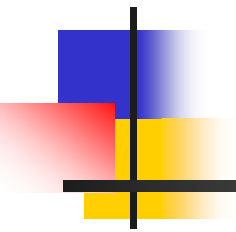
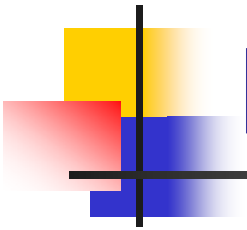


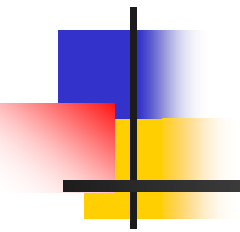
Sieci mobilne i bezprzewodowe

Franciszek Seredynski
PJWSTK
sered@pjwstk.edu.pl



Literatura

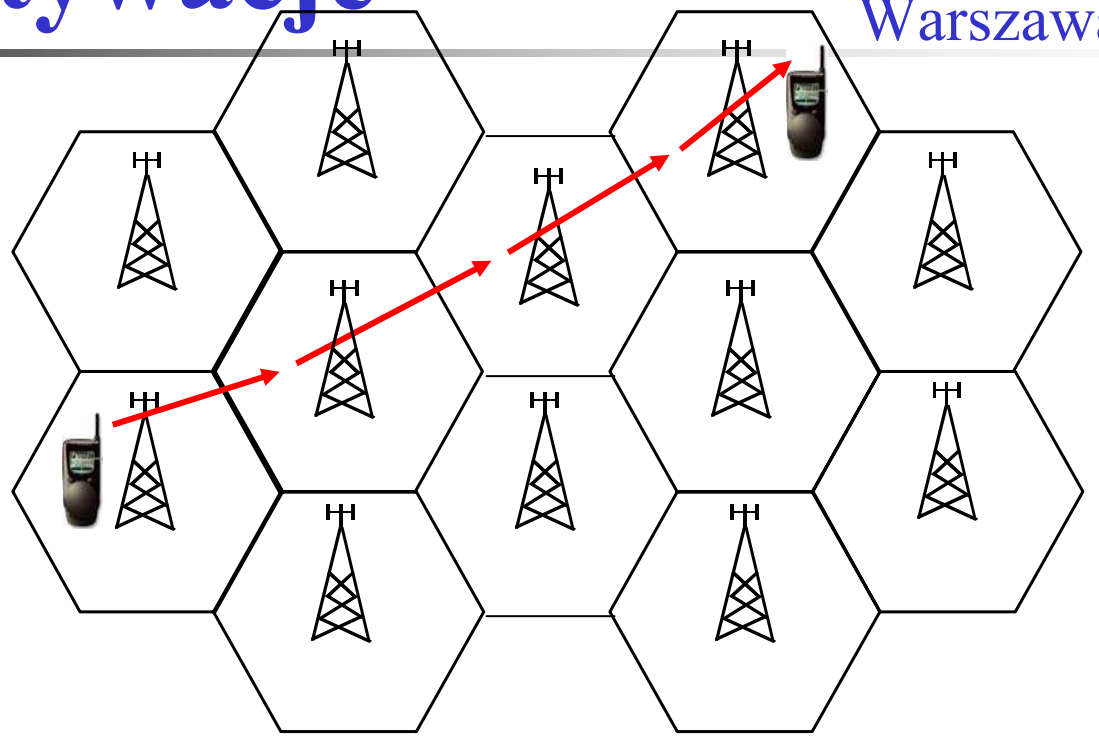
- D. P. Agrawal, Q.-A. Zeng, ***Introduction to Wireless and Mobile Systems***, 2e, Thomson, 2006
- W. Stallings, ***Wireless Communications and Networks***, 2e, Pearson Prentice Hall, 2005
- M. Ilyas, I. Mahgoub (eds.), ***Mobile Computing Handbook***, Auerbach 2005



Wprowadzenie

Motywacje

Warszawa



Barcelona

Podtrzymywanie bezprzewodowego połączenia telefonicznego między urządzeniami mobilnymi poruszajacymi się w obszarze geograficznym

Technologie bezprzewodowe

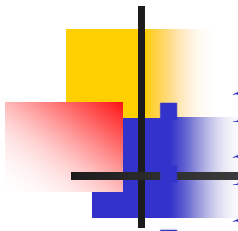
- Sieci komórkowe
- Systemy satelitarne, GPS
- Sieci ad hoc (doraźne) i sieci sensorowe
- Bezprzewodowe WPAN (wireless personal area networks):

- 802.15.4, 802.15.1 Bluetooh

- Bezprzewodowe WLAN (wireless local area networks):
  - 802.11
  - 802.11b (WiFi)
  - 802.11g
  - 802.11a HiperLAN
- Bezprzewodowe WMAN (wireless metropolitan area networks):

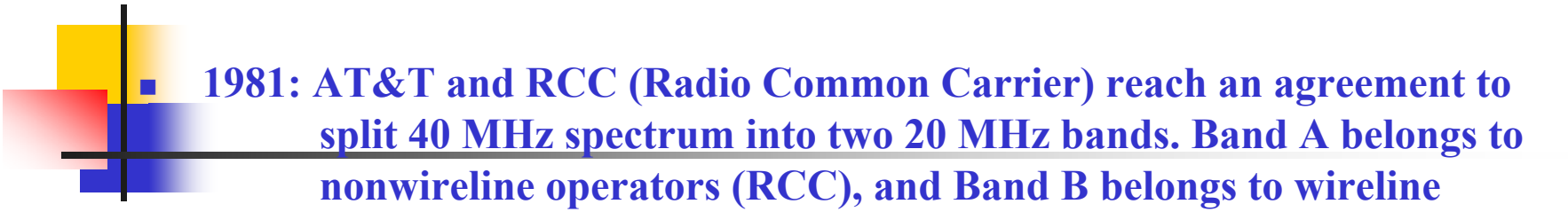
-802.16

The History of Mobile Radio Communication (1/3)



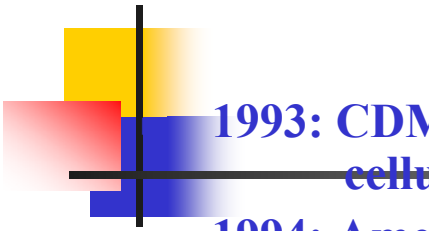
- 1880: Hertz – Initial demonstration of practical radio communication
- 1897: Marconi – Radio transmission to a tugboat over an 18 mi path
- 1921: Detroit Police Department: -- Police car radio dispatch (2 MHz frequency band)
- 1933: FCC (Federal Communications Commission) – Authorized four channels in the 30 to 40 MHz range
- 1938: FCC – Ruled for regular service
- 1946: Bell Telephone Laboratories – 152 MHz (Simplex)
- 1956: FCC – 450 MHz (Simplex)
- 1959: Bell Telephone Laboratories – Suggested 32 MHz band for high capacity mobile radio communication
- 1964: FCC – 152 MHz (Full Duplex)
- 1964: Bell Telephone Laboratories – Active research at 800 MHz
- 1969: FCC – 450 MHz (Full Duplex)
- 1974: FCC – 40 MHz bandwidth allocation in the 800 to 900 MHz range
- 1981: FCC – Release of cellular land mobile phone service in the 40 MHz bandwidth in the 800 to 900 MHz range for commercial operation

The History of Mobile Radio Communication (2/3)



- 1981: AT&T and RCC (Radio Common Carrier) reach an agreement to split 40 MHz spectrum into two 20 MHz bands. Band A belongs to nonwireline operators (RCC), and Band B belongs to wireline operators (telephone companies). Each market has two operators.
- 1982: AT&T is divested, and seven RBOCs (Regional Bell Operating Companies) are formed to manage the cellular operations
- 1982: MFJ (Modified Final Judgment) is issued by the government DOJ. All the operators were prohibited to (1) operate long-distance business, (2) provide information services, and (3) do manufacturing business
- 1983: Ameritech system in operation in Chicago
- 1984: Most RBOC markets in operation
- 1986: FCC allocates 5 MHz in extended band
- 1987: FCC makes lottery on the small MSA and all RSA licenses
- 1988: TDMA (Time Division Multiple Access) voted as a digital cellular standard in North America
- 1992: GSM (Groupe Speciale Mobile) operable in Germany D2 system

The History of Mobile Radio Communication (3/3)



- 1993: CDMA (Code Division Multiple Access) voted as another digital cellular standard in North America
- 1994: American TDMA operable in Seattle, Washington
- 1994: PDC (Personal Digital Cellular) operable in Tokyo, Japan
- 1994: Two of six broadband PCS (Personal Communication Service) license bands in auction
- 1995: CDMA operable in Hong Kong
- 1996: US Congress passes Telecommunication Reform Act Bill
- 1996: The auction money for six broadband PCS licensed bands (120 MHz) almost reaches 20 billion US dollars
- 1997: Broadband CDMA considered as one of the third generation mobile communication technologies for UMTS (Universal Mobile Telecommunication Systems) during the UMTS workshop conference held in Korea
- 1999: ITU (International Telecommunication Union) decides the next generation mobile communication systems

  (e.g., W-CDMA, cdma2000, etc)

Generacje telefonii komórkowej (1)

- Generacja I (1G) - systemy oparte na technice analogowej,
  - świadczą głównie zwykłe rozmowy telefoniczne
  - funkcjonują na częstotliwości rzędu 450MHz,
- Generacja II (2G) - systemy oparte na technice cyfrowej,
  - funkcjonują na częstotliwości rzędu 900MHz,
  - w ramach systemu GSM dostępne są między innymi usługi takie, jak: poczta głosowa, przeniesienie połączenia, blokowanie połączeń, oczekiwanie na połączenie, zawieszenie połączenia, połączenie konferencyjne, identyfikacja rozmówcy, biling (szczegółowy rachunek), możliwość przesyłania danych komputerowych i faksów, przesyłanie wiadomości tekstowych, w 1997 r. poprawiono funkcjonalność sieci - dodano dwie szybsze technologie transmisji danych: HSCSD (High Speed Circuit Swiched Data) do 115kb/s i GPRS (General Packed Radio Service) do 170kb/s;

Generacje telefonii komórkowej (2)

- Generacja III (3G) - systemy cyfrowe, zapewniają korzystanie z bardzo dużego zakresu usług, w tym multimedialnych w skali wykraczającej poza możliwości systemów drugiej generacji (GSM) oraz zdolność do połączenia możliwości korzystania z komponentów naziemnych i satelitarnych o globalnym zasięgu, umożliwia integrację wszystkich systemów radiokomunikacyjnych, zaprojektowany pod kątem jak największej wydajności w transmitowaniu danych (384Kb/s - 2Mb/s).
- Generacja IV (2010 ?)

  Od pewnego okresu trwają badania nad nową technologią - 4G. Komercyjny debiut tej sieci jest przewidywany na rok 2010. Definicja 4G przyjęta przez Międzynarodową Unię Telekomunikacyjną ITU mówi, że pobieranie danych w takich sieciach powinno odbywać się z prędkością 1Gb/s w sytuacji gdy telefon jest nieruchomy oraz około 100Mb/s podczas szybkiego przemieszczanie się abonenta.

First Generation Cellular Systems and Services

1970s	Developments of radio and computer technologies for 800/900 MHz mobile communications
1976	WARC (World Administrative Radio Conference) allocates spectrum for cellular radio
1979	NTT (Nippon Telephone & Telegraph) introduces the first cellular system in Japan
1981	NMT (Nordic Mobile Telephone) 900 system introduced by Ericsson Radio System AB and deployed in Scandinavia
1984	AMPS (Advanced Mobile Phone Service) introduced by AT&T in North America

Second Generation Cellular Systems and Services

1982	CEPT (Conference Europeenne des Post et Telecommunications) established GSM to define future Pan-European Cellular Radio Standards
1990	Interim Standard IS-54 (USDC) adopted by TIA (Telecommunications Industry Association)
1990	Interim Standard IS-19B (NAMPS) adopted by TIA
1991	Japanese PDC (Personal Digital Cellular) system standardized by the MPT (Ministry of Posts and Telecommunications)
1992	Phase I GSM system is operational
1993	Interim Standard IS-95 (CDMA) adopted by TIA
1994	Interim Standard IS-136 adopted by TIA
1995	PCS Licenses issued in North America
1996	Phase II GSM operational
1997	North American PCS deploys GSM, IS-54, IS-95
1999	IS-54: North America IS-95: North America, Hong Kong, Israel, Japan, China, etc GSM: 110 countries

Third Generation Cellular Systems and Services (1/2)

IMT-2000 (International Mobile Telecommunications-2000):

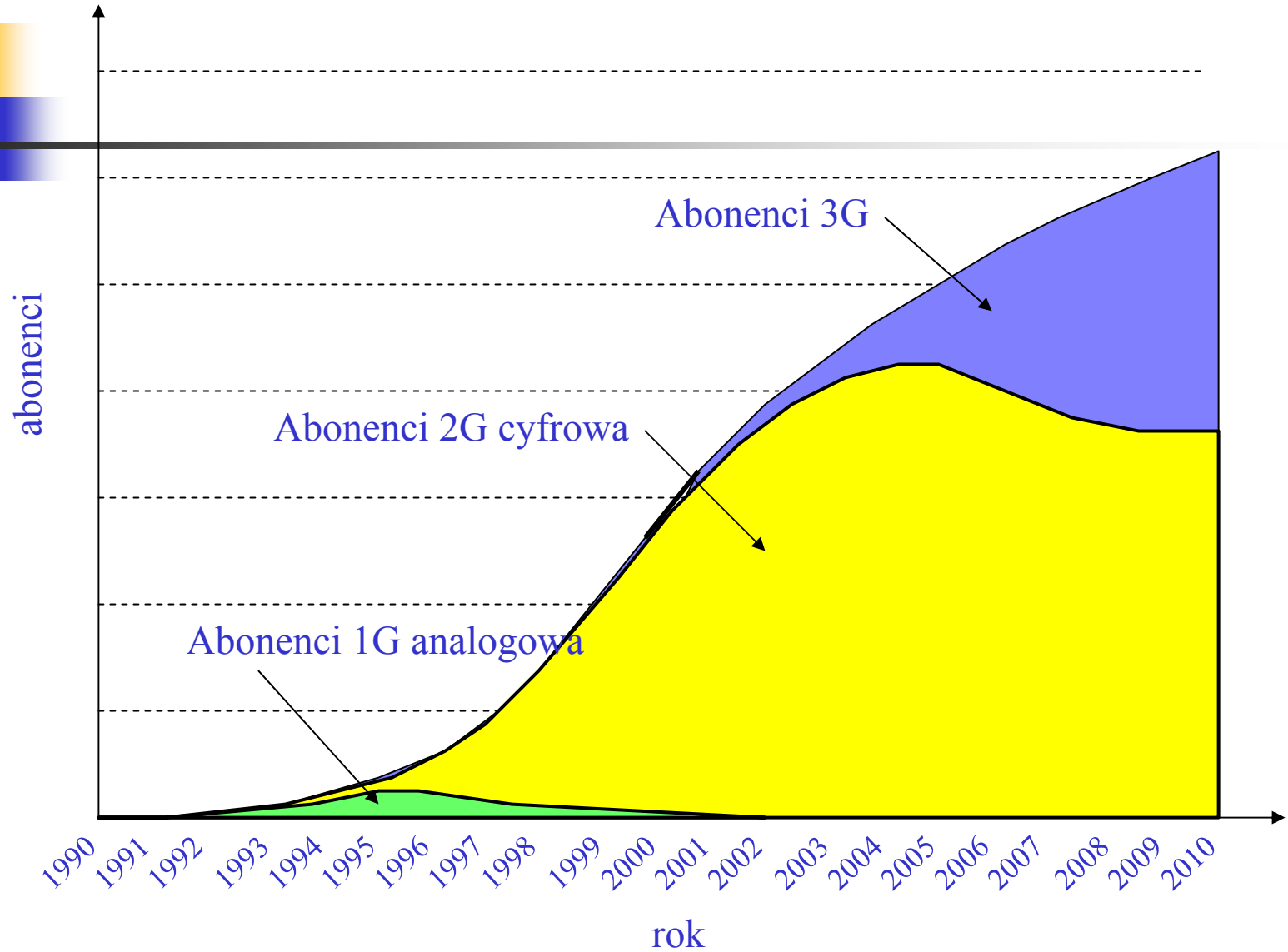
- Fulfill one's dream of anywhere, anytime communications a reality.

- **Key Features of IMT-2000 include:**
  - High degree of commonality of design worldwide;
  - Compatibility of services within IMT-2000 and with the fixed networks;
    - High quality;
    - Small terminal for worldwide use;
    - Worldwide roaming capability;
    - Capability for multimedia applications, and a wide range of services and terminals.

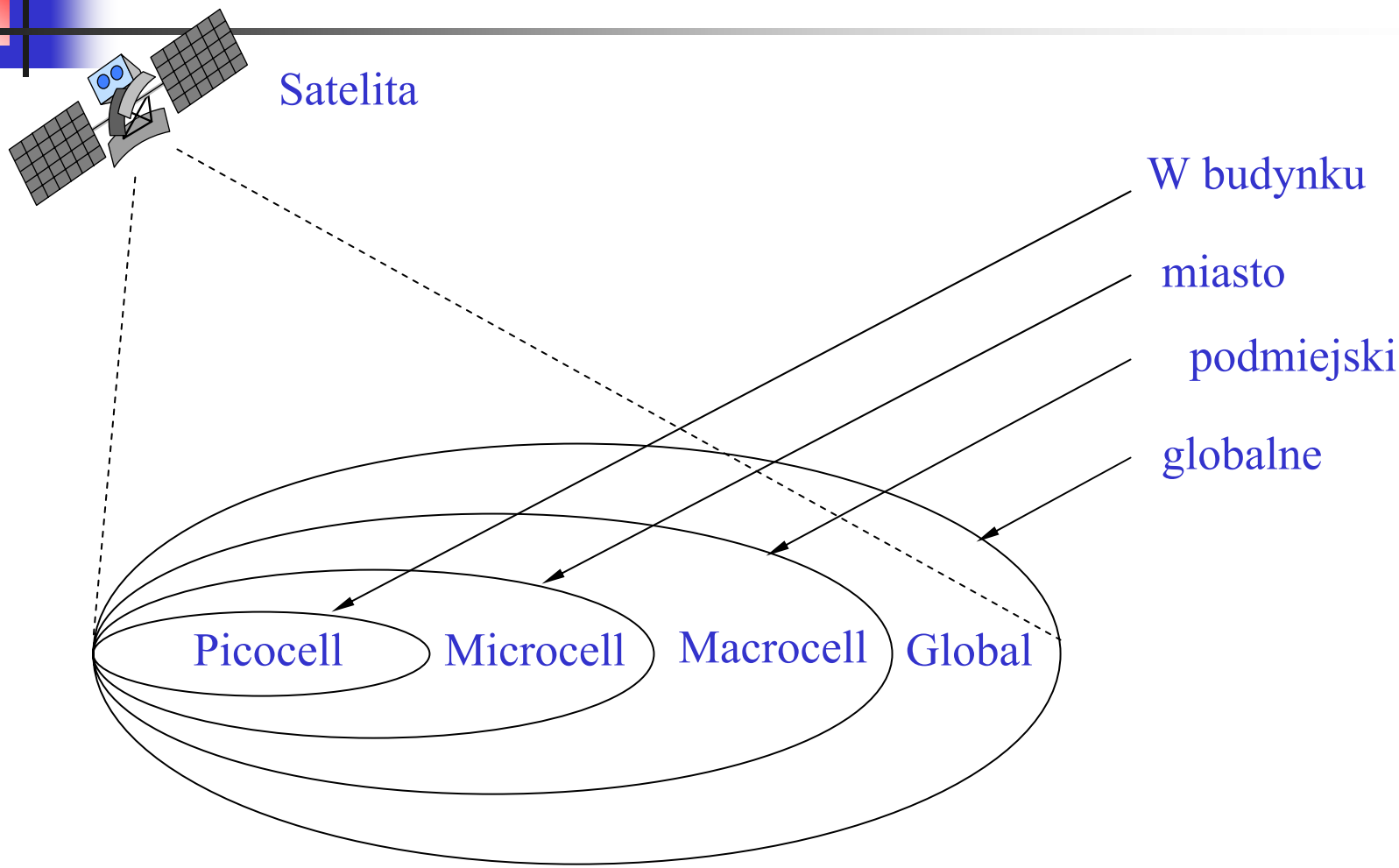
Third Generation Cellular Systems and Services (2/2)

- **Important Component of IMT-2000 is ability to provide high bearer rate capabilities:**
  - 2 Mbps for fixed environment;
  - 384 Kbps for indoor/outdoor and pedestrian environments;
  - 144 kbps for vehicular environment.
- **Standardization Work:**
  - Release 1999 specifications
  - In processing
- **Scheduled Service:**
  - Started in October 2001 in Japan (W-CDMA)

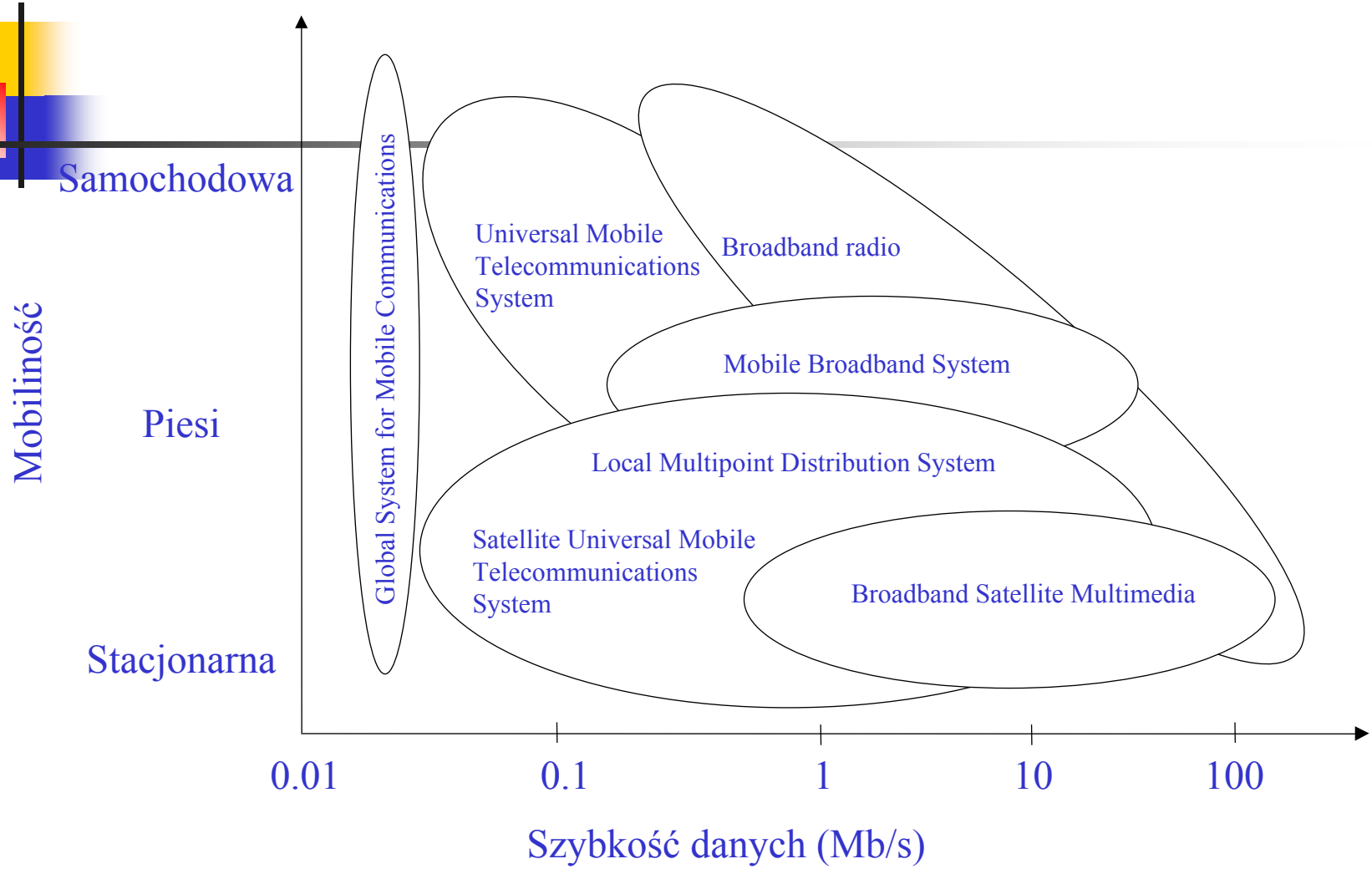
Wzrost liczby abonentów



Aspekt pokrycia w mobilnych komunikacyjnych systemach 3 generacji

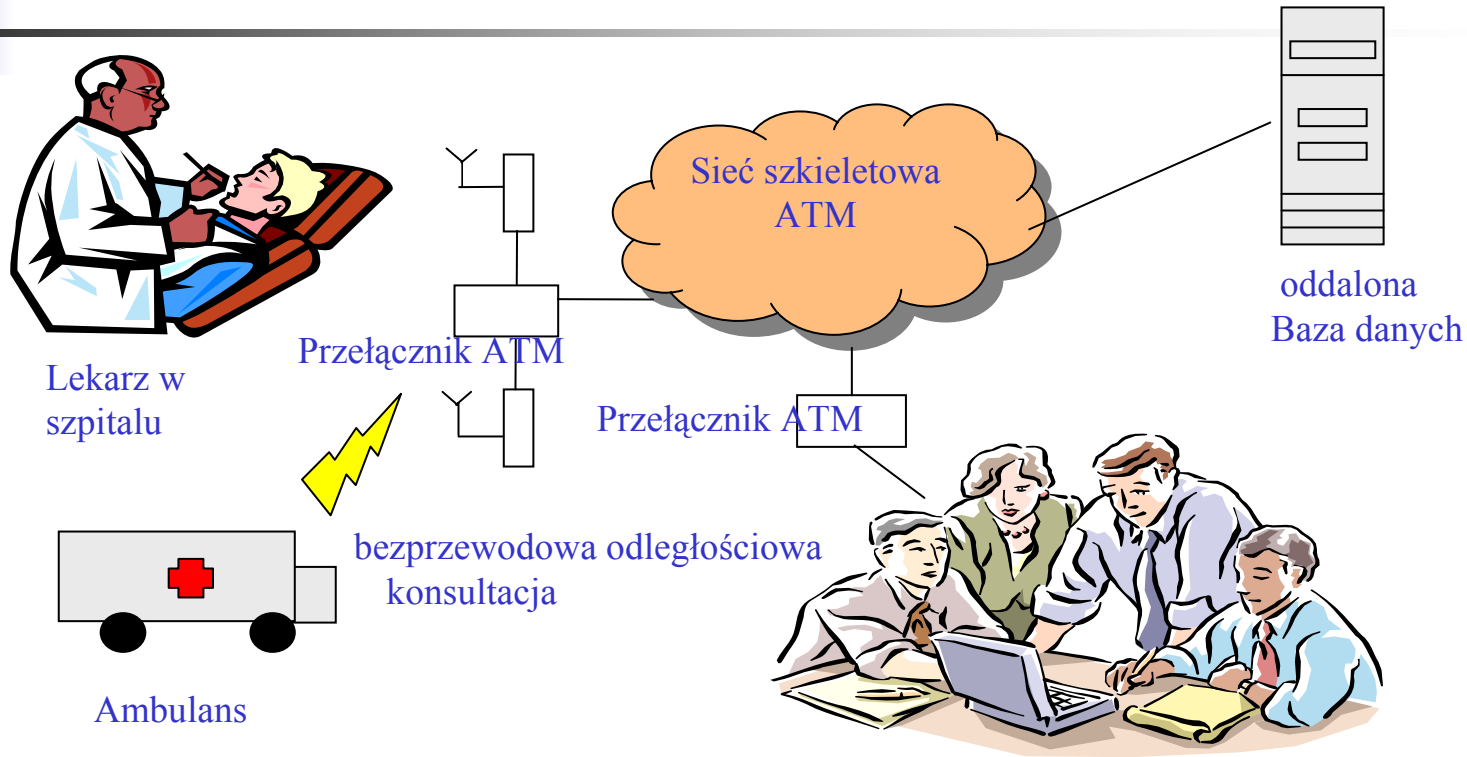


Prędkości transmisji

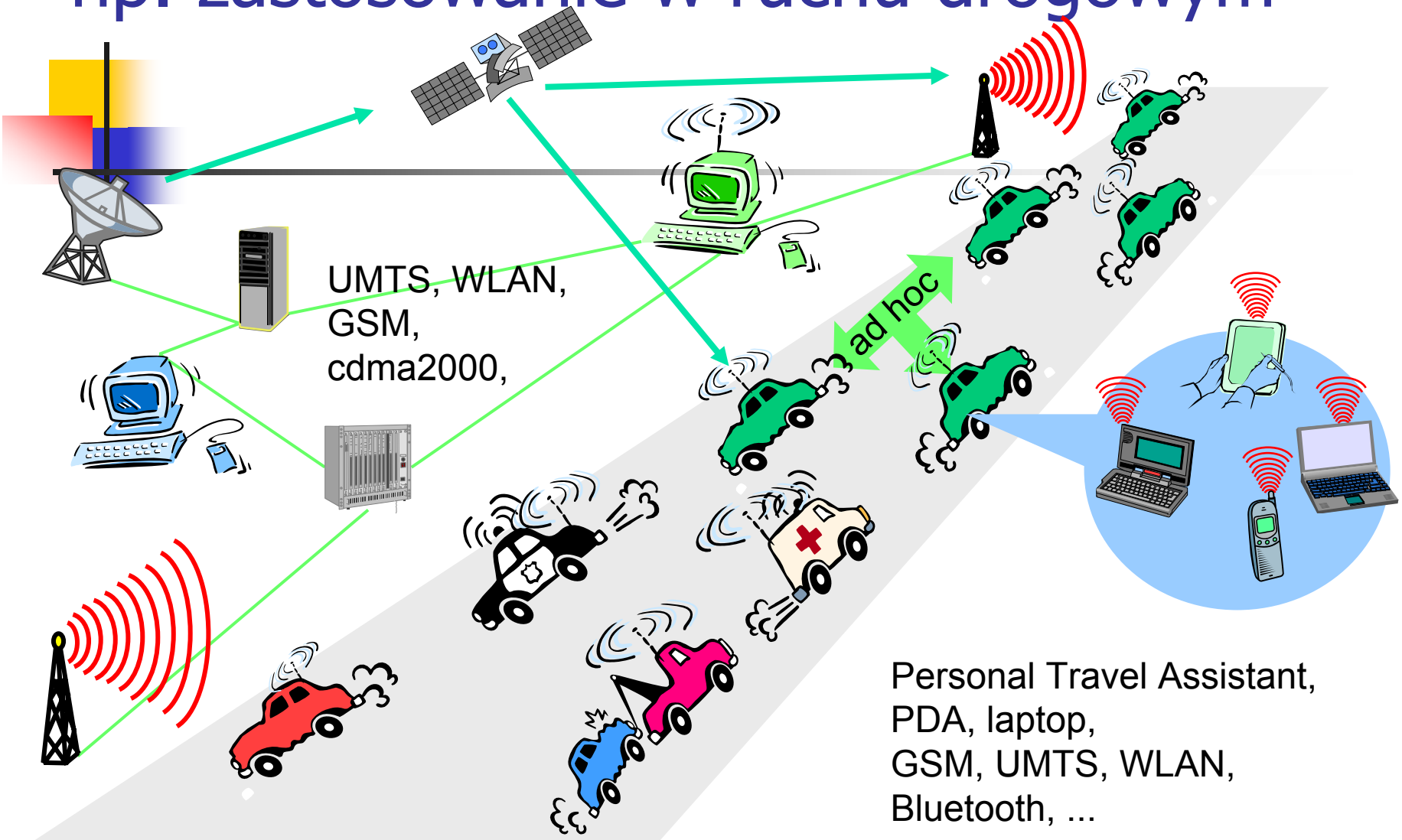


Prędkości transmisji jako funkcja mobilności w niektórych systemach o dostępie radiowym

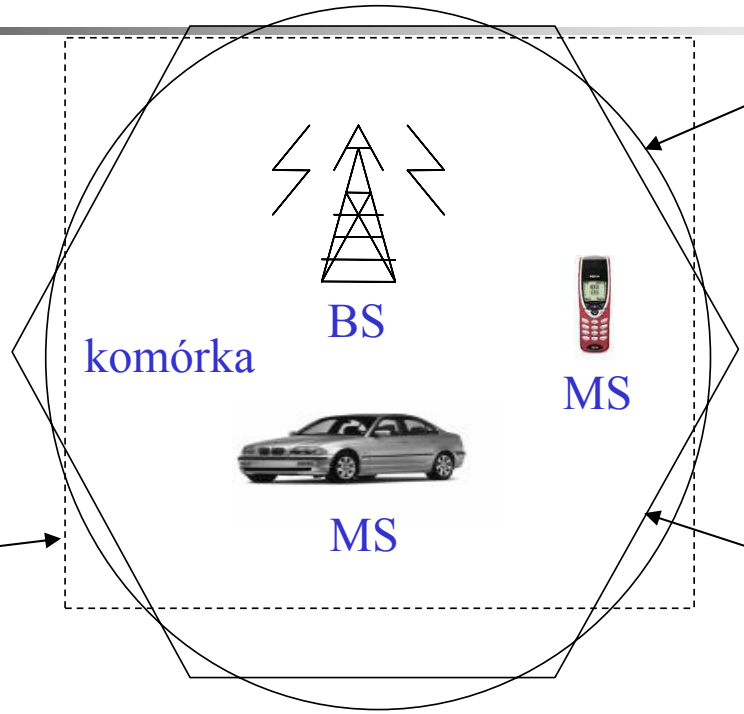
np. zastosowania medyczne



np. zastosowanie w ruchu drogowym



Sieci komórkowe



Idealna powierzchnia komórki (promień 2-10 km)

Alternatywny kształt komórki

Powierzchnia sześciokątnej komórki używana w większości modeli

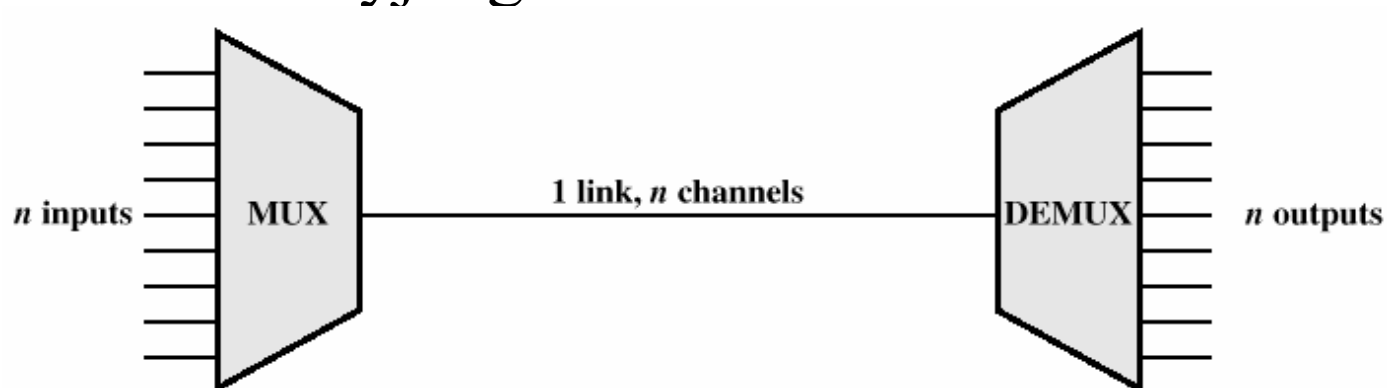
Pojedyńcza komórka sieci ze stacjami mobilnymi (MS) oraz stacją bazową (BS)

Pojedyńcza komórka

- W każdej komórce wielu użytkowników jest obsługiwanych przez pojedyńczą BS
- Jeżeli zamierza się powiększyć obszar komórki to dodatkowe BS-y są umieszczane w tych obszarach
- ograniczony zakres częstotliwości jest przydzielony do obsługi komórki
- Żeby zwiększyć efektywność systemu pewne techniki **multipleksowania** są używane

Multipleksowanie

- Pojemność medium transmisyjnego przekracza zwykle pojemność wymaganą
- Multipleksowanie – przenoszenie wielu sygnałów w pojedyńczym medium
  - Bardziej efektywne użycie medium transmisyjnego



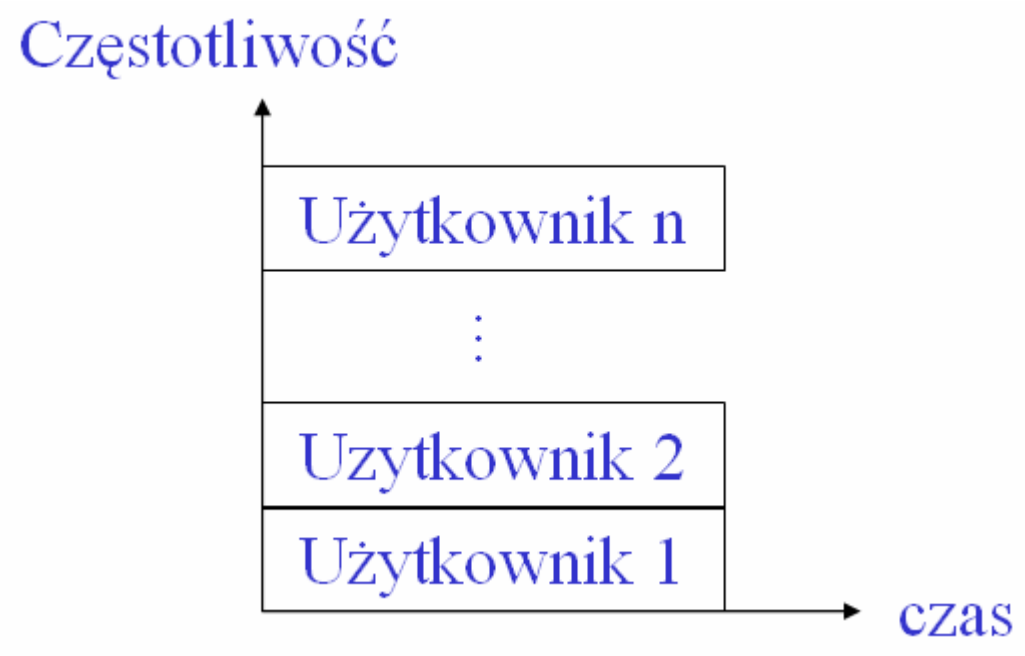
Techniki multipleksowania

- FDMA (**Frequency Division Multiple Access)**
- TDMA **(Time Division Multiple Access)**
- CDMA **(Code Division Multiple Access)**
- OFDM **(Orthogonal Frequency Division Multiplexing)**

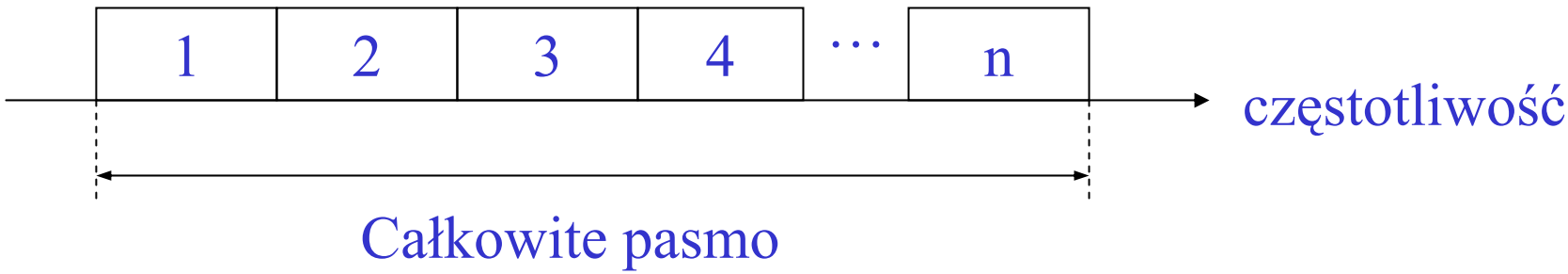
- Nowa technika SDMA **(Space Division Multiple Access)** jest również aktualnie testowana z użyciem anten mikrofalowych

FDMA (Frequency Division Multiple Access)
(multipleksowanie z podziałem częstotliwości) - w systemach 1G

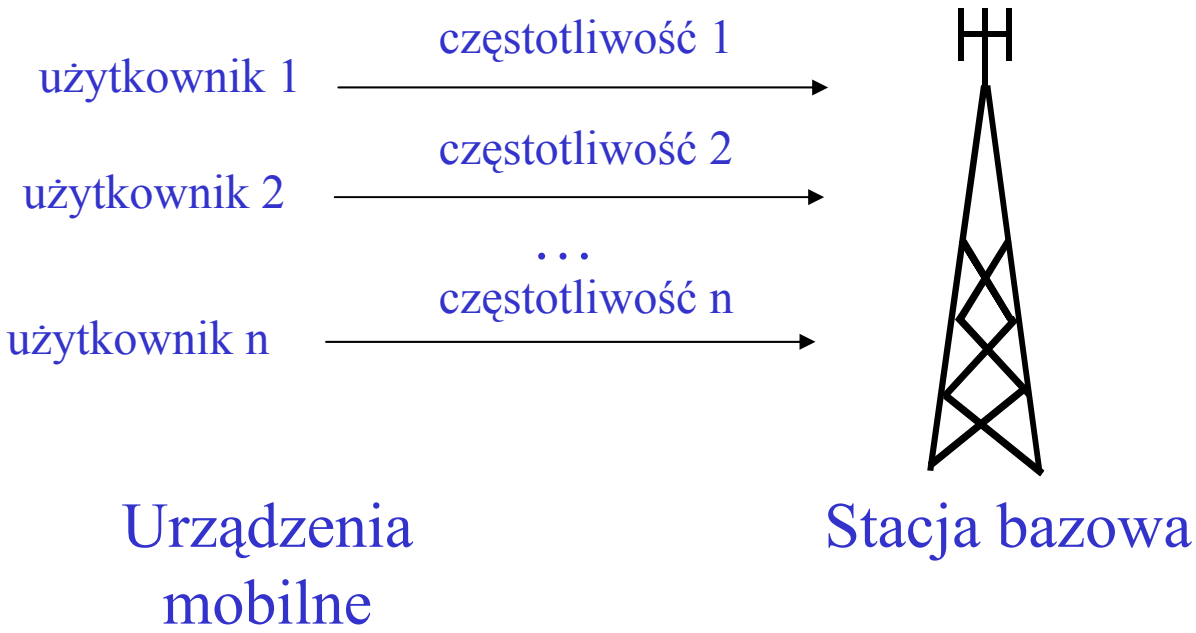
- Pasmo częstotliwości jest dzielone na podpasma nazywane **kanałami**
- Pojedyńczy kanał jest przydzielany przez BS do uzytkownika



Struktura pasma w FDMA



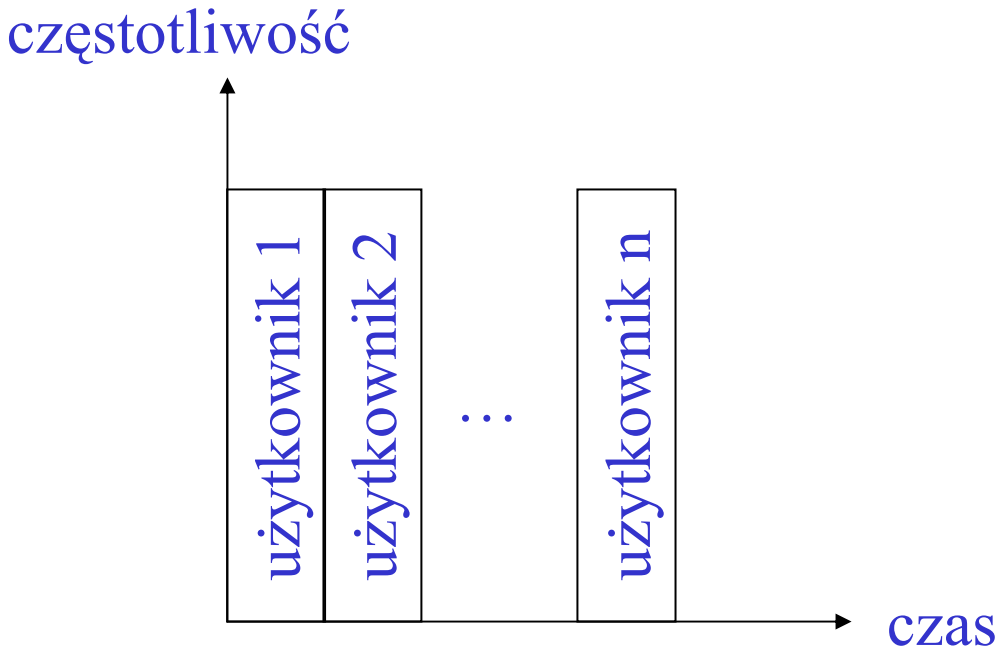
Przydział kanału w FDMA

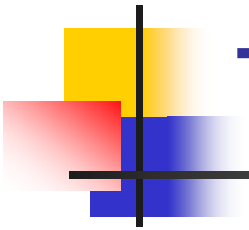


TDMA (Time Division Multiple Access)

(multipleksowanie z podziałem czasu)

– w większości systemów 2G

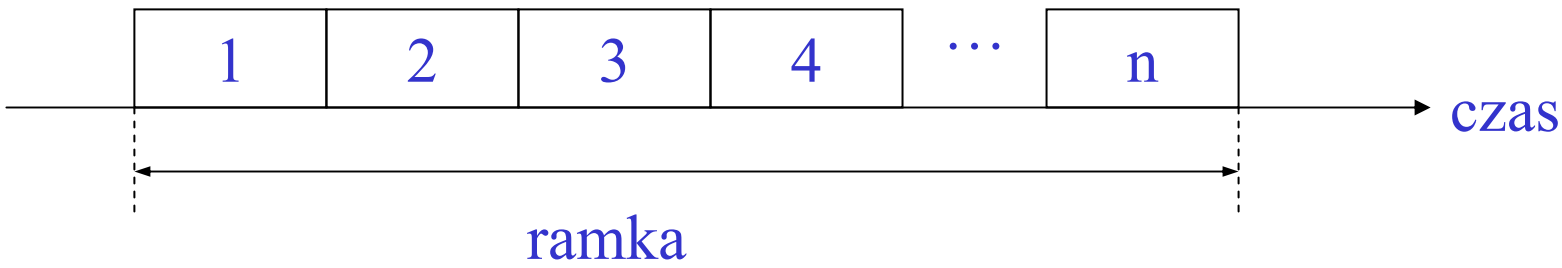




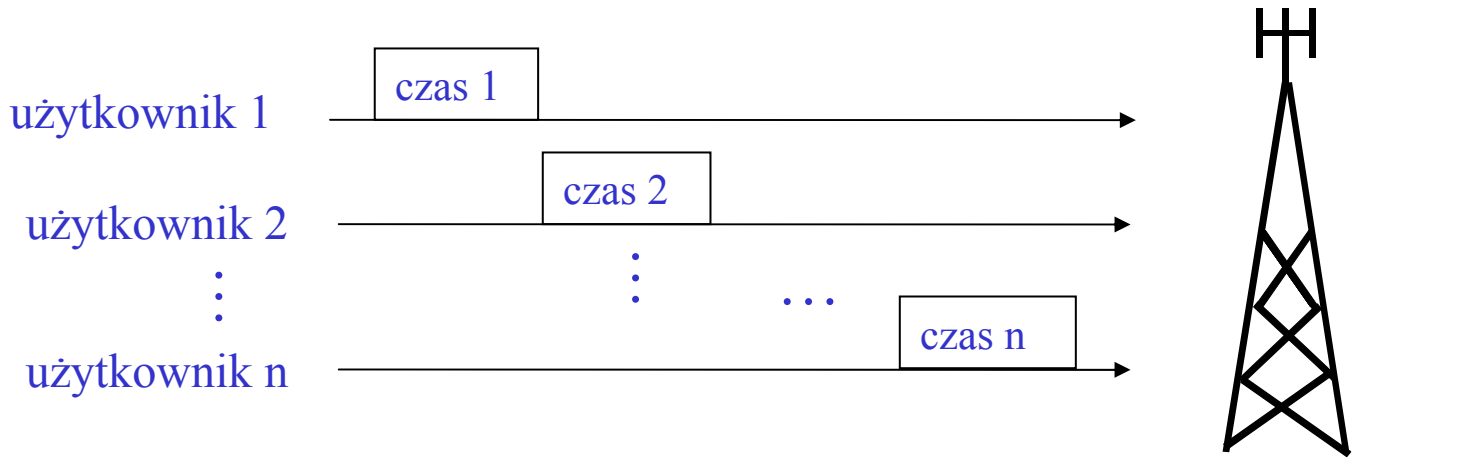
TDMA

- Czas dzielony jest na ramki o stałej długości
- Każda ramka składa się ze stałej liczby sczelin czasowych
- Dla danego połączenia BS przydziela jedną szczelinę czasową – tę samą w kolejnych ramkach

Struktura ramki TDMA



Ilustracja ramki TDMA dla wielu użytkowników



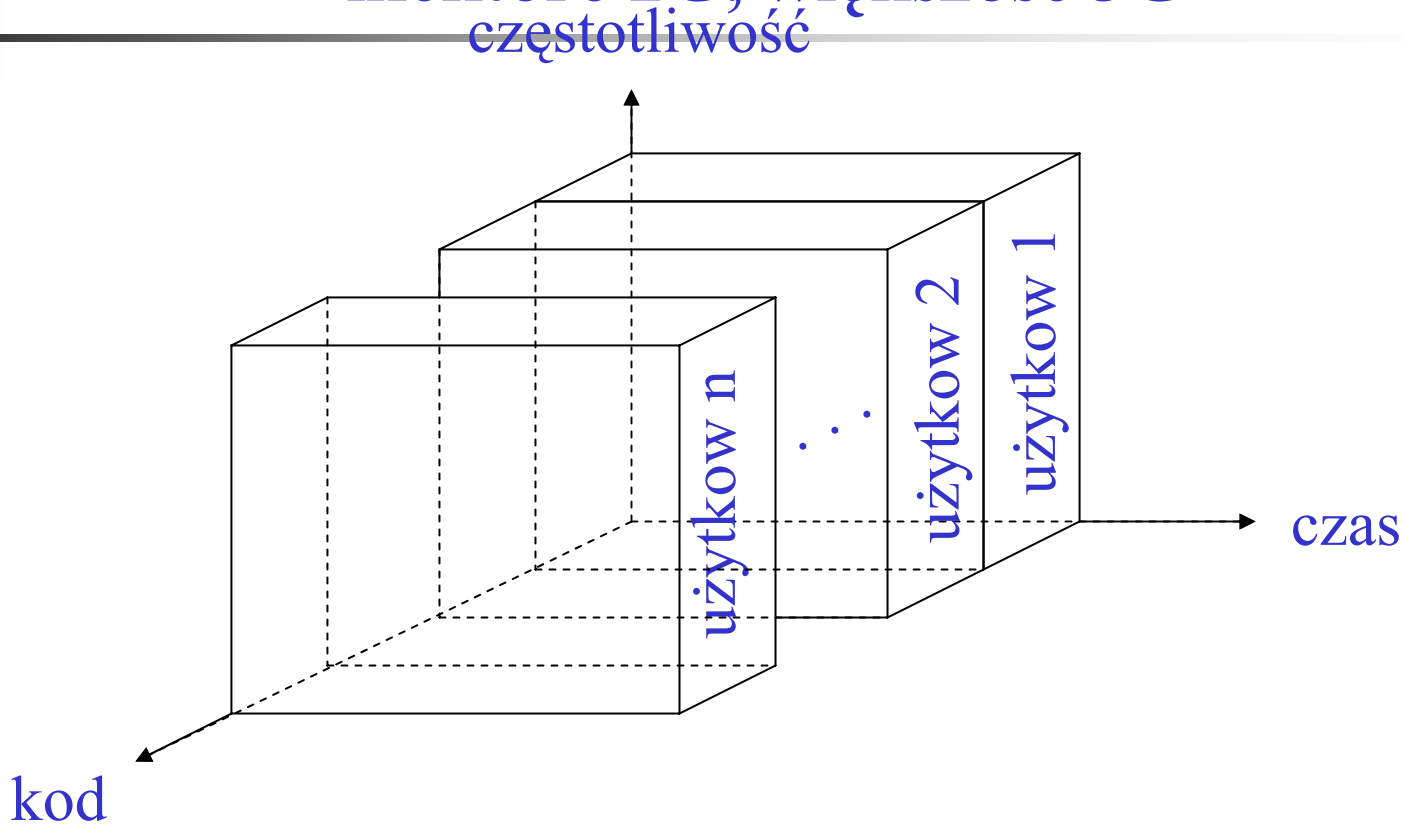
Urządzenia mobilne

Stacja bazowa

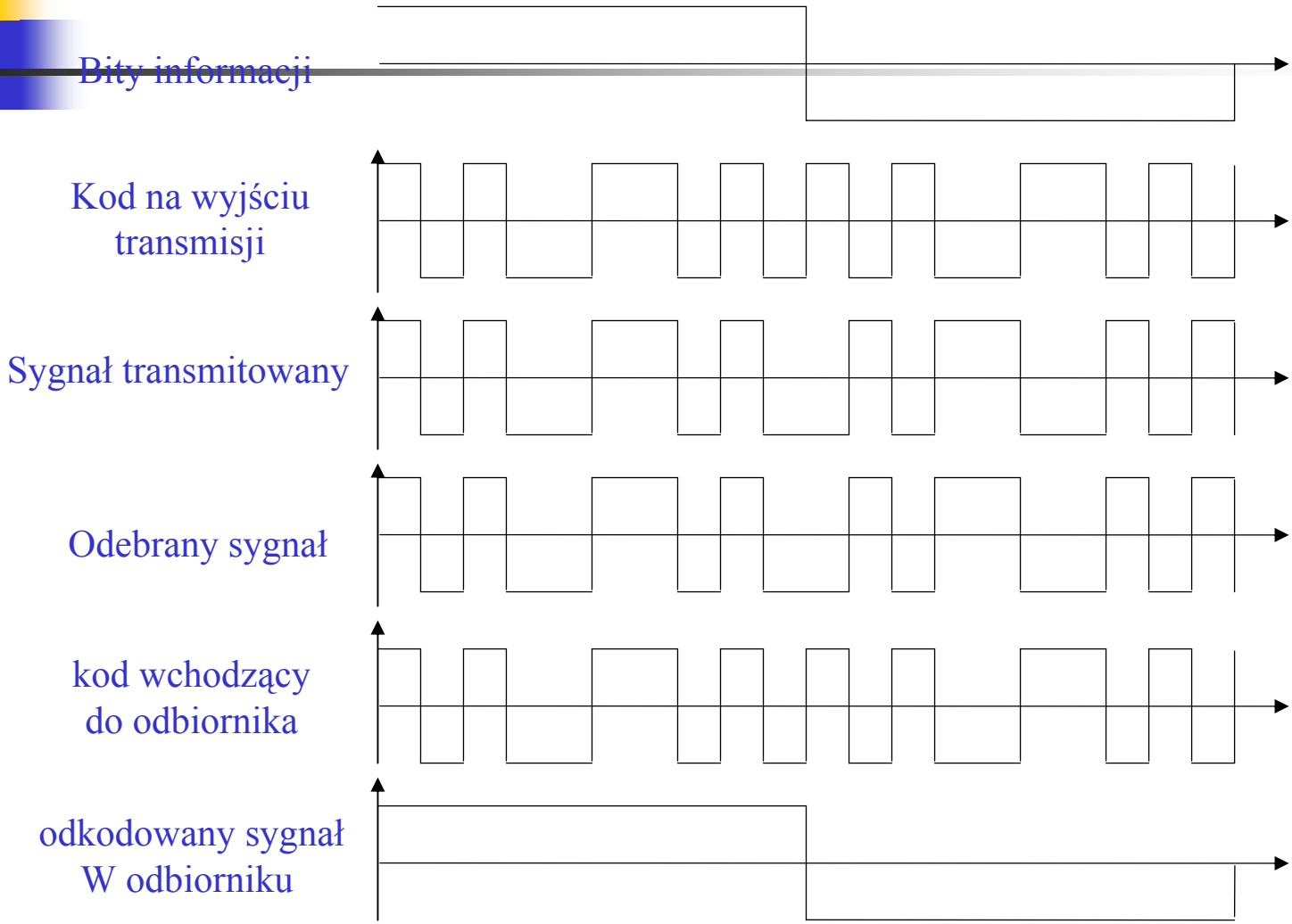
CDMA (Code Division Multiple Access)

(multipleksowanie z podziałem kodu)

– niektóre 2G, większość 3G



Transmitowane i odbierane sygnały w systemie CDMA



OFDM (Orthogonal Frequency Division Multiplexing)

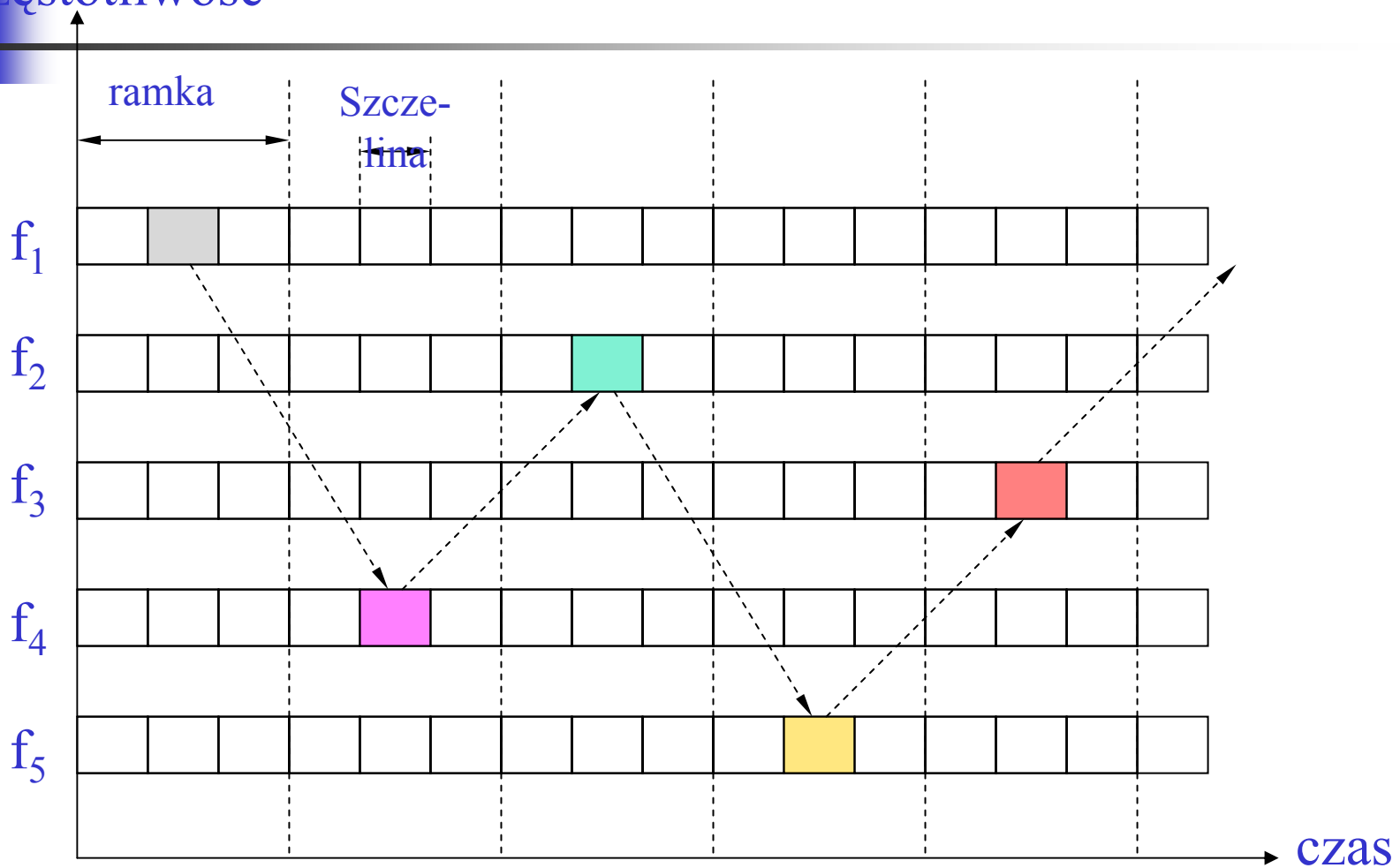
- Pojawiła się niedawno – pozwala na równoległą transmisję danych z użyciem wielu kanałów
- Używa technik transmisji wielonośnikowych, aby efektywnie redukować odbicia sygnałów radiowych w terenie

Techniki oparte na kombinacji FDMA, TDMA i CDMA

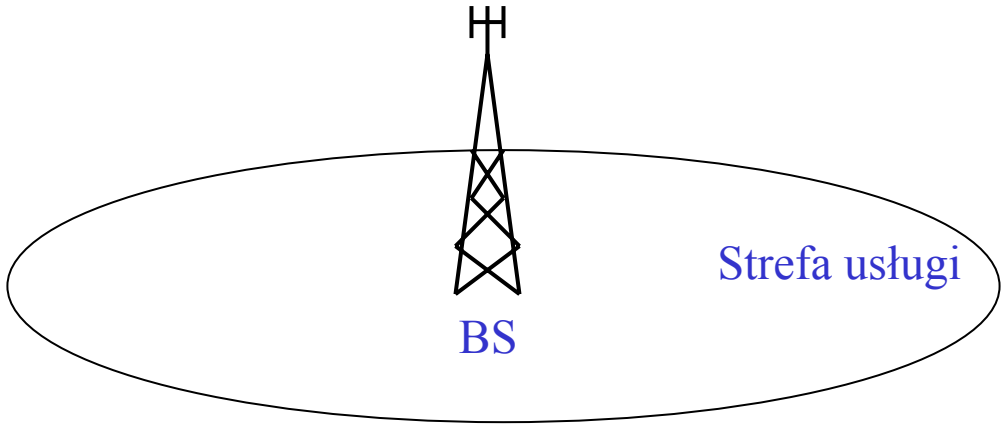
- Istnieje szereg technik będących wariantami i kombinacjami znanych już technik
- Jedną z nich jest tzw. **frequency hopping** – technika oparta na przeskokach częstotliwości (kombinacja FDMA i TDMA):

  - pojedyńczy użytkownik wykorzystuje jeden kanał przez określony czas, a następnie zmienia kanał na inny
  - każdy użytkownik ma określoną własną sekwencję zmian kanałów
  - ta technika oryginalnie była opracowana dla wojska w związku z problem, aby skutecznie przesyłać informację jeżeli nieprzyjaciel zagłusza określony zakres częstotliwości

Przeskoki częstotliwości: kombinacja FDMA i TDMA

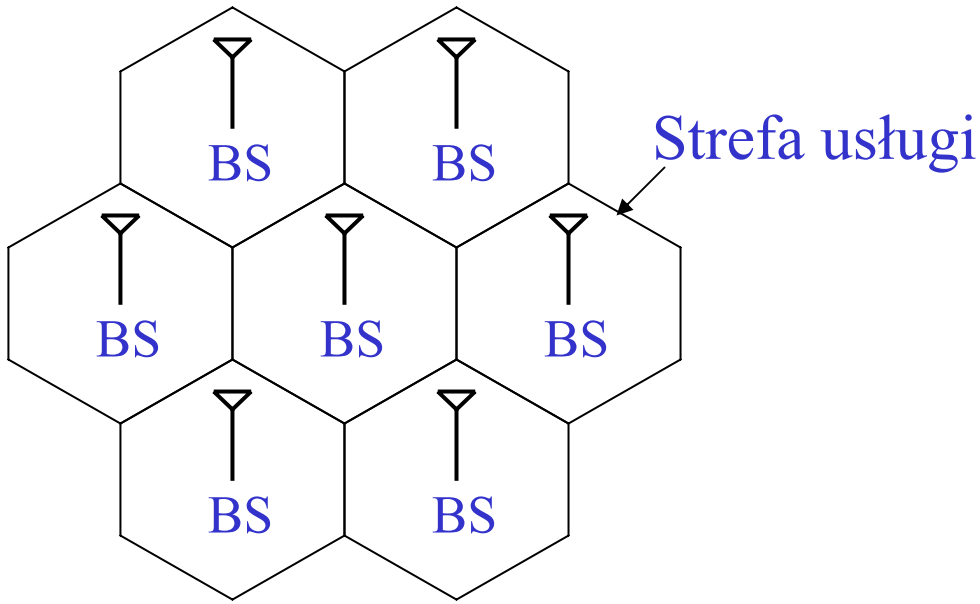


Ewolucja infrastruktura systemów komórkowych

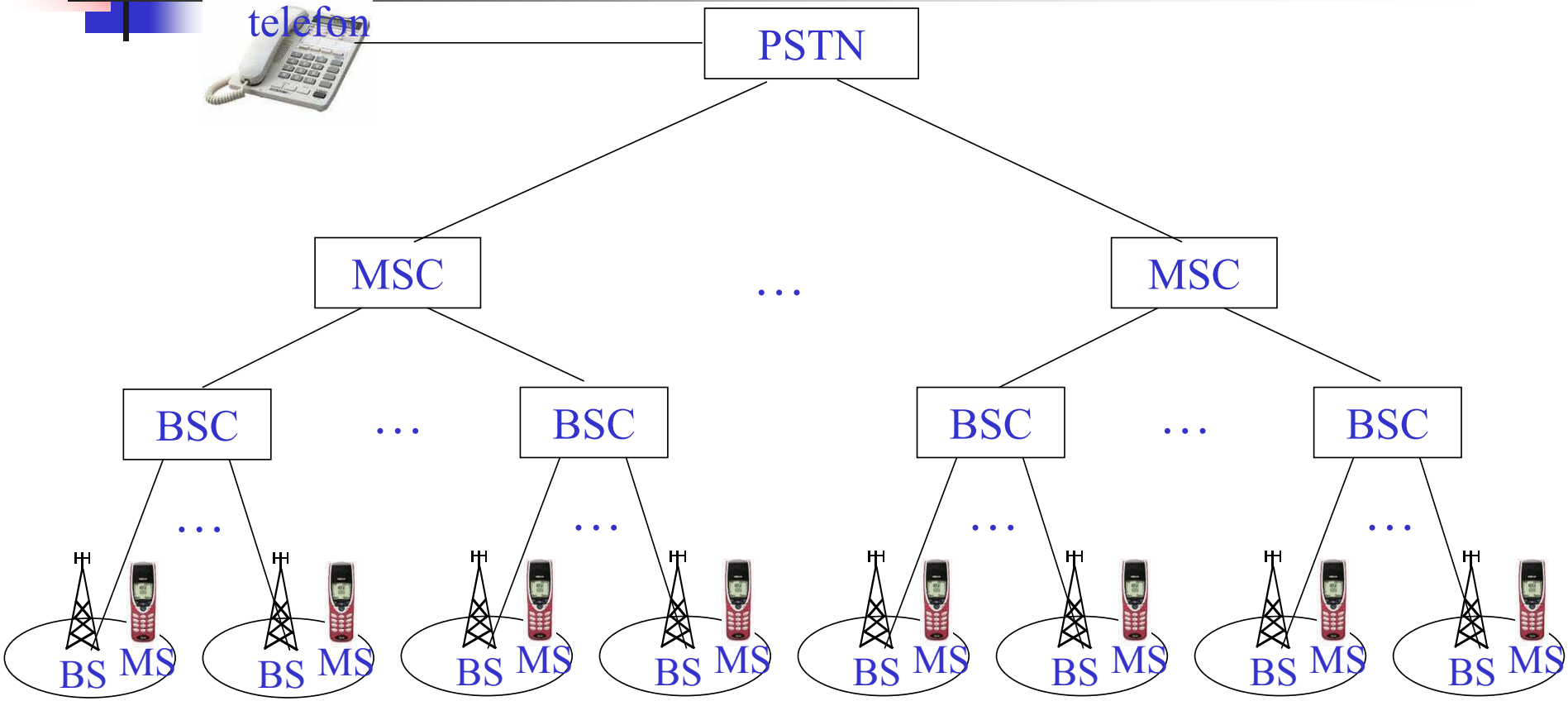


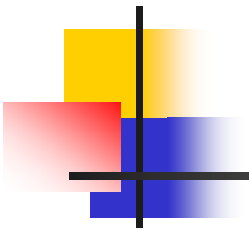
Wczesne systemy bezprzewodowe: *Duża strefa*

System komórkowy: mała pojedyńcza strefa

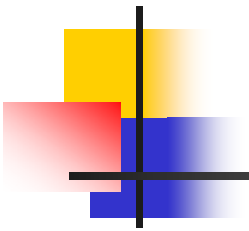


MS (mobile station), **BS** (base station), **BSC** (BSController), **MSC** (mobile switch center), **and PSTN** (public switched telephone network)





- BS składa się z odbiornika bazy (BTS) oraz kontrolera BS (BSC)
- Wieża i antena są częściami BS, podczas gdy pozostały sprzęt należy do BSC
- HLR (home location register) oraz VLR (visitor location register) to dwa zbiory wskaźników, które zapewniają mobilność i używanie tego samego numeru na całym świecie
- HLR jest ulokowany w MSC, w którym urządzenie mobilne jest zarejestrowane i gdzie informacja o początkowym jego położeniu oraz o bilingu jest przechowywana
- VLR zawiera informacje o wszystkich MS odwiedzających obszar danego MSC

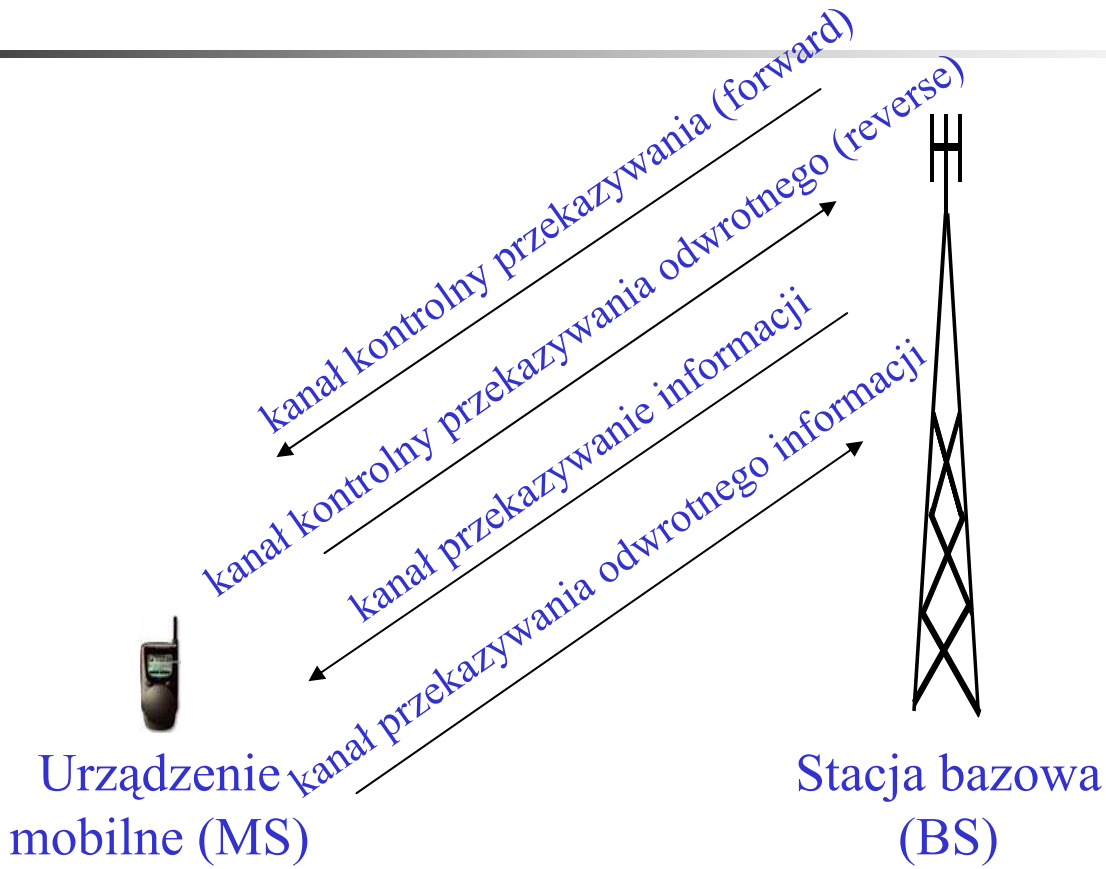


- Do obsługi każdego komórkowego (mobilnego) urządzenia potrzebne są 4 kanały zapewniające wymianę danych lub synchronizację między BS i MS

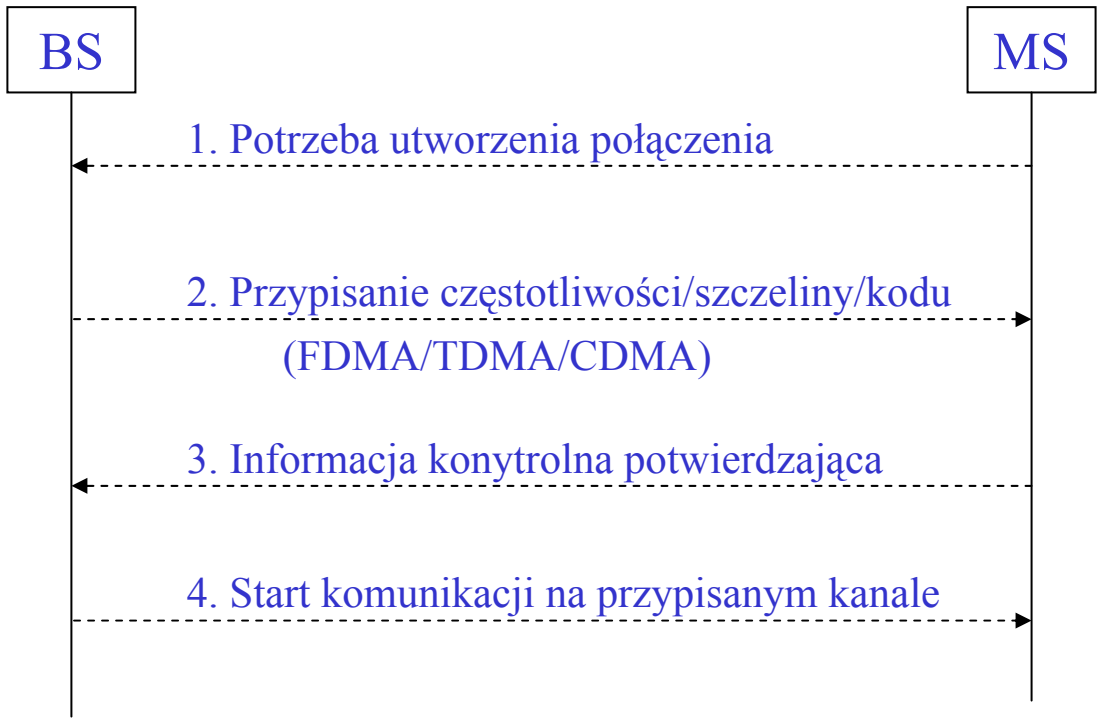
  - 2 kanały kontrolne: wymiana danych dotyczących uwierzytelnienia, danych o abonencie, ..

  - 2 kanały informacyjne do celów transmisji danych

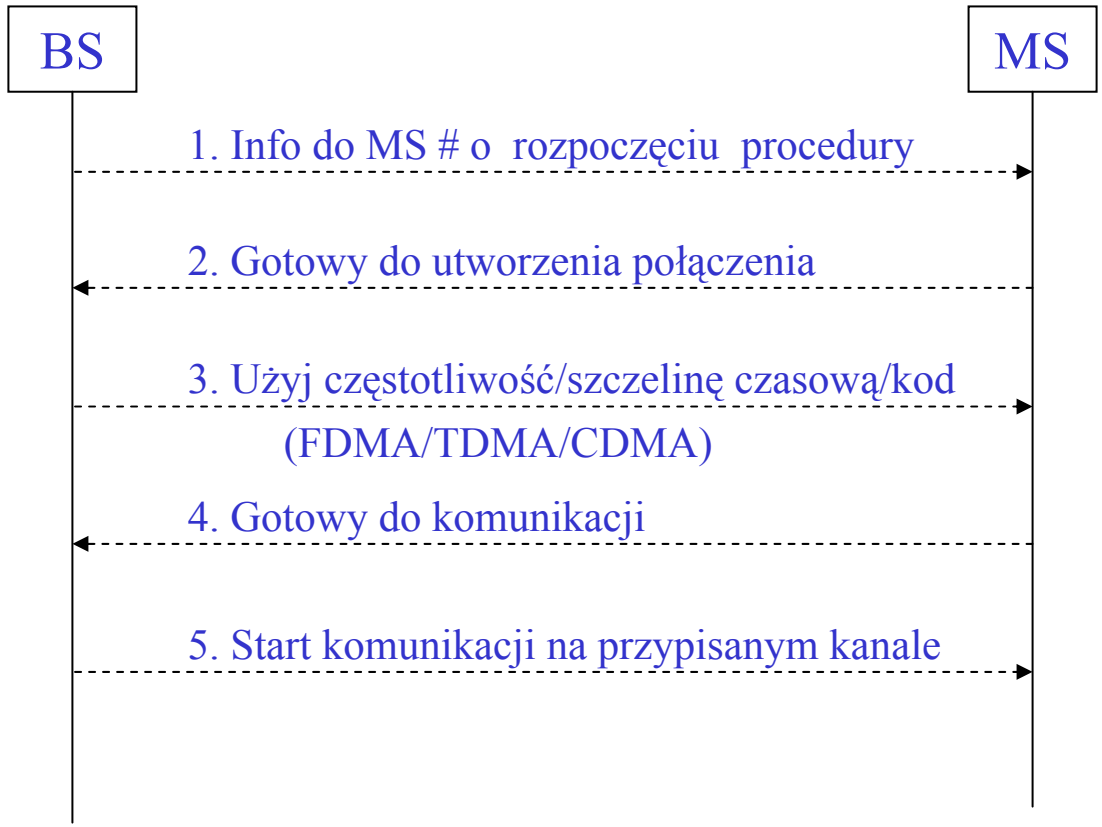
Kanały kontrolne i informacyjne



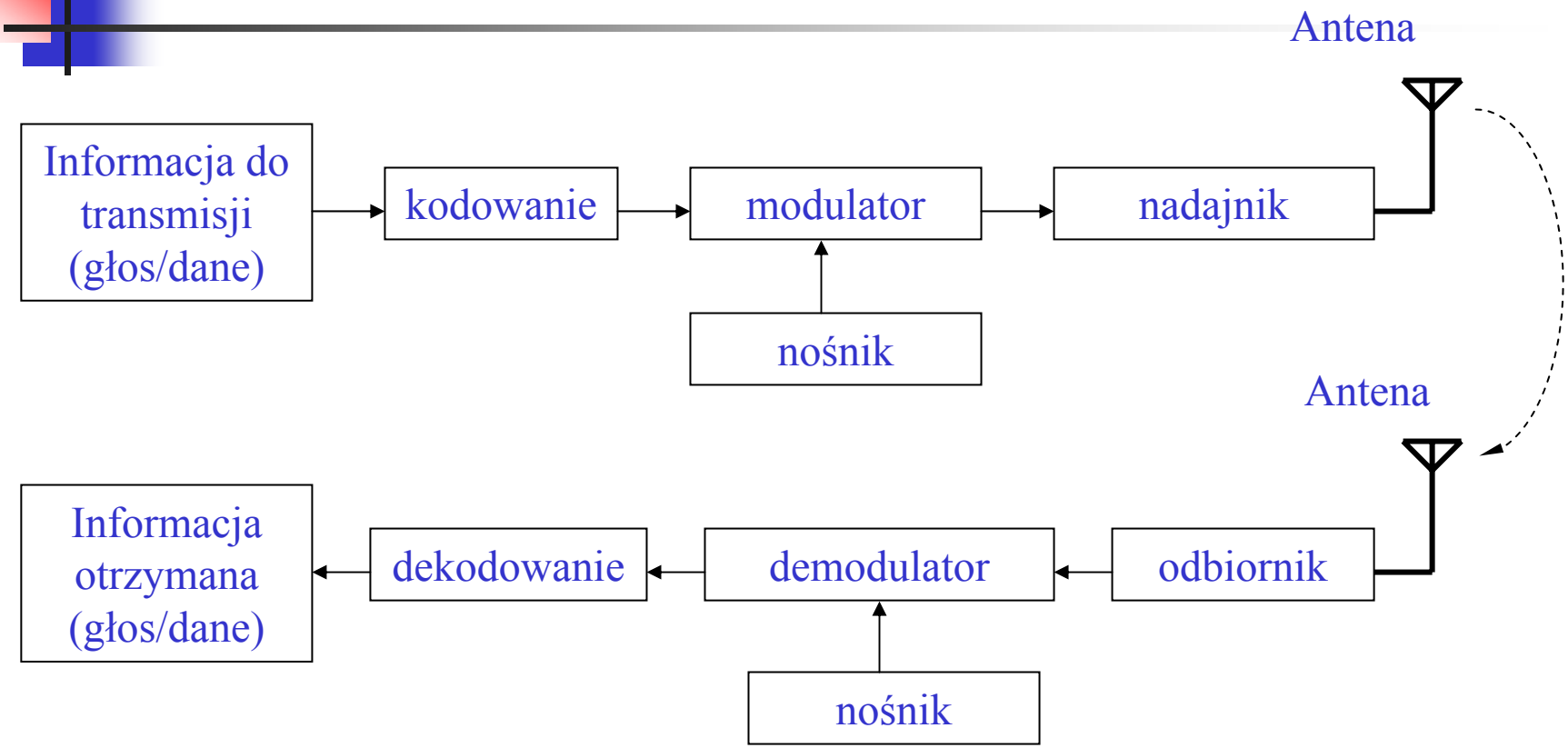
Kroki kanału kontrolnego poprzedzające rozpoczęcie pracy kanału informacyjnego między MS a BS (handshake steps)



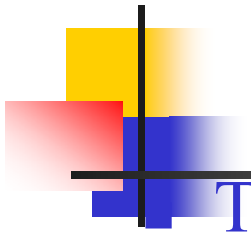
Kroki kanału kontrolnego poprzedzające rozpoczęcie pracy kanału informacyjnego między BS a MS (handshake steps)



Uproszczony bezprzewodowy system komunikacyjny



Systemy satelitarne

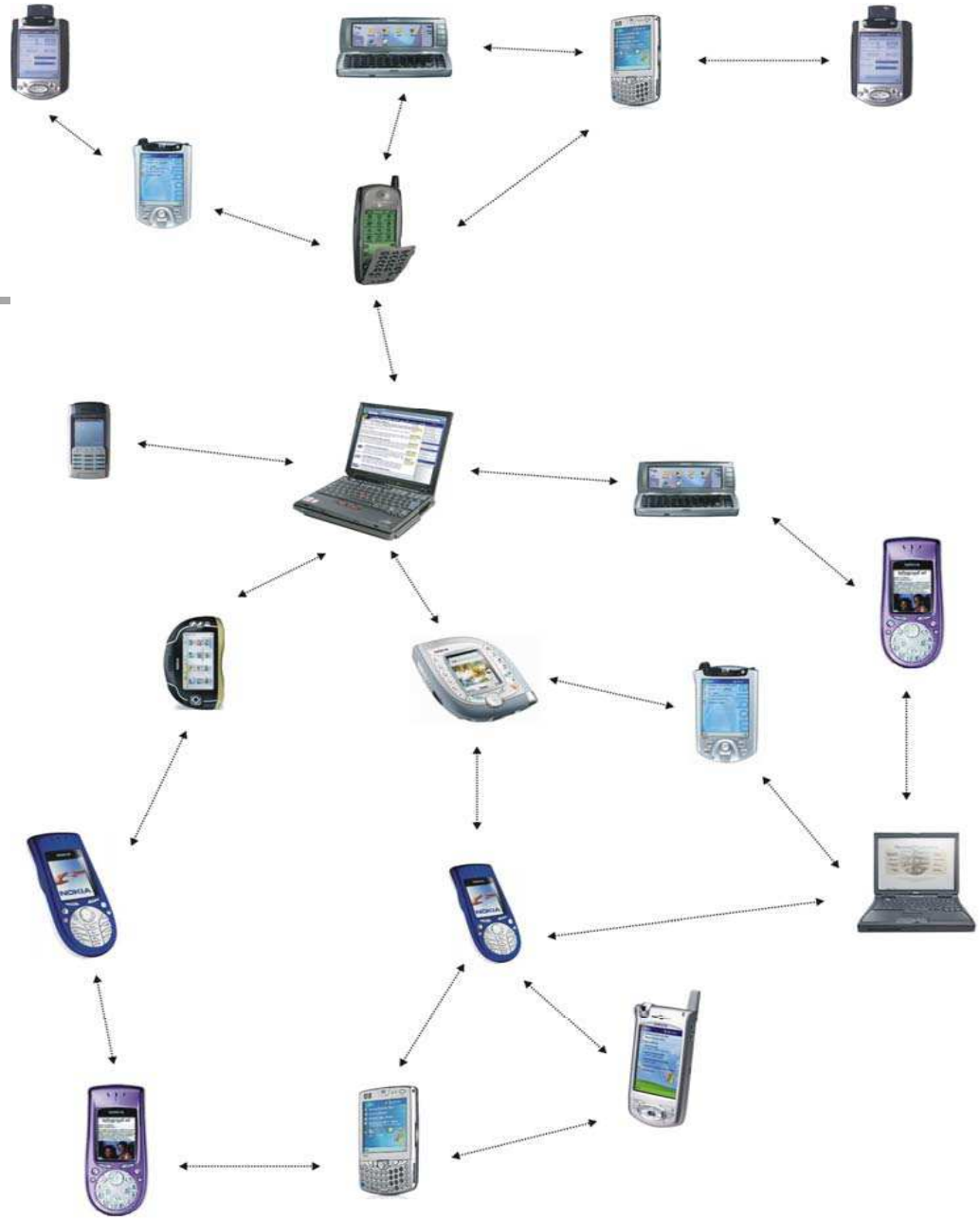


- Tradycyjne zastosowania
  - Satelity do prognozowania pogody
  - Transmisje radiowe i TV
  - satelity militarne
- Zastosowania telekomunikacyjne
  - Globalne połączenia telefoniczne
  - szkielet sieci globalnej
  - GPS

Sieci ad hoc

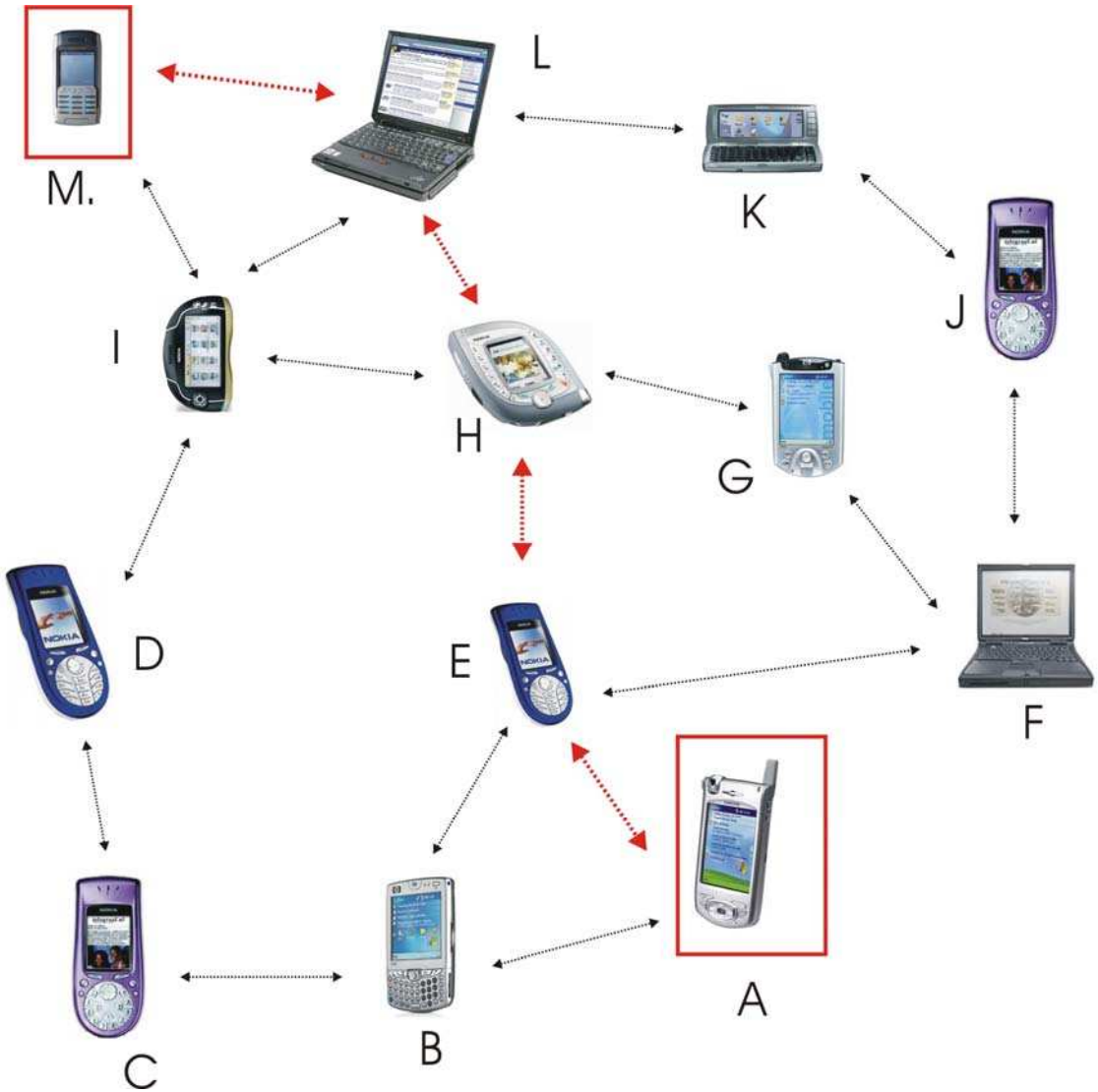
- Składają się z urządzeń mobilnych wyposażonych w karty do komunikacji bezprzewodowej (w jednym określonym standardzie)

- Każde urządzenie potrafi „rozmawiać” z każdym znajdującym się w jego radiowym „polu widzenia”



Komunikacja typu multi hop

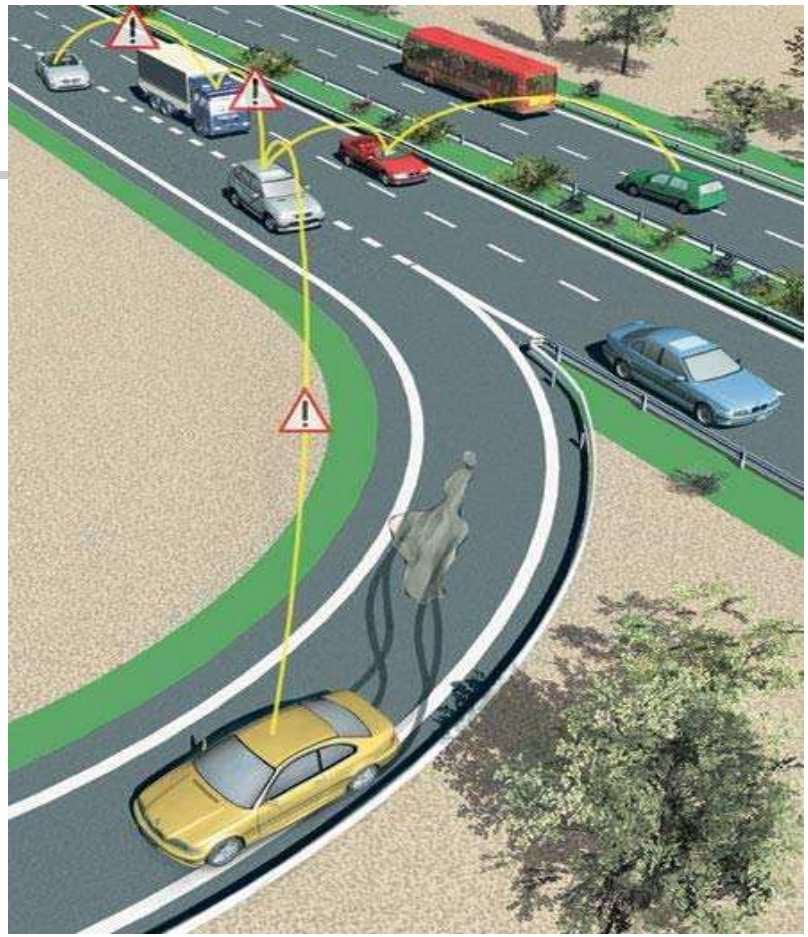
- Węzeł A komunikuje się z węzłem M
- W tym celu wykorzystuje węzły pośredniczące, E, H, L



Zastosowanie sieci ad hoc w przemyśle motoryzacyjnym

- Firma BMW pracuje nad projektem inteligentnego auta wykorzystującego m.in. sieci ad hoc.

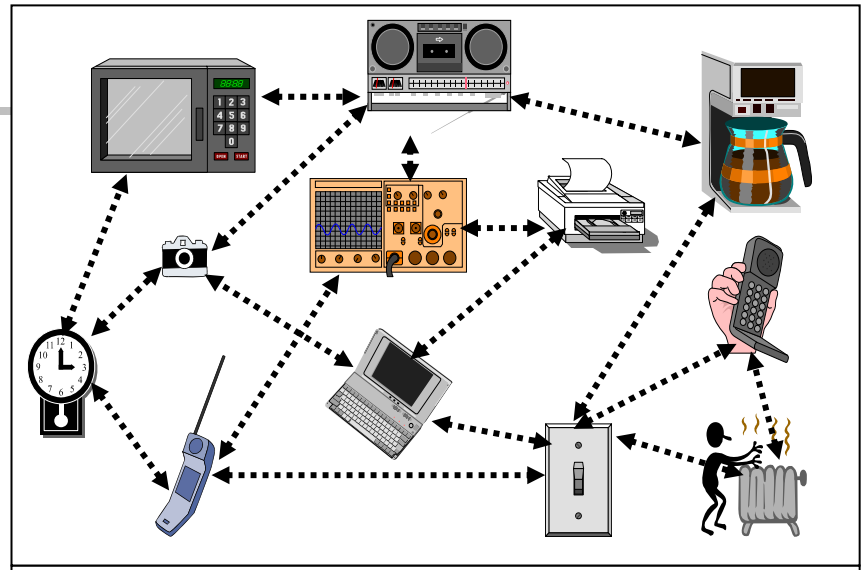
- Zastosowanie sieci ad hoc w samochodach umożliwia wymianę informacji pomiędzy samochodami. Przykładowo mogą to być ostrzeżenia o zagrożeniach, korkach itp.

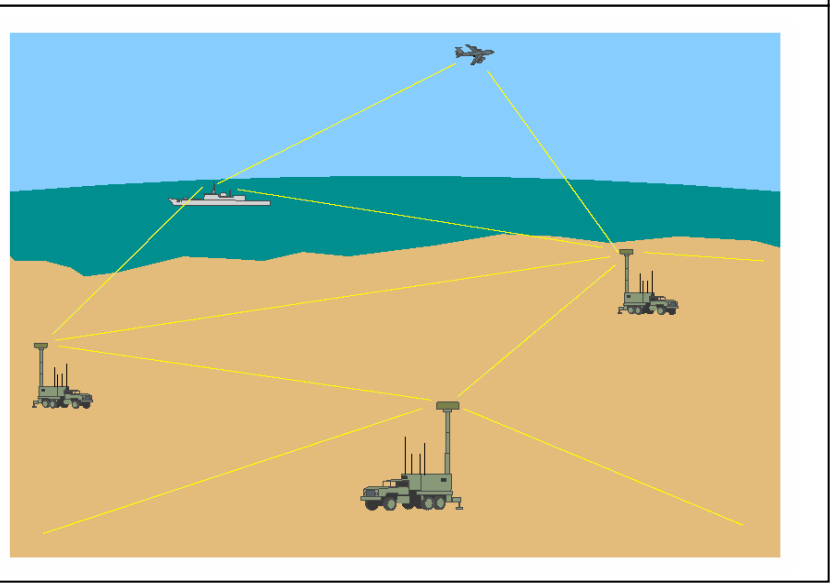


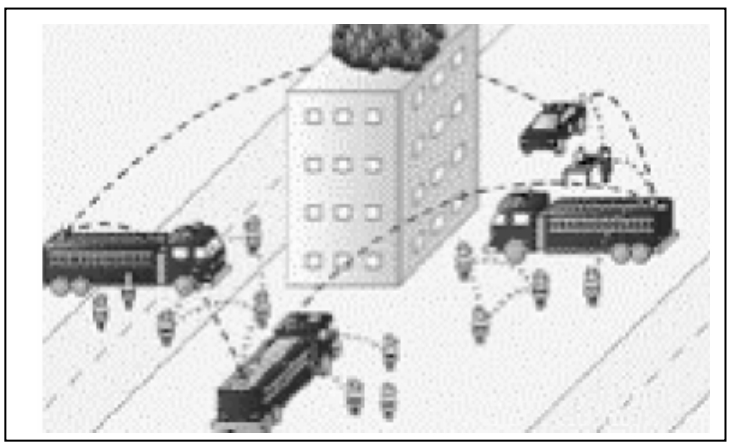
Ostrzeżenie przed niebezpieczeństwem

Zastosowania sieci ad hoc

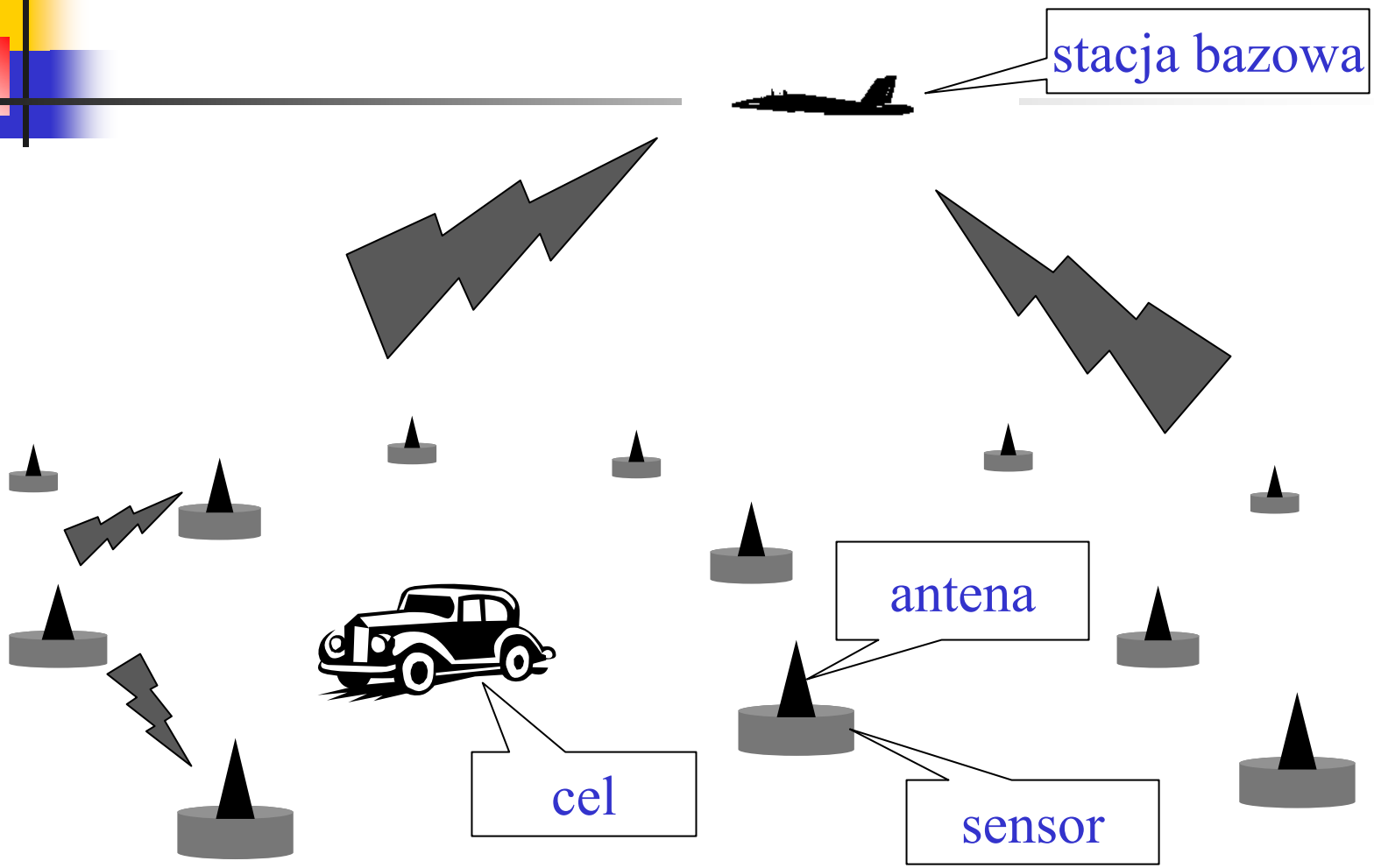
- Private Area Networks, projekt cybernetycznego domu – brak kabli, samokonfigurowalne, wymiana dokumentów i gier, „sterowanie mikserem”
- Akcje ratunkowe
- Konferencje
- Operacje militarne







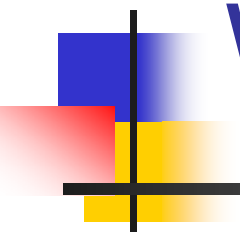
Bezprzewodowe sieci sensorowe



Ważniejsze technologie sieci bezprzewodowych

- IEEE 802.11, 30m
- HiperLAN, 30m
- Sieci ad hoc, >500m
- Sieci sensorowe, 2m
- Home RF, 30m
- Ricochet, 30m
- Sieci Bluetooh, 10m

- Peer-to-peer połączenia
- Lotniska, sprzęt AGD
- Pole walki, zagrożenia
- Fabryki chemiczne, nuklearne
- Domy
- Lotniska, biura
- biura



Wprowadzenie-koniec

Podstawy transmisji sygnałów

Sygnał elektromagnetyczny

- Jest funkcją czasu
- Może być również wyrażony jako funkcja częstotliwości
  - Sygnał składa się ze składowych o róznych częstotliwościach

Koncepcja sygnału

- sygnał analogowy – intensywność sygnału zmienia się w sposób łagodny w czasie
  - Brak przerw czy nieciągłości w sygnale
- sygnał cyfrowy – podtrzymywana jest intensywność sygnału na stałym poziomie przez pewien okres czasu a następnie zmienia się on do innego stałego poziomu
- sygnał periodyczny – sygnał analogowy lub cyfrowy, którego obraz powtarza się periodycznie (cyklicznie) w czasie

$$s(t+T) = s(t) \quad -\infty < t < +\infty$$

gdzie T jest okresem sygnału

- sygnał aperiodyczny – sygnał analogowy lub cyfrowy, którego obraz nie powtarza się w czasie

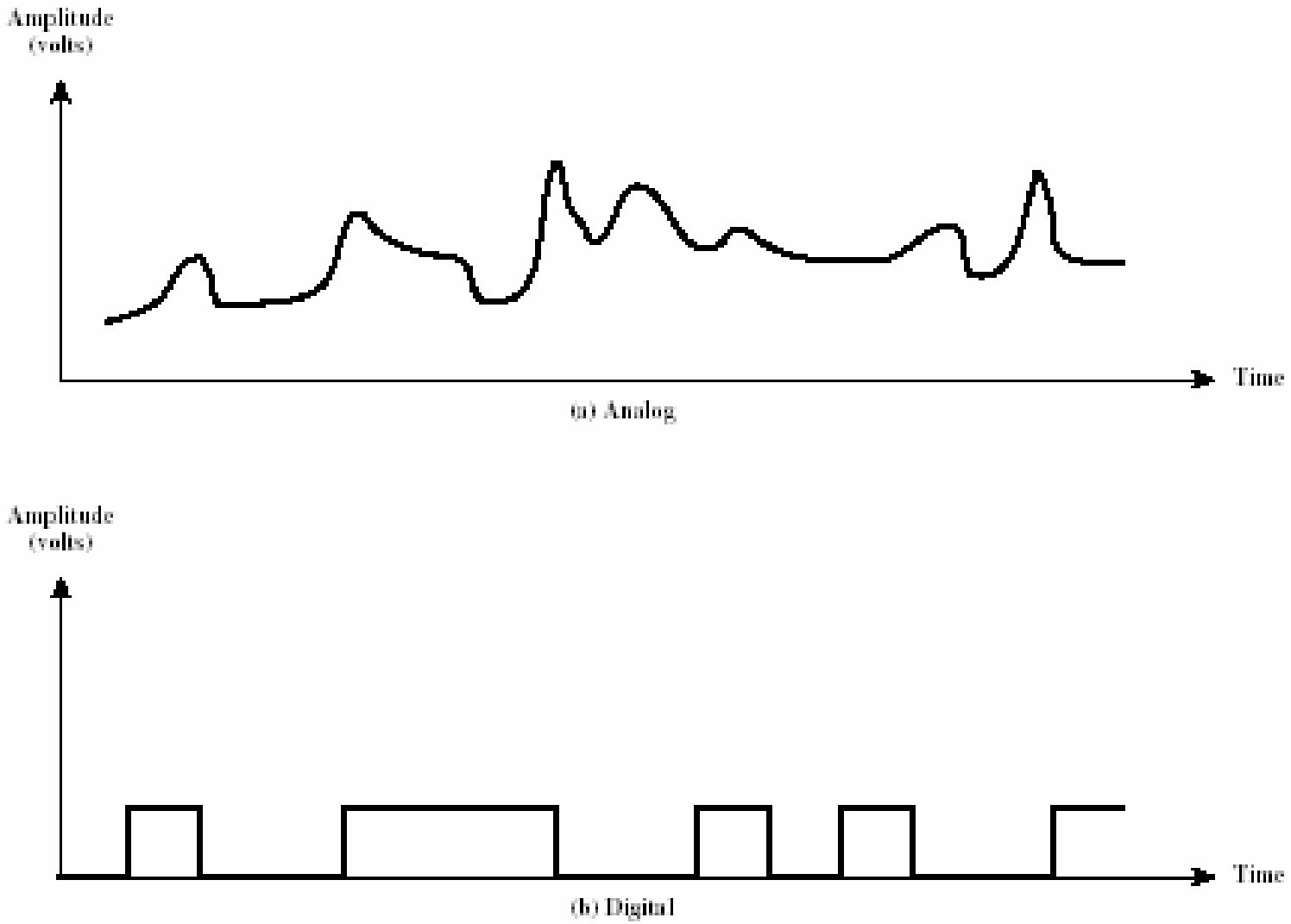


Figure 2.1 Analog and Digital Waveforms

Koncepcja sygnału (cd.)

- amplituda (*A*)
  - maksymalna wartość lub siła sygnału w czasie
  - Zwykle mierzona w voltach
- częstotliwośc (*f*)
  - Liczba powtórzeń (cykli) sygnału w ciągu jednej sekundy; jednostką częstotliwości jest herc (Hz) odpowiadający jednemu powtórzeniu sygnału w ciagu 1 sekundy

Koncepcje sygnału (cd.)

- Okres (T)
  - wielkość czasu jaką zajmuje jedno powtórzenie sygnału
  - $T = 1/f$
- Faza (ϕ) - miara względnej pozycji w czasie wewnątrz pojedyńczego okresu sygnału
- Długość fali (λ) - odległość zajmowana przez pojedyńczy cykl sygnału
  - Np: Prędkość światła v = $3x10^8$ m/s. To długość fali $\lambda f = v$ (lub $\lambda = vT$).

Parametery fali sinusoidalnej

- Ogólna fala sinusoidalna
  - $s(t) = A \sin(2\pi ft + \phi)$
  - uwaga: 2π radianów = 360° = 1 okres
- Rys 2.3 pokazuje efekt zmian każdego z trzech parametrów
  - (a) $A = 1$, $f = 1$ Hz, $\phi = 0$; tak więc $T = 1$s
  - (b) zredukowana amplituda; A=0.5
  - (c) zwiększona częstotliwośc; $f = 2$, tak więc $T = ½$
  - (d) przesunięcie fazowe; $\phi = \pi/4$ radiany (45 stopni)

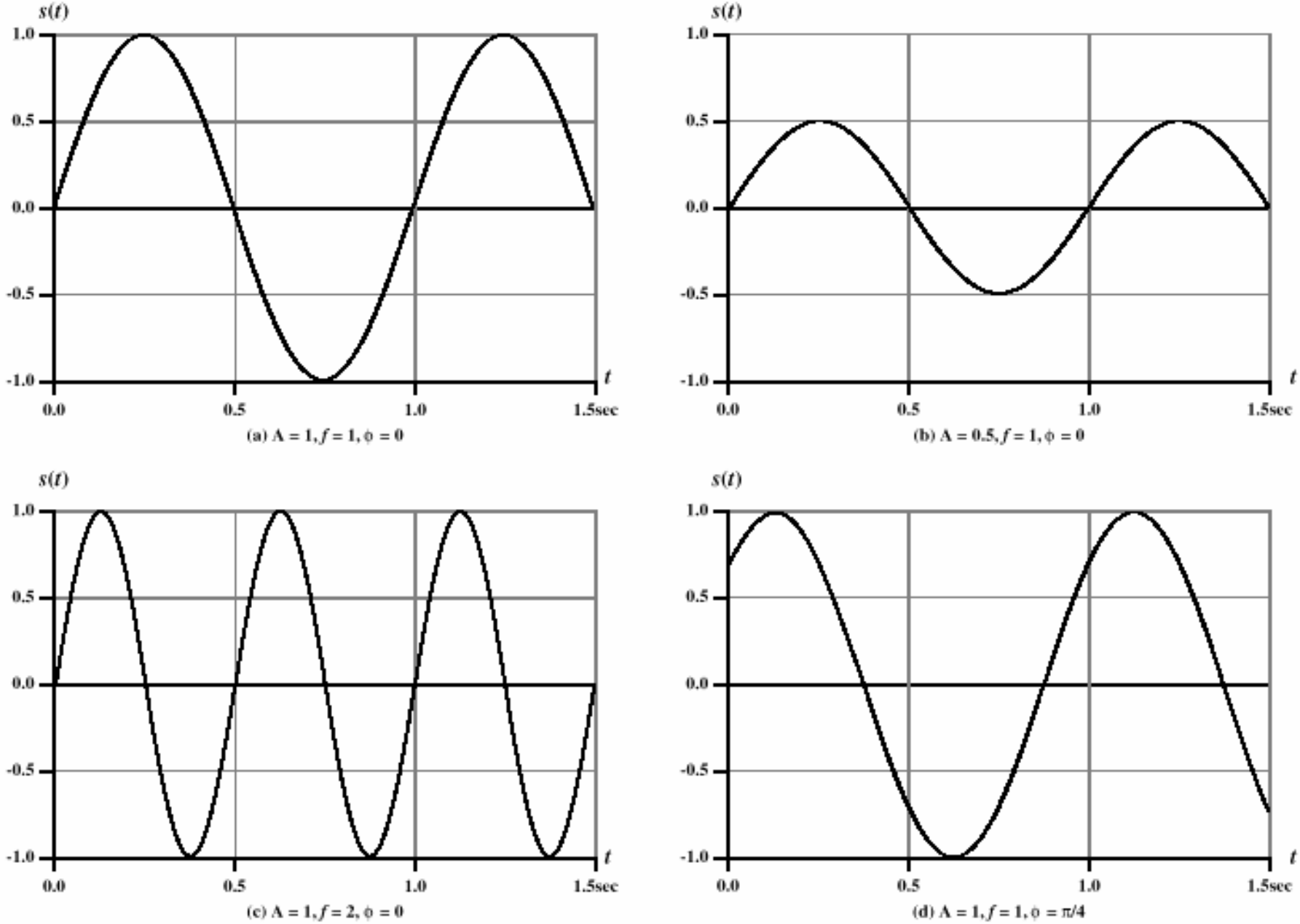


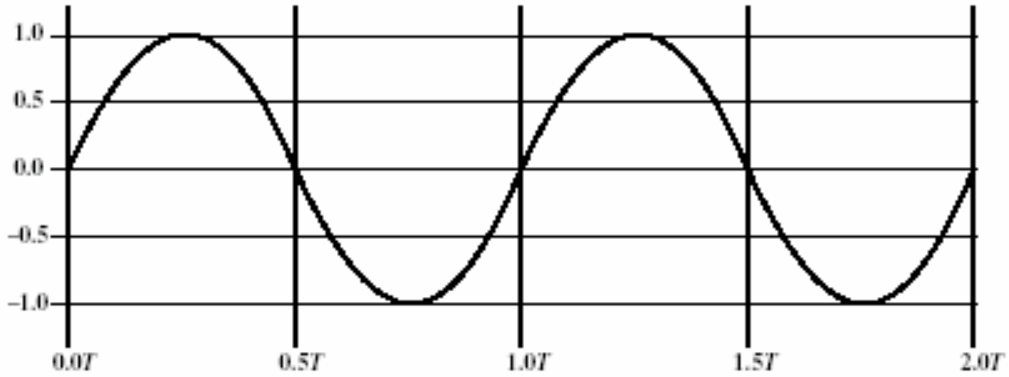
Figure 2.3 $s(t) = A \sin(2\pi ft + \phi)$

Koncepcje związane z częstotliwością

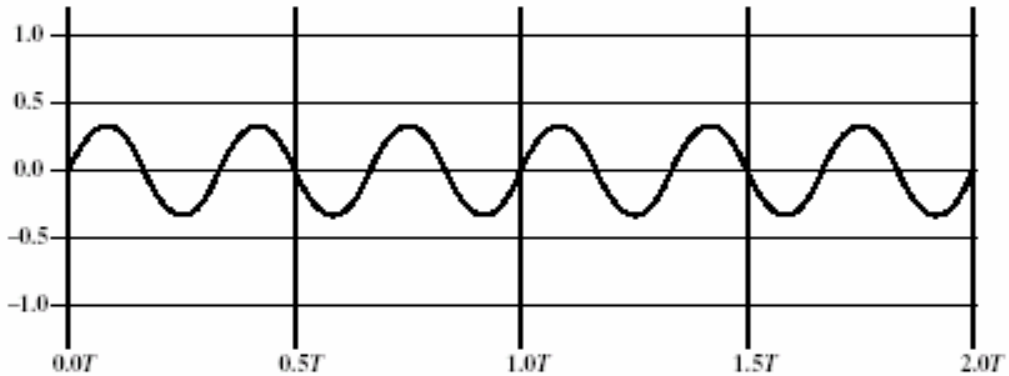
- Sygnał elektromagnetyczny może składać się z wielu częstotliwości.
  - przykład:

    $$s(t) = (4/\pi)(\sin(2\pi ft) + (1/3)\sin(2\pi(3f)t))$$

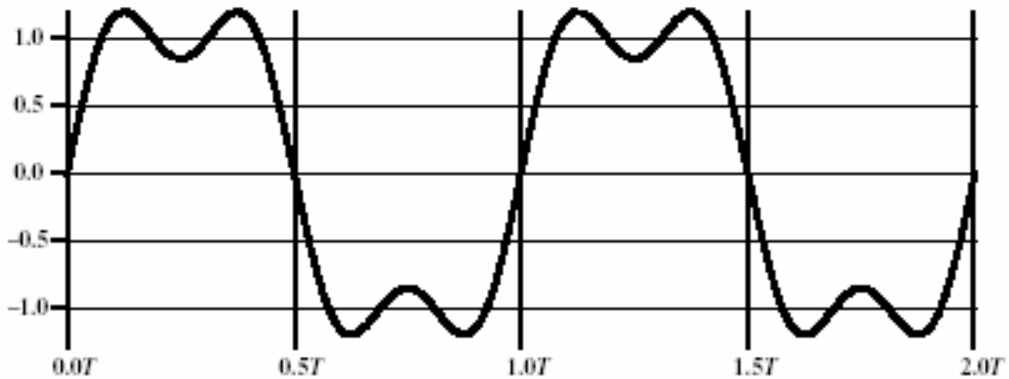
    - Rys. 2.4(a) + Fig. 2.4(b) = Fig. 2.4(c)
    - Widoczne są dwie składowe częstotliwości: f i 3f.
  - Na podstawie analizy Fouriera, każdy sygnał utworzony jest ze składowych o różnych częstotliwościach,
    - wszystkie składowe są falami sinusoidalnymi o różnych amplitudach, częstotliwościach i fazach.



(a) sin (2 *ft*)



(b) (1/3) sin (2 (3*ft*)

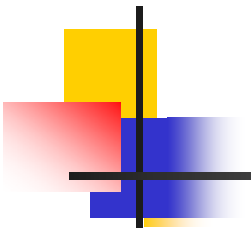


(c) (4/) [sin (2 *ft*) + (1/3) sin (2 (3*ft*)]

Figure 2.4 Addition of Frequency Components (*T* = 1/*f*)

Koncepcje związane z częstotliwością (cd.)

- Spektrum – zakres częstotliwości które zawiera sygnał
  - na Rys. 2.4(c), spektrum rozciaga się z f do 3f.
- Absolutne pasmo - szerokość spektrum sygnału
  - na Rys. 2.4(c), wynosi ono 3f – f = 2f.
- Efektywne pasmo lub pasmo –
  - sygnał może zawierać wiele częstotliwości.
  - Ale większośc energii może być skoncentrowana na wąskiej grupie częstotliowości.
  - Te częstotliwości są efektywnym pasmem.



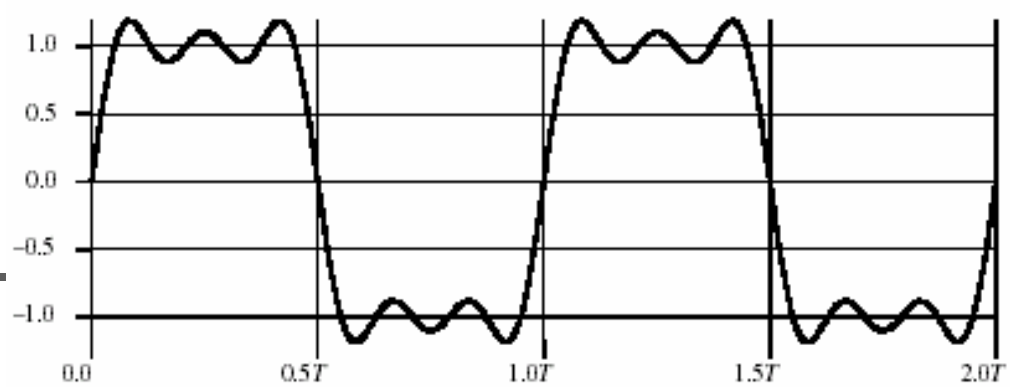
- częstotliwośc podstawowa –
  - gdy wszystkie składowe częstotliwości sygnału są całkowitoliczbowymi wielokrotnościami jednej częstotliwosci, to nazywana jest ona częstotliwością podstawową
  - (przykład wczesniejszy) f oraz 3f ➔ częst. Podst. = f
- okres całego sygnału jest równy okresowi częstotliwości podstawowej.
  - Patrz, Rys. 2.4 znowu!

Dane a sygnały

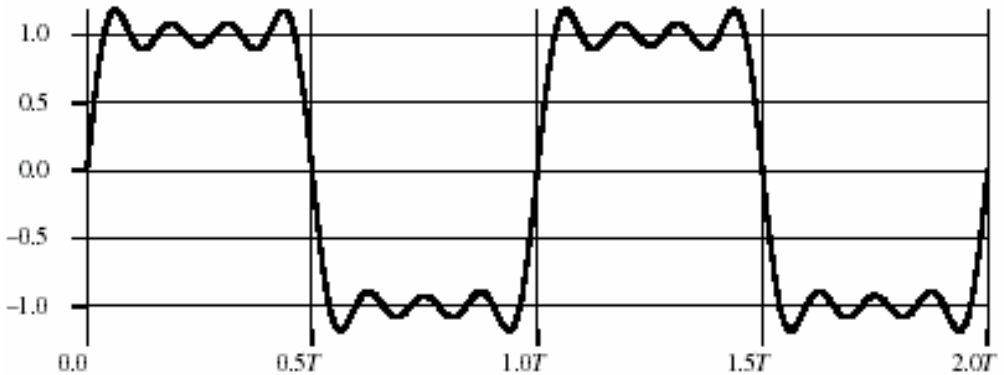
- Sygnały - elektryczna lub elektromagnetyczna reprezentacja danych
- Dane – byty, które przenoszą znaczenia lub informację
- Transmisja – przenoszenie danych przez propagację i przetwarzanie sygnałów

Aproksymacja funkcji kwadratowej przez sygnały

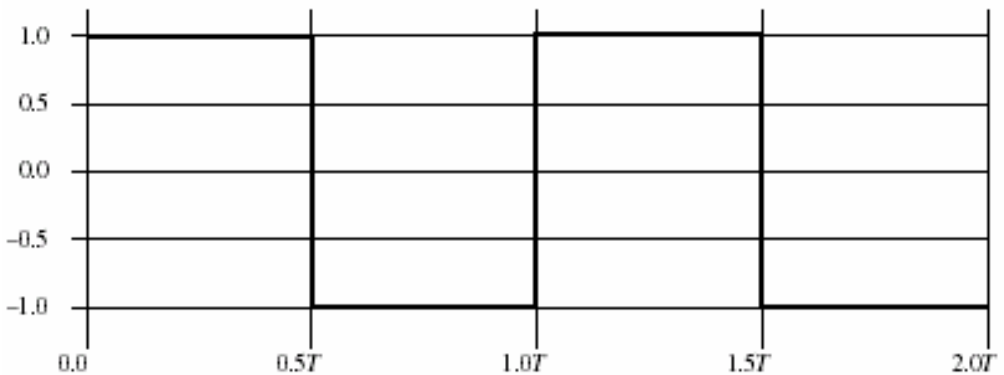
- dodanie częstotliwości 5f do Rys. 2.4(c) ➔ Rys. 2.5(a)
- dodanie częstotliwości 7f do Rys. 2.4(c) ➔ Rys. 2.5(b)
- dodanie wszystkich częstotliwości 9f, 11f, 13f, ... ➔ Rys. 2.5(c), funkcja kwadratowa
  - Ta funkcja kwadratowa posiada nieskończoną liczbę składowych częstotliwości i w ten sposób nieskończone pasmo.



(a) (4/) [sin (2 ft) + (1/3) sin (2 (3ft) + (1/5) sin (2 (5ft)]



(b) (4/) [sin (2 ft) + (1/3) sin (2 (3ft) + (1/5) sin (2 (5ft) + (1/7) sin (2 (7ft)]

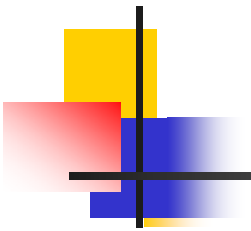


(c) (4/) $\sum$ (1/k) sin (2 (kft), for k odd

Figure 2.5 Frequency Components of Square Wave ($T = 1/f$)

Prędkość danych a pasmo

- przypadek I: (Rys. 2.5(a))
  - niech f = 10^6 cykli/sec = 1 MHz
  - Składowe częstotliwości: 1f, 3f, 5f
  - Absolutne pasmo = 5f – 1f = 4f = 4 MHz
  - Prędkość danych = 2 Mbps (1 bit na 0.5 us)
- przypadek II: (Rys. 2.5(a))
  - niech f = $2x10^6$ cykli/sec = 2 MHz
  - Składowe częstotliwości: 1f, 3f, 5f
  - Absolutne pasmo = 10M – 2M = 8 MHz
  - Prędkość danych = 4 Mbps (1 bit na 1/4 us)



- przypadek III: (Rys. 2.4(c))
  - niech f = $2x10^6$ cykli/sec = 2 MHz
  - częstotliwości: 1f, 3f
  - Absolutne pasmo = 6M – 2M = 4 MHz
  - Prędkość danych = 4 Mbps (1 bit na 1/4 us)

- ** porównaj absolutne pasmo i prędkość danych w tych przykładach!

Kilka pojęć dotyczących pojemności kanału

- prędkość danych - prędkość z jaką dane mogą być przesyłane (bps)
- pasmo - pasmo transmitowanego sygnału ograniczone nadajnikiem oraz naturą of medium transmisyjnego (herc)
- szum
- Pojemność kanału – maksymalna prędkość z jaką dane mogą być transmitowane poprzez daną drogę komunikacyjną, lub kanał, przy zadanych warunkach
- Stopa błędów – prędkość z jaką pojawiają się błędy

Pasmo Nyquist'a

- dla zadanej wielkości pasma B, najwyższa prędkość transmisji danych jest równa 2B:
  - $C = 2B$
  - *np: B=3100 Hz; C=6200 bps*
- Przy wielopoziomowym sygnale
  - $C = 2B \log_2 M$, gdzie M jest liczbą dyskretnych poziomów sygnału lub napięcia

Stosunek sygnał-szum

- Jest to stosunek mocy sygnału (signal power) do mocy zawartej w szumie (noise power), który jest obecny w jakimś konkretnym punkcie transmisji
- Zwykle jest mierzony w odbiorniku
- Stosunek sygnał-szum (signal-to-noise ratio (SNR, or S/N))

$$(SNR)_{\text{dB}} = 10 \log_{10} \frac{\text{signal power}}{\text{noise power}}$$

  - = 10 $\log_{10}$ SNR
  - $(\text{SNR})_{10}$ określa się w decybelach (db)
  - Wysoka wartość SNR oznacza sygnał wysokiej jakości.
  - SNR ustanawia górną granicę osiągalnej prędkości danych.

Teoretyczna pojemność kanału wg. formuły Shannona

- Maksymalna pojemność kanału (bit./s):

$$C = B\log_2(1+\mathrm{SNR})$$

  - uwaga: SNR nie w db.
- W praktyce, tylko znacznie mniejsze prędkości są osiągane
  - Formula zakłada istnienie białego szumu (szum termiczny)
  - Szum impulsowy nie jest brany pod uwagę

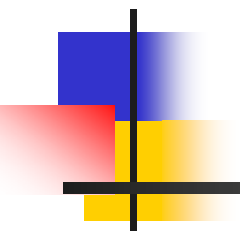
Klasyfikacja mediów Transmisyjnych

- Medium transmisyjne
  - Fizyczna droga między nadajnikiem a odbiornikiem
- Media przewodzące
  - Fale są przewodzone wzdłuż medium trwałego
  - np., miedziana skrętka pary przewodów, miedziany kabel współosiowy, światłowód
- Media nieprzewodzące
  - zapewniają środki transmisji ale nie przewodzą sygnałów elektromagnetycznych
  - Zwykle określa się je jako media transmisji bezprzewodowej
  - np., atmosfera, przestrzeń kosmiczna

Ogólne zakresy częstotliwości

- Zakres częstotliwosci mikrofalowych
  - 1 GHz do 40 GHz
  - Kierunkowe anteny możliwe
  - Służą do transmisji na dużą odległość, połączenia typu punkt-punkt
  - Używane w komunikacji satelitarnej
- Zakres częstotliwości radiowych
  - 30 MHz do 1 GHz
  - Służą w zastosowaniach wymagających anten dookólnych (omnidirectional)
- Zakres częstotliwości podczerwonych
  - około, $3x10^{11}$ do $2x10^{14}$ Hz
  - Użyteczne w zastosowaniach wymagających połączeń typu wielodostępowy punkt-punkt wewnątrz zamkniętych obszarów

Propagacja fal w środowisku mobilnym



Spektrum fal radiowych

Podział spektrum fal radiowych

Napisał SP8QED

Sunday, 06 March 2005

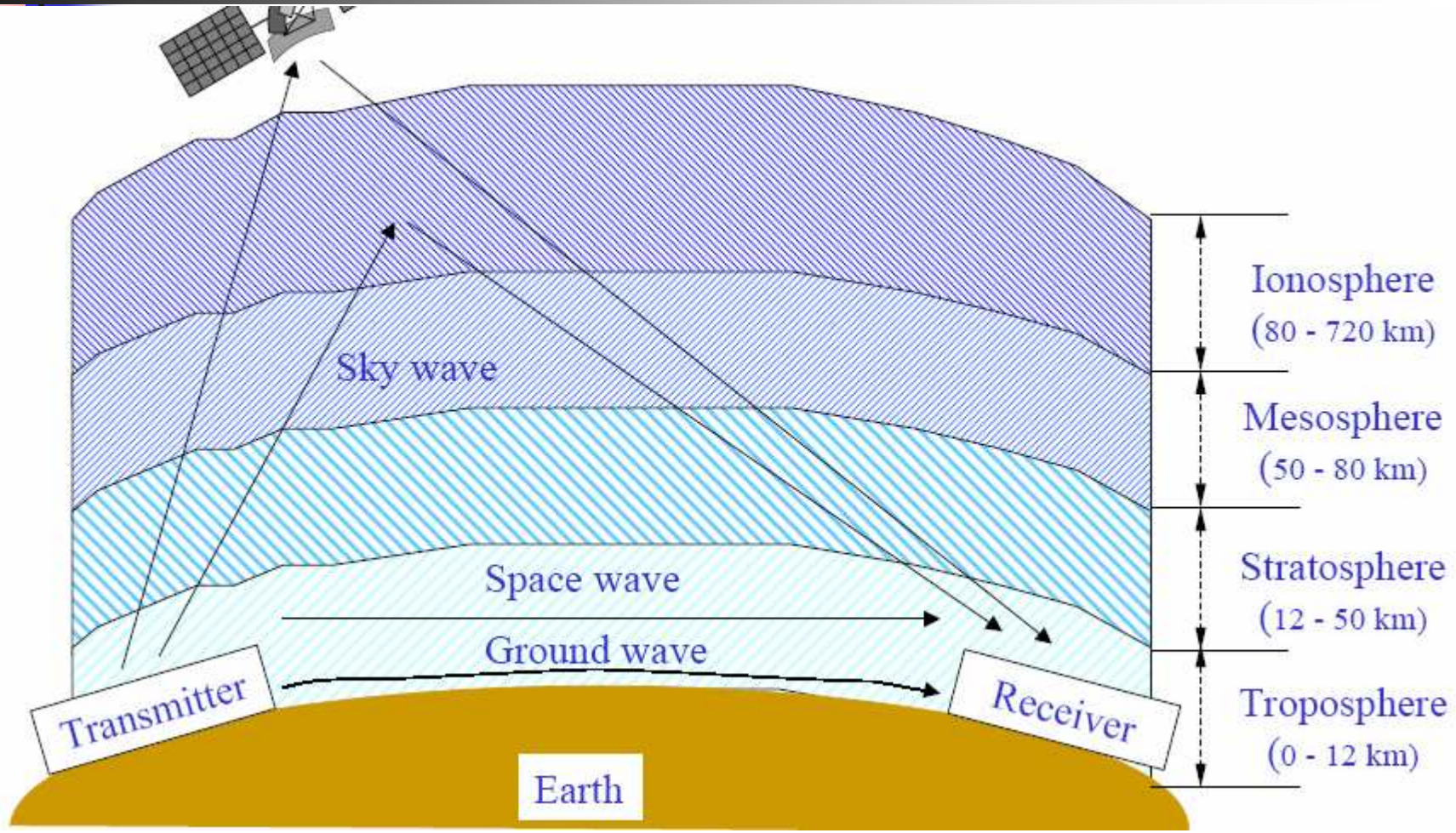
od	do	długość fal	nazwa i oznaczenie międzynarodowe	inne oznaczenia	nazwa i oznaczenie polskie
3Hz	30Hz	100 tys. km-10 tys. km	ULF ultra low frequency		
30Hz	300Hz	10 tys. km-1 tys. km	ELF extremly low frequency		
300Hz	3000Hz	1000km-100km	VF voice frequency		
3kHz	30kHz	100km-10km	VLF very low frequency		fale b. długie, fale myriametrowe
30kHz	300kHz	10km-1km	LF low frequency	LW - long wave	fale długie, fale kilometrowe
300kHz	3MHz	1000m-100m	MF medium frequency	MW - medium wave	fale średnie, fale hektometrowe
3MHz	30MHz	100m-10m	HF high frequency	KW - ?	fale krótkie, fale dekametrowe, KF
30MHz	300MHz	10m-1m	VHF very high frequency		UKF fale ultrakrótkie, fale metrowe
300MHz	3GHz	100cm-10cm	UHF ultra high frequency		fale decymetrowe
3GHz	30GHz	10cm-1cm	SHF super high frequency		fale centymetrowe
30GHz	300GHz	10mm-1mm	EHF extremly high frequency		fale milimetrowe

Prędkość, długość, częstotliwość fali

- Prędkość światła=długość fali x częstotliwość =
  =3 x 10^8m/s =300 000 km/s

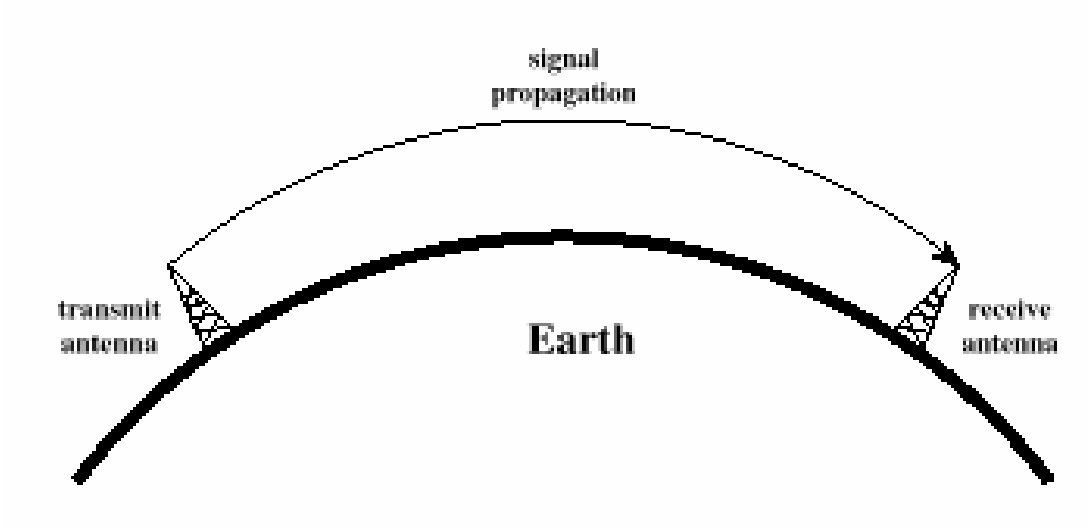
System	Frequency	Wavelength
AC current	60 Hz	5,000 km
FM radio	100 MHz	3 m
Cellular	800 MHz	37.5 cm
Ka band satellite	20 GHz	15 mm
Ultraviolet light	10^{15} Hz	10^{-7} m

Typy fal


Sky wave
Space wave
Ground wave
Transmitter
Receiver
Earth
Ionosphere
(80 - 720 km)
Mesosphere
(50 - 80 km)
Stratosphere
(12 - 50 km)
Troposphere
(0 - 12 km)

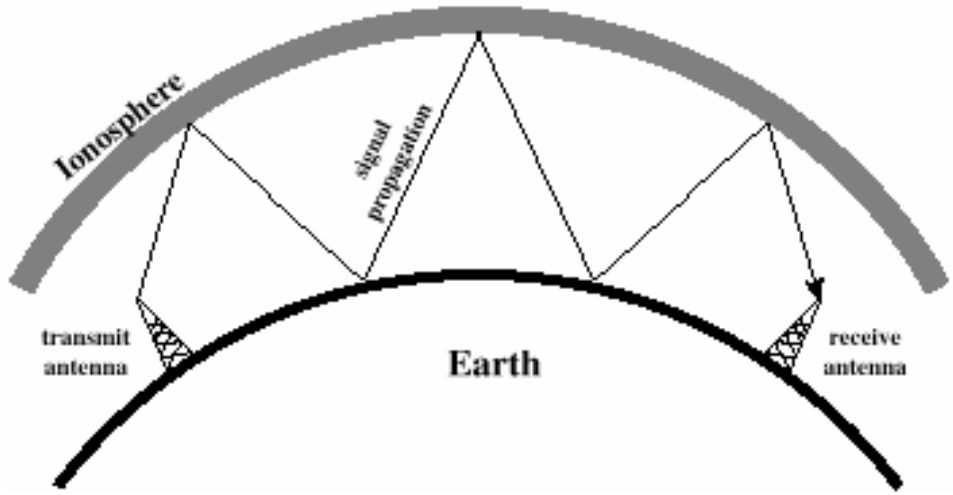
Propagacja fali przyziemnej (Ground Wave)

- Rozprzestrzenia wzdłuż konturów powierzchni Ziemi
- Może być propagowana na znaczne odległości
- częstotliwości aż do 2 MHz
- Np.
  - AM radio



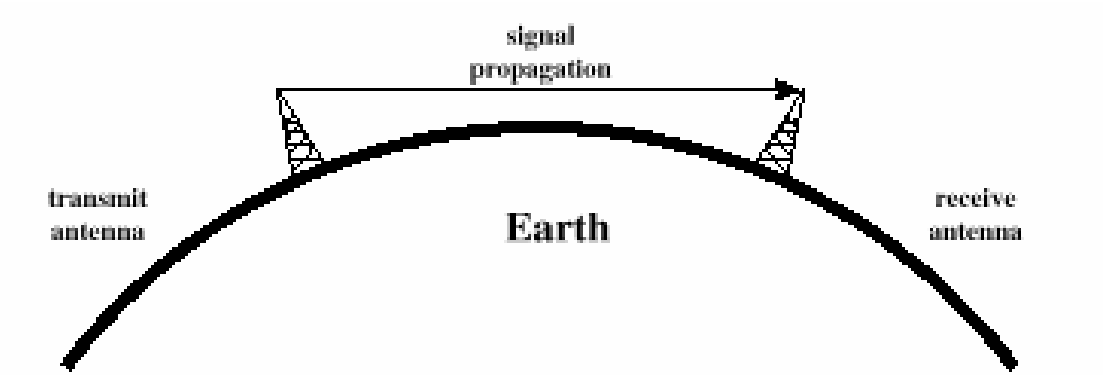
Propagacja fali jonosferycznej (sky wave)

- Sygnał odbijany od zjonizowanego poziomu atmosfery do powierzchni Ziemi
- Sygnał może wykonać pewną liczbę skoków, tam i z powrotem między jonosferą i powierzchnią Ziemi
- Efekt odbicia jest spowodowany załamaniem fali
- Np.
  - Radio amatorskie
  - CB radio



Propagacja w linii widoczności (Line-of-Sight, LOS)

- Antena nadająca i antena odbiorcza muszą być w linii pola widzenia (dla fal powyżej 30 MHz)
- Załamanie
  - Fale mikrofalowe uginają się lub załamuja w atmosferze
  - Prędkość fali elektromagnetycznej jest funkcją gęstości medium
  - Gdy fala zmienia medium, zmienia się jej prędkość
  - Fale uginają sie lub załamują się na granicy między jednym i drugim medium



Zakresy fal radiowych

Classification Band	Initials	Frequency Range	Characteristics
Extremely low	ELF	< 300 Hz	
Infra low	ILF	300 Hz ~ 3 kHz	
Very low	VLF	3 kHz ~ 30 kHz	
Low	LF	30 kHz ~ 300 kHz	Surface/ground wave
Medium	MF	300 kHz ~ 3 MHz	
High	HF	3 MHz ~ 30 MHz	Sky wave
Very high	VHF	30 MHz ~ 300 MHz	Space wave
Ultra high	UHF	300 MHz ~ 3 GHz	
Super high	SHF	3 GHz ~ 30 GHz	
Extremely high	EHF	30 GHz ~ 300 GHz	Satellite wave
Tremendously high	THF	300 GHz ~ 3000 GHz	

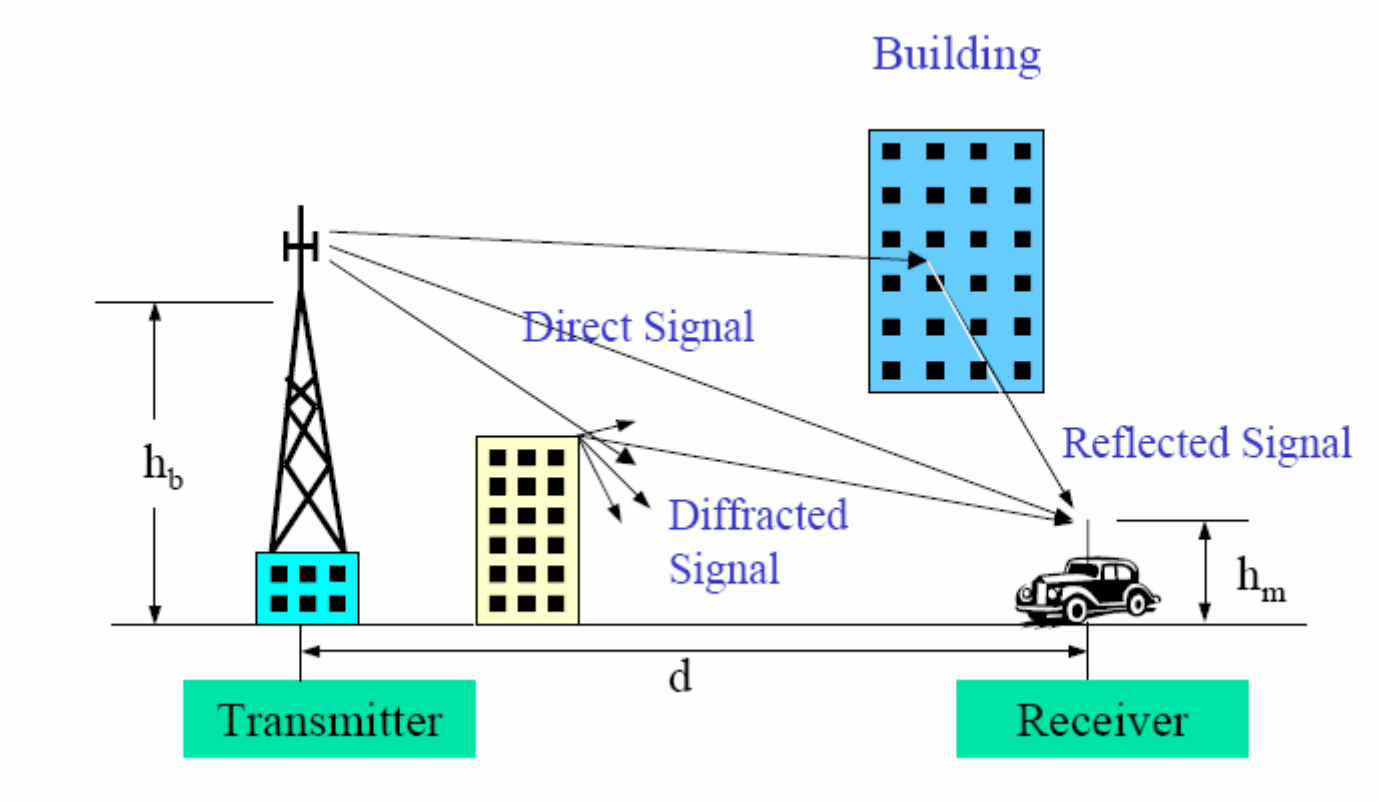
Mechanizmy propagacji

- odbicie
  - Na propagację fali wpływają obiekty, które są duże w porównaniu z długością fali

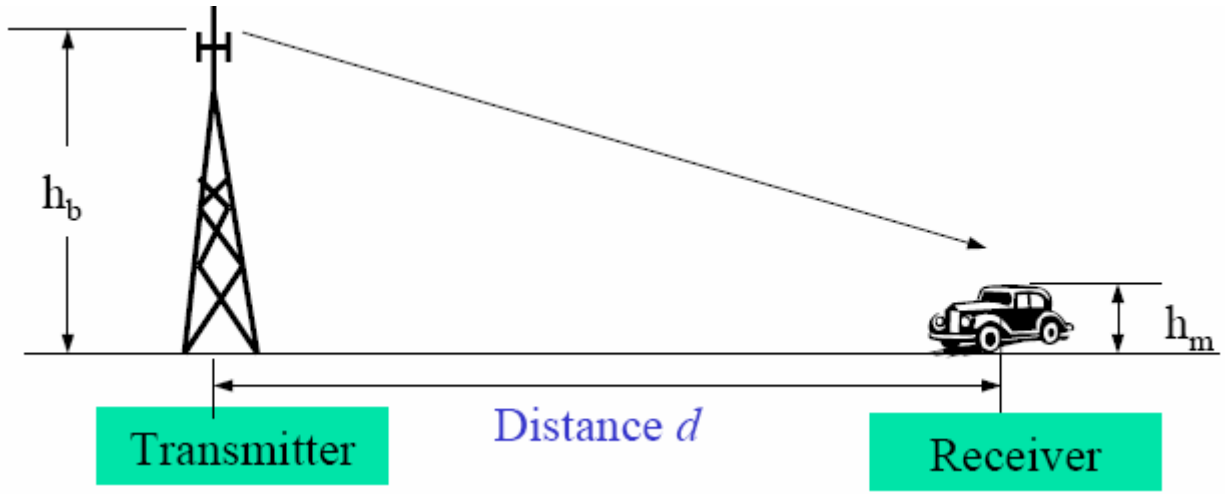
    - np. powierzchnia Ziemi, budynki, ściany, itp.
- Załamanie
  - Na droge radiową między nadajnikiem i odbiornikiem mają wpływ kształty z ostrymi nieregularnymi krawędziami
  - Fale uginają się w pobliżu przeszkód gdy tylko obok nich przechodzą
- Rozproszenie
  - Obiekty mniejsze niż długość fali

    - np. liście, znaki drogowe, lampy

Efekty propagacji radiowej



Propagacja w próżni



- Moc sygnału otrzymanego w odległości d:

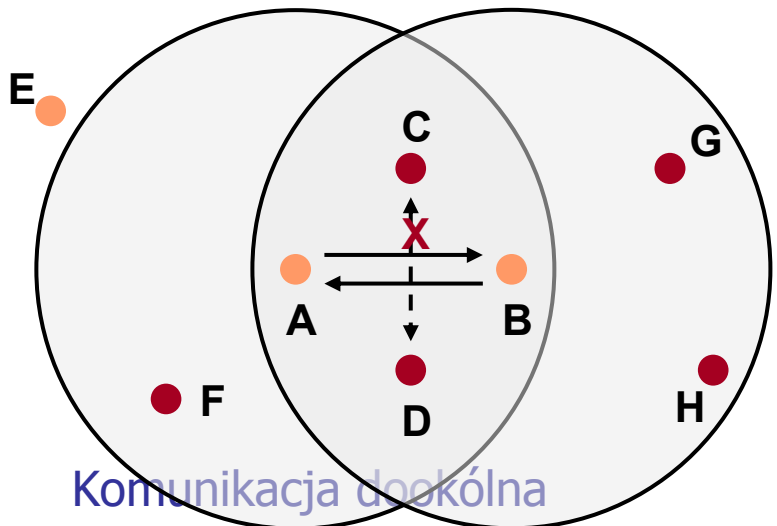
$$P_r = \frac{A_e G_t P_t}{4\pi d^2}$$

gdzie P_t jest transmitowaną mocą, A_e jest efektywnym obszarem, a G_t jest zyskiem anteny

Anteny

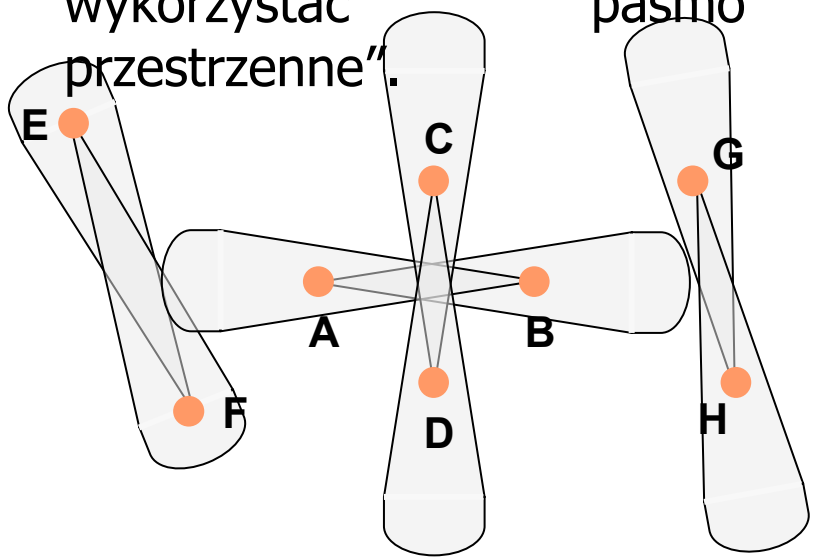
Dookólna (Omnidirectional) Antena – niska wydajność w bezprzewodowych sieciach ad hoc z powodu ograniczonych możliwości wykorzystania przestrzeni.

- **Węzły w strefie ciszy**



Komunikacja dookólna

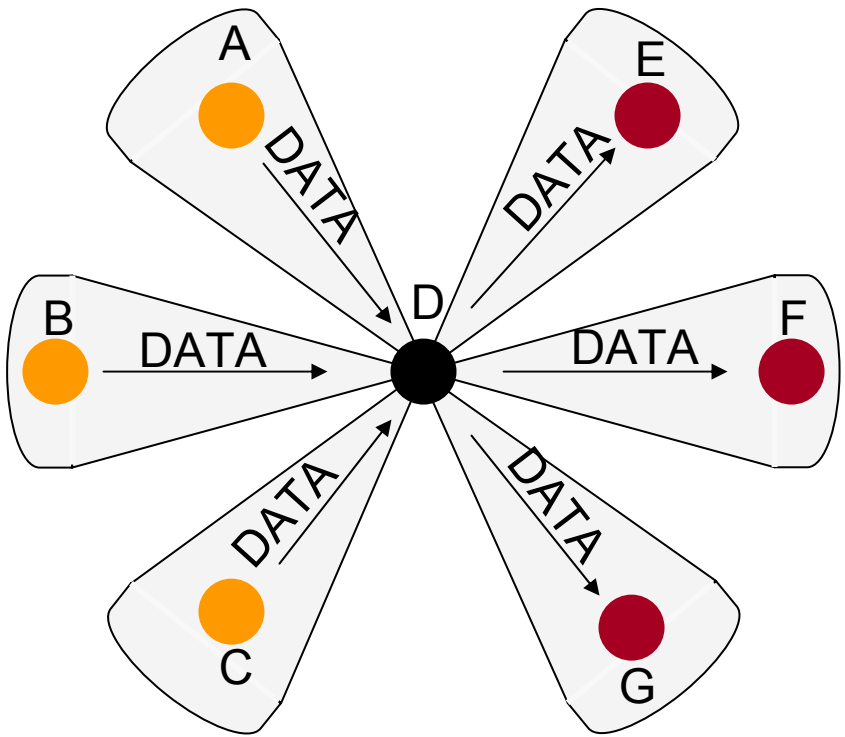
Antena kierunkowa – lepsze możliwości wykorzystania przestrzeni. Ale węzeł w dalszym ciągu nie jest w stanie całkowicie wykorzystać "pasmo przestrzenne".



Komunikacja kierunkowa

Anteny wielokierunkowe

- Określane również jako Multiple Beam Antenna Array (MBAA) – wykorzystuje w pełni pasmo przestrzenne.
- węzeł może inicjować więcej niż jedna jednoczesnych transmisji (lub odbiorów).



Zysk anteny

- Jest miarą kierunkowości anteny; jest określany przez moc wyjściową w specyficznym kierunku porównywaną do mocy produkowanej we wszystkich kierunkach przez doskonałą antenę dookólną
- Dla kołowej reflektorowej anteny zysk G anteny:

$$G = \eta\,(\pi D f / c)^2, \quad c = \lambda f$$

η = współczynnik efektywności (zależy od rozkładu pola elektrycznego, strat, itp., zwykle 0.55)

D=średnica

tak więc $G = \eta(\pi D / \lambda)^2$ (c-prędkość światła)

Przykład:

- Antena ze średnicą D=2 m, częstotliwośc f= 6 GHz, długość fali =0.05m, G=39.4 db
- Częstotliwość=14GHz, D=2, długość fali=0.021m, G=46.9 db

- Im wyższa częstotliwość tym wyższy zysk dla anteny tego samego rozmiaru

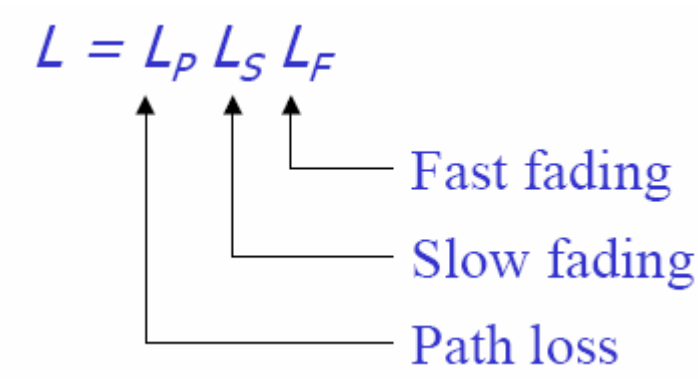
Propagacja naziemna

- Moc otrzymanego sygnału:

$$P_r = \frac{G_t G_r P_t}{L}$$

gdzie G_r jest zyskiem anteny odbiornika,
L jest stratą propagacji w kanale,
tzn.

$$L = L_P L_S L_F$$



(szybkie tłumienie)
(powolne tłumienie)
(stratą drogi)

Strata mocy (path loss) w próżni

- Jest to wielkość mocy utraconej w przestrzeni
- Definicja utraty mocy L_p:

$$L_P = \frac{P_t}{P_r},$$

Strata mocy w prożni:

$$L_{PF}(dB) = 32.45 + 20\log_{10} f_c(MHz) + 20\log_{10} d(km),$$

gdzie f_c jest częstotliwością nośną.

Widać, że im większa f_c tym więsza jest strata mocy

Strata odległościowa (path loss) w próżni

- Prosta formuła:

$$L_p = \mathrm{A}\, d^{-\alpha}$$

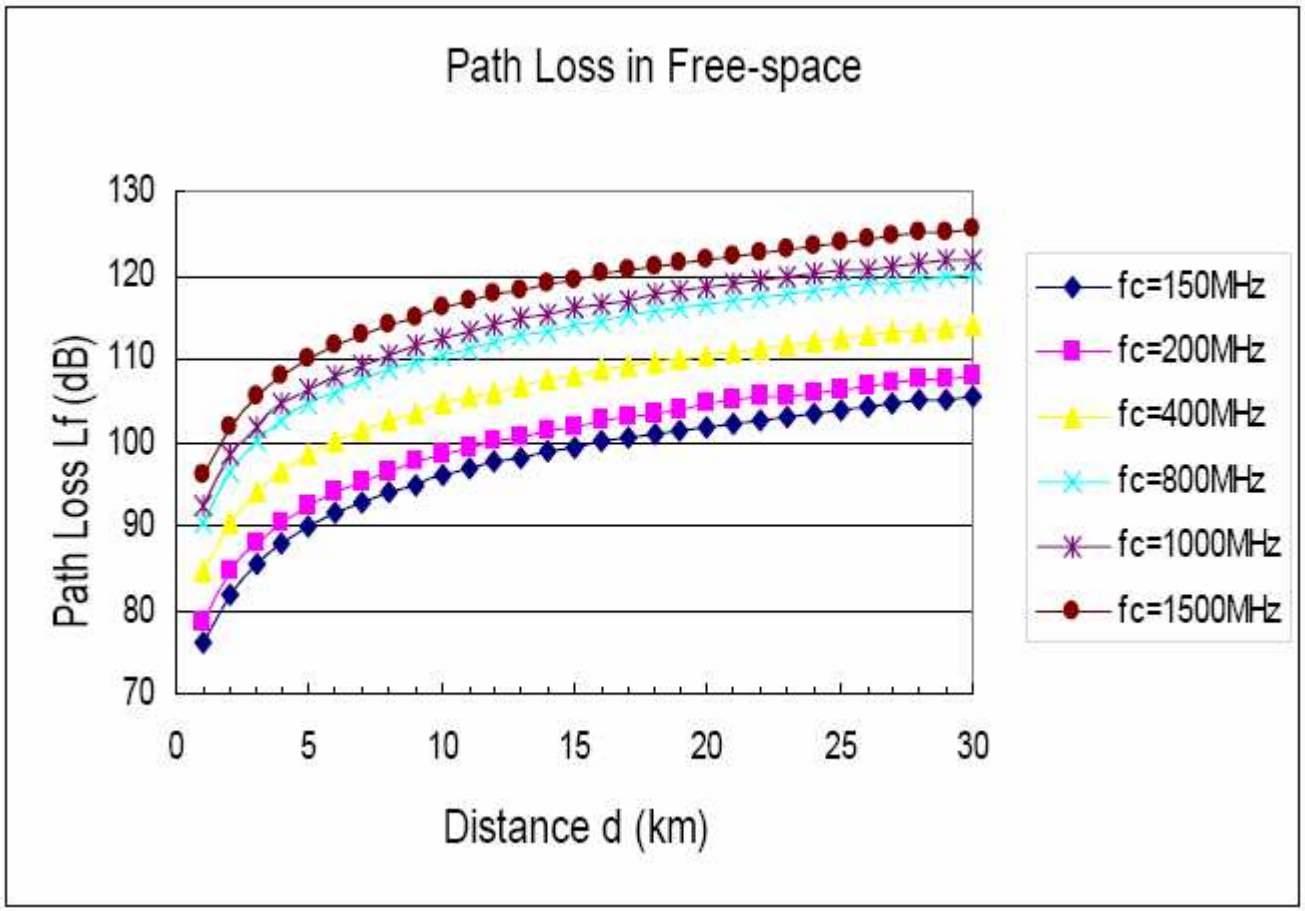
gdzie

A i α : stałe propagacji

d: odległość między nadajnikiem i odbiornikiem

α : ma wartośc 3 ~ 4 w typowym miejskim obszarze

Przykład strat odległościowych (w próżni)



Strata odległościowa (obszar miejski (urban), podmiejski (suburban), otwarty (open))

- Urban area:

$$L_{PU}(dB) = 69.55 + 26.16\log_{10} f_c(MHz) - 13.82\log_{10} h_b(m) - \alpha\left[h_m(m)\right] + \left[44.9 - 6.55\log_{10} h_b(m)\right]\log_{10} d(km)$$

where

$$\alpha\left[h_m(m)\right] = \begin{cases} \left[1.1\log_{10} f_c(MHz) - 0.7\right]h_m(m) - \left[1.56\log_{10} f_c(MHz) - 0.8\right], & for\ large\ city \\ \left.\begin{array}{ll} 8.29\left[\log_{10} 1.54h_m(m)\right]^2 - 1.1, & for \quad f_c \le 200MHz \\ 3.2\left[\log_{10} 11.75h_m(m)\right]^2 - 4.97, & for \quad f_c \ge 400MHz \end{array}\right\}, & for\ small\ \&\ medium\ city \end{cases}$$

- Suburban area:

$$L_{PS}(dB) = L_{PU}(dB) - 2\left[\log_{10}\frac{f_c(MHz)}{28}\right]^2 - 5.4$$

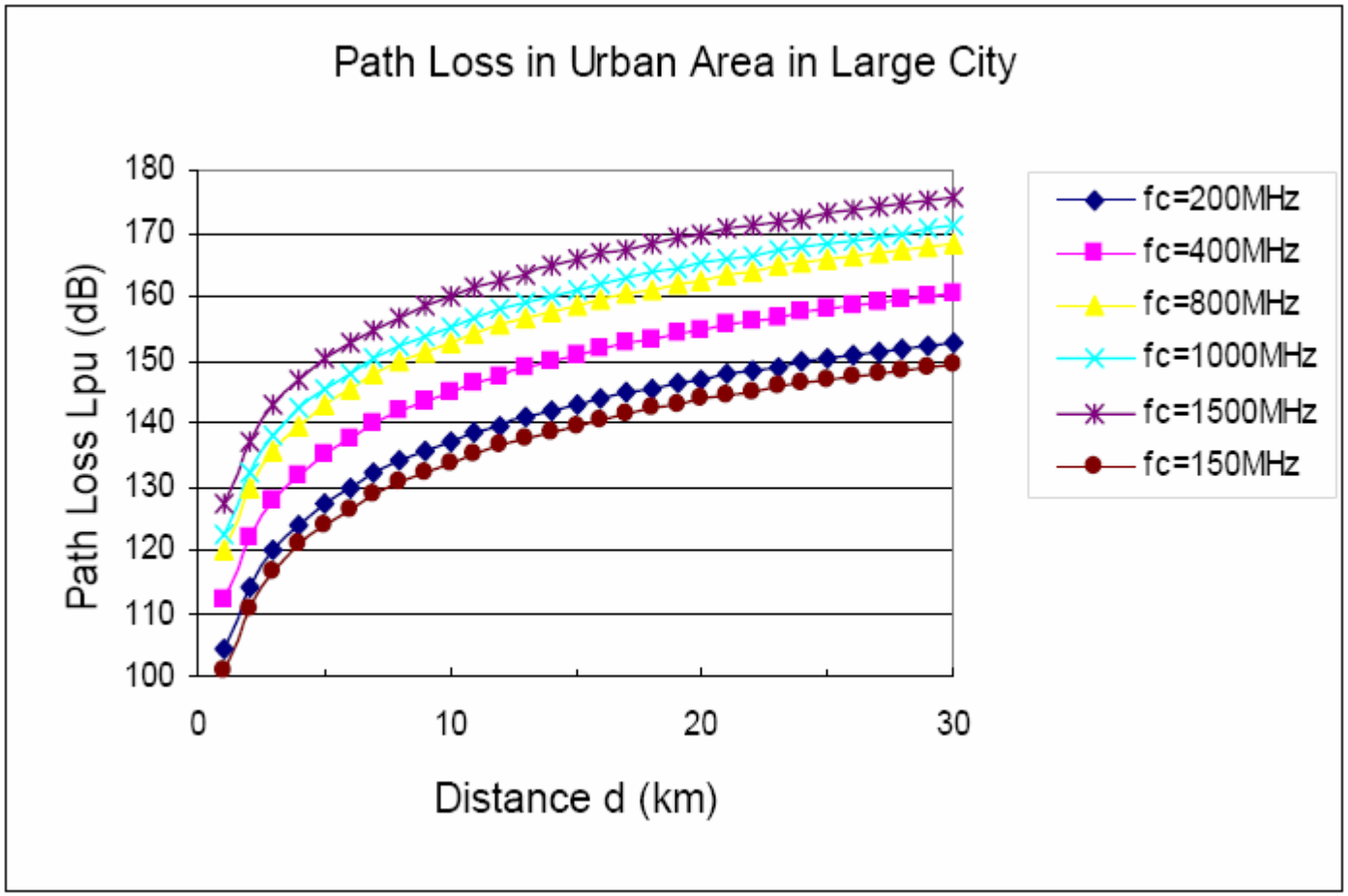
- Open area:

$$L_{PO}(dB) = L_{PU}(dB) - 4.78\left[\log_{10} f_c(MHz)\right]^2 + 18.33\log_{10} f_c(MHz) - 40.94$$

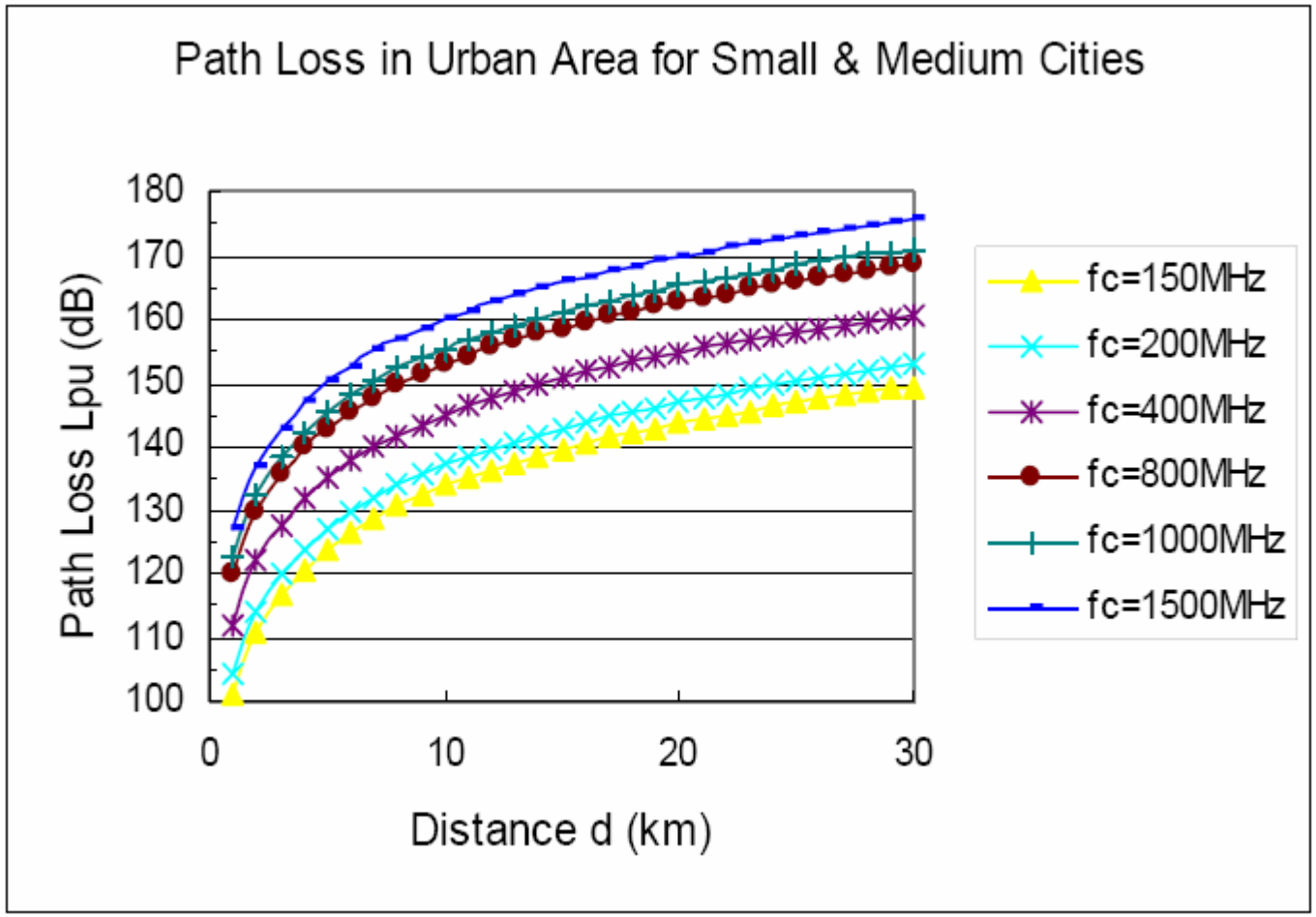
Strata odległościowa

- Straty odległościowe w zmniejszającym się porządku:
  - Obszar miejski (duże miasto)
  - Obszar miejski (średnie i małe miasto)
  - Podmiejski obszar
  - Otwarty obszar

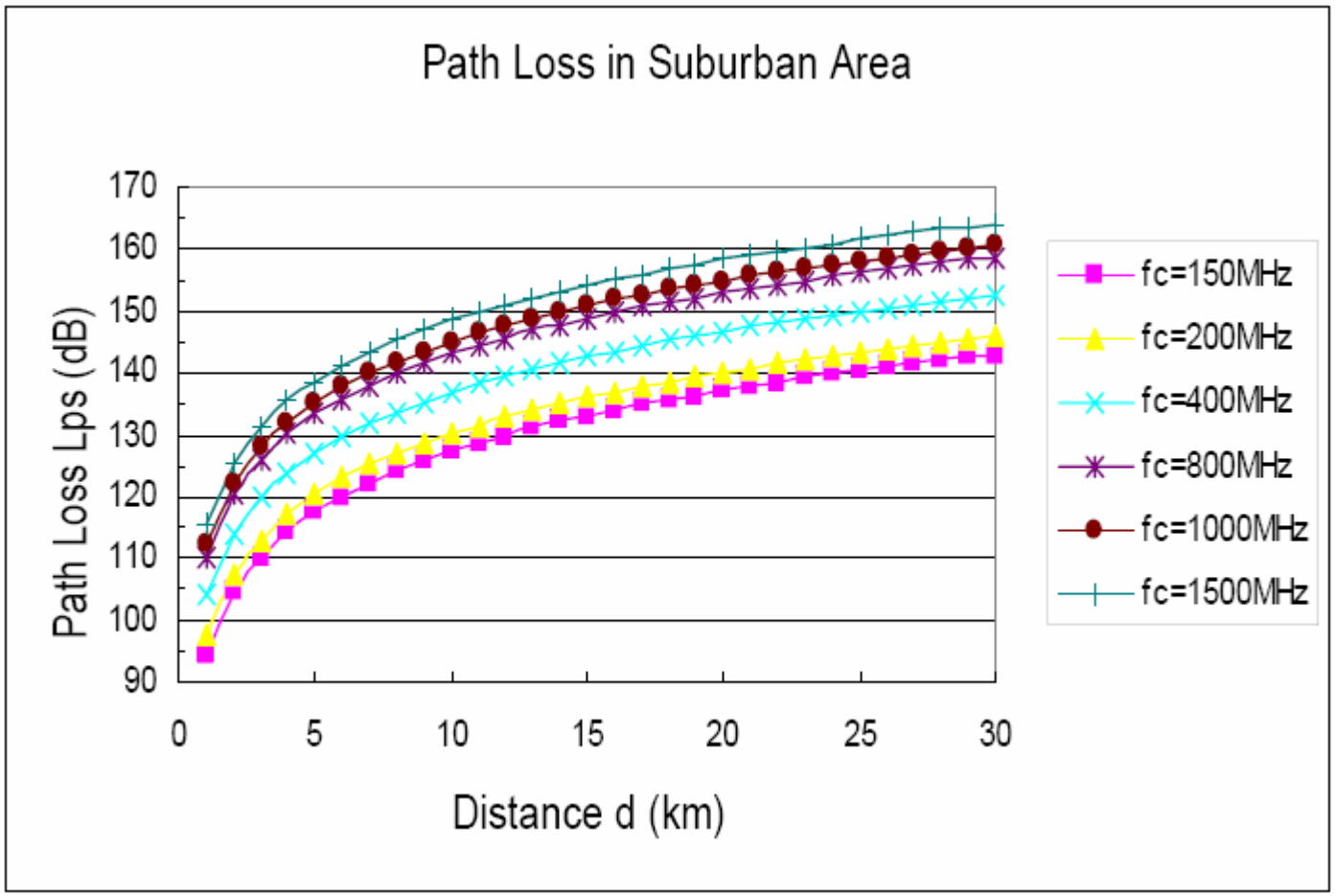
Przykład strat odległościowych (obszar miejski: duże miasto)



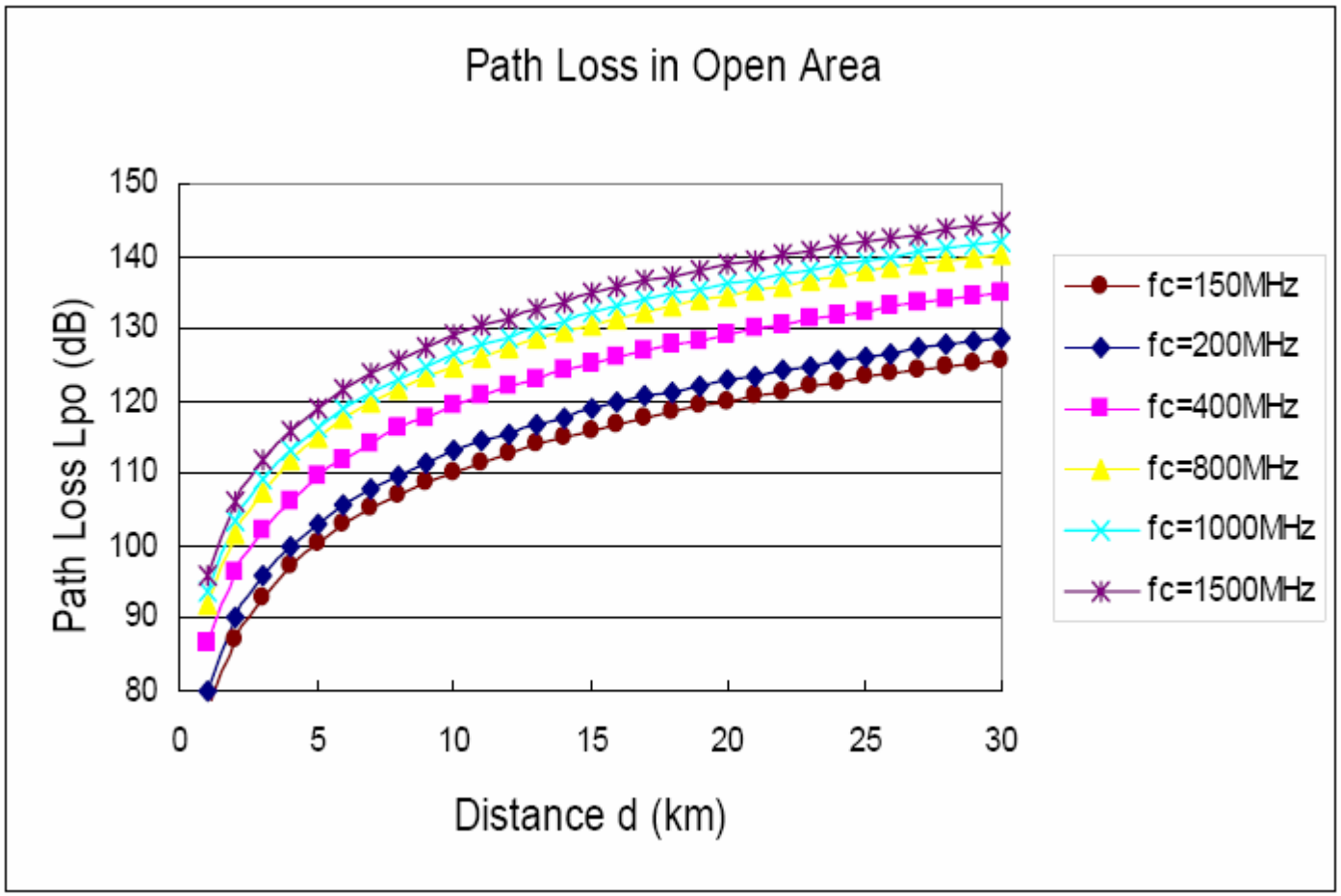
Przykład strat odległościowych (obszar zabudowany: średnie i małe miasta)



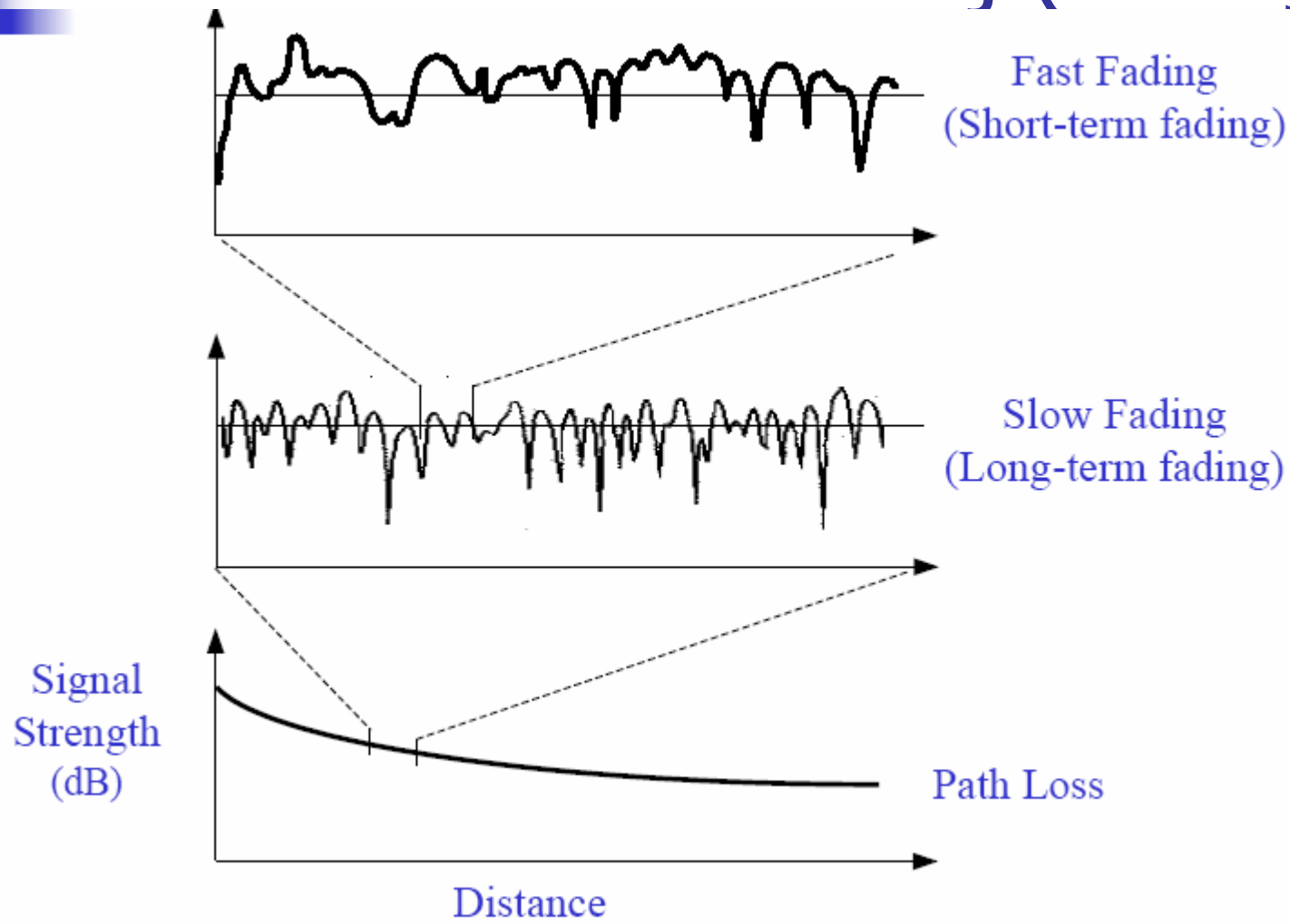
Przykład strat odległościowych (obszar podmiejski)



Przykład strat odległościowych (otwarty obszar)



Tłumienie fali radiowej (fading)



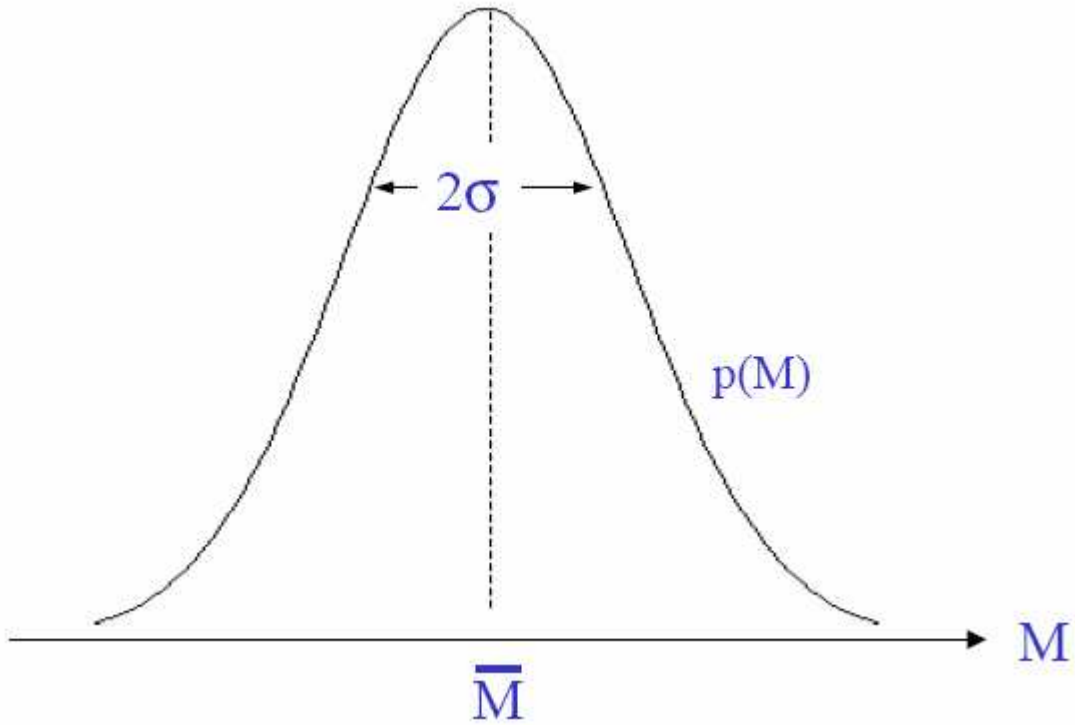
Powolne tłumienie

- Jest spowodowane długoterminowymi przestrzennymi i czasowymi zmianami w odległościach między nadajnikiem i odbiornikiem, które powodują zmiany w średnim poziomie
- Poziom otrzymywanego sygnału okreslany jest rozkładem log-normal z funkcją rozkładu prawdopodobieństwa

$$p(M) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(M-\overline{M})^2}{2\sigma^2}},$$

gdzie M jest faktycznym otrzymanym sygnałem na poziomie m w decybelach (db)(tzn. $M=10\log_{10}m$), $\overline{M}$ -średni dla obszaru poziom sygnału, tzn. średnia z M określona na dostatecznie długiej odległości, σ -standardowe odchylenie w decybelach

Rozkład log-normal



Funkcja rozładu prawdopodobieństwa otrzymywanego poziomu sygnału

Szybkie tłumienie

- Sygnał z nadajnika może być odbity od takich obiektów jak wzgórza, budynki lub pojazdy

  - gdy MS znajduje się daleko od BS to rozkład otrzymanego sygnału podlega rozkładowi Rayleigh

$$p(r) = \frac{r}{\sigma^2} e^{-\frac{r^2}{2\sigma^2}}, \quad r > 0$$

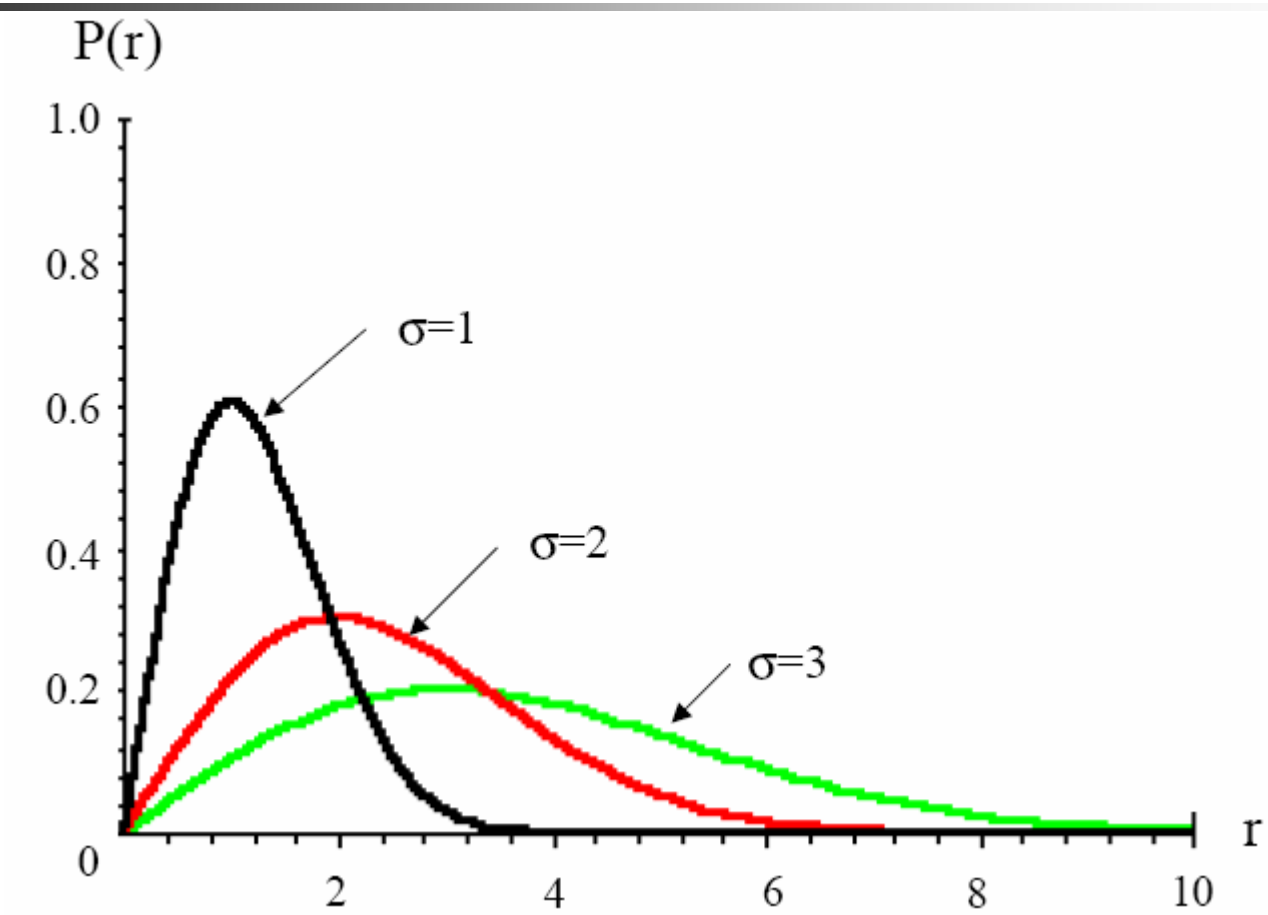
gdzie σ jest standardowym odchyleniem

- Środkowa wartość r_m sygnału wewnątrz przykładowego zakresu powinna spełniać warunek:

$$P(r \le r_m) = 0.5$$

- To odpowiada $r_m = 1.777\sigma$

Rozkład Rayleigh



Funkcja rozładu prawdopodobieństwa otrzymywanego poziomu sygnału

Szybkie tłumienie (cd.)

- Gdy MS jest daleko od BS to krzywa rozkładu otrzymywanego sygnału podlega rozkładowi Rician; jego funkcja rozkładu prawdopodobieństwa:

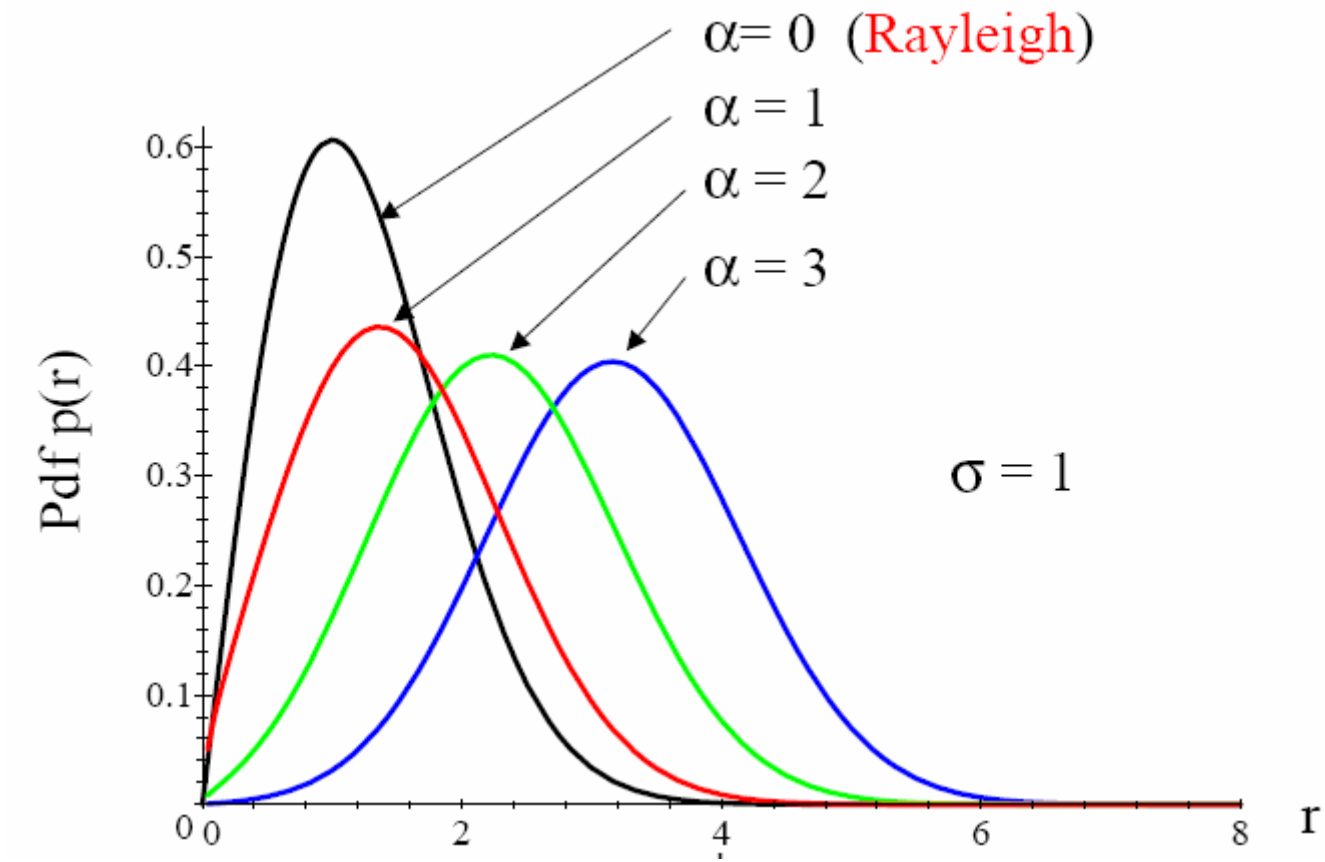
$$p(r) = \frac{r}{\sigma^2} e^{-\frac{r^2+\alpha^2}{2\sigma^2}} I_0\left(\frac{r\alpha}{\sigma}\right), \quad r \geq 0$$

gdzie:

σ - standardowe odchylenie

I_0 - funkcja Bessela zerowego rzędu

Rozkład Rician



Funkcja rozładu prawdopodobieństwa otrzymywanego poziomu sygnału

Przesunięcie Dopplera

- Effekt Dopplera: gdy fala od nieruchomej BS i odbiornik MS poruszają się naprzeciwko siebie, to częstotliwość otrzymywanego sygnału nie będzie taka sama jak u źródła
- Przesunięcie Doplera w częstotliwości
  - Gdy oni poruszają się naprzeciw to częstotliwość otrzymywanego sygnału będzie większa niż u źródla
  - Gdy oni oddalają się to częstotliwość się zmniejsza

gdzie f_c jest częst $f_R = f_C - f_D$ a źródła,

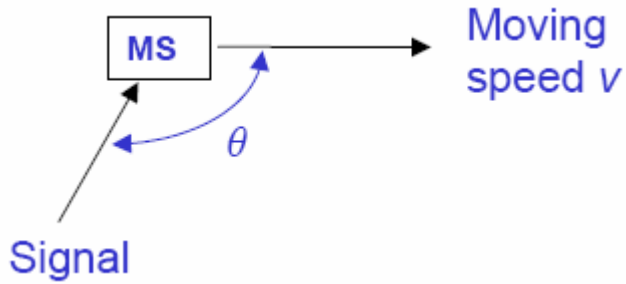
f_d jest częstotliwością Doplera

- Przesunięcie Doplera w częstotliwości

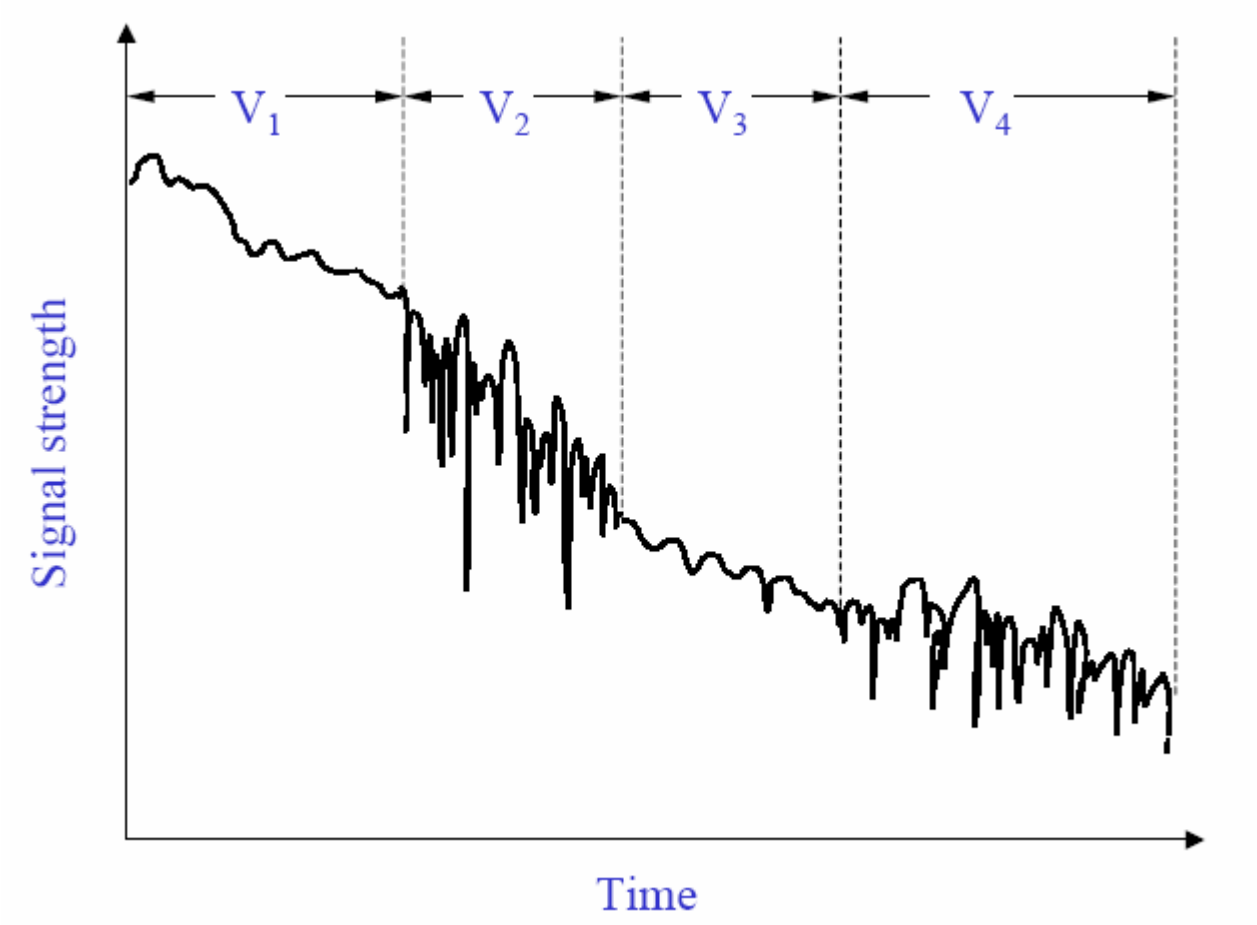
$$f_D = \frac{v}{\lambda}\cos\theta$$

gdzie v jest prędkością MS,

λ jest długością fali nośnika



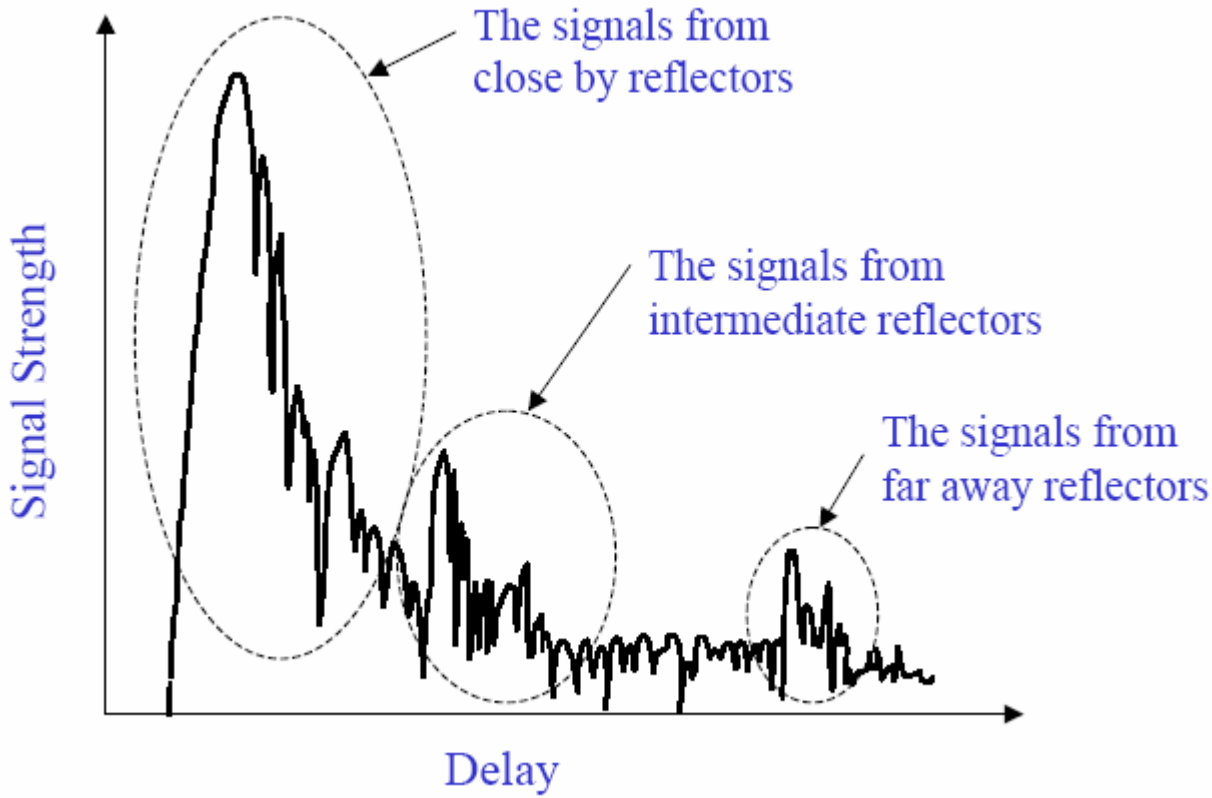
Efekt poruszającej się prędkości



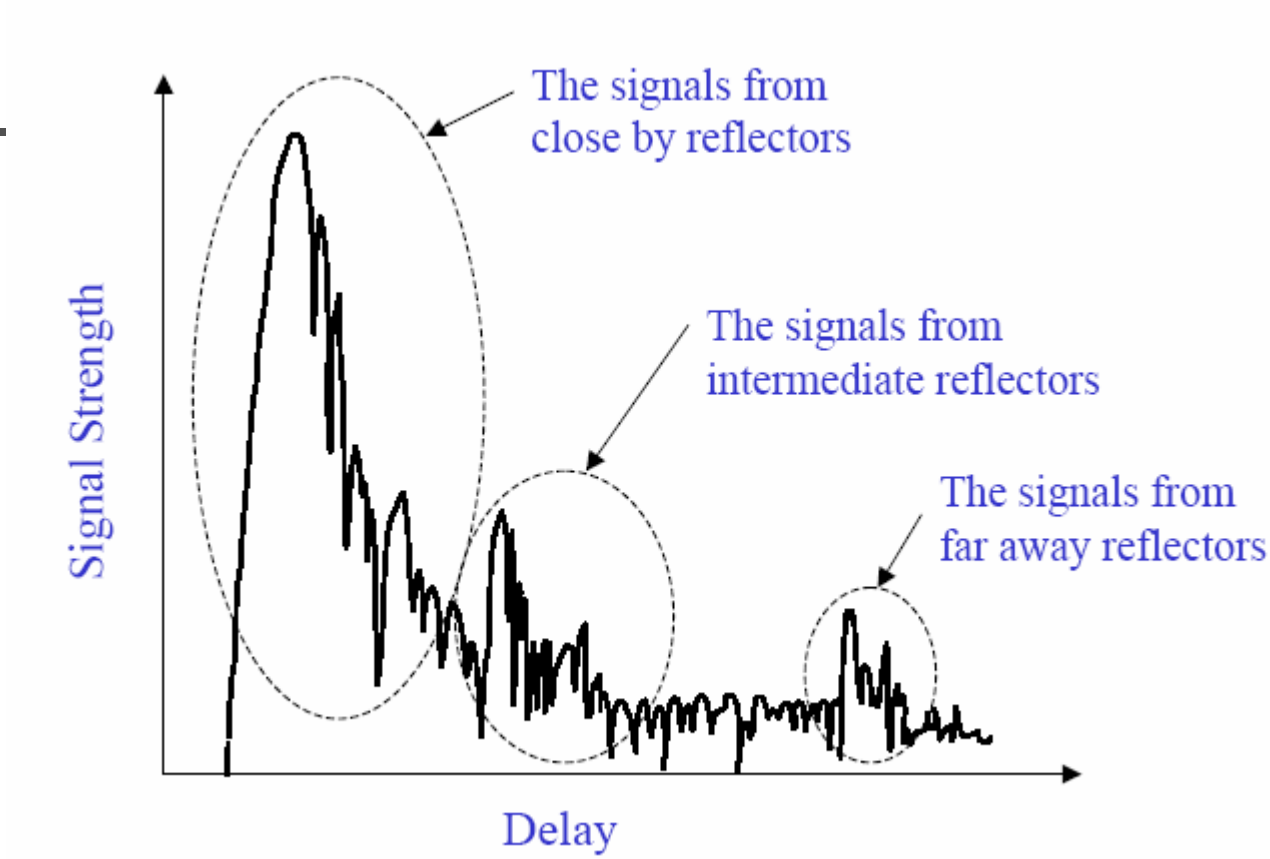
Rozpostarcie opóźnienia

- W czasie propagacji sygnału od nadajnika do odbiornika, sygnał odbija się raz lub więcej
- To powoduje, że sygnał przychodzi różnymi drogami
- Każda droga ma inną długość, tak więc czas przybycia sygnału różnymi drogami jest różny
- Ten efekt, który powoduje rozpostarcie sygnału nazywany jest „rozpostarciem opóźnienia”

Rozpostarcie opóźnienia



Rozpostarcie opóźnienia



- Rozpostarcie opóźnienia wynosi około 3us w obszarze miejskim i do 10us w terenie pagórkowatym

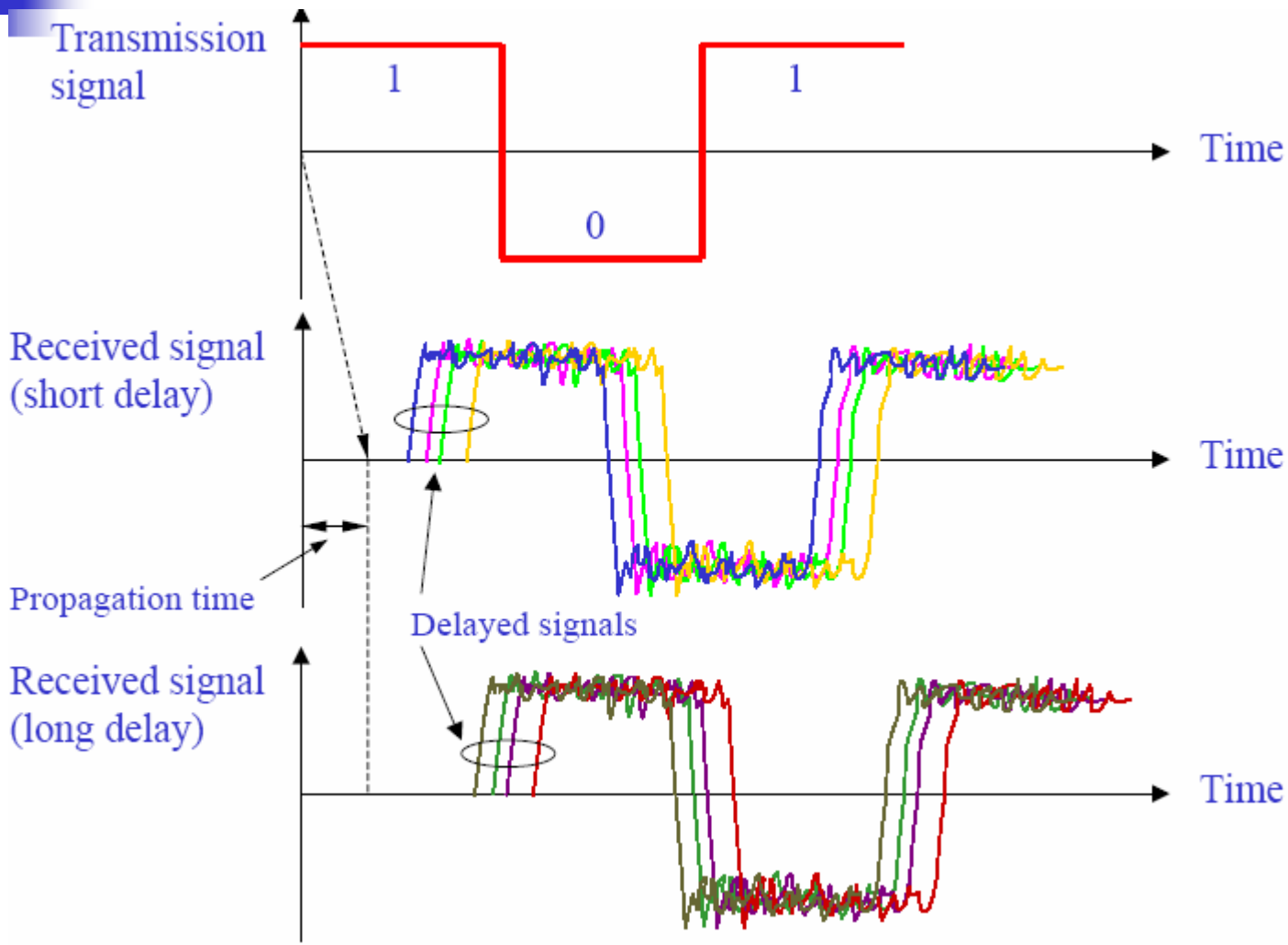
Interferencja międzysymbolowa

- Jest wynikiem wielotorowości sygnałów i spowodowanch tym opóźnień czasowych
- Ma wpływ na stopę błędów kanału (patrz, rysunek)
- Drugi multipath sygnał jest opóźniony tak dużo, że jego część może być otrzymana w czasie interwału drugiego symbolu
- aby mieć mała bitową stopę błędu

$$R < \frac{1}{2\tau_d}$$

- R (prędkość transmisji cyfrowej) jest ograniczona przez rozpostarcie opóźnienia

Interferencja międzysymbolowa



Pasmo koherencji (spójności)

- Pasmo koherencji B_c:

  - reprezentuje korelację między 2-ma zanikającymi sygnałami o częstotliwościach f_1 i f_2
  - jest funkcją rozprzestrzeniania opóźnienia
  - dwie częstotliwości, które są większe niż pasmo koherencji zanikają niezależnie od siebie
  - koncepcja użyteczna dla dywersyfikacji odbioru: wiele kopii tej samej wiadomości jest wysyłanych przy uzyciu róznych częstotliwości

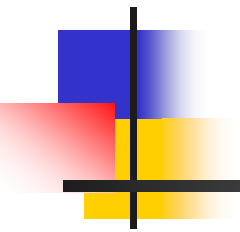
-

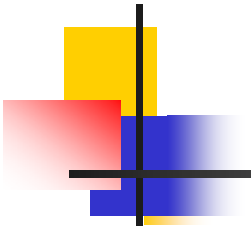
Międzykanałowa interferencja

- Komórki mające tą samą częstotliwość interferują między sobą
- r_d jest chcianym sygnałem
- r_u jest interferującym niechcianym sygnałem
- β jest współczynnikiem protekcji, takim że $r_d \leq \beta r_u$ (takim, że sygnały interferują najmniej)
- Jeżeli P jest prawdopodobieństwem, że $r_d \leq \beta r_u$

- Prawdopodobieństwo międzykanałowe $P_{co} = P$

Mobilne systemy komunikacyjne

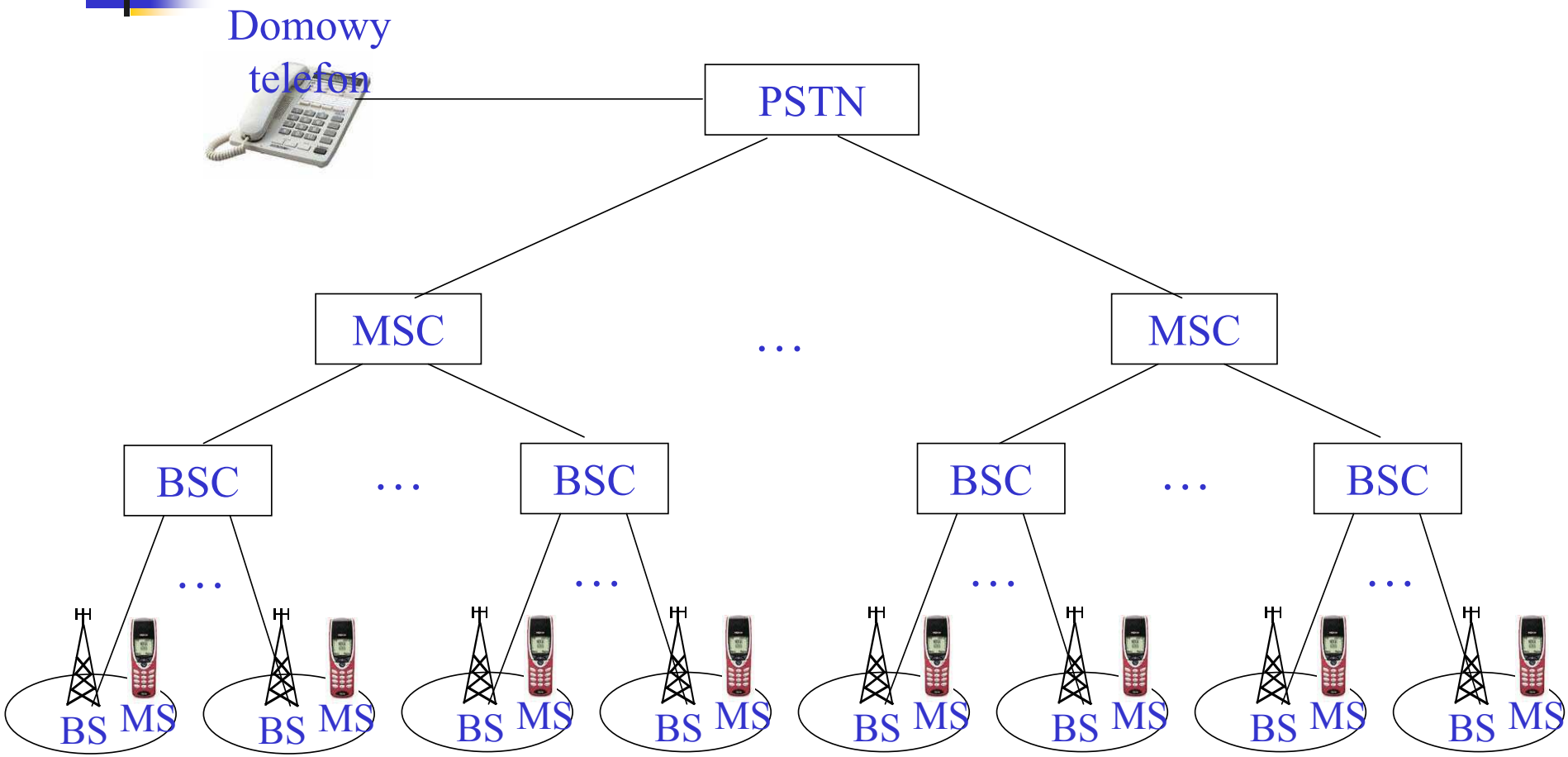




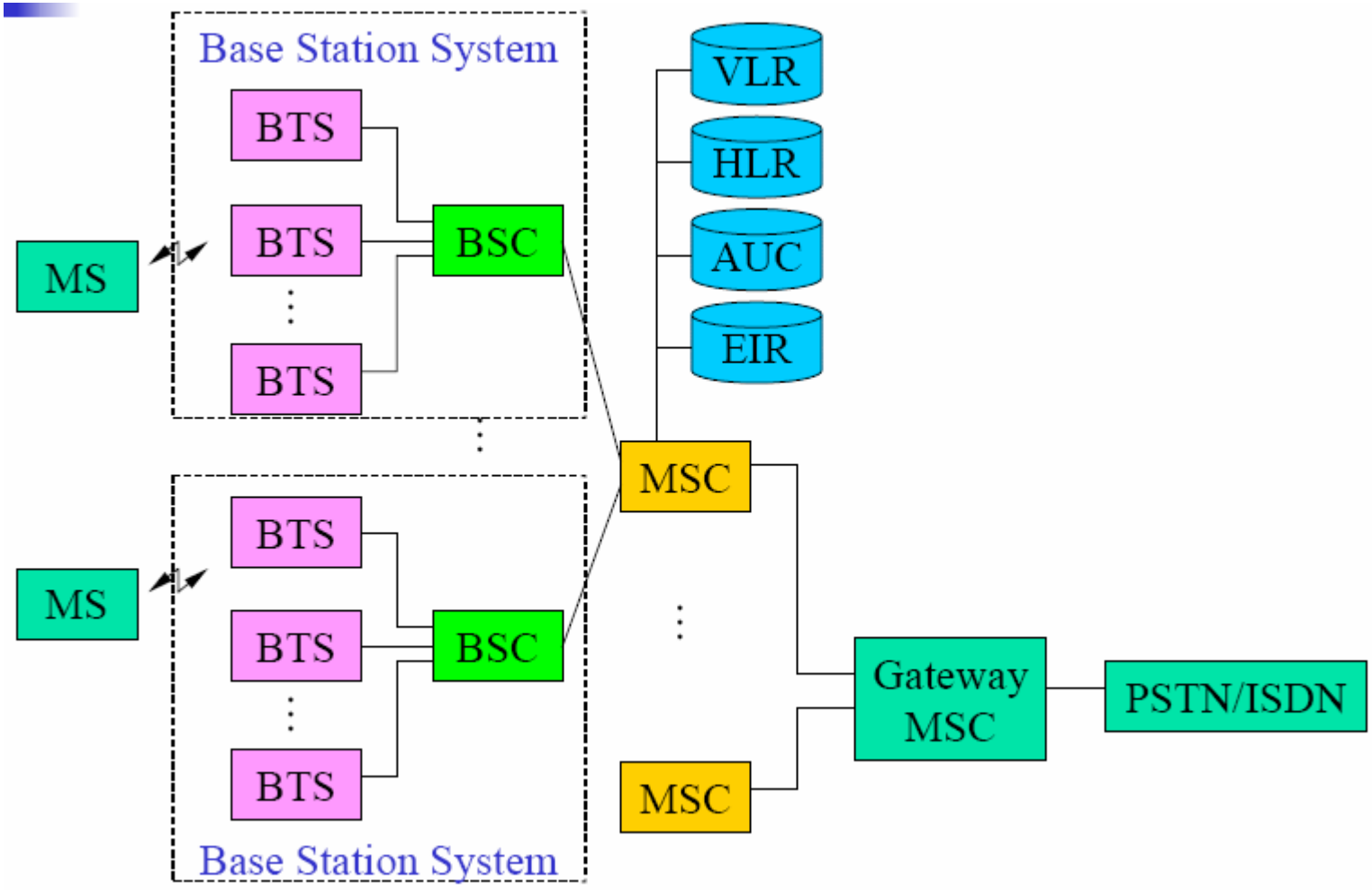
Spis treści

- Infrastruktura systemów komórkowych
- Rejestracja
- Przenoszenie połączenia
- Roaming
- Multicasting (multiemisja)
- Bezpieczeństwo i prywatność

MS (mobile station), **BS** (base station), **BSC** (BSController), **MSC** (mobile switch center), **and PSTN** (public switched telephone network)



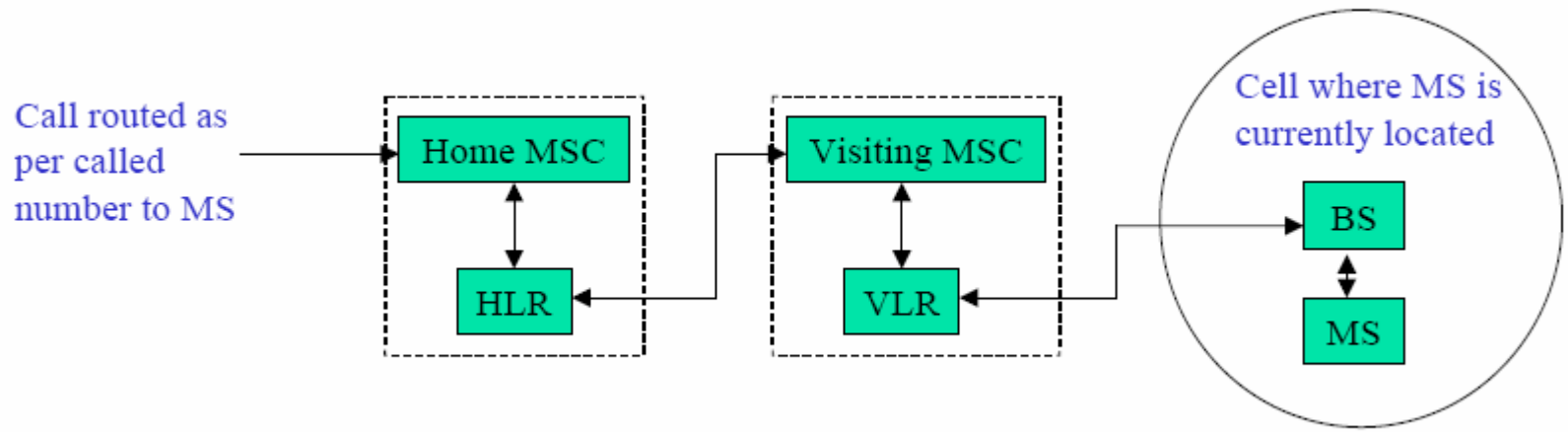
System komórkowy



VLR/HLR

- VLR zawiera informację o wszystkich wizytujących MS-ach w danym obszarze zarządzanym przez MSC
- VLR posiada wskaźniki do HLR-ów wizytujących MS-ów
- VLR pomaga w rozliczeniach oraz pozwoleniach dostępu wizytujących MS-ów

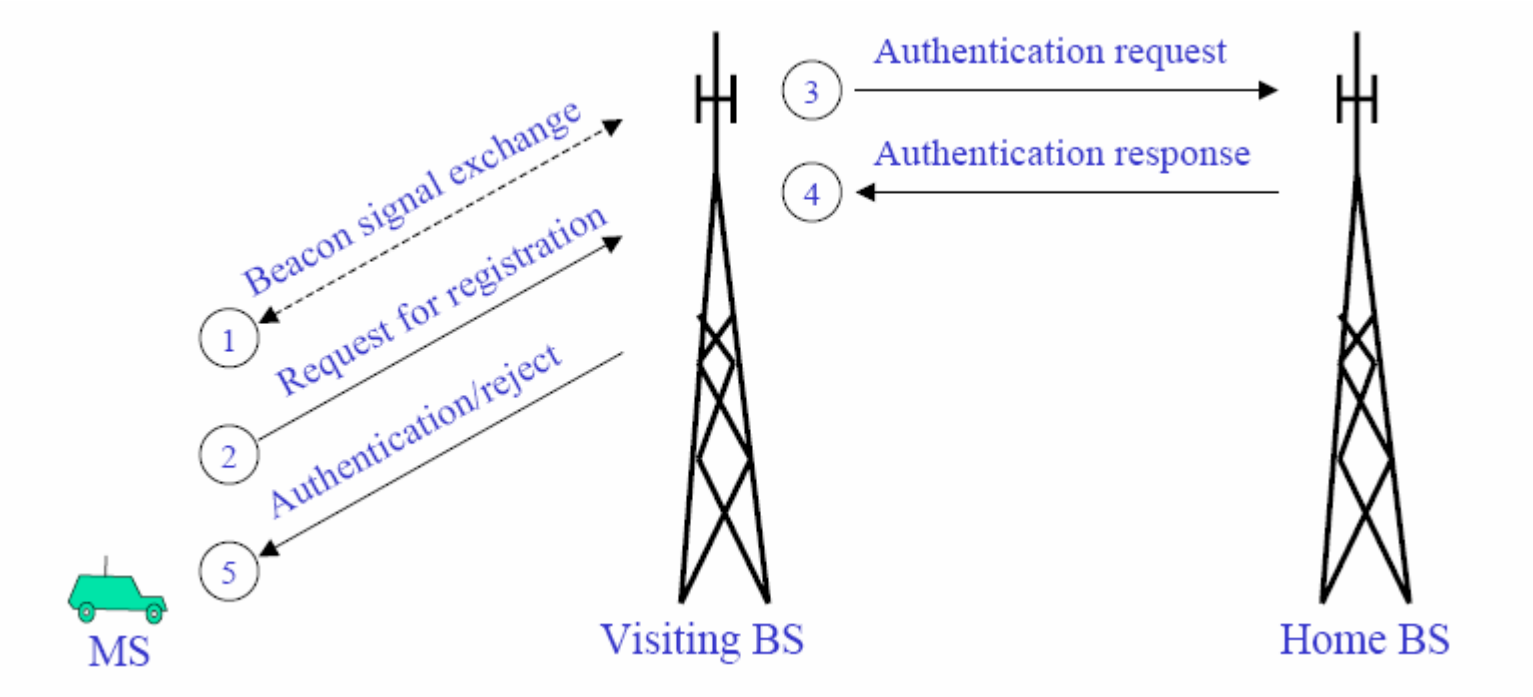
Przekierowanie rozmowy do MS-a w obszarze wizytowanym



Rejestracja

- System bezprzewodowy musi wiedzieć czy MS w danej chwili znajduje sie w swoim domowym obszarze czy w jakimś innym obszarze (rutowanie przychodzących rozmów)
- Jest to realizowane przez periodyczną wymianę sygnałów między BS-ami i MS-ami nazywanych sygnałami znacznika (beacons)
- BS periodycznie rozsyła sygnał znacznika (co 1 sek), aby odnajdywać i testować MS-y znajdujące się wokół niej
- Każdy MS nasłuchuje sygnałów znacznika (boje sygnalowe); jeżeli usłyszał sygnał znacznika, którego nie słyszał do tej pory to dodaje go do tablicy aktywnych znaczników sygnałowych
- Ta informacja jest używana przez MS do odnajdywania najbliższej BS
- Sygnał znacznika zawiera taką informację jak: identyfikator sieci komórkowej, znacznik czasu, adres bramki, idendyfikator obszaru stronicowania, itp.

Używanie telefonu mobilnego poza obszarem subskrypcji



Kroki rejestracji

- MS nasłuchuje sygnałów znacznika czasowego; jeśli odbierze nowy znacznik to MS dodaje go do tablicy aktywnych znaczników sygnałowych
- Jeżeli MS zdecyduje, że musi komunikować się poprzez nowy BS to jądro tablicy inicjuje proces przeniesienia połączenia
- MS lokalizuje najbliższy BS poprzez

  przetwarzanie poziomu użytkownika
- Wizytowany BS wykonuje przetwarzanie poziomu użytkownika i określa
  - Kim jest jest użytkownik
  - Jakie są jego uprawnienia dostępu
  - Jaki jest jego domowy MSC, który prowadzi jego rozliczenia
- Domowy MSC wysyła odpowiednią odpowiedź autoryzacji do bieżącego obsługującego BS
- BS zatwierdza/nie zatwierdza dostęp użytkownika

Zastosowania i charakterystyki sygnałów znacznika czasowego

- W USA te sygnały są transmitowane przez system AMPS (Advanced Mobile Phone System) lub CDPD (Cellular Digital Packet Data) system
- W Europie i Azji przez system drugiej generacji GSM
- W zależności od aplikacji sygnały o różnych częstotliwościach są używane

Zastosowania i charakterystyki sygnałów znacznika czasowego

Application	Frequency band	Information carried
Cellular networks	824–849 MHz (AMPS/CDPD), 1,850–1,910 MHz (GSM)	Cellular IP network identifier, gateway IP address, paging area ID, timestamp
Wireless LANs (discussed in Chapter 14)	902–928 MHz (industrial, scientific, and medical band for analog and mixed signals) 2.4–2.5 GHz (ISM band for digital signals)	Traffic indication map
MANETs (discussed in Chapter 13)	902–928 MHz (ISM band for analog and mixed signals) 2.4–2.5 GHz (ISM band for digital signals)	Network node identity
GPS	1575.42 MHz	Timestamped orbital map and astronomical information
Search and rescue	406 and 121.5 MHz	Registration country and ID of vessel or aircraft in distress
Mobile robotics	100 kHz–1 MHz	Position of pallet or payload
Location tracking	300 GHz–810 THz (infrared)	Digitally encoded signal to identify user's location
Aid to the impaired	176 MHz	Digitally coded signal uniquely identifying physical locations

Przeniesienie połączenia

- Jest to zmiana zasobów radiowych z danej komórki do przyległej
- Przeniesienie połączenia zależy od rozmiaru komórki, jej długości granic, siły sygnału, zanikania sygnału, odbicia, itp.
- Przeniesienie połączenia może być inicjalizowane przez MS lub BS i może nastapić z powodu
  - Połączenia radiowego
  - Zarządzania sieciowego
  - Kwestii związanych z jakością obsługi

Przeniesienie połączenia (cd.)

- Przeniesienie połączenia typu łącze radiowe jest spowodowane mobilnością MS-a. Zależy ono od:
  - Liczby MS-ów w komórce
  - Liczby MS-ów, które właśnie opuściły komórkę
  - Liczby połaczeń generowanych w komórce
  - Liczby połączeń tranferowanych z sąsiednich komórek przez przeniesienie połączenia
  - Liczby i długości połączeń zakończonych w komórce
  - Liczby połączeń, które były przeniesione do sąsiednich komórek
  - Liczby aktywnych połaczeń w komórce
  - Wielkości populacji w komórce
  - Całkowitego czasu trwania połączenia w komórce
  - Czasu pojawienia się połączenia w komórce
  - Itp.

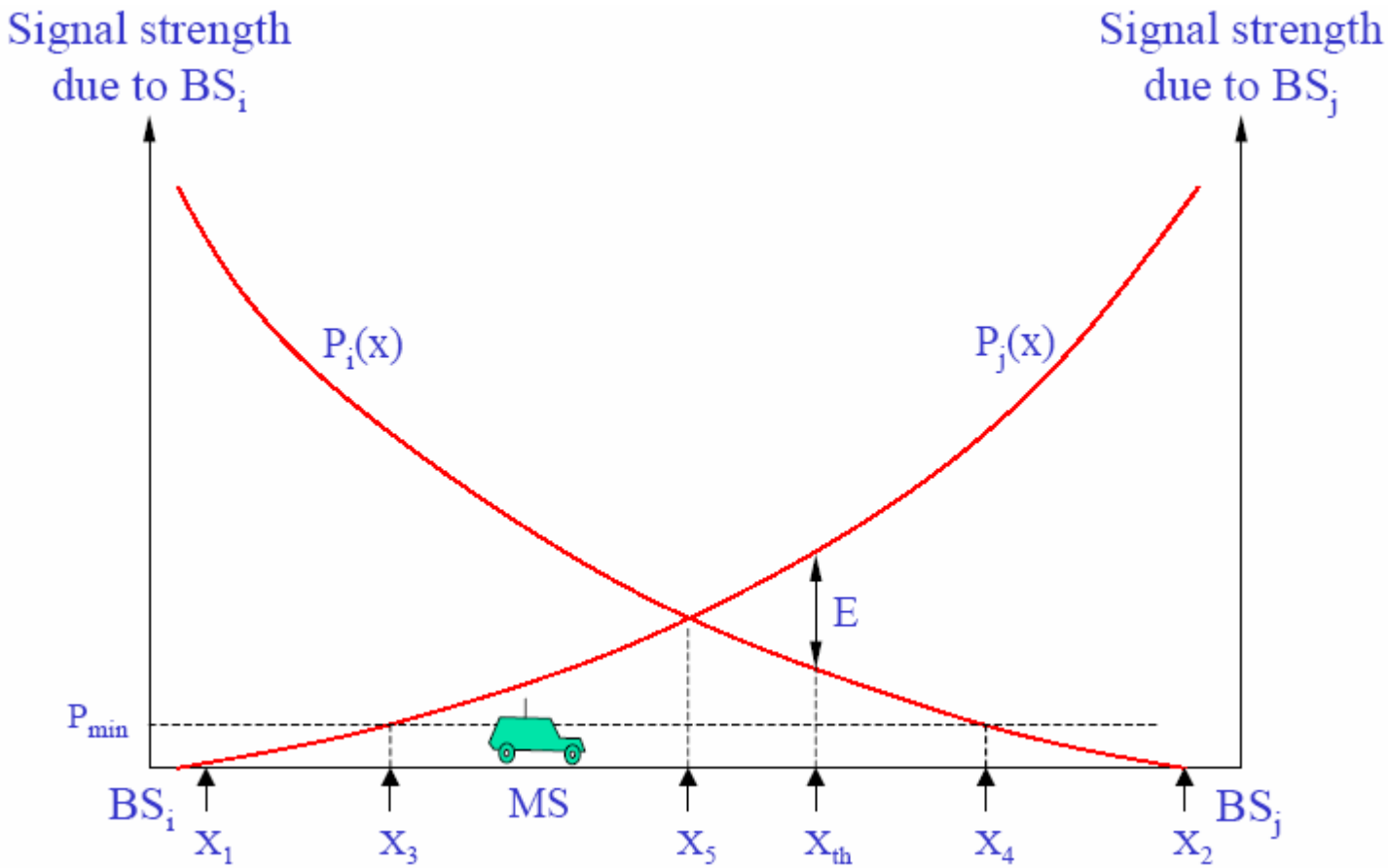
Przeniesienie połączenia (cd.)

- System zarządzania siecią może spowodować przeniesienie połączenia jeżeli pojawi się drastyczne niezbalansowanie obciążenia w przyległych komórkach i wymagane jest optymalne zbalansowanie zasobów
- Przeniesienie z powodu obsługi jest powodowane degradacją jakości obsługi (QoS)

Wybór czasu przeniesienia połączenia

- Czynnikami, które decydują o wyborze właściwego czasu przeniesienia połączenia są:
  - Siła sygnału
  - Faza sygnału
  - Kombinacja siły i fazy sygnału
  - Stopa błędów bitów (BER-bit error rate)
  - Odległość
- Konieczność przeniesienia połączenia jest określana przez
  - Siłę sygnału
  - Stosunek sygnału nośnika do sygnału interferencji (CIR-carrier to interference ratio)

Inicjalizacja przeniesienia połączenia



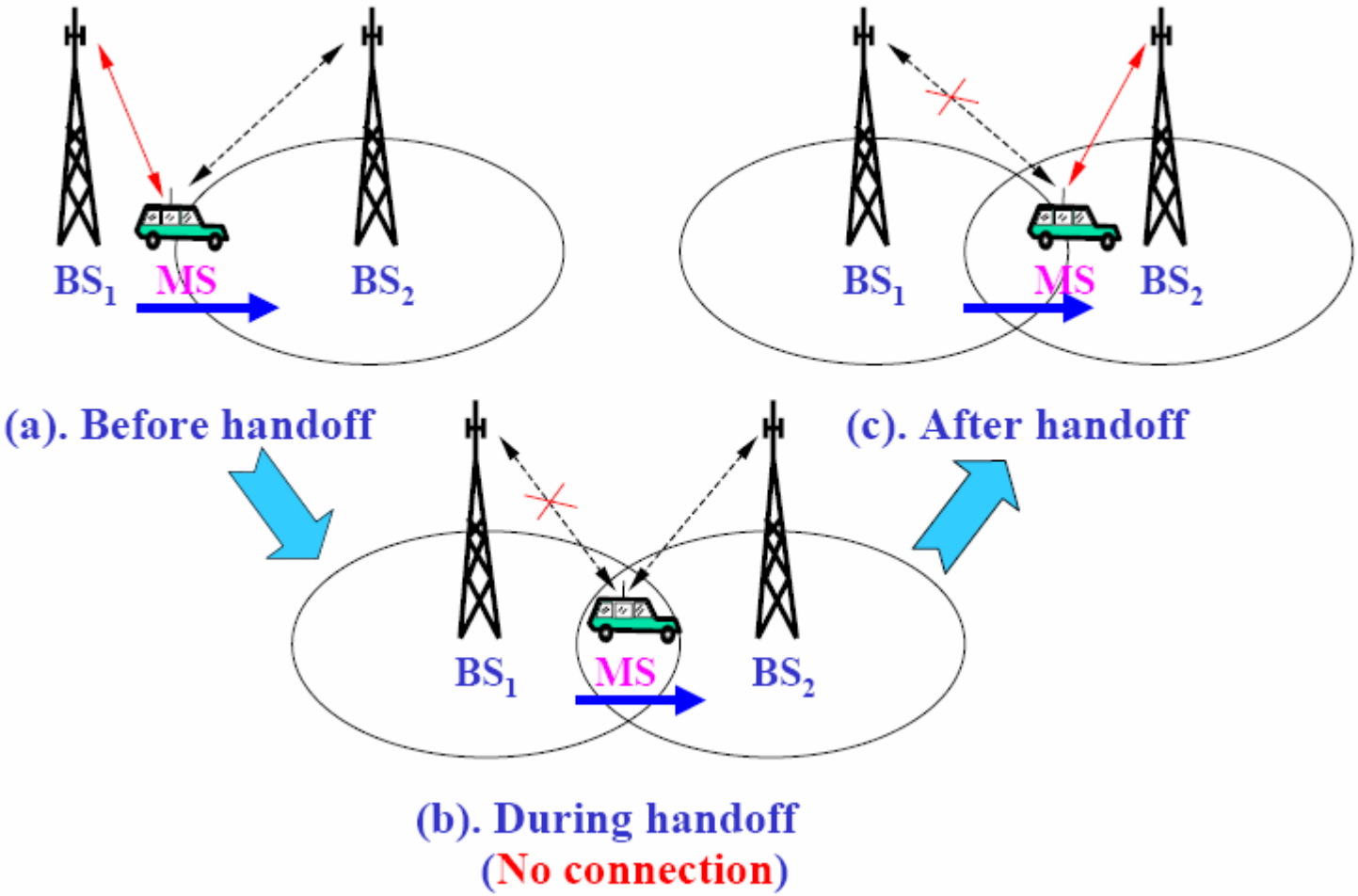
Inicjalizacja przeniesienia połączenia (cd.)

- Region X_3-X_4 jest regionem gdzie w zależności od innych czynników przeniesienie połączenia może nastąpić
- Jedna z możliwości przeniesienia połączenia jest jego realizacja w X_5, gdzie siły obu sygnałów są równe
- Jeżeli MS porusza się do tyłu i do przodu wokół X_5, to wynikiem tego będą często wykonywane przeniesienia połaczenia (efekt ping-ponga)
- Dlatego pozwala się MS-owi pracować z bieżącym BS tak długo jak siła sygnału nie zniży się do progowej wartości E
- Różne systemy komórkowe posługują się różnymi procedurami przeniesienia połączenia

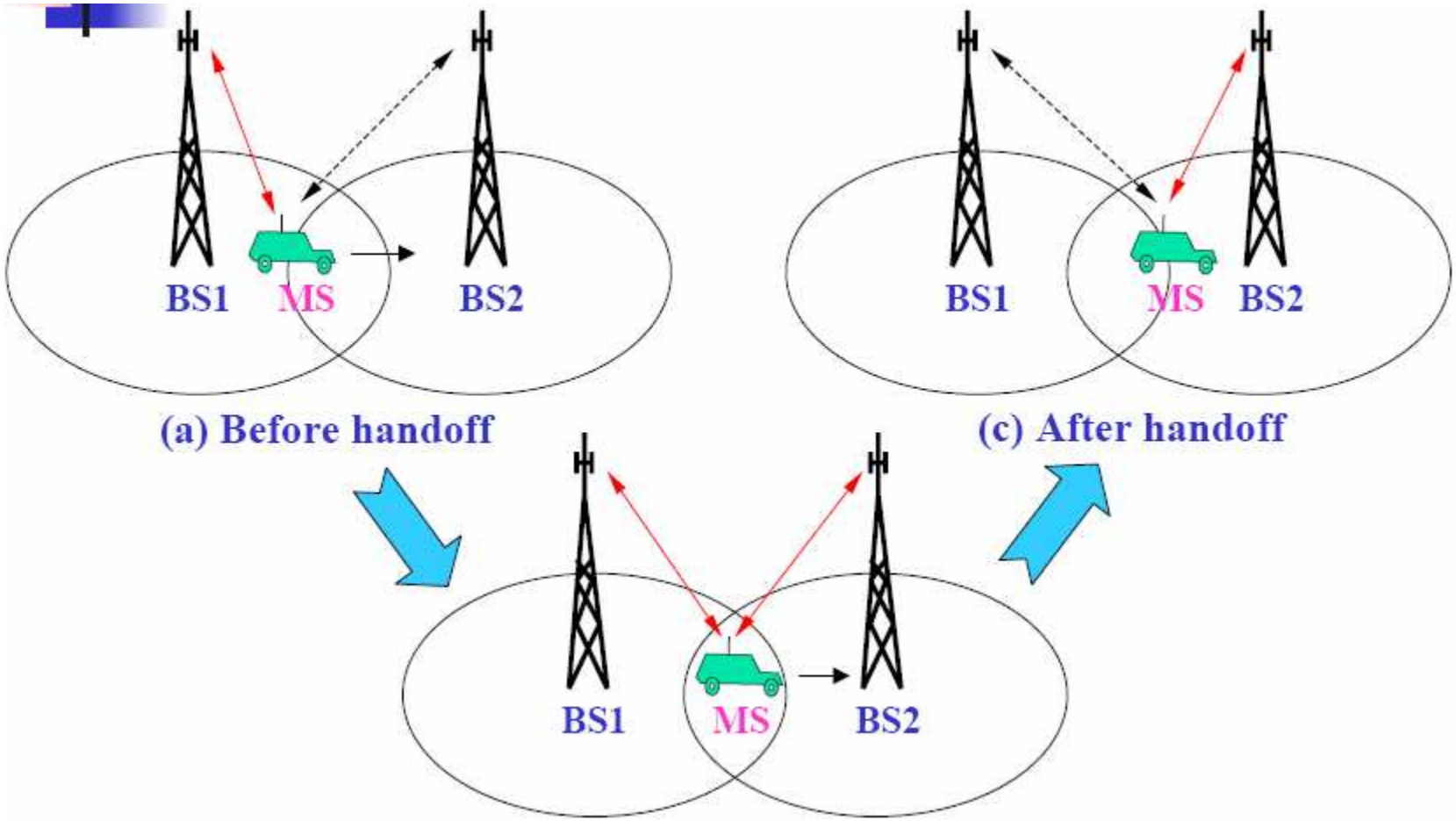
Typy przeniesienia połączenia

- Twarde przeniesienie połączenia (break before make)
  - Zwolnienie bieżących zasobów danego BS-a przed uzyskaniem zasobów z następnego BS-a
  - FDMA, TDMA realizują takie przeniesienia
- Miękkie przeniesienie połączenia (make before break)
  - W CDMA, ponieważ ten sam kanał jest używany należy zmienić kode przeniesienia połaczenia jeżeli ten kod nie jest ortogonalny do kodu w następnym BS
  - Dlatego, jest mozliwe aby MS komunikował się jednocześnie z danym BS oraz z nowym BS

Twarde przeniesienie połączenia



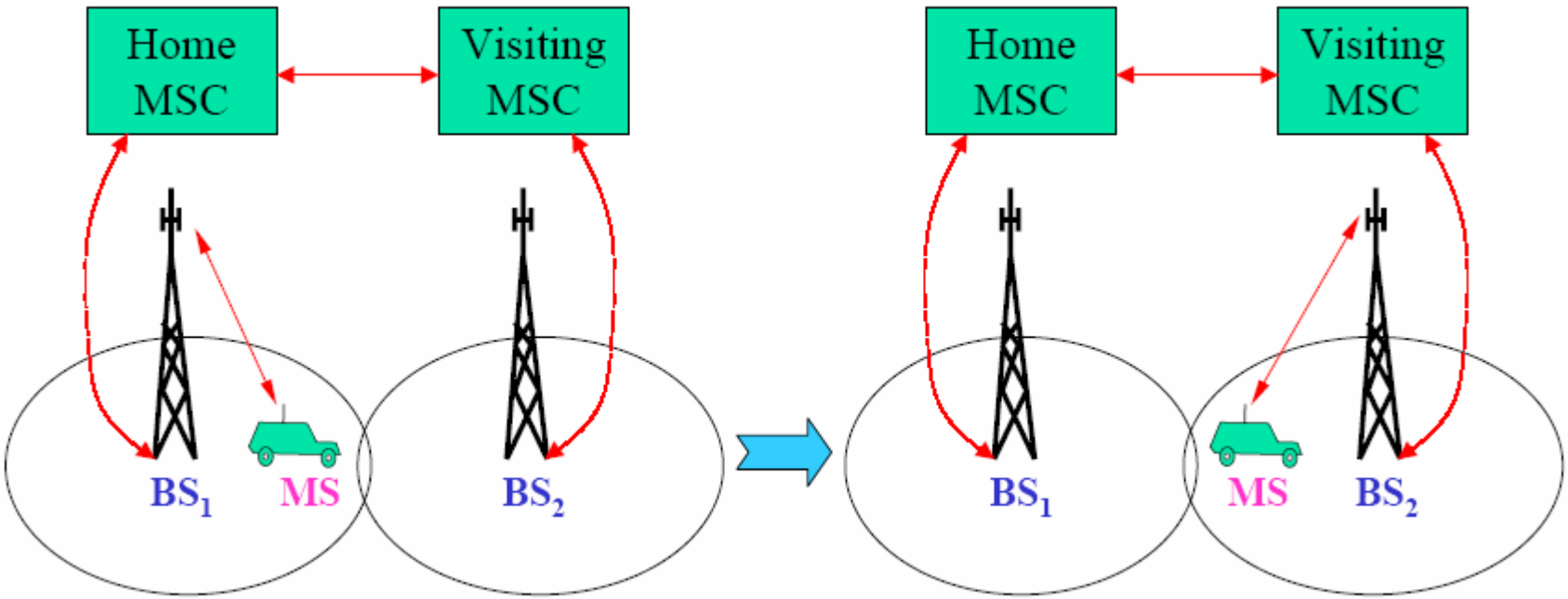
Miękkie przeniesienia połączenia (tylko dla CDMA)



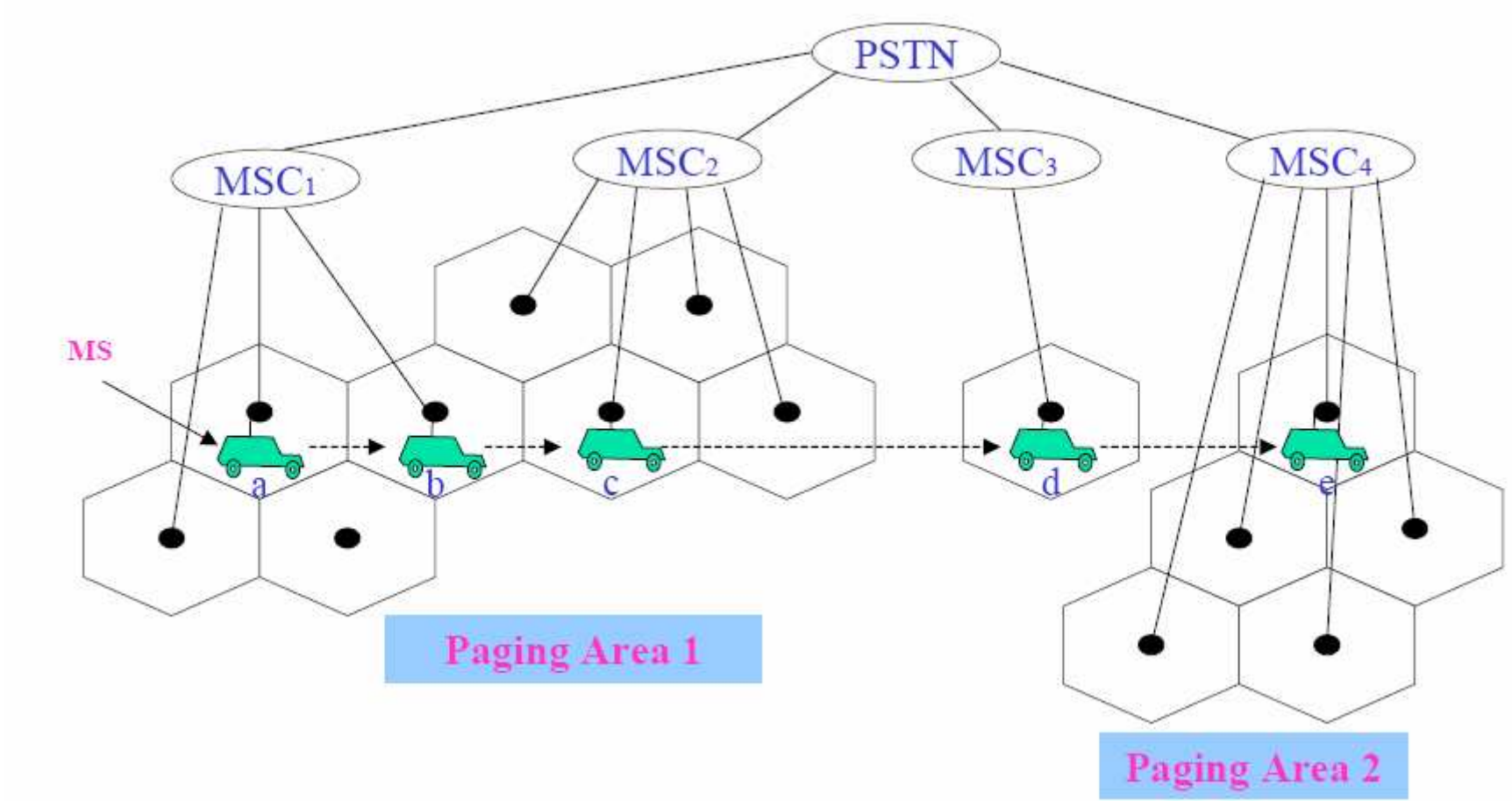
Roaming

- Odbywa się gdy MS przechodzi z komórki znajdującej sie w obszarze zarządzanym przez jeden MSC do komórki zarządzanej przez inny MSC
- sygnały znaczników czasowych oraz użycie HLR-VLR umożliwia roaming wszędzie pod warunkiem, że prowajderzy używają tego samego zakresu częstotliwości

Roaming


Home MSC
Visiting MSC
BS1
MS
BS2
Home MSC
Visiting MSC
BS1
MS
BS2

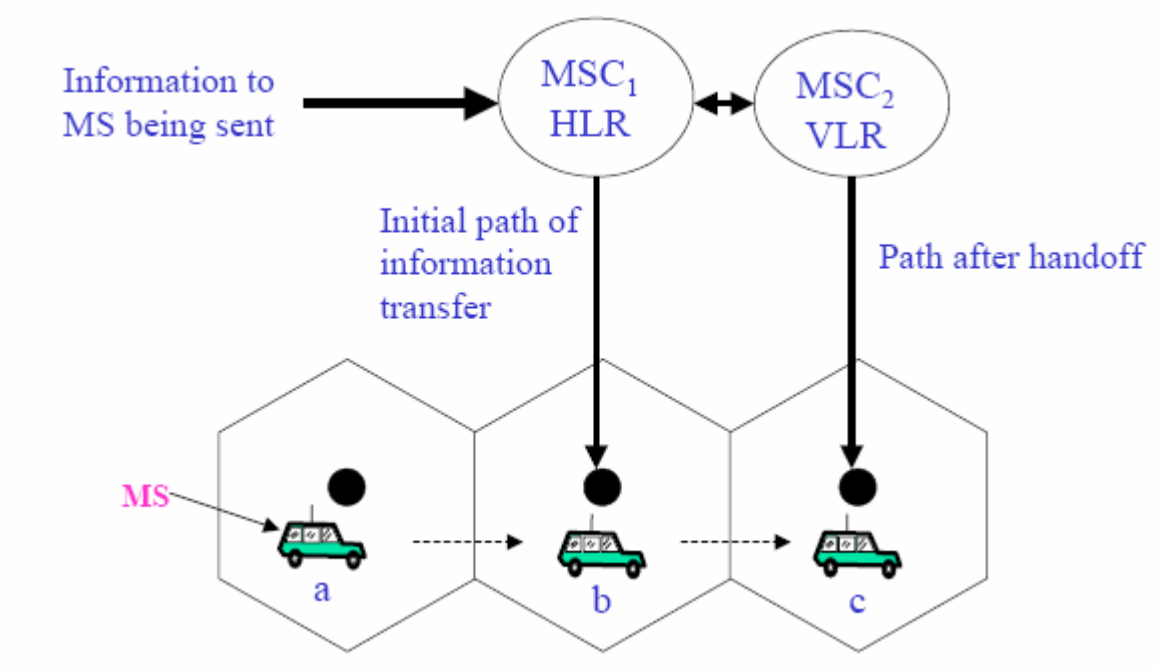
Scenariusze przeniesienia połączenia przy różnych stopniach mobilności



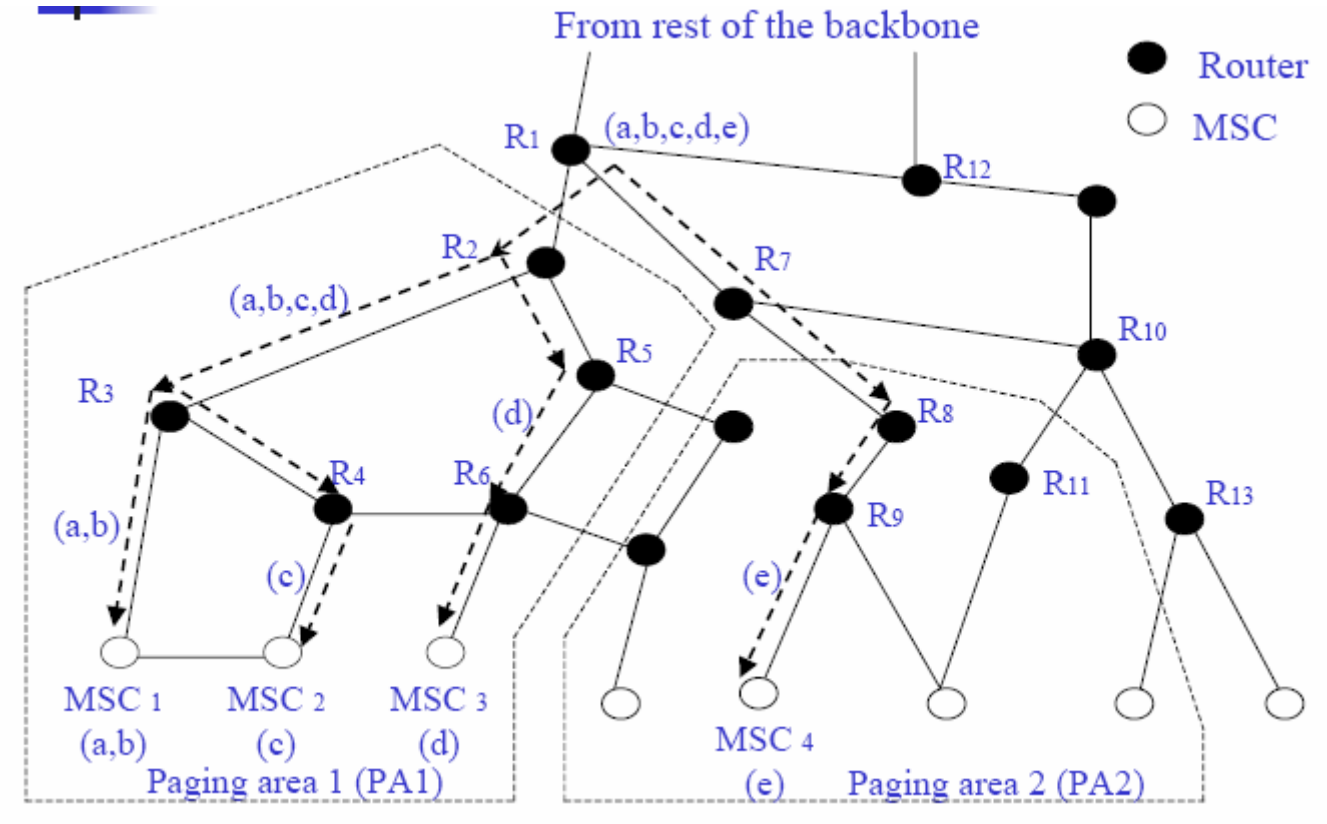
Możliwe sytuacje podczas przeniesienia połączenia

- Załóżmy, że MSC_1 jest właściwe dla danego MS z punktu widzenia jego rejestracji, podliczania, uwierzytelnienia, itp.
- Gdy przeniesienie połączenia następuje z pozycji „a” do „b” to rutowanie jest wykonane przez MSC_1 wyłącznie
- Gdy przeniesienie połączenia następuje z „b” do „c” to dwukierunkowe pointery są ustawiane, aby połączyć HLR należące do MSC_1 z VLR należące do MSC_2
- Gdy przeniesienie połączenia następuje z „d” do „e” to rutowanie informacji z użyciem HLR-VLR może nie być adekwatne („d” jest w innym *obszarze stronicowania-PA*)
- PA-obszar pokryty przez jeden lub kilka MSC w celu odnajdywania bieżącej lokalizacji MS-ów
- Koncepcja sieci szkieletowej

Droga transmisji informacji gdy MS przechodzi z „b” do „c”



Ilustracja połączeń MSC (Mobile Switching Center) do sieci szkieletowej oraz rutowanie/rerutowanie



Sieć szkieletowa

- Rutowanie odbywa się zgodnie z topologią sieci szkieletowej
- Linie przerywane pokazują możliwe drogi dla połączeń realizowanych dla MS-ów mających różne lokalizacje
- Jedną z opcji jest odnalezienie rutera wzdłuż oryginalnej drogi skąd nowa droga musi się rozpocząć, aby osiagnąć MSC wzdłuż nakrótszej drogi

Domowi agenci (HA-home agents), obcy agenci (FA-foreign agents) oraz mobilne IP

- Dwa ważne softwerowe moduły związane są z ruterami: domowy agent (HA-home agent) oraz obcy agent (FA-foreign agent)
- MS jest również zarejestrowany w ruterze i zwykle ruter najbliższy do domowego MSC (dla danego MS) może być wybrany, aby służyć jako HA
- Gdy MS przenosi się z domowej sieci to softwerowy moduł FA w nowej sieci pomaga dla MS forwardując dla niego pakiety
- Funkcjonalność HA-FA jest w jakiś sposób podobna do HLR-VLR

Domowy MSC i domowy agent (HA) dla poprzedniej sieci

Home MSC	MSC_1	MSC_2	MSC_3	MSC_4
Selected router for maintaining its home agent	R_3	R_4	R_6	R_9

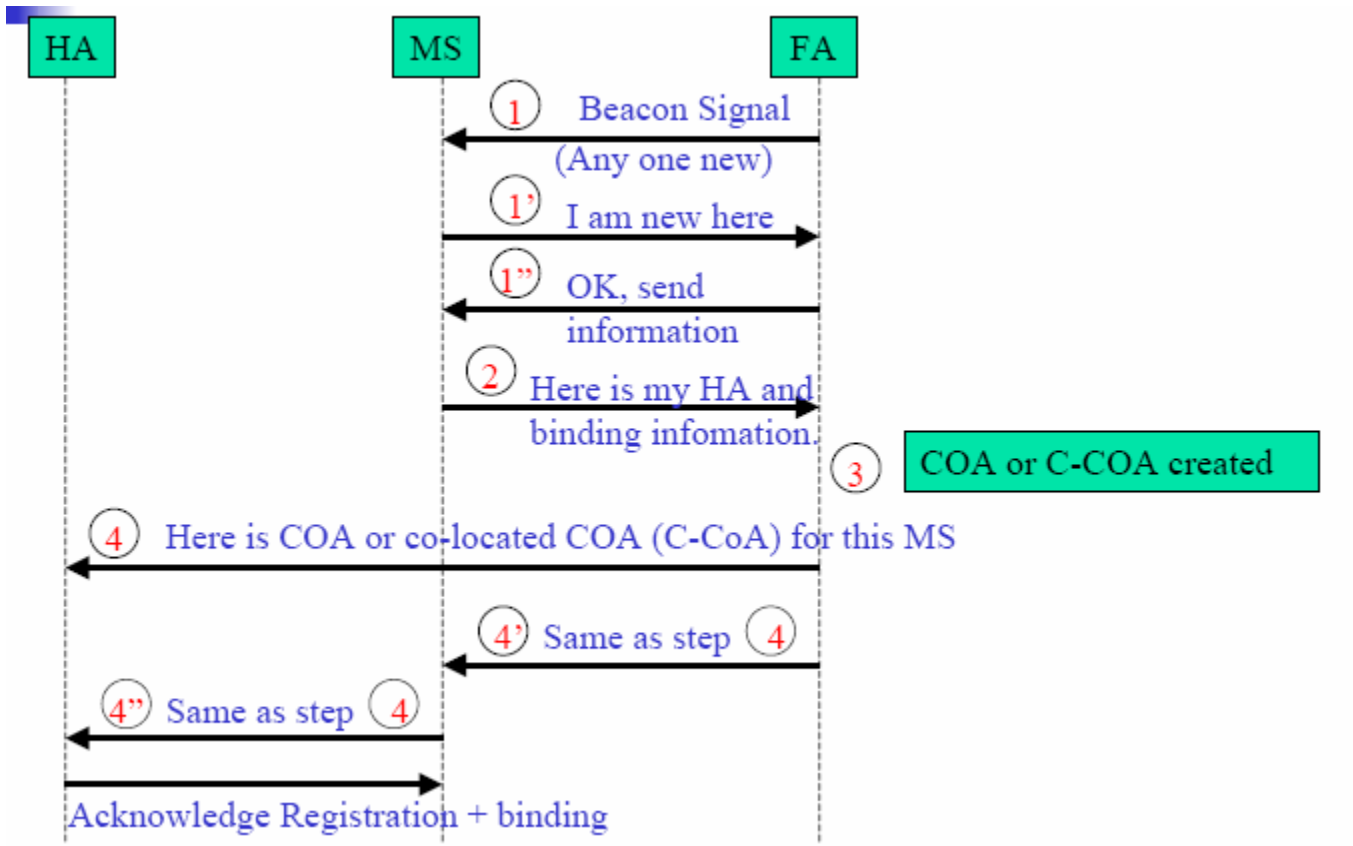
Ustanowienie połączenia z użyciem HA-FA

- Jeżeli MS przenosi się do nowej sieci to jego HA pozostaje niezmieniony
- MS odkrywa FA w nowej sieci przez detekcję periodycznych sygnałów znaczników czasowych, które transmituje FA
- MS może również wysłać własną wiadomość (agent solicitation messages) z prośbą o przydział agenta, na którą FA odpowie
- Gdy FA odkryje nowego MS to przydziela mu CoA (care-of address) używając do tego protokołu dynamicznej konfiguracji hosta (DHCP-dynamic host configuration protocol)
- Po otrzymaniu CoA przez MS, rejestruje on swój CoA w swoim HA oraz limit czasu ważności tej rejestracji
- Taka rejestracja jest inicjalizowana albo bezpośrednio przez MS w HA domowego rutera lub pośrednio przez FA

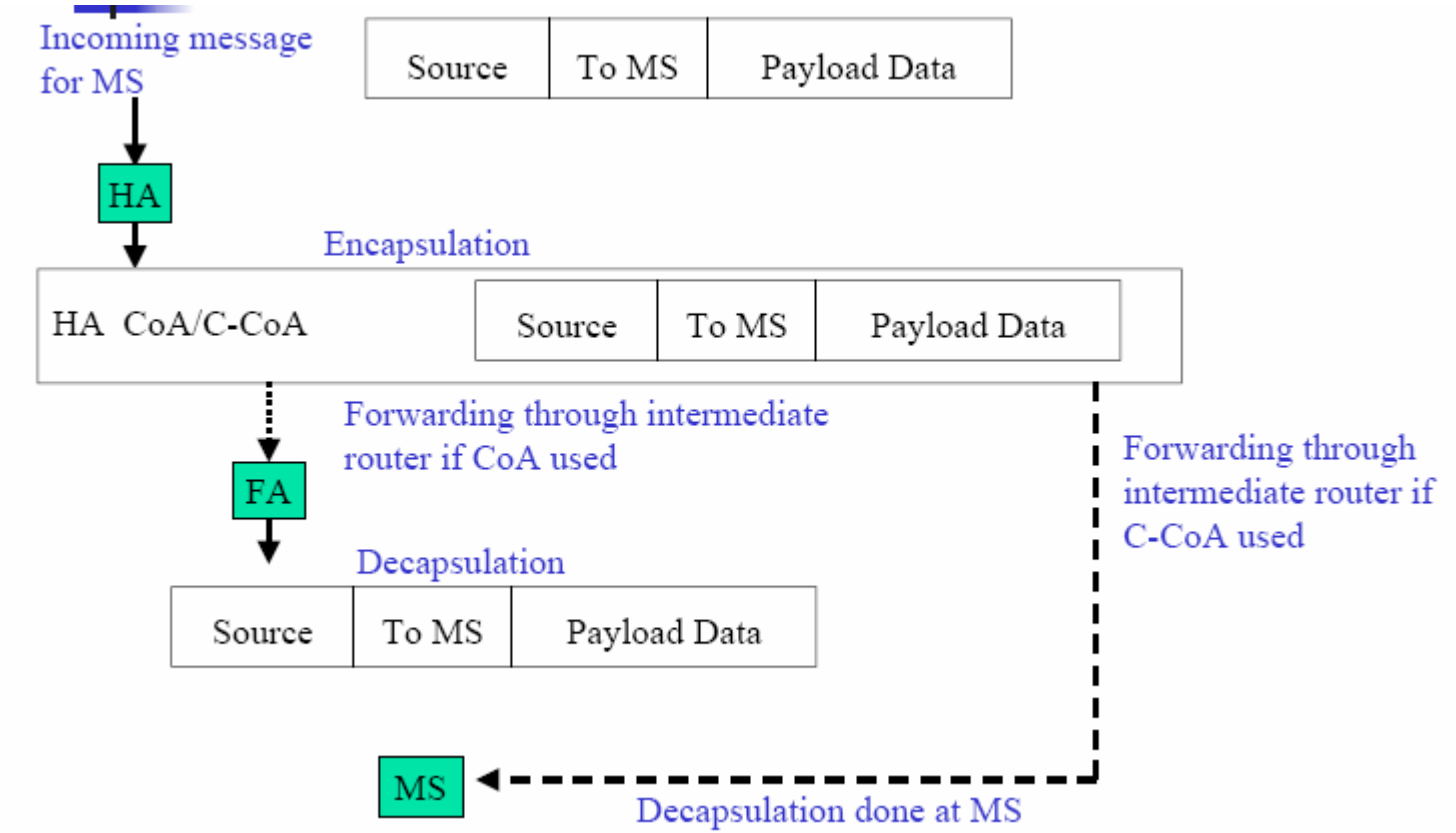
Ustanowienie połączenia (cd.)

- HA potwierdza swoje zobowiązania poprzez odpowiedź do MS
- Wiadomość wysłana z dowolnego źródła do MS posiadającego domowy adres jest otrzymywana przez HA
- Sprawdzane są zobowiązania, CoA tego MS-a jest wstawiane do pakietu i forwardowane do sieci
- Jeżeli CoA konkretnego FA było użyte to pakiet dojdzie do tego FA, który na podstawie CoA przekaże pakiet do MS-a poprzez poziom łącza
- Takie internetowe środowisko nazywane jest mobilnym IP
- Po upływie czasu zobowiązania, jeżeli MS w dalszym ciągu chce, aby pakiety były forwardowane przez HA to musi odnowić swoją rejestrację
- Gdy MS powraca do swojej domowej sieci to informuje o tym HA, które nie będzie już forwardować pakietów do FA

Rejestracja procesu między FA, MS oraz HA gdy MS przechodzi do obszaru stronicowania



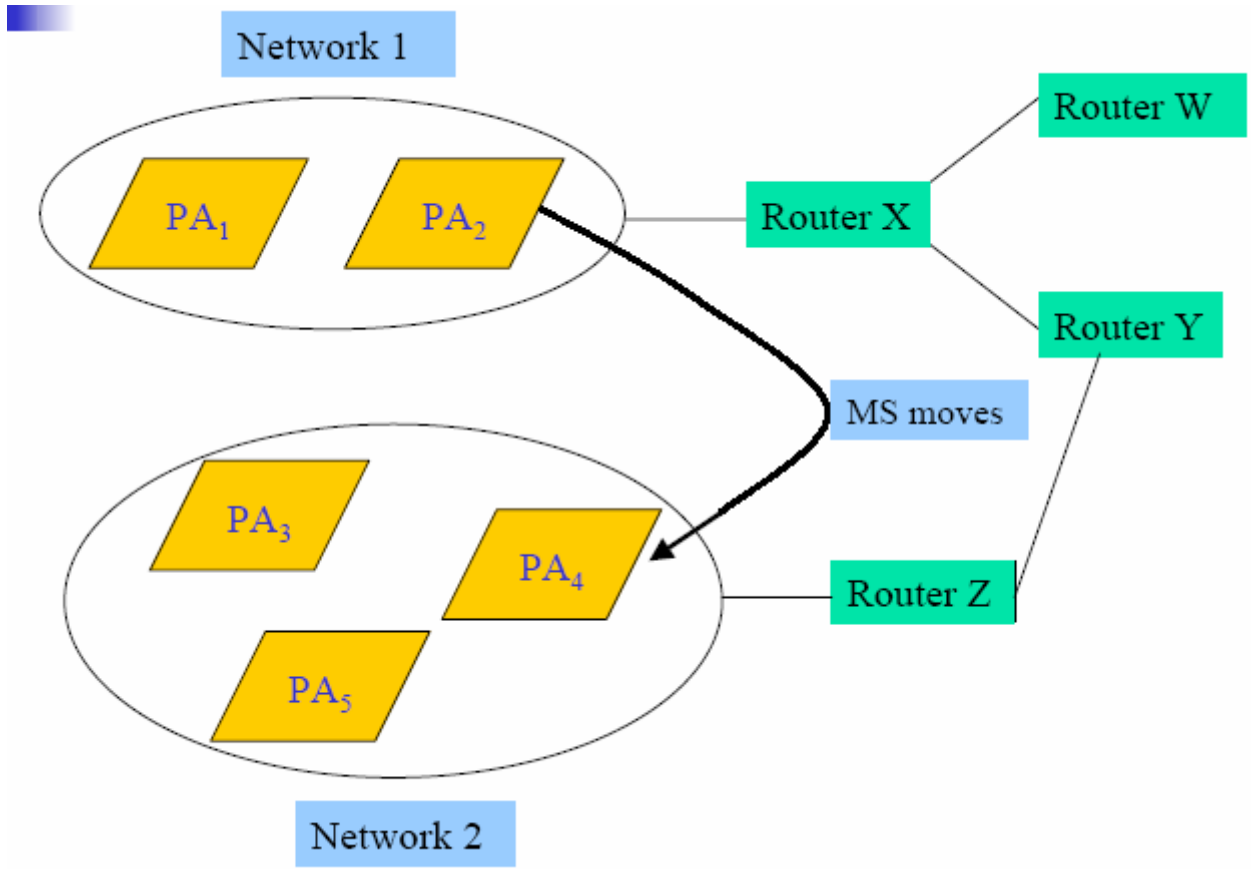
Forwardowanie wiadomości z użyciem pary HA-FA



Rutowanie w ruterach sieci szkieletowej

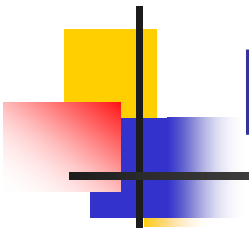
- Jak FA odnajduje HA danego MS-a ?
- Jedno z możliwych podejś może polegać na posiadaniu przez każdy ruter globalnej tablicy każdego MSC, tak aby móc określić drogę z FA do HA dla danego MS
- Wady: zbyt obszerna informacja wymagana; pewne sieci mogą nie akceptować tego, aby informacja o wszystkich ich ruterach była dostępna dla zewnętrznych sieci (tylko informacja o sieciowych bramach jest dostarczana)
- Rozwiązanie: użycie schematu rozproszonego rutingu

Ilustracja obszarów stronicowania (PAs – paging areas) oraz połączenia ruterów sieci szkieletowej



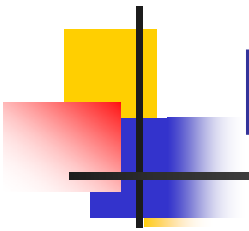
Rozproszona tablica rutowania oraz lokalizacja obszarów stronicowania

Table at router W		Table at router X		Table at router Y		Table at router Z	
Route to PA	Next hop	Route to PA	Next hop	Route to PA	Next hop	Route to PA	Next hop
1	X	1	-	1	X	1	Y
2	X	2	-	2	X	2	Y
3	X	3	Y	3	Z	3	-
4	X	4	Y	4	Z	4	-
5	X	5	Y	5	Z	5	-



Multicasting

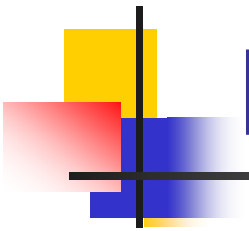
- Proces transmisji wiadomości ze źrodła do wielu odbiorców poprzez użycie adresu grupowego dla wszystkich hostów, które chcą być członkami grupy
- Redukuje to liczbę transmitowanych wiadomości w porównaniu z wielokrotną transmisją do pojedynczych odbiorców
- Jest użyteczny w video/audio konferencjach lub grach, w których bierze udział wielu uczestników



Multicasting

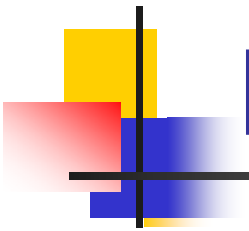
- Multicasting może być realizowany przez tworzenie albo struktury drzewa w oparciu o technikę drzew źródłowych (source based tree), albo struktury drzewa w oparciu o technikę drzew rdzeniowych (core based tree)
- Technika drzew źródłowych: dla każdego źródła w grupie utrzymywana jest najkrotsza droga łącząca członków grupy – źródło jest korzeniem drzewa
- Technika drzew rdzeniowych: konkretny ruter jest obierany rdzeniem i drzewo jest utrzymywane z rdzeniem służącym jako korzeń

  - każde źródło forwarduje pakiet do rutera-rdzenia, który z kolei forwarduje go w drzewie, aby dotrzeć do wszystkich członków multicastowej grupy



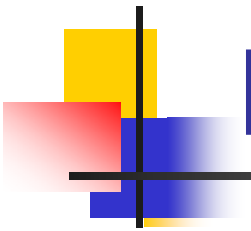
Multicasting

- Dwukierunkowe tunelowanie (Bi-directional tunneling-BT) oraz zdalna subskrypcja (Remote Subscription) były zaproponowane przez IETF (Internet Ingeneering Task Force) w celu realizacji multicastingu w Mobile IP
- Przy podejściu BT, gdy MS przechodzi do obcej sieci, HA jest odpowiedzialne za forwardowanie multicastowych pakietów do MS
- W protokole zdalnej subskrypcji, gdy MS przechodzi do obcej sieci, FA (jeżeli jeszcze nie jest członkiem grupy multicastowej) wysyła do drzewa prośbę o przyłączenie; następnie MS otrzymuje bezpośrednio pakiety multicastowe przez FA



Multicasting

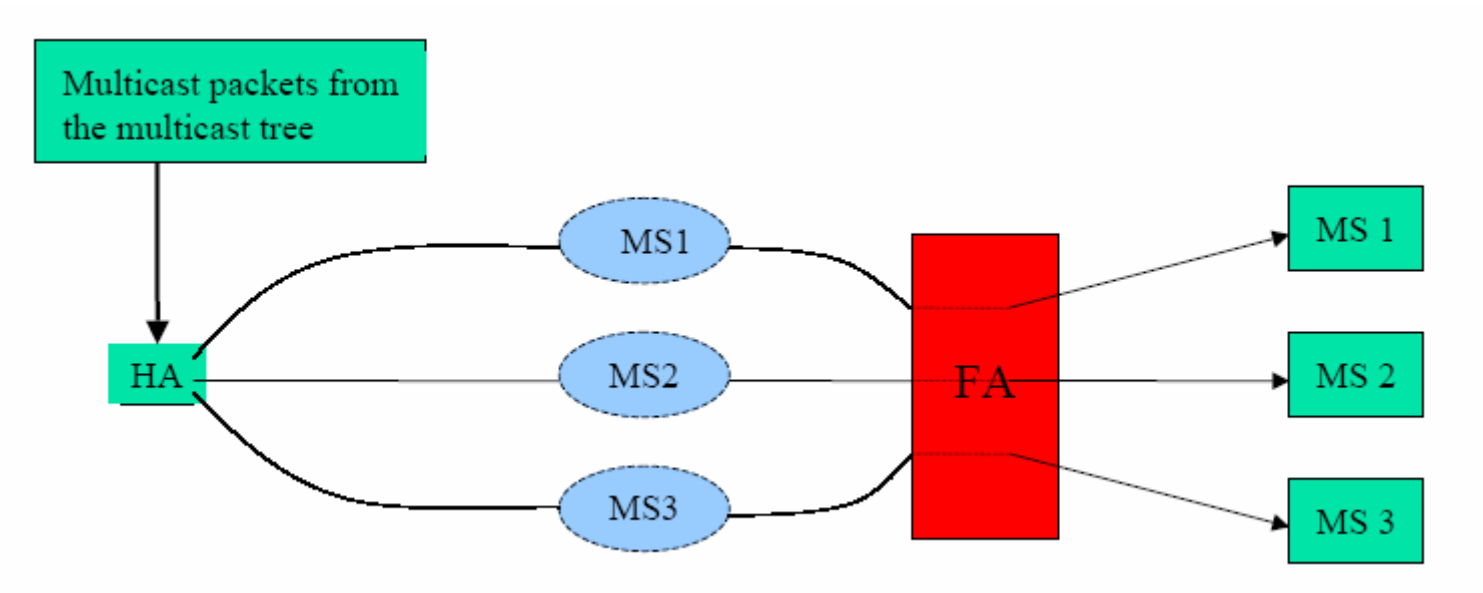
- Algorytm oparty na zdalnej subskrypcji jest prosty i zapobiega duplikacji pakietów oraz dostarczaniu pakietów nieoptymalną drogą
- Może spowodować przerwanie dostarczania danych dopóki FA nie będzie przyłączone do drzewa
- Skutkiem jego działania jest powstawanie szeregu drzew typu przyłącz oraz odłącz podczas ciągłego ruchu MS
- Natomiast, przy podejściu BT, HA tworzy dwukierunkowy tunel do FA i kapsułkuje pakiety dla MS
- Następnie FA forwarduje pakiety do MS



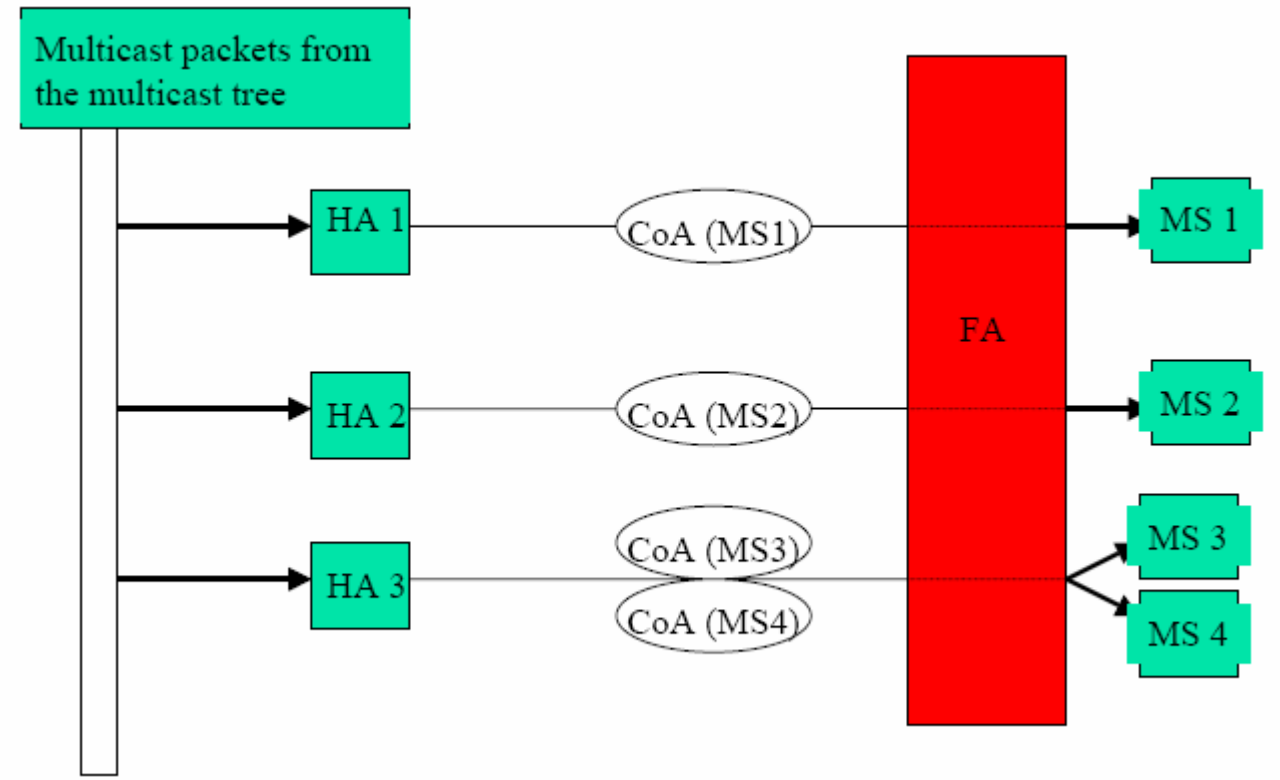
Multicasting

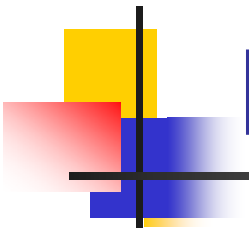
- Podejście BT zapobiega utracie danych z powodu poruszania się MS
- Jednak może spowodować duplikację pakietów jeżeli kilka MS-ów należących do tego samego HA, które jednocześnie zapisały się do tej samej grupy multicastowej porusza się do tego samego FA
- Również powoduje Problem conwergencji tunelowej, gdzie jeden FA może posiadać kilka MS-ów zapisanych do tej samej grupy, należących do różnych HA i każdy HA może forwardować pakiet dla swojego MS-a do tego samego FA

Duplikacja pakietów przy użyciu BT (bidirectional tunneling) podejścia



Problem konwergencji tunelowej

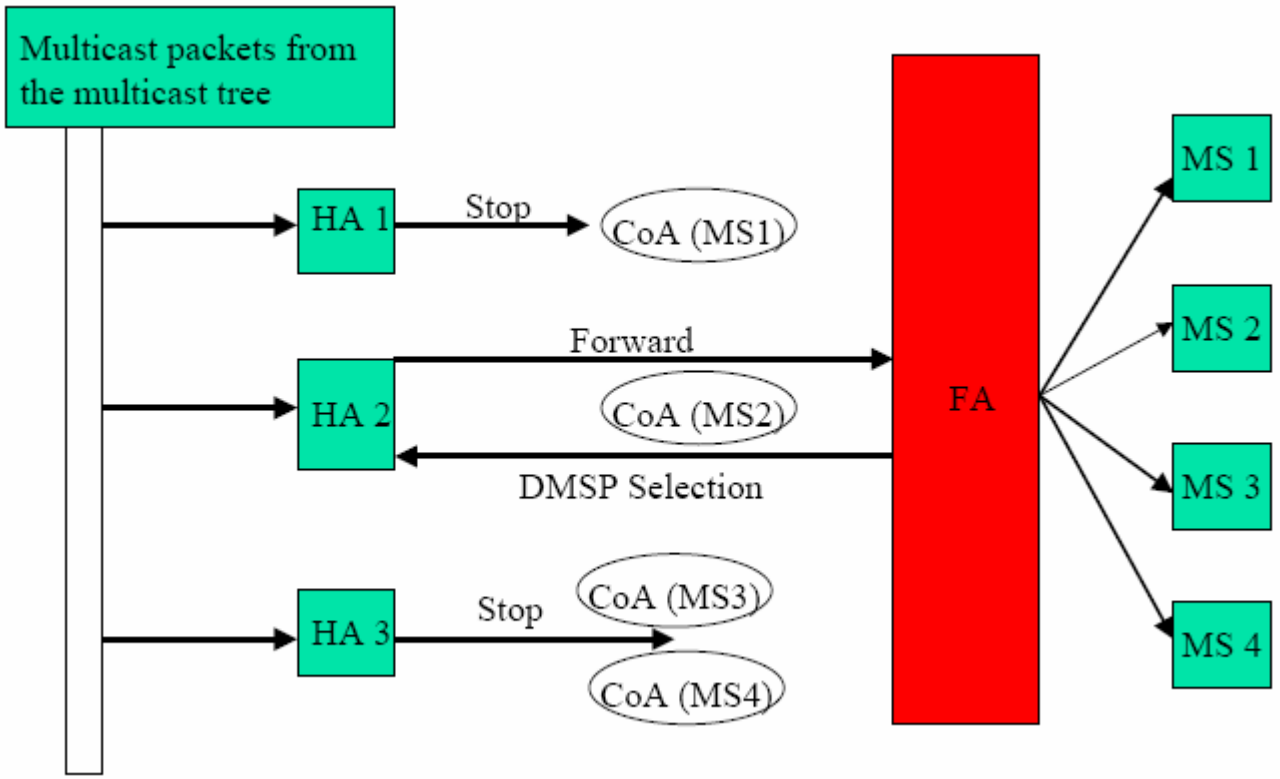




Multicasting

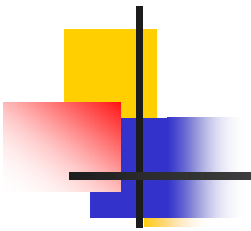
- W celu rozwiązania Problemu konwergencji tunelowej, zaproponowano protokół MoM, wg. którego FA wybiera spośród HA jednego HA dla poszczególnej grupy, nazywanego mianowanym prowajderem multicastowej obsługi
- Pozostałe HA nie forwardują pakietów do FA

Ilustracja protokołu MoM



Bezpieczeństwo i prywatność

- Transfer wiadomości w otwartym medium jakim jest przestrzeń powietrzna jest podatny na różne ataki
- Jednym z takich problemów jest „zagłuszanie” przez bardzo silną transmitującą antenę
- Problem można rozwiązać używając metody skakania po częstotliwościach w kolejnych odstępach czasu
- Używa się wielu technik szyfrowania, aby uniemożliwić nieautoryzowanym użytkownikom interpretację sygnałów



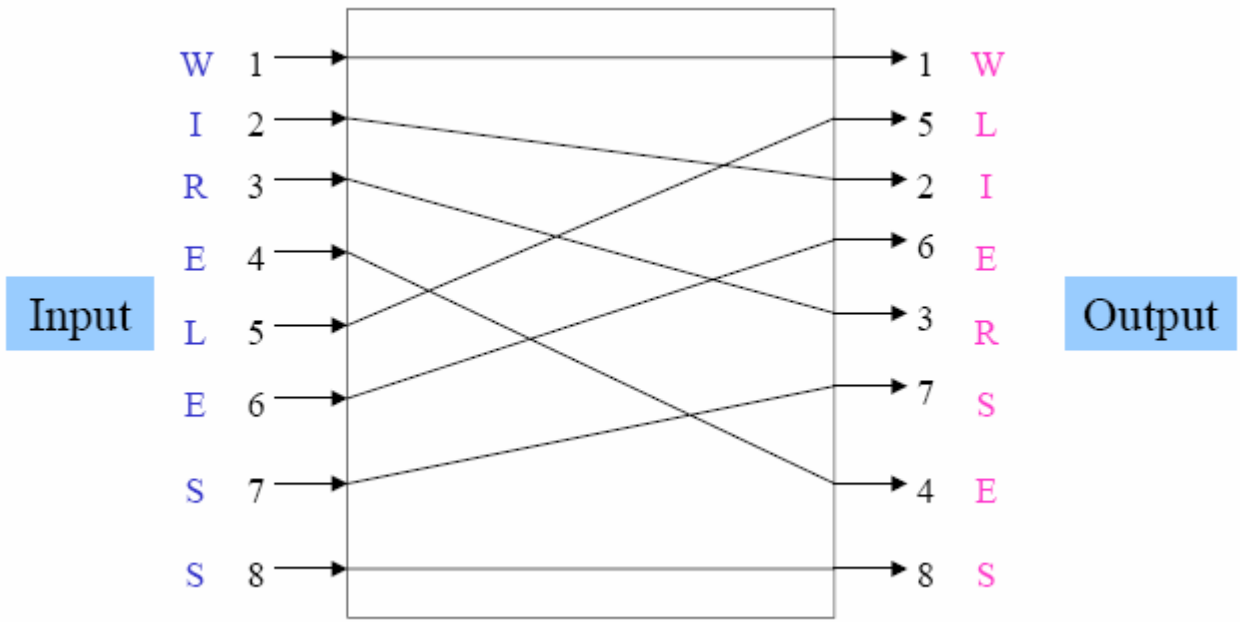
Dwie techniki szyfrowania

- Szyfrowanie z kluczem symetrycznym
  - Np. DES, AES
- Szyfrowanie z kluczem publicznym
  - np. RSA

Szyfrowanie z kluczem symetrycznym

- Permutacja bitów przed ich transmisją w uprzednio zdefiniowany sposób – jeden z elementów szyfrowania
- Taka permutowana informacja może być odtworzona z użyciem operacji odwracającej
- Jednym z takich algorytmów jest DES (Data Encrytption Standard)

Funkcja prostej permutacji



Bity informacji przed transmisją oraz po ich otrzymaniu z użyciem DES

57	49	41	33	25	17	9	1
61	53	45	37	29	21	13	5
58	50	42	34	26	18	10	2
62	54	46	38	30	22	14	6
59	51	43	35	27	19	11	3
63	55	47	39	31	23	15	7
60	52	44	36	28	20	12	4
64	56	48	40	32	24	16	8

(a) Permutation before transmission

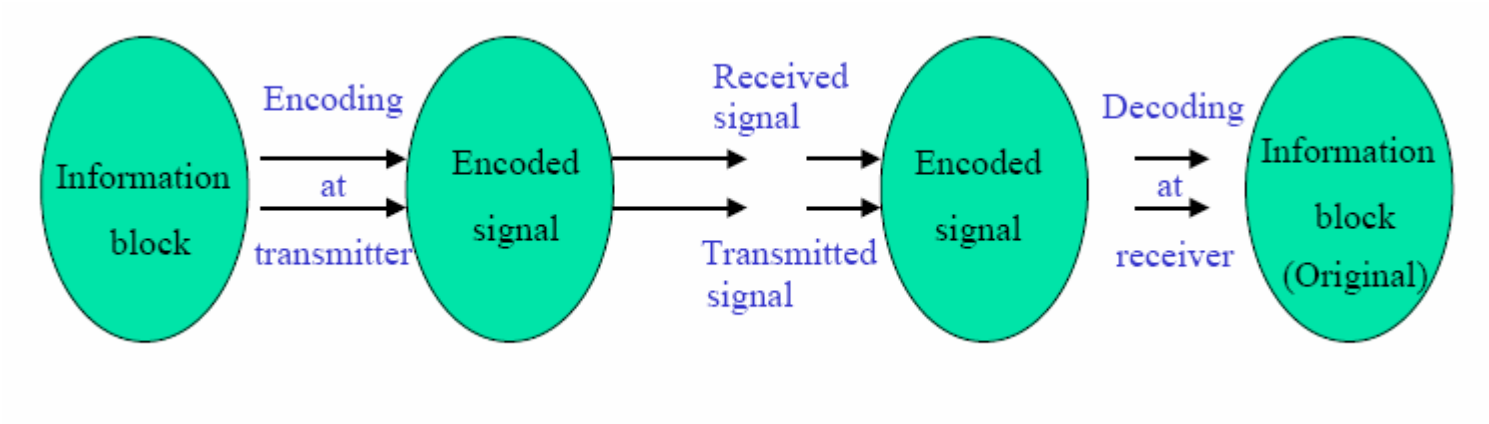
8	24	40	56	16	32	48	64
7	23	39	55	15	31	47	63
6	22	38	54	14	30	46	62
5	21	37	53	13	29	45	61
4	20	36	52	12	28	44	60
3	19	35	51	11	27	43	59
2	18	34	50	10	26	42	58
1	17	33	49	9	25	41	57

(b) Permutation after reception

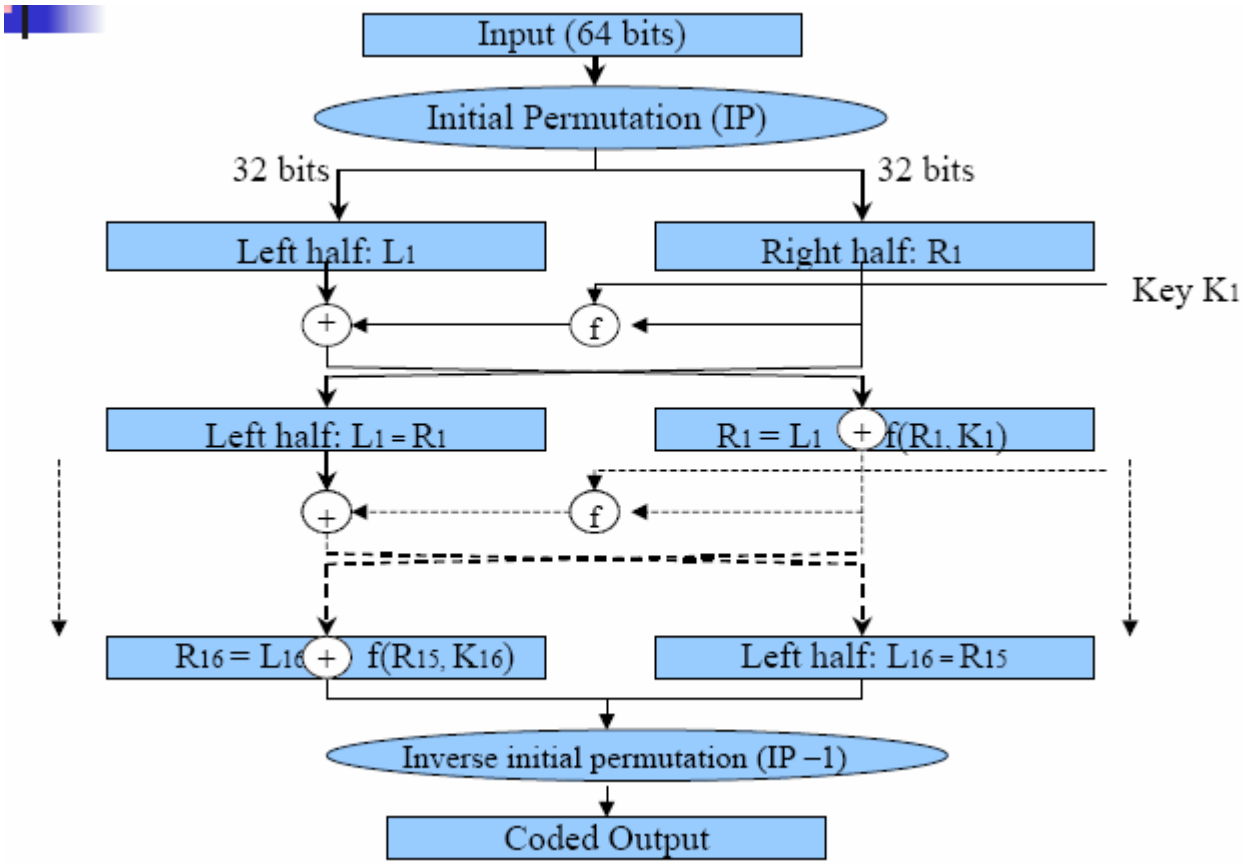
Szyfrowanie z kluczem symetrycznym

- Złożony schemat szyfrowania polega na transformacji bloków wejściowych w pewną zakodowaną formę
- Zakodowana informacja jest w sposób unikalny zamieniana na informację użyteczną
- Najprostsza tranformacja zakłada logiczną lub arytmetyczną operację lub obie operacje

Proces generyczny kodowania i dekodowania



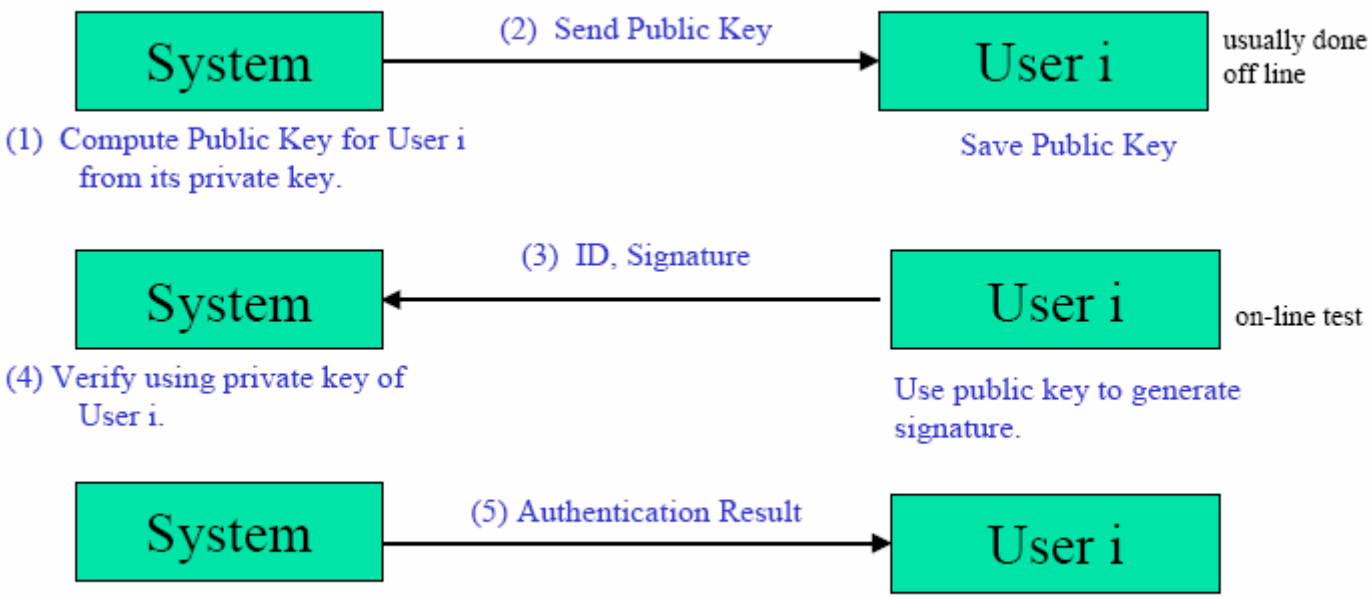
Permutacja i kodowanie informacji w DES



Uwierzytelnianie

- Ma na celu upewnienie się, że użytkownik jest autentyczny
- Używa się funkcji haszującej działającej na związanej z użytkownikiem unikalnym identyfikatorze (niepełny dowód)
- Inne podejście polega na użyciu dwóch związanych ze sobą kluczy (technika szyfrowania z kluczem publicznym)
- Jeden z nich znany jest tylko dla systemu generującego klucz (klucz prywatny), drugi klucz jest używany przy wysyłaniu do świata zewnętrznego (klucz publiczny)
- Algorytm RSA – najbardziej znany system z kluczem publicznym

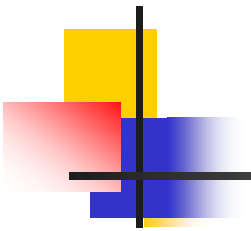
Kroki uwierzytelnienia klucza publicznego/prywatnego



Uwierzytelnianie (Algorytm RSA)

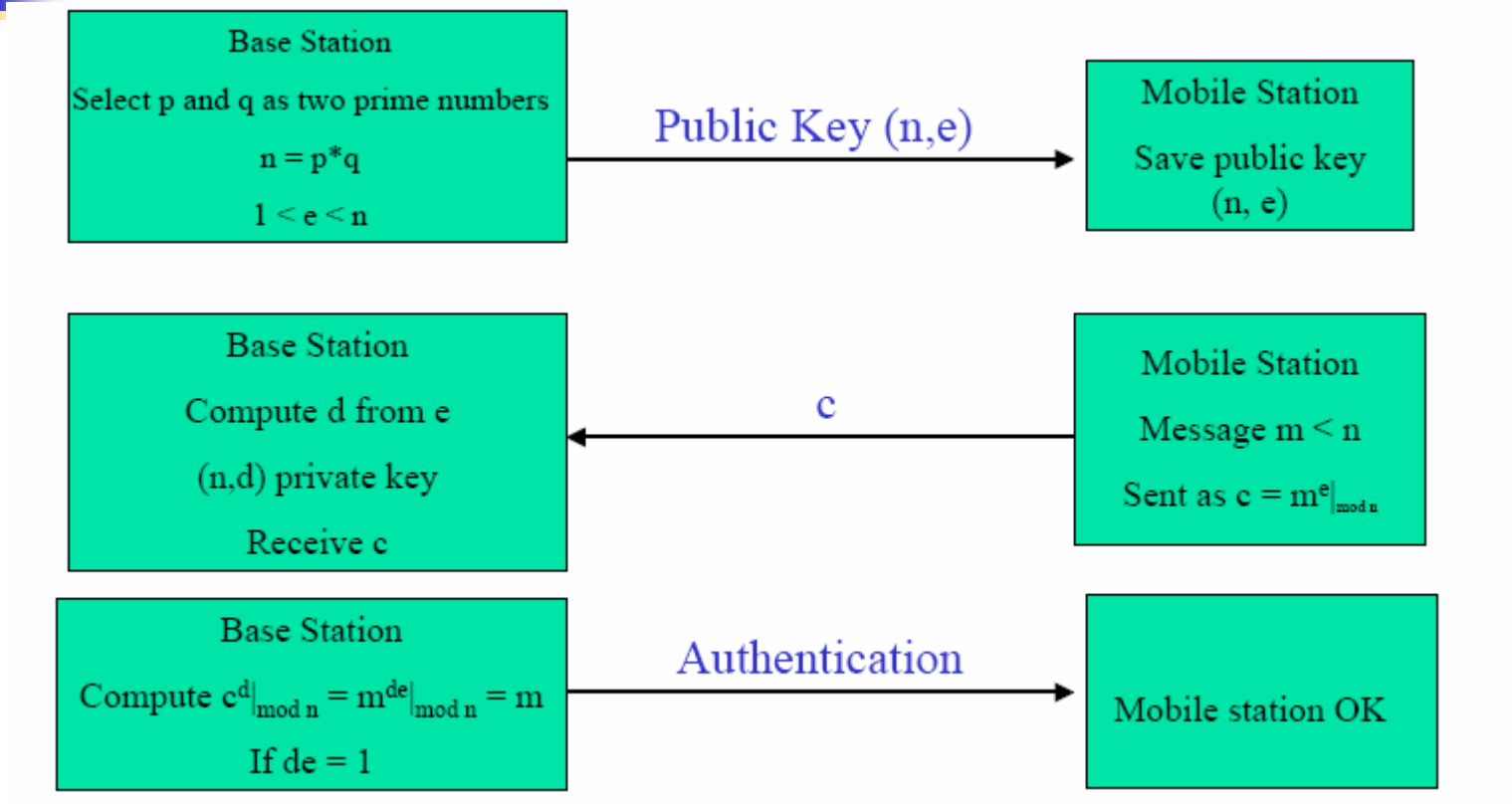
- W algorytmie RSA 2 duże liczby pierwsze *(p, q)* są wybierane; *n=p*q*; wybiera się liczbę *e* w celu użycia (n,e) jako klucza publicznego i jest ona wysyłana do użytkownika.
- Użytkownik przechowuje ją i kiedykolwiek wiadomość *m<n* ma być wysłana, użytkownik oblicza $c^d|_{mod\ n}$ i wysyła do systemu. Po otrzymaniu c system oblicza $c = m^e|_{mod\ n}$ gdzie *d* jest obliczane na podstawie klucza prywatnego *(n,e)*

$$c^d|_{mod\ n} = (m^e|_{mod\ n})^d|_{mod\ n} = (m^e)^d|_{mod\ n}$$
$$= m^{ed}|_{mod\ n}$$

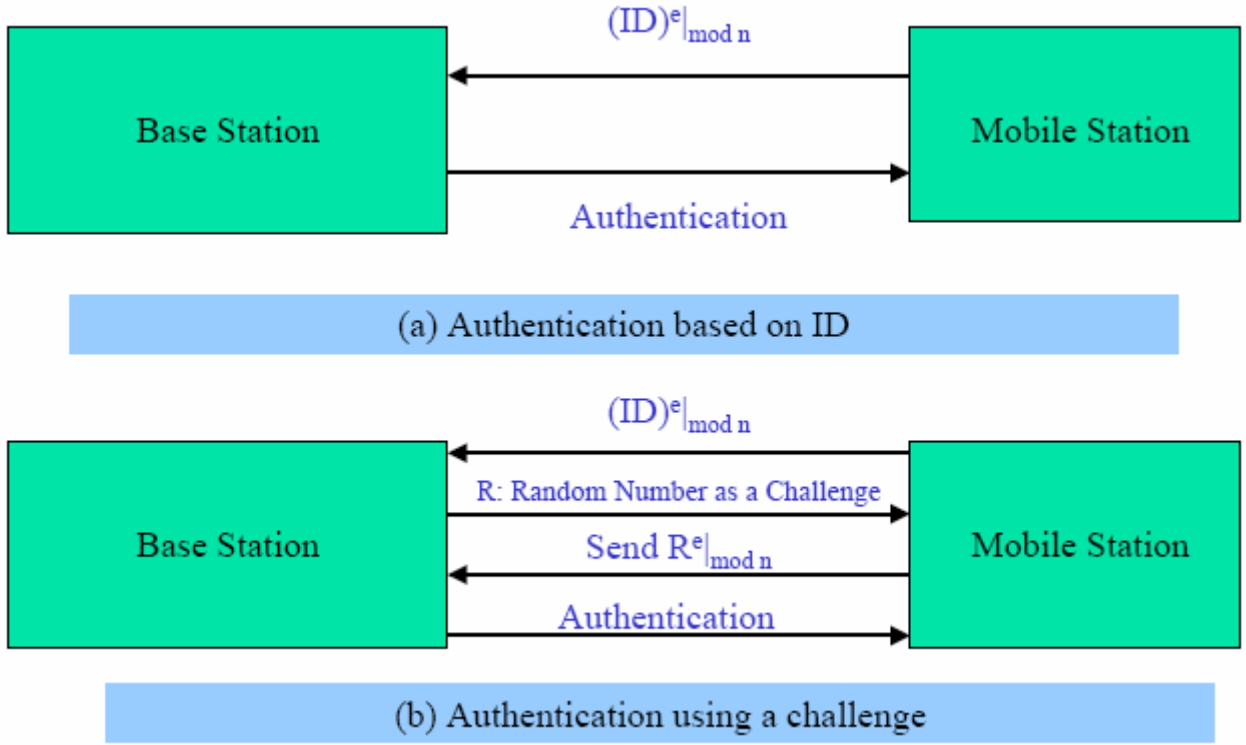


- Aby miało to wartość równą *m, ed* musi być równe 1
- To oznacza, że *e* oraz *d* muszą być .. mod *n* (lub mod *p*q*)
- To może być spełnione jeżeli e jest liczbą pierwszą w stosunku do *(p-1)*(q-1)*
- Korzystając z tej zależności można uzyskać oryginalną wiadomość

Uwierzytelnianie wiadomości przy użyciu klucza publicznego/prywatnego



Uwierzytelnianie MS-a przez BS



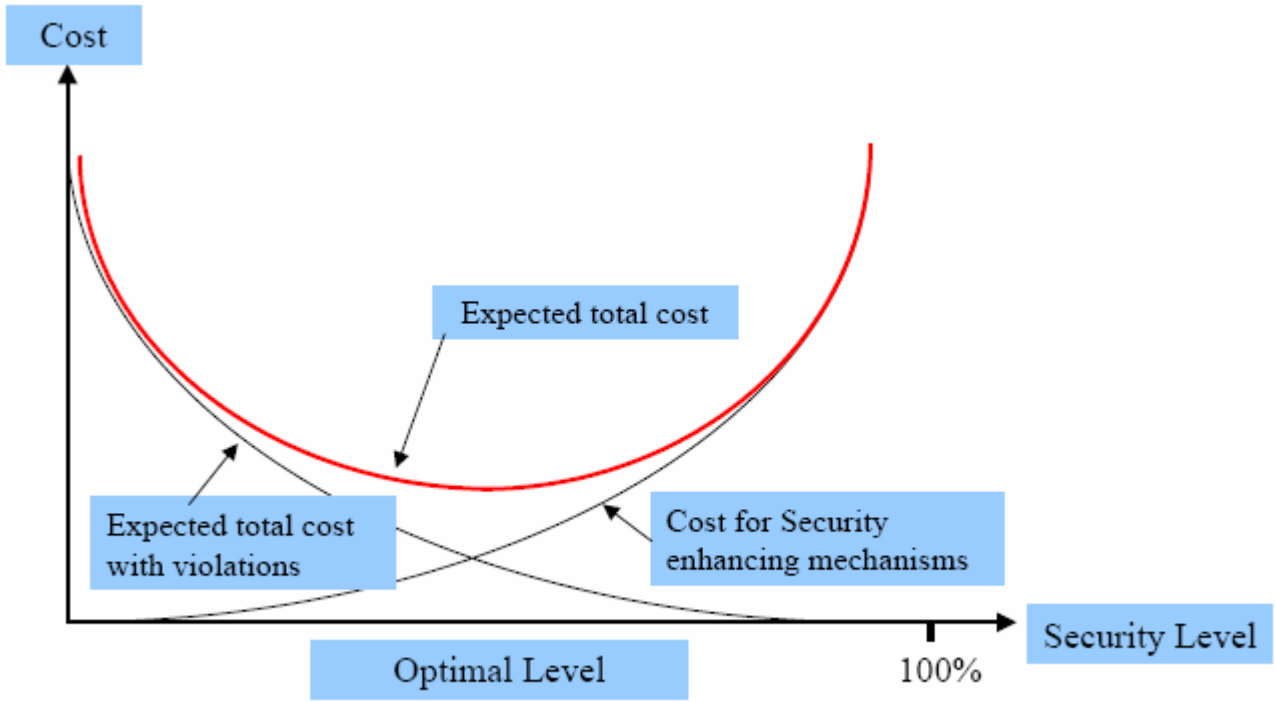
Bezpieczeństwo systemów bezprzewodowych

- Podstawowe usługi bezpieczeństwa:
  - Poufność: tylko autoryzowana strona może mieć dostęp do informacji systemu oraz transmitowanych danych
  - Niezaprzeczalność: nadawca i odbiorca nie mogą mogą zaprzeczyć, że transmisja się odbyła
  - Uwierzytelnienie: nadawca informacji jest prawidłowo identyfikowany
  - Integralność: zawartość wiadomości może być modyfikowana tylko przez autoryzowanego użytkownika
  - Dostępność: zasoby są dostępne tylko dla autoryzowanych użytkowników

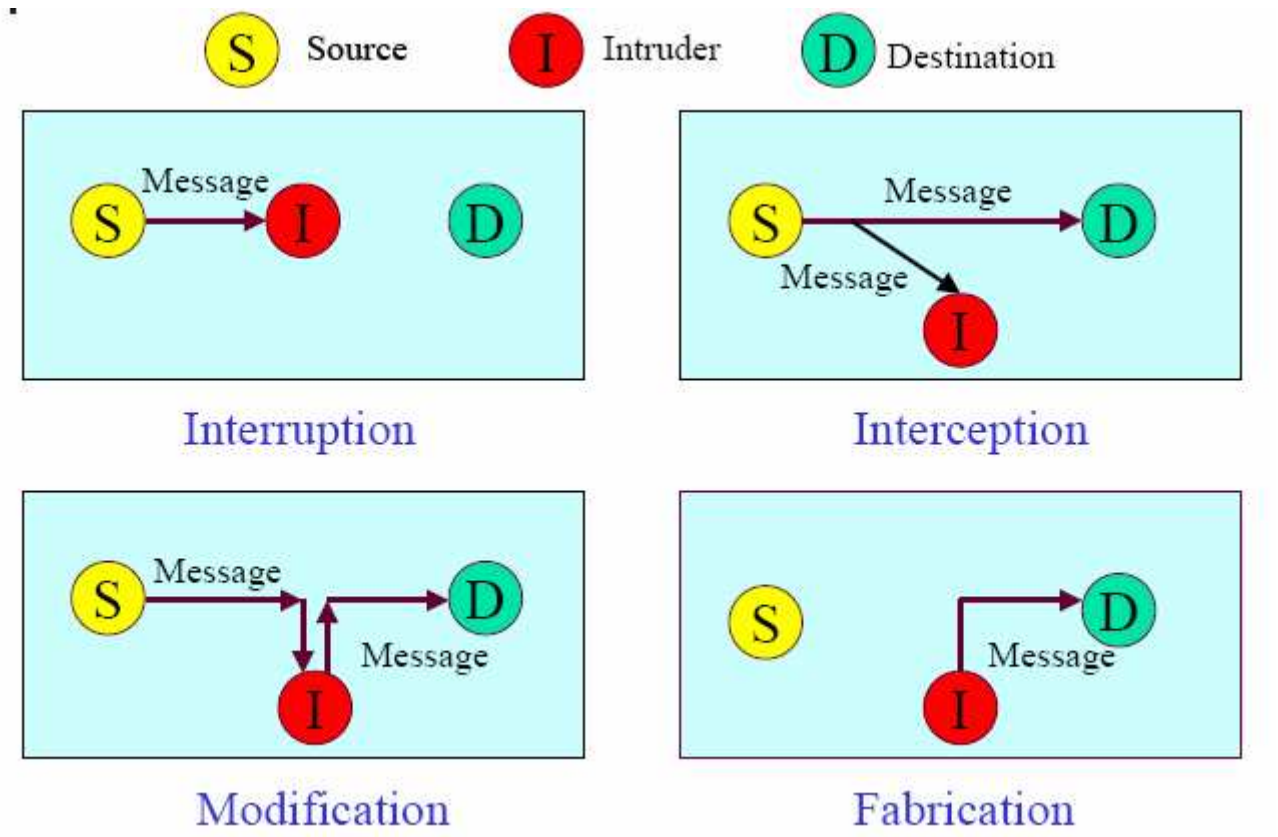
Bezpieczeństwo systemów bezprzewodowych

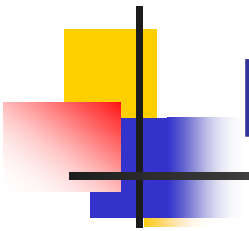
- Mechanizmy bezpieczeństwa:
  - Prewencja bezpieczeństwa: wymusza bezpieczeństwo w czasie funkcjonowania systemu
  - Detekcja bezpieczeństwa: odkrywa próby naruszenia bezpieczeństwa
  - Odtworzenie: odtwarzanie systemu do stanu przed naruszeniem bezpieczeństwa

Funkcja kosztu bezpiecznego systemu bezprzewodowego



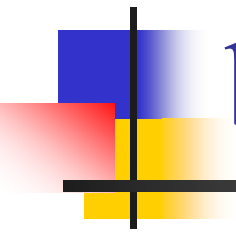
Kategorie zagrożeń bezpieczeństwa (typy ataków)





Bezpieczeństwo bezprzewodowe

- **Ataki aktywne**: gdy ma miejsce modyfikacja danych lub fałszywa transmisja danych
  - Maskarada: dany podmiot pretenduje bycie innym podmiotem
  - Replay: przechwycenie informacji i jej retransmisja w celu wywołania nieautoryzowanego efektu
  - Modyfikacja wiadomości
  - Odmowa usługi (Denial of service – DoS)
- **Pasywne ataki**: celem intruza jest uzyskanie informacji (monitorowanie, podsłuchiwanie transmisji)



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/s0 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 mozliwość 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 umożliwiaja pracę w obu zakresach

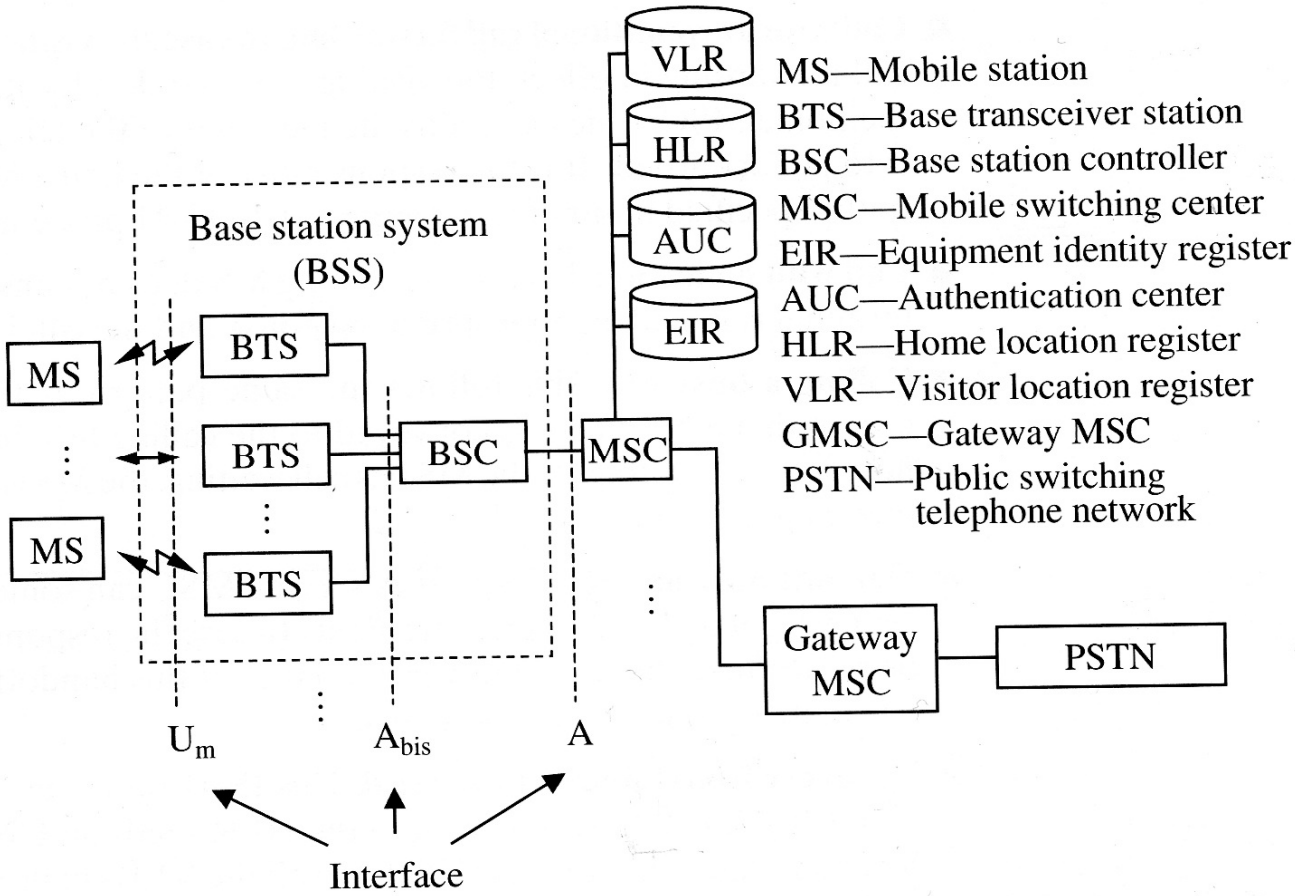
GSM: główne założenia standardu

- Opierano się na doswiadczeniach 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

Infrastruktura 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

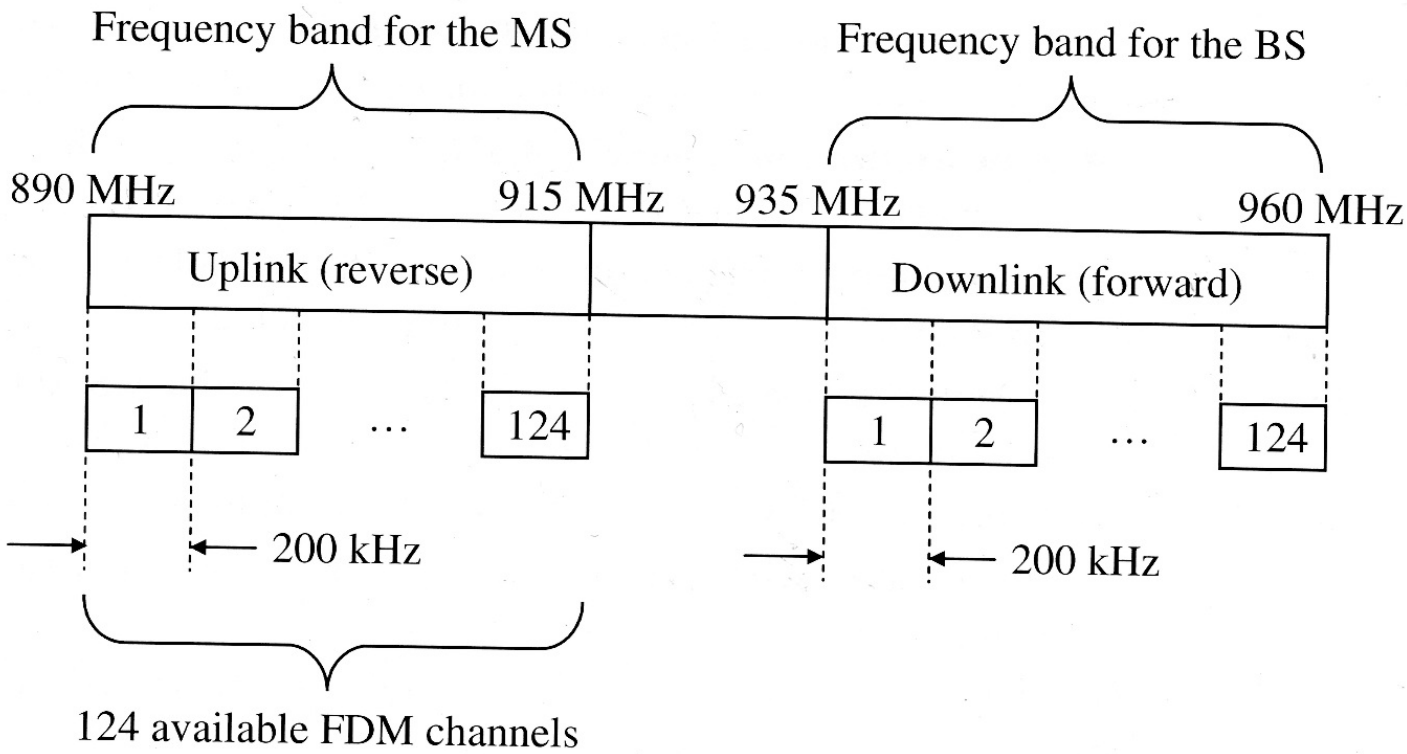
EIR (Equipment identity register)

- Jest to baza danych, która zawiera informację 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)

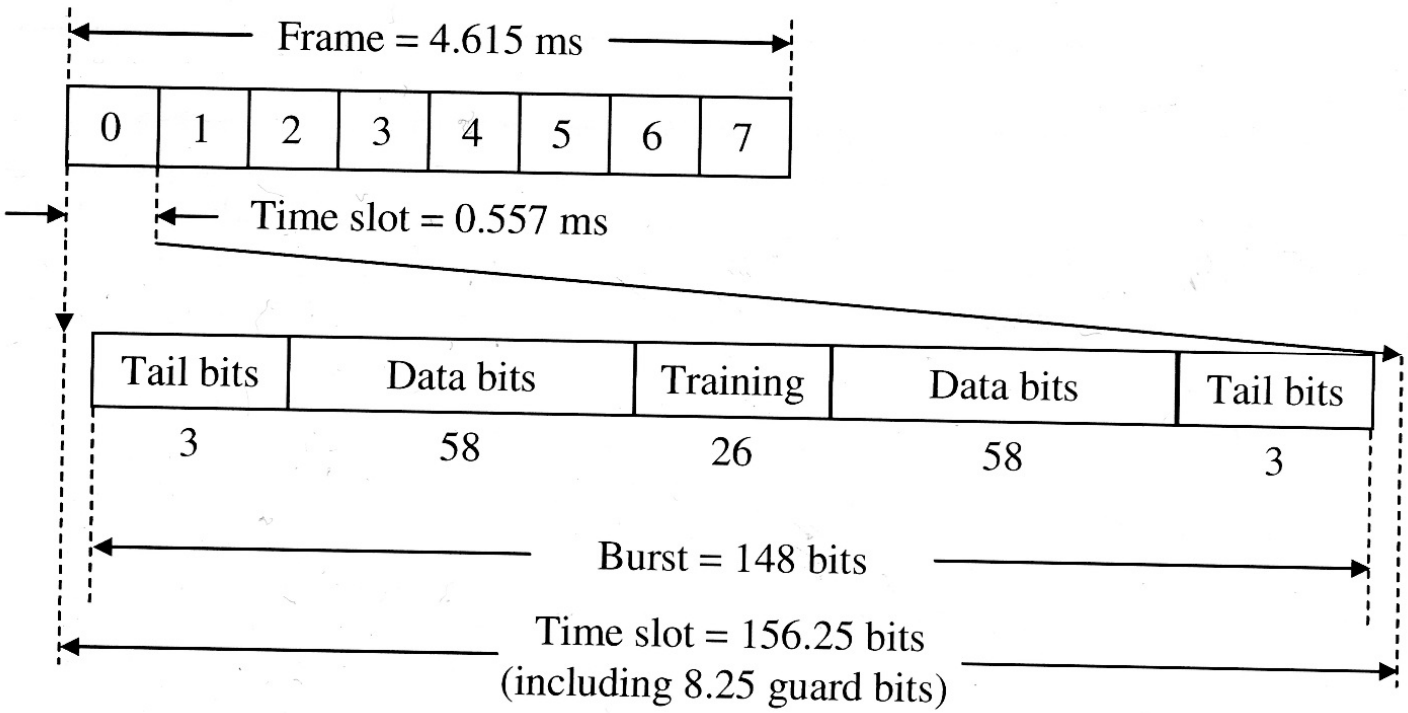
Zakresy częstotliwości (FDMA) i kanały fizyczne



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-kanał (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

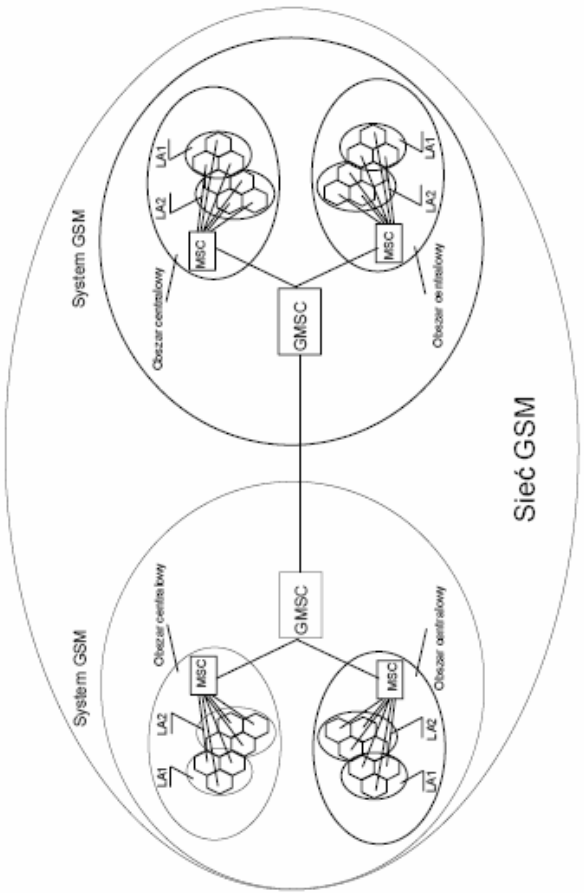
Grupa kanałów sterujących CCCH

- 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 uzyciem 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 sterujacego FACCH transmitujacego 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 któreg:
  - 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

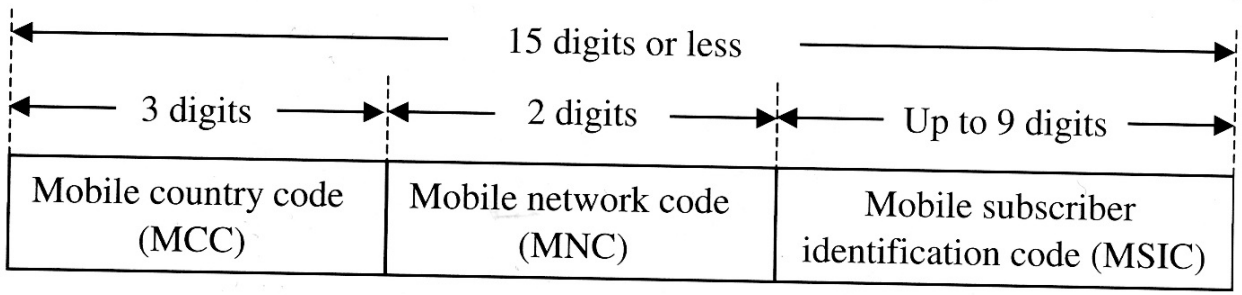
System numeracji stosowany w sieci GSM

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 ≠ droga połączenia,
• różne numery dla usług, • różne numery dla różnych grup użytkowników

MSISDN – numer międzynarodowy abonenta sieci ISDN: MSISDN =kraj + operator + abonent
• nr katal.użytk.,• rozumiany w całej sieci,• określa typ dostępnej usługi, a nie terminal,
• w HLR numer MSISDN → MISI,• zgodny z numeracją w sieci ISDN.
IMSI – numer międzynarodowy abonenta ruchomego (użytk.): 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.połącz.): 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
IDEI – 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 abonena 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 szczegolności uzyskuje się w info o PLMN (home public Land Mobile Network) danego użytkownika

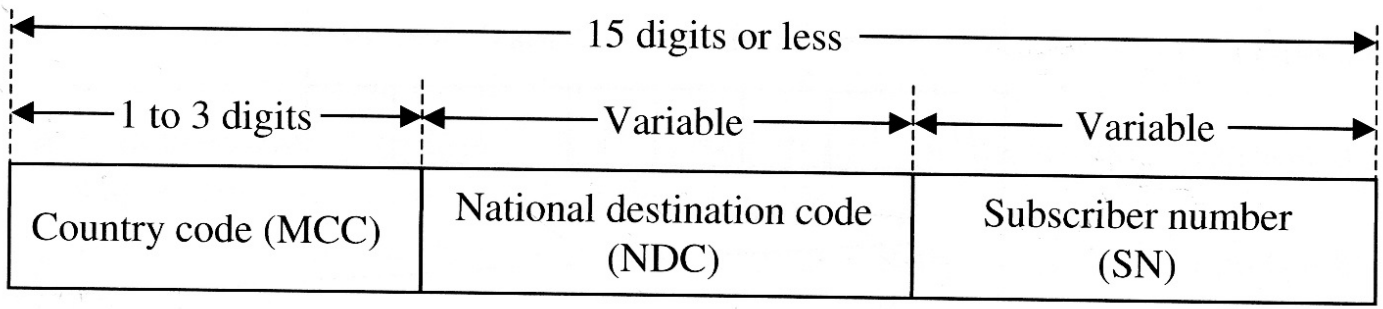


Numery identyfikujące użytkownika: SIM

- 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 rownież pamięć umożliwiającą przechowywanie krótkich wysyłanych wiadomości
- Umożliwia roaming (tzw. SIM roaming) z telefonem lub bez niego

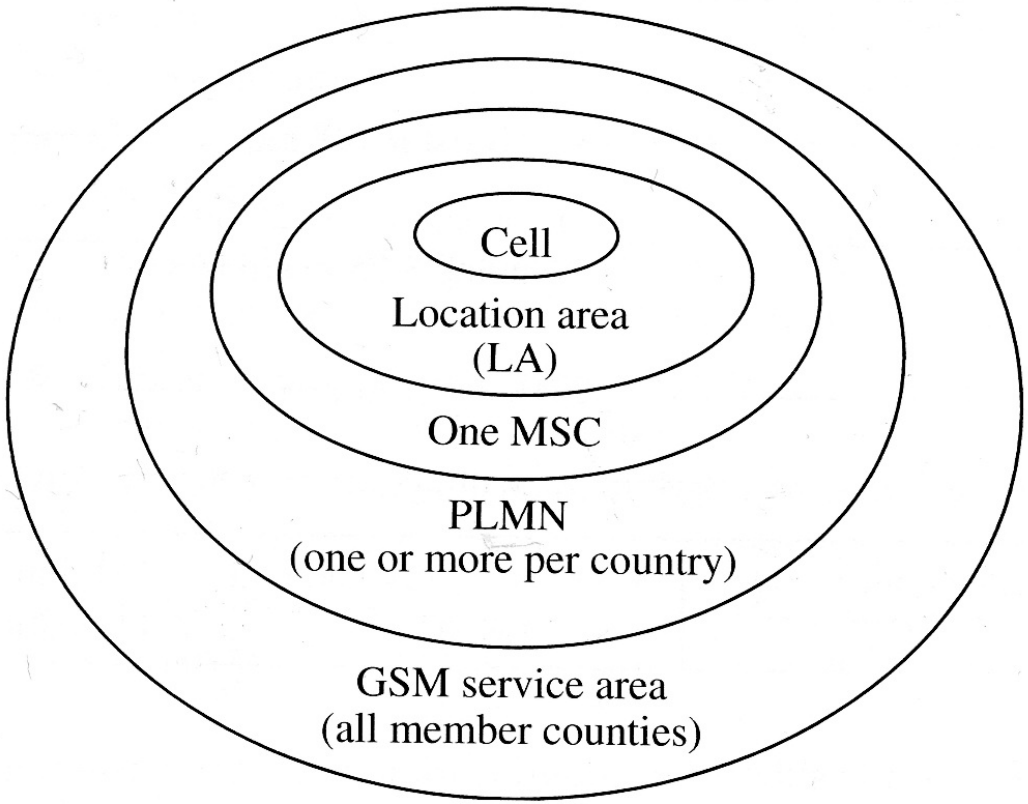
Numery identyfikujące użytkownika: MSISDN

- 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



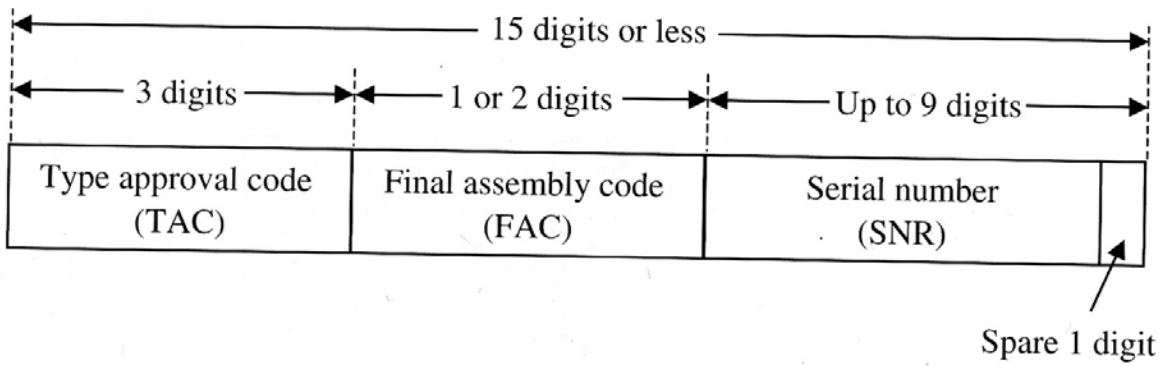
Numery identyfikujące użytkownika: LAI

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



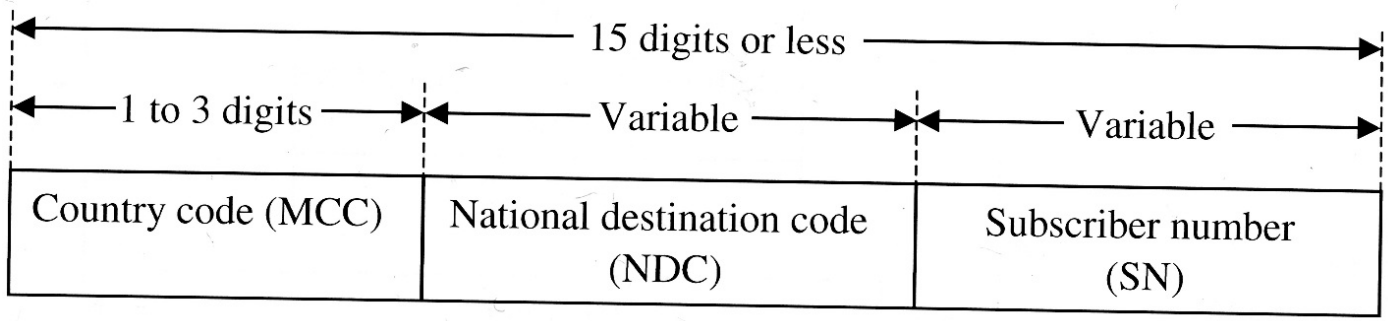
Numery identyfikujące użytkownika: IMSEI

- 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 zwiekszyć 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 ≠ droga połączenia,
• różne numery dla usług, • różne numery dla różnych grup użytkowników

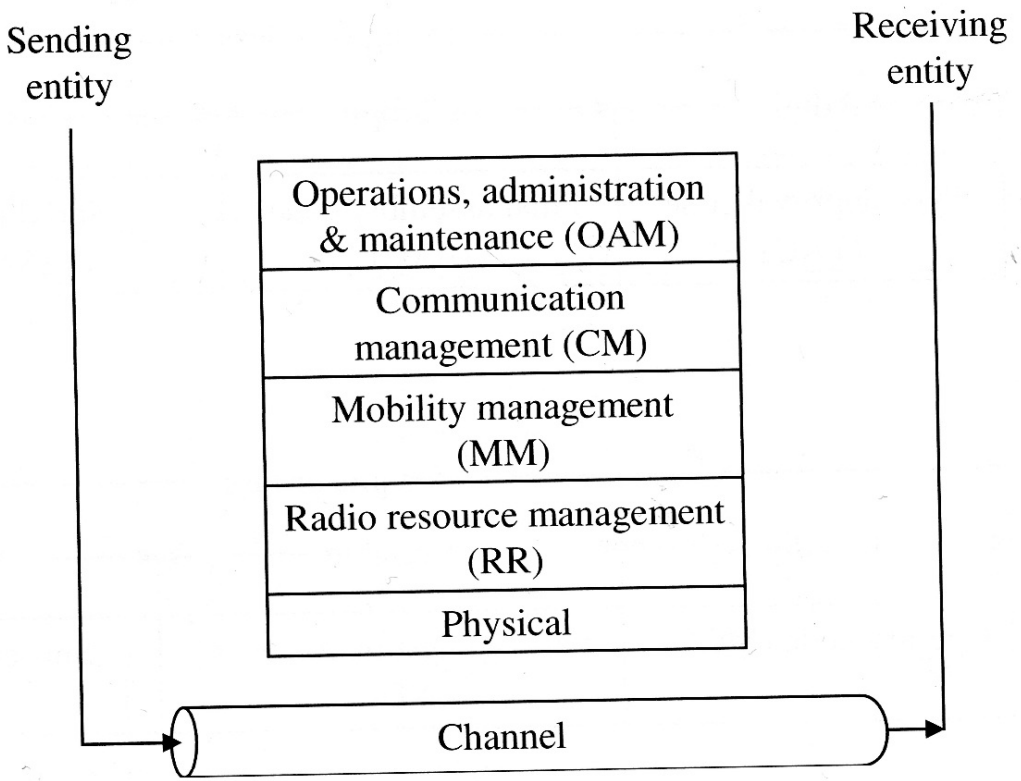
MSISDN – numer międzynarodowy abonenta sieci ISDN: MSISDN =kraj + operator + abonent
• nr katal.użytk.,• rozumiany w całej sieci,• określa typ dostępnej usługi, a nie terminal,
• w HLR numer MSISDN → MISI,• zgodny z numeracją w sieci ISDN.
IMSI – numer międzynarodowy abonenta ruchomego (użytk.): IMSI =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.połącz.): 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
IDEI – 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 abonena 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”.

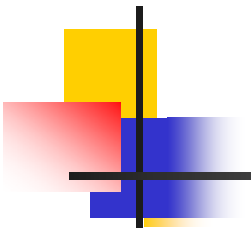
Interfejsy GSM

- 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

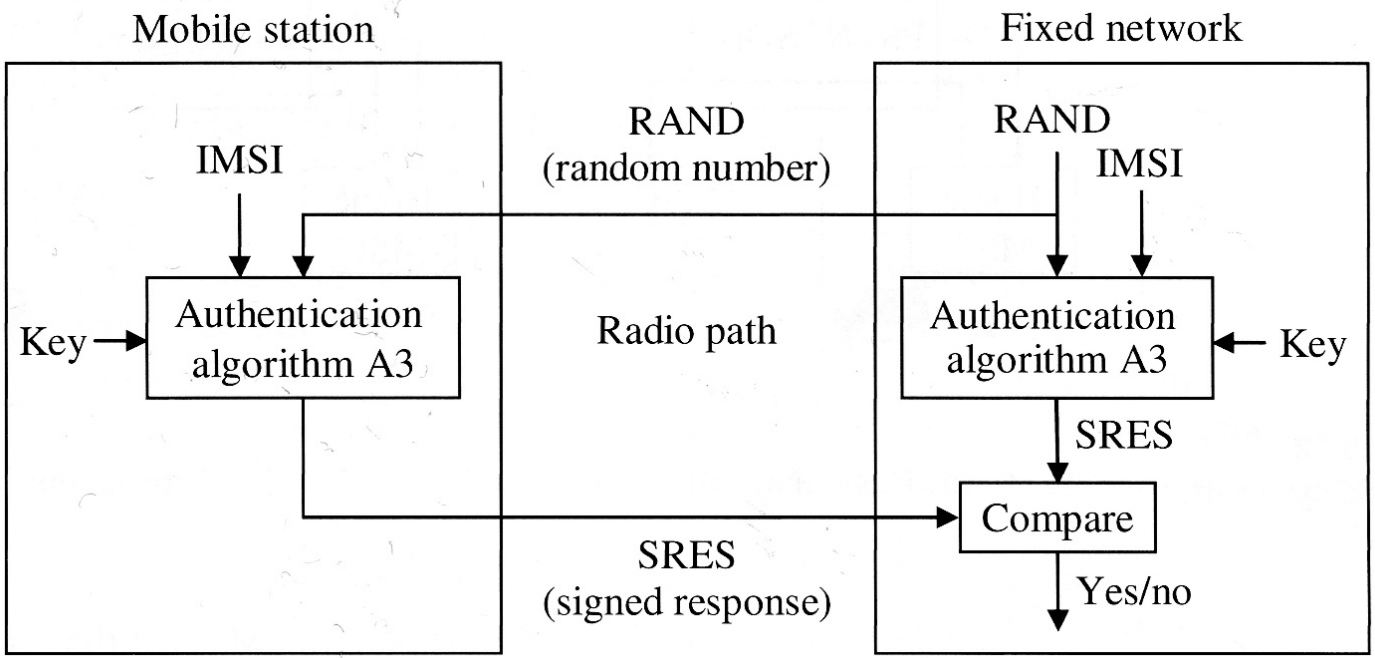
Uwierzytelnienie w GSM

- 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



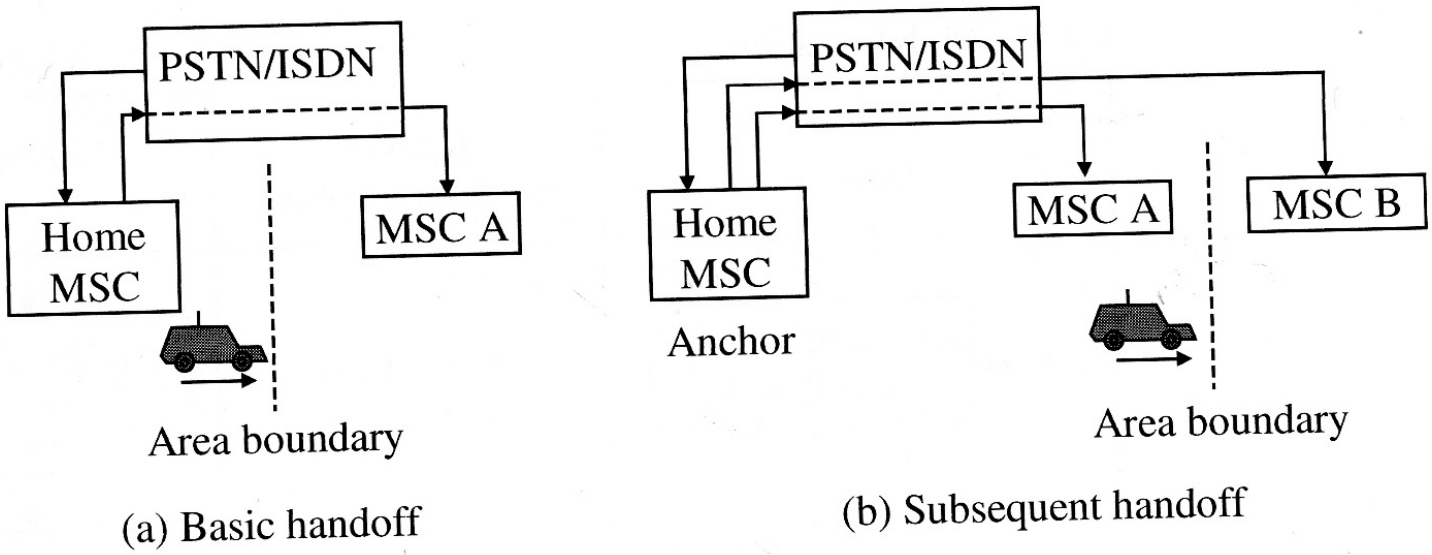
Przeniesienie połączenia

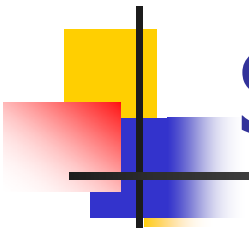
- W GSM istnieją cztery kategorie przeniesienia połączenia
- Wewnątrz komórki/wewnątrz BTS (np. z powodu wysokiej interferencji)
  - Następuje zmiana częstotliwości w tej samej komórce lub zmiana szczeliny czasowej
- Międzykomórkowy/wewnątrz BTS
  - Następuje zmiana kanału między dwoma komórkami zarządzanymi 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





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