ESE 3400: Medical Devices Lab

Lec 17: November 14, 2022

RF ID and Wireless Communication

Today

- RF ID technology
- Wireless Communication
  - Bluetooth LE

RF ID

RF ID

- Radio Frequency Identification (RFID), a wireless technology primarily known from the field of logistics, has become a focal point in hospitals and similar areas
- RFID makes it possible to manage hospital beds from a central location or track the whereabouts of surgical instruments

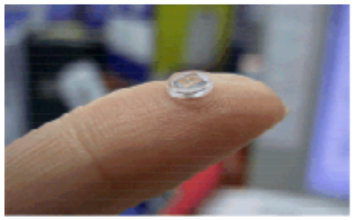
Optimization of Clinical Use

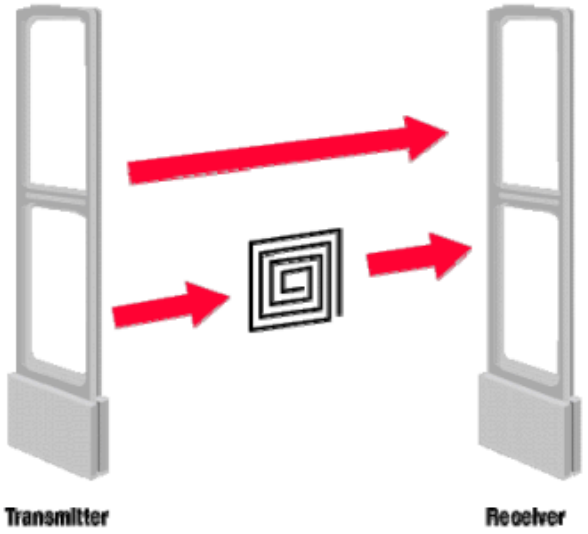
- Medical accessories now provides new possibilities in the area of intensive care
- For example, hospital staff can be relieved of routine activities when a signal indicates that a water trap must be replaced or a ventilator automatically adjusts settings of a connected accessory such as a ventilation hose
- This enables the optimization of clinical workflows.

RFID simplifies the connection and monitoring of medical accessory components

What is RFID

- Radio Frequency Identification
- Reader queries using RF
- Tag/Fob sends its ID using RF





RFID Tags

- Tag = Antenna, Radio receiver, radio modulator, control logic, memory and a power system
- Power Source:
  - Passive Tags: Powered by incoming RF. Smaller, cheaper, long-life. Approx range 5m.
  - Active Tags: Battery powered. Can be read 100 ft away. More reliable reading.
  - Semi-Passive tags: Transmit using 'Backscatter' of readers' RF power. Battery for logic. Range like passive. Reliability like active.

RFID Readers

- Sends a pulse of radio energy and listens for tags response
- Readers may be always on, e.g., toll collection system or turned on by an event, e.g., animal tracking
- Postage stamps size readers for embedding in cell phones
  Larger readers are size of desktop computers
- Most RFID systems use License-exempt spectrum
- Trend towards high-frequency

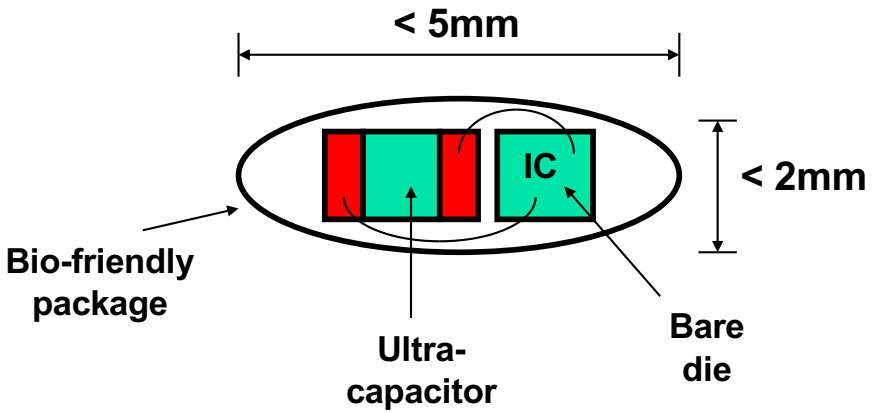
Band	Frequency	λ	Classical Use
LF	125-134.2 kHz	2,400 m	Animal tagging and keyless entry
HF	13.56 MHz	22 m	
UHF	865.5-867.6 MHz (Europe) 915 MHz (USA) 950-956 MHz (Japan)	32.8 cm	Smart cards, logistics, and item management
ISM	2.4 GHz	12.5 cm	Item Management

Microchip Implants

- Microchip implants are generally shaped like cylinders.
- They contain a small microchip, a bio-safe epoxy resin, and a copper antenna wire coil encased in glass.
- Microchips used for both animals and humans are field powered and have no battery or power source.
- Therefore, they are inert until they come within the field produced by a reader device, which implants communicate with over a magnetic field.

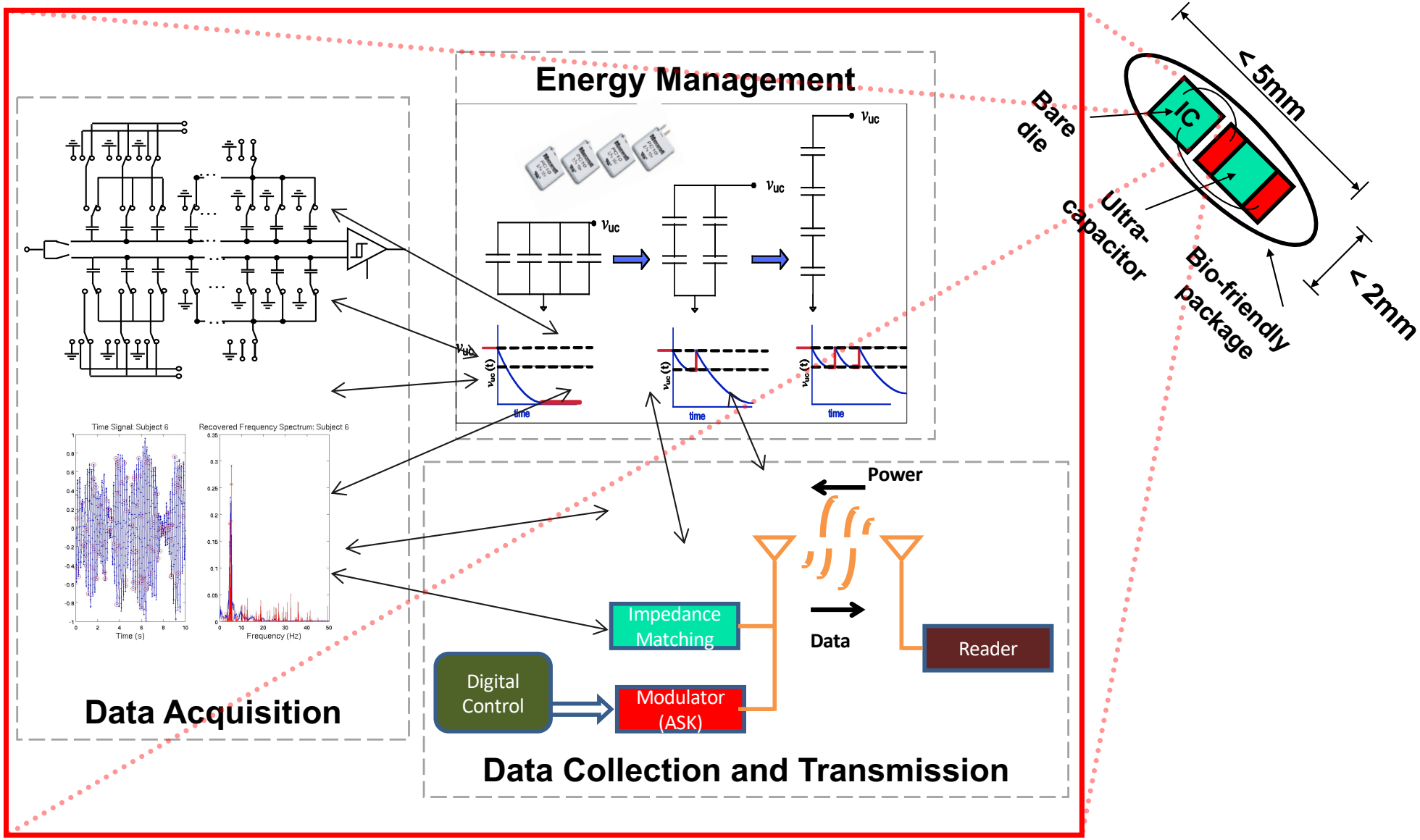
Minimally Invasive Implant to Combat Healthcare Noncompliance

- Non-compliance causes 300,000 U.S. deaths annually
- 10-25% of hospital & nursing home admissions
  - > $39 billion



- **Model for implants: reconfigurable RFID tags that periodically record specific biometric**
  - During the read operation, energy storage element is recharged
  - **Size of package small enough to allow injection**
    - **Actigraphy expected to be clinically useful**
  - Platform allows for any sensor that gathers information on a slow time scale

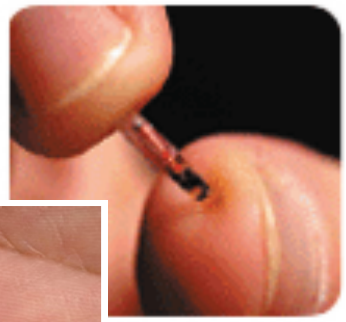
MicroImplant: An Electronic Platform for Minimally Invasive Sensory Monitors



Commercial Products

Respironics

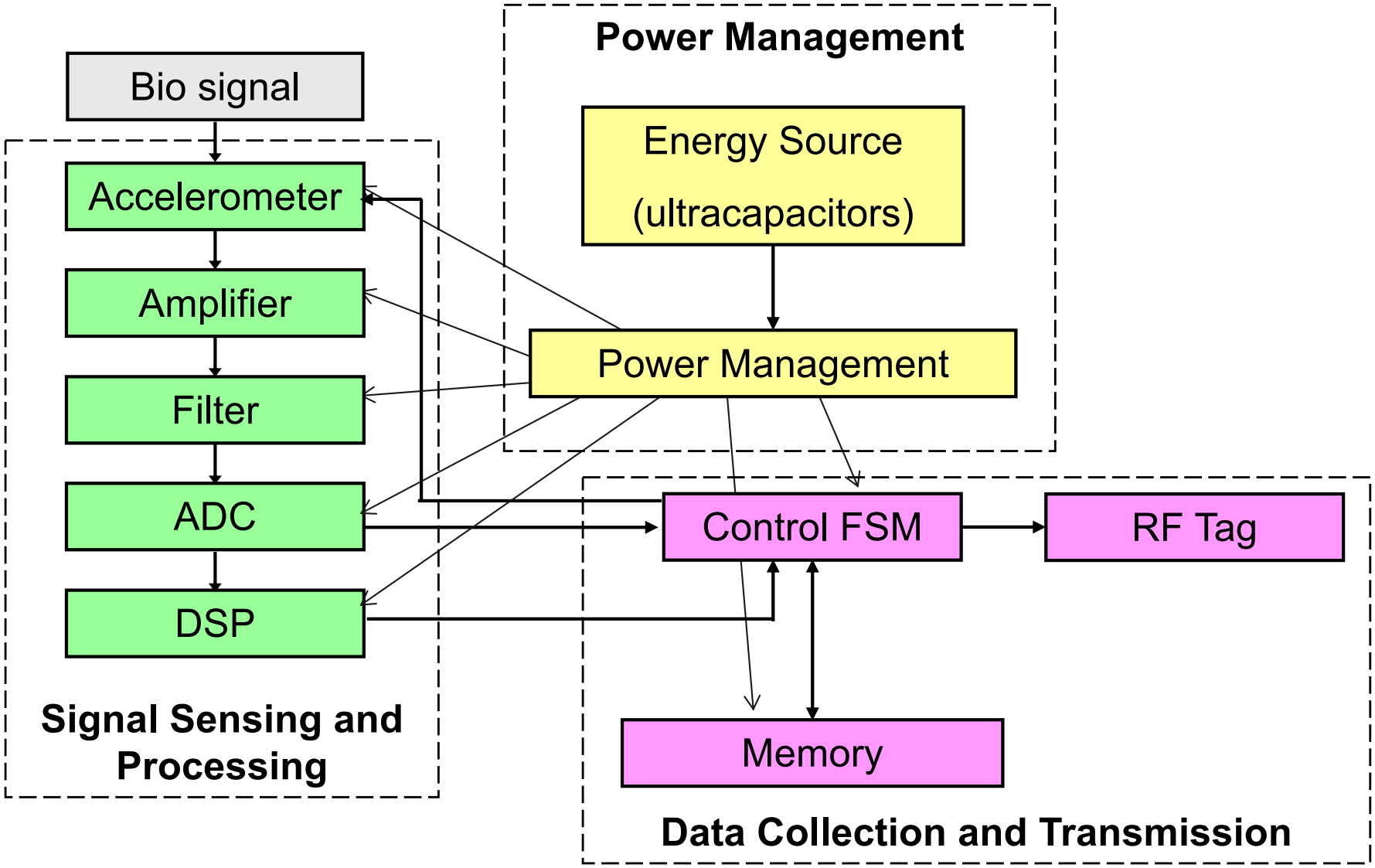
<2mA from 1.05-1.5V battery



VeriChip™

- For the desired functionality, current products are:
  - Too power hungry
  - Too big
- Proposed design meets desired functionality with
  - A new power management scheme to eliminate a battery
  - System design that includes application as a system tradeoff to optimize circuits
    - Ex. tradeoff speed for power

System Diagram



Bluetooth LE

Motivation

- With micro-sized, ultra-thin, flexible, and biocompatible electronic systems
- giving way to wearable and implantable devices that can achieve the same functionality at greatly reduced patient discomfort
- In addition, wireless medical solutions are often much more affordable for patients and lower cost for healthcare providers

Bluetooth Low Energy

- Bluetooth technologies epitomize recent advances in wireless technologies that allow for the remote operation of mobile medical devices
- In 2010, Bluetooth released its latest wireless platform: Bluetooth Low Energy (BLE), aimed at creating wireless applications in numerous fields including healthcare
  - provides devices with wireless communications at aggressive power metrics and low costs without sacrificing performance relative to other wireless standards.

Bluetooth Low Energy

Parameter	Value	Unit
Open Field Transmission Range	150	m
Output Power	10	dBm
Max Current Draw	15	mA
Sleep Current	1.0	µA
Carrier Frequency	2.4	GHz
Data Throughput	1.0	Mbps

Bluetooth Low Energy Specifications. Source: Bluetooth 4.0: Low Energy (2010, p. 8).

Other Protocols

	ANT	Bluetooth	Bluetooth LE	ZigBee
Standardisation	Proprietary	Standard	Standard	Standard
Topologies	Point-to-point, star, tree, mesh[3]	Point-to-point, scatternet	Point-to-point, star, mesh	Mesh
Band	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz (+ sub-GHz for ZigBee PRO)
Range	30 metres at 0 dBm[8]	1–100 metres	10–600 metres in air (Bluetooth 5)	10–100 metres
Max data rate	Broadcast/Ack - 200 Hz[9] × 8 bytes × 8 bits = 12.8 kbit/s Burst - 20 kbit/s[9] Advanced Burst - 60kbit/s[9]	1-3 Mbit/s[8]	125 kbit/sec, 250 kbit/sec, 500 kbit/sec, 1 Mbit/s,[8] 2 Mbit/s (Bluetooth 5 PHY speeds)	250 kbit/s (at 2.4 GHz)
Application throughput	0.5 Hz to 200 Hz (8 bytes data)[9]	0.7-2.1 Mbit/s[8]	305 kbit/s[8] (Bluetooth 4.0)	
Max nodes in piconet	65533 per shared channel (8 shared channels) [8]	1 sink and 7 active sensors, 200+ inactive[8]	1 sink and 7 sensors (but scatternet unlimited),[8] mesh - 32767[10]	star - 65536[8]
Security	AES-128 and 64-bit key	56-128 bit key	AES-128	AES-128
Modulation	GFSK	GFSK	GFSK	OQPSK

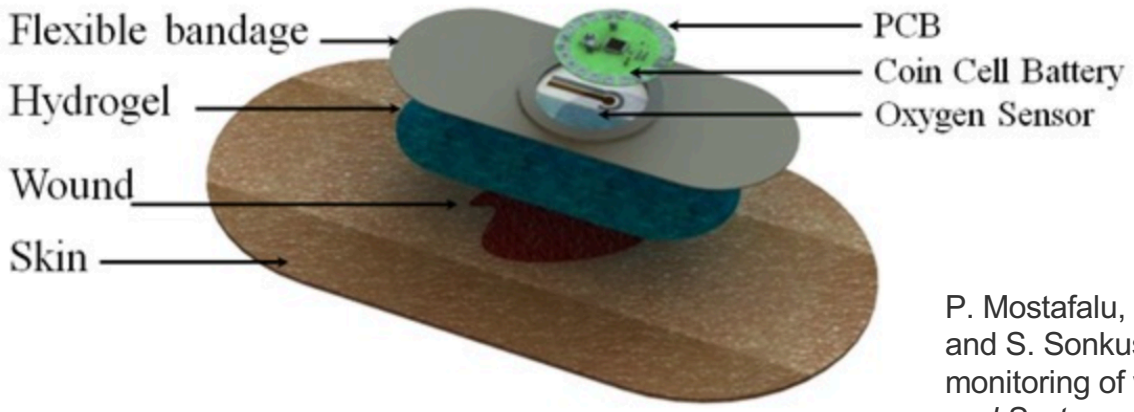
Power Comparison

EXPERIMENTAL RESULTS USING 3.3 V SUPPLY

	BLE	ZigBee	ANT
Time of one connection ±SD*	1150 ms ±260 ms	250 ms ±9.1 ms	930 ms ±230 ms
Sleep current	0.78 uA	4.18 uA	3.1 uA
Awake current	4.5 mA	9.3 mA	2.9 mA
Min current (at 120 sec interval)	10.1 uA	15.7 uA	28.2 uA
Optimal sleep interval	10.0 s	14.3 s	15.3 s
*SD: standard deviation			

A. Dementyev, S. Hodges, S. Taylor and J. Smith, "Power consumption analysis of Bluetooth Low Energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario," *2013 IEEE International Wireless Symposium (IWS)*, 2013, pp. 1-4, doi: 10.1109/IEEE-IWS.2013.6616827.

Example: Smart Wound Dressing



P. Mostafalu, W. Lenk, M. Dokmeci, B. Ziaie, A. Khademhosseini and S. Sonkusale, "Wireless flexible smart bandage for continuous monitoring of wound oxygenation," *2014 IEEE Biomedical Circuits and Systems Conference (BioCAS) Proceedings*, 2014, pp. 456-459, doi: 10.1109/BioCAS.2014.6981761.

- A flexible, galvanic oxygen sensor on the order of 100 μm in diameter
- The oxygen sensor is interfaced via a flexible conductor to an analog-front-end circuit for amplification
- The output of the analog-front-end is read into a microcontroller through an analog-to-digital converter
- Data is converted back to a voltage value and wirelessly transmitted to a nearby computer or smartphone via a Bluetooth Low Energy

Security Risks of Wireless Communication

- A typical mobile medical device will have a low-power wireless communications system, such as a BLE or ZigBee radio.
- The use of low power radios requires an intermediate base station in close proximity to the user (e.g. 150 meters maximum for BLE) where data can be dumped and subsequently uploaded to a "secure" server
- The transmission of data across a wireless network presents a glaring security vulnerability if malicious hackers can penetrate the network security and gain access to confidential patient information.
- Furthermore, if the medical device itself can directly be accessed or programmed from a remote location, such as the previously discussed smart wound dressing, malicious hackers could actually hijack operation of the device to steal private information or cause device malfunction.

Security Breaches

- Three categories (Rushanan, 2014):
  - Telemetry Interface Breaches
    - Passive – eavesdropping breaching patient confidentiality
    - Active – jam, modify or forge the information exchange
  - Software Threats
  - Hardware/Sensor Threats
    - Eg. Rowhammer attack

M. Rushanan, A. D. Rubin, D. F. Kune and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," *2014 IEEE Symposium on Security and Privacy*, 2014, pp. 524-539, doi: 10.1109/SP.2014.40.

Example: Insulin Pump

- Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System
  - Jerome Radcliffe
- Used a relatively cheap microcontroller and available details on wireless communication command codes
- Can potentially alter readings or dosages

- https://cs.uno.edu/~dbilar/BH-US-2011/materials/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf

Security Solutions

- Advances in electrical engineering and related fields such as computer science can certainly mitigate these risks as well
- Researches are investigating highly advanced data encryption methods, security protocols, and trust models to help secure wireless medical instruments

Example: Trustworthy Data Collection

- Public-key cryptography standard (IEEE 1363) with a complex, probabilistic trust model to demonstrate highly trustworthy data collection
- Data is scrambled and two "keys" are required to unscramble
  - Keys are mathematically related but computationally infeasible to generate private from public
- Trust model no longer binary but continuous between 0 and 1

Hu F, Hao Q, Lukowiak M, Sun Q, Wilhelm K, Radziszowski S, Wu Y. Trustworthy data collection from implantable medical devices via high-speed security implementation based on IEEE 1363. IEEE Trans Inf Technol Biomed. 2010 Nov;14(6):1397-404. doi: 10.1109/TITB.2010.2049204. Epub 2010 Apr 26. PMID: 20423808.

Big Ideas

- RF ID used to automate and optimize clinical systems
  - Tags hold information and transmit data to reader
  - Mostly near field use
- Wireless communication
  - Needs to be low energy
    - BLE is taking over as industry standard
  - Poses security risk
    - Need trustworthy security protocols

Admin

- Finish Lab 9 by tomorrow
  - Submit Google Colab PDF in Canvas
  - Keep filled out Google Colab doc in drive
    - You each have your own drive
- Lab 10 tomorrow
  - CircuitPython and BLE
- Quiz 2 Monday
  - Wednesday lecture review
- Project details on Wednesday