

dr inż. Sławomir Hausman

Zastosowania bezprzewodowych systemów nadzoru i monitorowania System GSM

Zadanie nr 14 – Studia podyplomowe „Bezprzewodowe systemy nadzoru i monitorowania



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Prezentacja multimedialna
współfinansowana przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego
w projekcie

*„Innowacyjna dydaktyka bez ograniczeń
– zintegrowany rozwój Politechniki Łódzkiej –
zarządzanie Uczelnią,
nowoczesna oferta edukacyjna
i wzmacniania zdolności do zatrudniania
osób niepełnosprawnych”*



Politechnika Łódzka
Instytut Elektroniki

90-924 Łódź, ul. Żeromskiego 116,
tel. 042 631 28 83
www.kapitalludzki.p.lodz.pl



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Prezentacja multimedialna współfinansowana przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Początki były trudne ale ciekawe ...



Foto - Rich Howard



Politechnika Łódzka
Instytut Elektroniki

Zastosowania bezprzewodowych systemów nadzoru i monitorowania : GSM



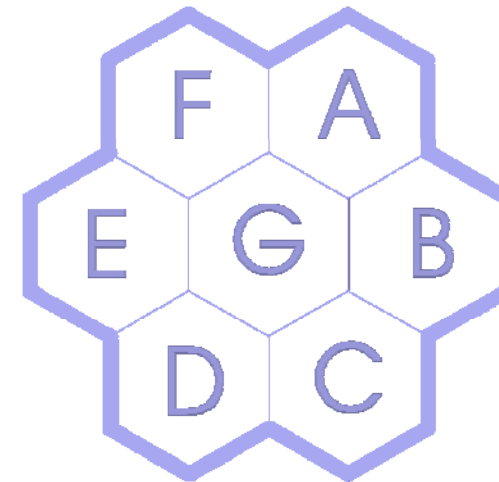
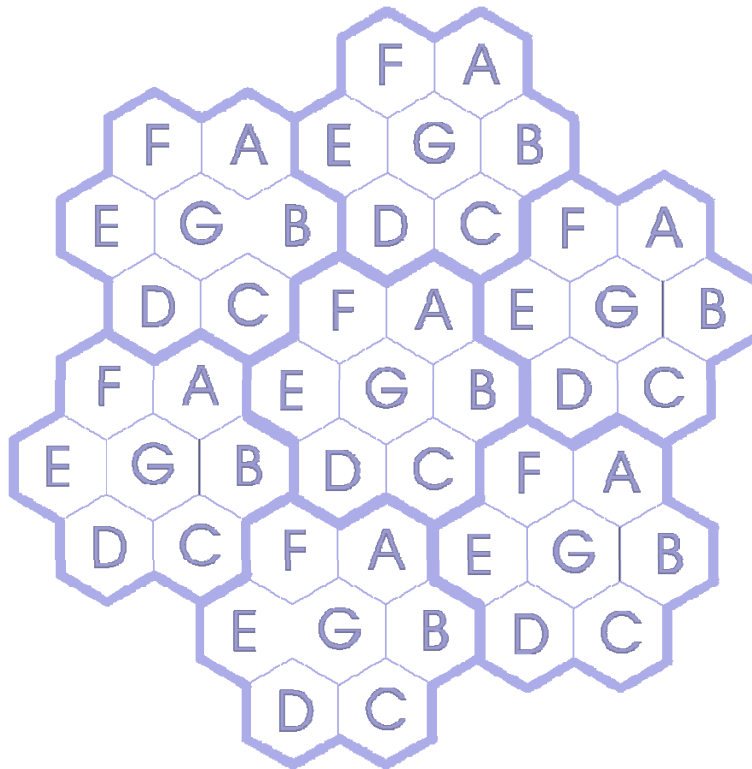
Koncepcja systemów komórkowych

- Stacje bazowe używające tych samych częstotliwości muszą być umieszczone w takich odległościach, aby wzajemnie się nie zakłócały.
- W każdym systemie z powtarzaniem częstotliwości występują zakłócenia wspólnokanałowe. Zadaniem projektantów jest ich **utrzymanie zakłóceń wspólnokanałowych na poziomie dopuszczalnym** dla danego typu transmisji.
- Każda stacja bazowa otrzymuje tylko pewną część z całkowitej puli częstotliwości używanych w systemie. Sąsiadujące ze sobą stacje bazowe używają różnych zestawów częstotliwości, aby uniknąć zbyt silnych zakłóceń wspólnokanałowych.
- **Obszar geograficzny obsługiwany przez jedną stację bazową zwany jest komórką.**
- W systemach z powtarzaniem częstotliwości im większa jest liczba komórek tym większa jest pojemność systemu.





Koncepcja przestrzennego zwielokrotniania częstotliwości



Zespół siedmiokomórkowy

*Koncepcja systemów komórkowych – z przestrzennym zwielokrotnianiem częstotliwości.
Różne litery określają różne zestawy częstotliwości.*





Całkowita pojemność systemu komórkowego

K_F – liczba kanałów FDMA w jednej komórce;

K_T – liczba kanałów TDMA dla jednej nośnej;

$K = K_F K_T$ – liczba kanałów FDMA/TDMA w jednej komórce;

N – liczba komórek w jednym zespole komórkowym – typowo od 4 do 12.

P – liczba zespołów komórkowych w systemie; (PN to liczba wszystkich komórek w systemie)

C – całkowita liczba kanałów w systemie;

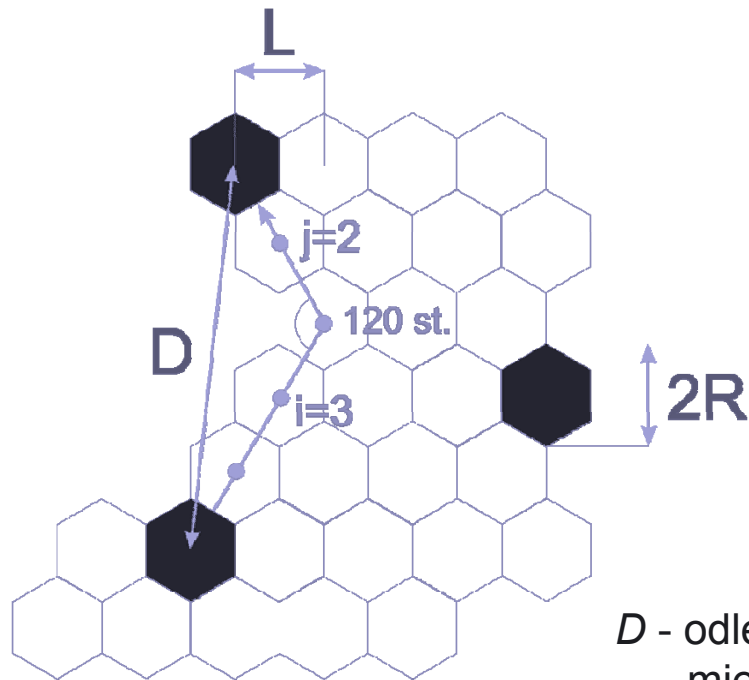
$$C = K_T K_F P N = K P N$$

Jeśli wielkość zespołu N ulega zmniejszeniu, a rozmiar komórki pozostaje stały, to dla zapewnienia łączności na tym samym obszarze trzeba użyć większej liczby zespołów P , ale dzięki temu zwiększa się pojemność systemu.





Geometria heksagonalnych systemów komórkowych



D - odległość koordynacyjna (najmniejsza odległość między stacjami współnokanałowymi)

R - promień komórki

$L = R^{1/3}$ - odległość modułowa

i, j - współzrzedne skośnokątne siatki ze stacją bazową w punkcie $(0,0)$





Liczność zespołów komórkowych

Ponieważ dla powierzchni pokrytej przystającymi do siebie sześciokątami, rozmieszczonymi co 60° każdy z nich ma sześciu równoodległych sąsiadów, to możliwe są tylko niektóre kształty i liczności zespołów N .

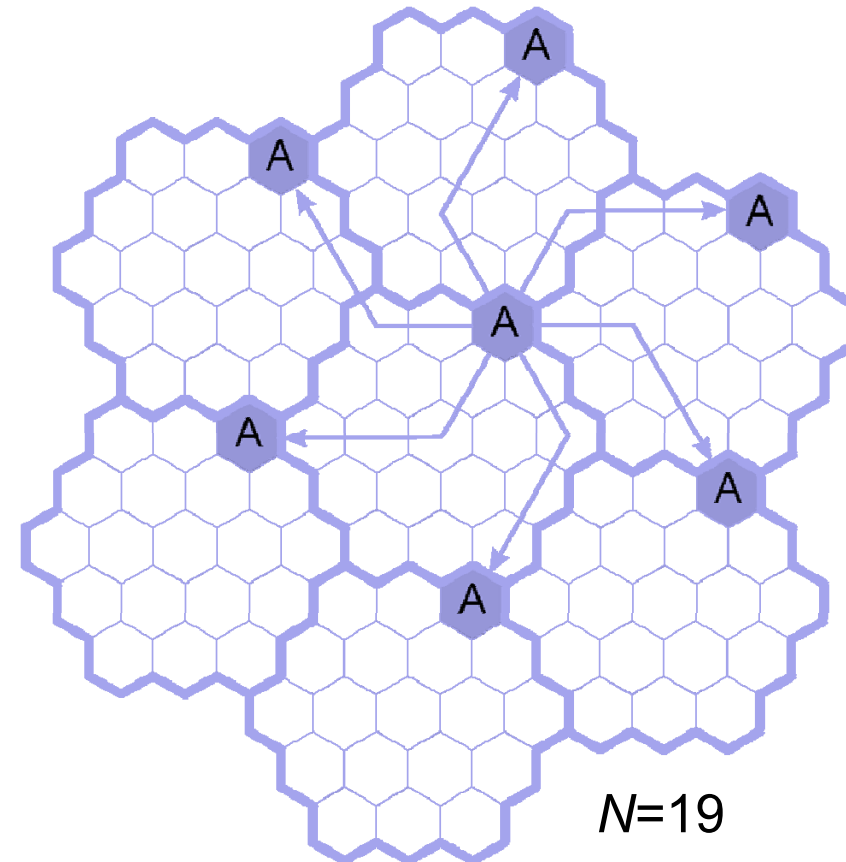
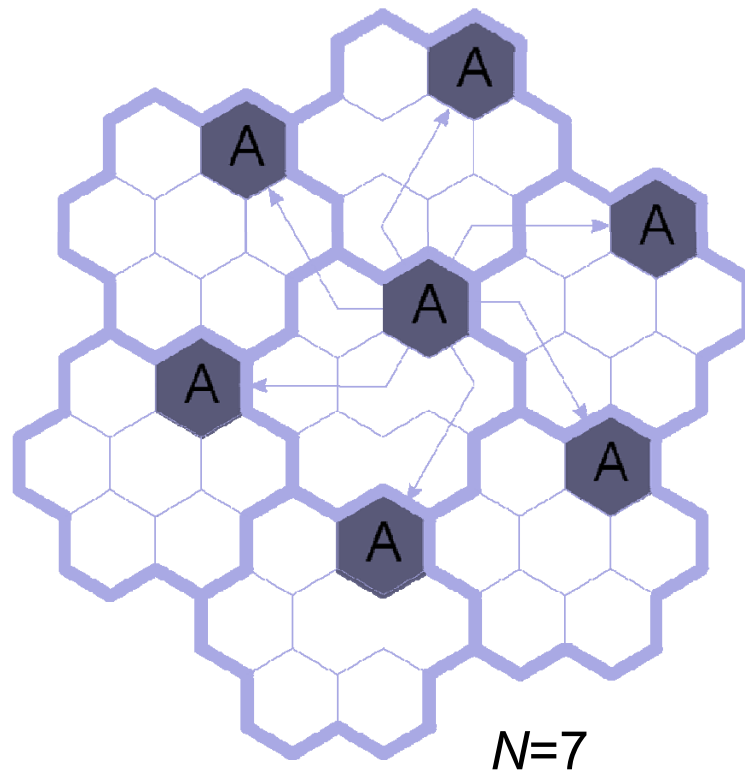
$$N = i^2 + ij + j^2$$

	i=0	i=1	i=2	i=3
j=0	–	1	4	9
j=1	1	3	7	13
j=2	4	7	12	19
j=3	9	13	19	27

Przykładowe liczności zespołów komórkowych. Najczęściej stosowane wielkości zespołów zacieniowano.



Interferencje wspólnokanałowe



Budowa systemu z zespołów o różnej liczności N



Stosunek mocy sygnału do mocy interferencji wspólnokanałowych

$$\frac{C}{I} \approx \frac{C}{\sum_{i=1}^L I_i}$$

gdzie:

C – moc sygnału użytecznego;

I_i – moc zakłócenia pochodzącego od i -tej komórki wspólnokanałowej;

L – liczba komórek wspólnokanałowych.





Zależność mocy odebranej od odległości

W dużym uproszczeniu można przyjąć, że zależność mocy odebranej P_R w danej odległości d od stacji bazowej od mocy P_0 odebranej w pewnej odległości odniesienia d_0 może być wyrażona wzorem

$$P_R = P_0 \left(\frac{d_0}{d} \right)^n$$

ŚRODOWISKO	n
wolna przestrzeń	2
gładka ziemia	4
teren wysoko zurbanizowany	2,5 – 5
wnętrze budynków przy braku widzialności optycznej	4 – 6





Stosunek mocy sygnału do mocy interferencji wspólnokanałowych

$$\frac{C}{I} = \frac{R^{-n}}{\sum_{i=1}^L D_i^{-n}}$$

$$Q = \frac{D}{R} = \sqrt{3N} \quad \text{- współczynnik powtarzania częstotliwości}$$

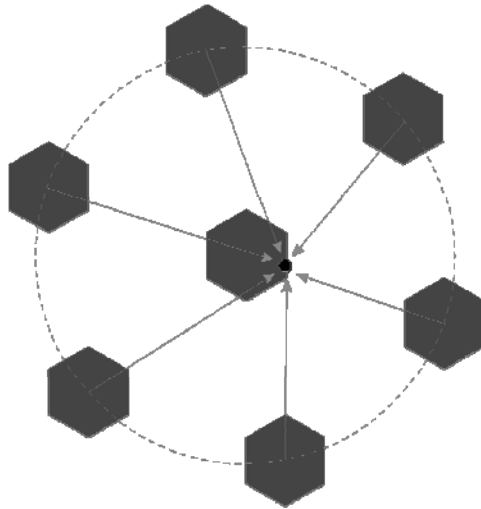
$$\frac{C}{I} = \frac{(D/R)^n}{L} = \frac{Q^n}{L} = \frac{(\sqrt{3N})^n}{L}$$

Im większa jest liczba komórek N w zespole, tym mniejsze są zakłócenia wspólnokanałowe C/I ale jednocześnie tym gorsze jest wykorzystanie zasobów widmowych.



Stosunek mocy sygnału do mocy interferencji wspólnokanałowych

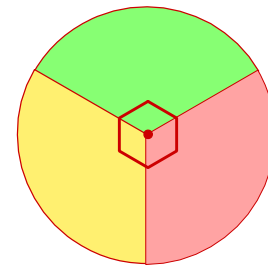
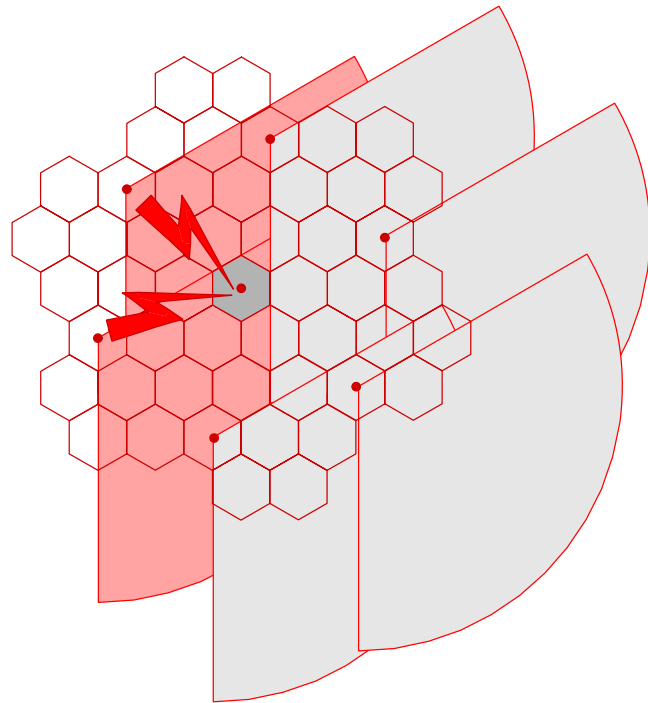
$$\frac{C}{I} = \frac{R^{-n}}{2(D-R)^{-n} + (D-R/2)^{-n} + (D+R/2)^{-n} + (D+R)^{-n} + D^{-n}}$$



$$\frac{C}{I} = \frac{1}{\frac{2(Q+1)^n + (Q-1)^n}{(Q^2-1)^n} + \frac{(Q+0.5)^n + (Q-0.5)^n}{(Q^2-0.25)^n} + \frac{1}{Q^n}}$$

Najgorszy stosunek C/I występuje w przypadku, gdy terminal znajduje się na granicy komórek.

Sektoryzacja



Sektory po 120 stopni



Zakłócenia wspólnokanałowe pochodzą tylko od dwóch komórek z pierwszego pierścienia sąsiadujących zespołów, a nie od 6 jak przy braku sektoryzacji. Sektoryzacja powoduje zmniejszenie efektu wiązki !



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Prezentacja multimedialna współfinansowana przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Przykłady systemów antenowych stacji bazowych GSM



Politechnika Łódzka
Instytut Elektroniki

Zastosowania bezprzewodowych systemów nadzoru i monitorowania : GSM



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Prezentacja multimedialna współfinansowana przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

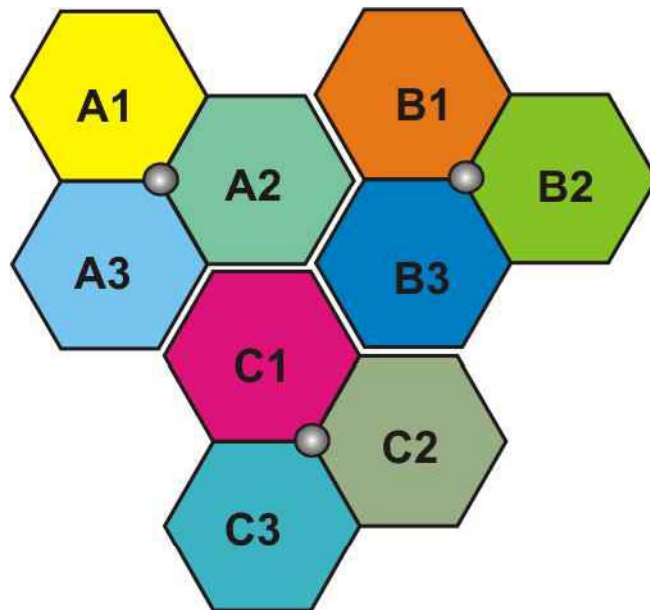
Przykłady systemów antenowych stacji bazowych GSM



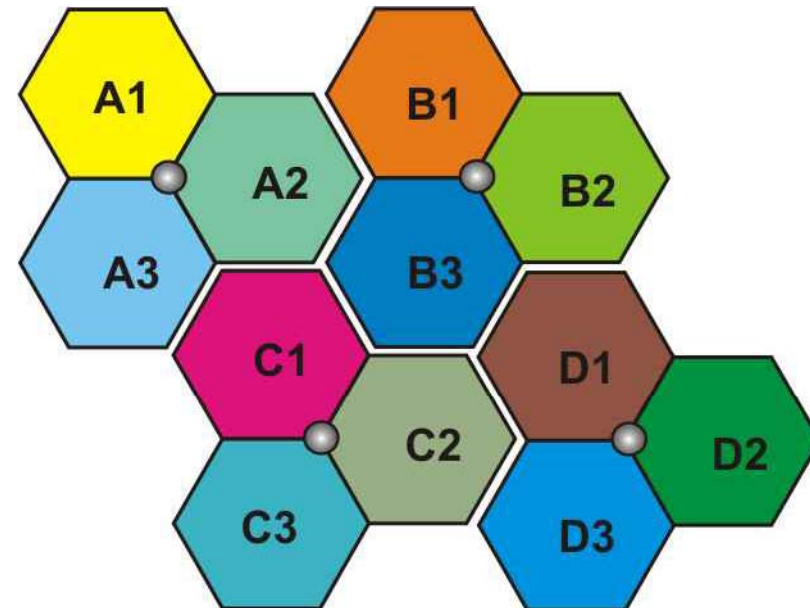
Politechnika Łódzka
Instytut Elektroniki

Zastosowania bezprzewodowych systemów nadzoru i monitorowania : GSM

Schematy przestrzennego zwielokrotniania częstotliwości



3/9

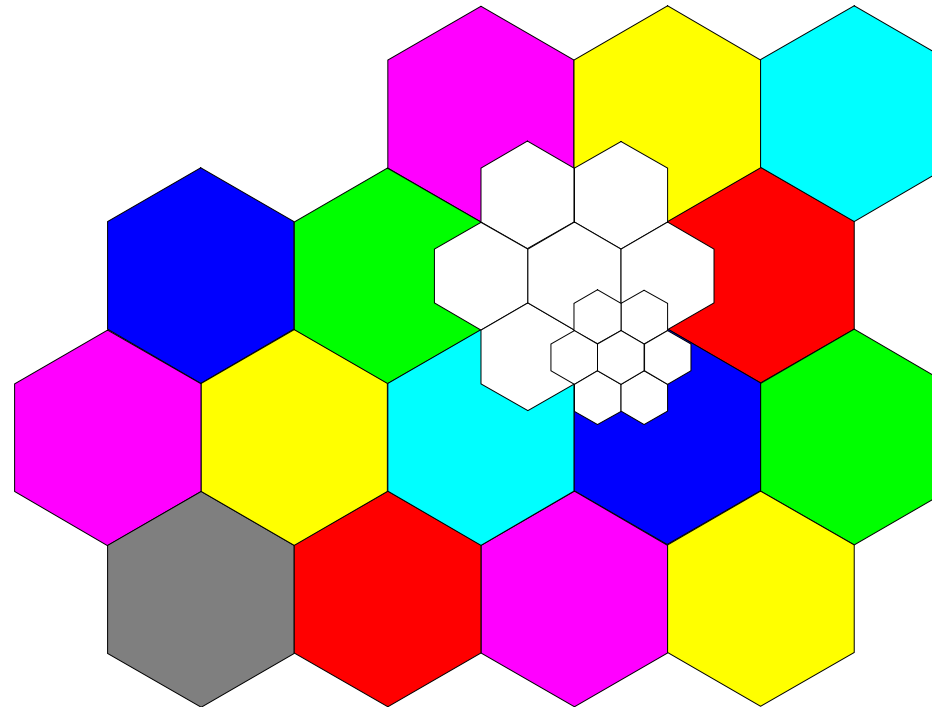


4/12

Typowe zespoły komórkowe z sektoryzacją stosowane w systemach GSM



Podział komórek w obszarach o dużej gęstości ruchu



Podział komórek jest procesem polegającym na zastąpieniu większej komórki zespołem komórek mniejszych. Zwiększa to lokalnie pojemność systemu. Podział komórek może być wprowadzany łatwo i stopniowo, gdyż nie zaburza planu przydziału częstotliwości.



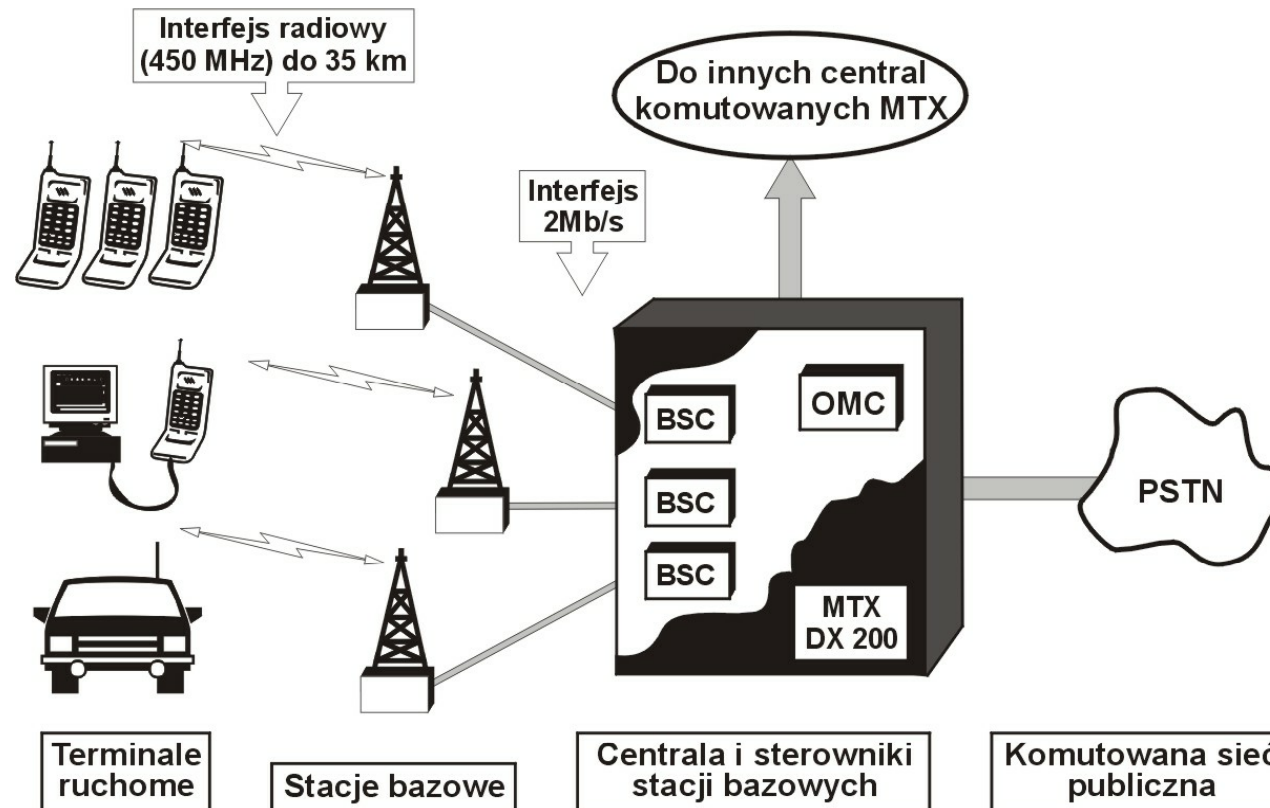


System NMT (Nordic Mobile Telecommunications)

- Pierwszy w Polsce system telefonii komórkowej NMT450i został uruchomiony przez PTK Centertel w czerwcu 1992 roku. Jest on oparty na skandynawskim standardzie NMT, opracowanym w końcu lat 70-tych i uruchomionym w Skandynawii w 1981 roku.
- Duże zainteresowanie ze strony abonentów zmusiło konstruktorów do opracowania zmodyfikowanej wersji systemu, o pięciokrotnie większej pojemności. System ten pod nazwą NMT900 został uruchomiony w Skandynawii w 1986 roku.

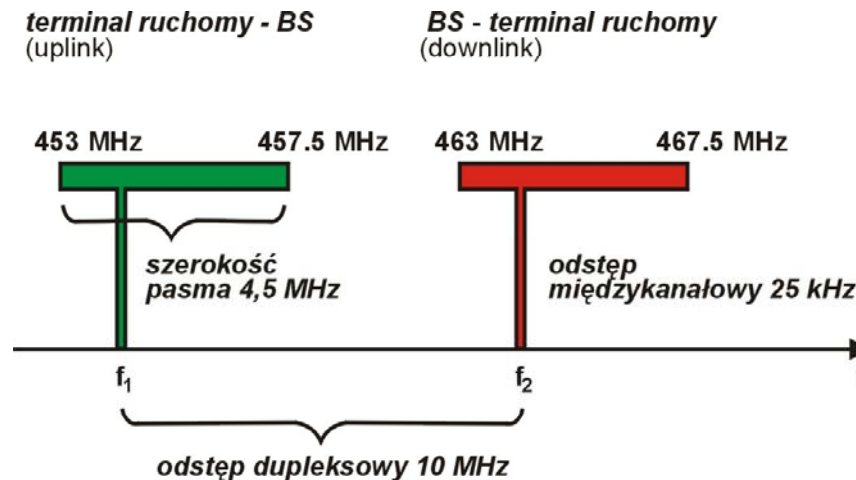


System NMT (Nordic Mobile Telecommunications)



Architektura systemu NMT

System NMT (Nordic Mobile Telecommunication)



- W Polsce na potrzeby NMT wydzielono pasma przesunięte o 500 kHz w dół w stosunku do wymienionych powyżej, tj. 452,5-457 MHz (uplink) i 462,5 - 467 MHz (downlink), system zaś dla odróżnienia nazwano NMT450i.
- Szerokość kanału wynosi 25 kHz. Do transmisji mowy zastosowano analogową modulację FM z dewiacją częstotliwości $f = 5$ kHz.
- W każdej komórce systemu przewidziano przynajmniej jeden kanał, na którym stacja bazowa nadaje swoje dane identyfikacyjne.



System NMT (Nordic Mobile Telecommunication)

- W paśmie 900 MHz dla systemu NMT900 wydzielono dwa zakresy o szerokości 25 MHz każdy (1000 kanałów częstotliwościowych po 25 kHz):
 - 890-915 MHz (transmisja od terminala do stacji bazowej),
 - 935-960 MHz (transmisja od stacji bazowej do terminala).
- Odstęp dupleksowy pomiędzy kierunkami transmisji wynosi 45 MHz.
- W systemie NMT 900 istnieje możliwość wykorzystywania kanałów o szerokości 12,5 kHz. Otrzymuje się wówczas 2000 kanałów.
- Maksymalna moc nadajnika stacji bazowej wynosi 50 W (NMT450) lub 25 W (NMT900), a poziomy mocy terminali ruchomych to: 15 / 1,5 / 0,15 W dla NMT450 oraz 6 / 1 / 0,1 W dla NMT900.





System NMT (Nordic Mobile Telecommunication)

- **Śledzenie położenia abonenta** - odbywa się to z dokładnością do obszaru centralowego. Informacja o bieżącym położeniu terminala jest przekazywana do centrali macierzystej.
- **Zestawianie połączeń** - wywołanie abonenta polega na wysłaniu do obszaru przywołań, na którego terenie on się znajduje wiadomości z numerem wywoływanego terminala. Jest ona rozgłaszana przez wszystkie stacje bazowe tego obszaru. Po rozpoznaniu wywołania terminal zgłasza gotowość do odebrania rozmowy, a centrala przydziela mu wolny kanał radiowy.
- **Przełączanie kanałów** w czasie rzeczywistym - realizowane przez centralę MTX na podstawie wyników pomiaru jakości połączenia wykonywanych przez stację bazową:
 - poziom mocy sygnału odbieranego od stacji ruchomej,
 - wartość stosunku sygnału do szumu SNR specjalnego sygnału pilota o częstotliwości ok. 4 kHz, a więc leżącej ponad pasmem rozmównym terminala (Sygnał pilota jest nadawany do terminala, a następnie odsyłany przez niego do stacji bazowej.).





System NMT (Nordic Mobile Telecommunication)

Usługi

- analogowa transmisja głosu;
- transmisja danych (600 bit/s) - przez przystawkę modemową podłączaną do stacji ruchomej;
- warunkowe i bezwarunkowe przenoszenie rozmów;
- selektywne blokowanie połączeń;
- połączenia konferencyjne;
- poczta głosowa;
- zdalne sterowanie za pomocą kodów klawiszy DTMF.





Historia powstania systemu GSM

- 1982 – W ramach CEPT (fr. Conférence Européenne des Postes et Télécommunications) powstała grupa robocza GSM (fr. Groupe Spéciale Mobile). Zadaniem GSM było opracowanie systemu komórkowego wspólnego dla Unii Europejskiej. Założenia: wspólny interfejs radiowy, znacząco większa pojemność niż dla systemów analogowych, konkurencyjne koszty.
- 1986 – GSM podejmuje decyzję o tym, że nowy system będzie cyfrowy (lepsze wykorzystanie zasobów widmowych, szyfrowanie mowy,).
- 1987 – Podpisanie przez 13 krajów GSM MoU (ang. GSM Memorandum of Understanding).
- 1989 – Przejęcie prac standaryzacyjnych przez ETSI (ang. European Telecommunications Standards Institute) oraz zmiana znaczenia skrótu GSM (ang. Global System for Mobile communications).
- 1992 – Uruchomienie pierwszych komercyjnych systemów GSM.
- 1996 – Uruchomienie dwóch sieci GSM w Polsce.



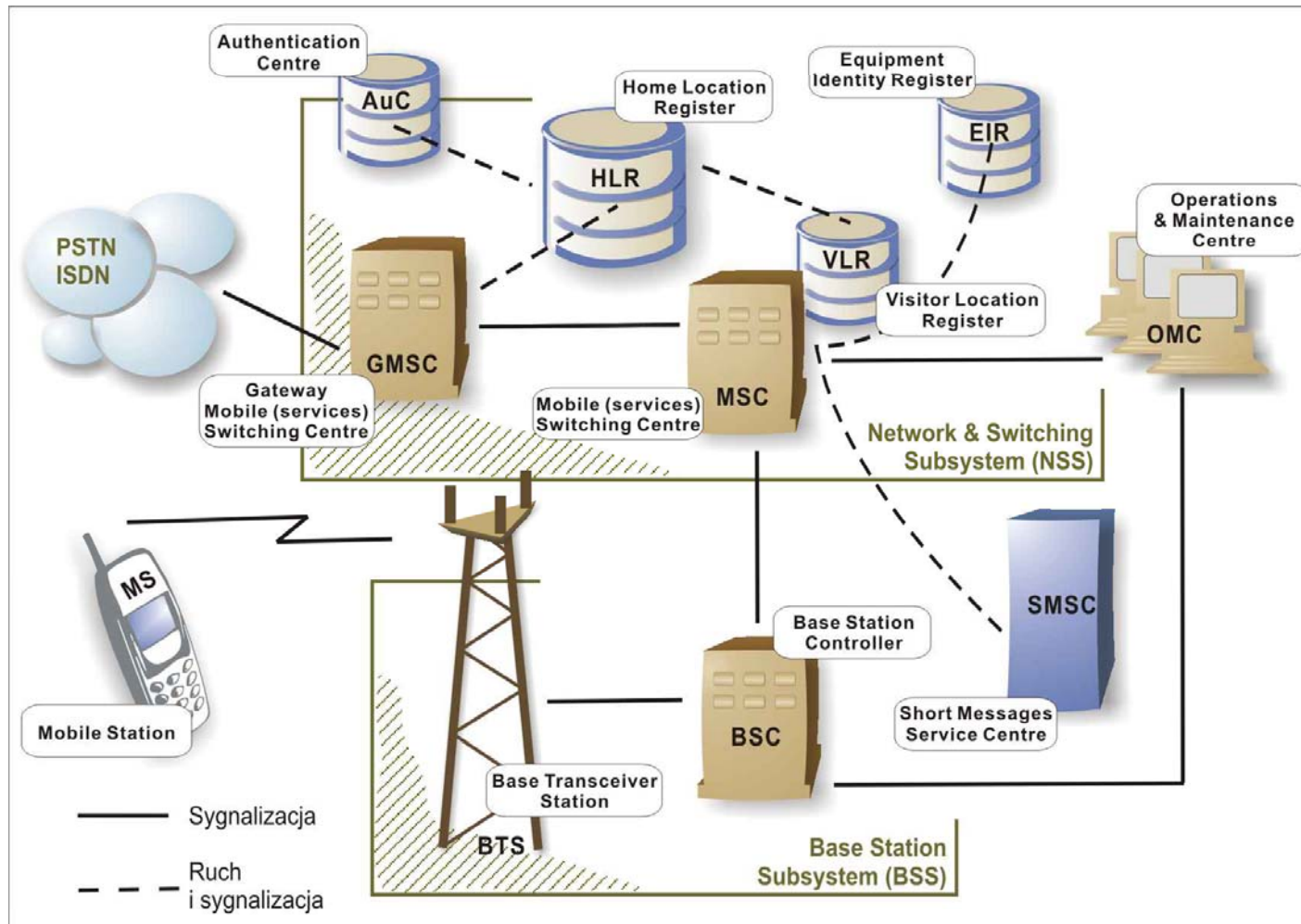


Historia powstania systemu GSM

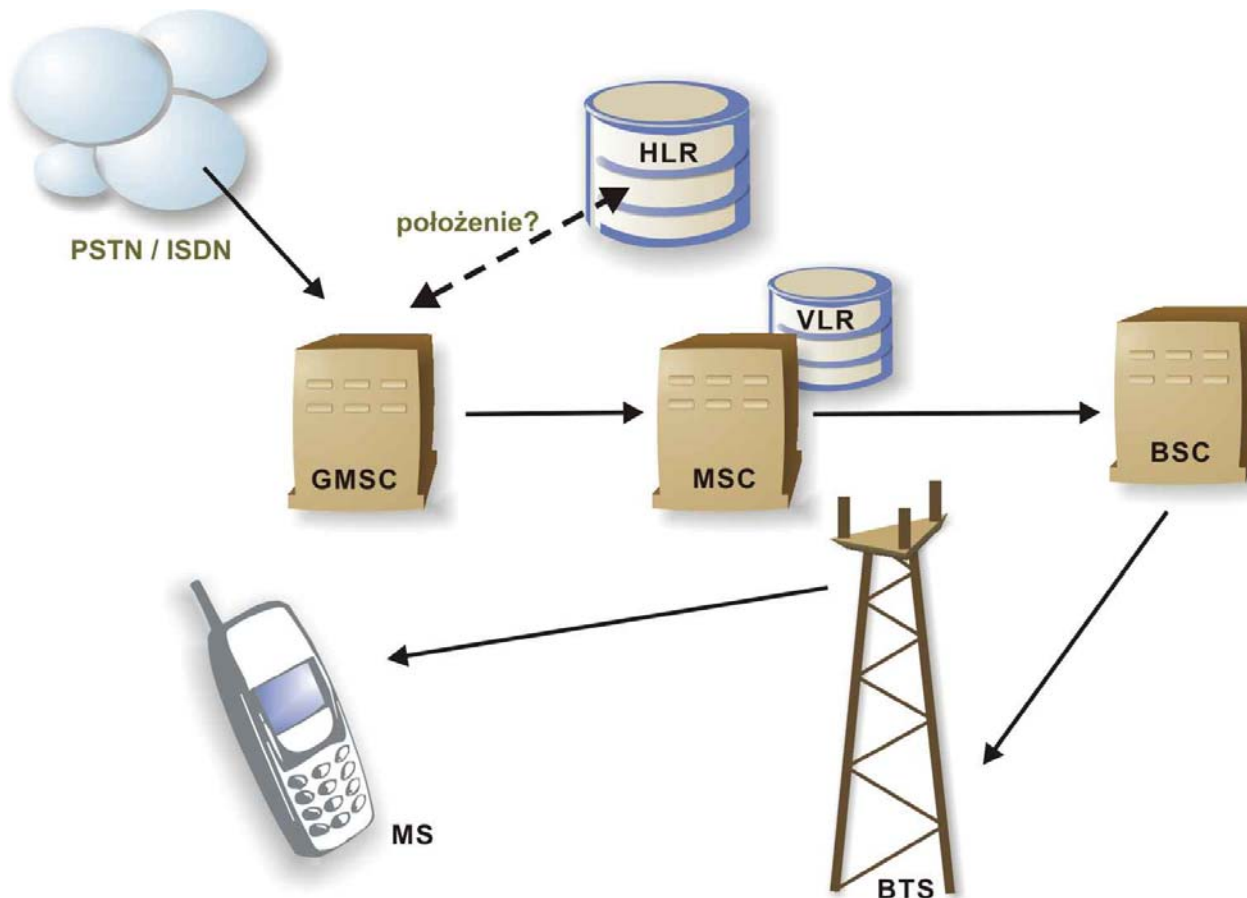
- 1982 – W ramach CEPT (fr. Conférence Européenne des Postes et Télécommunications) powstała grupa robocza GSM (fr. Groupe Spéciale Mobile). Zadaniem GSM było opracowanie systemu komórkowego wspólnego dla Unii Europejskiej. Założenia: wspólny interfejs radiowy, znacząco większa pojemność niż dla systemów analogowych, konkurencyjne koszty.
- 1986 – GSM podejmuje decyzję o tym, że nowy system będzie cyfrowy (lepsze wykorzystanie zasobów widmowych, szyfrowanie mowy,).
- 1987 – Podpisanie przez 13 krajów GSM MoU (ang. GSM Memorandum of Understanding).
- 1989 – Przejęcie prac standaryzacyjnych przez ETSI (ang. European Telecommunications Standards Institute) oraz zmiana znaczenia skrótu GSM (ang. Global System for Mobile communications).
- 1992 – Uruchomienie pierwszych komercyjnych systemów GSM.
- 1996 – Uruchomienie dwóch sieci GSM w Polsce.



Architektura systemu GSM

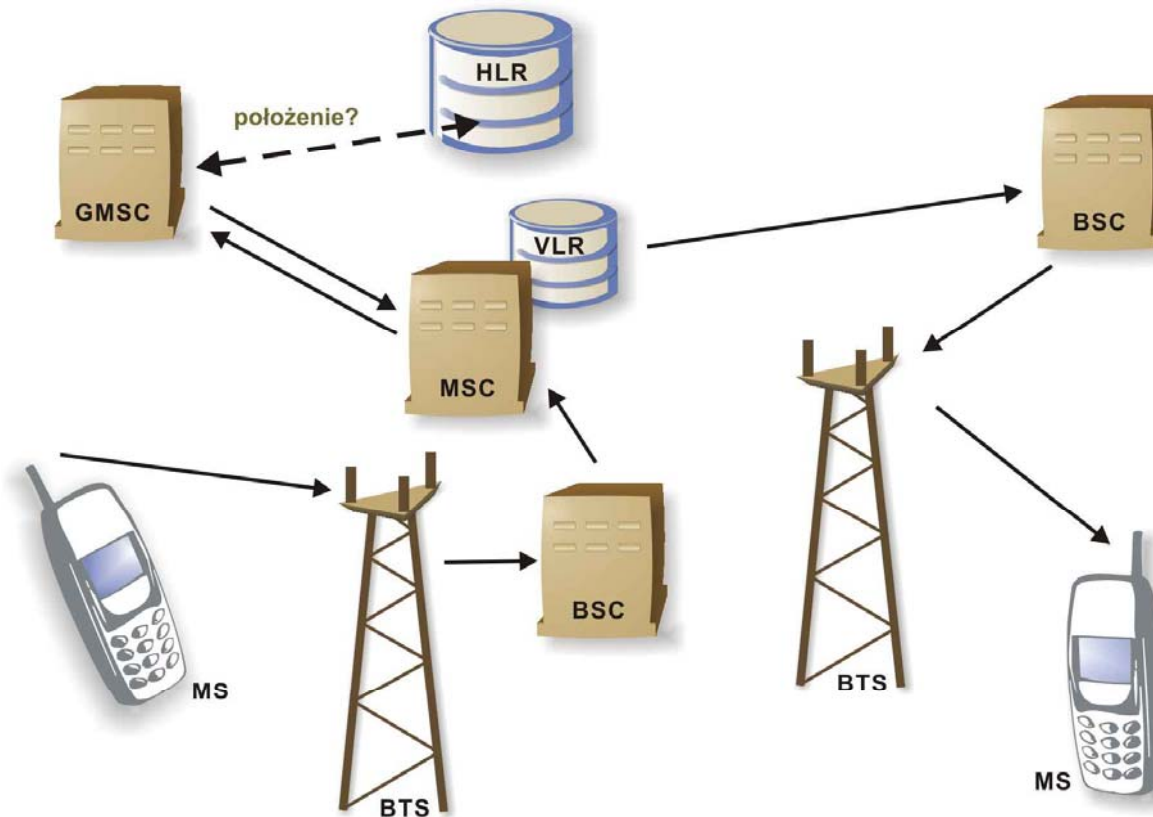


Połączenie przychodzące z PSTN



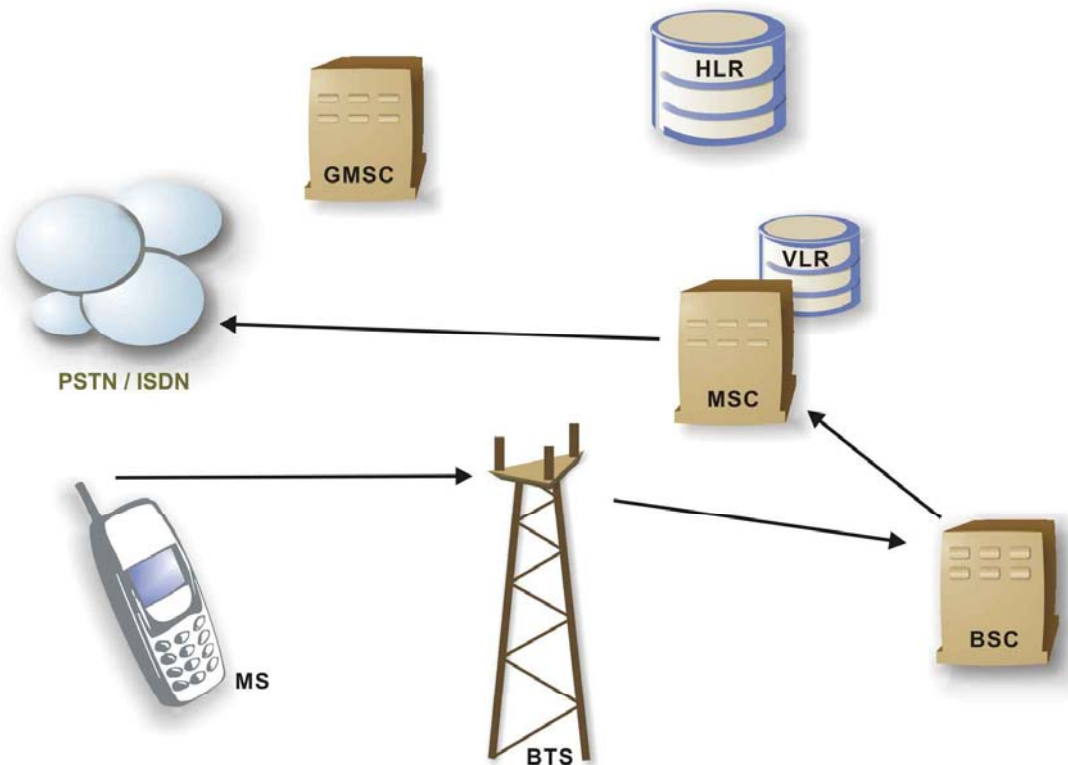


Połączenie wewnątrzsystemowe

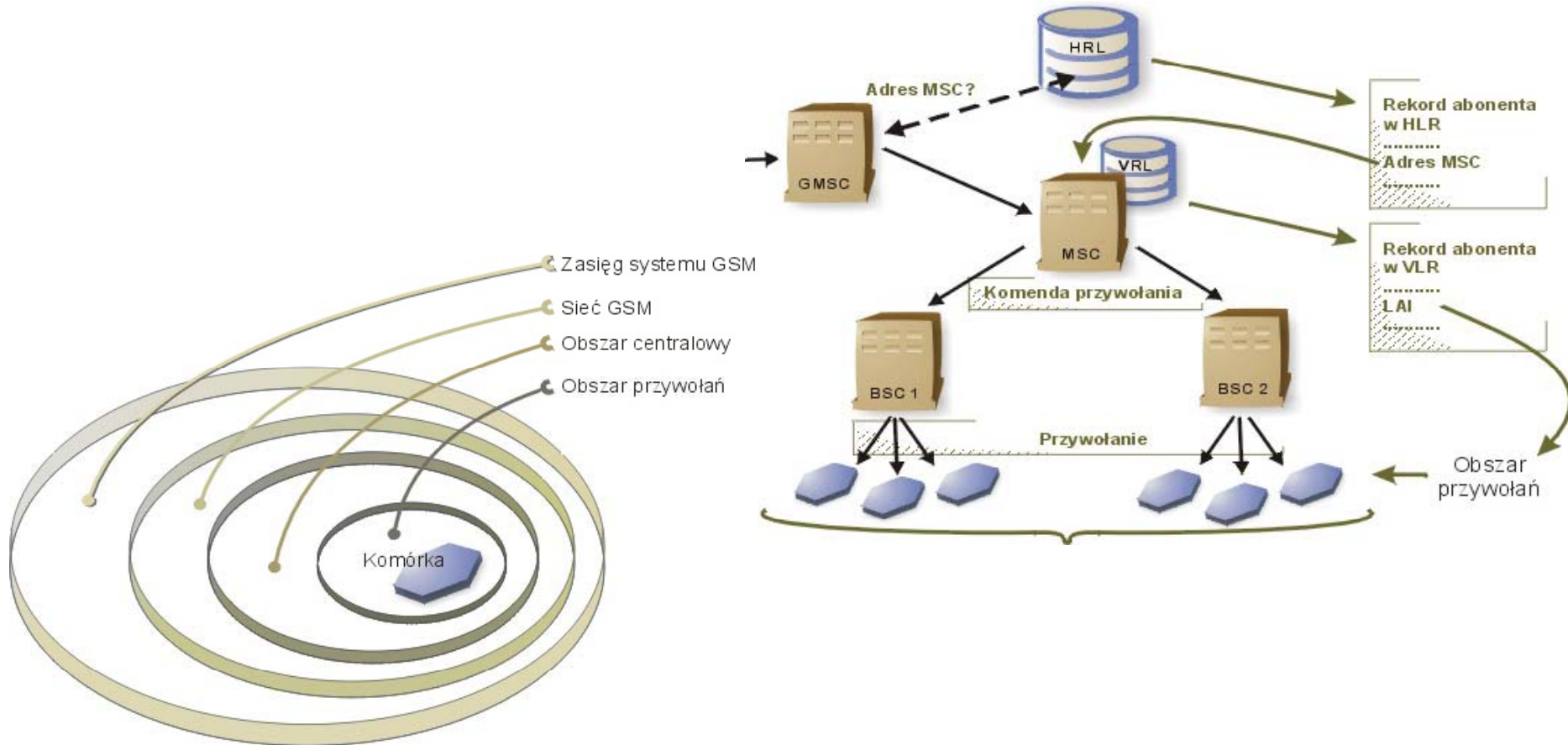




Połączenie wychodzące do PSTN



Hierarchia geograficzna systemu GSM

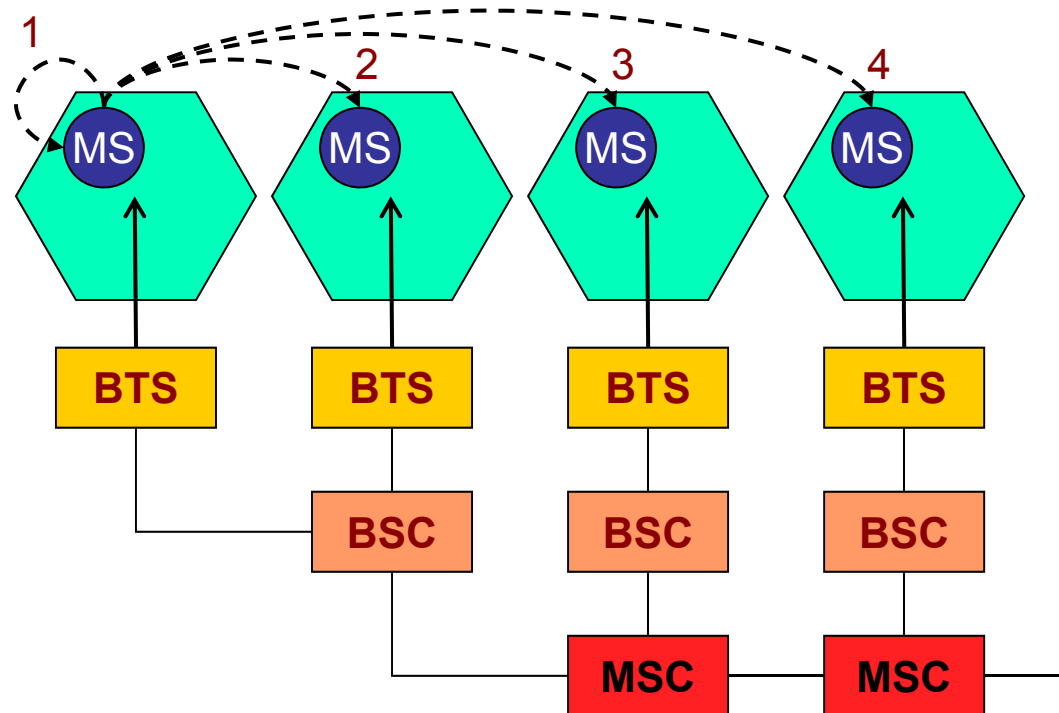


Hierarchia geograficzna systemu GSM i znaczenie obszaru przywołań.

Zastosowania bezprzewodowych systemów nadzoru i monitorowania : GSM



Przeniesienie obsługi połączenia



Przeniesienie (ang. handover) obsługi trwającego połączenie z jednej stacji bazowej do innej: 1) w ramach tej samej stacji bazowej, 2) w ramach tego samego kontrolera BSC, 3) w ramach tej samej centrali MSC, 4) międzycentralowe.





Przeniesienie obsługi połączenia

Przeniesienia mogą być:

- inicjowane przez stację ruchomą,
- inicjowane przez MSC (np. dla zrównoważenia obciążenia ruchem).

W czasie niewykorzystywanych szczelin czasowych stacja ruchoma skanuje Broadcast Control Channel maksymalnie 16 sąsiednich komórek i tworzy listę 6 stacji bazowych o najsilniejszym sygnale (kandydatów do przeniesienia). Lista ta jest przekazywana do BSC i MSC co najmniej raz na sekundę.



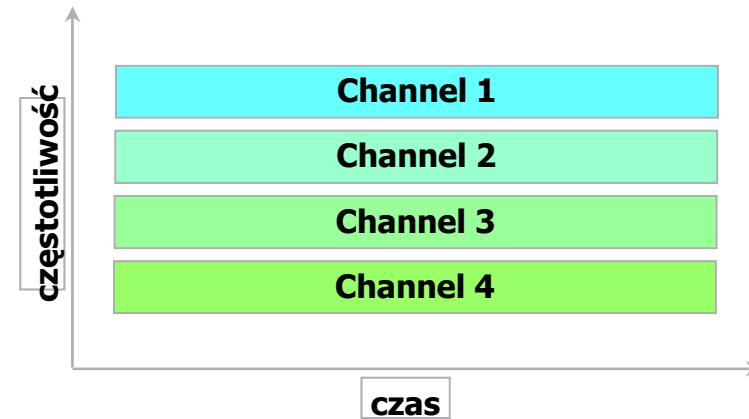
Przeniesienie obsługi połączenia

- **Algorytm minimalnej akceptowalnej jakości** daje pierwszeństwo sterowaniu mocą nad przeniesieniami – jeśli wskaźnik jakości transmisji (np. stopa błędu – BER) pogorszy się do nieakceptowanej wartości to stacja bazowa zwiększa moc nadawania przez terminal. Jeśli dalsze zwiększanie mocy nie jest już możliwe, to następuje przeniesienie obsługi. Jest to metoda prostsza i częściej stosowana.
- **Algorytm budżetu mocy** stosuje przeniesienia tak, aby zachować lub poprawić wybrany wskaźnik jakości transmisji bez zwiększania mocy nadawania terminala. Jest to pierwszeństwo przeniesień nad sterowaniem mocą. Metoda jest bardziej skomplikowana w realizacji.

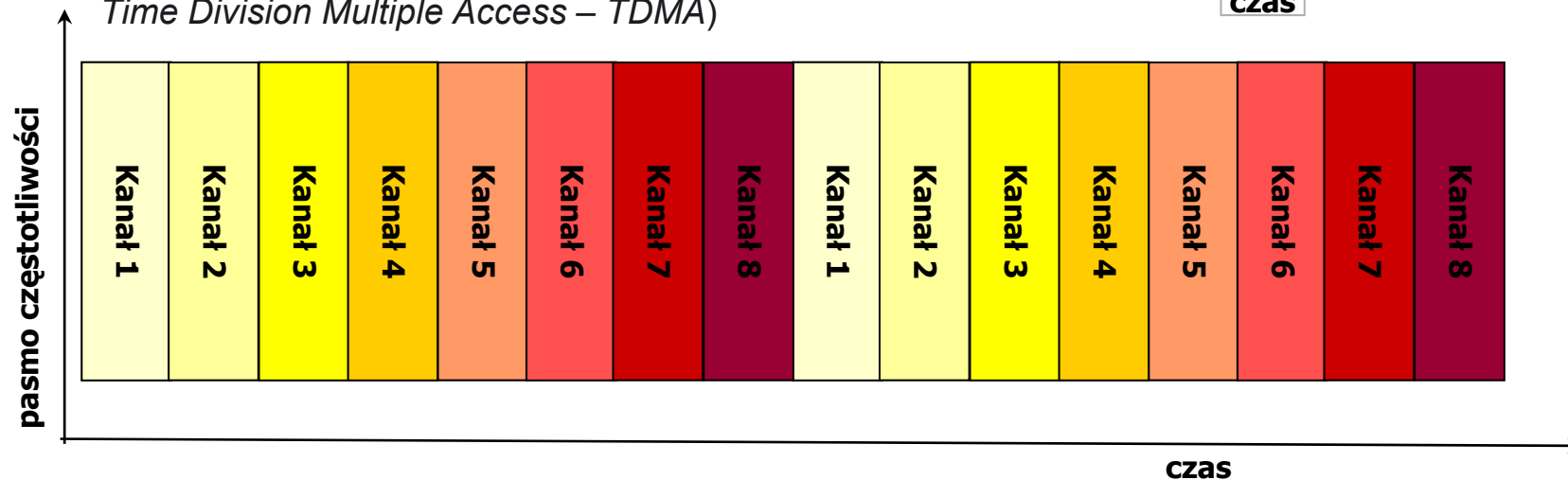


Wielodostęp

Wielodostęp z podziałem częstotliwości (ang. *Frequency Division Multiple Access – FDMA*)

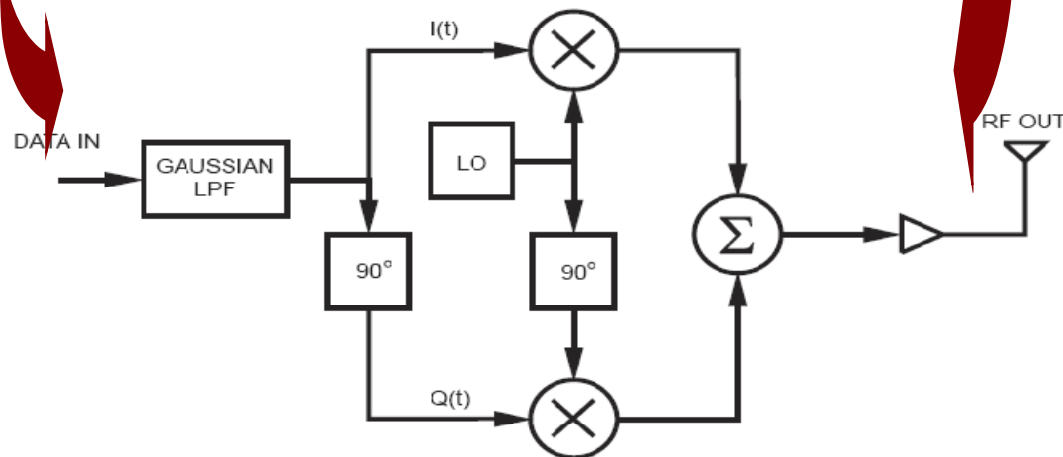
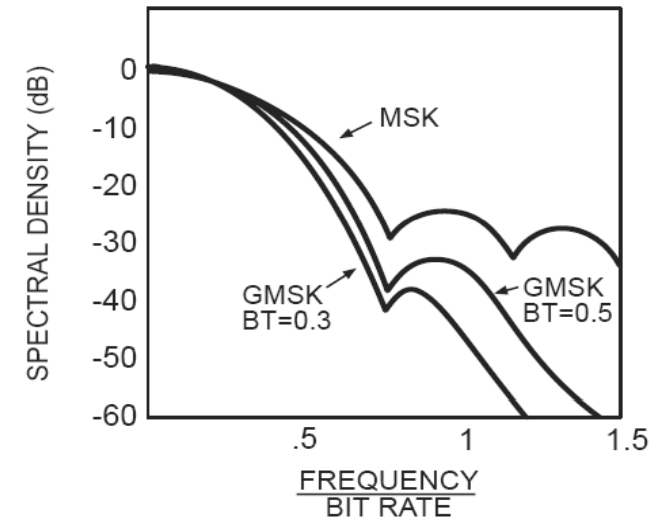
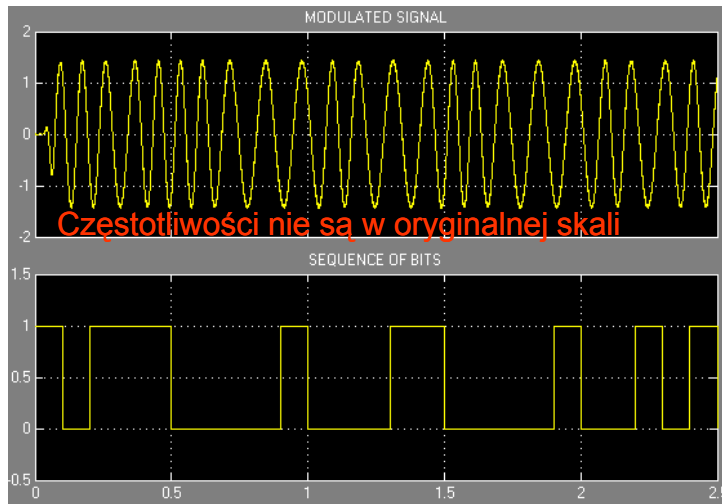


Wielodostęp z podziałem czasu (ang. *Time Division Multiple Access – TDMA*)



W systemie GSM stosowany jest wielodostęp FDMA/TDMA

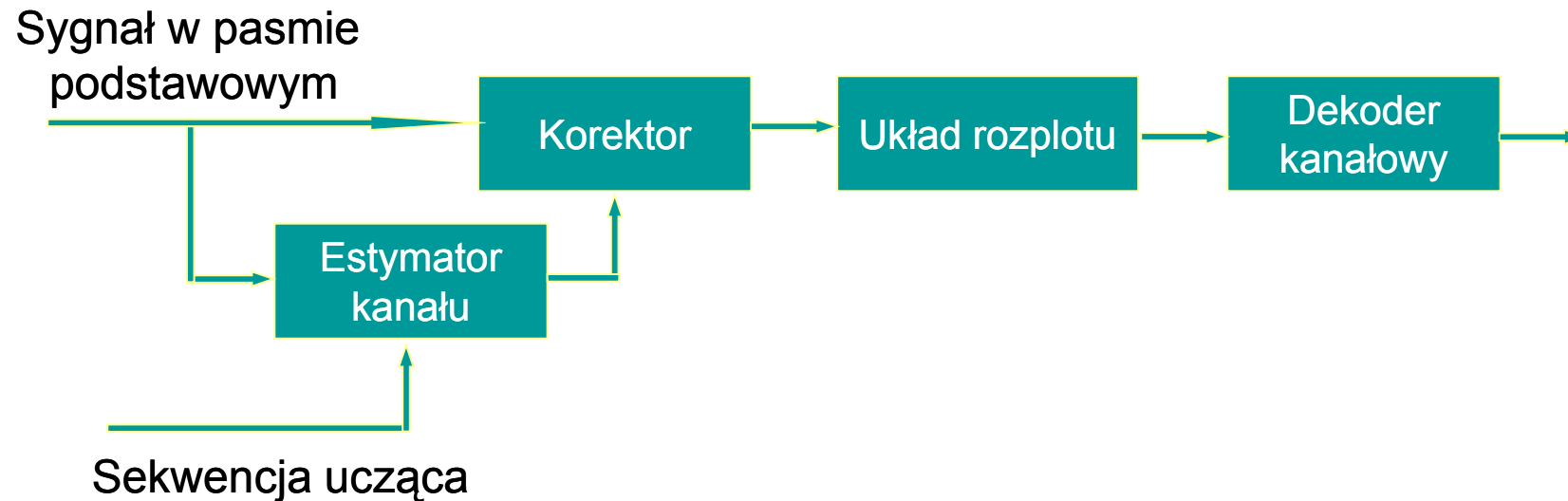
Modulacja GMSK



GMSK modulator block diagram[<http://www.eetchina.com>]



Korekcja charakterystyki kanału



Czas trwania bitu to $3,69 \mu\text{sec}$ – Stosuje się korekcję adaptacyjną pozwalającą zmniejszać skutki dyspersji czasowej do $15 \mu\text{sec}$.





Korekcja charakterystyki kanału

a)

Numer sekwencji	Sekwencja
0	00100 1011100001000100 10111
1	00101 1011101111000101 10111
2	01000 0111011101001000 01110
3	01000 1111011010001000 11110
4	00011 0101110010000011 01011
5	01001 1101011000001001 11010
6	10100 1111101100010100 11111
7	11101 1110001001011101 11100

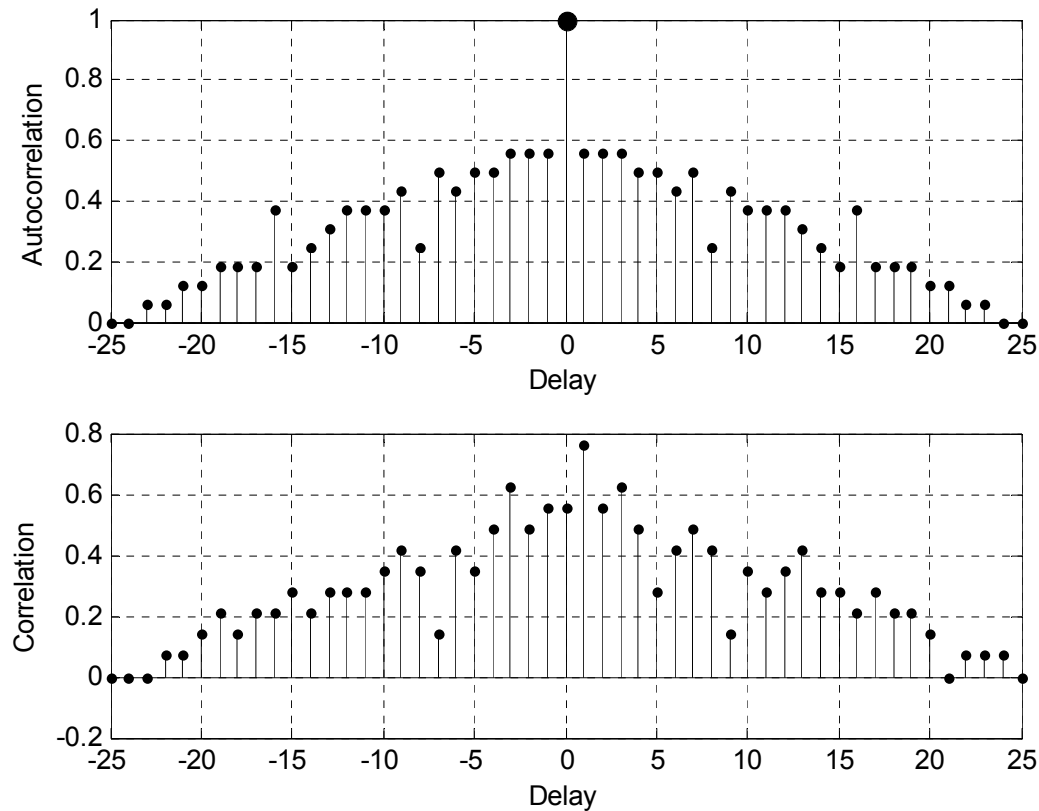
b) **1011100101100010000001000000111100101101010001010111011000011011**

a) dla pakietu normalnego (26 bitów), b) dla pakietu synchronizacji (64 bity)





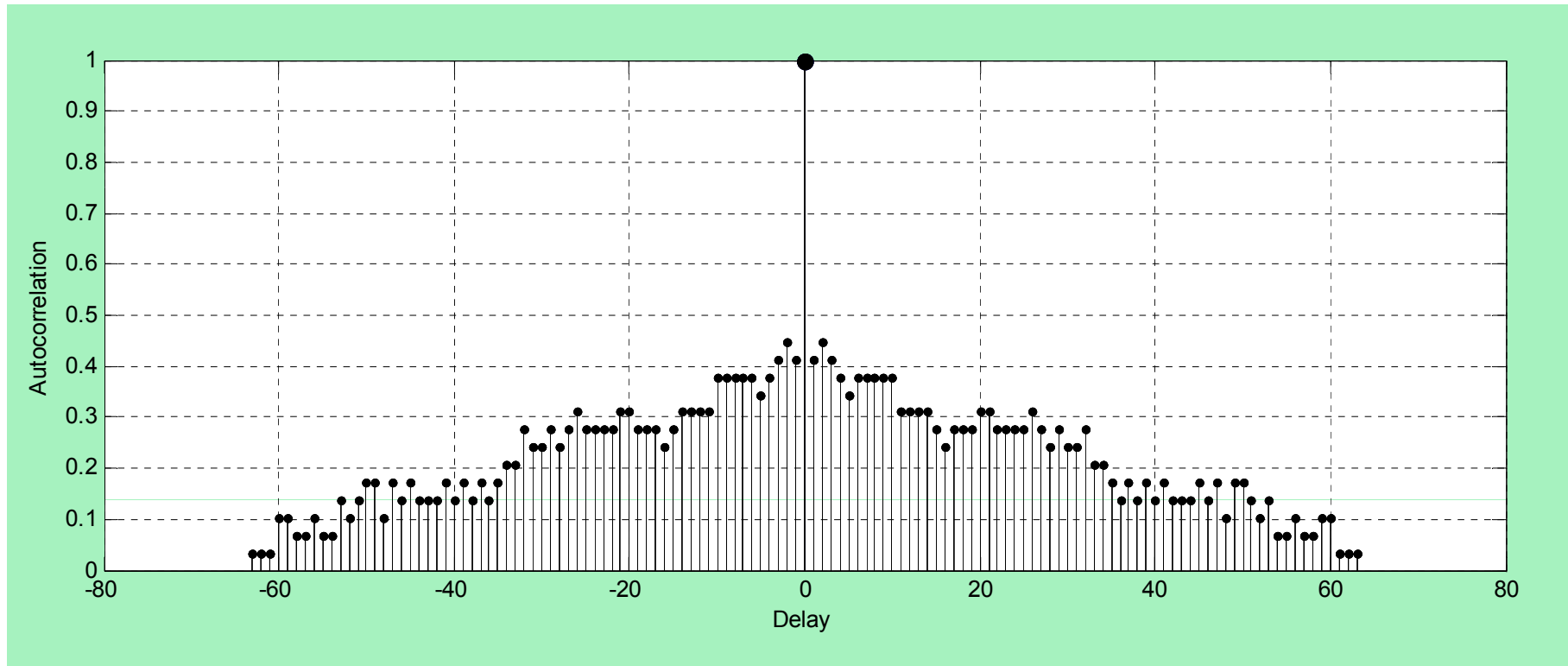
Korekcja charakterystyki kanału



*Autokorelacja sekwencji dla pakietu normalnego (26 bitów):
sekwencje 1 i 3*



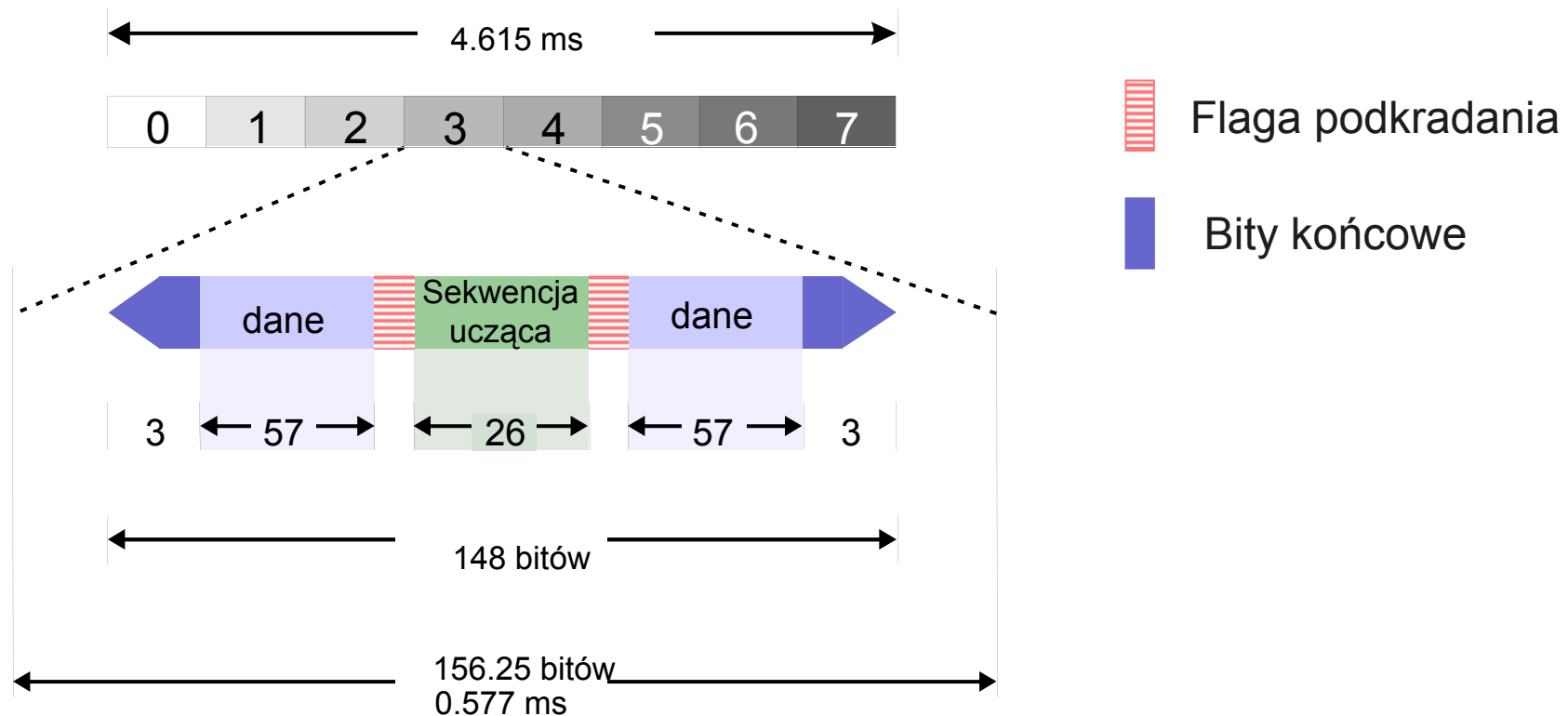
Korekcja charakterystyki kanału



Autokorelacja sekwencji dla pakietu synchronizacji (64 bity)

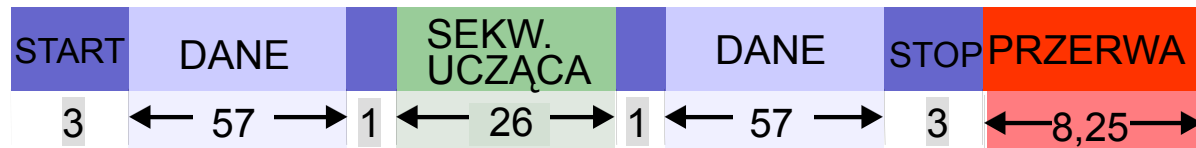


Struktura pakietu normalnego

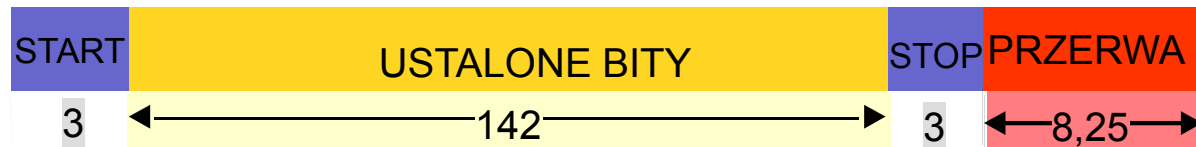




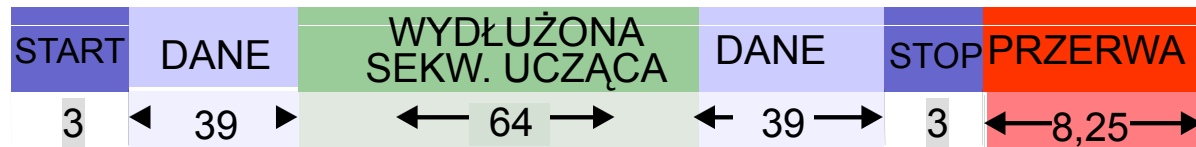
Struktura różnych rodzajów pakietów



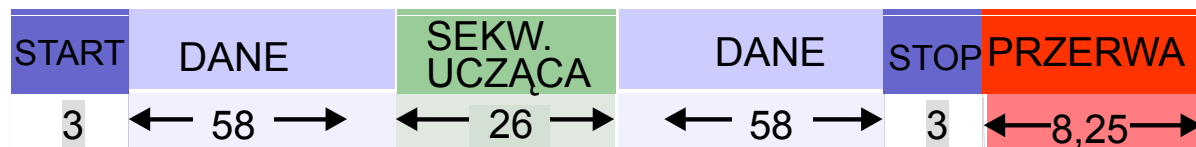
pakiet normalny



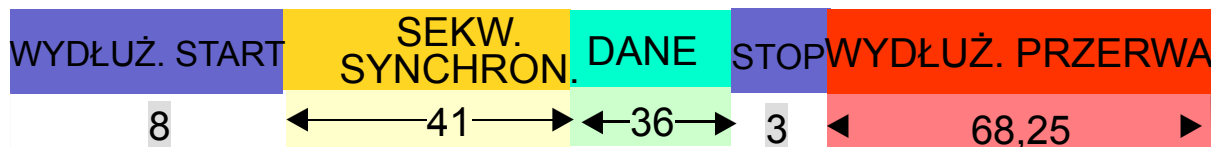
pakiet korekcji
częstotliwości



pakiet
synchronizacji



pakiet
zastępczy



pakiet
dostępu



Dupleks z przesunięciem w czasie



Nadawanie przez BTS



Nadawanie przez MS

Przesunięcie o 3 szczeliny

Łącze „w górę” jest przesunięte w stosunku do „łącza w dół” o czas trwania 3 szczelin czasowych.

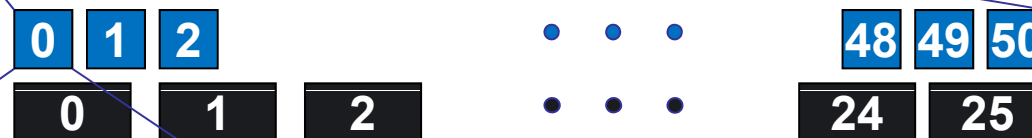


Hierarchia ramek

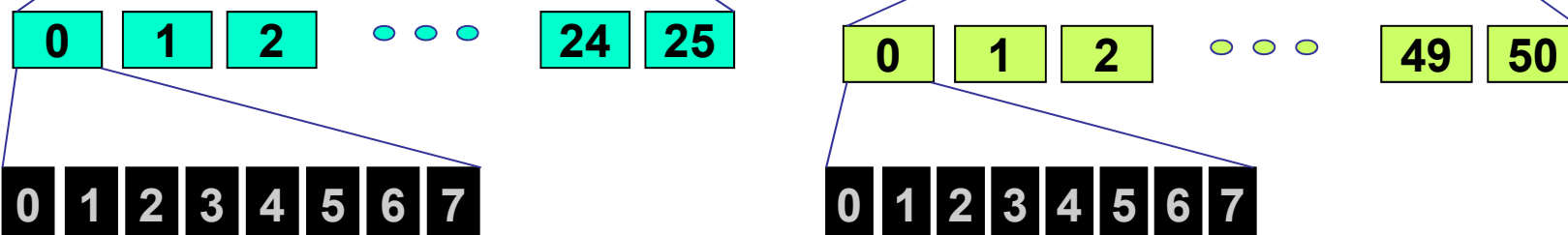
1 hiperramka = 2048 superramka = 2 715 648 ramek (3 h 28 min. 53,76 s)



1 superramka = 1326 ramek = 26 multiramek lub 51 mutliramek (6,12 s)



1 multiramka = 26 ramek (120 ms) or 51 ramek (235,38 ms)

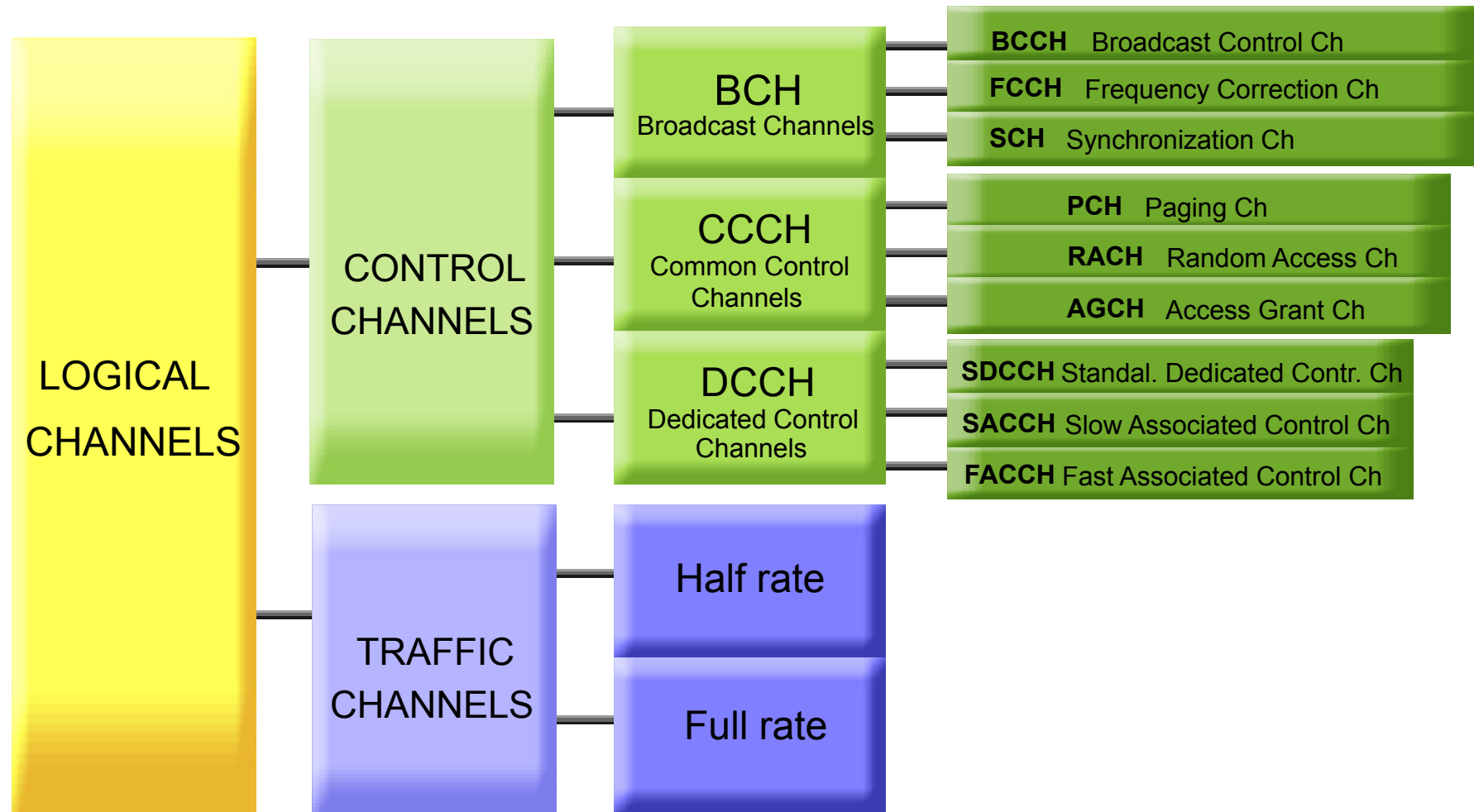


szczeliny czasowe w ramce





Kanały logiczne





Kanały logiczne

- **TCH** (Traffic CHannels) - kanały rozmówne
 - TCH full-rate (13 kb/s)
 - TCH half-rate (6.5 kb/s)
- **BCH** (Broadcast CHannels) - kanały rozsiewcze
 - FCCH (Frequency Correction CHannel) - kanał korekcji częstotliwości
 - SCH (Synchronization CHannel) - kanał synchronizacyjny
 - BCCH (Broadcast Control Channel) - rozsiewczy kanał sygnalizacyjny
- **CCCH** (Common Control CHannels) - wspólne kanały sygnalizacyjne
 - PCH (Paging CHannel) - kanał przywoławczy
 - RACH (Random Access CHannel) - kanał wielodostępu
 - AGCH (Access Grant CHannel) - kanał przydziału łącza





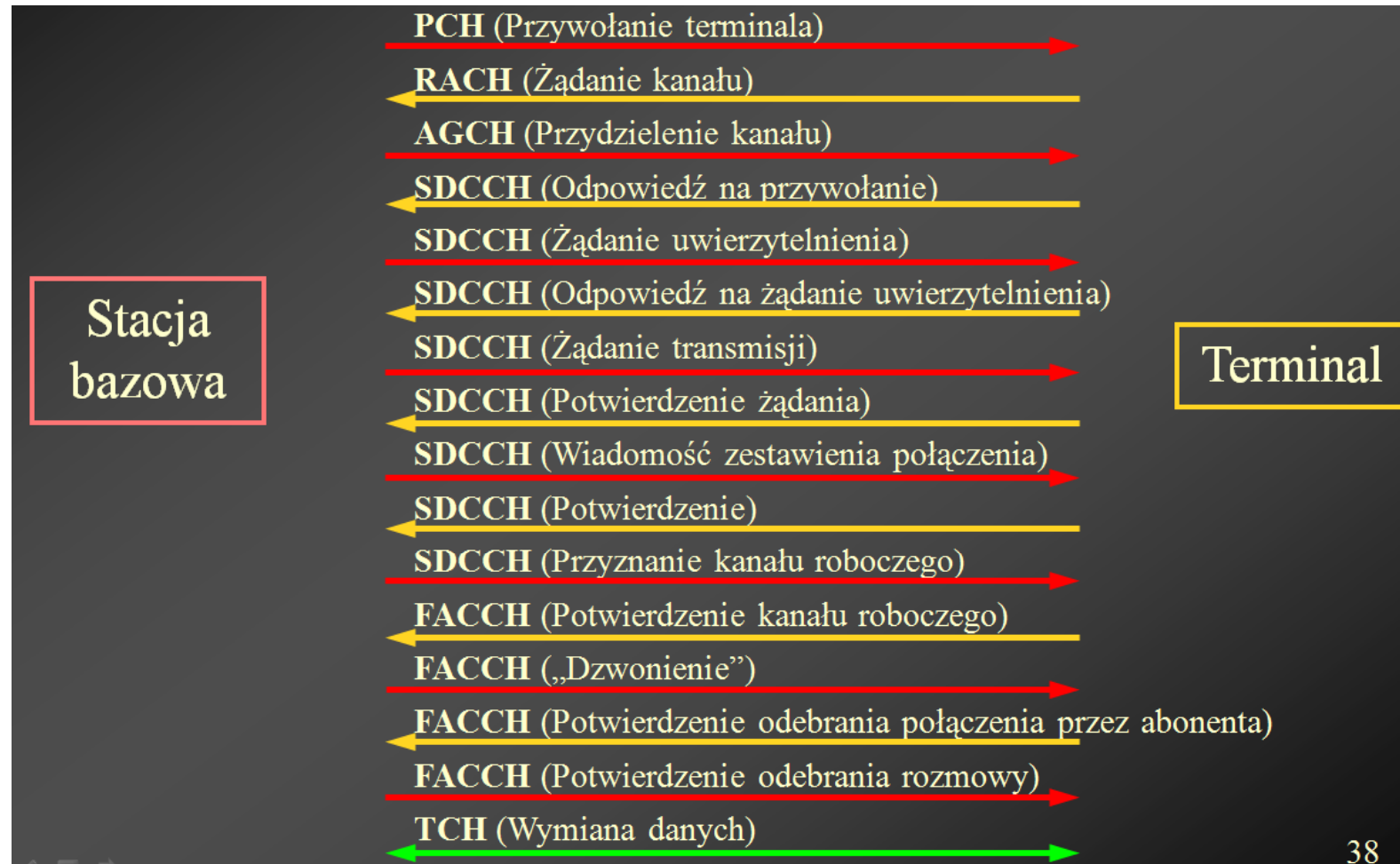
Kanały logiczne

- **DCCH** (Dedicated Control CHannels) - dedykowane kanały kontrolne
 - SDCCH (Standalone Dedicated Control Channel) - wydzielony kanał sygnalizacyjny
 - SACCH (Slow Associated Control CHannel) - wolny pomocniczy kanał sygnalizacyjny
 - FACCH (Fast Associated Control CHannel) - szybki pomocniczy kanał sygnalizacyjny



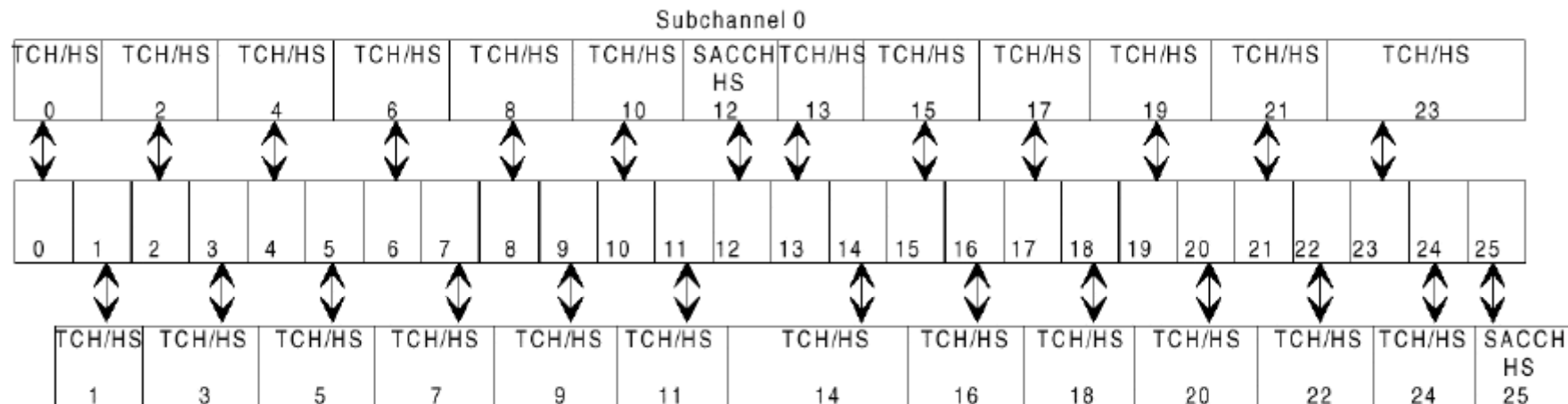
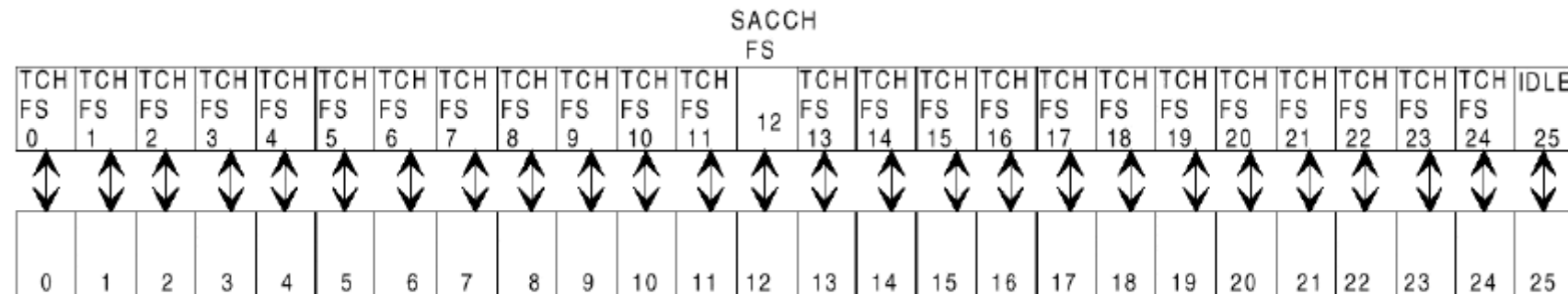


Przykład sygnalizacji przy zestawianiu połączenia przychodzącego

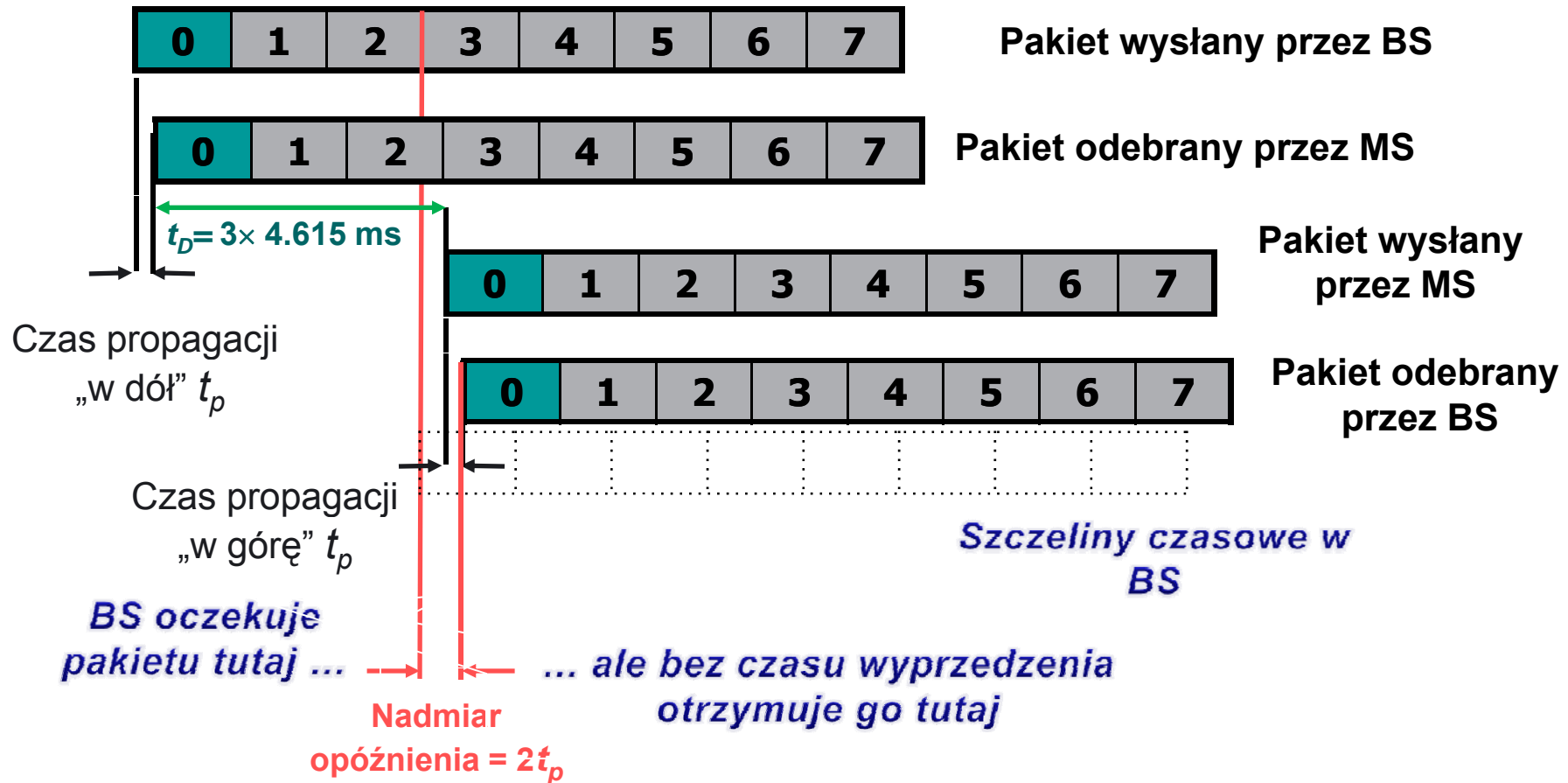




Przeniesienia obsługi połączenia

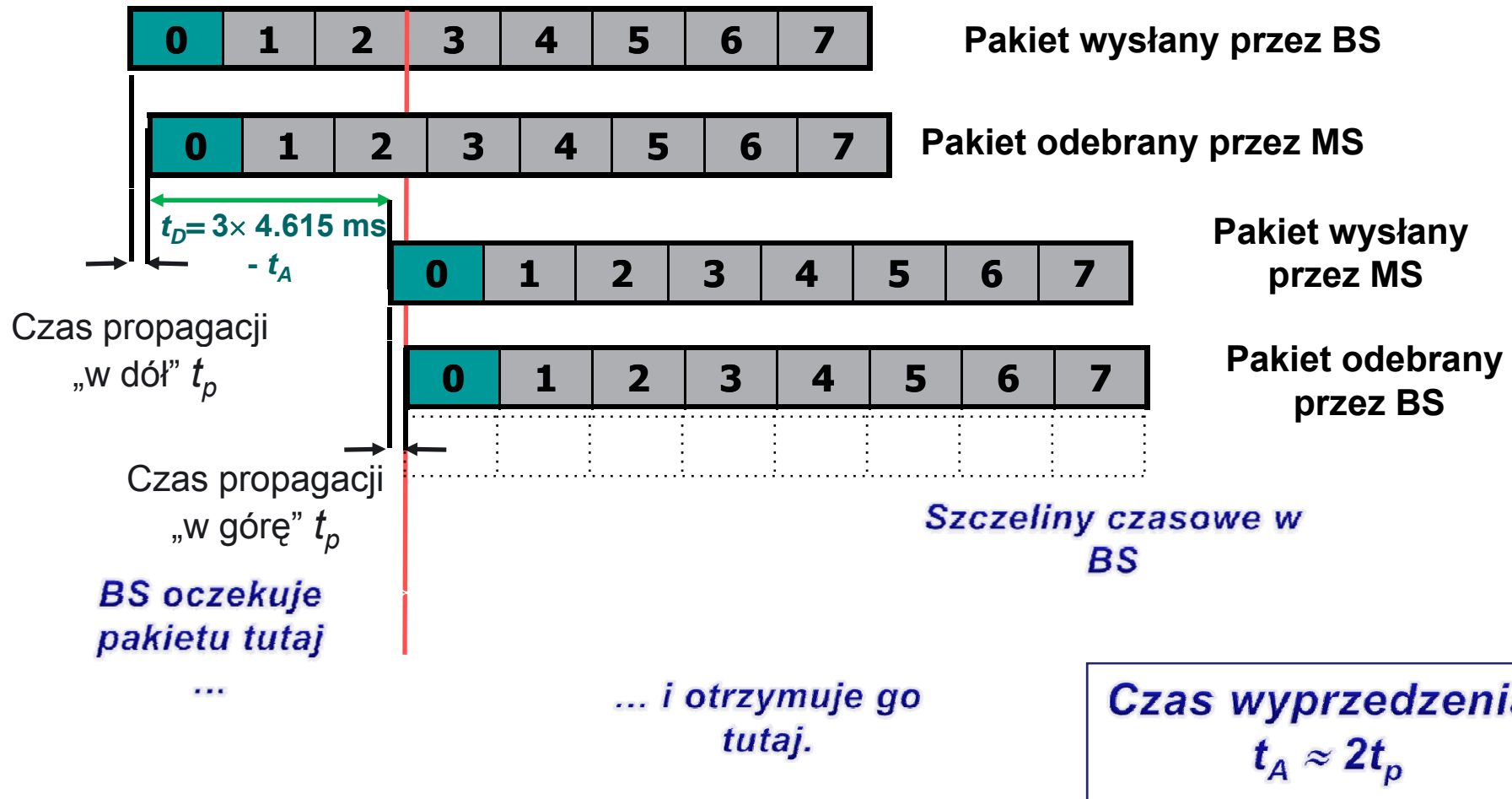


Czas wyprzedzenia (timing advance)





Czas wyprzedzenia (timing advance)



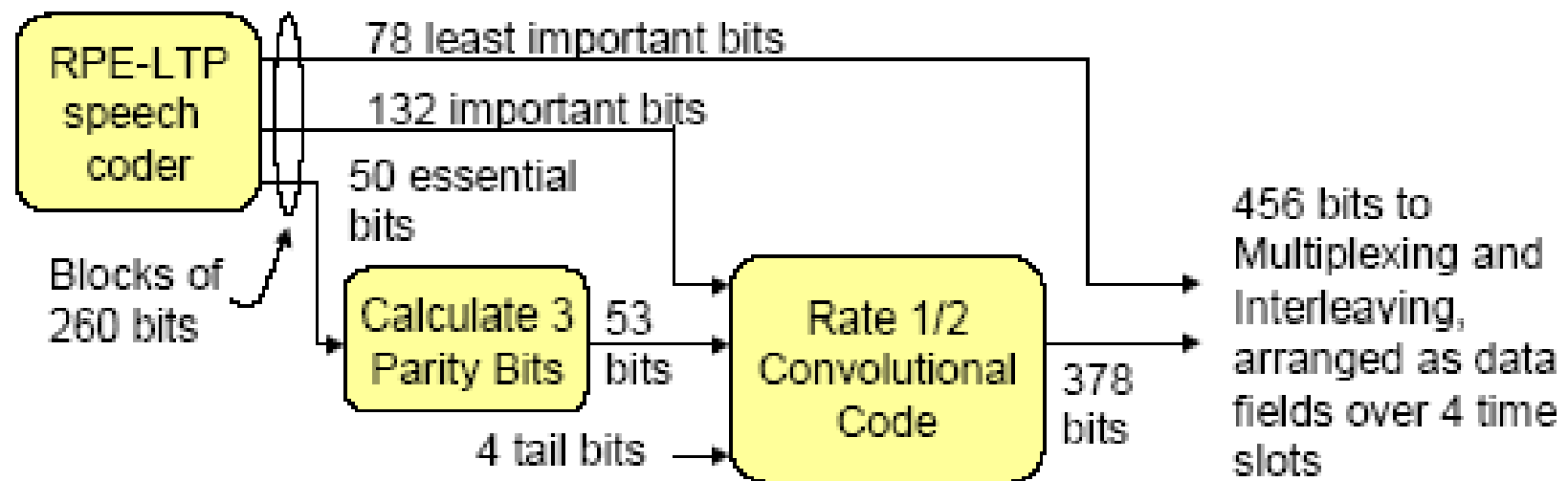
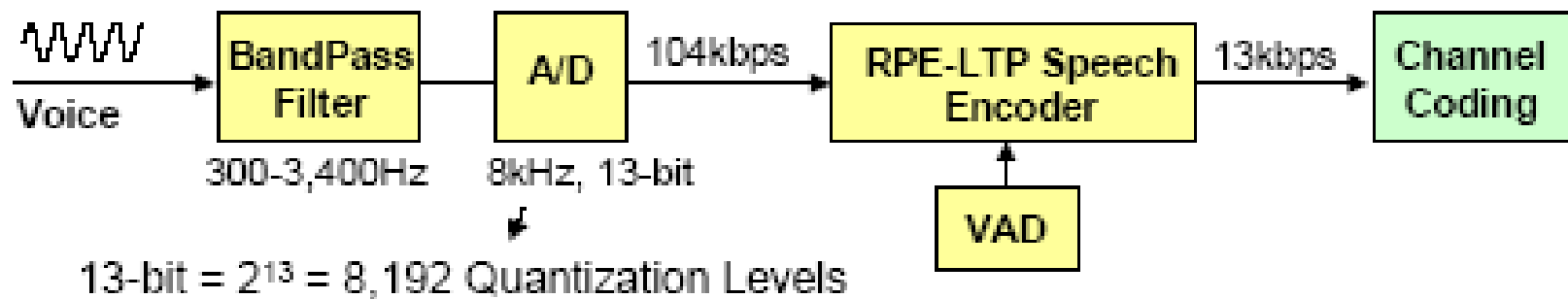


Czas wyprzedzenia (timing advance)

- MS musi przyspieszyć transmisję pakietów o czas odpowiadający drodze propagacji sygnału: $BS \rightarrow MS + MS \rightarrow BS$.
- TA jest reprezentowane jako liczba 6-bitowa, czyli są 64 wartości (0-63). Jednostką jest czas trwania jednego bitu, tj. $3,69 \mu s$ (554 m).
- W podstawowej wersji TA umożliwia kompensację opóźnienia dla maksymalnej odległości odpowiadającej czasowi trwania 31,5 bity tj. $113,3 \mu s$, co z kolei odpowiada odległości $MS \rightarrow BS \sim 35 \text{ km}$. Istnieją rozwiązania takie jak ER (Extended Range) lub firmowe typu ERC (ang. Extended Range Cell), zwiększające zasięg np. do ok. 120 km.



Kompresja i kodowanie sygnału mowy





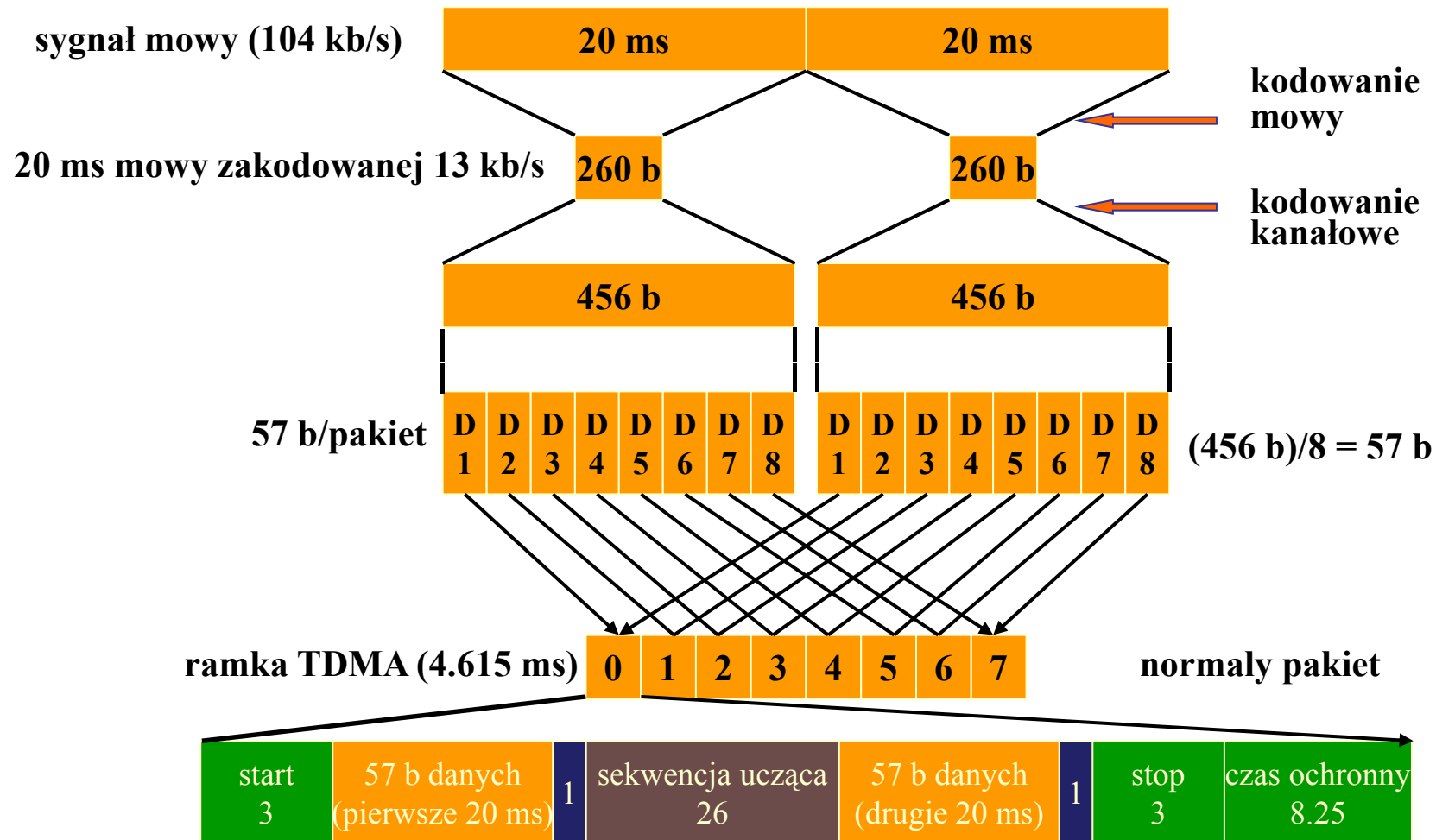
Kompresja i kodowanie sygnału mowy

- Full rate (FR) 13 kbit/s , Regular pulse excitation – Long Term Prediction (RPE-LTP)
- Half rate (HR) 5.65 kbit/s VSELP
- **Enhanced full rate (EFR) 12.2 kbit/s ACELP**
- Adaptive Multi Rate (AMR) ACELP, 12.2, 10.2, 7.95, 7.4, 6.7, 5.9, 5.15, 4.75 kbit/s





Transmisja mowy





Skakanie po częstotliwościach (FH – *Frequency Hopping*)

- Wolne skakanie po częstotliwościach (Slow Frequency Hopping) ze zmianą co 4.615 ms jest zaimplementowane we wszystkich terminalach.
- **Cyclic hopping mode** – sekwencyjnie po określonym zbiorze częstotliwości,
- **Random hopping mode** – jedna z 63 sekwencji pseudolosowych.
- Skoki częstotliwości są skoordynowane w ramach grup komórek, tak aby uniknąć nadmiernych interferencji wspólnokanałowych.
- Terminal otrzymuje informacje o trybie skakania i zbiorze częstotliwości za pośrednictwem kanału BCCH.





Skakanie po częstotliwościach (FH – *Frequency Hopping*)

Zalety FH:

- pomaga zmniejszać skutki szybkich zaników,
- zakłócenia wspólnokanałowe uśredniają się w całym systemie i można przyjąć, że są o ok. 6 dB mniejsze niż bez zastosowania FH.
- Kanały rozgłoszeniowe i wspólne kanały sygnalizacyjne są lokalizowane na częstotliwościach, które nie podlegają FH.
- FH jest obligatoryjną funkcją terminali ale nie wszystkie stacje bazowe muszą ją implementować.





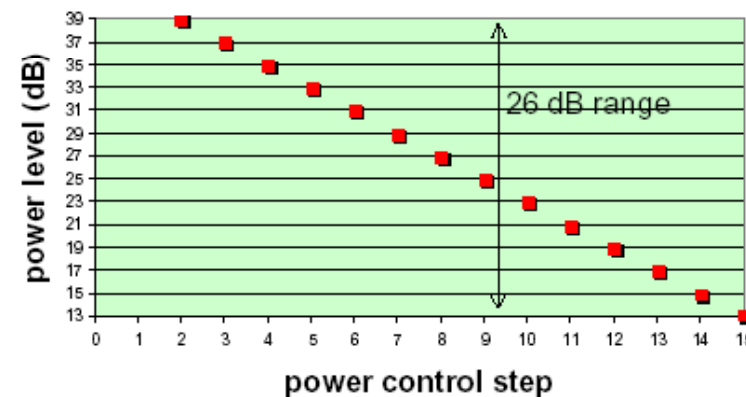
Sterowanie mocą nadawania terminala

Sterowanie mocą nadawania terminala:

- zmniejsza zapotrzebowanie na energię z akumulatora,
- obniża poziom zakłóceń wspólnokanałowych w systemie
- zmniejsza ew. zagrożenia zdrowotne powodowane promieniowaniem elektromagnetycznym terminala.

Decyzja o zmianie mocy podejmowana jest przez BS na podstawie ciągłego pomiaru stopy błędu albo mocy sygnału odebranego z MS.

- Minimalna moc to 13 dBm (20 milliwatts).
- Zmiana może następować w krokach 2 dB co 60 ms.
- Średnia moc promieniowania terminala jest o ok. 8 dB mniejsza od mocy szczytowej (nadawanie tylko w jednej szczelinie czasowej w każdej ramce).

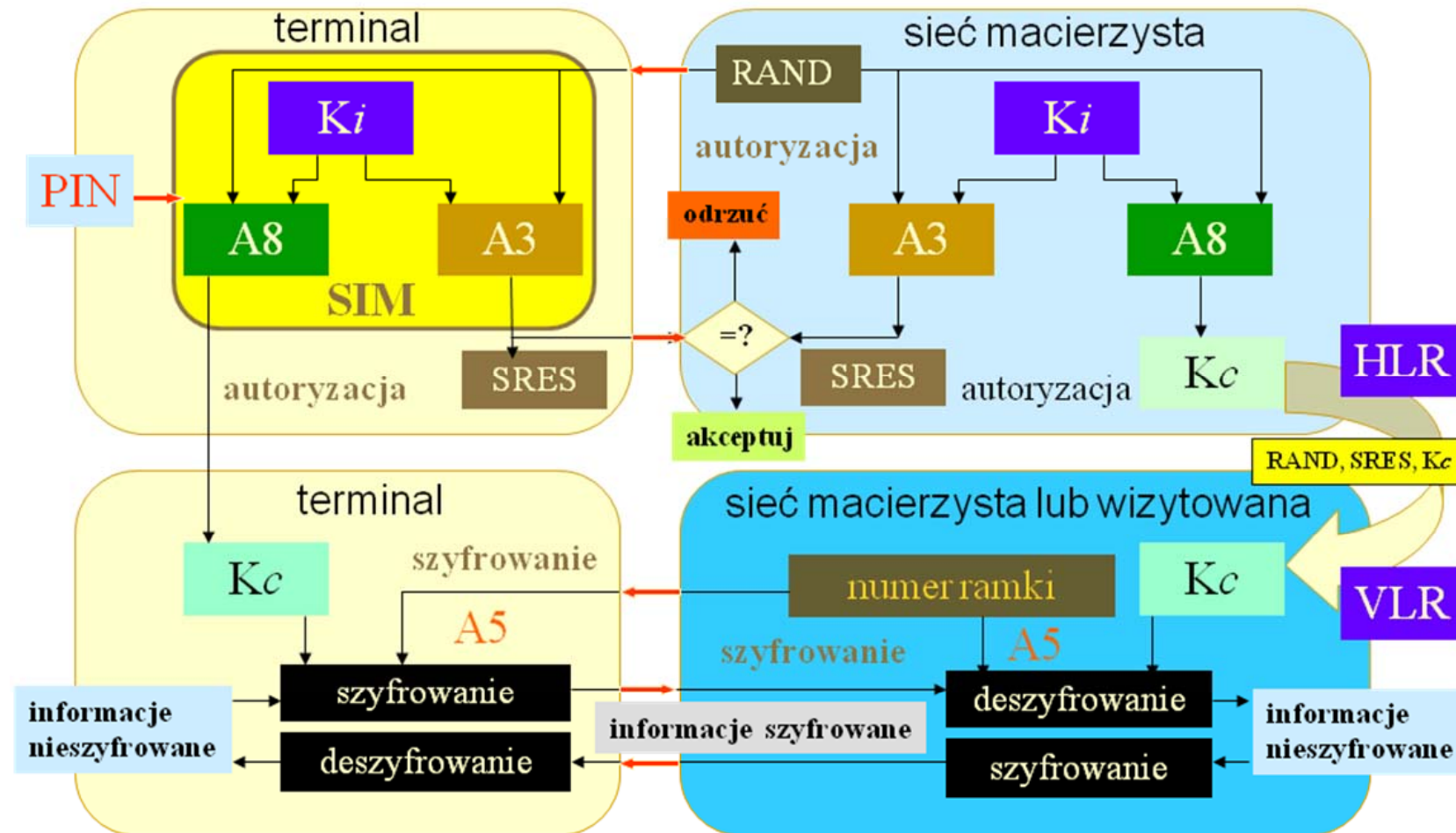




Transmisja nieciągła i odbiór nieciągły

- Aby zmniejszyć moc zużywaną przez MS oraz poziom zakłóceń wspólnokanałowych stosuje się rozwiązanie znane jako **Discontinuous Transmission** (DTX). Terminal transmituje wtedy, gdy VAD (ang. Voice Activity Detector) wykryje aktywność głosową użytkownika. W pozostałym czasie u drugiego korespondenta generowany jest “szum komfortu” sztucznie generowany z wykorzystaniem ramek SID (ang. Silence Descriptor).
- **Discontinuous Reception** (DRX) - MS nasłuchuje kanału pagingowego tylko w swoim podkanale.

Uwierzytelnianie użytkownika i szyfrowanie informacji





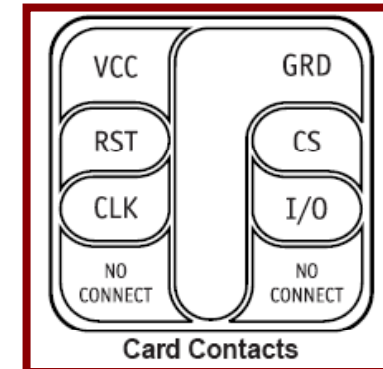
Uwierzytelnianie użytkownika i szyfrowanie informacji

- A3 - algorytm używany przy autoryzacji - wyznacza SRES na podstawie RAND i K_i
- A5 - algorytm używany do szyfrowania
- A8 - algorytm używany do generacji liczb losowych
- K_i - indywidualny klucz identyfikacji
- K_c - klucz używany do szyfrowania danych użytkownika (także mowy) oraz danych systemowych w kanale radiowym
- RAND - liczba losowa
- SRES - odpowiedź terminala na liczbę losową RAND



Subscriber Identity Module (SIM)

- Separacja tożsamości użytkownika i MS.
- Algorytmy kryptograficzne w tym ochrona przez PIN i PUK
- Przechowywanie inf. do billingu, SMS, książka telefoniczna
- Dane dotyczące organizacji danej sieci GSM



SIM zawiera:

- Dane zapisane przez operatora (np. o preferowanych operatorach rovingu)
- Zmieniane przez użytkownika (np. lista numerów skróconych)
- International Mobile Subscriber Identity (IMSI).

Zawartość SIM może być zmieniana za pośrednictwem:

- klawiatury MS
- dołączonego urządzenia peryferyjnego
- OTA (ang. Over the Air) - SIM Toolkit

Styk	Zastosowanie
Vcc	Power
RST	Reset
CLK	Clock signal
RFU	Reserved for future use
GND	Ground
Vpp	Programming power (to program EEPROM of first generation ICCs)
I/O	Input/output line (half-duplex communication)
RFU	Reserved for future use



Numeracja i anonimowość abonenta

- **TMSI** (Temporary mobile subscriber international number)
tymczasowy numer abonenta ruchomego
- **IMSI** (Identification mobile subscriber international number)
międzynarodowy numer abonenta ruchomego
- **IMEI** (International mobile equipment identity)
międzynarodowy numer terminala ruchomego
- **LAI** (Location area identification number)
numer identyfikacyjny obszaru przywołań





Numeracja i anonimowość abonenta

$$\text{MSISDN} = \text{CC} + \text{NDC} + \text{SN}$$

- **MSISDN** **Mobile Station ISDN Number**
- **CC** **Country Code**
- **NDC** **National Destination Code**
- **SN** **Subscriber Number**

$$\text{IMSI} = \text{MCC} + \text{MNC} + \text{MSIN}$$

- **IMSI** **International Mobile Subscriber Identity**
- **MCC** **Mobile Country Code**
- **MNC** **Mobile Network Code**
- **MSIN** **Mobile Station Identification Number**





Numeracja i anonimowość abonenta

IMEI = TAC + FAC + SNR + spare

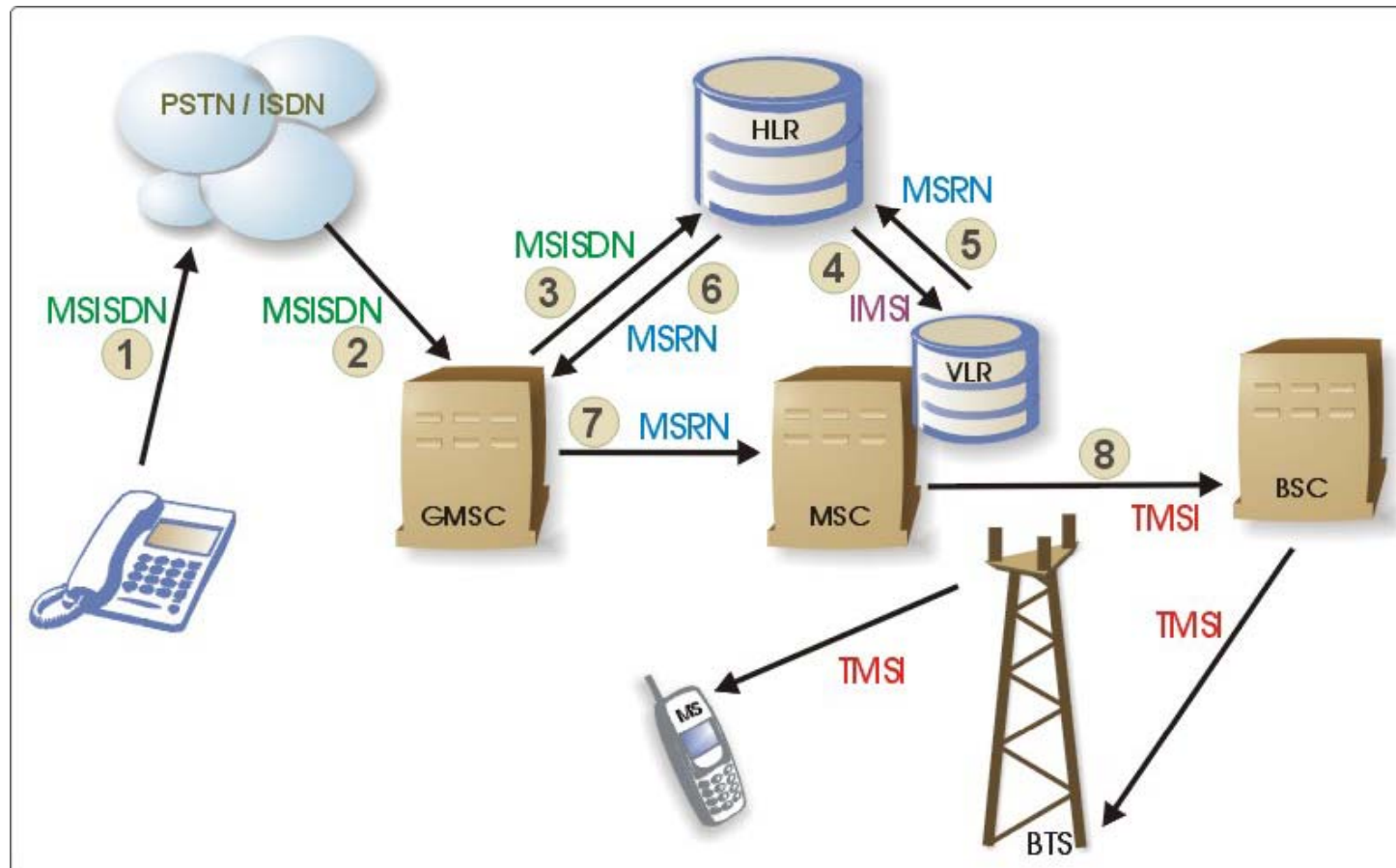
- **IMEI** **Internal Mobile Equipment Identity**
- **TAC** **Type Approval Code**
- **FAC** **Final Assembly Code, identyfikuje producenta**
- **SNR** **Serial Number**

IMEISV = TAC + FAC + SNR + SVN

- **IMEISV** **International Mobile Equipment Identity and Software Version**
Number
- **SVN** **Software Version Number**



Numeracja i anonimowość abonenta





Lokalizacja elementów bezpieczeństwa w systemie

L.p.	Element systemu	Element bezpieczeństwa
1.	Mobile station (MS)	A5, IMEI
2.	Subscriber identity module (SIM)	A3, A8, IMSI, K_i , TMSI / LAI, K_c / CKSN
3.	Authentication center (AUC)	A3, A8, IMSI / K_I
4.	Home location register (HLR)	pakiet IMSI / RAND / SRES / K_c
5.	Visitor Location register (VLR)	pakiet IMSI / RAND / SRES / K_c , pakiet MSI / TMSI / LAI / K_c / CKSN
6.	Mobile switching center (MSC)	A5, tryplet TMSI / IMSI / K_c
7.	Base station controller (BSC)	A5, tryplet TMSI / IMSI / K_c

