CSE570 Spring 2020

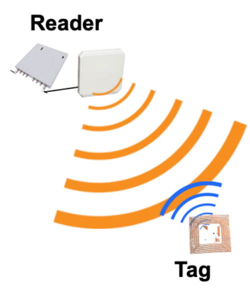
Wireless and Mobile Networks

RFID, NFC, Backscatter

1

RFID

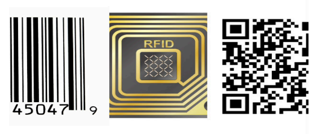
- Radio Frequency IDentification (RFID) is a method of remotely storing and retrieving data using devices called RFID tags and RFID Readers

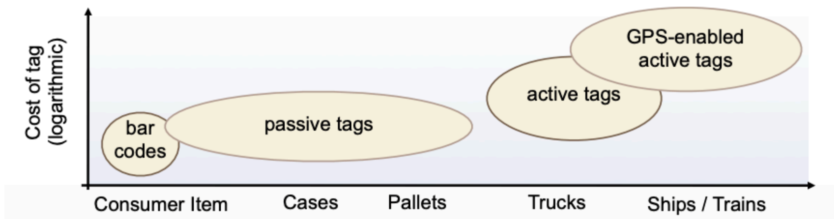


2

Automated Identification

- Bar codes, QR codes, NFC etc.
- Variety of Tags in the Market





3

RFID Tags in Use

4

Types of RFID Tags

- RFID Reader Tag

- **Passive Tags: rely on an external energy source to transmit**
  - » In the form of a reader that transmits energy
  - » Relative short range
  - » Very cheap
- **Active Tags: have a battery to transmit**
  - » Has longer transmission range
  - » Can initiate transmissions and transmit more information
  - » A bit more like a sensor
- **Battery Assisted Passive tags are a hybrid**
  - » Have a battery transmit
  - » But need to be woken up by an external source

5

RFID Characteristics

Band	Regulations	Range	Data speed	ISO/IEC 18000 section	Remarks	Approximate tag cost in volume (2006) US $
120–150 kHz (LF)	Unregulated	10 cm	Low	Part 2	Animal identification, factory data collection	$1
13.56 MHz (HF)	ISM band worldwide	10 cm–1 m	Low to moderate	Part 3	Smart cards (ISO/IEC 15693, ISO/IEC 14443 A, B). ISO-non-compliant memory cards (Mifare Classic, iCLASS, Legic, Felica ...). ISO-compatible microprocessor cards (Desfire EV1, Seos)	$0.50 to $5
433 MHz (UHF)	Short range devices	1–100 m	Moderate	Part 7	Defense applications, with active tags	$5
865–868 MHz (Europe) 902–928 MHz (North America) UHF	ISM band	1–12 m	Moderate to high	Part 6	EAN, various standards; used by railroads[16]	$0.15 (passive tags)
2450–5800 MHz (microwave)	ISM band	1–2 m	High	Part 4	802.11 WLAN, Bluetooth standards	$25 (active tags)
3.1–10 GHz (microwave)	Ultra wide band	Up to 200 m	High	Not defined	Requires semi-active or active tags	$5 projected

Do you see any discrepancy?

6

RFID Working Principle

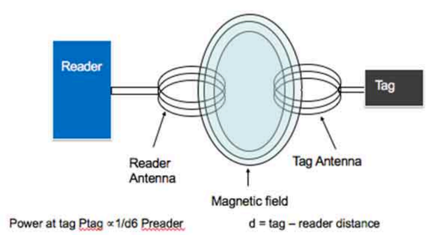
- LF & HF: Inductive coupling
- UHF: Propagation/Backscatter coupling

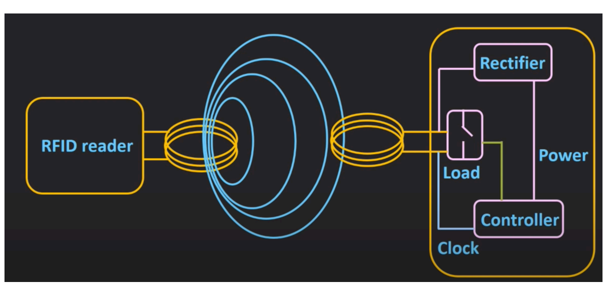
- Coupling definition
  - The transfer of energy from one medium to another medium

7

Inductive Coupling (Near field)

- Shared magnetic field
- Load Modulation

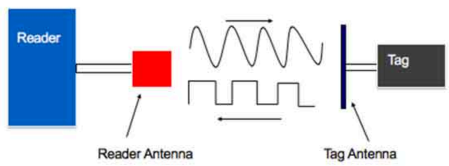




8

Backscatter Coupling (Far field)

- The energy is received by the tag antenna and a small amount energy is then reflected back to the reader
- Backscatter modulation



- UHF (915MHz) : Far field propagation : Pt ∝ 1/d2

9

Near Field vs Far Field

- Within the near-field, the magnetic field intensity decays rapidly as $1/d^3$
- When the magnetic field strength is translated into power available to the tag, the power attenuates according to $1/d^6$
- In the far-field the power at the tag is attenuated to $1/d^2$

10

RFID PHY Layer

- Depends on the frequency band used
- Different modulations used by reader and tag
  - Different constraints, e.g. power and complexity

11

RFID MAC Layer

- Typically assumed that only one reader is present, i.e. no need for MAC on the reader
- MAC for tags is a challenge: very high concentrations of tags are present in many contexts
  - And tags are dumb, i.e. cannot have sophisticated protocols
- Two types of schemes used (standard)
  - Aloha
  - Remember tag IDs

12

NFC

- One device combines the functionality of
  - An RFID reader device
  - An RFID transponder (tag)
  - Bit rates ranging from 106 Kbs to 424 Kbs
- Operates at 13.56 MHz (High frequency band) and is compatible to international standards
- Use of NFC is growing fast
  - Driven by NFC Forum (founded by Nokia, Philips, and Sony in 2004)

13

NFC Devices

Example: contactless payment applications
Sony FeliCa, Asia
MIFARE, Europe
Google Wallet


(c) Google

Modes of operation

- **Smart Card emulation (ISO 14443):**
  - » Phone can act as a contactless credit card
  - » Information can be generated rather than pre-stored
- **Reader mode**
  - » Allows NFC devices to access data from an object with an embedded RFID tag
  - » Enables the user to initiate data services, i.e., retrieval of rich content, advertisements, ..
- **Peer-to-peer (ISO 18092)**
  - » Allows two way communication between NFC devices
  - » NFC can act as smart tag, i.e., generates information

14

Applications

RFID
- Retail
- Logistics
- Supply chain management
  - » accurate inventories
  - » product safety and quality

NFC
- Mobile payment
- Mobile ticketing
- Pairing of devices (esp. Bluetooth devices)
- Download of information from "smart posters"

15

Some Concerns

- RFID tags raise a number of security concerns:
  - » Privacy risks, e.g., eavesdropping
  - » Cloning and forging of tags
- Specific disadvantages due to tag limitations
  - » Encryption algorithms are too complex to be implemented on tags
- But also specific advantages:
  - » Tags are slow to respond, maximum no. of read-out operations
  - » Adversary has to be physically close

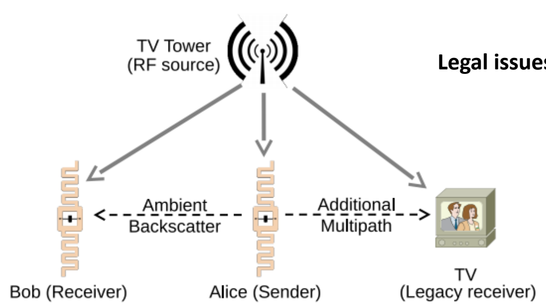
16

Backscatter Communication

- Backscatter
  - The reflection of waves, particles, or signals back to the direction from which they came.
- Ambient backscatter
  - Signals are everywhere (e.g., TV, WiFi, Cellular)
  - Doesn’t require specific power infrastructure
  - Works by modulating the reflection of an existing RF signal
  - No interference with legacy devices

17

Ambient Backscatter



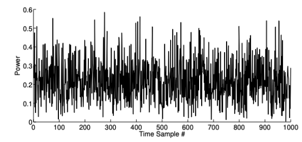
Legal issues in licensed spectrum?

- Communication between two battery-free devices. One such device, Alice, can backscatter ambient signals that can be decoded by other ambient backscatter devices.
- To legacy receivers, this signal is simply an additional source of multi-path, and they can still decode the original transmission.

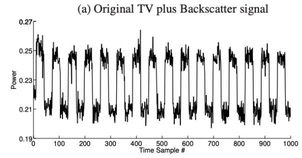
18

Ambient Backscatter Challenges

1. The ambient signals are controlled by the sender, TV, WiFi, etc.
   a) Variational signal
   b) Signal encoded
   Solution: slow down the ambient signal. How?
   a) Average the received signal across multiple samples.



(a) Original TV plus Backscatter signal



(b) Signal After Averaging

2. Averageing digital samples requires data conversion (A/D): energy costive.
   Solution: Use RC circuit.

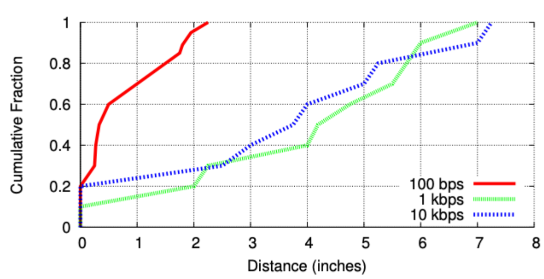
3. Collision if many devices need to share the channel.
   Solution:
   a) Devices can decode each other's transmissions.
   b) Energy detection by leveraging the property of the analog comparator.

19

Ambient Backscatter Performance

	Tx	Rx
Ambient Backscatter	0.25uW	0.54uW
Traditional Backscatter	2.32uW	18uW

Less power consumption



Interference when close to legacy receivers

20

Scaling Backscatter Networks

https://www.usenix.org/system/files/nsdi19spring_hessar_prepub.pdf

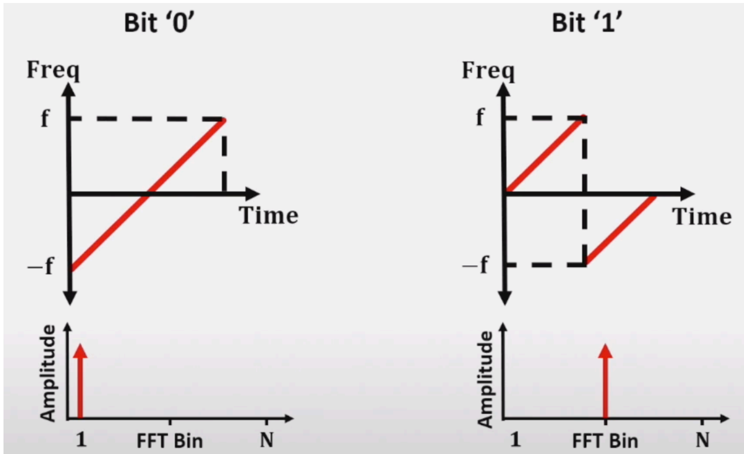
21

Scaling Backscatter Networks

- NetScatter
  - Hundreds of backscatter tags having concurrent transmissions
  - A Distributed Coding mechanism
    - Chirp spread spectrum
  - Time synchronization issue
  - Near-far problem
  - A deployment of 256 tags

22

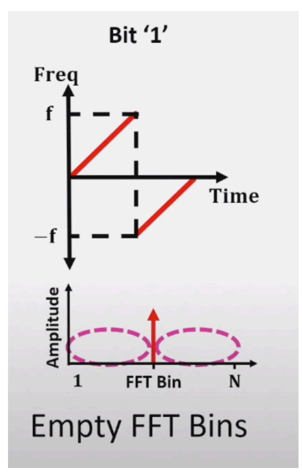
Let's Revisit Chirp Spread Spectrum from LoRa



23

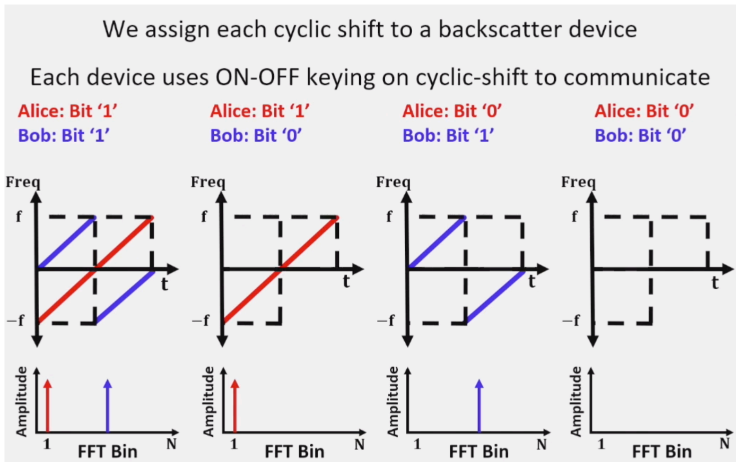
Leveraging Chirp Spread Spectrum (CSS)

- Key insight: there is only one peak at each time step
- Idea: Can we make different tags to use different frequencies at the same time, so that each of their transmissions fall in different bins?



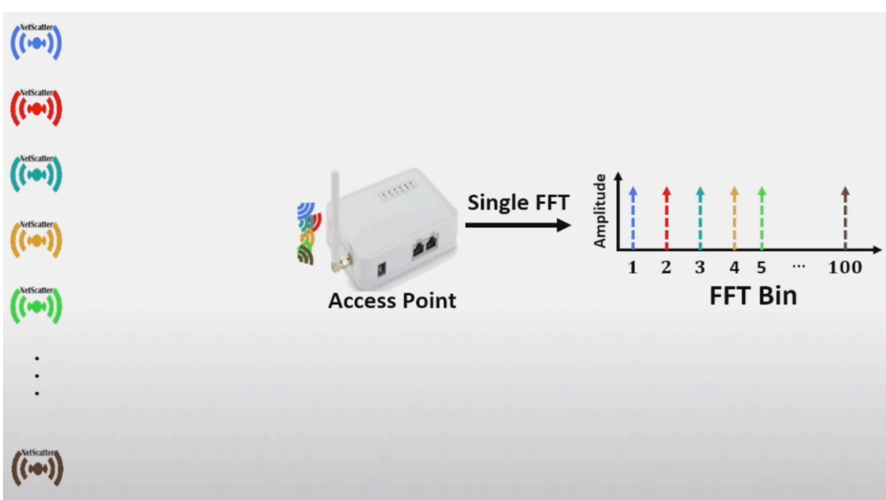
24

Distributed CSS



25

Distributed CSS



26

How Many Concurrent Txs?

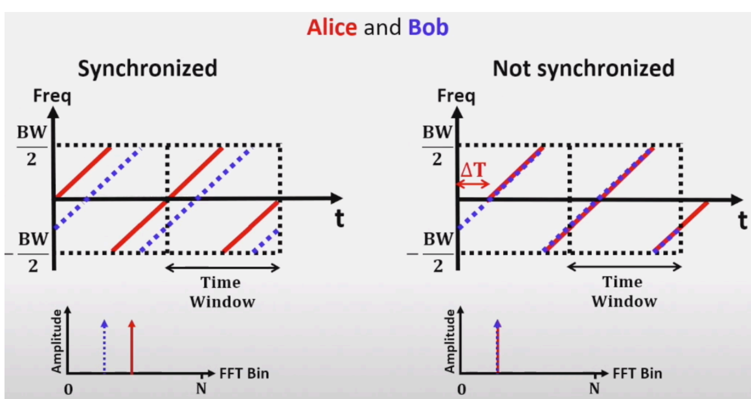
Typical LoRa configuration

- Uses 500 kHz BW
- 512 cyclic-shifts

Theoretically, we can support 512 concurrent transmissions using only 500 kHz BW

27

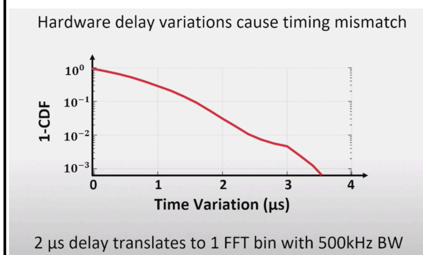
Practical Issues: Synchronization

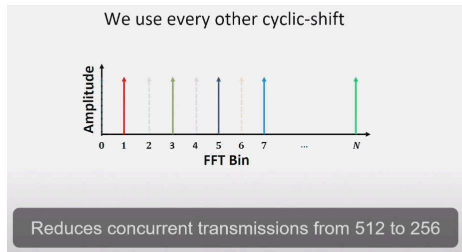


Causes interference between Alice and Bob

28

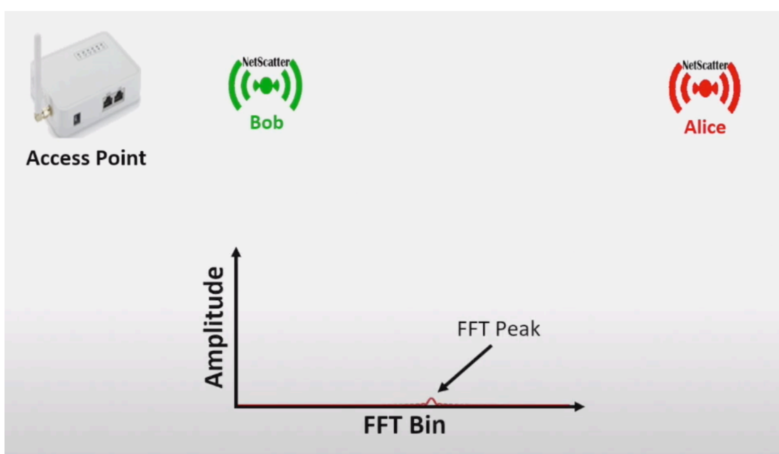
Practical Issues: Synchronization





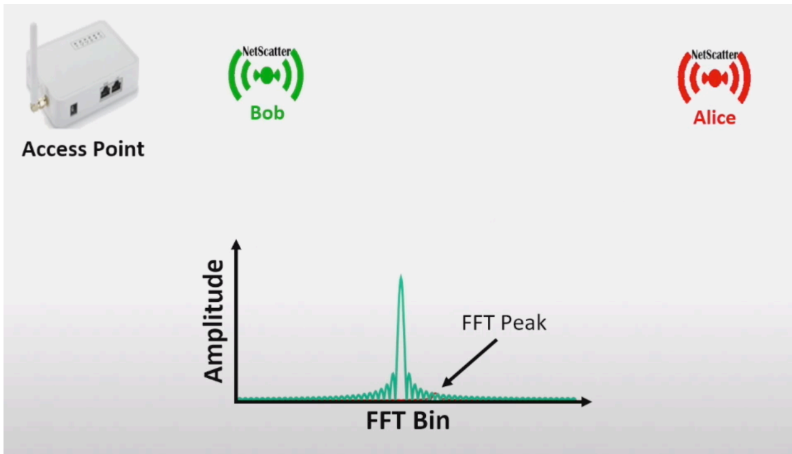
29

Practical Issues: Near-Far Problem



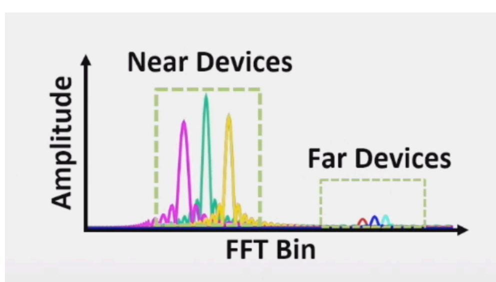
30

Practical Issues: Near-Far Problem



31

Practical Issues: Near-Far Problem



Clustering solves the problem

32

Summary

- RFID/NFC
- Near Field Vs. Far Field
- Backscatter
- Ambient Backscatter
- Scaling Backscatter Networks

33