Silicon Flatirons

KNOW WHAT'S NEXT.

Radio Spectrum Tutorial

Prepared for Silicon Flatirons Conference

Saving Our Spectrum: Handling Radio Layer Vulnerabilities in Wireless Systems

Dale N. Hatfield

Keith D. Gremban

October 10, 2019

COLORADO LAW

UNIVERSITY OF COLORADO **BOULDER**

Basic Wireless Concepts

Challenge of Explaining How Radio Works

"You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat."

Albert Einstein

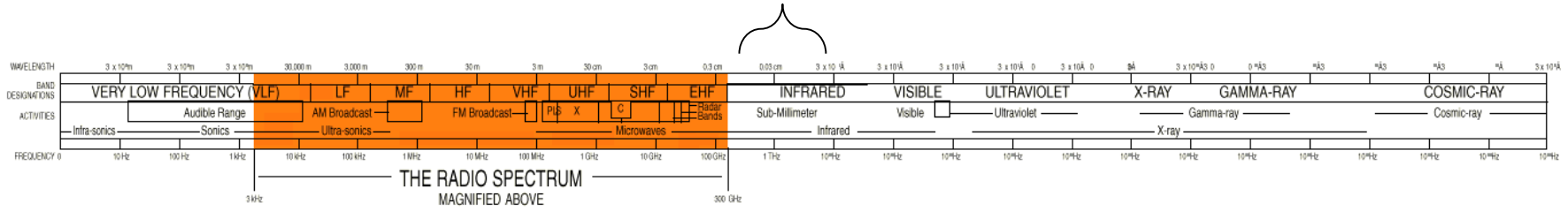
Basic Wireless Concepts

- What Is Spectrum?
  - “Spectrum” is a conceptual tool used to organize and map a set of physical phenomena
  - Electric and magnetic fields produce (electromagnetic) waves that move through space at different frequencies
  - The set of all possible frequencies is called the “electromagnetic spectrum”

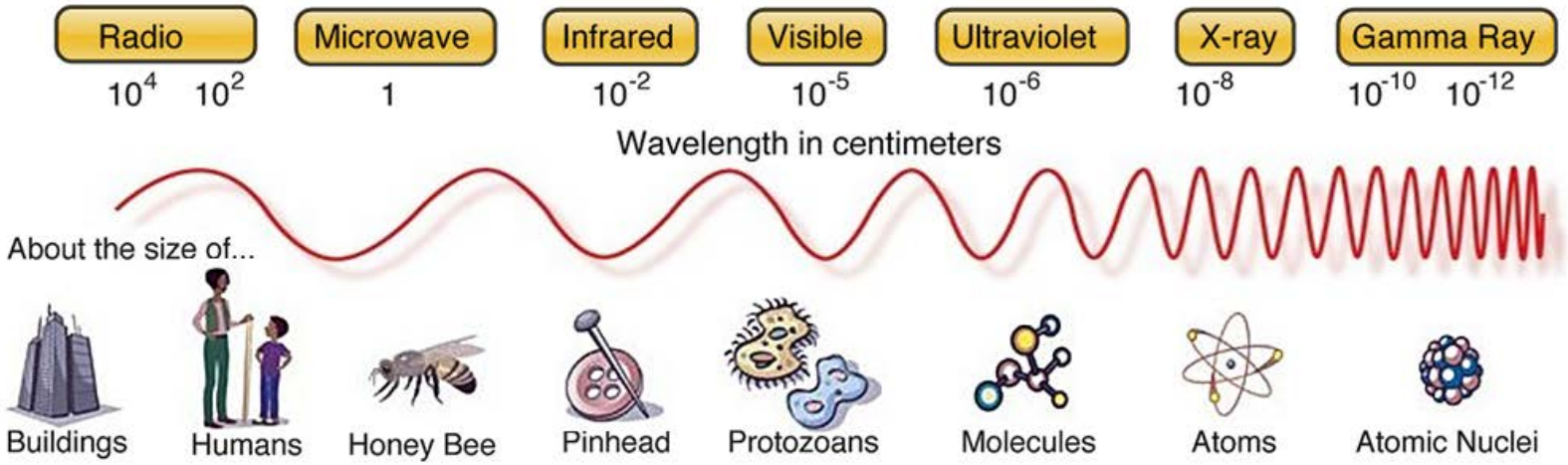
Basic Wireless Concepts

- What Is Spectrum?
  - The subset of frequencies between 3,000 Hz and 300 GHz is known as the “radio spectrum”
  - Note that radio waves do not require a medium per se, that is, radio waves can travel through a vacuum (e.g., outer space)

Electromagnetic Spectrum

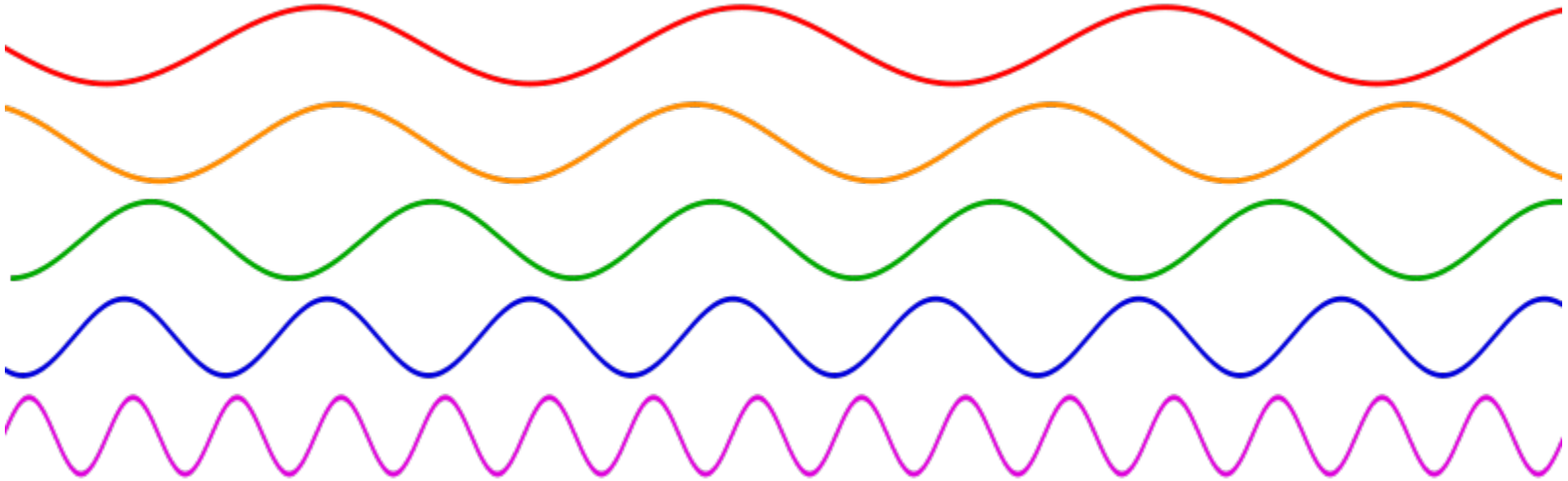


Basic Wireless Concepts



Basic Wireless Concepts

Waves With Different Frequencies/Wavelengths

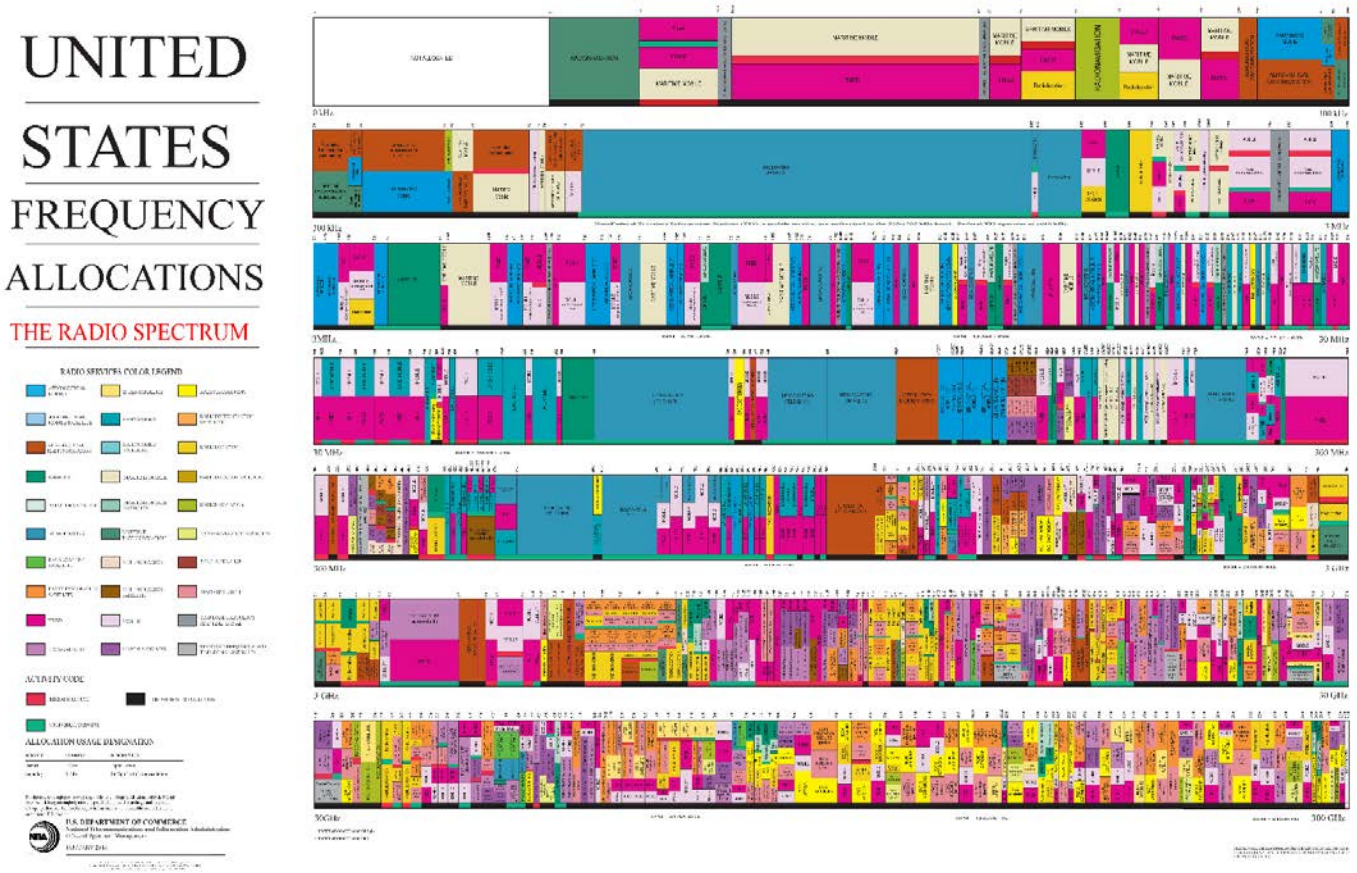


Basic Wireless Concepts

- The range of electromagnetic frequencies called the radio spectrum can be further divided into smaller and smaller increments:
  - Allocations
  - Assignments
  - Individual Channels
  - Further subdivision (e.g., signaling and payload)

Basic Wireless Concepts

U.S. Domestic Spectrum Allocations



Source: https://www.ntia.doc.gov/files/ntia/publications/january_2016_spectrum_wall_chart.pdf

Basic Wireless Concepts

- Spectrum Sharing and Interference
  - Spectrum can be shared in three dimensions: frequency, space and time
  - Some interference (“spillover”) in each spectrum dimension is unavoidable in a practical sense
  - Managing interference is a key element of spectrum management
  - Four basic steps in spectrum management include allocation, service rules, assignments, and enforcement

Basic Wireless Concepts

- Characteristics of Different Frequencies
  - Some Factors Vary with Frequency
    - How fast the wave weakens with distance
    - Size of efficient antennas
    - Ability of the waves to penetrate buildings
    - Ability of the waves to penetrate through trees and other vegetation
    - Reflectivity of various objects to the waves
    - Refractivity
    - Doppler shift due to motion
  - Leads to Notion of “Beachfront Property”

Basic Wireless Concepts

- Sources of Interference and Noise Beyond "Spillover" from Existing Systems
  - Natural Interference (e.g., static from lightning)
  - Intentional Radiators (e.g., jammers)
  - Unintentional Radiators (e.g., microwave oven leakage)
  - Incidental Radiators (e.g., unlicensed garage door openers)
  - Passive Monitoring*

Wireless and Cybersecurity

- CIA - a cybersecurity framework
  - C – Confidentiality
    - Ensure that data access is restricted to authorized entities
    - *Example attack: data breach*
  - I – Integrity
    - Prevent data modification or deletion by unauthorized entities
    - *Example attack: Stuxnet*
  - A – Availability
    - Ensure access to data on demand by authorized entities
    - *Example attack: DDoS, ransomware*

Wireless and Cybersecurity

The Open Systems Interconnect (OSI) Model

Layer	Functionality
Application	Where applications live
Presentation	Formats for communication
Session	Sets up and takes down connections
Transport	Reliable receipt of messages
Network	Routes data over multiple links
Link	Transmits/receives data reliably over a link
Physical	Communications medium: fiber, wire, RF

Wireless and Cybersecurity

- Wireless is like person A shouting to person B across a room
  - Everyone can hear what you're saying (confidentiality risk)
  - 'Man-in-the-middle' could impersonate A (integrity risk)
  - Room noise may prevent B from hearing A (availability risk)
- How do you secure something that everyone has access to?

Wireless and Cybersecurity

Types of attacks on wireless systems:

- **Sniffing** – listening to wireless traffic for unencrypted data
  - *Example: wifi sniffers collect usernames and passwords on open networks*
- **Spoofing** – one user masquerades as another
  - *Example: CU generating fake presidential alerts; IMSI catchers (Stingrays)*
- **Jamming** – deliberate interference with ‘noisier’ signal
  - *Example: military ‘barrage’ jamming; interfering with particular packets*
- **Big Data** – Integration of multiple sources over time/space
  - *Example: ‘pattern of life’ analysis to determine identities or activities*

Wireless and Cybersecurity

The world is becoming increasingly wireless. Does this increase risks?

Some plausible scenarios – now and in the near future

- Intercept a wifi signal to eavesdrop through an IoT device
- Lose passwords to a wifi sniffer
- Re-route an autonomous vehicle using GPS spoofing
- Cause an accident on the Intelligent Transportation System by jamming or spoofing intervehicle communications
- DDoS attack on critical, wireless-dependent infrastructure
- Others?

Wireless and Cybersecurity

Summary

- The world is becoming increasingly dependent on wireless
  - Reduce capital expenditures by not installing wires/fiber
  - Some analysts predict 90% of IP addresses will be connected via wireless
- Wireless presents unique vulnerabilities:
  - Medium is fundamentally broadcast in nature
  - The medium is accessible to anyone – friends, adversaries, pranksters, ….
  - Cannot isolate wireless systems behind a firewall
  - Difficult to tell if an attack is taking place
- Need to identify/analyze attack vectors and mitigate risks
  - Quantify likelihood vs. severity
  - Prioritize responses
  - Allocate resources

Questions?