Mobile Cellular

Mata Kuliah...

Teknologi Komunikasi dan Keamanan data

Arifin Noor Asyikin

STIKI MALANG

6 Oktober 2009

Mobile Cell

- Ponsel merupakan gabungan dua teknologi, yaitu **telepon** (Alexander Graham Bell, 1876) dan **Radio** (Nikolai Tesla, 1880; Guglielmo Marconi, 1894)
- Sebelum ponsel, orang harus memasang telepon radio di mobil.
- Pada sistem sistem telepon-radio, terdapat tower antena pusat di tiap kota, mungkin ada 25 channel frekuensi tiap tower.
  - Artinya, telepon di mobil harus memiliki transmiter yang cukup kuat, selain itu dengan channel terbatas tidak semua orang dapat menggunakan pada saat bersamaan
- Lalu, muncul sistem cellular, yang membagi suatu kota/daerah menjadi beberapa sel kecil.
  - Memungkinkan penggunakan frekuensi ulang pada satu kota, sehingga jutaan pemakai dapat menggunakan ponsel bersamaan.

Konsep Selular Analog

- Setiap sel (terdiri dari 7 sel hexagonal grid), menggunakan 1/7 dari channel suara duplex
- Sehingga: setiap sel memiliki frekuensi unik dan dapat menghindari tabrakan (*collision*)
  - Sebuah cell-phone carrier mendapat 832 frekuensi radio
  - Setiap ponsel menggunakan 2 frekuensi/panggilan (channel duplex), sehinggal ada 395 kanal suara per carrier. (42 frekuensi lain untuk channel kontrol)
    - (832 – 42) / 2 = 395
  - Sehingga, setiap sel memiliki sekitar 56 kanal suara.
    - 395 / 7 = 56,429 => 56
  - Jadi, pada setiap sel, **56** orang dapat saling berbicara pada saat sama.

Transmisi Selular Analog

- Ponsel memiliki transmisi berkekuatan rendah (0.6 watt dan 3 watt)
- Keuntungan:
  - Transmisi base station dan ponsel tidak akan berada diluar sel.
  - Konsumsi listrik ponsel juga rendah, sehingga baterai dapat berukuran sekecil mungkin
- Setiap carrier memiliki sebuah *Mobile Telephone Switching Office (MTSO)* yang menangani semua hubungan ponsel dengan PSTN dan mengontrol semua base station

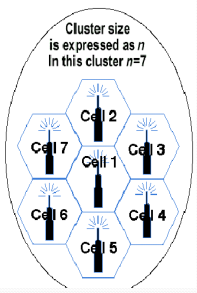
Konsep Detail Telepon Selular

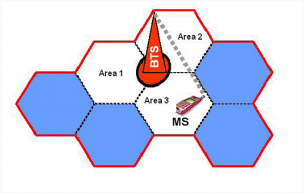
- Suatu area (kota misal), dibagi menjadi beberapa sub area (sel)
- Setiap sel berukuran rata-rata 26 km²
- Ruang lingkup suatu sel berbentuk hexagon dan membentuk suatu hexagon grid besar.
- Oleh karena ponsel dan base station menggunakan transmiter bertenaga rendah, frekuensi yang sama dapat digunakan ulang pada sel yang **tidak** berdekatan
- Setiap sel memiliki sebuah base station yang terdiri dari tower dan bangunan kecil berisi perangkat radio



Arsitektur Sistem S

- Sel
  - Unit dasar sistem selular
  - Ukuran sel tergantung pada area
- Cluster
  - Sekumpulan sel
  - Tidak ada channel frekuensi yang digunakan ulang

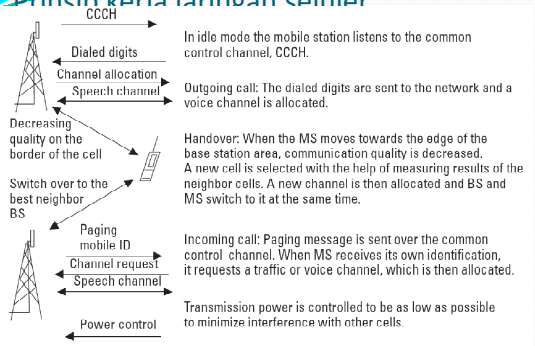




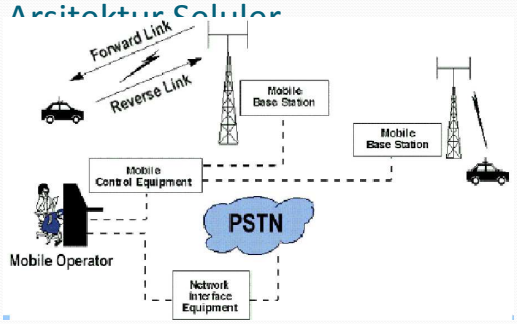
Area Splitting

- Membagi satu sel menjadi beberapa subsel
- Tujuan: membagi suatu area yang terlalu padat agar layanan dapat masih tersedia

Prinsip kerja jaringan seluler



Arsitektur Seluler



Referensi

- PSTN – Public Switch Telephone Network
- MTSO – Mobile Telephone Switching Office (Provider cellular)
  - Kantor pusat untuk mobile switching
  - Di dalamnya terdapat MSC (Mobile Switching Center), field monitoring dan relay stations untuk pemindah panggilan dari/ke cell site dengan PSTN
  - MSC mengontrol panggilan, billing, lokasi pelanggan cell site dengan sistem antena
- Mobile subscriber unit (MSU) - ponsel

Kode-kode ponsel

- Setiap ponsel memiliki kode khusus untuk menunjukkan identitas ponsel, pemilik dan penyedia layanan.
- Electronic Serial Number (ESN)
  - Nomor unik 32 bit yang ditanam waktu pembuatan ponsel
    - 8 digit kode manufaktur, 18 digit SN, 6 digit reserved
  - Skrng diganti IMEI = 56 digit
- Mobile Identification Number (MIN)
  - 10 digit dari nomor SIM Card
- System Identification Code (SID)
  - 5-digit angka yang dapat menghubungkan ponsel dengan provider cellular (bisa juga BTS)

SIM CARD

- Tahun 1991 -> munich card (Giesecke & Devrient)
- 3 digit = Mobile Country Code
- 2 digit = Mobile Network Code
- 10 digit = Mobile Station Identification Number
- SIM = Subcriber Identity Module => Smart Card
- RUIM = Removable User Identity Module
  - Untuk CDMA

Mekanisme Pemanggilan

- Ketika **On**, akan dicari SID pada channel control
  - Channel control adalah frekuensi khusus dimana ponsel dan BTS berkomunikasi untuk setup panggilan dan pergantian channel
  - Jika tidak ditemukan SID, akan muncul "no service"
- Jika ditemukan SID, akan dicocokan dengan SID pada ponsel (pada kartu), jika ya, ponsel berada dalam jaringan **sistem home**.
- Dengan SID, ponsel mengirimkan registration request, dan MTSO mencatat lokasi ponsel
- Jika ada panggilan masuk, MTSO akan mencari posisi ponsel Anda di sel mana.

Mekanisme Pemanggilan

- MTSO akan menyiapkan **dua frekuensi** agar ponsel dapat menerima panggilan
- MTSO berkomunikasi dengan ponsel melalui kanal kontrol untuk memberitahu frekuensi mana yang digunakan.
  - Dan ketika ponsel dan tower dapat berpindah ke frekuensi tersebut, koneksi terbentuk.
  - Anda berbicara dua arah dengan teman Anda.
- Ketika Anda bergerak ke tepi sel, sinyal akan melemah. Sementara itu, BTS berikut yang Anda tuju mendeteksi sinyal ponsel Anda menguat.
- Kedua BTS akan berkoordinasi lewat MTSO, dan pada saat itu, melalui kanal kontrol, ponsel Anda mendapat informasi perubahan kanal frekuensi.
  - Inilah yang disebut **hand off**

Roaming

- Apabila kode SID pada Control Channel **tidak cocok** dengan kode SID yang telah terprogram sebelumnya di dalam database MTSO
- MTSO dari sel dimana Anda sedang roaming akan menguji apakah SID Anda valid dengan menghubungi MTSO jaringan home Anda
- Sistem home memverifikasi ponsel Anda ke lokal MTSO, kemudian menelusuri ponsel Anda yang sedang berada pada selnya
- Sangat cepat waktunya

1G : AMPS (Advanced Mobile Phone System)

- Menggunakan rentang frekuensi 824 Mhz – 894 Mhz
  - 824 – 849 Mhz untuk uplink: sinyal dari ponsel
  - 869 – 894 Mhz untuk downlink: sinyal ke ponsel
- Setiap operator memiliki 832 frekuensi: 790 untuk suara dan 42 untuk data (kontrol)
- Dua frekuensi digunakan membentuk 1 kanal
  - Total ada 416 kanal dan dibagi dalam 7 sel
- Menerapkan modulasi FM. Lebar kanal suara 30 Khz

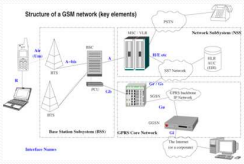
1 G:

- Teknologi lain:
  - NMT (Nordic Mobile Telephone) => Switzerland, Netherlands
  - TACS (Total Access Communications System) => United Kingdom
  - C-450 => West Germany, Portugal, South Africa
  - Radiocom 2000 => France
  - RTMI => Italy

GSM (Global System for Mobile Communication)

- GSM distandarisasi oleh "Groupe Spécial Mobile".
  - Eropa & Asia menerapkan GSM 900 dan GSM 1800. Sedangkan untuk US, GSM 1900
- Untuk dapat terhubung pada jaringan GSM, pemakai harus memiliki subscriber identification module (SIM) card.
- GSM 900 menyediakan 124 kanal full duplex, 25 MHz
- GSM1800 menyediakan 374 kanal full duplex, 25 MHz
- *Roaming technology*: complete communication from anywhere in world
  - Providers establish *roaming areas*: higher cost for users when outside home area
- GSM offers SMS service

infrastruktur GSM



Arsitektur GSM

- Switching Subsystem
  - HLR (Home Location Register), merupakan database yang digunakan untuk manajemen dan penyimpanan subcriptions
  - MSC (Mobile services Switching Center), melakukan fungsi telephone switching
  - VLR (Visitor Location Register), database untuk memyimpan informasi mengenai subscribers yang diperlukan oleh MSC untuk melayani visiting subscribers
  - AUC (Authentication Center), menyediakan fungsi authentikasi dan enkripsi
  - EIR (Equipment Identity Register), merupakan database yang menyimpan informasi mengenai identitas mobile equipment (IMEI)

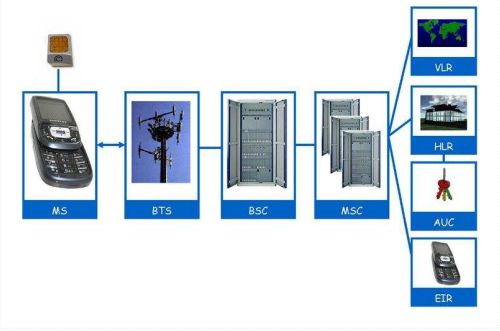
GSM Arsitektur

- Base Station Subsystem
  - BSC (Base Station Controller), menyediakan fungsi kontrol dan link antara MSC dan BTS
  - BTS (Base Transceiver Station), merupakan radio equipment (transceiver dan antena). Sekelompok BTS dikontrol oleh satu BSC
- Mobile Station (MS)
  - Mobile Equipment (ME) => handset
  - Subscriber Identity Module (SIM) card, merupakan card yang berisi informasi mengenai user subscription



Layanan Data GSM

- GPRS: General Packet Radio Service (2.5G)
  - Layanan WAP dan MMS
  - Wireless access to packet data networks, e.g. to the Internet
  - Volume-based billing
  - Instant Messaging; Push to Talk
  - Data rate: 160 kbps (real: 30 – 70 kbps)
  - *Packet data traffic channels (PDCHs)*
    - Transmit data packets (like SMS)
    - Always on connectivity
- EDGE: Enhanced Data rates for GSM Evolution (3G)
  - Data rate: 473,6 kbps (384) – 3G
  - Video service (VOIP) dan layanan multimedia lain (streaming)

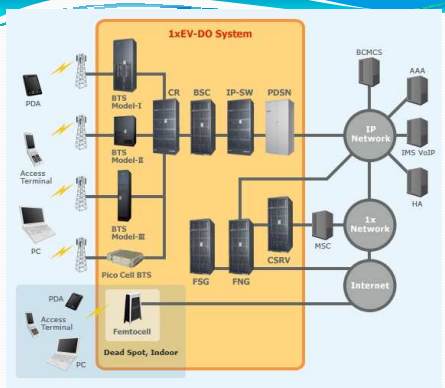


3 Class of Message Services of GSM/GPRS

- In GSM/GPRS network, conventional circuit switched services (speech, data, and SMS) and GPRS services can be used in parallel. Three classes are defined:
  - Class A mendukung GPRS dan GSM secara bersama-sama (2on)
  - Class B mendukung GPRS dan GSM, namun hanya aktif salah satu saja pada suatu saat
  - Class C mendukung GPRS dan GSM, namun harus di switch secara manual

CDMA

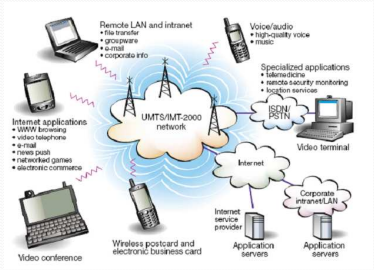
- CdmaOne technologies and standards associated with CDMA *Telecommunications Industry Association (TIA)* and *International Telecommunications Union (ITU)* regulate standards
- Ada 2 standard:
  - Qualcomm memperkenalkan merk cdmaOne (CDMA 2G), dan CDMA2000 (CDMA 3G): CDMA2000 1xEV
  - 3G Standard: W-CDMA
    - Universal Mobile Telecommunications System (UMTS) ~ Eropa/Jepang
    - Freedom of Mobile Multimedia Access (FOMA) ~ NTT DoCoMo dan Vodafone
- CDMA2000 is family of technology types
  - *CDMA 1xMC* Similar to EDGE
    - 1xMC upgrades voice and data capacity
  - *CDMA 1xEV*
    - Separates voice and data into two separate channels
    - *1xEV-DO*: data only transmissions
    - *1xEV-DV*: expands DO to handle voice
  - *CDMA 3xMC*
    - Upgrade 1xMC to 3G networks
    - Similar to UMTS – voice and data



W-CDMA

- W-CDMA protokol pengiriman berkecapatan lebih tinggi yang digunakan di sistem FOMA (Freedom of Mobile Multimedia Access) Jepang dan sistem UMTS (sistem 3G) yang dirancang untuk menggantikan jaringan 2G GSM.
- W-CDMA adalah wideband spread-spectrum mobile air interface yang memanfaatkan metode CDMA untuk mencapai kecepatan lebih tinggi dan mendukung lebih banyak pemakai daripada pensinyalan TDMA dalam jaringan GSM.
- W-CDMA pesaing CDMA2000.

3 G can..



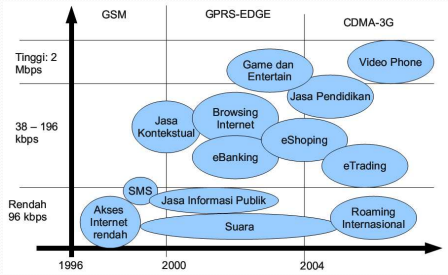
3.5 G

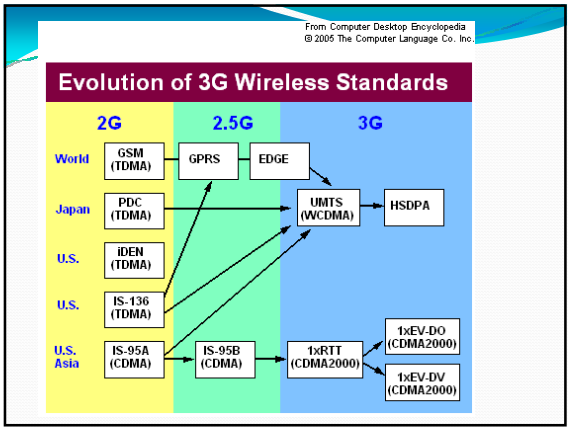
- HSDPA (High-Speed Downlink Packet Access)
  - Downlink speeds: 1.8, 3.6, 7.2 dan 14.4 Mbps
  - Included in UMTS Release 5 Specification
- HSUPA (High-Speed Uplink Packet Access)
  - Uplink speeds up to 5.76 Mbps
  - Included in UMTS Release 6 Specification

4G

- 4G Working Group has defined following objectives of 4G wireless communication standard
  - Spectrally efficient system
  - High network capacity, more simultaneous users per cell
  - 100 Mbps in moving, 1000 Mbps while in fixed position
  - Mendukung HDTV
  - All IP, packet-switched network

Evolusi Aplikasi Mobile



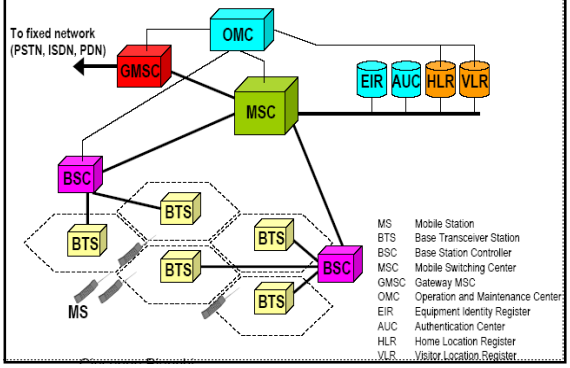


GLOBAL SISTEM FOR MOBILE COMMUNICATION (GSM)

Overview

Global System for Mobile communication (GSM) adalah sebuah standar global untuk komunikasi bergerak digital. GSM adalah nama dari sebuah group standarisasi yang dibentuk di Eropa tahun 1982 untuk menciptakan sebuah standar bersama telpon bergerak selular di Eropa yang beroperasi pada daerah frekuensi 900 MHz. GSM saat ini banyak digunakan di negara-negara di dunia

GSM essential components



Mobile Station

- Merupakan terminal yang dipakai oleh pelanggan untuk melakukan proses komunikasi
- Terdiri dari :
  - Mobile Equipment (ME)/HP
  - Subscriber Identification Module (SIM)



- Catatan : MS tidak akan dapat berhubungan tanpa SIM card

Mobile Equipment

- Merupakan terminal tranceiver
- Diidentifikasikan dengan IMEI tertentu
- IMEI = International Mobile Equipment Identity



SIM Card

- Subscriber Identity Module (SIM) adalah sebuah smart card yang berisiwhich stores seluruh informasi user dan beberapa feature dari GSM
- Informasi yang ada berupa :
  - ***Authentication Key "Ki"***
  - ***2 algorithma enkripsi. Yaitu algoritma autentikasi A3 dan A8 sebagai cipher key***
  - ***IMSI and TMSI***
  - ***Service tambahan***
- SIM card dilindungi oleh sebuah mekanisme Personal Identity Number (PIN) yang dimiliki user

Base Station Subsystem(BSS)

- BSS terdiri dari dua buah perangkat :
  - ✓ Base Transceiver Station (BTS)
  - ✓ Base Station Controller (BSC)
- Antara BTS dan BSC dihubungkan oleh Abis interface

Base Tranceiver Station (BTS)

- BTS merupakan tranceiver yang mendefinisikan sebuah sel dan menangani hubungan link radio dengan MS.
- BTS terdiri dari perangkat pemancar dan penerima, seperti antenna dan pemroses sinyal untuk sebuah interface.
- BTS berkomunikasi dengan MS dengan Um interface

Base Station Controller

- BSC mengatur sumber radio untuk sebuah BTS atau lebih.
- BSC menangani radio-channel setup, frequency hopping, and handover intern BSC

Network Sub-system (NSS)

NSS terdiri dari :

- Mobile Switching Center (MSC)
- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Authentication Center (AuC)
- Equipment Identity Register (EIR)

Mobile Switching Center (MSC)

- Melakukan fungsi switching dasar
- Mengatur BSC melalui A-interface
- Sebagai penghubung antara satu jaringan GSM dengan jaringan lainnya melalui Internetworking Function (IWF)

Authentication Center (AuC)

- Berisi parameter authentikasi pelanggan untuk mengakses jaringan GSM.
- AuC berisi parameter seperti Ki, algorithma A3 atau A8
- AuC memproduksi tiga buah parameter autentikasi seperti (SRES, RAND, Kc) dan menyimpannya di VLR.

Home Location Register (HLR)

- HLR berisi rekaman database permanen dari pelanggandan merupakan database user yang utama.
- HLR juga berisi rekaman lengkap lokasi terkini dari user.

Visitor Location Register (VLR)

- VLR berisi database smentara dari pelanggan
- VLR digunakan untuk pelanggan lokal dan yang sedang melakukan roaming.
- VLR memiliki pertukaran data yang luas daripada HLR.
- VLR diakses oleh MSC untuk setiap panggilan, dan MSC dihubungkan dengan VLR
- Setiap MSC terhubung dengan sebuah VLR, tetapi satu VLR dapat terhubung dengan beberapa MSC

Equipment Identity Register (EIR)

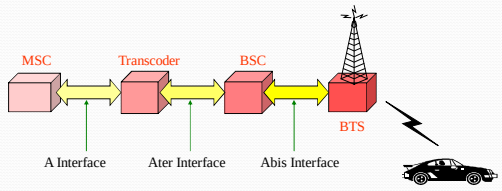
- EIR merupakan register penyimpan data seluruh mobile stations
- EIR berisi IMEIs (international Mobile Equipment Identities), yang merupakan nomor seri perangkat + tipe code tertentu
- Mobile Equipment dibagi menjadi tiga kelompok :
  - ✓ *Blacklist*
  - ✓ *Grey list*
  - ✓ *White list*

* catatan: EIR belum diterapkan di Indonesia.

Operation Sub-system (OSS)

- Operation and Maintenance Jaringan
- Pengaturan pelanggan dan tagihan
- Pengaturan Mobile Equipment

Interface

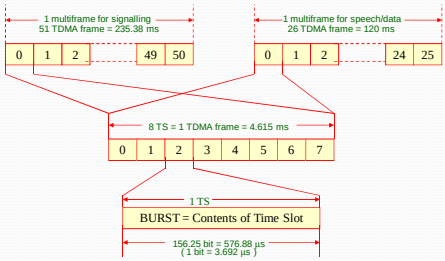


Konsep kanal pada GSM

Kanal terdiri dari dua jenis :

1. Kanal fisik:
   - Satu TimeSlot(TS) frameTDMA merupakan satu kanal fisik
   - Setiap carrier RF terdiri dari 8 TS(CH 0 – 7)
2. Kanal *Logic*:
   - Kanal Trafik (TCH) dapat membawa suara atau data untuk layanan komunikasi. TCH dibagi dua jenis, *full rate channel* dengan Bit rate 13 Kbps dan *half rate channel* dengan kecepatan bit 6,5 Kbps
   - Kanal Kontrol digunakan untuk keperluan signalling
   - Kanal logik ditumpangkan pada kanal fisik

Struktur Frame GSM



Kanal kontrol BCH

Broadcast Control Channel (BCH)

- Terdiri dari Broadcast ControlChannel (BCCH), FCCH (Frequency Correction Channel), SCH (Syncronisation Channel)
- Pembacaan FCCH, BCCH, dan SCH harus dilakukan tiap kali MS pindah sel

FCCH (Frequency Correction Channel)

- *Arah downlink*
- *Point to Multipoint*
- *Sinkronisasi frekuensi MS*
- *Gelombang sinus*

SCH (Syncronisation Channel)

- *Arah downlink*
- *Point to Multipoint*
- *TDMA frame structure (untuk sinkronisasi frame)*
- *Info BSIC (Base Station Identity Code)*

Kanal Logik BCH

BCCH (Broadcast Control Channel)

- ***Arah downlink***
- ***Point to Multipoint***
- ***Informasi LAI (Location Area Identity)***
- ***Informasi power output maksimum MS***
- ***Informasi BCCH carrier sel yang berdekatan***

Kanal logik CCCH

Common Control Channel (CCCH)

PCH (Paging Channel)

- Arah downlink
- Point to Multipoint
- Paging message (IMSI/TMSI)

RACH (Random Access Channel)

- Uplink
- Point to Point
- MS call set up

AGCH (Access Grant Channel)

- Downlink
- Point to Point
- Menyediakan kanal signalling (SDCCH)

Kanal logik DCCH

Dedicated Control Channel (DCCH)

SDCCH (Stand Alone Dedicated Control Channel)

- Arah downlink dan uplink
- Point to Point
- Call set up
- Authentication
- Location Updating
- Short message dan cell broadcast
- Menyediakan TCH

Kanal Logik DCCH

Dedicated Control Channel (DCCH)

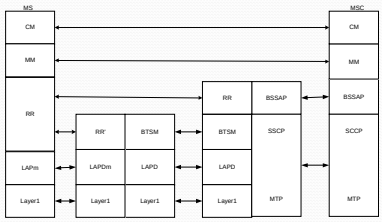
SACCH (Slow Associated Control Channel)

- Downlink dan uplink
- Point to Point
- Uplink : MS measurement data
- Downlink :
  - ✓ MS power output
  - ✓ Timing advanced

FACCH (Fast Associated Control Channel)

- Downlink dan uplink
- Point to Point
- Handover
- Stealing mode (pengganti sementara TCH)

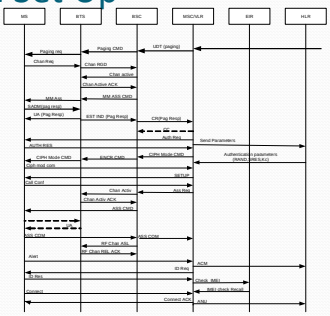
Signalling MS-BSC-MSC



Signalling Protocol

- ***Radio Recource(RR): mengalokasi,dealokasi parameter-parameter kanal radio. Penting untuk set-up komunikasi pada MS***
- ***Mobility Management(MM): mengatur administrasi lokalisasi MS dan handover***
- ***Circuit Mode Connection Call Protocol (CM atau CC): mengatur administrasi pembangunan dan pemutusan komunikasi***
- ***BTS Managemen(BTSM) melewati Abis Interface***
- ***BSS Aplication Part (BSSAP)melewati A interface***
- ***Layer transport diduduki oleh protokol SS7,SCCP,dan MTP***
- ***Mobile Applicaton Part (MAP) digunakan untuk pensinyalan antara MSC,HLR, dan VLR***

Call Set Up



Call Set Up

- ***Permintaan panggilan akan diteruskan ke seluruh Base Station diseluruh lokasi area.***
- ***Ketika MS yang dituju ditemukan, MS akan meminta sebuah interface kanal radio, dan BSC akan memberikannya.***
- ***Ketika kanal aktif, MS akan mengirim PAG RESP sebagai tanda bisa dipanggil, dan siap untuk menjawab panggilan.***
- ***MSC akan mengomentari authentikasi dari MS dan parameter harus dicek di HLR, dengan mengirim permintaan 'send parameter'.***
- ***Proses Encripsi diinisialisasi dengan sinyal CIPH MODE.***
- ***Jika sukses, panggilan akan dikirim ke MS, yang merespon dengan CALL Conf untuk menandai MS dapat merespon semua jenis panggilan.***
- ***Jika sukses, sebuah kanal trafik akan dialokasikan dengan sinyal ASS, terdengar alarm dan terjadi hubungan.***
- ***Atau juga, MSC akan mengecek IMEI MS Pada EIR(optional)***

Handover1

- Handover adalah proses perpindahan kanal trafik user pada saat user aktif tanpa terjadi pemutusan hubungan
- Penyebab Handover antara lain pergerakan dari user dan melemahnya sinyal terima dari satu sel

Handover2

- Handover dibagi menjadi :
  1. ***Intra-cell HandOver: pemindahan hubungan ke kanal yang berbeda pada satu BTS yang sama***
  2. ***Intern-cell HandOver: pemindahan hubungan antar BTS yang berbeda dalam satu BSC***
  3. ***MSC intern HandOver: pemindahan hubungan yang terjadi antar BSC dalam satu MSC***
  4. ***MSC ekstern HandOver: Pemindahan hubungan antar BTS dari MSC yang berbeda***

NEXT

- Wi-Fi