

Sieci urządzeń mobilnych

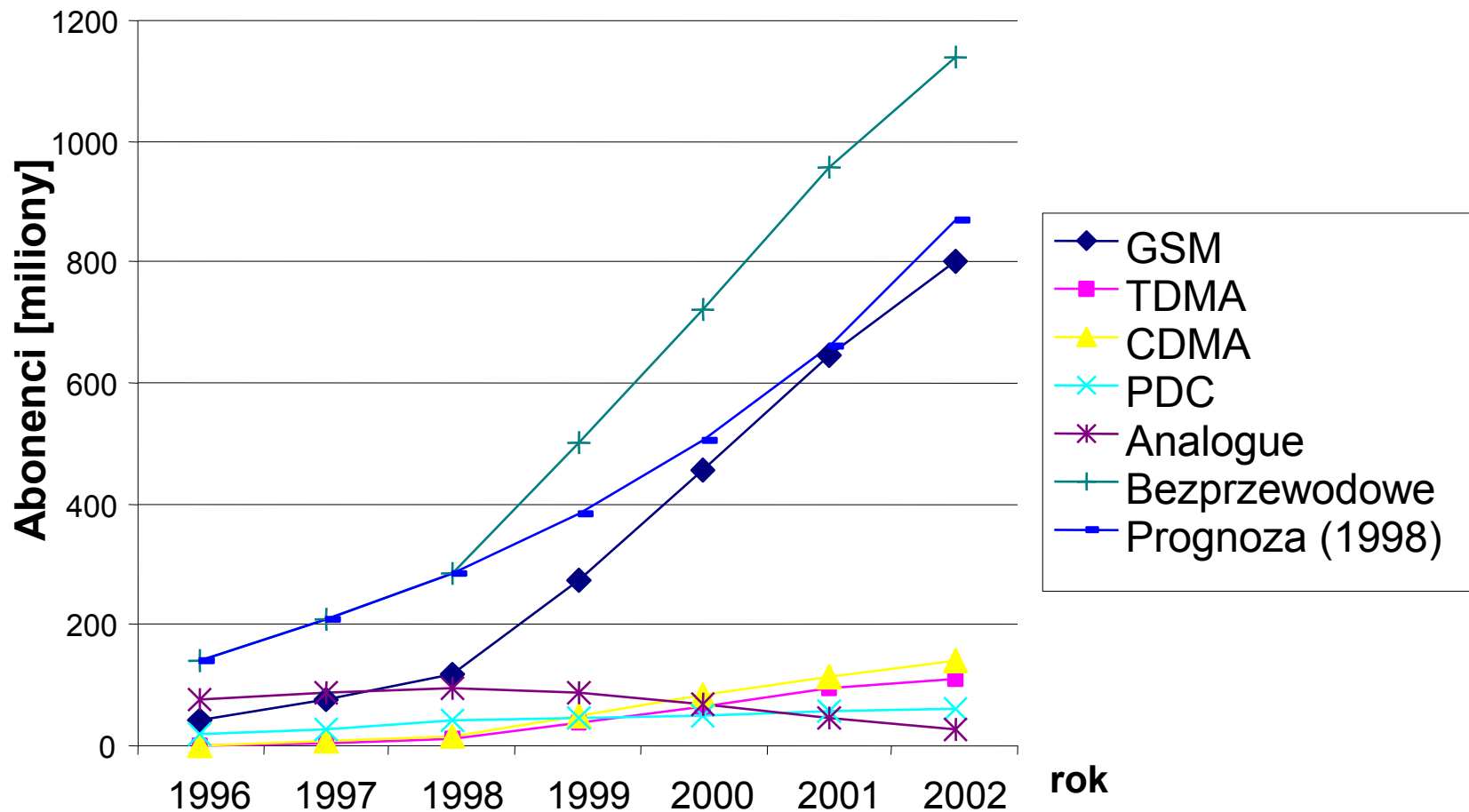
Część 3 wykładu

SKO2

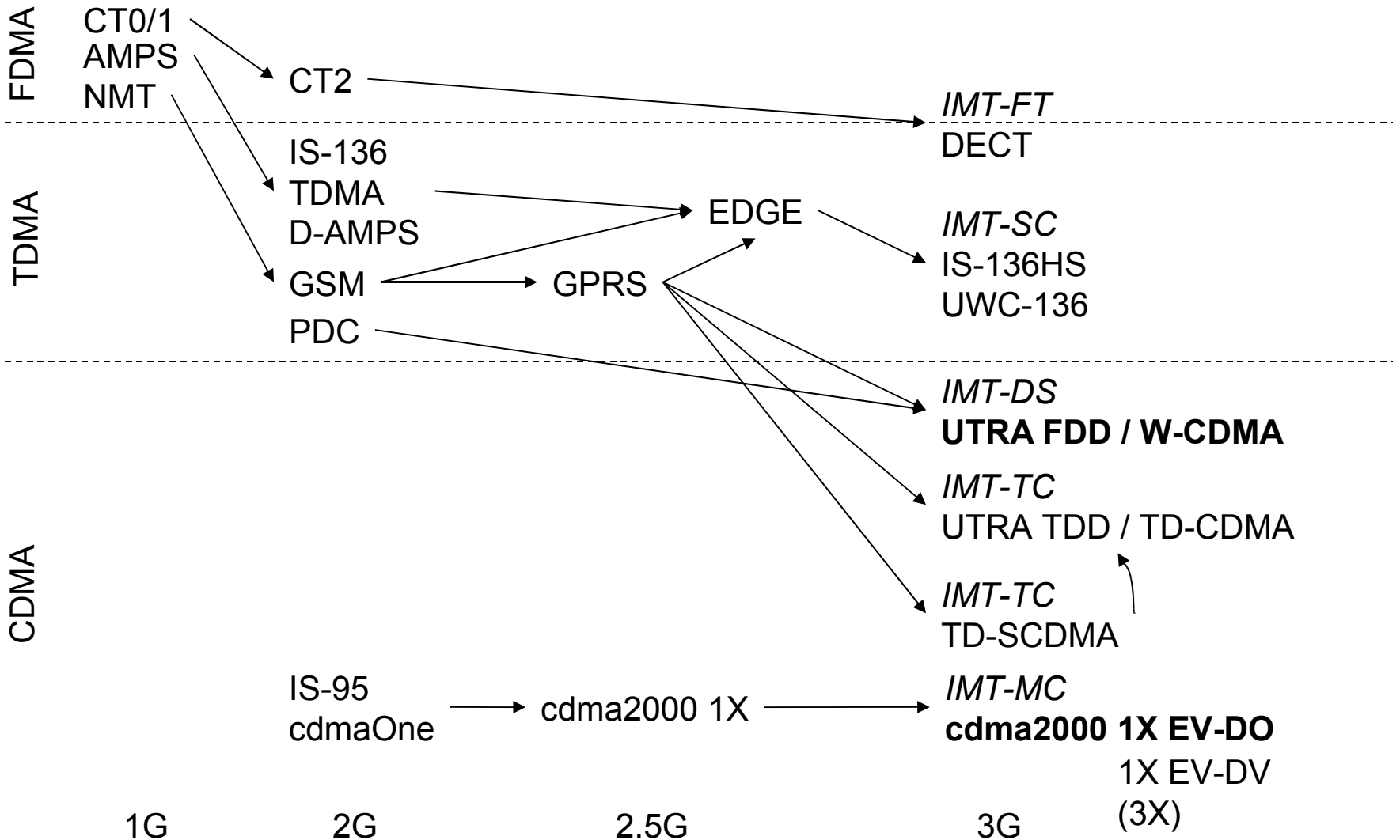
Mapa wykładu

- ❑ Wprowadzenie
 - Dlaczego mobilność?
 - Rynek dla mobilnych urządzeń
 - Dziedziny badań
- ❑ Transmisja radiowa
- ❑ Protokoły wielodostępowe
- ❑ *Systemy GSM*
- ❑ Systemy satelitarne
- ❑ Bezprzewodowe sieci lokalne

Telefonia mobilna na świecie



Rozwój mobilnych systemów telekomunikacyjnych



Historia GSM

- We wczesnych latach 1980tych, szybki wzrost analogowej telefonii komórkowej w Europie
- Różne kraje mają niekompatybilne urządzenia i działania
- **Groupe Spécial Mobile (GSM) (1982)**
 - Dobra jakość mowy
 - Mały koszt terminali i usług
 - Obsługa międzynarodowego roamingu
 - Obsługa naręcznych terminali
 - Obsługa wielu nowych usług
 - Wydajność spektralna
 - Kompatybilne z ISDN
- Global System for Mobile Communication
- Usługi komercyjne rozpoczęte w połowie 1991 roku
- w 1993 było 36 sieci GSM w 22 krajach
- Ameryka Północna weszła z opóźnieniem w dziedzinę GSM z wariantem GSM zwanym PCS1900

Historia: c.d.

Dziś:

- swobodny roaming w całej Europie
- wielu dostawców na całym świecie używa GSM (ponad 184 krajów w Azji, Afryce, Europie, Australii, Ameryce)
- ponad 747 milionów abonentów
- ponad 70% wszystkich cyfrowych telefonów używa GSM
- ponad 10 miliardów SMSów miesięcznie w Niemczech, > 360 miliardów/rocznie na świecie

GSM a telefonia tradycyjna (PSTN)

□ Komunikacja

- mobilna, bezprzewodowa (tradycyjna telefonia w ograniczonym zakresie)
- obsługuje komunikację głosu i danych - ale tradycyjna telefonia też

□ Globalna mobilność

- międzynarodowy numer telefoniczny
- karta SIM daje niezależność od aparatu, operatora
- sieć zajmuje się prezentacją dostosowaną do warunków lokalnych

GSM a telefonia analogowa (mobilna)

- Większa ilość użytkowników
 - wydajniejsze wykorzystanie częstotliwości, mniejsze komórki, więcej użytkowników w komórce
- Wysoka jakość transmisji
 - wysoka jakość i odporność dźwięku dla bezprzewodowych, nieprzerwanych rozmów, także przy wysokiej prędkości ruchu (n.p., z samochodów, pociągów)
- Usługi ochrony informacji
 - kontrola dostępu, uwierzytelnienie za pomocą karty SIM i numerów PIN/PUK

Wady GSM

- ❑ Nie ma doskonałych systemów!!
- ❑ brak szyfrowania od końca do końca
- ❑ brak pełnej przepustowości ISDN (64 kb/s) do użytkownika
- ❑ zmniejszanie koncentracji przy prowadzeniu pojazdów
- ❑ promieniowanie elektromagnetyczne
- ❑ utrata prywatności
- ❑ dostępność informacji o lokalizacji
- ❑ duża złożoność systemu
- ❑ braki kompatybilności w standardach GSM

Usługi udostępniane przez GSM



- usługi nośne: usługi komunikacji danych pomiędzy punktami dostępowymi
 - komunikacja danych do 9,6 Kb/s
- usługi telekomunikacyjne:
 - telefonia
 - numery awaryjne
 - SMS: *Short Messages Service* (do 160 bajtów)
 - poczta głosowa
 - faks Group 3
 - poczta elektroniczna
- usługi uzupełniające
 - Identyfikacja
 - blokowanie połączeń
 - przekazywanie połączeń

Architektura systemu GSM



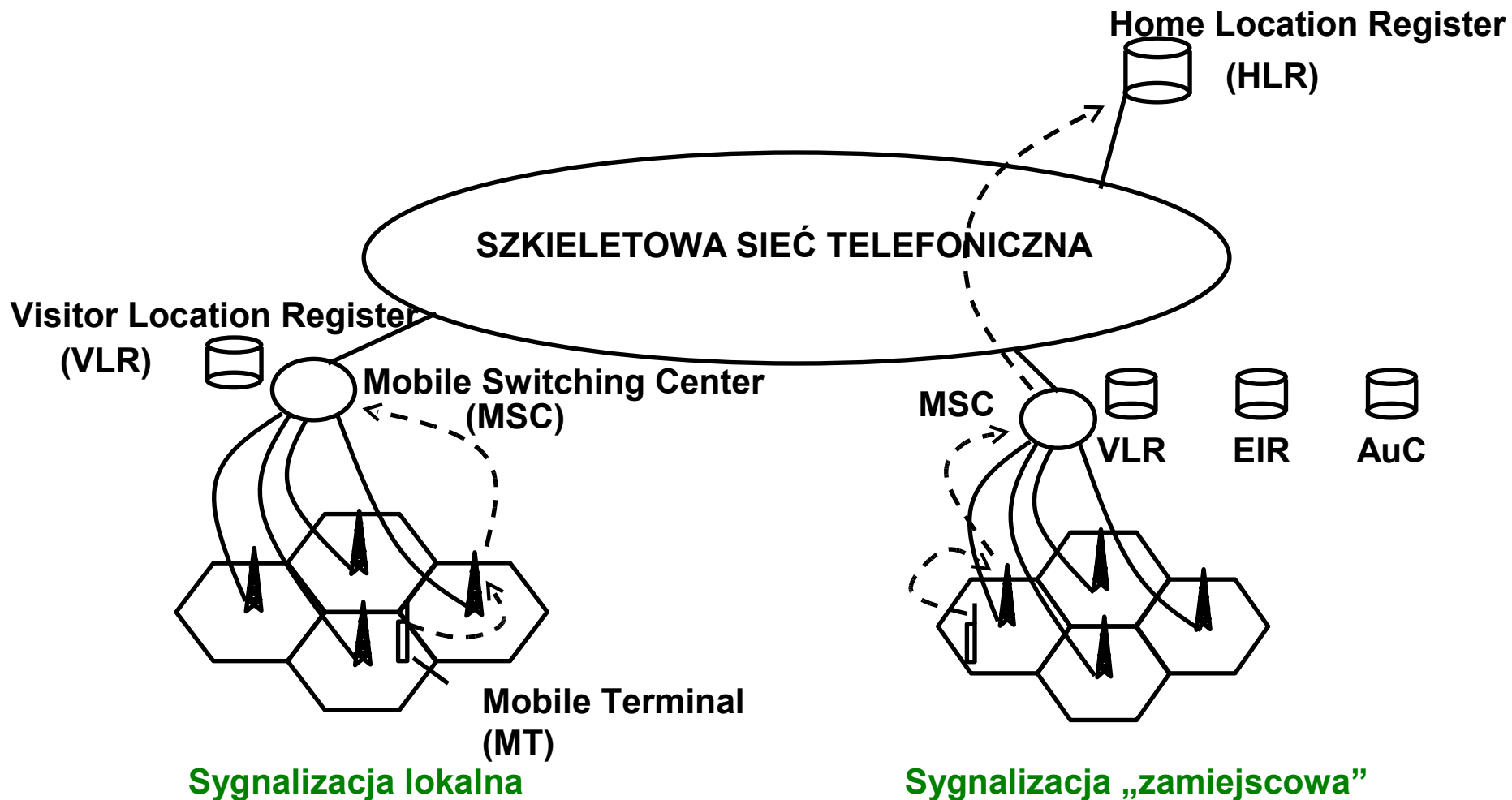
- GSM jest siecią PLMN (*Public Land Mobile Network*)
 - wielu dostawców może tworzyć sieci w standardzie GSM w jednym kraju
 - składniki:
 - MS (stacja mobilna): noszona przez abonenta, zawiera
 - urządzenie mobilne (terminal)
 - kartę *smart card* zwaną *Subscriber Identity Module* (SIM)
 - użytkownik może mieć dostęp do usług objętych abonamentem niezależnie od terminala

Architektura systemu GSM

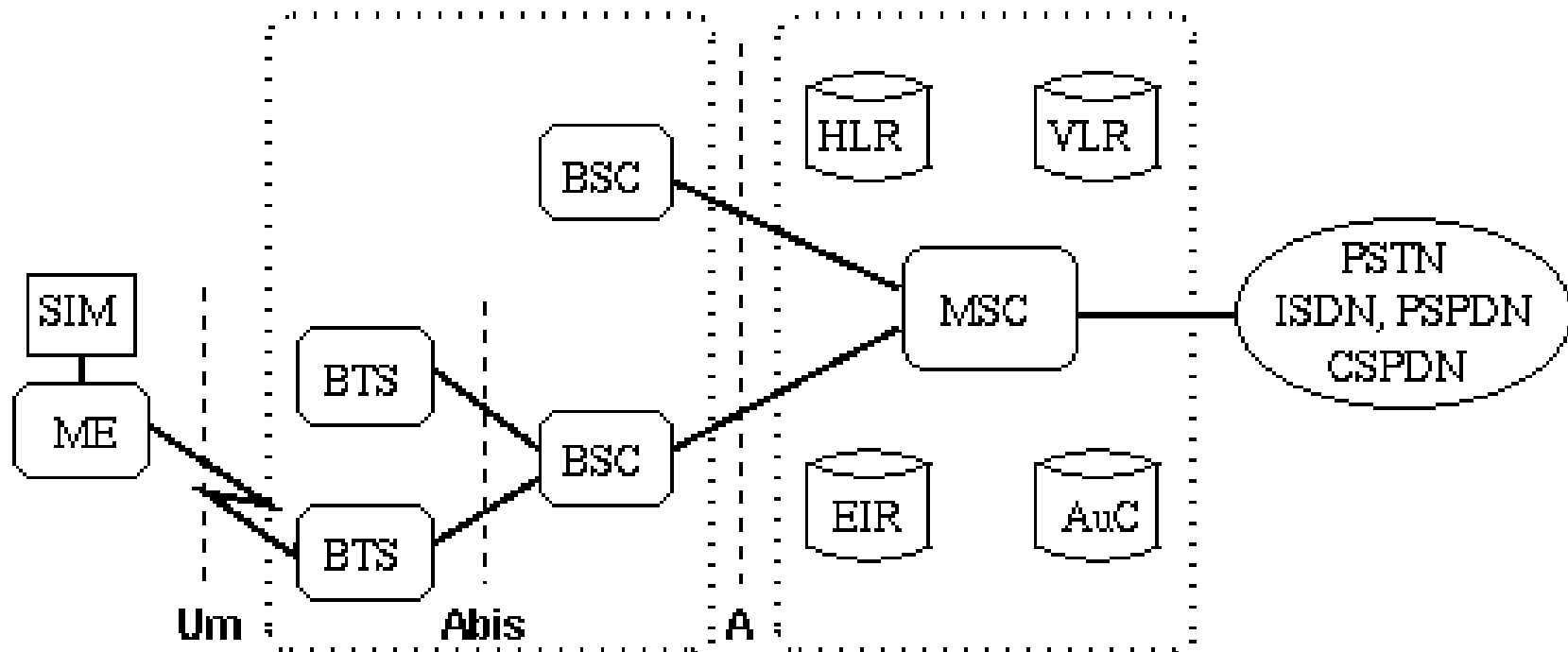


- BS (stacja bazowa, *base station*): steruje łączem radiowym do stacji mobilnej MS
- MSC (*mobile switching center*): przełącza połączenia mobilnych użytkowników, także pomiędzy użytkownikami mobilnymi i PSTN
- LR (*location register*)
- podsystemy
 - RSS (radiowy): obejmuje wszystkie aspekty radiowe
 - NSS (sieci): przełączanie, przekazywanie połączeń, przekazywanie między komórkami
 - OSS (operacyjny): zarządzanie siecią

Architektura systemu GSM



Architektura systemu GSM



**Mobile
Station**

Base Station Subsystem

Network Subsystem

SIM Subscriber Identity Module
 ME Mobile Equipment
 BTS Base Transceiver Station

BSC Base Station Controller
 HLR Home Location Register
 VLR Visitor Location Register

MSC Mobile services Switching Center
 EIR Equipment Identity Register
 AuC Authentication Center

Podsystem radiowy

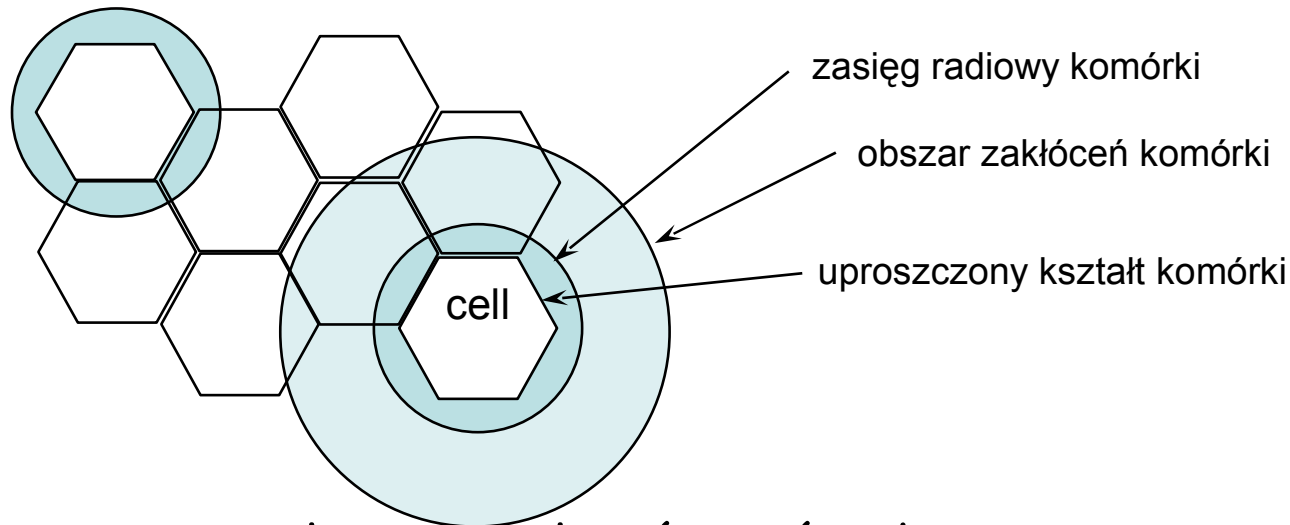


- ❑ Podsystem radiowy obejmuje sieć komórkową aż do przełączników
- ❑ Składniki
 - podsystem stacji bazowej (*Base Station Subsystem, BSS*):
 - Base Transceiver Station (BTS): składniki radiowe, w tym nadajnik, odbiornik, antena
 - Base Station Controller (BSC): przełączanie pomiędzy BTS, sterowanie BTS, zarządzanie zasobami radiowymi
 - $BSS = BSC + \text{suma}(BTS) + \text{połączenia}$
 - Stacje mobilne (MS)

GSM: sieć komórkowa



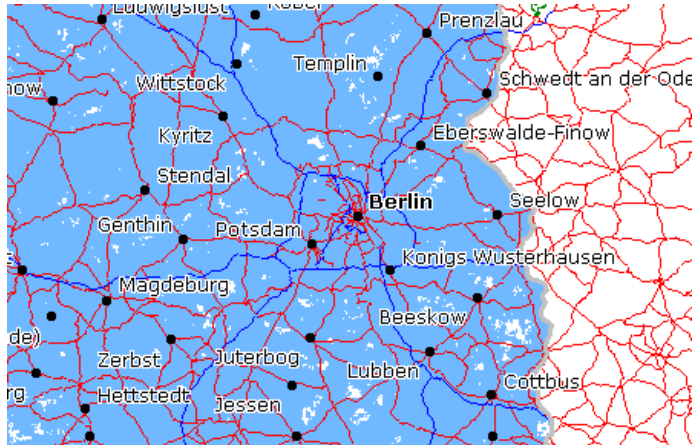
podział obszaru na komórki



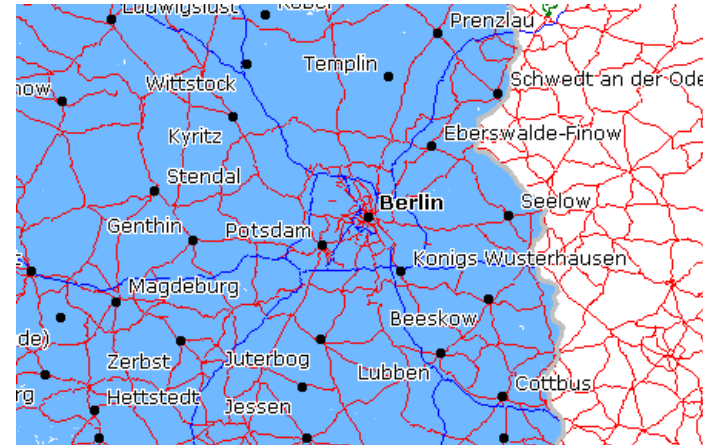
- używa wielu częstotliwości nośnych
- różne częstotliwości w sąsiednich komórkach
- rozmiary komórek wahają się od 100 m do 35 km zależnie od gęstości użytkowników, geografii, mocy nadajnika itd.
- sześciokątny rozmiar komórek to uproszczenie (komórki nakładają się, rozmiary zależą od geografii)
- jeśli mobilny użytkownik zmienia komórkę:
 - ⇒ przekazanie (*handover*) połączenia do sąsiedniej komórki

Przykładowy zasięg sieci GSM

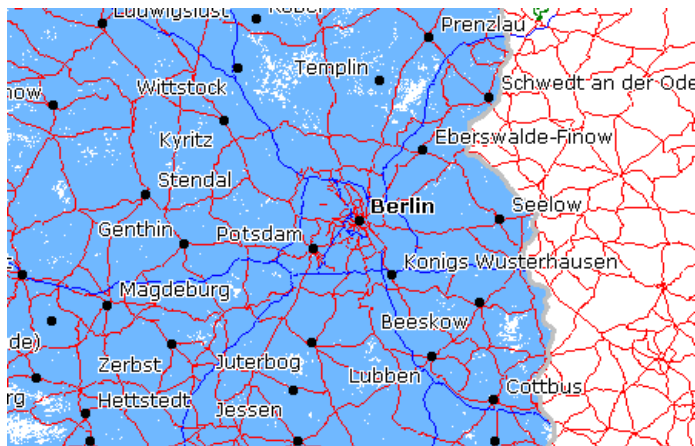
T-Mobile (GSM-900/1800) Berlin



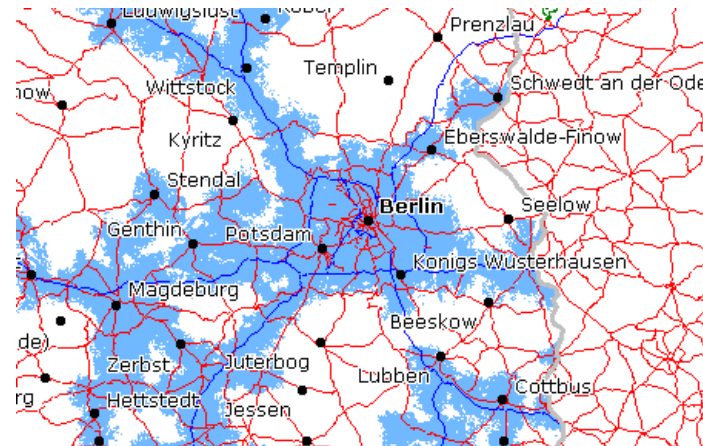
Vodafone (GSM-900/1800)



e-plus (GSM-1800)



O₂ (GSM-1800)



BTS a BSC

Funkcja	BTS	BSC
Zarządzanie kanałami radia		X
Skakanie po częstotliwościach	X	X
Zarządzanie kanałami naziemnymi		X
Odwzorowanie kanałów naziemnych na radiowe		X
Kodowanie i dekodowanie kanału	X	
Adaptacja przepustowości	X	
Szyfrowanie	X	X
Paging	X	X
Pomiar sygnału uplink	X	
Pomiary ruchu		X
Uwierzytelnienie		X
Rejestrowanie i aktualizacja położenia		X
Przekazywanie (Handover)	SKO2	X

Stacja mobilna



- Terminal do usług GSM
- Stacja mobilna (MS) składa się z:
 - MT (*Mobile Termination*):
 - oferuje funkcje wykorzystywane przez wszystkie usługi MS
 - odpowiada punktowi zakończenia sieci (*Network Termination, NT*) w sieci dostępowej ISDN
 - punkt końcowy interfejsu radiowego (U_m)
 - Wykonuje wszystkie czynności multipleksacji (TDMA, FDMA)

Stacja mobilna



- TA (Terminal Adapter):
 - adaptacja terminala,
- TE (Terminal Equipment):
 - urządzenie peryferyjne MS, oferuje usługi użytkownikowi
 - nie zawiera funkcji GSM
 - przykład: aparat fotograficzny
- SIM (Subscriber Identity Module):
 - personalizuje stację mobilną, zapisuje parametry użytkownika
 - Zawiera: PIN, PUK, Klucz uwierzytelnienia K_i , międzynarodowy identyfikator użytkownika IMSI
- Dynamiczne informacje przechowywane przez MS
 - Klucz szyfrowania K_c , tymczasowy identyfikator TMSI, identyfikator obszaru LAI

Podsystem sieci



- *Network Switching Subsystem* NSS jest głównym składnikiem sieci GSM
 - przełączenie, zarządzanie mobilnością, połączenia z innymi sieciami, sterowanie systemem
- Składniki
 - *Mobile Services Switching Center* (MSC) steruje wszystkimi połączeniami do/z mobilnego terminala w domenie MSC przez oddzielną sieć
 - wiele BSC może być zarządzanych przez jednego MSC

Podsystem sieci



- Bazy danych
 - ważne: skalowalność, duży rozmiar, małe opóźnienie
- *Home Location Register (HLR)*

centralna baza danych z danymi użytkownika, stałe i pół-stałe dane użytkownika są przypisywane do HLR (jeden operator może mieć wiele HLR)

 - Dane o użytkowniku: numer ISDN (MSISDN), zamówione usługi (przekazywanie połączeń, roaming, GPRS), międzynarodowy identyfikator (IMSI), aktualny obszar (LA), numer roamingu (MSRN), aktualny VLR i MSC.
- *Visitor Location Register (VLR)*

lokalna baza dla podzbioru danych użytkownika, w której są dane wszystkich użytkowników znajdujących się aktualnie w domenie VLR

 - Trochę jak cache dla danych z HLR

Mobile Services Switching Center



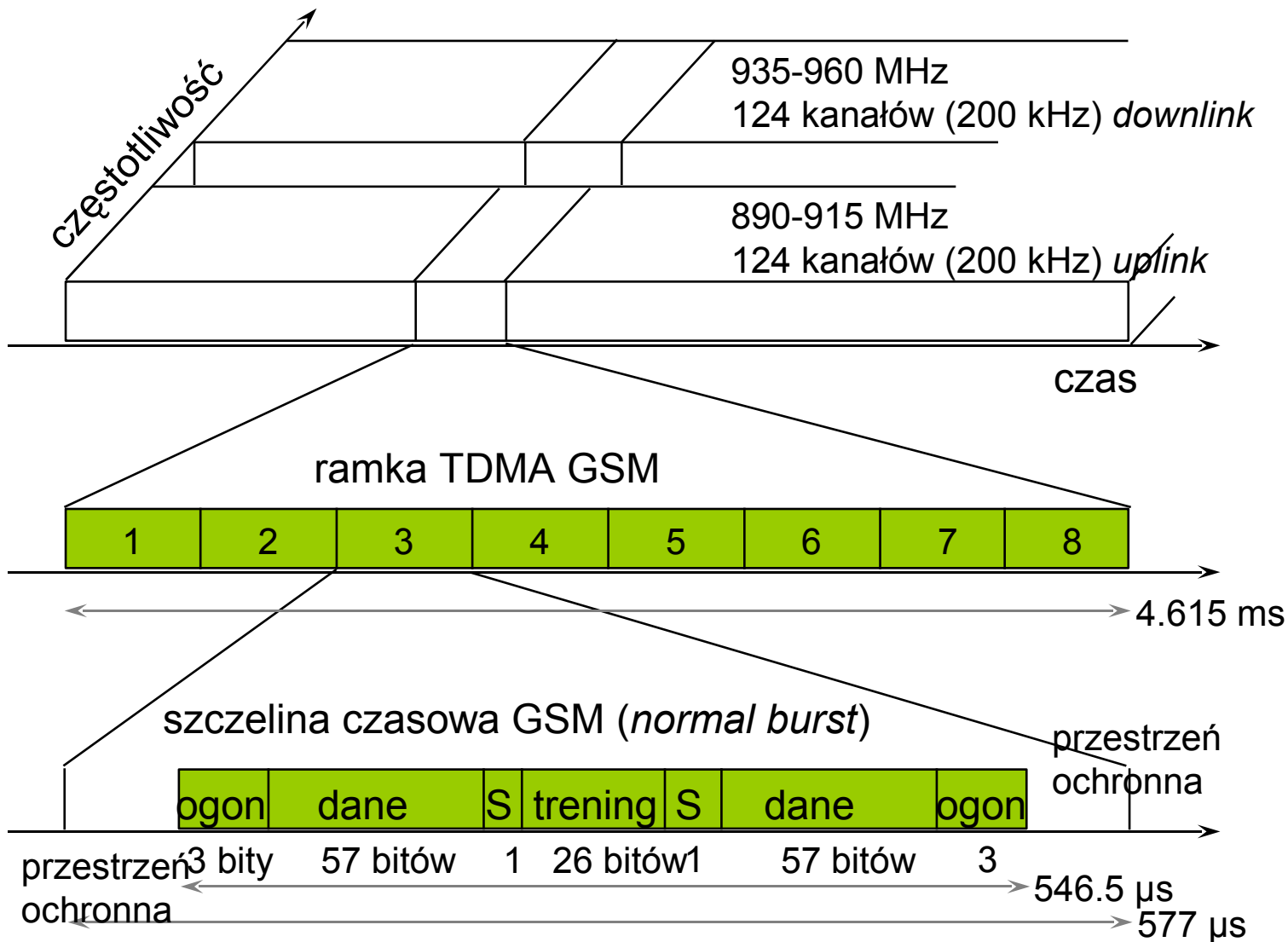
- *MSC (mobile switching center)* ma centralną rolę w *GSM*
 - funkcje przełączania
 - zarządzanie zasobami sieci
 - funkcje intersieci przez *Gateway MSC (GMSC)*
 - integracja wielu baz danych
 - funkcje pagera i przekazywania połączeń
 - rejestracja połączenia i przekazywanie informacji o połączeniu
 - nowe usługi (faks, komunikacja danych)
 - usługa SMS
 - tworzenie i przekazywanie informacji księgowej i bilingowej

Podsystem operacyjny

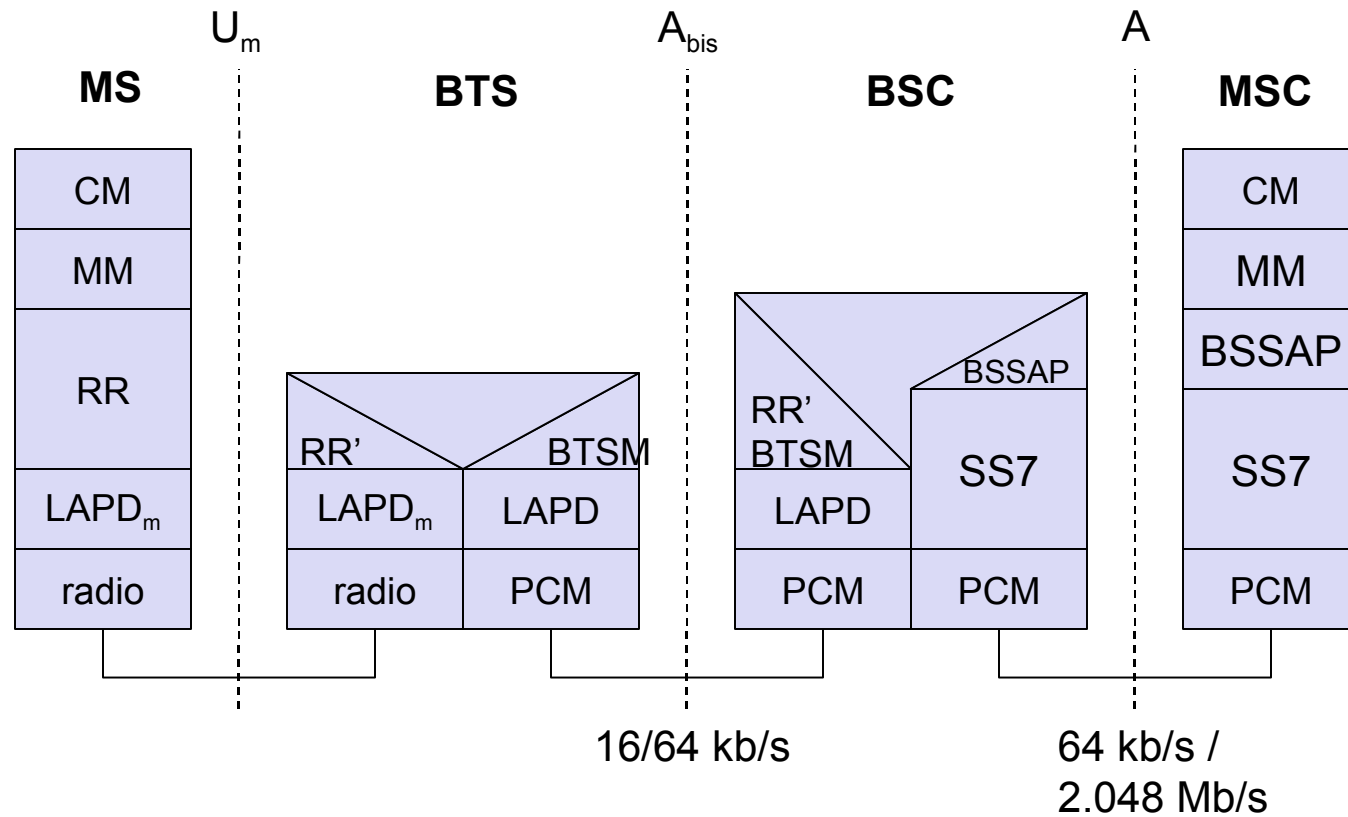


- ❑ *OSS (Operation Subsystem)* pozwala na centralne zarządzanie wszystkimi podsystemami GSM
 - Używa koncepcji TMN!
- ❑ Składniki
 - Centrum uwierzytelnienia (AUC)
 - generuje parametry uwierzytelnienia na żądanie VLR
 - parametry uwierzytelnienia są używane do uwierzytelnienia terminala mobilnego i szyfrowania informacji przez interfejs radiowy systemu GSM
 - Rejestr identyfikacji urządzeń (EIR)
 - rejestruje terminale mobilne GSM i uprawnienia użytkowników
 - skradzione lub uszkodzone terminale mogą być zablokowane i niekiedy zlokalizowane
 - Centrum operacyjne i utrzymaniowe (OMC)
 - różne możliwości sterowania podsystemem radiowym i sieci

GSM-900 - TDMA/FDMA



Protokoły sygnalizacyjne GSM

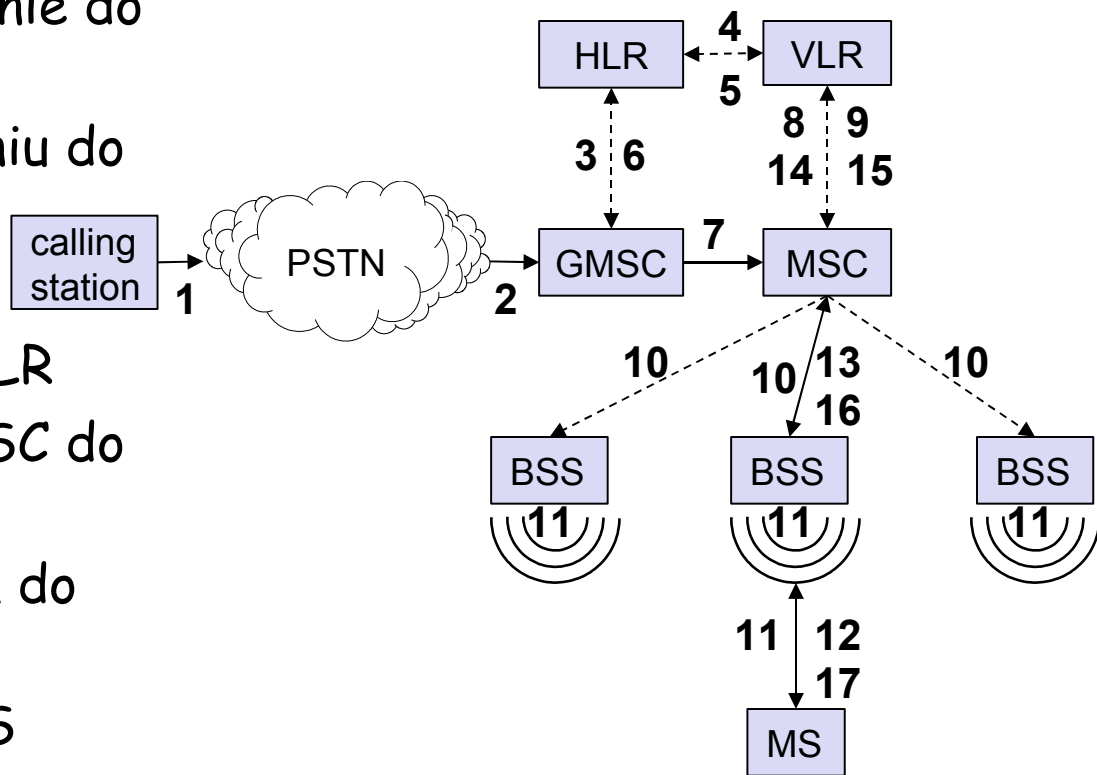


Rozmowa ze stacją mobilną



- ❑ 1: połączenie z abonentem GSM
- ❑ 2: przekazywanie połączenie do GMSC
- ❑ 3: sygnalizacja o połączeniu do HLR

- ❑ 4, 5: żądanie MSRN od VLR
- ❑ 6: przekazanie adresu MSC do GMSC
- ❑ 7: przekazanie połączenia do odpowiedniego MSC
- ❑ 8, 9: pobranie statusu MS
- ❑ 10, 11: paging MS
- ❑ 12, 13: MS odpowiada
- ❑ 14, 15: kontrola bezpieczeństwa
- ❑ 16, 17: tworzenie połączenia

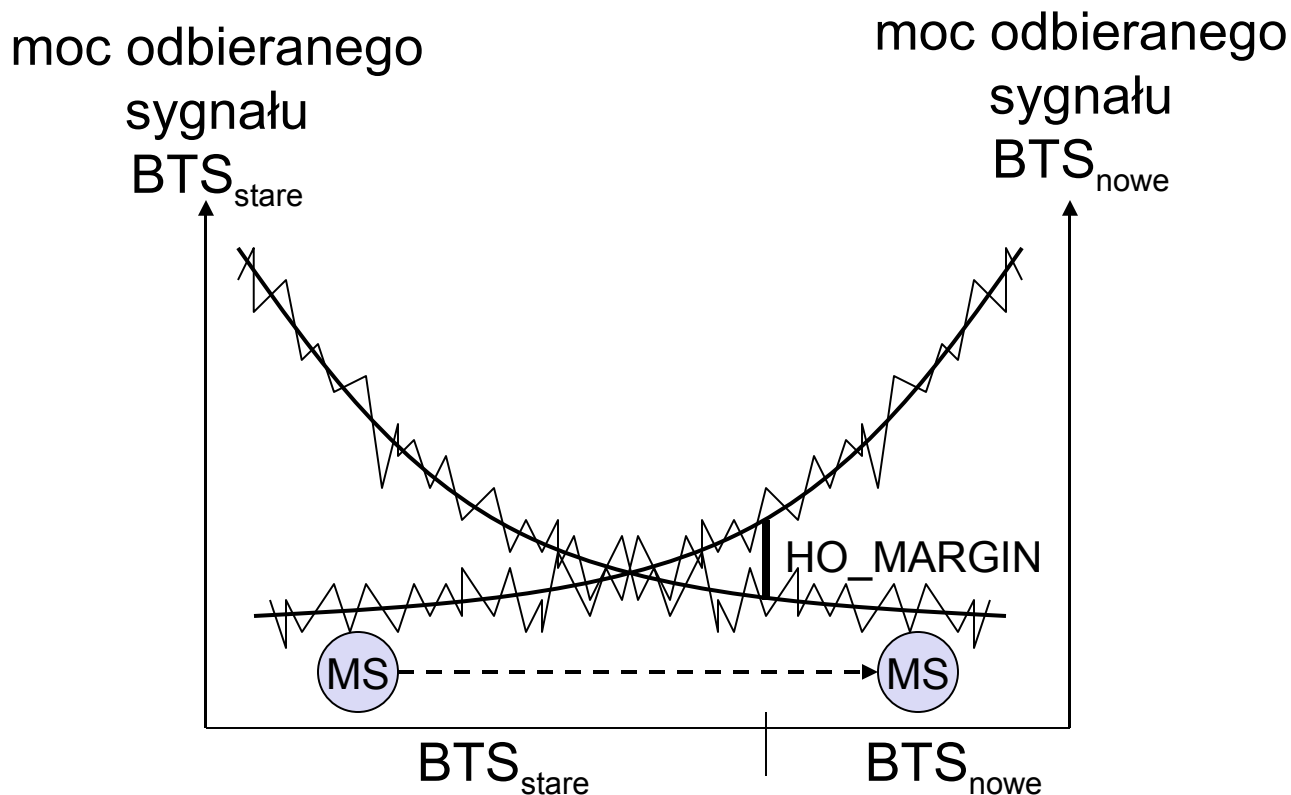


Przekazywanie połączeń



- ❑ Stacja mobilna wychodzi poza zasięg BTS
- ❑ Równoważenie obciążenia
- ❑ przekazywanie wewnątrz komórki:
zakłócenia na jednej częstotliwości mogą spowodować, że BSC zmieni częstotliwość nośną

Decyzja o przekazywaniu



Uwierzytelnienie



- ❑ dwie jednostki funkcjonalne,
 - karta SIM w stacji mobilnej,
 - centrum uwierzytelnienia (AuC)
- ❑ abonent otrzymuje tajny klucz
- ❑ AuC generuje losowy numer i wysyła do terminala
- ❑ Oba używają losowego numeru, razem z tajnym kluczem abonenta oraz algorytmem szyfrującym zwanym A3, żeby wygenerować podpisaną odpowiedź (SRES), która jest wysyłana spowrotem do AuC
- ❑ Stacja zostaje uwierzytelniona, jeśli obie wartości się zgadzają

Ochrona informacji w GSM



□ Usługi

○ poufność

- głos i informacje sygnalizujące są szyfrowane na łączu radiowym (po pomyślnym uwierzytelnieniu)

○ anonimowość

- tymczasowy identyfikator TMSI (*Temporary Mobile Subscriber Identity*)
- przydzielany na nowo po każdej zmianie położenia
- szyfrowana transmisja

□ 3 algorytmy określone dla GSM

- A3 dla uwierzytelnienia ("sekret", otwarty interfejs)
- A5 dla szyfrowania (standaryzowane)
- A8 dla generacji klucza ("sekret", otwarty interfejs)

Komunikacja danych w GSM - 1



- W standardzie, możliwość transmisji tylko 9.6 kb/s
 - zaawansowane kodowanie pozwala na 14,4 kb/s
 - nie wystarcza dla aplikacji Internetu i multimedialnych
- HSCSD (*High-Speed Circuit Switched Data*)
 - jest to głównie aktualizacja oprogramowania
 - łączy szereg szczelin czasowych w celu zwiększenia przepustowości
 - zaleta: łatwe w użyciu, stała jakość, proste
 - wada: blokowane są kanały do transmisji głosu

Komunikacja danych w GSM - 1



- *GPRS (General Packet Radio Service)*
 - komutacja pakietów
 - używa wolnych ramek tylko, gdy musi wysłać pakiet (n.p., 50 kb/s używając chwilowo 4 szczelin)
 - standard gotów w 1998, wchodzi w użycie w 2001
 - zaleta: bardziej elastyczne
 - wada: potrzebna większa inwestycja (nowy sprzęt)