LECTURE 4

Medium Access Control

Introduction

- What is medium access?
  - Who gets to transmit? How? When?
  - Multiplexing
    - How many stations can share a single link
      - FDMA, TDMA, CDMA in circuit switched voice networks
      - CSMA/CD in Ethernet (simplicity)
  - Duplexing
    - How communication from station A to station B is separated from the communication from station B to station A
    - FDD or TDD
- Impact of architectures
  - Infrastructure – centralized, fixed base station
  - Ad hoc – distributed, peer-to-peer
- Simplicity and overhead

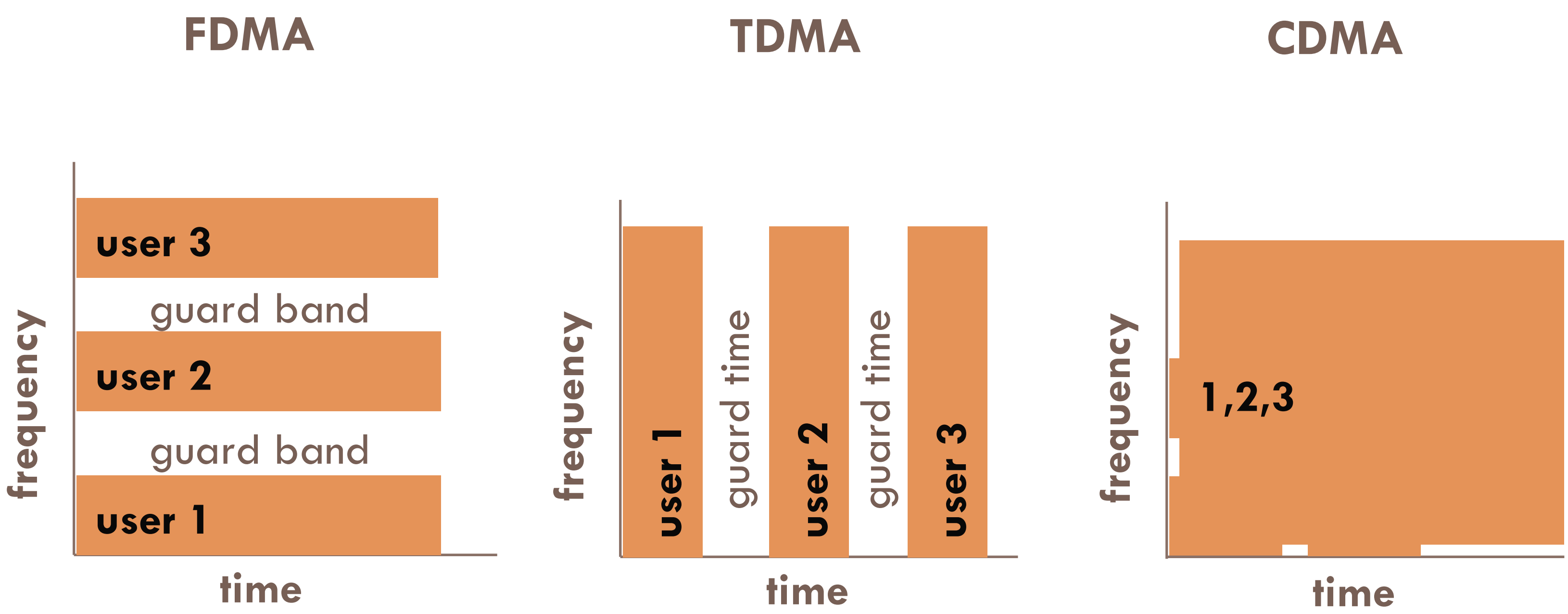
Duplexing Modes

- Simplex – one way communication (e.g., broadcast AM)
- Duplex – two way communication
  - TDD – time division duplex
    - Users take turns on the channel
  - FDD – frequency division duplex
    - Users get two channels – one for each direction of communication
      - For example one channel for uplink (mobile to base station) another channel for downlink (base station to mobile)
  - Half-duplex
    - As in 802.11, a device cannot simultaneously be transmitting and receiving

Centralized Multiple Access Techniques

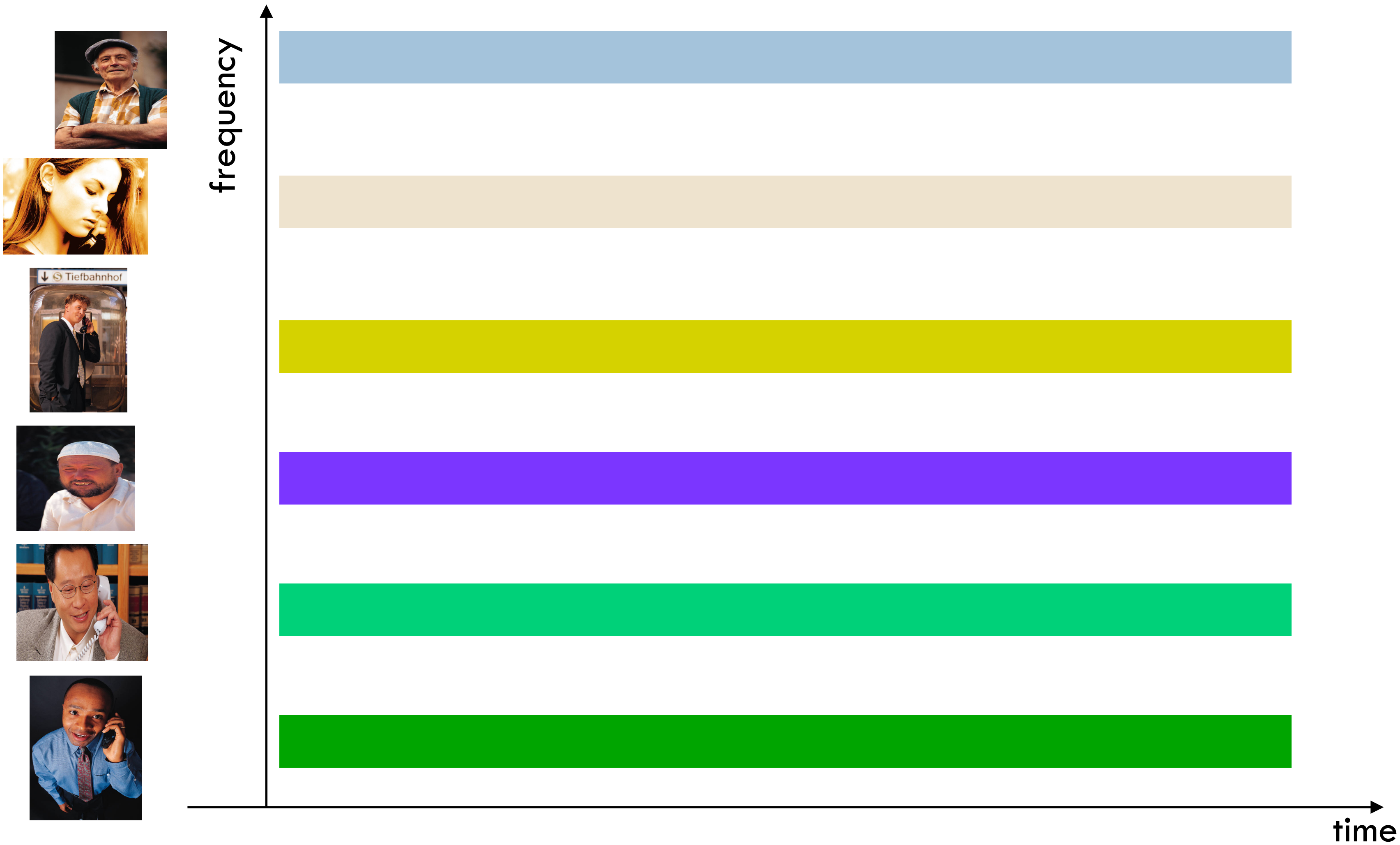
- FDMA (frequency division multiple access)
  - Separate spectrum into non-overlapping frequency bands
  - Assign a certain frequency to a transmission channel between a sender and a receiver
  - Different users share use of the medium by transmitting on non-overlapping frequency bands at the *same time*
- TDMA (time division multiple access):
  - Assign a fixed frequency to a transmission channel between a sender and a receiver for a certain amount of time (users share a frequency channel in time slices)
- CDMA (code division multiple access):
  - Assign a user a unique code for transmission between sender and receiver, users transmit on the same frequency at the same time

Multiple Access (cont)

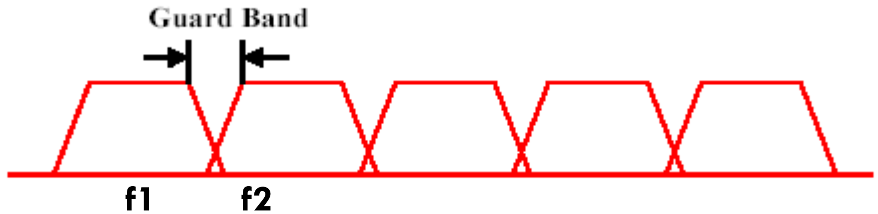


Wireless systems often use a combination of schemes; GSM – FDD/FDMA/TDMA

Frequency division multiple access

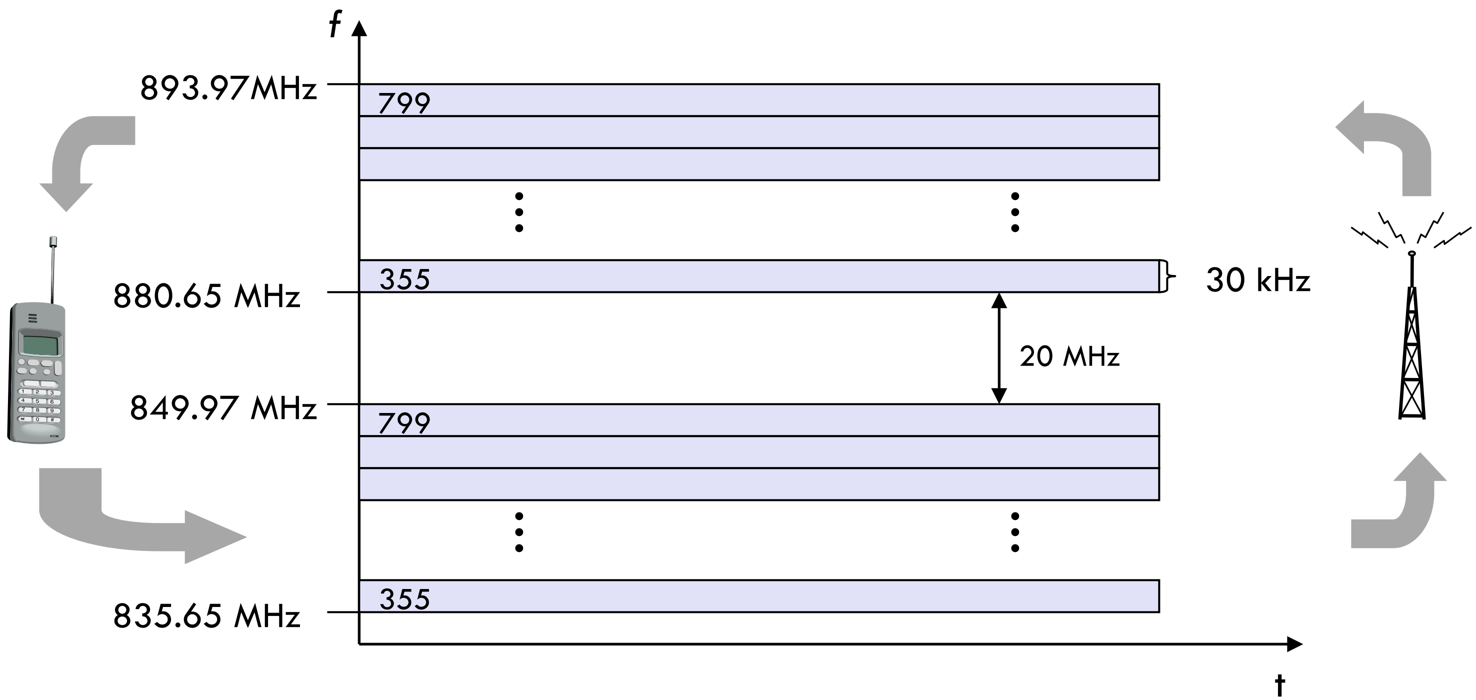


FDMA



- FDMA – simplest and oldest
- Band of width *F* is divided into *T* non-overlapping frequency channels
  - Guard bands minimize interference between channels
  - Each station is assigned a different frequency
- Can be inefficient if more than *T* stations want to transmit or traffic is bursty
  - Results in unused bandwidth and delays
- Receiver requires high quality filters for adjacent channel rejection
- Used in First Generation Cellular (AMPS, NMT, TACS)

FDD/FDMA - general scheme, example AMPS (B block)

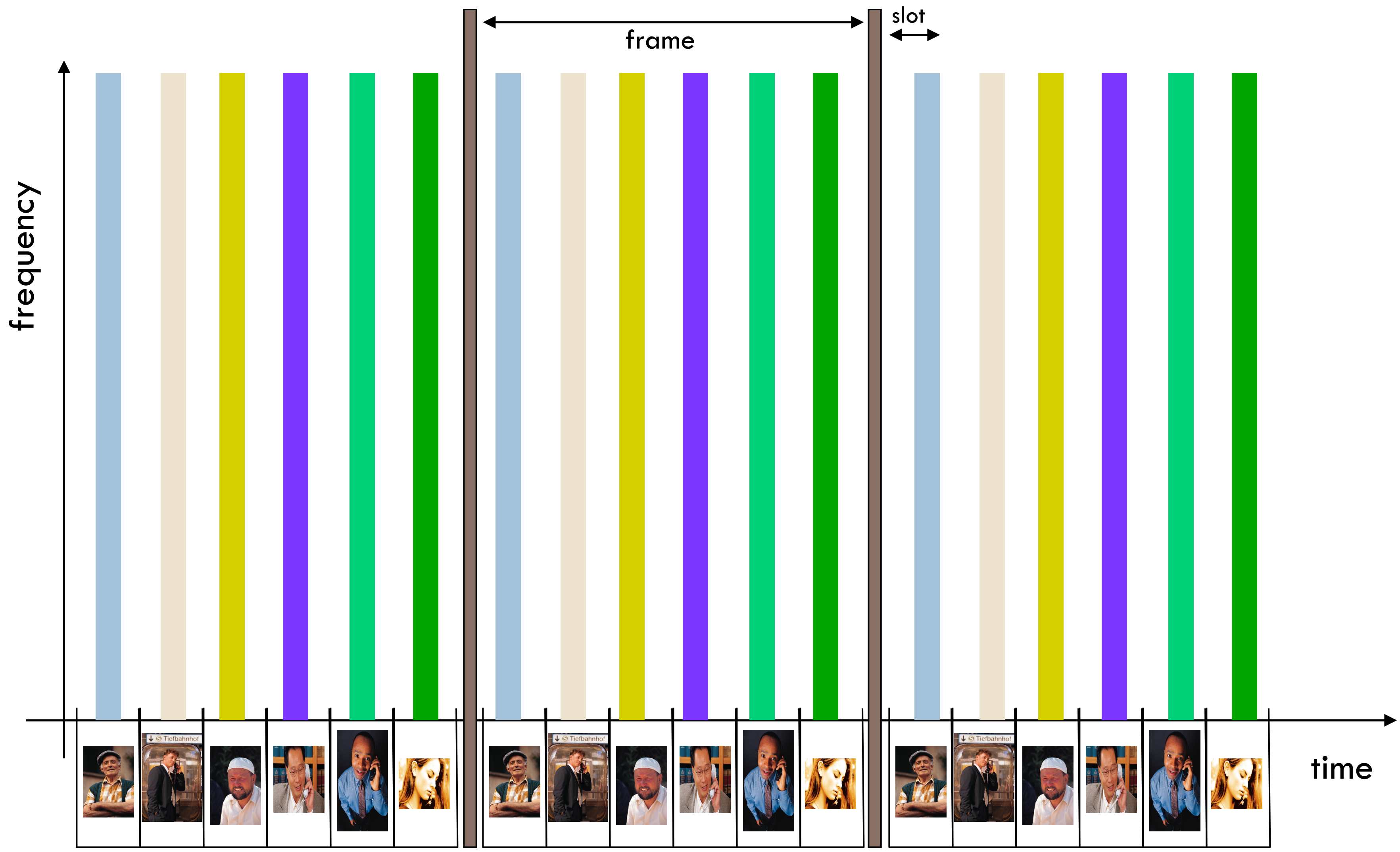


f(c) = 825,000 + 30×(channel number) kHz <- uplink

f(c) = f uplink + 45,000 kHz <- downlink

In general all systems use some form of FDMA

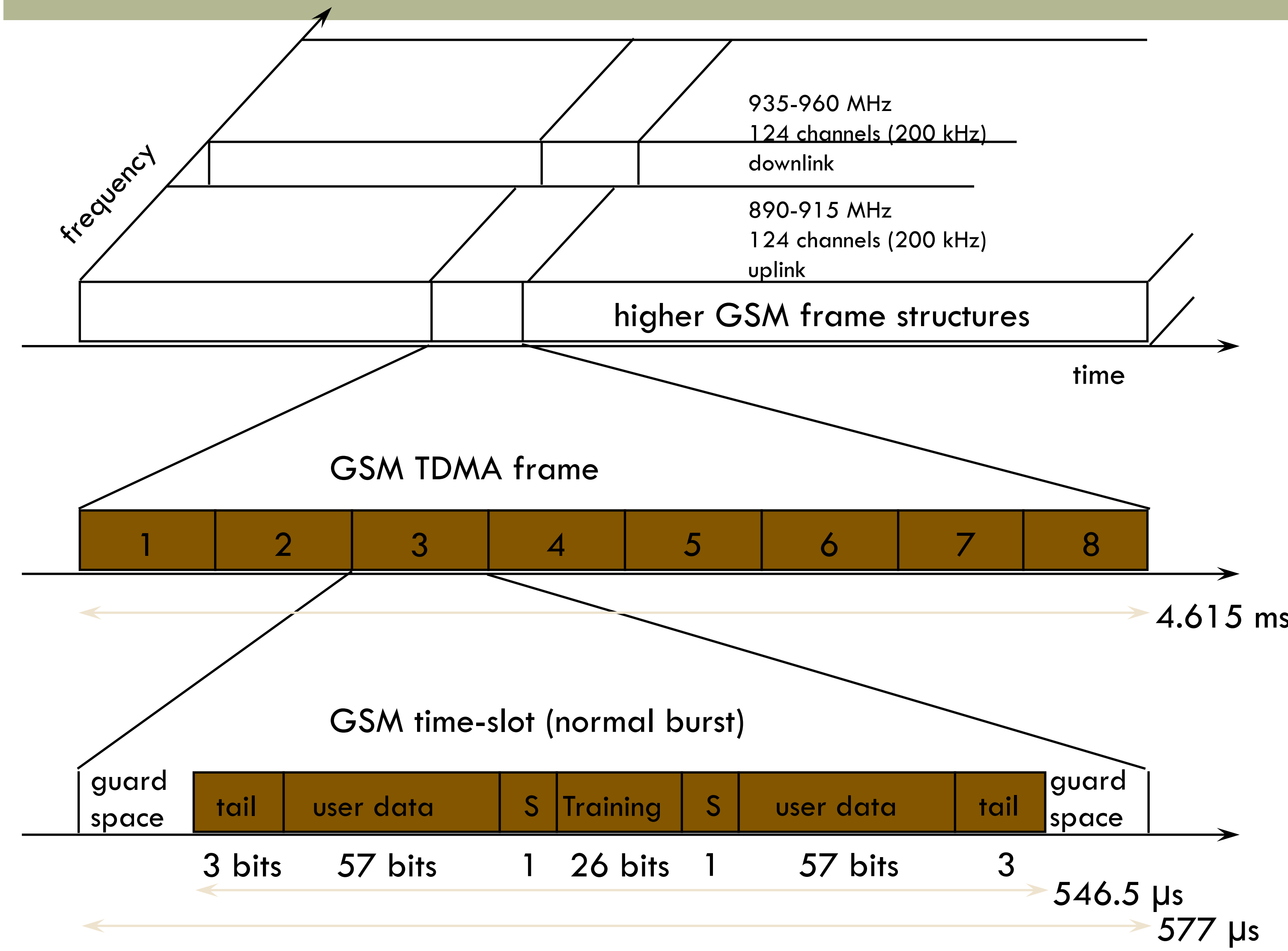
Time Division Multiple Access



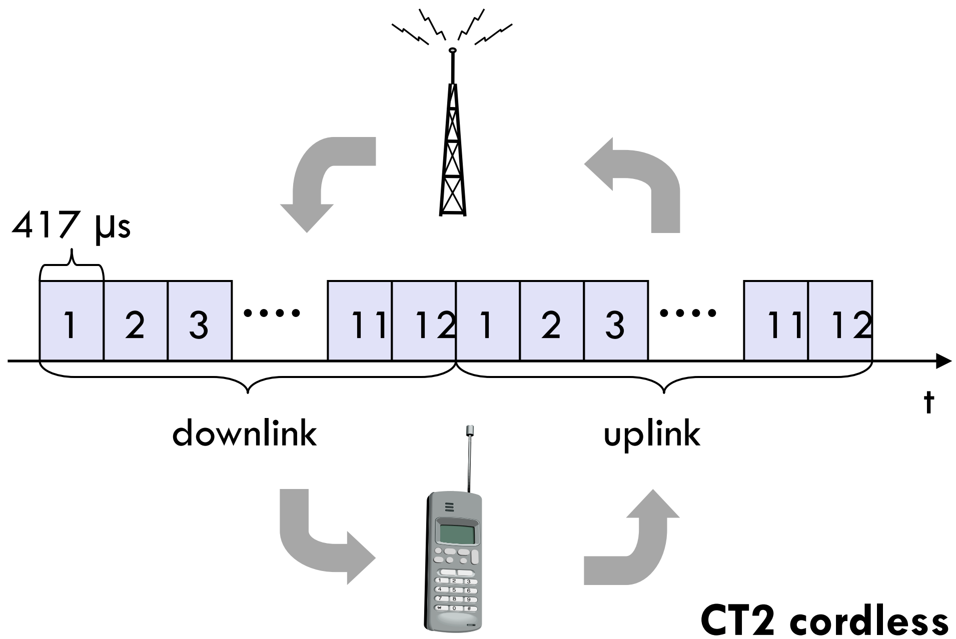
TDMA

- Users share same frequency band in non-overlapping time intervals,
  - E.g. Round robin
- Receiver filters are just windows instead of bandpass filters (as in FDMA)
- Guard time can be as small as the synchronization of the network permits
  - All users must be synchronized with base station to within a fraction of guard time
  - Guard time of 30-50 μs common in TDMA
- Used in GSM, NA-TDMA, (PDC) Pacific Digital Cellular

GSM - TDMA/FDMA/FDD

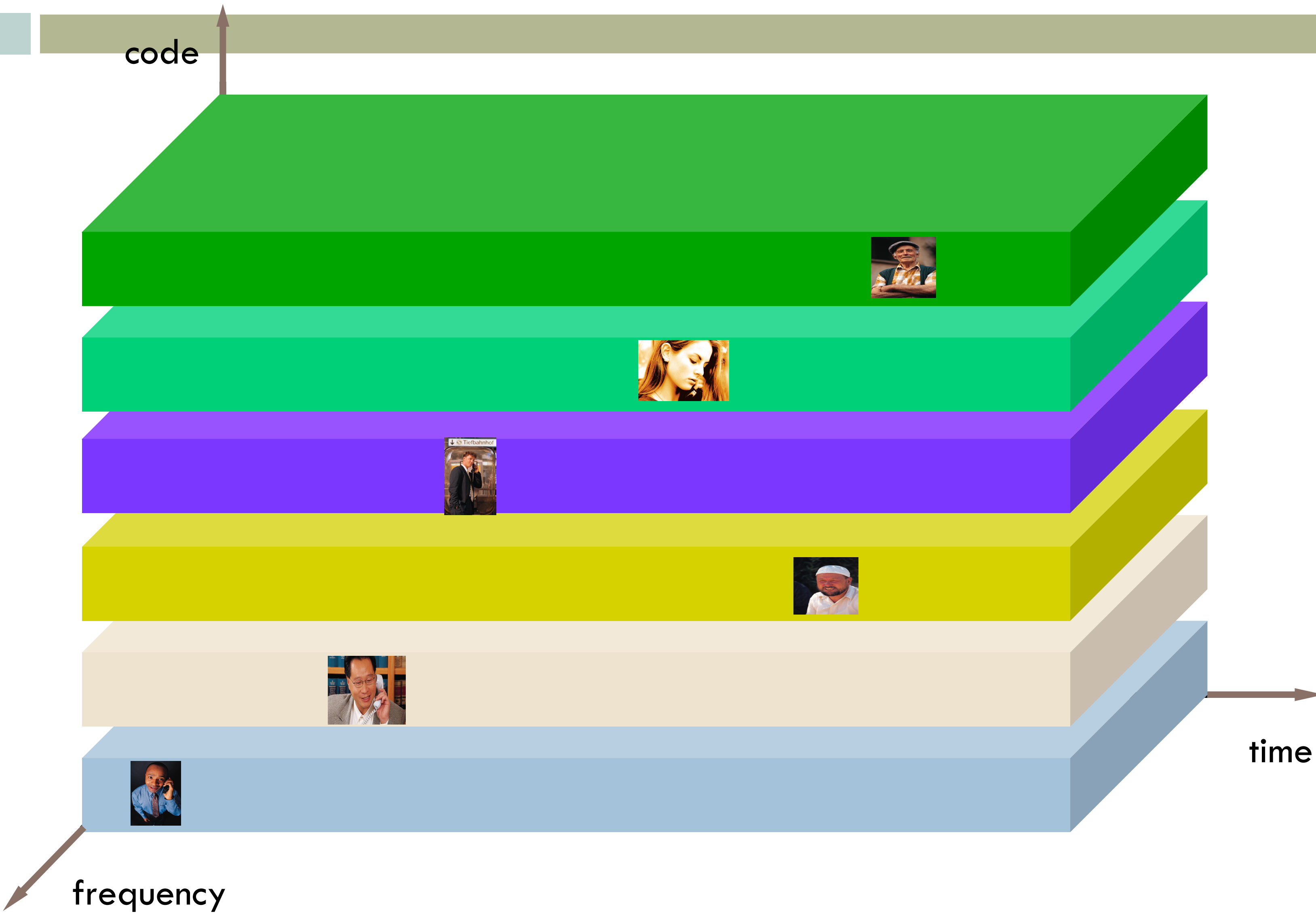


TDD/TDMA - example



CT2 cordless phone standard

Code Division Multiple Access

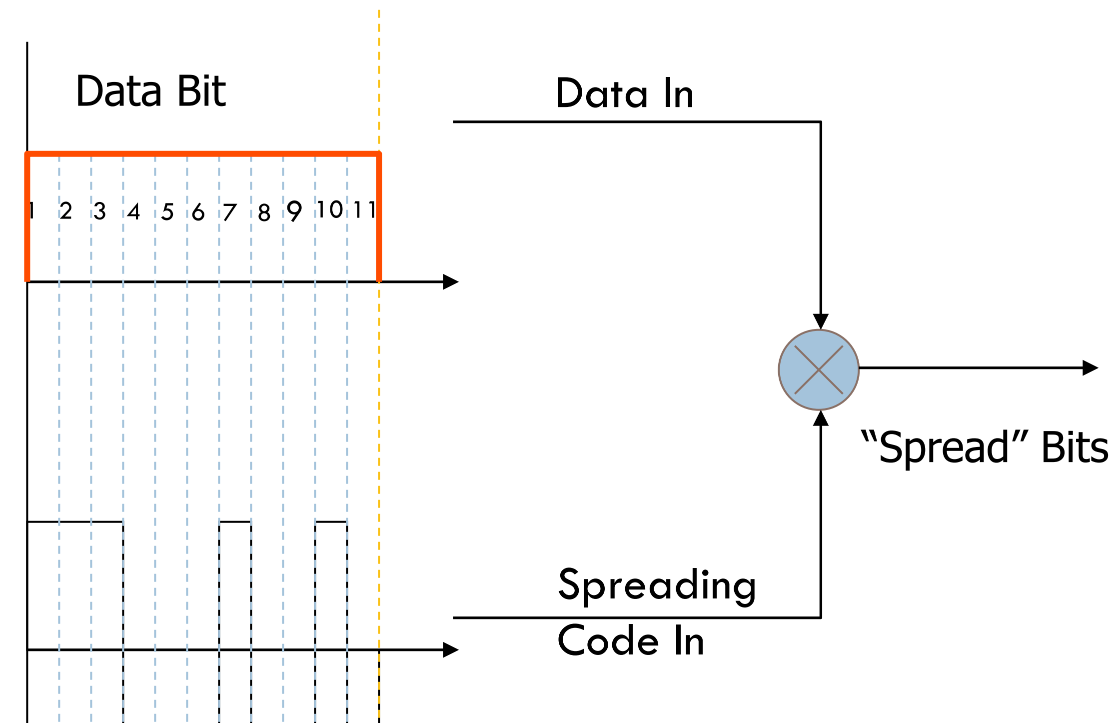


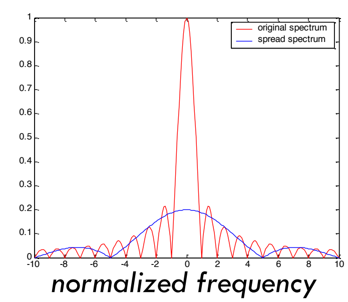
CDMA

- Narrowband message signal is multiplied by very large bandwidth spreading signal using direct sequence spread spectrum
- All users can use same carrier frequency and may transmit simultaneously
- Each user has own unique access spreading codeword which is approximately orthogonal to other users codewords
- Receiver performs time correlation operation to detect only specific codeword, other users codewords appear as noise due to decorrelation.

DSSS Modulation

- The original data stream is "chipped" up into a pattern of pulses of smaller duration
- Good **autocorrelation** properties
- Good **cross-correlation** properties with other patterns
- Each pattern is called a spread spectrum code or spread spectrum sequence
  - E.g. Walsh Code

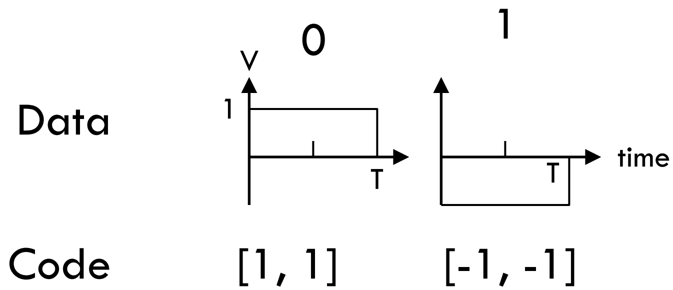


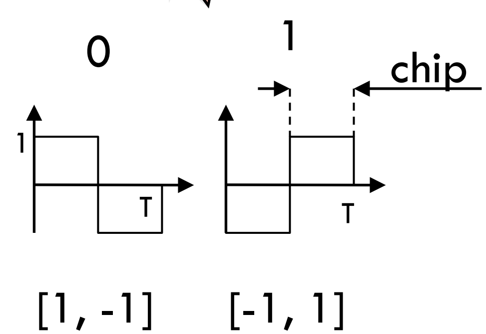


Simple example illustrating CDMA

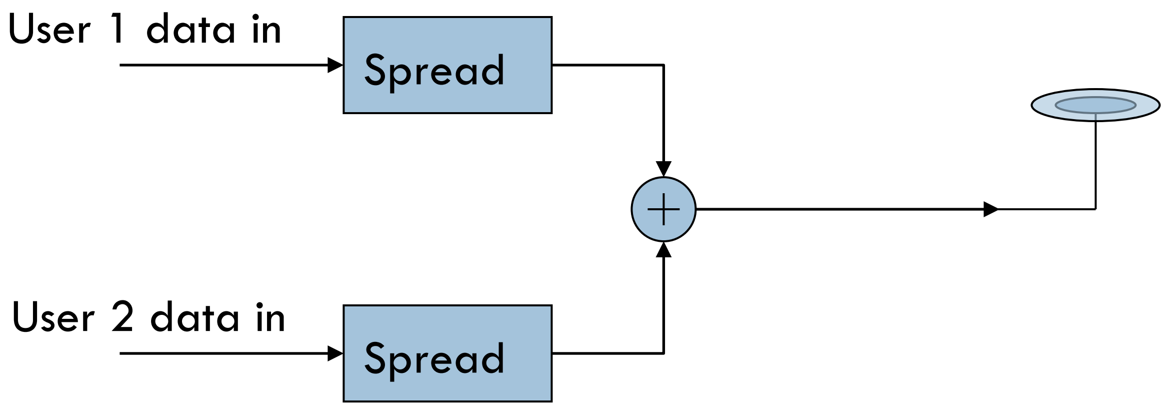
- **Traditional**
- To send a 0, send +1 V for T seconds
- To send a 1, send -1 V for T seconds
- Use separate time slots or frequency bands to separate signals

- **Simple CDMA**
- To send a 0, Bob sends +1 V for T seconds; Alice sends +1 V for T/2 seconds and -1 V for T/2 seconds
- To send a 1, Bob sends -1 V for T seconds; Alice sends -1 V for T/2 seconds and +1 V for T/2

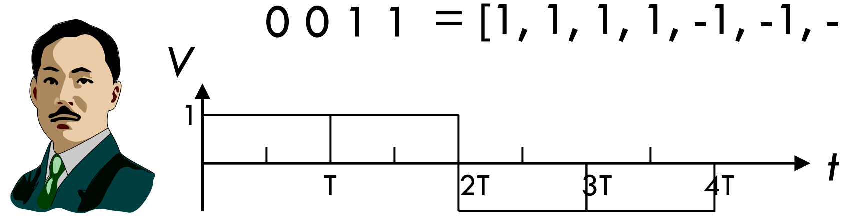




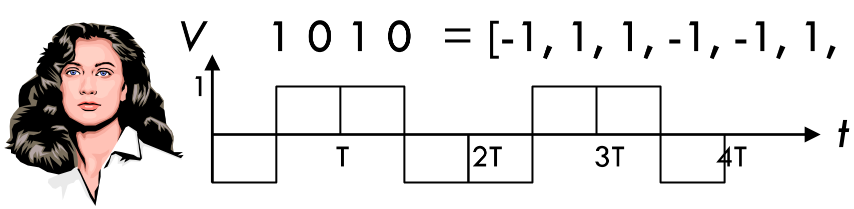
Simple CDMA Transmitter

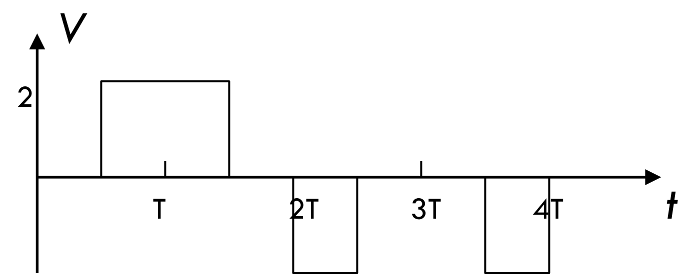


0 0 1 1 = [1, 1, 1, 1, -1, -1, -1, -1]



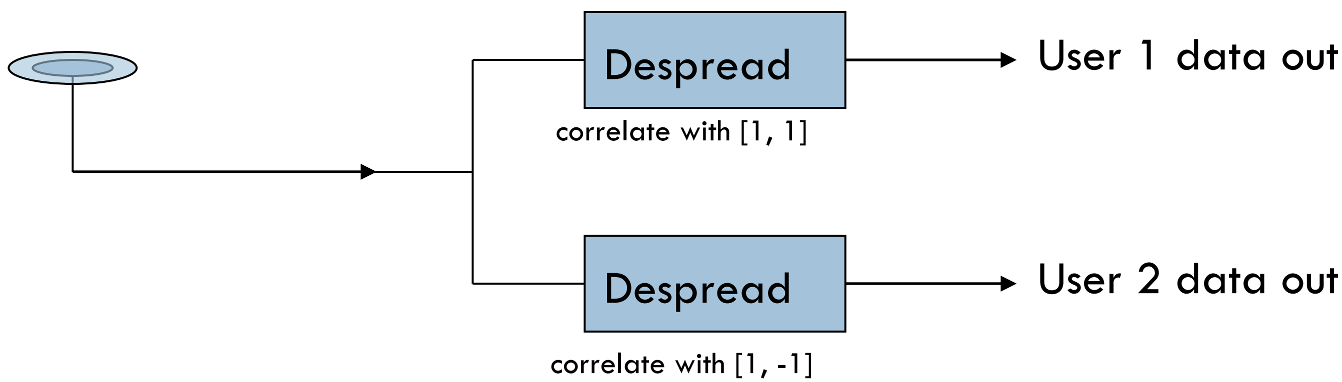
1 0 1 0 = [-1, 1, 1, -1, -1, 1, 1, -1]

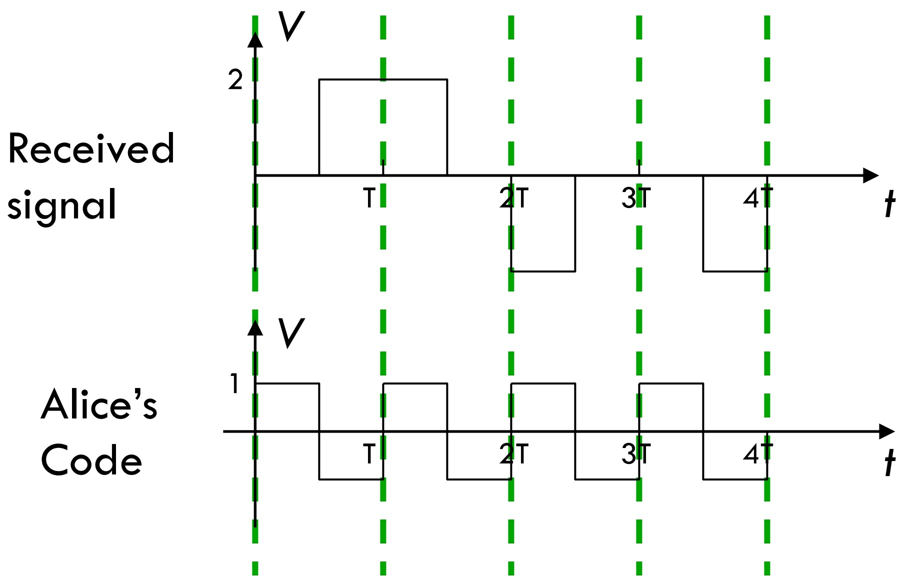


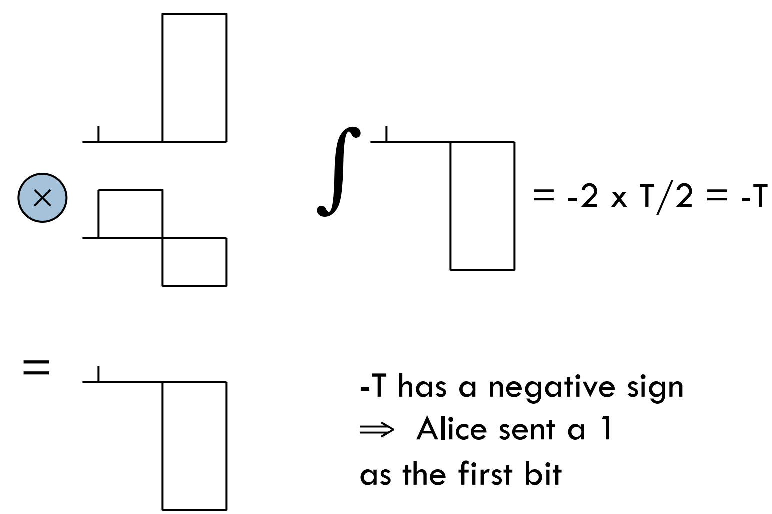


Transmitted signal

Simple CDMA Receiver







Simple CDMA continued

- Proceeding in this fashion for each "bit", the information transmitted by Alice can be recovered
- To recover the information transmitted by Bob, the received signal is correlated bit-by-bit with Bob's code [1,1]
- Such codes are "orthogonal"
  - Multiply the codes element-wise (dot product)
    - $[1,1] \times [1,-1] = [1,-1]$
  - Add the elements of the resulting product
    - $1 + (-1) = 0$ => the codes are orthogonal
- CDMA used in IS-95 standard and both 3G standards: UMTS, cdma2000
- CDMA has big capacity advantage as frequency reuse cluster size = 1

Orthogonality

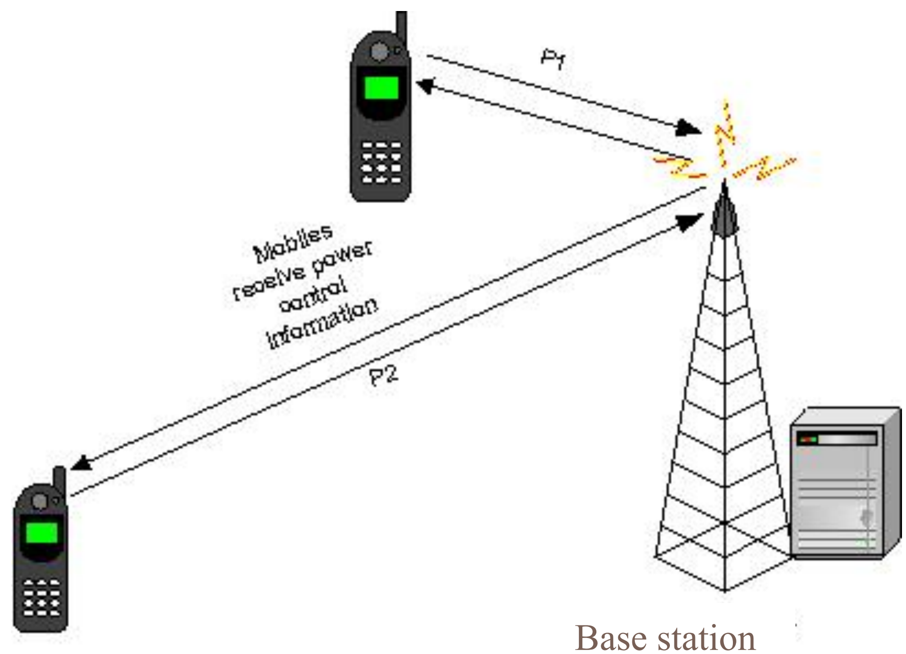
- Orthogonality important
  - High autocorrelation (dot product with itself should be high)
  - Low cross-correlation (dot product with other codes ≈ 0).
- Barker codes – [1, -1, 1,1, -1,1,1,1,-1,-1,-1] has these properties.
  - Product of Barker code with a shifted version has low value.
  - Typically used for synchronization in CDMA systems.

Impact of noise

- The decoding should be possible even if there is noise.
- Note that if there is too much noise, the decorrelation could yield erroneous results.
- Similarly if one signal is much stronger than the other, decorrelation could yield erroneous results.
  - Near far problem.

CDMA Properties: Near-Far Problem

- A CDMA receiver cannot successfully de-spread the desired signal in a high multiple-access-interference environment
- Unless a transmitter close to the receiver transmits at power lower than a transmitter farther away, the far transmitter cannot be heard
- Power control must be used to mitigate the near-far problem
- Mobiles transmit at such power levels to ensure that received power levels are equal at base station
- Power control and channel problems!



Random access protocols

- ALOHA
  - Transmit whenever you want
    - If you are acknowledged, everything is fine
    - Otherwise retransmit packets
  - Low throughput (18%)
  - Slotted versions are slightly better
    - Transmission attempts can take place only at discrete points of time

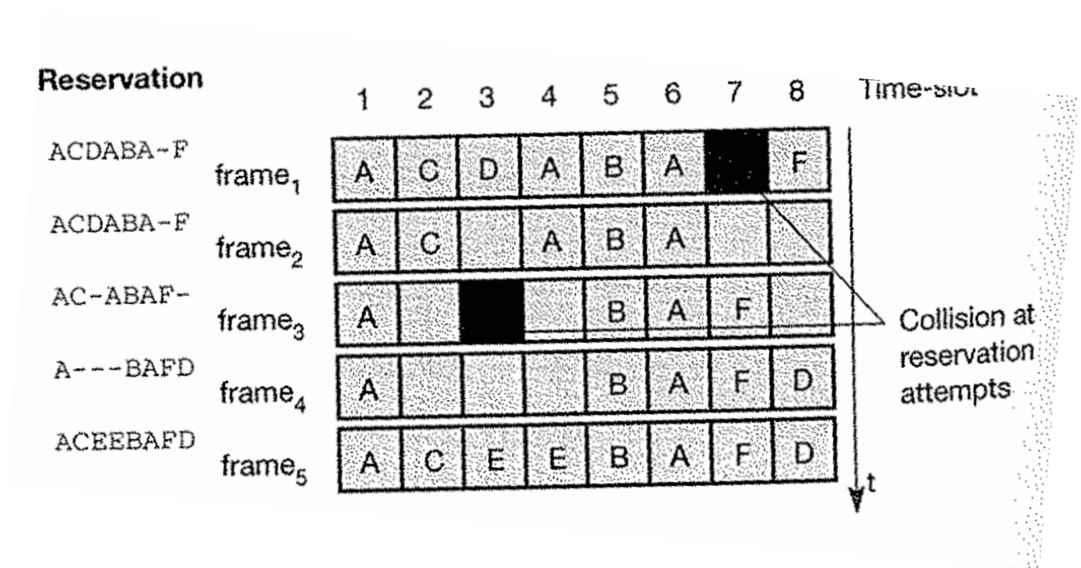
Use of ALOHA in Cellular Networks

- To set up a call, MSs initially employ slotted ALOHA to send some information to the BS
  - Called "random access channel" or something similar
- If successful, they are "assigned" a frequency channel and time slot or spread-spectrum code
- If unsuccessful, they try again
  - MS gives up if repeated tries fail
    - Collisions (congestion), poor channel quality, etc.

Packet Reservation Multiple Access (PRMA)

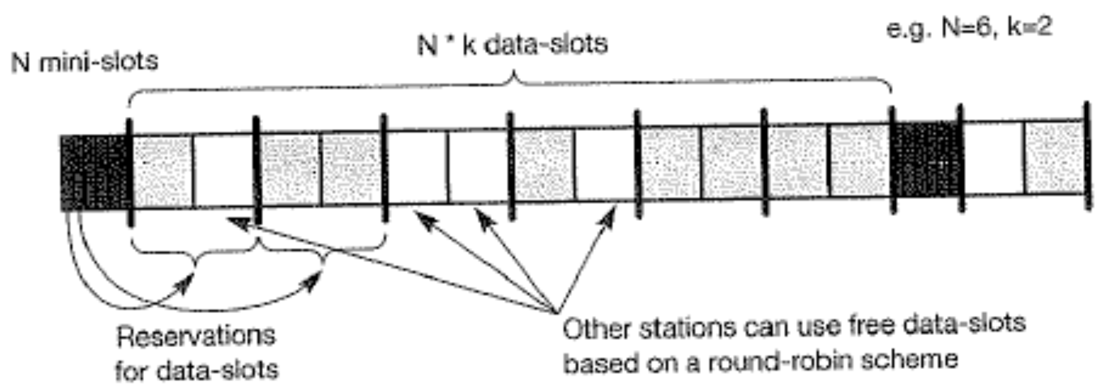
- Implicit reservations.
- Base station indicates which slots are free in a frame. (e.g. in the figure 7th slot is free)
- Stations contend for free slot using Aloha.

• If successful, they hold onto the slot.
• If collision occurs, the slot is open again for contention.



Reservation TDMA

- Mini-slots at the beginning of the frame – each slot assigned to a station.
  - These slots are used to reserve data slots (upto some maximum number)
- Unused data slots can be used by other stations.
  - Assignment could be round robin or using Slotted Aloha.



Carrier Sensing

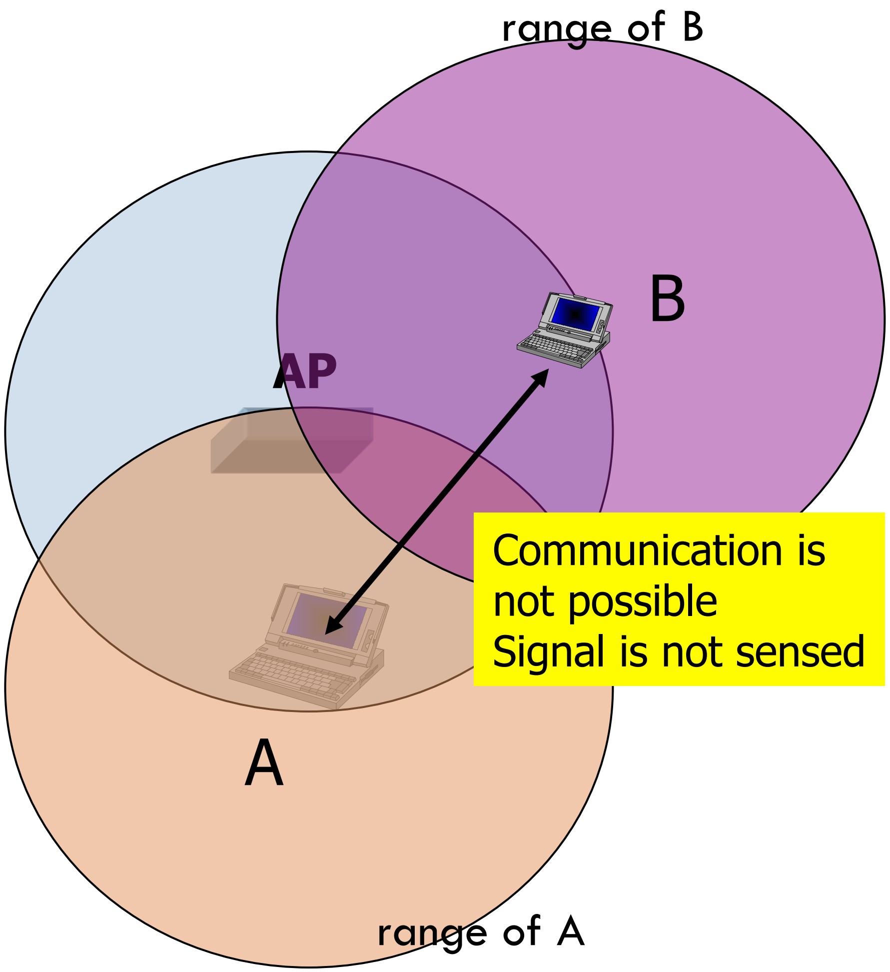
- Carrier sensing
  - It is an improvement of ALOHA (no carrier sensing in ALOHA)
  - Depending on the protocol a variety of CSMA protocols exist
    - Non-persistent
    - *p*-persistent
    - Binary exponential back-off
  - Collision detection Vs Collision avoidance
- Most random access protocols are based on some form of carrier sensing!

Problems with carrier sensing

- The signal strength is a function of distance and location
  - Path loss and shadow fading
  - Not all terminals at the same distance from a transmitter can "hear" the transmitter and vice versa
- The hidden node problem
- The exposed node problem
- Capture

The Hidden Terminal Problem

- A MS that is within the range of the destination but out of range of a transmitter
- MS A transmits to the AP
- MS B cannot sense the signal
  - MS B may also transmit resulting in collisions
  - MS B is called a "hidden terminal" with respect to MS A



Mechanisms for overcoming collisions due to hidden terminals

- Busy-tone multiple access (BTMA)
  - Out of band signaling scheme
  - Any node that hears a transmission will transmit a busy tone in an out of band channel
  - Also called Inhibit Sense Multiple Access (see book).
- Control handshaking
  - Use a three-way handshake
  - Terminal A sends a short request-to-send (RTS) packet to the AP
  - The AP sends a short clear-to-send (CTS) packet that is received by Terminal A AND Terminal B
  - Terminal B defers to terminal A

Exposed Terminal Problem

- Opposite of hidden terminals
- The exposed terminal is in the range of the transmitter but outside the range of the destination
- Terminals may unnecessarily backoff
  - Low utilization of bandwidth
- Solutions
  - Proper frequency planning
  - Intelligent thresholds for carrier sensing

Capture

- Capture
  - A receiver can "cleanly" receive a signal from one of many simultaneous transmissions
- Suppose MS-A, MS-B and MS-3 all simultaneously transmit to an AP with the same transmit power
  - MS-A is the closest and its signal is received with a larger strength obscuring the transmissions from MS-B and MS-C
  - The AP is said to have "captured" the signal from MS-A
  - Common in FM or FSK transmissions but not a big problem in other systems
- Capture improves the throughput
- Capture results in unfair sharing of bandwidth
  - Need protocols to ensure fairness

Problems with Collision Detection

- Collision detection is easier at baseband than at RF frequencies
  - Receive and transmit frequencies are the same
    - There is a significant leakage of the transmitted signal onto the receiver antenna – “self interference”
    - Transmitting and receiving at the same time is very hard
  - Receive and transmit frequencies are different
    - Circuitry cost and power consumption become prohibitive for collision detection by a MS
  - Transmissions from ground level can be detected at a tower but not at the ground level
  - Collision results in a significant shift in voltage that is detected – fades could obscure this shift

Collision avoidance mechanisms

- Waiting times before transmission
  - If the MS finds the channel idle, it still waits for a fixed amount of time before transmitting
- Random backoff upon detecting a busy channel
  - Randomness reduces the chance of two MSs transmitting at the same time
- Contention resolution mechanisms
  - Use windows where a MS asserts itself or yields to other MS based on several different protocols
  - Randomly addressed polling (uses CDMA)
- Idle sensing at the BS/AP
  - If the uplink and downlink transmissions are separated in frequency, the busy nature of the uplink is communicated to the MSs by the BS/AP

The HIPERLAN/1 MAC Protocol

- It is based on carrier sensing, but of a type unlike IEEE 802.3 or IEEE 802.11
- It is called EY-NPMA: Elimination Yield Non-preemptive Priority Multiple Access
- The idea is to make the probability of a "single" transmission at the end of the contention cycle as close to 1 as possible.
- Section 7.4.1 in book.

The MAC Protocol Continued

- If a MS senses a medium to be free for at least 1700 bit durations, immediate transmission is allowed
  - Each data frame MUST be acknowledged by an ACK
- Otherwise, the MS goes through two phases once the medium becomes idle:
  - Prioritization
  - Contention
    - Elimination
    - Yield
  - Transmission

Prioritization

- Determine the highest priority of a data to be sent by competing MSs
- Allow only those stations with high priority frames to contend for the channel
- Data packets have several types of priorities
  - 5 priorities with Hiperlan
- A node with priority p will listen to p-1 time slots (usually 1 to 5 slots of 256 bits each)
  - If the medium is idle after the (p-1)-st slot, the MS will send a burst of 256 bits asserting its priority
  - If the medium becomes busy with a burst any time before, the MS will defer to the next transmission cycle
- Many MSs may have the same priority, but the ones with low priority are eliminated from contention

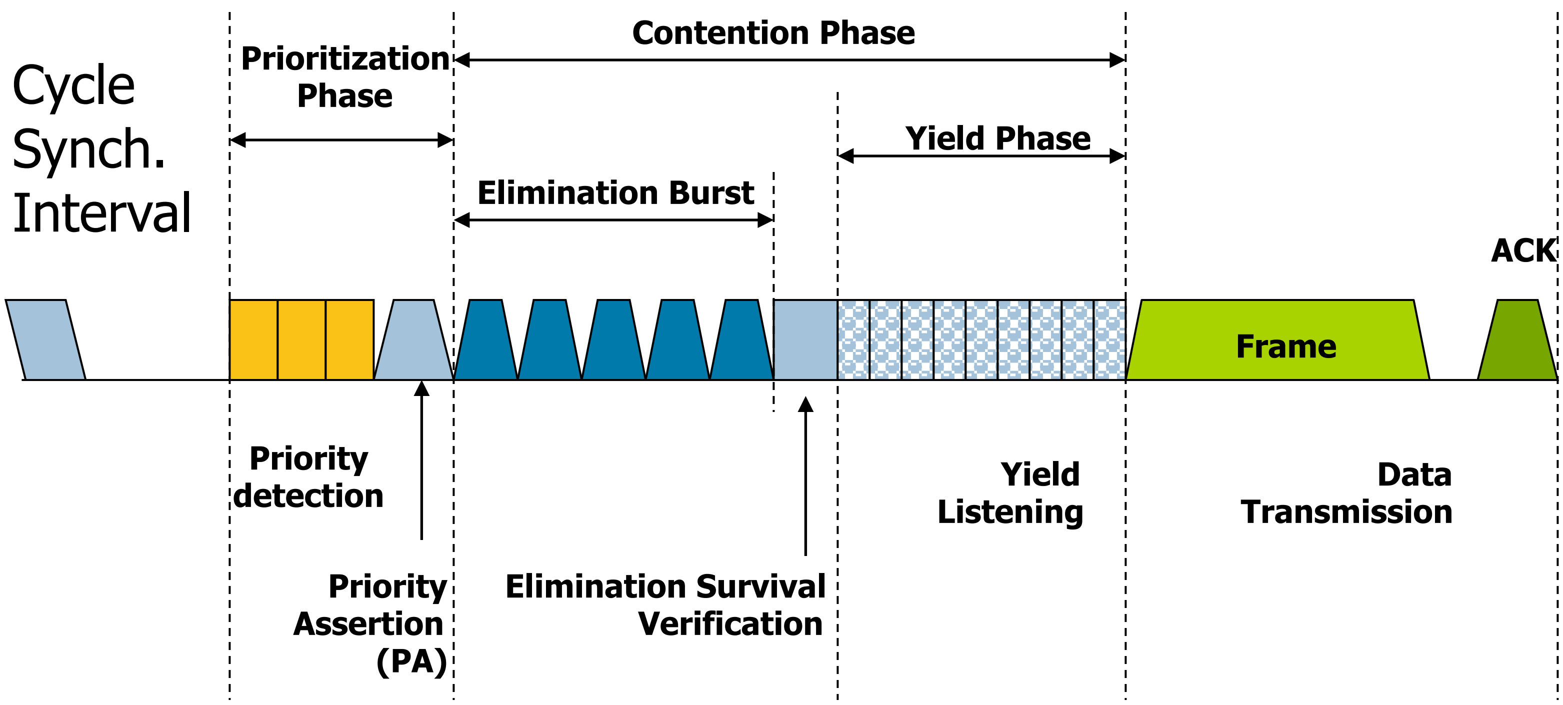
Contention (Elimination)

- Slots of size 256 bits are defined
- Randomly, MSs select the number of slots for which they will send a burst continously
- The maximum number of slots is 12
- The probability of the burst being "n" slots is (p is usually 0.5)
  - $p^n (1-p)$ for $n < 12$
  - p^n for $n = 12$
- After sending a burst, a MS listens to the channel for 256 bit durations (elimination survival verification interval)
- If it hears a burst in this period, it eliminates itself
- Longest burst wins!

Contention (Yield)

- The remaining MSs have a random yield period
- Each MS will "listen" to the channel for the duration of its yield period which is geometrically distributed
  - Prob (listening to n slots) = $0.9^n\ 0.1$ for $n < 14$ and 0.9^{14} for $n=14$
- If a MS senses the channel to be idle for the entire yield period, it has survived <whew!!>
  - Shortest Idle period wins
- It will start transmitting data and will automatically eliminate other MSs that are listening to the channel

Channel Access Cycle in HIPERLAN



Summary

- If simplicity demands a decentralized medium access protocol, CSMA or any of its variants is preferred
- CSMA in wireless networks leads to the hidden terminal, exposed terminal and sometimes the capture problem
- Collision detection in wireless networks is extremely difficult
- Systems that use CSMA are
  - CDPD
  - IEEE 802.11
  - HIPERLAN/1