# Mobile Network 2017 - Summary

## Contents

# 1 Wireless communication and mobility

- ▷ **user mobility**: users communicate "anytime, anywhere, with anyone"
- ▷ **device portability**: devices can be connected anytime, anywhere to the network

Wireless networks in comparison to fixed networks:

- ▷ Higher data loss-rates due to interferences
- ▷ Restrictive regulations of frequencies
- ▷ Lower transmission rates
- ▷ Lower security, Higher jitter
- ▷ Fluctuation quality of the links
- ▷ Unknown location of the mobile station

# 2 Wireless Network Models

Need to satify **coverage requirements** & **service requirements**
Resources to be managed/conserved: **frequency spectrum**, **power consumption**, **infrastructure and terminal cost**
**Interference** often limites the performance of the system
**Technical measures** of a wireless network: number of subscribers served, overall bandwidth provided, BER, delay, user data rate, coverage, outage probability, ...
**Common Service types**

- ▷ **Best Effort traffic**: guarantee minimum throughput. Utilize all available throughput at any time
- ▷ **Guaranteed service traffic**: constant data rate and delay

Network/infrastructure deployment: how many, where, what infrastructure and how much spectrum?
**Radio Resources allocation**: Given a set of base stations, allocate spectrum, power, ...
**Interference Models**: Propagation conditions on link $(i, j)$ given by $G_{ij}$ where $G$ is the link gain matrix.
**SINR** of uplink, downlink:

$$\Gamma^u_{i_0 j} = \frac{P_j G_{i_0 j}}{\sum_{m \neq j} P_m \theta_{0,m} G_{i_0 m} + N_{i_0}}$$

$$\Gamma^d_{i_0 j} = \frac{P_{i_0} G_{i_0 j}}{\sum_{b \neq i_0} P_b \theta_{0,b} G_{i_0 b} + N_j}$$

with $\theta$ the normalized cross-correlation term.
Guaranteed service quality $\rightarrow$ boundaries on $\Gamma^u_{i_0 j}$ and $\Gamma^d_{i_0 j}$
$M$ terminals active, $Y$ terminals served, $Z = M - Y$ assignment failure.
**Assignment failure rate**:

$$v = \frac{E[Z]}{E[M]} = \frac{E[Z]}{\omega A}$$

with $\omega$ the terminal per unit area and $A$ the area.
**Capacity**: the maximum allowed traffic load in order to keep the assignment failure rate below some threshold.
**Resource Management Strategies**

- ▷ **Static assignment**: based on statistical information during planning phase of the network
- ▷ **Perfect dynamic channel assignment**: based on instantaneous values. Traffic and interference adaptive assignment
- ▷ **Random assignment**: DS-CDMA, ALOHA, ...

# 3 Medium Access Control

MAC protocols handle channel sharing between multiple terminals.
**Challenges for wireless networks**

- ▷ Signal experiences relfection, diffraction, ...
- ▷ Broadcast nature of the medium
- ▷ Half-duplex: sending data usually prevents receiving

**Performance Measures**

- ▷ **Delay**: between arrival time and time the message sent to receiver
- ▷ **Quality** of data received:
  - ▷ **BER**: Bit Error Ratio
  - ▷ $p_{BER}$: Bit Error Probability
  - ▷ **Packet Error Rate** $= 1 - (1 - p_{BER})^N$
- ▷ **Throughput**: expected number of messages delivered to the receiver per time unit.
- ▷ **Normalized link delay**: 1 / throughput

## 3.1 Contention-free MAC protocols

Each terminal sends packets using predetermined time slots, frequency bands, or codes. A central scheduler coordinates the transmissions of different terminals, and **there will be no collisions** in the network.
Pros and cons:

- \+ Appropriate for QoS guarantee
- \+ Works also with heavily loaded networks
- \- Dynamic schemes have high complexity

Wireless resources can be divided into orthogonal partitions called **channels** and these can be assigned to different terminals.
**Static resource partitioning**

### 3.1.1 TDMA - Time Division Multiple Access

- ▷ All terminals are synchronized
- ▷ Flexible in handling different rate requirements

### 3.1.2 FDMA - Frequency Division Multiple Access

- ▷ Not efficient for traffic with different rate requirements
- ▷ Need guard bands between adjacent bands $\rightarrow$ lower thrghput

### 3.1.3 OFDMA - Orthogonal Division Multiple Access

- ▷ Like FDMA but uses orthogonal sub-carriers
- ▷ Doesn't need guard band between adjacent frequency bands
- ▷ Allows overlapping adjacent spectrum bands $\rightarrow$ more spectrum efficient
- ▷ Easy to implement and used in 4G

### 3.1.4 CDMA - Code Division Multiple Access

- ▷ Terminals send on whole frequency bandwidth
- ▷ Each sender has a unique code $\rightarrow$ XOR the signal with it
- \- Higher complexity of the receiver
- \- All signals should have the same strength at the receiver
- \+ Huge code space compared to frequency space
- \+ More robust to jamming and eavesdropping
- ▷ Used in 3G and Wifi

### 3.1.5 SDMA - Space Division Multiple Access

- ▷ Uses the spatial separation to reuse frequency spectrum
- ▷ Useful when terminals are located far from each other
- ▷ Use intelligent signal processing and antenna arrays so it can reuse frequency spectrum within the same cell.
- ▷ Often combined with other partitioning methods.

**Dynamic resource partitioning**
Network resources can be dynamically allocated using a central scheduler to achieve better network performance.

- \+ Good performance in heavy traffic
- \+ QoS guarantee
- \- Higher complexity and cost
- \- Not scalable

### 3.1.6 Poll-based access protocol

- ▷ Designate device as a channel access administrator
- ▷ Admin queries other terminals to see if they have packets
- ▷ If so, they transmit packets in the following several time slots
- ▷ Higher overhead as polling consumes a lot of bandwidth and turnaround time increases time overhead.

### 3.1.7 Token-based access protocol

- ▷ Token is passed in a orderly fashion between the terminals.
- ▷ Terminal holding the token has the channel access.

## 3.2 Contention-based MAC protocols

- ▷ Terminals access channel randomly when they have packets to send.
- ▷ No terminals is superior to another station
- ▷ Terminals decide when to send based on a procedure defined by the protocol
- ▷ Allows packet collisions
- \+ Good performance in low-traffic networks
- \+ Low complexity

### 3.2.1 Pure ALOHA

1. If there is a message to send, send it
2. 
   - ▷ If the transmission succeeded → step 1
   - ▷ If the transmission failed, wait a random time → step 1

- ▷ Poor performance with high traffic

### 3.2.2 Slotted ALOHA

- ▷ Terminals are synchronized and can send packets only at the beginning of a time slot
- ▷ The average number of messages arriving to the system has to be equal to the average number of departing messages.
- ▷ Mathematical model
  - ▷ $M$: # terminals
  - ▷ $\lambda_i = \lambda/M$: message arrival rate
  - ▷ $\sigma_i$: message retransmission rate
  - ▷ $\delta_i = \lambda_i + \sigma_i$: message attempt rate
  - ▷ $q = e^{-M\delta_i}$: successful transmission probability
  - ▷ $\Rightarrow \lambda_i = q\delta_i$: for stable equilibrium
  - ▷ $p = 1 - e^{-\delta_i}$: transmission probability
  - ▷ Overall network thrghput:

$$\lambda = \sum_{i=0}^{M} \lambda_i = M\delta_i e^{-M\delta_i}$$

### 3.2.3 CSMA - Carrier Sense Multiple Access

- ▷ Abort transmission as soon as a collision is detected
- ▷ **Non-persistent CSMA**:
  1. If the channel is sensed idle → send
  2. Otherwise → wait a random amount of time and → step 1
- ▷ **1-persistent CSMA**:
  1. If the channel is sensed idle → send
  2. Otherwise sens until idle → send
- ▷ **p-persistent CSMA**:
  1. If the channel is sensed idle → send with prob $p$
     Otherwise → delay its transmission by one time slot
  2. If channel busy → continue sensing until idle → step 1

### 3.2.4 CSMA/CD - with Collision Detection

- ▷ If collision during transmission → stop and signal collision
- ▷ If collision occurs several time → increase time window (exp)
- ▷ **Not appropriate for wireless networks**
- ▷ **Hidden Terminal Problems**: Senders sense idle but receiver in the middle get both messages at the same time.
- ▷ **Exposed Terminal Problem**: Senders sense channel busy while the receivers actually isolated

### 3.2.5 CSMA/CA - with Collision Avoidance

1. At new transmission → choose backoff counter randomly
2. Sense the channel:
   - ▷ if idle for DIFS (Duration Inter-Frame Space) → step 3
   - ▷ Otherwise → continue sensing
3. Count down using backoff counter while channel remains idle.
   - ▷ If the channel sensed busy → step 2.
   - ▷ If the counter is zero → transmit data immediately.

▷ **Request To Send (RTS)**, **Clear To Send (CTS)** packets, carrying data length solve exposed & hidden terminal issue

### 3.2.6 CRA - Conflict Resolution Algorithms

Resolves conflicts → users are scheduled using distributed algo.

▷ Each terminal is uniquely numbered

▷ When conflict occurs → enters *conflict resolution mode* until the conflict has been resolved → check last digit on IDs

### 3.2.7 Reservation-Based Protocols

▷ Very costly to loose one long data packet when collision

▷ Reserve resources (time, frequency, ...) for data transmission

▷ Two phases: 1. reservation phase, 2. data transmission phase

▷ **Scheduling-based**: Central scheduler first collects networks information and then schedule the resources

▷ **Contention-based**: Short reservation pckt w/ ALOHA, CRA

### 3.2.8 Bit-map protocol

▷ Terminals are numbered

▷ Send short reservation packet in the corresponding time slot

▷ Send data in the data phase folling order in resrvation phase.

▷ Station see all 1-bits resrvation transmitted during resrvation phase. Station know which stations want to transmit.

▷ After the resrvation phase, stations that asserted to transmit sends its frame in the order of station number.

▷ Efficiency: $\frac{d}{(d+N)}$, $d$ # bits in the packet, $N$ # terminals

### 3.2.9 Bianchi's model

▷ Semi-analytical model to express performance of networks.

▷ Use 2D Markov C. of $m+1$ backoff stages in which each stage represent the backoff time counter of a node. Transitions take place upon collisions and successful transmissions

▷ In each stage, CW is the maximum value for the contention window and is equal to $2^i(CW_{min}+1)$

▷ If a correct transmission takes place, a random backoff will be chosen between 0 and $CW_0 - 1$ with probability $\frac{1-p}{CW_0}$

▷ In the case of a collision, a random back will be chosen between 0 and $CW_i - 1$ with probability $\frac{p}{CW_i}$

▷ State are represented as $\{s(t), b(t)\}$, $b(t)$: counter, $s(t)$: stage

▷ This model assumes that packets collide with probability $p$

▷ With $\pi$ the probability to send a packet: $p = 1 - (1-\pi)^{N-1}$

▷ Stationary distribution of the chain:

$$b_{i,k} = \lim_{t\to\infty} P(s(t) = i, b(t) = k), i \in \{0, m\}, k \in \{0, CW_i - 1\}$$

▷ Thansmission occurs when backoff time counter = 0, therefore:

$$\pi = \sum_{i=0}^{m} b_{i,0}$$

▷ Close form of $b_{i,k}$

$$\begin{cases} b_{i,0} &= p^i b_{0,0} & 0 < i < m \\ b_{m,0} &= \frac{p^m}{1-p} b_{0,0} & \\ b_{i,k} &= \frac{CW_i - k}{CW_i} b_{i,0} & 0 \le i \le m, 0 < k < CW_i - 1 \end{cases}$$

Imposing normalization condition, we obtain $b_{0,0}$ as function of $p$:

$$b_{0,0} = \frac{2(1-2p)(1-p)}{(1-2p)(W_{min}+1) + pW_{min}(1-(2p)^m)}$$

$$\pi = \frac{b_{0,0}}{1-p} = \frac{2}{1 + W_{min} + pW_{min}\sum_{k=0}^{m-1}(2p)^k}$$

▷ **Saturation throughput**: average information payload transmitted in a slot time over the average duration of a slot time:

$$\tau = \frac{P_s P_{tr} L}{P_s P_{tr} T_s + P_{tr}(1-P_s)T_c + (1-P_{tr})T_{id}}$$

with

$$P_{tr} + 1 - (1-\pi)^N \text{ and } P_s = \frac{N\pi(1-\pi)^{N-1}}{1-(1-\pi)^N}$$

$T_{id}$: duration of the idle period, $T_c$: average time spent in collision, $T_s$: average time needed to transmit a packet of size $L$

# 4 Scheduling

Users have different service requirements so we need a flexible service architecture to intergrate different types of services on a single air-interface. Also, QoS metrics differ between different applications

## 4.1 Reservation-based access protocol w/ centr. sched.

- ▷ Most used access protocol in wireless cellular networks
- ▷ High efficiency and flexibility in managing wireless resources.
- ▷ **Physical Downlink Control Channel (PDCCH)**:
  → conveys control information for each user.
- ▷ **Physical Downlink Shared Channel (PDSCH)**:
  → multiplex the data of all terminals.
- ▷ Reservation phase: PDCCH. Data phase: PDSCH
- ▷ During the reservation phase, one can estimate channel and adapt scheduling in consenquence.
- ▷ Wireless scheduling suffers from **supporting a mix of classes** of traffic desiring different QoS.
  - ▷ Conversational: Preserve time relation.
  - ▷ Streaming: Preserve time relation
  - ▷ Interactive: Request response pattern, preserve payload
  - ▷ Background: Destination is not expecting data within a certain time, preserve payload
- ▷ **Channel Variation**: Channel is unstable, hard to predict, capacity of the link varies w.r.t. time and locations.
- ▷ Difficult to estimate the amount of resources needed. Thus, it is needed to use an adaptive procedure to assure QoS.
- ▷ For $M$ uplink users, the sum of the data rates is bounded

$$\sum_{i=1}^{M} r_i \leq W \log_2 \left(1 + \frac{\sum_i P_i g_{i0}}{N_0 W}\right)$$

  with $W$: frequency bandwidth, $P_i$: transmission power, $g_{i0}$: power gain of the channel and $N_0$: noise spectral density
- ▷ In the downlink, the base station sends independent data streams to multiple users.
- ▷ Assuming $g_{01} \leq g_{02} \leq ...$, the capacity region is:

$$r_m \leq W \log_2 \left(1 + \frac{P_m g_{0m}}{\sum_{i=m+1}^{M} P_i g_{0m} + N_0 W}\right), \forall m$$

## 4.2 Wireless Packet Scheduling Algorithms

- ▷ Increase flexibility in adaptation to QoS and channel
- ▷ Significant performance improvement
- ▷ Model contains M users served on a single channel, TDMA; each user has a buffer to store the packets to be sent.
- ▷ Queue modeling: At timeslot t, queue of user i updates:

$$q_i[t+1] = q_i[t] + d_i[t] - n_i[t]$$

  $d_i[t]$: new bits arriving, $n_i[t]$: # bits scheduled to transmit

$S_i$: long-run throughput for user $i$ can be predicted using

$$\hat{S}_i[t] = (1 - \frac{1}{\tau})S_i[t-1] + \frac{1}{\tau}\hat{r}_i[t]I[i]$$

where $\tau >> 1$ scheduler's constant, $\hat{r}_i$: expected data rate

### 4.2.1 Round-robin scheduling

- ▷ One of the simplest scheduling algorithms
- ▷ Users are scheduled in round robin
- ▷ All users scheduled the same amount of resources

### 4.2.2 Max throughput scheduling

- ▷ Schedule the minimal in each time slot → total network throughput is maximized.
- ▷ Most aggressive packet scheduler
- unfairness and coverage limitations. i.e. terminals in unfavorable positions may never be served.

### 4.2.3 Proportional Fair Scheduling

- ▷ Compromised policy to balance the competing interests of maximizing total network throughput and providing all terminals with at least a minimum level of service.
- ▷ Meets the **Proportioanl fairness criterion** → When the scheduling result is already proportional fair, changing the scheduling such that the throughput of any user is increased by a percentage, the cumulative decrease of the throughputs of the other users will be higher.

### 4.2.4 Max-Min Scheduling

- ▷ Objective: maximize the minimum user throughput
- ▷ Scheduling result is max-min fair iff increase of thrghput of one user results in decrease of a user with a smaller thrghput

### 4.2.5 Max Utility Scheduling

- ▷ All previous schedulers do not consider QoS
- ▷ Utility ≡ satisfaction of each user given allocated resources
- ▷ Model the QoS perception of users
- ▷ Objective: maximize the sum utility of all users

$$\max \sum_{i=0}^{M-1} U_i(S_i)$$

- ▷ Utility function determined based on traffic characteristics
- ▷ Different utility functions can be designed:
  - ▷ Max-throughput: $U_i(S_i) = S_i$
  - ▷ Proportional fair: $U_i(S_i) = \ln(S_i)$
  - ▷ **Alpha Fair Utility**: Contains a parameter $a$ which mesures how fair the scheduler is. Get max throughtput when $a = 1$ and is propotional fair when $a = 0$

$$U_\alpha(S) = \begin{cases} \frac{S^{1-\alpha}}{1-\alpha} & \alpha \geq 0 \text{ and } \neq 1 \\ \ln(S) & \alpha = 1 \end{cases}$$

### 4.2.6 Scheduling in OFDMA Systems

- ▷ One more dimension of resources: subcarrier allocation
- ▷ Different users experience: different gains because of frequency selectivity in channels
- ▷ Scheduling of subcarriers in an adaptive way based on the instantaneous channel qualities.
- ▷ Use adaptive subcarrier assignment, power allocation, modulation and coding to exploit the diversity in multiple users and frequency to improve the network performance.
- ▷ Usually combined w/ modulation and coding to improve perf.
- ▷ Additional signal overhead is necessary so the base station can inform all users the resource allocation results
- ▷ Round-robin, max-throughput, PF, max-min and max-utility scheduling can all be done for OFDMA
- ▷ **Power adaptation**: Each subcarrier should be assigned to the user with the highest Y (ratio between the channel gain and the interference) as the rate increase by using any amoung of power on any subcarrier will be maximized if the subcarrier has the hightest Y.
- ▷ Scheduling in OFDMA is usually based on optimization techniques to compute how much power should be used on each subcarrier. Generally no closed-form expressions.
- ▷ Expected overall throughput

$$R[t] = \sum_{i=1}^{M} R_i[t] = \sum_i \sum_j W \log_2 \left(1 + \frac{p_{ij}[t] y_{ij}[t]}{\theta}\right) \underbrace{I(i,j)}_{\text{assignement}}$$

  $y_{ij}[i]$: ratio between channel gain and interference

- ▷ Without power adaptation (max-thrput)

$$I^*(i,j) = \begin{cases} 1 & \frac{p_{ij}[t] y_{ij}[t]}{\theta} \geq \frac{p_{mj}[t] y_{mj}[t]}{\theta}, \forall m \\ 0 & \text{otherwise} \end{cases}$$

- ▷ With power adaptation (max-thrput)

$$I^*(i,j) = \begin{cases} 1 & y_{ij}[t] \geq y_{mj}[t], \forall m \\ 0 & \text{otherwise} \end{cases}$$

- ▷ Base station defines power allocation $p_{ij}$ to maximize thrput

# 5 Principles of cellular systems

- ▷ Cellular networks contain a set of fixed base stations
- ▷ Signal power decreasing with the distance → terminals connect to the closest base station

$$SNR = \frac{c_t P_t}{r^\alpha N}$$

  $r$: distance, $c_t$: antenna constant, $\alpha$: propagation constant

- ▷ Considering **shadow fading** → received SNR becomes random - $G$ lognormal distribution. To preserve the same cell coverage area, need an extra **fade margin** $M$ at the transmitter

$$P\left(\frac{c_t G P_t M}{r^\alpha N} \leq y_0\right) \leq p_{out}$$

- ▷ W/ known radius, # cells required to cover the service area is the ratio between total area and cell area.
- ▷ The **decibel**: dimensionless unit → power ratio. Express the magn. of a physical quantity relative to a reference level
- ▷ A value expressed in dB is computed as

$$10 \log_{10}(P/P_{\text{ref}})$$

- ▷ **Capacity of a wireless network (or radio capacity)** is measured as the average number of simultaneous radio links supported by the system.
- ▷ **Area capacity**: # users per cell per unit area ratio.

$$\text{area capacity} = (C/(KA_{\text{cell}})) \tag{1}$$

- ▷ Trade off between quality (SINR) and capacity in the network
  → i.e.: with large clusters, the reuse distance is larger and thus the quality of the connections is increased
- ▷ Queueing modelling: **Blocking probability**

$$P_{block} = \frac{\rho^\eta/\eta!}{\sum_{k=0}^{\eta} \rho^\eta/k!}, \rho = \frac{\lambda}{\mu}$$

- ▷ Outage probability ≡ average over the pdfs of $t$
- ▷ # assignment failures in a network with $n$ channels, $M$ mobiles is given by
  $Z = max(0, M-n) + Q$ with $Q$: # mobiles having a channel but bad SINR
- ▷ **Assignment failure rate**:

$$v_p = \frac{E[Z]}{E[M_c]} = \sum_{k=\eta}^{\infty} (k-\eta) \frac{(\omega A_c)^{k-1}}{k!} e^{-\omega A_c}$$

  $\omega$ the number of calls (Poisson distributed) per unit area

- ▷ **Relative traffic load**:

$$\bar{\omega}_\eta = \frac{\omega A_c}{\eta}$$

- ▷ The system capacity can also be defined in terms of a combined blocking and signal outage, or **Grade of Service**

Fun facts:

- ▷ Cellular networks are based on efficient spectrum reuse
- ▷ Directional antennas reduce interference, improve coverage
- ▷ Cell capacity depends on the cell size
- ▷ Small cells → better capacity
- ▷ Fading reduces the capacity of wireless networks

Design of wireless networks consists of two steps:

1. Coverage planning
2. Frequency allocation

## 5.1 Coverage planning

- **Connection region** of a base station is the geometrical region where the received signal power from that base station is larger that that from any other base station.
- **Coverage area** of each base station ≡ **cell**.
- **Coverage planning problem**: find the required number of base s to be used with the servie area
- Common model used is uniform hexagonal-shaped areas
- It is pretty easy to compute the radius of the cells and # of cells required to cover the service area
- channels / cells: $C$ available channels, K groups

$$\eta = \left\lfloor \frac{C}{K} \right\rfloor$$

- **Normalized reuse distance**

$$\frac{D}{R} = \sqrt{3K}$$

with $R$ the radius, $D$ distance between cells

## 5.2 Frequency Planning

- SINR at any receiver located in cell $k$

$$\Gamma_k = \frac{c\frac{P_t}{r^\alpha}}{\sum_{i=1\ldots B} \frac{cP_t}{d_i^\alpha} + N}$$

## 5.3 Static channel allocation

- # simultaneous connections within the service area is often larger that # orthogonal waveforms. → usefull to reuse same frequency within the service area as often as possible
- The higher the propagation loss as a function of distance, the more often we can reuse the spectrum
- **Reuse distance** is the minimum physical distance between two transmitters using the same waveform, required to achieve a certain link quality
- In **Fixed channel allocation (FCA)**, each access port is assigned a certain fixed number of channels. This allocation is achieved by dividing the C available channels into K (reuse factor) groups (clusters) of equal size. The access port has the right to use these channels freely to communicate with its terminals, but cannot use any channel from another group.
- To maintain a sufficiently high SINR, the channels in a group cannot be reused in a cell that is too close to the first cell

## 5.4 Best-effort data services

- **bandwidth** of each channel: $W = W_s/K$ with $W_s$ the total bandwidth
- **Instantaneous data rate** within a cell at distance $d = D/D_0$ from the base station

$$R(d) = \min(R_{max}, cW \log_2(1 + \Gamma(d)))$$

with $D_0$ the radius of the cell and $\Gamma(d) = \frac{\Gamma(D_0)}{d^\alpha}$

- The data rate at the center of the cell is limited by peak rate $R_{max}$

## 5.5 Directional antennas and sectorizations

- directional receiving antenna → reduce interference
  → ↓ the number of base station sites → ↓ infrastructure costs

# 6 More on cellular networks

## 6.1 Capacity of CDMA Cellular Networks

- Techniques to reduces interference:
  - Multi-sectorized antennas
  - Discontinuous transmission mode
- **Power Control**: for a single cell, all uplink signals should be received ≈ with the same power at the base station
- **Pilot signal**: transmitted by the base station: used by each mobile to set its own power
- Average energy per bit, compared to noise power density:

$$\left(\frac{E_b}{I_0}\right)_i = \frac{W}{R}\frac{G_{ii}P_i}{\sum_{k\neq i} G_{ki}P_k} + N_0W = \frac{W}{T}\Gamma_i$$

with $R = 1/T_s$: data rate, $W$: interference bandwidth, $N_0$: additive noise power density.

- single cell case:

$$SNR = \frac{S}{(N-1)S} = \frac{1}{N-1}$$

with $S$: power from single user, $N$: # users

- bit energy to noise ratio

$$\frac{E_b}{N_0} = \frac{S/R}{(N-1)(S/W)} = \frac{W/R}{N-1}$$

with $W$:available bandwith, $R$: bitrate, $N_0$: noise spectral density

- taking thermal noise $\eta$ into account

$$\frac{E_b}{N_0} = \frac{W/R}{(N-1)+(\eta/S)} \Rightarrow N = 1 + \frac{W/R}{E_b/N_0} - (\eta/S)$$

- To increase this number, switch off user while not talking and antenna sectorization:

$$\frac{E_b}{N_0} = \frac{W/R}{(N_s-1)\delta+(\eta/S)} \Rightarrow N_s = 1 + \delta\left[\frac{W/R}{E_b/N_0}\right]$$

with $N_s$: # users per sector

## 6.2 Femtocells

- Home base stations for mobile networks
- Licensed spectrum, low-power, low-range, better thrghput, better coverage, ...
- Susceptible to security attacks

## 6.3 Frequency management

- In all countries of the world, the licensed spectrum is managed by the government and leased to private operators
- Auction or beauty contest based on very detailed dossiers
- Currently trying to allocate more frequencies for more bandwidth in mobile communication → a new total auction
- Mobile network is doubling every 9-12 mounths.
- Auctions is a transparent procedure and let the market determines the value of frequencies
- With auction of small frequency blocks, the market decides on the scope of the licences
- More rules to prevent people to abuse the auction

# 7 Association and Handover

- To each active terminal, in order to maximize system utility, we need to assign transmit power, waveform, base station
- Association on the move : **handover**

## 7.1 Mobility management

- *While inactive*: track the location of the terminal and wake it up when necessary (e.g. to update location area)
- *While connected*: handover → timely selection of base stations based on signal quality measurements.

## 7.2 Handover types

- **Involved networks**
  - Horizontal handover: within a single network of homogeneous radio access technology (RAT)
  - Vertical handover: between different networks, heterogeneous RATs
- **Hard handover**: only one base stations serving at a time
- **Soft handover**: multiple base stations can simultaneously serve a mobile terminal. Can lead to a better usage of radio resources, at the expense of higher complexity

## 7.3 Handover phases

1. Measurement and decision
2. Resource management
3. Execution (handshaking)

## 7.4 Performance metric

- Handover failure probability
  - Handover attempts fail
  - Prob. that signal quality is below the required value
- Handover frequency

## 7.5 Handover decision criteria

- Received signal strength (cell boudaries)
- Signal to interference ratio

## 7.6 Handover resource management

- Resource reservation for handover
- Protection of ongoing services is more important than accepting new services
- Its significance depends on delay tolerance of the service

## 7.7 Handover execution

- System and mobile should reach agreement on which base station to pass, which waveform, authentification, ...
- Procedure has to be fast and reliable

## 7.8 Load balancing

- Traffic load fluctuates a lot over time
- neighbor cell may have much lighter load at the moment

# 8 F-Transport

## 8.1 Reminder TCP

- Reliable, in-order packets delivery
- Single path
- Congestion avoidance and control
- Three-way handshake
- Lost packet detection using sequence numbers and ACKs

Nowadays, hosts have several interfaces, or multiple addresses for a single interface. Addresses of mobile hosts can change as they move from one network to another. Current TCP is not designed to switch between interfaces as they come and go.
**Link aggregation**: combine multiple channels at different frequencies and use different radio technologies into a single link

## 8.2 Multipath TCP (MPTCP)

MPTCP is a modification of TCP presenting regular TCP interfaces to applications, spreading data across several TCP subflows. Achieve higher throughput, failover from one path to another and seamless mobility.

- First establish the intial subflow
- Then additional subflows can be established
- At least one of those need to differe between two subflows: Local IP, Remote IP, Local Port, Remote Port
- Use two levels of sequence numbers to prevent gaps in seq.
- Dseq: data sequence number (SQN) and seq is the additional SQN carried inside the TCP option. It ensures that the segments sent on any given subflow have consecutive SQNs.
- On linux, upon timeout expiration, re-evaluate whether packet could be retransmitted over another subflow
- Upon loos of a subflow, all the unacknowledged data are retransmitted on other subflows

### 8.2.1 MPTCP Congestion Control

- Each path runs its own congestion control, detect, respond
- MPTCP send all its traggic on its least-congested paths
- Users get at least as much thrghput as w/ single-path TCP

### 8.2.2 MPTCP Congestion Control Algorithm

- A connection consits of a set of subflows R
- Each subflow maintains a congestion window
- Specific rules on how to increase and decrease the windows
- Still experimental, but largely deployed on smartphones

# 9 Wireless Network Security

- In wireless networks, sending and receiving messages do not need physical access to the network
- Wirelees communications have a broadcast nature, therefore, transmissions can be overheard by anyone in range
- Easy to, eavesdrop, replay messages, jamming, ...
- Security requirements
  - Confidentiality: use encrypted messages
  - Authenticity: origin of the message must be verified
  - Replay detection
  - Integrity: messages stay un-modified
  - Access control: access provided only to legitimate entities
  - Protection against jamming

## 9.1 Cellular Network Security

### 9.1.1 GSM (2G) - Global System for Mobile com.

- Provides subscriber authentication
- use long-term secret key to generate session keys
- Provides protection of the subscriber's identity from eavesdroppers
- Provides confidentiality of communications
- User devices have SIM card (Subscriber Identity Module)
  - Allows to authenticate on the network
  - Contains a secret key
  - Encrypted with a PIN (Personal Identification Number)
  - User permanent identity, **IMSI** (International Mobile Subscriber Identity)
  - If possible don't use IMSI but temporary TMSI
- weaknesses:
  - Unilateral authentication
    $\rightarrow$ fake base station can pretend to be legitimate network
  - No security within the wired network
  - Uses 1st generation of cryptography
  - SIM cloning

### 9.1.2 UMTS (3G) - Universal Mobile Telecom. Systems

- Provides protection against false base station
- Key lengths were increased $\rightarrow$ stronger encryption
- Security mechanism within the networks
- However no end-to-end encryption

### 9.1.3 LTE (4G) - Long Term Evolution

- Even more secure
- Completely IP-based
- Security principles:
  - Permanent security association with home network
  - New Key hierarchy
  - Reciprocal authentication mechanisms
  - Trusted environment (in isolation from the OS)
  - DoS protection of the network
  - User privacy
  - Authorization required for connection to core networks

### 9.1.4 WEP - Wired Equivalent Privacy

- Before association, the station needs to authenticate itself
- Default key is manually installed in every station and the AP
- Default keys need to be changed when a member leaves the group, practically impossible to change in every device simultaneously
- hence, supports **multiple default keys**: message header contains a key ID, tells which key should be used for decryption
- Weaknesses:
  - Authentication is one-way only
  - Same key is used for authentication and encryption
  - No session key is established during authentication
  - No replay messages protection
  - Broken authentication protocol

### 9.1.5 WPA/WPA2 - WiFi Protected Access

- Authentication process results in a shared session key
- Different functions use different keys
- Integrity protection is improved
- Weaknesses:
  - Weak passwords
  - TKIP (encryption algo) has been broken
  - PIN can be bruteforced easily in 2 hours

### 9.1.6 Wireless Pairings

- Used when there is no central authority distributing keys
- Devices pair by themselves and set up keys
- Use symmetric key techniques or Diffie-Hellman

### 9.1.7 Diffie-Hellman Protocol

- Enables secret key establishment in cleartext
- Fully resits passive attackers
- Not secure against active attackers, hence need authentication
- Based on the discrete logarithm problem:
  - $A$ generates $a$, computes and send $(g^a \mod p)$. $B$ generates $b$, computes and send $(g^b \mod p)$. They can both generate the key

    $$k = (g^b \mod p)^a = (g^a \mod p)^b$$

    with $p$ a prime number and $g$ a generator of $Z_p^*$

### 9.1.8 Other techniques

- **Short String Comparison**: Display hash of the key on the screen, visually compare
- **Seeing is Believing**: Uses optical channel (in which impossible to perform MitM attack) to validate key exchange.
- **Loud and Clear**: Human-assisted string comparison using voice communication
- **Shake Them Up**: Rely on the fact that the attacker does not know which device transmits at which time
- **Integrity Regions**: Distance-bounding protocols (proved that devices are at most at X cm from each others)

#### 9.1.9 In practice

- Bluetooths's device pairing aims at creating one shared secret called the Link Key. This key is used both for authentication and encryption. Uses a PIN-based protocol called **Link Manager Protocol (LMP)**
- **Sound-Proof**: Sense ambient audio to verify proximity of the two devices

# 10 Privacy in Mobile Network

- **Privacy control**: ability of individuals to determine when, how, and to what extend information about themselves is revealed to others
- **Anonymity**: hiding who performed a given action
- **Untraceability**: making difficult for adversary to identify that given actions were performed by the same subject
- **Unlinkability**: hiding relationships between any item
- **Unobservability**: hiding of the items themselves
- **Pseudonymity**: use of a pseudo instead of real identity
- **Anonymity set**: subjects that might performed the action
- **Privacy metrics**:
  - **Anonymity set**: set of subjects that mights have performed the action
  - Measure of anonymity:

$$-\sum_{\forall x \in A} p_x \log p_x$$

    $A$: anonymity set, $p_x$: prob. that $x$ performed the action
  - Measure of unlinkability

$$-\sum_{\forall R \subseteq I_1 \times I_2} p_r \log p_r$$

    $p_r$: prob real relationship between elements in $I_1$ and $I_2$
  - Measure of certainty:

$$-\sum_{v \in V} p_v \log p_v$$

    $V$: set of possible values, $p_v$: prob that the value is $v$ for a given user

## 10.1 Location privacy

- With location-based services, users upload location episodically on network
- Use pseudo is a solution for the location privacy problem
- However changing pseudo at each timestamp is ineffective against a global eavesdropper (can predict your next location and infer the new pseudonym)
- **Mix zone**: unobserved zone where the vehicles change pseudo
- Vehicles do not know where the mix zone is
  $\rightarrow$ need to change pseudo frequently
- **Model of the mix zone**:
  - $p_{ij}$: prob exiting at $j$ and entering at $i$
  - $D_{ij}$: RV representing time that elapses between entering at $i$ exiting at $j$
  - $d_{ij} = P(D_{ij} = t)$
  - $P($ exit at $j$ at $t$ and enter at $i$ at $\tau) = p_{ij} d_{ij(t-\tau)}$
  - each possible mapping between exit and enter events is represented by a permutation $\pi$:

$$m_\pi = (N_1 <> X_{\pi[1]}, ..., N_k <> X_{\pi[k]})$$

$$P(m_\pi, \bar{X}|\bar{N}) = \prod_{i=1}^{k} p_{n_i x_{\pi[i]}} d_{n_i x_{\pi[i]}}(t_{\pi[i]} - \tau_i) = q_\pi$$

$$H(\bar{N}, \bar{X}) = -\sum_{\pi} \frac{q_\pi}{\sum_{\pi'} q_{\pi'}} \log\left(\frac{q_\pi}{\sum_{\pi'} q_{\pi'}}\right)$$

- **Tracking game**: adversary picks a vehicle in the obeserved zone. When this vehicle enters a mix zone, estimates time to enter other obvesable zones. When a vehicule enter obversable zone, compute probability of vehicle to be the one.
- Level of privacy is the success probability of the adversary
- **Location-Privacy Meter (LPM)**: open source software tool to quantify location privacy
- **Adversary model**: using observation and knowledge such as users' mobility profiles, the adversary can infer location by computing some probability distribution.
- **Inference Attack**: TODO -¿ uses de-anonymization and de-obfuscation

## 10.2 IMSI catchers

- **IMSI**: International Mobile Subscriber Identity
- Fake mobile towers acting between the target mobile phone and the service provider's real towers
- Used to track users, eavesdropping calls, geotargeting ads
- Used by law enforcement and intelligence agencies
- Use lack of mutual authentication, lack of encryption in the current mobile network implementations (mainly GSM, 2G)
- We can catch them using the constant parameters broadcasted by the cell towers

# 11 Hands-On Exercise 1

- **Distributed coordination function (DCF)** is the basic medium access mechanism of IEEE 802.11, and uses a CSMA/CA algorithm.
  - Basic access method: is channel busy, a backoff time is randomly chosen in $[0, CW]$. This timer is decremented by one as long as the channel is sensed idle for a *distributed inter frame space* $DIFS = SIFS + 2 \times SlotTime$. $CW$ is doubled after each unsuccessful transmission. When the backoff timer reaches zero, the source transmits the data packet. The ACK is transmitted by the receiver immediately after a period of time called *short inter frame space* SIFS. When a packet is transmitted, all other stations hearing this transmission adjust their *network allocation vector* NAV, maintaining a prediction of future traffic on the medium.
  - Optional channel access method with *request-to-send* RTS and *clear-to-send* CTS exchanged.
- **Point coordination function (PCF)** is a centralized, polling-based access mechanism which requires the presence of a base station that acts as an access point. An RTS frame should be transmitted by the source and the destination should accept the data transmission by sending CTS frame prior to the transmission of the actual data packet.