Mobilkommunikation - Mobile Communications

Lecture 10: Cellular Communication Systems

Prof. Dr.-Ing. Markus Fidler

Institute of Communications Technology
Leibniz Universität Hannover

July 1, 2016

Previous lectures

- WPAN: wireless personal area network
  - IEEE 802.15, Bluetooth
  - personal surrounding
- WLAN: wireless local area network
  - IEEE 802.11, Wifi
  - home, office, campus
- WMAN: wireless metropolitan area network
  - IEEE 802.16, WiMAX
  - last mile (DSL substitute)
  - no or only nomadic mobility (extensions for mobility exist)

Today's lecture

- WWAN: wireless wide area network
- cellular telecommunication systems with full mobility support
- ETSI, 3GPP standards

Digital cellular networks

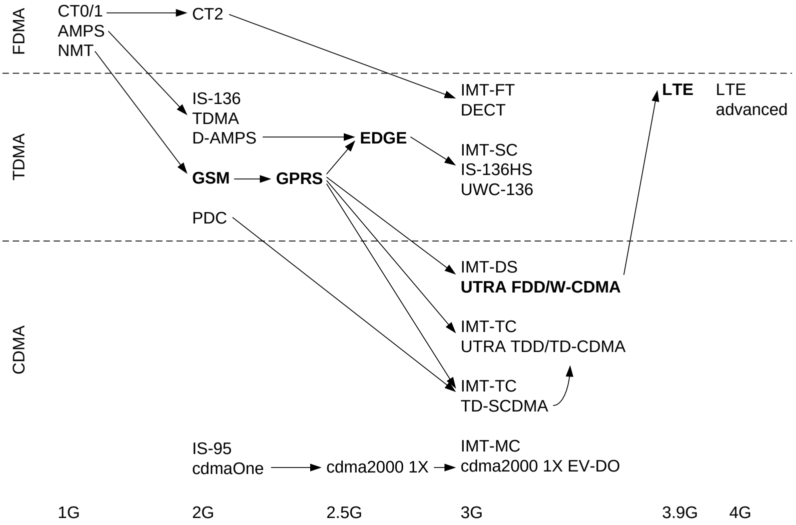
Generations

- 1G: analog mobile telephony
- 2G: digital mobile telephony
- 3G: mobile packet data services
- 4G: high speed mobile data services

Divide of digital systems

- Europe: GSM (global system for mobile communications)
- Japan: PDC (personal digital cellular)
- USA: TDMA, CDMA
  - market forces have not succeeded to select one system
  - divided market with several non inter-operable systems

Digital cellular networks



FDMA

CT0/1
AMPS
NMT

CT2

TDMA

IS-136
TDMA
D-AMPS

GSM

GPRS

EDGE

PDC

IMT-FT
DECT

IMT-SC
IS-136HS
UWC-136

LTE

LTE
advanced

CDMA

IMT-DS
UTRA FDD/W-CDMA

IMT-TC
UTRA TDD/TD-CDMA

IMT-TC
TD-SCDMA

IS-95
cdmaOne

cdma2000 1X

IMT-MC
cdma2000 1X EV-DO

1G 2G 2.5G 3G 3.9G 4G

Outline

Global System for Mobile Communications (GSM)

- Services
- Architecture
- Radio Interface
- Protocols
- Localization and Calling
- Handover
- Security

Overview

Standardization

- foundation of the groupe spéciale mobile (GSM) in 1982
- later renamed global system for mobile communications (GSM)
- with UMTS transferred to the 3. generation partnership project (3GPP)

Frequency bands

- 900: uplink 890-915 MHz, downlink 935-960 MHz
- 1800: uplink 1710-1785 MHz, downlink 1805-1880 MHz
  - named digital cellular system (DCS)
- 1900: uplink 1850-1910 MHz, downlink 1930-1990 MHz
  - named personal communications service (PCS)

Mobile services

Mobile services provided to the customers by GSM

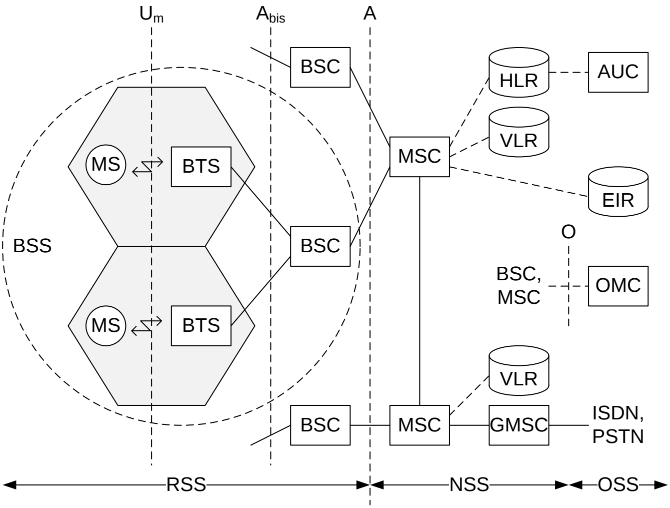
- **bearer services:** data (non-voice) services of up to 9.6 kb/s
  - transparent: constant delay and throughput, uses only FEC
  - non-transparent: variable delay and throughput, adds ARQ
- **tele services:**
  - telephony with high-quality digital voice codecs
  - short messages service (SMS) carrying up to 160 characters
  - multimedia message service (MMS) including pictures, video clips, etc.
  - fax (group 3)
- **supplementary services:**
  - user identification
  - call forwarding
  - multiparty communication etc.

Components and subsystems

GSM has a complex hierarchical architecture (many acronyms)

- components
  - MS: mobile station
  - BTS: base transceiver station
  - BSC: base station controller
  - MSC: mobile services switching center
  - GMSC: gateway mobile services switching center
  - VLR: visitor location register
  - HLR: home location register
  - EIR: equipment identity register
  - AUC: authentication centre
- subsystems
  - BSS: base station subsystem
  - RSS: radio subsystem
  - NSS: network and switching subsystem
  - OSS: operation subsystem

Elements and interfaces



Radio subsystem (RSS)

Components

- mobile stations (MS)
- base station subsystem (BSS)
  - several base stations (BTS)
  - one base station controller (BSC)

Interfaces

- $\mathrm{U_m}$: MS-BTS, radio interface
- $\mathrm{A_{bis}}$: BTS-BSC, multiplexed 16 kb/s connections
- A: BSC-MSC, 30 multiplexed 64 kb/s connections over PCM-30
- O: BSC-OMC, signalling system 7 (SS7) over X.25

Base station subsystem (BSS)

Base transceiver stations (BTS)

- radio equipment
  - antennas
  - amplifiers
  - signal processing
- forms a radio cell or several cells using sectorized antennas
- a cell can measure up to 35 km depending on
  - the environment: buildings, mountains
  - the traffic load

Base station controller (BSC)

- manages several BTSs
- reserves radio frequencies
- handles the handover between BTSs within the BSS
- performs paging of the MS

Mobile station (MS)

User independent equipment (hard- and software)

- has a unique international mobile equipment identity (IMEI)
    - registered in the equipment identity register (EIR)
    - used for theft protection
- has to be unlocked using a SIM

Subscriber identity module (SIM)

- identifies the user
- contains secured user related information
    - personal identity number (PIN)
    - PIN unblocking key (PUK)
    - authentication key (K_i)
    - algorithms for ciphering
    - international mobile subscriber identity (IMSI)

Network and switching subsystem (NSS)

Components

- mobile services switching center (MSC)
- gateway mobile services switching center (GMSC)
    - integrated services digital network (ISDN)
    - public switched telephone network (PSTN)

Databases

- home location register (HLR)
- visitor location register (VLR)

Mobile services switching center (MSC)

Fixed backbone of the GSM network

- MSCs are high performance ISDN switches
- MSCs are connected among each other
- MSCs are connected to BSCs
  - a single MSC typically manages a number of BSCs in a geographical region
- GMSCs connect the GSM network to PSTN or ISDN networks
- MSCs perform signalling using SS7
  - connection setup and release
  - handover of connections to other MSCs
  - supplementary services, e.g. call forwarding

Location register (LR)

Home location register (HLR)

- central master database
- stores all user related data
  - static data
    - international mobile subscriber identity (IMSI)
    - mobile subscriber ISDN number (MSISDN)
    - subscribed services, e.g. roaming restrictions
  - dynamic data
    - current location area (LA)
    - mobile subscriber roaming number (MSRN)

Visitor location register (VLR)

- dynamic database associated to each MSC
- stores user related data for MSs that are currently in the LA
- the VLR copies relevant information from the HLR

Operation subsystem (OSS)

Operation and maintenance center (OMC)

- centralized operation and maintenance

Authentication center (AUC)

- information for authentication of MSs
- information used for encryption of user data

Equipment identity register (EIR)

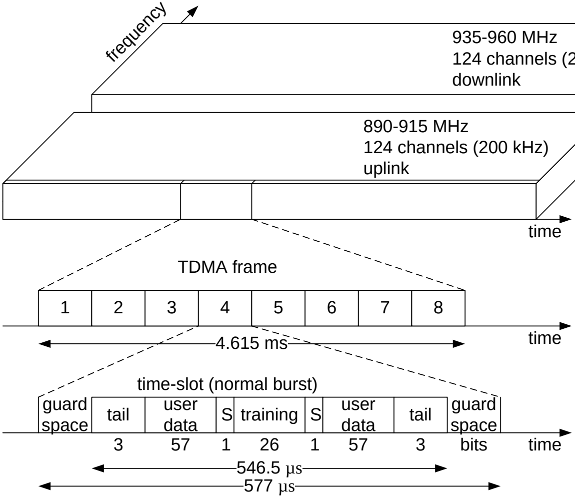
- stores IMEIs of all MSs
- blacklists stolen MSs
- graylists malfunctioning MSs
- whitelist of valid IMEIs

Radio interface

U_m radio interface combines

- space division multiple access (SDMA): cells with BTSs
- frequency division multiple access (FDMA)
  - GSM 900: 124 channels of 200 kHz width each
  - a BTS usually manages about 10 channels
- time division multiple access
  - repeated frames each of 4.615 ms duration
  - frames are subdivided into 8 time slots each of 577 μs duration
  - data bursts are 546.5 μs long and carry 148 bits leaving 30.5 μs guard space to avoid overlap due to different path delays
  - the raw data rate of a TDM channel is about 32 kb/s
- frequency division duplexing (FDD) with 45 MHz separation of uplink (890-915 MHz) and downlink (935-960 MHz)
  - given a downlink slot the corresponding uplink slot starts 3 time slots later; allows implementing half-duplex transceivers
- optional slow frequency hopping (frequency selective fading)

TDMA frame


frequency
935-960 MHz
124 channels (200 kHz)
downlink
890-915 MHz
124 channels (200 kHz)
uplink
time
TDMA frame
1
2
3
4
5
6
7
8
4.615 ms
time
time-slot (normal burst)
guard space
tail
user data
S
training
S
user data
tail
guard space
3
57
1
26
1
57
3
bits
time
546.5 µs
577 µs

Bursts

Normal burst

- tail: 3 bits all set to 0; allows enhancing receiver performance
- S: indicates whether the burst contains user or network control data
- training sequence:
  - adapt the parameters of the receiver to the current conditions
  - select the strongest signal in case of multi-path propagation

Burst types

- normal burst: for data transmission
- frequency correction burst: to correct the MSs local oscillator
- synchronization burst: with an extended training sequence
- access burst: for initial connection setup
- dummy burst: used if no data is available for a slot

Logical channels

Channels

- **physical channels:** TDM channel, one slot every 4.615 ms
- **logical channels:** are mapped onto physical channels, e.g. using TDM
  - channel 1 takes up every 4th slot (even)
  - channel 2 takes up every 2nd slot (odd)

Two groups of logical channels

- **traffic channels (TCH):** used to transmit user data
  - full-rate TCH (TCH/F): 22.8 kb/s
    - full rate (FR) voice: 13 kb/s + error correction code
  - half-rate TCH (TCH/H): 11.4 kb/s
    - half rate (HR) voice: 5.6 kb/s + error correction code
- **control channels (CCH):** used to transmit control data
  - many different with specific tasks

Control channels

- **broadcast control channel (BCCH):** used by the BTS to signal information to all MSs, e.g. cell identifier, options (frequency hopping), frequencies of this and neighboring cells
  - **frequency correction channel (FCCH)**
  - **synchronization channel (SCH)**
- **common control channel (CCCH):** exchange of information regarding connection setup; unidirectional
  - **paging channel (PCH):** for calls towards the MS
  - **random access channel (RACH):** for MS originated calls; uses slotted ALOHA multiple access
  - **access grant channel (AGCH):** used by the BTS to grant the MS access to a TCH or SDCCH

Control channels continued

- **dedicated control channel (DCCH):** bidirectional
  - **stand-alone dedicated control channel (SDCCH):** exchange information for TCH establishment before it exists
  - **slow associated control channel (SACCH):** associated with a TCH to exchange system information, e.g. channel quality and signal power level
  - **fast associated control channel (FACCH):** uses timeslots otherwise used by the TCH if more signalling information, e.g. for handover, has to be transmitted

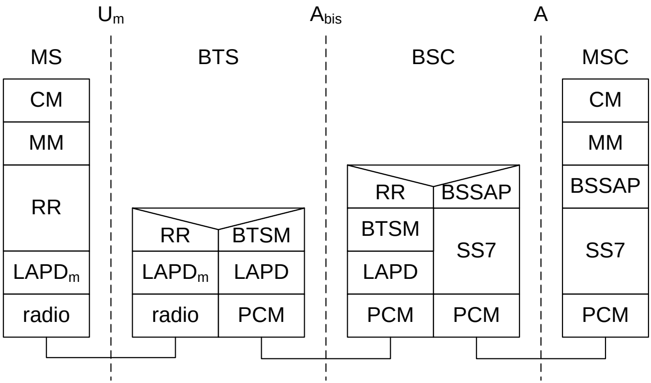
- **traffic multiframe**
  - repeated pattern consisting of 26 slots
  - 12 TCH/F slots, 1 SACCH slot, 12 TCH/F slots, 1 unused
    - each burst carries 114 bit user data and is repeated every 4.615 ms resulting in 24.7 kb/s
    - 24 out of 26 slots are used for the TCH/F yielding 22.8 kb/s
    - 1 out of 26 slots is used for the SACCH yielding 950 b/s

Frame hierarchy

Each slot is uniquely identified by its frame and slot number

- **time slot:** 577 μs
  - burst with 114 data bits
- **TDMA frame:** 4.615 ms
  - 8 slots
- **multiframe:** 120 resp. 235.4 ms
  - traffic multiframe: 26 TDMA frames
  - control multiframe: 51 TDMA frames
- **superframe:** 6.12 s
  - 51 traffic multiframes or
  - 26 control multiframes
- **hyperframe:** 3 h 28 min 53.76 s
  - 2048 superframes

Protocol stack



CM: call management
MM: mobility management
RR: radio resource management
LAPD: link access procedure D

BSSAP: BSS application part
BTSM: BTS management
SS7: signalling system 7
PCM: pulse code modulation

Layer 1

Functions of the physical (radio) layer

- digital modulation using GMSK
- channel coding, i.e. error detection and correction using FEC
- encryption and decryption of data
- multiplexing of bursts into TDMA frames
- synchronization of MSs with the BTS
- measurements of channel quality
- timing advance

Timing advance

Timing advance

- a distance of 35 km causes a round trip time of 0.23 ms, i.e. the burst of a MS in 35 km distance from the BTS is late by 0.23 ms at the BTS
- using 0.577 ms slots a guard space of 0.23 ms makes up 40 %
- bursts have to be sent early by the MS by one RTT
- the BTS informs the MS about the current RTT
- GSM allows a timing advance of 63 bit times of 3.69 μs each resulting in 0.23 ms, i.e. allowing for 35 km cell radius
- GSM works with a guard space of only 30.5 μs

Voice transmission

- TCH/F offers 22.8 kb/s
  - 13 kb/s digital voice
  - plus redundancy and CRC
- interleaving to reduce burst errors
- delay due to TDMA channel and interleaving is about 60 ms
- voice activity detection
  - only transmit voice data when there is a voice signal
  - during periods of silence comfort noise is generated at the receiver
  - comfort noise uses parameters from the current background noise of the sender

Layer 2

LAPD$_m$ is a lightweight data link layer protocol

- similar to other "standard" data link protocols
- adapted to the radio layer (reduced functionality)

Basic functions of LAPD$_m$

- segmentation and reassembly
  - map higher layer data units into bursts
- connection-oriented reliable (acknowledged) service
  - re-sequencing of data frames
  - flow control
- connectionless unreliable (unacknowledged) service

Layer 3

Layer 3 is divided into several sublayers

- **radio resource management (RR)**
  - setup, maintenance, and release of radio channels
  - BSS functions are split between BTS and BSC
- **mobility management (MM)**
  - location updating
  - registration, authentication, identification
  - provision of a temporary mobile subscriber identity (TMSI)
- **call management (CM)**
  - **call control (CC):** call establishment, call clearing
  - **short message service (SMS):** uses SDCCH or SACCH
  - **supplementary services (SS):** e.g. call forwarding

Localization

Automatic worldwide localization of users

- the same phone number is valid worldwide
- system knows where a user currently is
  - HLR always knows the current location area (LA)
  - periodic location updates
  - if a mobile moves into the range of a new VLR the VLR requests all required user information from the HLR
- roaming: access services using a visited network
  - networks of different providers (often not supported due to competition)
  - networks of different providers in different countries (international roaming)

Numbers and identities: static

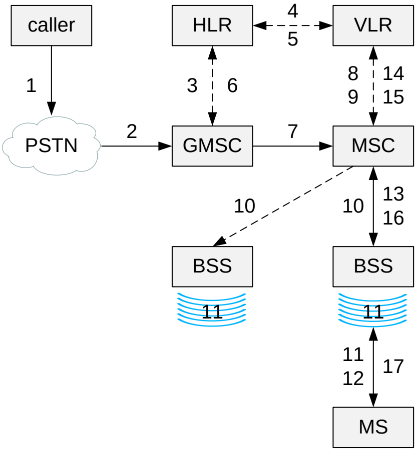
- **international mobile subscriber identity (IMSI):** international unique identification of a subscriber consisting of
  - mobile country code (MCC)
  - mobile network code (MNC)
  - mobile subscriber identification number (MSIN)
- **mobile station international ISDN number (MSISDN):** phone number, associated with the SIM not the mobile phone
  - country code (CC)
  - national destination code (NDC)
  - subscriber number (SN)

Numbers and identities: dynamic

- **location area identity (LAI):** consists of
  - mobile country code (MCC)
  - mobile network code (MNC)
  - location area code (LAC)
- **temporary mobile subscriber identity (TMSI):**
  - used to hide the IMSI
  - assigned temporarily by the VLR
  - only valid within the location area of the VLR
  - LAI and TMSI identify a user
- **mobile station roaming number (MSRN):** generated by the VLR on request from the MSC for incoming calls, consists of
  - visitor country code (VCC)
  - visitor national destination code (VNDC)
  - visitor subscriber number (VSN)

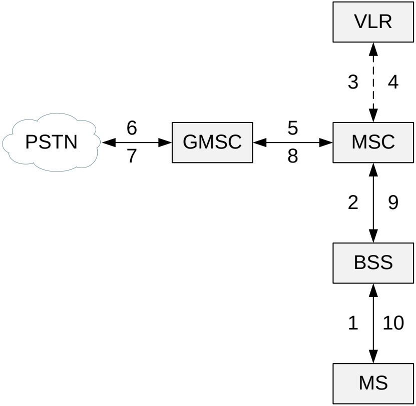
Mobile terminated call (MTC)

- 1: calling a GSM subscriber
- 2: forwarding call to GMSC
- 3: signal call setup to HLR
- 4,5: request MSRN from VLR
- 6: notify GMSC about responsible MSC
- 7: forward call to MSC
- 8,9: get current status of MS
- 10,11: paging of MS
- 12,13: MS answers
- 14,15: security checks
- 16,17: set up connection

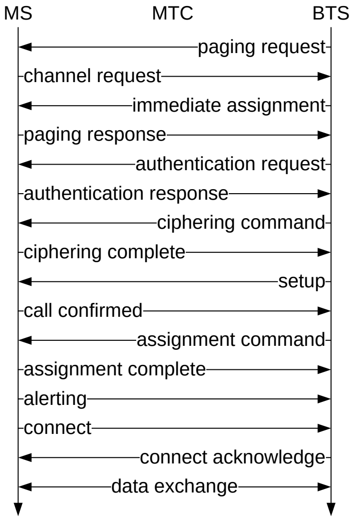


Mobile originated call (MOC)

- 1,2: connection request
- 3,4: security check
- 5-8: check if resources are available (circuit switching)
- 9,10: set up connection



Message flow for call establishment



MS MTC BTS

← paging request

channel request →

← immediate assignment

paging response →

← authentication request

authentication response →

← ciphering command

ciphering complete →

← setup

call confirmed →

← assignment command

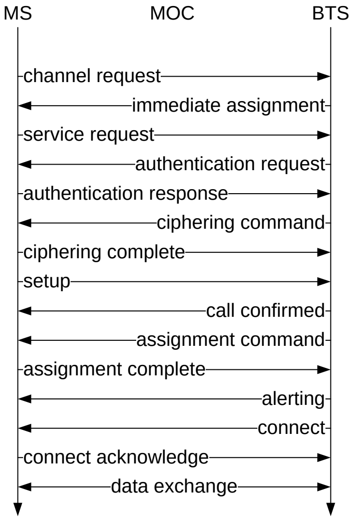
assignment complete →

alerting →

connect →

← connect acknowledge

← data exchange →



MS MOC BTS

channel request →

← immediate assignment

service request →

← authentication request

authentication response →

← ciphering command

ciphering complete →

setup →

← call confirmed

← assignment command

assignment complete →

← alerting

← connect

connect acknowledge →

← data exchange →

Handover

Handover of a MS from one cell to another

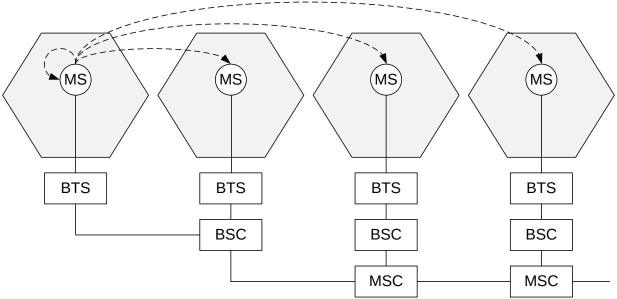
- without cut-off, i.e. call drop
- target maximum handover duration of 60 ms

Two main (among others) reasons for handover

- MS moves out of the range of a BTS
  - the quality of the radio link drops
  - the received signal level decreases
  - the transmission error rate increases
- traffic in one cell may be too high
  - handover is done for load balancing

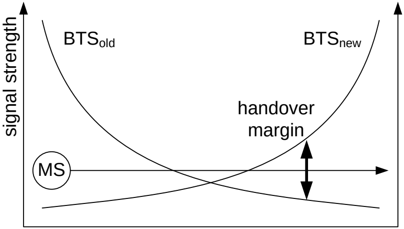
Types of handover

- **intra-cell:** change of carrier frequency
- **inter-cell, intra-BSC:** the BSC performs the handover
- **inter-BSC, intra-MSC:** handover from one BSS to another BSS controlled by the MSC
- **inter-MSC:** handover from one MSC to another MSC, both MSCs perform the handover together

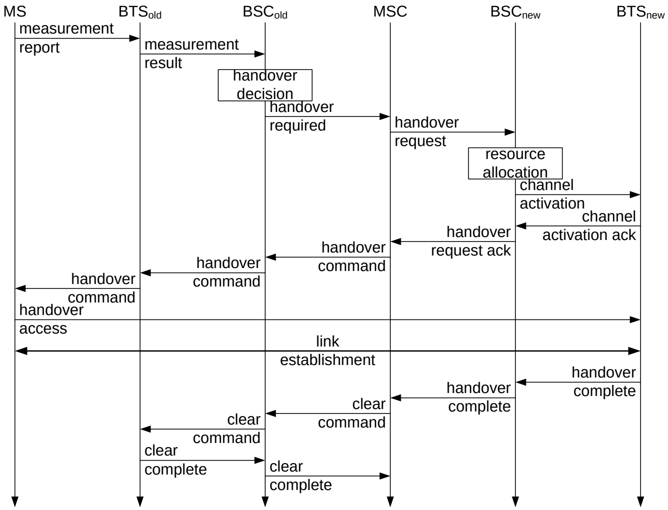


Handover decision

- MS measures signal strength of its and neighboring BTSs
- measurements are taken periodically every 0.5 s
- measurements are sent to the BSC for handover decision
- averaging to compensate for short-term fluctuations
- handover margin uses hysteresis to avoid oscillations



Inter-BSC, intra-MSC handover procedure



Security

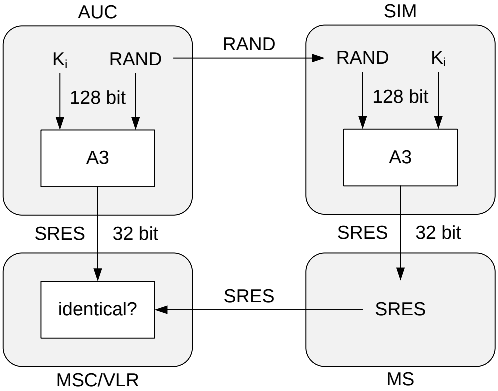
Security services

- **access control and authentication:**
  - authentication of a valid user for the SIM using the PIN
  - authentication of the subscriber for the network using a challenge-response scheme
- **confidentiality:**
  - user data is encrypted between MS and BTS
- **anonymity:**
  - user identifiers that reveal the identity are not transmitted over the air (except for initial identification), instead a temporary TMSI is assigned by the VLR

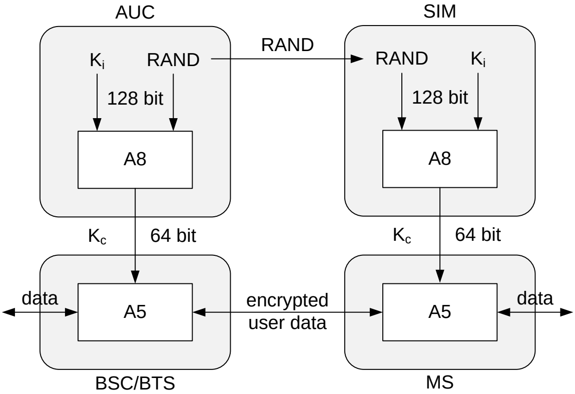
Algorithms

- **A3:** for authentication, secret, in SIM and AUC
- **A5:** for encryption, public, implemented in devices
- **A8:** for generation of the cipher key, secret, in SIM and AUC

Authentication



Encryption


AUC
SIM
K_i
RAND
RAND
RAND
K_i
128 bit
128 bit
A8
A8
K_c
64 bit
K_c
64 bit
data
A5
encrypted user data
A5
data
BSC/BTS
MS

Literature

- Jochen Schiller, Mobile Communications, Second Edition, Addison-Wesley, 2003.
- ITU-D, Guidelines on the smooth transition of existing mobile networks to IMT 2000
- Matthias Hollick, Mobile Networking, TU Darmstadt, 2008.