UMTS

- … 3. Generation der Mobilfunknetze
  - GSM gehört zur 2. Generation
- Ziel: Weiterentwicklung von GSM
  - Höhere Datenraten
  - Erweitertes Dienstekonzept
  - Globales Roaming
    - Auch zwischen verschiedenen Betreibern
    - Handover zwischen GSM und UMTS (später auch WLAN)
  - Handhabbare kleine Endgeräte für den Benutzer
- Anforderungen hinsichtlich der Datenrate
  - mindestens 144 kbit/s im ländlichen Raum (Ziel: 384 kbit/s)
  - mindestens 384 kbit/s in den Vorstädten (Ziel: 512 kbit/s)
  - bis zu 2 Mbit/s für geringe Distanzen im Innern eines geschlossenen Gebäudes
- … hohe Anforderungen an Luftschnittstelle
  - UTRAN (UMTS Terrestrial Radio Access Network)
    - Neues drahtloses Zugangsnetz

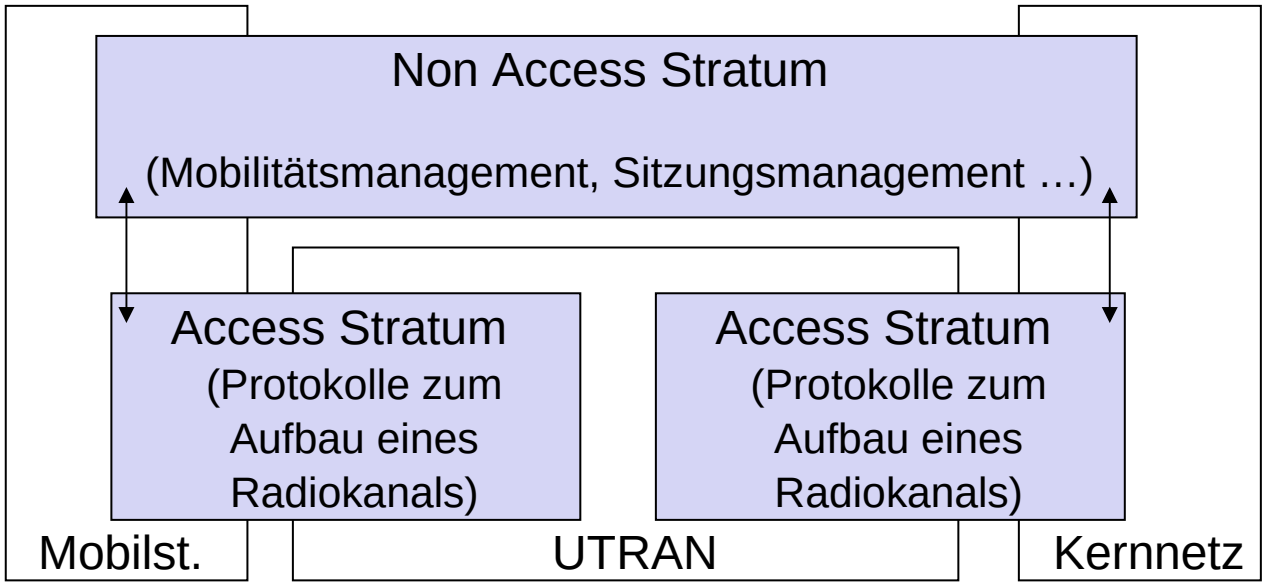
[II.4]

Von GSM zu UMTS

- Radio Access Bearer (Bearer: Träger)
  - Für die Übertragung von Nutz- und Signalisierdaten erforderlicher Übertragungskanal
    - Von MSC oder SGSN initiiert
    - Keine genauen Angaben über Beschaffenheit, nur Eigenschaften
      - Z.B. Dienstklasse, maximale Datenrate
      - UTRAN ist dann für Bereitstellung verantwortlich, z.B.
        - Auswahl des Kodierungsverfahrens
        - Auswahl logischer und physikalischer Kanäle
        - Auswahl der Protokolle (z.B. Fehlerbehebung)
  - Gegliedert in
    - Radio Bearer auf der Luftschnittstelle
    - I_u Bearer im UTRAN

… was ist anders?

- Trennung Access Stratum (AS) und Non Access Stratum (NAS)
  - Access Stratum: Zugangsebene
    - Funktionalitäten des Funknetzes und Kontrolle aktiver Verbindungen
      - Z.B. Handoverkontrolle
  - Non Access Stratum
    - Protokolle, die direkt zwischen Mobilstation und Kernnetz abgewickelt werden
      - Z.B. Mobilitätsmanagement
  - Ermöglicht Weiterentwicklung der Luftschnittstelle ohne erhebliche Auswirkungen auf Kernnetzwerk



… was ist anders?

- Einheitliches Protokoll auf der Luftschnittstelle
  - RLC/MAC
    - Radio Link Control / MAC Protokoll
      - Ähnlich zum RLC/MAC Protokoll bei GPRS
- Weiteres
  - CDMA auf Luftschnittselle
    - Zellatmung
      - Größe einer Zelle passt sich automatisch an
  - Erweiterte Mobilitätsunterstützung
    - Makrodiversität
    - Soft-Handover
  - Geografische Zone
    - Verbreitung von Information im Netz nach rein geografischen Gesichtspunkten
      - UTRAN bestimmt Zellen, an die die Information gesendet wird
      - Bei GSM händische Konfiguration erforderlich, z.B. falls neue Zelle hinzukommt

… wer bekommt welche Frequenzen?

STAND DER LIZENZVERGABE

Versteigerung UMTS/IMT-2000-Lizenzen

Runde 173 Datum 17.08.00 Uhrzeit 15:51:26

Höchstgebote für Frequenzblöcke (mind. 2 Blöcke erforderlich für Lizenz)

Bieter	Anzahl der Frequenzblöcke 1	2	3	Lizenzgebot (TDM)	(€ in Tsd)
E-Plus Hutchison	2 x 5 MHz	2 x 5 MHz		16.418.200	8.394.492
Group 3G	2 x 5 MHz	2 x 5 MHz		16.446.000	8.408.706
Mannesmann Mobilfunk	2 x 5 MHz	2 x 5 MHz		16.473.800	8.422.920
MobilCom Multimedia	2 x 5 MHz	2 x 5 MHz		16.370.000	8.369.848
T-Mobil	2 x 5 MHz	2 x 5 MHz		16.582.200	8.478.344
VIAG Interkom	2 x 5 MHz	2 x 5 MHz		16.517.000	8.445.008
debitel Multimedia	ausgeschieden				
Lizenzsumme				98.807.200	50.519.319

RUNDENERGEBNIS

Versteigerung UMTS/IMT-2000-Frequenzen

Runde: 9

Lfd. Nr.	Umfang	Höchstbieter	Höchstgebot (TDM)	Höchstgebot* (€ in Tsd)
13	1 x 5 MHz konkret	E-Plus Hutchison	73.600	37.631
14	1 x 5 MHz	MobilCom Multimedia	121.000	61.866
15	1 x 5 MHz	T-Mobil	122.700	62.736
16	1 x 5 MHz	Mannesmann Mobilfunk	121.000	61.866
17	1 x 5 MHz	Group 3G	122.700	62.736
		Summe Höchstgebote	561.000	286.835

* Eurowerte gerundet

VIAG Interkom ausgeschieden

UTRA-FDD

- Uplink 1920-1980 MHz
- Downlink 2110-2170 MHz
- Duplexabstand 190 MHz
- 12 Kanäle zu je 5 MHz

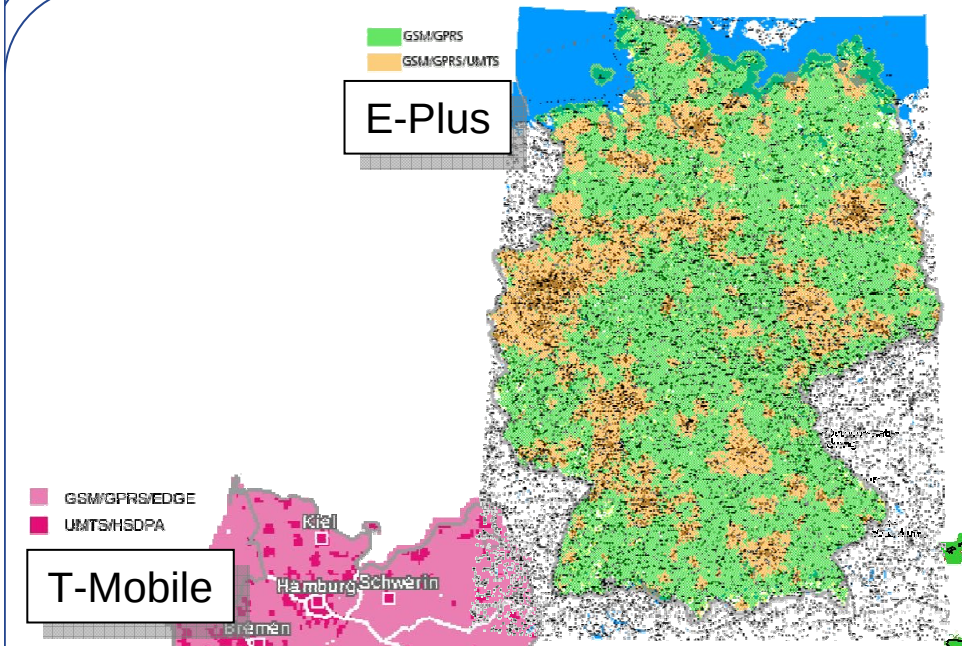
UTRA-TDD

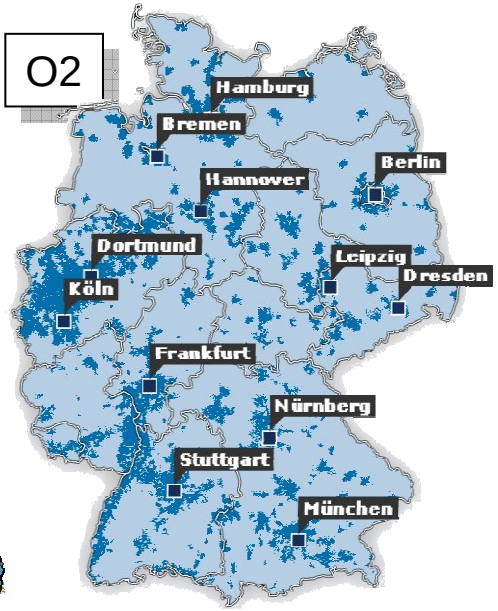
- 1900-1920 MHz,
- 2010-2025 MHz;
- je 5 MHz Kanäle

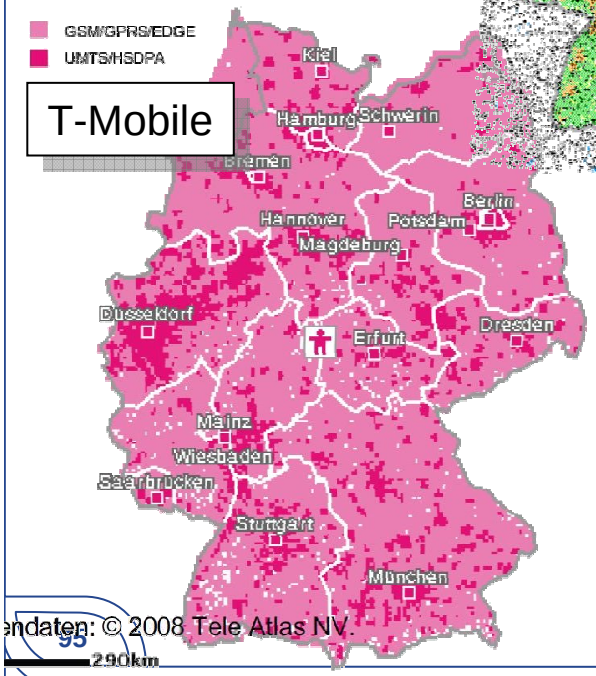
Abdeckung: 25% in der Bevölkerung bis 12/2003, 50% bis 12/2005

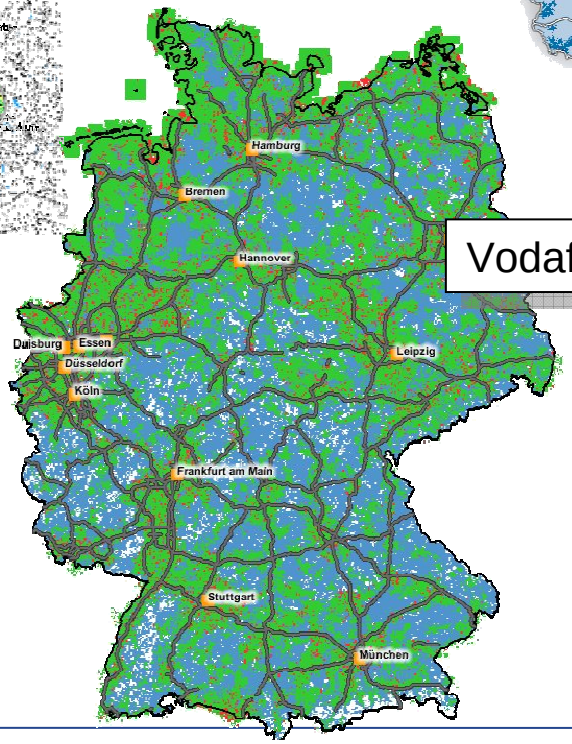
Summe: **99,3682 Mrd. DM**

Flächendeckung von 3G (Deutschland)







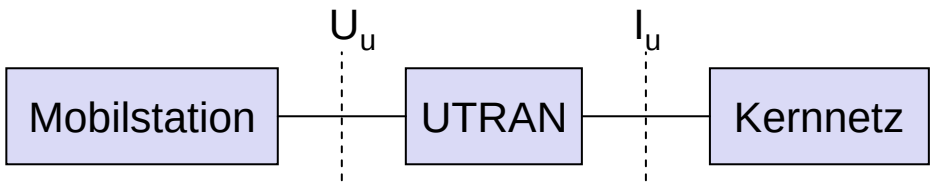


Stand: Mai 2010
nach Angaben der
Betreiber

endaten: © 2008 Tele Atlas NV.

3.2 UMTS Architektur

- Mobilstationen (User Equipment - UE)
  - Entspricht den Mobilstationen in GSM
- UTRAN (UMTS Terrestrial Radio Access Network)
  - Entspricht dem Funkteilsystem in GSM
  - Kapselung der funkspezifischen Abläufe
    - Wichtiger Unterschied zu GSM
  - Mobilität auf Zellenebene
- Kernnetz (Core Network - CN)
  - Handover zwischen Systemen
  - Lokationsmanagement falls keine dedizierte Verbindung zwischen Mobilstation und UTRAN besteht
  - Verbindung verschiedener Netze (GSM, ISDN, Internet …)

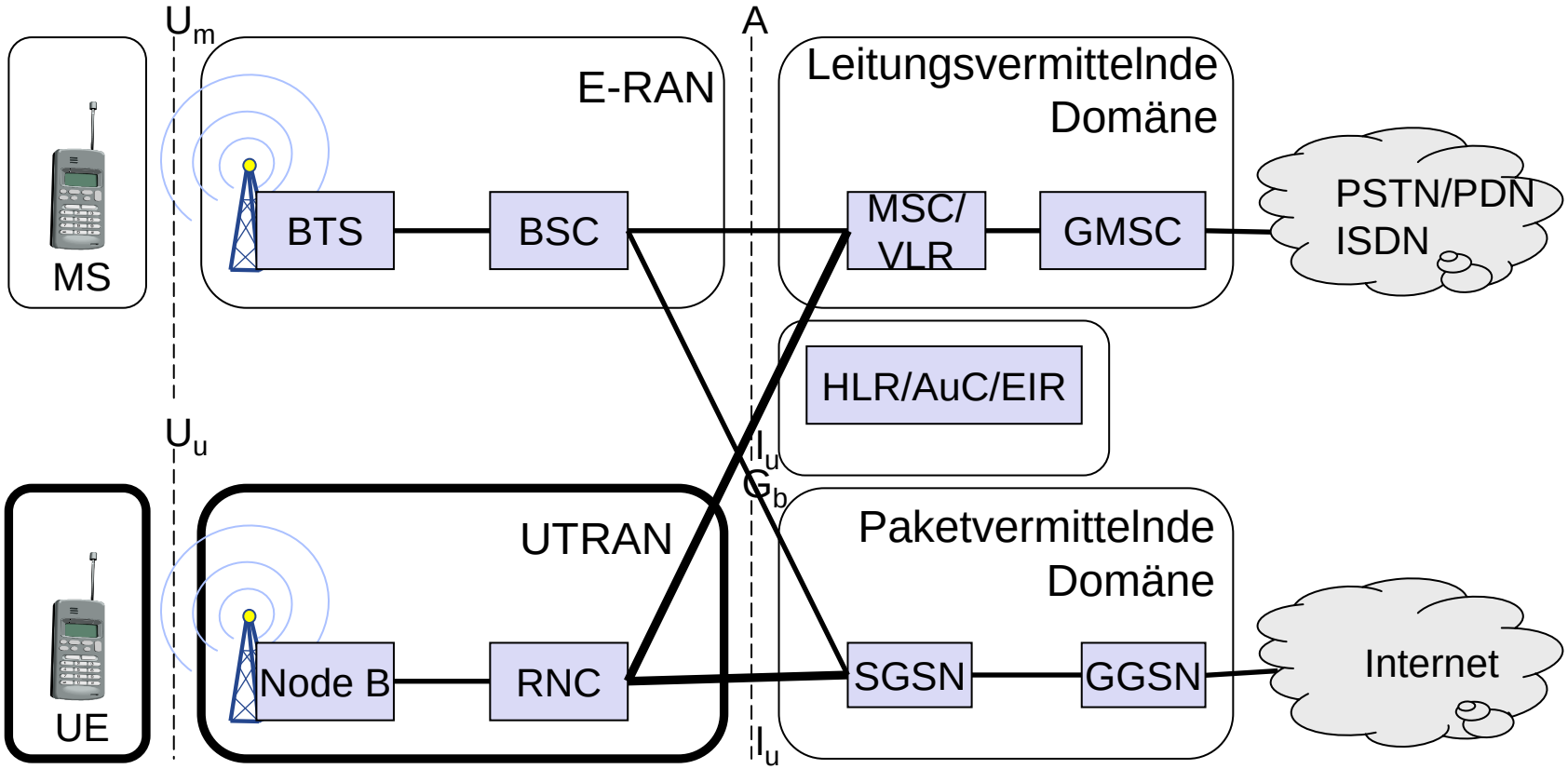


… verschiedene Phasen der Einführung

- Einführung von UMTS in verschiedenen Phasen, z.B.
  - Release 99
    - Weiternutzung von GSM-Infrastruktur im Kernnetz
      - GPRS und EDGE
      - Zwei „getrennte“ Infrastrukturen für Leitungsvermittlung und Paketvermittlung
    - UTRAN kommt hinzu
    - Heute im Einsatz
  - Release 6
    - „All-IP“
      - Ein Paketvermitteltes Kernnetz
      - IMS: IP-based Multimedia Subsystem
    - GERAN (GSM/EDGE RAN)
- … mehr Informationen in [II.12, 2.1]
  - … Release zunächst durch Jahreszahl identifiziert (99), dann durch laufende Nummer (4, 5, 6)

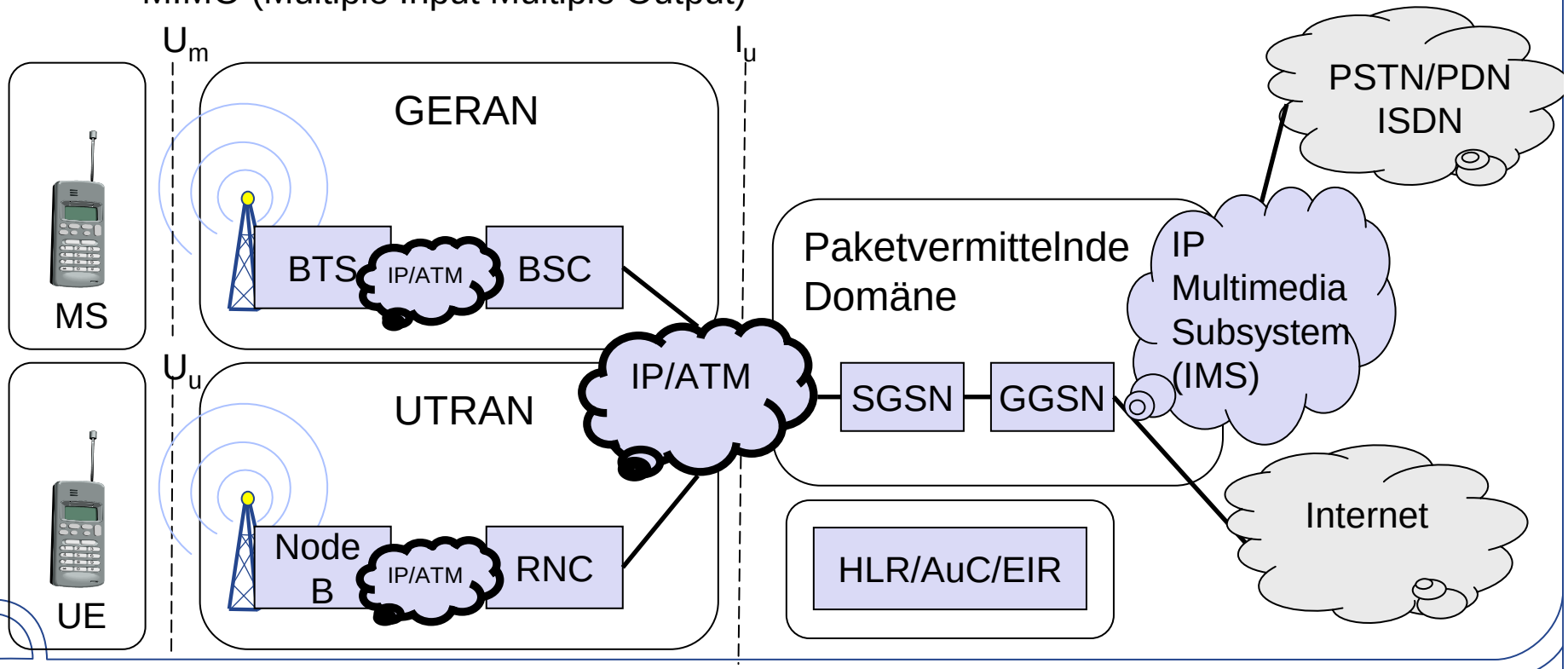
Release 99

- Neues Zugangsnetz (UTRAN – UMTS Terrestrial Radio Network)
  - W-CDMA (Wideband CDMA)
    - Kein Zeit- und Frequenzmultiplex
    - Individuelle Codes pro Benutzer



Release 6

- … über Release 4 und 5 hin zu einem „All-IP Netzwerk“
  - IP-basierte Übertragung (Ende-zu-Ende)
  - Netzwerk-kontrollierte Handover
- Erneuerungen an der Funkschnittstelle
  - HSDPA (High-speed Downlink Packet Access)
  - MIMO (Multiple Input Multiple Output)

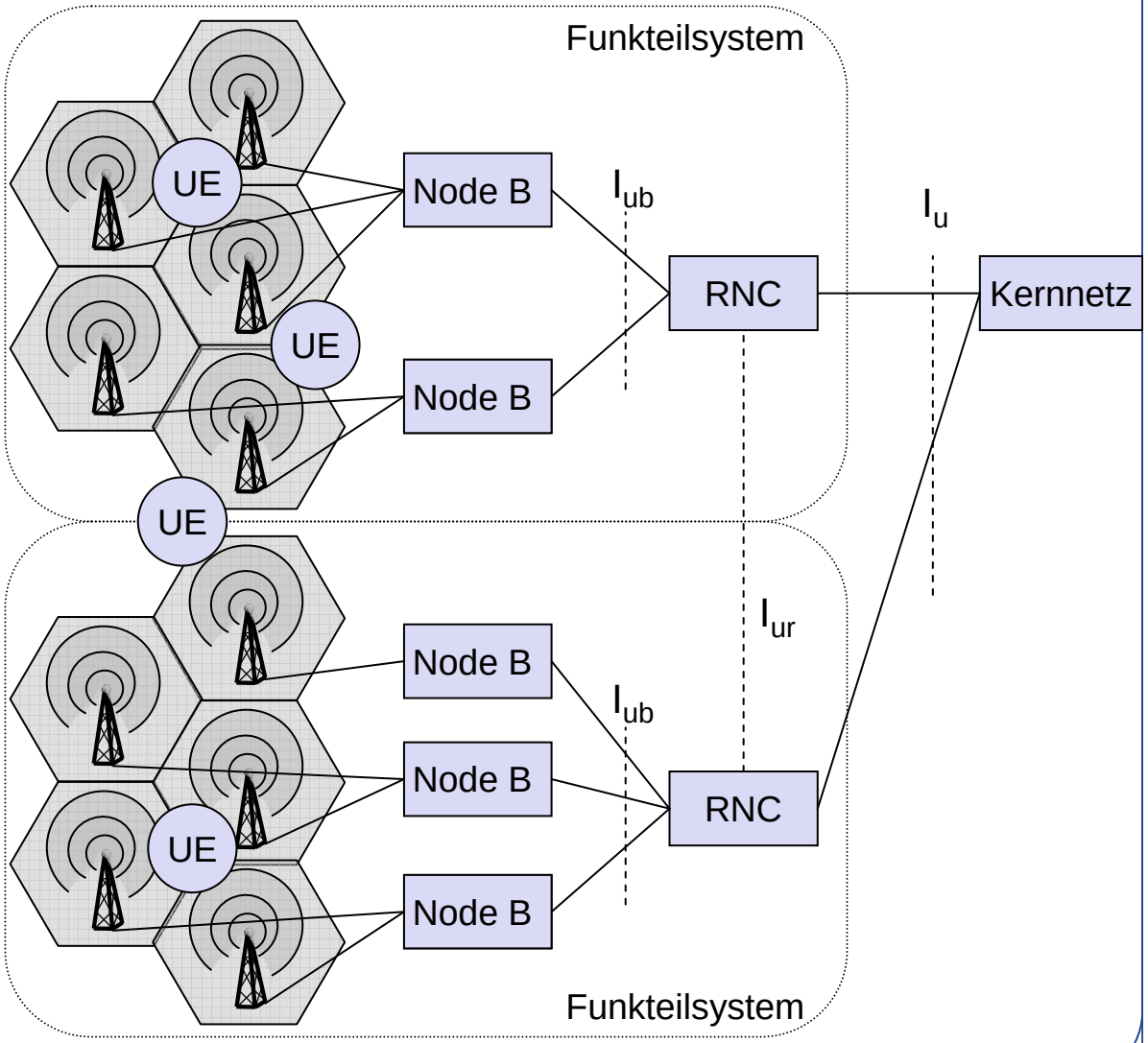


3.3 UTRAN

- Neues Zugangsnetz für UMTS
  - Komponenten
    - RNC (Radio Network Controller)
      - Entspricht Feststationssteuerung (BSC) von GSM
      - Funktionsweise unterscheidet sich stark von BSC
        - Relocation, Makrodiversität …
      - Verantwortlich für Handover-Entscheidungen
    - Node B
      - Entspricht Basisstation (BTS) von GSM
      - Sicherstellung der Sende- und Empfangsfunktion
      - Kann eine oder mehrere Zellen umfassen
  - Einführung einer neuen Schnittstelle
    - I_{ur}-Schnittstelle zwischen RNCs

UTRAN Architektur

- Funkteilsystem
  - Radio Network Subsystem - RNS
  - UTRAN besteht aus mehreren Funkteilsystemen
- Node B
  - kann FDD, TDD oder beides unterstützen
- Zelle
  - bietet FDD oder TDD



SRNC und DRNC

- Aktive Mobilstation
  - Logische Verbindung zwischen Mobilstation und einem RNC wird hergestellt
    - Serving RNC (SRNC)
  - Verbindung bleibt auch bei Mobilität erhalten
- Problem
  - Mobilstation kann sich bewegen und Zuständigkeitsbereich des SRNC verlassen
  - Drift-RNC (DRNC)
    - RNC, der für eine entfernte Zelle zuständig ist
      - Physikalische Verbindung zum DRNC
    - Daten werden über SRNC und DRNC an Mobilstation weitergeleitet
      - DRNC nimmt die Rolle eines Routers ein
      - Logische Verbindung zum SRNC bleibt erhalten
        - SNRC kann verlagert werden

Funktionen des UTRAN

- Zugangskontrolle (Admission Control)
  - Zur Vermeidung von Überlastsituationen
    - Zugangskontrolle für neue Verbindungen
    - Neukonfiguration bestehender Verbindungen
    - Belegung von Ressourcen für Makrodiversität und Handover
  - Im SNRS angesiedelt
- Staukontrolle
  - Bei Entstehung von Überlast Überführung des Systems in stabilen Zustand
- System Information Broadcasting
  - Verteilen von für den Betrieb erforderlicher Information an Mobilstation
- Verschlüsselung
  - Findet auf der Luftschnittstelle statt
  - Sowohl in der Mobilstation als auch im UTRAN angesiedelt

Funktionen des UTRAN

- Handover
  - Mobilitätsverwaltung an der Luftschnittstelle
  - Verbindungsweiterleitung an andere Netze möglich (z.B. GSM)
  - Einhaltung einer vom Kernnetz geforderten Dienstgüte
  - Sowohl in der Mobilstation als auch im SRNS angesiedelt
- SRNC-Verlagerung
  - Die Rolle von SNRC und DRNC kann sich im Verlauf einer Verbindung ändern
  - Wird vom SRNC initiiert
- Konfiguration des Funknetzes
- Funkkanalmessungen
  - Überwachung einer Reihe von Parametern an der Luftschnittstelle
    - Z.B. Empfangspegel, Bitfehlerwahrscheinlichkeit, Dopplerverschiebung, aktueller Grad der Synchronisation
  - Sowohl in der Mobilstation als auch im UTRAN angesiedelt

Funktionen des UTRAN

- Makrodiversität
  - Datenströme können über mehrere verschiedene Wege zur Mobilstation gesendet werden
  - Daten von einer Mobilstation können an mehreren Basisstationen empfangen und wieder zusammengeführt werden
    - Im SRNC, DRNC oder Node B möglich
  - Wird nur im FDD-Modus verwendet
  - Im UTRAN angesiedelt
- Funkträgersteuerung
  - Bereitstellung bzw. Auflösung von Funkträgerdiensten für den Auf- und Abbau einer Verbindung sowie bei Handovern
- Funkbetriebsmittelverwaltung
  - Vergabe und Freigabe von Funkressourcen
  - Im RNC angesiedelt

Funktionen des UTRAN

- Datenübertragung auf der Luftschnittstelle
  - Multiplexen von Trägerdiensten und Mobilstationen
  - Segmentieren und Reassemblieren von Nachrichten
  - Bestätigte bzw. unbestätigte Übertragung
- Leistungssteuerung (FDD- und TDD-Modus)
  - Steuerung der Sendeleistung
    - Reduktion von Interferenzen
    - Aufrechterhaltung der Verbindungsqualität
  - Basisstationen nutzen Messwerte der Mobilstationen
  - Basisstationen senden Zell- und Systemparameter
- Kanalkodierung
  - Systematisches Hinzufügen von Redundanz
  - Kann für verschiedene logische Kanäle und für verschiedene Trägerdienste unterschiedlich sein
- Zufallszugriff
  - Slotted-Aloha Protokoll
  - Kollisionsauflösung erforderlich

3.4 Luftschnittstelle (U_U)

- Bestandteile der MAC-Schicht (von oben nach unten)
  - Broadcast/Multicast Control (BMC)
  - Packet Data Convergence Protocol (PDCP)
  - Radio Link Control (RLC)
  - Medium Access Control (MAC)

- Physikalische Schicht
  - Mehrfachzugriff
    - CDMA
  - Duplexverfahren
    - Frequenzduplex (FDD)
      - Mehrfachzugriff durch Kombination aus FDMA und CDMA
    - Zeitduplex (TDD)
      - Mehrfachzugriff durch Kombination aus TDMA und CDMA

FDD versus TDD

- Asymmetrischer Verkehr
  - Bei FDD erhalten i.d.R. beide Kommunikationsrichtungen einen gleichen Anteil des Frequenzspektrums zugeteilt
  - Bei TDD bevorzugte Behandlung durch Zuteilung nicht symmetrischer Ressourcen möglich
    - Genaue Synchronisation erforderlich

- FDD stand bei Entwicklung von UMTS im Vordergrund
  - TDD im folgenden nicht weiter betrachtet

CDMA

- Bandbreite je Trägerfrequenz: 5 MHz
- Übertragungsgeschwindigkeit
  - 3,84 Mchip/s
    - Unabhängig vom Spreizfaktor (= Chiprate / Bitrate)
    - Mit Spreizfaktor variiert die Datenrate
    - Orthogonal Variable Spreading Factors - OVSF
  - Großer Spreizfaktor
    - Datenrate pro Benutzer sinkt
    - Größere Robustheit
    - Größere Anzahl an Codes und damit an Benutzern
      - Bei Spreizfaktor von 8, 383 kbit/s im Downlink für 8 Benutzer
    - Reduktion des Signal-Rausch-Abstands
      - Da mehr Chips pro Bit
      - Zieht Reduktion der Sendeleistung nach sich

Near-Far Effekt

- Folge von CDMA
  - Alle Mobilstationen nutzen im Uplink zum gleichen Zeitpunkt die gleiche Frequenz
    - Unterscheidung nur durch den Code möglich
  - Weiter entfernte Mobilstationen müssen mit größerer Sendeleistung senden → Near-Far Effekt
    - Die am nächsten zur Basistation lokalisierte Mobilstation kann die anderen Mobilstationen übertönen
    - Einzelne Mobilstation kann gesamte Zelle blockieren
- Problem
  - Die an der Basisstation ankommende Leistungsstärke der Signale unterschiedlicher Mobilstationen muss identisch sein
    - Kein Übertönen durch einzelne Mobilstationen

Leistungsregelung

- Ziel
  - Gleiche Empfangsleistung an der Basisstation für alle Mobilstationen
- Leistungkontrolle
  - Anpassung der Sendeleistung der Mobilstationen 1500 mal pro Sekunde
    - In GSM nur ein oder zwei mal pro Sekunde
  - Anpassung der Leistungsstärke pro Bit bei allen Mobilstationen
    - Minimierung der Interferenz innerhalb einer Zelle
  - Berücksichtigung der angeforderten Dienstgüte

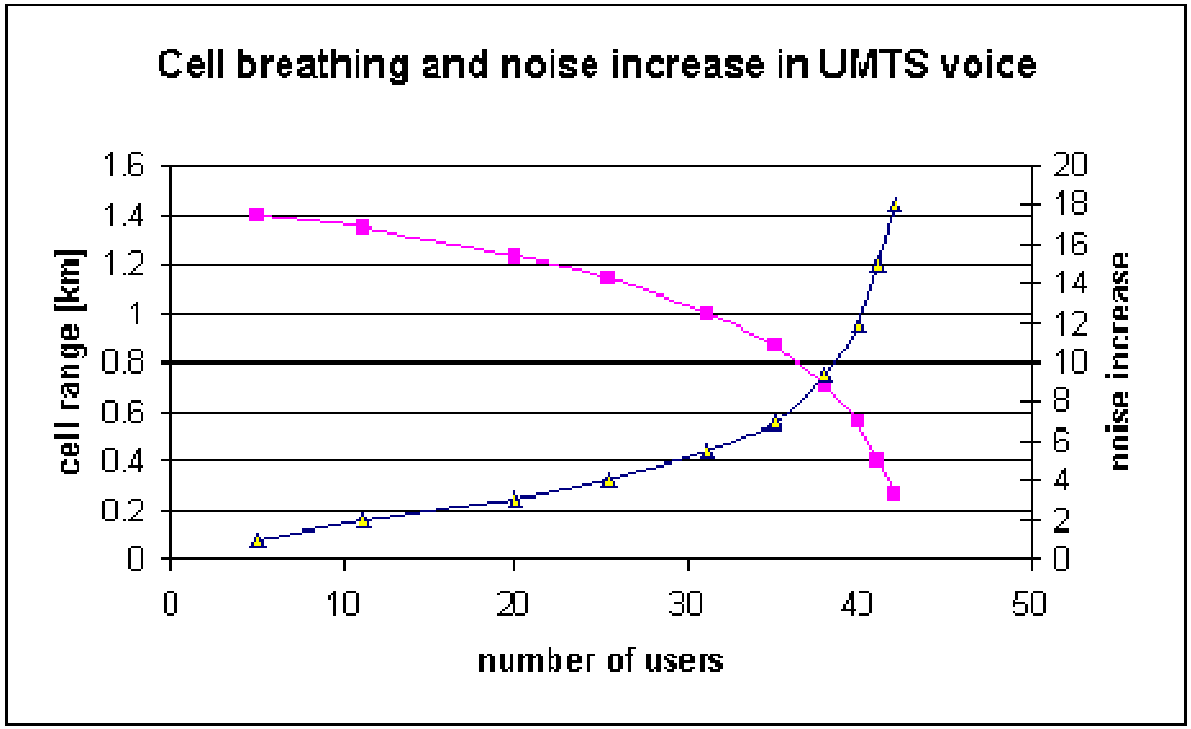
Zellatmung

- GSM
  - Mobilstation erhält volle Leistung der Basisstation
  - Anzahl eingebuchter Mobilstationen hat keinen Einfluss auf die Zellengröße
- UMTS
  - Zellengröße ist eng korreliert mit der Kapazität der Zelle
  - Kapazität ist bestimmt durch den Signal-Rausch-Abstand
  - Rauschen entsteht durch vorhandene Interferenz
    - anderer Zellen
    - anderer Teilnehmer
  - Interferenz erhöht das Rauschen
  - Mobilstationen an der Zellengrenze können das Signal (aufgrund der Sendeleistungsbeschränkung, 2 Watt) nicht weiter verstärken ⇨ keine Kommunikation möglich
  - Beschränkung der Teilnehmeranzahl notwendig

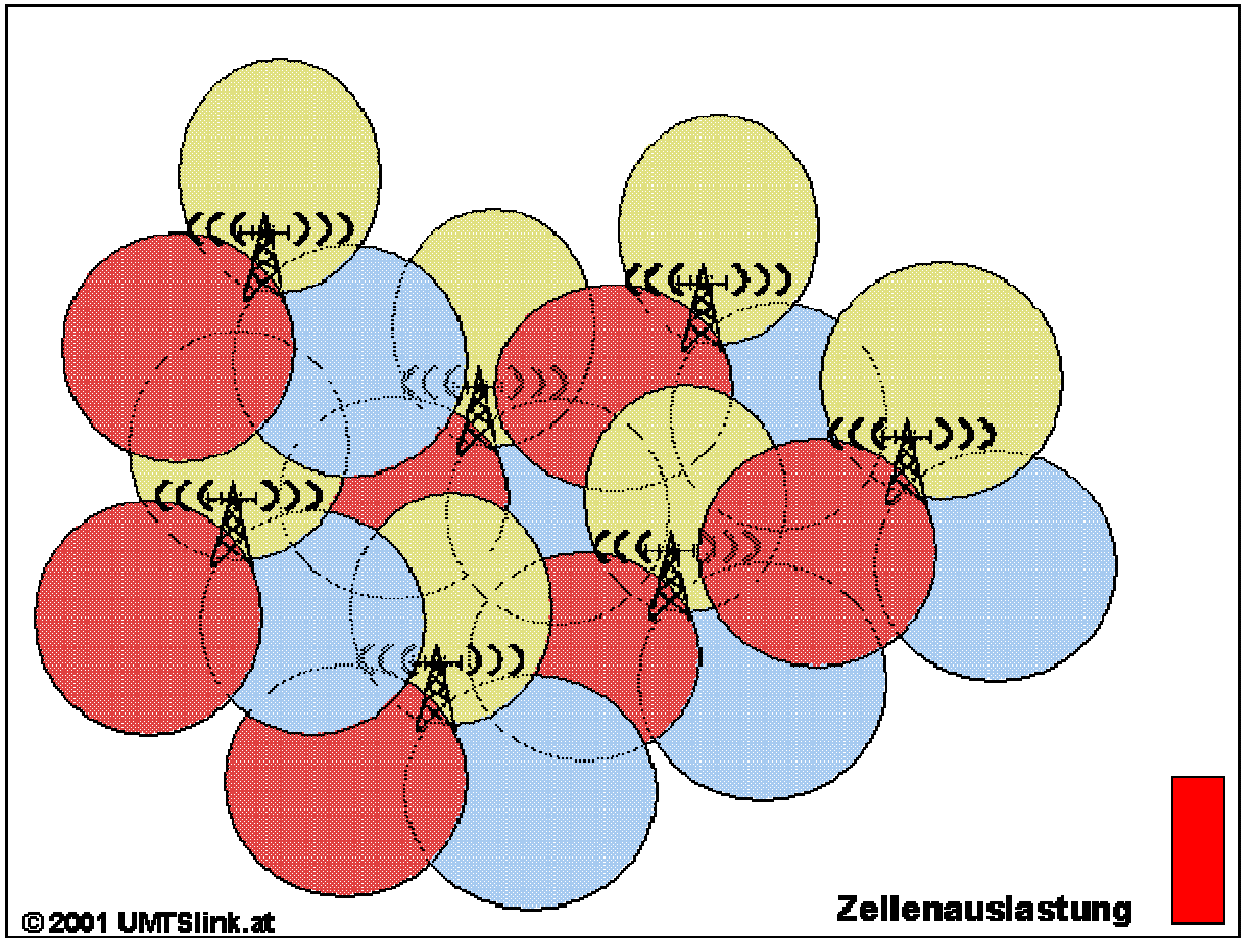
Zellatmung

- Beispiel
  - Der am weitesten entfernte Teilnehmer sendet mit maximaler Sendeleistung
  - Neuer Teilnehmer möchte hinzukommen
    - Durch neue Verbindung erhöht sich für alle die Interferenz
    - Sendeleistung muss erhöht werden
    - Teilnehmer kann Sendeleistung nicht erhöhen
      - Kann von der Basisstation nicht mehr empfangen werden, Kommunikationsverbindung bricht ab
  - <u>Maximale geografische Versorgungsfläche der Zelle ändert sich</u>
    - Als Zellatmung bezeichnet
    - Zellatmung erschwert die Netzwerkplanung erheblich
- Netz kontrolliert Sendeleistung und kann neuen Teilnehmer abweisen
  - Kann Interferenzniveau durch Wahl anderer Codes beeinflussen

Zellatmung: Beispiel



Zellatmung: Beispiel



[II.13]

Vorteile der Luftschnittstelle U_U

- Kürzere Verzögerungszeiten
  - Keine ständige Neuzuweisung von Ressourcen wie bei GPRS
  - Ständiger Kanal durch Code
- Keine Unterbrechungen bei Zellwechseln
  - Handover wird vom Netzwerk kontrolliert
    - Soft-Handover (s. unten)
  - Bei GPRS von der Mobilstation kontrolliert
    - 1-3 Sekunden Unterbrechungszeit
- Größere Bandbreite
  - Datenrate von 384 kbit/s im Downlink möglich (Spreizfaktor 8)
  - Bei GSM durch 200 kHz Bandbreite einer Trägerfrequenz stark begrenzt
- Flexible Codeänderung

Kanalstruktur auf der Luftschnittstelle

- Logische Kanäle
  - Welcher Typ von Information wird übertragen?
- Transportkanäle
  - Zuordnung zwischen logischen und physikalischen Kanälen
- Physikalische Kanäle
  - Übertragungsmedium

Kanalstruktur auf der Luftschnittstelle

- Strukturierung in der physikalischen Schicht
  - Übertragung so genannter Transportblöcke
- Zwei Arten von Transportkanälen
  - Dedizierte Transportkanäle
    - Können über einen physikalischen Kanal eindeutig einer Mobilstation zugeordnet werden
    - Dedizierter Kanal (Dedicated Channel – DCH)
      - Bidirektionaler Kanal; exklusiv einer Mobilstation zugeordnet
      - Datenrate kann alle 10 ms geändert werden
    - Schneller Uplink Kanal (Fast Uplink Signalling Channel – FAUSCH)
      - Benutzt Mobilstation, um mitzuteilen, dass sie einen neuen dedizierten Kanal benötigt
      - Existiert nur im Uplink und nur bei FDD
    - ODMA dedizierter Kanal (ODMA Dedicated Channel – ODCH)
      - ODMA: Opportunity Driven Multiple Access
      - Im TDD-Modus kann Mobilstation als Relay dienen
      - ODCH wird dann zum Transport von Daten genutzt
      - Bidirektionaler Kanal
      - Datenrate kann alle 10 ms angepasst werden

Transportkanäle

- Gemeinsame Transportkanäle
  - Adressierung zur Unterscheidung der Mobilstationen erforderlich
  - Random Access Channel (RACH)
    - Alle Mobilstationen konkurrieren um diesen Kanal
    - Zufallszugriff
    - Übermittlung nicht-zeitkritischer Steuer- und Nutzdaten
  - ODMA Random Access Channel (ORACH)
    - Zufallszugriff im Relay-Betrieb
  - Broadcast Channel (BCH)
    - Rundsenden von Systeminformation in einer Zelle
    - Existiert nur im Downlink; hat feste Datenrate
  - …

Physikalische Kanäle im FDD-Modus

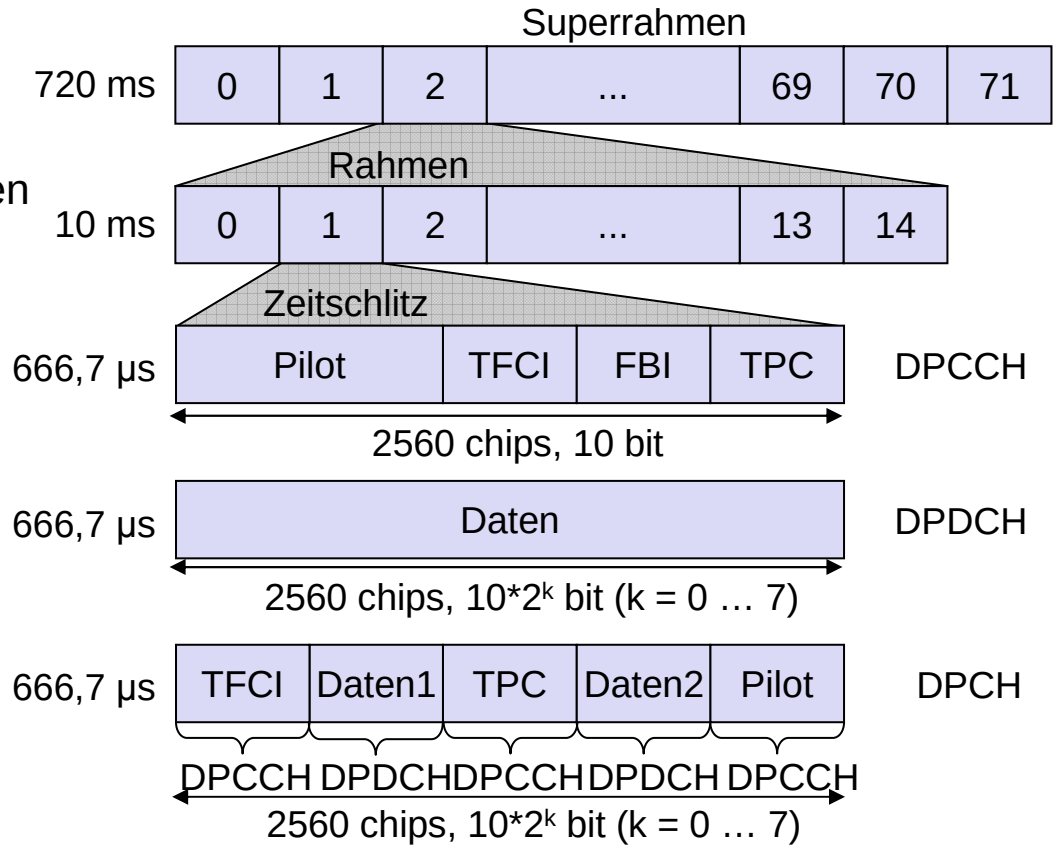
- Kanal charakterisiert durch
  - Mittenfrequenz und Spreizcode
- Dedizierte physikalische Kanäle
  - Uplink Dedicated Physical Data Channel (DPDCH)
    - Übertragung von Nutzdaten, Mobilitätsmanagement etc.
    - Schicht-1-Verbindung besitzt mehrere oder keinen DPDCH
    - Existiert nur auf dem Uplink
  - Dedicated Physical Control Channel (DPCCH)
    - Steuerung der Datenübertragung
      - Übertragung von Information der physikalischen Schicht
    - Existiert nur auf dem Uplink
    - Jede Schicht-1-Verbindung besitzt genau einen DPCCH
  - Dedicated Physical Channel (DPCH)
    - Erfüllt Aufgaben von DPDCH und DPCCH auf dem Downlink
    - Existiert nur auf dem Downlink

Physikalische Kanäle im FDD-Modus

- Gemeinsame physikalische Kanäle
  - Synchronization Channel (SCH)
    - Zellsuche und Synchronisation der Mobilstationen
    - Existiert nur im Downlink
  - Common Control Physical Channel (CCPCH)
    - Verteildienste im Downlink
  - Common Pilot Channel (CPICH)
    - Unterstützung der Makrodiversität
    - Verteilung der gleichen vordefinierten Codesequenz in verschiedenen Zellen
  - Physical Random Access Channel (PRACH)
    - Trägt den RACH
    - Zufallszugriff, Übertragung kleiner Datenmengen
  - …

Rahmenstruktur bei FDD

- Abbildung der physikalischen Kanäle auf einheitliche Rahmenstruktur
  - Burstaufbau für die dedizierten Kanäle
  - Je 15 Bursts formen 10ms langen Rahmen
  - 72 Rahmen bilden einen Superrahmen
- Informationen in den Bursts
  - Pilot
    - Bekannte Bitfolge
    - Liefert Bewertung des Kanals
  - TPC (Transmit Power Control)
    - Regeln der Sendestärke
  - TFCI (Transport Format Combination Indicator)
    - Signalisiert Format der Transportblöcke
  - FBI (Feedback Information)
    - Nur im Uplink

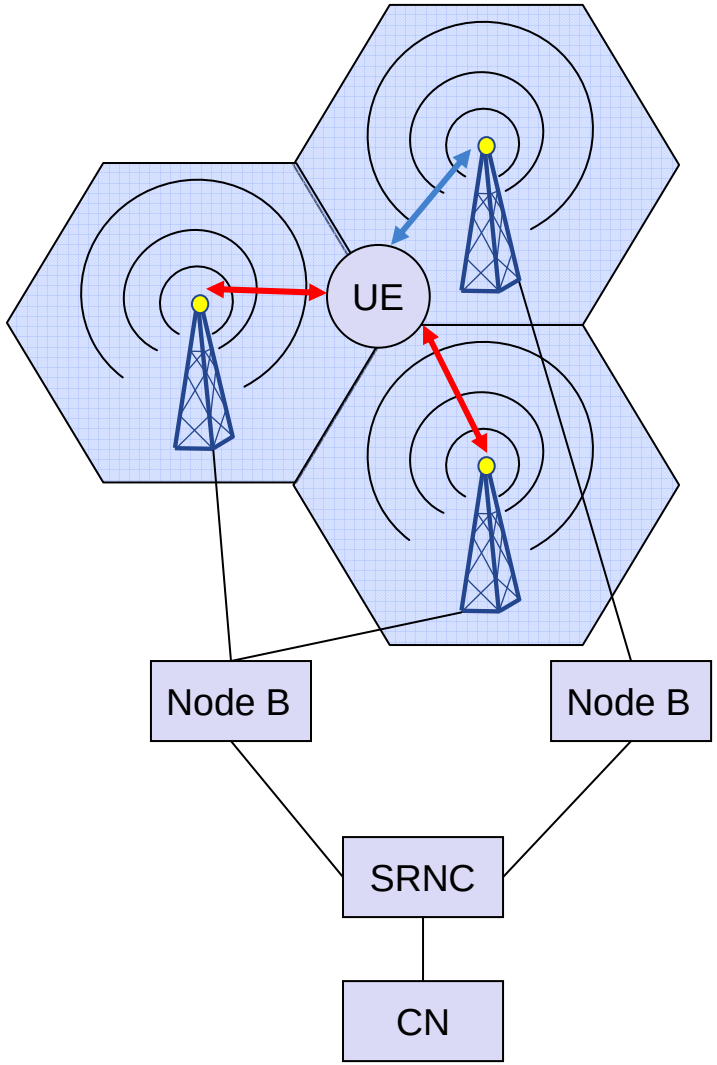


Logische Kanäle

- Erbringen die Dienste der MAC-Schicht
- Gegliedert in
  - Kontrollkanäle
    - Z.B. für Synchronisation, Broadcast, Paging
  - Verkehrskanäle
    - Übertragung von Nutzdaten
- … Abbildung auf Transportkanäle und von diesen auf physikalische Kanäle

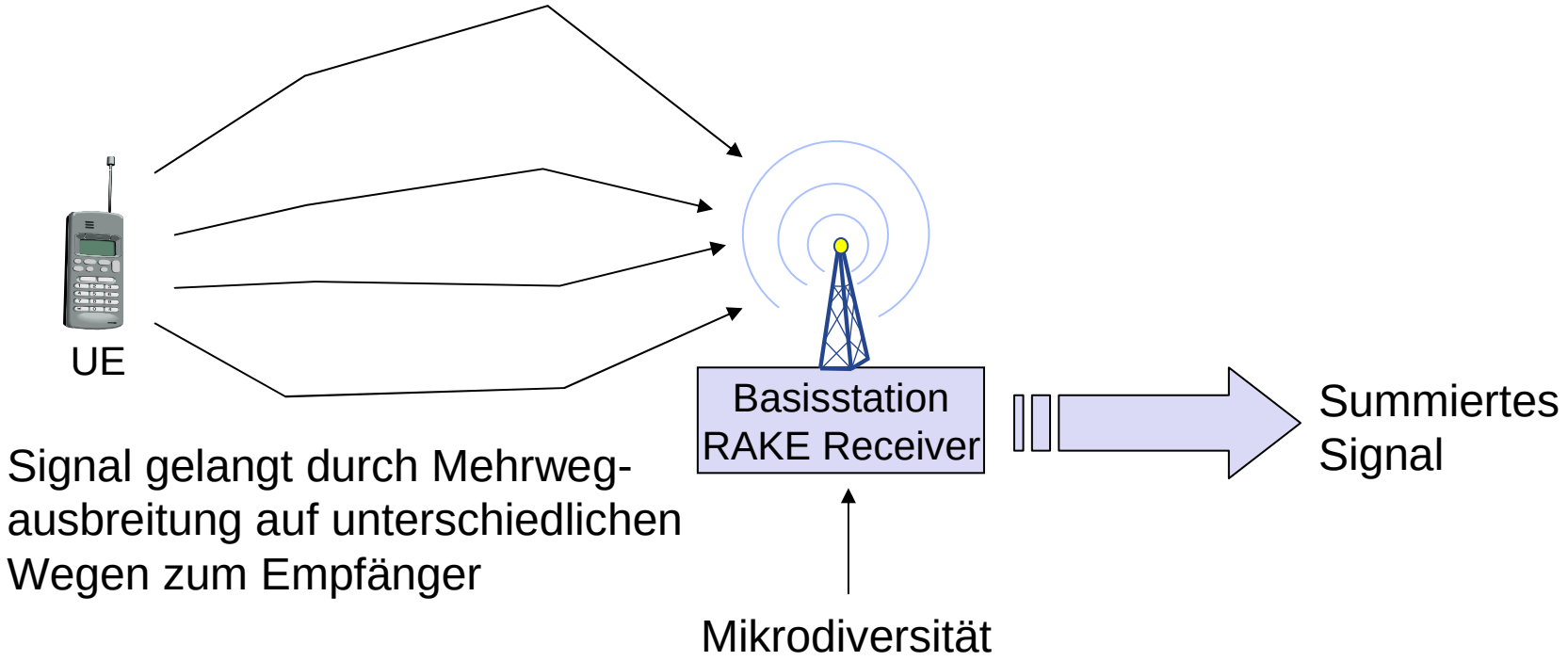
Mobilitätsunterstützung: Makrodiversität

- Prinzip
  - Senden des gleichen Datenstroms über verschiedene physikalische Kanäle
  - nur im FDD-Modus
- Uplink
  - Gleichzeitiges Empfangen der Daten der Mobilstation an verschiedenen Node B
  - Wiedergewinnung des Datenstroms im Node B, SRNC oder DRNC
- Downlink
  - Gleichzeitiges Senden der Daten in unterschiedlichen Zellen
  - Unterschiedliche Spreizcodes in verschiedenen Zellen



Mobilitätsunterstützung: Mikrodiversität

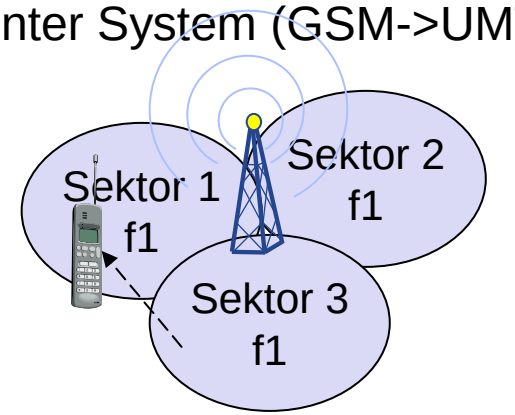
- Durch Mehrwegausbreitung zeitlich versetzte Signalkomponenten werden im RAKE-Receiver konstruktiv vereinigt
- Das resultierende Signal ist „besser“ als die beste Einzelsignalkomponente



Mobilitätsunterstützung: Handover

- Mehrere Handoververfahren
  - Hard Handover
    - Verbindung zu altem Node B wird abgebaut <u>bevor</u> neue aufgebaut wird
  - Soft Handover
    - Verbindung zu altem NodeB wird abgebaut <u>nachdem</u> neue aufgebaut wird
  - Softer Handover
    - Verbindung über mehrere Sektorantennen eines Node B
  - Soft-Softer Handover
    - Soft und softer Handover gleichzeitig

- Unterstützte Handover in UMTS
  - Intra NodeB / Inter-cell (softer Handover)
  - Inter NodeB (hard & soft Handover)
    - Inter-frequency, Intra-frequency
  - Inter RNC (hard, soft & soft-softer)
  - Inter MSC
  - Inter SGSN
  - Inter System (GSM->UMTS)



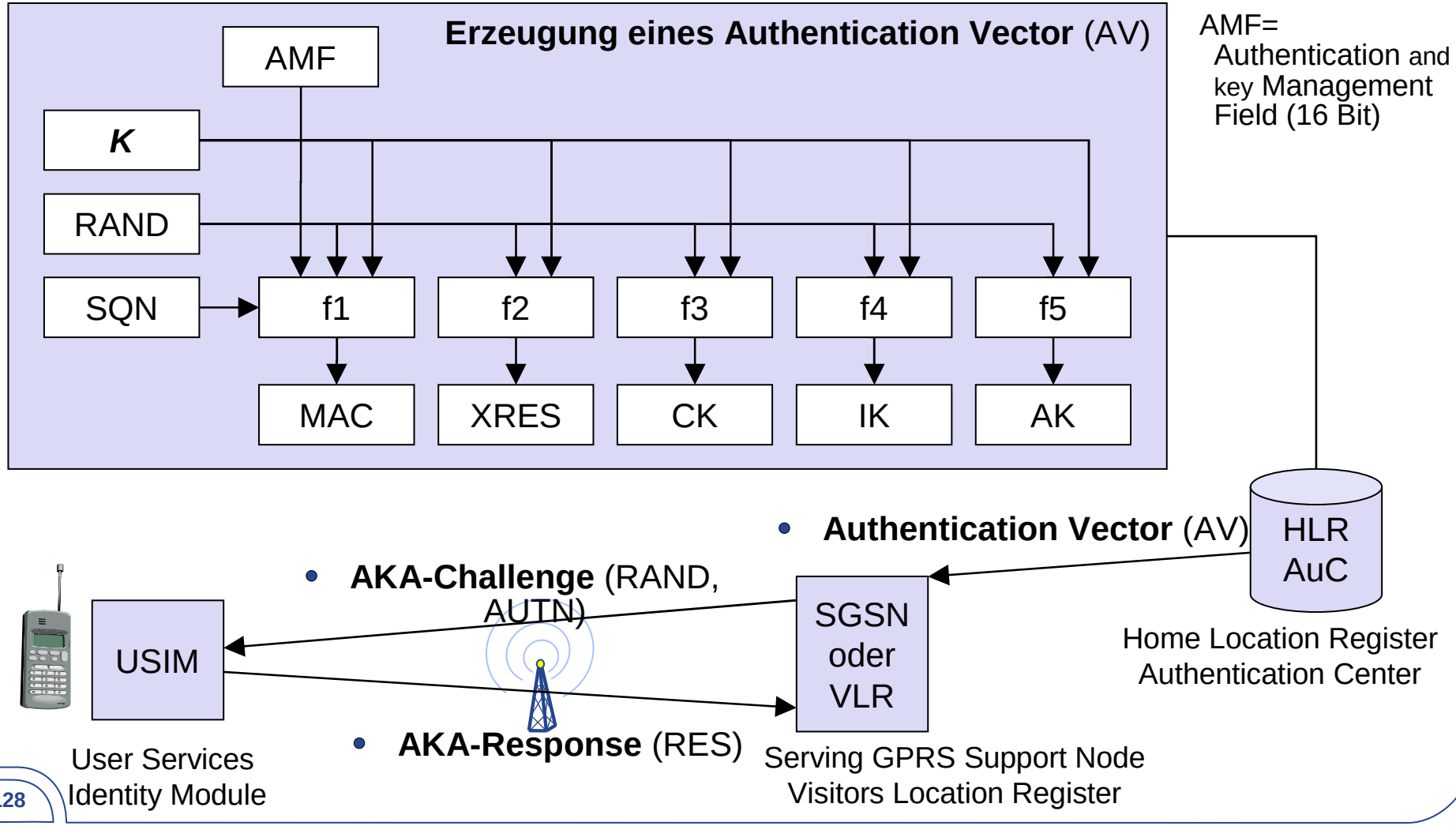
Inter-cell Handover

3.5 Sicherheit in UMTS

- Authentifikation
  - Geheimer Schlüssel K (Master Key)
    - nur dem USIM in der Mobilstation und dem HLR/AuC bekannt
  - Authentifizierung im VLR oder SGSN
    - Fordern Authentisierungsvektoren (AV) beim HLR/AuC an.
      - RAND (random challenge) zur Authentifikation des Teilnehmers
      - XRES (expected response) zur Authentifikation des Teilnehmers
      - CK (cipher key) zum Schutz der Vertraulichkeit
      - IK (integrity key) zum Schutz der Integrität
      - AUTN (authentication token) zur Authentifikation des Netzwerks
    - Mobilstation (USIM) erhält RAND und AUTN
      - Prüft AUTN
      - Berechnet RES auf die Herausforderung RAND
    - VLR bzw. SGSN erhalten RES zurück
      - Vergleich mit XRES
- Integrität und Vertraulichkeit
  - Auf Anordnung des MSC/VLR oder SGSN
    - Verschlüsselung bzw. Integritätsschutz zwischen Mobilstation und RNC über RLC-Schicht mit CK bzw. IK

Authentifikation in UMTS

- Authentication and Key Agreement (AKA) in UMTS



Authentifikation in UMTS

- Funktionen für Authentication and Key Agreement
  - f1: Berechnung eines MAC (Message Authentication Code)
  - f2: Berechnung von XRES
  - f3, f4, f5: Berechnung eines Schlüssels aus einer Zufallszahl
  - $\oplus$ XOR, || Konkatenation
- Erzeugen eines AV (5-Tupel) im HLR/AuC
  - Erzeugen einer zufälligen Sequenznummer SQN (einmal am Anfang)
  - Erzeugen einer zufälligen Herausforderung RAND (pro AV)
  - AMF (authentication and key management field)
    - z.B. zur Unterscheidung mehrerer alternativer Algorithmen
  - MAC = $f1_K$ (SQN || RAND || AMF)
  - XRES = $f2_K$ (RAND)
  - CK = $f3_K$ (RAND)
  - IK = $f4_K$ (RAND)
  - AK = $f5_K$ (RAND), anonymity key, um SQN zu anonymisieren
  - AUTN = ((SQN $\oplus$ AK) || AMF || MAC)
  - AV = (RAND || XRES || CK || IK || AUTN)

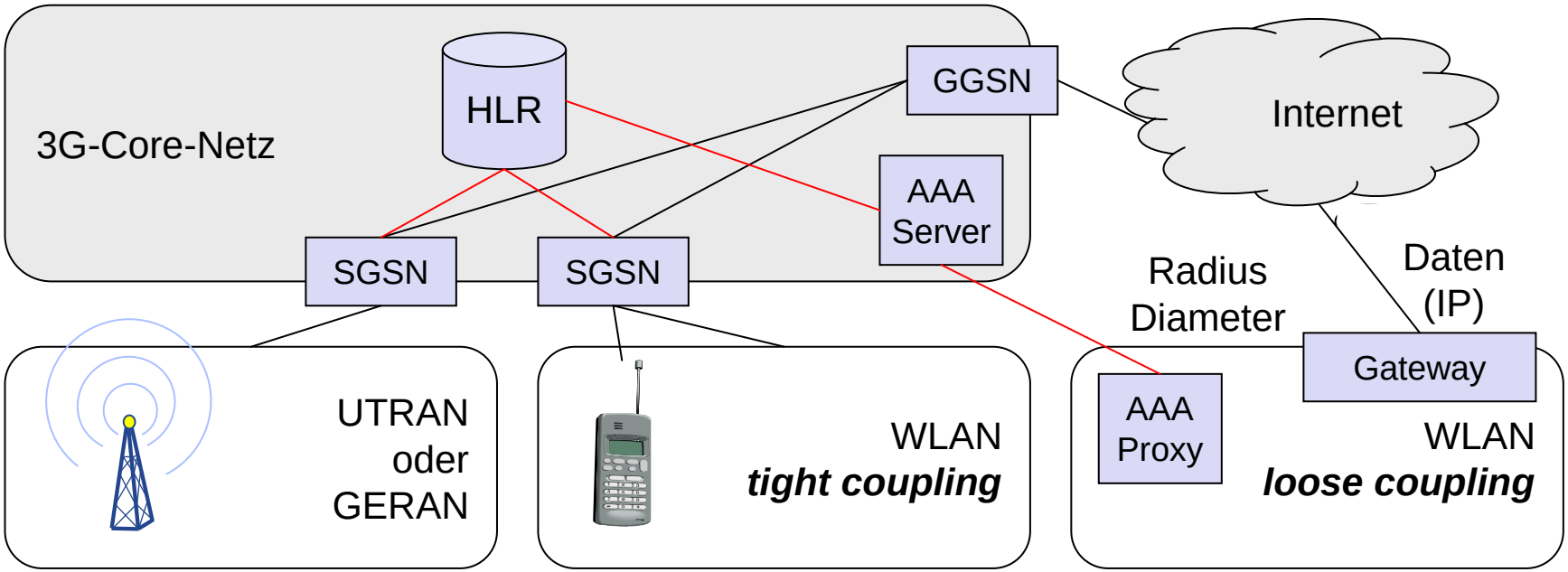
Authentifikation in UMTS

- Operationen im USIM
  - Empfangen von RAND und AUTN vom VLR oder SGSN
  - AK = $f5_K$ (RAND)
  - SQN = (SQN ⊕ AK) ⊕ AK
  - XMAC = $f1_K$ (SQN || RAND || AMF), expected MAC
  - Vergleichen von XMAC mit MAC (aus AUTN)
    - Falls ungleich, ist Authentifikation des Netzwerks fehlgeschlagen
      - Zelle wird von der Mobilstation als gesperrt angesehen
  - Prüfung, ob Sequenznummer im erwarteten Bereich liegt
  - RES = $f2_K$ (RAND)
  - Antwort an VLR oder SGSN mit RES
  - CK = $f3_K$ (RAND)
  - IK = $f4_K$ (RAND)
- Operationen im VLR bzw. SGSN
  - Empfangen von RES vom USIM
  - Vergleichen von RES mit XRES (aus AV vom HLR/AuC)
    - Falls ungleich, ist Authentifikation des Teilnehmers fehlgeschlagen

3.6 IP Multimedia Subsystem (IMS)

- Spezifikation zur Beschreibung der Architektur für die Implementierung von Telefon- und Multimedia-Diensten in Next Generation Networks
- Ziel: Nutzung der im Internet verfügbaren Dienste innerhalb von zellularen Netzen
  - Konvergenz von Sprache, Video und Daten in einem zellularen, IP-basierten Netz
  - Schließt Lücke zwischen Zellularen und IP-Netzen
- Entwicklung
  - Erstmals definiert in 3GPP Release 5
    - Session Initiation Protocol (SIP) als Signalisierungsprotokoll festgelegt
  - Parallel dazu Definition eines anderen IMS von 3GPP2
    - Nord-amerikanischer und asiatischer Raum
    - Interoperabilität zu IMS von 3GPP

3.7 WLAN-Integration – Ansätze

- Zwei grundlegende Ansätze
  - Tight Coupling
    - WLAN als zusätzliches Zugangsnetz in UMTS
    - Über eine I_u-Schnittstelle mit Kernnetz verbunden
    - Problem: erfordert kompletten 3G-Protokollstack im WLAN
  - Loose Coupling
    - WLAN als getrenntes Zugangsnetz
    - direkt mit dem Internet verbunden
    - gekoppelt über AAA (Authentification, Authorization, Accounting)
- In UMTS Release 6 wird Loose Coupling umgesetzt

WLAN-Integration – Architektur