

Mobiele Communicatie

Gilles Callebaut

10 juni 2016

Prof: Lieven De Strycker

1 H2: Draadloze transmissie

Direct Sequence Spread Spectrum (**DSSS**)

▷ Originele datastroom vergroten voor robuustheid of voor multiplexering (zie CDMA).

Code Division Multiple Access (**CDMA**)

▷ Multiple access realiseren via het toepassen van orthogonale of quasi-orthogonale codes.

Frequency Hopping Spread Spectrum (**FHSS**)

▷ Discreet veranderen van carrier frequentie. De sequentie is afkomstig van een pseudo random sequentie.

Twee versies:

- Fast hopping
Meerdere frequenties per user bit
- Slow hopping
Meerdere user bits per frequentie

Space Division Multiple Access (**SDMA**)

▷ Multiplexering op basis van ruimte.

- Gebruikt in cellen
- Probleem van interferentie tussen verschillende cellen

Hergebruiken van frequenties als ver van elkaar verwijderd zijn

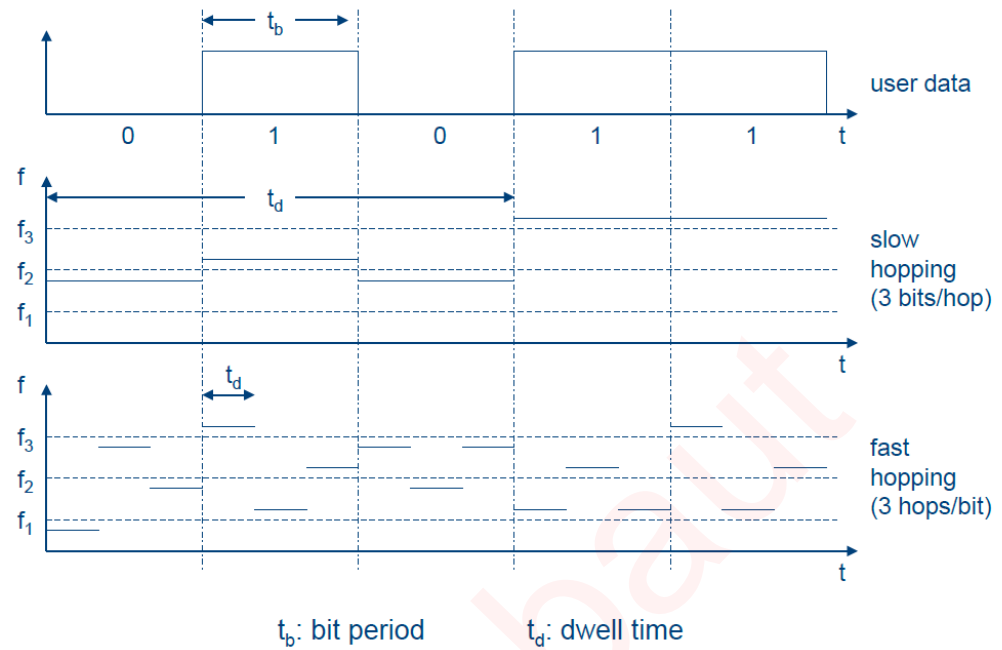
- Fixed frequency assignment
- Dynamic frequency assignment

Frequentie kiezen op basis van buuren. Zo kan er meer capaciteit worden voorzien als er meer trafiek is.

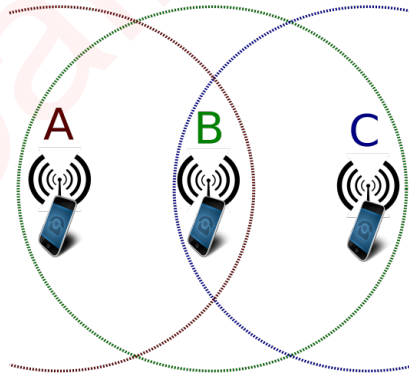
Hidden terminals

▷ Hidden terminals:

- $A \rightarrow B$



- $C \rightarrow B$ (C ziet A niet, Carrier Sense faalt)
- Collisie in B (Collision Detectie faalt want A en C zien de collision niet)



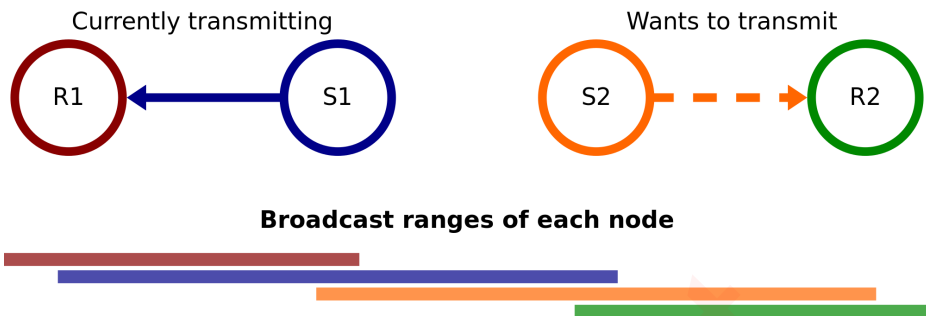
Exposed terminals

▷ Exposed terminals:

- $S_1 \rightarrow R_1$
- $S_2 \rightarrow R_2$ (S_2 wacht tot medium vrij, want ziet $S_1 \rightarrow R_1$)
- Maar S_2 reikt niet tot R_1 dus hij wacht voor niets

$\Rightarrow S_2$ is *exposed* to S_1

Exposed terminal problem

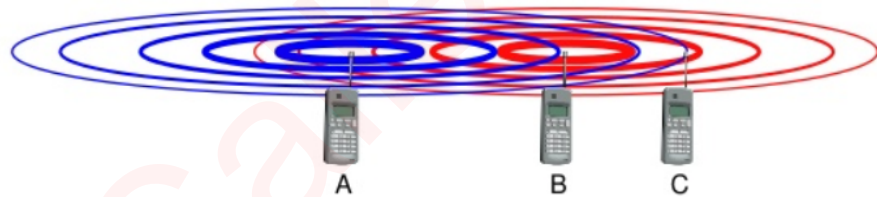


Near and far terminals

▷ Near and far terminals:

- $A \rightarrow C$
- $B \rightarrow C$
- Signaal van B verbergt A 's signaal $\rightarrow C$ kan A niet ontvangen

\Rightarrow Precieze *power control* noodzakelijk (ook bij CDMA)



Frequency Devision
Multiple Access (**FDMA**)

▷ Toewijzen van een frequentie kanaal tussen een zender en ontvanger

- Permanent (e.g., radio broadcast)
- Slow hopping (e.g., GSM)
- Fast hopping (FHSS)

Time Division Multiple
Access (**TDMA**)

▷ Toewijzen van een vaste zend frequentie band tussen de zender en ontvanger, voor een bepaalde hoeveelheid tijd.

Probleem van vertraging door de verschillende afstanden tussen zenders en ontvanger.

Oplossingen:

1. Guard time

De guard time tussen de verschillende time slots is even groot als de tijdsduur nodig voor een pakket om naar de buitenste kring te gaan en terug.

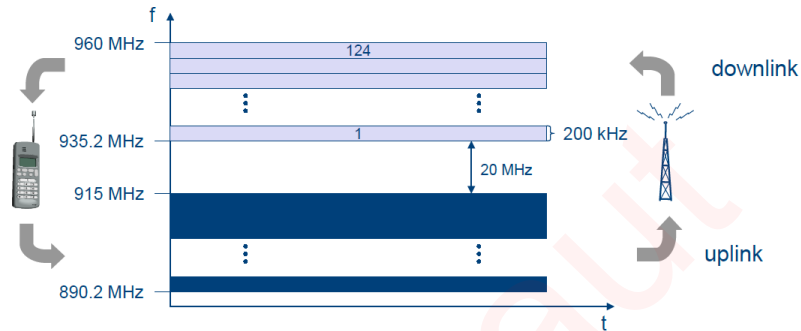
\Rightarrow Heel lage efficiëntie

2. Time advance

Vertraging opmeten en compenseren door gebruiker vroeger te laten zenden.

Frequency Division
Duplex/FDMA
(**FDD/FDMA**)

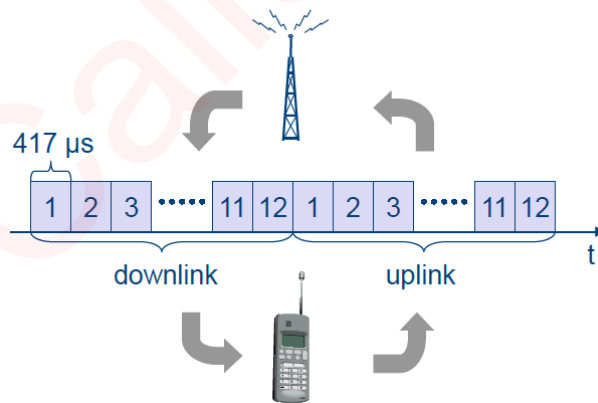
▷ FDD wordt gebruikt om een duplex kanaal op te zetten. Hierbij kan er simultaan verzonden worden over een up- (mobile → base station) en downlink (base → mobile station). (e.g. GSM)



Duplex distance : 45 MHz

Time Division
Duplex/FDMA
(**FDD/FDMA**)

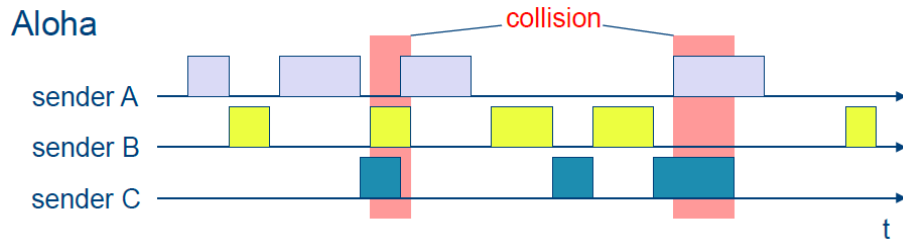
▷ TDD wordt gebruikt om een duplex kanaal op te zetten. Hierbij worden verschillende slots toegewezen voor de uplink en downlink (gebruik makend van dezelfde frequentie).



Aloha

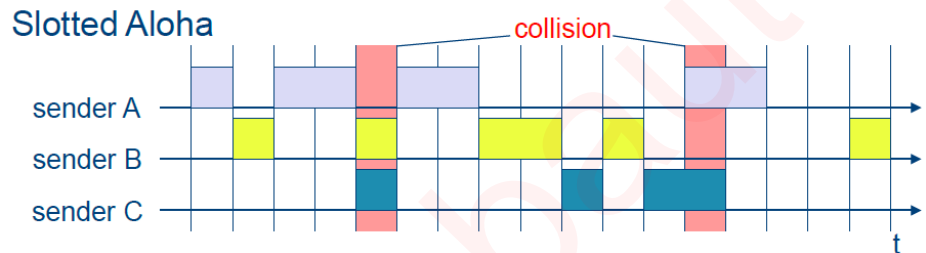
▷ Aloha is een TDM zonder *control access*. Elk station kan het medium benaderen op elk tijdstip.

- Random
- Gedistribueerd (geen centrale arbiter)
- Bij botsing: oplossen in hogere lagen (e.g. retransmissie)
- (+) bij lichte *load*



Slotted Aloha

▷ Slotted Aloha werkt verder op Aloha, hierbij gebruikmakend van tijdssloten. Het zenden mag enkel beginnen aan het begin van een tijdsslot. Hierdoor moeten de zenders gesynchroniseerd zijn.



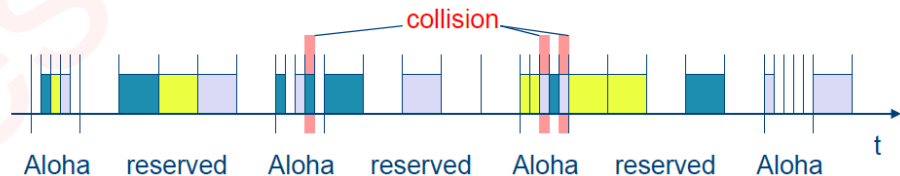
Demand Assigned Multiple Access (**DAMA**)

▷ Expliciet Reservation of Reservation Aloha kent twee modes:

1. ALOHA mode voor reservatie (veroveringsfase)
Competitie voor kleine reserveringssloten, waarbij botsingen mogelijk zijn
2. Gereserveerde sloten voor data transmissie, waarbij **geen** botsingen mogelijk zijn

De time slots worden RR opgevuld zoals aangegeven in de reservation list, die wordt verstuurd van base naar de mobile stations (synchroniseren).

Als er wordt gezien dat een gereserveerd slot leeg is, dan mag er ook gezonden worden.



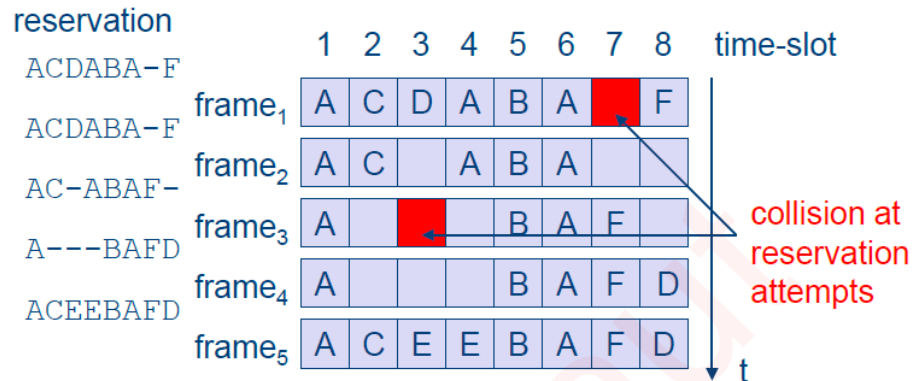
Packet Reservation Multiple Access (**PRMA**)

▷ Implicit Reservation:

- Aantal slots worden samengenomen in een frame
- Frames worden telkens herhaald
- De satelliet zendt de reservaties per frame uit
- Stations willen een slot veroveren op basis van slotted Aloha
- Als een station een slot heeft veroverd, dan wordt deze slot automatisch toegewezen aan dat station voor alle opvolgende frames (zolang het station

iets wil zenden)

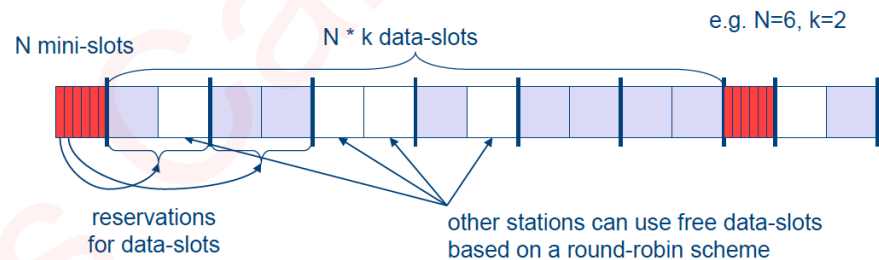
- Als het slot leeg is, dan zal in het volgende frame weer worden gevochten om een reservatie voor dat slot



Reservation TDMA

▷ Reservation TDMA:

- Elke frame bestaat uit N mini-slots en x data-slots
- Elk station heeft zijn eigen mini-slot (nu wel mini-slot gereserveerd per gebruiker) en kan tot k data-slots reserveren via zijn mini-slot (i.e. $x = N \cdot k$)
- Best-effort trafiek kan worden gerealiseerd door het zenden van pakketten tijdens de lege data-slots.



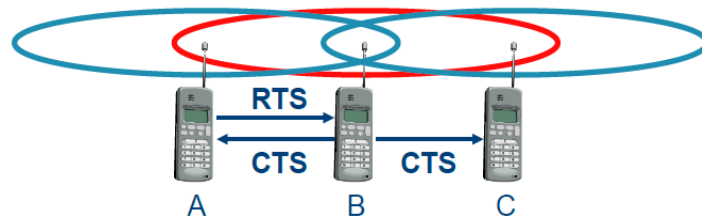
Multiple Access with Collision Avoidance (MACA)

▷ MACA lost het probleem op van *hidden* en *exposed terminals*, en heeft geen base station nodig. Dit door gebruik van kleine pakketjes voor *collision avoidance*.

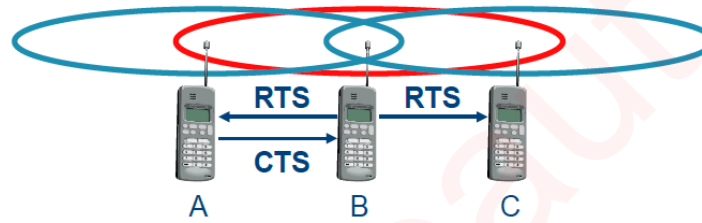
- RTC (request to send)
Een zender vraagt het recht om te zenden naar een ontvanger
- CTS (clear to send)
De ontvanger geeft het recht om te zenden als het klaar is om een pakket te ontvangen

Het pakket bevat:

- Zenders adres
- Ontvangers adres
- Grootte van pakket (en dus transmissieduur)



Figuur 1: Maca avoids the problem of hidden terminals



Figuur 2: Maca avoids the problem of exposed terminals

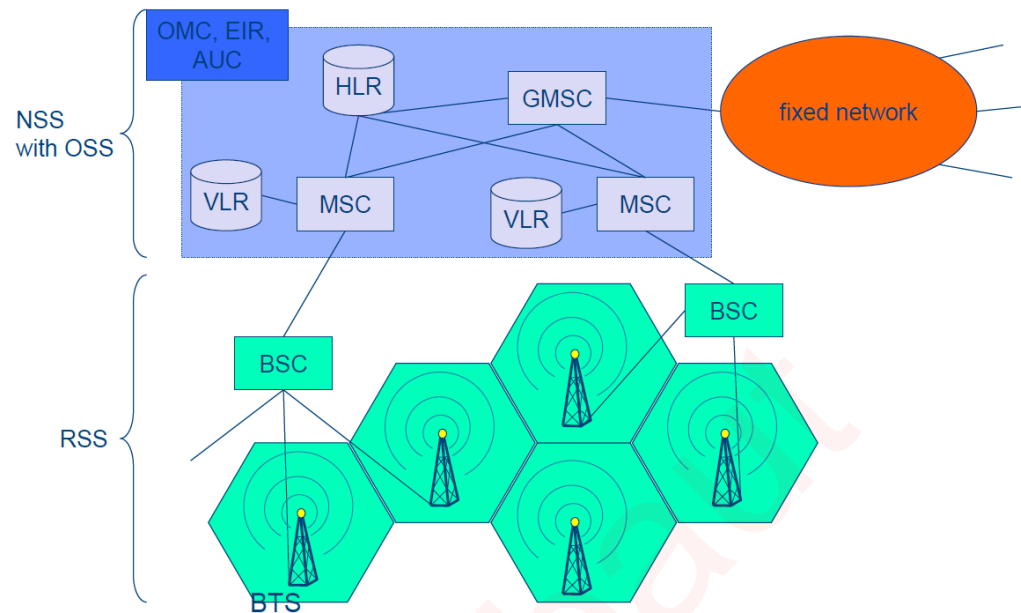
2 H4: Telecommunicatiesystemen

2.1 GSM

GSM

▷ GSM bestaat uit drie subsystemen:

- RSS (radio subsysteem)
 - BSS (Base Station Subsystem)
 - * BTS (Base Transceiver Station)
 - * BSC (Base Station Controller)
 - MS (Mobile stations)
- NSS (network en switching subsysteem)
Call forwarding, handover, switching, billing mobility management
 - MSC (Mobile Services switching Center)
 - HLR (Home Location Register)
 - VLR (Visitor Location Register)
- OSS (operation subsysteem)
Management of the network
 - AUC (Authentication Center)
 - EIR (Equipment Identity Register)
 - OMC (Operation and Maintenance Center)



Figuur 3: GSM overview

2.1.1 RSS

Radio SubSystem (RSS)	<p>▷ Het RSS bestaat uit het cellulaire mobiele netwerk tot aan de switching centra. Het bestaat uit de volgende componenten:</p> <ul style="list-style-type: none"> • Base Station Subsystem (BSS) • Mobile stations (MS)
Base Station Subsystem (BSS)	<p>▷ Het BSS bestaat uit een BSC verbonden met een aantal BTS'en.</p> <ul style="list-style-type: none"> • Base Transeiver Station (BTS) • Base Station Controller (BSC)
Base Transeiver Station (BTS)	<p>▷ Het BTS bestaat uit alle radio componenten¹ en is geconnecteerd met een MS via de U_m interface (radio interface) en met de BSC via de A_{bis} interface.</p>
U_m interface	<p>▷ De U_m interface voorziet alle mechanismen voor draadloze transmissie (e.g. TDMA, FDMA).</p>
Base Station Controller (BSC)	<p>▷ De BSC beheert veelal de BTS's, bepaald welke frequentie wordt gekozen binnen welke cel, schakelen in real-time naar andere BTS's, multiplexeren van binnen komende signalen,...</p>
Mobile Station (MS)	<p>▷ De MS is de terminal voor het gebruik van de GSM diensten en bestaat uit</p>

¹receiver, amplifiers, signal processing, antenne - als directed antennas worden gebruikt kan één BTS meerdere cellen omvatten

twee delen:

1. User-independend hard- en software
 - International Mobile Equipment Identity (IMEI)
 - RF, display, keyboard, camera, games, Bluetooth
2. Subscriber Identity Module (SIM)
 - Personalizes the MS
 - Billing, subscriber diensten, International Mobile Subscriber Identity² (IMSI), Temporary-IMSI (TMSI), authentication information, ciphering information, Location Area Identification (LAI)

2.1.2 NSS

Network and Switching Subsystem (**NSS**)

▷ NSS is de hoofdcomponent van het publieke mobiele GSM netwerk.

Deze bestaat uit:

- MSC (Mobile Services Switching Center)
Controleert alle connecties binnen het domein van de MSC, die enkele BSC's kan omvatten.
- Databanken
 - HLR (Home Location Register)
 - VLR (Visitor Location Register)

Mobile Services switching Center (**MSC**)

▷ De MSC speelt een centrale rol in GSM:

- Opzetten connecties met andere MSC's
- Opzetten connecties met BSC's via *A*-interface
- Vormen het vaste backbone netwerk van een GSM systeem
- Connectie met vaste netwerken (PSTN, ISDN, ...) via Gateway MSC (**GMSC**)
- Connectie met openbare netwerken zoals Interworking functions (IWF)
- Integratie met databanken
- Specifieke functies voor paging en call forwarding

²Een International Mobile Subscriber Identity, afgekort IMSI, is een uniek nummer verbonden aan alle GSM- en UMTS-gebruikers van mobiele telefoons. Het is opgeslagen op de SIM in de telefoon en wordt door de telefoon naar het netwerk van de telecomaandbieder gestuurd. Het wordt ook gebruikt om andere gegevens over de mobiel uit de HLR te verkrijgen. Om af luisteren van het IMSI-nummer te bemoeilijken, wordt dit nummer zo min mogelijk verstuurd en wordt in plaats ervan een willekeurig gegenereerd TMSI-nummer verstuurd.

- Locatie registratie en forwarding van locatie info
- Ondersteuning voor SMS

De MSC heeft enkel een VLR, dit in tegenstelling tot GMSC die zowel een VLR als een HLR heeft.

Gateway Mobile Switching Centre (**GMSC**)

▷ De Gateway Mobile Switching Centre (GMSC) is een speciale versie van de Mobiele Schakel Centrale (MSC) die wordt gebruikt om gesprekken van en naar externe netwerken te routeren. Als een gebruiker een gesprek wil beginnen met iemand die zich buiten het netwerk bevindt, dan wordt het gesprek via een GMSC naar het betreffende externe netwerk geleid. Dit kan het openbare telefoonnet zijn, maar bijvoorbeeld ook een ander mobiel netwerk. Anderzijds komen de gesprekken voor mobiele gebruikers van een extern netwerk bij de GMSC binnen. De GMSC routeert het gesprek dan naar de MSC waaronder de mobiele gebruiker zich bevindt.

Home Location Register (**HLR**)

- ▷ De HLR houdt informatie van de *home-subscribers* bij in een centrale databank.
- Bijhouden van relevante gebruikersinfo
 - Statische data:
 - Mobile subscriber ISDN number (MSISDN)
 - Afgenomen diensten (vb. doorschakelen)
 - International mobile subscriber identity (IMSI)
 - Dynamische data:
 - Location area (LA) van de MS
 - Mobile subscriber roaming number (MSRN)
 - Actuele VLR en MSC

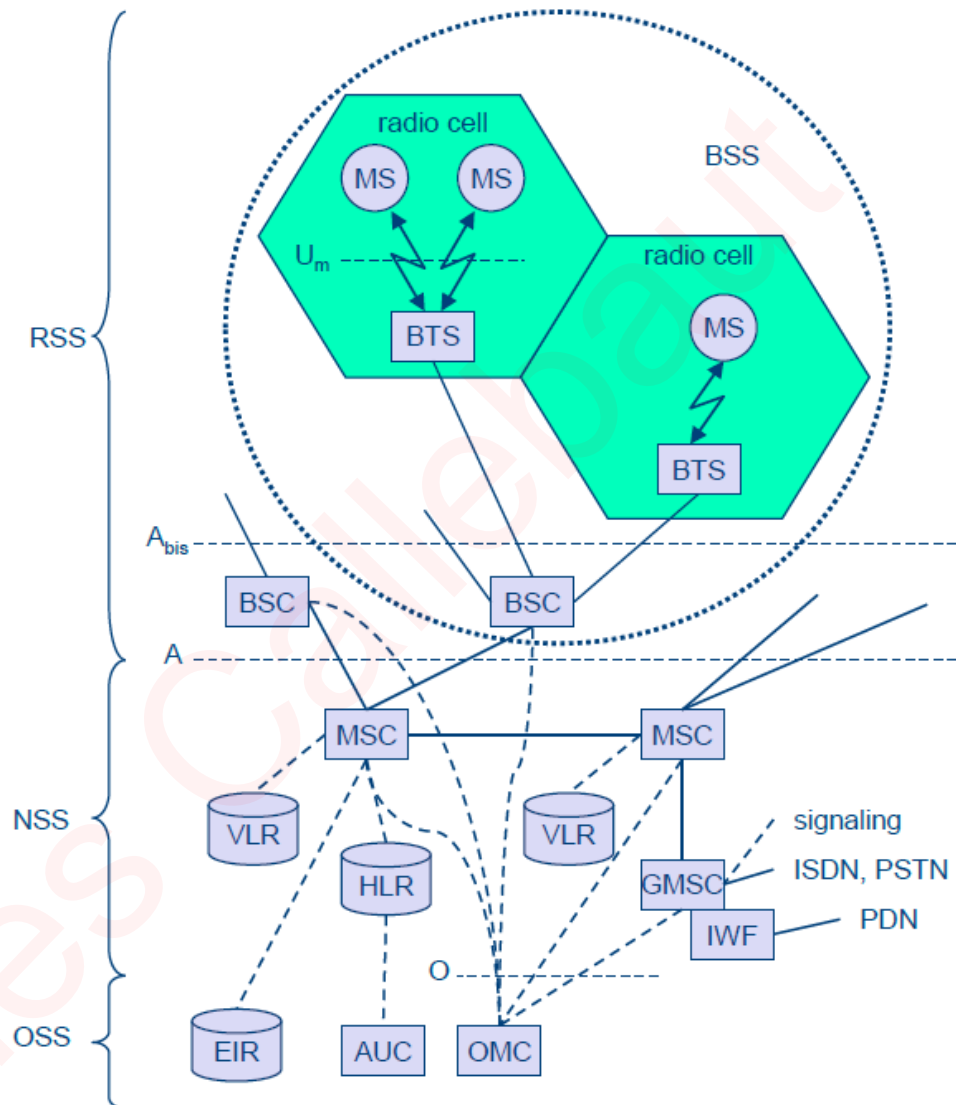
Visitor Location Register (**VLR**)

- ▷ Deze databank houdt alle informatie bij van alle *current users* in het domein van de MSC.
- Hoort bij MSC
 - Dynamische database, houdt alle gegevens bij die van belang zijn voor de huidige MS-gebruikers die op dat moment in het LA zich bevinden dat bij de MSC hoort.
 - Bevat kopie van relevante gegevens uit HLR, die gekopieerd worden wanneer MS een LA binnenkomt waar het VLR voor verantwoordelijk is.

2.1.3 OSS

Operating Subsystem (**OSS**)

▷ Het OSS maakt een centrale operatie mogelijk, en beheert en onderhoudt alle GSM subsystemen.



Figuur 4: GSM overview met interfaces

De componenten:

- AUC (Authentication Center)
- EIR (Equipment Identity Register)
- OMC (Operation and Maintenance Center)

Authentication Center
(**AUC**)

▷ Het AUC genereert specifieke authenticatie parameters op aanvraag van een VLR. Deze parameters worden gebruikt voor authenticatie van de mobiele terminals en encryptie van de user data (*on the air interface*) binnen het GSM netwerk.

Equipment Identity
Register (**EIR**)

▷ De EIR registreert de GSM mobiele stations (IMEI). Gestolen of slecht functionerende mobiele stations kunnen worden geblokkeerd en soms zelfs gelokaliseerd.

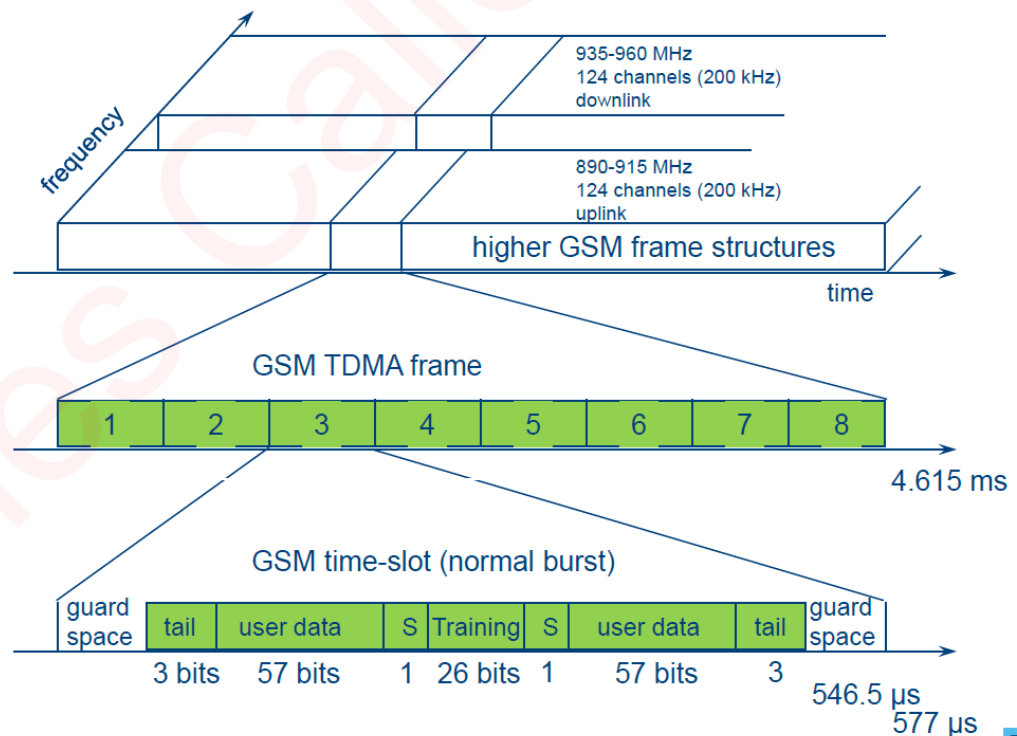
Operation and
Maintenance Center
(**OMC**)

▷ Het OMC monitort en bestuurt alle andere netwerkentiteiten via de *O*-interface.

2.1.4 GSM radio-interface

TDMA/FDMA

▷ De U_m interface wordt weergegeven in Figuur 5. Er worden 248 kanalen opgezet via FDMA. Deze kanalen worden nog eens opgedeeld in GSM TDMA frames. Zo'n frame bestaat uit 8 GSM time slots. Deze slots zijn redelijk kort vermits langere slots zorgt voor meer delay (de tijd tussen de herhaling van een frame wordt lang).



Figuur 5: GSM Radio-interface: TDMA/FDMA

De space-guards zijn nodig bij timing advance en ook door de hardware traagheid van bijvoorbeeld versterkers.

De up- en downlink verschilt in drie tijdsslot om geen full-duplex te moeten ondersteunen en omdat er zo tijd over is voor frequentie-hopping.

GSM time-slot:

training sequentie wordt gebruikt zodat de ontvanger zijn parameters kan aanpassen naar het beste pad.

S deze vlag zal indiceren of het data veld gebruikt wordt voor netwerk controle data

Logische kanalen Logische kanalen gebruiken de fysieke kanalen om informatie door te sturen: user data, signaling en 'idle' informatie. De logische kanalen kunnen worden opgesplitst:

- Dedicated channels (per gebruiker)

TCH ▷

- Transmissie van user data (TCH)

TCH/F ▷

- * TCH/F: Traffic CHannel/Full rate

TCH/H ▷

- * TCH/F: Traffic CHannel/Half rate

CCH ▷

- Signaling related to a call (CCH)

Verschillende CCH's worden gebruikt in het GSM systeem om medium access te controleren, trafiek kanalen te alloceren of mobiliteit te behe-
ren.

SACCH ▷

- * Slow Associated Control CHannel (SACCH)

- Data in parallel met de user data (altijd)
- niet-belangrijke procedures
- e.g., metingen van de kwaliteit van de radio link

FACCH ▷

- * Fast Associated Control CHannel (FACCH)

- Geen apart kanaal, zal een deel van het TCH in beslag nemen (stealing flags → helf van de user bits in beslag nemen)
- Fast signaling (snelle afhandeling)
- e.g., tijdens call setup, authenticatie en handover

- Signaling not related to a call

SDCCH ▷

- * Stand-alone Dedicated Control CHannel (SDCCH)

- Zolang de MS geen TCH heeft opgesteld met de BTS gebruikt het de SDCCH

- Benodigdheden om een TCH op te zetten
- Zorgen dat er connectie kan worden gemaakt met het netwerk, voor als er iemand belt
- e.g. authenticatie, location updating, call forwarding control

- Common channels (voor alle gebruikers)

FCCH ▷

- Frequency Correction CHannel (FCCH)

- * synchronization purpose between BTS and GSM Mobile
- * downlink channel and carry continuous wave signal which helps mobile find the frequency offset between BTS and MS

SCH ▷

- Synchronization CHannel (SCH)

- * Once the Mobile is frequency synchronized with BTS, it need to be time synchronized which is done using GSM SCH transmitted by BTS in downlink.
- * SCH carry frame number and BSIC (Base Station Identity Code) which helps Mobile synchronize with GSM frame structure (time-slots) as well as helps in identification of the Base station in the GSM network.

BCCH ▷

- Broadcast Control CHannel (BCCH)

- * Downlink only signalling channel
- * Algemene informatie over het netwerk voor het MS
- * e.g. naburige cellen

RACH ▷

- Random Access CHannel (RACH)

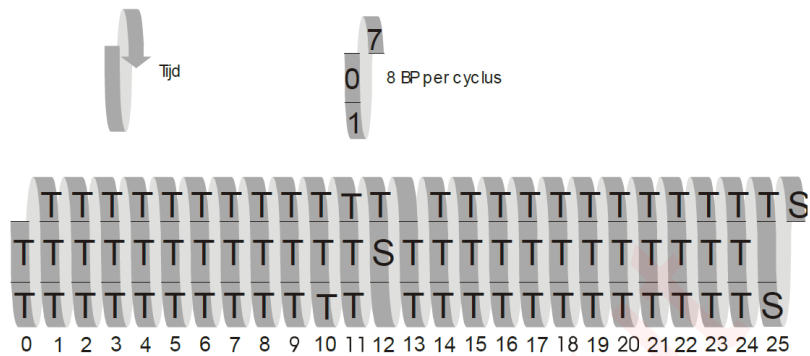
- * Uplink, gebruikt door MS → Setup a call
- * Lege tijdsslots → random kiezen (Slotted Aloha)

PAGCH ▷

- Paging and Access Grant CHannel (PAGCH)

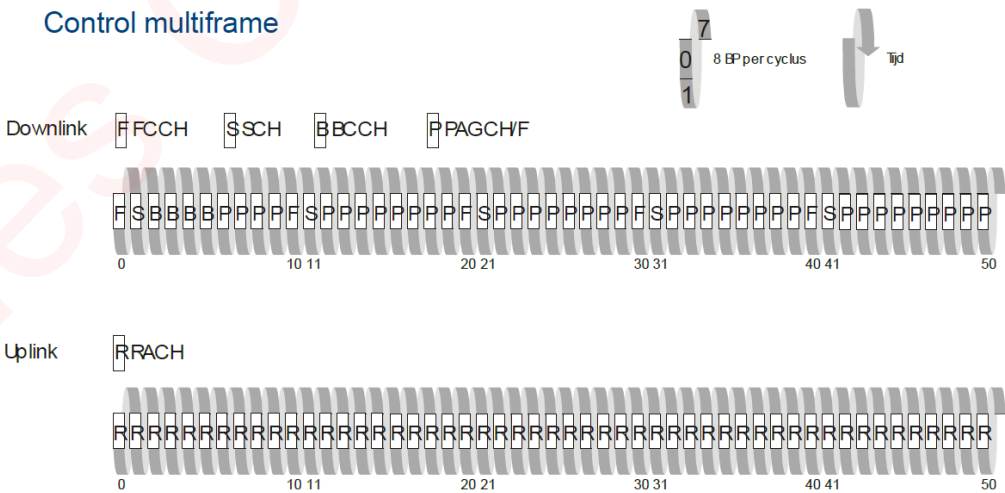
- * Downlink
- * Paging: call from the BTS to setup a call
- * Access grant: response van de BTS op een RACH (je kan een TCH of SDCCH gebruiken voor de verdere connection setup)

Mapping van logische naar fysische kanalen



Figuur 6: Trafiek multiframe GSM
(T indiceert user trafiek in de TCH/F en S indiceert signaling trafiek in de SACCH)

Er is expres 1 tijdsslot leeggelaten zodat er zeker eens naar de downlink kan geluisterd worden. Vermits de lengtes van down en uplink 26 en 51 zijn, verschuiven ze over elkaar en wordt er zo voor gezorgd dat er een kans bestaat dat alle soorten zeker kan worden gelezen.



Figuur 7: Controle multiframe GSM

2.1.5 Roaming

- Locatie van een subscriber wordt geüpdatet ook al is hij 'idle'
- HLR bevat informatie over de momentele locatie
- VLR communiceert met de HLR over locatie wijzigingen
- Als MS het Location Area (LA) van een nieuwe VLR binnen treedt, zendt de HLR alle nodige informatie naar het nieuwe VLR

LA ▷

GSM numbers Om een MS te localiseren en op te bellen zijn er enkele nummer nodig:

MSISDN ▷

- Mobile Station International ISDN nummer (MSISDN)
 - Nummer die gebruikt wordt om een subscriber op te bellen

CC, NDC, SN ▷

- Country Code (CC) + National Destination Code (NDC) + Subscriber Number (SN)

IMSI ▷

- International Mobile Subscriber Identity (IMSI)
 - Intern uniek nummer om een subscriber uniek te identificeren

MCC, MNC, MSIN ▷

- Mobile country Code (MCC) + Mobile Network Code (MNC, e.g. Proximus) + Mobile Subscriber Identification Number (MSIN)

TMSI ▷

- Temporary Mobile Subscriber Identity (TMSI)
 - Tijdelijke versie van de IMSI
 - IMSI nooit door de lucht verzonden voor veiligheidsredenen (e.g. anders zou een persoon worden gevolgd/gelocaliseerd op basis van zijn IMSI)
 - De TMSI wordt toegewezen door de VLR

MSRN ▷

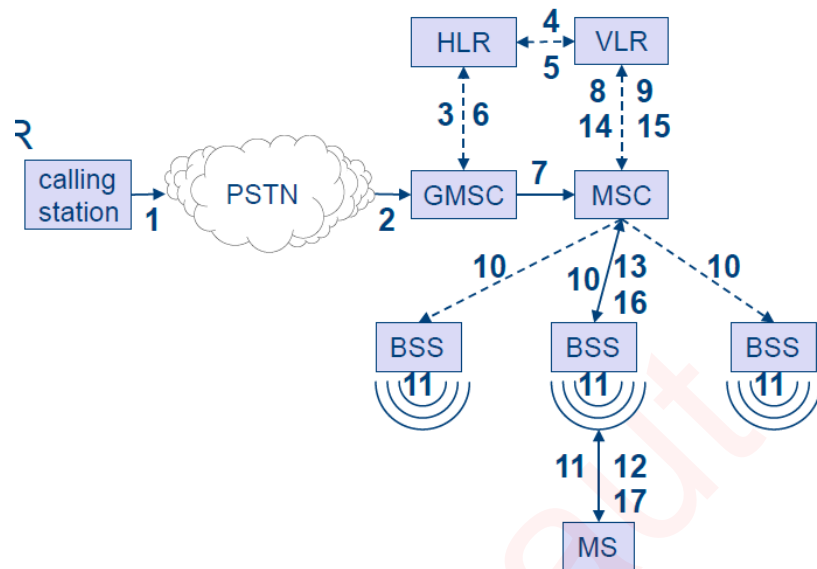
- Mobile Station Mobile Roaming Number (MSRN)
 - Toegewezen door de VLR

VCC, VNDC ▷

- Visitor Country Code (VCC) + Visitor National Destination Code (VNDC)
- De MSRN helpt de HLR om een subscriber te zoeken voor een inkomende oproep
- Tussen de HLR en VLR wordt veel geschakeld, op basis van de MSRN weet de schakelcentrale naar waar de oproep naartoe moet

Mobile Terminating Call (MTC)

▷ Telefoongesprek waarbij de mobiele gebruiker opgebeld wordt (i.e. de ontvanger is).



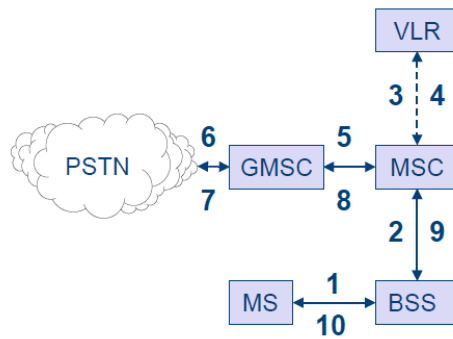
Figuur 8: MTC

- 1** Calling a GSM subscriber (via MSISDN)
- 2** Forwarding call to GMSC (op basis van national destination code)
- 3** Signal call setup to HLR
- 4,5** Request MSRN from VLR + MSC van de BSS
- 6** Forward responsible MSC to GMSC
- 7** Forward call to currnt MSC
- 8,9** Get current status of MS
- 10,11** Paging of MS in LA (Paging wordt verstuurd naar alle BSS waarvoor de MSC verantwoordelijk is, de juiste BSS zoeken is te tijdsintensief)
- 12,13** MS answers
- 14,15** Security checks
- 16, 17** Setup connection

Het opzetten van een MTC is dus een vrij complex proces, omdat hier location management bij komt kijken. Voor het gesprek kan worden opgezet moet de mobiele gebruiker immers gelokaliseerd worden.

Mobile Originating Call
(**MOC**)

▷ De MS zal nu een telefoongesprek starten.



Figuur 9: MOC

1,2 Connection Request

3,4 Security Check

5-8 Check resources (free circuit)

9,10 Setup call

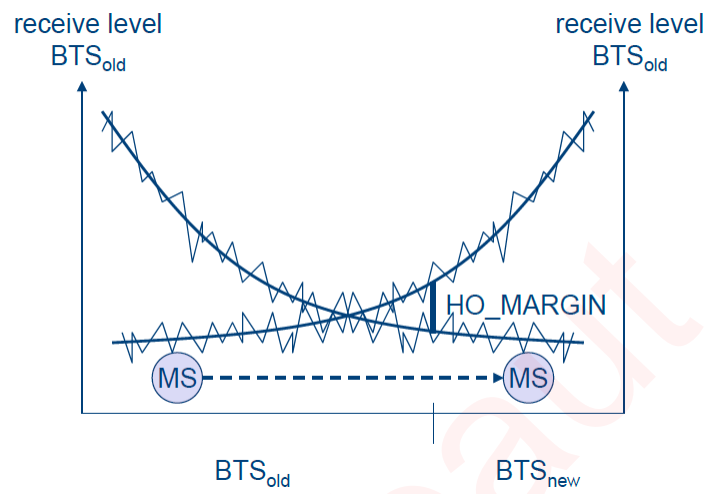
2.1.6 Handover

Redenen om handovers te doen:

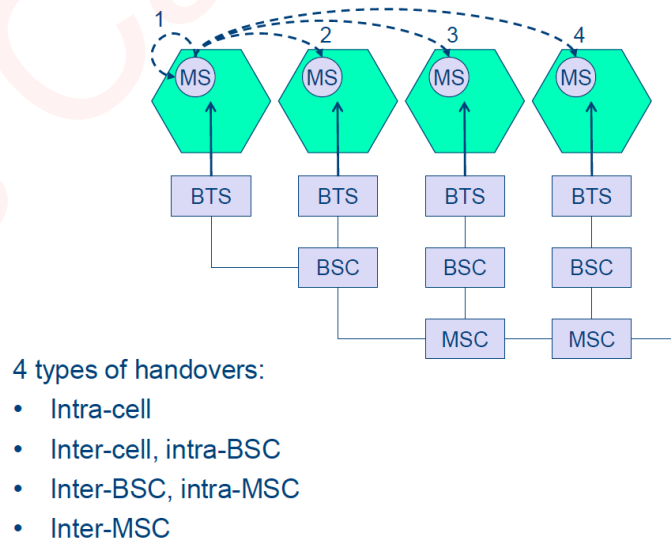
- Signaal kwaliteit
- Trafiek in 1 cel wordt te hoog (load balancing)

Handover decisie

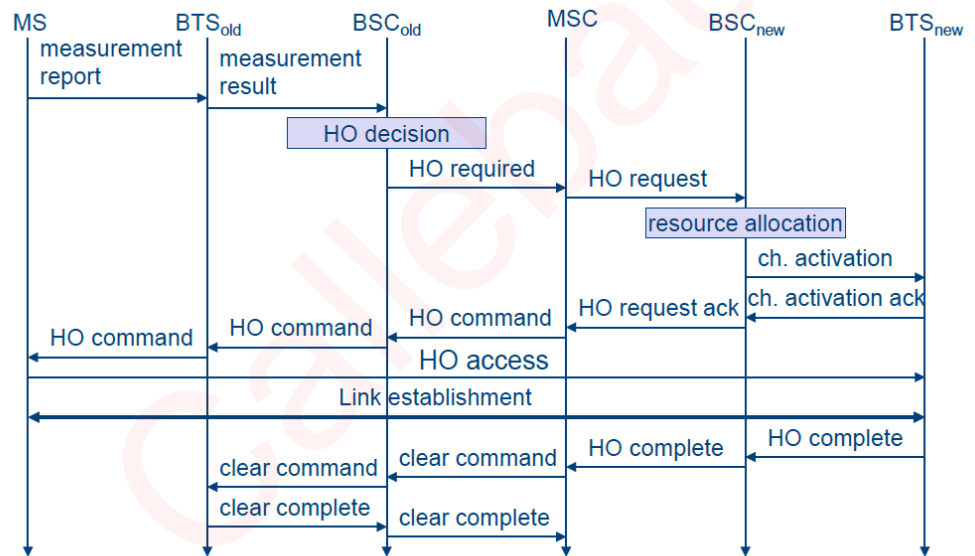
- MS en BTS meten (in respectievelijk de down en uplink)
- MS zend om de 0,5 sec metingen uit over het momentele kanaal en de kwaliteit van sommige BCCH kanalen in de aangelegen cellen
- BSC verzameld deze meetwaarden
- De BSC vergelijkt deze met de HO_MARGIN (om ping-pong effecten te vermijden)



Figuur 10: Handover decisie



Figuur 11: 4 Types of Handover



Figuur 12: Handover Procedure (inter BSC, intra-MS)

2.1.7 Security

GSM biedt enkele veiligheidsdiensten aan:

- Access control / Authentication
 - Authenticatie van de gebruiker aan de SIM (Subscriber Identity Module) via een PIN (Personal Identification Number)
 - Subscriber authenticatie (SIM \Leftrightarrow netwerk via challenge/response methode)
- Confidentiality
 - Na succesvolle authenticatie wordt user-related data geëncrypteerd
- Anonymity
 - TMSI
 - TMSI wordt vernieuwd door de VLR bij elke locatie verandering, i.e. Location UPdate (LUP)
 - Data wordt geëncrypteerd

SIM, PIN ▷

LUP ▷

Drie algoritmes in GSM

- A3 voor authenticatie in SIM en AuC
- A5 voor encryptie
- A8 voor sleutel generatie in SIM en AuC

Netwerk providers kunnen gebruik maken van sterkere mechanismen voor authenticatie of gebruikers kunnen gebruik maken van sterkere end-to-end encryptie.

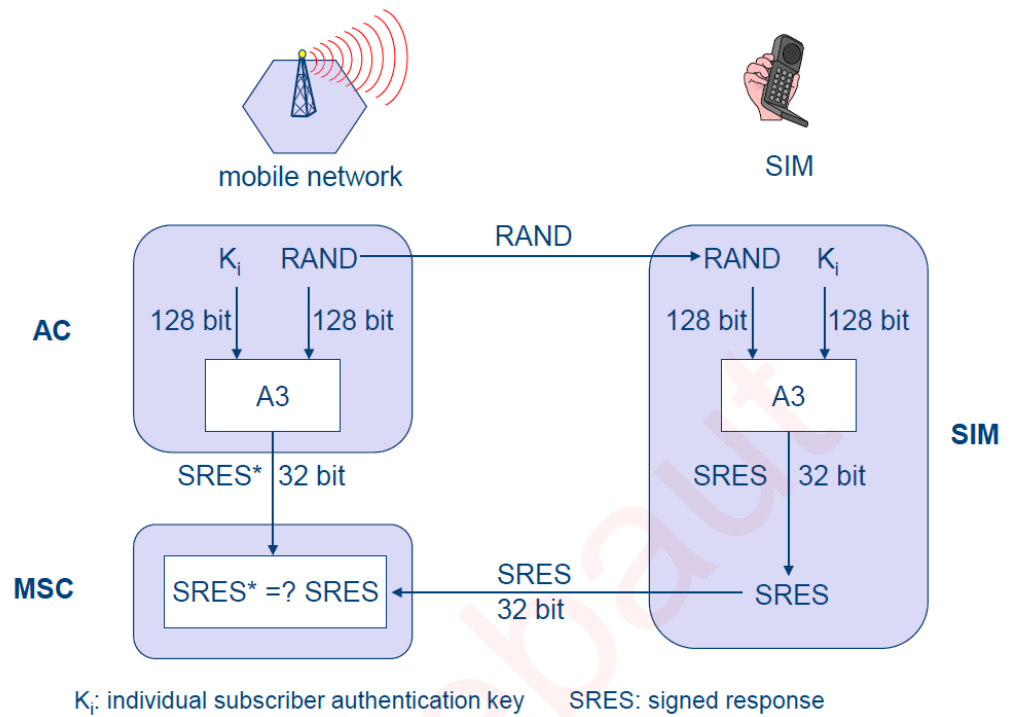
Authenticatie De SIM bevat:

- Een individuele authenticatie sleutel K_i
- De user identification (IMSI)
- A3 Algoritme

Procedure:

- AC genereert een random $RAND$ als challenge
- De AuC genereert een challenge-response set () en de K_c (zie encryptie)
- Deze set wordt doorgestuurd naar de HLR
- De momentele VLR vraagt de corresponderende waarden op voor een $RAND$ en SRES

SRES ▷

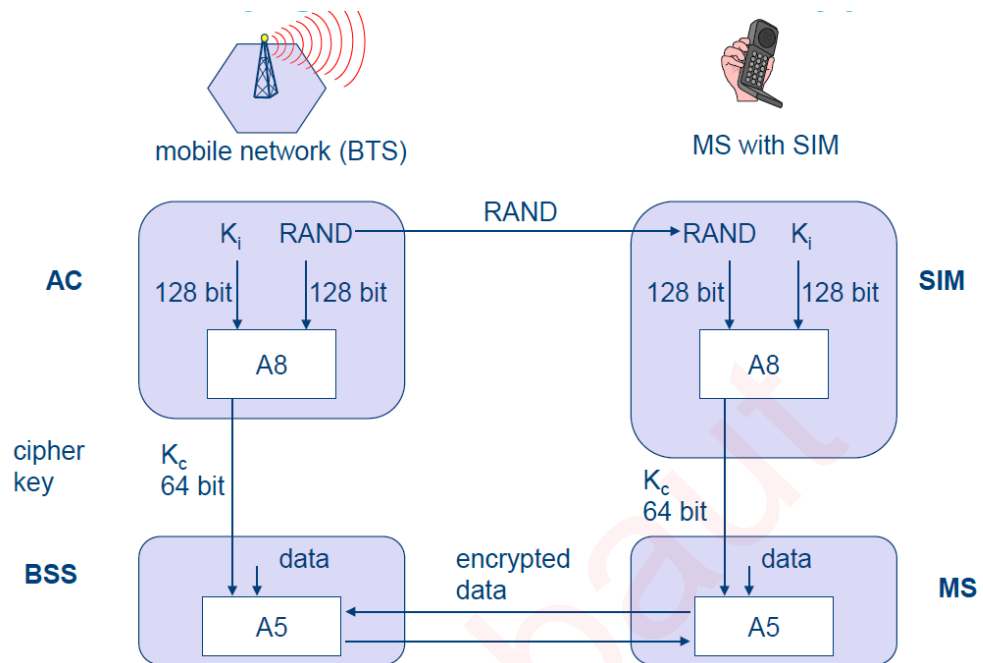


Figuur 13: Authenticatie procedure in een GSM netwerk
AC (Access control) - SRES (Signed response) - K_i (individual key)

- Na het signen van de challenge wordt deze vergeleken in de VLR

Encryptie

- Na authenticatie kunnen het MS en de BSS starten met encryptie
- K_c is gegenereerd uit de K_i en een random waarde (die wordt meegedeeld met de MS) via A8 (in de AuC)
- Encryptie/decryptie gebeurt a.d.h.v. A5



Figuur 14: Encryptie in het GSM netwerk

2.1.8 Nieuwe data services

High Speed Circuit
Switched Data (**HSCSD**)

AIUR >

▷ HSCSD:

- Vooral software update
- Meerdere time-slots samen nemen om een hogere AIUR (Air Interface User Rate) te verkrijgen
- De allocatie kan asymmetrisch zijn (down- vs uplink)
- Probleem: zenden en ontvangen op hetzelfde moment (MS)

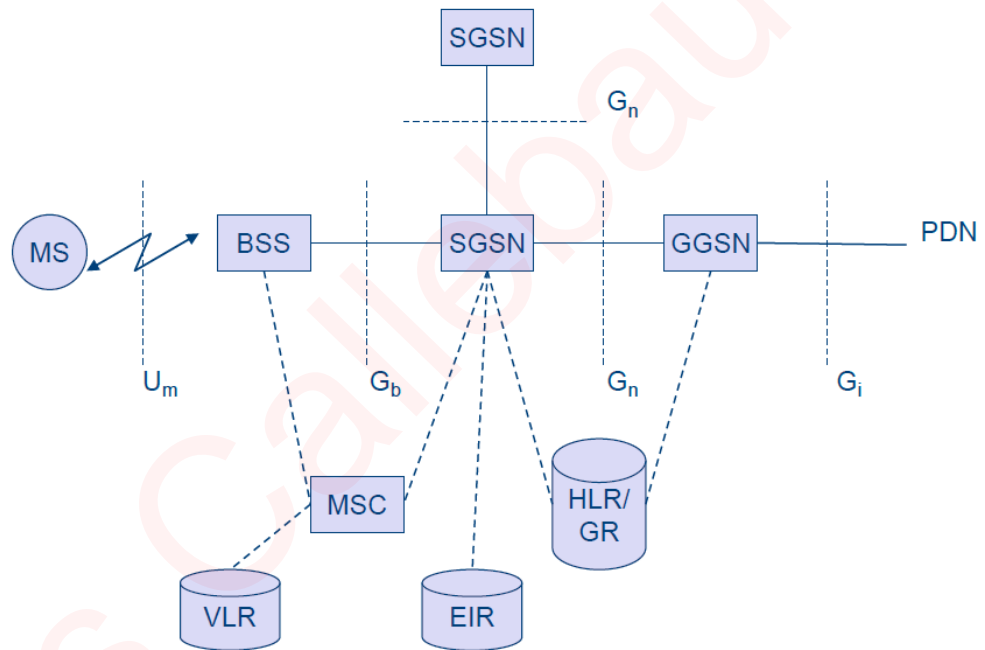
General Packet Radio
Service (**GPRS**)

GPRS

- Packet switching
- Gebruik maken van free slots enkel als de data pakketten klaar zijn om te verzenden
- Meer efficiënt gebruik van bronnen voor *packet oriented services*
- Kosten zijn nu gerelateerd aan data volume
- 'Always on': er moet geen connectie worden opgezet om data te versturen

GPRS' algemene concepten:

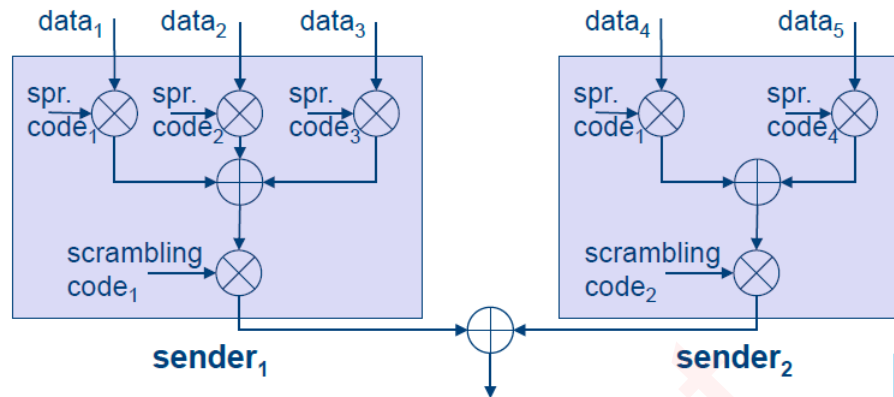
- De operator wijst tussen 1 en 8 timeslots in een frame toe aan GPRS (aantal is afhankelijk van operator)
- GPRS timeslots worden gedeeld door alle actieve gebruikers (het aantal is niet op voorhand vastgelegd maar wordt toegewezen 'on demand')
- Up- en downlink timeslots worden gealloceerd onafhankelijk van elkaar
- Alle GPRS diensten lopen in parallel met de conventional GSM services
- GPRS voorziet enkele code schemes die een trade-off maken tussen data rates en error rates
- GPRS kan een QoS profiel specificeren



Figuur 15: GPRS architectuur en interfaces

Componenten in GPRS:

- GSN (GPRS Support Nodes)
 - GGSN (Gateway GPRS support Node)
GPRS netwerk ↔ externe PDN (packet Data Networks)
 - SGSN (Serving GPRS Support Node)
Ondersteunen van de MS via de G_b -interface
- GR (GPRS register)
Houdt individuele MS' locatie bij (user addresses), aanvullen met IP-adressen



Figuur 16: Spreading en scrambling van gebruikersdata
 Spreading codes zullen de chipping rate veranderen ($3.84 \text{ Mchips/s} = 5 \text{ MHz}$)
 Scrambling codes zullen de BB niet opdrijven

2.2 UMTS

Spreading en scrambling van gebruikersdata

▷ In UMTS wordt er dus gebruik gemaakt van CDMA i.p.v. FDMA/TDMA zoals in 2G (GSM).

Er wordt gebruik gemaakt van twee code:

1. Spreading codes

- Scheiden van datastromen afkomstig van eenzelfde zender (multiplexeren van data binnen eenzelfde bron)
- Verschillende gebruikersdata snelheden toegelaten door verschillende SF's
- Spreading codes zijn orthogonaal (OVSF)

2. Scrambling codes

- Onderscheiding maken tussen zenders via quasi orthogonale codes
- Gemakkelijk beheer van codes: elk station kan dezelfde codes gebruiken
- Precieze synchronisatie is niet nodig

In feite moet er een onderscheid gemaakt worden tussen de processing gain en de spreidingsfactor. De processing gain bevat alle factoren die zorgen voor een vergroting van de bandbreedte. Hierin zit niet alleen de spreidingsoperatie, er kunnen ook andere bewerkingen tussen de brondata en de uitgezonden data zijn die bijdragen tot de vergroting van de bandbreedte. Foutcorrectiecodes bijvoorbeeld zijn ook vervat in de processing gain. De spreidingsfactor daarentegen is het aantal chips dat per databit gebruikt wordt. De spreidingsfactor heeft dus enkel te maken met de spreidingsoperatie op zich. De processing gain is gekoppeld met

de mogelijkheid van een CDMA-systeem om de interferentie met andere signalen te onderdrukken.

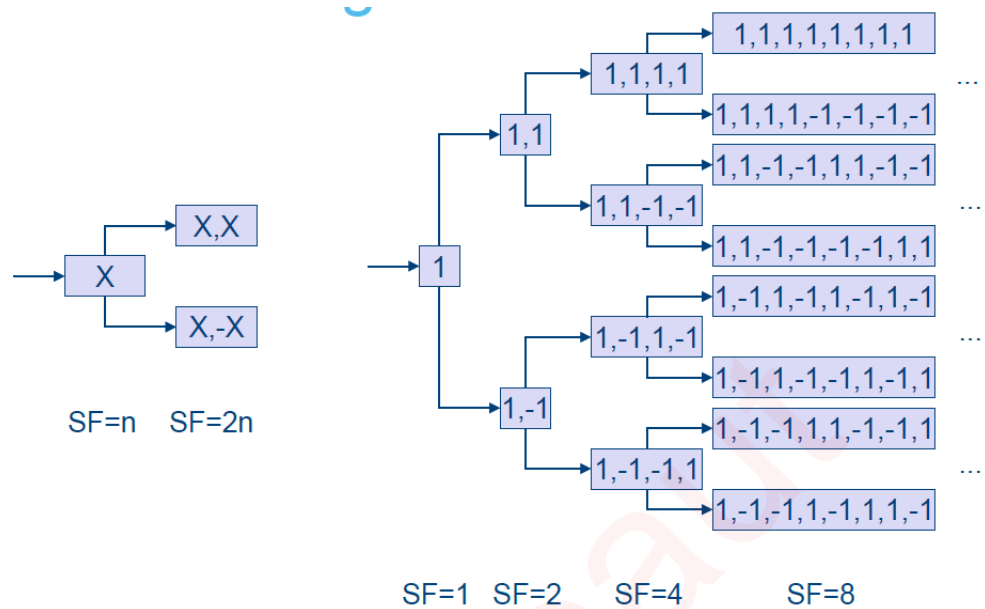
In UMTS wordt een vaste chiprate van 3.84 Mchips per seconde gebruikt. Dit levert bij de gebruikte modulatievorm een benodigde bandbreedte van 5 MHz op. Sommige tweede generatiesystemen zoals IS-95 gebruikten ook al CDMA-technieken, maar met een veel kleinere chiprate, vandaar de naam Wideband CDMA in UMTS. Een spraaktoepassing met een bitrate van 12.2 kbps heeft dan een processing gain van $25 \text{ dB} = 10 \log(3.84e6/12.2e3)$. Na de despreading moet het signaalvermogen typisch enkele dB boven het ruis- en interferentievermogen liggen. Stel dat voor het spraaksignaal na de despreading een E_b/N_o van 5 dB nodig is (E_b de energie per databit en N_o de ruis en interferentievermogendichtheid). Dan mag het gespreide breedbandsignaal een signaal-tot-interferentieverhouding (SIR, Signal-to-Interference Ratio) van 5 dB min de processing gain hebben, wat gelijk is aan -20 dB . Met andere woorden het signaalvermogen kan 20 dB onder het ruis- en interferentievermogen zitten en toch kan de ontvanger het signaal nog detecteren. Omdat het breedbandsignaal onder het niveau van de thermische ruis kan zitten, is het moeilijk te detecteren zonder de kennis van de juiste spreidingssequentie. Dit is de reden waarom de spread spectrum systemen hun oorsprong vinden in militaire toepassingen.

OSVF

Orthogonal Variable
Spreading Factor (OVSF)

▷ SF codes zijn orthogonaal met alle andere codes met uitzondering die uit eigen tak.

Stel twee signalen met verschillende bit-rates, door het toepassen van OVSF codes met verschillende SF (Spreading Factor) kan men eenzelfde chip snelheid verkrijgen.



Figuur 17: Generatie van OSVF

2.2.1 WCDMA

Wideband CDMA
(**WCDMA**)

▷ W-CDMA (of UTRA FDD) gebruikt de DS-SS channel access methode met een paar van kanalen met een breedte van 5 MHz. Er wordt gebruik gemaakt van tijdsloten van 10 ms voor periodieke functies en niet voor TDM.

Uplink

- De datastroom in de uplink bestaat uit een reeks verschillende logische kanalen: data en signaling. De data heeft een hogere bitrate en heeft dus een kleinere spreadingsfactor nodig.

De signaling (met zijn controle kanalen) worden gemultiplexed met de data stroom via spreading codes.

- De bronnen worden van elkaar gekoppeld door scrambling codes.

DPCCH, DPDCH ▷

De uplink DPCCH (Dedicated Physical Control Channel) en uplink DPDCH (Dedicated Physical Data Channel), de controle en data kanalen worden gemultiplexed via spreading codes.

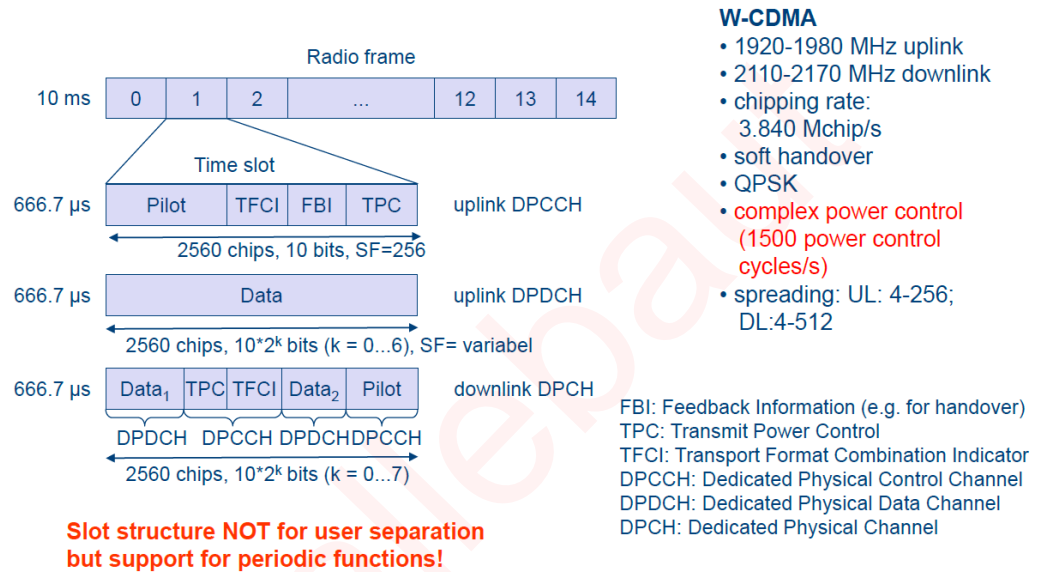
Downlink

- Onderscheiden van de verschillende antennes gebeurt via scrambling codes

- De verschillende stromen van één antenne naar meerdere apparaten wordt gemultiplexed via spreading codes
- Eén enkele stroom (per toestel) bestaat uit data en signaling die via TDM wordt gemultiplexed.

DPCCH, DPDCH ▷

De downlink DPCH (Dedicated Physical Channel) gebruikt TDM om controle- en gebruikersdata te multiplexen.



Figuur 18: UMTS FDD frame structuur

UTRAN architectuur

UMTS Terrestrial Radio Access (**UTRA**)

▷ UMTS ondersteunt enkele verschillende *terrestrial air interfaces*, i.e. UMTS Terrestrial Radio Access (UTRA).

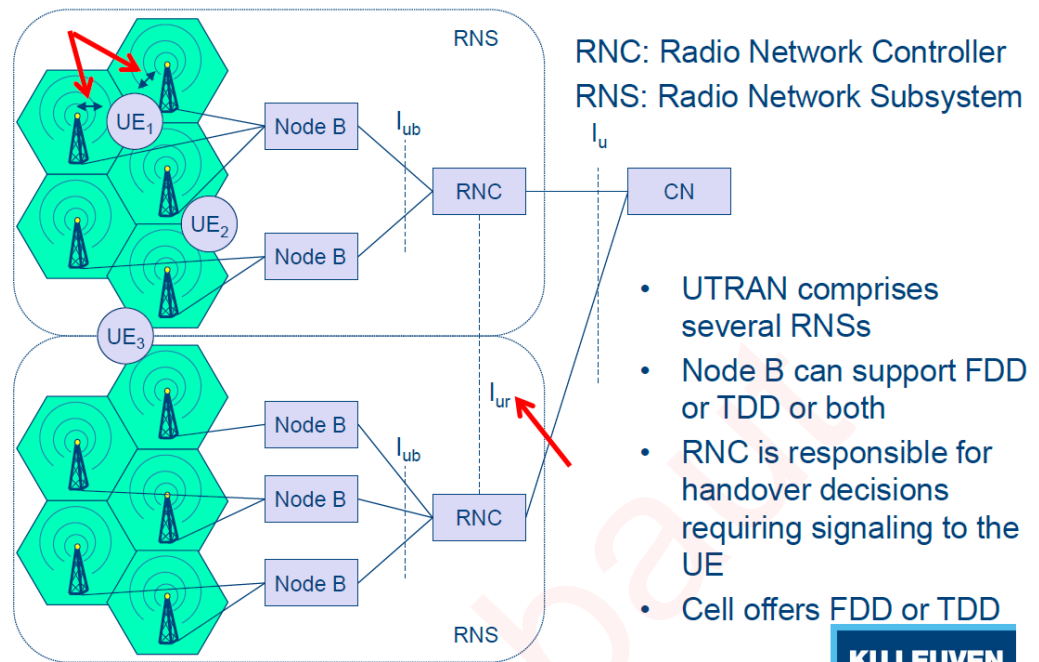
Er zijn enkele verschillen op te merken tussen UMTS en GSM

- Communicatie met meerdere stations tegelijkertijd is mogelijk
- De BSC (van GSM), hier RNC's (Radio Network Controller) kunnen onderling ook verbonden zijn. Hierdoor kunnen handovers direct worden geregeld. In tegenstelling tot GSM waarbij een handover verliep over de MSC.

RNC ▷

UTRAN functies

- RNC
 - Call administration control
 - Congestion control
 - Radio channel encryption



Figuur 19: UTRAN architectuur
De rode pijlen wijzen op de verschillen met GSM

- System information broadcasting
- Multiplexing and protocol conversions
- Radio resource control
- Outer loop power control (minimaliseren van interferentie tussen naburige cellen of de grootte van de cel controleren)
- Handover and RNS relocation (dit is het geval als een UE zich buiten de range bevindt van een RNC, en een nieuwe RNC moet worden aangesteld)
- Node B
 - Connectie met één of meerder antennes (i.e. cellen)
 - Inner loop power control
 - Softer handover

Core netwerk architectuur

Core Network(CN)

▷ Het CN is opgesplitst in twee logische domeinen:

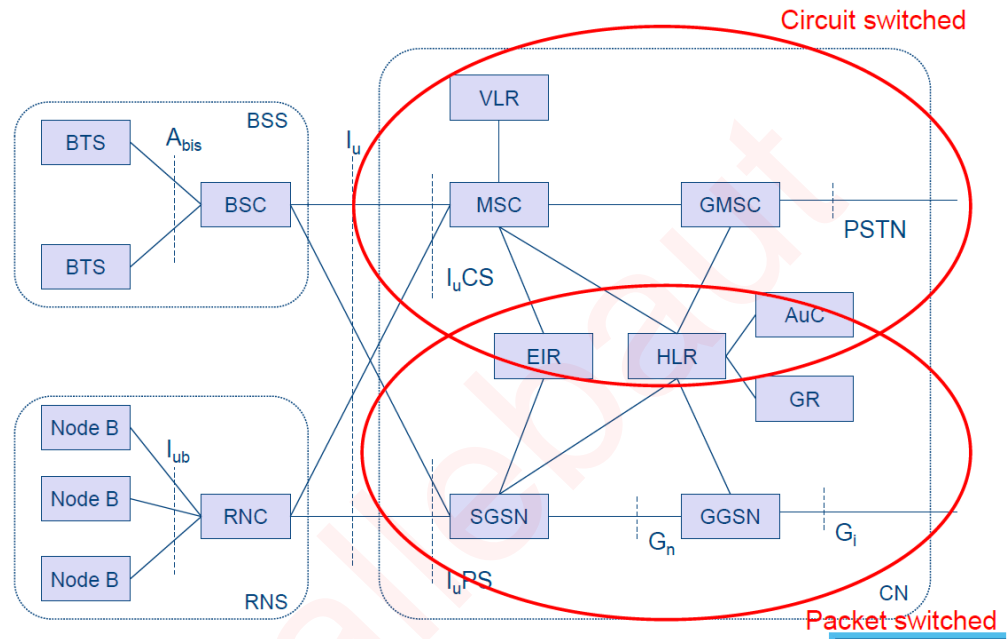
CSD ▷

1. Circuit Switched Domain (CSD)

- Circuit switched diensten inclusief signaling

PSD ▸

- Resource reservatie bij connectie setup
 - GSM componenten (MSC, GMSC, VLR)
2. Packet Switched Domain (PSD)
- GPRS componenten (SGSN, GGSN)



Figuur 20: Core netwerk architectuur

Ondersteuning van mobiliteit - Handover

Hard handover Switching gebeurt tussen verschillende antennes of verschillende systemen op een bepaald ogenblik. ULTRA TDD kan enkel harde handovers maken en geen soft handovers.

Inter frequency handover veranderen van carrier frequency

inter system handover veranderen tussen systemen (e.g. GSM ↔ IMT-2000)

Soft handover Dit is enkel mogelijk in UTRA FDD mode.

En maakt gebruik van *macro diversity*. een UE kan signalen ontvangen van drie verschillende antennes (die eventueel verspreidt liggen over meerdere node B's). Hierdoor kunnen overgangen naar andere cellen doorgaan zonder het proces te moeten stoppen. Dit is verborgen voor de CN.

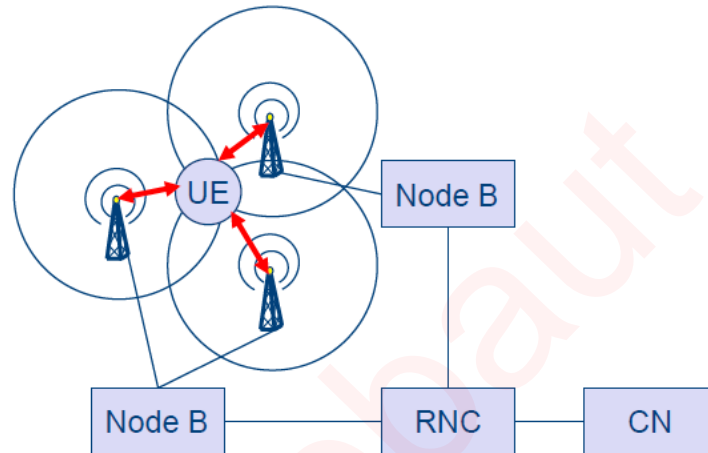
Uplink

- Gelijktijdige ontvangst van UE data in verschillende node B's

- Reconstructie van de data in de RNC

Downlink

- Gelijktijdige transmissie van data via de verschillende cellen
- Verschillende spreading codes in verschillende cellen



Figuur 21: Macro diversiteit

Eén RNC beheert de connectie en zendt de data naar de CN, maar de CN is niet op de hoogte van de parallelle connecties. Wanneer een soft handover moet gebeuren tussen twee node B's die niet dezelfde CN hebben wordt de volgende procedure gevormd (zie Figuur 22 op de pagina hierna):

SRNC ▷

- De RNC die de data verstuurd van en naar de CN wordt de SRNC (serving RNC) genoemd

DRNC ▷

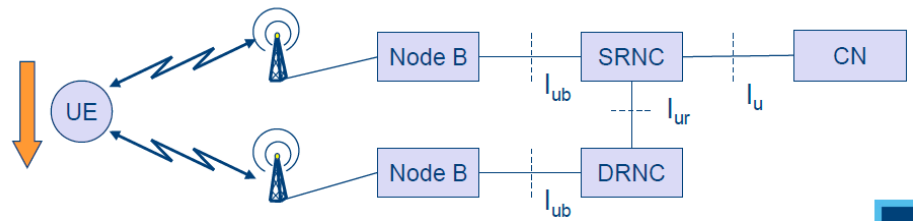
- De nieuwe RNC wordt de DRNC (Drift RNC)
- Data die wordt opgevangen door de DRNC wordt doorgestuurd naar de SRNC
- SRNC combineert beide datastromen en stuurt deze naar de CN (die van niets op de hoogte is)

SRNC relocation ▷

Als de UE nog meer naar beneden zakt en niets meer verzendt naar de SRNC dan moet een SRNC relocation uitgevoerd worden, i.e. de DRNC wordt de nieuwe SRNC. Hierdoor moet de CN op de hoogte gebracht worden (door de oorspronkelijke SRNC) en spreekt men dus van een harde handover.

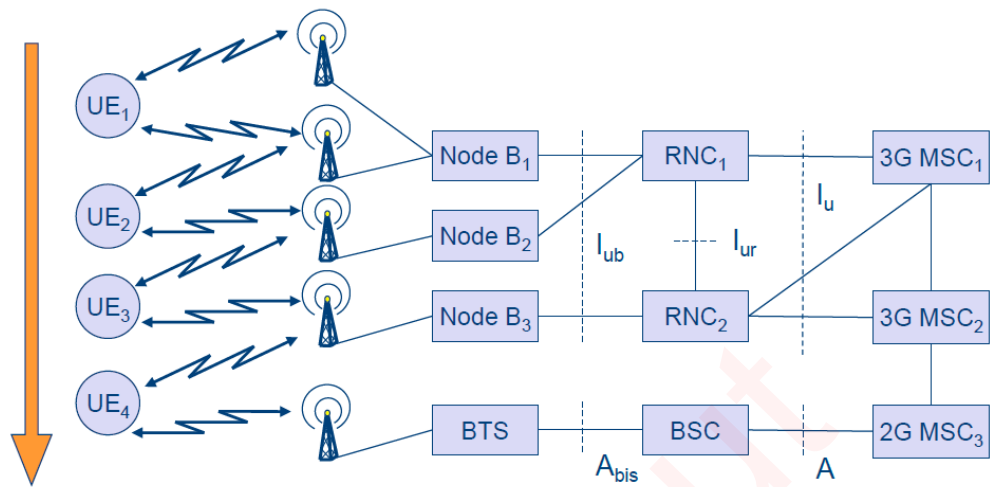
Verschillende types van handover in UMTS:

- Soft handover



Figuur 22: Soft handover in een UTRA netwerk

- Intra-node B, intra-RNC
 UE_1 wisselen tussen verschillende antennes binnen eenzelfde Node B
- Inter-node B, intra-RNC
 UE_2 verplaatst zich van Node B_1 naar B_2 , waarbij deze nodes vallen onder eenzelfde RNC, nl. RNC_1
- Soft of hard handover
 - inter-RNC
 UE_3 verplaatst zich van node B_2 naar node B_3
 1. internal inter-RNC: RNC_1 kan zich gedragen als $SRNC$ en RNC_2 als de $DRNC$. Hierbij moet de CN niet op de hoogte gebracht worden en spreekt men dus van een soft handover.
 2. external inter-RNC: Relocatie van de controlling RNC, de interface I_u is verplaatst en is dus een harde handover.
- Hard handover
 - inter-MSR
 MSC_2 neemt in dit geval de controle over
 - inter-system
 UE_4 verplaatst zich van een 3G UMTS naar een 2G GSM netwerk



Figuur 23: Voorbeeld handover types in UMTS/GSM

Breathing Cells

- GSM
 - Mobiele apparaten krijgen exclusieve signalen van de base station
 - Aantal devices in een cel beïnvloed niet de grootte van die cel
- UMTS
 - Cel grootte cel capaciteit
 - Signal-to-Noise ratio bepaalt de cel capaciteit
 - Noise wordt gegenereerd door interferentie van:
 - * Andere cellen
 - * Andere gebruikers in de cel (Opstapeling schijfjes → kan niet meer volledig worden weggefilterd)
 - De interferentie-level vergroot het noise level
 - Apparaten op de buitenste ring van de cel hebben geen power genoeg om de base station te bereiken en vallen dus uit de cel
 - Er is dus een limitatie van maximale hoeveelheid gebruikers

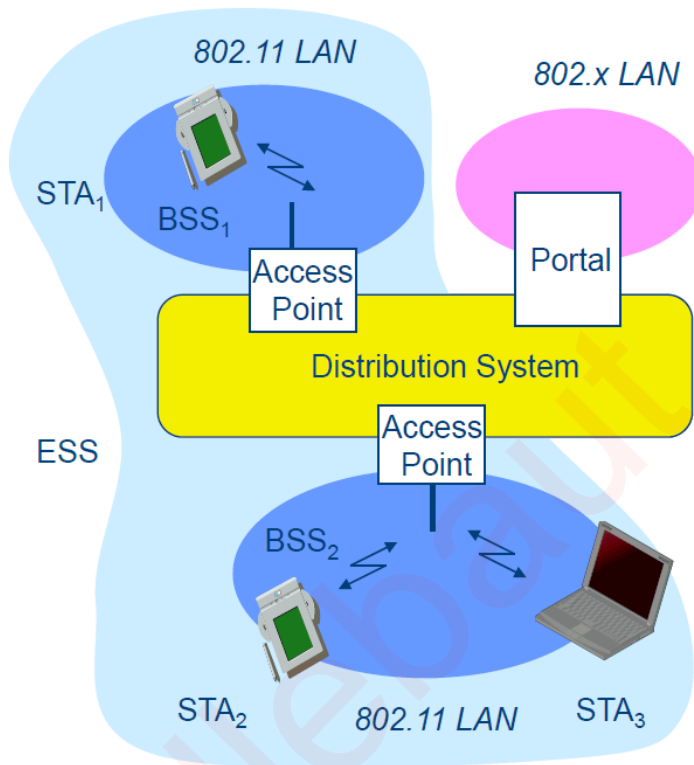
3 H7: Draadloos LAN

3.1 WiFi

WiFi ▷ WiFi is een WLAN (Wireless version of LAN) gebaseerd op IEEE 802.11. IEEE beschrijft de fysische en MAC-laag.

3.1.1 Architectuur van een infrastructuur netwerk

- STA ▷ • Station (STA)
- Terminal met toegang mechanismen tot het wireless medium en radio contact met het access point
- BSS ▷ • Basic Service Set (BSS)
- Groep van stations die dezelfde radio frequentie gebruiken
- Access Point (AP)
- Station die is geïntegreerd in het WLAN en het gedistribueerd systeem
- Portal
- Brug naar andere (wired) netwerken
- Distributed System
- ESS ▷ – Interconnectie netwerk om één logisch netwerk (ESS: Extended Service Set) op te bouwen gebaseerd op enkele BSS'en
- Layer 2 connectie
- In de praktijk is dit vaak een Ethernet LAN, waarbij AP fungeert als een Ethernet Bridge



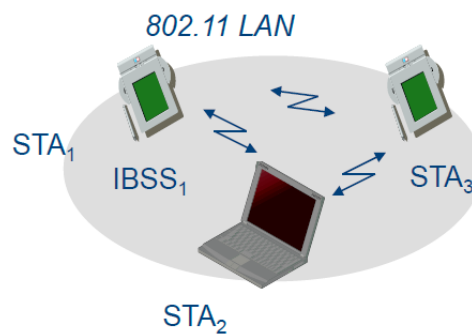
Figuur 24: 802.11 - Architectuur van een infrastructuur netwerk

3.1.2 Architectuur van een adhoc netwerk

Directe communicatie tussen de toestellen met een gelimiteerd bereik.

- Station (STA)
- Independent Basic Service Set (IBSS)
 - Groep van stations die dezelfde radio frequentie gebruiken

IBSS ▷



Figuur 25: 802.11 - Architectuur van een ad-hoc netwerk

3.2 IEEE 802.11

3.2.1 Lagen en functies van IEEE 802.11

- MAC
 - access mechanisms, fragmentation, encryption
- MAC Management
 - authentication, synchronization, roaming, MAC MIB (management information base), power management
- PLCP (Physical Layer Convergence Protocol)
 - clear channel assessment signal (carrier sense)
- PMD (Physical Medium Dependent)
 - modulation, coding
- PHY Management
 - channel selection, PHY MIB (management information base)
- Station Management
 - coordination of all management functions (e.g. interaction with distribution system)

DLC	LLC		Station Management
	MAC	MAC Management	
PHY	PLCP	PHY Management	
	PMD		

Figuur 26: 802.11 - Lagen en functies

3.2.2 Physical layer of IEEE 802.11

- 3 versies
 - 2 lagen gebaseerd om radio transmissie (voornamelijk in de 2.4 GHz band)
 - 1 IR

CCA ▷

- Alle PHY versies geven een CCA (Clear Channel Assessment) signaal aan de MAC om te weten of het medium ilde is

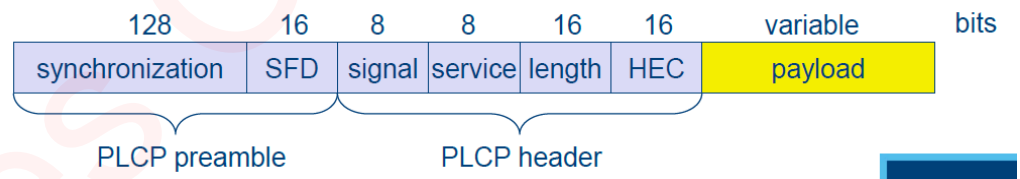
- FHSS
- DSSS (enkel voor robuustheid niet voor multiplexering)
- IR

3.2.3 DSSS PHY packet format

SFD ▷

- Synchronization
 - synch., gain setting, energy detection (CCA), frequency offset compensation
- SFD (Start Frame Delimiter)
 - 1111 0011 1010 0000
- Signal
 - data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service (future use)
- Length (lengte van de payload)
- HEC (Header Error Check)
 - Signal, service en lengte wordt beschermd via deze checksum d.m.v. een standaard polunomial ($x^{16} + x^{12} + x^5 + 1$)

HEC ▷



Figuur 27: DSSS PHY packet format in IEEE 802.11

3.2.4 De MAC laag in IEEE 802.11

IEEE 802.11 ondersteunt twee trafiek diensten waarvan er maar één in de praktijk wordt gebruik.

Asynchronous Data Service (Trafiek dienst)

- Uitwisselen van data pakketten gebaseerd op "best-effort"
- Ondersteuning voor broadcast en multicast

DFWMAC ▷

Binnen IEEE 802.11 zijn er drie access methodes gedefinieerd. Deze mechanismen worden ook DFWMAC (Distributed Foundation Wireless MAC) genoemd, hierbij slaat 'Distributed' op de afwezigheid van een centraal controle mechanisme.

DFWMAC (Access methodes)

DFWMAC-DCF
CSMA/CA ▷

1. DFWMAC-DCF CSMA/CA (mandatory) (DCF=Distributed coordination function)

- collision avoidance via randomized "back-off" mechanism
- minimum distance between consecutive packets
- ACK packet for acknowledgements (not for broadcasts)

DFWMAC-DCF w/
RTS/CTS ▷

2. DFWMAC-DCF w/ RTS/CTS (optional)

- avoids hidden terminal problem

DFWMAC- PCF ▷

3. DFWMAC- PCF (optional) (PCF=Point coordination function)

- access point polls terminals according to a list

Alle access methoden berusten op dezelfde parameters voor controle van de wachttijden voor medium access. Deze zijn ontworpen voor prioriteiten toe te kennen aan het verzenden van pakketten.

- Dit door het definiëren van verschillende inter frame spaces
- Geen garantie, harde prioriteiten

SIFS ▷

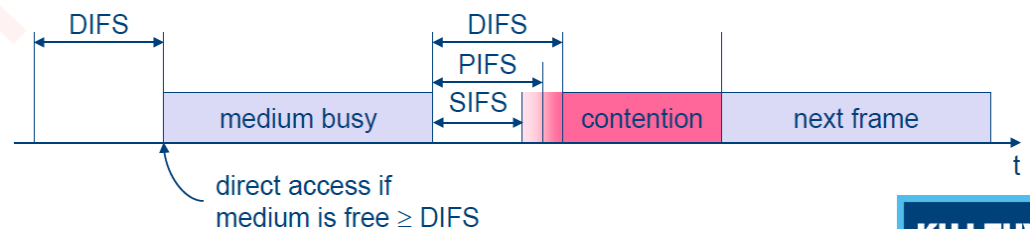
- SIFS (Short Inter Frame Spacing)
 - highest priority, for ACK, CTS, polling response (korte controle signalen)

PIFS ▷

- PIFS (PCF IFS)
 - medium priority, for time-bounded service using PCF

DIFS ▷

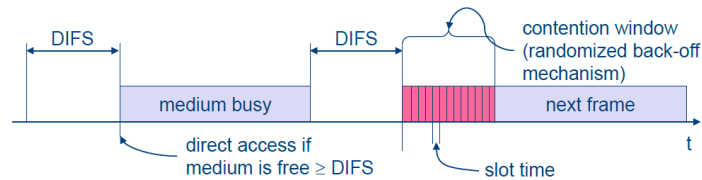
- DIFS (DCF, Distributed Coordination Function IFS)
 - lowest priority, for asynchronous data service



Figuur 28: MAC prioriteiten in IEEE 802.11
Medium bussy wordt gedetecteerd door de CCA In de contention periode zullen nodes proberen om het medium te accessen

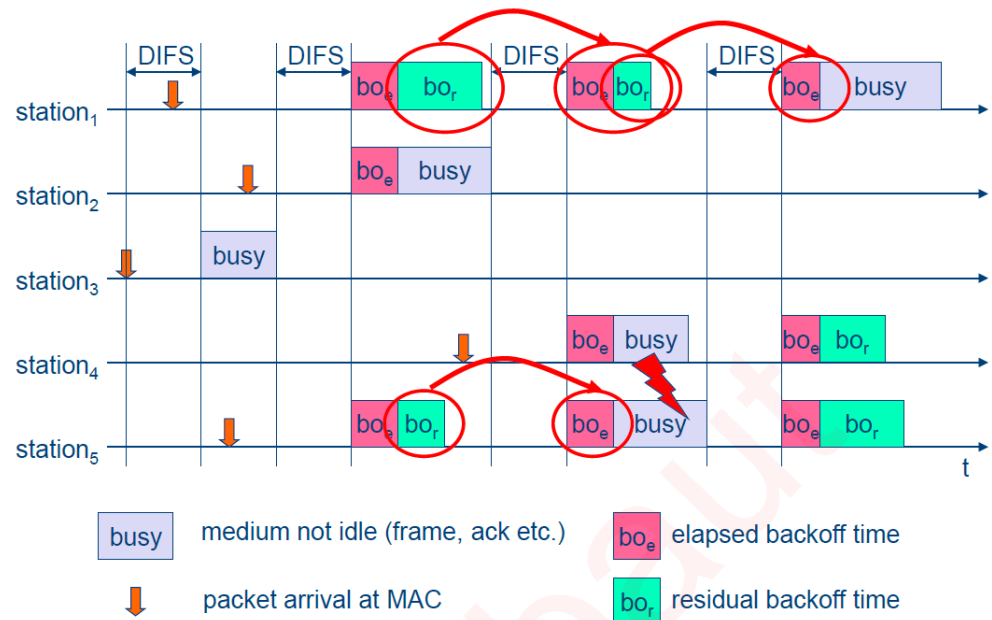
(1) CSMA/CA access methode in MAC laag van IEEE 802.11

▷ CSMA/CA:



Figuur 29: CSMA/CA access methode (1) in MAC laag

- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)
- Windows is variabel, hoe meer collisions hoe groter het window. Als het medium vaak onbezet is zal de window terug verkleinen.

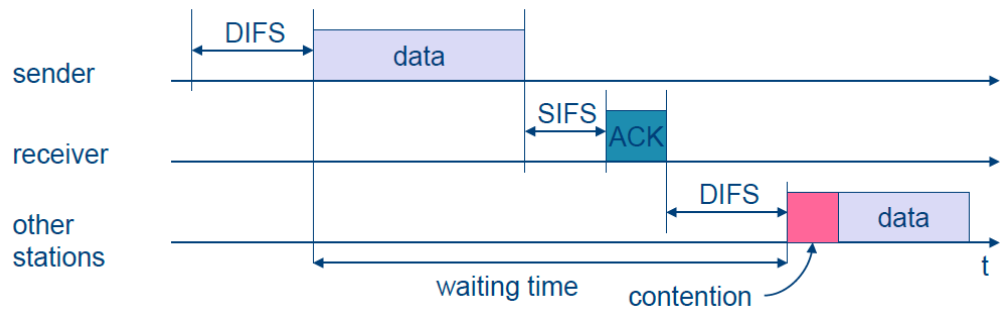


Figuur 30: CSMA/CA competing stations

Voor fairness wordt er geen nieuwe random b_0 gestart maar de backoff timer verloopt gewoon verder. Bij botsing wordt er een nieuwe random gegenereerd. Het collision window start met een minimale lengte, als er een botsing gebeurt dan verdubbelt het window in grootte. Dit noemt men exponential backoff.

Wanneer we unicast berichten willen verzenden moet er ook nog een *ACK* worden teruggestuurd.

- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (correcte checksum CRC bij de ontvanger)
- automatic retransmission of data packets in case of transmission errors



Figuur 31: CSMA/CA competing stations

Het verzenden van data en het ontvangen van de ACK vormt een atomische operatie, een atomisch geheel, vermits het direct kan sturen achter SIFS in tegenstelling tot de rest van de pakketten die DIFS moeten wachten plus een additionele random wachttijd.

(2) DFWMAC-DCF with RTS/CTS access methode in MAC laag van IEEE 802.11

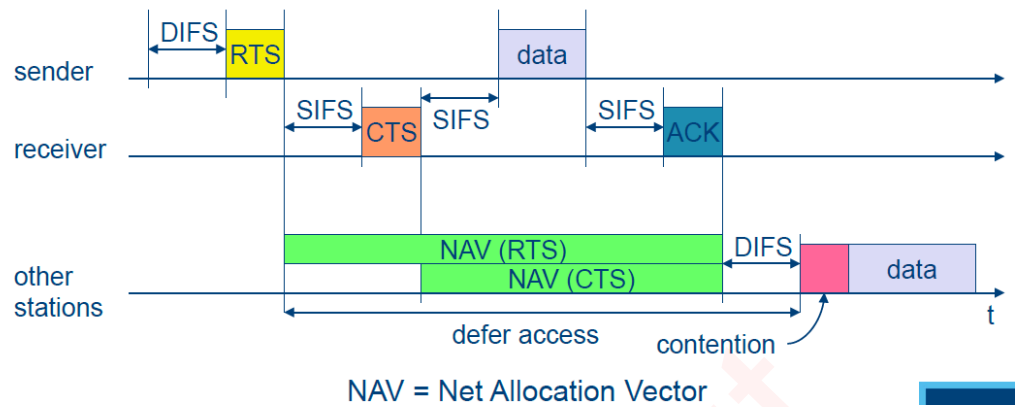
DFWMAC-DCF with
RTS/CTS

▷ DFWMAC-DCF in combinatie met RTS/CTS lost het probleem op van hidden terminals. Dit probleem komt voor als een station twee andere kan ontvangen, maar die twee stations elkaar niet kunnen ontvangen.

Zenden van unicast pakketten

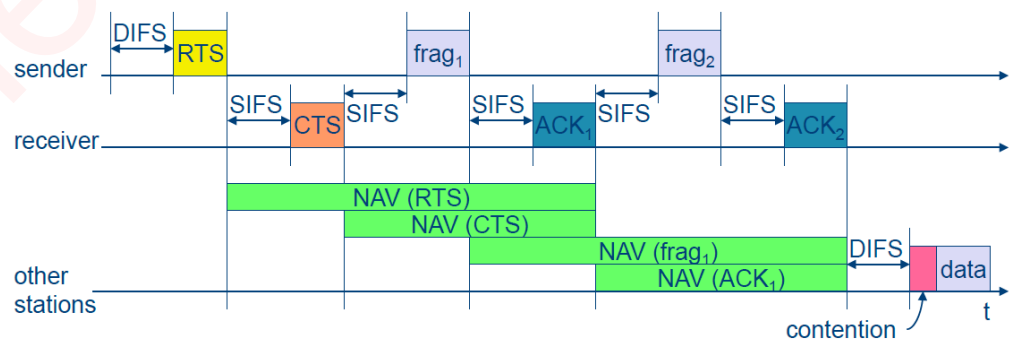
NAV ▷

- station can send RTS with reservation parameter (NAV - Net Allocation Vector) after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS (again with reservation parameter) after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS



Figuur 32: DFWMAC-DCF met RTS/CTS

Fragmentatie Als het netwerk onbetrouwbaar is, is de kans groot dat pakketten worden verloren, waardoor deze opnieuw moeten worden verzonden. Daarom zenden we beter kleinere pakketten (fragmenteren) i.p.v. lange pakketten.



Figuur 33: DFWMAC-DCF met RTS/CTS in fragmentation mode
De NAV zal nu ook in de fragment pakketten en de verschillende ACK's zitten

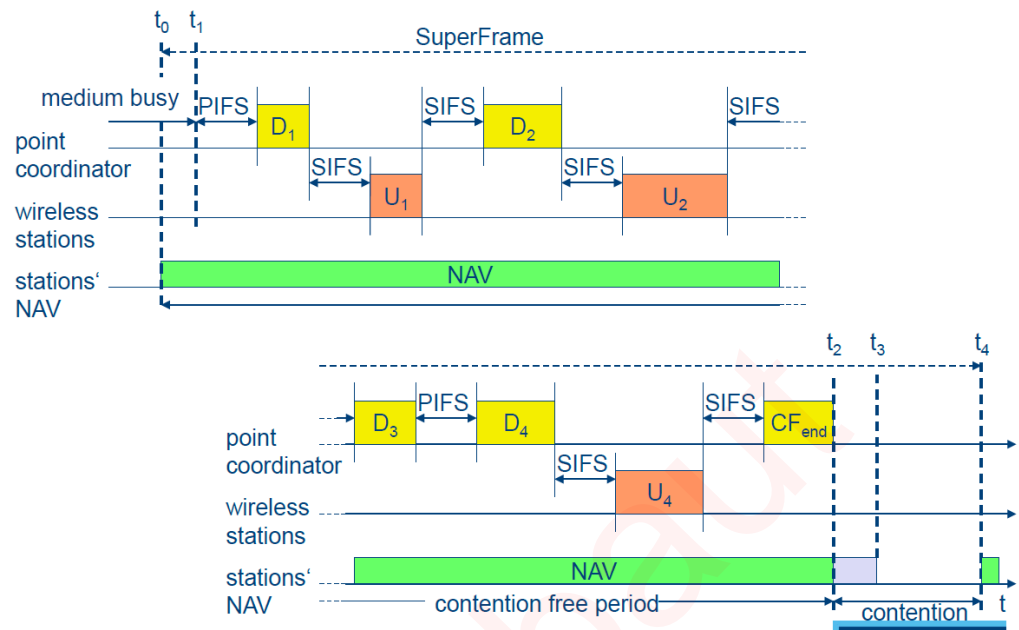
(3) DFWMAC-PCF access methode in MAC laag van IEEE 802.11

▷ De vorige twee mechanismen kunnen geen maximum access delay of minimum transmissie BB garanderen. In DFWMAC-PCF zal het AP de rol nemen van centrale coördinator die de nodes zal pollen. Hierbij wordt PCF geboden boven DCF mechanismen.

- De point co-ordinator splitst de access time in super frame periodes
- Superframe bestaat uit:
 - Contention free period
 - Contention period
- De contention periode kan worden voor de twee bovenvermelde access methodes

Uitleg bij Figuur 34 op de volgende pagina:

- De contention free period van de superframe zou moeten starten op t_0 dit is echter niet mogelijk doordat het medium bezet is. De PCF wordt uitgesteld door de DCF, de start van het superframe wordt uitgesteld.
- Coördinator moet *PIFS* wachten om het medium te verkrijgen ($PIFS < DIFS$, geen ander station eerst).
- De coördinator zend (downstream) D_1 naar het eerste station die kan antwoorden achter *SIFS* (upstream)
- De coördinator wacht weer *SIFS* voor een andere station te pollen
- Als een station niets te zeggen heeft (en dus niets terugstuurt), wacht de coördinator *PIFS* alvorens een ander station te ondervragen
- De coördinator sluit af met CF_{end} om het einde te verkondigen van de contention-free periode
- Normaal was er via de NAV gezet dat de periode zou duren tot t_3 maar via de CF_{end} begint deze al vanaf t_2

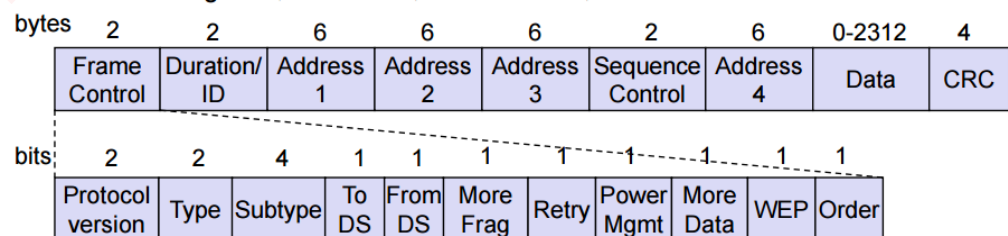


Figuur 34: DFWMAC-PCF

Zorgen dat interactieve zaken in de superframe gebeuren vermits er een gegarandeerde timing is. Dit is vergelijkbaar met een TDMA systeem met TDD transmissie.

802.11 - Frame formaat

- Duration
 - for NAV with RTS/CTS and fragmentation
- Addresses
 - 48 bit MAC addresses: receiver, transmitter (physical), BSS identifier, sender (logical), depend on DS-fields (see further)
- Sequence numbers
 - important against duplicated frames due to lost ACKs



Figuur 35: 802.11 - Frame formaat

- Types
 - control frames (RTS/CTS), management frames (Beacons), data frames
- Subtype
 - e.g. subtypes of management frames: 0000 association request, 1000 beacon
 - e.g. subtypes of control frames: 1011 RTS, 1100 CTS
- TO/From DS (zie verder)
- More frag
 - more fragments follow
- Retry
 - current frame is a retransmission of a earlier frame
- Power management
 - indicate status of a station after a successful frame transmission
- More data
 - sender has more packets available for receiver (e.g. AP signals to station in low power mode that more packets are available)
- WEP (Wired Equivalent Privacy) aan/uit
- Order
 - received frames must be processed in strict order

WEP ▷

DS ▷

Het frame bevat een aantal adressen die afhankelijk zijn van het DS (Distributed System). Er zijn vier mogelijke MAC adres formaten mogelijk:

1. Ad-hoc netwerk
DA en SA zijn identiek aan de physical receiver en sender
2. Infrastructuur netwerk (from AP)
DA is de logische en fysische ontvanger, SA is de logische zender, het source address van de MAC frame
3. Infrastructuur netwerk (to AP)
BSSID, is het fysieke ontvangers adres, het AP. SA is de logische en fysische zender van de frame en de DA is de logische ontvanger
4. Infrastructuur netwerk binnen DS
Dit is voor pakketten die tussen twee AP's over een gedistribueerde systeem worden verzonden. De RA is het MAC adres van de ontvangende AP en de TA is het zendende AP.

Afkortingen:

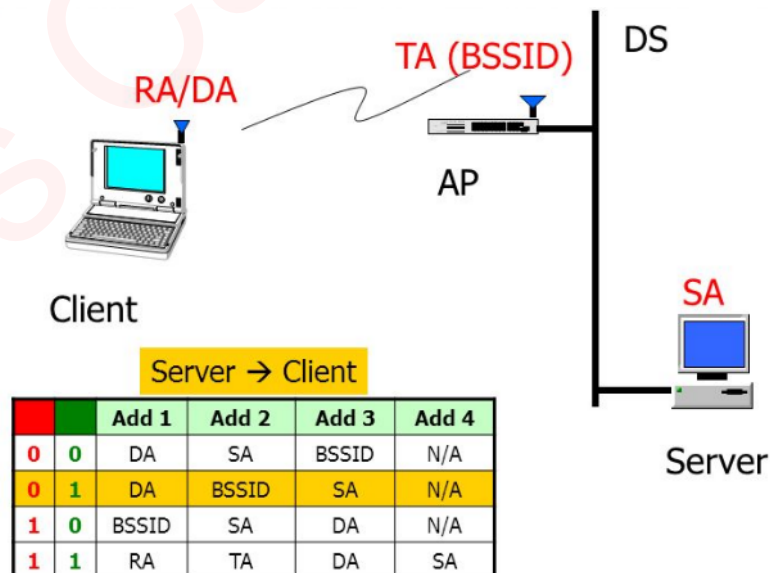
scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

Figuur 36: MAC address format

Adressen 1 en 2 zijn fysieke adressen en adressen 3 en 4 stelt de logische verbinding voor

Adres 1 is voor de ontvanger en adres 2 is voor de verzender, dit moet geweten zijn om een ACK te kunnen versturen.

- DS: Distribution System
- AP: Access Point AP: Access Point
- DA: Destination Address
- SA: Source Address
- BSSID: Basic Service Set Identifier
- RA: Receiver Address
- TA: Transmitter Address



Figuur 37: MAC address format

MAC management

- Synchronization
 - try to find a LAN, try to stay within a LAN
 - synchronisation of internal clocks, generations of beacons
- Power management
 - sleep-mode without missing a message
 - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
 - integration into a LAN
 - roaming, i.e. change networks by changing access points
 - scanning, i.e. active search for a network
- MIB - Management Information Base
 - managing, read, write (accessible via SNMP - Simple Network Management Protocol)
 - contain all information on current state of AP or station

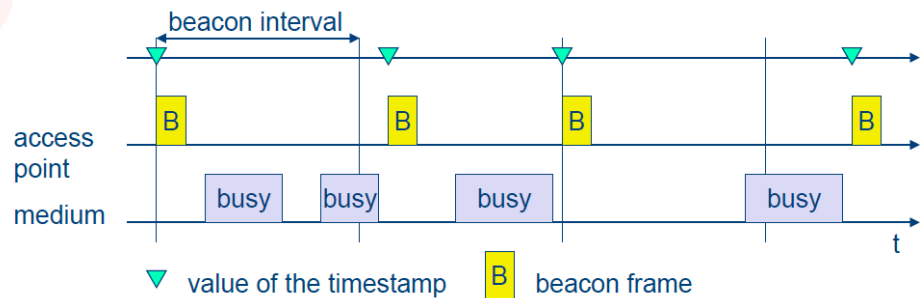
TSF ▷

MAC management - Synchronisatie Synchronisatie wordt gerealiseerd via een Beacon. Timing Synchronisation Function (TSF) is nodig voor:

- Power management
- PCF (superframe prediction)
- FHSS (hopping sequence)

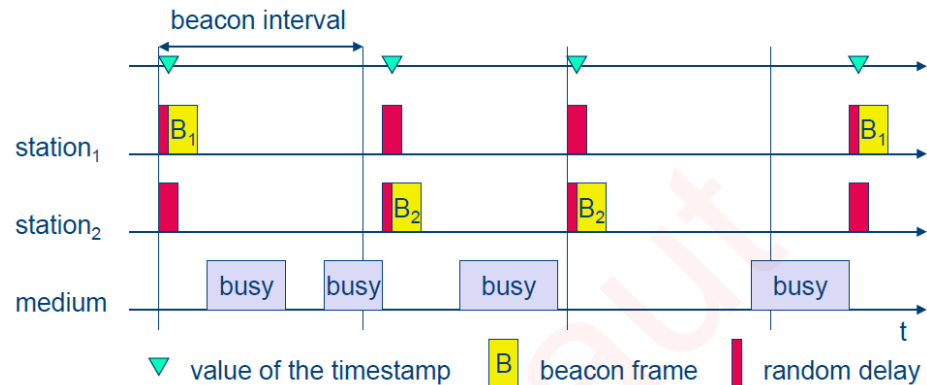
De beacons (time stamp + andere info) worden quasi periodisch verzonden.

- In een infrastructuur netwerk worden de beacons verzonden door de AP



- In een ad-hoc netwerk

- hebben alle stations een eigen synchronisatie klok.
- After beacon interval all stations start sending a beacon, random back-off applied so one beacons wins, all other stations adapt their clock and suppress the transmission of their beacon for this cycle



MAC management - Power Management

- Mobile means batteries \Rightarrow power saving is crucial
- Idea: switch the transceiver off if not needed
 - easy for transmitter, but for receiver ?
- States of a station: sleep and awake
Periodes afspreken van wanneer te slapen en wanneer wakker te zijn
- Data can be buffered at sender.
- Timing Synchronization Function (TSF)
 - stations wake up at the same time
 - sender informs the receivers if it has buffered data
 - these receivers stay awake

Power wordt dus bespaard via wake-up patterns

- Infrastructuur

- AP buffers all dataframes for stations using power saving
- Traffic Indication Map (TIM)

* Lijst van stations waarvoor unicast frames zijn opgeslagen in de AP

TIM \triangleright

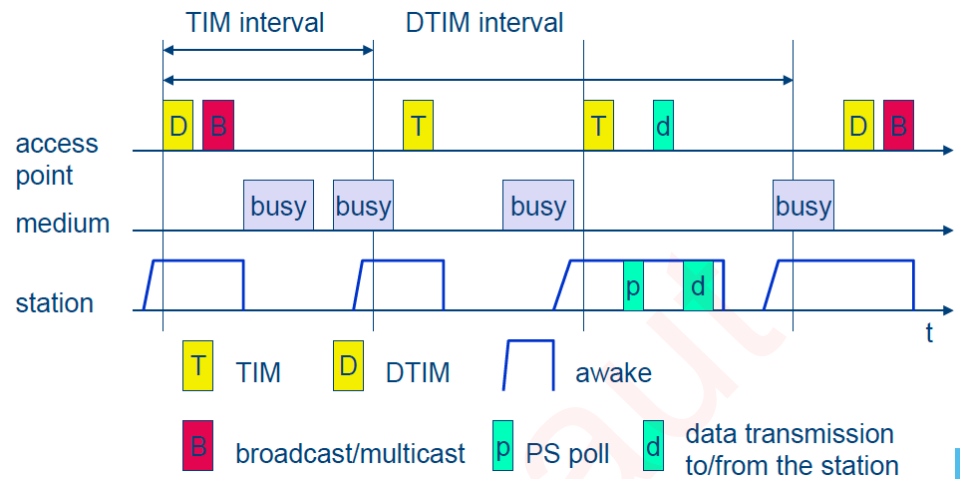
- Delivery Traffic Indication Map (DTIM)

* list of broadcast/multicast receivers transmitted by AP

DTIM \triangleright

PS ▷

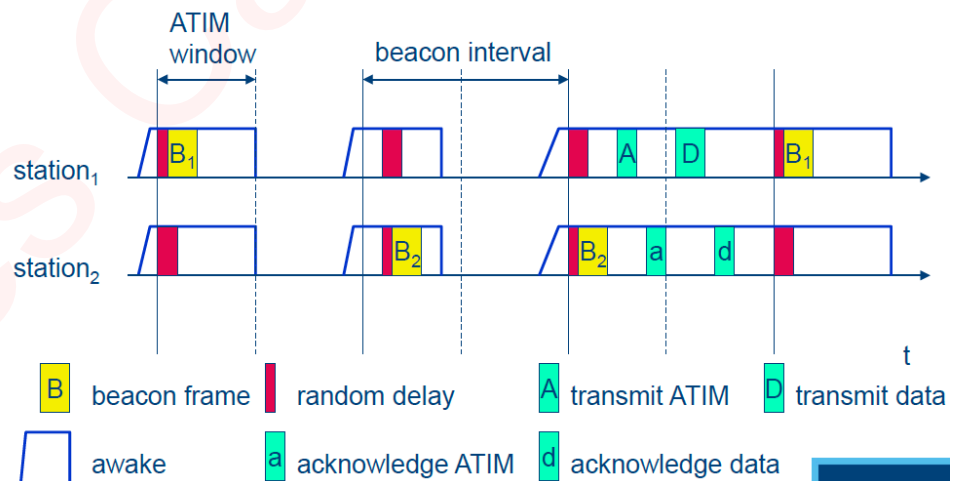
- Als de AP laat weten dat een station een pakket heeft, zal dat station een PS (Power Saving) poll sturen waarna het AP data verzend



- Ad-hoc

ATIM ▷

- Ad-hoc Traffic Indication Map (ATIM)
 - * announcement of receivers by stations buffering frames
 - * more complicated -no central AP
 - * collision of ATIMs possible (scalability?)



MAC management - Roaming No or bad connection? Then perform:

- Scanning
 - scan the environment, i.e., listen into the medium for beacon signals (passive scanning) or send probes into the medium and wait for an

answer (active scanning)

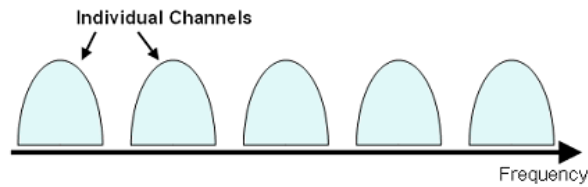
- Reassociation Request
 - station sends a request to one or several AP(s)
- Reassociation Response
 - success: AP has answered, station can now participate
 - failure: continue scanning
- AP accepts Reassociation Request
 - signal the new station to the distribution system
 - the distribution system updates its data base (i.e., location information)
 - typically, the distribution system now informs the old AP so it can release resources

3.2.5 Wijzigingen nieuwe IEEE 802.11 standaarden

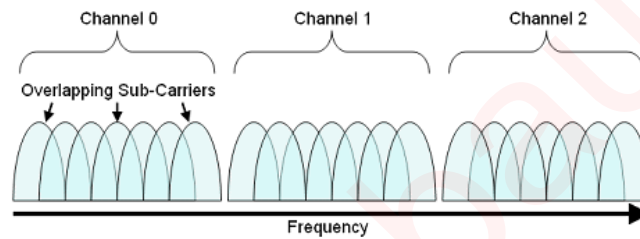
- IEEE 802.11b
 - Het fysieke frame formaat wordt aangepast voor de snelheid op te voeren:
 - Nieuw formaat met verkorte header
 - De PLCP header kan met een grotere snelheid worden verstuurd. De preamble blijft op 1 Mbit/s zodat andere (trage) stations dit ook kunnen lezen
- IEEE 802.11a
 - Maakt gebruik van OFDM (Orthogonal Frequency Division Multiplexing) i.p.v. DSS. Bij OFDM splitst men een bitstroom met hoge bitsnelheid op in een zeer groot aantal parallelle bitstromen met lage bitsnelheid (5 keer 200 kbits/s).

OFDM ▷

FDM

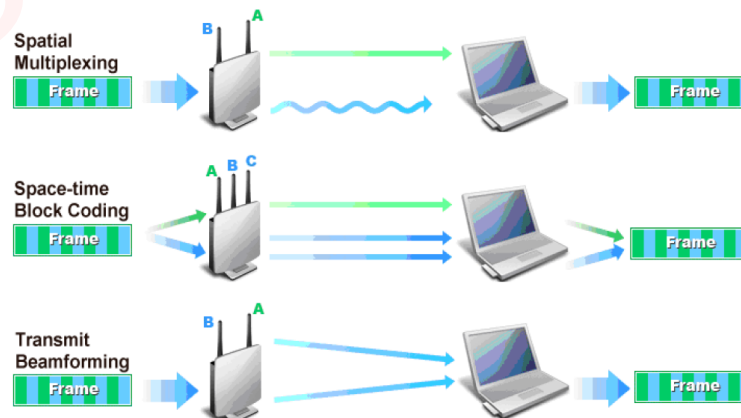


OFDM



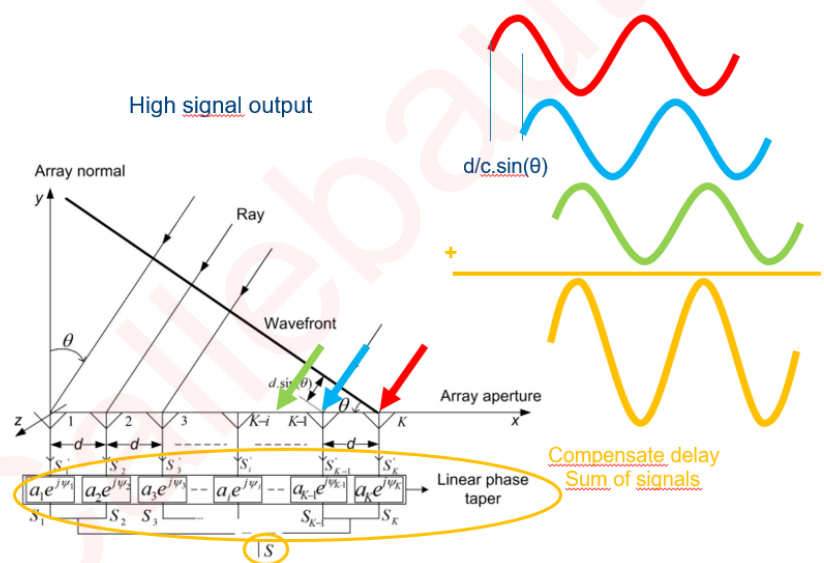
Some of the sub-carriers in some of the OFDM symbols may carry pilot signals for measurement of the channel conditions (i.e., the equalizer gain and phase shift for each sub-carrier). Pilot signals and training symbols (preambles) may also be used for time synchronization (to avoid intersymbol interference, ISI) and frequency synchronization (to avoid inter-carrier interference, ICI, caused by Doppler shift).

- IEEE 802.11n
 - Ondersteuning voor meerdere antennes:
 - Spatial multiplexing
 - Space-time Blocking Coding
 - Transmit Beamforming



- IEEE 802.11ac

- Multiuser MIMO
- Beamforming
 - * Gebaseerd op antenne arrays
 - * Signalen die binnen komen ondervinden een vertraging afhankelijk van hun hoek
 - * Hetzelfde voor het zenden, delay van signalen zo vormen dat de signalen in fase zijn bij de receiver



- IEEE 802.11 ad

In de 60 GHz band, waar veel wordt geabsorbeerd wordt door de lucht. Er is dus daar zeker nood aan beamforming.

3.3 Bluetooth

Bluetooth

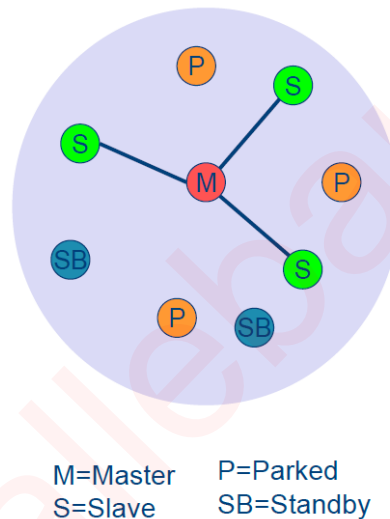
▷ Bluetooth maakt gebruik van FHSS op basis van de pseudo random sequentie van de master, en van TDD voor het scheiden van zenden en ontvangen. Om netwerken van elkaar te onderscheiden wordt er gebruik gemaakt van FH-CDMA.

3.3.1 Piconet

De apparaten connecteren op een ad hoc manier.

- One unit acts as master and the others as slaves for the lifetime of the piconet

- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern
- Participation in a piconet = synchronization to hopping sequence
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)
- Parked devices have no active connection, but are known and can be activated within ms



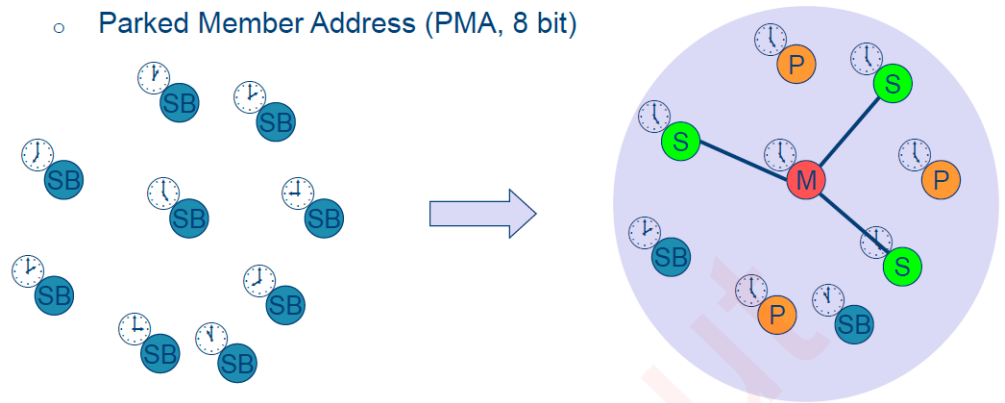
Figuur 38: Piconet

Vormen van een piconet

- All devices in a piconet hop together
 - Master gives slaves its clock and device ID
 - Hopping pattern: determined by device ID (48 bit, unique worldwide)
 - Phase in hopping pattern determined by clock
- AMA ▷
- Active Member Address (AMA) van 3 bits, dus er kunnen 7 actieve nodes worden aangesproken
- PMA ▷
- Parked Member Address (PMA)
 - Delen van eenzelfde 1 MHz band met alle nodes binnen hetzelfde netwerk

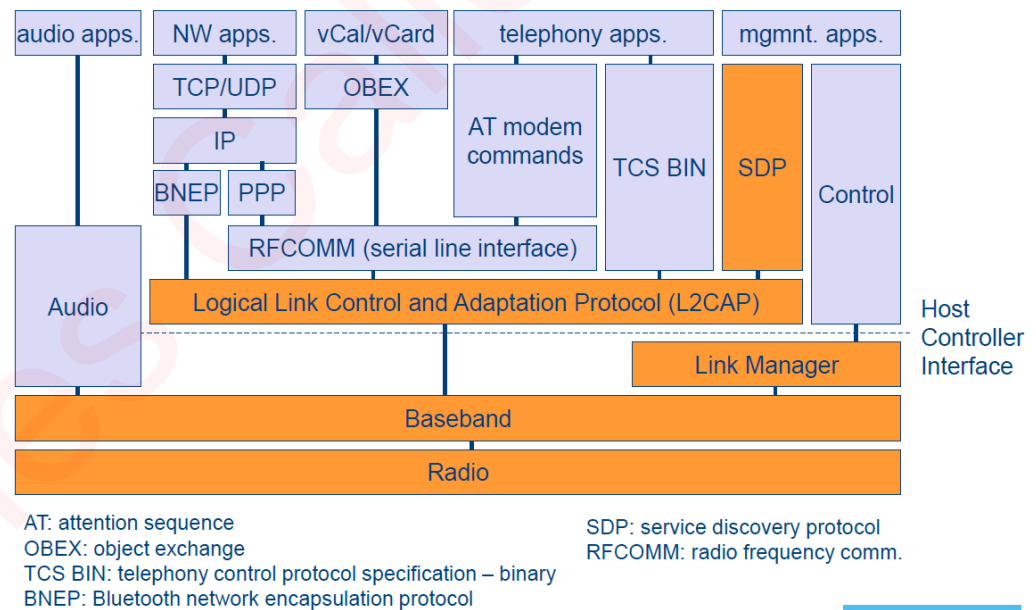
Delen van masters of slaves door meerdere piconetten wordt ook ondersteund onder de vorm van scatternet. Maar wordt praktisch niet gebruikt.

- Addressing
 - Active Member Address (AMA, 3 bit)
 - Parked Member Address (PMA, 8 bit)



Figuur 39: Vormen van een Piconet
Adressen worden verkort want communiceren met 48 bit adressen wordt te intensief

3.3.2 Bluetooth protocol stack



Figuur 40: Protocol Stack

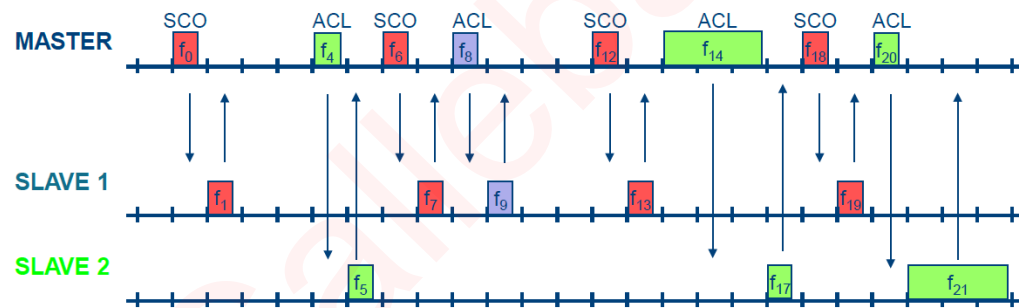
3.3.3 Frequentie selectie tijdens transmissie

De master of slaves kunnen kiezen om 1-slot, 3-slot of 5-slot pakketten te versturen, tijdens de transmissie wordt er niet overgegaan naar een andere frequentie (i.e. geen hopping tijdens transmissie).

- Polling-based TDD packet transmission
 - 625 μ s slots, master polls slaves
- SCO (Synchronous Connection Oriented) – Voice
 - Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point
- ACL (Asynchronous ConnectionLess) – Data
 - Variable packet size (1,3,5 slots), asymmetric bandwidth, point-to-multipoint

SCO ▷

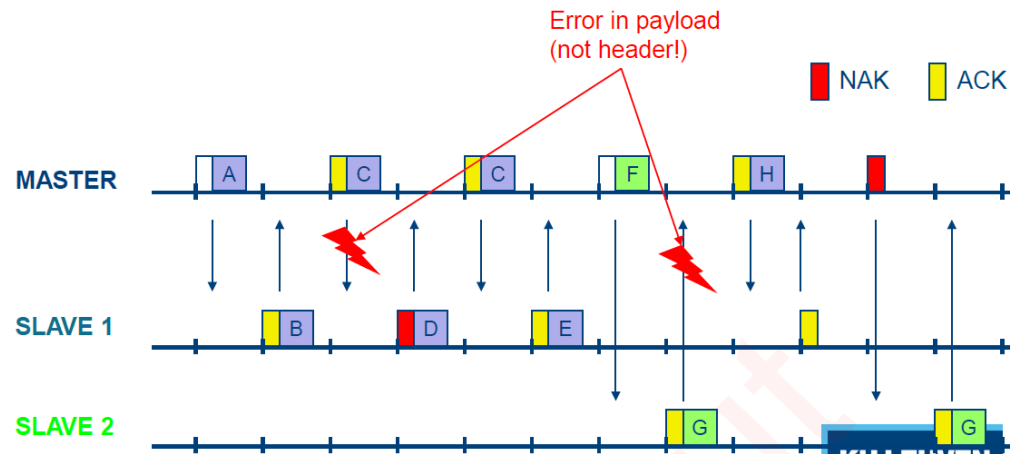
ACL ▷



Figuur 41: Data transmissie in BT

3.3.4 Robuustheid

- Slow frequency hopping with hopping patterns determined by a master
 - Protection from interference on certain frequencies
 - Separation from other piconets (FH-CDMA)
Elke piconet springt op basis van quasi orthogonale codes (de device ID), die op voorhand zo is vastgelegd.
- Retransmission
 - ACL only, very fast
- Forward Error Correction
 - SCO and ACL



Figuur 42: Voorbeeld robuustheid in BT

3.3.5 Low Energy

Bluetooth bespaart energie via een aantal factoren:

- Low power baseband states:

Park release AMA, get PMA

Hold stop ACL, SCO is nog mogelijk, mogelijk nog deelnemen in ander piconet

Sniff periodisch luisteren

Standby description

- Power class: class 1 (max. 100 mW), class 2 (max 2.5 mW), class 3 (max 1 mW).

Bluetooth low energy

- Kleine pakketjes: reduceren van tx/rx tijd
- Simpele protocollen
- Minder RF kanalen om discovery/connection sneller te doen verlopen
- 3 advertisement channels (vaste beacon frequentie zonder hopping). Zo dat slaves niet moeten zoeken voor apparaten in de buurt (dit was zeer tijdsintensief). Deze kanalen zijn zo gelokaliseerd dat ze minst mogelijke interferentie hebben met de WiFi-kanalen.

3.4 ZigBee

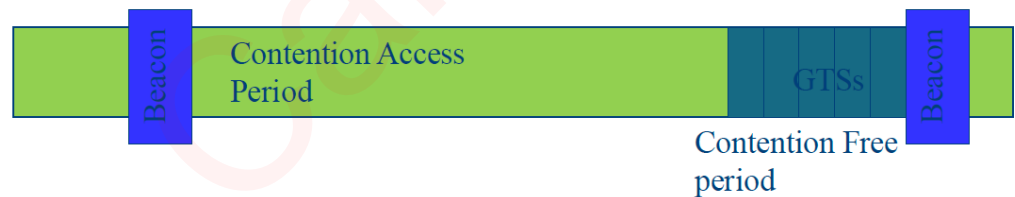
3.4.1 Devices

- Coordinator
- Router (routing in tree of mesh topologie)
- End device

3.4.2 MAC

- CSMA/CA
- Beacons synchronization (beaconless mode possible)
- Superframe
 - Network devices send data frame in contention access period using CSMA-CA
 - Reception confirmed with an acknowledge frame
 - Optional: Guaranteed Timeslots (GTSs), integer multiple of timeslots (timeslot = 1/16 of time between two beacons), no CSMA-CA

GTS ▷



Figuur 43: ZigBee MAC