GSM

Grundlagen zu GSM

Gerhard, Dimi, Marc

Hochschule für Technik und Wirtschaft Aalen, ACC Akut

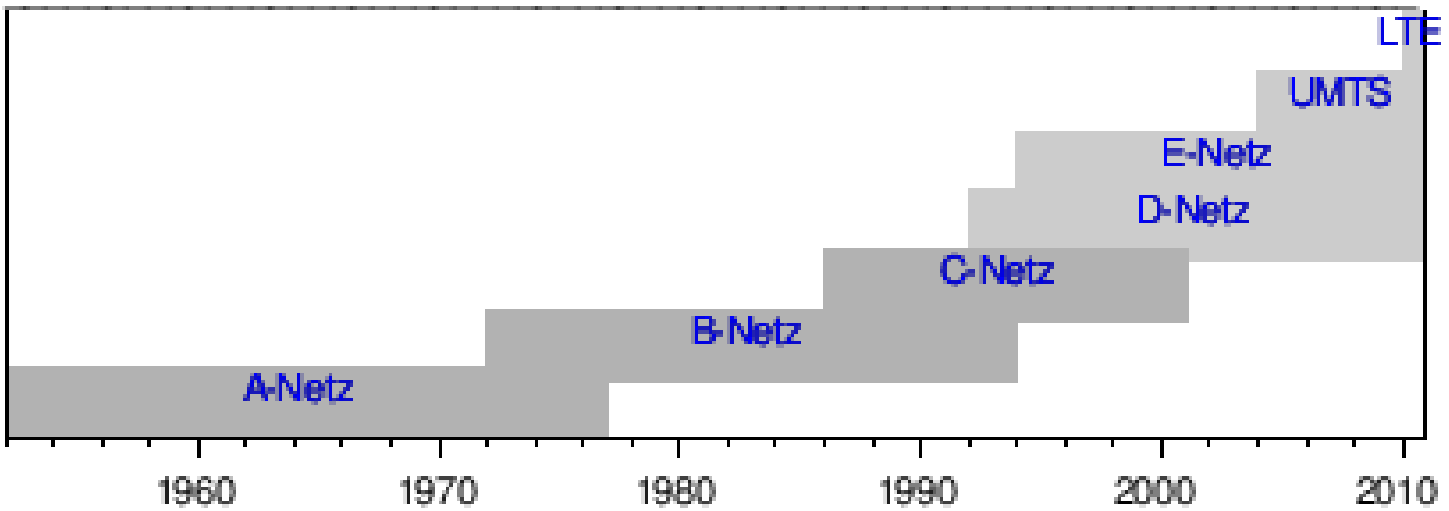
7. April 2013

Inhaltsverzeichnis

Übersicht

Geschichte I

- GSM = Global System for Mobile Communications.
- Zweite Generation (*2G*), technische Grundlage der D- und E-Netze.
- Nachfolger von A-Netz, B-Netz, C-Netz.



1

Geschichte II

- 1982: Mobilfunk-Arbeitsgruppe bei CEPT wird eingerichtet.
- 1990: GSM 900-Spezifikation (*Phase 1*) verabschiedet. Hersteller können mit Entwicklung und Produktion beginnen.
- 1991: Erste lauffähige Systeme werden vorgeführt.
- 1991: GSM 1800-Spezifikation (*DCS 1800*) verabschiedet.
- 1992: Start in Deutschland.

Geschichte III

2

Geschichte IV

- GSM gibt es in über 200 Ländern.
- Im März 2006 nutzten weltweit 1,7 Milliarden Menschen GSM und täglich kommen eine Million neue Kunden dazu.
- 2011 über 4,4 Milliarden Nutzer weltweit.

[1] Quelle: Wikipedia (https://de.wikipedia.org/w/index.php?title=D-Netz&oldid=96313780)

[2] Quelle: Wikipedia (https://de.wikipedia.org/w/index.php?title=Datei:GSM-Telefone-1991.jpg&filetimestamp=20061208135743)

Übersicht

Paketvermittlung

- Nachrichten werden in kleine Datenpakete unterteilt.
- Typischer Aufbau eines Pakets:

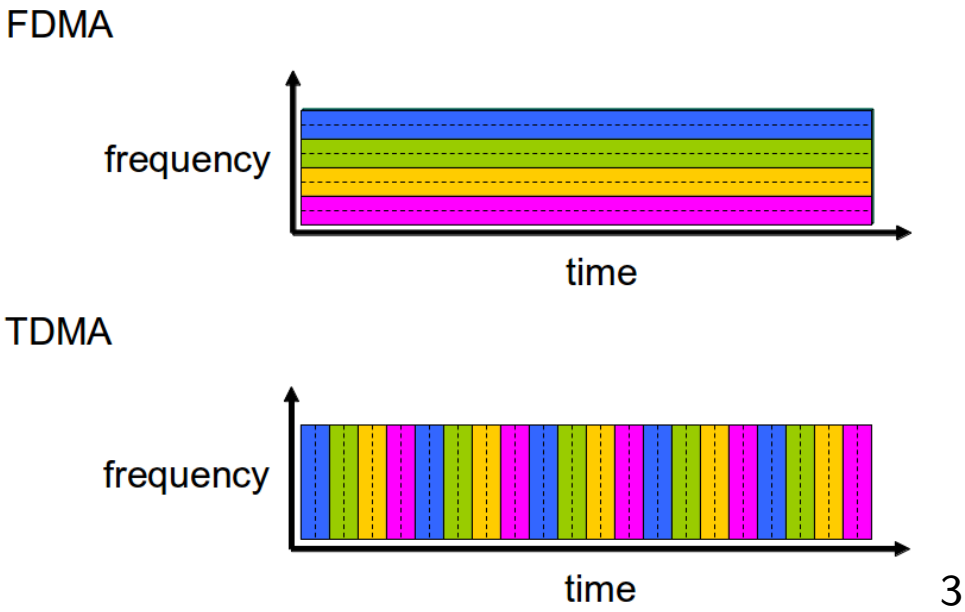
Quelle des Paketes	Ziel des Paketes
Paketlaufnummer	Klassifizierung des Paketes
Länge des Datenteils	

- Jedes Paket könnte eine eigene Route nehmen.
- z.B. genutzt bei Computernetzwerken (*IP*).

Leitungsvermittlung

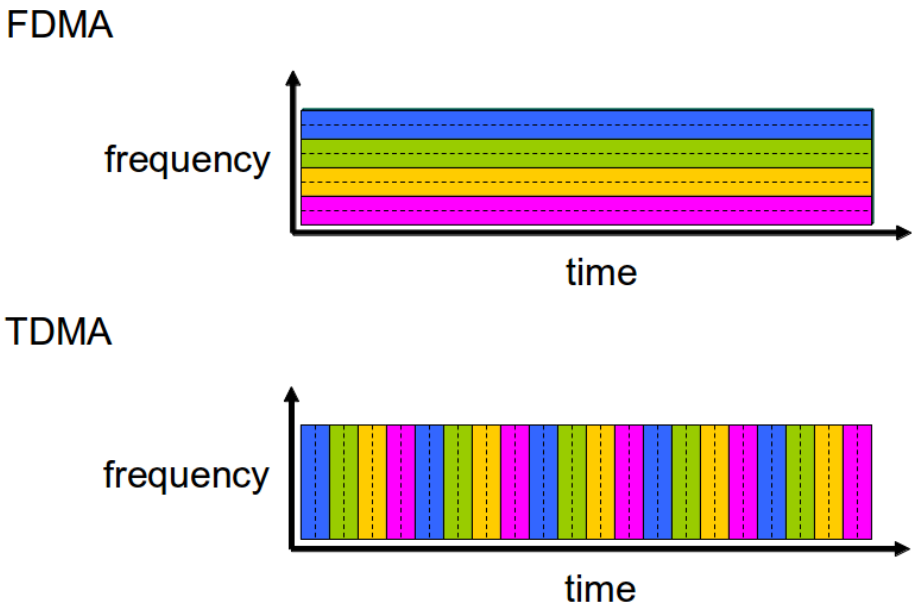
- Beim Verbindungsaufbau fest durchgeschaltete Leitung.
- Steht danach einem Teilnehmer exklusiv zur Verfügung (auch wenn keine Daten übertragen werden).
- z.B. genutzt bei GSM und Festnetz ohne *VoIP*.

Multiplexverfahren



[3] Quelle: J.F Kurose, K.W. Ross, Computer Networking

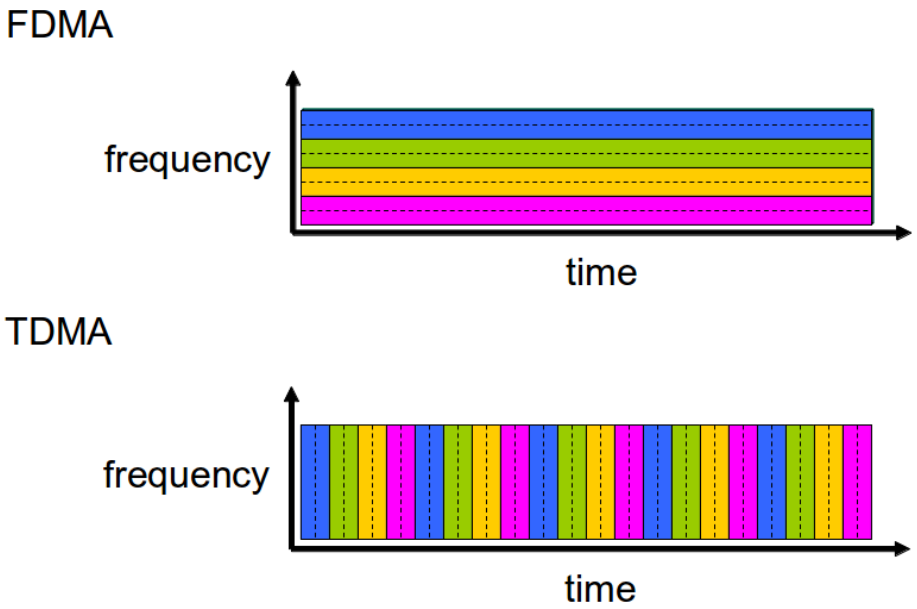
Multiplexverfahren



- Frequency Division Multiple Access (*FDMA*): Dem Sender wird ein bestimmter Frequenzbereich auf einem Übertragungskanal zugeordnet. (vergleiche Radio)

[3] Quelle: J.F Kurose, K.W. Ross, Computer Networking

Multiplexverfahren

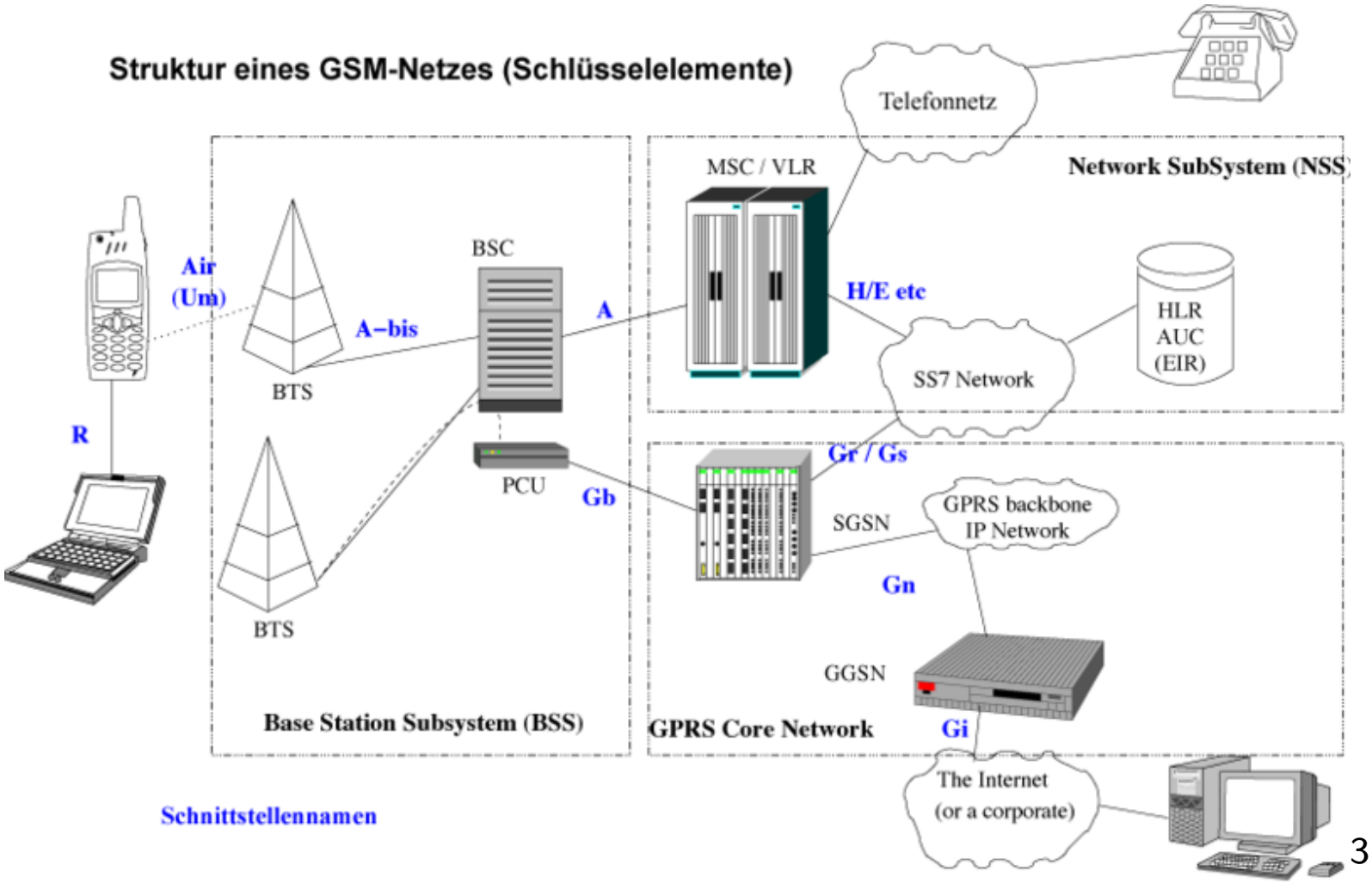


- Frequency Division Multiple Access (*FDMA*): Dem Sender wird ein bestimmter Frequenzbereich auf einem Übertragungskanal zugeordnet. (vergleiche Radio)
- Time Division Multiple Access (*TDMA*): Dem Sender wird ein bestimmter Zeitabschnitt auf einem Übertragungskanal zugeordnet.

[3] Quelle: J.F Kurose, K.W. Ross, Computer Networking

Übersicht

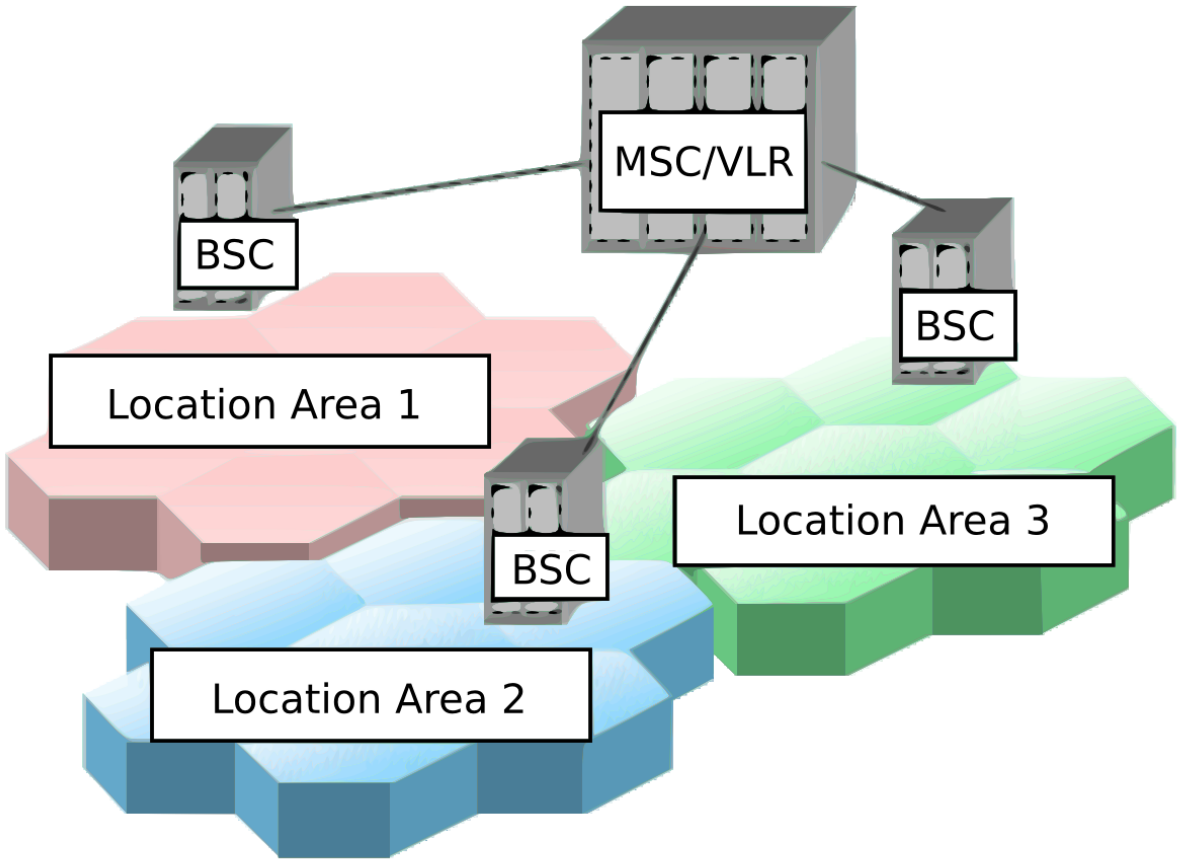
GSM Netzaufbau



[3]

[3] Quelle: Wikipedia (https://de.wikipedia.org/w/index.php?title=Datei:Gsm_netzwerk.png&filetimestamp=20110131195933)

GSM Netzaufbau - LA - *Location Area*



4

[4] Quelle: http://engineermahmoud.blogspot.de/2011/01/gsm-6-location-area.html

GSM Netzaufbau - Begrifflichkeiten

- MS - Mobile Station

BSS - Base Station Subsystem

- BTS - Base Transeiver Station
- BSC - Base Station Controller

NSS - Network Subsystem

- MSC - Mobile Switching Center
- HLR - Home Location Register
- VLR - Visitor Location Register
- AuC - Authentification Center
- SMSC - Short Message Service Center

GSM Netzaufbau - MS - *Mobile Station*

- Mobiles Endgerät, z.B. Handy.
- enthält **Sim-Karte**, diese enthält u.a. folgendes:
  - MikroController mit Datenspeicher (u.a. Kontakte und SMS).
  - IMSI (*International Mobile Subscriber Identity*).
  - geheimer Schlüssel K_i (gemeinsames Geheimnis mit dem Netzanbieter)
  - Prozessor der SIM Karte zur Generierung der Signed Response (*SRES*).
  - auslesen der nicht geschützten Informationen mit Tools möglich (z.B. SIM-Spy).

GSM Netzaufbau - BTS - *Base Transeiver Station* I

5

GSM Netzaufbau - BTS - *Base Transeiver Station* II

- Stellt den Einstiegspunkt für MS zum Netzwerk dar.
- Laut Presseberichten hat jeder Netzwerkbetreiber in Deutschland einige zehntausend Basisstationen.
- BTS Reichweite theoretisch 35km.
- In Städten 3-4km, Innenstädten 100m.
- Auf dem Land auch selten über 15km (auch wegen 1-2 Watt Sendeleistungsbegrenzung).
- Maximal 30 aktive Teilnehmer pro BTS, daher Einschränkung der Reichweite.
- Grobe Näherung inklusive passiver Teilnehmer: 1800 pro BTS.
- ca. 20 BTS pro Location Area.

GSM Netzaufbau - BTS - *Base Transeiver Station* III

- Vor allem auf Erhöhungen zu finden.
- Kommuniziert über das Um-Interface mit der MS.
- Kommuniziert über das Abis-Interface mit der BSC.
- Benachbarte BTS dürfen nicht die gleiche Frequenz nutzen (Interferenz).
- BTS mittels Sektorenantennen in Sektoren eingeteilt. Diese decken z.B. nur 120 Grad der 360 Grad des BTS-Bereichs mit je unterschiedlichen Frequenzen ab. Dadurch können Frequenzen öfter wiederverwendet werden.

[5] Quelle: Wikipedia (https://de.wikipedia.org/w/index.php?title=Datei:D2_d58_a.jpg&filetimestamp=20050313174310), GSM Grundlagen (Literatur)

GSM Netzaufbau - BSC - *Base Station Controller*

- An einem BSC können mehrere BTS angeschlossen sein.
- Sorgt für den Handover einer MS zwischen angeschlossenen BTS.
- Am BSC kommen auch Pegelmessungen,
  Location Updates, ... an.
- Regelt das Bereitstellen von Channels und das Paging.

GSM Netzaufbau - MSC - *Mobile Switching Center*

- Jede MSC hat ein VLR.
- An einem MSC können mehrere BSC angeschlossen sein.
- Regelt das Routing von Anrufen und SMS.
- Authentifiziert die MS.
- Speicherung von Abrechnungsdaten.
- Inter-BSC-Handover.
- Kann für mehrere Location Areas verantwortlich sein.

GSM Netzaufbau - VLR - *Visitor Location Register* I

- Speichert alle aktuellen Teilnehmer der MSC (u.a. mit ihrer Location Area).
- Betritt eine MS eine neue Location Area, startet die MS eine Prozedur um sich zu registrieren.
- Das MSC speichert die neue Location Area in das VLR. Falls die MS noch nicht in dem VLR registriert war, wird eine temporäre Kopie der benötigten Daten vom HLR in das VLR abgelegt.

GSM Netzaufbau - VLR - *Visitor Location Register* II

- Speichert u.a. folgende Daten:
  - IMSI, TMSI.
  - LAI (*Location Area Identification*).
  - MSISDN *(Mobile Subscriber Integrated Service Digital Network Number)* Die Handy-Nummer. Enthält u.a. die HLR-Adresse.
  - MSRN *(Mobile Station Roaming Number*), dient zum internationalen Routing durch GSM-Netze (International Call Routing).
    Besteht aus:
    - Visitor Country Code (*VCC*).
    - Visitor National Destination Code (*VNDC*).
    - Visitor Mobile Switching Center (*VMSC*).
    - Visitor Subscriber Number (*VSN*).

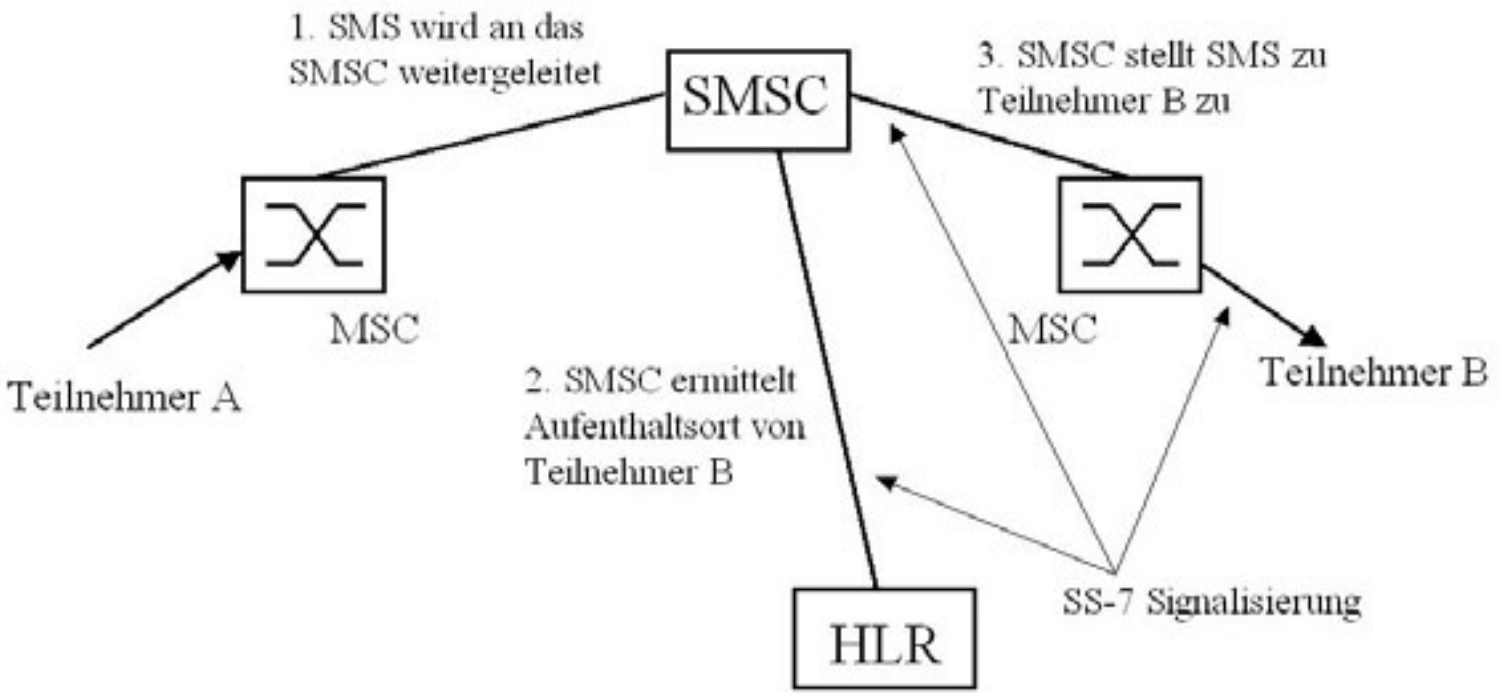
GSM Netzaufbau - HLR - *Home Location Register*

- Teilnehmer-DB eines GSM Netzwerks.
- Heimatregister einer Mobilfunknummer.
- Wird vom VLR abgefragt, wenn ein Mobiltelefon beispielsweise eingeschaltet wird.
- Es kann mehrere HLR geben, z.B. als “verteilte“ Datenbank.
- Speichert u.a. folgende Daten:
  - MSISDN.
  - MSRN im HLR (Heimatland) wird aktualisiert, sobald sich die MS in einem VLR im Ausland befindet.
  - IMSI
  - Dienstprofil (Anrufweiterleitung, Dienstrestriktionen,...).

GSM Netzaufbau - AuC - *Authentification Center*

- Speichert Daten zur Authentifizierung der MS und der Verschlüsselung.
- z.B. einen geheimen, mit der SIM-Karte gemeinsamen Schlüssel ($\rightarrow K_i$).
- Authentifizierung über Challenge-Response-Verfahren.

GSM Netzaufbau - SMSC - *Short Message Service Center*



[6]

[6] Quelle: Grundkurs Mobile Kommunikation, Seite 31, Abb. 1.17

Übersicht

IMSI (*International Mobile Subscriber Identity*)

- Weltweit eindeutige Nummer für Mobilfunkteilnehmer.
- Wird auf SIM-Karte gespeichert.
- Besteht aus maximal 15 Ziffern:
  - Mobile Country Code (MCC), 3 Ziffern.
  - Mobile Network Code (MNC), 2 oder 3 Ziffern.
  - Mobile Subscriber Identification Number (MSIN), 1-10 Ziffern.
  - Bsp: 262 07 9745642247: MCC=262 für Deutschland, MNC=07 für O2, MSIN= 9745642247 für den Teilnehmer.

TMSI (*Temporary Mobile Subscriber Identity*)

- Lokale, zeitlich beschränkte Identifikationsnummer innerhalb einer Location Area.
- Wird für Verbindungsaufbau genutzt (Paging Requests).
- Ändert sich unterschiedlich oft, abhänig vom Netzbetreiber
- Erschwert das Erstellen von Bewegungsprofilen.
- Wird vom VLR zugewiesen.

ARFCN (*Absolute Radio Frequency Channel Number*)

- Aus der ARFCN lassen sich die Up- und Downlinkfrequenzen eines Kanalpaars berechnen.

$$f_{downlink} = f_{uplink} + Abstand \tag{1}$$

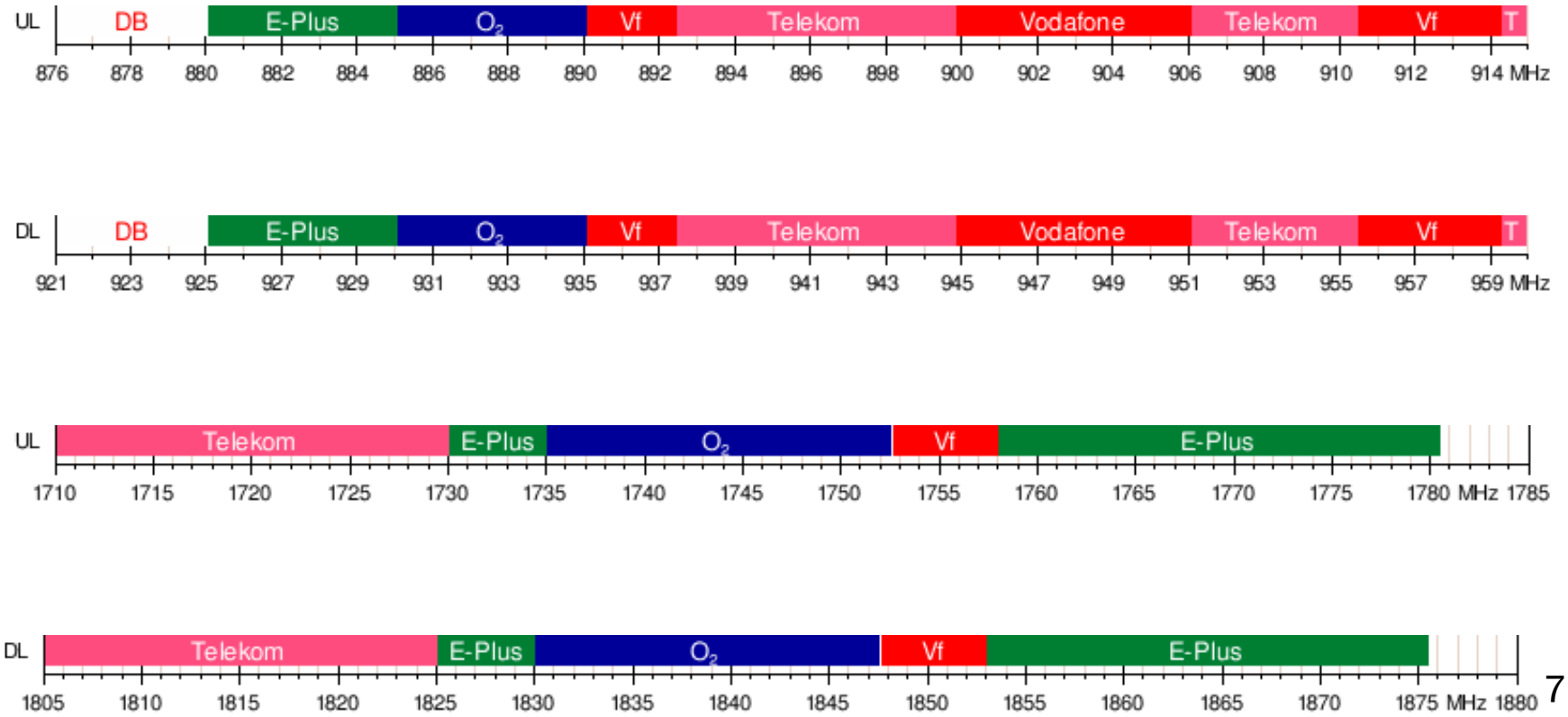
$$f_{uplink} = Startfrequenz + (ARFCN - Offset) \cdot 0,2\text{MHz} \tag{2}$$

$$ARFCN = \frac{f_{uplink} - Startfrequenz}{0,2\text{MHz}} + Offset \tag{3}$$

Name	ARFCNs	Startfrequenz	Offset	Abstand	Uplinkfrequenzen	Downlinkfrequenzen
GSM 850	128 - 251	824,2 MHz	128	45 MHz	824,2 - 848,8 MHz	869,2 - 893,8 MHz
P-GSM	1 - 124	890,0 MHz	0	45 MHz	890,2 - 914,8 MHz	935,2 - 959,8 MHz
E-GSM	0 - 124	890,0 MHz	0	45 MHz	890,0 - 914,8 MHz	935,0 - 959,8 MHz
DCS 1800	512 - 885	1710,2 MHz	512	95 MHz	1710,2 - 1784,8 MHz	1805,2 - 1879,8 MHz
PCS 1900	512 - 810	1850,2 MHz	512	80 MHz	1850,2 - 1909,8 MHz	1930,2 - 1989,8 MHz

Übersicht

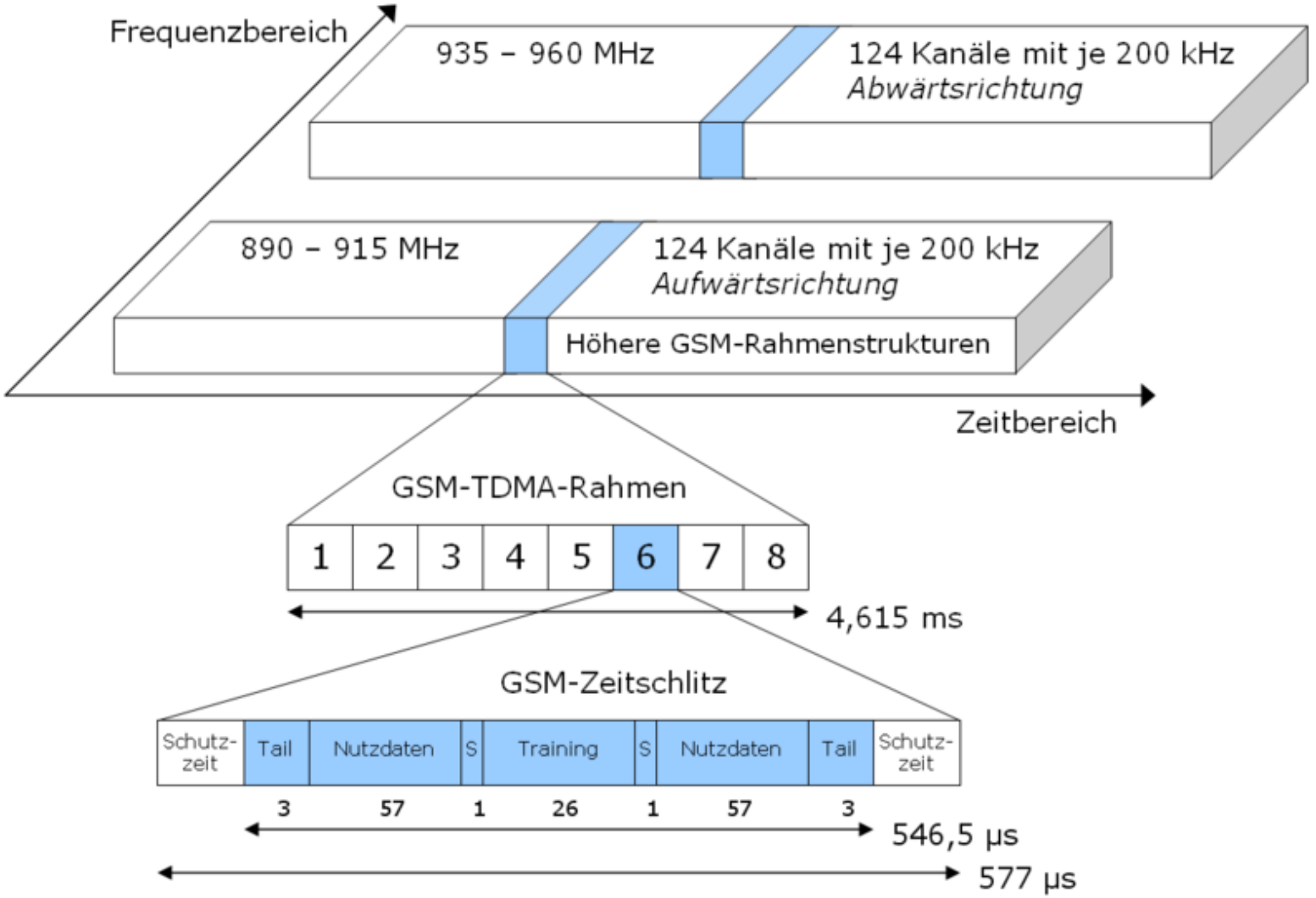
Frequenzverteilung in Deutschland



[7]

[7] Quelle: Wikipedia (https://de.wikipedia.org/w/index.php?title=Global_System_for_Mobile_Communications&oldid=95548871)

Multiplexverfahren im GSM Netz



8

[8] Quelle: Wikipedia (https://de.wikipedia.org/wiki/Datei:Gsm-rahmenstruktur.png)

logische GSM-Channel

- Mehrere TDMA-Rahmen werden zusammengefasst um logische Channels abzubilden.
- Für Signalisierungschannel werden 51 TDMA-Rahmen zu einem Multirahmen zusammengefasst, für Trafficchannel 26.
- Über eine Zuordnungsvorschrift werden Bursts bestimmten Timeslots zugewiesen. Diese Slots werden wiederum bestimmten Frames zugewiesen.
- Logische Channels sind in zwei unterschiedliche Channel-Gruppen unterteilt: Signalisierungschannel und Trafficchannel.

logische GSM-Channel - Trafficchannel

Traffic Channel dienen der Nutzdatenübertragung und lassen sich aufteilen in:

- TCH/F (full rate) $\rightarrow$ nutzt jeden Timeslot eines Multiframes zur Übertragung.
- TCH/H (half rate) $\rightarrow$ nutzt nur jeden zweiten Timeslot aus einem Multiframe zur Übertragung. $\rightarrow$ Die effektive Datenrate im TCH/H ist also nur halb so groß.

Dedicated Control Channel

Ein Dedicated Control Channel (*DCCH*) ist ein point-to-point Control Channel. Wichtige DCCHs sind:

- SDCCH (*stand-alone DCCH*).
  - Signalisierungskanal, der nicht an die Reservierung eines TCH gebunden ist.
  - Wird verwendet, wenn zwischen BTS und MS noch kein Signalisierungskanal besteht.
  - z.B. für SMS Übertragung und Zuordnung eines TCH.
- FACCH (f*ast accosiated control channel*).
- SACCH (*slow accosiated control channel*).

Dedicated Control Channel

Ein Dedicated Control Channel (*DCCH*) ist ein point-to-point Control Channel. Wichtige DCCHs sind:

- SDCCH (*stand-alone DCCH*).
- FACCH (f*ast accosiated control channel*).
  - Wird für Signalisierungsinformationen genutzt, die schnell an der MS ankommen müssen. (z.B.Handover-Kommando)
  - Keinen eigenen Platz im Multiframe, ersetzt im TCH einen Burst mit seinen Daten. Wird der MS durch das Stealing-Bit signalisiert.
  - Der FACCH ist bi-direktional.
- SACCH (*slow accosiated control channel*).

Dedicated Control Channel

Ein Dedicated Control Channel (*DCCH*) ist ein point-to-point Control Channel. Wichtige DCCHs sind:

- SDCCH (*stand-alone DCCH*).
- FACCH (f*ast accosiated control channel*).
- SACCH (*slow accosiated control channel*).
  - Ist einer aktiven MS zugeordnet.
  - Zur Übertragung von weniger zeitkritischen Informationen.
  - z.B. Uplink für Messergebnisse.

non-Dedicated Control Channel

Die non-Dedicated Control Channel teilen sich auf in:

- Broadcast Control Channel.
- Common Control Channel.

Beide sind point-to-multipoint, also von einer Base Station zu mehreren MS.

non-Dedicated Control Channel

Die non-Dedicated Control Channel teilen sich auf in:

- Broadcast Control Channel.
  Wird dazu genutzt, der MS verschiedene Informationen bekannt zu machen. Dies sind beispielsweise Informationen die nötig sind um auf das Netzwerk zugreifen zu können (z.B.Synchronisierungsdaten) (Übung)
- Common Control Channel.

Beide sind point-to-multipoint, also von einer Base Station zu mehreren MS.

non-Dedicated Control Channel

Die non-Dedicated Control Channel teilen sich auf in:

- Broadcast Control Channel.
- Common Control Channel.
  Besteht u.a. aus 3 Teilen:
  - RACH (*Random Access Channel*) - Uplink, MS zum Netzwerk. Wird z.B. genutzt um einen Dedicated Control Channel anzufordern.
  - AGCH (*Access Grant Channel*) - Downlink, Netzwerk zur MS. Wird genutzt um einen Dedicated Control Channel zuzuweisen.
  - PCH (*Paging Channel*) - Downlink, Netzwerk zur MS. Wird verwendet um inaktive Teilnehmer über den Empfang einer SMS oder eines eingehenden Anrufen zu benachrichtigen.

Beide sind point-to-multipoint, also von einer Base Station zu mehreren MS.

Übersicht

LAPDm

- Link Access Procedure for the Dm-Channel.
- An LAPD angelehntes Protokoll (ISDN).
- Bitorientiertes, synchrones Protokoll.
- Wird zwischen MS und BTS (*Um Interface*) “gesprochen“.
- Soll zuverlässige Datenübertragung gewährleisten.

Übersicht

Radio Ressource Management (RR)

Hauptaufgabe des RR ist die Verwaltung der logischen Channel sowohl auf MS als auch auf Netzseite. Zudem werden durch das RR viele Systeminformationen, Paging-Nachrichten, Measurement Reports, usw übertragen.

- Handover: Funkzellenwechsel, falls anderes Signal besser ist.
- Die MS führt laufend Feldstärkenmessungen seiner und der Nachbarzellen durch. Diese werden durch das RR an den BSC gesendet. Der BSC entscheidet ob ein Handover geschehen soll und reserviert in diesem Fall die nötigen Ressourcen.

Radio Ressource Management (RR) - *Systeminformationen*

RR ist für die Übertragung vieler Systeminformationen (SI) zuständig.

- SI 2, 2ter, 2quater, 2bis: Frequenzen und Zugriffsberechtigungen der Nachbarzellen werden gebroadcastet (über BCCH).
- SI 3: u.a. Cell Identity, MCC, MNC, LAC
- SI 5 und 6: BCCH-Frequenzen der Nachbarzellen. SI dieses Typs werden auf dem SACCH übertragen, damit eine MS auch bei aktiver Verbindung nach einem Handover (kann in diesem Moment SI 2 nicht lesen) die Frequenzen kennt.

Radio Ressource Management (RR) - *Paging Requests*

RR ist für Paging Request zuständig.

- Kommt ein Anruf oder eine SMS für eine MS an, werden in der kompletten Location Area Paging Request ausgeschickt. Die MS muss darauf reagieren.

Mobility Management (MM)

- Hauptaufgabe des MM ist es den Standort der MS zu aktualisieren, wenn sie sich von einer zu einer anderen Location Area bewegt. (*Location Update Procedure*)
- Zudem wird die Location Area der MS in regelmäßigen Abständen an MSC/VLR gemeldet. Falls eine MS auf ein Paging nicht reagiert, wird es dort als inaktiv markiert. Um die Markierung wieder zu löschen ist die regelmäßige Location Update Procedure nötig.
- Inter-MSC Location Update: In diesem Fall muss das neue MSC/VLR das HLR über den Wechsel des Teilnehmers in die neue Area informieren. Das HLR löscht die Daten des Teilnehmers daraufhin im alten MSC/VLR.
- Ist für die Authentifizierung der MS verantwortlich.

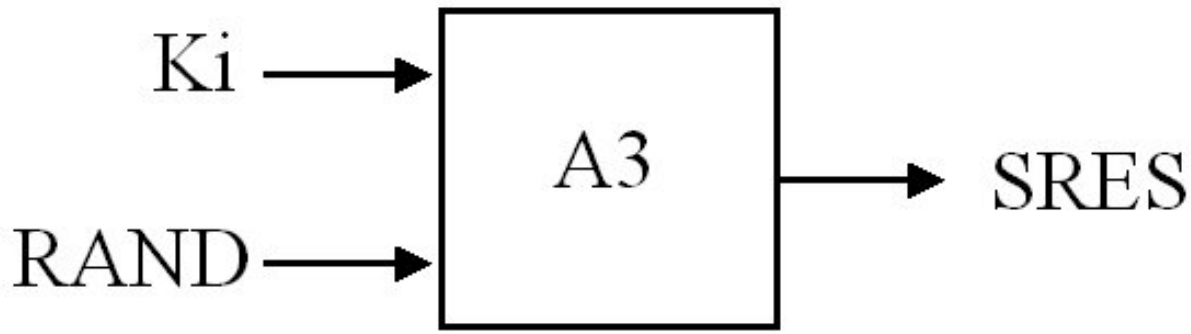
Connection Management (CM)

- Call Control ist für das Auf- und Abbauen von Anrufen und zugehörigen Funktionen (z.B. Halten) verantwortlich.
- Neben dem Call Controll ist das Connection Management u.a. für das SMS- und das Mobile IP Protokoll zuständig.

Übersicht

Authentifizierung im GSM-Netz

- Im AuC wird gespeichert: K_i und der zu verwendende Verschlüsselungsalgorithmus.
- K_i wird nie über die Luftschnittstelle übertragen.
- Challenge-Response-Authentifizierung.
- Beim Einbuchen in ein Netz wird vom VLR beim AuC ein Authentifizierungsdatensatz angefordert.



9

[9] Quelle: Grundkurs Mobile Kommunikation, Seite 28, Abb. 1.14

Authentifizierung im GSM-Netz

1. AuC erstellt eine Zufallszahl RAND.

Authentifizierung im GSM-Netz

1. AuC erstellt eine Zufallszahl RAND.
2. RAND und K_i wird mit dem A3-Algorithmus verschlüsselt

Authentifizierung im GSM-Netz

1. AuC erstellt eine Zufallszahl RAND.
2. RAND und K_i wird mit dem A3-Algorithmus verschlüsselt
3. (*SRES*, K_c, RAND) wird an VLR übertragen.

Authentifizierung im GSM-Netz

1. AuC erstellt eine Zufallszahl RAND.
2. RAND und K_i wird mit dem A3-Algorithmus verschlüsselt
3. (*SRES*, K_c, RAND) wird an VLR übertragen.
4. RAND wird dann an die MS gesendet.

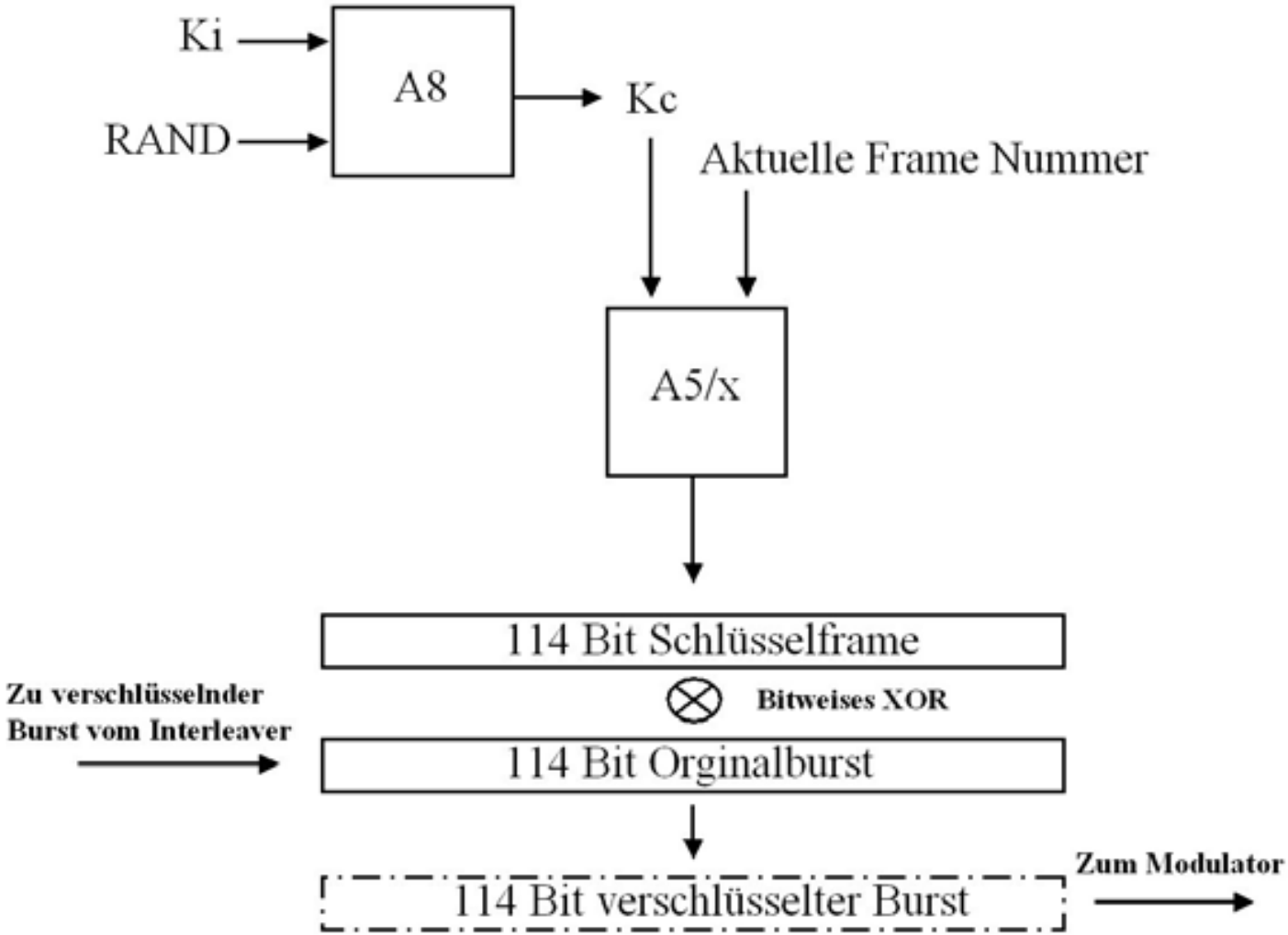
Authentifizierung im GSM-Netz

1. AuC erstellt eine Zufallszahl RAND.
2. RAND und K_i wird mit dem A3-Algorithmus verschlüsselt
3. (*SRES*, K_c, RAND) wird an VLR übertragen.
4. RAND wird dann an die MS gesendet.
5. Die MS (genauer: die SIM-Karte) verschlüsselt RAND und den gespeicherten Schlüssel K_i mit dem A3-Verschlüsselungsalogorithmus.

Authentifizierung im GSM-Netz

1. AuC erstellt eine Zufallszahl RAND.
2. RAND und K_i wird mit dem A3-Algorithmus verschlüsselt
3. ($SRES$, K_c, RAND) wird an VLR übertragen.
4. RAND wird dann an die MS gesendet.
5. Die MS (genauer: die SIM-Karte) verschlüsselt RAND und den gespeicherten Schlüssel K_i mit dem A3-Verschlüsselungsalogorithmus.
6. Das Ergebnis ($SRES_{MS}$) wird an das MSC zurückgeschickt. Passt der empfangene Wert mit $SRES_{AuC}$ zusammen, ist die MS authentifiziert.

Verschlüsselung von Daten-Bursts

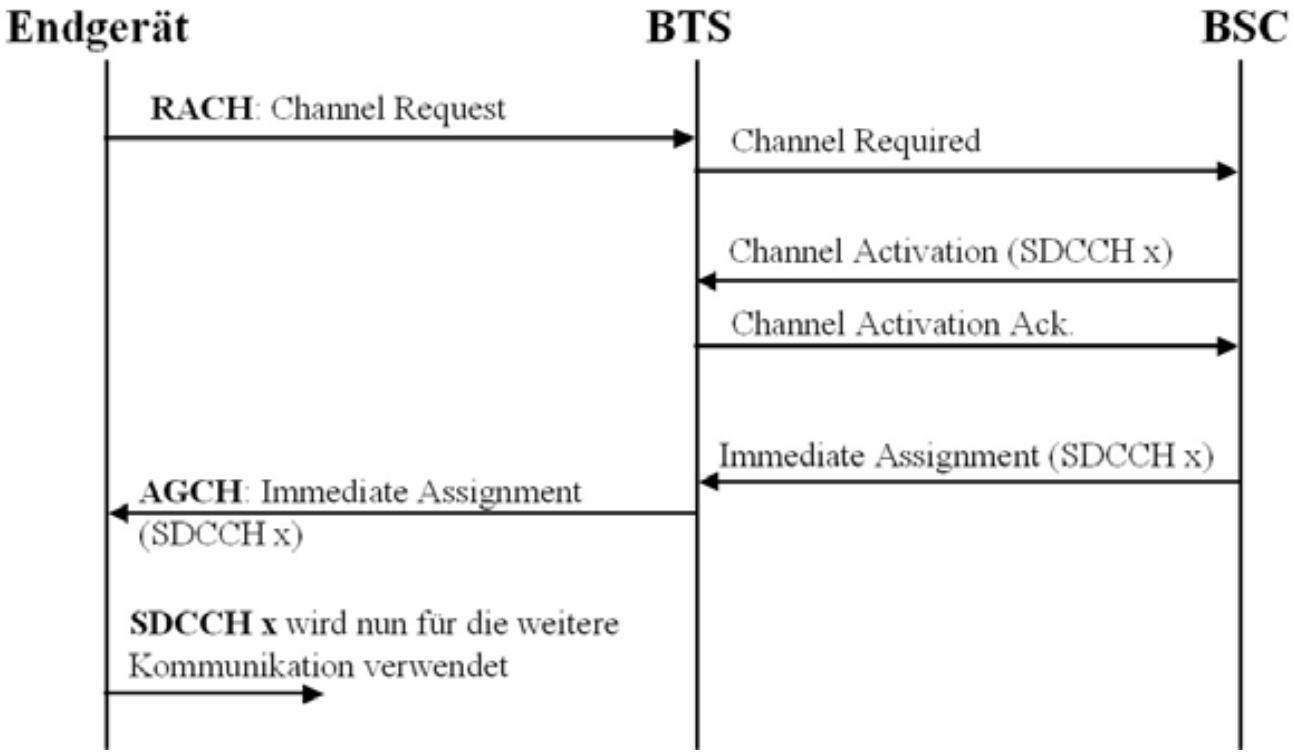


10

[10] Quelle: Grundkurs Mobile Kommunikation, Seite 62, Abb. 1.38

Verbindungsaufbau (ausgehend)

- RACH (Einziger CCCH von MS zu Netz).
- Wird genutzt falls MS über den PCH (*Pagingchannel*) gerufen wird, oder falls man selbst eine Verbindung aufbauen möchte (Telefonieren / SMS / ...).
- Kollisionen können im RACH auftreten.



[11]

[11] Quelle: Grundkurs Mobiele Kommunikationssysteme, Seite 44, Abb. 1.26

Übersicht

Sicherheitslücken und Schwachstellen im Design

- Optionale Verschlüsselung auf der Luftschnittstelle.
- Keine Verschlüsselung auf dem Abis Interface (BTS zu BSC).
- Schwachstelle A5/2 Verschlüsselung: Für Export in Länder mit Exportverbot für Sicherheitstechnik. Verwendung seit 06/2007 vom 3GPP nicht mehr empfohlen. $\rightarrow$ Berechnung des Schlüssels mit aktuellen PCs innerhalb von Sekunden.
- Keine Authentifizierung des Netzwerks gegenüber dem Endgerät. ($\rightarrow$ IMSI-Catcher)
- GSM Standard: Wenn keine Verschlüsselung verwendet wird $\rightarrow$ Symbol anzeigen. (Gut um IMSI-Catcher zu entdecken.)
  Aber: Operator kann ein SIM-Card Bit setzen, sodas dieses Feature abgeschaltet wird. Dies ist fast immer der Fall.

Passive, Semi-Aktive, Aktive Angriffe

Passive Angriffe:

- Daten entschlüsseln ohne MS oder GSM-Netz zu beeinflussen.

Semi-Aktive Angriffe:

- Siehe *Semi-Aktiver Angriff auf A5/1 und A5/3*.

Aktive Angriffe:

- IMSI-Catcher setzt Gespräche gefangener MS wieder ins GSM-Netz um. (Man in the Middle)

Angriff auf die Verschlüsselung I

Passiver Angriff auf A5/1 möglich unter folgenden Voraussetzungen:

- 4 OsmocomBB Handys.
- Mit den 4 Handys aufgezeichneter Datenstrom.
- Rainbowtables (frei im Internet downloadbar).
- Einige Software-Tools, leider nicht alle veröffentlicht. :-(
- Gespräche und SMS können in wenigen Minuten entschlüsselt werden.

Angriff auf die Verschlüsselung II

Semi-Aktiver Angriff auf A5/1 und A5/3:

- Verbindung aufzeichnen.
- MS zu eigener BTS verbinden lassen.
- Zur Verbindung A5/2 zuweisen, ohne neue Authentifizierung.
- Ciphering-Key K_c kann berechnet werden.
- Der gleiche Schlüssel wurde auch in der zuvor aufgezeichneten Verbindung verwendet $\rightarrow$ Entschlüsselung der aufgezeichneten Verbindung möglich.

Identitätsdiebstahl

- Gültige Verbindung Abhören (mit Osmocom)
- Schlüssel K_c brechen (geht in wenigen Sekunden).
- Mit gebrochenem K_c abgehörte Daten enschlüsseln.
- Aktuelle TMSI den Daten entnehmen.
- Die beiden authentifizierenden Merkmale K_c und TMSI sind nun bekannt.
- Osmocom Handy mit vorprogrammierten authentifizierungs Merkmalen (K_c, TMSI) kann Abgehörtes Handy emulieren.

IMSI-Catcher

4 grundlegende Funktionen

- Ermittlung der IMSI
- Ermittlung der IMEI
- Lokalisierung der MS
- Gespräche abhören

[1]

[1] Quelle: http://www.handyblocker.org/imsi-catcher/IMEI-catcher-5000.htm

IMSI-Catcher - Ermittlung der IMSI und IMEI

Zur Ermittlung der IMSI führt der IMSI-Catcher folgende Schritte durch:

1. Klon einer Funkzelle einer Basisstation, die sich in der Nähe des IMSI Catchers befindet. (Eher eine mit schlechter Qualität)
2. Die MS buchen sich in die Basisstation ein, weil die simulierte Basisstation die höchste Qualität hat.
3. Mittels eines *IMSI_Request*-Befehls kann die Basisstation die IMSI der MS ermitteln.

- Funktioniert nur, weil GSM eine einseitige Authentifizierung macht: MS authentifiziert sich am Netz (siehe vorherige Folien), Netz aber nicht bei der MS.

Die Ermittlung der IMEI erfolgt auf ähnliche Art und Weise.

DoS einer Zelle

Funktionsweise:

- Anmelde-Nachricht über RACH senden (100-200 pro Sekunde).
- *Immediate Assignment*-Nachricht ignorieren.
- Die BTS hält den Timeslot reserviert (für ca. 2 bis 5 Sekunden).

Bedeutung:

- Eine in dieser Zelle eingebuchte MS kann nicht mehr Anrufen oder SMS schreiben.
- Laufende Gespräche sind nicht betroffen
- Manche MS verbinden sich möglicherweise mit der Nachbarzelle.
- Angriff ist anonym da keine Authentifizierung statt gefunden hat.
- Jamming (MS sendet so stark, dass andere MS von der BTS überhört werden.)

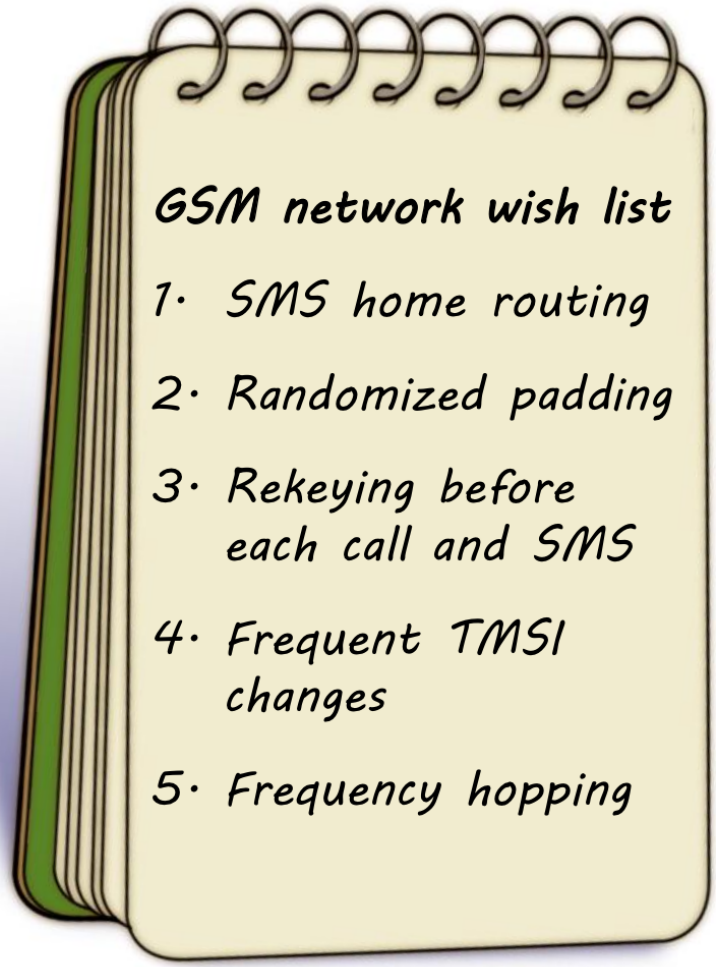
DoS eines Handys

1. Falsch formatierte SMS an Handy mit Parsing-Fehler senden.
2. Handy stürzt beim Verarbeiten der SMS ab.
3. Handy muss neu gestartet werden (manchmal auch Automatisch).

- Im schlimsten Fall:
  - Handy hat Empfang der SMS nicht dem SMSC gemeldet.
  - SMS wird nach Neustart sofort wieder ausgeliefert $\rightarrow$ Endlosschleife.

Übersicht

GSM - Wishlist



12

[12] Quelle: Karsten Nohl, Sylvain Munaut, GSM Sniffing, 27c3

Aktuelles I

- Warum GSM-Security? GSM wird von 88% der Deutschen über 14 genutzt. Es gibt insgesamt 98 Millionen aktive Handys.
- Demgegenüber: 60% der Deutschen nutzen regelmäsig das Internet.
- Also: Weg von TCP/IP, neue Welten entdecken!

Aktuelles II

- 2010: mindestens 440.783 Stille SMS in Deutschland alleine von Zoll, BKA, BVS (250.000 davon in NRW) ermöglichten es Gespräche und SMS zu belauschen.
- 2011 in Dresden: wurden bei einer Anti-Nazi-Demo 896.072 Verkehrsdatensätze, 257.858 Rufnummern und 40.732 Bestandsdaten von Ermittlungsbehörden bei den Providern abgefragt. Zudem wurden IMSI-Catcher eingesetzt.
- gern genutztes Ermittungsinstrument: Funkzellenabfrage. Dresden zu den Anti-Nazi-Demos und Berlin nach Auto-Bränden aber auch in vielen anderen Fällen
- Personen in Einkaufzentren tracken. (USA, Projekt wurde gestoppt). http://www.theregister.co.uk/2011/11/29/cellphone_tracking_nixed/

Übersicht

Literatur

- Grundkurs Mobile Kommunikationssysteme, Martin Sauter, Vieweg + Teubner Verlag — Springer Fachmedien Wiesbaden GmbH 2011, 4. überarbeitete und erweiterte Auflage, ISBN: 978-3-8348-1407-4
- GSM-Standards, http://www.3gpp.org/specification-numbering

Links I

Videos:

- 27c3 Video über OsmocomBB: http://mirror.fem-net.de/CCC/27C3/mp4-h264-HQ/27c3-3952-en-running_your_own_gsm_stack_on_a_phone_osmocombb.mp4
- 28c3 Video mit dem Titel "Defending Mobile Phones". (u.A. Hack um auf Kosten anderer zu telefonieren.): http://ftp.ccc.de/congress/28C3/mp4-h264-HQ/28c3-4736-en-defending_mobile_phones_h264.mp4
- 27c3 Video: Person finden anhand der Telefonnummer, SMS sniffen, Telefonate abhören. (Alles mit nur 4 "OsmocomBB-Handys"): http://mirror.fem-net.de/CCC/27C3/mp4-h264-HQ/27c3-4208-en-wideband_gsm_sniffing.mp4

Links II

Videos:

- 26c3 Video mit dem Titel “Playing with the GSM RF Interface“. Zeigt eine DoS-Angriff der eine ganze Zelle mit nur einem Handy lahm legen kann: http://ftp.ccc.de/congress/26c3/mp4/26c3-3608-en-playing_with_the_gsm_rf_interface.mp4
- 26c3 Video mit dem Titel “GSM: SRSLY?“ (Allgemeines zur Lage von GSM): http://ftp.ccc.de/congress/26c3/mp4/26c3-3654-en-gsm_srsly.mp4
- 27c3 Video über SMS basierte Angriffe auf Handys: http://mirror.fem-net.de/CCC/27C3/mp4-h264-HQ/27c3-4060-en-attacking_mobile_phones.mp4
- 26c3 Video mit dem Titel “Using OpenBSC for fuzzing of GSM handsets“: http://ftp.ccc.de/congress/26c3/mp4/26c3-3535-en-using_openbsc_for_fuzzing_of_gsm_handsets.mp4

Links III

Audio:

- Chaosradio Express: GSM Security (Seeeehr zu empfehlen!) http://chaosradio.ccc.de/cre179.html
- Chaosradio: Handyschnüffelein http://chaosradio.ccc.de/cr170.html
- Chaosradio Express: OpenBSC http://chaosradio.ccc.de/cre120.html
- Chaosradio Express: TETRA Bündelfunk (Nicht direkt GSM, aber ähnlich) http://chaosradio.ccc.de/cre183.html