

## *Practical Exercise 1*

## Technology Basics

**Mobile Business I (WS 2010/11)**

Prof. Dr. Kai Rannenberg

T-Mobile Chair of Mobile Business & Multilateral Security  
Johann Wolfgang Goethe University Frankfurt a. M.



- Exercise 1: Mobile Communication Services
- Exercise 2: Architecture of the GSM system
- Exercise 3: 3G/UMTS, 4G, LTE
- Exercise 4: Cell Based Communication
- Exercise 5: Wireless LAN

- a) Which are the three basic services in a GSM network?
- b) Please describe each one of these services.
- c) When establishing a data connection over a GSM network, which are the relevant Mobile Data Services?
- d) Please state the advantages and disadvantages of
  - (i) packet-oriented and
  - (ii) circuit-switched mobile data services.

- 1. Carrier services***
- 2. Telecommunications services***
- 3. Supplementary services***

***Carrier services:***

- Services to transfer **data** over the GSM network
  - The original GSM standard provides maximum data transfer rates of 9.6 kbit/s (inappropriate for multimedia applications nowadays).
- The focus of GSM standardization was on voice services.

## ***Telecommunications services:***

- Telecommunication services (mainly **voice**) support the mobile communications among users
  - Telephone calls in high quality
  - Short messages (Short Message Service - SMS)
  - Fax
  - Europe-wide emergency number (112): All operators have to provide it with highest priority and free of charge

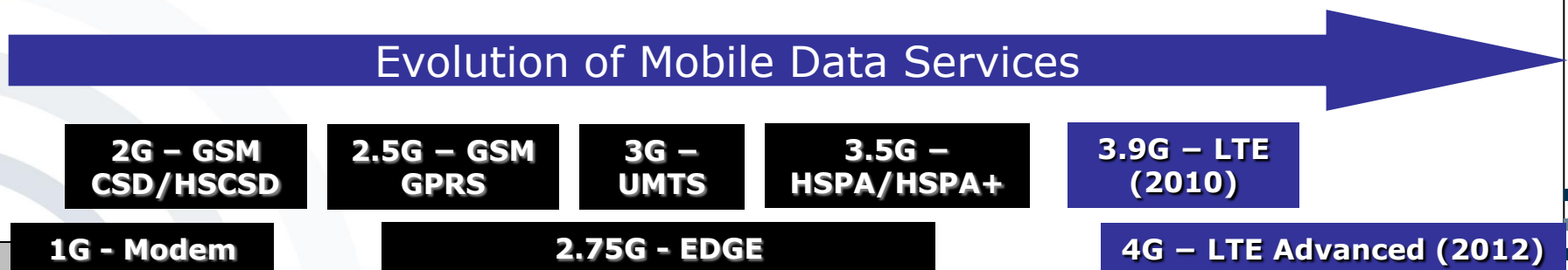
➔ Telecommunication services play a central role in the GSM standard.

## ***Supplementary services:***

- GSM provides a number of supplementary services (specific to network operators), such as:
  - *Caller ID*
  - *Call redirect*
  - *Closed user groups (e.g. company-internal network or GSM-R)*
  - *Teleconference (up to 7 participants)*

- **Modem** (modulator-demodulator) in analogue mobile networks (300 - 2400 bit/s)
- **CSD** (Circuit Switched Data) in GSM networks (9.6 Kbit/s)
- **HSCSD** (High-Speed Circuit Switched Data) in GSM networks (28.8, 43.2, or 57.6 Kbit/s)
- **GPRS** (General Packet Radio Service)
- **EDGE** (Enhanced Data Rates for Global Evolution)
- **UMTS** (Universal Mobile Telecommunications System)
- **HSPA** (High-Speed Packet Access), **HSPA+** (=Evolved HSPA)
- **LTE, LTE Advanced** (Long Term Evolution)

## Evolution of Mobile Data Services



### *General Packet Radio Service (GPRS)*

- First package-based data service
- Employment of time multiplex procedure for data services
- Dynamic allocation of radio channels among the subscribers in a radio cell
- Channels are only blocked when data is actually transferred.
- Package orientation implies the introduction of new billing methods.

- Up to 8 time slots can be occupied per time frame (at the moment 4 in practice).
- In contrast to Circuit Switched Data, the GPRS data service requires an extensive upgrade of the GSM architecture with new network components.
- In spite of better network utilization and volume based billing at the beginning, the data transfer costs were much higher than those of connection oriented data services (c't 9/2002, S. 100).
- The data transfer costs of GPRS data services have been lowered through new price models (especially free volume with higher basic charge).

- Advantages of (packet-oriented) GPRS over Circuit Switched Connections (CSD, HSCSD)

Economical network utilization

„Always-online“ allows offering new push services.

New billing methods can be realized (packet-oriented network).

- Disadvantages of (packet-oriented) GPRS compared to Circuit Switched Connections (CSD, HSCSD)

Existing GSM infrastructure must be upgraded implying high investments as well as new terminals

New push services require new security concepts, e.g. because of unintentional data reception (& payments for these data).

- Exercise 1: Mobile Communication Services
- Exercise 2: Architecture of the GSM system
- Exercise 3: 3G/UMTS, 4G, LTE
- Exercise 4: Cell Based Communication
- Exercise 5: Wireless LAN

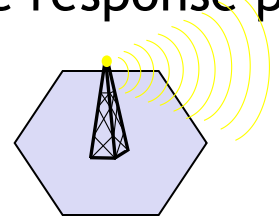
## Exercise 2: Architecture of the GSM system

- a) What are the three “security services” offered by GSM?
- b) Please outline and comment on the security model of the GSM infrastructure regarding subscriber authentication (challenge-response procedure for subscriber authentication).
- c) Name the weaknesses of the GSM security model and describe in particular the possible consequences resulting from these weaknesses.

The GSM system offers different “security services“:

- **Access control and authentication:**
  - Authentication of the subscriber to the SIM by input of a PIN and to the GSM network by Challenge-Response-Procedure
- **Confidentiality:**
  - Data & voice transferred between mobile station and BTS are encrypted.
- **(Partial) Anonymity:**
  - No transfer of data which can identify the subscriber via radio, instead temporary identification
  - (Temporary Mobile Subscriber ID, TMSI)

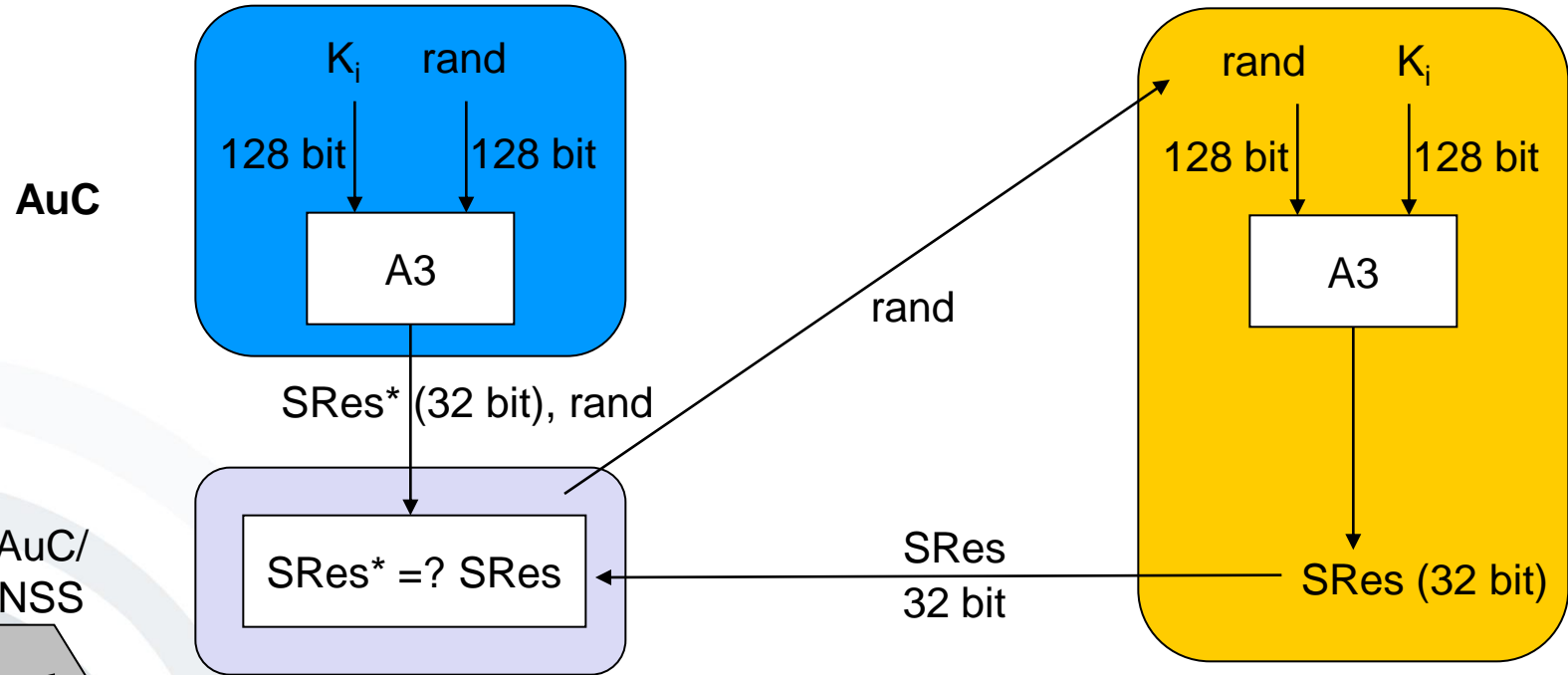
- Challenge response protocol



Mobile network



SIM



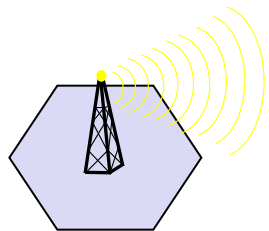
AuC/  
NSS

2a/b

$K_i$ : individual subscriber authentication key  
A3: („secret“) authentication algorithm

SRes: signed response

- Challenge-Response-Procedure (Subscriber Authentication)  
Authentication is based on the individual key  $K_i$ , the subscriber identification IMSI (International Mobile Subscriber Identity) and a secret algorithm A3.
- $K_i$  and A3 are stored on the SIM and deposited in the AuC.
  1. AuC creates random number *rand*.
  2. AuC encrypts *rand* and  $K_i$  via A3 (->SRes\*).
  3. AuC transfers *rand* and SRes\* to VLR.
  4. VLR transfers exclusively *rand* to SIM.
  5. SIM computes with “own”  $K_i$  and A3 Signed Response SRes.
  6. The SRES computed by the SIM is transmitted to the VLR and is compared with SRES\*.
  7. If SRES\* and SRES are equal the subscriber is authenticated successfully.

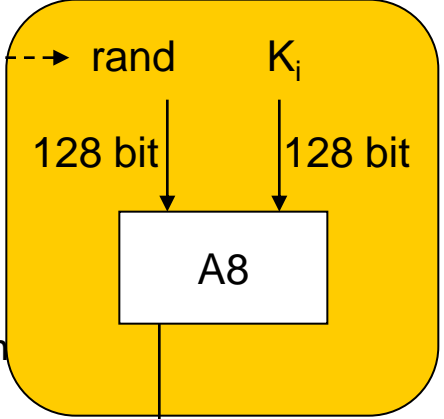
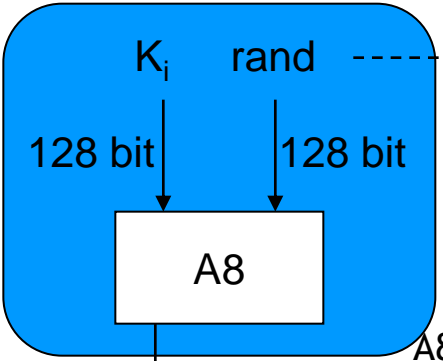


mobile radio network

MS with SIM

AuC

SIM

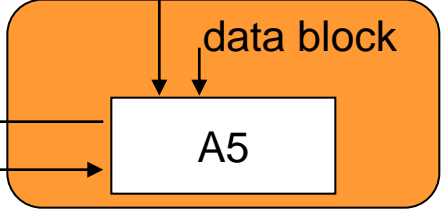
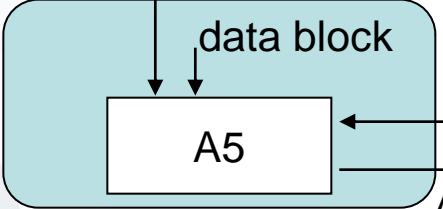


rand

A8 for key computation ("secret")

$K_c$   
64 bit

$K_c$   
64 bit



coded data blocks

A5 for encryption

BTS

MS

2a

- **GSM provides encryption of voice and data transferred via the air interface:**
  1. AuC creates random number rand.
  2. AuC generates the key  $K_c$  for the encryption of the transferred data via rand,  $K_i$  and A8.
  3. VLR transfers only rand to SIM.
  4. SIM computes the key  $K_c$  using A8, the rand received and the local  $K_i$
  5. Mobile station and mobile radio network use generated  $K_c$  and algorithm A5 for encryption and decryption of sent and received data.

- Partial Anonymity:
  - In order to guarantee the anonymity of the users **temporary** user identification (TMSI = Temporary Mobile Subscriber Identity) is used.
  - Temporary user identification is updated automatically from time to time or on demand.
  - Data which identify users are not transferred.
  - **Example:** Anonymous charging is (technically) possible via prepaid card.

- Solely authentication of the terminal/subscriber toward the **GSM network**. The network does not authenticate itself.
  - Assumption that the network is trustworthy per se
  - Security model was developed at a time with a provider monopoly
- Subscriber localization is almost exclusively controlled by the network.
  - Centralized movement tracking is possible
  - In order to avoid localization the subscriber must switch off the terminal.

- Security model bases partly on secret encryption algorithms.
  - A3 and A8 were published without authorization.
  - Some operators use non-standardized algorithms.
- No encryption from terminal to terminal but solely over the air interface
  - Encryption deactivation by the network possible, without notification of the users
- Encryption comparatively “weak” because of key length (64 bit)
  - Sometimes the real key length is shorter.

- Exercise 1: Mobile Communication Services
- Exercise 2: Architecture of the GSM system
- Exercise 3: 3G/UMTS, 4G, LTE
- Exercise 4: Cell Based Communication
- Exercise 5: Wireless LAN

- a) What are the additional security features which were implemented in 3G (UMTS) networks compared to those of GSM?
- b) What are the characteristics of 4G networks, how does LTE relate to 4G and what does it mean?

- UMTS complements the security mechanisms known by GSM:
  - Enhanced participant authentication (EMSI)
  - Network authentication
  - Integrity protection of data traffic
  - Transferred security keys are also encrypted in the fixed network (e.g. HLR-VLR)
  - Increased key length
  - End-to-End encryption is possible.

### 4<sup>th</sup> Generation Networks

- Collection of ideas for the future design of wireless communication networks.
- 4G networks will integrate a wide range of different wireless technologies, including technologies from existing 3G networks
- Components that are also discussed for 4G include:
  - Multiple antennas for the mobile devices
  - Smart antennas and “Beamforming”
  - Adaptive modulation and coding of the sent data
  - Usage of IP version 6 for the transmission of data-packets
  - Mesh networks

## *Long Term Evolution (LTE)*

- **LTE** makes 100 Mbit/s downlink and 50 Mbit/s uplink speed (theoretically) possible
  - New mobile network, like GSM and 3G/UMTS
  - „Pre-4G technology“ as it does not meet the IMT-Advanced (4G) requirements
    - Peak data rate of 100 Mbit/s for high mobility applications such as mobile access
    - Approx. 1 Gbit/s for low mobility applications such as nomadic/local wireless access
- **Development of LTE Advanced** is still in progress
  - Will make use of the frequency spectrum more efficiently resulting in higher data rates (above 100 Mbit/s, towards 1 Gbit/s)



<http://www.3gpp.org/LTE>

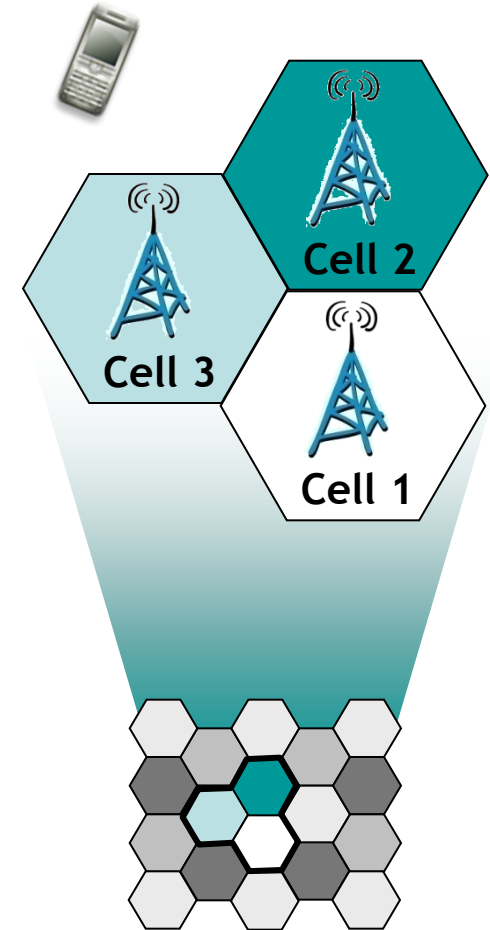


<http://www.3gpp.org/LTE-Advanced>

- Exercise 1: Mobile Communication Services
- Exercise 2: Architecture of the GSM system
- Exercise 3: 3G/UMTS, 4G, LTE
- Exercise 4: Cell Based Communication
- Exercise 5: Wireless LAN

- a) What does cell-based communication mean and what are the implications (basic principle, physical form, dependencies)?
- b) Write down the advantages and drawbacks of cellular networks compared to alternative solutions.
- c) In this context, explain “Multiplexing” and why it is used in communication systems.

- Cellular networks are radio networks consisting of several transmitters.
- Each transmitter or base station, covers a certain area ➔ **a cell**.
- Cell radii can vary from tens of meters to several kilometres.
- The shape of a cell is influenced by the environment (buildings, etc) and usually neither hexagonal nor a perfect circle, even though this is the usual way of drawing them.



- Cellular networks offer a number of advantages compared to alternative solutions:
  - **Higher capacity:** Cells offer the possibility to “reuse” the transmission frequencies assigned to mobile devices (e.g. by multiplexing). In order to do so, the networks need a thorough planning of the position of base stations and their frequencies.
    - ➔ More users can use the infrastructure
  - **Reduced transmission power:** Reduced power usage for the mobile device, due to the fact that only a limited amount of transmission power is needed in a small cell, compared to a far away base station.
    - ➔ Reduced power consumption for mobile devices

- Cellular networks offer a number of advantages over alternative solutions:
  - **Robustness:** Cellular systems are decentralised with regard to their base stations. In the case that one antenna fails, only a small area gets affected.
    - ➔ Failure of one base station does not affect the complete infrastructure
  - **Better coverage:** Cells can be adapted to geographic conditions (mountains, buildings, etc.).
    - ➔ Better availability of the infrastructure

- However, there are also some drawbacks of cell based communication infrastructures :
  - **Required infrastructure:** A complex and costly infrastructure is required, in order to link all base stations. This includes switches, antennas, location registers, etc.
  - **Handover needed:** When changing from one cell to another, a handover mechanism is needed that allows a change of cells in real-time. These mechanisms are complex.
  - **Frequency planning:** The distribution of the frequencies being used for the base stations needs to be planned carefully, in order to minimise interferences, etc.

- Fundamental mechanism in communication system
- Describes how several users can share a medium (e.g. mobile network) with minimum or no interference.
- **Goal:** Most efficient usage of a medium
- **Abstract example:** Traffic (users) using a highway with several lanes (medium) without accidents (interference)

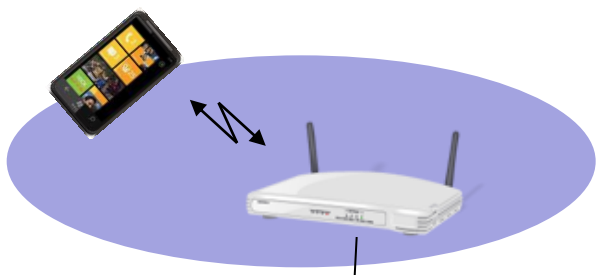
- Exercise 1: Mobile Communication Services
- Exercise 2: Architecture of the GSM system
- Exercise 3: 3G/UMTS, 4G, LTE
- Exercise 4: Cell Based Communication
- Exercise 5: Wireless LAN

- a) What are the components in a Wireless LAN?
- b) Name two types of Wireless LAN networks.
- c) In a wireless LAN environment, what is a so-called “Distribution system”? Also please explain Wireless LAN roaming within a distribution system.
- d) There are numerous methods for Wireless LAN encryption. Which one of these offers reasonably secure encryption, using a pre-shared key?

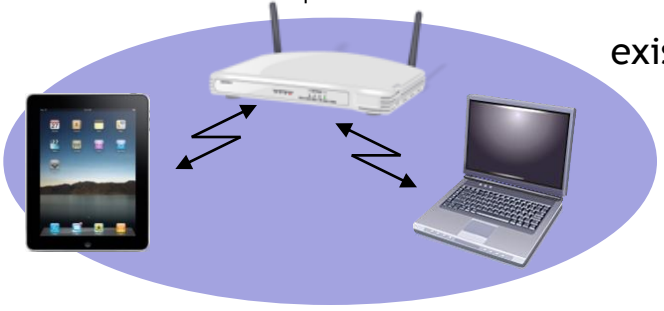
- Components (802.11b)
  - Access Point (AP)  
Sender and receiver station that allows the connecting of **multiple** receiving stations
  - Stations  
End-systems that establish a wireless connection e.g. by using an Access Point (e.g. a notebook with built-in Wireless LAN)



## Infrastructure Network



## existent cable based Network

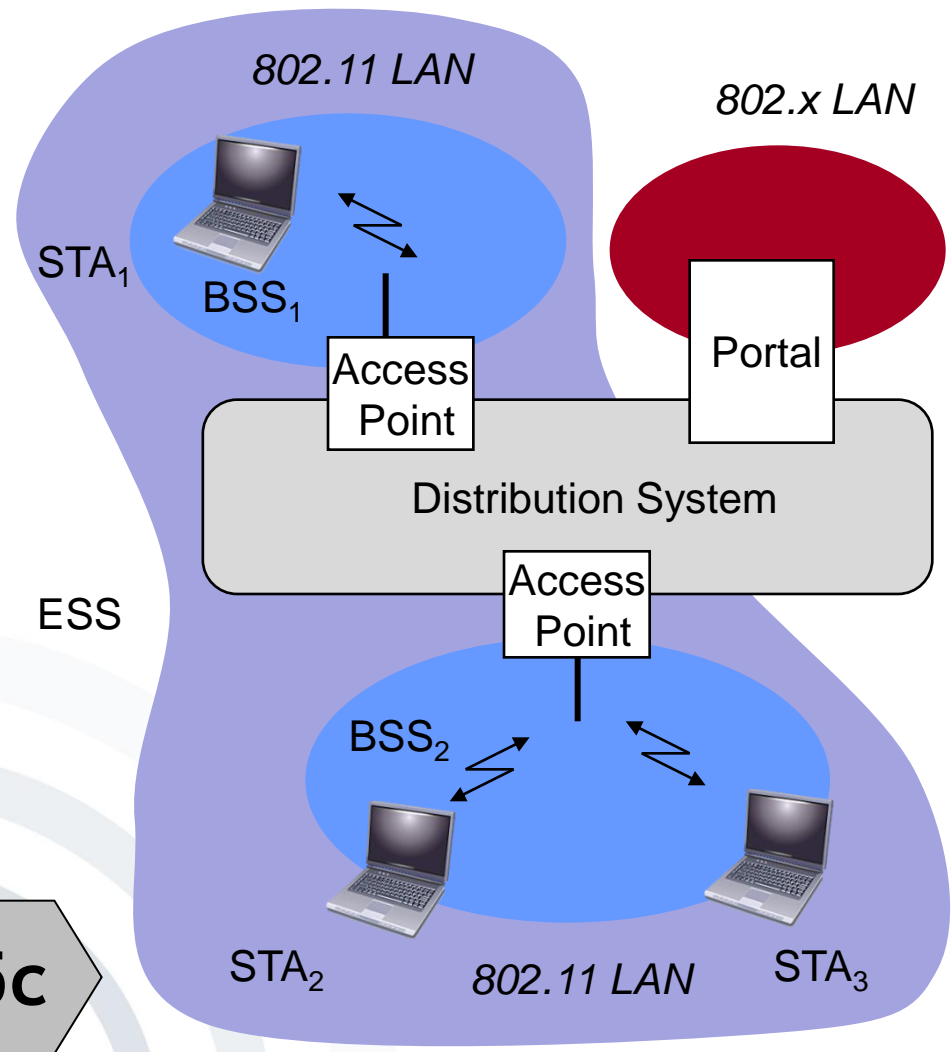


## Ad hoc Networks



5b

[Based on Sauter2008]



## Station (STA)

- Computer with access to the wireless medium and radio
- Contact to the AP

## Basic Service Set (BSS)

- Group of stations, which use the same radio frequency

## Access Point

- Station which is integrated into the radio as well as the fixed local area network (distribution system)

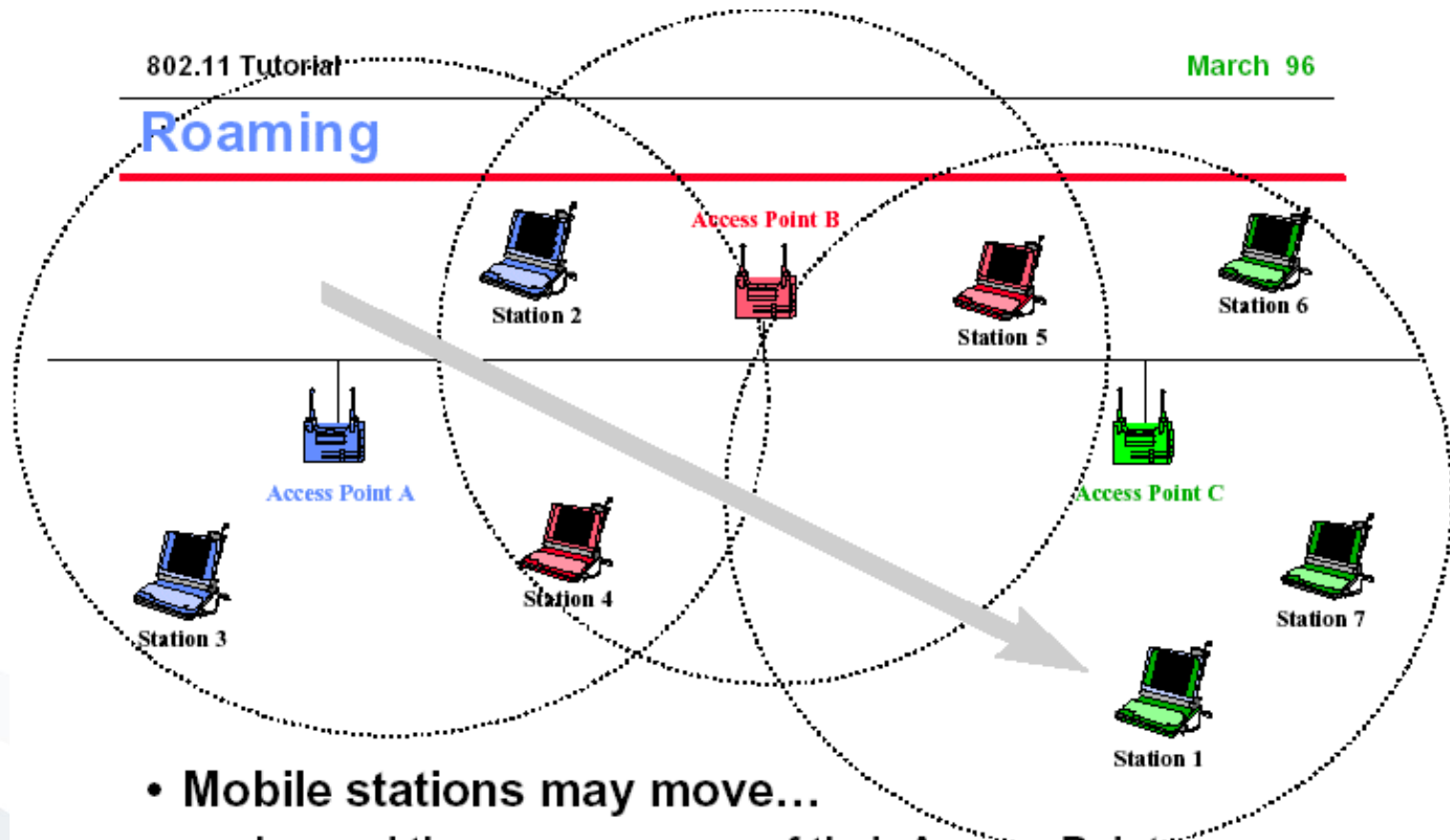
## Portal

- Transfer into another network

## Distribution systems

- Connection of different cells for building up a larger network (EES: Extended Service Set)



5c



- Mobile stations may move...
  - beyond the coverage area of their Access Point
  - but within range of another Access Point
- Reassociation allows station to continue operation

[IEEE1996]

- Approaches to perform roaming
  - By a combination of several Access Points a so-called distribution system is growing.
  - Every Access Point covers one radio cell.
  - Upon leaving a radio cell the station starts scanning for other existing Access Point and tries to connect.
  - Following the connection to a new Access Point the distribution system and the Access Point that was used before will be informed.

- There are numerous methods for Wireless LAN encryption.
- We are only looking at methods that use a pre-shared key (PSK).
- Most encryption methods are outdated and hence insecure:
  - Wired Equivalent Privacy (WEP) 64-bit 
  - Wired Equivalent Privacy (WEP) 128-bit 
- WEP 128-bit can be by-passed within minutes [Heise 2007].



- **Wi-Fi Protected Access** was developed by the Wi-Fi Alliance [Wi-Fi 2010]
- There are two versions of **Wi-Fi Protected Access**, WPA and WPA2:
  - **WPA** includes most of the 802.11i standard.
  - **WPA2** includes **802.11i** to full extent and also the Advanced Encryption Standard (AES).



- This set of slides is based upon the following lectures:
  - ***Lecture 2:*** Mobile Telecommunication Infrastructures
  - ***Lecture 3:*** Wireless internet-oriented Infrastructures and Protocols
  - ***Lecture 4:*** Mobile Communication Services