ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Communication Systems

GSM

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer

CoNe
Freiburg

IIF
INSTITUT FÜR
INFORMATIK
FREIBURG

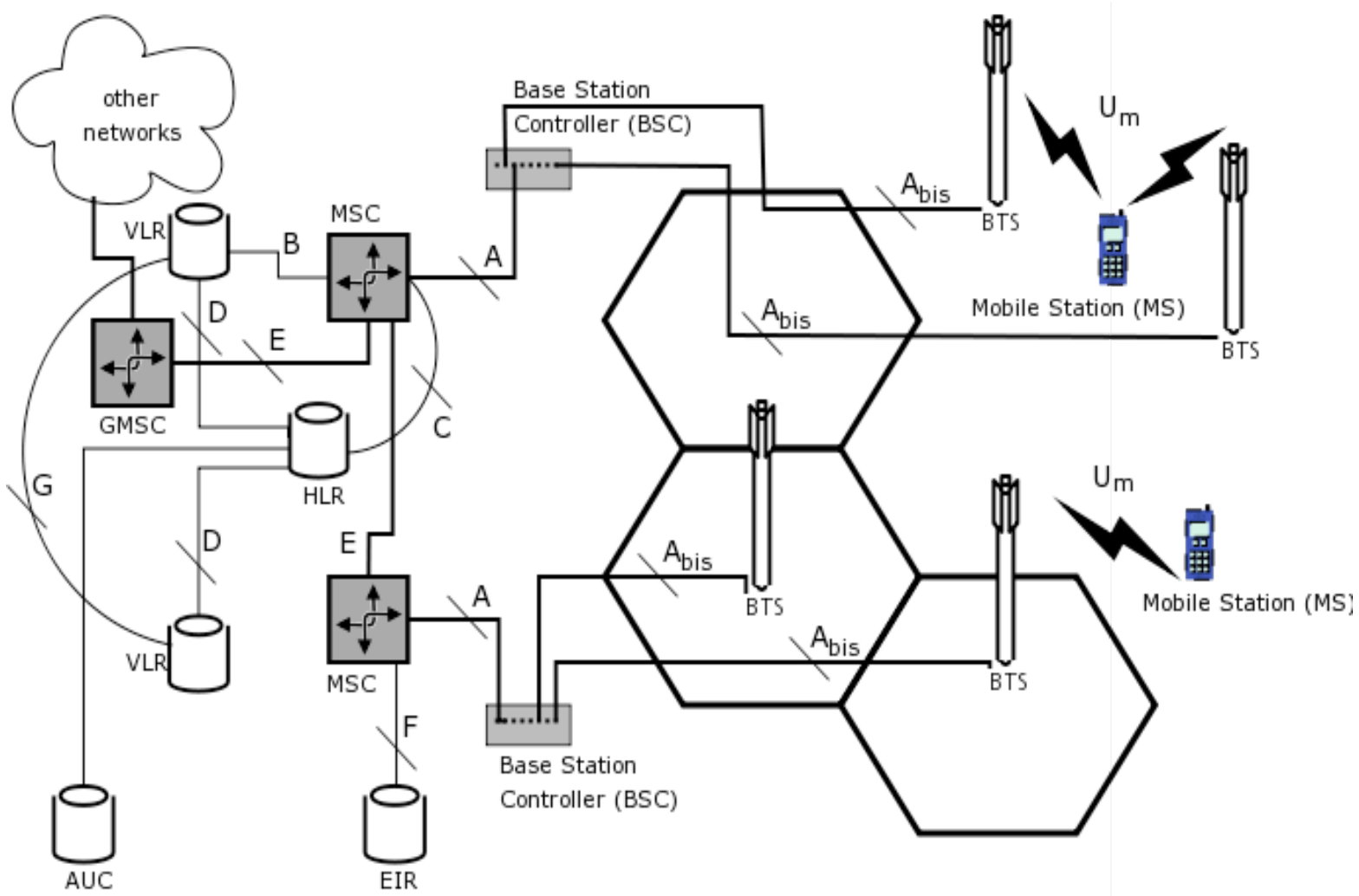
Organization

- I. Data and voice communication in IP networks
- II. Security issues in networking
- **III. Digital telephony networks and voice over IP**

last to final lecture

- Extension of GSM overview
  - GSM interfaces
  - GSM network components
    - Mobile switching center,visitor location register, home location register, authentication center, mobile stations, SIM, radio subsystem...
  - Radio interface Um, Control channels, Network control, SS7
  - Call setup
  - Authentication, Authorization, Access - Security issues will be handled in the last lecture
- Practical part will deal with a software telephony switching system – many of the implemented features are derived from the traditional telephony systems

GSM interfaces and components



GSM interfaces and components

- Like in the digital telephony network interfaces between the different components are defined
  - Um is the radio interface (m for mobile) between the mobile stations and the base station transceiver, modeled after the user interface in the ISDN world (Uk0 , UG2)
  - Abis is the interface between BTS and BSC
  - A the interface of the BSC to the MSC
- The network subsystem defines the following interfaces
  - B between MSC and visitor location register (VLR)
  - C between MSC and home location register (HLR)

GSM interfaces and components

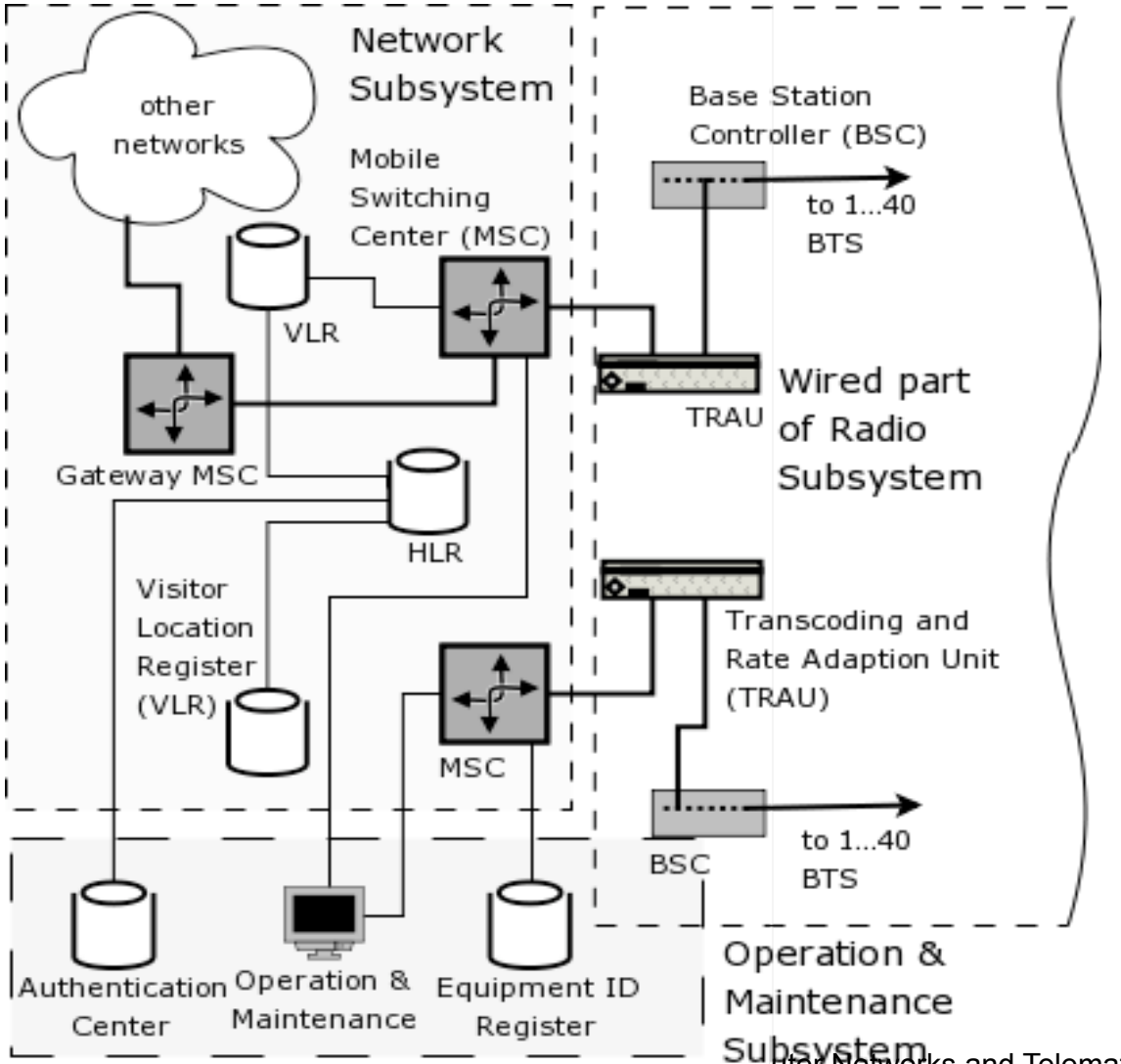
- The several MSC are interconnected via
  - E interfaces, this is the interface to Gateway MSC too
  - F defines the interface to the equipment identifier register (EIR)
  - The different VLR talk to each other (needed when hand-overs between different MSC occur) via G interface
- Operation & Maintenance Subsystem (OSS) is the whole systems management layer
  - Network measurement and control functions
  - Monitored and initiated from the OMC (Operation and Maintenance Center)
  - Network Administration

GSM interfaces and components

- OMC keeps track of configuration, operation, performance management, statistics
  - Collection and analysis, network maintenance
  - Commercial operation & charging
  - Accounting & billing
  - Security Management, e.g. Equipment Identity Register (EIR) management

GSM network components

- Network and radio subsystem are supervised by OMC
- Many BSCs are controlled by Mobile Switching Center (MSC), which is part of Network subsystem
- Somewhere in between is the TRAU (Transcoding and Rate adaption Unit)



GSM components – network operation, MSC

- A provider network has in general many distributed MSCs
- Thus the MSC is a typical ISDN switching center with additional components for mobility management
  - Many standards and interfaces discussed in last lecture apply here too
  - Controls the access and authorization of mobile subscribers
  - Gets the user data from HLR and copies it to the VLR of all MS in range

GSM components - MSC

- To convert 13kbit/s (from MS), 16kbit/s (from BSC because of some added in-band information) to 64kbit/s ISDN data rate a TRAU is typically included in between MSC and BSC
- Performs all the switching and routing functions of a fixed network switching node and adds specific mobility-related functions, like
  - Allocation and administration of radio resources
  - Management of mobile users
  - Registration, authentication
  - Manages handover execution and control
  - Does paging (search for MS within the BSCs)

GSM components – visitor location register (VLR)

- MSC looks up users and communication information in VLR
  - VLR is a temporary database dynamically updated when subscribers enter or leave vicinity of the serving MSC
  - one database per MSC (or per group of MSCs), typically joint MSC-VLR implementation
  - Idea: Avoid heavy MSC-VRL signaling load on network links
  - VLR entries contain the following information:
    - Every user / MSISDN actually staying in the administrative area of the associated MSC
    - Entry created when an MS enters the MSC area (registration)
    - May store data for roaming users (subscribed to different operators)

GSM components – visitor location register (VLR)

- VLR entries contain the following information:
  - Tracking and routing information
  - Mobile Station Roaming Number (MSRN)
  - Temporary Mobile Station Identity (TMSI) assigned by MSC
  - Location Area Identity (LAI) where MS has registered needed for paging and call setup

GSM components – home location register (HLR)

- While VLR keeps user data only temporarily, the permanent storage of data takes place in HLR
  - Each mobile provider keeps such a database to store its subscribers information
  - Subscriber and subscription data
    - IMSI, MSISDN
    - Parameters (authorization) for additional services
    - info about user equipment (IMEI)
    - Authentication data
  - Service setup for call deflection, mobile phone box, ...

GSM components – authentication center (AUC)

- Typically seen as part of OMC
- Associated to HLR (home location register)
  - Might be integrated with HLR
  - Search key: IMSI
  - Responsible of storing security-relevant subscriber data
  - Subscriber's secret key K_i (for authentication)
  - Shared encryption key on the radio channel (K_c)
  - Algorithms to compute temporary keys used during authentication process

GSM components – mobile stations (MS)

- GSM separates user mobility from equipment mobility by defining two distinct components
- Mobile Equipment (ME)
  - Or Mobile Terminal (MT) – it is the cellular telephone itself (mobile phone hardware)
  - It has its own address / identifier: IMEI (International Mobile Equipment Identity)
- Composed of the technical components for user interaction: keypad, display, speaker and microphone, may contain
  - Interfaces for additional services like fax or data (peripheral connections as Bluetooth, IrDA or serial connections might be available too)

GSM components – mobile stations (MS)

- Five transmit power classes defined for MS in 900MHz band
  - 20, 8, 5, 2, 0.8 Watt – normally used are 8W for vehicular and 0.8W for portable devices
  - Only two classes for 1800MHz band: 1 and 0.25W
- Implementations
  - Early devices were single band for GSM900 or DCS1800 or PCS1900
  - Today mostly so called multi-band phones are sold (allow communication in two or all three GSM bands)
  - Newest devices are multi-mode which could handle both GSM and UMTS (and several data standards like GPRS)

GSM components – mobile stations (SIM)

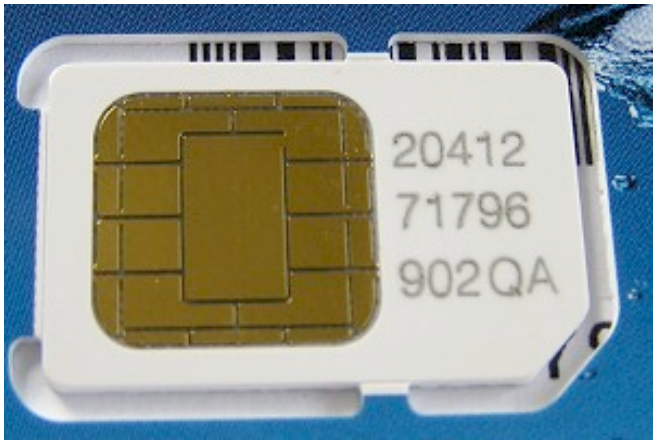
- Second component is the Subscriber Identity Module (SIM)
- SIM keeps the following addresses / identifiers:
  - IMSI (International Mobile Subscriber Identity) – 15-digit composed of Mobile Country Code, Mobile Network Code, Mobile Subscriber Identification Number
  - Is sent (for security reasons only) when entering network or doing location update
  - MSISDN (Mobile Subscriber ISDN number) of 15 digits is the telephone number users call, composed of Country Code (Germany 49, US 1), National Destination Code (Provider prefix without the 0), Subscriber Number

GSM components – mobile stations (SIM)

- The MSISDN is used for routing in traditional telephony networks (but not for routing in mobile)
  - Translated in MSC to TMSI, unique within a certain Location Area (LA), kept in the VLR
- TMSI is temporarily stored on SIM
  - Not fixed, regularly changed to avoid outside user tracking
- Same applies for MSRN (Mobile Station Roaming Number, GSM internally):
  - VCC = country code of visited mobile network
  - VNDC = location code (place where the user actually is)
  - VMSN = ID of the visited MSC
  - VSN = subscriber ID, assigned by VLR

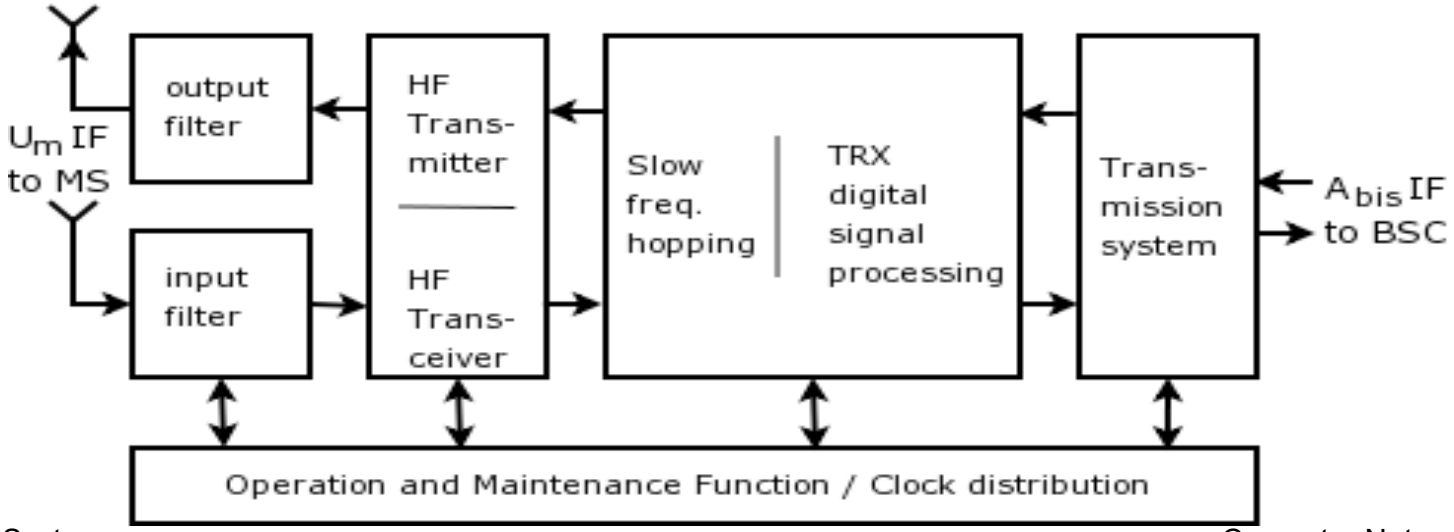
GSM components – mobile stations (SIM)

- MSRN is similarly composed to MSISDN, but location dependent
- SIM itself is piece of hardware, a plug-in-module, a so-called smart-card (or fixed chip within the phone – only on special devices)
  - Usually provided in the ID-000 format, which is about 0,76mm thick plastic with cast-in chip
  - It contains: a CPU, internal bus system connecting RAM and EEPROM and an electrical interface (contact pads on the upper side)



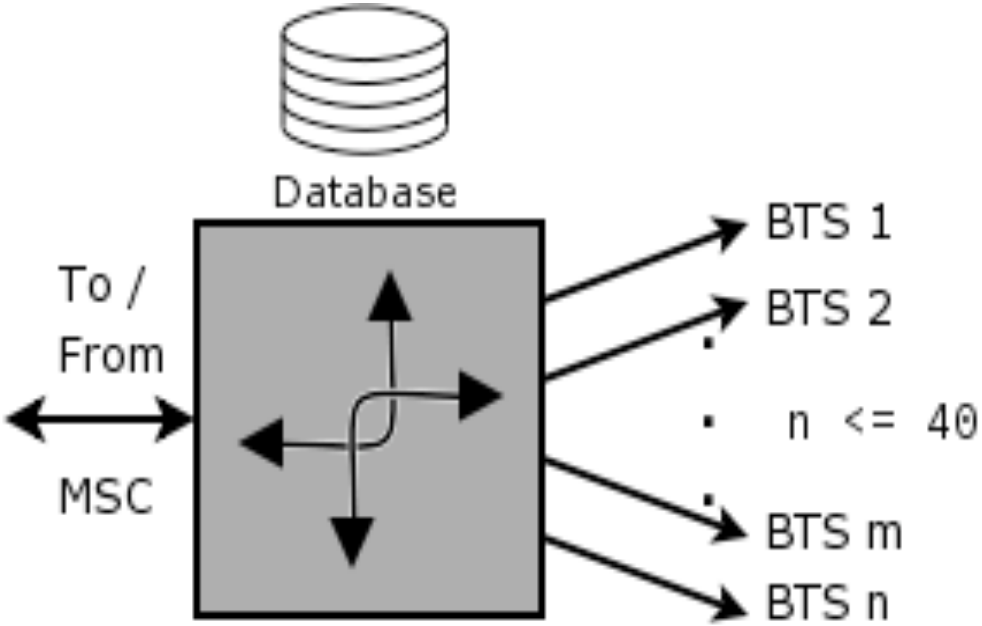
GSM components - radio subsystem (BTS)

- Radio interface functions (MS <-> BTS)
  - GMSK modulation-demodulation
  - channel coding, encryption/decryption
  - burst formatting, interleaving
  - signal strength measurements
  - interference measurements



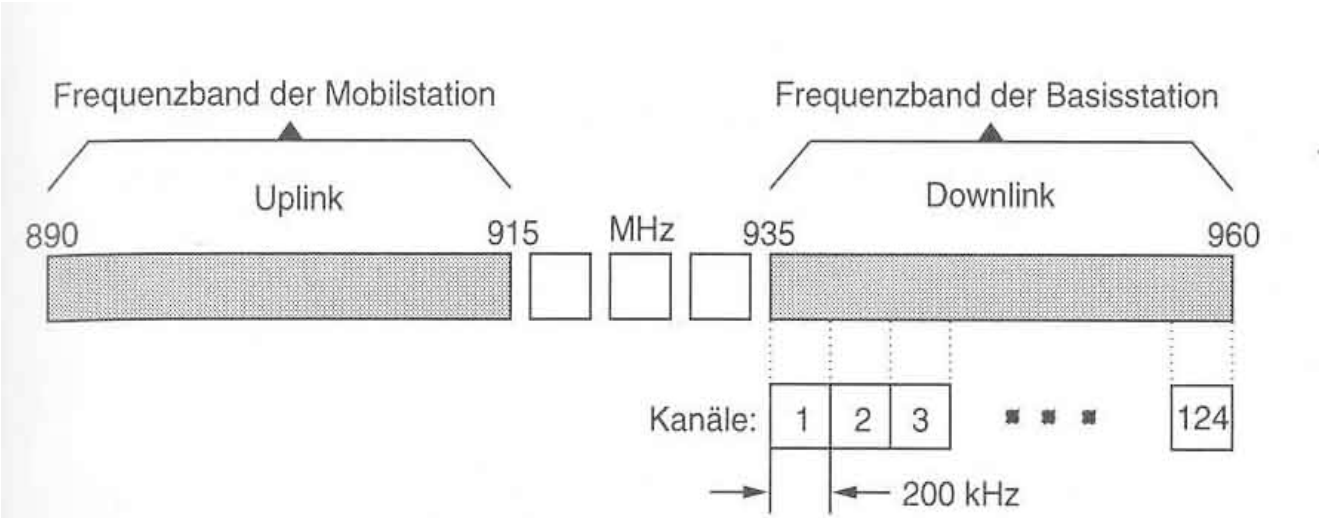
GSM components - radio subsystem (BSC)

- Functions of a BSC
  - One BSC may control up to 40 BTS (kept in database)
  - switch calls from MSC to correct BTS and conversely
  - Protocol and coding conversion for traffic (voice) & signaling (GSM-specific to ISDN-specific)
  - Manage mobility of MS (handover between different BTS)
  - Enforce power control



GSM – the radio interface Um

- Lets start with the physical layer of the beloved OSI model (for the last time)
- Um defines the communication of MS with the GSM infrastructure
- The bandwidth is 270,833kbit/s (bit rate not integer because derived from time slots as explained later)
- Because of the limited frequency band multiplex access is used

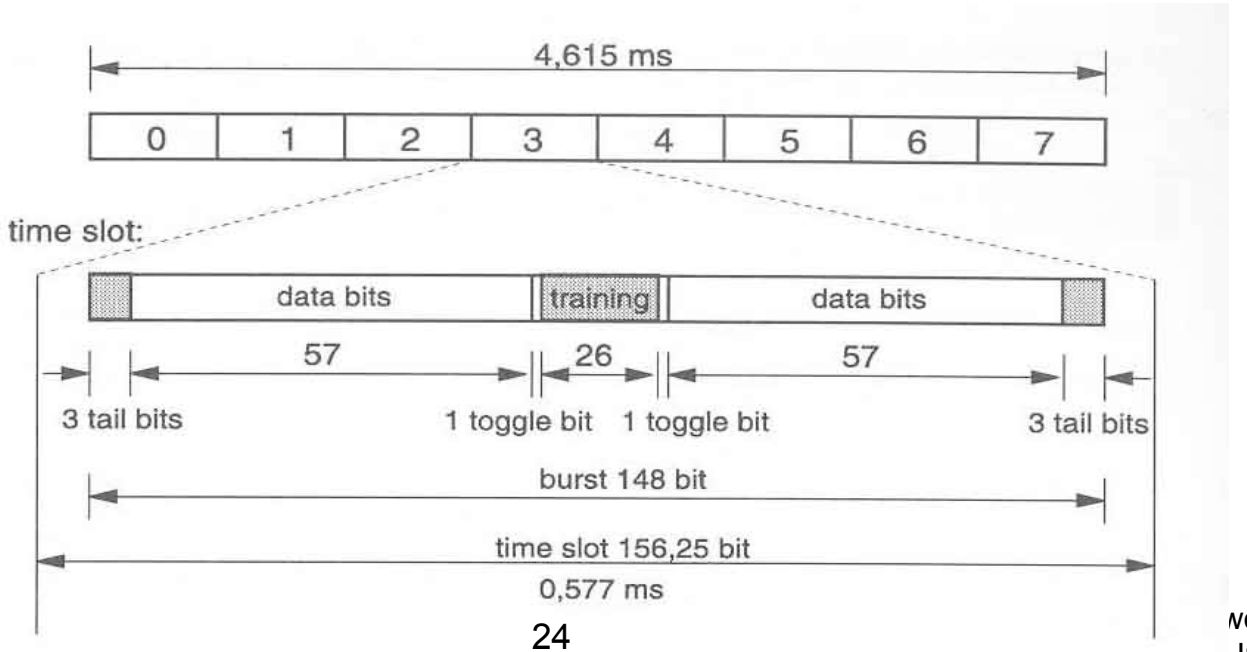


GSM – Um: FDM & TDM

- Frequency Division Multiplexing two 25MHz bands
  - Uplink (MS to BTS) = 890 – 915MHz.
  - Downlink (BTS to MS) = 935 – 960MHz
  - Each defined channel has a 200kHz bandwidth
  - Duplex spacing: 45MHz
  - Thus 124 bearer frequency pairs possible, suggested to use only 122 to keep additional guard top and bottom
  - In practice, due to power control and shadowing, adjacent channels cannot be used within the same cell…
- Additionally in each frequency channel Time Division Multiplexing (TDM) is applied

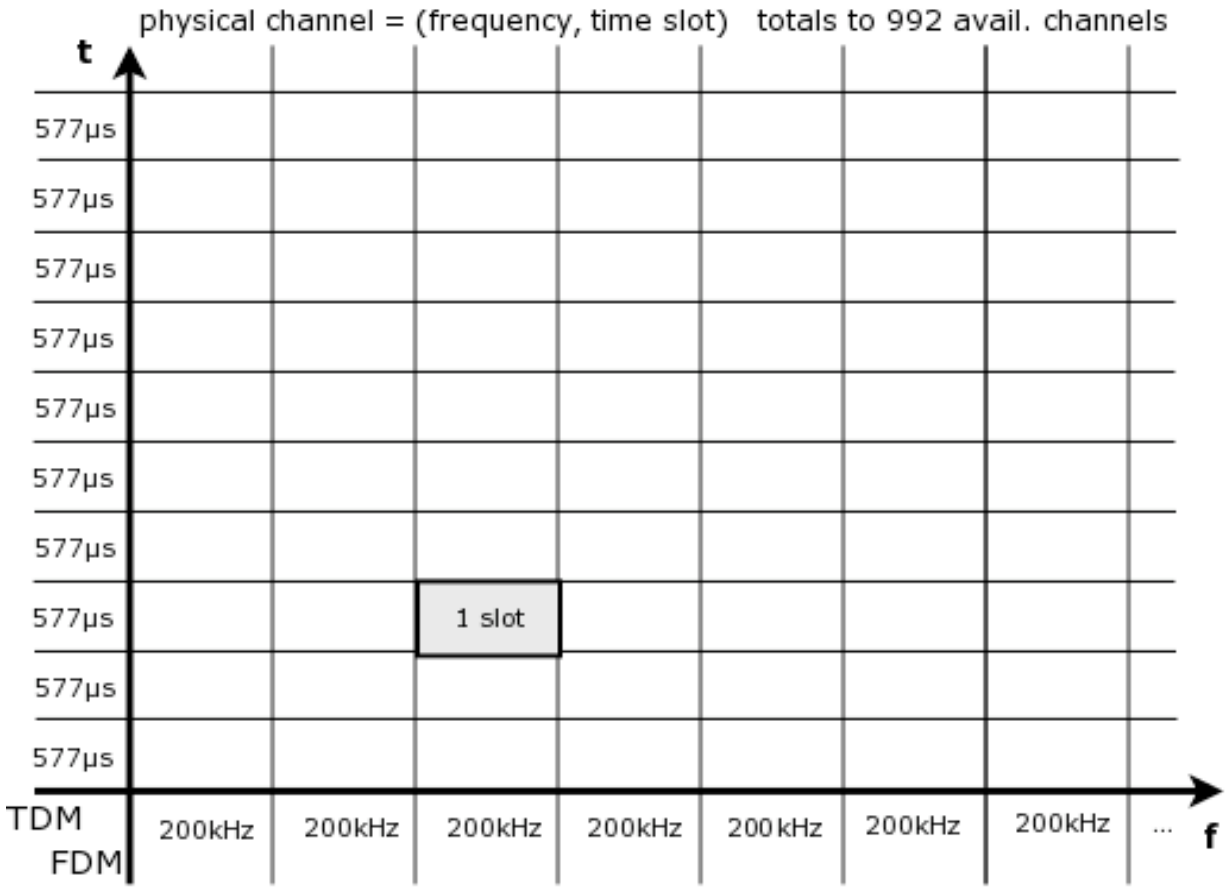
GSM – Um: FDM & TDM

- 8 periodic time slots - 0,577ms each
- TDM frame composed of 8 time slots equals to 4,615ms
- Every time slot a so called “burst” - succession of 148bit is transmitted
- Between the bursts a “security buffer” of 8,25bit/burst is put in between



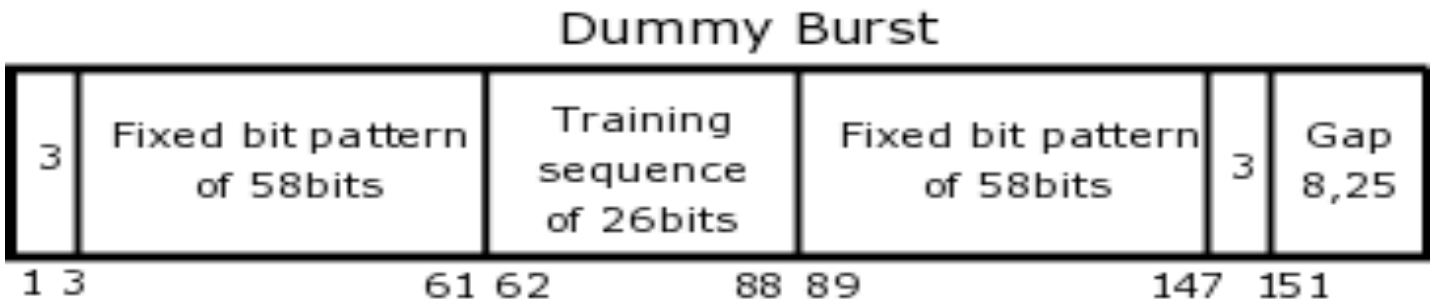
GSM – Um: FDM & TDM

- Through FDM/TDM hybrid in GSM 992 channels available
- In DCS1800 more channels: 75MHz band split into 200kHz channels allows a total of 374 carriers
- Thus 2992 physical channels available in E-GSM



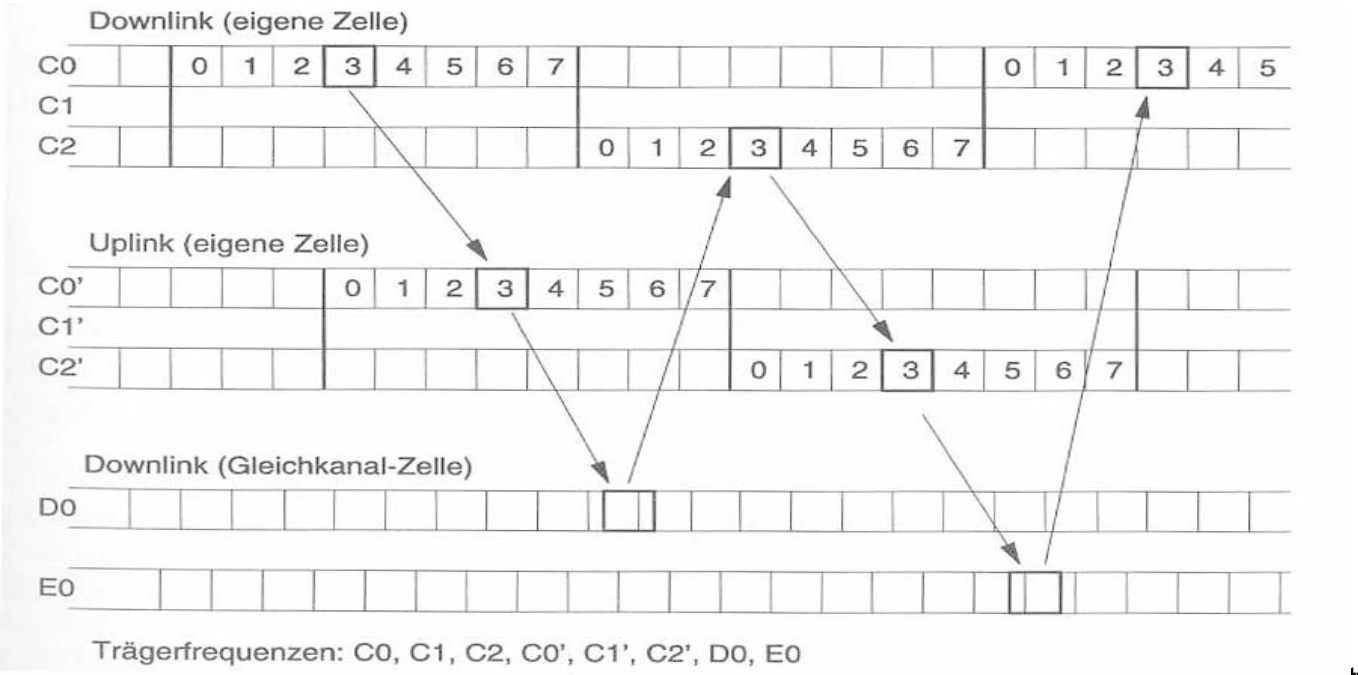
GSM – Um: burst types / dummy burst

- Five different burst types defined
  - Normal Burst
  - Access Burst
  - Frequency Correction Burst
  - Synchronization Burst
  - Dummy Burst to fill in inactive bursts in Broadcast Control Channel (BCCH, direction from BTS to MS) to have most power on this channel (helpful, when MS needs to find BCCH)



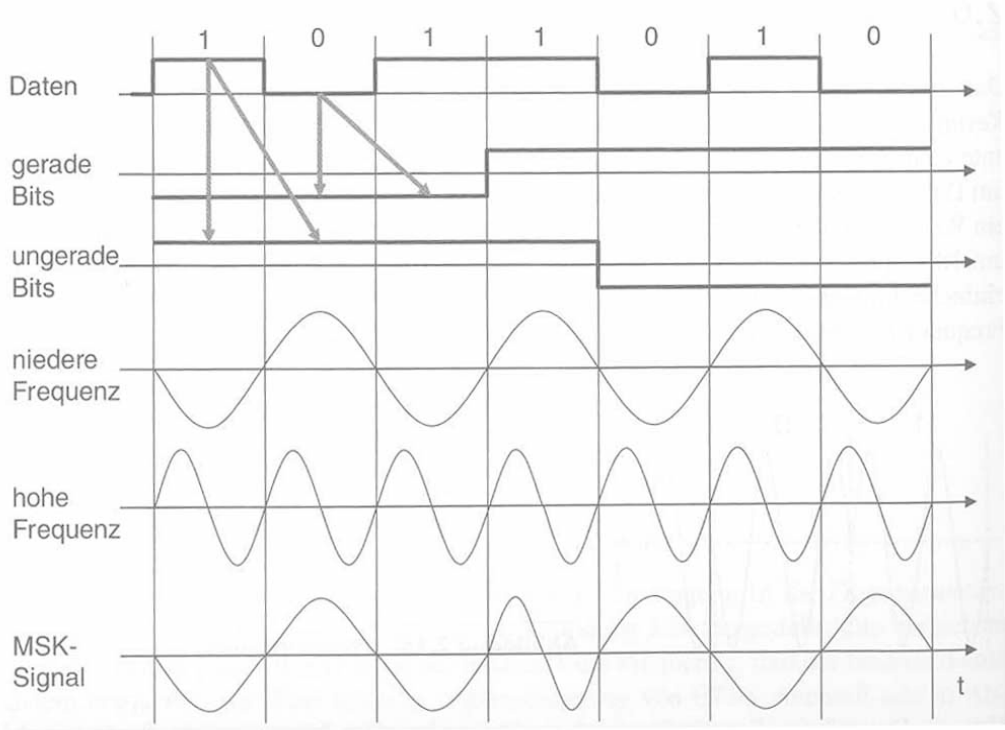
GSM – Um: frequency hopping

- Not all channels in a given cell are of equal quality and multi path reception / adjacent channels may disrupt communication
- Thus frequency hopping is introduced
  - avoid frequency-selective fading, co-channel interference



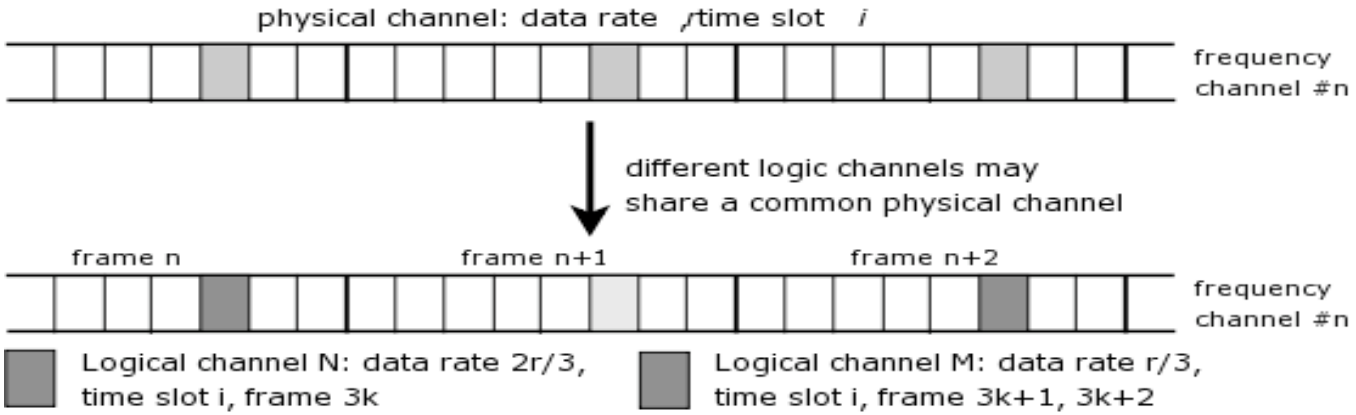
GSM – Um: GMSK modulation

- Split single bits into odd and even
- Double the time period of each bit
- Four cases
  - Bg=Bu=0 use f2 inverted
  - Bg=1,Bu=0 use f1 inv.
  - Bg=0,Bu=1 use f1
  - Bg=1, Bu=1 use f2



GSM – the Um logical layer

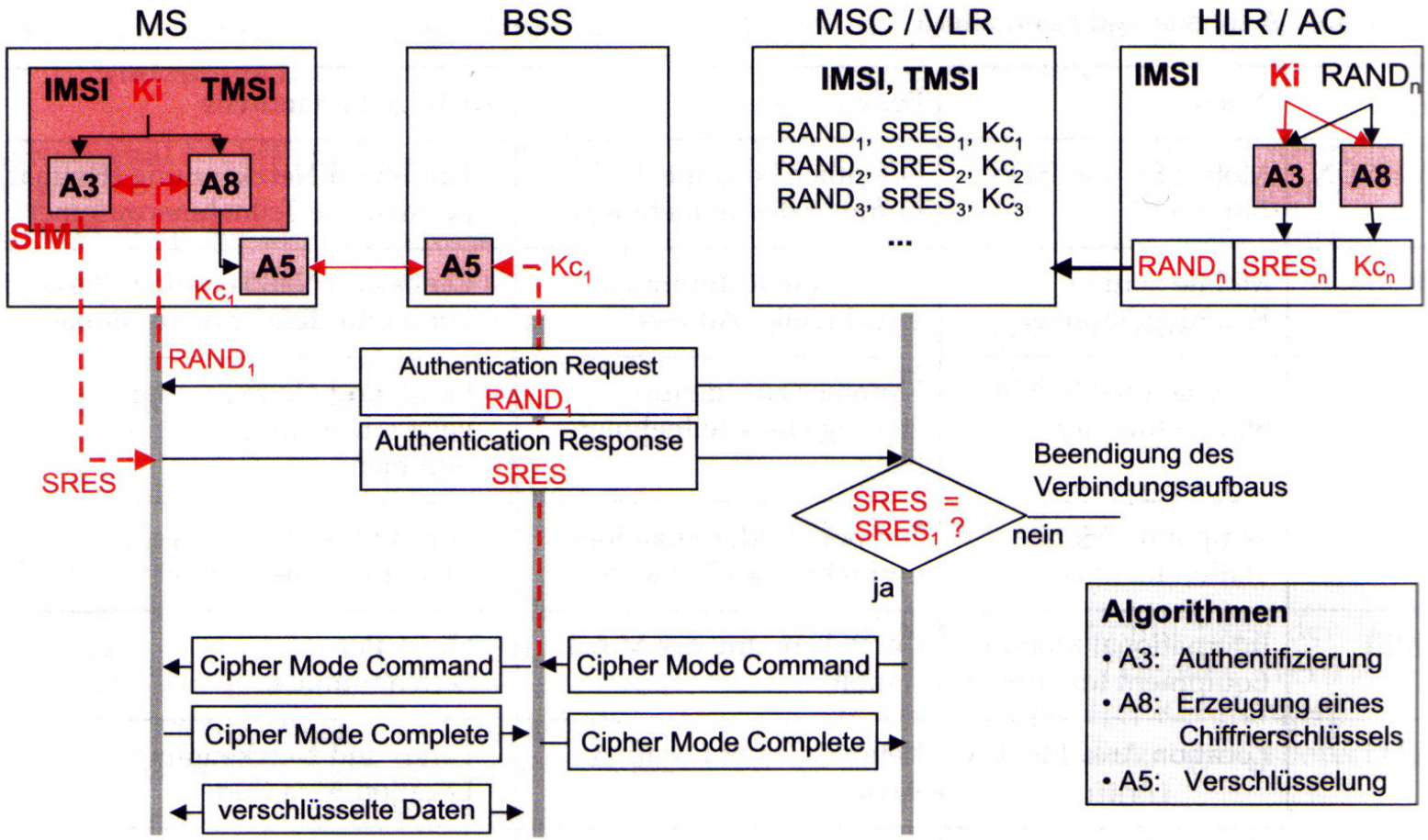
- The logical layer could be seen as the equivalent of OSI data link layer
  - Here are the logical channels mapped into the physical ones
  - Two distinctions: traffic channels and control channels
- The traffic channels carry the user data (voice, SMS, fax, ...)
  - Full rate channel: Bm 22,8kbit/s (TCH/F)
  - Half rate channel: Lm 13,4kbit/s (TCH/H)



GSM – control channels

- Beside the traffic channels are a group of control channels defined
- They handle system information, connection setup and connection control
- Broadcast Control Channel (BCCH) group handles beacon signaling, synchronization of MS with the serving BTS, timing advance adjustment, it comprises of
  - BCCH – Broadcast Control Channel
  - FCCH – Frequency Control Channel
  - SCH – Synchronization Channel

GSM – Authentication, Authorization, Access

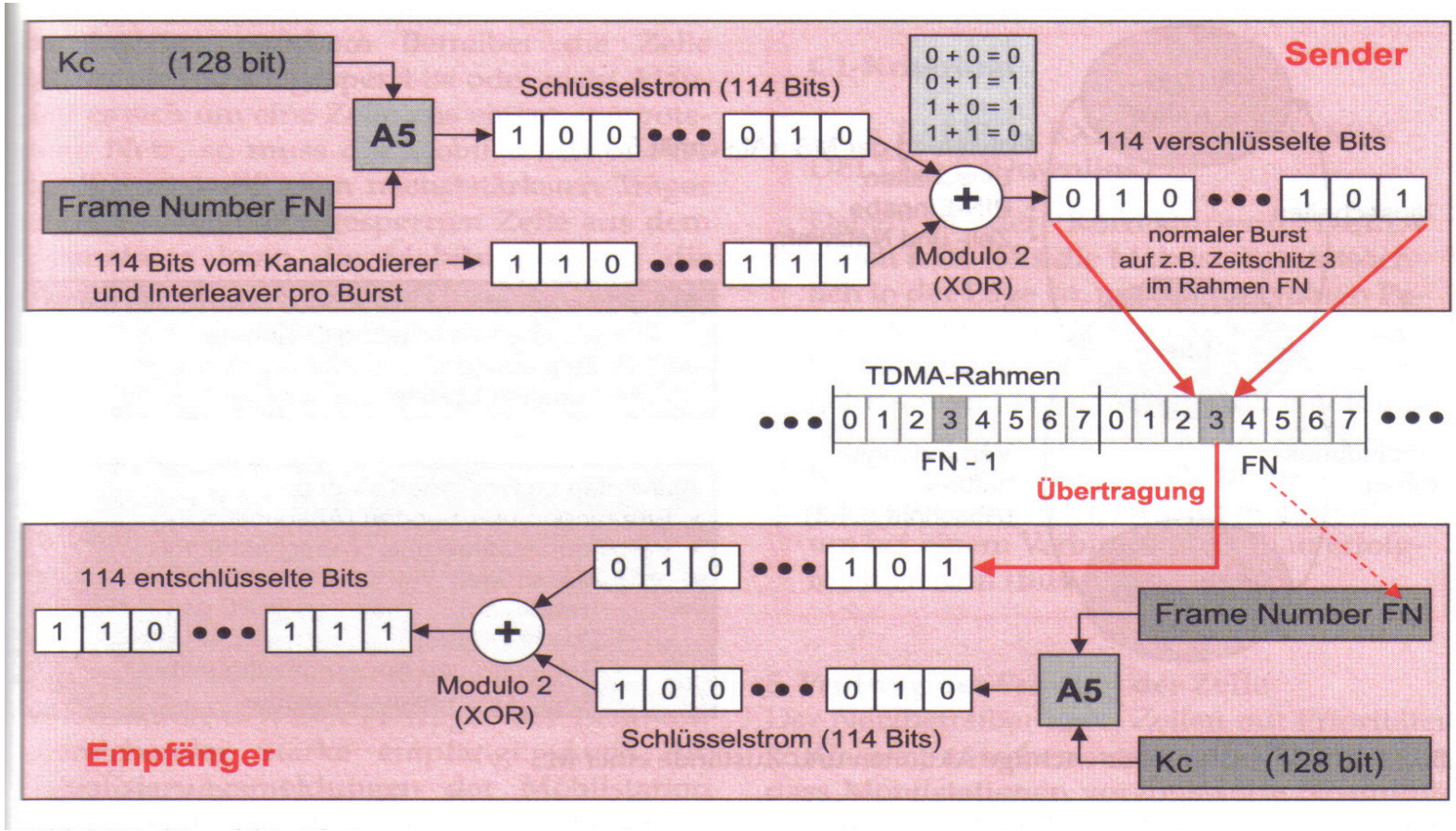


GSM – Authentication, Authorization, Access

- Sequence of authorization and generation of shared keys for encryption

1. The network sends an authentication request message to MS, conveying a 128-bit random number (RAND).
2. MS uses the RAND, the secret key Ki (stored at SIM), and the encryption algorithm A3, to compute a 32-bit number as a signed response (SRES).
3. MS computes the 64-bit ciphering key Kc using encryption algorithm A8, which will be later used in the ciphering procedure.
4. MS responses with an authentication response message containing SRES.
5. The network uses same parameters and algorithm to computer another SRES.
6. MS SRES and the network SRES are compared with each other. If mactch, the network accepts the user as an authorized subscriber. Otherwise, authentication is rejected.
7. After authentication has been successful, the network transmits a ciphering mode message to MS indicating whether encryption is to be applied.
8. In case ciphering is to be performed, the secret key Kc and encryption algorithm A5 are used for ciphering.

GSM – stream encryption



GSM literature, next lecture

- Some of the pictures are taken from text books or online sources
- German text books:
  - Jochen Schiller, Mobilkommunikation
  - Bernhard Walke, Mobilfunknetze und ihre Protokolle, Grundlagen GSM, UMTS, ...

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Communication Systems

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer