Mobilkommunikation, Architektur und Protokolle

Zusammenfassung MoKomAP HSR FS15

Emanuel Duss

2015-08-26 12:28

Inhaltsverzeichnis

Quellen

- Buch: Grundkurs Mobile Kommunikationssysteme. Martin Sauter. Vieweg. 2. Auflage. 2008.
- Vorlesungsfolien MoKomAP.

1 Mobile Kommunikation Grundlagen

1.1 Definition

- Benutzermobilität: Benutzer kann an jeder Zeit und an jedem Ort mit einem anderen Benutzer kommunizieren.
- Gerätemobilität: Gerät kann an jeder Zeit und an jedem Ort an ein Kommunikationsnetzz angeschlossen werden.
- Übertragung geschieht über eine spezielle Infrastruktur
- Teilnehmer kommunizieren mit Base Station (BS)
- BS sind über ein Netzwerk miteinander verbunden.
- Teilnehmerzahl ist begrenzt (begrenzte Übertragungsfrequenzen und erforderlicher Bandbreite)
- Grössere Übertragungsstörungen als im Festnetz
- Es können jegliche Art von Daten übermittelt werden, auch Multimediadaten.
- Es gibt private und öffentliche Netze.

1.2 Multiplextechniken

- Bereitstellung eines Mediums an mehrere Teilnehmer durch Multiplextechniken.
- Raummultiplex: Einteilung des Raumes in verschiedene Bereich. (Zellen, Kabelbündel)
- Zeitmultiplex (Time Division Multiple Access, TDMA): Nutzung des Mediums von jeder Person für eine bestimmte Zeitperiode. (Festnetz, GSM, Ethernet CSMA/CD)
- Frequenzmultiplex (Frequency Division Multiple Access FDMA): Jeder Teilnehmer hat eine eigene Frequenz. (Radio, TV, GSM)
- Codemultiplex: Alle senden auf gleicher Frequenz aber mit einem Code können die Teilnehmer unterschieden werden. (UMTS)

1.3 Ausbreitung von Wellen

- Abschattung (shadowing) durch Hindernis
- Reflexion: Reflektierte Signale sind schwächer
- Streuung (scattering)
- Beugung (diffraction): Ablenkung des Signals
- Dämpfung und Verzögerung: Quadratische Abnahme. Zeitsynchronisation ist orgstabhängig (time alignment)
- Inferenzen: Überlagerungen zwischen getrennten Kanälen (Konkurrieren von mehreren Mobilstationen)
- Zellgrenze: Linie mit gleicher Sendeleistung der Nachbarzelle. Deshalb Sechsecke.
- Multipath Fading: Signale kann mehrfach und zeitlich versetzt beim Empfänger ankommen.

1.4 Zellplanung

- Wie viele Zellen werden für die Netzabdeckung einer Region benötigt?
- Abhängig von
  - Anzahl Kanäle pro Zelle
  - Anzahl Teilnehmer pro Zelle
  - Qualität des Dienstes (Grade of Service, GOS)
  - Mittlere Verkehr einer Zelle
- Empfehlung: 25 - 35 mErlang und ein GOS von 2%
- Zelltypen: Pico-Zelle (100 m), Micro-Zelle (2 km), Macro-Zelle (35 km)
- Wie gross ist die Wahrscheinlichkeit, dass alle Bedienstationen blockiert sind?

Angebotener Verkehr:

$$A = \frac{n \cdot T}{3600}$$

- A: Angebotener Verkehr in Pseudoeinheit Erlang
- n: Mittlere Anzahl der Anrufe pro Zelle pro Stunde
- T: Mittlere Dauer eines Gespräches
- Beispiel:

Blockierungswahrscheinlichkeit:

$$B = \frac{\frac{A^n}{n!}}{\sum_{i=0}^{n} \frac{A^i}{i!}}$$

- A: Angebotener Verkehr in Pseudoeinheit Erlang
- N: Anzahl Kanäle (Bedienstationen)
- B: Blockierungswahrscheinlichkeit

2 GSM (Global System for Mobile Communication)

2.1 Geschichte

- A Netz (1958): Handvermittlung
- B Netz (1972): Selbstwahl
- C Netz (1985): Analoges Mobilfunknetz, Handover, Mobilbux, Rufumleitung
- D Netz (1990): GSM

2.2 Leitungsvermittelnde Datenübertragung

- GSM Netz: Anfang der 90er Jahre
- Leitungsvermittelnde Datenübertragung: Leitung wird von Switching Center über eine Switching Matrix zwischen zwei Teilnehmer geschaltet.
- Die Übertragung ist heute digital (Analog - Digital (Übertragung) - Analog)
  - Bearer Independent Core Network: Heute werden die Pakete per IP oder ATM übertragen
- Es wurde die selbe Hardware für das Telefonnetz verwendet, jetzt kann der Benutzer sein Standort aber frei wählen und wechseln. Deshalb ist keine 1:1 Zuordnung zwischen Teilnehmer und Leitung möglich.
- Mobile Station (MS): Endgerät.
- Multiplexingtechniken: Raummultiplex, Frequenzmultiplex, Zeitmultiplex
- Übertragungsprobleme:
  - Bitfehler $\rightarrow$ Kanalcodierung
  - Rayleigh Fading $\rightarrow$ Frequency Hopping
  - Time Dispersion $\rightarrow$ Adaptive Equalization
  - Rahmensynchronisation $\rightarrow$ Time Advance

2.3 Standards

- Standardisierung der Schnittstellen und technischen Vorgängen der ITU (International Telecommunication Union). Beispielsweise das Signalisierungssystem SS-7 für die Gesprächsvermittlung. Nationale Erweiterungen der Standards sind möglich.
- Das ETSI (European Telecommunication Standards Institute) hat GSM spezifiziert. Die sind in TS (Technical Specifications) beschrieben. Da die Standards auch ausserhalb Europa wichtig sind, gründeten sie das internationale 3GPP (3rd Generation Partnership Project) http://www.3gpp.org.

2.4 Übertragungsgeschwindigkeiten

- Kleinste Geschwindigkeit hat der Digital Signal 0 Kanal (DS0) mit 64 kbit/s welcher Sprachen und Daten übertragen kann.
- Die E-1 Verbindung überträgt 2048 MBit/s (2 Gbit/s) über Twisted Pair oder Koaxialkabel und ist in 32 Timeslots à 64 kbit/s aufgeteilt in denen DS0 Datenströme übertragen werden. Ein Timeslot pro E-1 wird für die Synchronisation reserviert.
  - Beispiel 31 Timeslots à 8 Bit bei 8000 Hz: 32 * 8 Bit * 8000 1/s = 2048 Mbit/s
- Da E-1 meist nicht ausreicht zwischen Vermittlungsstellen gibt es E-3, welche 34.368 MBit/s (512 DS0) unterstützt.
- STM (Synchronous Transfer Mode) ist ein optisches System welches zwischen 2300 (STM-1) bis 148'279 (STM-64) DS0 Kanäle unterstützt.

2.5 Signaling System 7 (SS-7)

2.5.1 Zweck und Komponenten

- Früher war die Signalisierung mit Pulswahl, heute mit Dual Tone Multi Frequency (DTMF) über einen eigenen Signalisierungskanal.
- Für den Austausch von Signalisierungsinformationen wird das SS7 Netz verwendet.
- Drei unterschiedliche Netzwerkknoten:
  - SSP (Service Switching Point) Vermittlungsstellen (Aufbau, zustellung oder Weiterleitung von Daten- oder Sprachverbindungen)
  - SCP (Service Control Point): Software mit Datenbank (Home Location Register, HLR) welche den Aufbau einer Verbindung beeinflussen. (Aufenthaltsort des Teilnehmers)
  - STP (Signaling Transfer Points): Weiterleitung von Signalisierungsnachrichten zwischen SSP und SCP.

2.5.2 Stack

- Layer 1 bis 3: MTP-1 bis MTP-3 (Message Transfer Part). Layer 3 ist gut mit IP vergleichbar.
- ISUP (ISDN User Part) Protokoll für Auf- und Abbau eines Übertragungskanals
  - MSC (Mobile Switching Center) Mobilfunkvermittlungsstelle an die der Telefonierende die Zielnummer übermittelt.
  - IAM (Initial Address Message): Aufbau des Nutzungskanals für die Sprachübertragung über einen STP. Infos wie Zielnummer und welcher Nutzkanal verwendet werden soll.
  - ACM (Address Complete Message): Nachricht zurück an MSC, falls das Zieltelefon klingelt.
  - ANM (Answer Message): Nachricht an MSC, falls der Hörer abgenommen wurde.
  - REL (Release Message): Meldung an Gegenüber, dass aufgelegt wurde.
  - RLC (Release Complete Message): Bestätigung, dass auflegen funktioniert hat.
- SCCP (Signalling Connection and Control Part): Layer 4 Kommunikation zwischen SSP und SCP. Statt einem Port wie in TCP/UDP gibt es die Subsystem Nummer (SSN)
- TCAP (Transaction Capability Application Part): Layer 5 Protokoll für den Zugriff die Datenbanken der SCP.
- MAP (Mobile Application Part): Kommunikation zwischen MSC und HLR um Teilnehmerinfos abzufragen oder zwischen zwei MSC um Bewegung zu anderem MSC mitzuteilen. MAP verwendet TCAP, SCCP und MTP.
- BSSMAP (Base Station Subsystem Mobile Application Part): Kommunikation zwischen MSC und Radionetzwerk. Setzt auf SCCP auf.
- DTAP (Direct Transfer Application Part): Austausch von Nachrichten zwischen MS und MSC.

2.6 GSM Subsysteme

- BSS (Basestation Subsystem): Auch Radio Netzwerk. Elemente für die Verbindung zwischen MS und Netzwerk über die Luftschnittstelle.
- NSS (Network Subsystem): Auch Core Network. Elemente für die Vermittlung von Gesprächen, Teilnehmerverwaltung und Mobilitätsmanagement.
- IN (Intelligent Network Subsystem): Besteht aus SCP Datenbanken welche zusätzliche Dienste bereitstellen (beispielsweise abziehen von Geld bei einem Prepaid Service).

2.7 Network Subsystem (NSS)

2.7.1 MSC (Mobile Switching Center)

- Kommunikation mit Teilnehmer (MS)
- Call Control (CC): Teilnehmer Registrieren (Telefon einschalten), Verbindungsaufbau (Call Routing), SMS weiterleiten
- Mobility Management: Authentifizierung (Authentication), Position mitteilen (Location Update), Positionsänderung mitteilen (Handover)
- Kommunikationsschnittstellen
  - A-Interface: E-1 Verbindung zwischen MSC und MS E-1 Leitungen.
  - E-Interface: E-1 Verbindungen zwischen den MSCs.
  - C-Interface: E-1 Signalisierungsverbindung zwischen MSC und HLR.
  - D-Interface: Kommunikation mit dem HLR
- Digitalisierung der Sprachübertragung:
  - Analoges signal auf 300 Hz bis 3400 Hz begrenzen, 8000 mal abtasten pro Sekunde und quantisieren (in 8 Bit Wert speichern).
  - Um leiste Töne (kleine Amplitude) gut zu übertragen, werden für diese mehr digitale Werte verwendet als für laute Töne.
  - Das kodierte Signal heisst PCM (Pulse Code Modulated), in Europa der a-Law Standard.
- Billing: MSC erstellt für jedes Gerät ein Billing Record welcher zum Abrechnungssystem übertragen wird (Quell-/Zielnummer, Funkzelle ID, Zeit Beginn, Dauer, . . .)
- Prepaid Billing: Wird während der Laufzeit mit einem IN System abgerechnet.

2.7.2 Visitor Location Register (VLR)

- Jede MSC hat ein VLR mit Infos über die aktuellen Teilnehmer und stellt eine lokale Kopie des HLR dar.

2.7.3 Home Location Register (HLR)

- Teilnehmerdatenbank des GSM Netzes, welche die folgenden Informationen speichern:
- IMSI (International Mobile Subscriber Identity): Weltweit eindeutige maximal 15 stellige Nummer eines Teilnehmers, welche auf der SIM Karte gespeichert wird.
  - MMC (Mobile Country Code): 3 stellige Land ID: CH: 228, DE: 262, USA: 310
  - MNC (Mobile Network Code): 2 stellige Provider ID
  - MSIN (Mobile Subscriber Identification Number): Eindeutig im nationalen Netzwerk.
  - Abfragen über serielle Verbindung zum Telefon mit `at+cimi`
- MSISDN (Mobile Subscriber ISDN Number): Maximal 15 stellige Telefonnummer
  - Country Code: CH: +41, DE: +49
  - NDC (National Destination Code): 3 stellige Vorwahl des Netzbetreibers

  - Rest: Eindeutige Nummer innerhalb eines Mobilfunknetzwerks
  - Mehrere Telefonnummern pro Teilnehmer: 1:1 oder 1:N Beziehung zwischen IMSI und MSISDN
  - Ermöglicht tausch der Telefonnummer ohne die SIM Karte zu wechseln.
  - Das Endgerät muss die eigene Telefonnummer somit nicht kennen, da diese übermittelt werden kann.
- MNP (Mobile Number Portability): Vorwahl kann einem Provider zugeordnet werden (Z.˜B. M-Budget Vorwahl +77 als Swisscom Provider)
- Basic Services: Infos über Dienste: Telefonie, SMS, Datenverbindung, Fax, ...
- Supplementary Services: Call Forward Unconditional (CFU), Call Forward Busy (CFB), Call Forward No Reply (CFNRY), Call Forward Not Reachable (CFNR), Sperren aller abgehenden Anrufe: Barring of All Outgoing Calls (BAOC), Sperren aller ankommenden Anrufe: Barring of All Incoming Calls (BAIC), Anklopfen: Call Waiting (CW), Call Hold (HOLD), Anrufnummer anzeigen: Calling Line Identification Presentation (CLIP), Rufnummer unterdrücken: Calling Line Identification Restriction (CLIR), Unterdrückte Rufnummern unterdrücken: Connected Line Presentation Restriction (COLR), Konferenztelefone: Multiparty (MPTY)
- Kunde kann Services oft mit Codes, welche mit $*$ beginnen (de)aktivieren.

2.7.4 Authentication Center (AC)

- Geheimer Schlüssel (Ki) abgelegt, Kopie davon auf der SIM Karte
- Nicht auslesbar gespeichert
- Authentifizierung am Netzwerk mit dem Schlüssel und einem Triplet.
- Triplet:
  - RAND (128 Bit Zufallszahl)
  - 32 Bit Signed Response (SRES): Wird aus Ki und RAND mit dem Authentifizierungsalgorithmus A3 erzeugt
  - Ciphering Key (Kc) wird aush Ki und RAND erzeugt und wird für die Verschlüsselung des Datenverkehrs nach erfolgreicher Authentifizierung verwendet.
- RAND, SRES und Kc werden an MSC übergeben, welcher die Teilnehmer autzentifziert. Zur Beschleunigung können mehrere Triplets in einer Nachricht zur MSC gesendet werden, welche im VLR gespeichert werden.
- MSC sendet MS Zufallszahl in Authentication Request. Die SIM Karte macht den A3 Authentifzierungsalgorithmus und sendet eine signierte Response (SRES) zurück. Der MSC kann prüfen, ob das stimmt und authentifiziert die MS.

2.7.5 Short Message Service Center (SMSC)

- Weiterleiten und speichern von SMS
- SMS wird an MSC über den Signalisierungskanal übertragen (DTAP SS-7 Nachricht)
- MSC leitet SMS an SMSC weiter, welche den Sender eine Bestätigung liefert.
- Das SMSC fragt das HLR nach dem aktuellen Aufenthaltsort des Empfängers und nimmt Kontakt mit dem diesem auf und schickt die Nachricht. Falls OK, wird die Nachricht im SMSC gelöscht.
- Ist der Teilnehmer nicht erreichbar, wird im VLR und im HLR ein "Waiting Flag" gesetzt und die Nachricht später zugestellt.
- Schaltet der Teilnehmer sein Mobiltelefon ein, verbindet er sich mit einer neuen MSC, welche vom HLR die Info bekommt, dass eine SMS vorliegt.
- Es gibt keine Ende zu Ende Empfangsbestätigung. Einige Provider haben dazu eigene Lösungen entwickelt.

2.8 Base Station Subsystem (BSS)

2.8.1 Frequenzbereiche

- GSM 900 MHz Frequenzband
  - Uplink: 890 bis 915 MHz, Downlink: 935 bis 960 MHz
  - Bandbreite von 25 MHz mit 125 Kanälen zu jeweils 200 kHz Bandbreite)
- Da dies nicht ausreicht wurden weitere Frequenzbänder eröffnet.
- GSM for Railways (GSM-R): für Eisenbahnen
- Ein Frequenz wird jeweils als Guard verwendet und steht für den Traffic nicht zur Verfügung.
- Ein Gespräch verwendet jeweils 2 Frequenzen (Up- und Downlink)

2.8.2 Base Transceiver Station (BTS)

- Basisstationen mit Antennen
- Ersetzen kabelgebundene Verbindung durch eine Funkschnittstelle (Luftschnittstelle, Air Interface).
- Zelle: Fläche, die ein BTS abdeckt.
  - Bis zu 35 km Radius
  - Begrenzte Anzahl Nutzer pro Zelle. Deshalb kleinerer Radius = mehr Zellen = mehr Benutzer.
- Inferenzen: Frequenzen dürfen Nachbarstationen nicht überlagern, da diese gegenseitig stören.
- Sektorisierung: Unterschiedliche Frequenzen pro Gebiet.

2.8.3 GSM Luftschnittstelle

- Weg zwischen BTS und Teilnehmer heisst Luftschnittstelle, Air Interface oder Um-Interface.
- Frequency Division Multiple Access (FDMA): Gleichzeitige Nutzung mehrerer Frequenzen pro Zelle damit mehrere Teilnehmer gleichzeitig kommunizieren können.
- Time Division Multiple Access (TDMA, Zeitmultiplex: Pro Trägerfrequenz mit 200 kHz Bandbreite können bis zu 8 Teilnehmer gleichzeitig kommunizieren.
- Frames: 4.615 ms lange Frames / 8 Timeslots = 577 μs
- Kapazität berechnen: 2 Frequenzen * 8 Timeslots = 16 Timeslots. Abzüglich 2 Timeslots für Signalisierungsaufgaben = 14 Timeslots. 4 davon könnten für paketorientierten Datendienst GPRS verwendet werden.
- Eine BTS versorgt jedoch mehr Teilnehmer, da nicht alle gleichzeigit telefonieren.
- Überprovisionierung: Ein Teilnehmer telefoniert pro Stunde 1 Minute. Somit gibt es 60 mal mehr passive als aktive Teilnehmer.
- Burst: Jeder Burst eines TDMA Frames wird in mehrere Teile unterteilt
  - Aufbau: Guard Time | Tail | Data | Stealing Flag | Training Sequence | Stealing Flag | Data | Tail | Guard Time
  - Guard Time: Pause um Überlappungen zu vermeiden, da die Teilnehmer unterschiedlich weit von der BTS sein können und die Daten somit früher oder später eintreffen. Mit Timing Advance kann dies noch mehr ausgeglichen werden.
  - Training Sequence: Immer gleiche Bitsequenz damit BTS Fehler wie Reflexion, Absorption und Mehrfachausbreitung korrigieren kann.
  - Tail: Markiert Anfang und Ende der Daten.
  - Stealing Flags: Signalisierungsinformationen statt Nutzdaten falls gesetzt.
- Logischer Kanal: Die Zeitschlitze werden in logische Kanäle eingeteilt. Beispielsweise ein Nutzdatenkanal oder ein Signalisierungskanal.
- Multiframe: Zusammenfassung von 51 Frames da es wesentlich mehr logische als physikalische Kanäle (Timeslots) gibt.
- Dedicated Channel: Logischer Kanal für einen einzelnen Benutzer.

  - Traffic Channel (TCH): Nutzdatenkanal in GSM für Sprache oder Daten
  - Fast Associated Control channel (FACCH): Dringende Signalisierungsnachrichten (wie Handover) im selben Timeslot wie der TCH da eher selten.
  - Slow Associated Control Channel (SACCH): Uplink: Messergebnisse von Signalpegelmessungen der aktiven und benachbarten Zellen übermitteln. Werden für Handover Entscheidungen verwendet. Downlink: Befehle für die Leistungsregelung an Mobiltelefon.
  - Standalone Dedicated Control channel (SDCCH): Signalisierungskanal während des Gesprächsaufbaus bis THC zugeordnet wurde oder für Locateion Update oder senden und empfangen von SMS.
- Common Channel: Logischer Kanal für mehrere Benutzer.
  - Synchronization Channel (SCH): Kanal für die Netzwerk- und Zellsuche.
  - Frequency Correction Channel (FCCH): Kalibrierung von Sende- und Empfangseinheiten sowie um Anfang eines Multiframes zu finden.
  - Broadcast Common Control Channel (BCCH): Überträgt Systeminformationen an Teilnehmer (Mobile Country Code, Cell ID, Frequenzen der Nachbarzellen)
  - Paging Channel (PCH): Ruft nicht aktive Teilnehmer beispielsweise für Anrufe oder SMS. In Nachricht ist IMSI oder temporäre ID (Temporary Mobile Subscriber Identity (TIMSI)).
  - Random Access Channel (RACH): Einziger Common Channel vom Endgerät richtung Netzwerk. Das Endgerät nimmt bei einer Aktion (Telefon, SMS) über den RACH über eine Channel Request Nachricht Kontakt mit dem Netzwerk auf um ein Dedicated Channel anzufordern. Dies geschieht über ein Zufallskanal, da die Teilnehmer untereinander nicht synchronisiert sind. Somit gibt es keine Gewährleistung dass zwei Geräte gleichzeitig auf das Netzwerk zugreifen wollen. Kollidierte Nachrichten gehen verloren. Falls OK wird ein SDCCH zugeordnet.
  - Access Grant Channel (AGCH): Information welcher SDCCH oder TCH ein Teilnehmer verwenden darf.
- Temporary Mobile Subscriber Identity (TIMSI): Temporäre ID um IMSI zu verbergen. Erhöht Anonymität.
- Leere Bursts: Ermöglicht dem Endgerät während einer aktiven Verbindung Messungen vorzunehmen, welche beispielsweise für Handover venötigt werden.
- Frequency Hopping: Wechselt ständig die Frequenzen um die Übertragungsqualität zu steigern, falls eine Frequenz gestört ist. Pro BTS können maximal 64 Frequenzen hierfür verwendet werden.
- Abis Interface: E-1 Verbindung zwischen BTS und BSC.

2.8.4 Base Station Controller (BSC)

- Zuständig für Aufbau, Abbau und Aufrechterhaltung aller Verbindungen.
- Aufbau eines Signalisierungskanals (Ausgehende Verbindung)
  - Channel Request Nachricht auf RACH an BSC um ein neuer Signalisierungskanal (SDCCH) zu aktivieren.
  - Antwort mit Immediate Assignment Nachricht auf AGCH mit Nummer des SDCCH.
  - Über diesen SDCCH können jetzt DTAP Nachrichten ausgetauscht werden.
- Aufbau eines Signalisierungskanals (Eingehende Verbindung)
  - BSC empfängt Paging Nachricht der MSC mit IMSI, TMSI und Location Area des Zieltelefons. Die Zellen dieser Location Area sind dem BSC über eine Datenbank bekannt.
  - Die Nachricht wird an alle Zellen dieser Location Area weitergeleitet.
  - Nach Empfang meldet sich das Endgerät mit einer Channel Request Nachricht
- Aufbau eines Sprachkanals (Abgehend und ankommend immer gleich)
  - MSC und Endgerät verständigen sich über den SDCCH
  - MSC schickt Assignment Request an BSC
  - BSC prüft auf freien TCH in der gewünschten Zelle

  - Endgerät wird der freie TCH mitgeteilt.
  - Endgerät wechselt auf den TCH und FACCH und sendet ein SABM Frame zur BTS, welches mit einem UA Frame bestätigt wird.
  - Endgerät schickt Assignment Complete an BSC, welche die Nachricht an die MSC weiterleitet.
- Handover
  - Wechsel zu einer Zelle mit besserer Funkverbindung.
  - Wird durch BSC ausgelöst.
  - Endgerät sendet Messergebnisse zur downlink Signalqualität über SACCH an BSC.
  - BTS misst uplink Signalqualität und übermittelt dise an das BSC.
  - Das Netzwerk teilt dem Endgerät die Frequenzen der Nachbarzellen über SACCH mit, damit das Endgerät diese in den Sendepause prüfen kann. Diese werden auch dem BSC übermittelt.
  - Das BSC entscheidet zu welcher Zelle gewechselt werden soll.
  - Zuerst wird in der neuen Zelle ein TCH aktiviert.
  - Über den FACCH wird ein Handover Command gesendet (Frequenz und Nummer des Timeslots des neuen TCH).
  - Endgerät ändert Sende/Empfangsfrequenz und synchronisiert mit der neuen Zelle mit 4 aufeinander folgeneden Bursts des Timeslots eine Handover Access Nachricht.
  - Hat das BTS den Handover korrekt erkannt, geht eine Establish Indication Nachricht zum BSC und eine UA Nachricht zum Endgerät.
  - Die BSC kann dann eine Sprachverbindung in die neue Zelle schalten.
  - Die BSC muss noch den TCH in der alten Zelle abbauen un dem MSC eine Nachricht über den erfolgen Handover schicken.
- Leistungsregelung: Leistung des Endgeräts kann anhand der Messwerte angepasst werden. BSC sendet entsprechende Info einmalig an BTS. BTS sendet diese Info periodisch am Anfang jedes SACCH Frames zum Endgerät. Zuerst hat man oft eine hohe Sendeleistung, welche dann Schritt für Schritt gesenkt wird.
- Timing Advance: Bewegt sich ein Teilnehmer auf eine BTS zu oder von einer weg, ändert sich die Zeit, welche ein Burst bis zur BTS braucht und würde einen benachbarten Burst überschneiden. Ein wenig hilft die Guard Time. Doch der Sendezeitpunkt aller Teilnehmer muss trotzdem überwacht und angepasst werden.
  - Timing Advance Regelung: Es gibt 64 Schritte (0-63). Pro Schritt kann die Enfernung zur BTS um 550 Meter angepasst werden (= Maximal 35.2 km).
  - Die Channel Requests brauchen nur wenig Daten und haben deshalb längere Guard Periods. Beim eintreffen dieser Nachricht misst der BTS die Verzögerung des Bursts und schickt in der Channel Request Antwort Nachricht eine Immediate Assignment Nachricht. Darin ist neben dem SDCCH auch der erste Timing Advance Wert enthalten.
  - Während der Verbindung übermittelt die BTS ständig neue Timing Advance Werte über den SACCH an das Endgerät.
- Erweiterter Zellradius: Der Zellradius kann bis zu 120 km ausgedehnt werden, beispielsweise für Küstenkommunikation. Dann kann nur jede zweite Timeslot verwendet werden. Dies erfordert spezielle Telefone mit einer Leistung bis 8 Watt.

2.8.5 Transcoding and Rate Adaption Unit (TRAU) für Sprachübertragung

- Bandbreite eines TCH: Verwendung aller Bursts eines 26 Multiframe (mit Ausnahme für den SACC und den Burst für die Pegelmessung der Nachbarzellen). Nutzdaten von 114 Bit pro Burst welcher alle 4.615 ms übertragen wird = 22.8 kbit/s. Wegen Fehlererkennung/Fehlerkorrektur sind nur etwa 13 kbit/s nutzbar.
- TRAU: Komprimierung und Dekomprimierung der Sprachdaten zwischen MSC und BSC.
- MSC schickt die Sprachdaten mit 64 kbit/s PCM Format ins Radionetzwerk. In der TRAU wird das Signal auf 13 kbit/s komprimiert und zur BSC geschickt. Dort wird es dekomprimiert und an das MSC weitergeschickt. Das Endgerät komprimiert und dekomprimiert die Daten ebenfalls.

Weiter nicht beschrieben, da nicht im Unterricht behandelt???

2.9 Mobility Management and Call Controll

2.9.1 Location Area und Location Area Update

- Location Area: Gebiet, welches mehrere benachbarte Zellen umfasst. In der Praxis sind dies etwa 20 Zellen pro Location Area.
- Über den BCCH informiert das Netz die Teilnehmer über die Location Area (Cell ID und Location Area ID).
- Wechselt ein Endgerät auf eine Zelle in einer neuen Location Area, muss dies dem Netzwerk mitgeteilt werden.
- Bei einem ankommenden Anruf/SMS muss das Netzerk den Teilnehmer einer Location Area in allen Zellen suchen.
- Das Endgerät schickt ein Location Update Request. Das Gerät muss hierzu authentifiziert sein und eine Verschlüsselung aktivieren.
- TMSI (Temporäre IMSI): Nachdem die Verschlüsselung aktiv ist, wird dem Endgerät eine TMSI zugewiesen, um die Identität des Teilnehmers zu schützen.
- Ist der Wechsel erfolgreich, wird dem Endgerät die Location Area Update Nachricht bestätigt und die Verbindung beendet.
- MSC Location Update: Wird die neue Location Area von einem anderen MSC/VLR verwaltet, muss das neue MSC/VLR das HLR über den Wechsel des Teilnehmers informieren.

2.9.2 Mobile Terminated Call

- Mobile Terminated Call: Anruf, der bei einem mobilen Terilnehmer eingeht.
- Der Aufenthaltsort des Zieltelefons muss zuerst im HLR ermittelt werden.
- G-MSC (Gateway MSC): MSC des Anrufers.
- V-MSC (Visited MSC): MSC der Zielnummer.
- SRI (Send Routing Information): G-MSC schickt ISUP über IAM Nachricht die Telefonnummer (MSISDN) der Zielnummer. Über eine SRI Nachricht an das HLR wird das V-MSC der Zielnummer bestummen.
- MSRN (Mobile Station Roaming Number): Das HLR ermittelt V-MSC und deren VLR. Eine Provide Roaming Number Nachricht wird an das V-MSC/VLR geschickt um die Zielnummer diese zu Informieren. Die IMSI wird einer temporären MSRN zugeordnet, welche dem HLR zurückgegeben wird. Das HLR gibt die MSRN an die G-MSC zurück.

2.10 Mobile Station

3 GPRS und EDGE

3.1 Leitungsvermittelnde Datenübertragung

- GSM für Sprachen optimiert.
- GPRS erweitert den GSM Standard um die Datenübertragung.

4 Mobile Positioning System (MPS)

4.1 Geschichte

- Legal Interception: Verfolgung durch Polizei

- Disaster and Emergency Management: Suche nach Vermissten und Hilfesuchenden
- Next Generation 911 (NG911): Suchradius < 10m in 95% der Suchfälle
- Problem: Unterscheidung Nah- und Fernbereich sowie in Städten mit Häusern wegen Abdeckungen und Reflexionen

4.2 Verfahren

- Modifiziertes User Equipment
  - UE unterstätzes Time Difference of Arrival (TDoA)
  - UE unterstätzes Time of Arrival (ToA)
  - GPS basiert
- Nicht modifiziertes UE
  - Angle of Arival (AoA)
  - Time Difference of Arrival (TDoA)
  - Time of Arrival (ToA)
  - Kombination aus AoA/ToA oder AoA/TDoA

4.3 ToA/TDoA

- Basiert auf einer zeitsynchronisierten (GPS) Location Measurement Units (LMUs) der Base Station.
- LMU wertet UpLink Call eines Subscribers aus
- Auf 50m genau, benötigt aber freie sicht zu min. 3 BS
- Messfehler: Wahrscheinlichster Ort berechnen und Vertrauensintervall angeben

4.4 Weiterentwicklung

- Kombination aus GSM + WiFi
- Fehler optimieren
- Phasenanalyse des Trägers, Problem bei langsamem UE
- Auswertung der Netzerkeigenschaften: Messreports, Cell ID, Signal Fingerprint. Hier muss der Provider jedoch Daten im Voraus sammeln.

5 General Packet Radio Service (GPRS)

6 Universal Mobile Telecommunication System (UMTS, 3G)

7 Long Term Evolution (LTE)

8 Evolved Packet System (EPS)

- EPC: Evolved Packet Core

9 WiMAX

10 Polycom

11 Bluetooth