CS/ECE 439: Wireless Networking

Fall 2026

GRAINGER ENGINEERING

COMPUTER SCIENCE

Welcome!

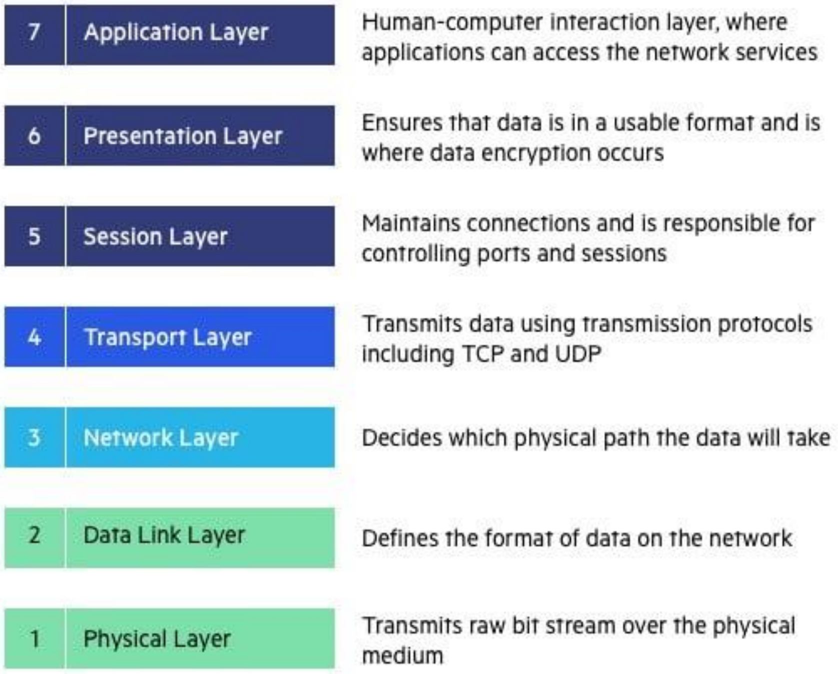
- Introduction
  - Who I am: Robin Kravets
  - What I have taught : CS 241, CS 438, CS 439, CS 538 and other grad networking courses
  - What I do: Wireless Networking and Mobile Computing research ➢ IoT!

- Who are you?
  - Grad/undergrad?
  - CS/ECE?
  - Taken CS 341 or ECE 391?
  - Taken CS/ECE 438?

- CS 439 TA
  - Max Han

What will we cover in this class?

- Wireless Networking …
  from the ground up
  - Wireless architecture
    - Physical layer
    - MAC layer
    - Transport layer
    - Mobility



What will we cover in this class?

- Wireless Networking … from the ground up
  - Wireless architecture
    - Physical layer
    - MAC layer
    - Transport layer
    - Mobility
  - For diverse technologies
    - Wi-Fi
    - Bluetooth
    - ZigBee
    - UWB
    - LoRa

What will we cover in this class?

- Wireless Networking …
  from the ground up
  - Wireless architecture
    - Physical layer
    - MAC layer
    - Transport layer
    - Mobility
  - For diverse technologies
    - Wi-Fi
    - Bluetooth
    - ZigBee
    - UWB
    - LoRa
  - In diverse environments
    - Mobile-to-mobile networks
    - Ad hoc networks
    - Sensor networks
    - Mesh networks
    - Internet of Things
  - Supporting diverse applications
    - No one-size-fits-all solution

What will you get out of this course?

- Learn about the unique challenges in wireless networking
  - Starting point is "regular" wired networks
- Gain an understanding of wireless technologies at the physical, MAC, and higher layers
  - Focus is on wireless protocols
- Get experience in working with wireless networks
  - Implementing protocols, algorithms
  - Measurements of wireless networks
- Get a broad view of the the state of the art and ongoing research in the wireless domain
  - Read and present hot topics and leading edge research papers

Course Contents

- Class participation 10%
  - You only get out of this class what you put into it!
- Class Attendance During Student Presentations 10%
- Class HW 10%
- Presentation of advanced topic 20%
  - In class presentation (20-30 min)
  - Summary of presentation topic
  - Attendance and participation required for group presentations
- Project: team-based, hands-on 45%
  - In-depth study and implementation of a particular problem
- Project Presentation 5%

Projects

- In-depth study of a particular use of wireless networks
  - Performance evaluation studies, protocol modifications, applications, measurements, ..
  - Must be wireless, but otherwise flexible
- Strongly prefer hands on projects
  - Real world is quite different from simulation and analysis
- Must carefully consider platform options
  - Real-world experiments
  - Simulator based
  - Emulator
  - Or could compare results in different environments

Class Project

- Considerations
  - Concrete outcomes
  - Learn something
- You should have the necessary background to complete the project
  - Do not attempt a project at the physical layer if your only background in this area is just the few lectures in this course.
  - Do not attempt a project that involves kernel or driver hacking if you have limited programming experience.
- The project needs to be feasible
  - Must be reasonable given the time available
  - Access to the necessary infrastructure
- Build a team with diverse skills to cover theoretical and practical topics

Project Timeline and Deliverables

- Team
  - Members 1 or 2
  - 3 person teams are rarely allowed and require prior permission
- Project Proposal
  - Plan, references
- Extended Project Proposal
  - Progress so far
  - ~5 pages plus extended references. Initial demos
- Status Report
  - Concrete demos and initial results
- Final Report
- Finals Week
  - Project presentations during finals week + demo video
  - Project Evaluations

4 Credit Students

- Students taking this class for 4 credits have two options. Please discuss with the professor and inform them of your choice.
  - If all team members are taking the class for 4 credits, the project can be increased in scope.
    - This must be approved by the professor during team meetings.
  - Otherwise, each student can submit a 10-page survey paper on an approved topic due the last day of class.

Presentation topics

- For each topic
  - Introduce advanced topics
  - Current technology and research in wireless networking
- Topic Teams = Project Teams
  - Based on a small set of papers or articles
  - Summarize the state of the art or current research
  - Apply critical thinking on the applicability and effectiveness of current proposals
  - Compare different solutions
  - Identify interesting future work
- Presentation in class
  - 20 – 30 min
  - Meet with me at least 7 days prior to presentation (mandatory)

Class Presentation

- When would this help me?
  - You are working for a company that is exploring a new wireless technology or market
  - You are asked to prepare a 30 minute presentation to introduce to new area
  - You are writing your first paper on a research project you just finished
  - You need to write a short related work section that includes a survey of existing work in the areas relevant to your research

Academic Honesty

- Your work in this class **must** be your own.
- If students are found to have cheated (e.g., by copying or sharing code for a project or copying any written text from existing material), **all** involved will at a minimum receive grades of 0 for the first infraction.
- If students are found to have use AI for their written material, no credit will be given.
  - AI tools are allowed for the class project
- Further infractions will result in failure in the course and/or recommendation for dismissal from the university.

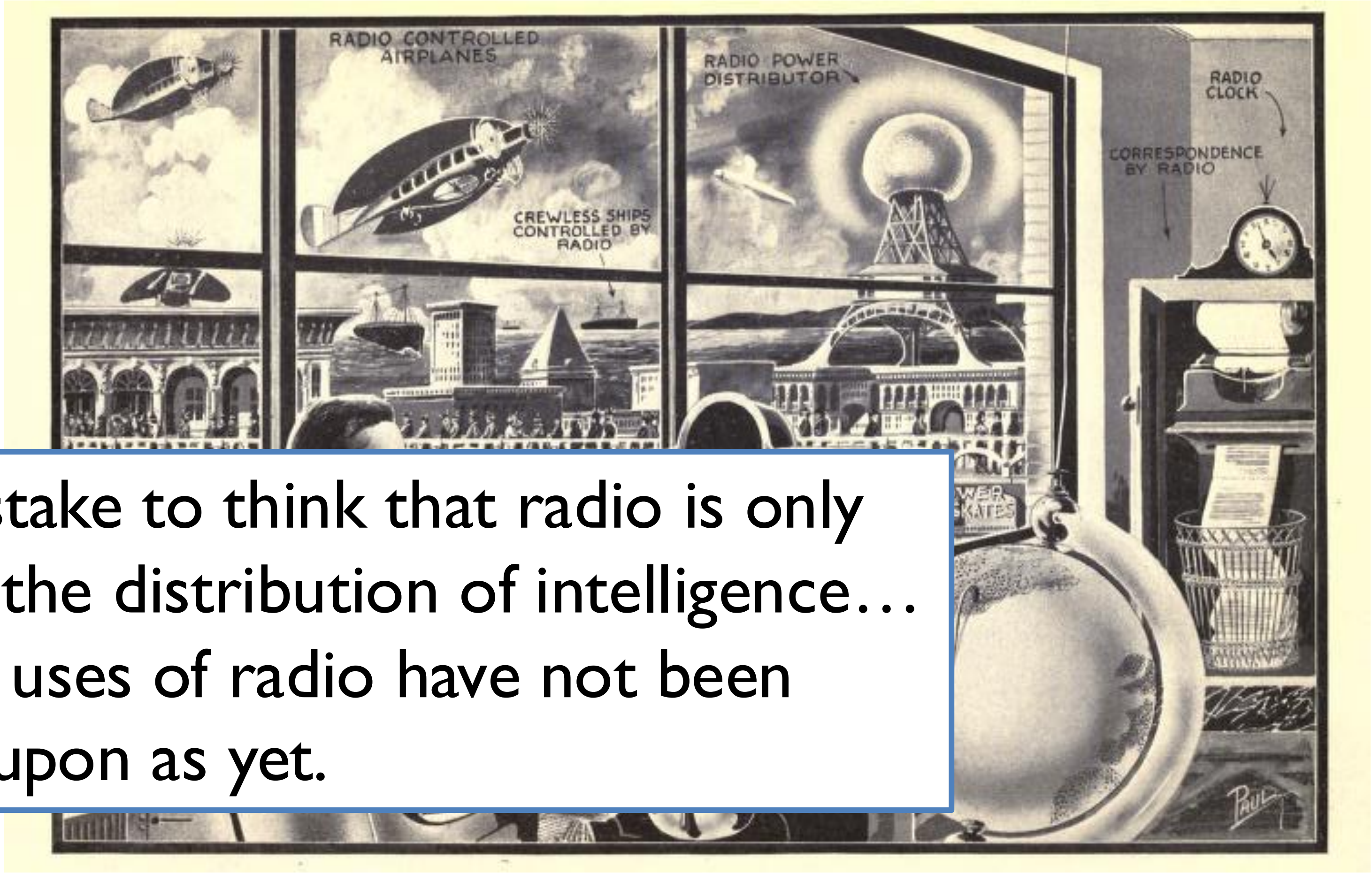
Course Material

- Final slides were prepared by the course instructor
- Some slides contain material from other sources
  - Slides from related courses
    - Special thanks to Nitin Vaidya and Romit Roy Choudhury (UIUC) and Peter Steenkiste (CMU) and Haitham Hassanieh (UIUC/EPFL)
  - Some figures are taken from textbooks
  - Some lectures contain material from research presentations prepared by the authors

Wireless Technology

A glimpse of the future

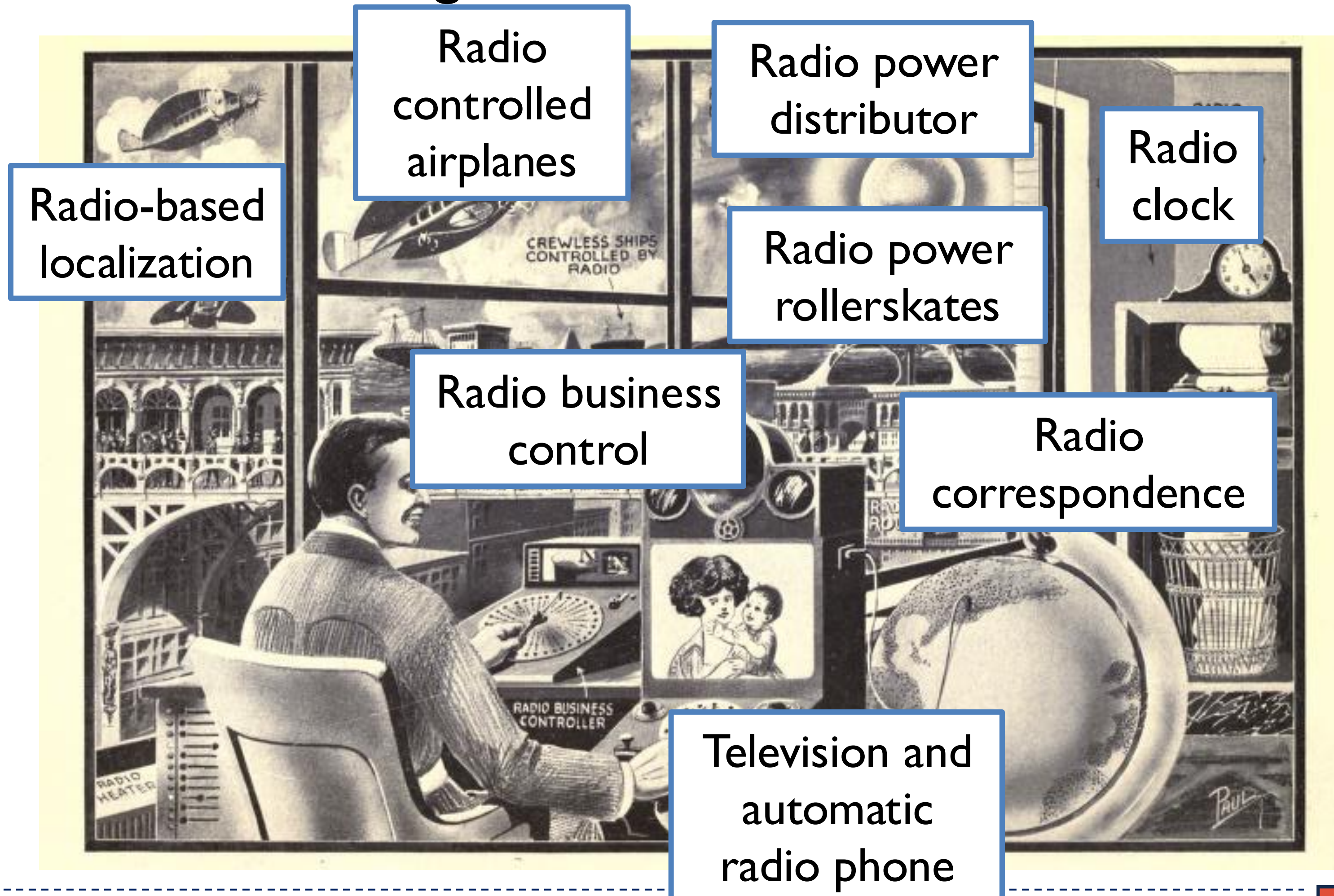
- 1922: "Radio for All", Hugo Gernsback



It is a mistake to think that radio is only good for the distribution of intelligence… the great uses of radio have not been touched upon as yet.

A glimpse of the future

- 1922: "Radio for All", Hugo Gernsback

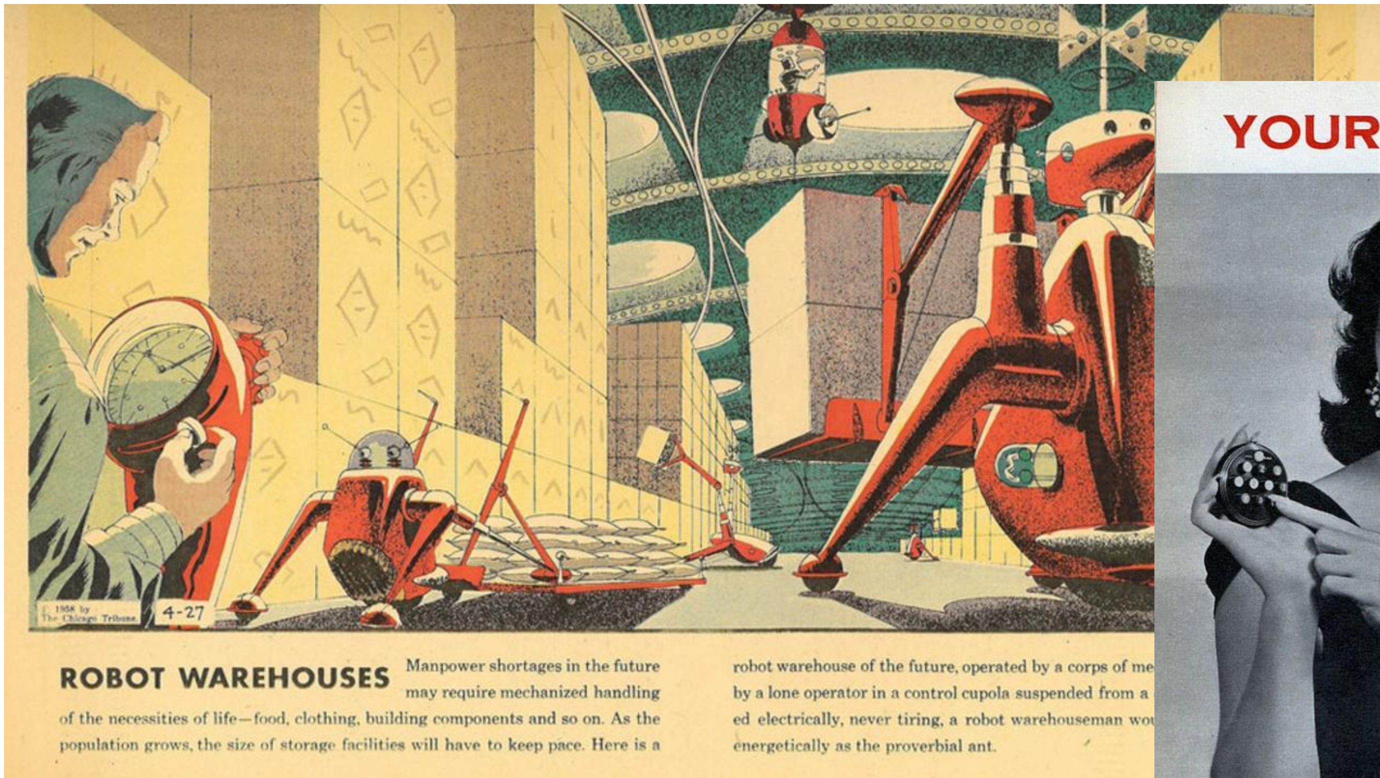


A glimpse of the future

- 1931
  - Erich Kästner's children's book: The 35th of May, or Conrad's Ride to the South Seas
  - "a science fiction nightmare city with mobile phones and moving walkways"

> "A gentleman who rode along the sidewalk in front of them, suddenly stepped off the conveyor belt, pulled a phone from his coat pocket, spoke a number into it and shouted: "Gertrude, listen, I'll be an hour late for lunch because I want to go to the laboratory. Goodbye, sweetheart!" Then he put his pocket phone away again, stepped back on the conveyor belt, started reading a book..."

A glimpse of the future



1950s

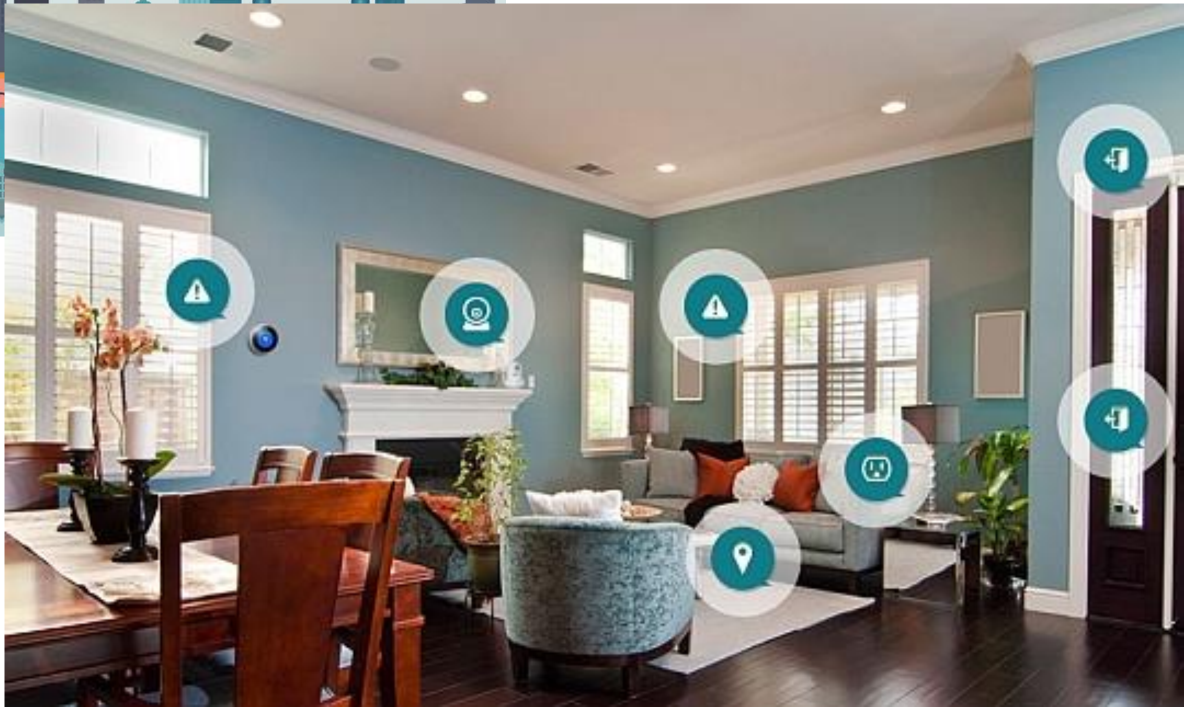
A glimpse of the future

Smart Cities

Smart Homes

The Dream

Smart Cities



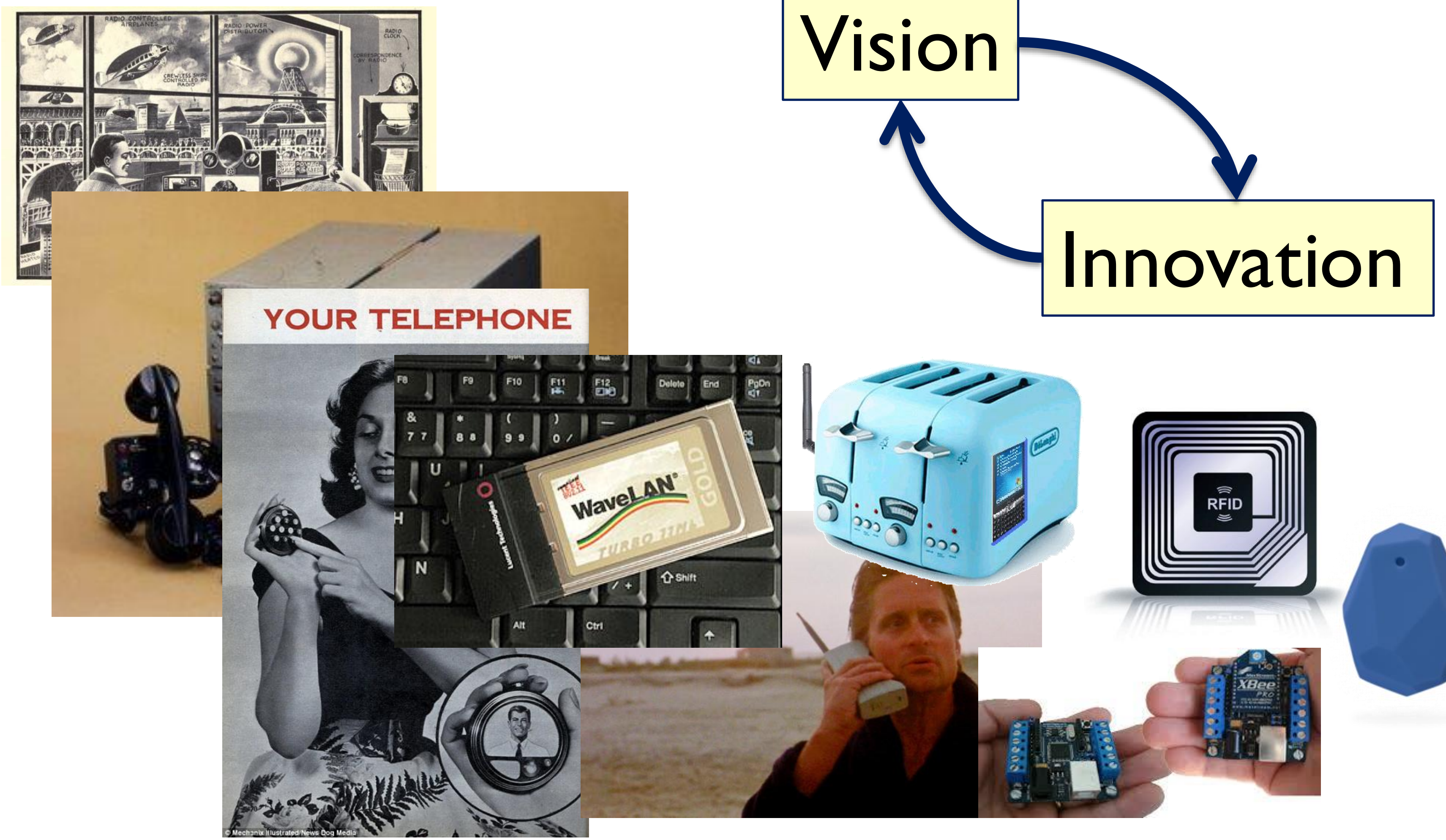
Smart Homes

Are we there yet and why is it taking so long?

The Road to Ubiquitous Wireless Access

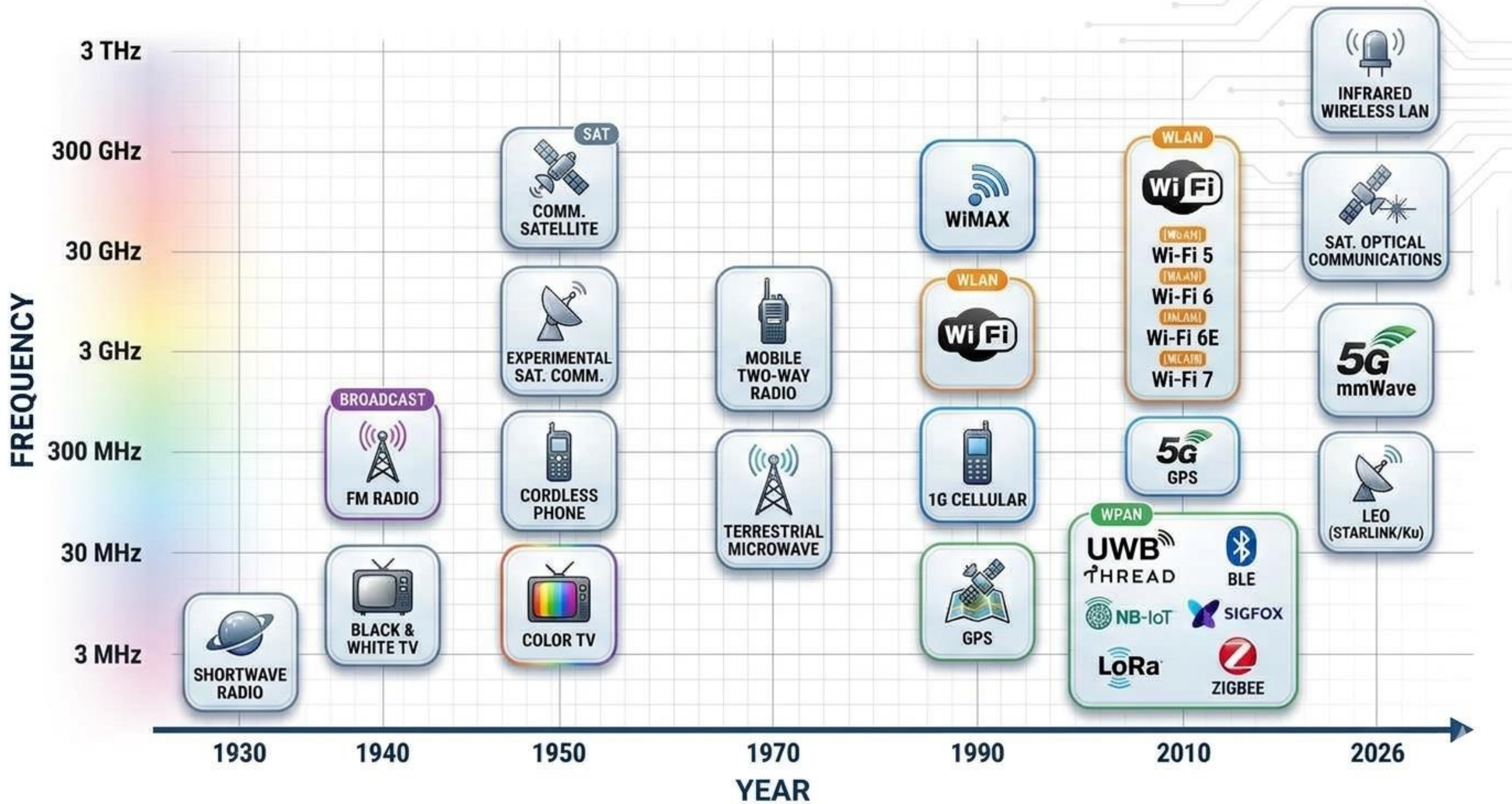
Vision

Innovation



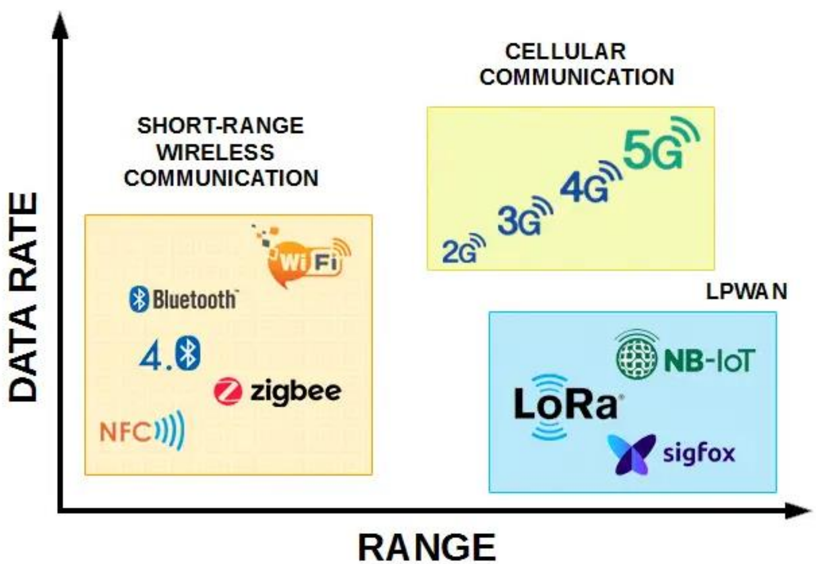
A Broad Spectrum of Wireless Technologies

You pick the best one …



Diversity is king

- Diverse application requirements
  - Energy consumption
  - Range
  - Bandwidth
  - Mobility
  - Cost

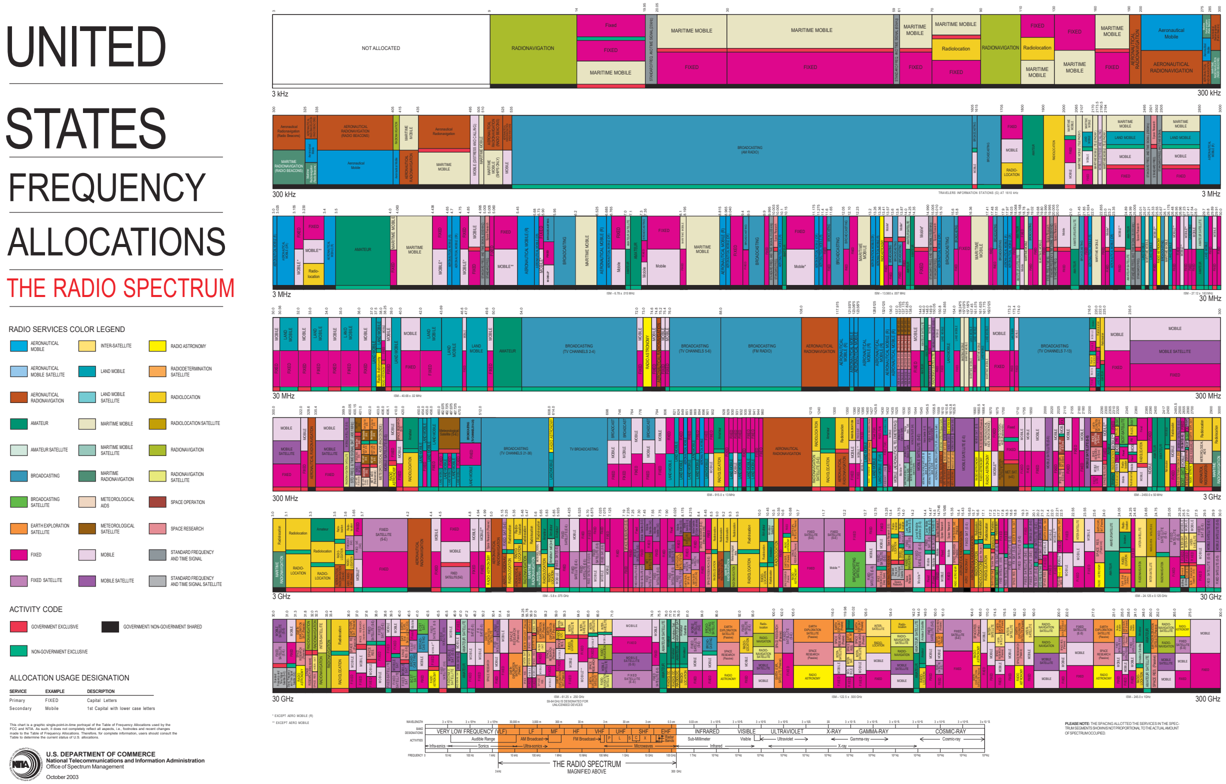


- Diverse deployments
  - Licensed vs. unlicensed
  - Provisioned vs. unprovisioned
- Diverse characteristics
  - Signal penetration
  - Frequency use
  - Cost
  - Market size
  - Age, integration

You pick the best one …

Range

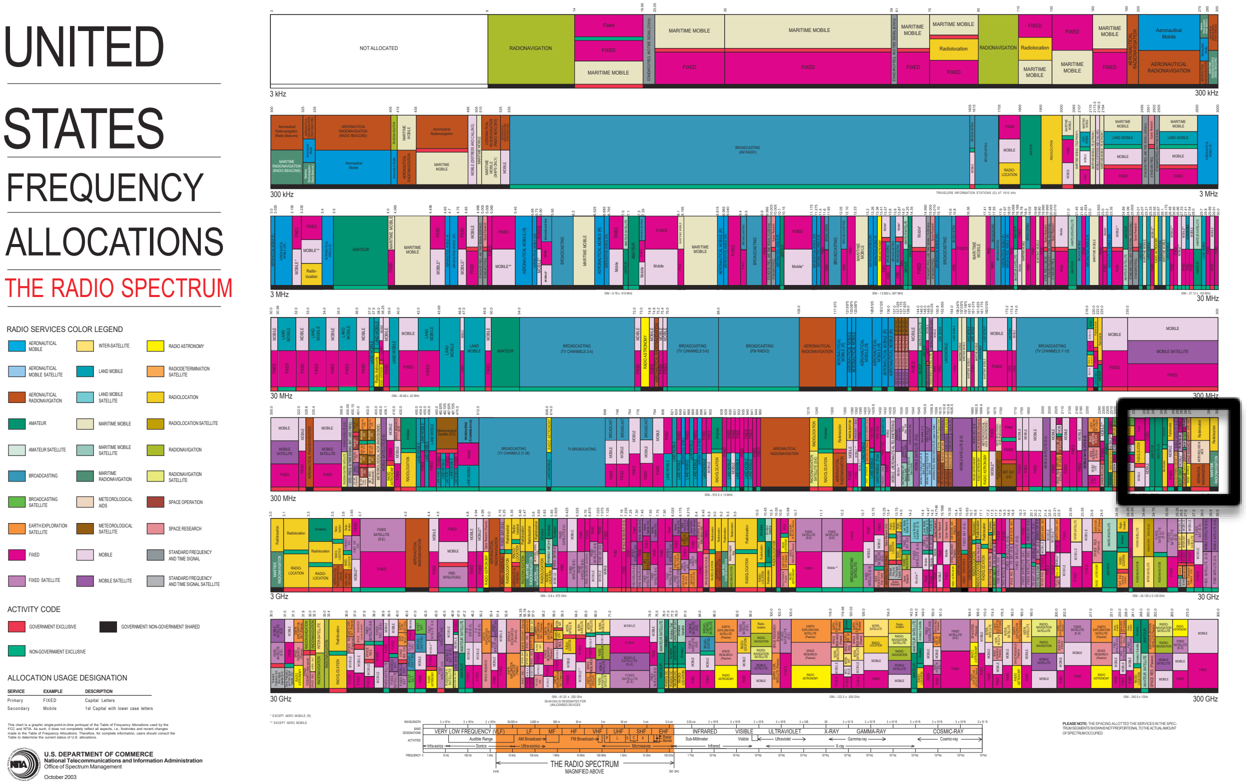
Radio communication



U.S. Spectrum allocation chart:

http://www.ntia.doc.gov/osmhome/allochrt.pdf

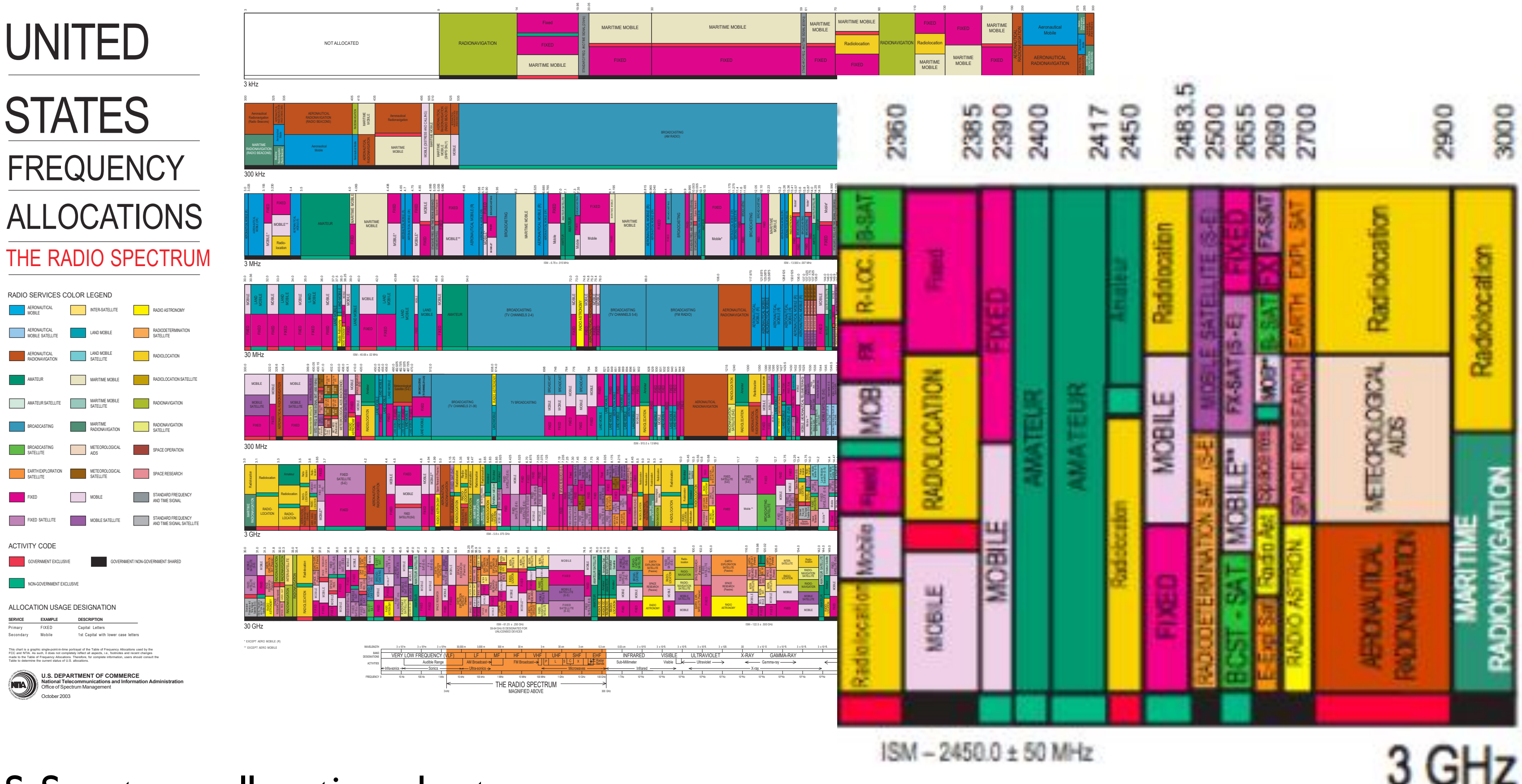
Radio communication



U.S. Spectrum allocation chart:

http://www.ntia.doc.gov/osmhome/allochrt.pdf

Radio communication



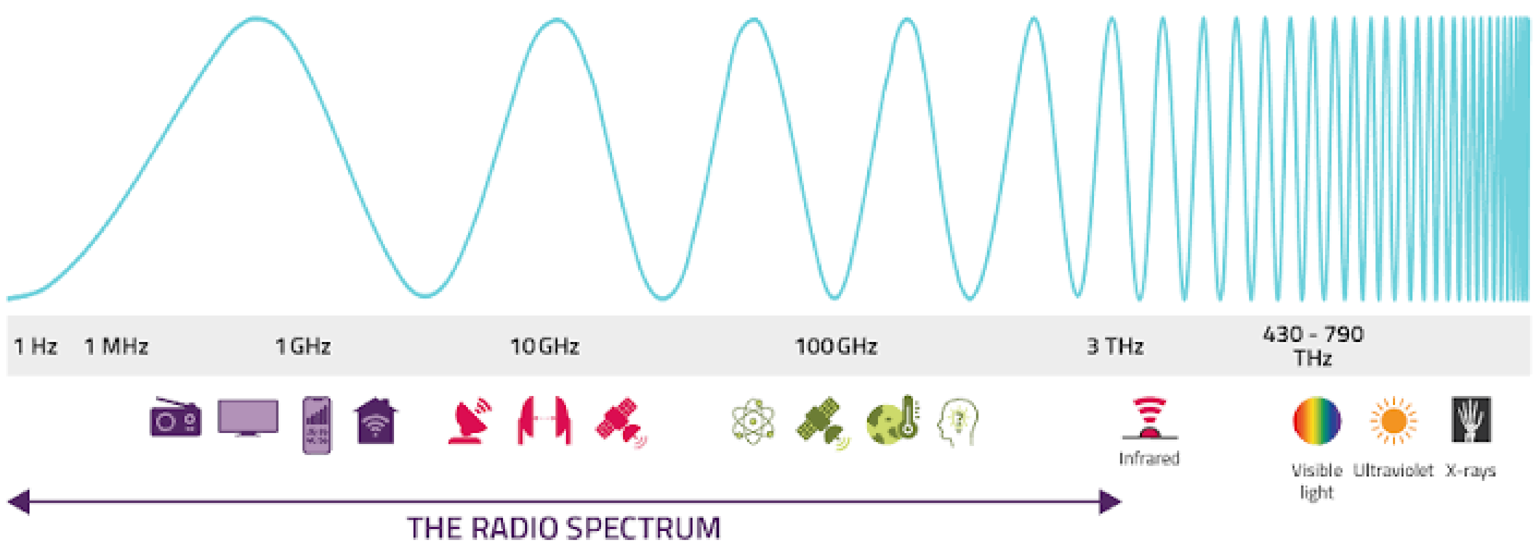
U.S. Spectrum allocation chart:

http://www.ntia.doc.gov/osmhome/allochrt.pdf

How is spectrum managed?

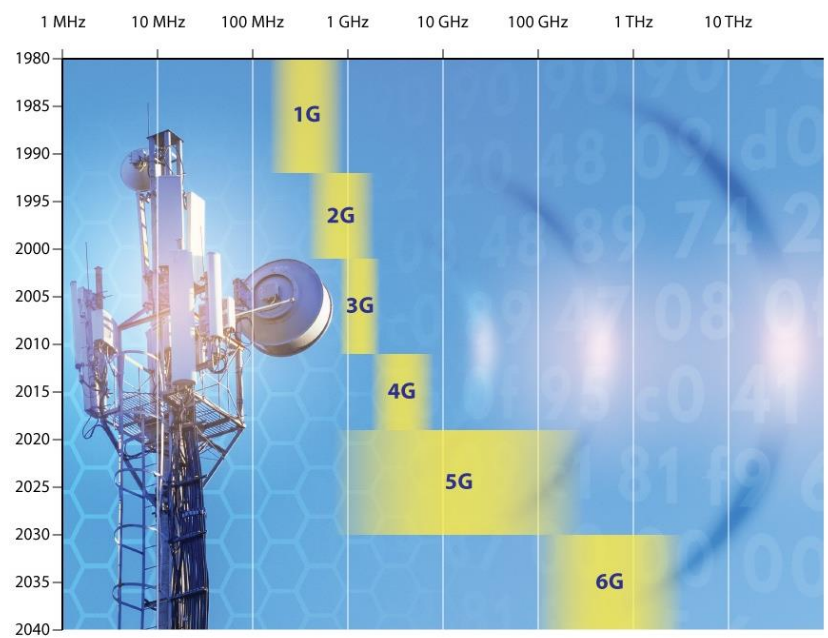
Radio Spectrum

- Limited spectrum
  - Must be shared among the various applications
- Spectrum access
  - Typically regulated by the government
    - Licensed v. Unlicensed



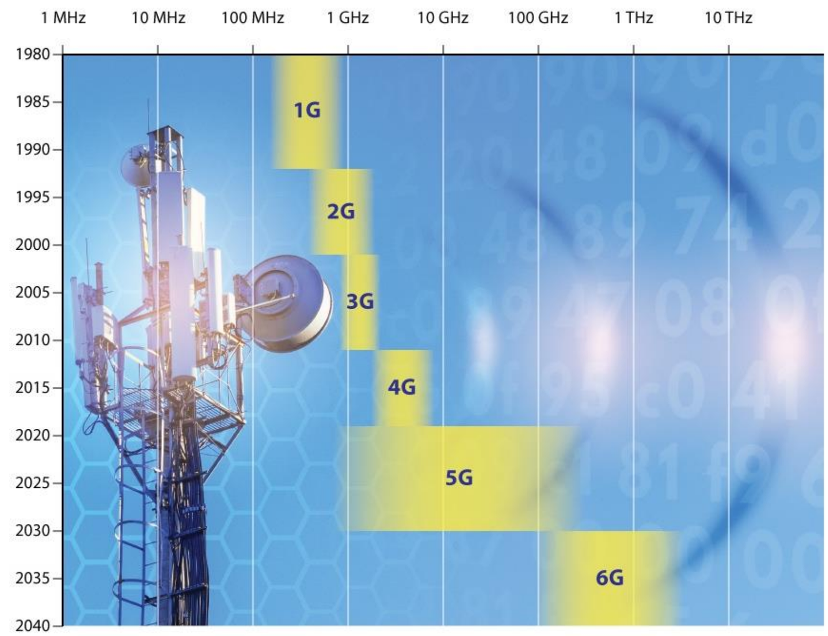
How Spectrum Gets Allocated

- Licensed spectrum
  - Cellular, TV Radio, Satellite, Public Safety, Wireless Mics, LTE/5G
  - U.S.
    - FCC allocates and enforces spectrum rights
  - International
    - ITU coordinates allocations globally so radios don't cross borders and collide



How Spectrum Gets Allocated

- Licensed spectrum
  - Since 1994, most licensed spectrum is allocated by competitive auction, not government directly
    - 2021 C-band auction (3.7–3.98 GHz, cleared for 5G)
      - $81.1 billion – largest spectrum auction in U.S. history
      - Verizon alone bid $45.5B
  - Exclusive use, but expensive and slow to acquire



How Spectrum Gets Allocated

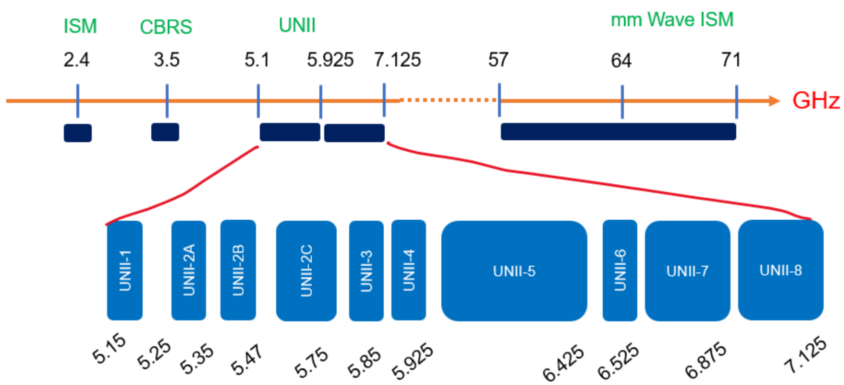
- Unlicensed spectrum
  - Industrial, scientific and medical (ISM) bands
  - Key bands:
    - 900 MHz, 2.4 GHz, 5 GHz, and now 6 GHz
  - Wi-Fi, Bluetooth, Zigbee, Z-Wave, Thread, UWB, LoRa, Cordless Phones, Baby Monitors, RFID, NFC, Garage Doors, Key Fobs

How Spectrum Gets Allocated

- Unlicensed spectrum
  - FCC rules
    - No license needed
    - No protection either
    - Guidelines: tolerate interference, don't cause harmful interference
  - The tradeoff
    - Free and open, but noisy and uncoordinated

How Spectrum Gets Allocated

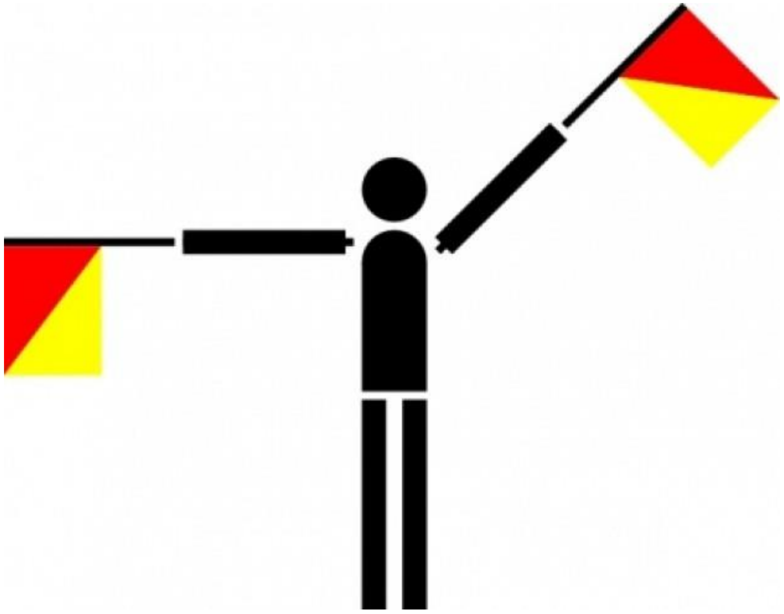
- 900 MHz ISM (902–928 MHz)
  - Z-Wave, some LoRa deployments, baby monitors, cordless phones
- 2.4 GHz ISM (2.400–2.4835 GHz)
  - Wi-Fi (802.11b/g/n/ax), Bluetooth, ZigBee, and most consumer wireless devices
  - 14 channels defined, only 1–11 usable in the U.S.
- 5 GHz U-NII (5.150–5.850 GHz, split into U-NII-1 through U-NII-4)
  - Wi-Fi (802.11a/n/ac/ax)
  - U-NII-2 requires DFS (dynamic frequency selection) to avoid interfering with radar
- 6 GHz (5.925–7.125 GHz, U-NII-5 through U-NII-8)
  - Opened up in 2020
  - Wi-Fi 6E/7 - 1.2 GHz of new unlicensed spectrum
- 60 GHz band (57–71 GHz)
  - Very high frequency, short range, huge bandwidth
  - WiGig (802.11ad/ay) and short-range radar/sensing applications
  - heavy atmospheric absorption limits range to tens of meters



What Makes Wireless Different?

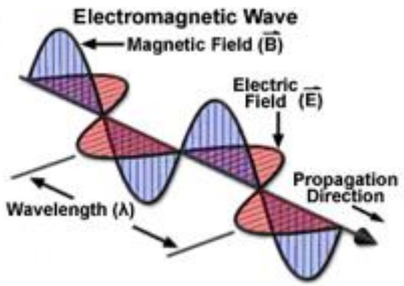
- Absence of wires facilitate mobility
- Signal attenuation
- Spatial reuse
- Diversity
  - Multi-user diversity
  - Antenna diversity
  - Time diversity
  - Frequency diversity
- Wireless devices often battery-powered
  - Need to conserve energy
- Broadcast medium
  - Easier to snoop on, or tamper with, wireless transmissions

Wireless through the ages …



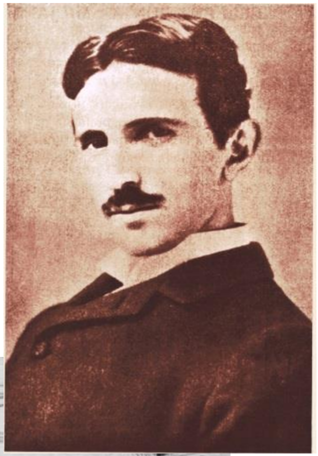
Birth of modern-day wireless communication

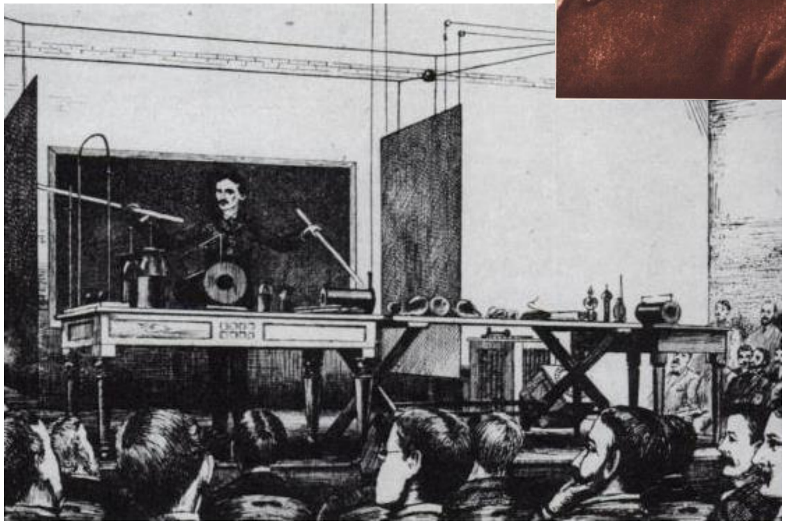
- 1865
  - Maxwell predicts existence of electromagnetic (EM) waves
- 1887
  - Hertz proves existence of EM waves



Birth of modern-day wireless communication

- 1896
  - Wireless telegraph invented by Guglielmo Marconi
  - Awarded the Nobel Prize in 1909!





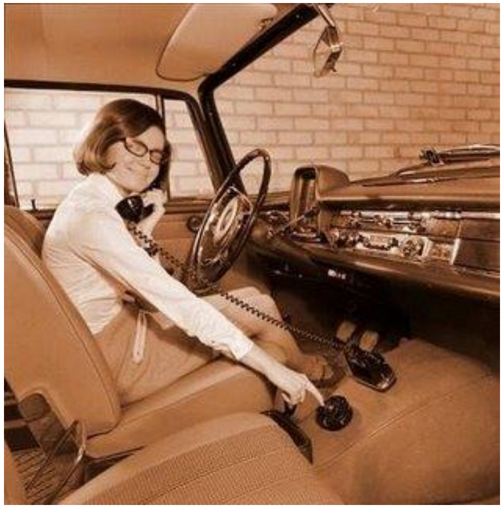
- 1893
  - Tesla credited with first radio communication

Birth of modern-day wireless communication

- 1900
  - First voice over radio transmission
  - Sent a brief, barely intelligible voice message about a mile
- 1901
  - Marconi: First telegraphic signal (Morse code ‘S’ – dot dot dot) traveled across the Atlantic ocean (3,500km/2,200mi).
  - Took another year for it to be bi-directional. And 5 years for commercial service
  - Modulates digital data onto an analog carrier to transmit Morse code
- 1906
  - First radio broadcast of voice and music
- 1935
  - Frequency modulation (FM) demonstrated by Armstrong

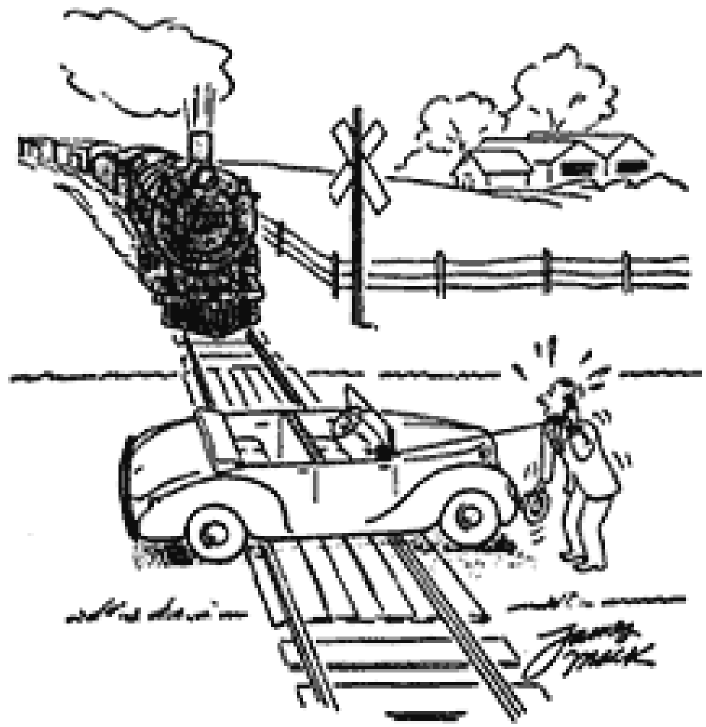
In the beginning …

- 1946
  - First interconnection of mobile users to public switched telephone network (PSTN)
  - Operator assisted with 250 maximum users
- Mobile ≠ Portable!
  - First mobile phone weighed 40 Kg!
  - Very bulky and expensive



Mobile Telephone System (MTS)

- October 2, 1946
  - Motorola communications equipment carried the first calls on Illinois Bell Telephone Company's new car radiotelephone service in Chicago
  - Few radio frequencies available
    - Service quickly reached capacity



"Hello, Mr. Bunting. I've changed my mind—I'll take that accident policy!"

April, 1948

Mobile Telephone System (MTS)

- 1946
  - 3 channels for all the users in the metropolitan area
    - Later more licenses were added bringing the total to 32 channels across 3 bands

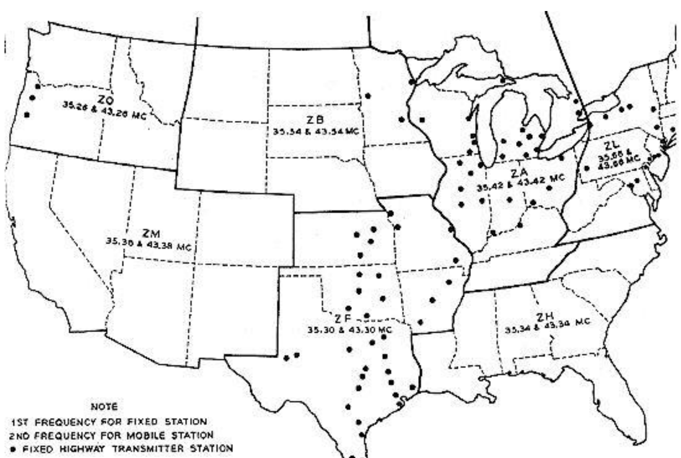
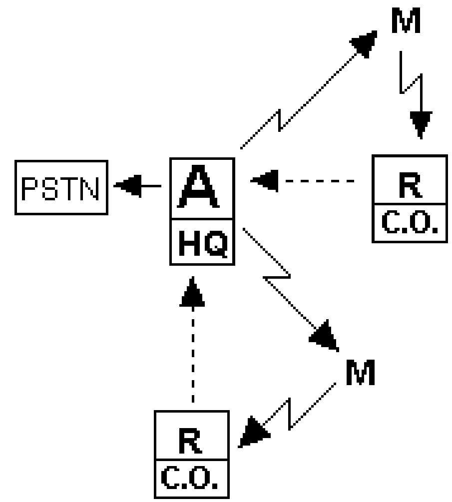
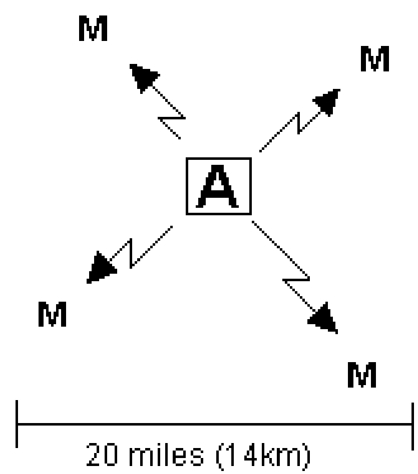


Fig. 1—Land stations and zones for the highway mobile radio-telephone system



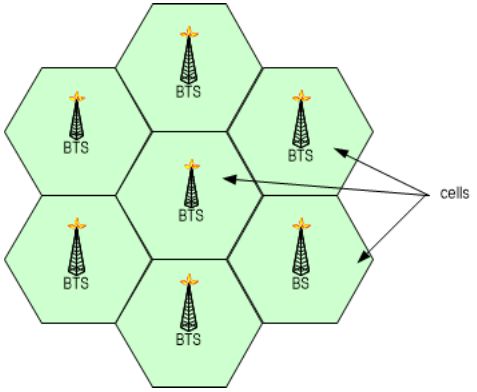


Who needs one anyway?

- The FCC commissioner Robert E. Lee
  - “mobile phones are a status symbol”
  - “Every family might someday believe that its car had to have one!”
  - “frivolous use of spectrum”
  - “It’s not going to be something you and I put in the car to call home and say we’re on the way home for dinner!”

From global to cellular

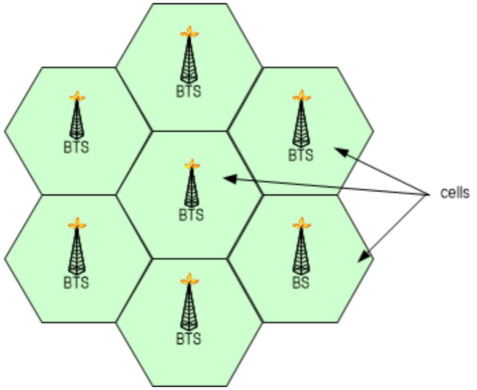
- 1947
  - Donald H. Ring outlined the idea in a Bell labs memo
  - Split an area into cells with their own low power towers
  - Each cell would use its own frequency



From global to cellular

- 1947
  - Donald H. Ring outlined the idea in a Bell labs memo
  - Split an area into cells with their own low power towers
  - Each cell would use its own frequency

- An idea before its time
  - Existing technology could not handle the "extreme" processing needs!
  - Handoff for thousands of users
  - Rapid switching infeasible
    - Maintain call while changing frequency



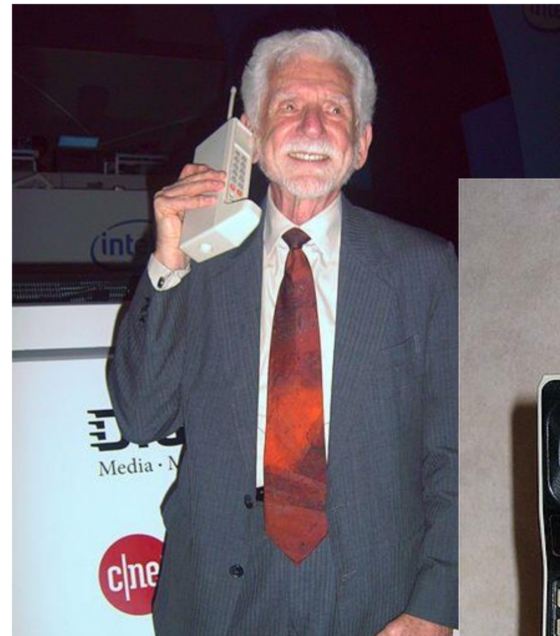
Almost there …

- 1947
  - William Shockley, John Bardeen, and Walter Brattain invented the transistor

- But true mobile coverage was still out of reach
  - A mobile phone needs to send a signal – not just receive and amplify
  - The energy required for a mobile phone transmission still too high for the high power/high tower approach – could only be done with a car battery

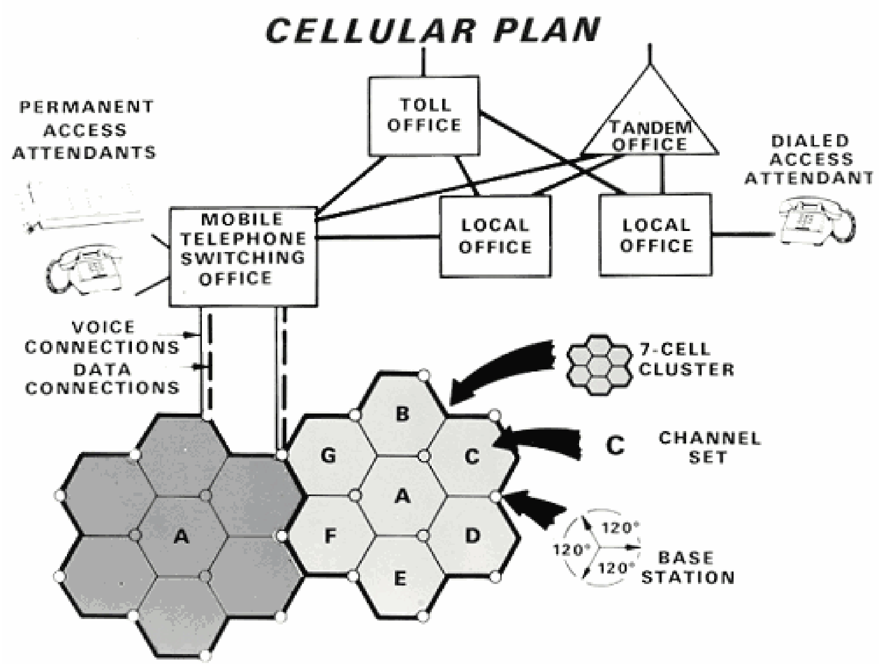
The first cell phone!

- Prototype
  - Dr. Martin Cooper of Motorola made the first publicized handheld mobile phone call on April 3, 1973
- Production
  - 10 years (1973-1983) and $100 million to develop!
- DynaTAC8000X
  - 2 pounds
  - 30 mins of talk time
  - 8 hours of standby
  - LED display for dialing or recall 30 phone numbers
  - $3,995!



Analog Cellular: 1G

- 1978
  - AMPS – Advanced/Analog Mobile Phone System
  - First complete cellular system (not handheld) deployed in the suburbs of Chicago
  - 10 1-mile radius cells
  - 135 custom-designed car phones
- Limitations
  - Unencrypted
  - Vulnerable to eavesdropping
  - Susceptible to "cloning"
  - Frequency-division multiple access (FDMA) required significant amounts of wireless spectrum



Used for On*Star until ~2010!

Digital Cellular: 2G

- GSM (3GPP)
  - 1991
    - First GSM network in Finland
  - TDMA
  - Digital, circuit-switched network optimized for full duplex voice telephony
  - Expanded to include data communications
    - Circuit-switched transport
    - Packet data transport via GPRS (General Packet Radio Services) and EDGE (Enhanced Data rates for GSM Evolution or EGPRS)
  - Evolved into 3G WCDMA / UMTS

- IS-95 / cdmaOne (3GPP2)
  - 1995
    - Developed by Qualcomm with Motorola and AT&T
    - First commercial deployment: Hong Kong (Dec. 1995); South Korea and the U.S. followed quickly
  - CDMA
    - Evolved into 3G CDMA2000

Two incompatible 2G paths → two incompatible 3G paths

Mobile Broadband: 3G & 4G

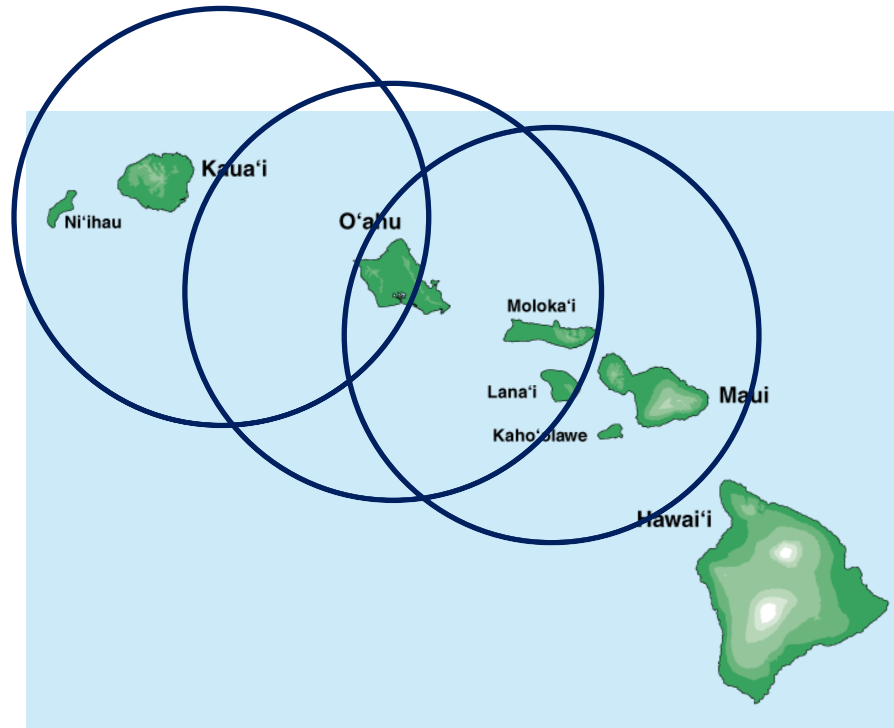
- 3G
  - Service goal: 14 Mbps
  - 2001
    - First commercial WCDMA network in Japan
  - 2002
    - First commercial CDMA2000 1xEV-DO network in South Korea
  - Improvements
    - streaming media (radio and television)
  - End of 2007
    - 295 million subscribers on 3G networks worldwide
    - 3G largely retired by U.S. carriers by 2022
- 4G
  - Service goal: 100 Mbps
  - 2008
    - Native IP
      - Mobile WiMAX
      - LTE Advanced
    - OFDMA
    - MIMO
  - End of 2025
    - 4G/LTE peaked at ~5.17 billion subscriptions in 2024, now declining as users migrate to 5G (GSA, 2025)

Mobile Broadband: 5G & 6G

- 5G
  - Service goal: 10Gbps
  - 2019
    - mmWave: 24 GHz - 54 GHz
    - Massive MIMO
    - Edge computing
    - Beamforming
    - Small cells
  - End of 2025
    - Over 3 billion subscribers on 5G networks worldwide, about 1/3 of all mobile subscriptions (GSMA/GSA, 2025)
    - Passed 1 billion 5G subscriptions in 2023 – the fastest generational ramp yet
- 6G
  - Service goals:
    - 1Tbps
    - msec latency
    - Location aware
  - Plans (2030?) – 3GPP finalized 6G Release 21 timeline in June 2026; spec completion targeted early 2029
    - Millimeter waves (30 to 300 GHz)
    - Terahertz radiation (300 to 3000 GHz)
    - Small cells
    - Beamforming

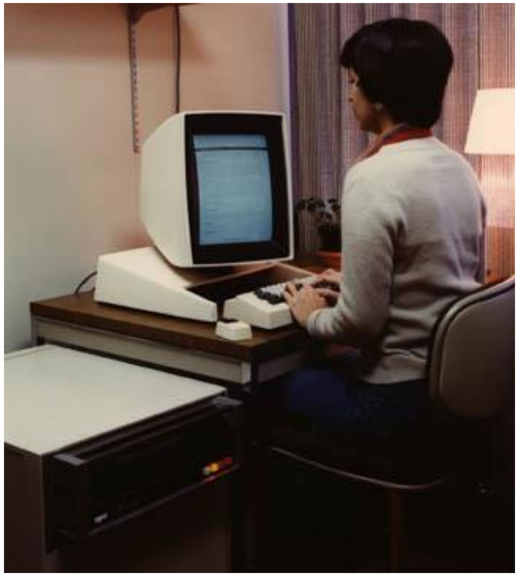
In the meantime …

- 1971: Aloha Packet Radio Network
  - Norm Abramson left Stanford to surf
  - Set up first data communication system for Hawaiian islands
  - Hub at U. Hawaii, Oahu
  - Two radio channels:
    - Random access: for sites sending data
    - Broadcast for hub rebroadcasting data



From Aloha comes Ethernet

- Ethernet
  - Developed by Xerox PARC, 1973
  - Standardized by Xerox, DEC and Intel in 1980
  - Later, IEEE 802.3 standard
  - Fast Ethernet (100 Mbps) - IEEE 802.3u standard
  - Switched Ethernet now popular
- Numerous standards with increasing bandwidth over the years
  - 10 Mbps – 100 Mbps – 1 Gbps – 10 Gbps



Xerox Alto, first machine networked with Ethernet

From Aloha comes Ethernet

- Ethernet
  - Developed by Xerox PARC, 1973
  - Stand
    Intel i
  - Later,
  - Fast E
    802.3
  - Switc
- Numer
  increasi
  years
  - 10 Mb
    Gbps


The New York Times

Turing Award Won by Co-Inventor of Ethernet Technology

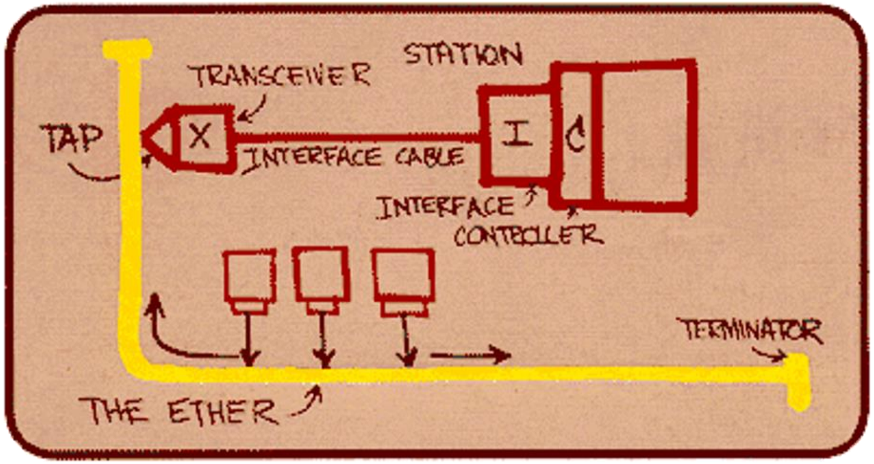
In the 1970s, Bob Metcalfe helped develop the primary technology that lets you send email or connect with a printer over an office network.

Give this article

Xerox Alto, first machine networked with Ethernet

Ethernet

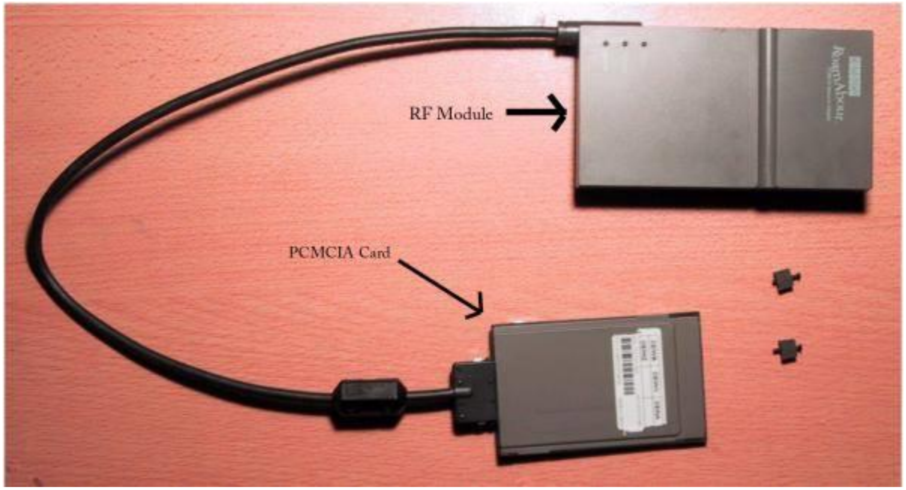
- "dominant" wired LAN technology:
  - Single chip, multiple speeds(e.g., Broadcom BCM5761)
  - First widely used LAN technology
  - Simple, cheap
  - Kept up with speed race: 10 Mbps – 10 Gbps



Metcalfe's Ethernet sketch

From Ethernet comes Wi-Fi!

- 1986
  - Wireless alternative for Ethernet and Token Ring
- 1995
  - FCC released ISM band for unlicensed use
  - WaveLAN
    - 900 MHz ISM band
    - 1 & 2 Mbps



Integrated Wi-Fi

- Antennas placed on the frame of the screen
- Mini-PCI format allows for full integration
- Latest radio technology may feature up to 3 antennas or more!

The growth of Wi-Fi

- **1997**
  - IEEE 802.11
    - DSSS
    - 2.4 GHz
    - 1 & 2 Mbps
- **1999**
  - IEEE 802.11b (Wi-Fi 1)
    - DSSS/CCK
    - 2.4 GHz
    - 11MBps
- **1999**
  - IEEE 802.11a (Wi-Fi 2)
    - OFDM
    - 5.8 GHz
    - 54MBps

The growth of Wi-Fi

- 2003
  - IEEE 802.11g (Wi-Fi 3)
    - OFDM
    - 2.4 GHz
    - 54MBps
- 2009
  - IEEE 802.11n (Wi-Fi 4)
    - HT-OFDM & MIMO
    - 2.4 GHz / 5 GHz
    - 54 Mbps to 600 Mbps

The growth of Wi-Fi

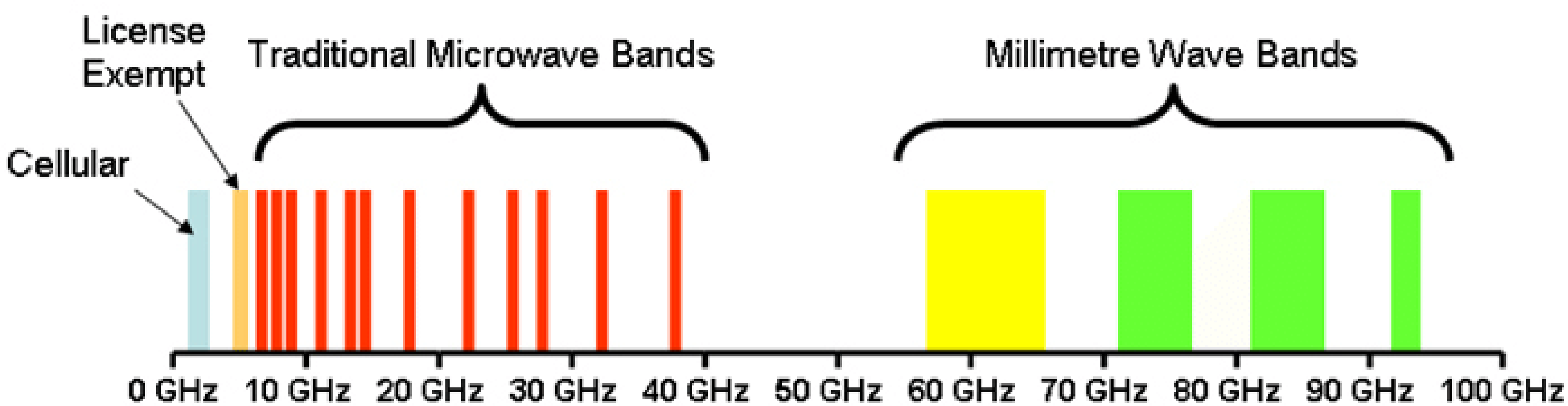
- 2013
  - IEEE 802.11ac - Wi-Fi 5
    - VHT-OFDM & MU-MIMO
    - (2.4 GHz legacy) 5 GHz
    - 6.9 Gbps
- 2019/20
  - IEEE 802.11ax - Wi-Fi 6 / Wi-Fi 6e
    - OFDMA
    - 2.4 GHz / 5 GHz / 6 GHz (e only)
    - 9.6 Gbps

The growth of Wi-Fi

- 2024
  - IEEE 802.11be – Wi-Fi 7
    - Multi-RU OFDMA & 4096-QAM
    - 2.4 GHz / 5 GHz / 6 GHz
    - 46.1 Gbps
    - Shipping in phones/laptops by 2025–26
- ~2028 Ratification
  - IEEE 802.11bn
    - Coordinated OFDMA & Multi-AP Spatial Reuse
    - 2.4 GHz / 5 GHz / 6 GHz / 60 GHz
    - 100+ Gbps
    - First branded routers expected summer 2026 – hardware ships before the standard is finished
    - Focus: reliability & latency, not just peak speed

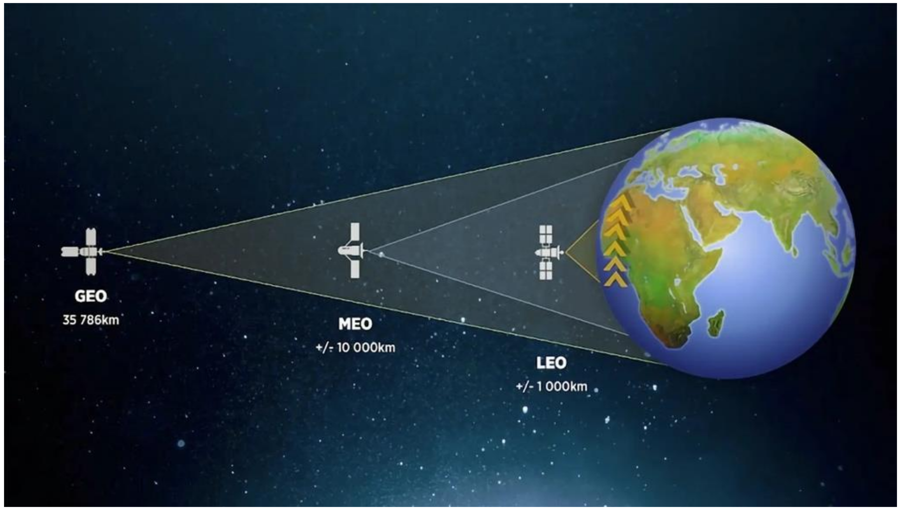
When Wi-Fi isn't enough: mmWave!

- Legacy Sub-6 GHz
  - cm to m wavelengths
  - Pass easily through concrete, foliage, and glass over miles
  - strict speed limits due to constrained bandwidth
- mmWave Bands
  - Ultra-short wavelengths
  - Sacrifice range and structural penetration for gigabits per second



Satellite Communication

- Geostationary
  - ~36,000 km altitude
    - ~240 ms one-way delay,
    - ~600 ms round-trip in practice
    - Fine for one-way TV broadcast
    - Painful for a phone call
  - 1962 – Telstar 1 (AT&T)
    - First active comsat
    - First live transatlantic TV
  - 1963–64 – Syncom 2 & 3 (Hughes)
    - First geostationary satellites
  - 1965 – Intelsat I ("Early Bird")
    - First commercial satellite service



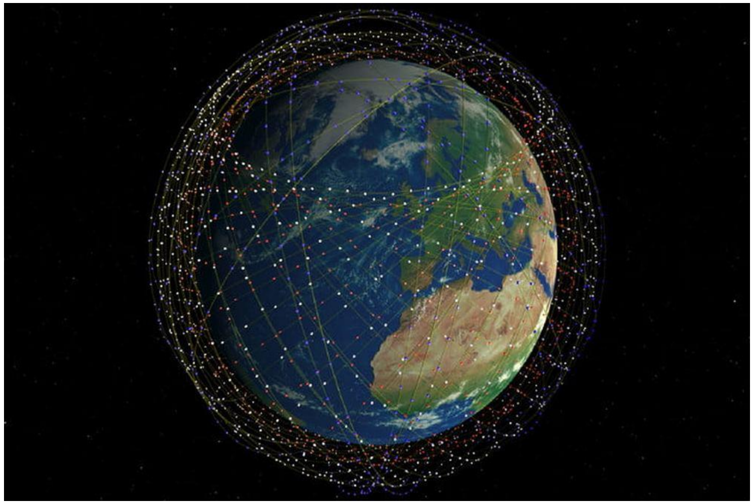
Satellite Communication

- LEO
  - 160–2,000 km altitude
  - Minimum 1.8 ms one-way, 3.7 ms minimum round-trip
  - 1998 – Iridium
    - 66-satellite LEO constellation, Extra altitude provided wider individual footprints since it only had 66 satellites
    - 780 km, 2.6 ms one-way, 5.2 ms round-trip
    - Lower altitude fixed the Geo delay problem — but bandwidth was tiny:
      - 2.4 kbps per channel, voice/text only
    - $5B to build. Bankrupt after 9 months (1999); relaunched 2001, still flying as a niche service

For 60 years, had to pick low delay (LEO, bandwidth-starved) or usable bandwidth (GEO, delay-crippled)

Satellite Communication

- 2019
  - Starlink and OneWeb relaunch the LEO broadband idea
- 2020–21
  - SpaceX tests inter-satellite laser links,
  - Launches the first laser-equipped satellites
    - Satellites start routing traffic to each other in orbit instead of through a ground station
- 2023
  - V2 Mini satellites
    - 4x the capacity of earlier generations, upgraded phased-array antennas
    - Added radio hardware needed to talk directly to unmodified cell phones
- By 2026
  - Scaled into the largest optical mesh network ever built
  - Carrying a large share of all Starlink traffic
    - Enables ocean and polar coverage without a nearby ground station



Satellite Broadband: The New Frontier (2026)

- LEO broadband access
  - 25–50 ms latency
    - Competitive with terrestrial broadband, not just “usable”
  - Starlink
    - 65–220 Mbps download / 10–15 Mbps upload in real-world use
    - 10,900+ satellites in orbit
    - Largest active constellation ever
    - Passed 10 million subscribers Feb. 2026
    - First satellite system to beat GEO’s delay and Iridium’s bandwidth at the same time
  - Amazon Kuiper
    - ~330–390+ satellites launched as of Aug. 2026;
    - Beta service targeted late 2026 / early 2027

Satellite Broadband: The New Frontier (2026)

- Satellite-to-phone (direct-to-cell)
  - No special hardware
    - An ordinary phone talks straight to a satellite
    - ~10 Mbps per beam, shared across every phone connecting through that coverage cell
    - Fine for texting, tight for more
  - Starlink + T-Mobile
    - 650+ direct-to-cell satellites
    - live texting across 11 countries
    - ~8M users
  - AST SpaceMobile + AT&T/Verizon
    - FCC-cleared 248-satellite constellation
    - Slipped from early 2026 to 2027

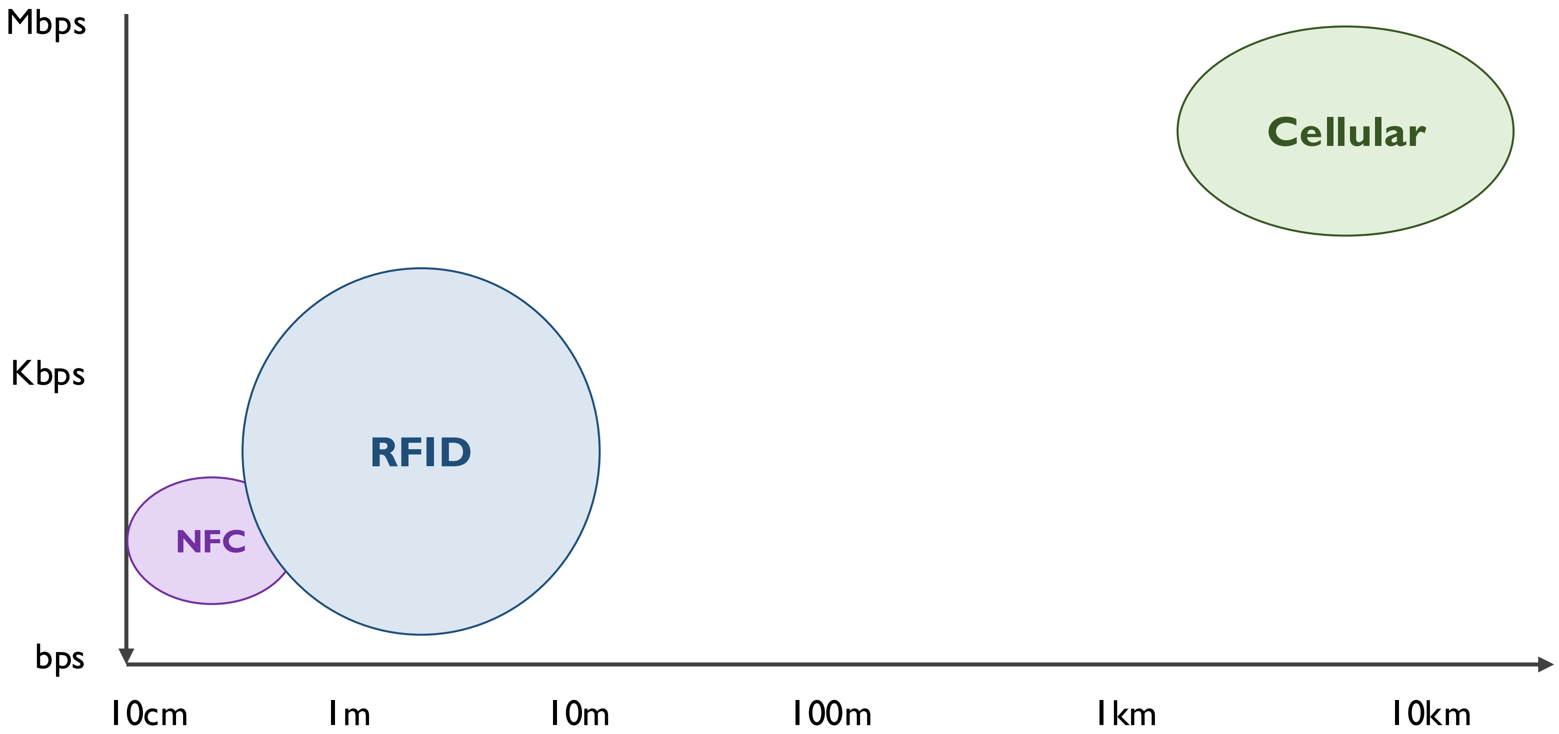
The bandwidth-vs-reach tradeoff isn't gone — it just moved from satellite-vs-satellite to dish-vs-phone-antenna

Backscatter Communication

- Low power
  - No Battery
- Low cost
  - 10 cents
- Low range
  - 10 – 15 meters
- Low Data rates
  - 10Kbps – 640 Kbps

No power: Range vs. Data Rate

- Range and data rate roughly trade off across wireless technologies



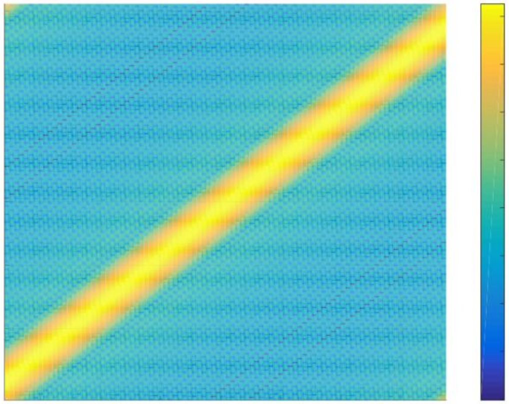
Backscatter trades range and speed for near-zero power

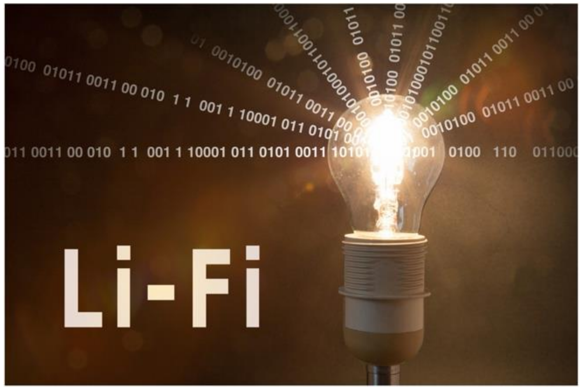
RFID: Radio Frequency Identification

- Passive RFID
  - No battery
  - Powered entirely by the reader's signal
  - Short range, but life span measured in decades
- Battery-assisted RFID
  - Battery powers onboard sensing/computation only
  - Radio is passive
- Active RFID
  - Has a battery and transmits its own signal
  - Longer range, but shorter life span
- Frequency bands (passive RFID)
  - LF/HF (125 kHz–13.56 MHz, same band as NFC)
    - < few cm, bps–kbps
  - UHF
    - a few meters, up to 100s of kbps
- Everywhere already
  - Inventory tags, access badges, toll passes, supply-chain tracking

And even more technologies

- Low power wireless
  - Bluetooth
  - ZigBee
  - UWB
  - LoRa
- Optical wireless
  - LiFi (Visible Light Communication)





Wireless Security: Threat Model

- Broadcast medium = no physical boundary
  - Anyone in range can receive or inject signals
- Core threats
  - Eavesdropping
  - Spoofing / impersonation
  - Jamming (denial of service)
  - Replay attacks
  - Man-in-the-middle
  - Traffic analysis / location tracking
- Wired vs. wireless security
  - Wired: physical access = de facto security boundary
  - Wireless: no equivalent — security must be built into the protocol
- Why this matters for this course
  - Security and privacy are explicit course outcomes
  - Every layer we study (PHY, MAC, network) has security implications

Wi-Fi Security Evolution: WEP to WPA3

- 1997 – WEP (Wired Equivalent Privacy)
  - RC4 stream cipher, static shared key
  - Weak IV reuse — crackable in minutes by mid-2000s
- 2003 – WPA (stopgap fix)
  - TKIP adds per-packet keying
  - Still built on RC4
- 2004 – WPA2
  - AES-CCMP replaces RC4/TKIP
  - Standard for over a decade
  - Broken by KRACK key-reinstallation attack (2017)
- 2018 – WPA3
  - SAE (Dragonfly) handshake replaces PSK
  - Resists offline dictionary attacks
  - Forward secrecy
  - Mandatory management-frame protection
  - Simplified onboarding for IoT devices
- Takeaway
  - Each generation patched the previous one's core flaw
  - Security protocols evolve alongside attacks — never "done"

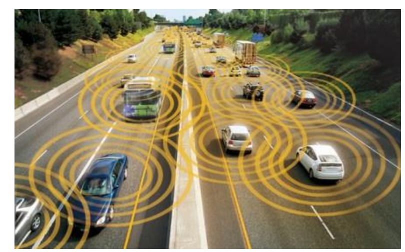
Beyond Wi-Fi: Security Across Wireless Technologies

- Cellular
  - 2G: no mutual authentication → fake base stations / IMSI catchers
  - 3G / 4G / 5G: SIM-based mutual authentication
- Bluetooth / BLE
  - Weak "just works" pairing mode
  - KNOB attack: forces short encryption keys
- Resource-constrained IoT
  - Many devices can't run standard crypto
  - Lightweight authentication is an open research area
- Open Problems
  - Physical-layer security: channel fading/RSS for key generation
  - Intrusion and jamming detection via signal characteristics
  - Privacy-preserving localization

Wireless communication is a tool

- How do we use it?

- Emergency broadcast systems
  - Restricted communication
- Device to infrastructure
  - Internet access, phone calls



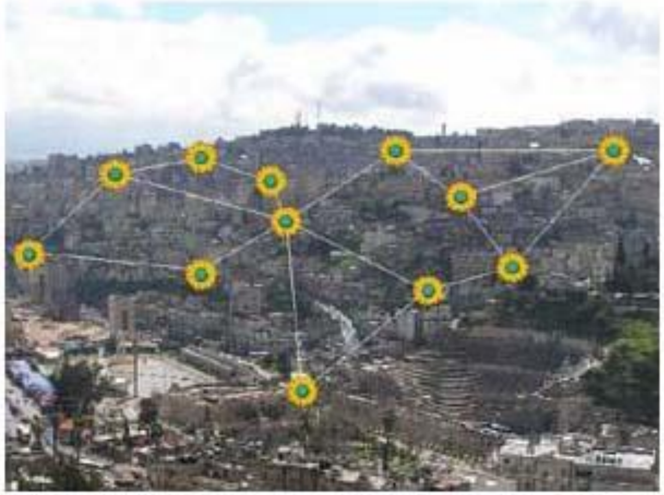
- Device to device
  - Sensor networks, vehicular networks, mobile social networks

Apps, apps and more apps

- The first killer apps
  - SMS
  - Ring tones
  - Replacement for landlines
- What drives mobile now
  - Videos
  - Gaming
  - Social media
  - Ecommerce
- Data communication is dominant
  - Always-on connectivity…
  - … while on the move

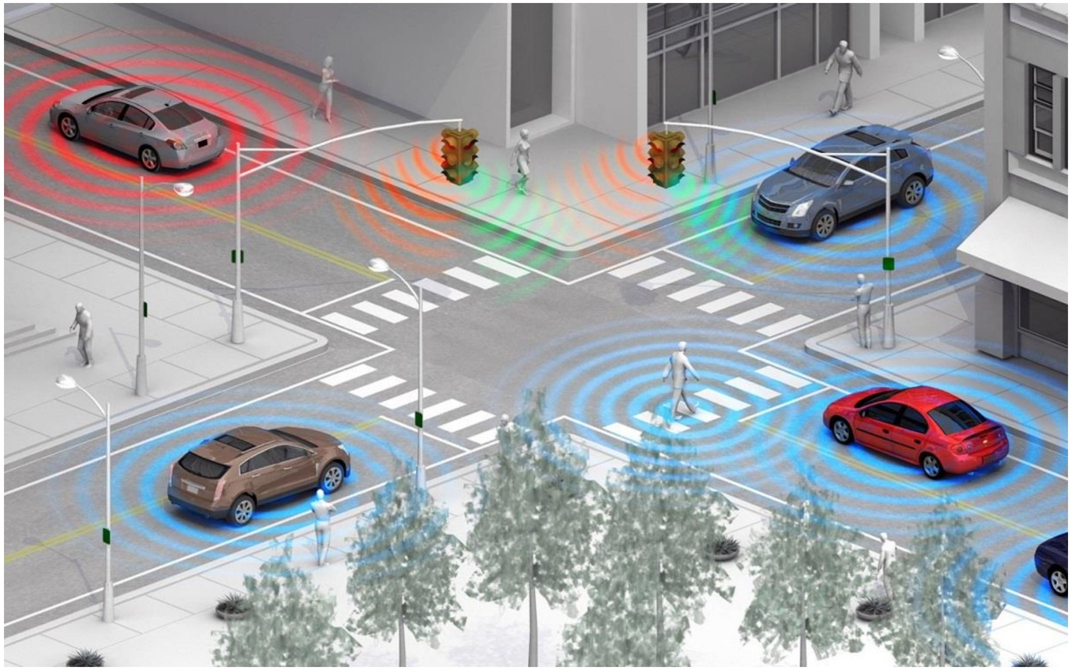
Large scale Wi-Fi access

- Wi-Fi in developing regions

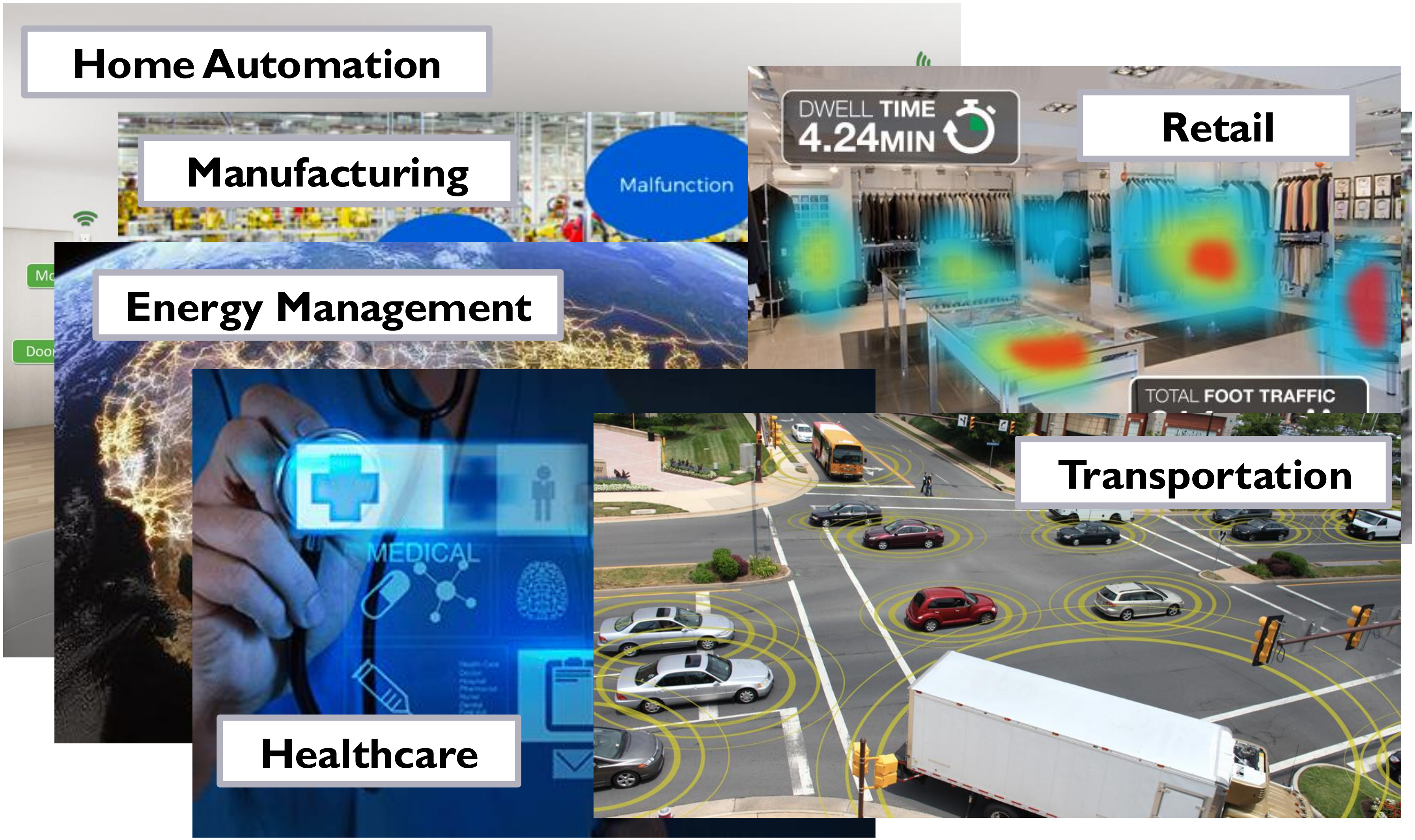


Vehicle-to-Vehicle Communication

- Sensing
- Safety
- Enhanced coverage



Internet of Things



How do we make this all happen

- Research!

Ubiquitous Services

Incentives

Loss Discrimination

Energy Savings

Spatial Reuse

Application

Security

Transport

Network

MAC / Link

PHY

Privacy

Eavesdropping

Mobility

Interference Mgmt.

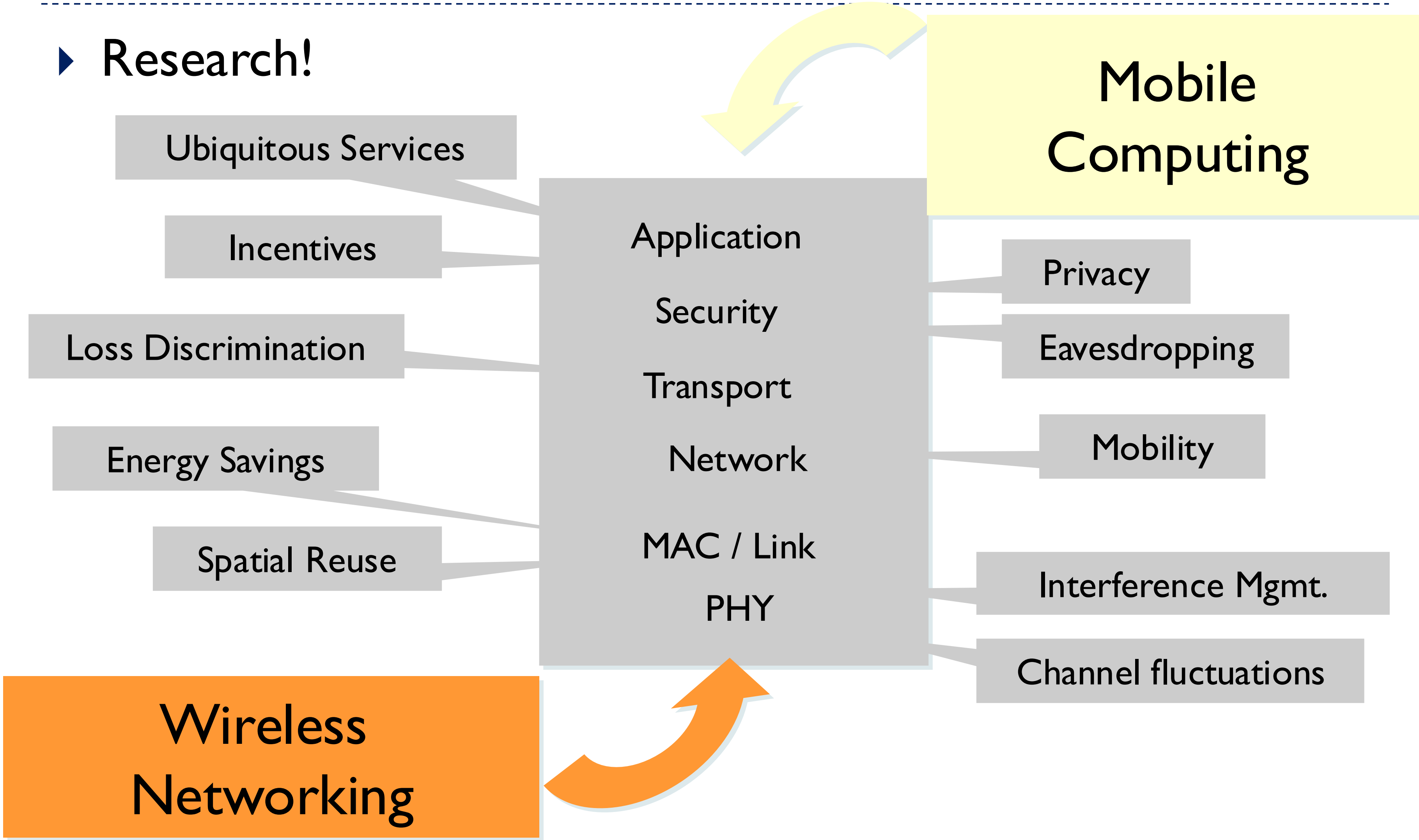
Channel fluctuations

Applications that exploit ubiquity and mobility. Challenges underlying such applications

Enabling wireless ubiquity. Showing what is feasible, and what is not …

How do we make this all happen

- Research!



At the End of this Course …

- You should understand
  - Physical layer (radios, rate, antennas, channels)
  - MAC protocols (who gets the chance to talk)
  - Cross-Layer protocols (interference cancellation, OFDM …)
  - Routing (path selection algorithms and issues)
  - Reliability (wireless congestion control, rate control)

  - Applications (social networks, personal networks, P2P networks)
  - Sensing Systems
    - Localization (extracting the location of a device)
    - Mobility (how it helps and disrupts communication)
    - Interfaces (phones are more than communication devices)
    - Privacy (how to protect a user from being tracked)

  - Energy-awareness (how it percolates various network functions)
  - Capacity (what is feasible, what are performance bounds)