

ECE 598HH: Advanced Wireless Networks and Sensing Systems

Lecture 1: Introduction to Wireless Research Haitham Hassanieh

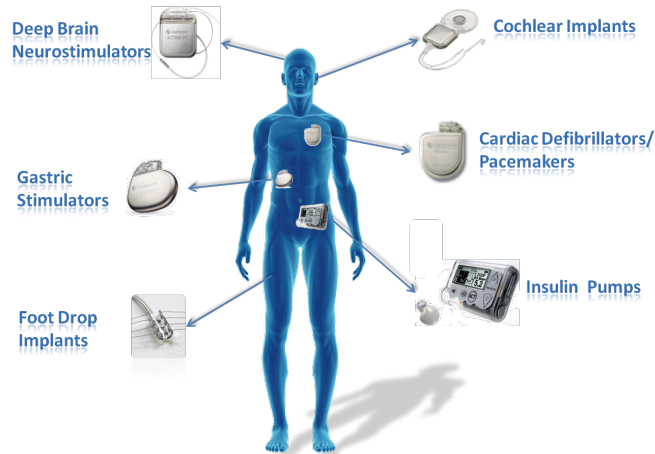


Wireless Networks Increasingly Prevalent

Wireless Homes



Wireless Biomedical Implants



Wireless Wearables



Cellular Networks



Wireless Sensors



UAVs



Wireless Data Centers



Wireless VR



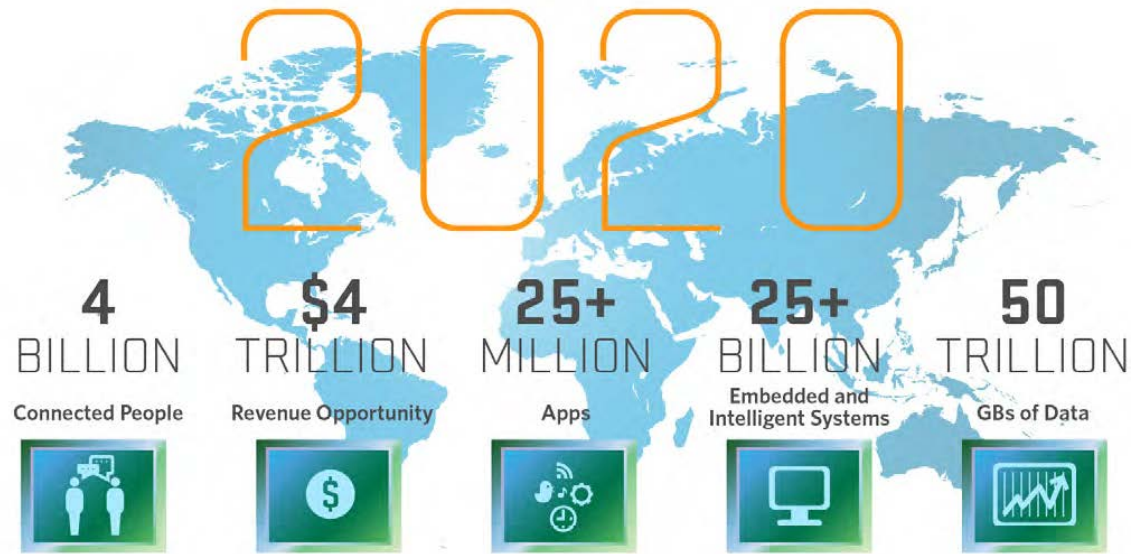
Wireless Vehicles



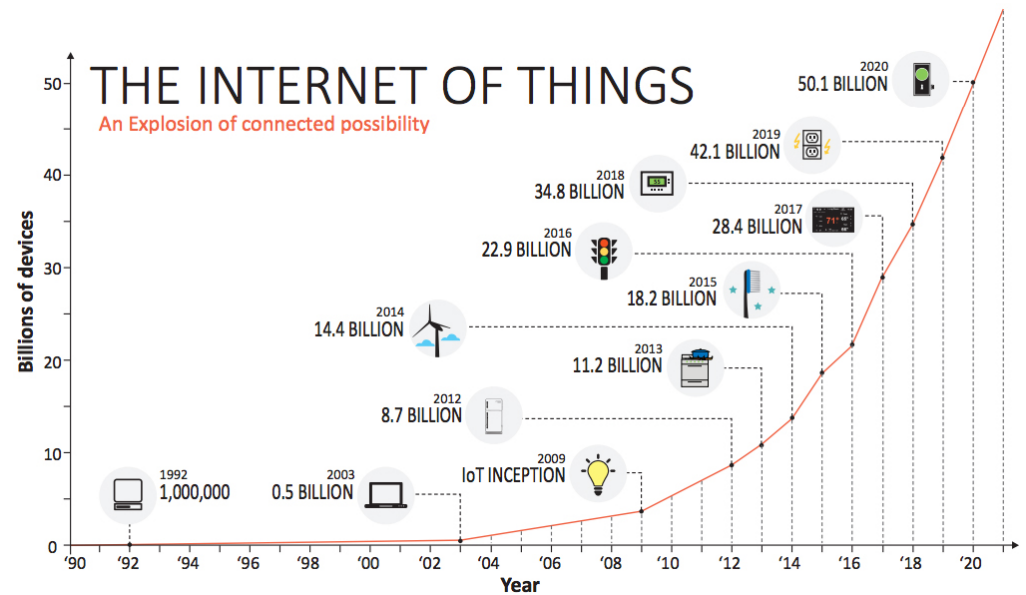
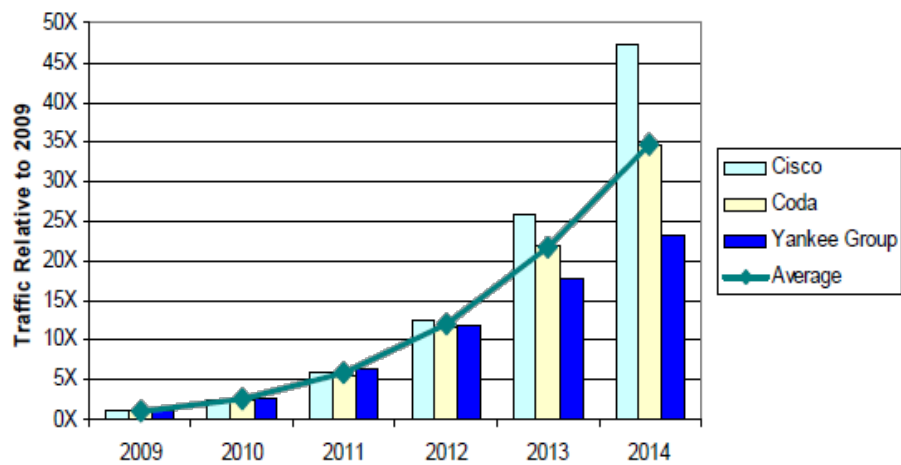
Increasing Demand for Wireless Connectivity

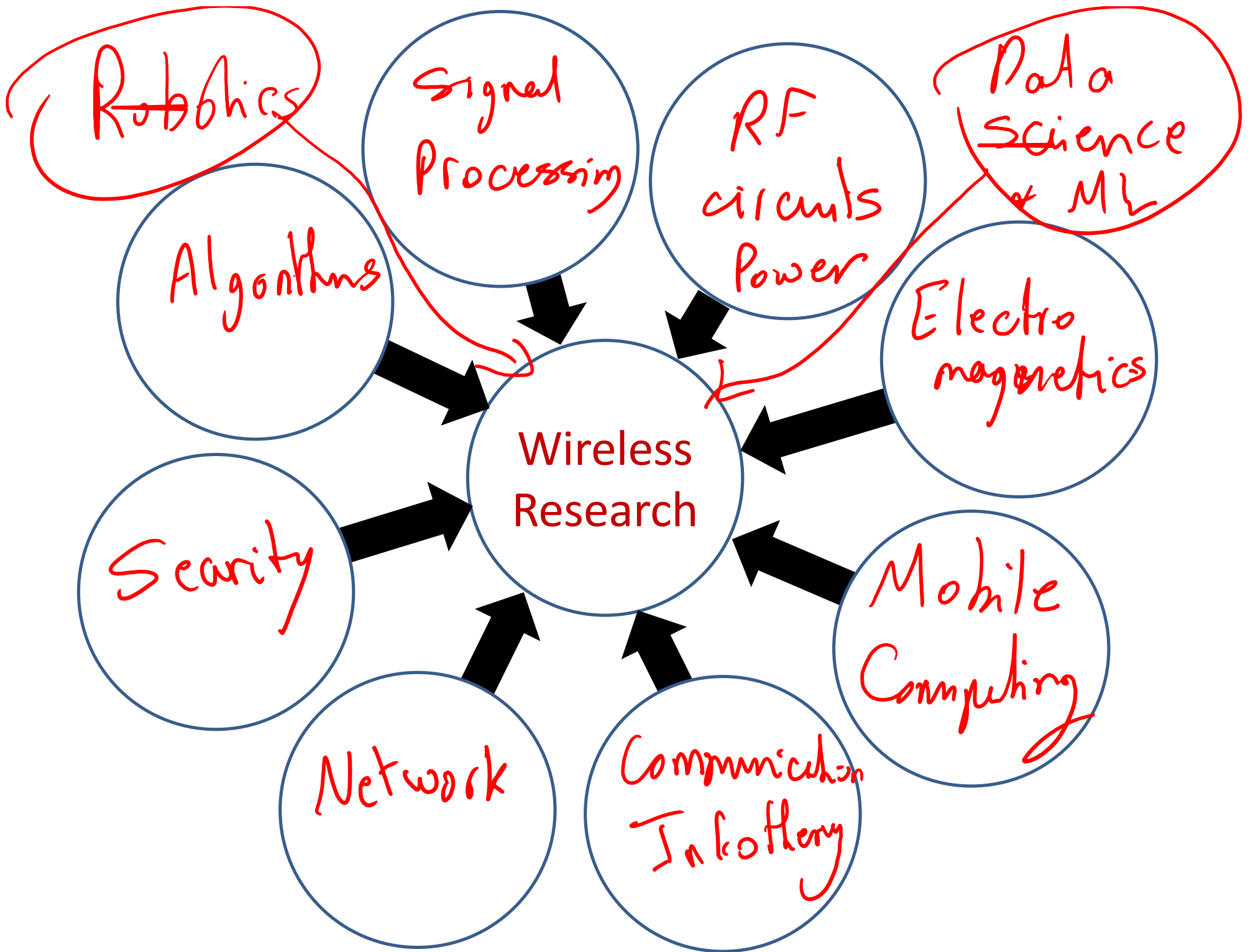


Increasing Demand for Wireless Connectivity



Source: Mario Morales, IDC





Course Information

- **Staff**

- Lecturer: Haitham Hassanieh, haitham@illinois.edu
- Office hours: Monday after class or by appointment
- TA: Suraj Jog, sjog2@illinois.edu

- **Material (new class)**

- Mainly research papers
- Lecture Slides/Notes

- **Prerequisites**

- Any undergraduate networking, wireless, communications or RF class
- Basic math and signal processing: probability, Fourier, ...
- Matlab or C programming (Important for the project).

Course Structure

- **Grading**
 - 50% Research Project: Proposal, Progress report, Poster, Final report
 - Research project: propose and test new ideas.
 - Negative results are OK
 - Idea can/should be related to your own research.
 - 10% Paper reviews
 - Review includes: 3 strengths, 3 weaknesses.
 - Review 10 out of the 25 assigned papers. Review due on compass before class.
 - **READ: How to read a paper?**
 - 20% Homework Assignments: 2 HWs
 - 20% Lab Assignments: 2 Labs
 - Learn how to use software defined radios in lab.
 - Run some measurements and write a Matlab code to process data. Submit your code & results
 - Bonus: Participation in class.
 - Expected to read all papers and participate in class.

Class Webpage

<https://courses.engr.illinois.edu/ece598hh/sp2018/>

ECE 598HH (Spring 2018): Advanced Wireless Networks and Sensing Systems



General Information

Course Schedule & Materials

Course Project

Course Description:

Wireless and mobile systems have become ubiquitous; playing a significant role in our everyday life. However, the increasing demand for wireless connectivity and the emergence of new areas such as the Internet of Things present new research challenges. This course introduces advanced research topics in wireless networks and mobile communication systems. In each lecture, we will discuss recent research papers that introduce new wireless designs, algorithms, protocols and applications. The papers are systems oriented and focus on practical challenges and solutions for building wireless and mobile systems. Students will also learn how to design and build wireless systems through a research oriented course project that focuses on the implementation aspects of practical systems.

Lecture Time & Location: Monday & Wednesday 3:00pm - 4:20pm in ECEB 4070

Instructor: [Haitham Hassanich](mailto:haitham@illinois.edu) (haitham@illinois.edu)

Office Hours: Monday 4:20pm - 5:00pm in ECEB 4070 or by appointment.

Course TA: [Suraj Jog](mailto:sjog2@illinois.edu) (sjog2@illinois.edu)

Office Hours: TBD

Topics:

► Cross Layer Networking

- Rateless Codes & Soft Information
- Interference Management
- Interference Alignment & Nulling
- Virtual MIMO
- Opportunistic Routing
- Network Coding
- Wireless Multipath TCP

► Internet of Things

- LoRa Networks
- Ultra-low Power Networking
- Ambient Backscatter
- Smart Cities and Environments

► Wireless Sensing

- Localization & Tracking
- Wireless Gesture Recognition
- Wireless Imaging
- Contactless Bio-Sensing

► Security

- Analog Cybersecurity
- Medical Devices Security
- RFIDs and Low Power Devices
- Physical Layer Security
- Wireless Vibrometry
- Acoustic IoT Security

► Emerging Technologies

- Millimeter Wave Systems
- Full Duplex Radios
- Software Defined Radios
- Cloud RAN
- 5G Cellular Systems
- Dynamic Spectrum Access
- Wireless Charging
- Robotics and Drones
- V2X Communications

ECE 598HH (Spring 2018): Advanced Wireless Networks and Sensing Systems



General Information

Course Schedule & Materials

Course Project

Note: This schedule is tentative and subject to change over time due to unforeseen events. Please check it regularly.

#	Date	Topics & Slides	Notes
	Jan. 15	Martin Luther King Day	
1	Jan. 17	Lee 1: Introduction: Overview & Logistics	Reading: How to Read a Paper
2	Jan. 22	Lee 2: Wireless Communication and Networks	
3	Jan. 24	Lee 3: Wireless Channel	
4	Jan. 29	Lee 4: OFDM	Optional Reading: [Thesis] (Chapter 3)
5	Jan. 31	Lee 5: Wireless MAC & Software Defined Radios Tutorial	Assigned Reading: [FICA]
6	Feb. 5	Lee 6: Rate Adaptation & Soft Information	Assigned Reading: [RRAA] , [PPR] Optional Reading: [SoftRate] , [SampleRate] , [Strider]
7	Feb. 7	Lee 7: Interference Management	Assigned Reading: [ZigZag] Optional Reading: [SIC] , [REMAP]
8	Feb. 9	Lab 1: USRP Software Defined Radio & OFDM	Due: Mar. 7 at 11:59pm
8	Feb. 12	Lee 8: MIMO 1: Multiplexing, Diversity, MU-MIMO	Optional Reading: [Textbook 2] (Chapter 7)
9	Feb. 14	Lee 9: MIMO 2: Interference Alignment and Nulling.	Assigned Reading: [IAC] Optional Reading: [Nplus]
10	Feb. 19	Lee 10: MIMO 3: Distributed MIMO	Assigned Reading: [MegaMIMO] Optional Reading: [AirShare] , [SourceSync] , [Vidyt]
11	Feb. 21	Lee 11: Wireless Localization 1: WiFi	Assigned Reading: [ArrayTrack] Optional Reading: [PinLoc] , [PinPoint] , [Chronos]
12	Feb. 26	Lee 12: Wireless Localization 2: RFID	► Homework 1 (Due: Mar. 26) Assigned Reading: [PinIt] , [RFDraw] Optional Reading: [RFCompass]
13	Feb. 28	Lee 13: Wireless Localization 3: RFID	Assigned Reading: [RFInd] , [RFly]
14	Mar. 5	Lee 14: Wireless Sensing 1: Tracking	Assigned Reading: [WiTrack] Optional Reading: [WiVi] , [WiTrack2]
15	Mar. 7	Lee 15: Wireless Sensing 2: Vital Signs & Imaging	► Lab Assignment 1 Due Assigned Reading: [VitalRadio] Optional Reading: [RFCapture]
8	Feb. 9	Lab 2: RFID Readers & Localization	Due: Apr. 2 at 11:59pm

Rest of Today's Lecture

Sample Class Topics

Introduction to Wireless Networks

Wireless networks provide advantages

- Mobility
- Eliminates piles of wires at home and office

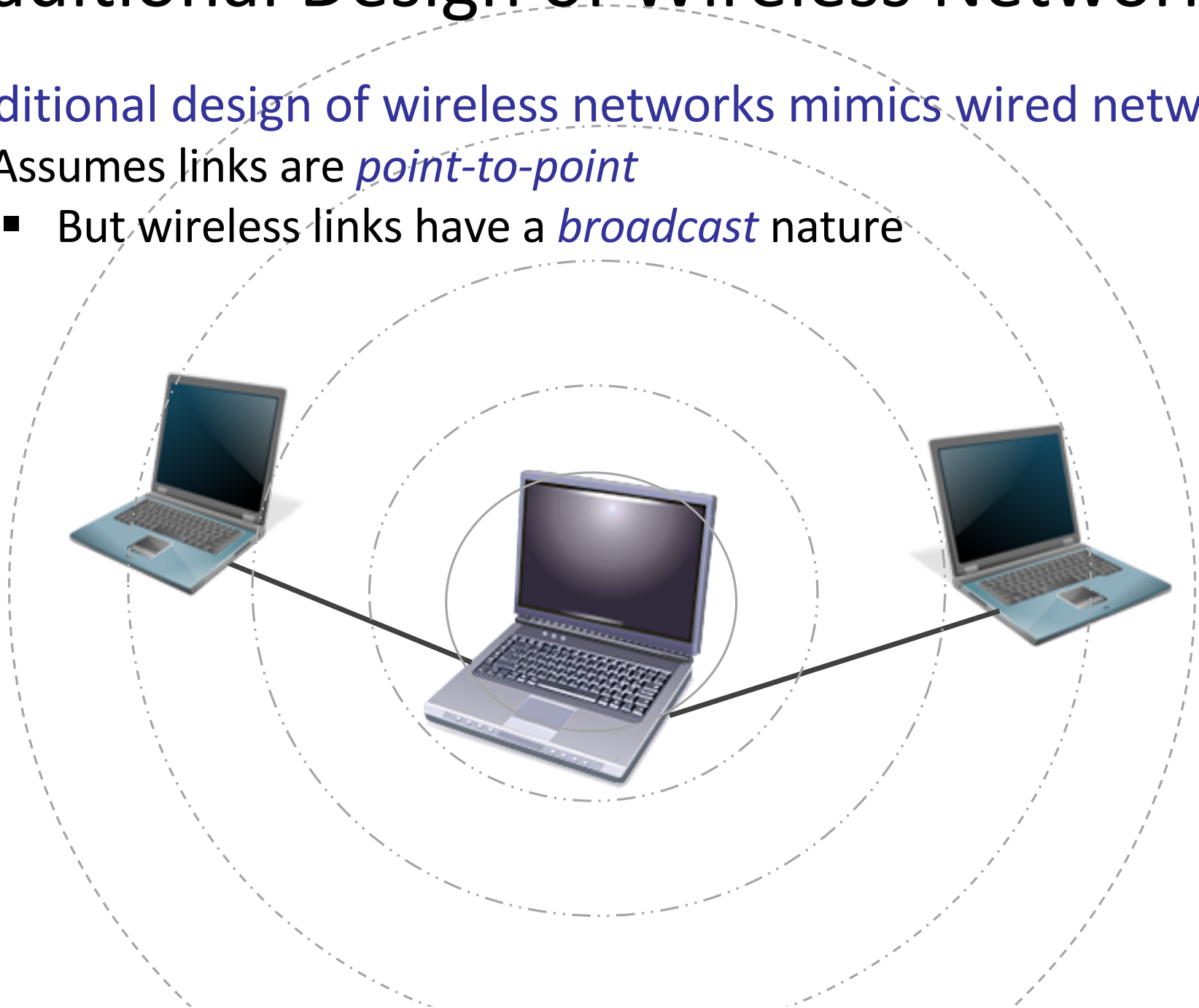
But wireless networks present different challenges

- The medium is shared → Nearby transmitters can interfere
→ Need medium access protocols
- The medium is shared → throughput is relatively low particularly when there are many devices
- Channel quality could be bad and/or unpredictable → high bit errors which could result in dead spots

Traditional Design of Wireless Networks

Traditional design of wireless networks mimics wired networks

- Assumes links are *point-to-point*
 - But wireless links have a *broadcast* nature



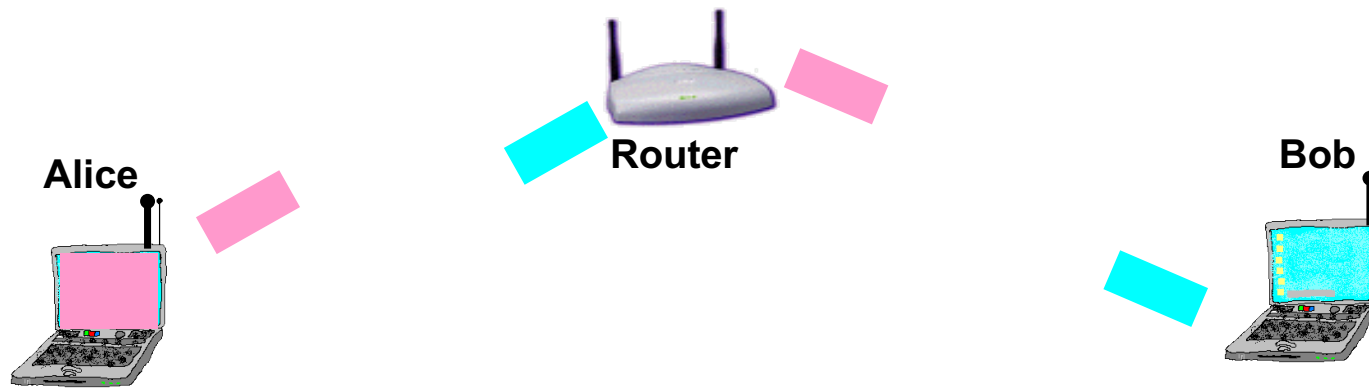
Why point-to-point is a suboptimal abstraction for wireless links?

Scenario: Alice and Bob want to exchange two packets; their radio range doesn't allow them to reach each other → they need a router to relay the packets between them



Scenario: Alice and Bob want to exchange two packets; their radio range doesn't allow them to reach each other → they need a router to relay the packets between them

Traditional Approach



Requires 4 transmissions

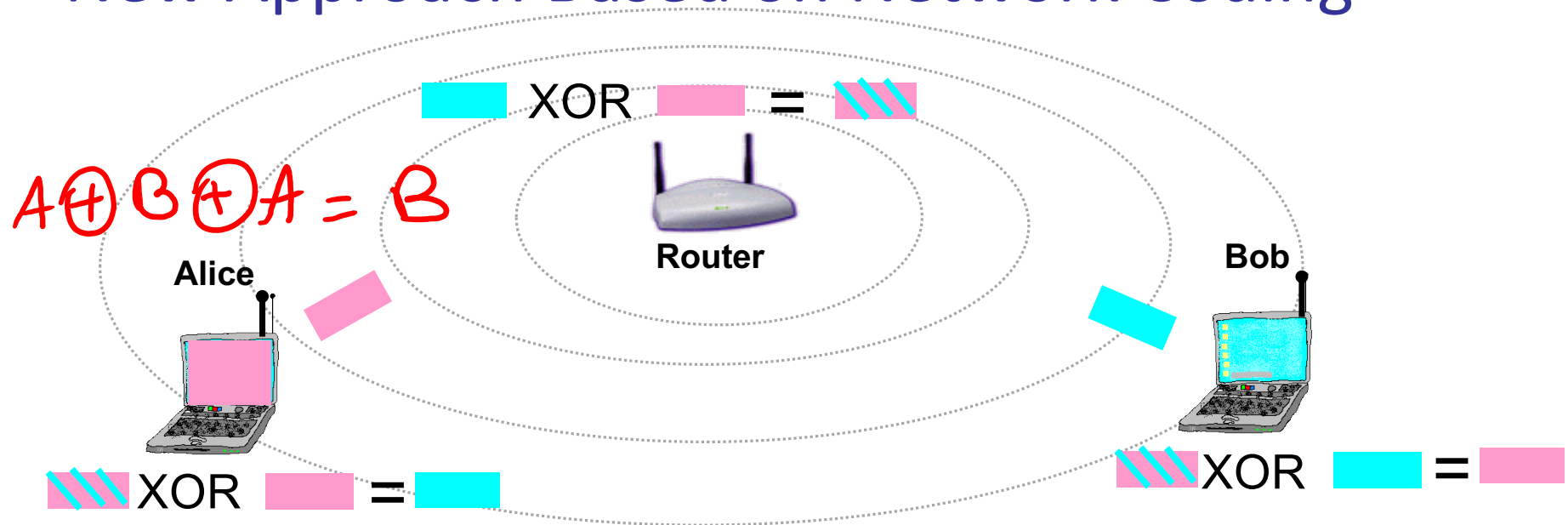
- Alice to router; Router to Bob; Bob to router; Router to Alice

But wireless links are *broadcast* not *point-to-point*!

- Can we exploit broadcast to do better?

Scenario: Alice and Bob want to exchange two packets; their radio range doesn't allow them to reach each other → they need a router to relay the packets between them

New Approach Based on Network Coding



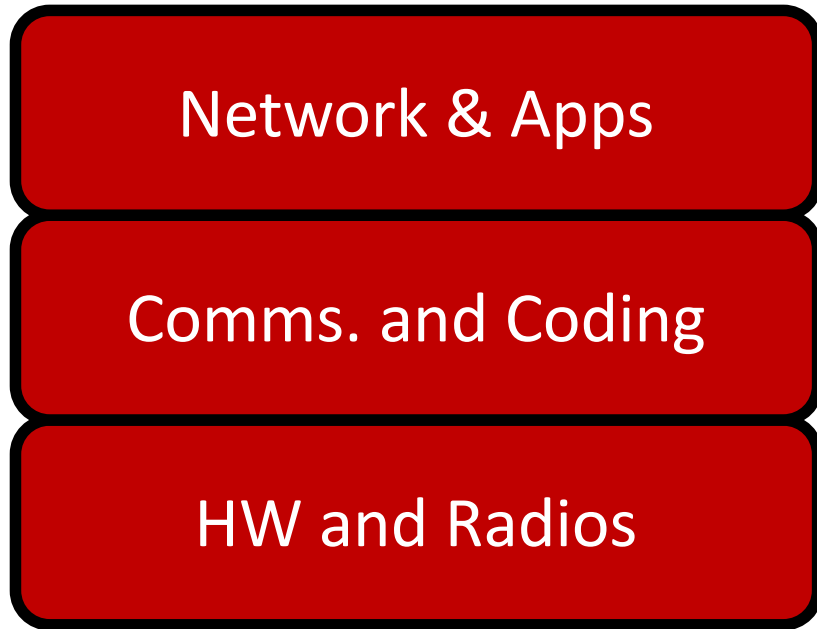
Requires 3 transmissions instead of 4

- Alice to router; Bob to router; and router to both Alice and Bob

Harnessing the broadcast nature of wireless via network coding increases throughput

Traditional Approach

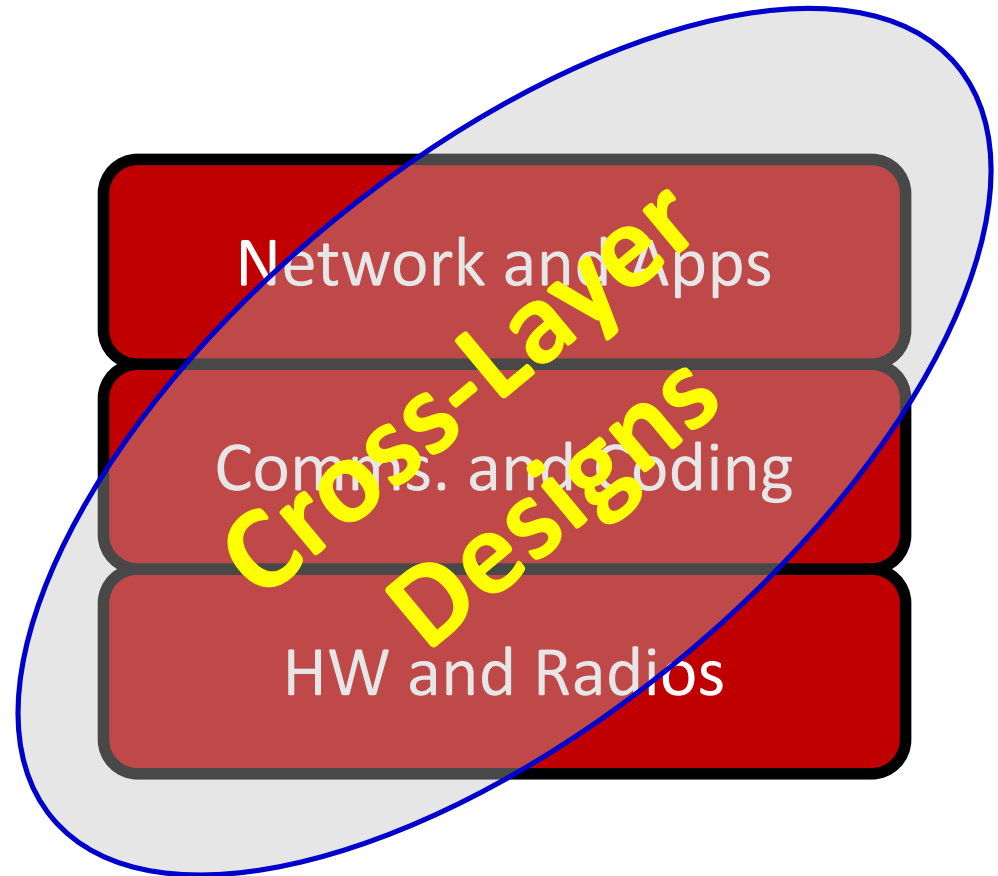
Optimize within isolated layers



Disruptive gains are unlikely

New Approach

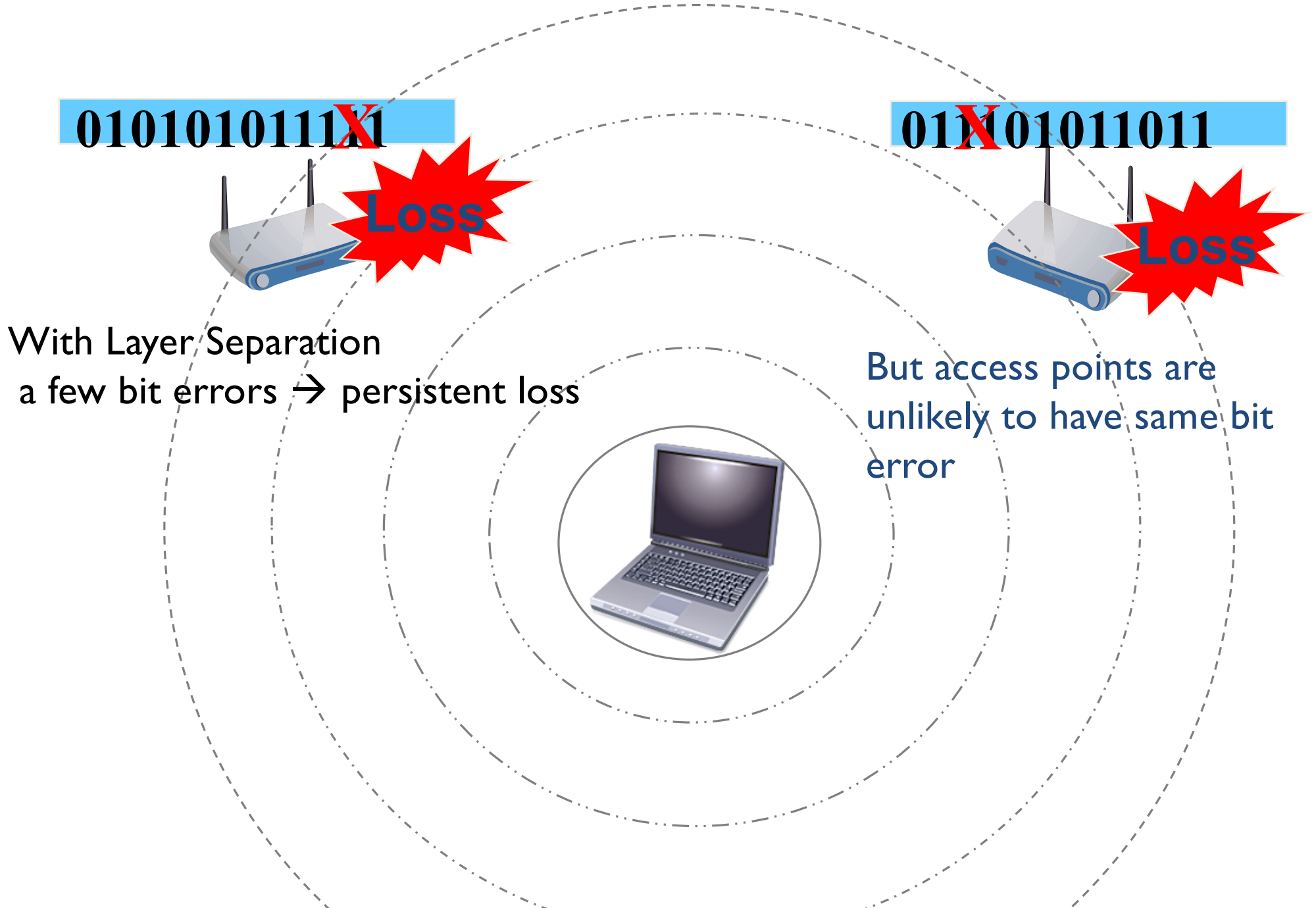
Optimize across the layers



Major opportunities!

Why layer separation is suboptimal?

Scenario: Laptop in a Dead Spot



0101010111

01101011011

Loss

Loss

With Layer Separation
a few bit errors → persistent loss

But access points are
unlikely to have same bit
error



Scenario: Laptop in a Dead Spot

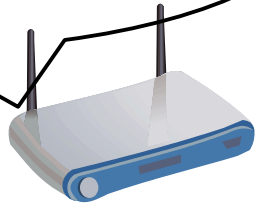


Solution: Cross-Layer Approach

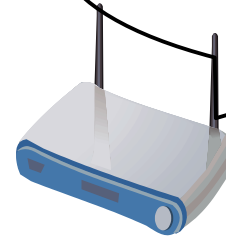
- Allow the layers to collaborate instead of acting separately
- PHY layer delivers partially correct packets
- Network layer combines correct bits across different access points to obtain correct packet

Challenge

First bit is “0”



First bit is “1”



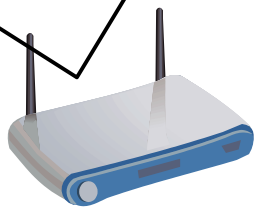
Which access point should we believe?

Solution: Network cooperates with physical layer

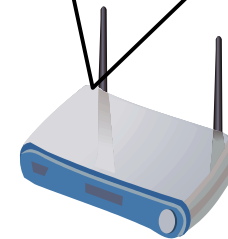


- Physical layer **already estimates a confidence** in its 0-1 decision
- If we expose this information to the network layer, we can compare bits in packets received at different APs

First bit is **“0”**
with **0.6 confidence**



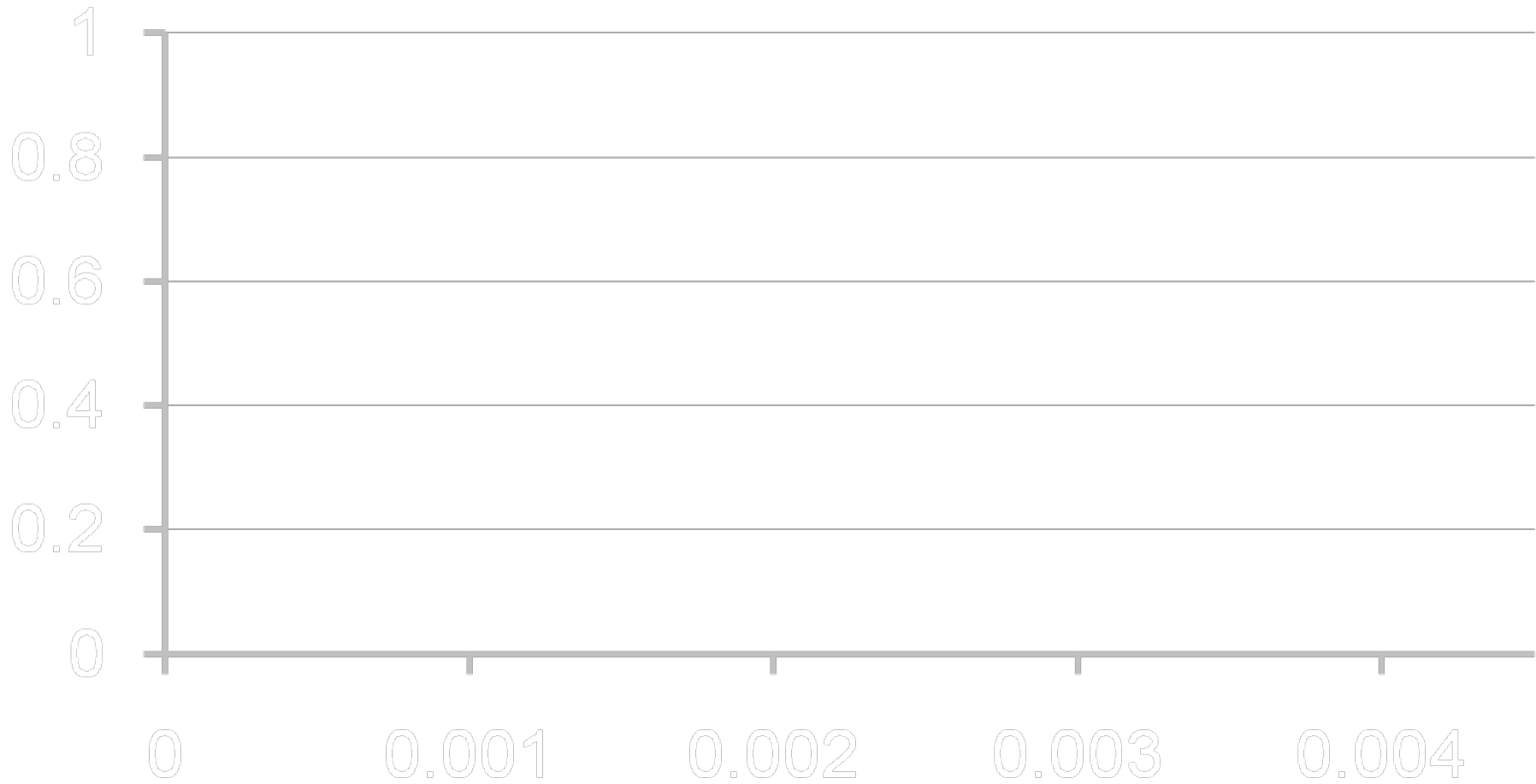
First bit is **“1”**
with **0.9 confidence**



- Assign to each bit the value that corresponds to a higher confidence

Experiment: Packet Delivery vs. Poor Coverage

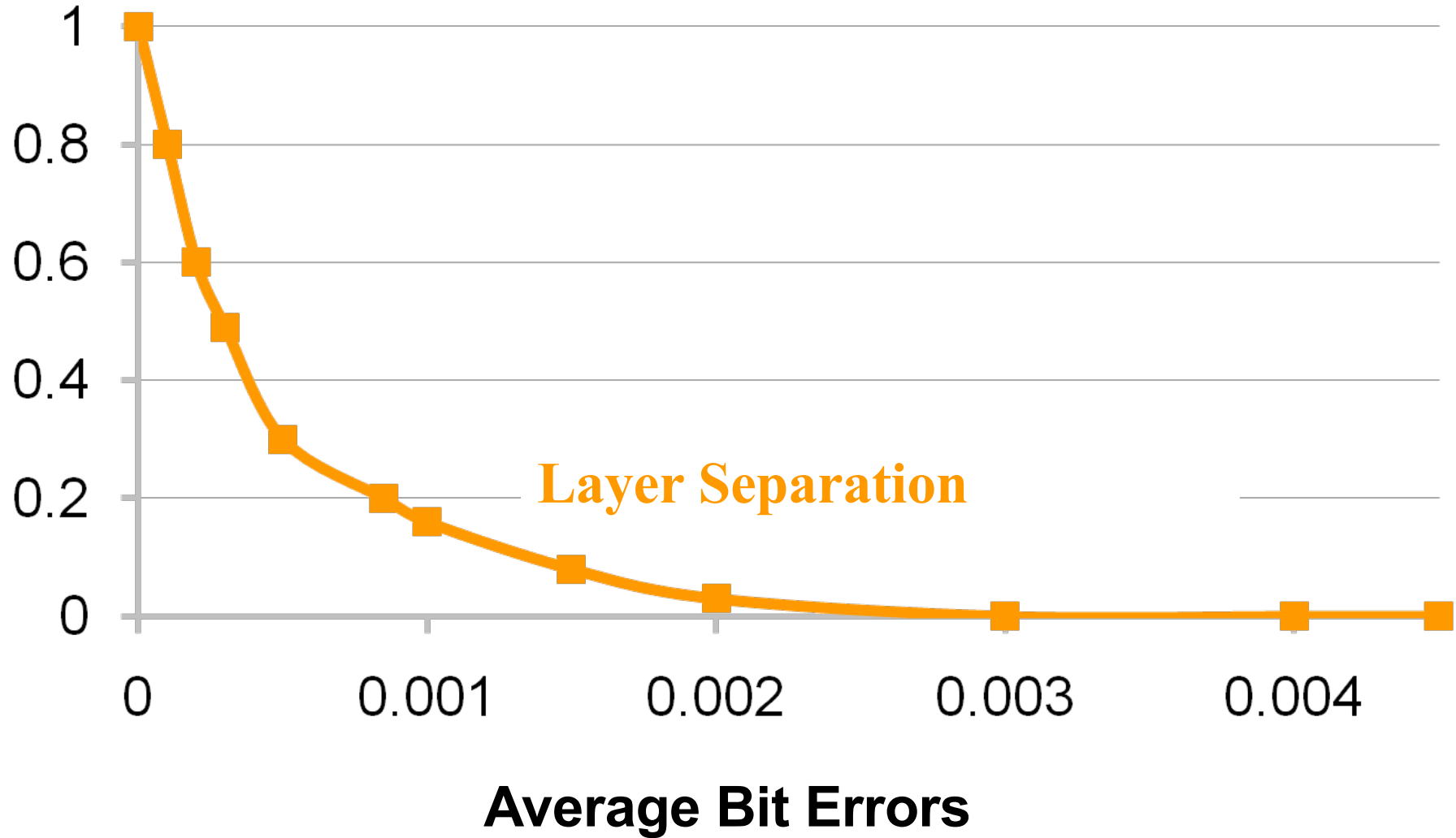
Fraction of Packets Delivered



Average Bit Errors

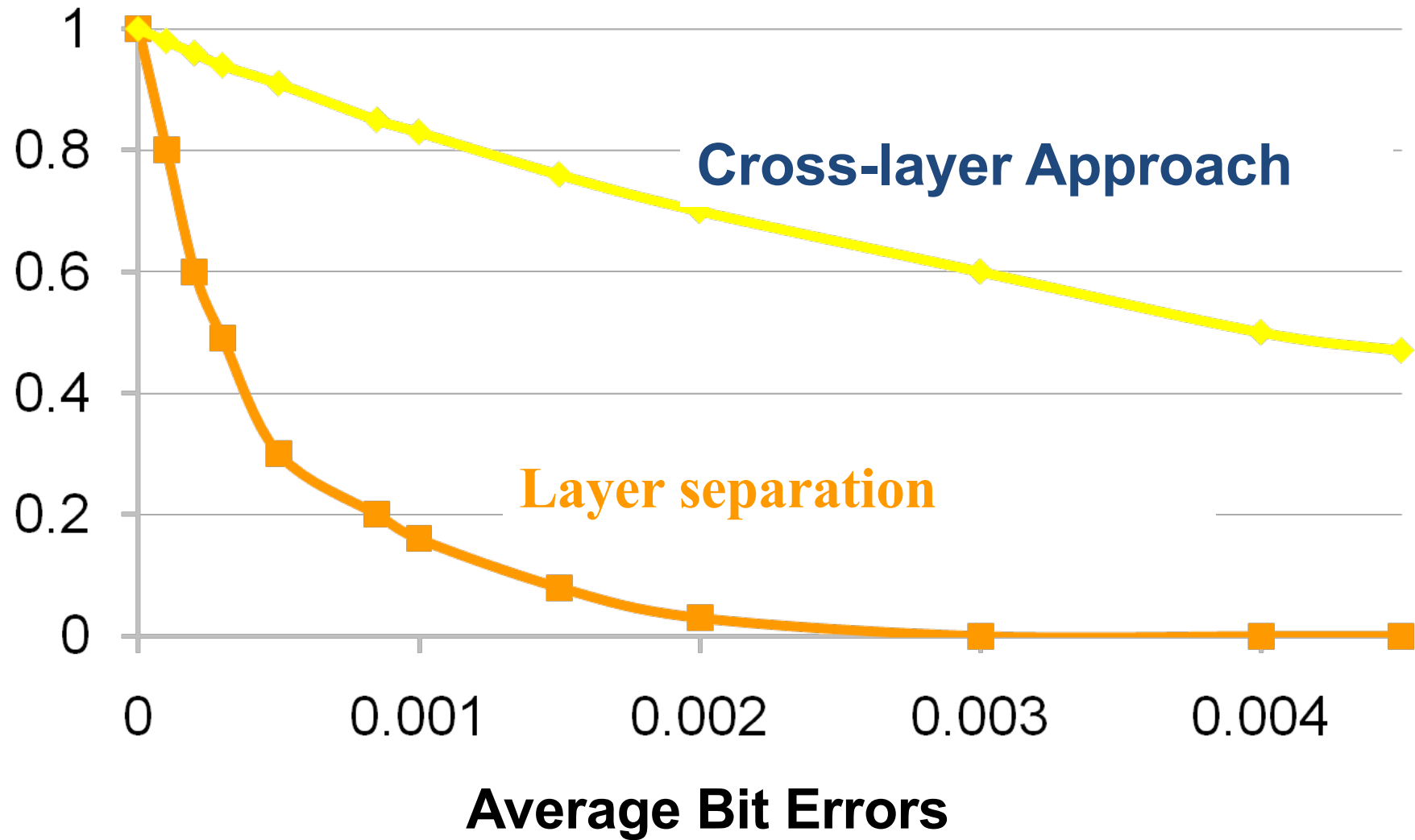
Experiment: Packet Delivery vs. Poor Coverage

Fraction of Packets Delivered



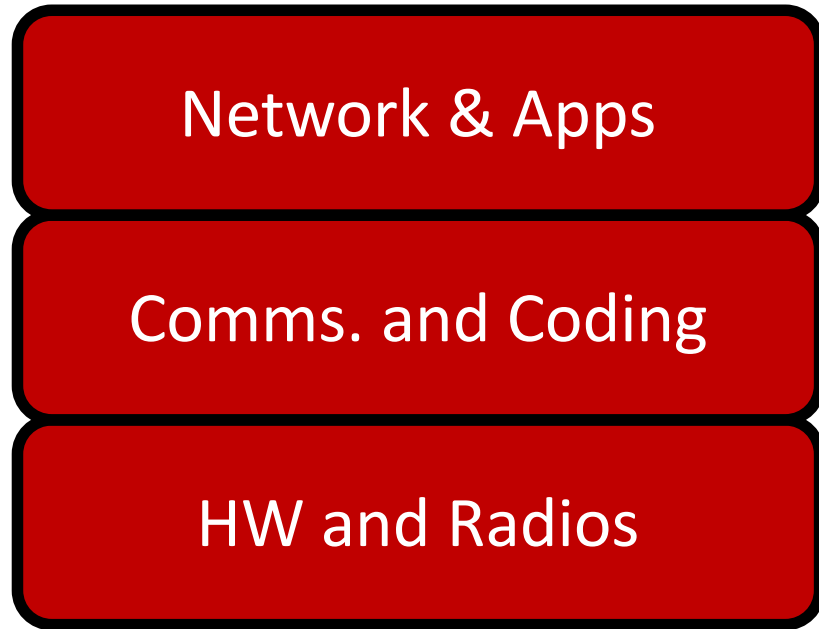
Experiment: Packet Delivery vs. Poor Coverage

Fraction of Packets Delivered



Traditional Approach

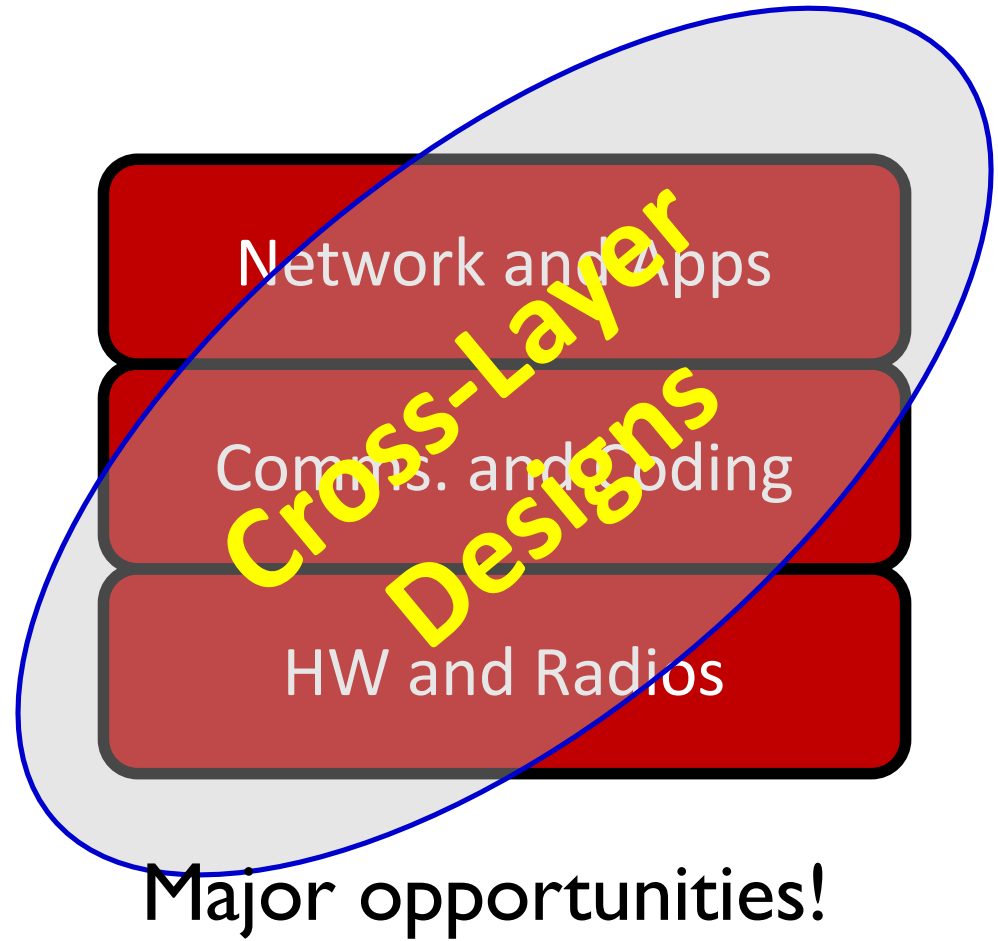
Optimize within isolated layers



Disruptive gains are unlikely

New Approach

Optimize across the layers



Fundamental Change in Network Architecture

New Services: Wireless Localization

GPS does not work indoor → Use WiFi to localize.



Indoor Navigation



Business Analytics



WiFi Geofencing



Indoor Robotic Navigation

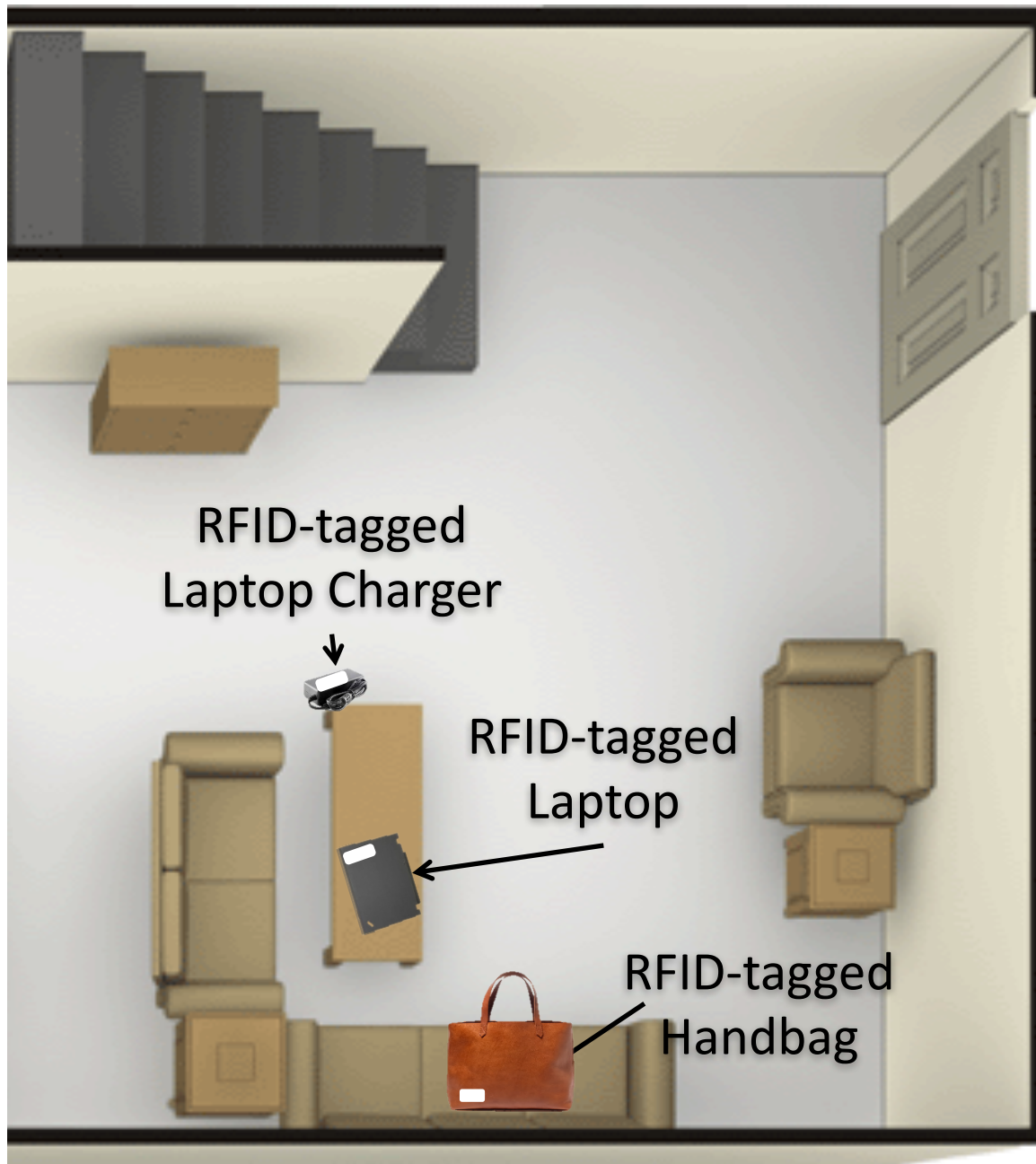
New Services: Wireless Localization

Localize Everything and Anything!



Battery-free stickers to tag any and every object

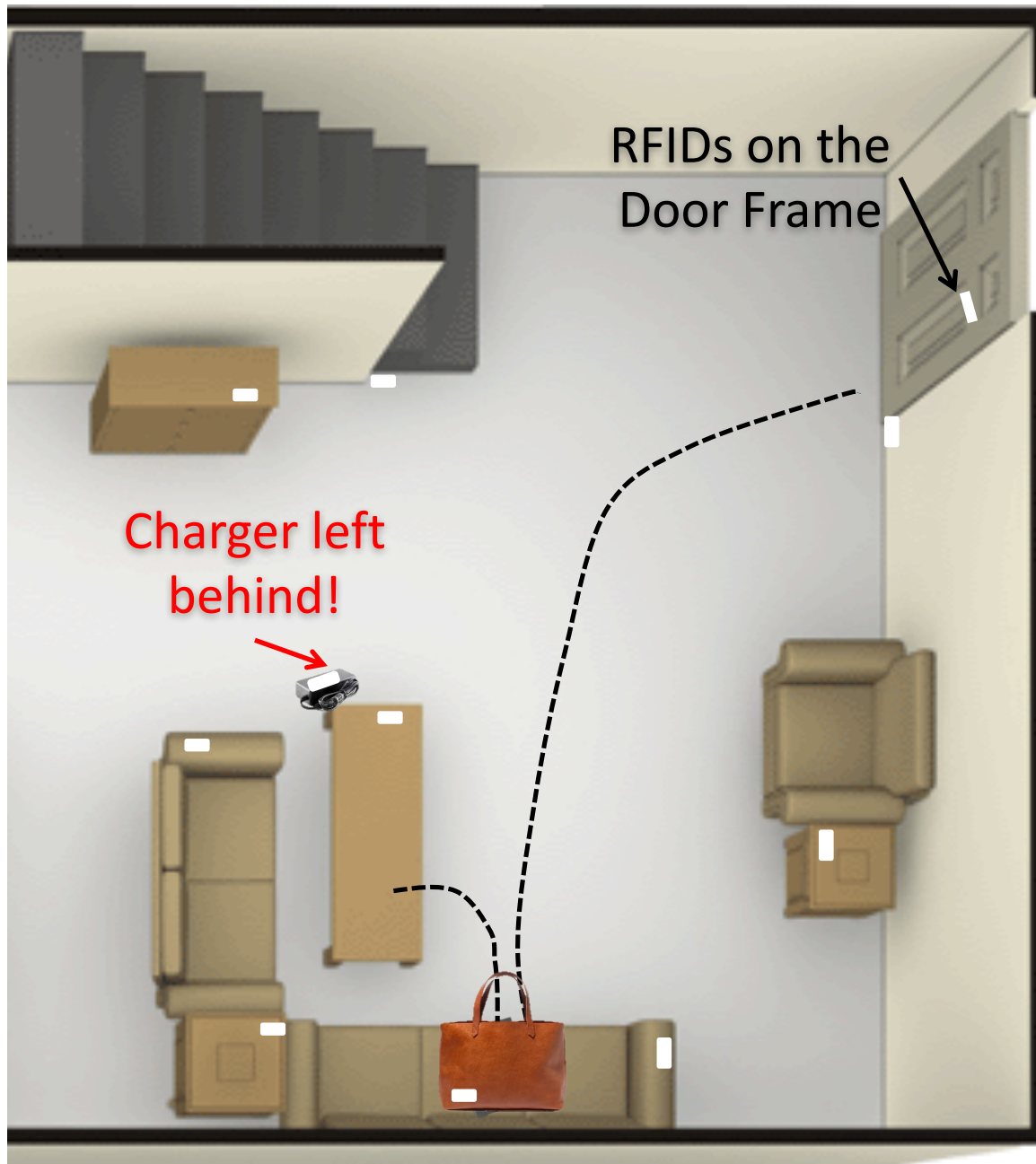
Smart Homes



Smart Homes



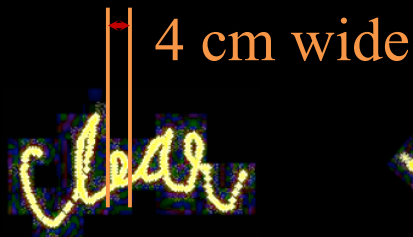
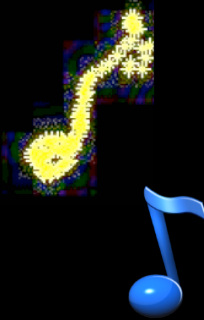
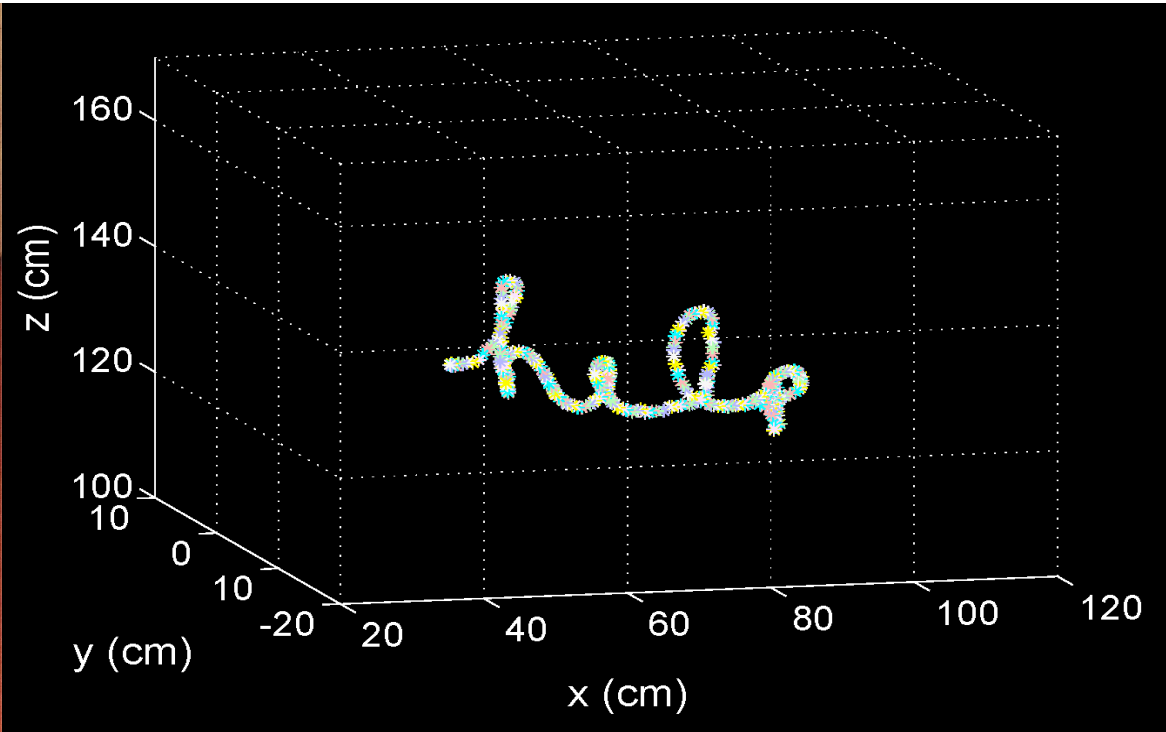
Smart Homes



How Do We Get Virtual Touch Screens?



How Do We Get Virtual Touch Screens?



"Clear"



"Jue"

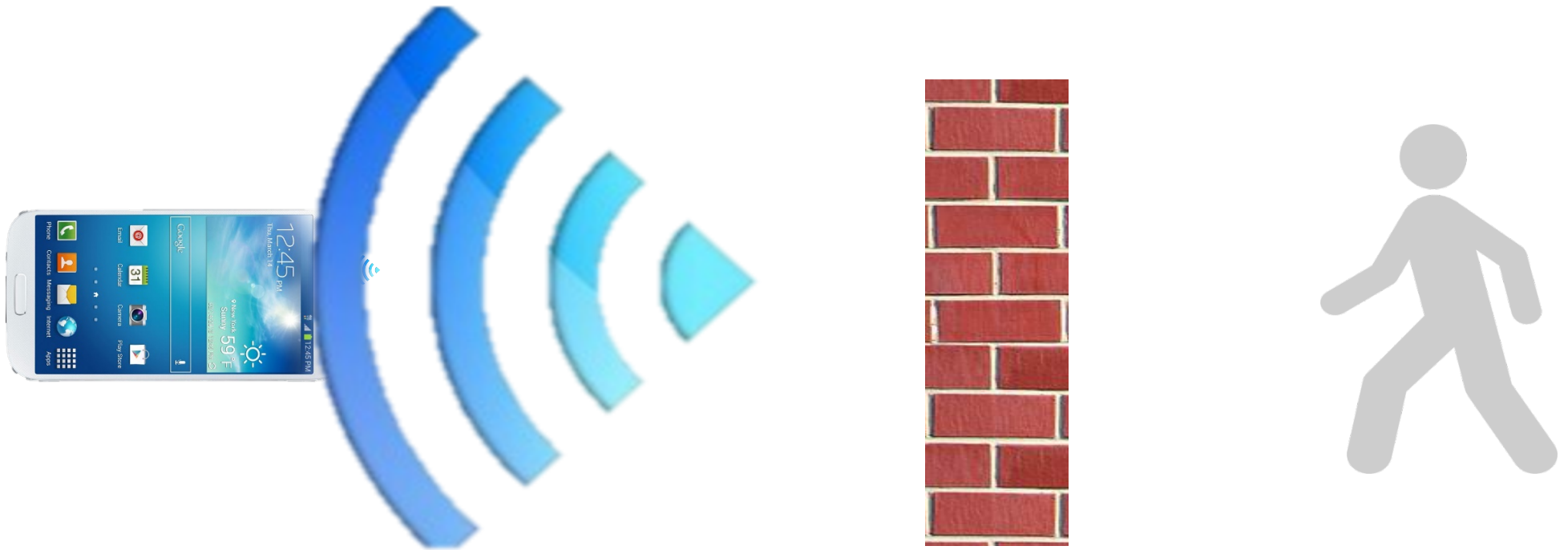
Can your cellphone give you X-ray vision?



See through-walls with WiFi

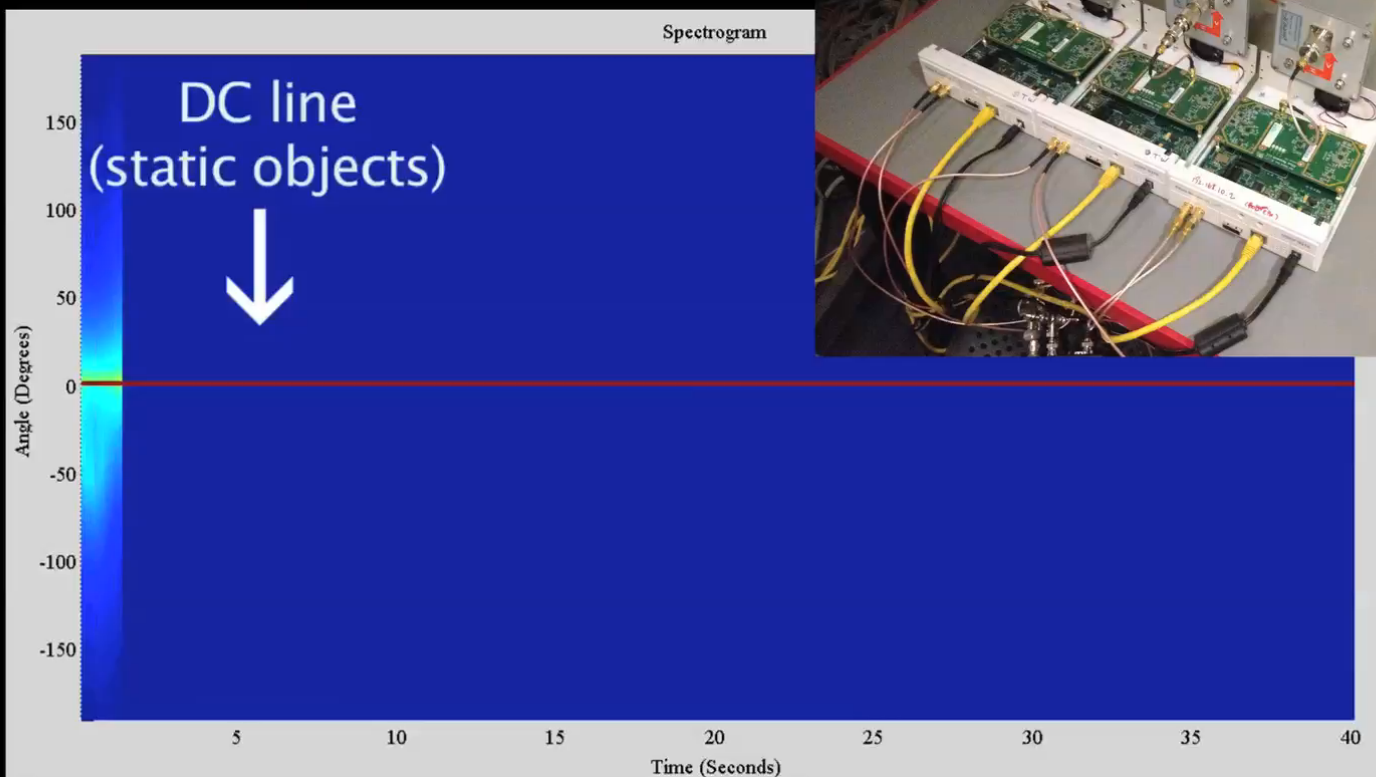
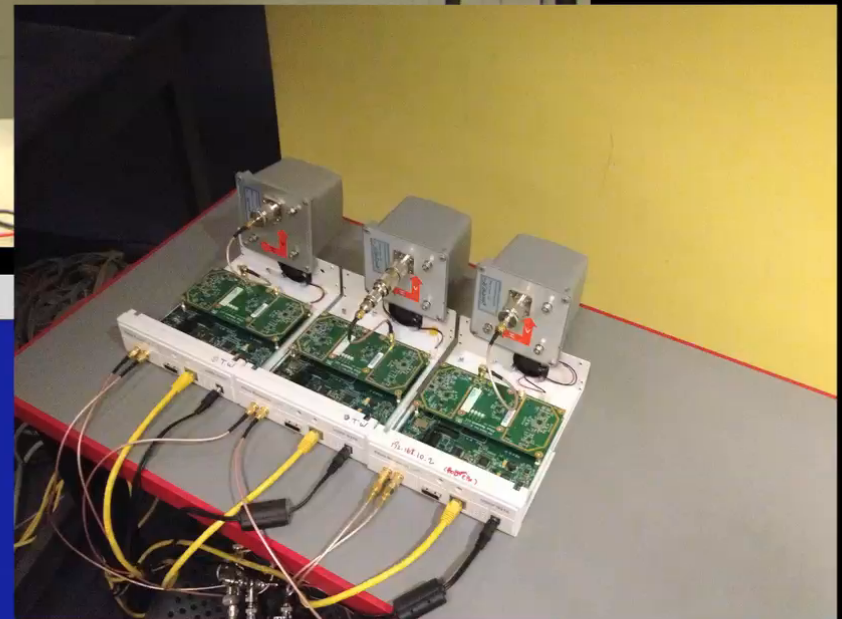


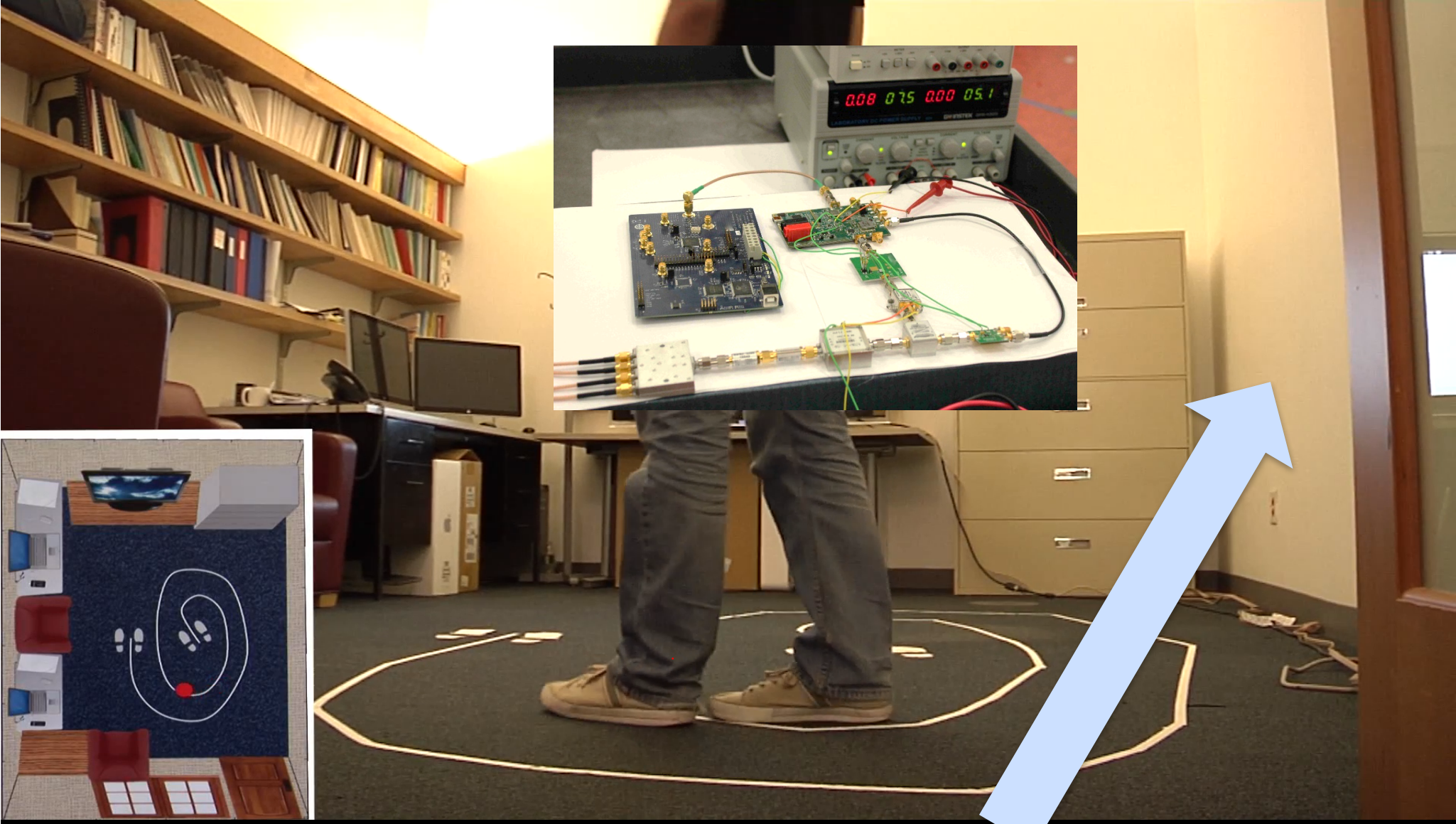
See through-walls with WiFi



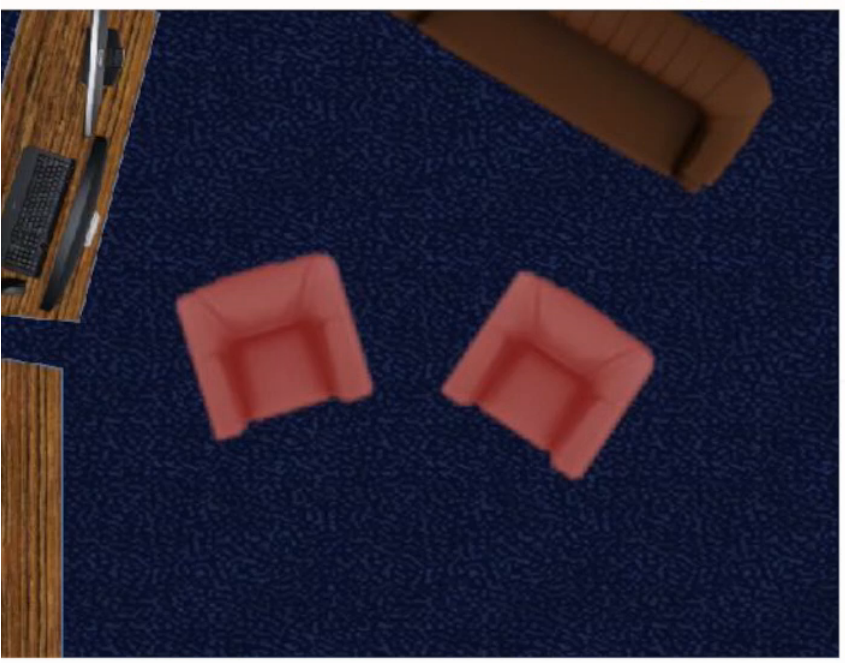
Wall reflection is 10,000x stronger than reflections coming from behind the wall

Solution: Use two transmit antennas and one receive antenna; the two transmitted waves cancel each other for static objects but not animated objects



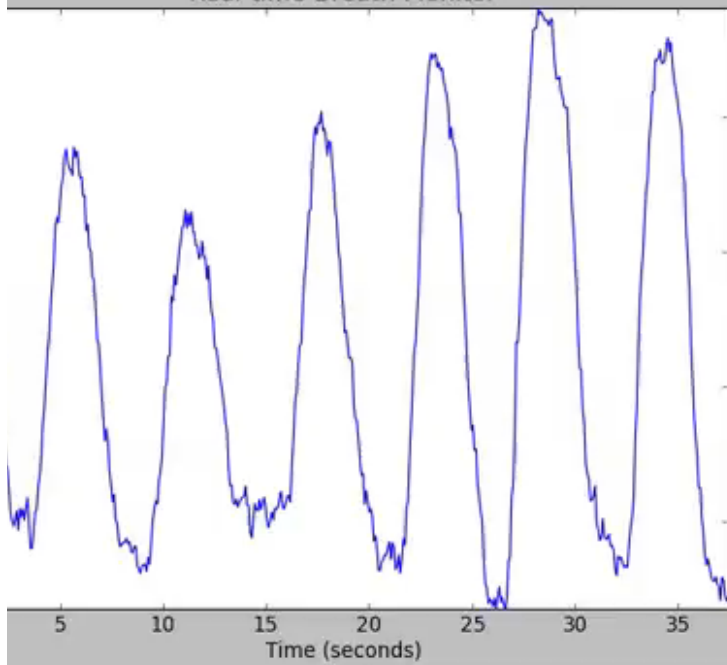


Wireless Device behind



e 1

Real-time Breath Monitor



Smart homes that monitor and adapt to our breathing and heart rates?

Personal Health



Baby Sleep



Elderly Health



Adapt Lighting and Music to Mood



Today: technologies for monitoring vital signs are cumbersome

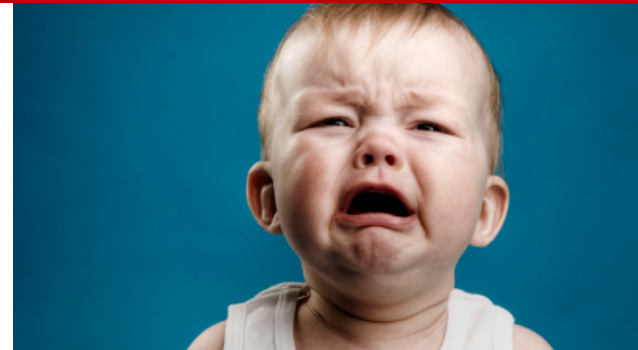
Breath Monitoring



Heart Rate Monitoring



Wireless enables contactless sensing: sense humans without any sensors on their bodies

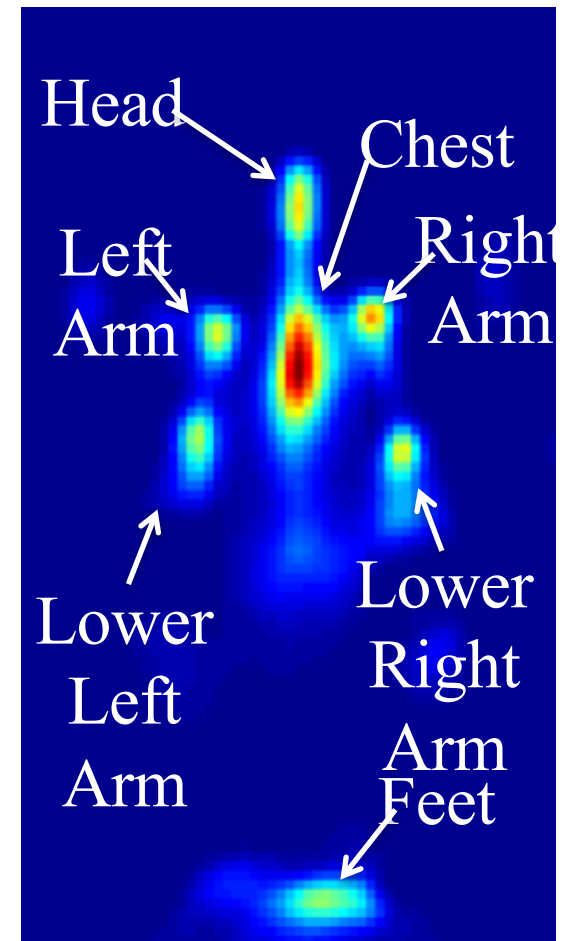
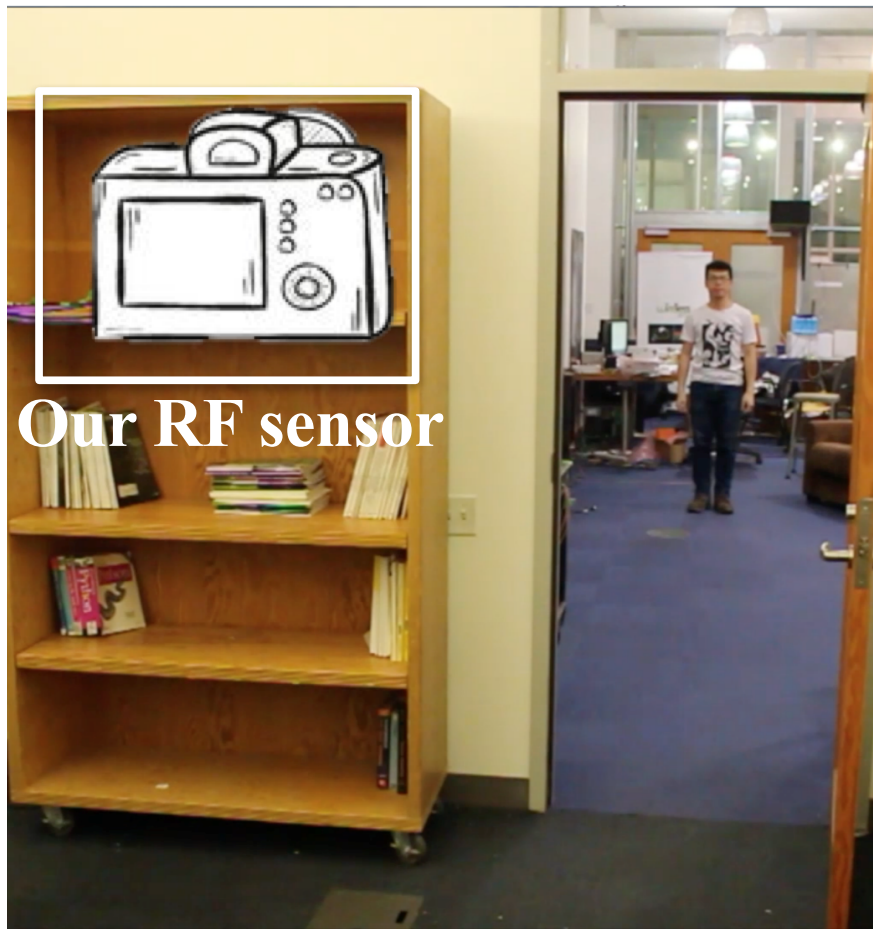


Baby Monitoring

2014-03-14 21:50:30



Imaging through occlusions using radio frequencies



Challenge: Don't get reflections from most points in RF

At frequencies that traverse walls, human body parts are specular (pure mirror)

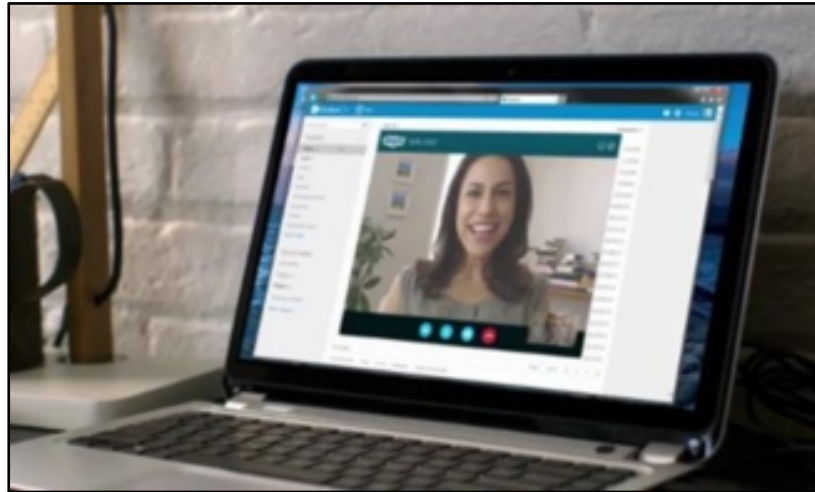


Human Walks toward Sensor

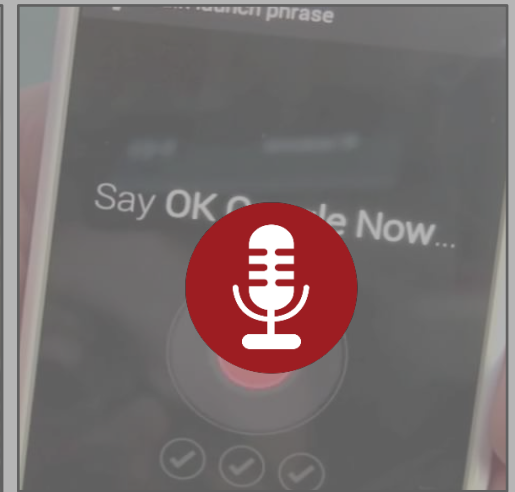
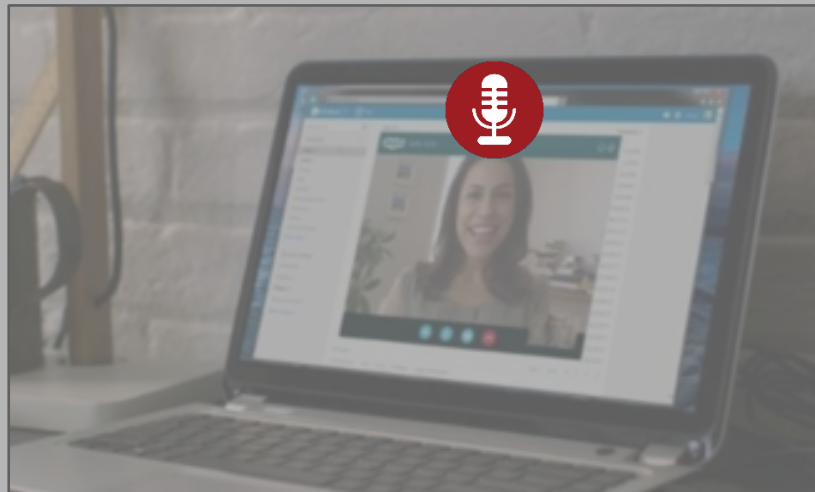


IoT Acoustic Security

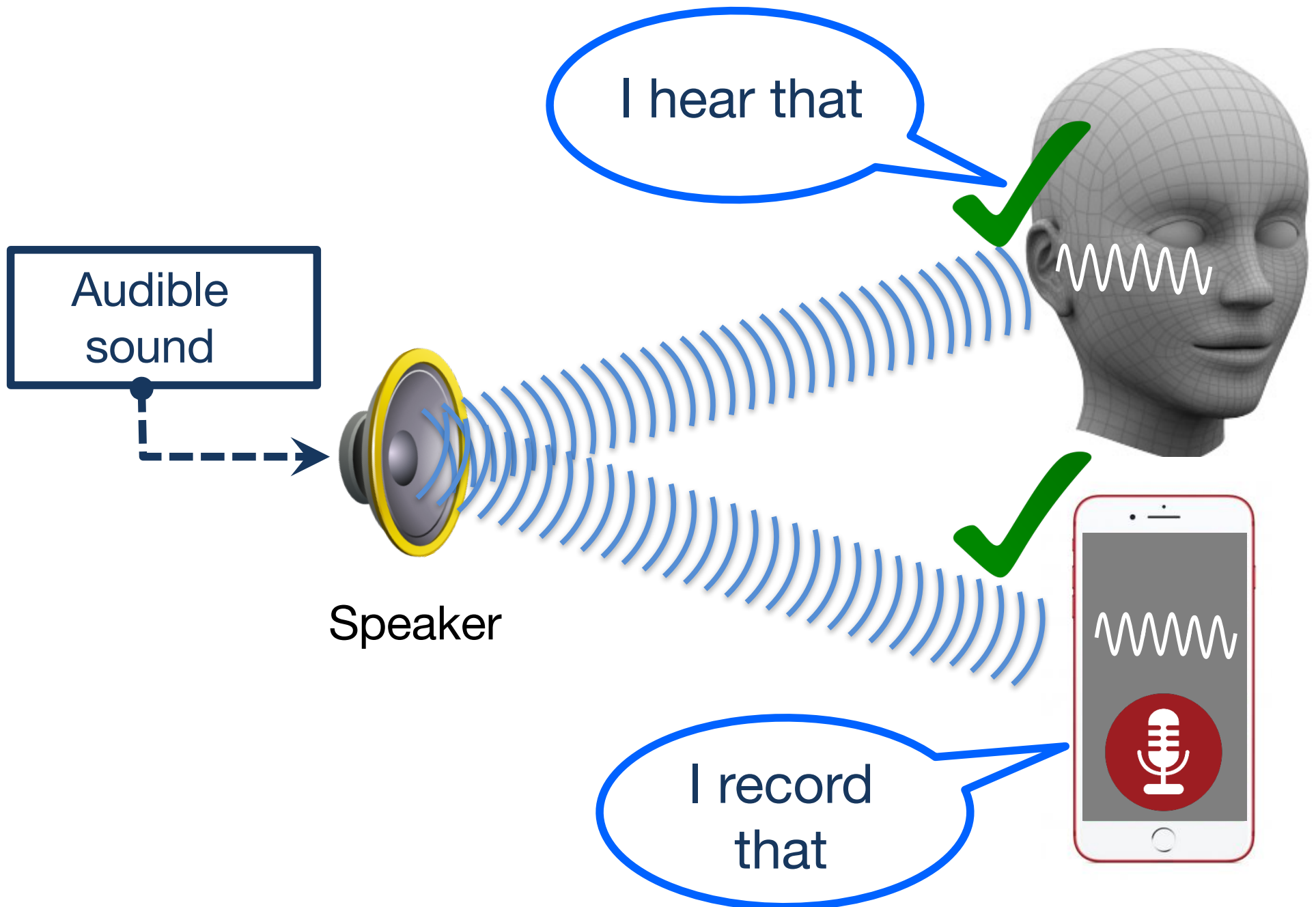
Microphones are everywhere



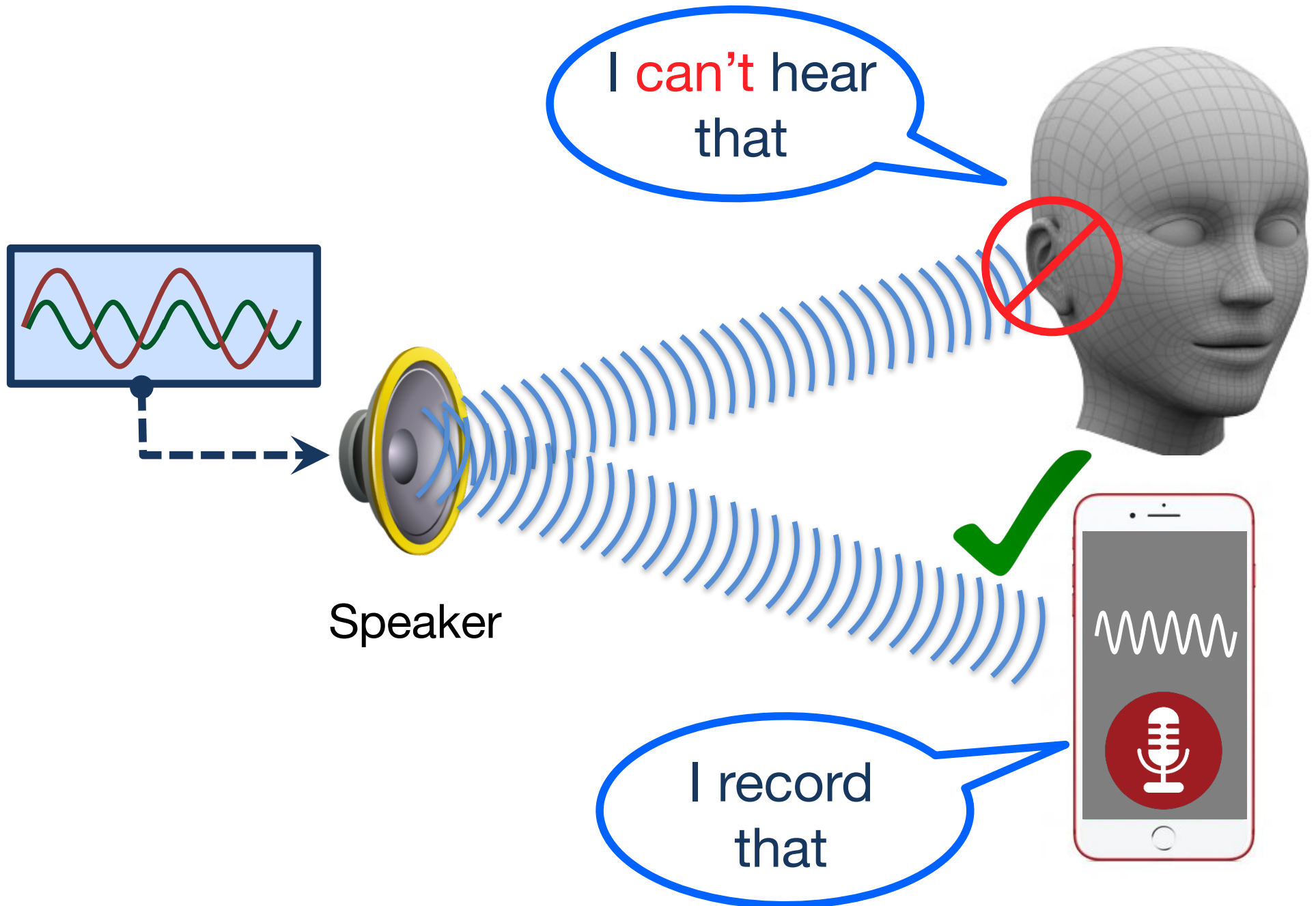
Microphones are everywhere

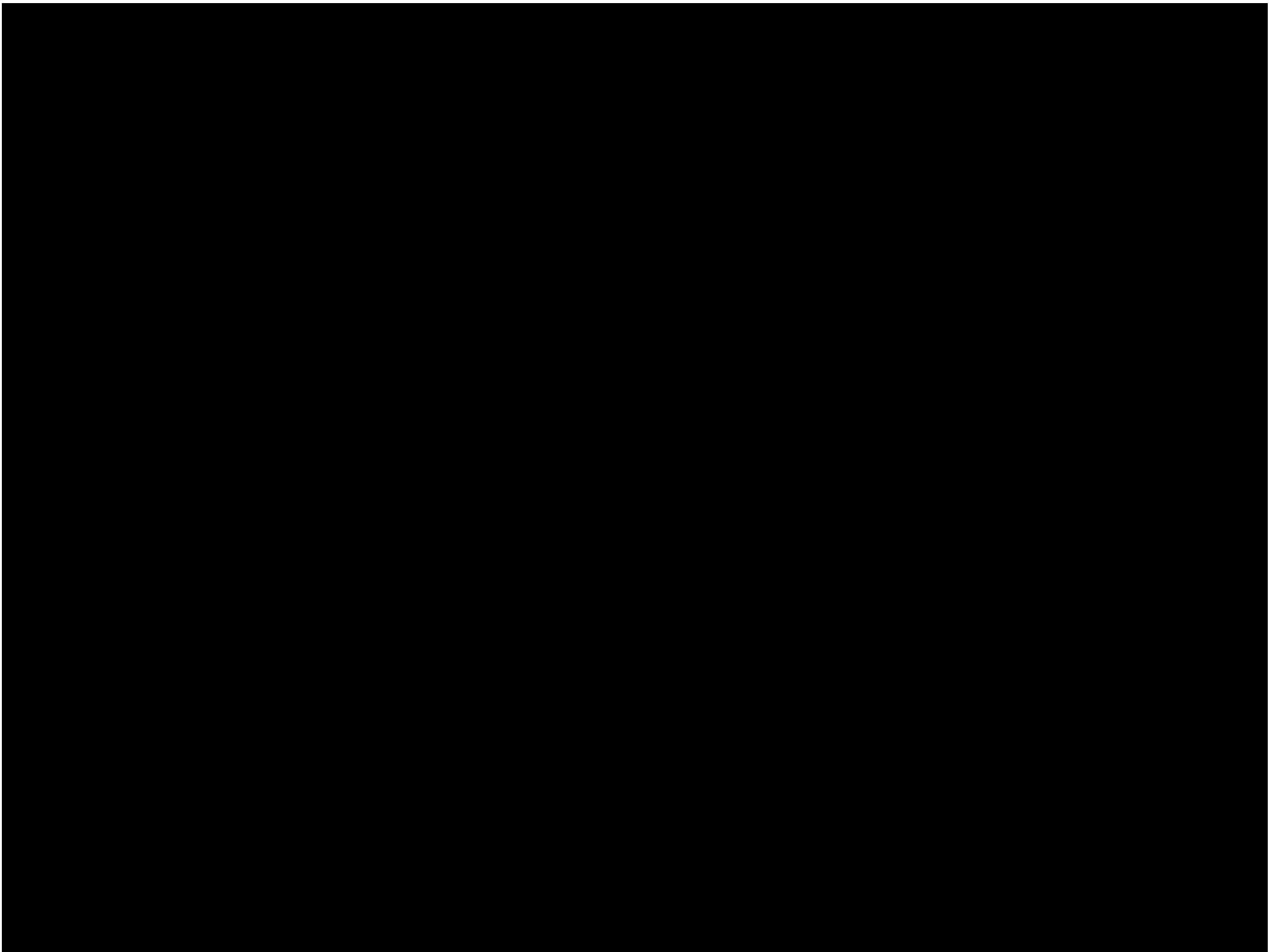


Microphones record audible sounds



Inaudible, but recordable !





Wireless Security

Medical implants and sensors are power limited

- ➔ Can't have strong cryptography
- ➔ Easy to eavesdrop on the signal, capture confidential data and hack devices.

RFIDs Are Used in Sensitive Applications



Access Control



Credit Cards



Passports



Pharmaceutical Drugs



Anti-Theft Car Immobilizers



Public Transportation

RFIDs Are Used in Sensitive Applications



Access Control
[SECRYPT'09, S&P'09
ESORICS'08, Usenix'08]



Credit Cards
[DefCon'13, ShmooCon'12,
DefCon'11 , Usenix'05]



Passports
[DefCon'12, HackaDay'12,
BlackHat'06]



Pharmaceutical Drugs
[CCS'09, RFID'06]



**Anti-Theft Car
Immobilizers**
[Usenix'12, Usenix'05]



Public Transportation
[Defcon'08, MIT'08, S&P'09]

Hacking RFIDs for Dummies



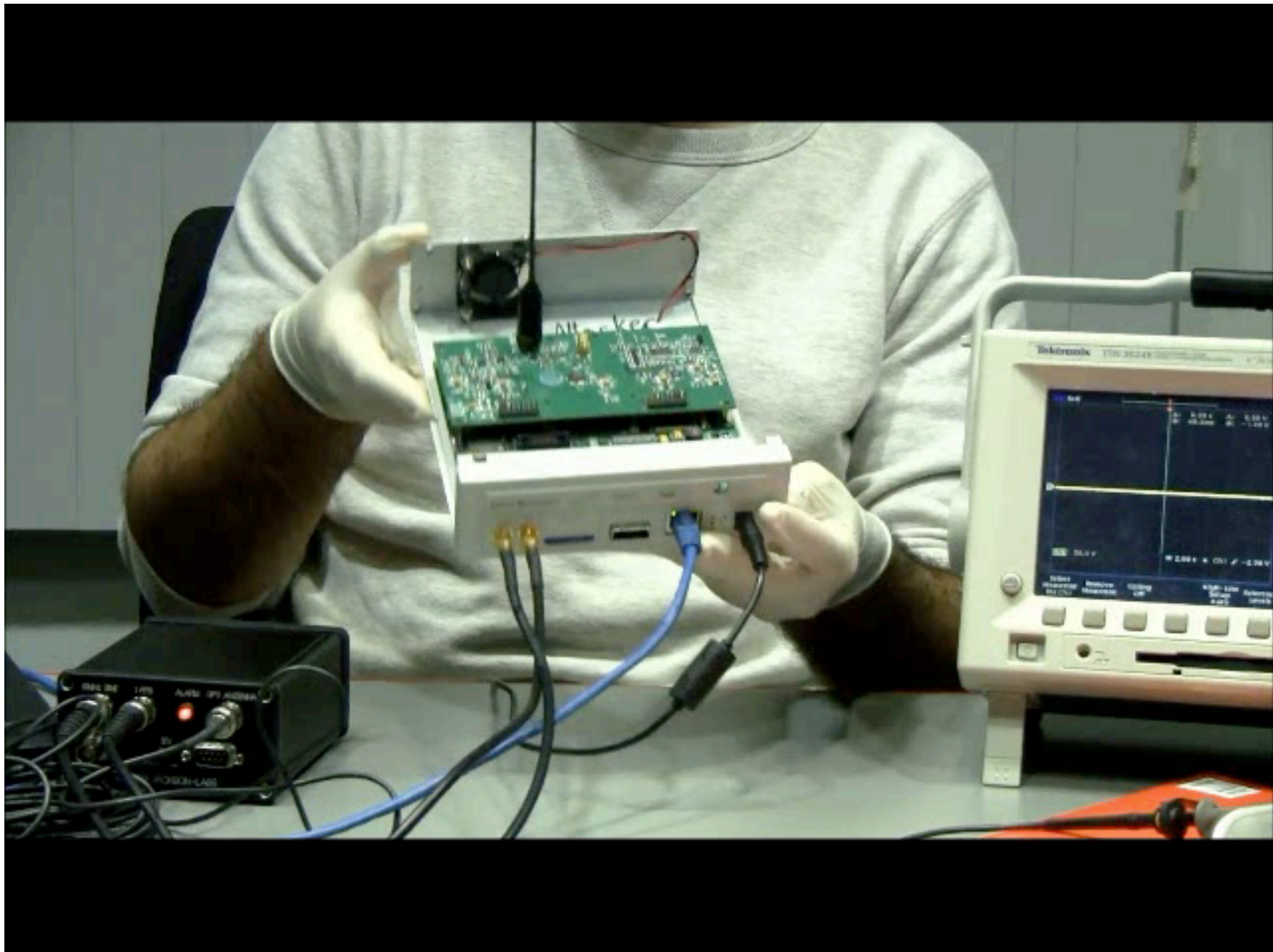
The screenshot shows a web browser window displaying a tutorial for the "Live RFID Hacking System" on the website www.openpcd.org/Live_RFID_Hacking_System. The page features a navigation bar with "Navigation", "Search", "Toolbox", "In other languages", and "Views". The main content area is titled "Live RFID Hacking System" and includes a sub-section "Bootable RFID Live Hacking System".

The article text includes:

- "The bootable Live RFID Hacking System contains a ready-to-use set of hacking tools for breaking and analyzing MIFARE Classic RFID cards and other well known card formats. It is built around PCSC-lite, the CCID free software driver and librfic that gives you access to some of the most common RFID readers. See our tutorial video for a quick introduction on how to break MIFARE Classic RFID card keys using our Live RFID Hacking System."
- A yellow callout box: "This RFID Live Hacking System is superseded by our OpenPCD 2 reader with librfic support - you can download the latest ISO image here. This page is only kept for historical reasons."
- "The MF0C/MF0UK tools of the Live system won't work inside virtualization software like VMware as virtualization seems to break the timing requirements of the MIFARE Classic attack tools - please boot from the CD/DVD instead."
- "Our RFID hardware projects for RFID Security Analysis" with links to "OpenPCD 2 RFID Reader for 13.56MHz", "OpenPICC RFID Emulator Project", and "OpenPICC SnifferOnly 13.56MHz".
- "Suggested RFID Reader for MIFARE Classic key recovery for this live system" with a note: "Please use the ACR122U102 Tikitag RFID reader for MIFARE key extraction (v1.02) - later versions or compatible models could work, but some later firmware revisions (ACR122U207) seem to be crash while breaking MIFARE Classic with mf0uk/mf0c. For normal use and known keys the other compatible readers should be fine though. Please send me a note if you successfully used another reader for key extraction using our Live CD. The firmware version is shown when using mf0c."
- "Note for touchatag reader users" with instructions: "If the pcsd daemon balls out on a touchatag reader with: 00000012 ccid_usb.c:901:ccid_check_firmware() Firmware (1.00) is bogus! Upgrade the reader firmware or get a new reader. 00000039 ifdhandler.c:101:IFDCreateChannelByName() failed 00000015 readerfactory.c:998:IFDInit122eReader() Open Port 200000 failed". It also says: "Just edit `/usr/local/openpcd/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist - IfDriverOptions` and set key from 0x0000 to 0x0005 to disable version checking."
- "Checksums" section with a code block:

```
Fedora-15-x86_64-Live-RFID-v02.iso
SHA256: 79373eef90ccbcf348d9a456356b7f22d07c9653d0df2d968fc44654db2d0e
MD5 : c8ef5ec1fcb012cd3b39f8c9e7579de
SHA1 : d854d9e89590c8a7668e2761806658957f51ae2
```
- "Tools Installed" section: "The most important tools are highlighted. The Fedora 15 based Live Dectop system runs Gnome 3 Desktop - just move your mouse cursor in the upper left corner to get a list of installed applications."
- "General Purpose Tools" section.

The right sidebar contains several video thumbnails with captions like "Breaking Mifare Classic using bootable Live DVD tutorial video - breaking derived keys with mf0c for two cards and comparing card using ktag" and "Shows the captured waveform with the demodulated LF RFID tag data using our LF RFID frontend for USB soundcards".



Physical Layer Security: Encryption on the Air

Encrypt using a random signal



Implant's
signal



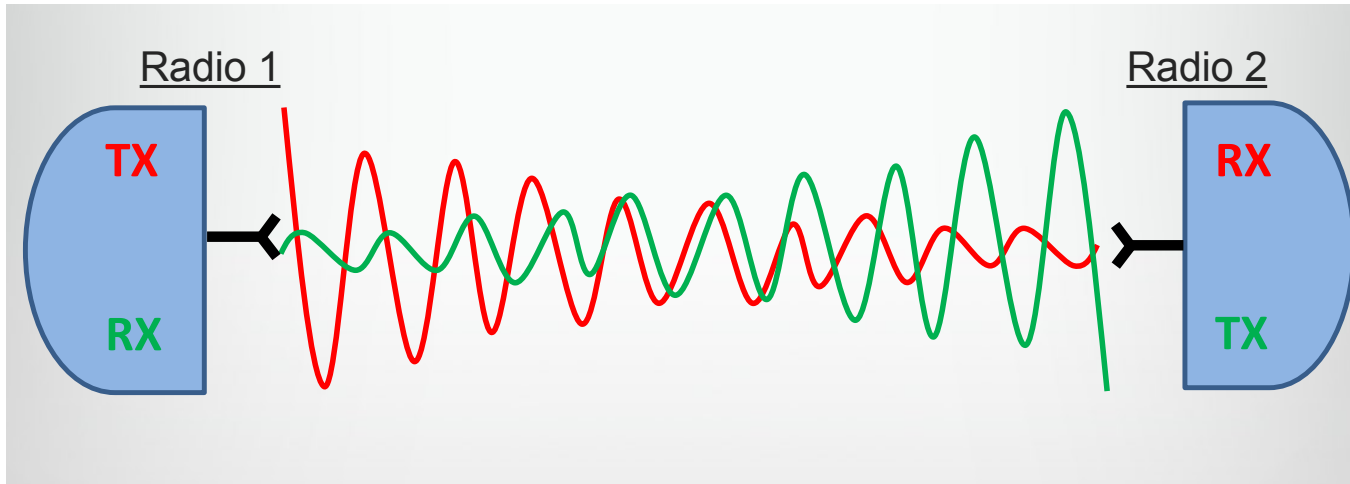
Random
Sum



Doesn't know jamming signal

Can secure medical devices even if they have no encryption or weak encryption

Today's Radios Are Half Duplex



Self Interference is hundred billion times 110dB+ stronger than the received signal!

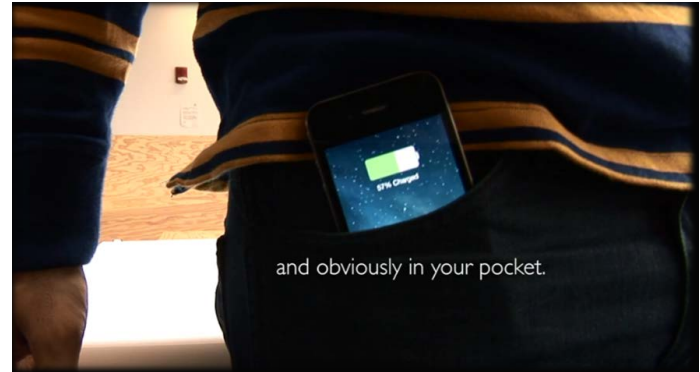
But we know the signal which we are transmitting!

→ Cancel the self-interference on the hardware

→ 1.97x increase in throughput

Full Duplex Radios: Major change in communication protocols

Wireless Charging



Other Topics Covered

Internet of Things

Acoustics



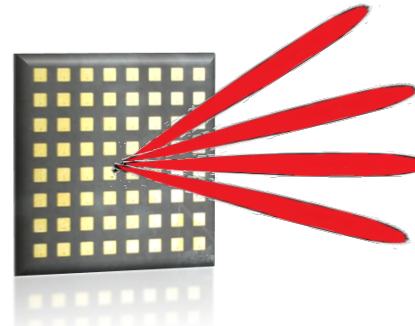
City Wide Networks



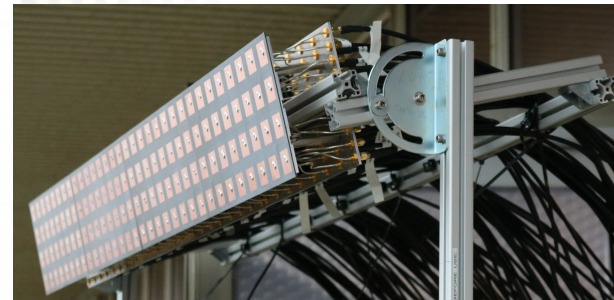
Drones



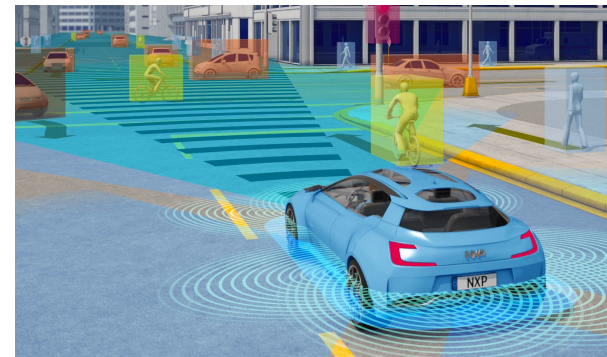
5G Networks



Millimeter Wave:
Wireless at Fiber
Optic Speeds



Massive
MIMO
Base stations



Autonomous
Vehicular
Networks