



Współczesne systemy bezprzewodowe: GSM



GSM (Global System for Mobile communications lub Groupe Speciale Mobile)

- Zainicjalizowany przez Komisję Europejską
- opracowany w 1982, aby stworzyć wspólny europejski standard systemu mobilnego i bezprzewodowego funkcjonującego na 900 MHz (system 2G)
- Głównym celem GSM było usunięcie niekompatybilności między istniejącymi systemami w celu umożliwienia roamingu dla dowolnego telefonu komórkowego
- System umożliwia transmisję mowy między MS-ami, realizację połączeń w warunkach sytuacji nadzwyczajnych oraz transmisję danych cyfrowych
- Obecnie jest najpopularniejszym standardem telefonii komórkowej (2006r: 1.7 mld abonentów w ponad 200 krajach)



Historia rozwoju standardu GSM

- **GSM 900 Phase 1:** 1988 – opublikowanie pierwszej specyfikacji
 - 1992-w Finlandii pierwsza sieć komercyjna
- **GSM Phase 2:** 1990 – rozpoczęto definiowanie standardu GSM 1800 nazywanego również **DCS** (Digital Communication System)
 - 1993-w W.Brytanii powstaje sieć DCS
- **GSM Phase 2+** - uwzględniono technologie przesyłania danych **HSCSD** (High Speed Circuit Switched Data) (57.6/14.4 kb/s) oraz **CAMEL**- umożliwiający pełny roaming usług bazujących na platformie sieci inteligentnych
 - 1997-częścią specyfikacje staje się technologia **GPRS** (30-80 kb/s)
 - USA-powstaje **GSM 1900** nazywany tam **PCS** (Personal Communications Services)
- Standard GSM jest dalej rozbudowywany
 - Wprowadzono nową technologię przesyłania danych **EDGE**-3 krotne polepszenie przepływności w stosunku do GPRS (GPRS i EDGE są nazywane technologią **2.5 G**)
 - Rozwijane są specyfikacje **3G**



Standardy GSM

- Różnią się używanym pasmem częstotliwości i rozmiarem komórek
- Aktualnie osiem zakresów radiowych
 - GSM 450 -współistnieją z NMT (1G), duże niezamieszkałe tereny
 - GSM 480 -współistnieją z NMT (1G), duże niezamieszkałe tereny
 - GSM 850 (większość państw obu Ameryk)
 - GSM 900 (P-GSM) (pozostałe części świata)
 - GSM 900 (E-GSM) (pozostałe części świata)
 - GSM-R (R-GSM) (sieci kolejowe)
 - DCS 1800 (GSM-1800) (pozostałe części świata)
 - PCS 1900 (GSM 1900) (większość państw obu Ameryk)



GSM: zakresy częstotliwości

| System | Band | Uplink | Downlink | Channel Number |
|-----------------|------|-----------------|-----------------|------------------------|
| GSM 400 | 450 | 450.4 - 457.6 | 460.4 - 467.6 | 259 - 293 |
| GSM 400 | 480 | 478.8 - 486.0 | 488.8 - 496.0 | 306 - 340 |
| GSM 850 | 850 | 824.0 - 849.0 | 869.0 - 894.0 | 128 - 251 |
| GSM 900 (P-GSM) | 900 | 890.0 - 915.0 | 935.0 - 960.0 | 1 - 124 |
| GSM 900 (E-GSM) | 900 | 880.0 - 915.0 | 925.0 - 960.0 | 975 - 1023, (0, 1-124) |
| GSM-R (R-GSM) | 900 | 876.0 - 880.0 | 921.0 - 925.0 | 955 - 973 |
| DCS 1800 | 1800 | 1710.0 - 1785.0 | 1805.0 - 1880.0 | 512 - 885 |
| PCS 1900 | 1900 | 1850.0 - 1910.0 | 1930.0 - 1990.0 | 512 - 810 |



GSM: rozmiary komórek

- Maksymalny rozmiar komórki: 35 km
- Dla systemów 1800/1900 MHz < 8 km (potrzebna jest duża energia do emitowania sygnału w tym zakresie)
- Rozwiązanie **extended range**: promień komórki do 120 km
 - Znaczne pogorszenie pojemności komórki
 - Stosowane gdy chce się obniżyć koszty pokrycia dużych, słabo zaludnionych terenów
 - GSM 400 – wymaga mniejszej energii do emitowania sygnałów na tak duże odległości
 - Niektórzy dostawcy oferują taką możliwość dla GSM 900
- Niektórzy operatorzy posiadają licencje na oba zakresy 900/1800 MHz
 - Najpierw pokrywają obszar za pomocą sieci GSM 900 (mniejszy koszt pokrycia obszaru)
 - Obszary o dużym ruchu telekomunikacyjnym (miasta, tereny turystyczne) są pokrywane GSM 1800 (większa liczba dostępnych kanałów)
 - Oferowane MS-y umożliwiają pracę w obu zakresach



GSM: główne założenia standardu

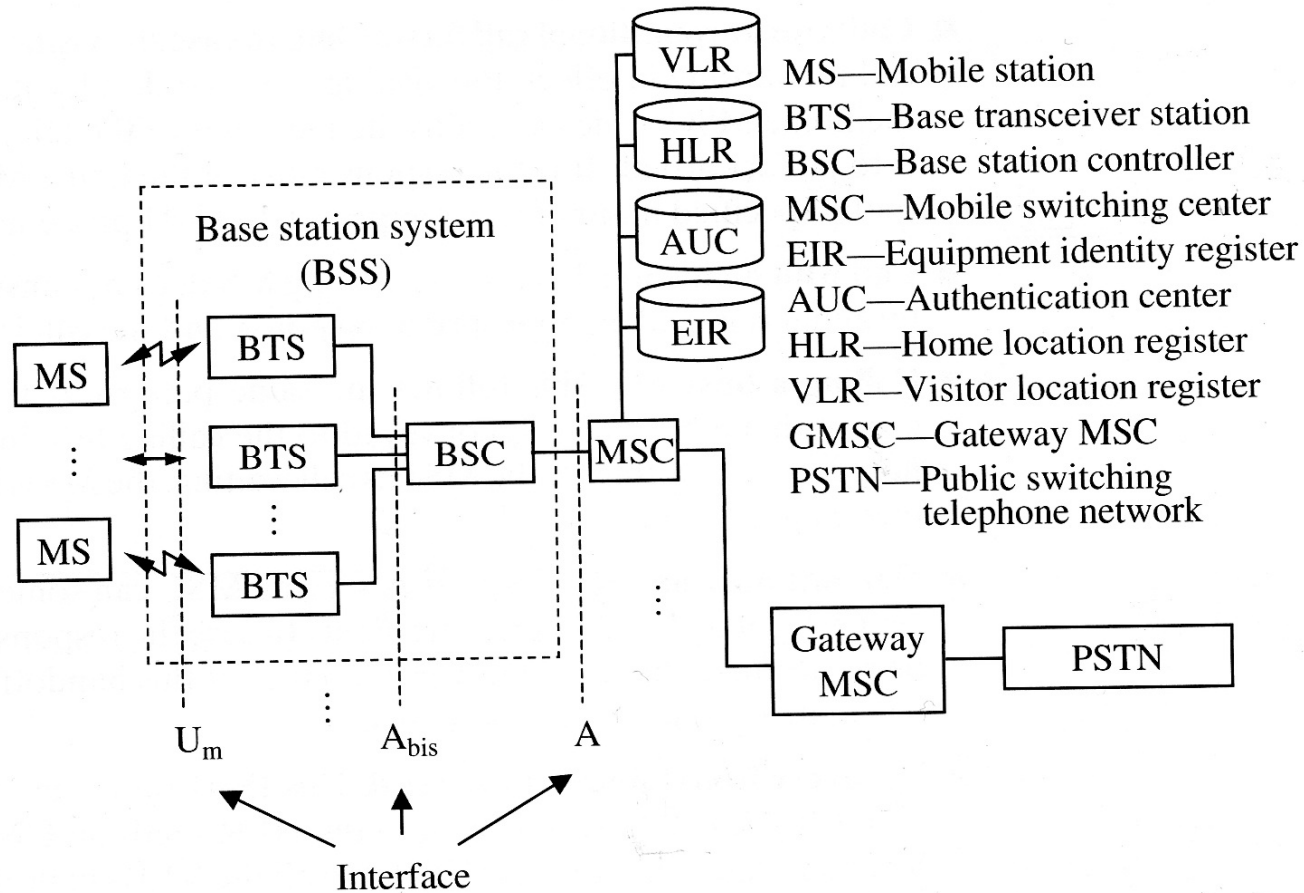
- Opierano się na doświadczeniach związanych z usługami cyfrowymi (standard **ISDN**) oferowanymi przez publiczną komutowaną sieć telefoniczną (**PSTN**), która dzisiaj prawie w całości jest siecią cyfrową (usługi analogowe – **POTS** (Plain Old Telephone Service))
- W strukturze obu sieci kontrola nad połączeniami jest wykonywana za pomocą protokołu sygnalizacyjnego **SS7**
- Głos o częstotliwości 300-3400 Hz jest zamieniany na postać cyfrową
- Zdefiniowane są pewne usługi, które są zintegrowane z siecią (np. przesyłanie faksu, krótkich wiadomości tekstowych, poczta głosowa, identyfikacja numeru, itp.)



GSM: główne założenia standardu

- Podstawowym założeniem standardu GSM była pełna mobilność abonenta; w tym celu wprowadzono
- Dodatkowe elementy infrastruktury umożliwiające przechowywanie informacji o położeniu abonenta, śledzeniu jego zmian oraz utrzymywanie odpowiedniej jakości transmisji podczas przemieszczania się abonenta
- Roaming
- Połączenie MS-a z siecią dzięki systemowi stacji BS-ów
- Dostęp do kanału radiowego odbywa się za pomocą technologii FDMA i TDMA

Infrastruktur GSM 900





BSC (Base station controller)

- główną funkcją jest nadzorowanie określonej liczby BTS-ów w celu zapewnienia ich właściwego działania
 - Wykonuje przeniesienia połączenia z jednego BTS-u do drugiego
 - Podtrzymuje odpowiednią moc sygnału
 - Administruje częstotliwościami między BTS-ami



MSC (Mobile switching center)

- Wykonuje funkcje przełączające systemu poprzez kontrolowanie połączeń przychodzących i wychodzących
- Wykonuje również funkcje sieciowego interfejsu i ogólnej sygnalizacji kanałowej
- GSM korzysta z dwóch ważnych baz danych HLR i VLR umożliwiających kontrolę bieżącego położenia MS-ów
- Jeżeli posiada interfejs do PSTN to nazywany jest MSC-bramą
 - Odpowiedzialny za kontaktowanie się z HLR
 - Centrala tranzytowa do innych sieci



AUC (Authentication center)

- Zapewnia uwierzytelnianie i szyfrowanie parametrów, które weryfikują użytkownika i zapewniają poufność każdego połączenia
- chroni operatorów sieciowych przed różnymi typami nadużyć oraz przechwytywania danych



EIR (Equipment identity register)

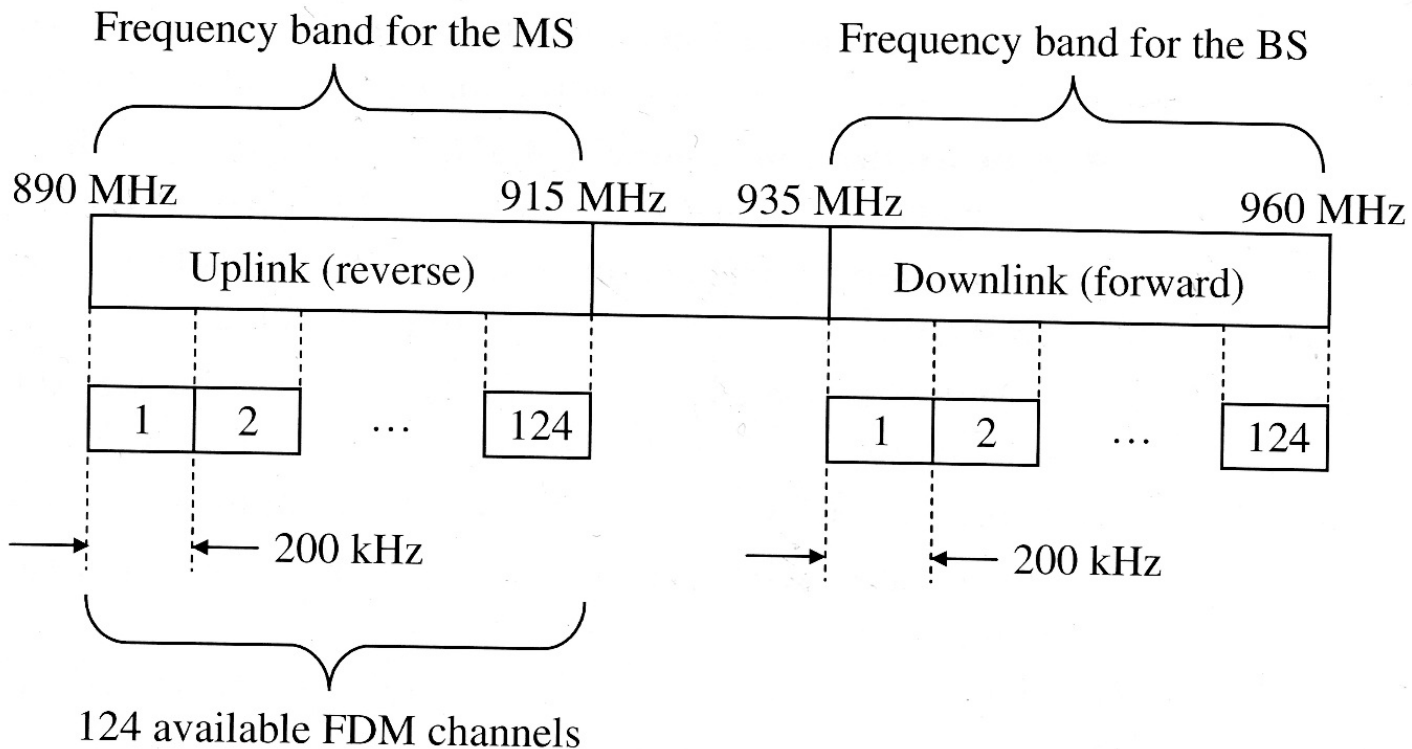
- Jest to baza danych, która zawiera informacje identyfikującą mobilne urządzenia, zapobiegającą połączeniom z MS-ów, które były ukradzione lub są nieautoryzowane



Zakresy częstotliwości i kanały

- Zakres częstotliwości 25 MHz jest podzielony na 124 kanały typu FDMA
- Każdy kanał ma swój numer: 1,2,...,124
- Każdy kanał obejmuje pasmo 200 kHz
- Każdy kanał posiada częstotliwość nośną (środkową)

Zakresy częstotliwości (FDMA) i kanały fizyczne

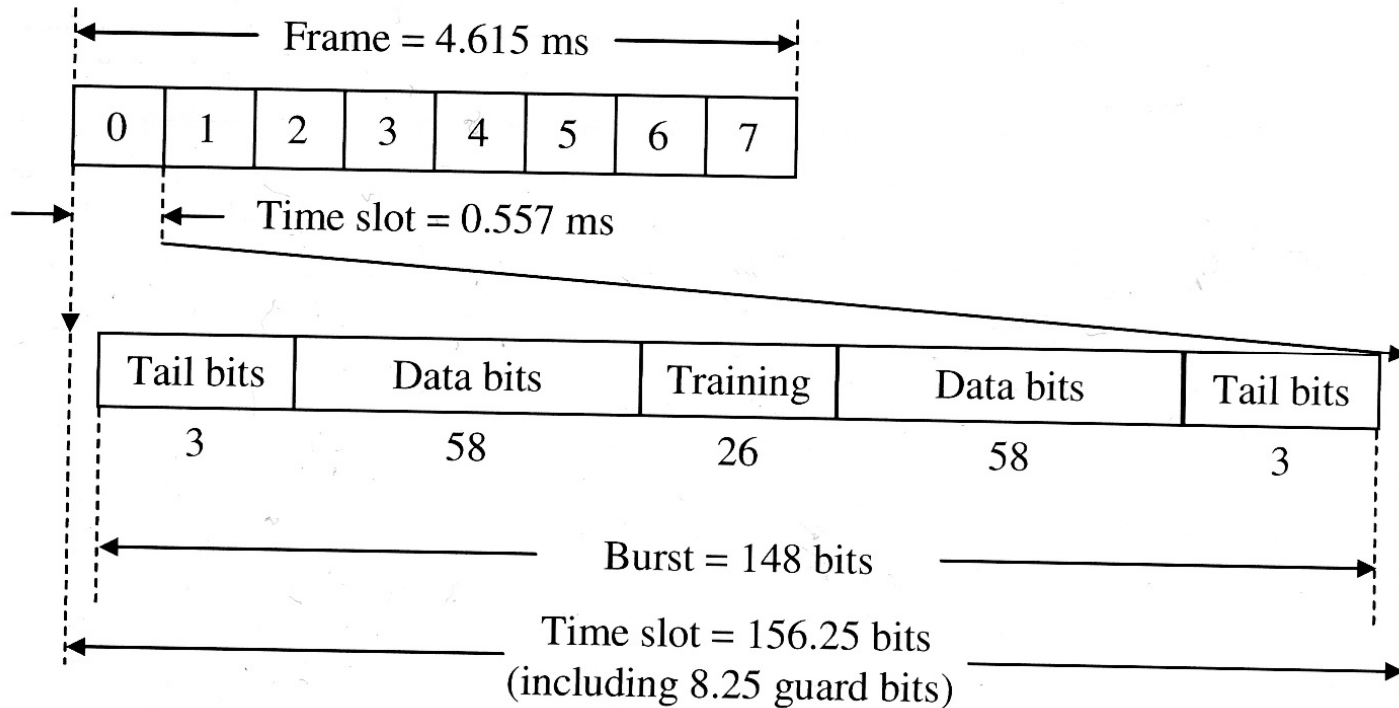




Kanały fizyczne: TDMA i ramki

- Każdy kanał używa TDMA w celu jego podziału czasowego na ramki o długości 4.615 ms; ramki mogą być łączone w multiframe, superframe oraz hyperframe
- Każda ramka podzielona jest na osiem szczelin czasowych o długości 0.557 ms
- To odpowiada 156.25 bitom: 148 bitów informacji + 8.25 bitów ochrony
- Zatem, na każdym kanale znajduje się 8 kanałów rozmównych (transmisja full rate) lub 16 kanałów rozmównych (half-rate)
- Opcjonalnie używa się przydziału kanału dla abonenta wykorzystując procedurę Frequency Hopping
- Pojedyncza komórka może wykorzystywać od 1 do 16 kanałów FMA, co odpowiada od 8 do 128 kanałów rozmównych typu full-rate lub od 1- do 256 kanałów typu half-rate

Ramka i szczeliny czasowe





Kanały logiczne

- W danym **kanale fizycznym** (szczelinie czasowej) mogą być przesyłane różne strumienie pakietów – mogą one mieć różne znaczenie i realizować różne cele
- Takie oddzielne strumienie pakietów tworzą tzw. **kanały logiczne**, które służą do organizacji wymiany informacji



Kanały logiczne

- **Szczelina 0** w **downlink-kanal** (nośna), jest używana do transmisji informacji systemowych do wszystkich MS-ów znajdujących się w zasięgu danego BS-a
- Na odpowiadającym kanale **uplink** w **szczelinie 0** MS-y zgłaszają potrzebę nawiązania połączenia
- Ta para kanałów w danej komórce służy więc do przesyłania informacji systemowych za pomocą kanałów logicznych



Kanały sterujące (logiczne) i kanały rozmówne

- Kanały sterujące mają na celu zapewnienie nieprzerwanej komunikacji między MS-ami i BS-ami
- 3 grupy kanałów sterujących używane są do kontroli komunikacji między MS-i i BS-i
- Dwa dedykowane kanały sterujące są używane wraz z kanałami rozmównymi do realizacji bieżącej komunikacji

Kanały sterujące (logiczne) i kanały rozmówne

Channels in GSM

| Channel | Group | Channel | Direction |
|-----------------|-------------------------------------|---|-----------|
| Control channel | BCCH (Broadcast control channel) | BCCH (Broadcast control channel) | BS → MS |
| | | FCCH (Frequency correction channel) | BS → MS |
| | | SCH (Synchronization channel) | BS → MS |
| | CCCH (Common control channel) | PCH (Paging channel) | BS → MS |
| | | RACH (Random access channel) | BS ← MS |
| | | AGCH (Access grant channel) | BS → MS |
| | DCCH (Dedicated control channel) | SDCCH (Stand-alone dedicated control channel) | BS ↔ MS |
| | | SACCH (Slow associated control channel) | BS ↔ MS |
| | | FACCH (Fast associated control channel) | BS ↔ MS |
| Traffic channel | TCH (Traffic channel) | TCH/f (Full-rate traffic channel) | BS ↔ MS |
| | | TCH/s (Half-rate traffic channel) | BS ↔ MS |



Grupa kanałów sterujących BCCH

- Kanał **BCCH** służy do transmisji informacji sterujących dotyczących sieci, danej komórki oraz komórek sąsiednich
- Kanał **FCCH** jest używany do dostrajania się częstotliwości nośnej MS-ów
- Kanał **SCH** służy do uzyskania przez MS-y synchronizacji ramkowej oraz identyfikacji BS-a



Grupa kanałów sterujących CCCH

- Kanał **CCCH** służy po uzyskaniu synchronizacji do nawiązywania połączenia i składa się z
 - Kanału dostępu losowego **RACH** wykorzystywanego przez MS-y do zgłaszania chęci uzyskania połączenia
 - Kanału przydziału dostępu **AGCH** za pomocą którego BS informuje MS o zgodzie na dostęp
 - Kanału **PCH** za pomocą którego BS inicjuje połączenie z MS



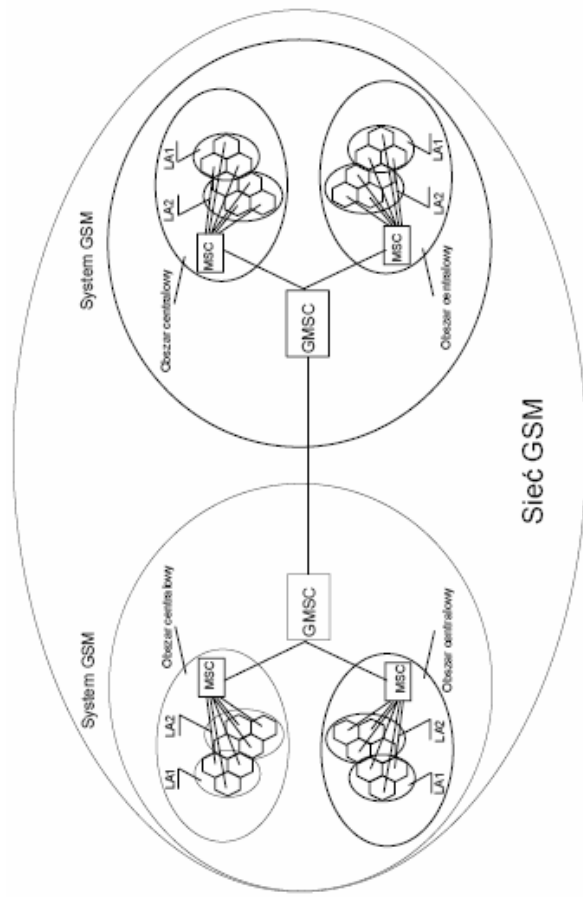
Kanał rozmówczy

- Transmisja informacji abonenta i skojarzonych z nią informacji sterujących odbywa się z użyciem następujących kanałów
 - Kanału rozmównego **TCH**, w którym transmitowane są ciągi binarne sygnału mowy lub danych abonenta; rozróżniamy kanały **TCH/Full Rate** i **TCH/Half Rate**
 - Kanału sterującego **SACCH** przekazującego informacje nakazujące np. zmianę mocy sygnału emitowanego przez MS przy przekazywaniu połączenia do sąsiedniego BS, itp.
 - Kanału sterującego **FACCH** transmitującego informacje nie cierpiące zwłoki
 - Kanału sterującego **SDCCH** używanego do wymiany informacji poprzedzającej uzyskanie połączenia, takiej jak np. potwierdzenie autentyczności abonenta oraz przydziału kanału rozmównego – wersji kanału **FACCH** stosowanej do przekazywania SMS-ów

Hierarchiczna struktura sieci



- **Komórka** - obszar obsługiwany przez stację bazową
- **Obszar przywołań (LA - ang. *Location Area*)** - część obszaru centralowego, wewnątrz którego:
 - nie trzeba uaktualniać danych o położeniu MS,
 - nadawana jest informacja przywoławcza do MS
- **Obszar centralowy (ang. *MSC Service Area*)** - obszar obsługiwany przez jedną centralę obszarową
 - informacja o położeniu MS przechowywana jest w HLR z dokładnością do obszaru centralowego
- **System GSM (ang. *PLMN Service Area*)** - obszar działania sieci GSM administrowany przez jednego operatora
 - w jednym kraju może być kilka systemów GSM
- **Sieć GSM (ang. *GSM Network Area, GSM Service Area*)** - cały obszar objęty zasięgiem usług GSM
 - geograficznie odpowiada wszystkim krajom (operatorom), w których działają systemy GSM



System numeracji stosowany w sieci GSM

Skomplikowany system numeracji związany jest z wielowarstwową strukturą sieci i złożonymi procedurami wymiany informacji pomiędzy jej poszczególnymi elementami:

- oddzielenie numeracji abonenta od numeracji usług i sprzętu, • numer \neq droga połączenia,
- różne numery dla usług, • różne numery dla różnych grup użytkowników

MSISDN – numer międzynarodowy abonenta sieci ISDN: MSISDN = kraj + operator + abonent

- nr katal. użyt., • rozumiany w całej sieci, • określa typ dostępnej usługi, a nie terminal,
- w HLR numer MSISDN \rightarrow MISI, • zgodny z numeracją w sieci ISDN.

IMSI – numer międzynarodowy abonenta ruchomego (użyt.): IMSI = kraj + operator + abonent

- numer (używany) wew. w sieci, • przydzielony przez operat., • zapisany w HLR, AuC, VLR i SIM

MSRN – numer chwilowy stacji ruchomej (do zestaw. łącz.): MSRN = kraj + operator + abonent

- generowana przez VLR (odpowiedź za zapytanie z HLR o położenie stacji (co do obsz. przywołań

TMSI – tymczasowy numer abonenta ruchomego • zakodowana wersja numeru MISI,

- przesyłany od BTS do MS w trakcie przywołania (identyf. abon.), • przydzielany przy 1-m zgł. MS

IMEI – międzyn. nr identyf. terminala IMEI = model + producent + urządzenie + dodatkowe

- pozwala na śledzenie terminali, ich blokowanie i kontrolę dostępu, • na stałe w terminalach i w EIR

LAI – numer (do identyf.) obszaru przywołań abonenta LAI = kraj + operator + obszar przywołań

- ruch w obszarze - bez aktualizacji w VLR.

CGI – numer globalny (danego obsz.) komórki CGI = kraj + operator + obszar przywołań + komórka

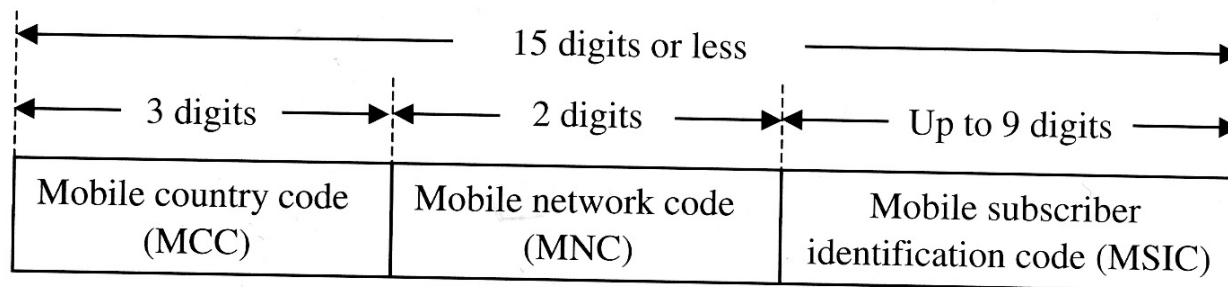
- rozpoznawanie odpowiadającego abonenta przez centralę, • również cele taryfikacyjne.

BASIC – numer identyfikacyjny stacji bazowej BASIC = kraj + grupa komórek

- używany przez MS do identyf. BS, • wykluczanie BS o silniejszym sygnale, ale dalej położonych,
- „problemy graniczne”.

Numery identyfikujące użytkownika: IMSI

- MS przechowuje **IMSI** (International mobile subscriber identity), które jest weryfikowane przez BS
- W szczególności uzyskuje się w info o PLMN (home public Land Mobile Network) danego użytkownika



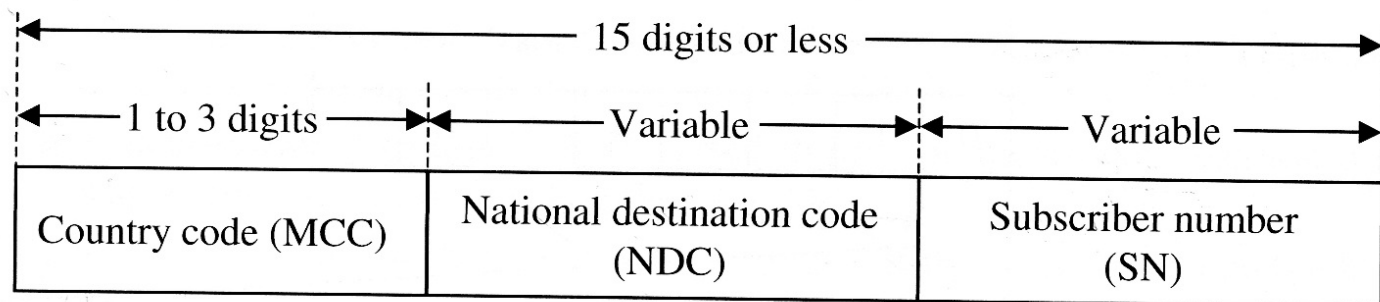


Numery identyfikujące użytkownika: SIM

- SIM (Subscriber identity module)
- Karta SIM – serce telefonu GSM
- MS przechowuje w karcie SIM: numer telefonu (lub numer używany do kontaktu z tym MS), personalny numer identyfikacyjny, parametry autoryzacji, itp.
- Karta SIM posiada również pamięć umożliwiającą przechowywanie krótkich wysyłanych wiadomości
- Umożliwia roaming (tzw. SIM roaming) z telefonem lub bez niego

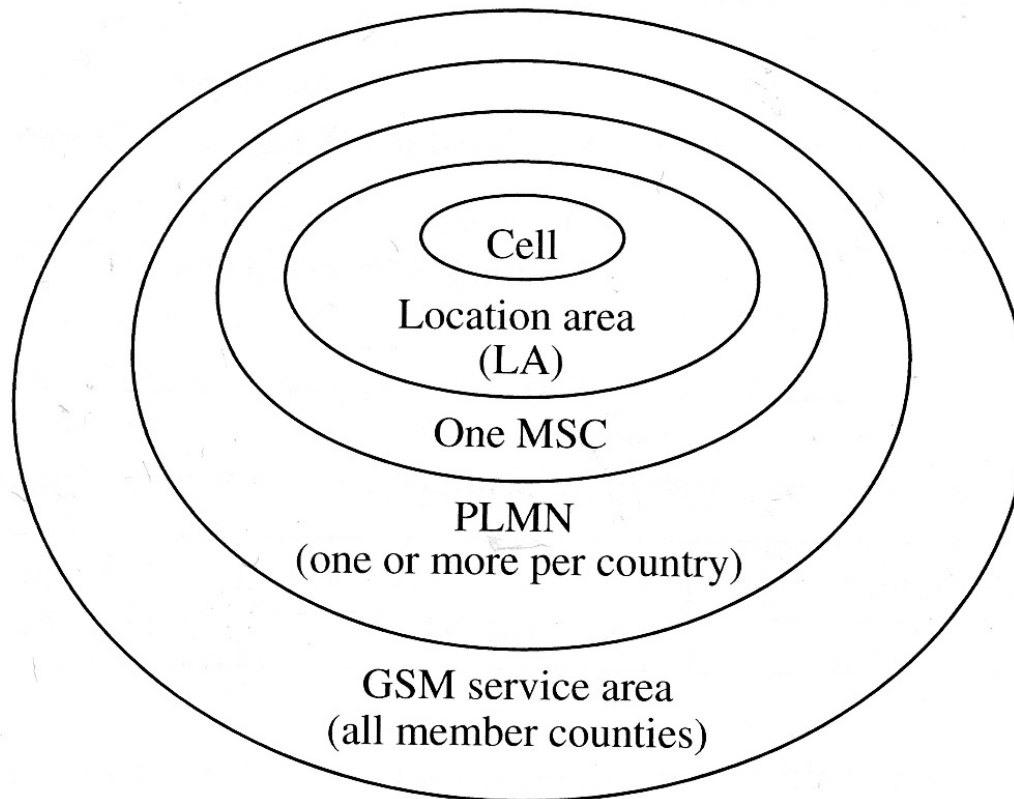
Numery identyfikujące użytkownika: MSISDN

- **MSISDN** (Mobile system ISDN) identyfikuje konkretnego abonenta MS-a
- W odróżnieniu od innych standardów, GSM nie identyfikuje danego MS, lecz konkretny **HLR**, który jest odpowiedzialny za kontakt z MS
- Format **MSISDN**



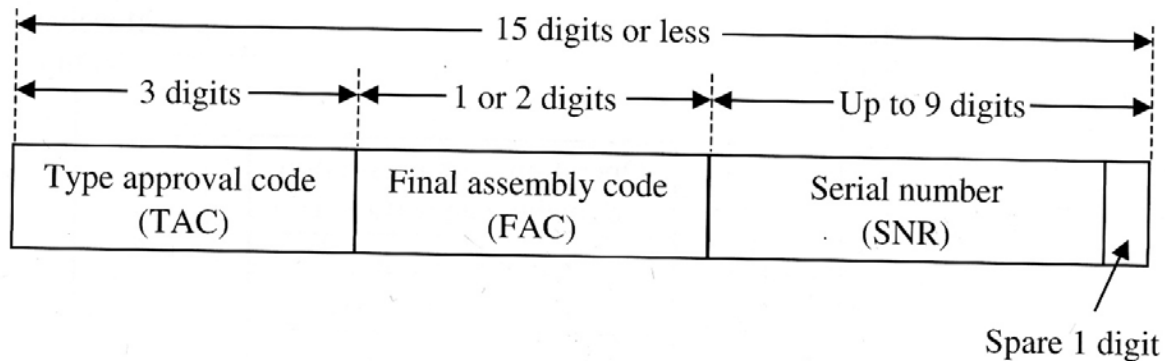
Numery identyfikujące użytkownika: LAI

- LAI (Location area identity) – przechowuje informację umożliwiającą łatwy dostęp MS-a do **hierarchicznej** struktury usług GSM



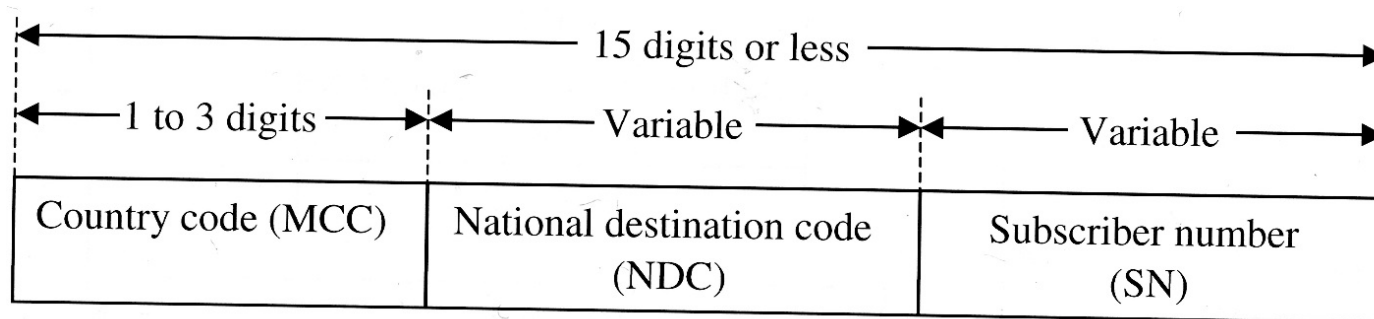
Numery identyfikujące użytkownika: IMSEI

- **IMSEI** (International MS equipment identity) zawiera numery identyfikacyjne produkowanych urządzeń systemu GSM



Numery identyfikujące użytkownika: MSRN

- **MSRN** (MS roaming number)
- Gdy MS wykonuje roaming uzyskuje od lokalnego MSC chwilowy numer, który jest przechowywany w **HLR**





Numery identyfikujące użytkownika: TMSI

- **TMSI** (Temporary mobile subscriber identity)
- Aby zwiększyć bezpieczeństwo przesyłanej w przestrzeni informacji zamiast identyfikacji fabrycznej **IMSEI** przesyłana jest chwilowa identyfikacja **TMSI**

System numeracji stosowany w sieci GSM

Skomplikowany system numeracji związany jest z wielowarstwową strukturą sieci i złożonymi procedurami wymiany informacji pomiędzy jej poszczególnymi elementami:

- oddzielenie numeracji abonenta od numeracji usług i sprzętu, • numer \neq droga połączenia,
- różne numery dla usług, • różne numery dla różnych grup użytkowników

MSISDN – numer międzynarodowy abonenta sieci ISDN: MSISDN = kraj + operator + abonent

- nr katal. użyt., • rozumiany w całej sieci, • określa typ dostępnej usługi, a nie terminal,
- w HLR numer MSISDN \rightarrow MSI, • zgodny z numeracją w sieci ISDN.

IMSI – numer międzynarodowy abonenta ruchomego (użyt.): IMSI = kraj + operator + abonent

- numer (używany) wew. w sieci, • przydzielony przez operat., • zapisany w HLR, AuC, VLR i SIM

MSRN – numer chwilowy stacji ruchomej (do zestaw. łącz.): MSRN = kraj + operator + abonent

- generowana przez VLR (odpowiedź za zapytanie z HLR o położenie stacji (co do obsz. przywołań

TMSI – tymczasowy numer abonenta ruchomego • zakodowana wersja numeru MSI,

- przesyłany od BTS do MS w trakcie przywołania (identyf. abon.), • przydzielany przy 1-m zgł. MS

IMEI – międzyn. nr identyf. terminala IMEI = model + producent + urządzenie + dodatkowe

- pozwala na śledzenie terminali, ich blokowanie i kontrolę dostępu, • na stałe w terminalach i w EIR

LAI – numer (do identyf.) obszaru przywołań abonenta LAI = kraj + operator + obszar przywołań

- ruch w obszarze - bez aktualizacji w VLR.

CGI – numer globalny (danego obsz.) komórki CGI = kraj + operator + obszar przywołań + komórka

- rozpoznawanie odpowiadającego abonenta przez centralę, • również cele taryfikacyjne.

BASIC – numer identyfikacyjny stacji bazowej BSIC = kraj + grupa komórek

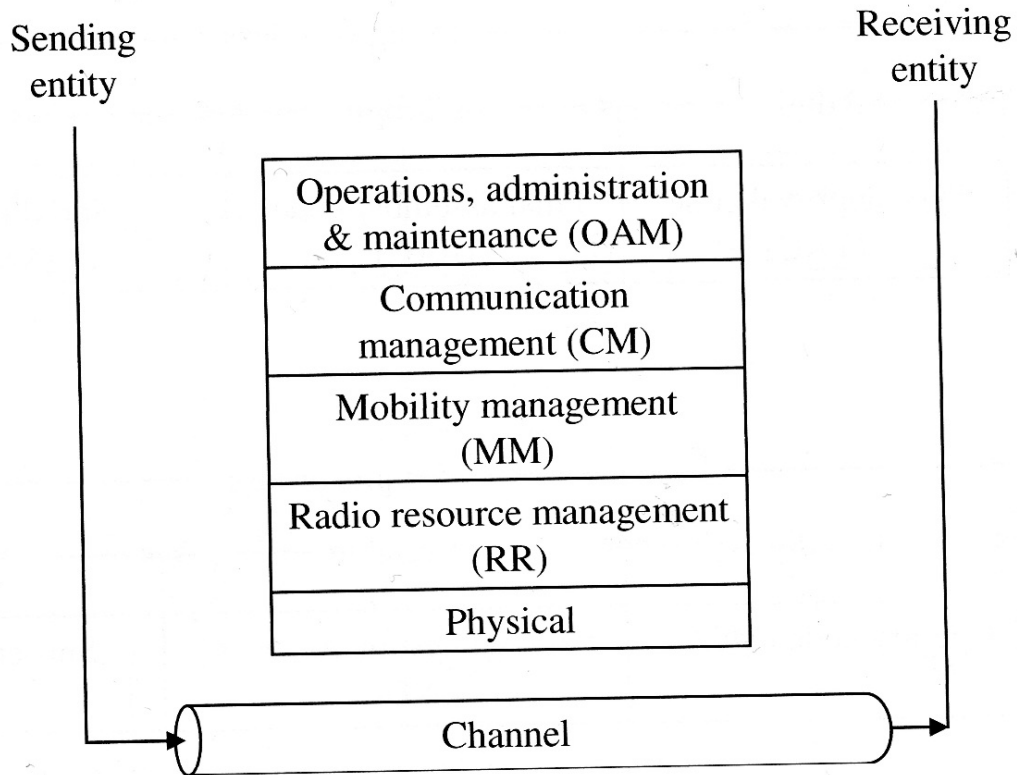
- używany przez MS do identyf. BS, • wykluczanie BS o silniejszym sygnale, ale dalej położonych,
- „problemy graniczne”.

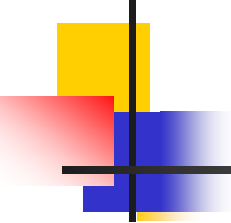
Interfejsy GSM

- W celu komunikacji między różnymi urządzeniami GSM przewidziano szereg interfejsów (MAPn – mobile application part)

| Interface Designation | Between | |
|-----------------------|---------|---------|
| U_m | MS-BTS | |
| A_{bis} | BTS-BSC | |
| A | BSC-MSC | |
| MAPn | B | MSC-VLR |
| | C | MSC-HLR |
| | D | HLR-VLR |
| | E | MSC-MSC |
| | F | MSC-EIR |
| | G | VLR-VLR |

Funkcjonalność GSM



- 
- **RR** ustanawia stabilne połączenia między MS-i oraz MSC i podtrzymuje je niezależnie od mobilności MS-ów; funkcje RR wykonywane są głównie przez MS-y i BSC-y
 - Funkcje **MM** (łącznie z bezpieczeństwem) są realizowane przez MS (lub SIM), HLR/AUC oraz MSC/VLR
 - **CM** jest używane do ustanawiania połączeń między użytkownikami oraz zarządzania krótkimi wiadomościami
 - **OAM** pozwala operatorowi monitorować i kontrolować system



Uwierzytelnienie w GSM

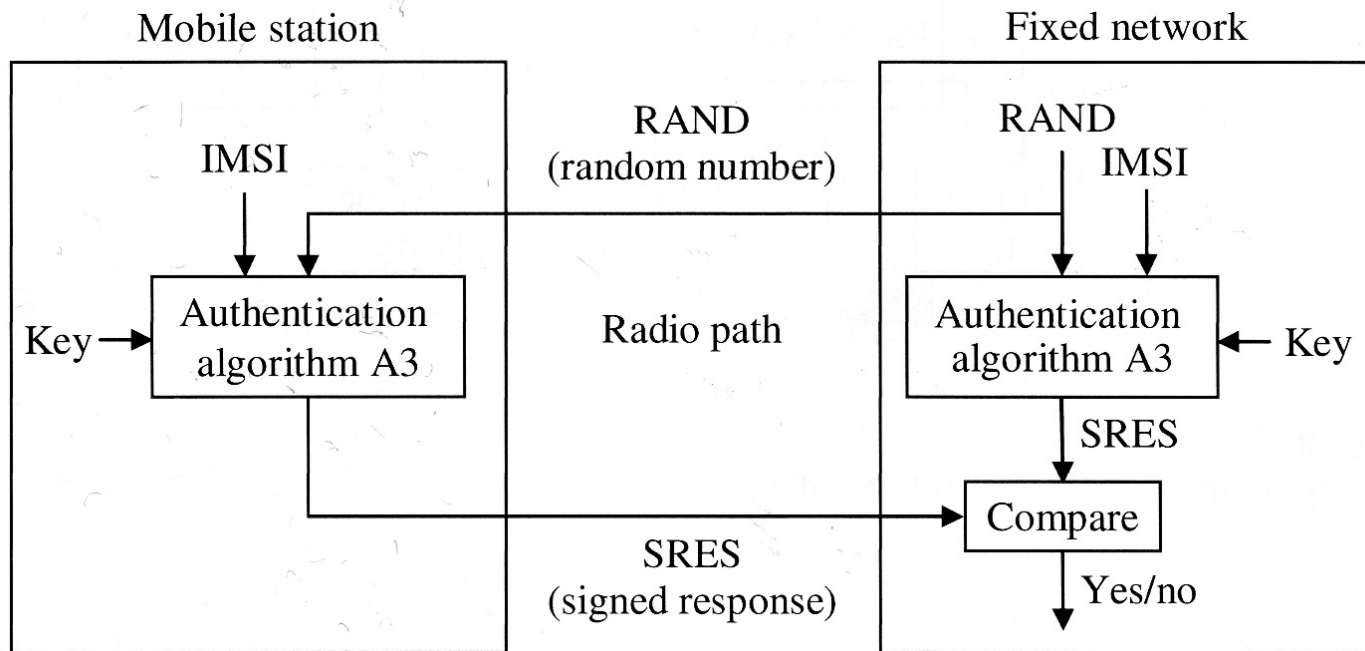
- MS, aby funkcjonować w MSC musi zarejestrować się w BSS, który przydziela kanały po uprzednim uwierzytelnieniu MS-a poprzez dostęp do VLR przez HLR tego MS-a
- Następnie MSC przyznaje MS-wi TMSI i aktualizuje jego VLR i HLR
- W przypadku połączenia nawiązywanego z telefonu w sieci PSTN pakiety przechodzą przez MSC-bramę do MSC, w którym znajduje się MS, po uprzednim pobraniu informacji z domowego HLR danego MS-a
- Jeżeli są to różne MSC-y to VLR bieżącego MSC-a kontaktuje się z HLR MSC-a, który jest domowym MSC-em dla MS-a, który powiadamia bieżącego MSC-a o przemieszczeniu się MS-a
- Tak więc, informacja w tych trzy rejestrach jest modyfikowana



Uwierzytelnienie w GSM

- Uwierzytelnienie w GSM odbywa się z pomocą sieci stałej, która jest używana do porównywania **IMSI** danego MS-a
- Gdy MS chce usługi to sieć stała wysyła do niego losową liczbę, a on używa algorytmu uwierzytelnienia, aby zaszyfrować tę liczbę z użyciem **IMSI** oraz klucza przechowywanego w pamięci
- Sieć stała odszyfrowuje zakodowaną liczbę i w przypadku zgodności obu liczb potwierdza uwierzytelnienie MS-a

Uwierzytelnienie w GSM





Przeniesienie połączenia

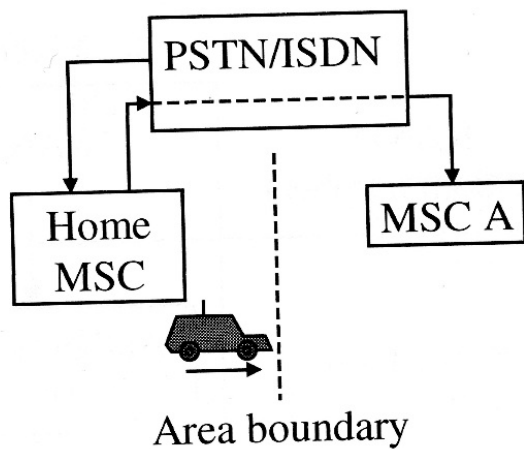
- W GSM istnieją cztery kategorie przeniesienia połączenia
- **Wewnątrz komórki/wewnątrz BTS** (np. z powodu wysokiej interferencji)
 - Następuje zmiana częstotliwości w tej samej komórce lub zmiana szczeliny czasowej
- **Międzykomórkowy/wewnątrz BTS**
 - Następuje zmiana kanału między dwoma komórkami zarządzanymi przez ten sam BSC; jest inicjalizowane przez żądanie jednego z BTS-ów skierowane do MSC



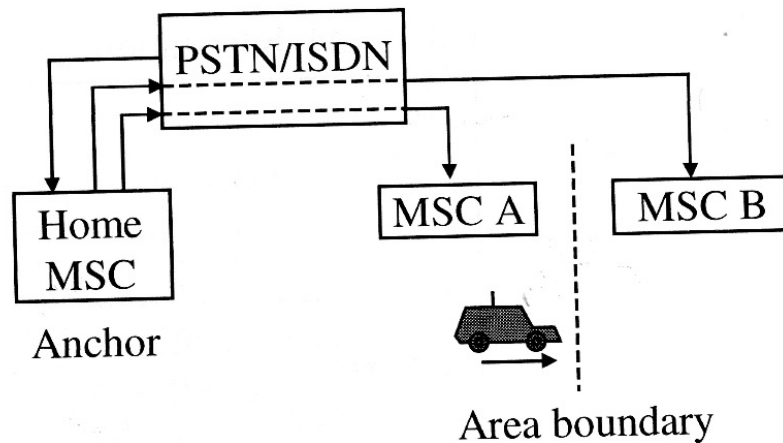
Przeniesienie połączenia

- **Między BSC/wewnątrz MSC**
 - Między komórkami obsługiwanymi przez różne BSC-y, ale podlegające jednemu MSC (gdy np. siła sygnału MS jest niższa niż dopuszczalny próg)
- **Między MSC-ami**
 - Połączenie jest zmieniane gdy MS przechodzi z komórki jednego MSC do komórki drugiego MSC (2 opcje)
 - **Bazowe przeniesienie** połączenia
 - **Kolejne przeniesienie** połączenia

Przeniesienie połączenia



(a) Basic handoff



(b) Subsequent handoff



SMS-y

- W tym celu w GSM wykorzystuje nieużywane zakresy (kanały sterujące)
- Potwierdza dostarczenie wiadomości
- Jest to usługa typu **zachowaj i przekaż** realizowana poprzez centra SMS-we (a nie bezpośrednio między nadawcą i odbiorcą); wiadomość może więc być przechowywana jeżeli odbiorca nie jest dostępny
- Realizowana równolegle z wysyłaniem/otrzymywaniem głosu/danych/faksu
- Pojedynczy SMS: do 160 znaków