CS598 Lecture 15

Backscatter Ideas

- Wi-Fi and other network technologies consume considerable power, with Wi-Fi using around 100 mW, while LTE/5G uses roughly 1 watt.
- Design low power Wi-Fi→ transmit really low power OFDM signals
  - Trade-off: lower range, lower SNR, lower data rate

RFIDs

- Stands for low frequency identification.
- Relies on small, battery-free tags that reflect high-power signals sent by specialized RFID readers to communicate data without needing a power source
- How it works:
  - Specialize reader (RFID reader in high power) transmit high power signal to Rx that have small chip with antennas.
  - Rx reflects signal back as square wave, therefore not necessary to generate its own power
    - Reflect → `1`
    - No reflect → `0`
  - RFIDs get 1, 0 sequence from the tag

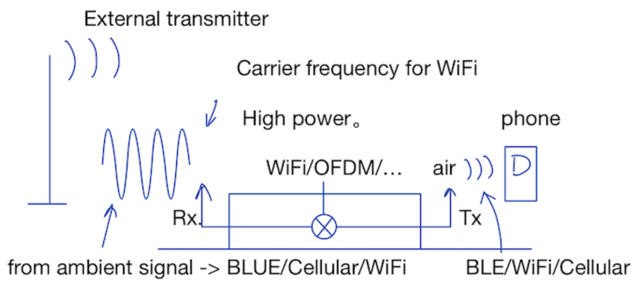
Medium Access

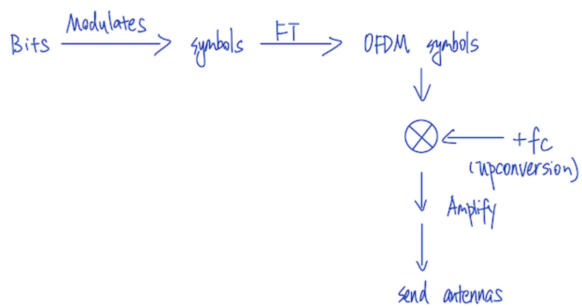
- Common forms of RFID used: EPC gen2/3
- Tx (Reader): Send a query message to multiple Rx
  - If there are only 3 RFIDs
  - Step 1. The reader pick one of slots from 0 to 3

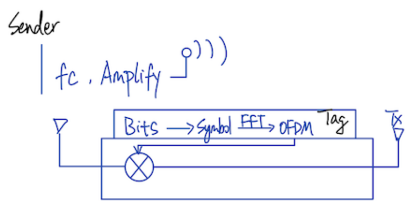
- Step 2. Each RFID pick one slot from 0 to 3.
    - If collisions in Rx exist, there must be at least 2 RFIDs picked the same slot.
    - The reader would double the size of the slots for free collision (i.e. the reader back-off the slot from 0 to 7)
- Pros:
  - Low power
  - Battery-free
  - Cost is cheap (each tag costs about 10 cents)
- Cons:
  - Specialized hardware
    - Need to have the RFID reader

Ambient Backscatter

- Can I have the RFID or zero power tag to be read from normal devices?
- Backscatter → Reflection-Based
- One version of Backscatter
  - Idea: Because we have many wireless signals like Wi-Fi or cellular networks, can we
    1. Harvest the energy
    2. Use them to communicate
    3. Is readable by commodity devices
  - You want your tag can be identify, and modulated, readable







- You have a external transmitter which transform a single carrier frequency for Wi-Fi in high power
- The tag: receive the signal, mixed Wi-Fi/OFDM/..., and send this over the air, and change it into Wi-Fi signal.
    - A little bit more expensive, but not much
- How to get from ambient signals? → Bluetooth / Cellular / Wi-Fi
- How to make transmit readable? → Wi-Fi / Cellular
- The tag only do from bits to OFDM symbols
    - The tag doesn’t need to reduce the carrier frequency of the signal since the device it would do it by itself.
    - The RFID tag only change the symbol format
- Pros: You can use off-the shelf reader (1 Mbps)

- Cons: You still need some external source.

WiTag

- Goals:
  - Compatible with existing Wi-Fi access points
  - Encryption
  - Battery-free
  - (We are okay with low throughput / inefficient design)

Frame Aggregation

- Initial design: Spend lots of time waiting
- To avoid overheads such as performing channel sensing and transmitting an acknowledgment per frame, multiple MAC Protocol DATA Units are combined into a larger aggregated frame and therefore improve the efficiency of the MAC layer.

Wi-Tag: Idea

App 1 App 2

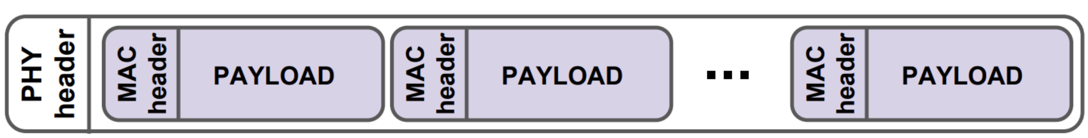
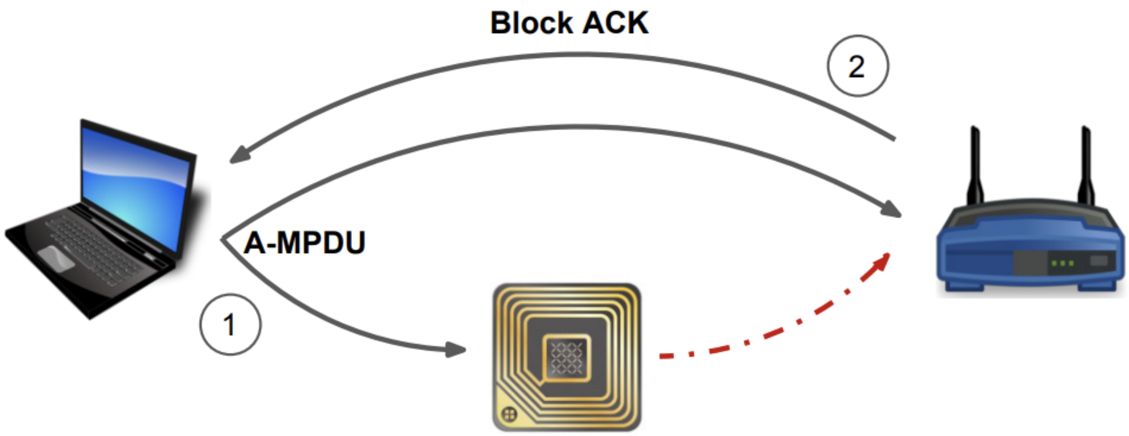


Figure 1: 802.11n/ac A-MPDU structure

- Each data unit has its own payload.



- **Overview:** WiTAG's tag selectively interferes with subframes in a query packet transmitted by a client to an access point. Then, the client device obtains the tag's data from the block ACK.
- Send all the packets in one packet
    - Aggregate packets in different application into one packet to send.
- Send the string like `1001` from the receiver (Block ACK)
    - 1 is the packet the receiver get, so the sender knows that no need to send that packet again.
    - 0 is the packet the receiver did not get, so the sender need to send that packet again.
- Issue: inefficient

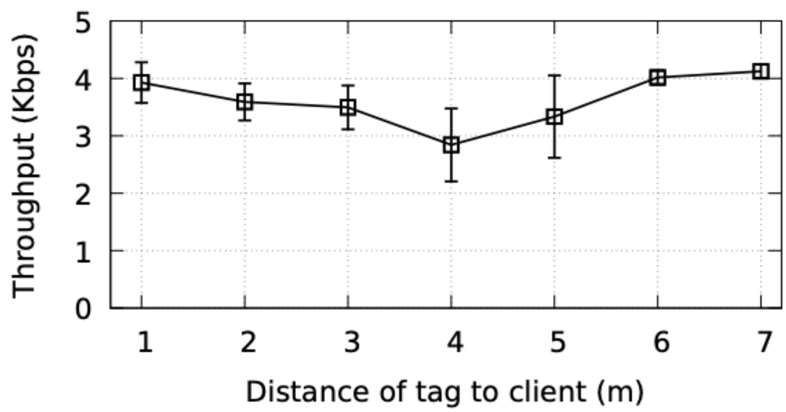
Corrupting Packets

- Computer x → h → AP y (direct channel = h)
- Computer x → h' → tag → h' → AP y (from tag: channel = h')

$$y = hx + h'x + n = (h + h')x + n$$

- Reflecting → $(h + h')x$
- Not Reflecting → hx Phase Difference = $\frac{|h'|}{h}$

- Phase states → off by 180′ $\frac{h+h'}{h-h'}$ Phase Difference = $\frac{2h'}{h}$
- Using a high Modulation → 64 / 128QAM
  - Even a small mistake/shifts in signal amplitude or phase can cause a great noise and lead to bit errors.
- Distances between the client and the AP have to be small (~5m)



(b) Throughput

  - Throughput become small since the tag is far away from both of AP and the client.
  - In the middle, we don't have the ability to change the power and can't flip bits easily→ increase the error rate and decrease the throughput.

$$SINR = \frac{P_{client}}{P_{Tag} + P_{Noise}}$$

$$P_{Tag} = \frac{\alpha}{D^2_{Tagclient} D^2_{TagAP}}$$

  - If the reflector is between the sender and receiver, then $D_s + D_r$ is constant and is equal to the distances between the sender and receiver.
  - Therefore, because the strength of the reflected signal (received at the receiver) is minimized, the BER is slightly increased.

- Pros
  - Works with existing hardware
- Cons
  - Not efficient
  - Low throughput
  - Low range
  - Interrupts actual data transmitting → waste the other resources
  - Normal losses