

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)

Domowy
telefon



PSTN

MSC

...

MSC

BSC

...

BSC

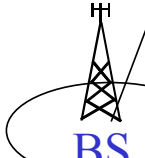
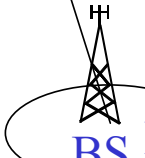
BSC

...

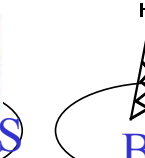
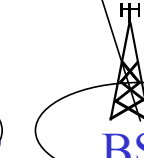
BSC



...



...



...



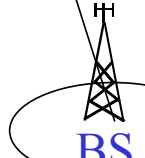
...



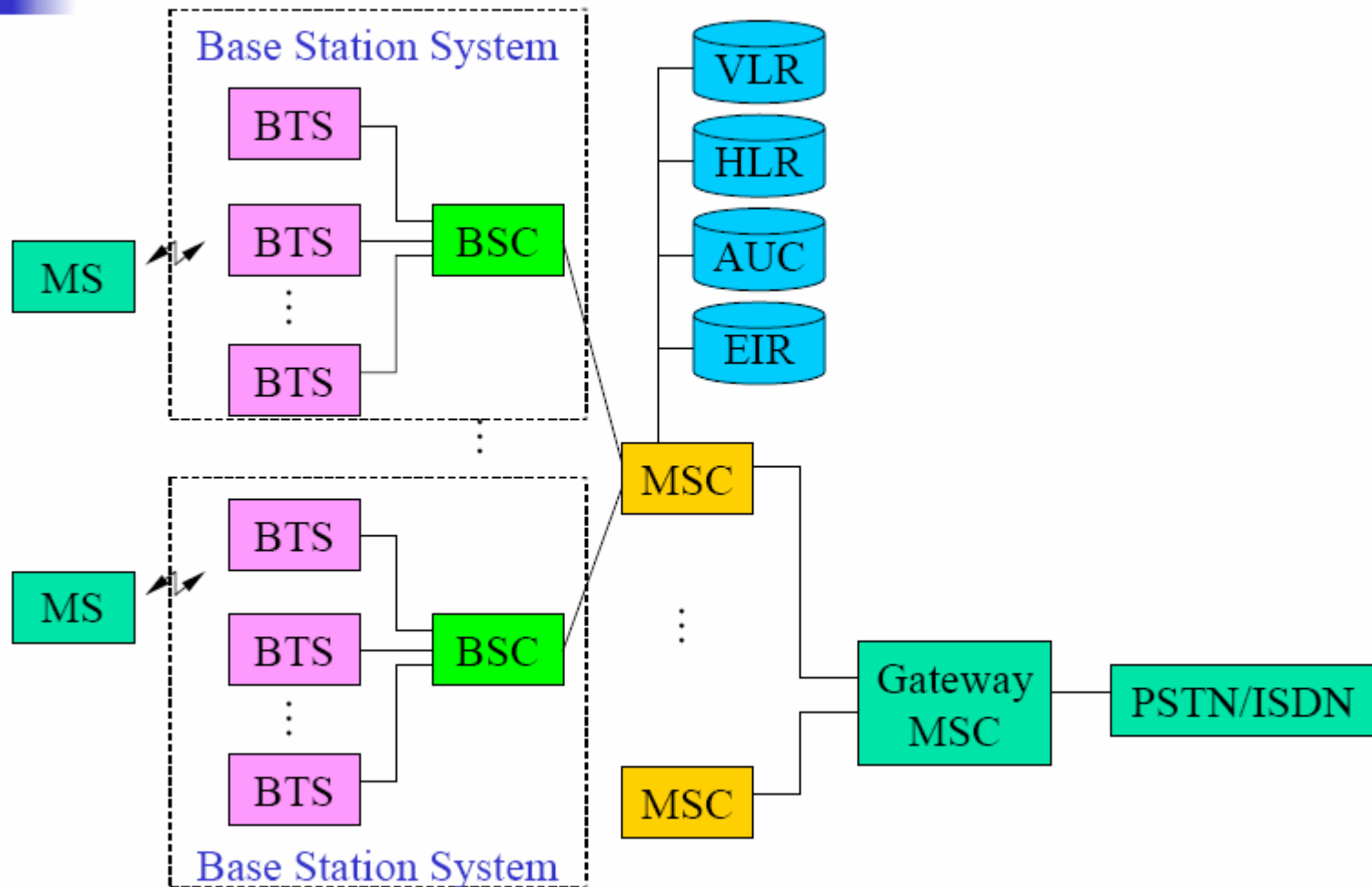
...



...



System komórkowy

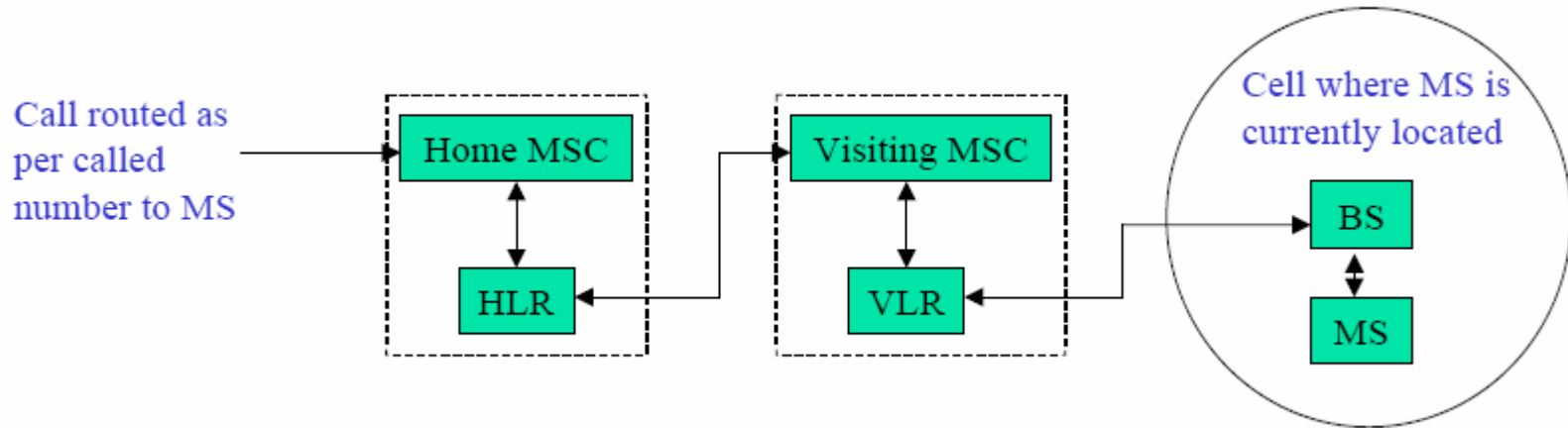




VLR/HLR

- 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

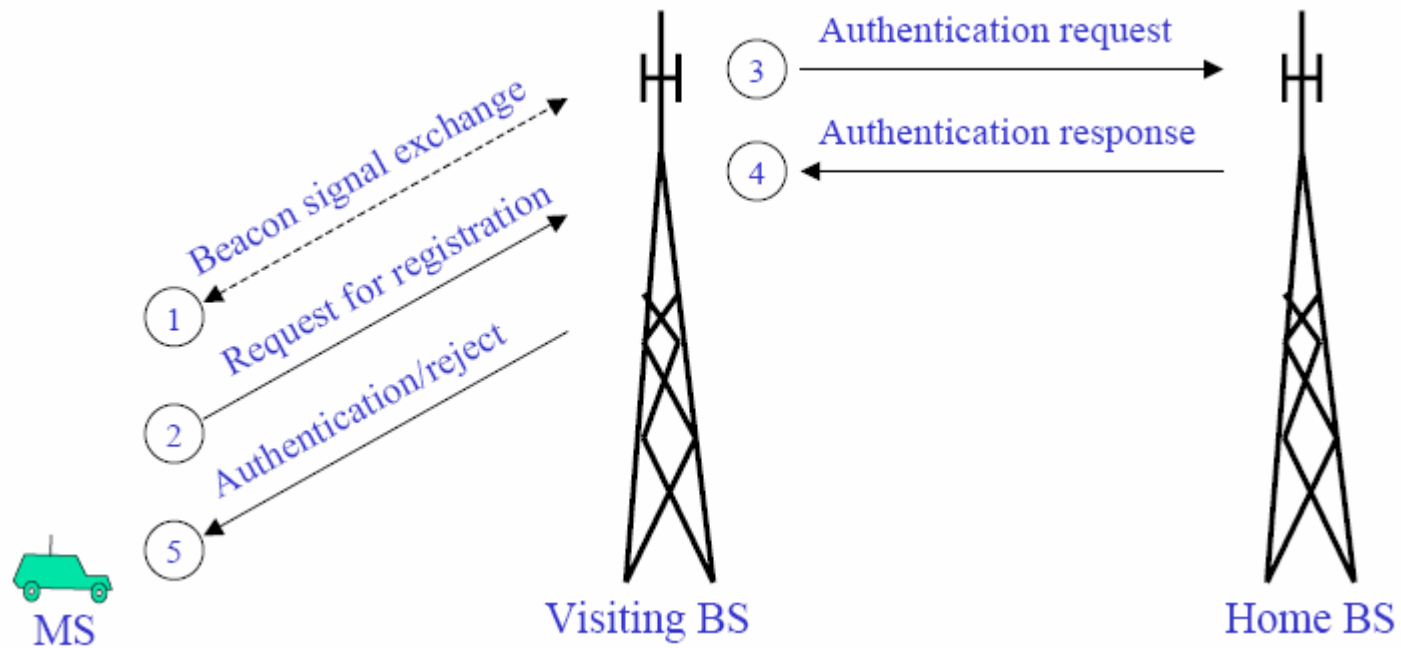




Rejestracja

- System bezprzewodowy musi wiedzieć czy MS w danej chwili znajduje się 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 sygnałowe); 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, identyfikator 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 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 nastąpić 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 połączeń generowanych w komórce
 - Liczby połączeń transferowanych z sąsiednich komórek przez przeniesienie połączenia
 - Liczby i długości połączeń zakończonych w komórce
 - Liczby połączeń, które były przeniesione do sąsiednich komórek
 - Liczby aktywnych połączeń w komórce
 - Wielkości populacji w komórce
 - Całkowitego czasu trwania połączenia w komórce
 - Czasu pojawienia się połączenia w komórce
 - Itp.



Przeniesienie połączenia (cd.)

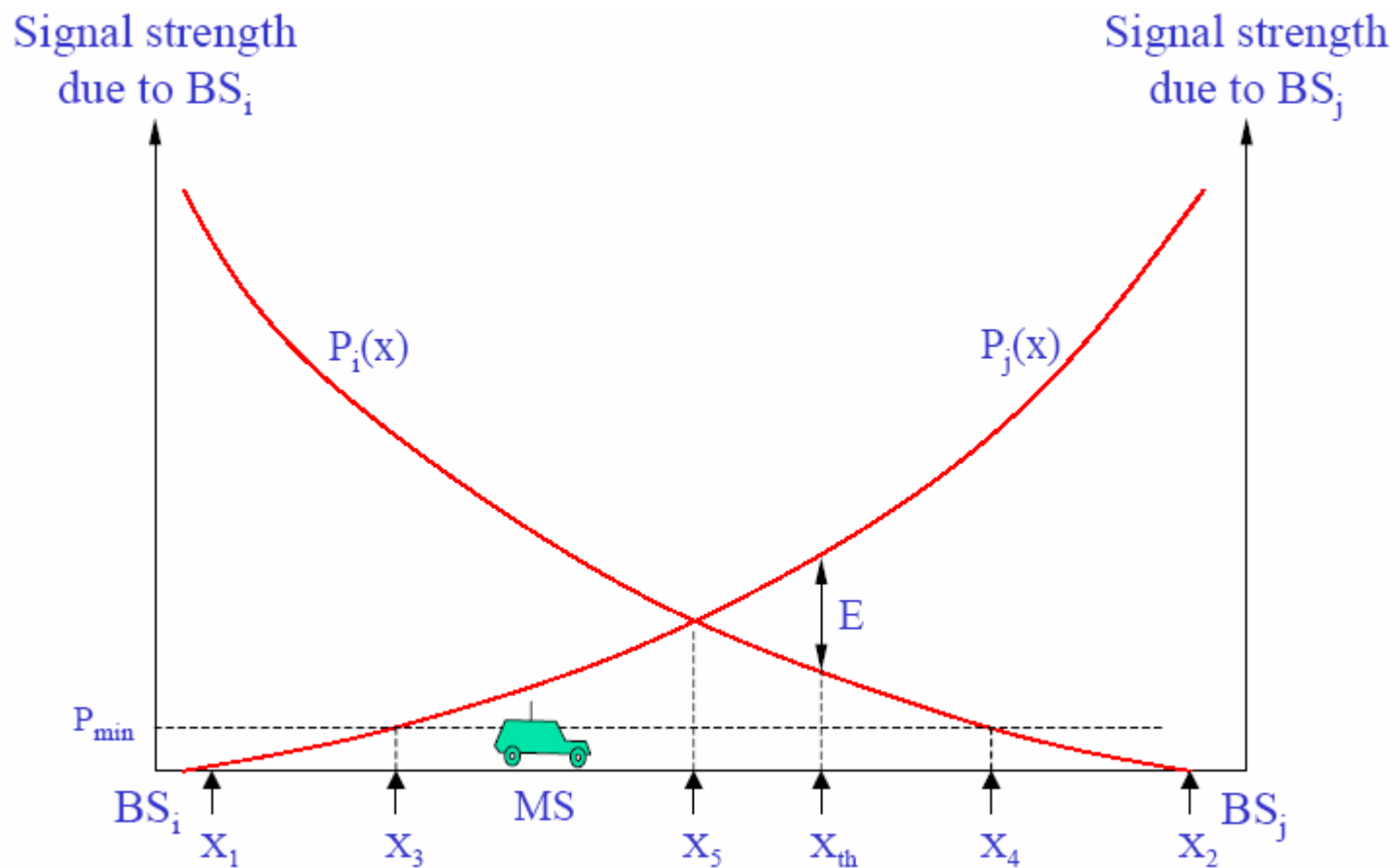
- System zarządzania siecią może spowodować przeniesienie połączenia jeżeli pojawi się drastyczne niezbalansowanie obciążenia w przyległych komórkach i wymagane jest optymalne zbalansowanie zasobów
- Przeniesienie z powodu obsługi jest powodowane degradacją jakości obsługi (QoS)

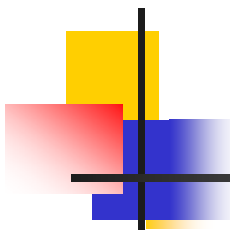


Wybór czasu przeniesienia połączenia

- Czynniki, 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.)

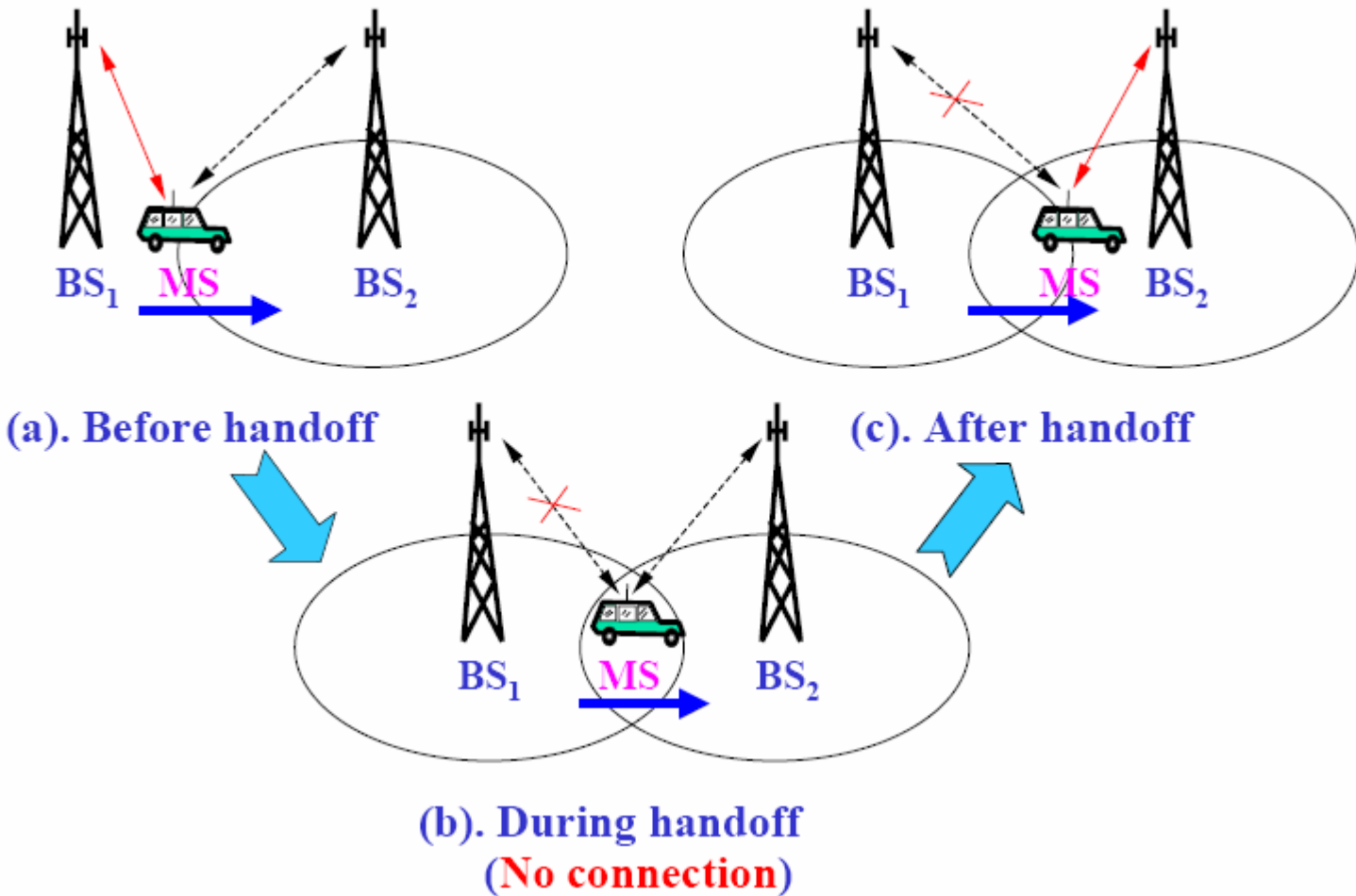
- Region X_3 - X_4 jest regionem gdzie w zależności od innych czynników przeniesienie połączenia może nastąpić
- Jedną z możliwości przeniesienia połączenia jest jego realizacja w X_5 , gdzie siły obu sygnałów są równe
- Jeżeli MS porusza się do tyłu i do przodu wokół X_5 , to wynikiem tego będą często wykonywane przeniesienia połączenia (**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



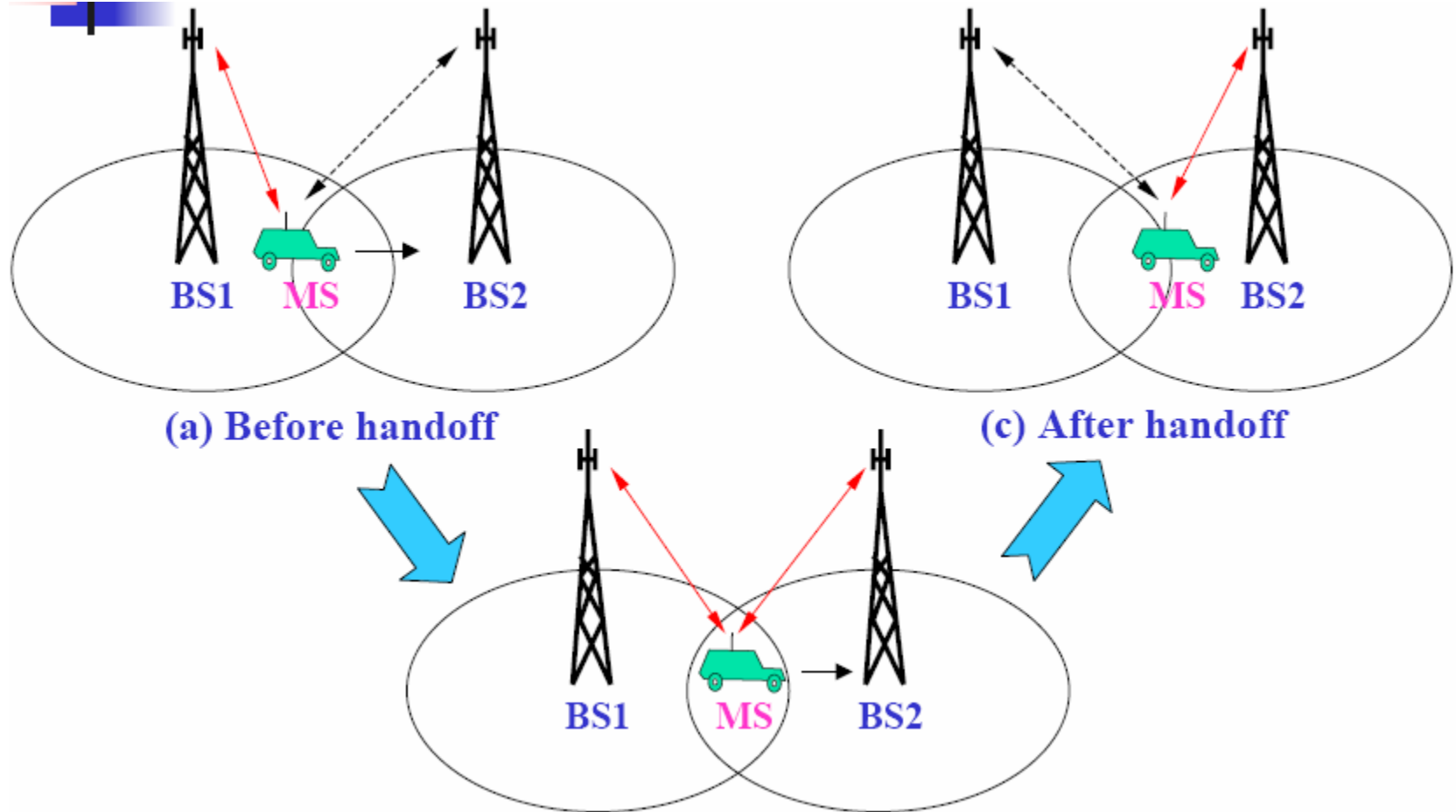
Typy przeniesienia połączenia

- 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 połączenia jeżeli ten kod nie jest ortogonalny do kodu w następnym BS
 - Dlatego, jest możliwe aby MS komunikował się jednocześnie z danym BS oraz z nowym BS

Twarde przeniesienie połączenia



Miękkie przeniesienia połączenia (tylko dla CDMA)

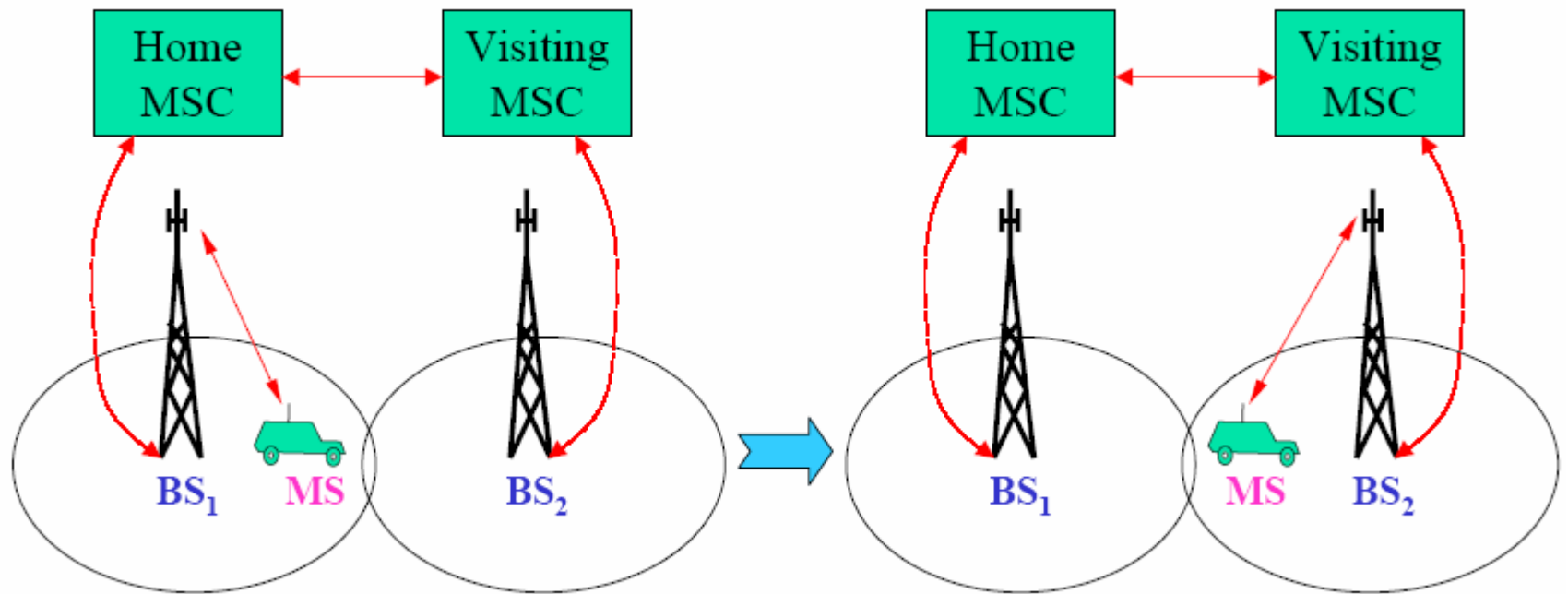




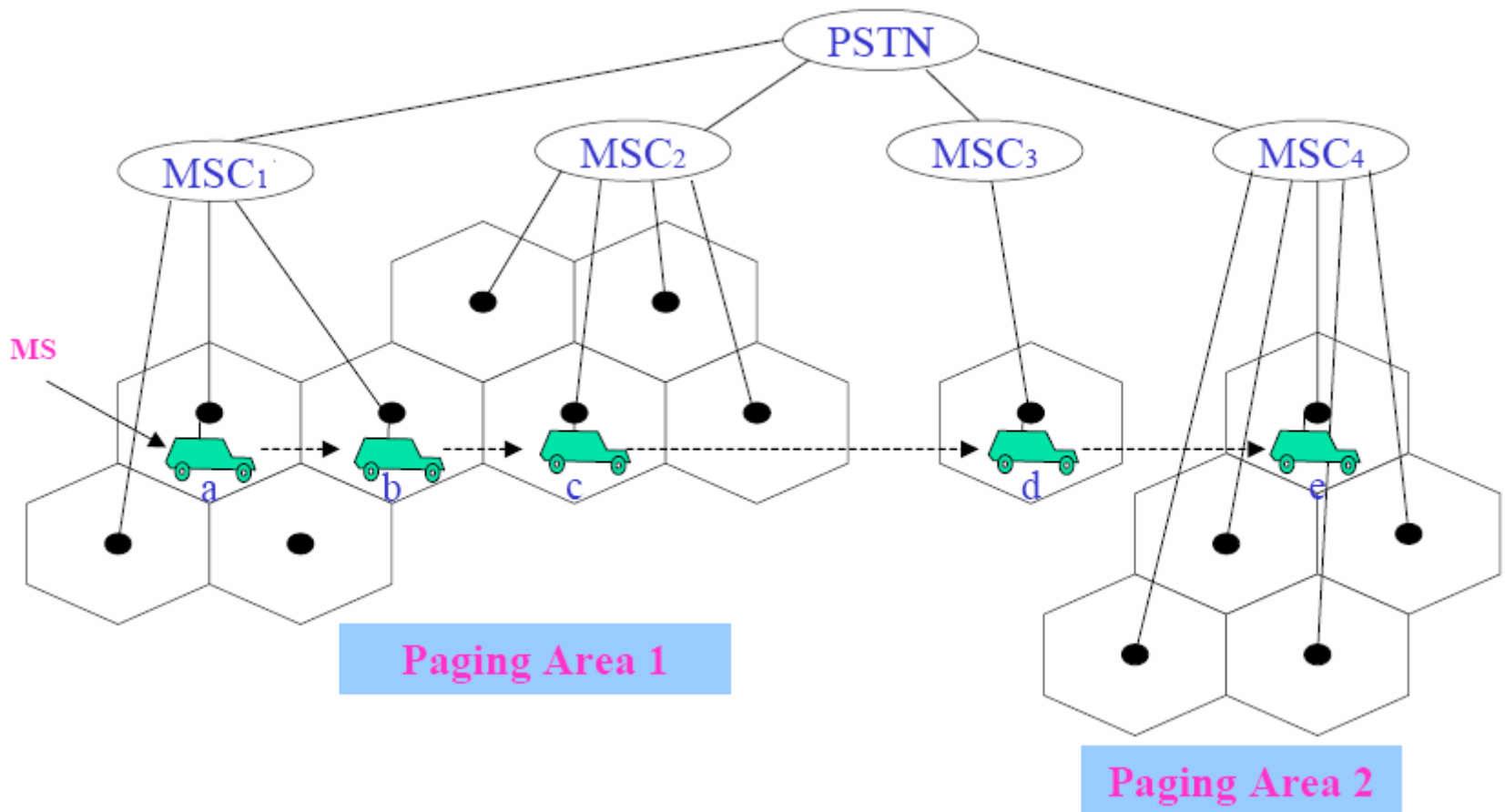
Roaming

- Odbywa się gdy MS przechodzi z komórki znajdującej się 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



Scenariusze przeniesienia połączenia przy różnych stopniach mobilności

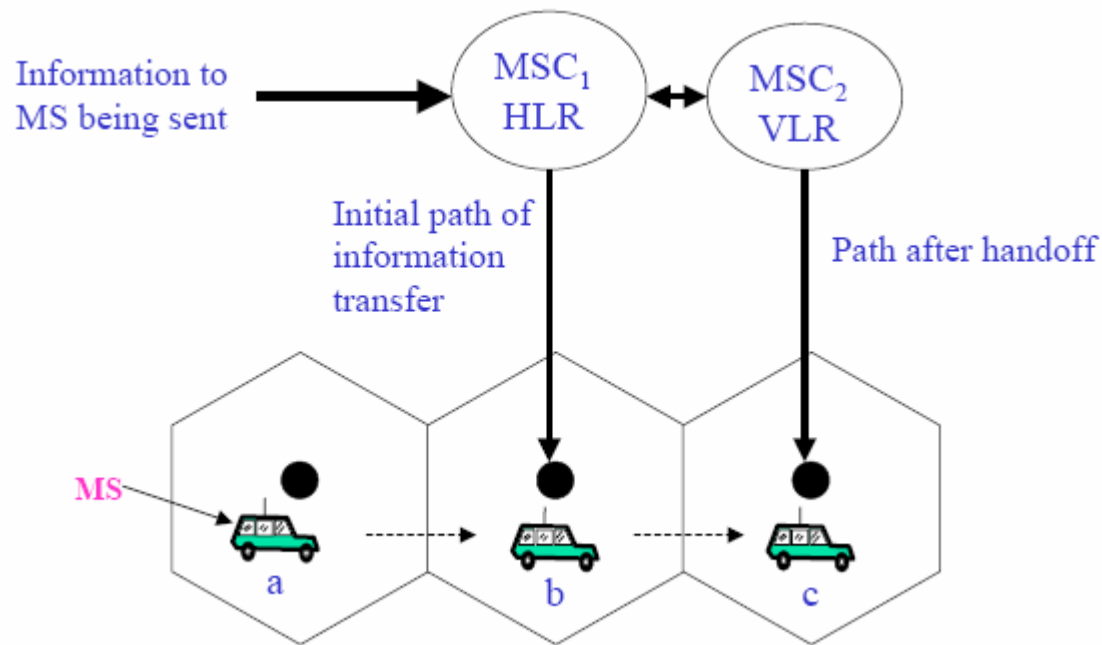




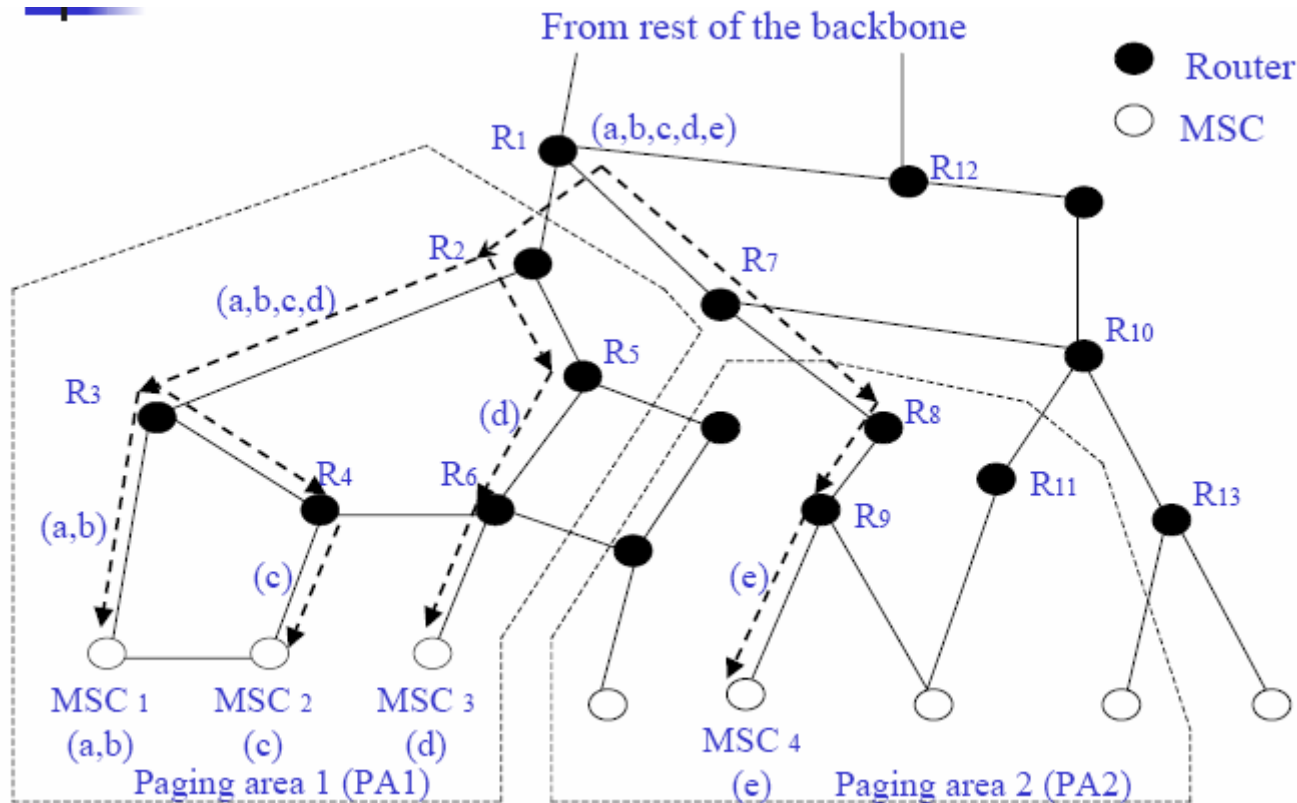
Możliwe sytuacje podczas przeniesienia połączenia

- 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 osiągnąć MSC wzdłuż najkrótszej 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

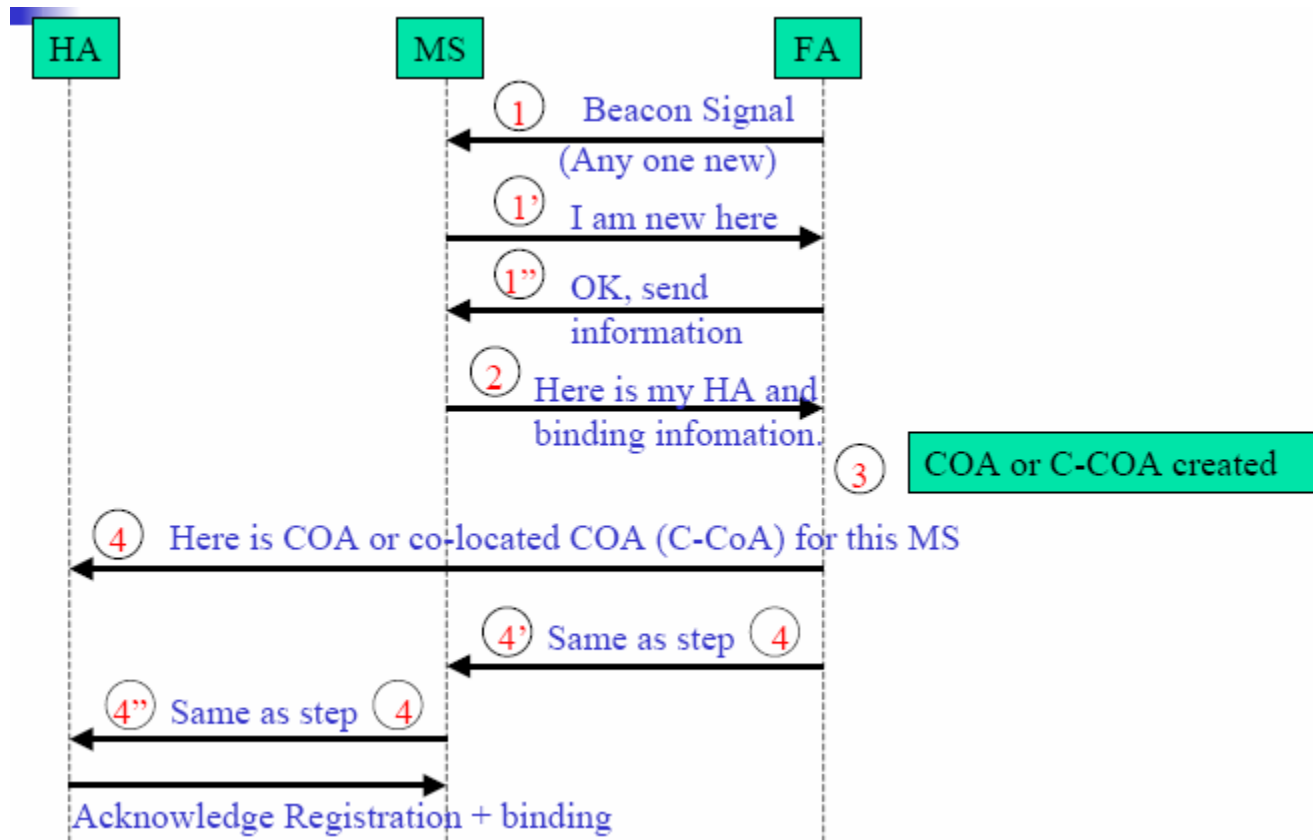
- Jeżeli MS przenosi się do nowej sieci to jego HA pozostaje niezmienny
- MS odkrywa FA w nowej sieci przez detekcję periodycznych sygnałów znaczników czasowych, które transmituje FA
- MS może również wysłać własną wiadomość (**agent solicitation messages**) z prośbą o przydział agenta, na którą FA odpowie
- 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



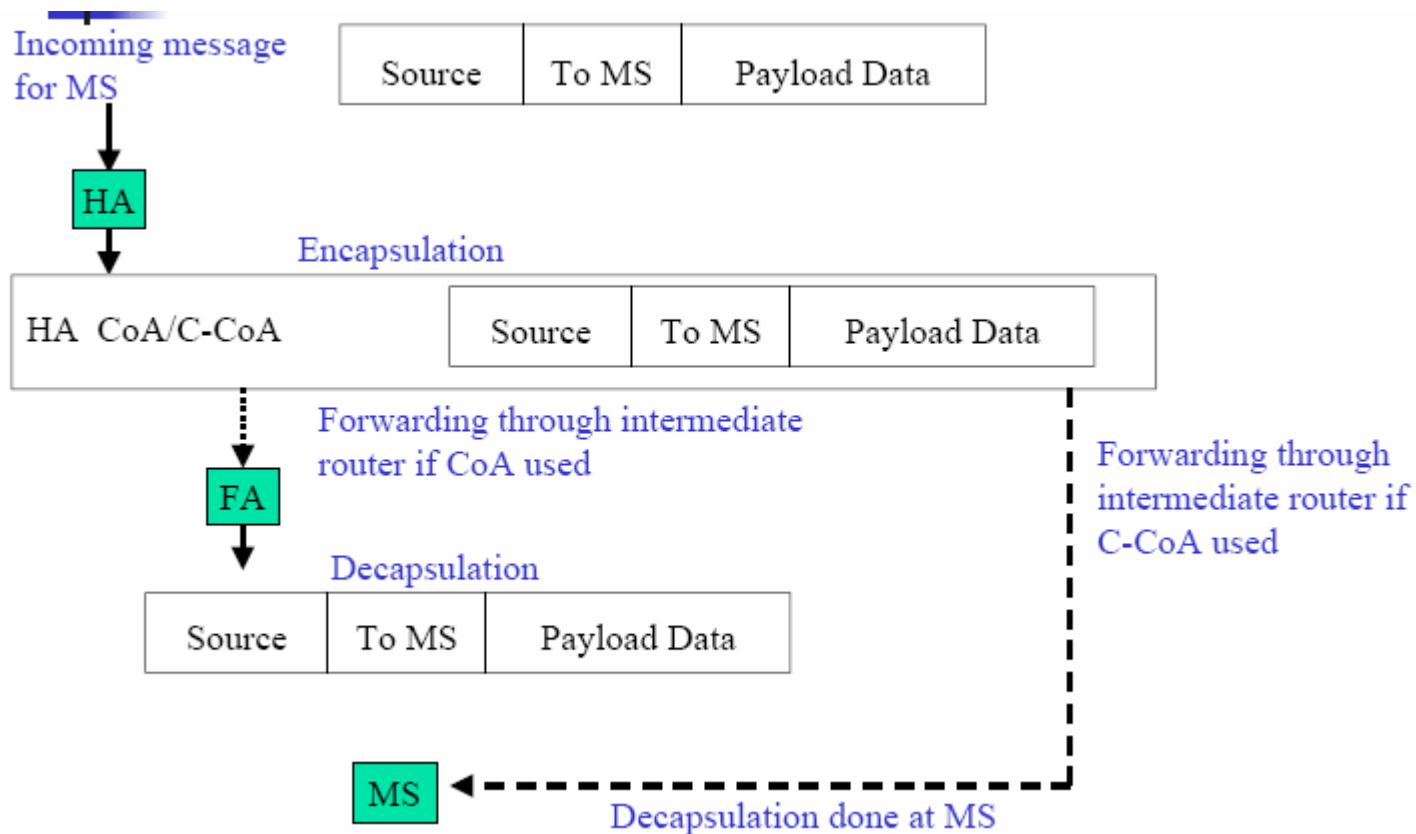
Ustanowienie połączenia (cd.)

- 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

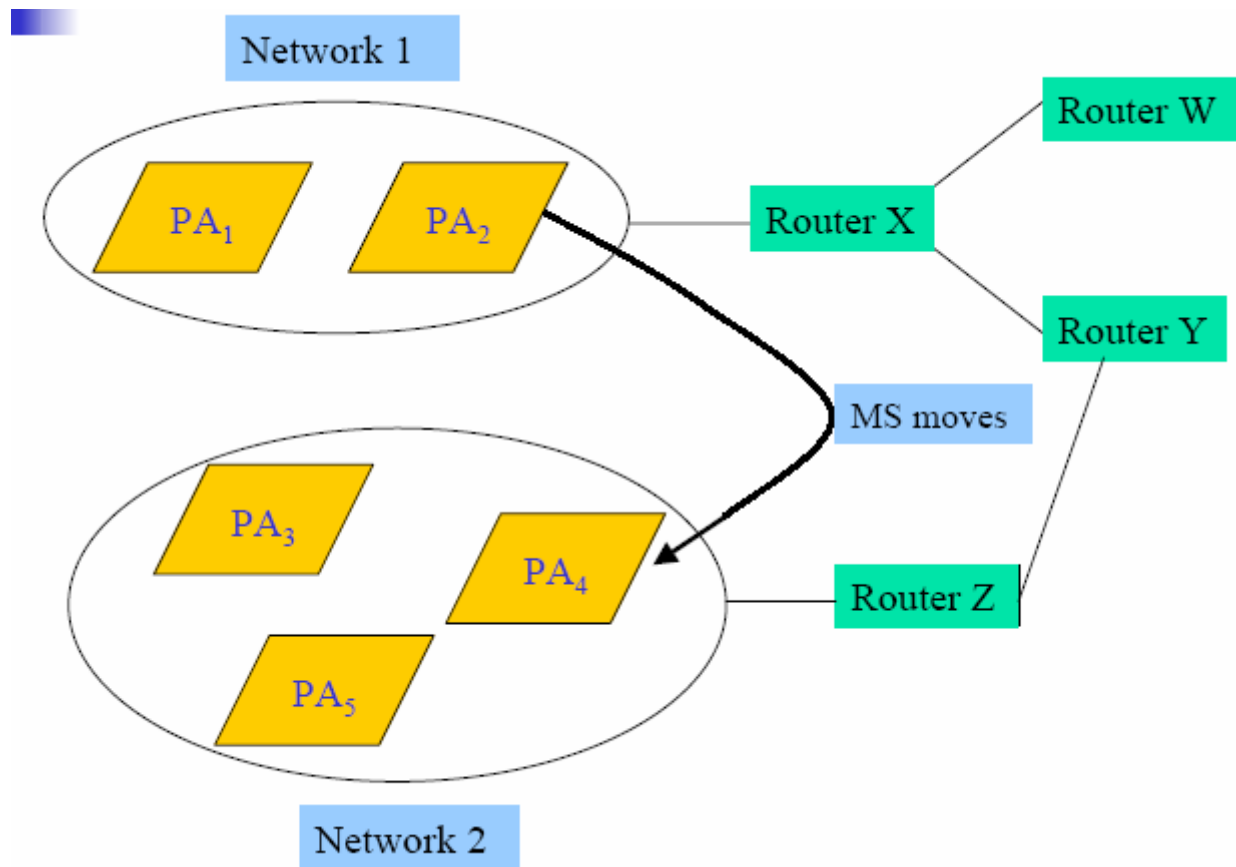




Rutowanie w ruterach sieci szkieletowej

- Jak FA odnajduje HA danego MS-a ?
- Jedno z możliwych podejść 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 routingu**

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 źródła 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 Engineering 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

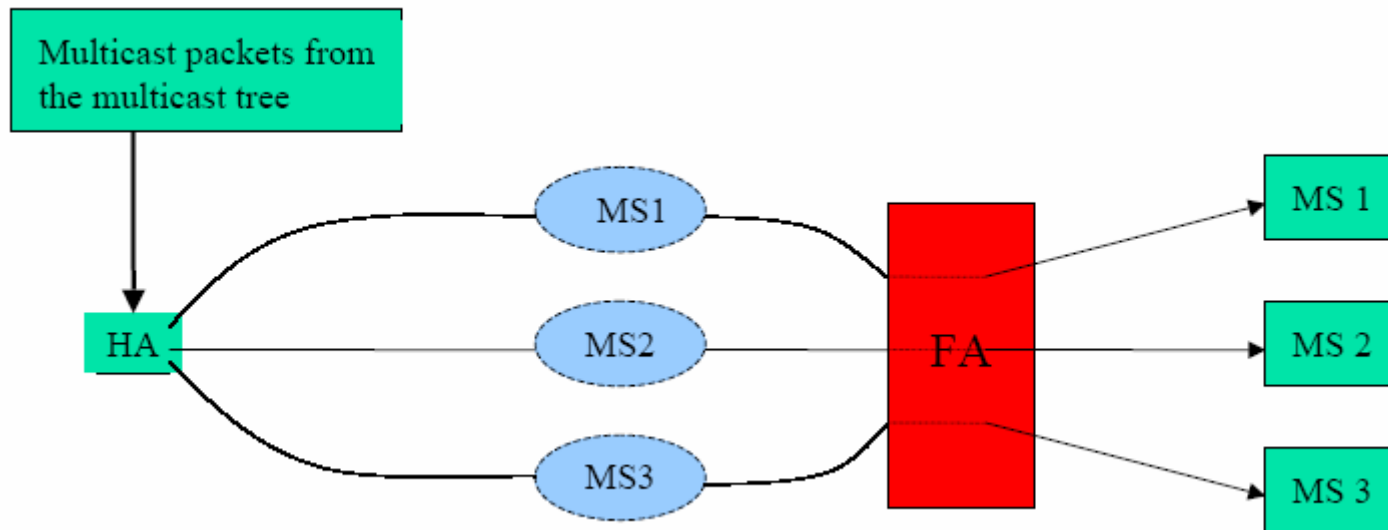
- Algorytm oparty na zdalnej subskrypcji jest prosty i zapobiega duplikacji pakietów oraz dostarczaniu pakietów nieoptymalną drogą
- Może spowodować przerwanie dostarczania danych dopóki FA nie będzie przyłączone do drzewa
- Skutkiem jego działania jest powstawanie szeregu drzew typu przyłącz oraz odłącz 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



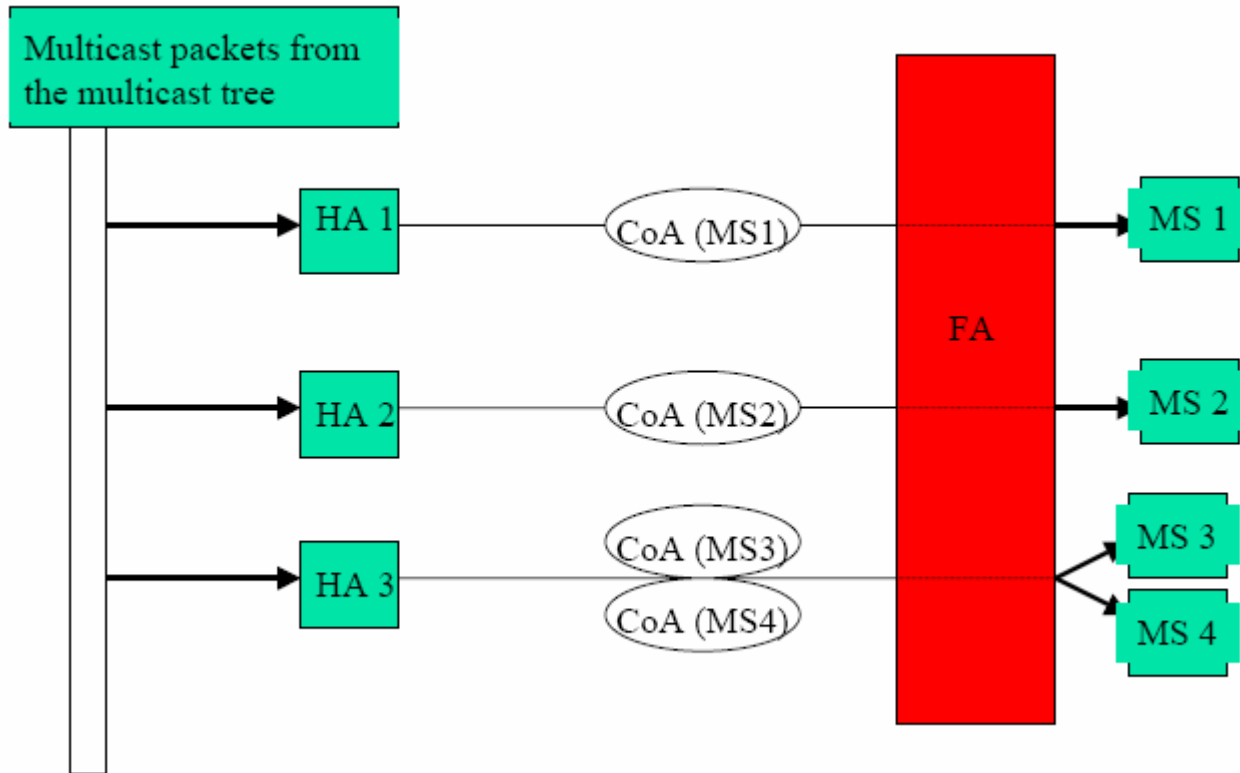
Multicasting

- 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 konwergencji 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

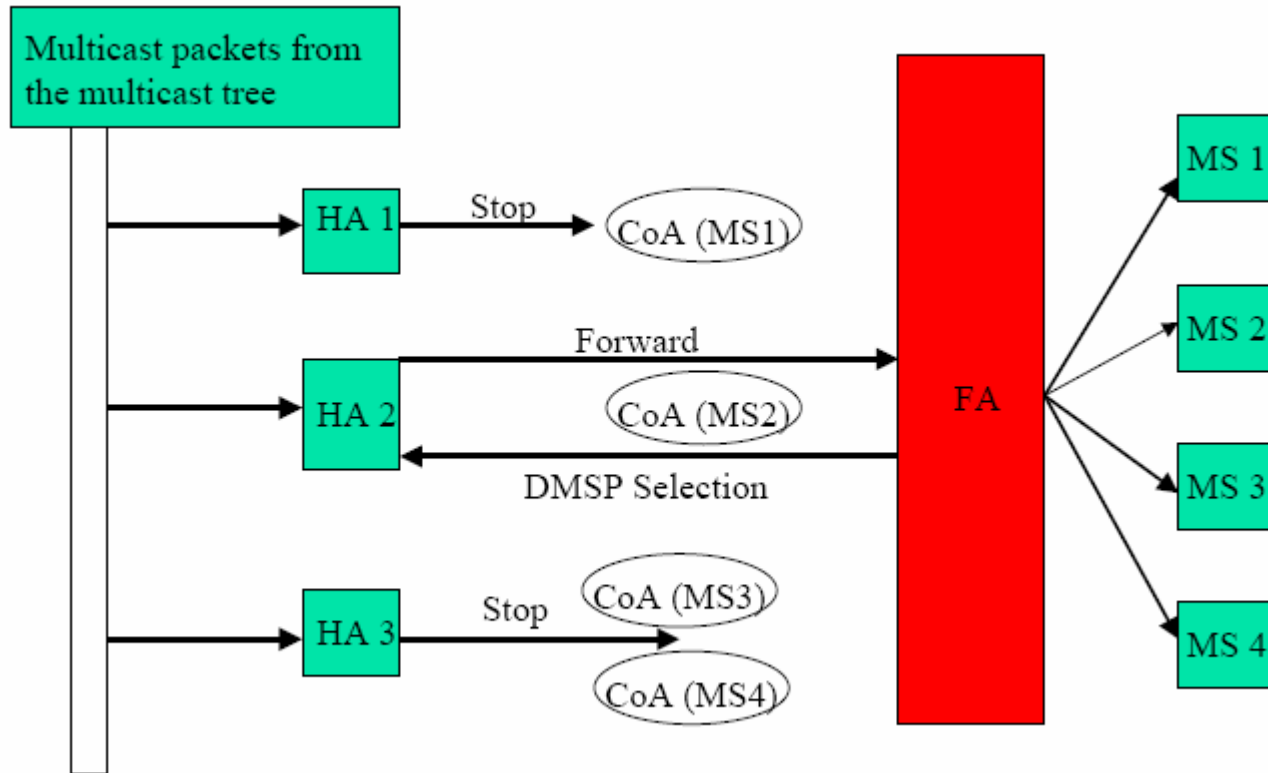




Multicasting

- W celu rozwiązania **Problemu konwergencji tunelowej**, zaproponowano protokół MoM, wg. którego FA wybiera spośród HA jednego HA dla poszczególnej grupy, nazywanego mianowanym prowadzającym 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 „zagłuszenie” 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

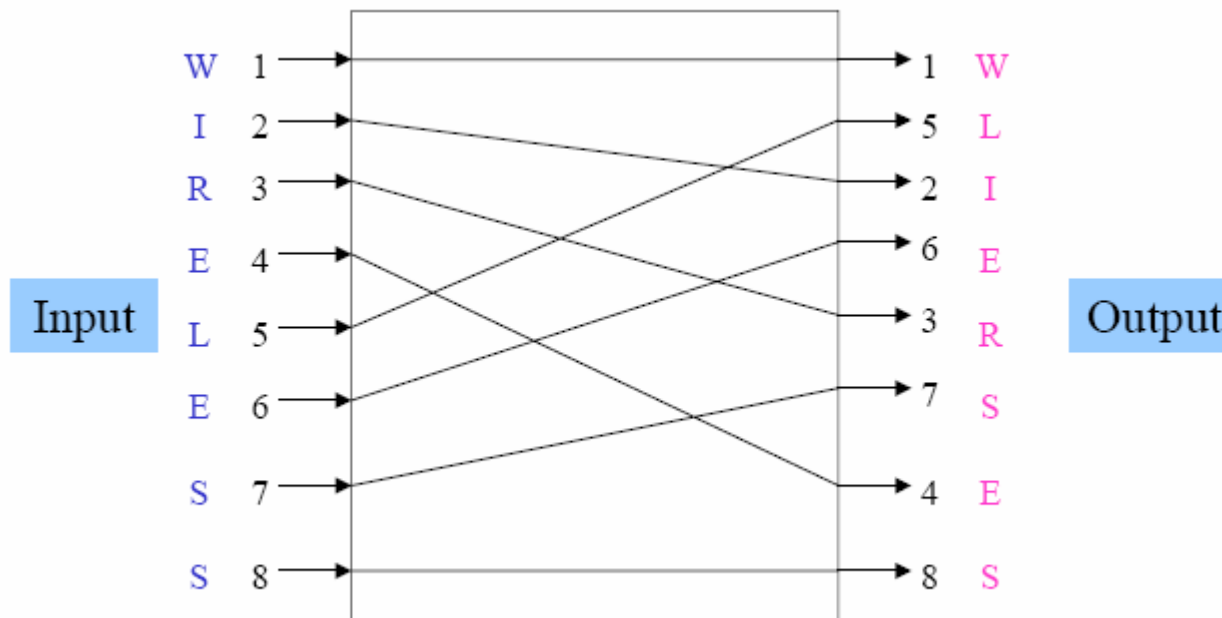
- Szyfrowanie z kluczem symetrycznym
 - Np. DES, AES
- Szyfrowanie z kluczem publicznym
 - np. RSA



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 Encryption 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

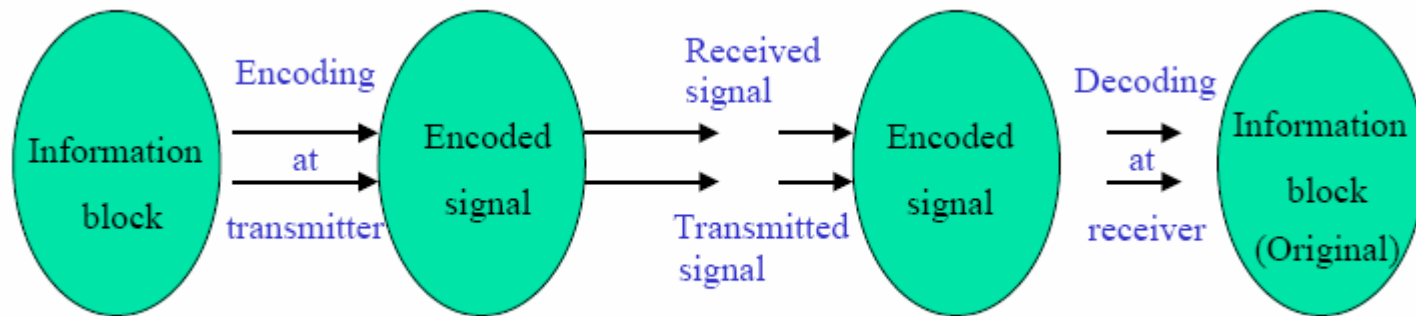
(b) Permutation after reception



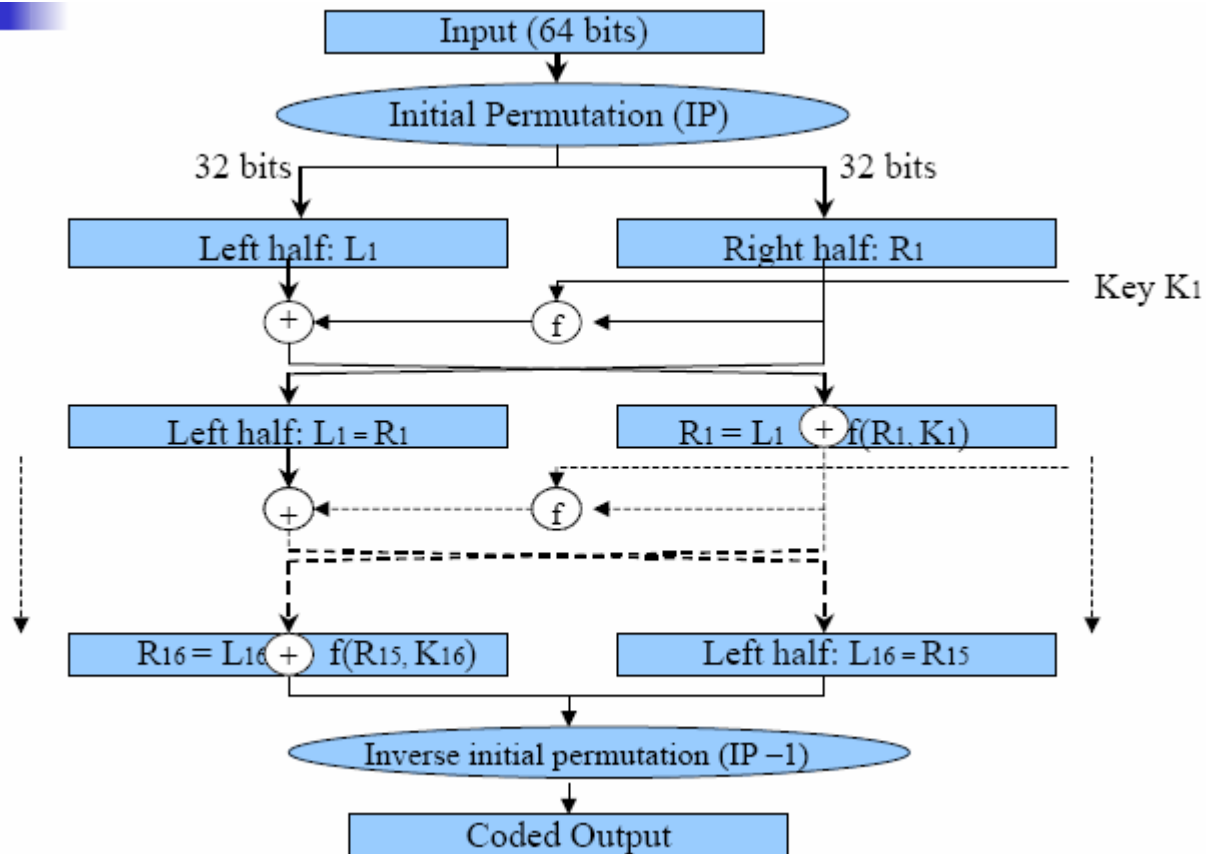
Szyfrowanie z kluczem symetrycznym

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

Proces generyczny kodowania i dekodowania



Permutacja i kodowanie informacji w DES

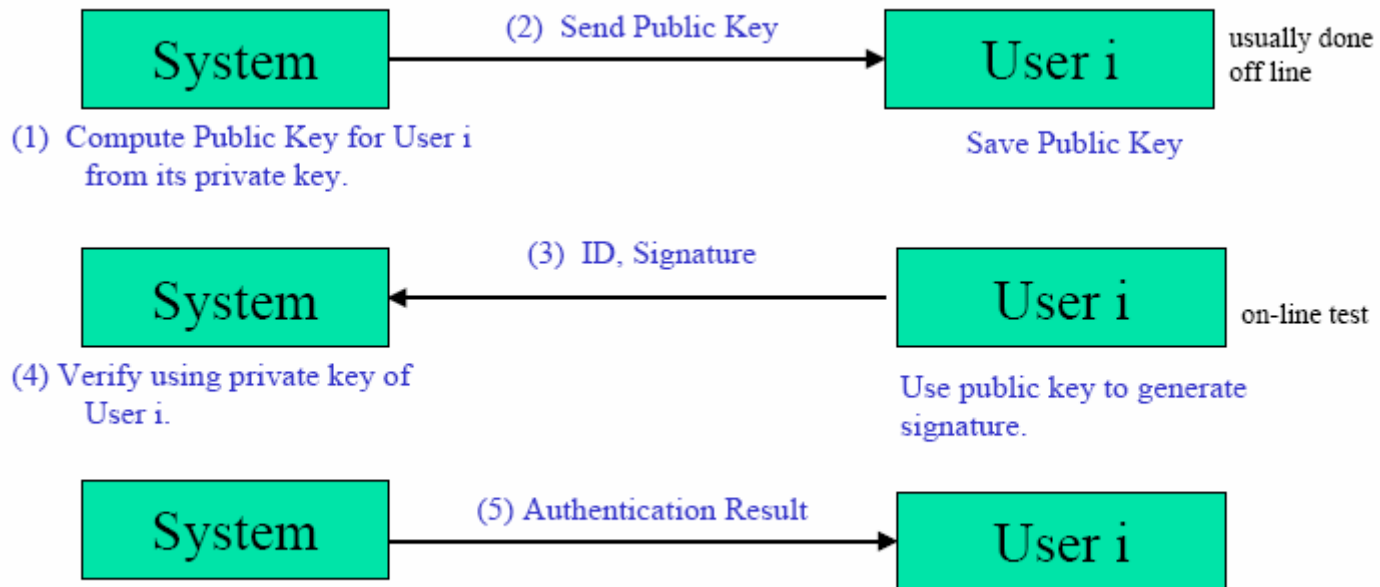




Uwierzytelnianie

- 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

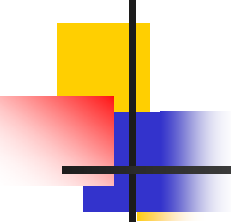




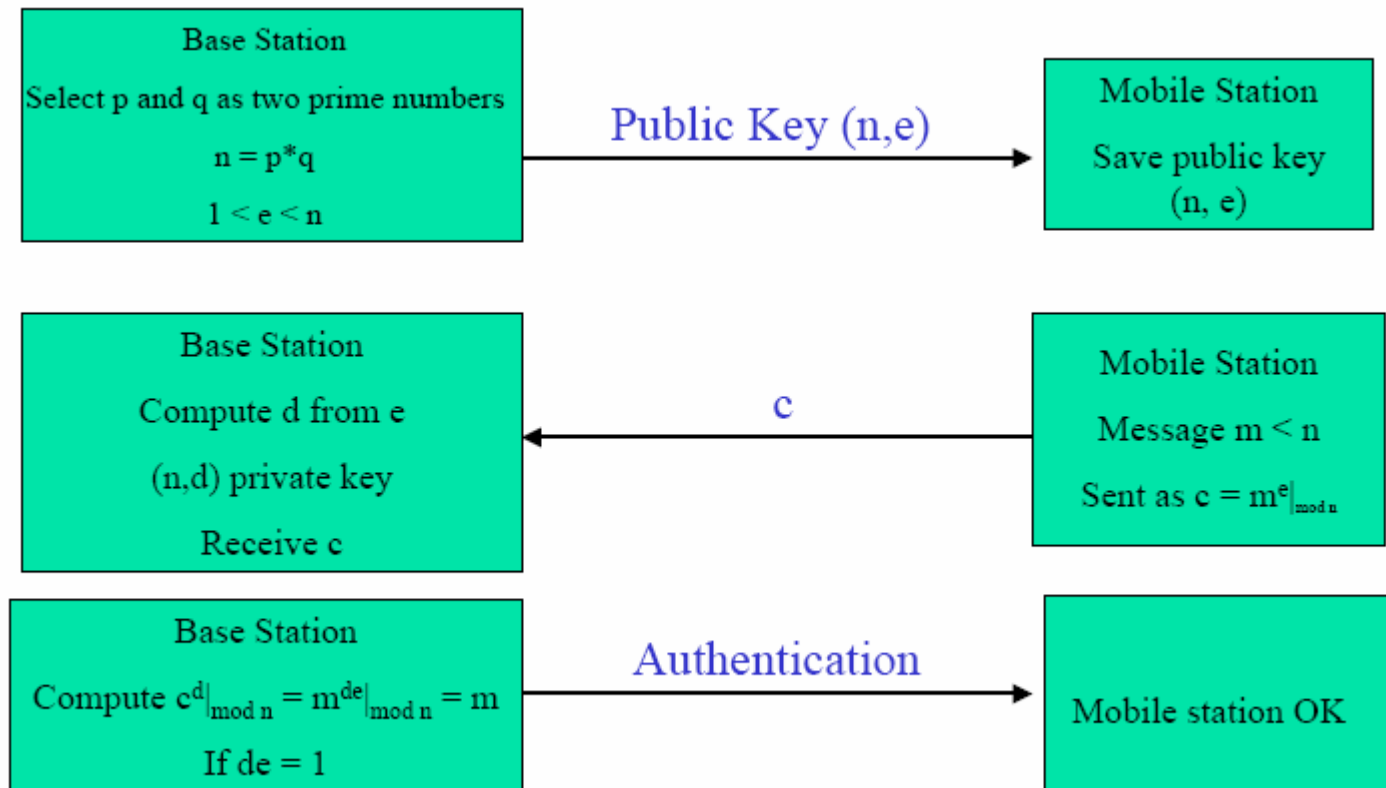
Uwierzytelnianie (Algorytm RSA)

- 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 $c^d \bmod n$ i wysyła do systemu. Po otrzymaniu c system oblicza $c = m^e \bmod n$ gdzie d jest obliczane na podstawie klucza prywatnego (n,e)

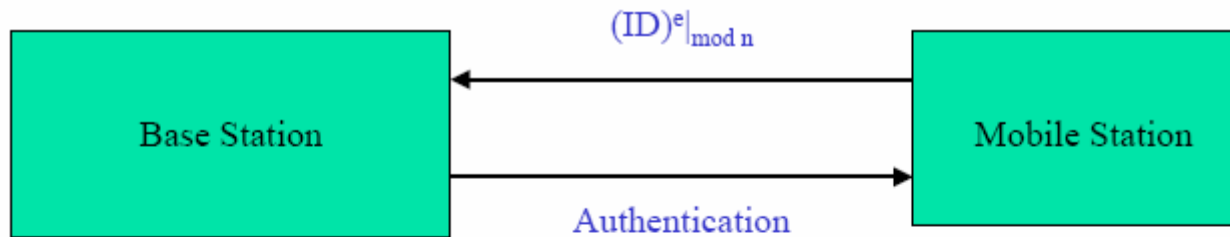
$$\begin{aligned} c^d \bmod n &= (m^e \bmod n)^d \bmod n = (m^e)^d \bmod n \\ &= m^{ed} \bmod n \end{aligned}$$

- 
-
- 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

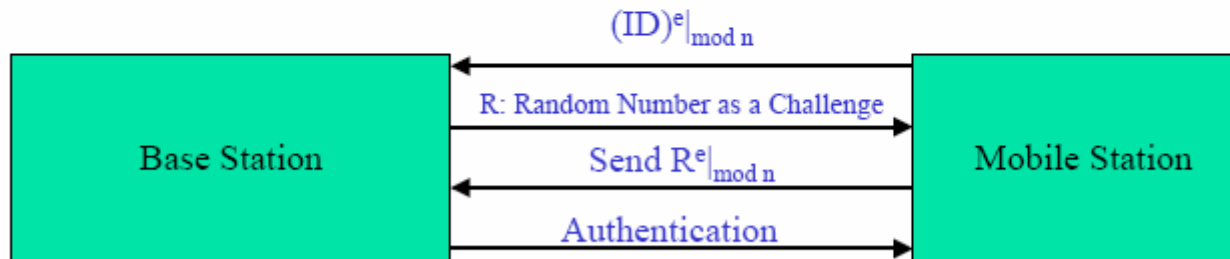
Uwierzytelnianie wiadomości przy użyciu klucza publicznego/prywatnego



Uwierzytelnianie MS-a przez BS



(a) Authentication based on ID



(b) Authentication using a challenge



Bezpieczeństwo systemów bezprzewodowych

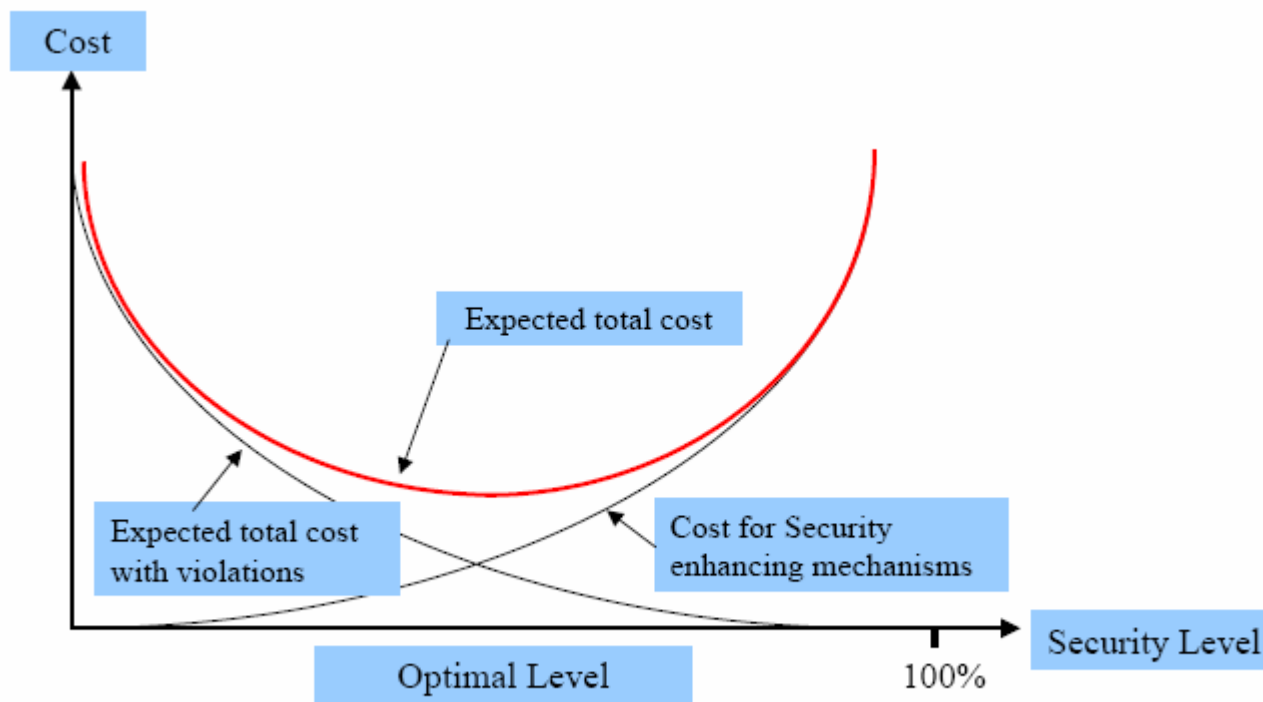
- Podstawowe usługi bezpieczeństwa:
 - **Poufność**: tylko autoryzowana strona może mieć dostęp do informacji systemu oraz transmitowanych danych
 - **Niezaprzeczalność**: nadawca i odbiorca nie mogą mogą zaprzeczyć, że transmisja się odbyła
 - **Uwierzytelnienie**: nadawca informacji jest prawidłowo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



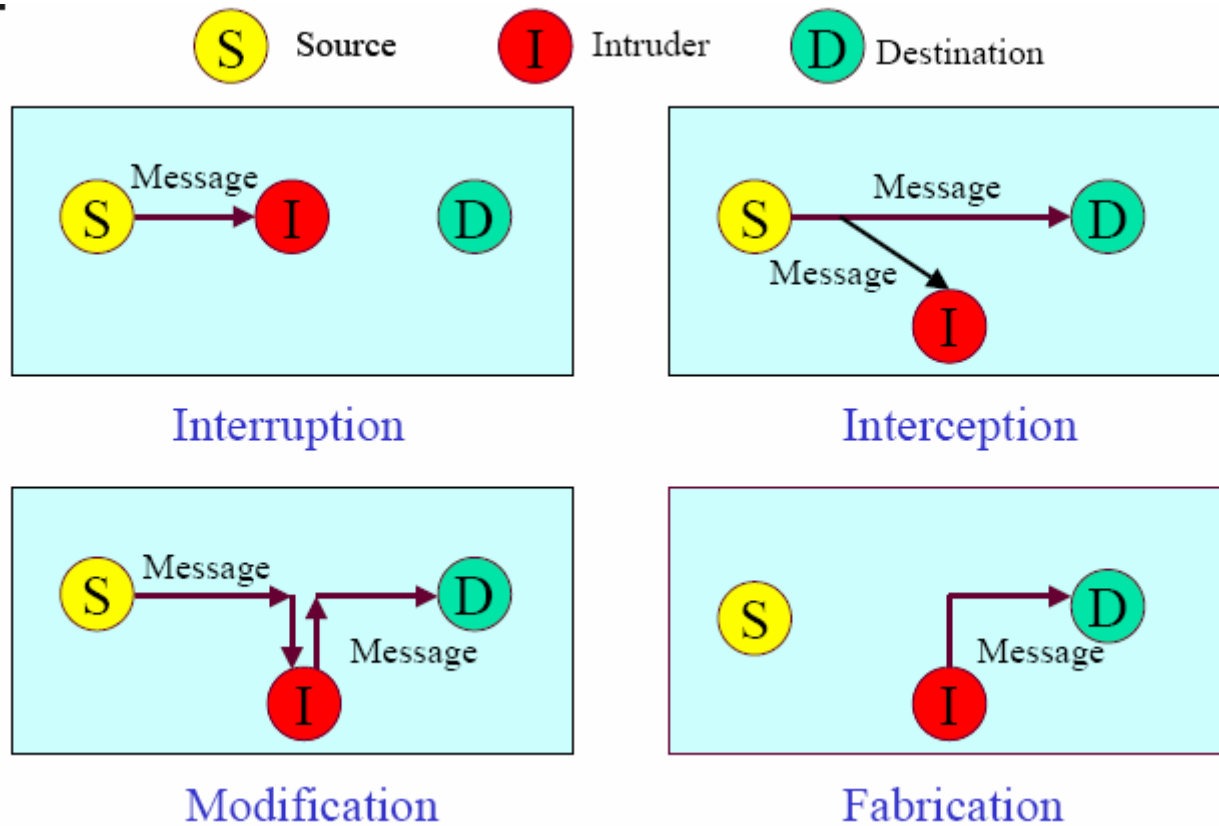
Bezpieczeństwo systemów bezprzewodowych

- 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)