Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors

Denis Foo Kune, John Backes, Shane S.Clark, Daniel Krammer,
Matthew Reynolds, Kevin Fu, Yongdae Kim, Wenyuan Xu

IEEE Symposium on Security and Privacy 2013

Presenter: JaeHoon Kim

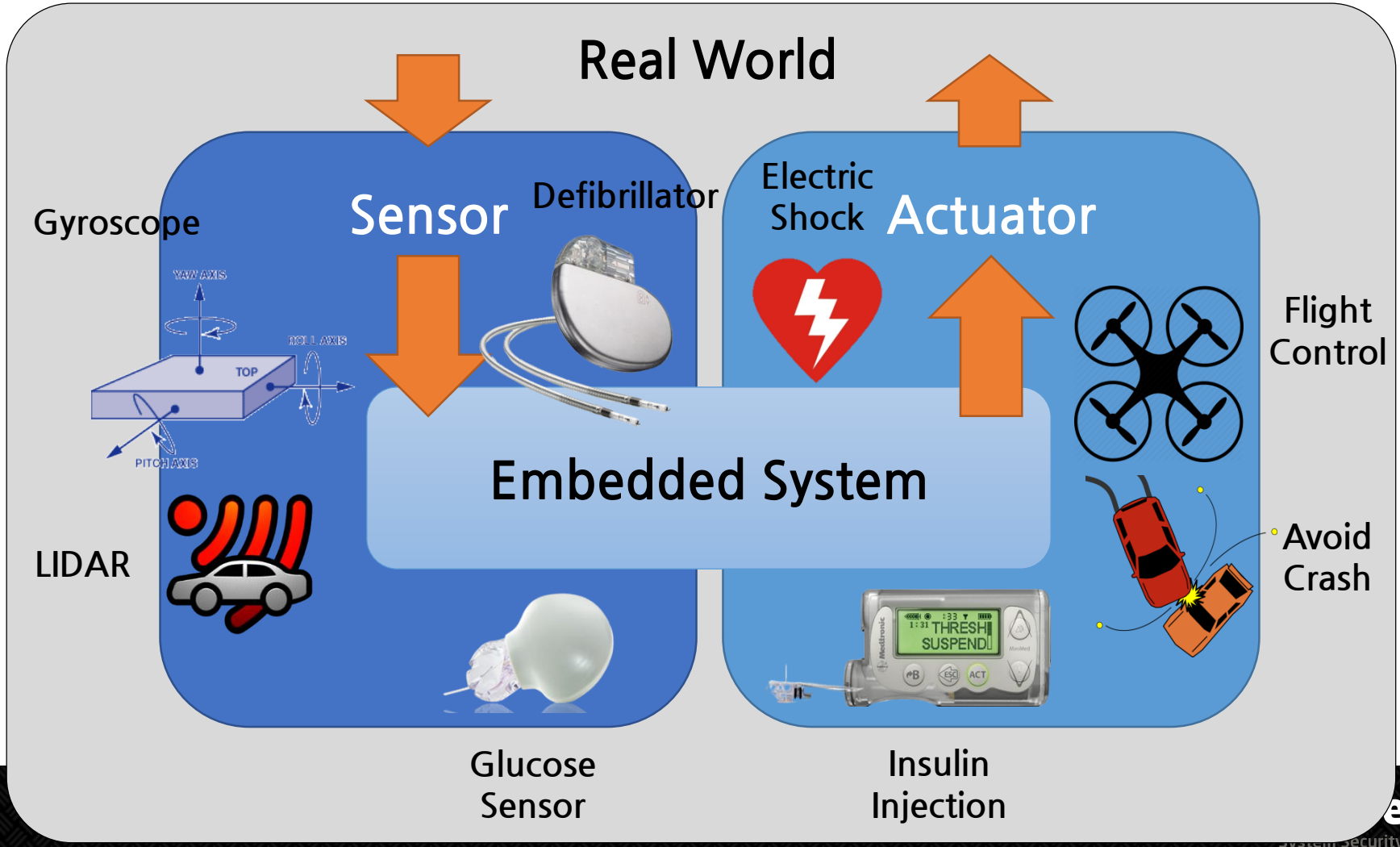
Outline

- Introduction & Background
- Baseband EMI Attack
- Amplitude-Modulated EMI Attack
- Defense
- Related Work
- Conclusion & Questions

Introduction & Background

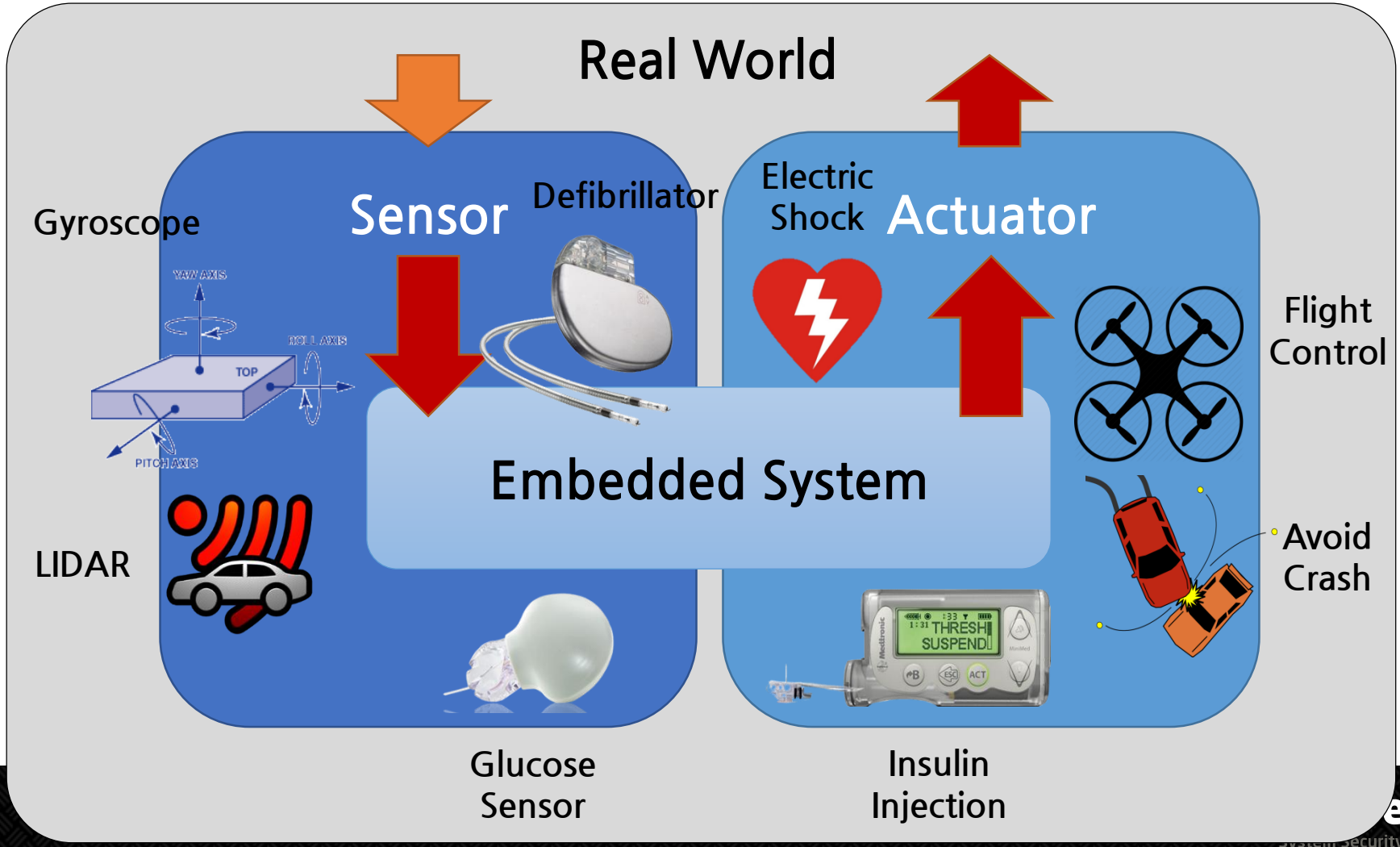
Sensing & Actuation

❖ Actuation and decision-making based on sensor data

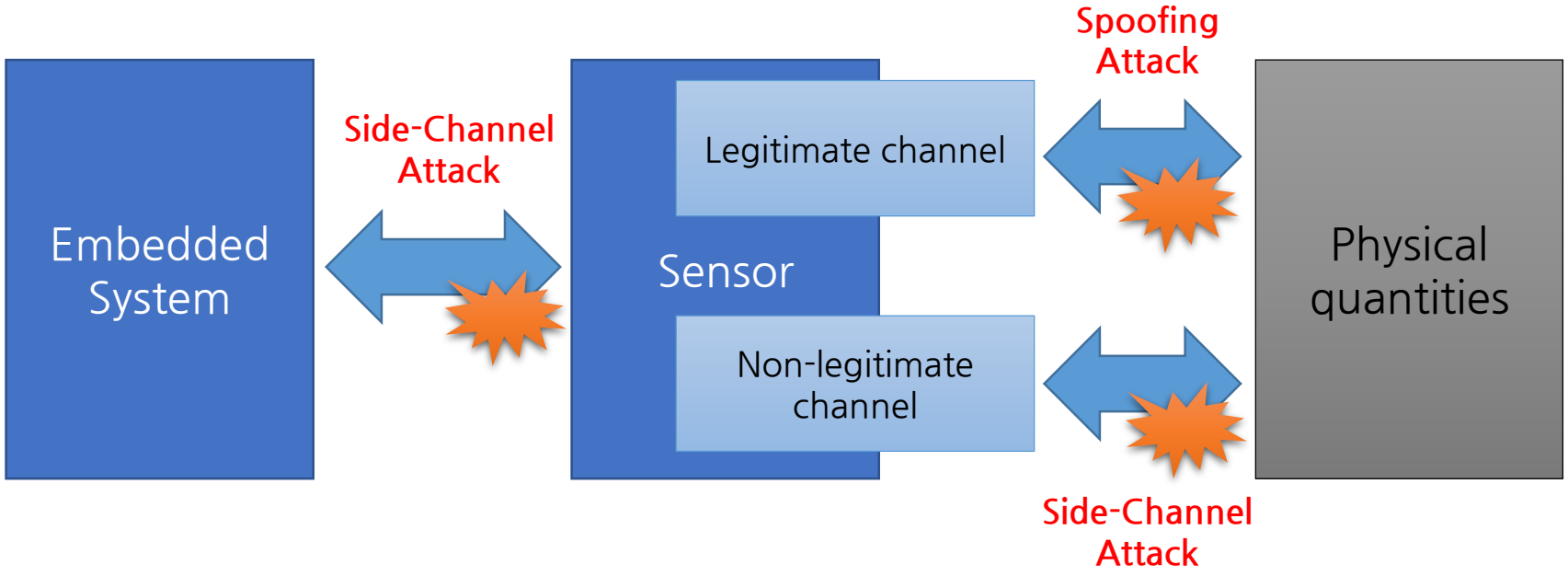


Sensing & Actuation

❖ Actuation and decision-making based on sensor data



Attack Vectors of Sensors



What is EMI?

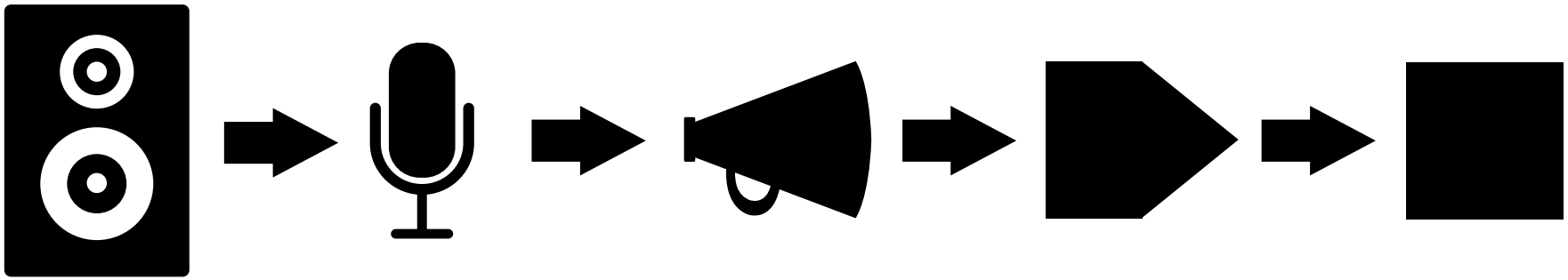
- Electro-Magnetic Interference

- A disturbance generated by an external source that affects an electrical circuit by induction, coupling, or conduction.

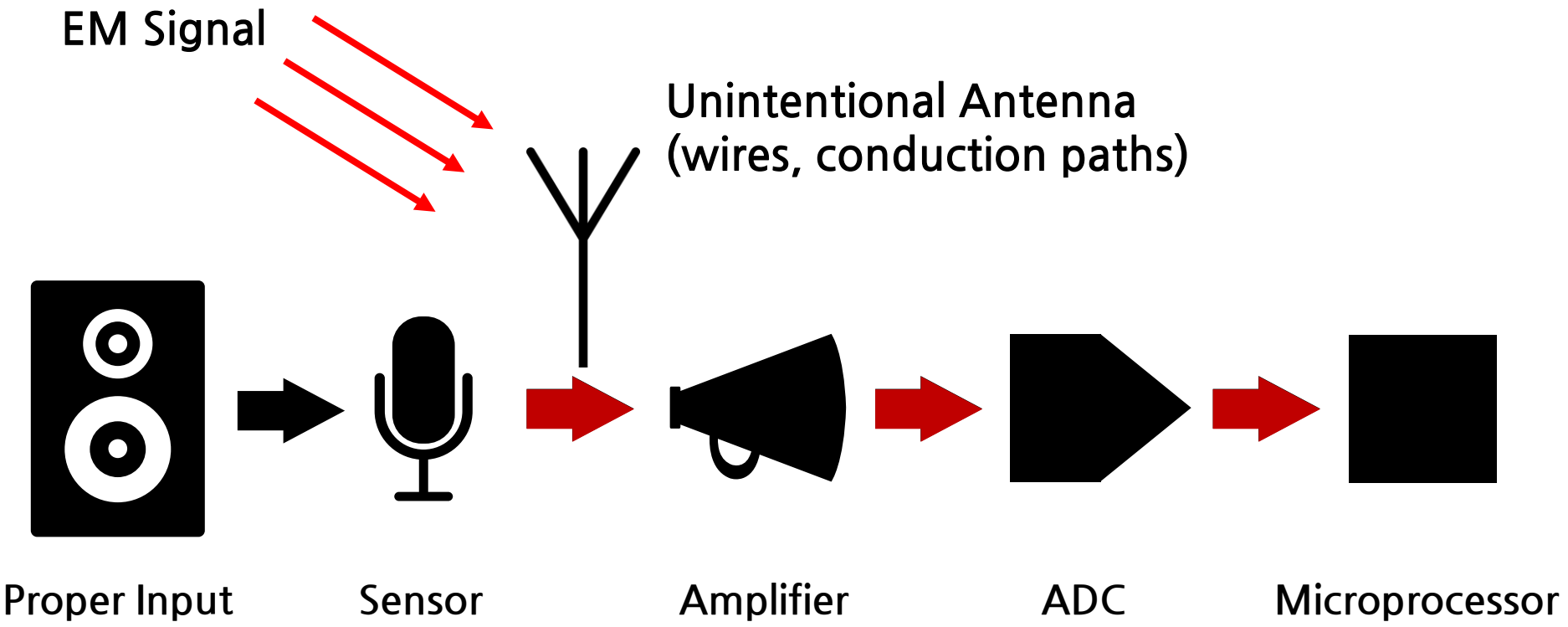
Classification of EMI Source

	Unintentional	Intentional
Low Power	Allow eavesdropping (Circuit design issue)	**Ghost Talk**
High Power	Impacts on circuits and sensors (lightning, transformer)	Can disable circuits

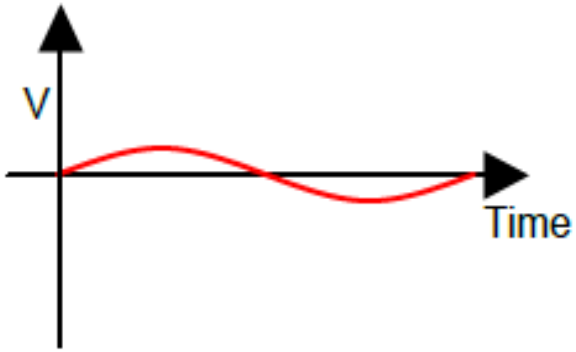
How EMI Affect to Circuits



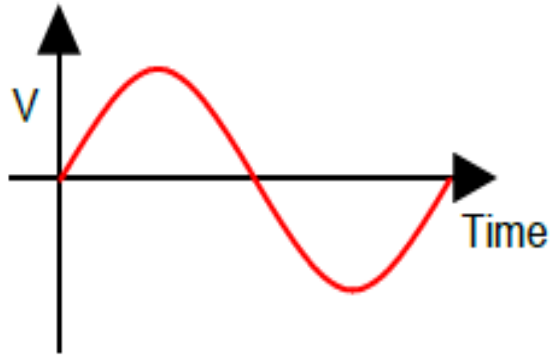
How EMI Affect to Circuits



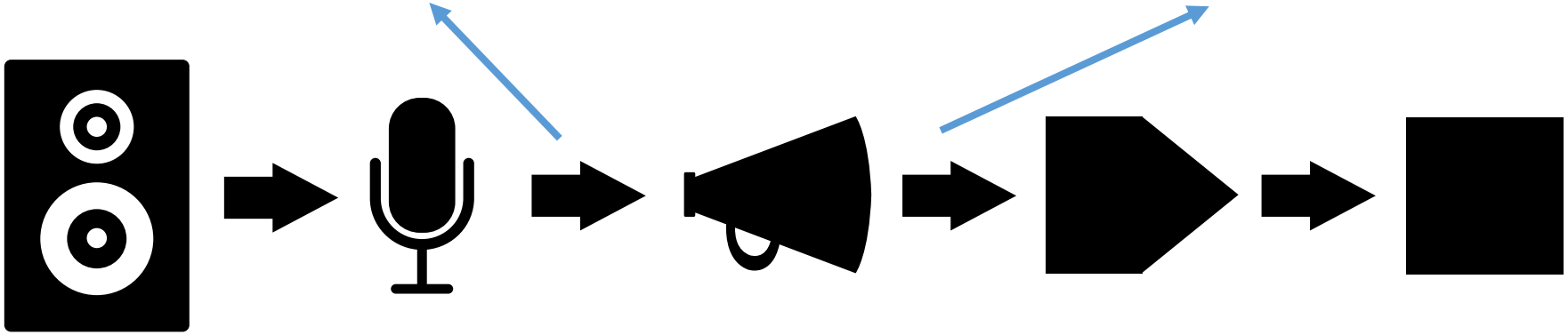
How EMI Affect to Circuits



On the order of a few mV

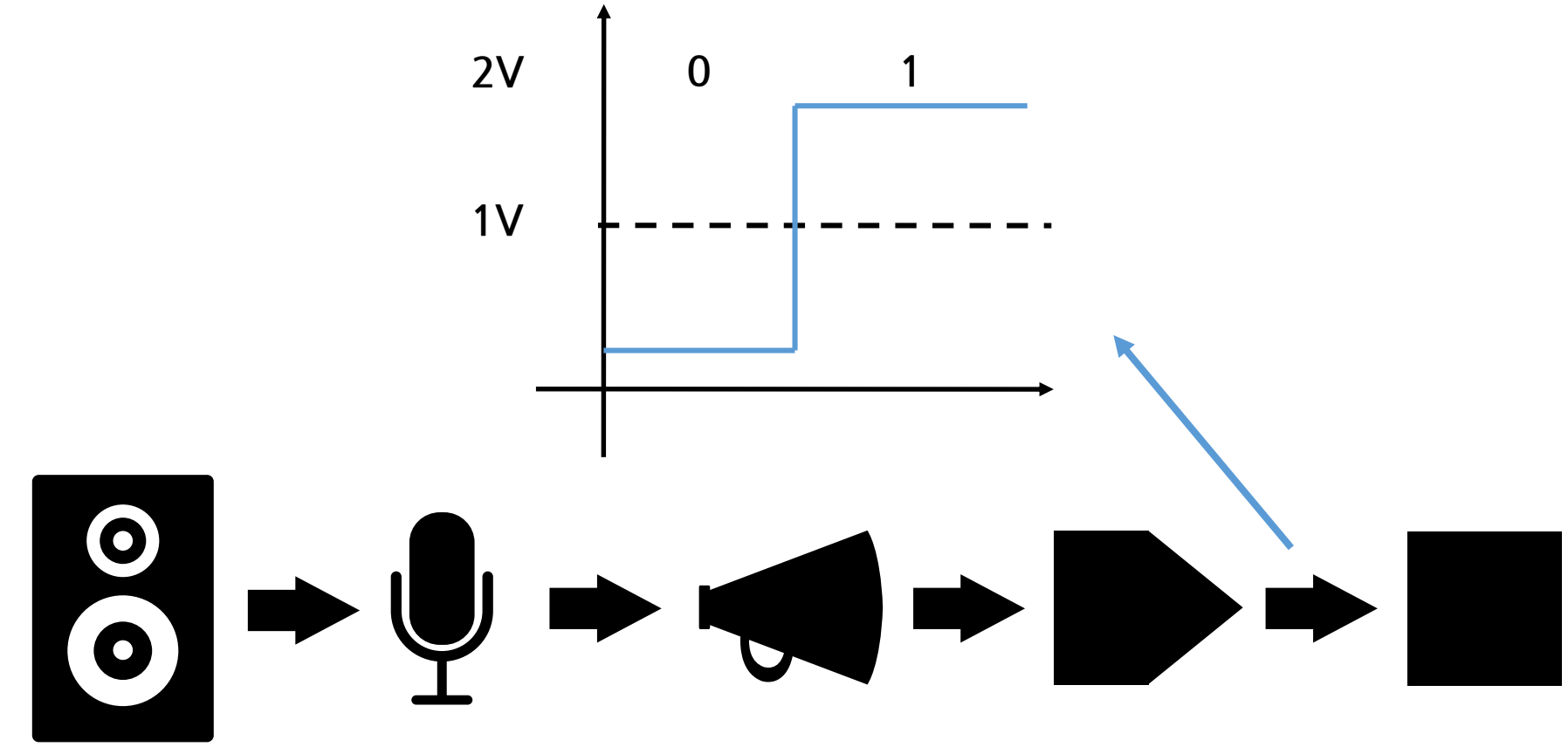


On the order of a few V

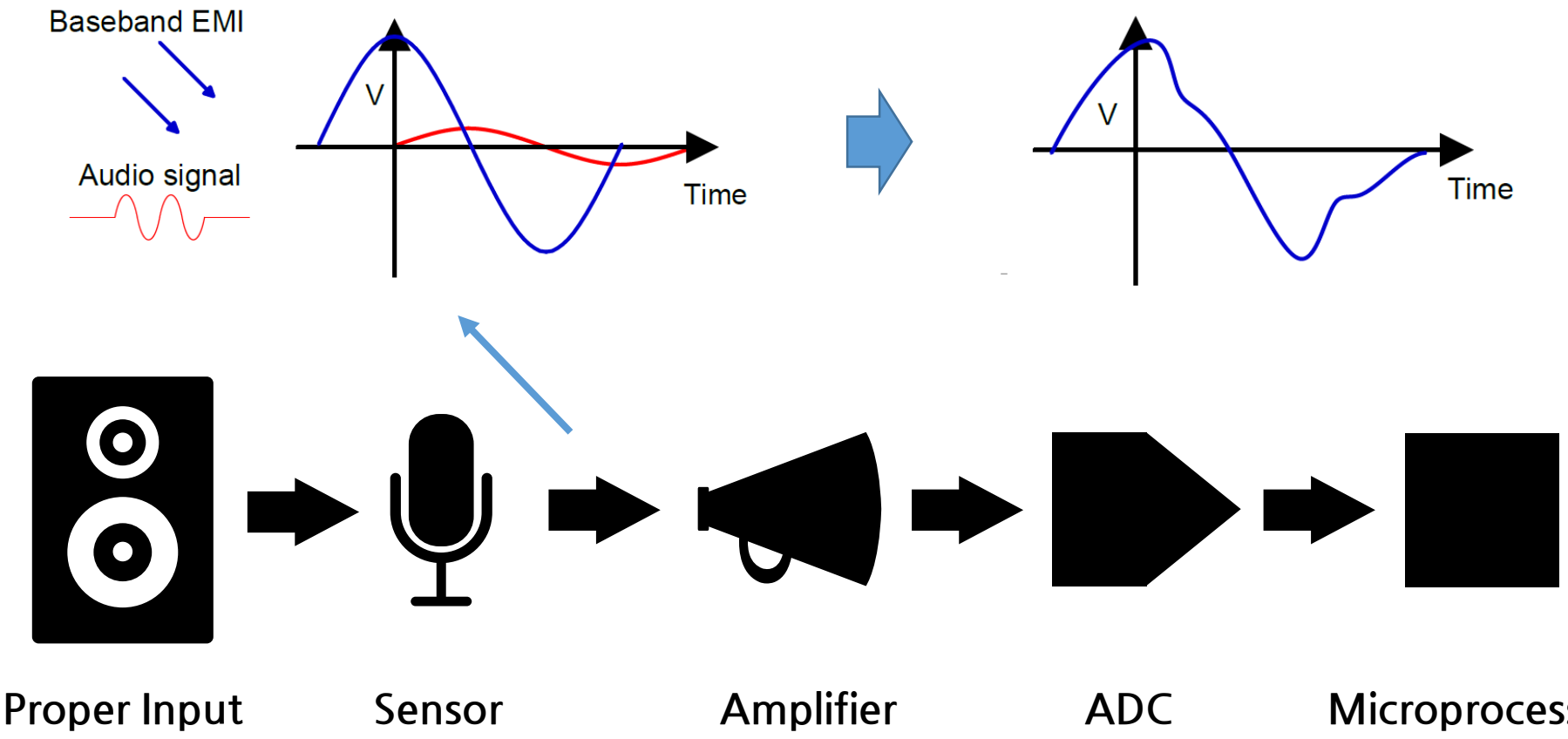


Proper Input Sensor Amplifier ADC Microprocessor

How EMI Affect to Circuits



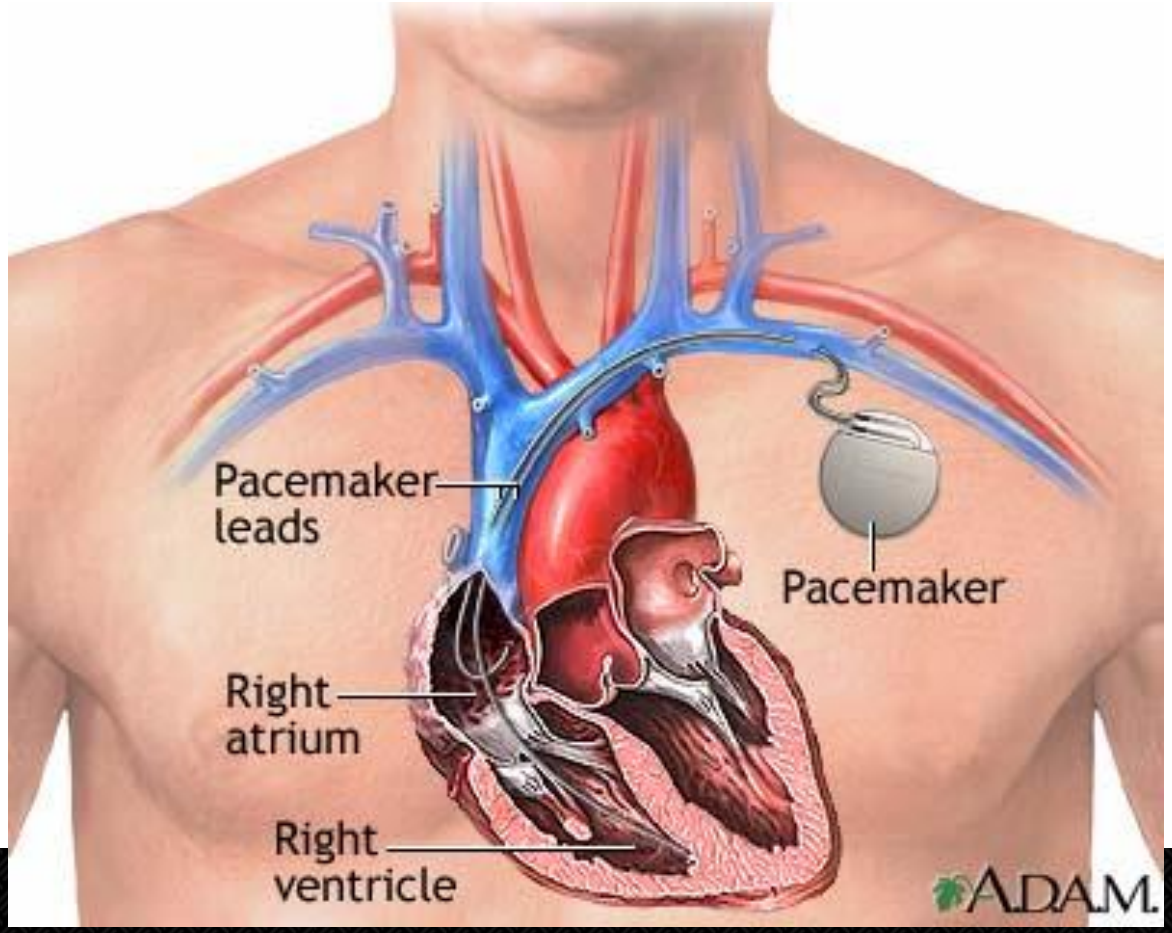
How EMI Affect to Circuits



Baseband EMI Attack

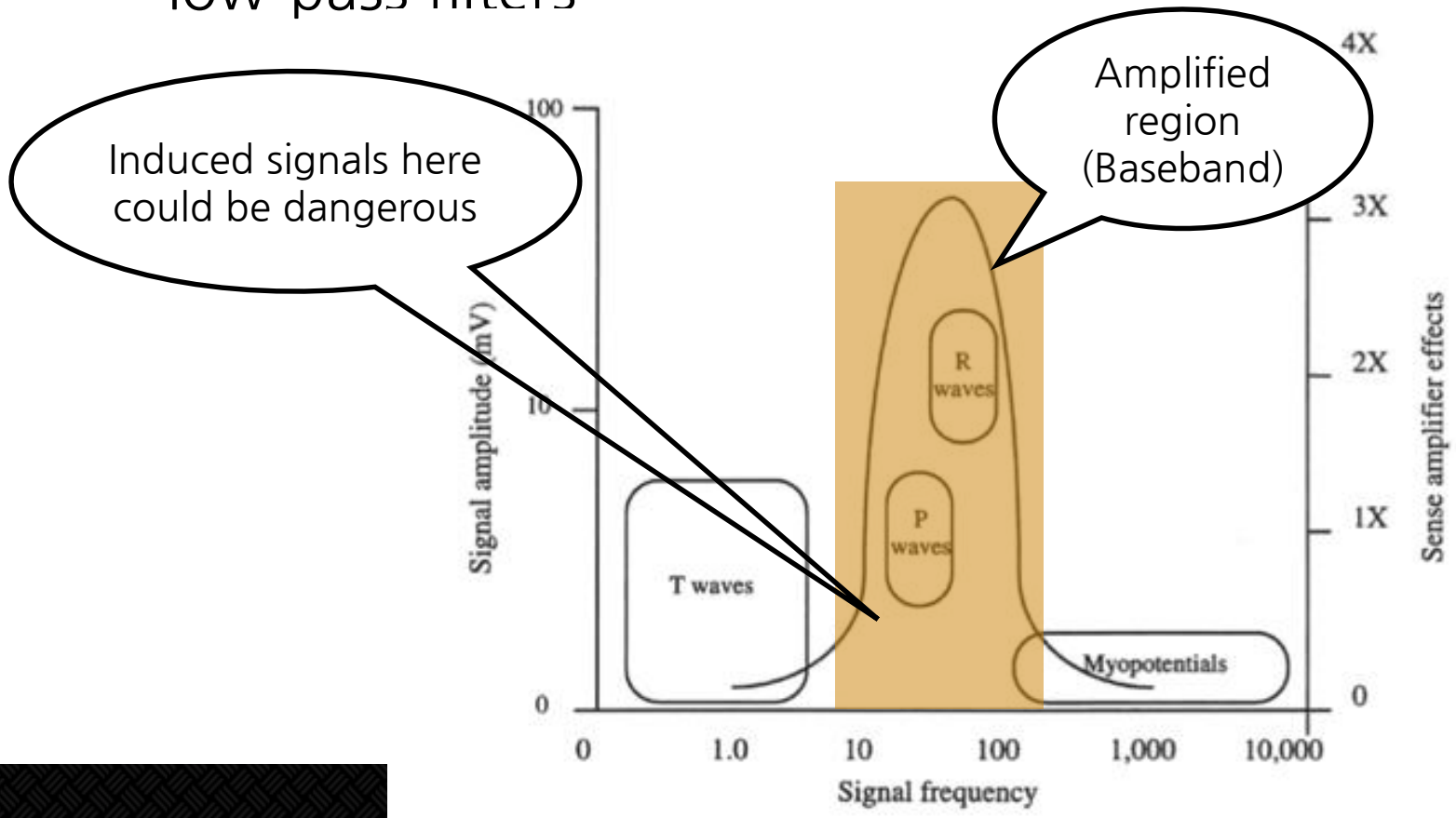
Cardiac Implantable Electrical Device (CIED)

- CIEDs are used to treat cardiac diseases with electrical stimulation



Cardiac Implantable Electrical Device (CIED)

- Safety-critical systems such as medical devices commonly operate on low frequency range and have low-pass filters

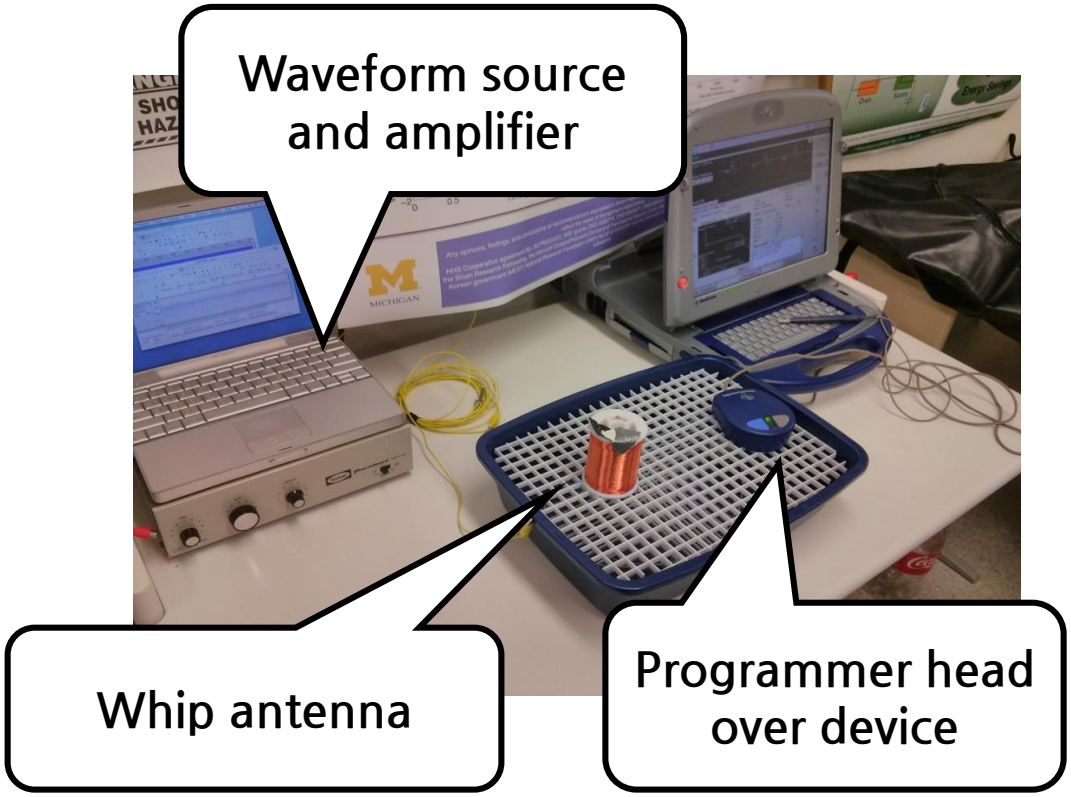


Cardiac Implantable Electrical Device (CIED)

Experimental Setup

- Goal
  - Create pacing inhibition and defibrillation shocks of CIED

- Conditions
  - Free air
  - Saline bath
  - Synthetic human



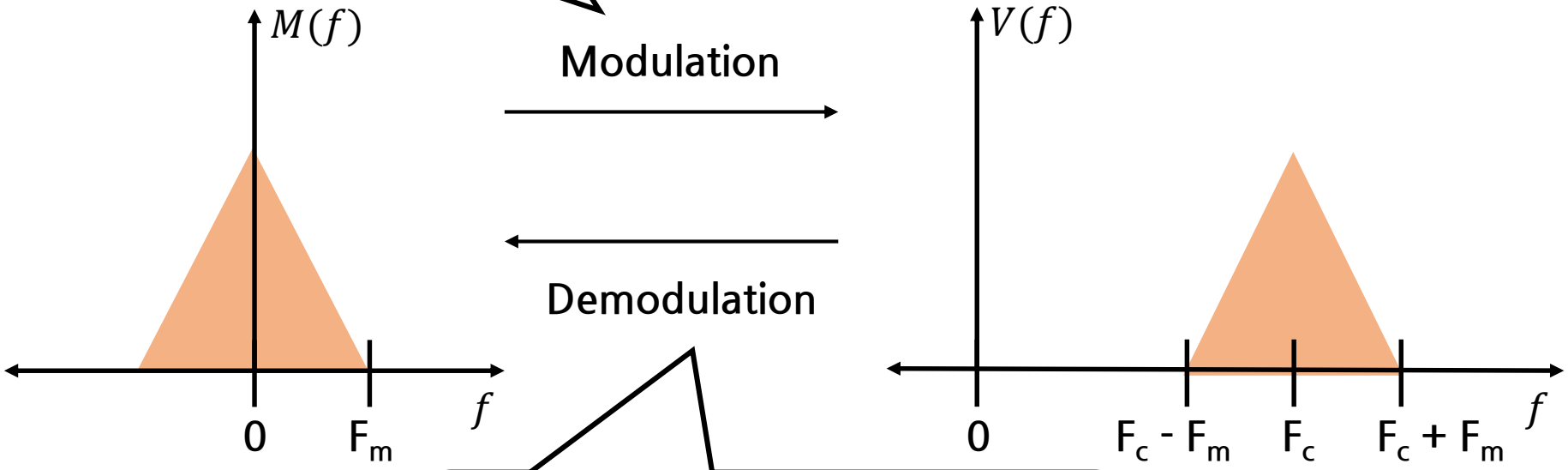
Result

Device	Open air	Saline Bath	Synthetic Human
Medtronic Adapta (Pacemaker)	1.40m	0.03m	*Untested*
Medtronic Insync Sentry (Defibrillator)	1.57m	0.05m	0.08m
Boston Scientific ICD (Defibrillator)	1.34m	*Untested*	*Untested*
St. Jude ICD (Defibrillator)	0.68m	*Untested*	*Untested*

Amplitude-Modulated EMI Attack

Amplitude Modulation

$$v(t) = (m(t) + 1)cos(2\pi F_c t)$$



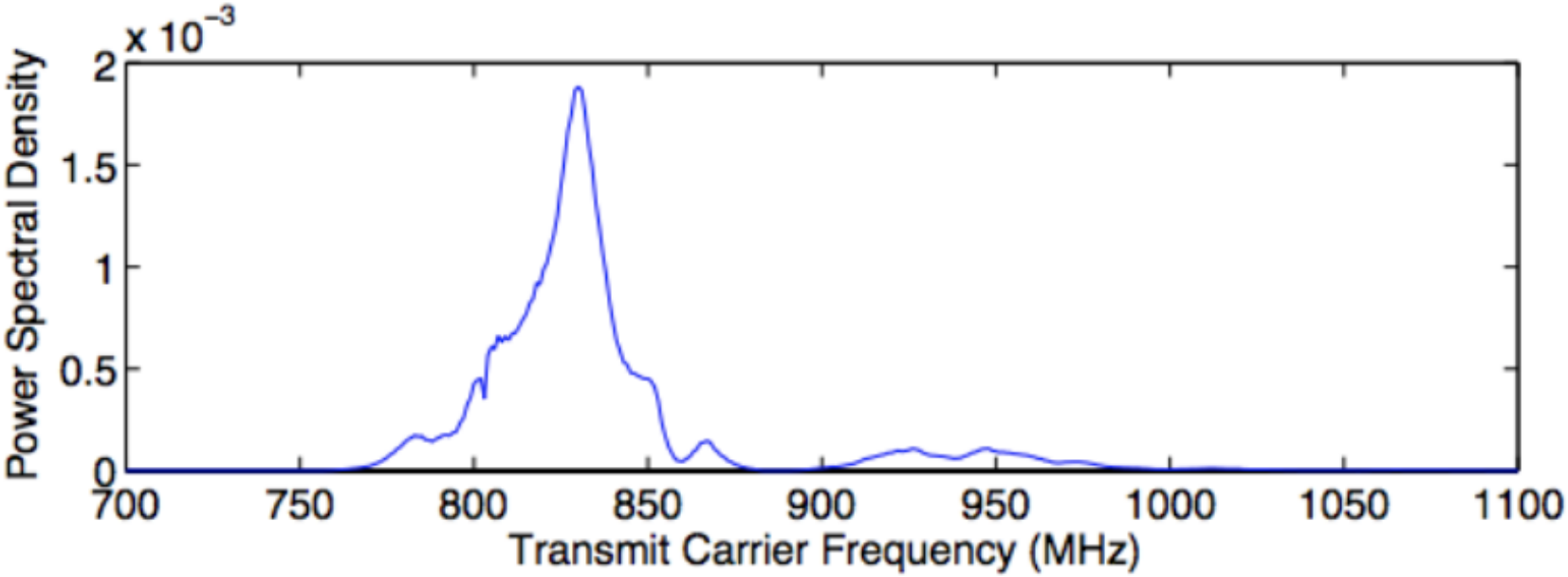
Nonlinear components

Analog-Digital Convertor (ADC)

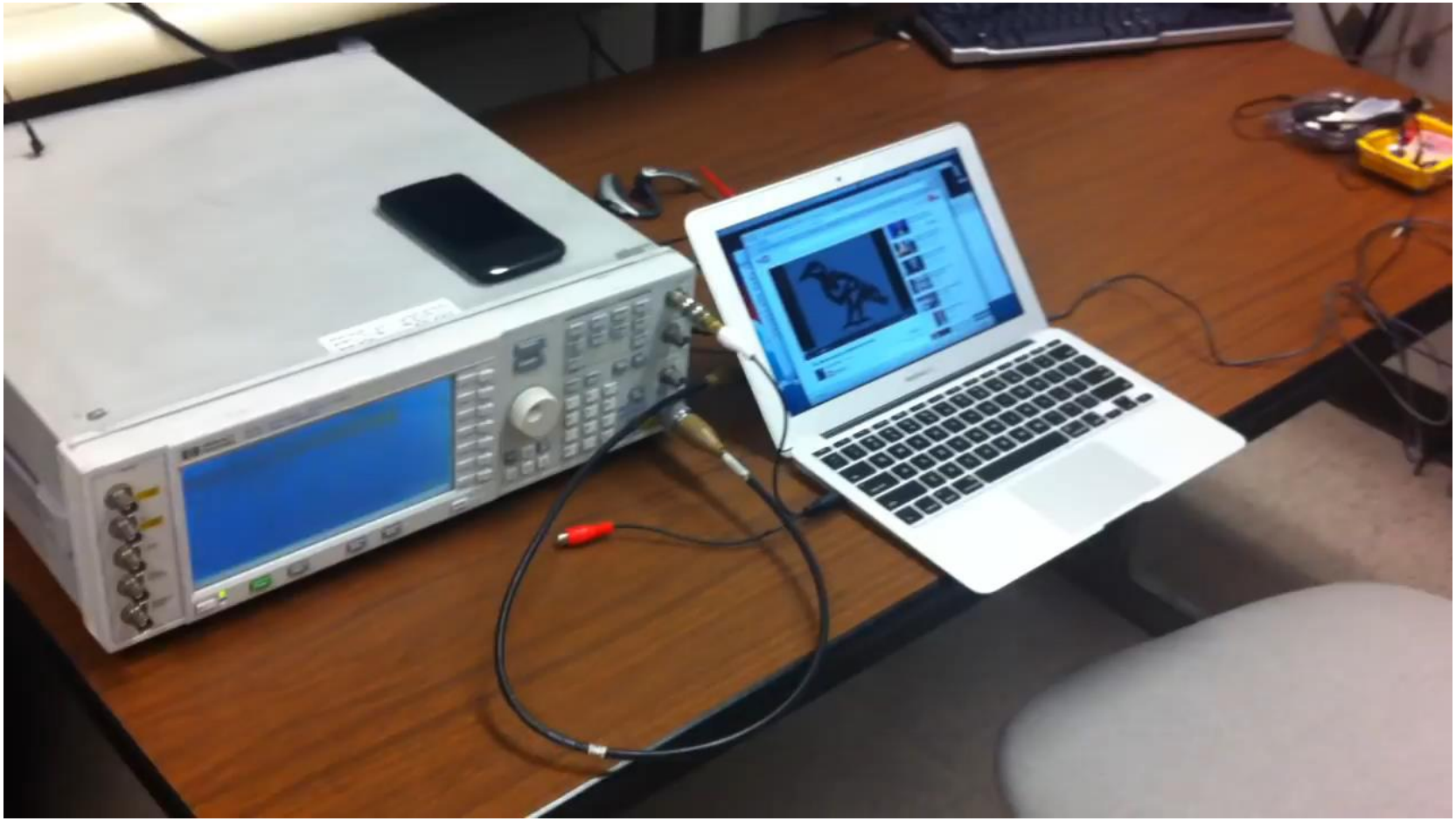
Capacitor & Diode

Amplitude Modulation

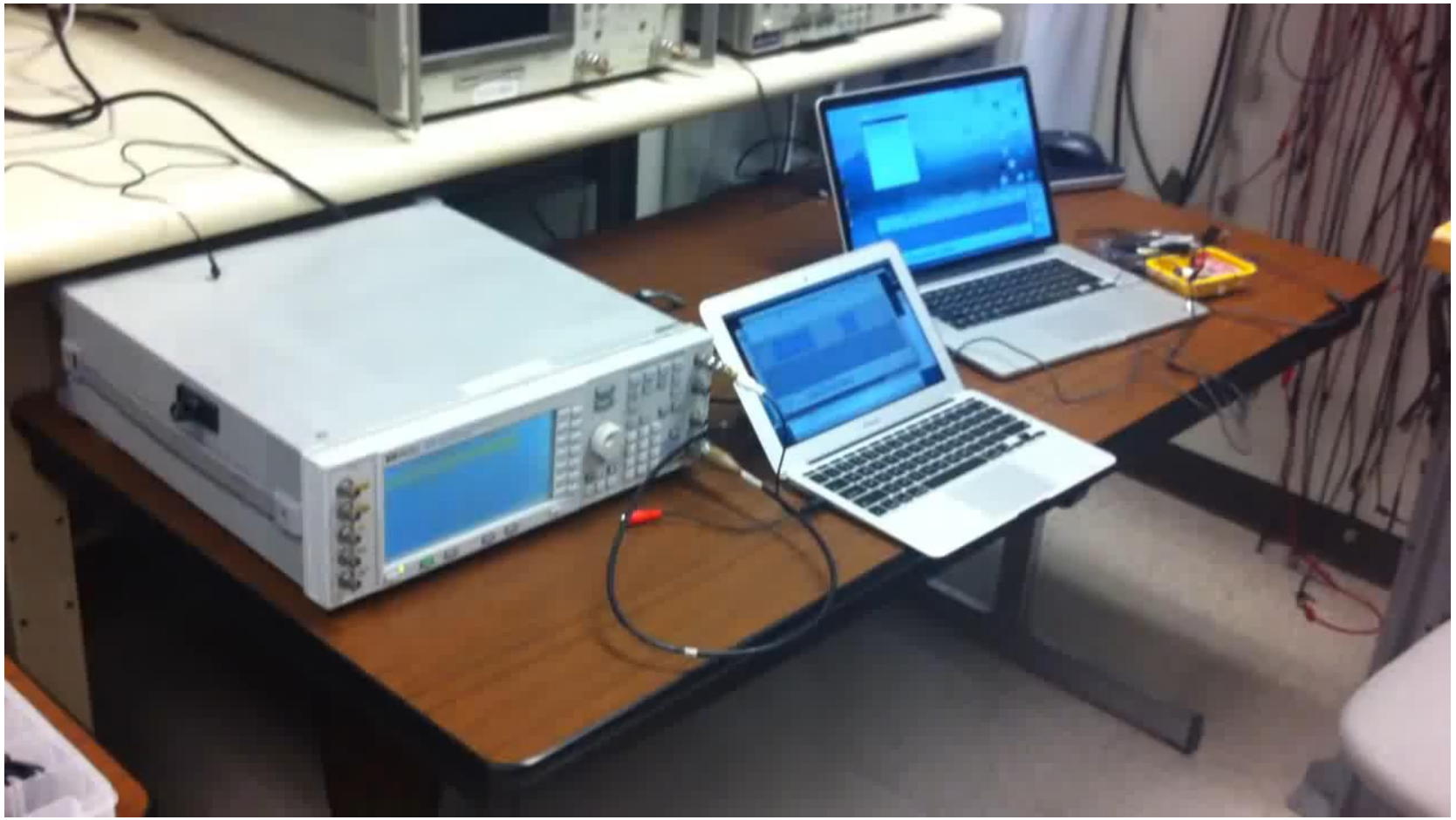
- Resonant Frequency



Demo - Injecting Voice Signal



Demo - Automated Dial-in System

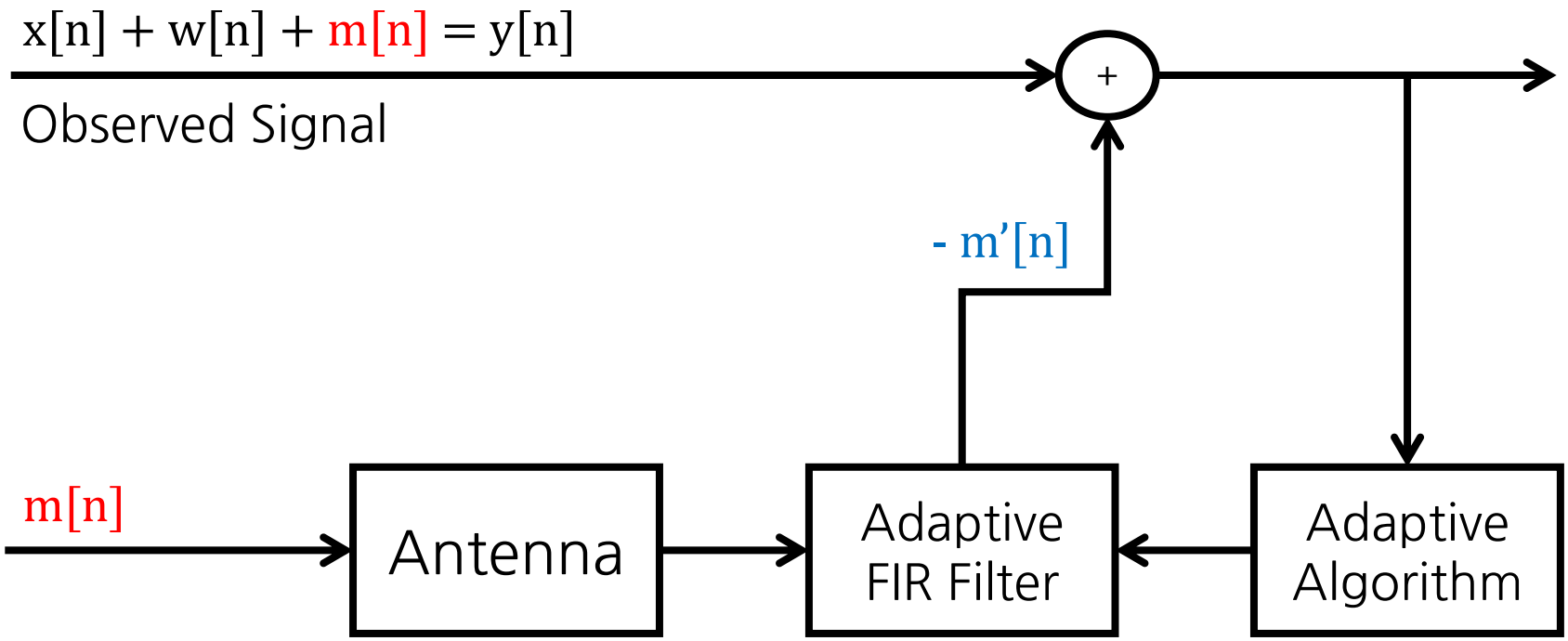


Defense

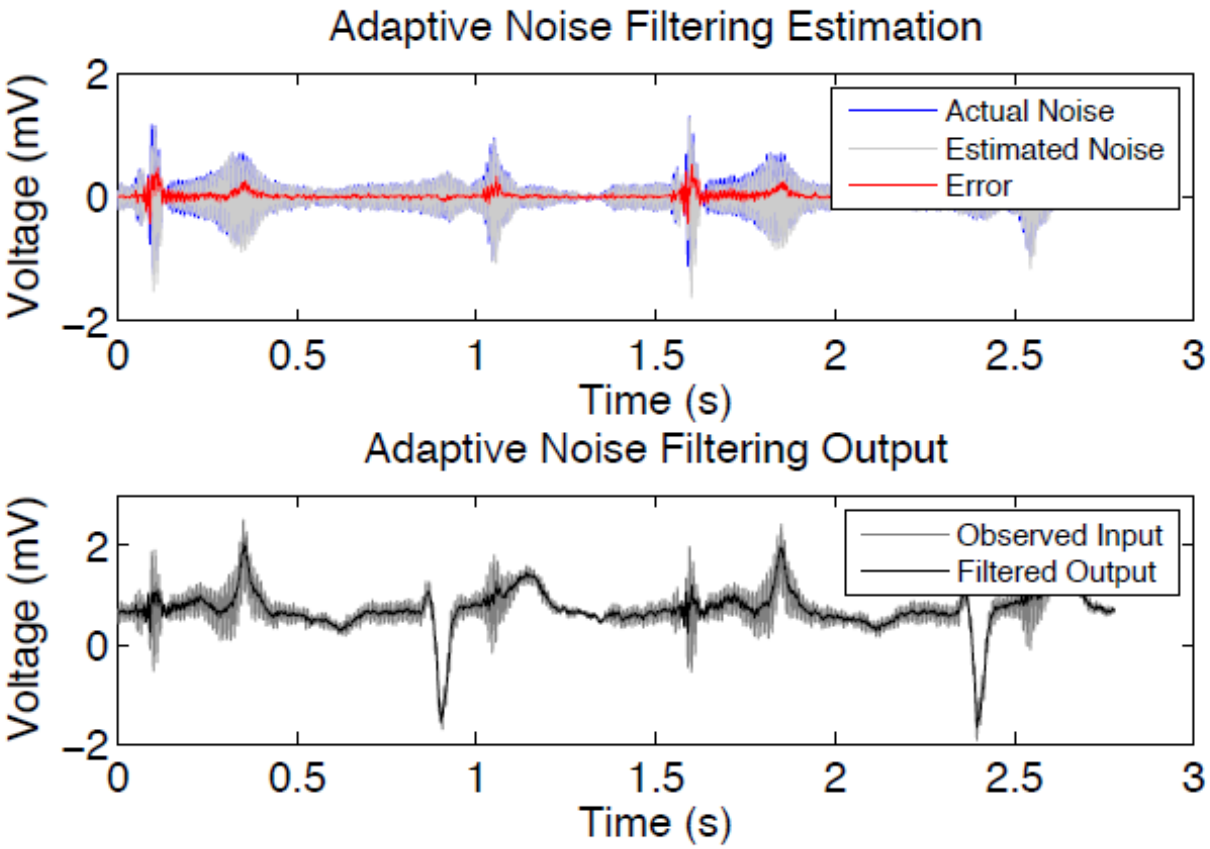
Analog Defense

Digital Defense

- Adaptive Filtering
  - Estimate the EMI level in the environment
  - Activate when EMI level is over the threshold
  - Estimate the induced voltage and clean the received signal



Digital Defense



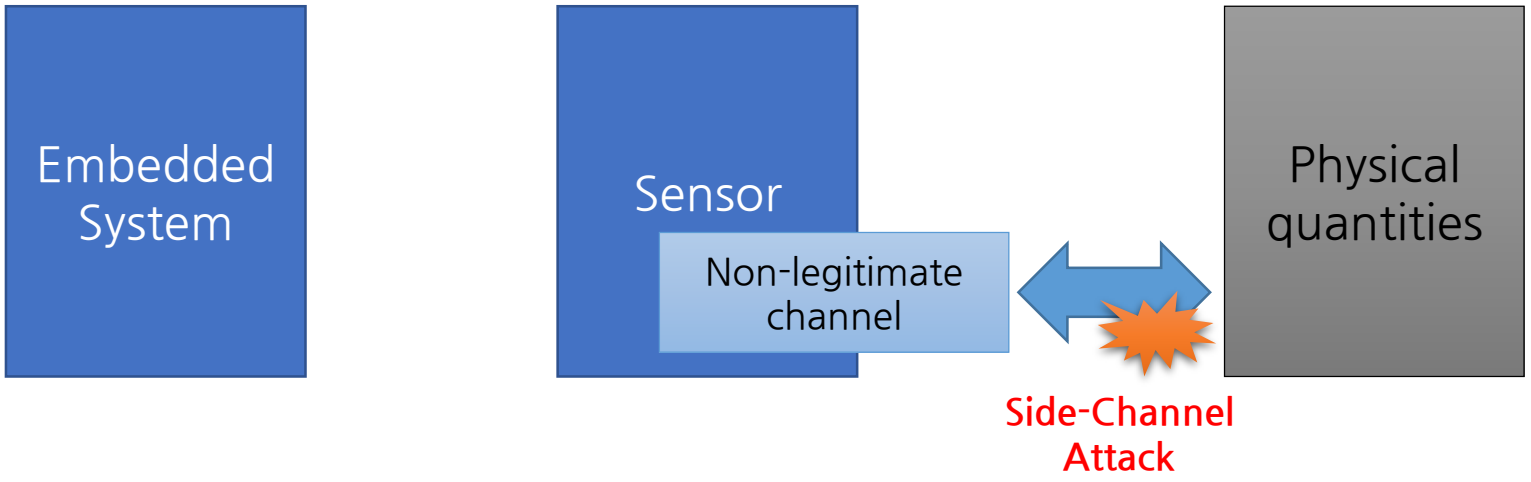
Related Work

Related Work

- "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses"
  - Demonstrate vulnerabilities of medical devices
- "Methodology for classifying facilities with respect to intentional EMI"
  - Investigate disruption to digital circuits by intentional and high intensity radiation
- TEMPEST
  - Spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations.

Work After This Work

- "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors"
- "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks"
- "Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors"



Conclusion

Conclusion

❖ Importance of sensor security

❖Intentional low-power EMI can inject malicious signal into analog sensors

- Baseband EMI Attack & Amplitude-Modulated EMI Attack
- Make pacing inhibition and defibrillation shocks of CIEDs
- Inject voice signal into microphone
- Inject DTMF signal into Bluetooth headset

❖ Defense method

- Adaptive filtering

Questions

❖ Q1: What is the difference between Ghost talk and Dolphin attack? (Tuan, 황영빈)

	Ghost Talk	Dolphin Attack
Attack vector	EMI	Acoustic signals
Injection spot	Between sensors and system (e.g. wire)	Sensor (Microphone)
Attack types	Baseband & Amplitude modulation	Amplitude modulation
Demodulator	Nonlinear components ADC Capacitor & Diode	Nonlinear components

Questions

- Q2: Many IoT devices, drones, and automobiles use sensors these days. Does this vulnerability exist? (이태화, 진영진)
  - YES!
  - Attacker have to know baseband or resonant frequency that accept by system
- Q3: There are many defense method, But this attack is still valid. Is there any realistic way than theoretical way for the manufacturer? (고우영)
  - Shielding
  - Cannot defense high power EMI

Questions

- Q4. EMI seems stealthy, powerful attack, but distance for this attack is quite limited. Is there EMI attack with longer attack range? (한상구)
  - Need high power

$$P_r = P_t G_t G_r (\frac{\lambda}{4\pi d})^2$$

- Q5. To prevent such attacks, can we apply interference cancellation technology widely used in the communication field? (김성중)
  - Adaptive filtering is a kind of interference cancellation method

Thank You