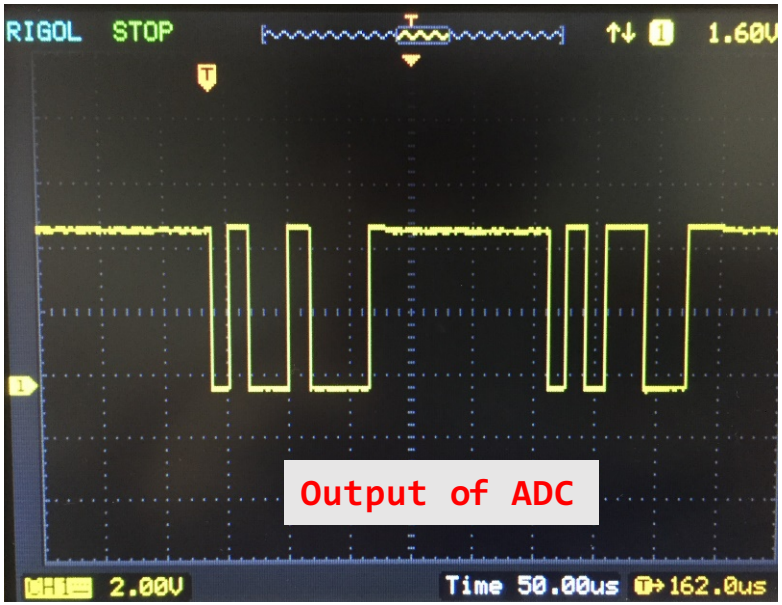


Hardware Analysis

❖ Sensor output is inserted to MCU1 after ADC

- 8-bit ADC (0 to 255)
- Digital signal indicates voltage level of the drop sensor

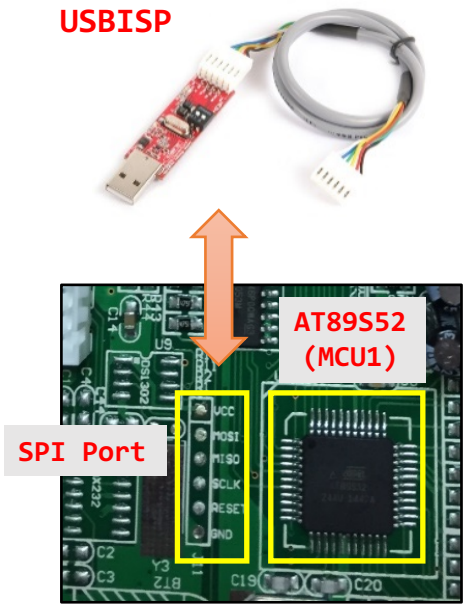


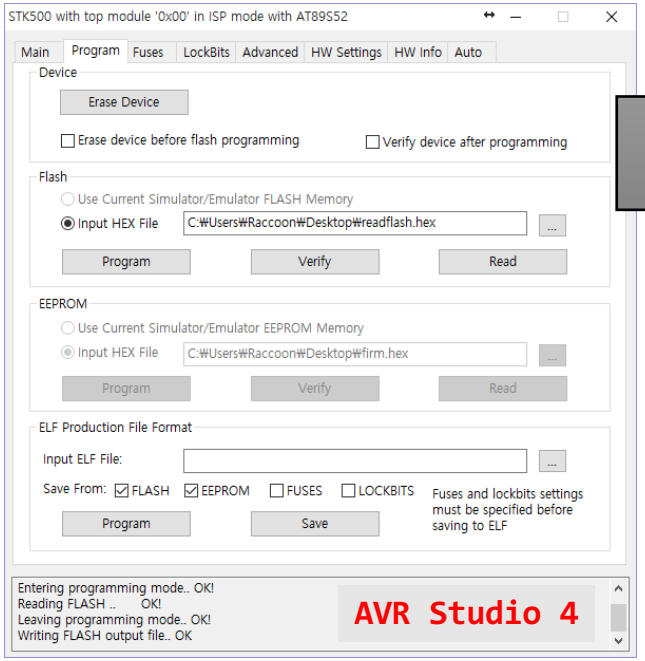


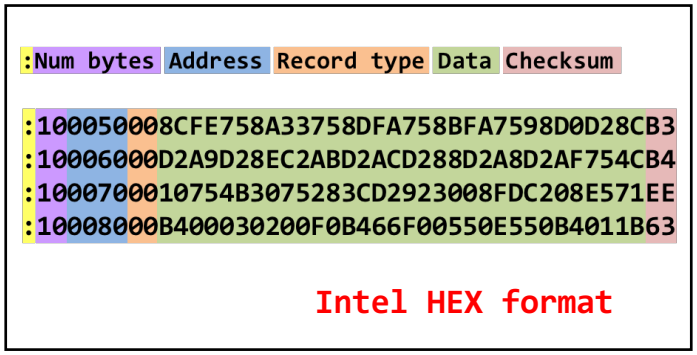
Firmware Extraction

❖ Extracting firmware of **MCU1** via SPI port

- Reading Flash memory using USBISP and AVR Studio
- Data section -> 8051 assembly -> IDA Pro







Firmware Analysis

❖ Finding sensor output in **Timer interrupt function**

```
code_432:
mov     RAM_41, #3
lcall   code_3C5
mov     RAM_30, RAM_42
lcall   code_2D2
jnb     RAM_20.3, code_451
```

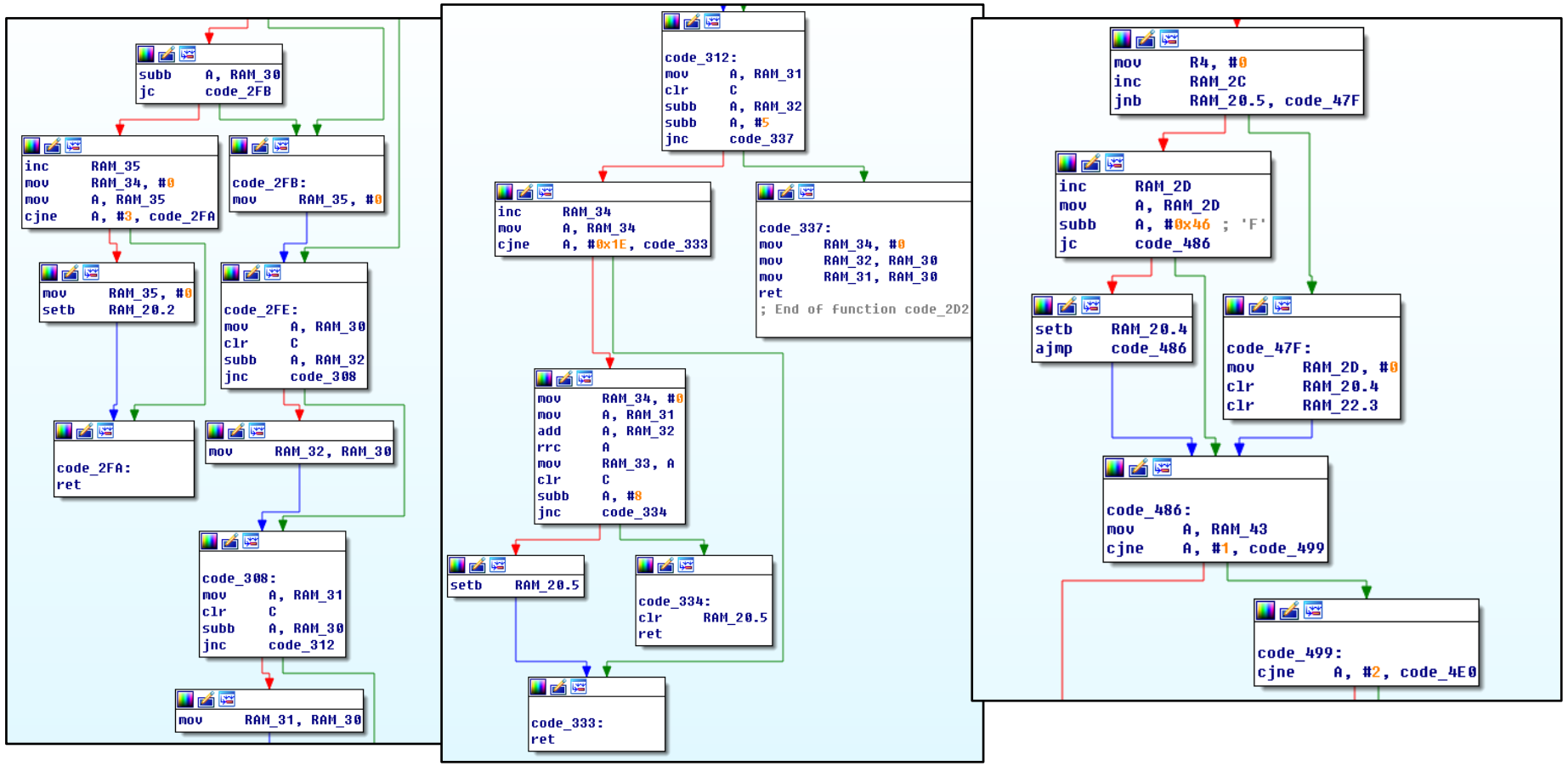
```
nop
nop
mov     B, #8           ; B Register
```

```
code_3E1:
lcall   code_3F2
clr     C
orl     C, P1.4         ; Port 1
mov     A, RAM_42
rlc     A
mov     RAM_42, A
djnz    B, code_3E1     ; B Register
```

Put 8-bit sensor output to RAM

```
setb    P1.5            ; Port 1
ret
; End of function code_3C5
```

Firmware Analysis



Drop Detection Algorithm

Algorithm 1: Simplified algorithm of sensing drops

Input: *Input*
Output: **Sensing drop**, **Alarm**
Data: *Maximum*, *Minimum*, *Average*

```
Loop
    Save sensing value to Input;
    if Input < Average − 16 then
        // Voltage drop by 0.32V
        Sensing drop; // A drop is sensed
        Send command through serial port
        return;
    end
    if Input < Minimum then
        Minimum = Input;
    end
    if Input > Maximum then
        Maximum = Input;
    end
    if Maximum − Minimum >= 5 then
        // Correct value after sensing drop
        Maximum = Input;
        Minimum = Input;
        return;
    else
        Average = (Maximum+Minimum)/2;
        if Average < 8 then
            // Average is lower than 0.16V
            Alarm; // Error occurred
        end
        return;
    end
EndLoop
```

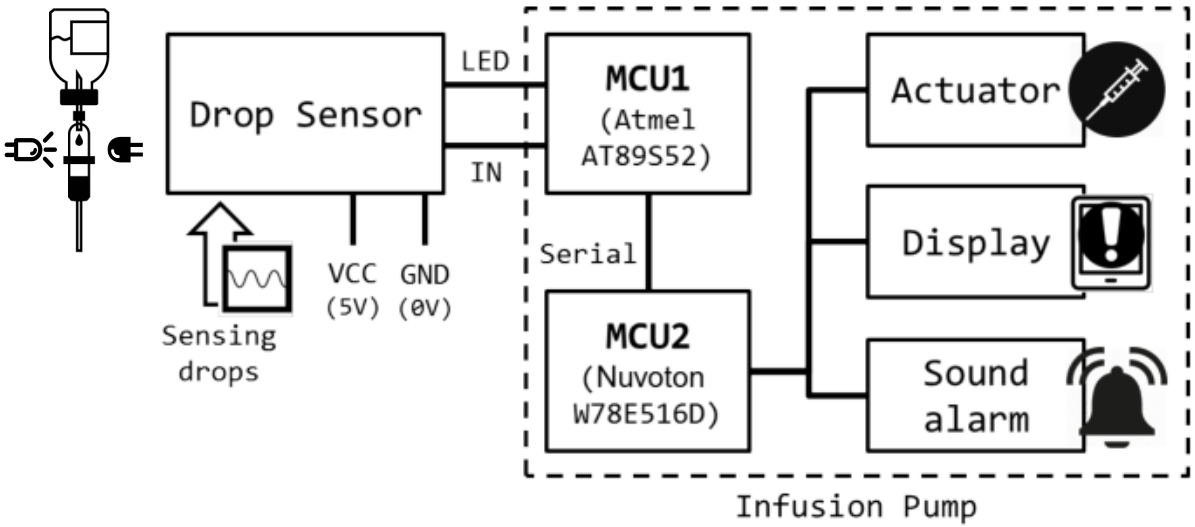
Sensing drop when voltage decreases by 0.32V

```
setb    RAM_20.3
setb    P1.1            ; Port 1
clr     RAM_20.2
mov     A, #0x11
mov     C, PSW.0        ; Program Status Word
mov     SCON.3, C       ; Serial Port Control
mov     SBUF, A         ; Serial Port Buffer
setb    RAM_21.5
```

Send command (0x11) through serial port, connected to MCU2

Pump1 Structure

1. Drop sensor output enters into AT89S52 (MCU1)
2. MCU1 sends data to W78E516D (MCU2) via serial comm.
3. MCU2 actuates peripherals with this data
   - Pins of MCU2 are directly connected to motor, display and alarm



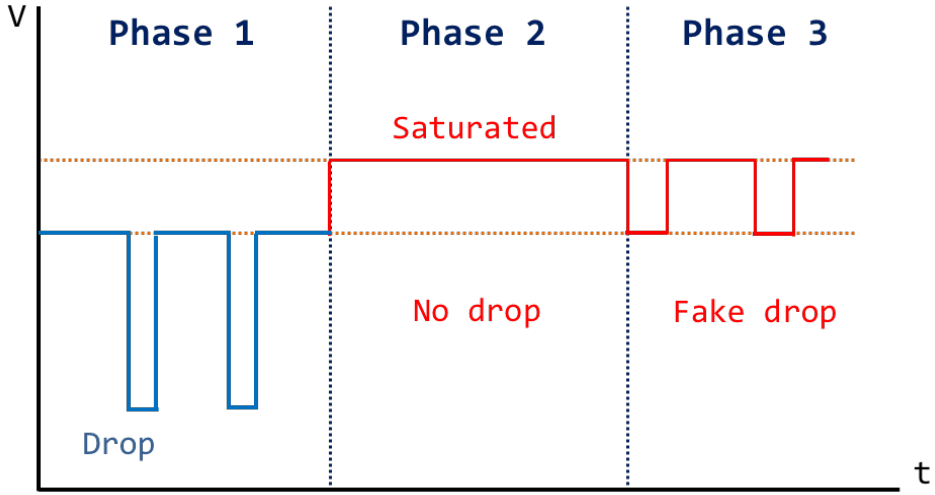
Vulnerability

- Drop sensor
  - Saturated with an external source
  - Cannot sense drops in saturation

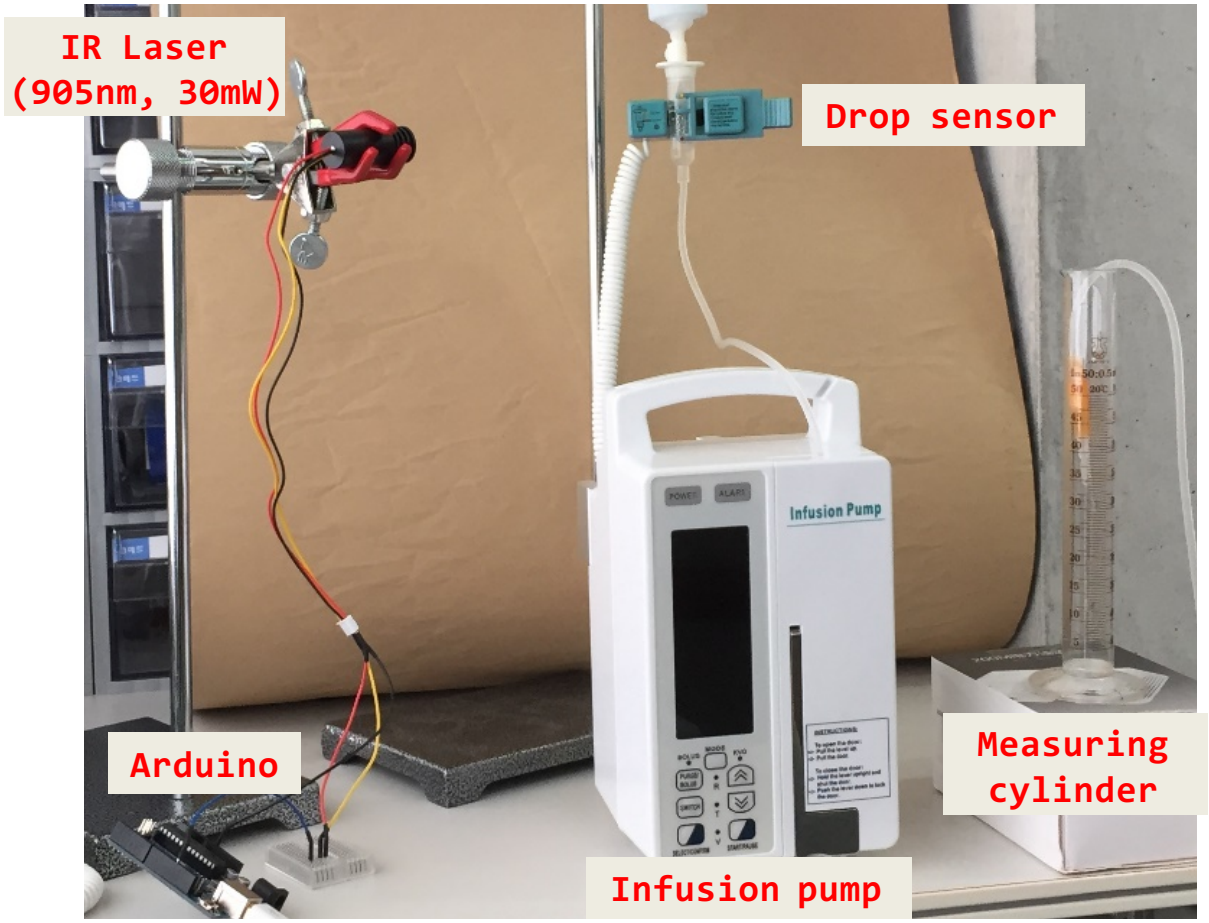
  → **Saturation**

- Drop detection algorithm
  - Counting drops based on a relative change in voltage
  - Making a voltage drop to sensor output

  → **Fake drop**

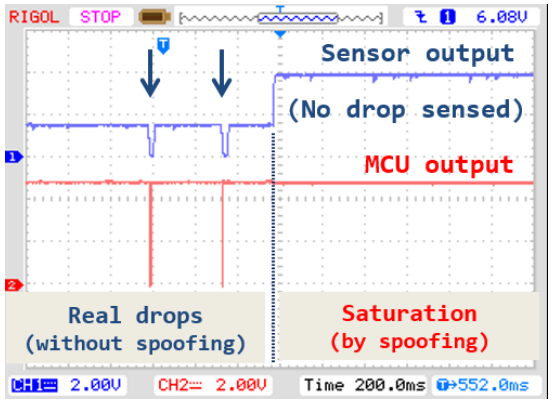


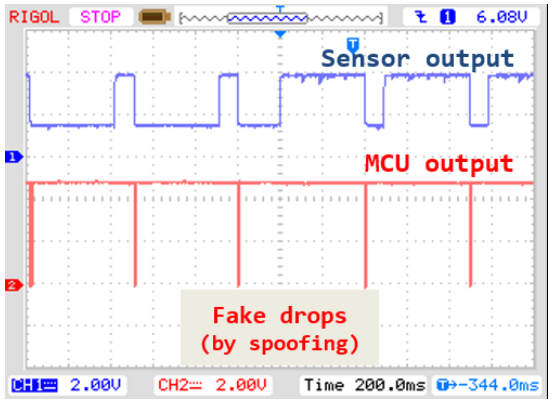
Experimental Setting



Experiment

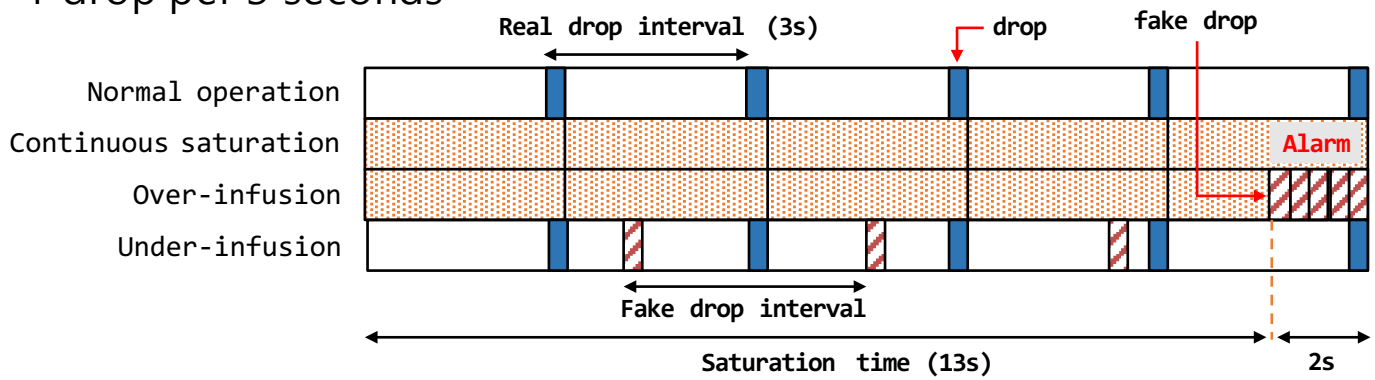
- Performed on both infusion pumps (Pump1, Pump2)
- **Saturation (failed in Pump2)**
  - Sensor is saturated when injecting IR laser to receiver
  - Drop sensor cannot sense real drops -> **Over-infusion**
- **Fake drops**
  - Sensor is deceived by fake drops with external IR
  - Pump perceives that there are drops already -> **Under-infusion**
- Both cases cause an **alarm**





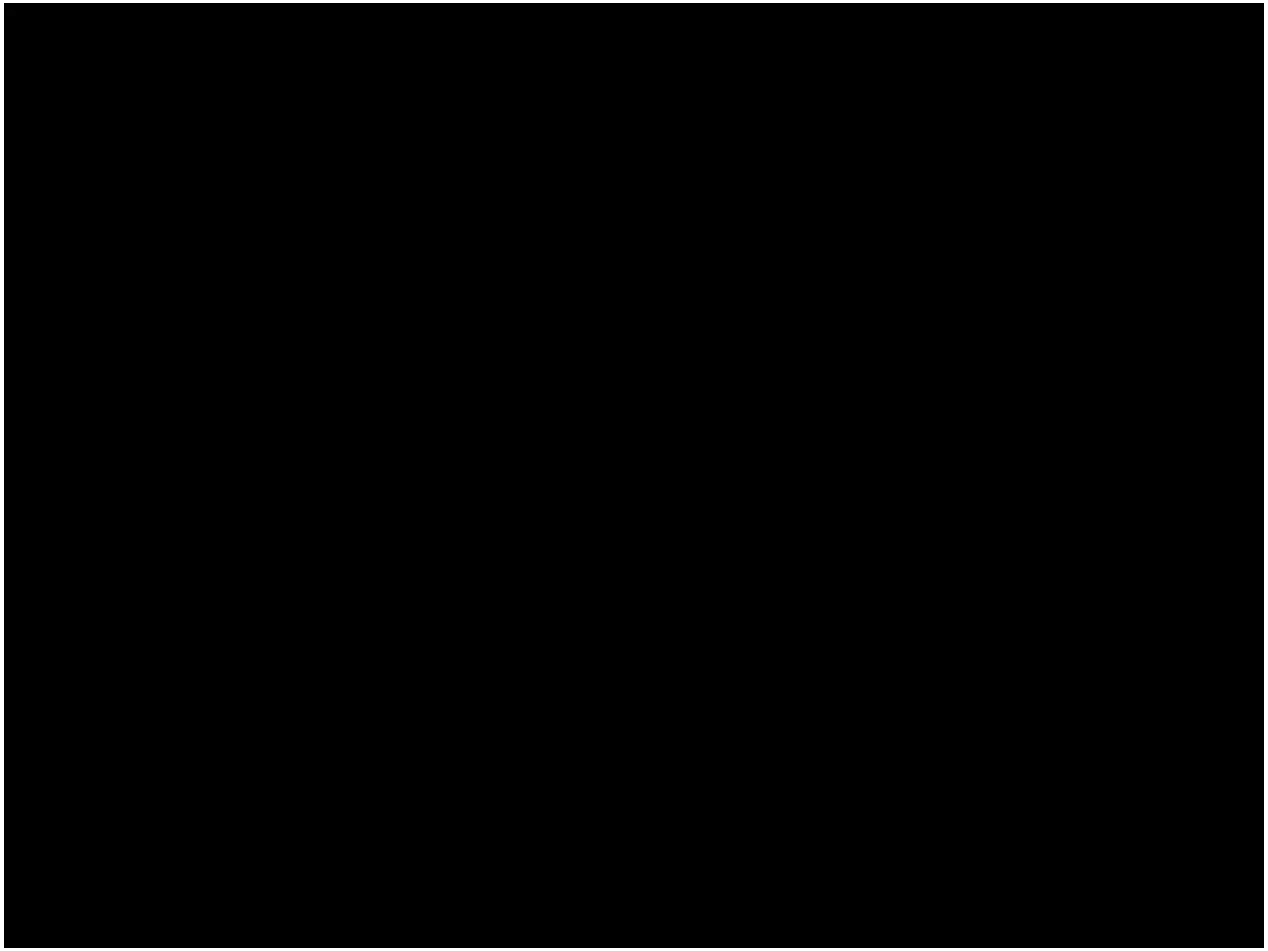
Spoofing Pattern

- Over-infusion
  - Alarm: "**No drop is detected**"
  - Inject some period and compensate insufficient drops
- Under-infusion
  - Alarm: "**Too many drops are detected**"
  - Find properly interval of fake drops experimentally
- Example (60mL/h setting)
  - 1 drop per 3 seconds



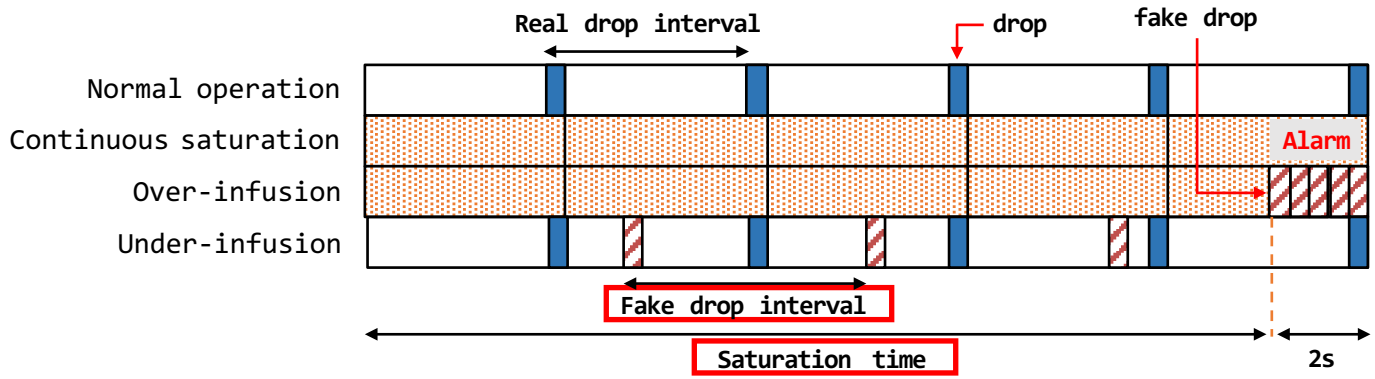
Demo (Over-infusion)

Demo (Under-infusion)



Spoofing Pattern

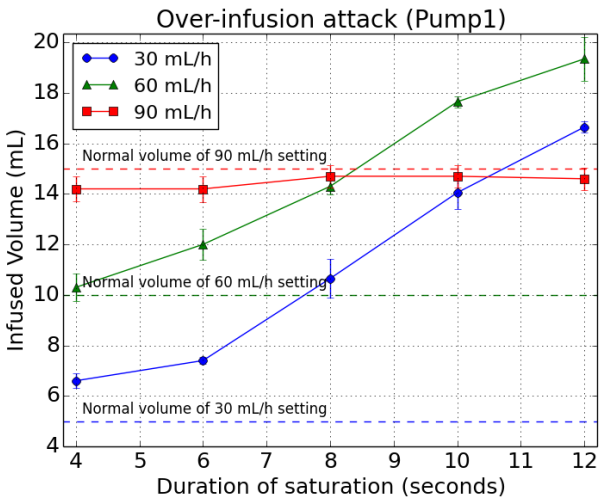
- Over-infusion
  - Alarm: "**No drop is detected**"
  - Inject some period and compensate insufficient drops
- Under-infusion
  - Alarm: "**Too many drops are detected**"
  - Find properly interval of fake drops experimentally

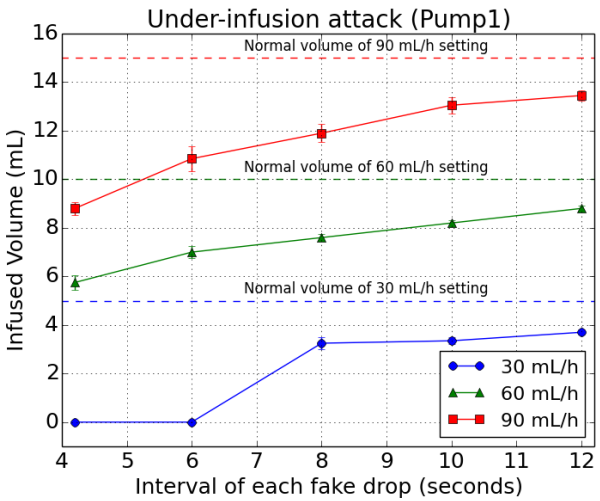


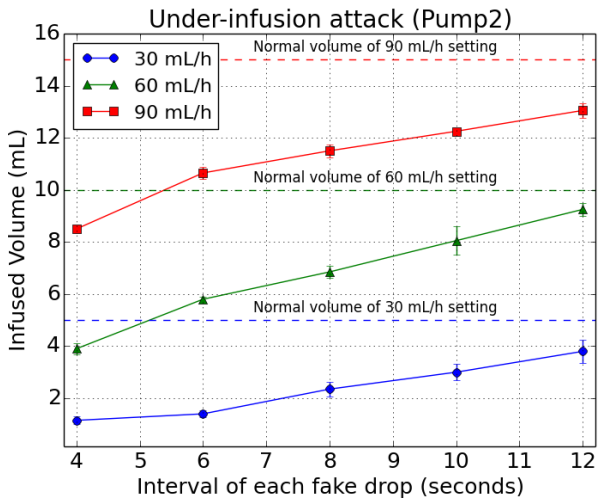
Results

❖ Controlling infused volume is possible

- By adjusting saturation time or fake drops
- Measured in 10 minutes and 5 times each (No alarm rings over 30 minutes)
- Over-infusion fails on Pump2

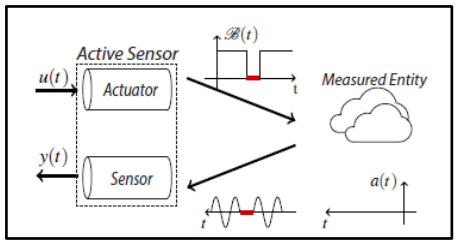






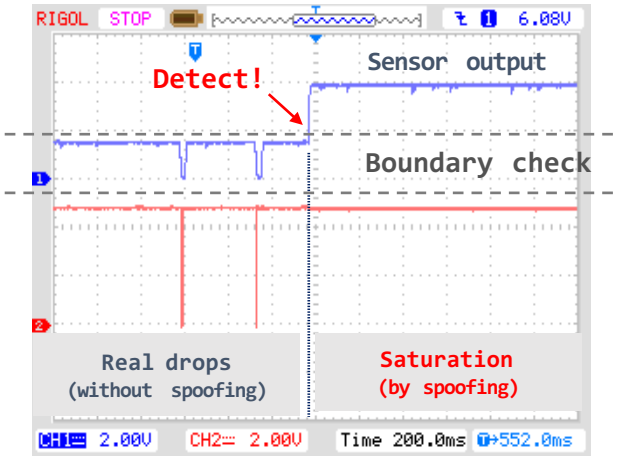
Discussion

❖ Attack distance
- Related to power of source
- Possible in the range of 12m with 30mW IR laser



Concept of PyCRA

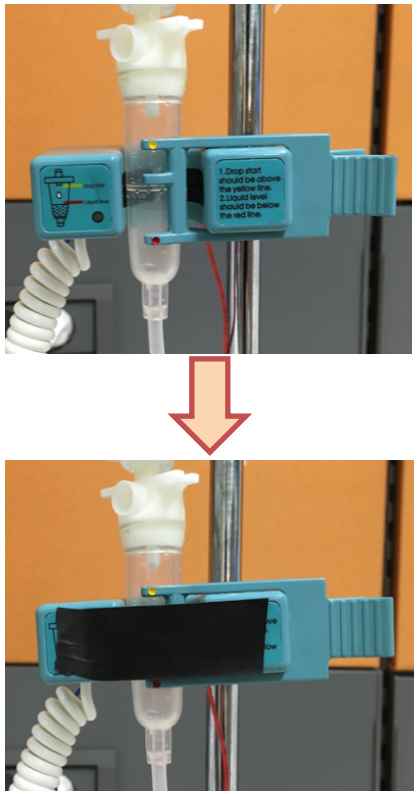
❖ Mitigation
- Authentication between emitter and receiver
  - PyCRA (CCS '15)
  - Generate random zero signal in an emitter
- Voltage level detection
  - Checking boundary of legitimate signal
- Physical isolation



Voltage level detection

Discussion

- Attack distance
  - Related to power of source
  - Possible in the range of 12m with 30mW IR laser
- Mitigation
  - Authentication between emitter and receiver
    - PyCRA (CCS '15)
    - Generate random zero signal in an emitter
  - Voltage level detection
    - Checking boundary of legitimate signal
  - Physical isolation



Conclusion

- Presenting a new type of sensor spoofing attack
  - Deceiving a sensor by saturation
- Analysis on medical infusion pumps
  - Finding vulnerability in drop detection algorithm
- Controlling infused fluid from 65% to 330%
- Note
  - Infusion pump was not communicating at all.
  - IR lay is invisible to human eyes.
  - FDA approved US devices?
- Sensor security
  - Most sensors are exposed to receive signal
  - Must be considered for safety

Thank You!

E-mail: ys.park@navercorp.com