mobile business

Exercise 1

Technology Basics I

Mobile Business I (WS 2017/18)

Ahmed Seid Yesuf

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

Overview

Practical Exercise 1 - Technology Basics

- Exercise 1: Cell-based communication
- Exercise 2: Data Transmission
  Paradigms for data transmission
- Exercise 3: Mobile Telecommunication Infrastructures
- Exercise 4: Classic Mobile Communication Services
- Exercise 5: Wireless LAN Components and Infrastructures

mobile business

Exercise 1: Cell-based communication (from L02)

a) What does **cell-based communication** mean and what are the implications,

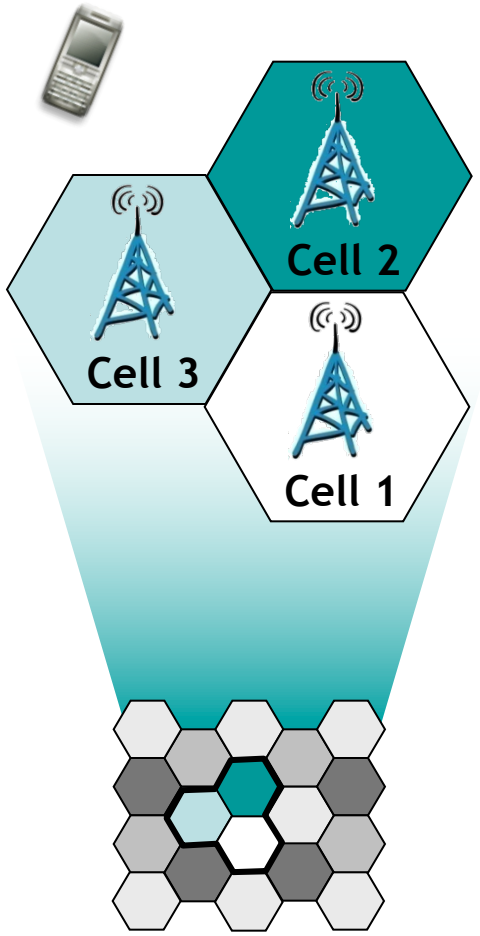
- basic principle,
- physical form,
- dependencies?

1a

Cell Based Communication (CBC)

What is a Cellular Network?

- 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.



[Sauter2008]

1a

Exercise 1: Cell-based communication

b) Write down the **advantages and drawbacks of cellular networks** compared to alternative solutions.

1b

Cell Based Communication (CBC)

Advantages of CBC (1)

- Cellular networks offer a number of advantages compared to centralised radio systems:
  - ***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

1b

[Sauter2008]

Cell Based Communication (CBC)

Advantages of CBC (2)

- 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

1b

[Sauter2008]

Cell Based Communication (CBC)

Disadvantages of CBC

- 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.

1b

[Sauter2008]

Exercise 1: Cell-based communication

c) In this context, explain “**Multiplexing**” and **why it is used** in communication systems.

1c

Cell Based Communication (CBC)

Multiplexing

- 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)

1c

Exercise 1: Cell-based communication

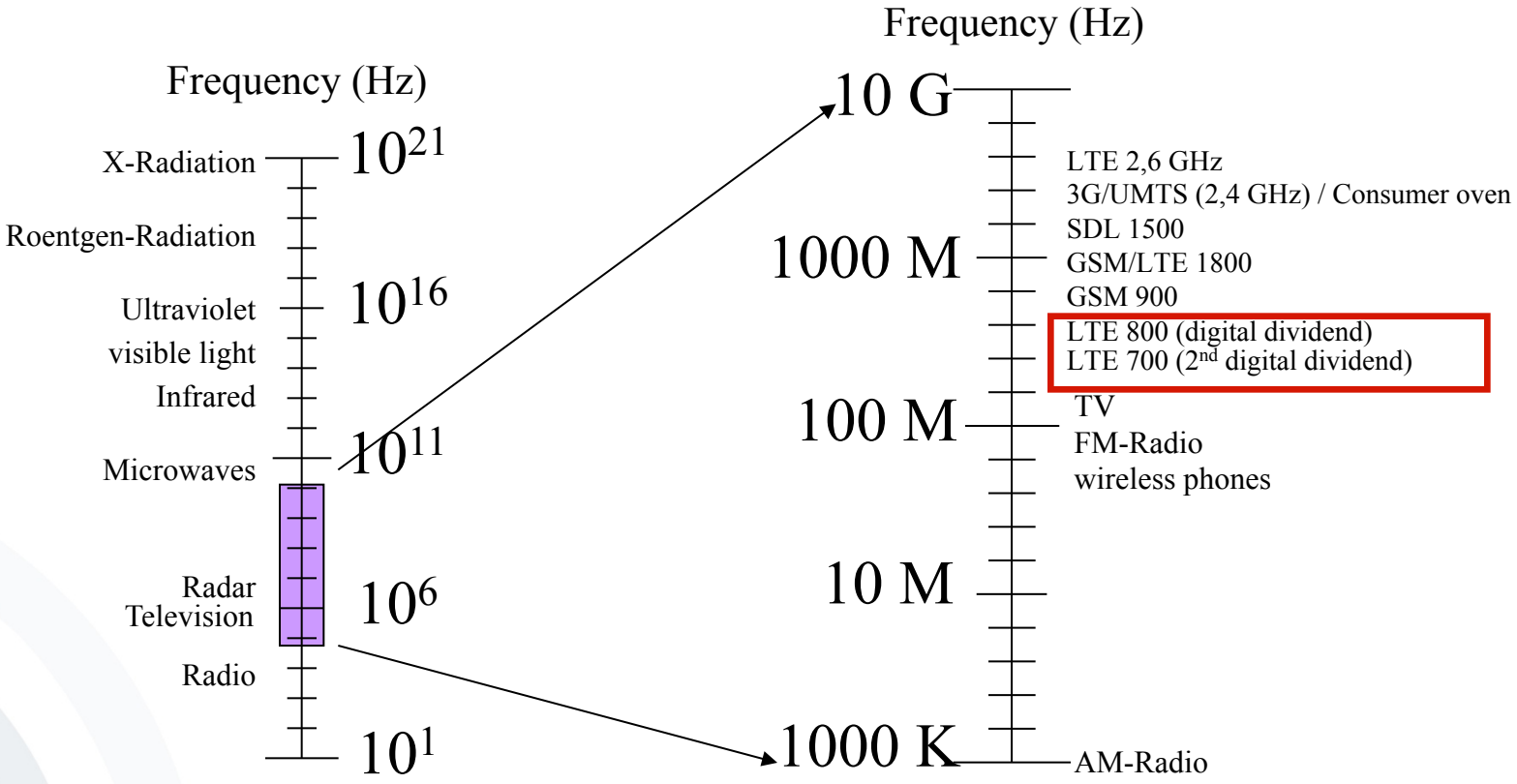
d) Explain the term “digital dividend”.

1d

Cell Based Communication (CBC)

Spectrum Ranges

Frequency range of instruments of entertainment and communication electronics



1d

Cf. [Heise2014] for more information on discussion related to the digital dividend.

Overview

Practical Exercise 1 - Technology Basics

- Exercise 1: Cell-based communication
- Exercise 2: Data Transmission
  Paradigms for data transmission
- Exercise 3: Mobile Telecommunication Infrastructures
- Exercise 4: Classic Mobile Communication Services
- Exercise 5: Wireless LAN Components and Infrastructures

Exercise 2: Data Transmission Paradigms (from L02)

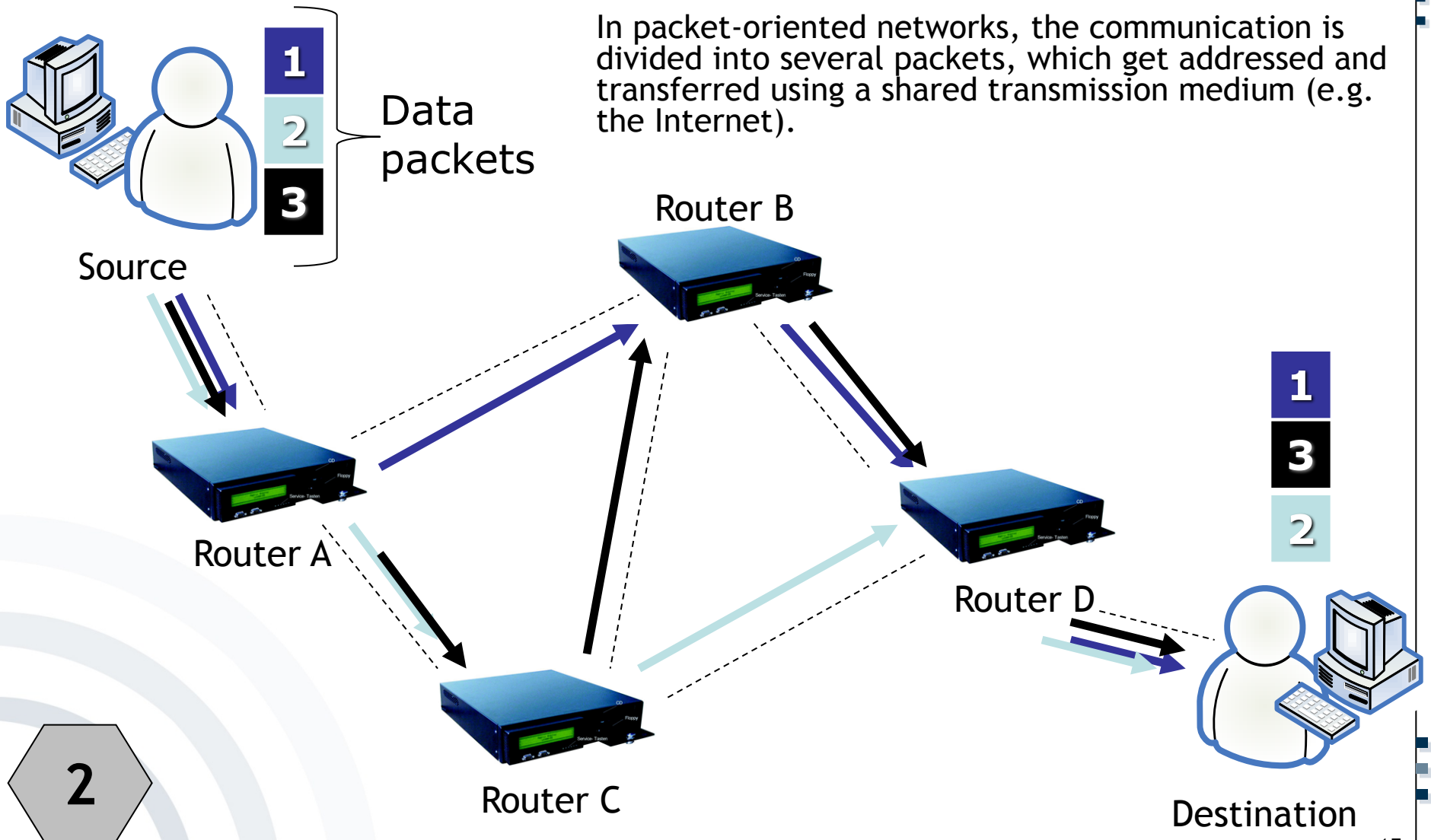
a) What are the **characteristics** (including advantages and disadvantages) of

(i) **packet-oriented** and

(ii) **circuit-switched** mobile data services?

Mobile Data Services
Packet-Oriented Networks

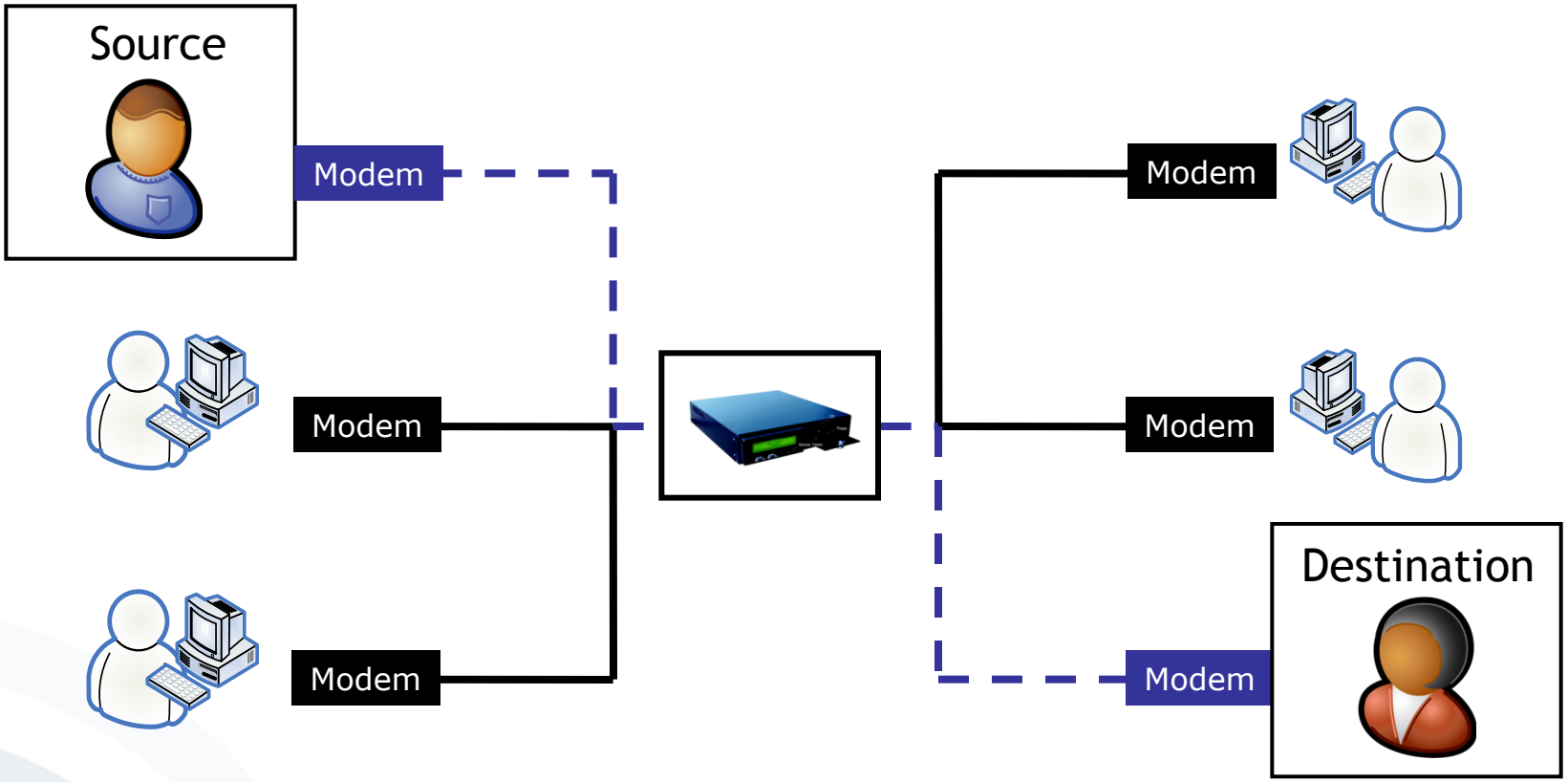
In packet-oriented networks, the communication is divided into several packets, which get addressed and transferred using a shared transmission medium (e.g. the Internet).



2

[M-Chair]

Mobile Data Services
Circuit-Switched Networks



2

In circuit-switched networks, the communication line is used exclusively for the communicating parties (similar to the phone system, CSD and HSCSD).

[M-Chair]

Mobile Data Services
Data Transmission Paradigms

There are two major paradigms for data transmission in communication networks:

- ***Circuit-Switched:*** In circuit-switched networks, the communication line is used exclusively for the communicating parties.
  - Connections are **exclusive** ➲ even if no data is transferred, the network resources are used.
  - In reality, the typical usage for voice connections is 30% of the network's capacity - for data transmission it is less than 10%.
  - The ***duration of a connection*** is used for billing purposes
  - Example: *Circuit Switched Data (CSD)* and *High-Speed Circuit Switched Data (HSCSD)* for Mobile Data Services

- ***Packet-Oriented:*** In packet-oriented networks, the communication is divided into several packets, which get addressed and transferred using a **shared** transmission medium.
  - The connection is kept all the time (always on). However, the network is only used when data is transmitted.
  - The capacity of the communication network is allocated dynamically.
  - For billing purposes, the ***amount of transferred data*** is used.
  - Example: GPRS for Mobile Data Services

[Schiller2003]

Exercise 2: Data Transmission Paradigms for Mobile Data Services

- Order of packets is not guaranteed (routing!)
- Possibly wide variation in the delay of packets

- **Quality of service (QoS)** and the **reservation of resources** help to avoid network congestion-related issues
  - QoS defined by ITU in 1994: Requirements on all the aspects of a connection

General Packet Radio Service (GPRS)

- First packet-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.
- Packet-orientation implies the introduction of new billing methods.

2

[Sauter2008]

Mobile Data Services
General Packet Radio Service (GPRS)

- 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).

2

[Sauter2008]

Mobile Data Services
General Packet Radio Service (GPRS)

- 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).

2

[Sauter2008]

Overview

Practical Exercise 1 - Technology Basics

- Exercise 1: Cell-based communication
- Exercise 2: Data Transmission Paradigms for data transmission
- Exercise 3: Mobile Telecommunication Infrastructures
- Exercise 4: Classic Mobile Communication Services
- Exercise 5: Wireless LAN Components and Infrastructures

Exercise 3: Mobile Telecommunication Infrastructures

a) Which are the three “security services” offered by GSM?

3a

GSM (2G)
Security Model

The GSM system offers different “security services“:

1. **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
2. **Confidentiality:**
   - Data & voice transferred between mobile station and BTS are encrypted.
3. **(Partial) Anonymity:**
   - No transfer of data which can identify the subscriber via radio, instead temporary identification
   - (Temporary Mobile Subscriber ID, TMSI)

3a

Exercise 3: Mobile Telecommunication Infrastructures

b) Please outline and comment on the security model of the GSM infrastructure regarding

1. subscriber authentication (challenge-response procedure for subscriber authentication)
2. confidentiality (encryption of voice and data)
3. (partial) anonymity

3b

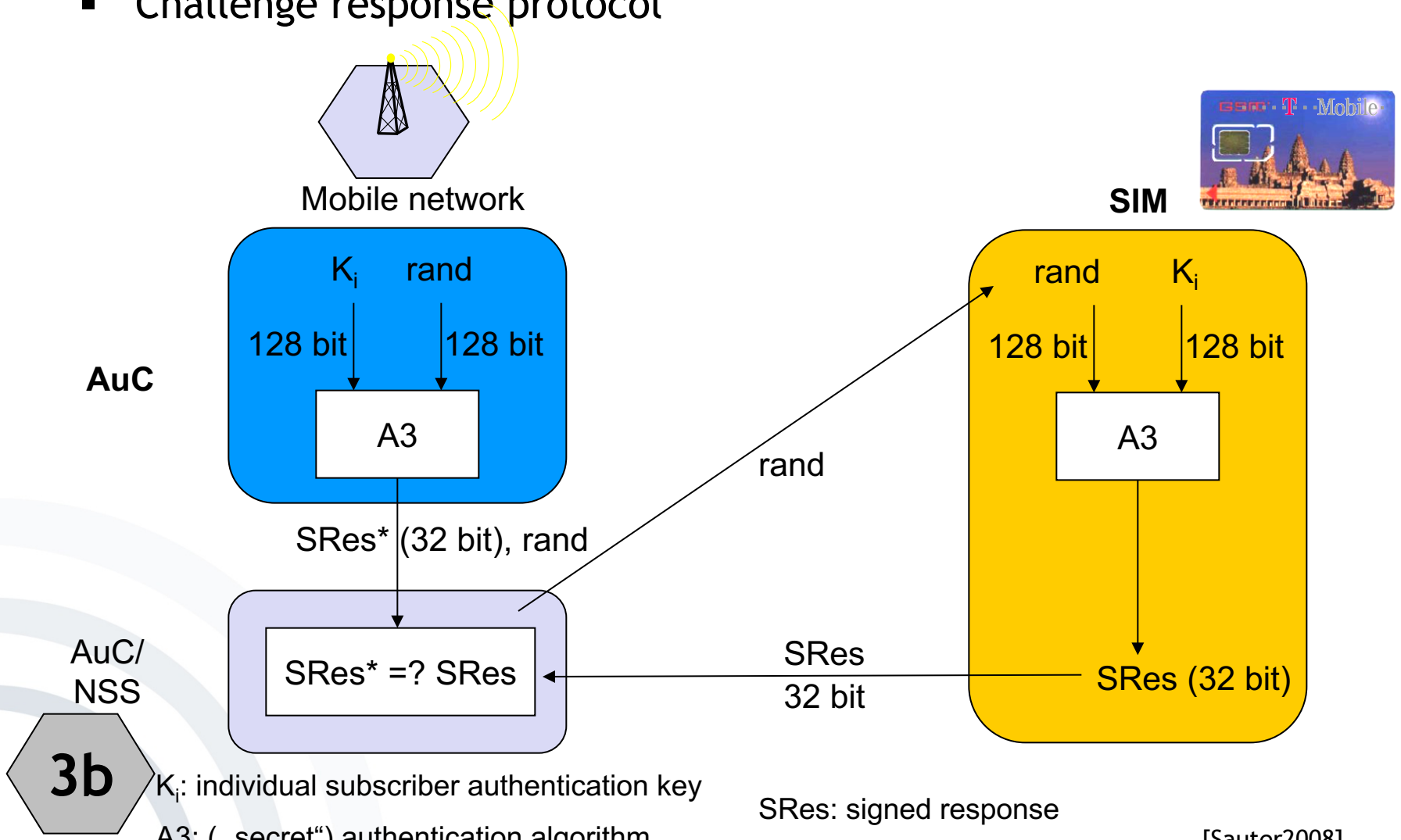
1. Subscriber authentication using Challenge-Response-Procedure

3b

GSM (2G)

SIM based subscriber authentication

- Challenge response protocol



GSM (2G)
Security Model

- 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.

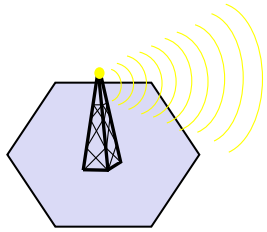
3b

2. Confidentiality:
   Encryption of voice and data transferred via the air interface

3b

GSM (2G)

Security Model – Encryption



mobile radio network

MS with SIM

AuC

SIM

K_i rand

rand

rand K_i

128 bit 128 bit

128 bit 128 bit

A8

A8

A8 for key computation
("secret")

K_c
64 bit

K_c
64 bit

data block

coded
data blocks

data block

BTS

MS

A5

A5

A5 for encryption

3b

[Sauter2008]

- **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.

3b

3. 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.

3b

Exercise 3: Mobile Telecommunication Infrastructures

c) Name the weaknesses of the GSM security model and describe in particular the possible consequences resulting from these weaknesses.

3c

GSM (2G)

Security Model – Shortcomings

- 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.

3c

GSM (2G)

Security Model – Shortcomings

- 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.

3c

Exercise 3: Mobile Telecommunication Infrastructures

d) What are the additional security features which were implemented in 3G (UMTS) networks compared to those of GSM?

3d

- 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.

3d

Overview

Practical Exercise 1 - Technology Basics

- Exercise 1: Cell-based communication
- Exercise 2: Data Transmission Paradigms for data transmission
- Exercise 3: Mobile Telecommunication Infrastructures
- Exercise 4: Classic Mobile Communication Services
- Exercise 5: Wireless LAN Components and Infrastructures

Exercise 4: Mobile Communication Services

a) Which are the so-called Classic Mobile Communication Services?

Classic Mobile Communication Services

- Voice / Fax Service
- Short Message Service (SMS)
- Mobile Data Services

Exercise 4: Mobile Communication Services

b) Please describe each one of these services.

4b

Classic Mobile Communication Services

- **Voice / Fax Service**
  - Regular telephone service and emergency call
  - Speech signals are digitally coded, using a bidirectional, symmetric, full-duplex point-to-point connection.
  - Capable of sending and receiving “Group 3” fax transmissions

4b

Classic Mobile Communication Services

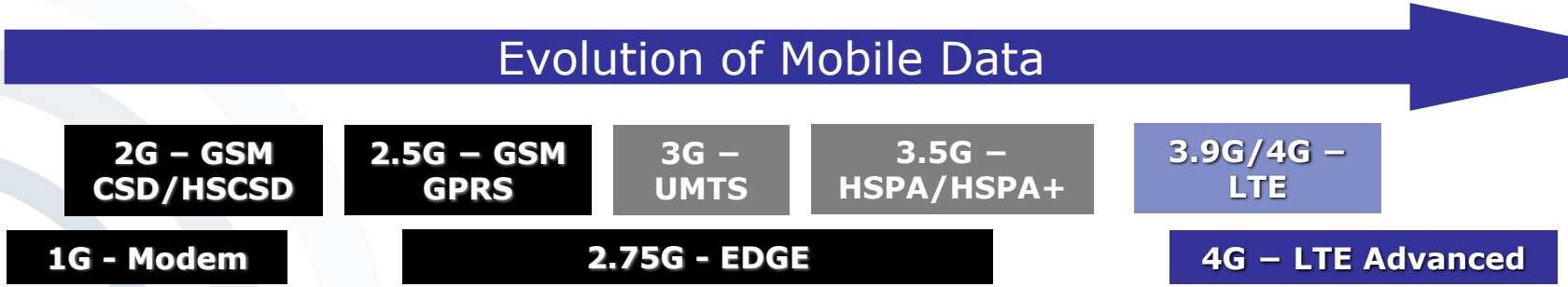
- Short Message Service (SMS)
  - Allows to send and receive short messages of up to 160 characters
    - ***7Bit***: 160 characters (plain text)
    - ***8Bit***: 140 characters (ASCII)
    - ***16Bit***: 70 characters (Unicode)
  - Several SMS types exist:
    - *Point-to-point SMS* (single recipient)
    - *Point-to-multiple SMS* (several recipients)
    - *Cell broadcast SMS* (all users in a cell are recipients)
  - Combination with other value added services (e.g. automated mailbox notification)
  - Messages are sent to an SMS service centre (SMSC) and are processed in a *store-and-forward mode*, meaning that messages that cannot be relayed will be stored and sent again later.

4b

Mobile Data Services

- **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 (57.6 Kbit/s max.)
- ***GPRS*** (General Packet Radio Service)
- ***EDGE*** (Enhanced Data Rates for Global Evolution)

4b



Exercise 4: Mobile Communication Services

c) Mobile Data is one of the Classic Mobile Communication Services above.

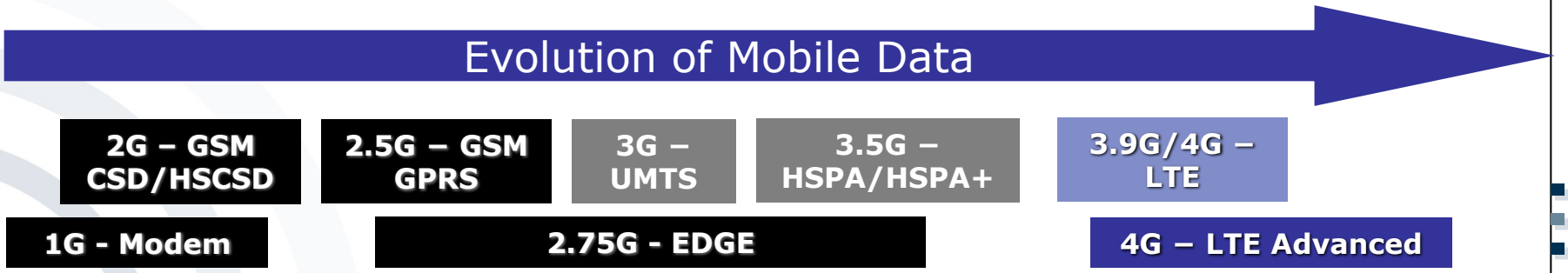
When looking at GSM networks, which are the relevant Mobile Data Services?

4c

Mobile Data Services

- **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 (57.6 Kbit/s max.)
- ***GPRS*** (General Packet Radio Service)
- ***EDGE*** (Enhanced Data Rates for Global Evolution)

4c



Overview

Practical Exercise 1 - Technology Basics

- Exercise 1: Cell-based communication
- Exercise 2: Data Transmission Paradigms for data transmission
- Exercise 3: Mobile Telecommunication Infrastructures
- Exercise 4: Classic Mobile Communication Services
- Exercise 5: Wireless LAN Components and Infrastructures

Exercise 5: Wireless LAN

a) What are the components in a Wireless LAN?

Components

- Components (802.11b)
  - Access Point (AP)

    Sender and receiver station that allows the connecting of **multiple** receiving stations

  - Stations

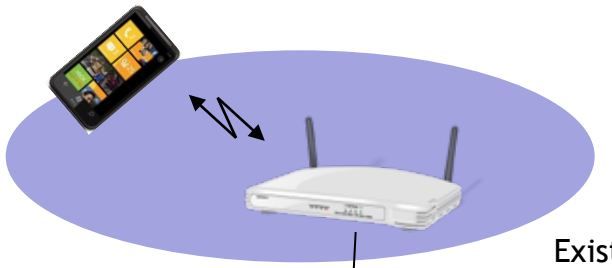
    End-systems that establish a wireless connection e.g. by using an Access Point (e.g. a notebook with built-in Wireless LAN)

5a

Exercise 5: Wireless LAN

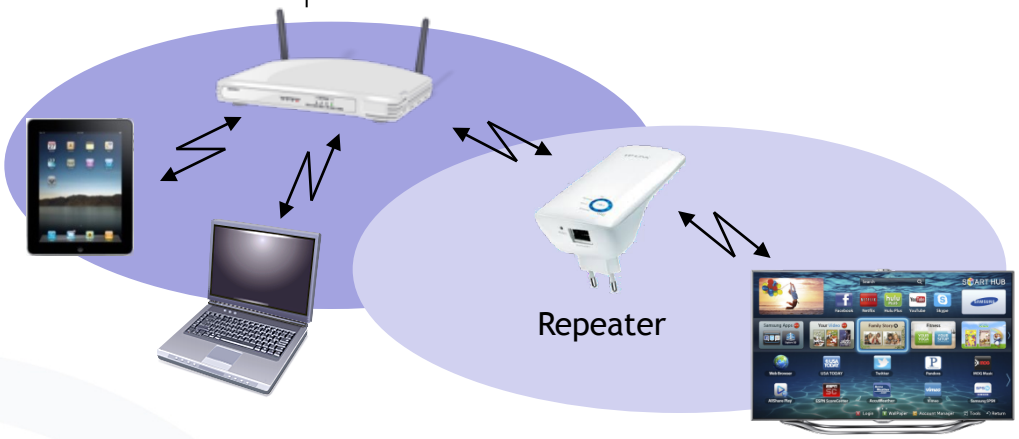
b) Name two types of Wireless LAN networks.

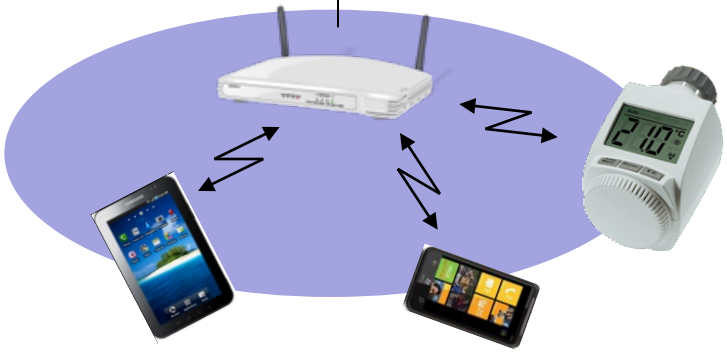
Wireless LAN Infrastructures



Infrastructure Network

Existing cable based Network





Ad hoc Networks

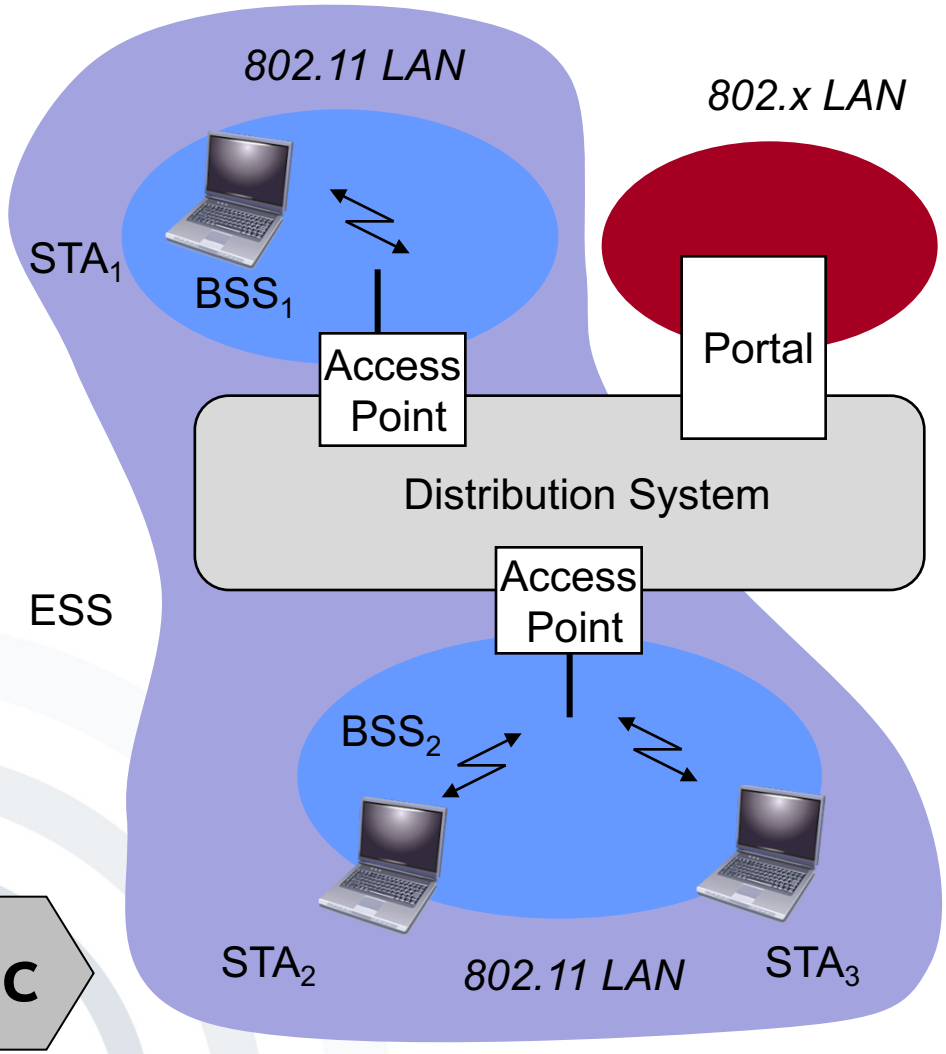
5b

Based on [Sauter 2008]

Exercise 5: Wireless LAN

c) In a wireless LAN environment, what is a so-called “Distribution system”? Also please explain Wireless LAN roaming within a distribution system.

Wireless LAN “Roaming”



Station (STA)

- Computer with access to the wireless medium and radio connect 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

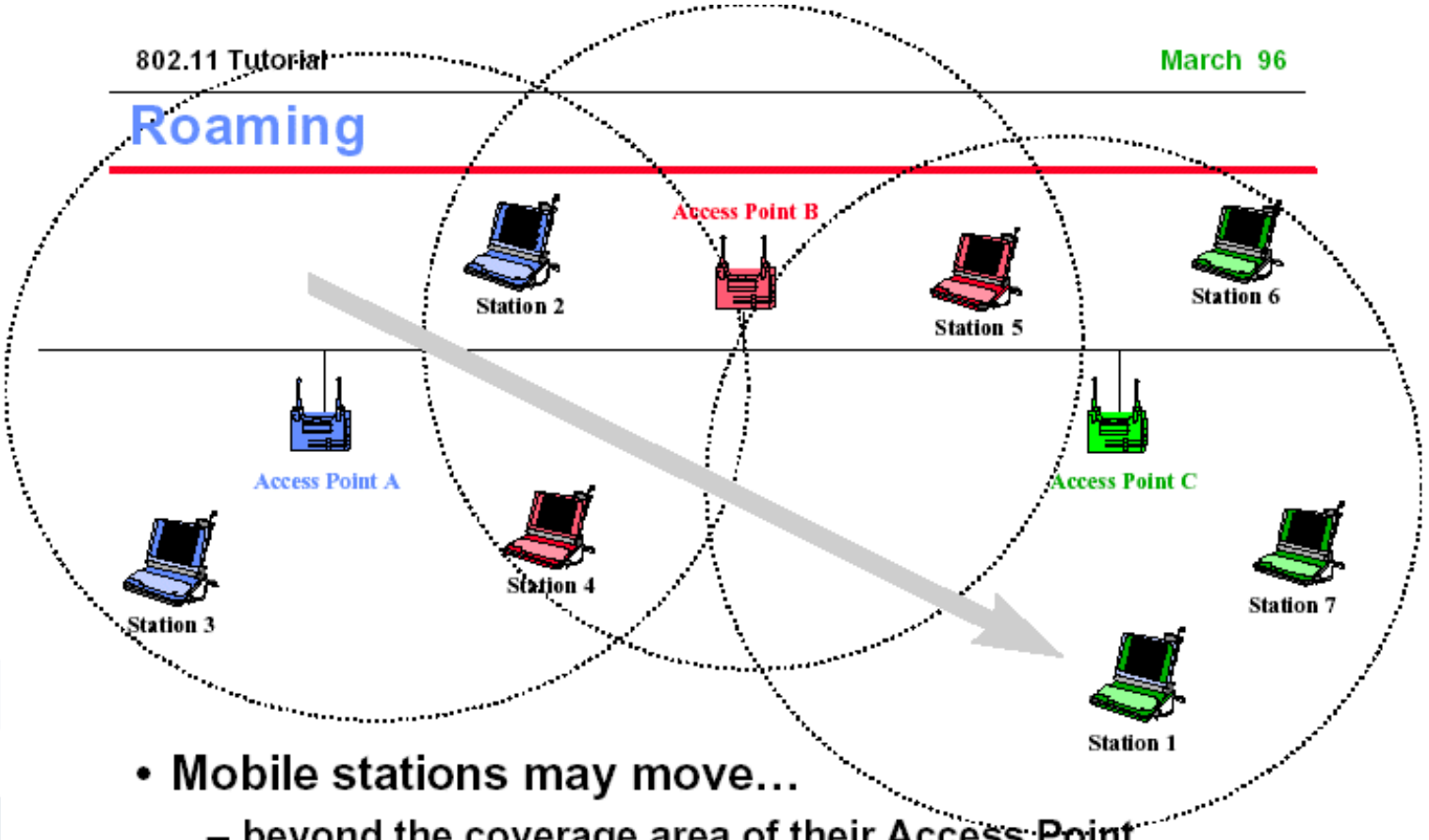
- Transfer into another network

Distribution systems

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

5c

Wireless LAN Roaming



- 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]

5c

Wireless LAN Roaming

- 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.

5c

Exercise 5: Wireless LAN

d) There are numerous methods for Wireless LAN encryption. Which one of these offers reasonably secure encryption, using a pre-shared key?

Wireless LAN state-of-the art encryption

- 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].

5d

Wireless LAN
State-of-the art Encryption

- **Wi-Fi Protected Access (WPA)** 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, but is **outdated and insecure** as it has various weaknesses:
    - Vulnerability to dictionary attacks when using a weak PSK
    - Other weaknesses inherited from earlier standards [ArsT 2008]
  - **WPA2** includes **802.11i** to its full extent and also the Advanced Encryption Standard (AES).

5d

Key Reinstallation Attacks (KRACKs) against WPA2

- The attack is mainly against the ***4-way handshake*** of the WPA2 protocol.
- The 4-way handshake protocol is mathematically proven, but it only assures the negotiated key remains secret, and that handshake messages cannot be forged.
- The attack doesn't leak the encryption key, but sensitive information (usernames, passwords, …) can be stolen.
- *Demo how to perform the attack – KRACK*
  https://www.youtube.com/watch?time_continue=4&v=Oh4WURZoR98

Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

Mathy Vanhoef
imec-DistriNet, KU Leuven
Mathy.Vanhoef@cs.kuleuven.be

Frank Piessens
imec-DistriNet, KU Leuven
Frank.Piessens@cs.kuleuven.be

https://www.krackattacks.com/

Literature

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