無線通訊系統
(Wireless Communications Systems)

國立清華大學電機系暨通訊工程研究所
蔡育仁
台達館 821 室
Tel: 62210
E-mail: yrtsai@ee.nthu.edu.tw

Chapter 4
Radio Network Planning Technologies for Wireless Communication Systems

Co-channel Interference and Frequency Reuse

Co-channel Interference

- At higher velocity, by using coding and interleaving,
  - Each coding block involves multiple independent fade intervals
  - The **average** received carrier-to-interference ratio, Λ, should exceed a receive threshold Λ_{th}
  - **Path loss and shadowing** determine the outage probability of CCI
- At lower velocity, the received signal **can not** be averaged over the fast envelope variations
  - Each coding block duration is smaller than the fade duration
  - The **instantaneous** received carrier-to-interference ratio, λ, should exceed a receive threshold λ_{th}
  - **Path loss, shadowing and envelope fading** determine the outage probability of CCI

Co-channel Interference Modeling

Multiple Log-Normal Interferences

- Co-channel interference: a combination of multiple log-normal interferences

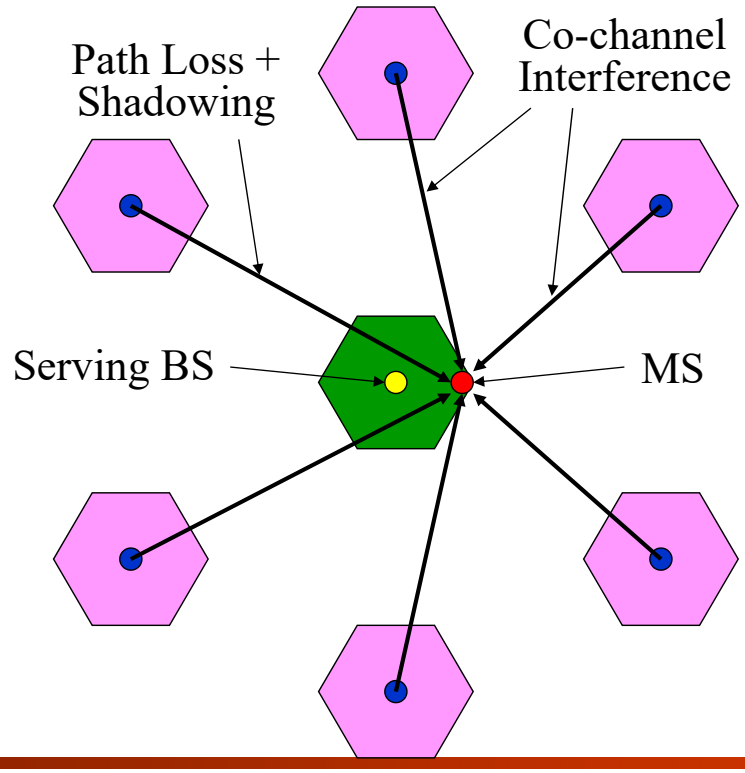
$$I = \sum_{k=1}^{N_I} \Omega_k = \sum_{k=1}^{N_I} 10^{\Omega_{k\,(\mathrm{dBm})}/10}$$

- $\Omega_{k(\mathrm{dBm})}$, $k = 1,\ldots, N_I$, are Gaussian random variables with means $\mu_{\Omega_k\,(\mathrm{dBm})}$ and variances $\sigma^2_{\Omega_k}$
- No known closed form expression exists for $N_I \geq 2$
- We can approximate CCI as another log-normal RV: $Z_{(\mathrm{dBm})}$, which is a Gaussian RV with mean $\mu_{Z\,(\mathrm{dBm})}$ and variances σ^2_Z

$$I = \sum_{k=1}^{N_I} 10^{\Omega_{k\,(\mathrm{dBm})}/10} \approx 10^{Z_{(\mathrm{dBm})}/10} = \hat{I}$$

- Methods: **Fenton-Wilkinson; Schwartz and Yeh; Farley**

Sum of Co-channel Interferences



Fenton-Wilkinson Method

- Obtain the mean $\mu_{Z(\text{dBm})}$ and variance σ_Z^2 by matching
  - the first two moments of the power sum I
  - the first two moments of the approximation $\hat{I}$
- Express by using natural logarithm:

$$\Omega_k = 10^{\Omega_{k(\text{dBm})}/10} = e^{\xi\Omega_{k(\text{dBm})}} = e^{\hat{\Omega}_k}$$

  - where

$$\xi = (\ln 10)/10 = 0.23026$$

$$\hat{\Omega}_k = \xi\Omega_{k(\text{dBm})}$$

$$\mu_{\hat{\Omega}_k} = \xi\mu_{\Omega_k(\text{dBm})}$$

$$\sigma^2_{\hat{\Omega}_k} = \xi^2\sigma^2_{\Omega_k}$$

Fenton-Wilkinson Method (Cont.)

- Moment generating function of a Gaussian RV:

X : Gaussian RV (μ, σ^2)

$$M_X(s) = E[e^{sX}]$$

$$= \int_{-\infty}^{\infty} e^{sx} \times \frac{1}{\sqrt{2\pi}\sigma} \times e^{\frac{-(x-\mu)^2}{2\sigma^2}} dx = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} \times e^{-\frac{x^2-(2\mu+2\sigma^2 s)x+\mu^2}{2\sigma^2}} dx$$

$$= \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma} \times e^{-\frac{[x-(\mu+\sigma^2 s)]^2}{2\sigma^2}} \times e^{\frac{2\mu\sigma^2 s+\sigma^4 s^2}{2\sigma^2}} dx = e^{s\mu+\frac{1}{2}s^2\sigma^2}$$

$$E[\Omega_k^n] = E[e^{n\hat{\Omega}_k}] = e^{n\mu_{\hat{\Omega}_k}+\frac{1}{2}n^2\sigma_{\hat{\Omega}_k}^2}$$

log-normal ← $E[\Omega_k^n]$; $E[e^{n\hat{\Omega}_k}]$ → Gaussian

***n* = 1, the first moment of a log-normal RV**

***n* = 2, the second moment of a log-normal RV**

Fenton-Wilkinson Method (Cont.)

- Suppose that $\hat{\Omega}_k, k = 1, ..., N_I$ are independent RVs with
  - Means: $\mu_{\hat{\Omega}_k}, k = 1, ..., N_I$
  - Identical variances: $\sigma_{\hat{\Omega}}^2$
- Identical variances are often assumed in macrocellular environments
  - The standard deviation of log-normal shadowing is largely independent of the radio path length
- Then equate the first two moments on both sides of

$$I = \sum_{k=1}^{N_I} e^{\hat{\Omega}_k} \approx e^{\hat{Z}} = \hat{I}$$

Fenton-Wilkinson Method (Cont.)

- Mean:

$$\mu_I = E[I] = E[\sum_{k=1}^{N_I} I_k] = \sum_{k=1}^{N_I} E[I_k] = \vdots = E[\hat{I}] = \mu_{\hat{I}}$$

$$\sum_{k=1}^{N_I} e^{\mu_{\hat{\Omega}_k} + (1/2)\sigma^2_{\hat{\Omega}_k}} = (\sum_{k=1}^{N_I} e^{\mu_{\hat{\Omega}_k}}) e^{(1/2)\sigma^2_{\hat{\Omega}}} = \vdots = e^{\mu_{\hat{Z}} + (1/2)\sigma^2_{\hat{Z}}}$$

- Variance:

$$\sigma_I^2 = \sum_{k=1}^{N_I} \sigma_k^2 = \sum_{k=1}^{N_I} \left(E[I_k^2] - E[I_k]^2 \right) = \sum_{k=1}^{N_I} \left(E[I_k^2] - \mu_{I_k}^2 \right) = \vdots = E[\hat{I}^2] - \mu_{\hat{I}}^2 = \sigma_{\hat{I}}^2$$

$$\sum_{k=1}^{N_I} (e^{2\mu_{\hat{\Omega}_k} + 2\sigma^2_{\hat{\Omega}_k}} - e^{2\mu_{\hat{\Omega}_k} + \sigma^2_{\hat{\Omega}_k}}) = \vdots = e^{2\mu_{\hat{Z}} + 2\sigma^2_{\hat{Z}}} - e^{2\mu_{\hat{Z}} + \sigma^2_{\hat{Z}}}$$

$$(\sum_{k=1}^{N_I} e^{2\mu_{\hat{\Omega}_k}}) e^{\sigma^2_{\hat{\Omega}}} (e^{\sigma^2_{\hat{\Omega}}} - 1) = \vdots = e^{2\mu_{\hat{Z}}} e^{\sigma^2_{\hat{Z}}} (e^{\sigma^2_{\hat{Z}}} - 1)$$

Fenton-Wilkinson Method (Cont.)

- Solve for $\mu_{\hat{Z}}$ and $\sigma^2_{\hat{Z}}$

$$\mu_{\hat{Z}} = \frac{\sigma^2_{\hat{\Omega}} - \sigma^2_{\hat{Z}}}{2} + \ln\left(\sum_{k=1}^{N_I} e^{\mu_{\hat{\Omega}_k}} \right)$$

$$\sigma^2_{\hat{Z}} = \ln\left((e^{\sigma^2_{\hat{\Omega}}} - 1) \frac{\sum_{k=1}^{N_I} e^{2\mu_{\hat{\Omega}_k}}}{\left(\sum_{k=1}^{N_I} e^{\mu_{\hat{\Omega}_k}} \right)^2} + 1 \right)$$

- Finally, we have

$$\mu_{Z(\text{dBm})} = \xi^{-1} \mu_{\hat{Z}}$$

$$\sigma_Z^2 = \xi^{-2} \sigma_{\hat{Z}}^2$$

Probability of CCI Outage

Probability of CCI Outage

- Consider an MS located at the location with a distance d_0 from the desired BS and distances d_k, $k = 1, 2, \ldots, N_I$, from the first tier co-channel BSs
- Define the distance vector $\mathbf{d} = (d_0, d_1, \cdots, d_{N_I})$
- The average received carrier-to-interference ratio (CIR)

$$\Lambda_{(\mathrm{dB})}(\mathbf{d}) = \Omega_{(\mathrm{dBm})}(d_0) - 10\log_{10}\sum_{k=1}^{N_I} 10^{\Omega_{(\mathrm{dBm})}(d_k)/10}$$

- Use the log-normal approximation

$$\mu_{Z(\mathrm{dBm})} = \xi^{-1}\mu_{\hat{Z}} \text{ and } \sigma_Z^2 = \xi^{-2}\sigma_{\hat{Z}}^2$$

$$\Lambda_{(\mathrm{dB})}(\mathbf{d}) = \Omega_{(\mathrm{dBm})}(d_0) - Z_{(\mathrm{dBm})}(d_1, d_2, \cdots, d_{N_I})$$

$$\mu_{\Lambda_{(\mathrm{dB})}(\mathbf{d})} = \mu_{\Omega_{(\mathrm{dBm})}(d_0)} - \mu_{Z_{(\mathrm{dBm})}}$$

$$\sigma^2_{\Lambda(\mathbf{d})} = \sigma^2_{\Omega} + \sigma^2_Z$$

Probability of CCI Outage (Cont.)

- The probability of CCI outage:

$$O_I(\mathbf{d}) = P_r(\Lambda_{(\mathrm{dB})}(\mathbf{d}) < \Lambda_{th(\mathrm{dB})})$$

$$= Q\left(\frac{\mu_{\Omega_{(\mathrm{dBm})}(d_0)} - \mu_{Z_{(\mathrm{dBm})}} - \Lambda_{th(\mathrm{dB})}}{\sqrt{\sigma_\Omega^2 + \sigma_Z^2}}\right)$$

CIR

- For $N_I = 1$, $\Lambda_{(\mathrm{dB})}(\mathbf{d})$ has the Gaussian density with mean and variance

$$\mu_{\Lambda_{(\mathrm{dB})}(\mathbf{d})} = \mu_{\Omega(d_0)} - \mu_{\Omega(d_1)}$$

$$\sigma^2_{\Lambda(\mathbf{d})} = \sigma^2_{\Omega(d_0)} + \sigma^2_{\Omega(d_1)} = 2\sigma^2_\Omega$$

- Then, we have

$$p_{\Lambda_{(\mathrm{dB})}(\mathbf{d})}(x) = \frac{1}{\sqrt{4\pi}\sigma_\Omega} \exp\left\{-\frac{(x - \mu_{\Lambda(\mathbf{d})})^2}{4\sigma_\Omega^2}\right\}$$

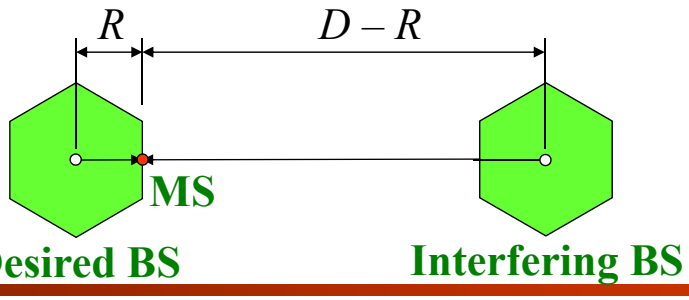
Probability of CCI Outage (Cont.)

- The probability of CCI:

$$O_I(\mathbf{d}) = P_r(\Lambda_{(\mathrm{dB})}(\mathbf{d}) < \Lambda_{th(\mathrm{dB})}) = \int_{-\infty}^{\Lambda_{th(\mathrm{dB})}} \frac{1}{\sqrt{4\pi}\sigma_\Omega} \exp\left\{-\frac{(x - \mu_{\Lambda(\mathbf{d})})^2}{4\sigma_\Omega^2}\right\} dx$$

$$= Q\left(\frac{\mu_{\Lambda(\mathbf{d})} - \Lambda_{th(\mathrm{dB})}}{\sqrt{2}\sigma_\Omega}\right)$$

- Consider the worst case situation:
  - The MS is located on cell edge and at a distance $D - R$ from a single co-channel BS



Probability of CCI Outage (Cont.)

- If a simple path loss model is applied

$$\mu_{\Omega(d)} = \mu_{\Omega(d_0)} - 10\beta \log(d/d_0)$$

- The probability of CCI:

$$O_I(R) = Q\left(\frac{\mu_{\Omega(R)} - \mu_{\Omega(D-R)} - \Lambda_{th(\text{dB})}}{\sqrt{2}\sigma_\Omega}\right) = Q\left(\frac{10\log_{10}\left(\frac{D}{R}-1\right)^\beta - \Lambda_{th(\text{dB})}}{\sqrt{2}\sigma_\Omega}\right)$$

$$\begin{aligned}
&\mu_{\Omega(R)} - \mu_{\Omega(D-R)} \\
&= [\mu_{\Omega(d_0)} - 10\beta \log(R/d_0)] - [\mu_{\Omega(d_0)} - 10\beta \log((D-R)/d_0)] \\
&= 10\beta[\log((D-R)/d_0) - \log(R/d_0)] \\
&= 10\beta[\log((D-R)/R) = 10\log(\tfrac{D}{R}-1)^\beta
\end{aligned}$$

- The area averaged probability of CCI:

$$O_I = \frac{1}{\pi R^2}\int_0^R O_I(r) 2\pi r \, dr$$

Determination of Frequency Reuse Factor

- The carrier-to-interference ratio margin (CCI margin) that can sustain a probability of CCI equal to $O(R)$:

$$M_\Lambda = \mu_{\Lambda(R)} - \Lambda_{th} = 10\log(\tfrac{D}{R}-1)^\beta - \Lambda_{th}$$

- For a co-channel reuse factor N, we have $D/R = \sqrt{3N}$
- Correspondingly, the reuse factor N is determined as

$$N = \tfrac{1}{3}[10^{\frac{M_\Lambda + \Lambda_{th}}{10\beta}} + 1]^2$$

  - where M_Λ can be determined by the acceptable probability of CCI

- A reduction in N can only be achieved by making Λ_{th} small

Question

- **Question:**
  - Why the carrier-to-interference ratio margin (CCI margin) is independent to the transmission power?
    - The co-channel interference is proportional to the transmission power
  - Can we improve the CIR by increasing the transmission power?
    - No. The CIR remains the same.

Cellular Coverage Planning

Cell Sectoring

Cell Sectoring

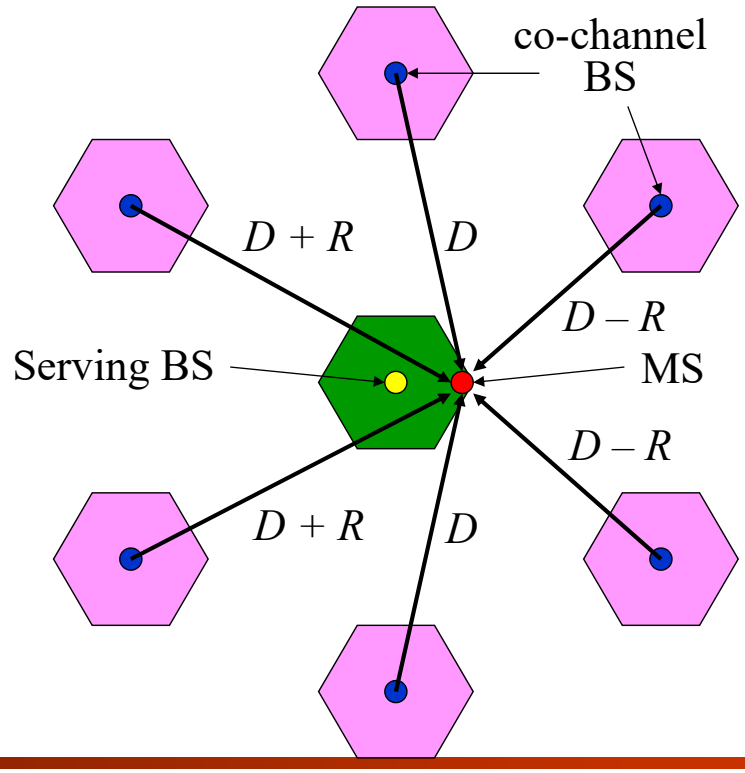
- Assuming that the BSs employ **omni-directional** antennas, the **worst case** of forward co-channel interference is
  - When an MS is located at the corner of a cell
  - Three pairs of BSs each at an approximate distance of ***D* – *R***, ***D*** or ***D* + *R***
- Assume that the simple path loss model is

$$\mu_{\Omega_p}(d) = \mu_{\Omega_p}(d_0) - 10\beta \log_{10}(d/d_0)$$

- If the value of $\mu_{\Omega_p}(d_0)$ (including Ω_t, G_T and h_b) is the same for all BSs, the worst case carrier-to-interference ratio is

$$\Lambda = \frac{1}{2}\frac{R^{-\beta}}{(D-R)^{-\beta} + D^{-\beta} + (D+R)^{-\beta}}$$
$$= \frac{1}{2}\frac{1}{\left(\frac{D}{R}-1\right)^{-\beta} + \left(\frac{D}{R}\right)^{-\beta} + \left(\frac{D}{R}+1\right)^{-\beta}}$$

Cell Sectoring (Cont.)



Cell Sectoring (Cont.)

- The worst case C/I with a path loss exponent $\beta = 3.5$ is

$$D/R = \sqrt{3N}$$

$$(\Lambda)_{\text{dB}} = \begin{cases} 14.3\,\text{dB}, & \text{for } N = 7 \\ 9.2\,\text{dB}, & \text{for } N = 4 \\ 6.3\,\text{dB}, & \text{for } N = 3 \end{cases}$$

- The minimum allowable cluster size is determined by the requirement of the radio receiver
- Due to **shadowing** and **multipath fading**, the worst case C/I values may be too small to yield an acceptable performance
  - An extra **co-channel interference margin** is required

Cell Sectoring (Cont.)

- **Cell sectoring** is a very common method that is employed in macrocellular systems to improve the receiving performance against co-channel interference
  - Each cell is divided into multiple radial sectors with **directional** BS antennas
  - The carriers assigned to each cell are further divided into multiple **disjoint sets** with each set assigned to a cell sector
- Current cellular systems are quite often deployed with 120º (**3-sector**) cell or 60º (**6-sector**) cell sectors
- The number of primary co-channel interferers is reduced:
  - for 3-sector cells: from 6 to 2; for 6-sector cells: from 6 to 1
- Disadvantages: Cell sectoring induces more **inter-sector handoff** and reduces **trunking efficiency**

3-sector Cell Sectoring

- For 3-sector cells, the primary interferers are located at approximate distances of D and $D + 0.7R$
  - The worst case carrier-to-interference ratio is

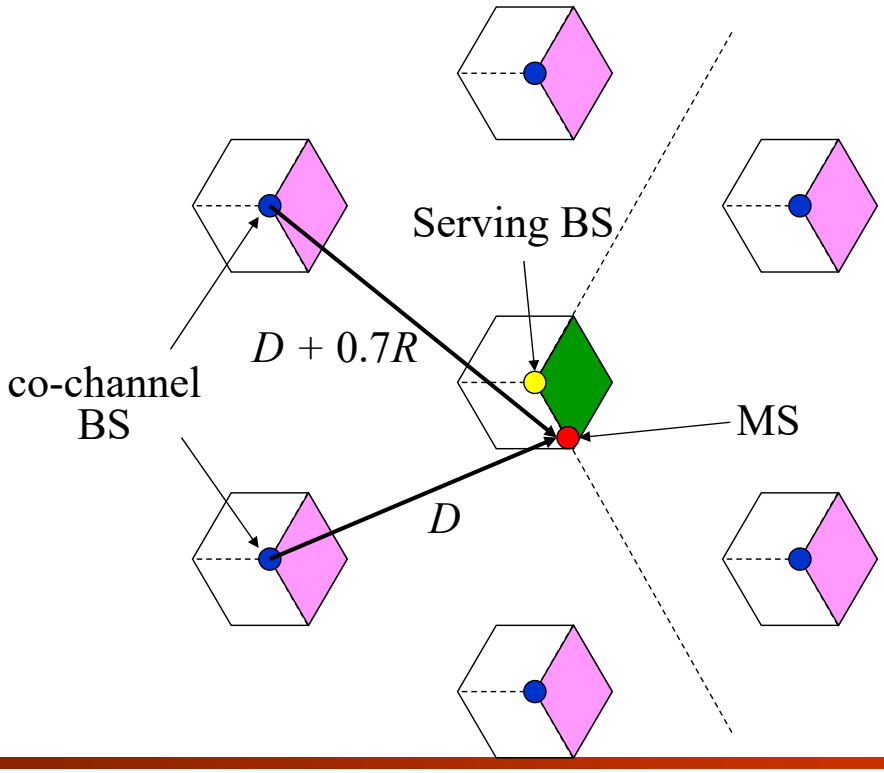
$$\Lambda = \frac{R^{-\beta}}{D^{-\beta} + (D + 0.7R)^{-\beta}} = \frac{1}{\left(\frac{D}{R}\right)^{-\beta} + \left(\frac{D}{R} + 0.7\right)^{-\beta}}$$

- The worst case C/I with a path loss exponent $\beta = 3.5$ is

$$(\Lambda)_{\text{dB}} = \begin{cases} 21.1\,\text{dB}, & \text{for } N = 7 \\ 17.1\,\text{dB}, & \text{for } N = 4 \\ 15.0\,\text{dB}, & \text{for } N = 3 \end{cases}$$

- Gain = 6.8 dB ($N = 7$); 7.9 dB ($N = 4$); 8.7 dB ($N = 3$)

3-sector Cell Sectoring (Cont.)



6-sector Cell Sectoring

- For 6-sector cells, the primary interferer is located at an approximate distance of $\boldsymbol{D + 0.7R}$
  - The worst case carrier-to-interference ratio is

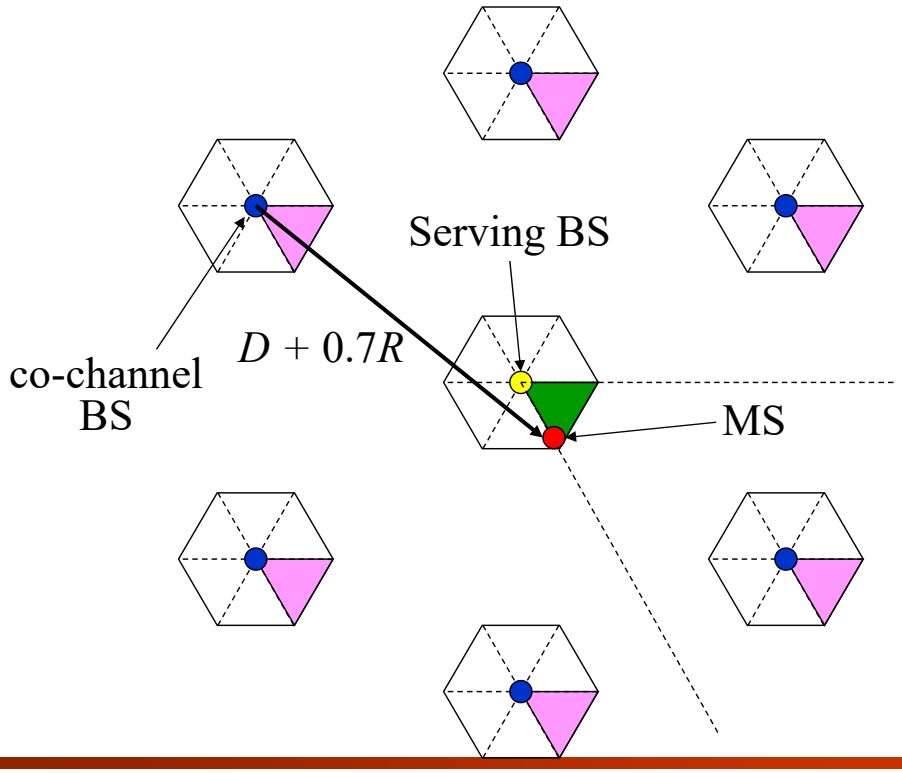
$$\Lambda = \frac{R^{-\beta}}{(D+0.7R)^{-\beta}} = \frac{1}{\left(\frac{D}{R}+0.7\right)^{-\beta}}$$

- The worst case C/I with a path loss exponent $\beta = 3.5$ is

$$(\Lambda)_{\text{dB}} = \begin{cases} 25.3\,\text{dB}, & \text{for } N = 7 \\ 21.7\,\text{dB}, & \text{for } N = 4 \\ 19.9\,\text{dB}, & \text{for } N = 3 \end{cases}$$

- Gain = 11.0 dB ($N = 7$); 12.5 dB ($N = 4$); 13.6 dB ($N = 3$)

6-sector Cell Sectoring (Cont.)

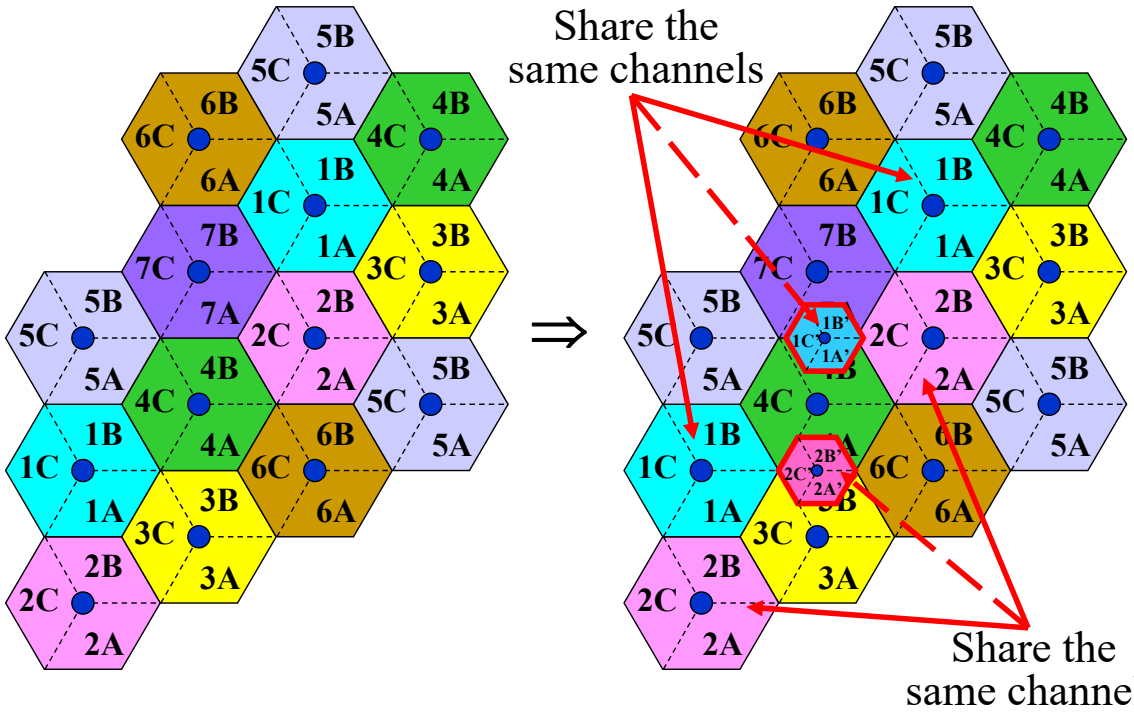


Cell Splitting

Cell Splitting

- Cell splitting refers to the process of splitting a cell into multiple smaller cells
  - By establishing some new and smaller cells at specific locations
  - **Large cells:** used in suburban and rural areas with low traffic loading
  - **Small cells:** used in urban areas with high traffic loading
- Considering the uniform grid of hexagonal cells:
  - If heavy traffic loading is experienced, then a split cell is introduced
  - The frequency assignment for the split cell is the group with the largest reuse distance

Cell Splitting (Cont.)



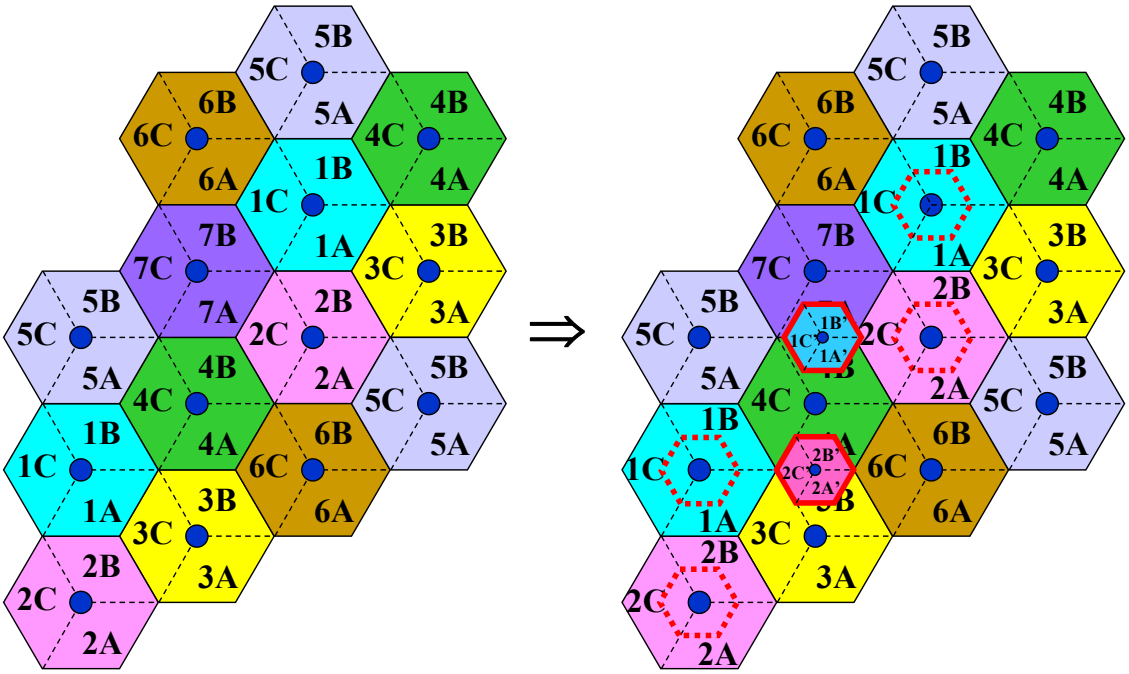
Frequency Assignment

- After introducing the split cells, additional changes in the frequency assignments may be required
  - In order to maintain the reuse constraint of the split cells
- **Channel segmenting**:
  - The channel sets in the co-channel cells are subdivided into **two groups**
  - The split cells and large co-channel cells are assigned **different groups** of channels
  - Decrease the trunking efficiency

Frequency Assignment (Cont.)

- To improve the trunking efficiency, we can apply the **overlaid inner cells** technique.
- Channel assignments for overlaid cells:
  - The co-channel cells are divided into **inner** and **outer** cells
  - The **inner and split cells** reuse the same group of channels
  - The **outer cells** use the other group of channels
  - **Handoffs** are required between inner and outer cells

Frequency Assignment (Cont.)



Transmit Power Assignment

- The received power for an MS located at the corner of the **original cell**:

$$\Omega(R_o) = A\Omega_o R_o^{-\beta}$$

- The received power on the boundary of the **split cell**:

$$\Omega(R_s) = A\Omega_s R_s^{-\beta}$$

- To keep the received power associated with an MS located on the cell boundary constant:

$$\Omega_s = \Omega_o \left(R_s / R_o\right)^{\beta}$$

- If $\beta = 4$ and $R_s = R_o/2$, then $\Omega_s = \Omega_o/16$
  - The split cells can reduce the transmission power level by 12 dB

Reuse Partitioning

Reuse Partitioning (Cont.)

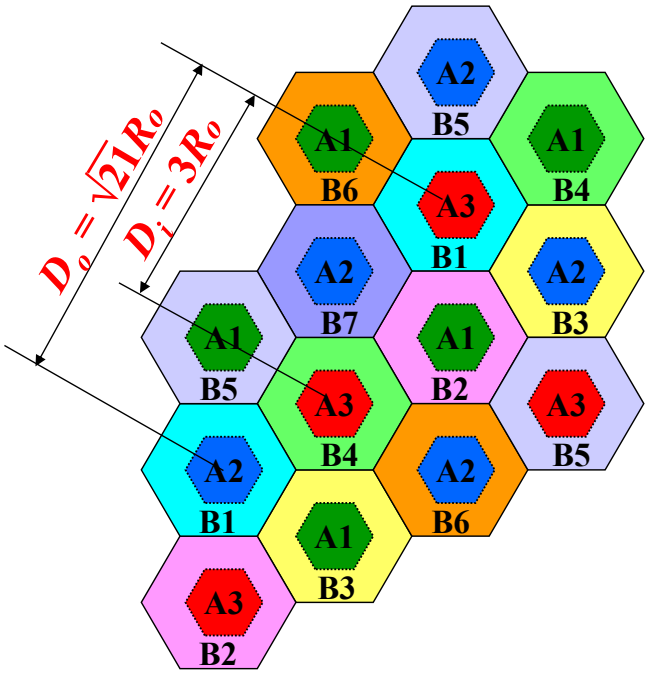
- **Reuse partitioning** is a technique that uses **multiple co-channel reuse factors** in the same deployment
- For example, channels are assigned to the inner and outer cells according to **3-cell** and **7-cell** reuse plans
  - Handoffs are required between inner and outer cells
- The reduced radii of the inner cells leads to an **increase** in the **cell capacity**
- Suppose that an acceptable link quality requires a co-channel reuse factor satisfying

$$D_i / R_i = D_o / R_o \approx 4.6 = \sqrt{3N} = \sqrt{3 \times 7}$$

  - where

R_i = radius of the inner cells; D_i = reuse distance for the inner cells;
R_o = radius of the outer cells; D_o = reuse distance for the outer cells;

Reuse Partitioning (Cont.)



Reuse Partitioning (Cont.)

$$D_o/R_o = 4.6; \quad D_i = \sqrt{3\times 3}R_o; \leftarrow$$ **3-cell reuse for inner cells**

- $D_i/R_i = 4.6 \rightarrow D_i/R_i = 4.6 = \sqrt{3\times 3}R_o/R_i \Rightarrow R_i = 0.65R_o$
- The area of an inner cell:

$$A_i = (0.65)^2 A_o = 0.43A_o$$

- Assume a homogenous traffic distribution
- If N_c channels are available in a cell (inner and outer cells)
  - 0.43 N_c channels should be assigned to the inner cells
  - 0.57 N_c channels should be assigned to the outer cells
- The number of total channels available in the system is

$N_T = (0.57\times 7 + 0.43\times 3)N_c = 5.28N_c$ ← **Equivalent $N = 5.28$**

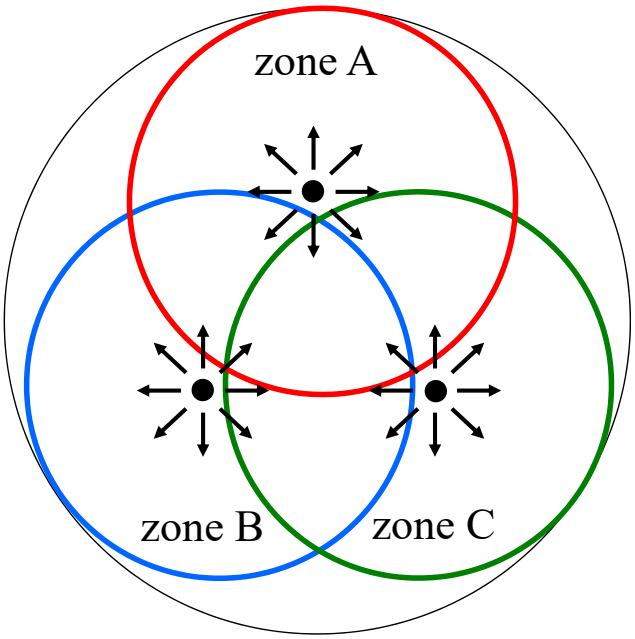
- If only the 7-cell reuse plan is used: $N_c' = N_T/7 = 0.754N_c$
- Improvement: $(N_c - N_c')/N_c' = 32.6\%$

Microcellular Systems

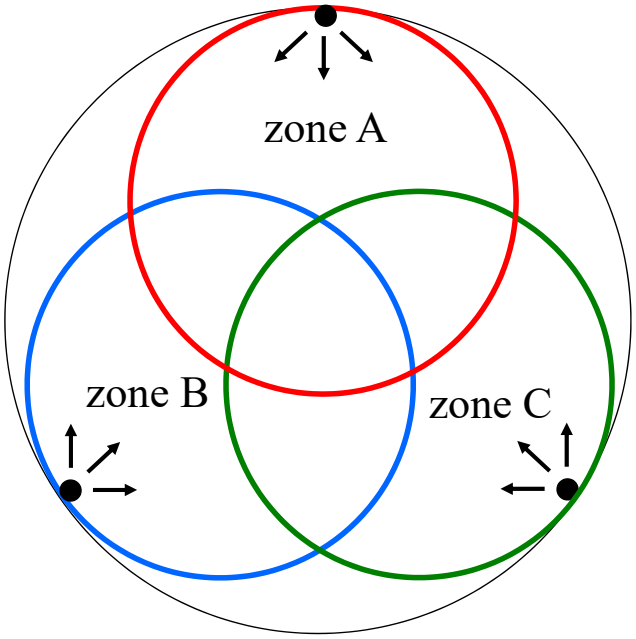
Microcellular Systems

- The microcellular systems can be deployed with multiple omni-directional or directional antennas within each cell
  - All zones sites receive the signal from an MS on the **reverse** link
  - Only the zone site receiving the **largest** signal will transmit to the MS on the **forward** link
  - **Center excited zones**: antennas locate on the center of zones
  - **Edge excited zones**: antennas locate on the edge of zones

Microcellular Systems (Cont.)



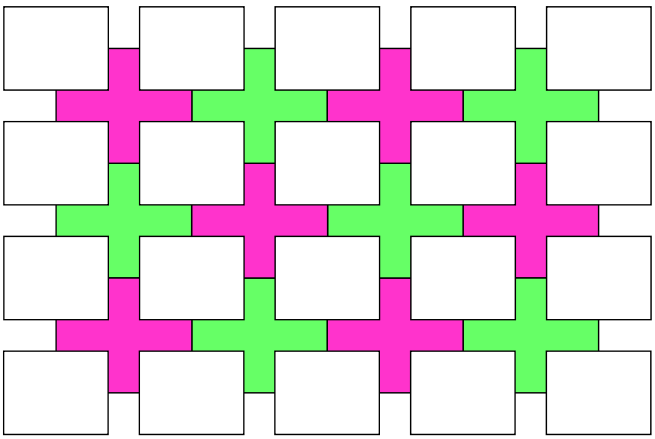
Center excited



Edge excited

Street Microcellular Systems

- Manhattan microcell deployment: BSs are located at every **intersection**
  - In order to eliminate the **corner effect**
- The co-channel interference is dominated by the **LOS** co-channel interferers (corner effect)



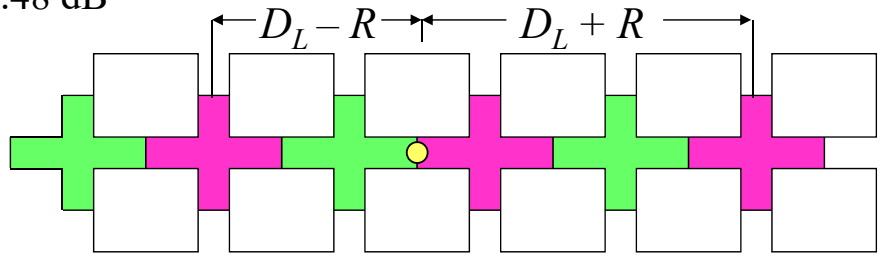
Street Microcellular Systems (Cont.)

- Using the **two-slop** path loss model, the worse case C/I is:

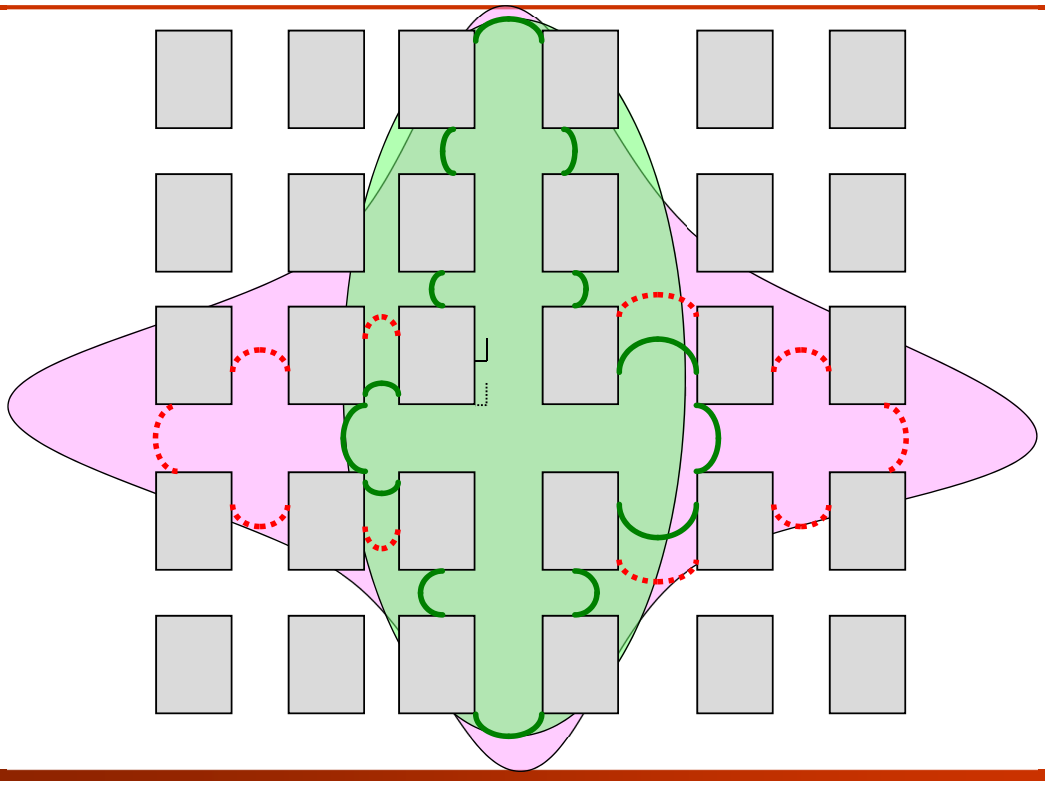
$$\frac{C}{I} = \frac{R^{-a}(1+R/g)^{-b}}{(D_L-R)^{-a}(1+(D_L-R)/g)^{-b}+(D_L+R)^{-a}(1+(D_L+R)/g)^{-b}}$$

$$= \frac{1}{(\frac{D_L}{R}-1)^{-a}\left[(\frac{g}{R}+\frac{D_L}{R}-1)/(\frac{g}{R}+1)\right]^{-b}+(\frac{D_L}{R}+1)^{-a}\left[(\frac{g}{R}+\frac{D_L}{R}+1)/(\frac{g}{R}+1)\right]^{-b}}$$

  - For 2-cell reuse: $D_L/R = 4$, $R = 100$ m, $g = 150$ m, $a = b = 2 \Rightarrow$ 13.3 dB
  - For 4-cell reuse: $D_L/R = 8$, $R = 100$ m, $g = 150$ m, $a = b = 2 \Rightarrow$ 25.48 dB

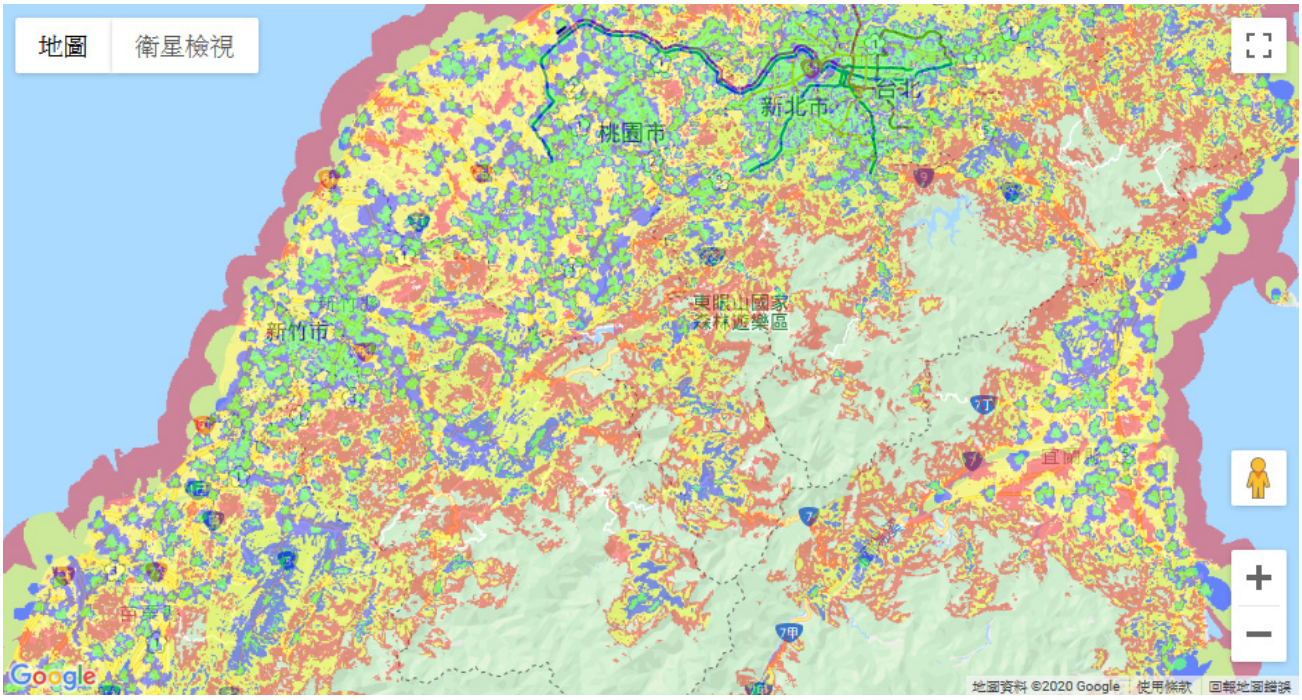


Street Microcellular Systems (Cont.)



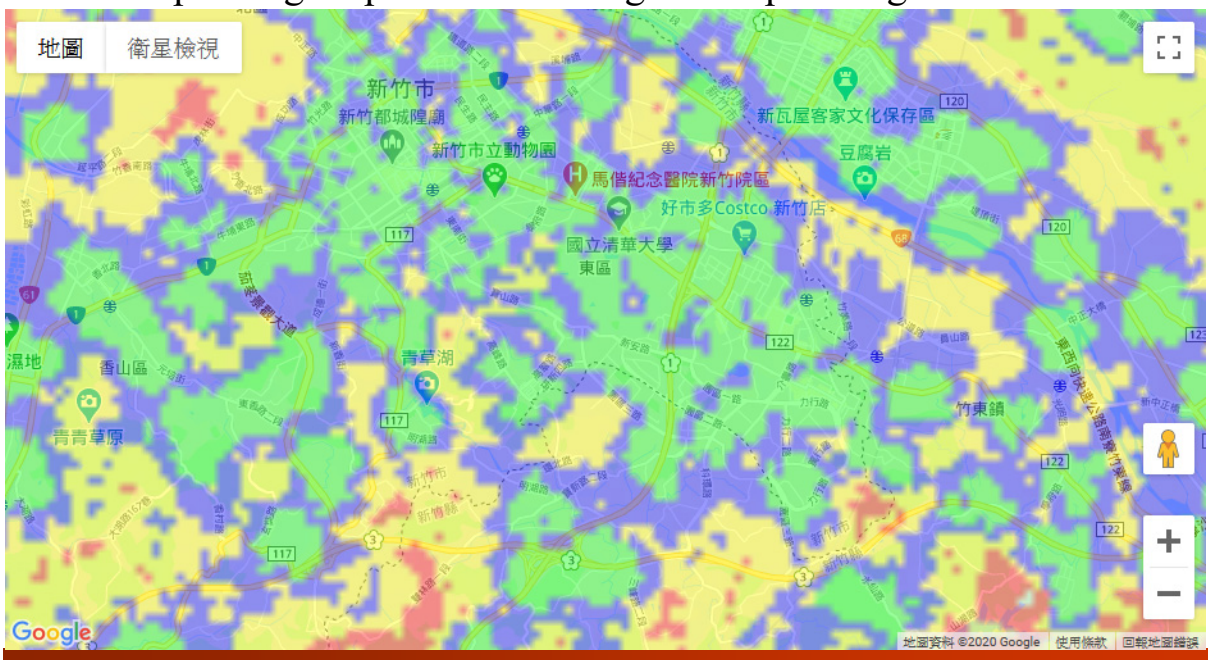
Cell Deployment

Deployment Planning



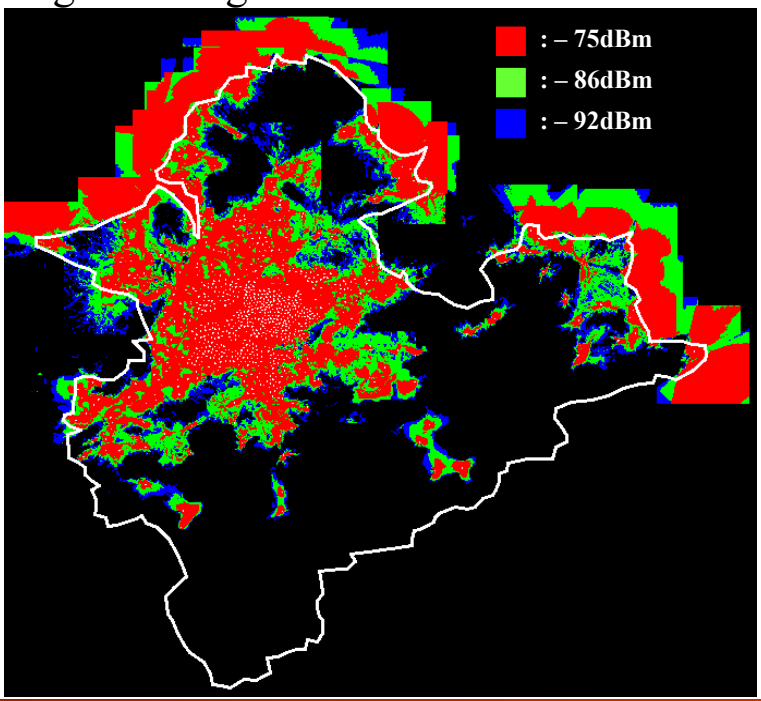
Deployment Planning (Hsinchu City)

- The service coverage map is only a reference
  - Depending on parameter setting on the planning tool



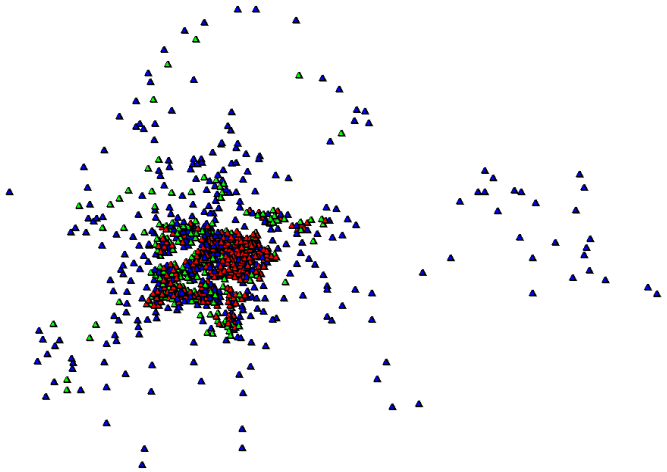
Deployment Planning (Taipei/New Taipei Cities)

- Received signal strength



Deployment Planning (Taipei/New Taipei Cities)

- In practical, the BS locations do not follow the hexagonal geometry

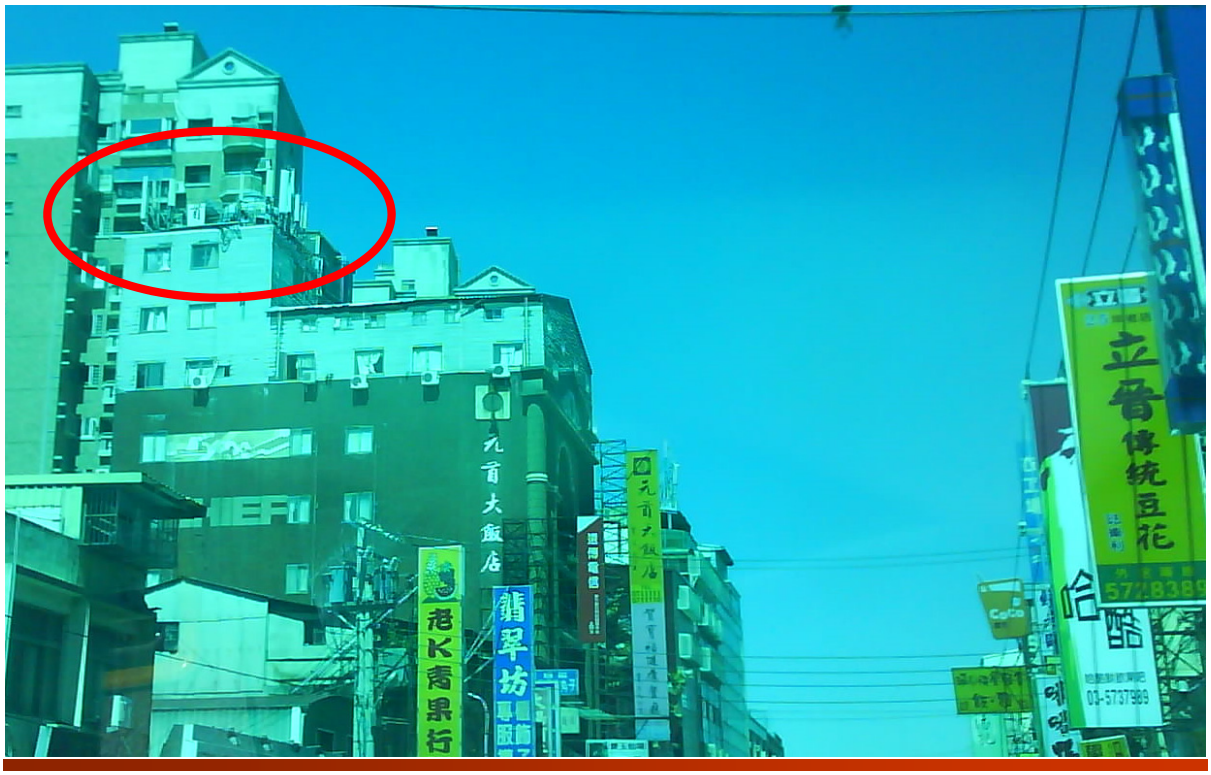


Some Examples

2-Sector Cell

3-Sector Cell

3-Sector Cell (Cont.)

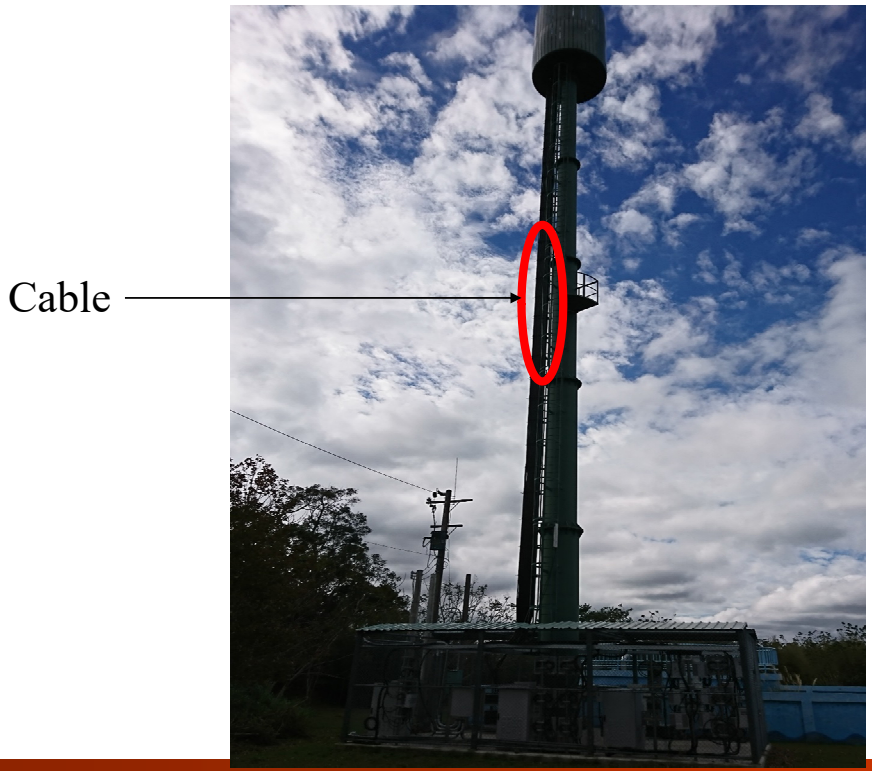


3-Sector Cell (Cont.)

Low-tier System (PHS)

Hidden Base Station

Hidden Base Station (Cont.)



Hidden Base Station at NTHU

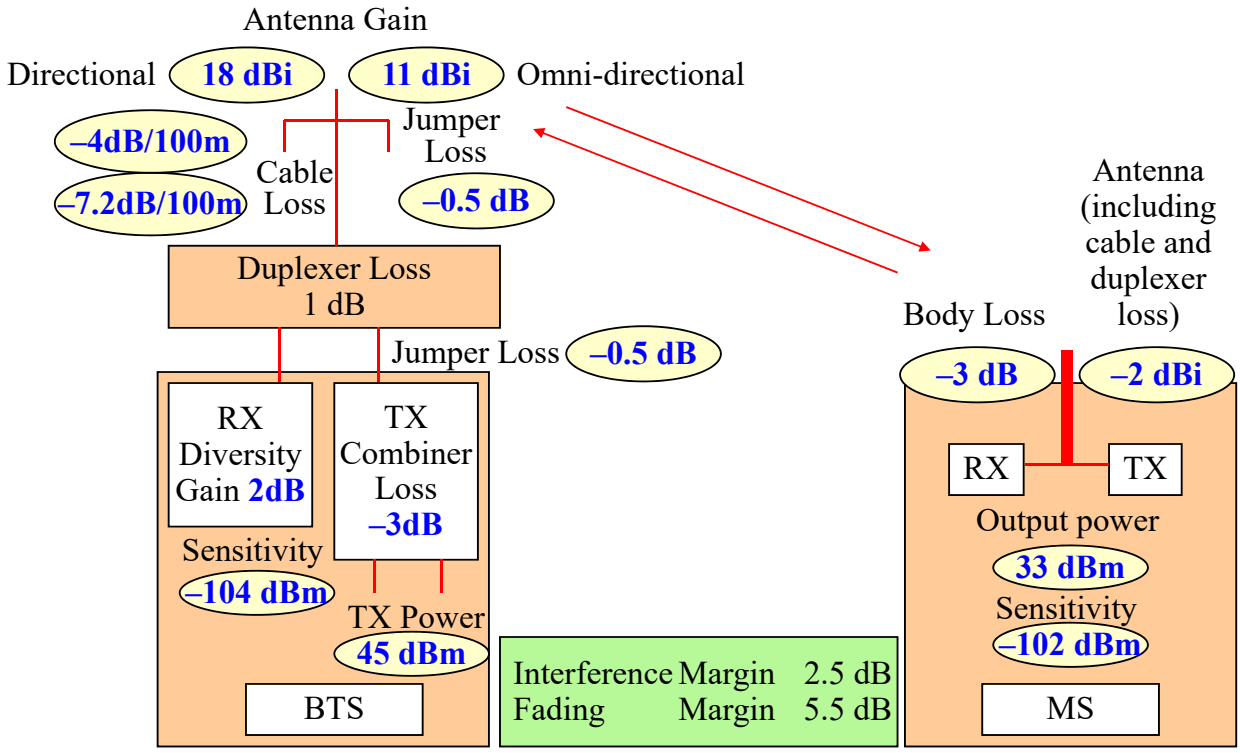
Hidden Base Station at NTHU (Cont.)

Antenna Systems

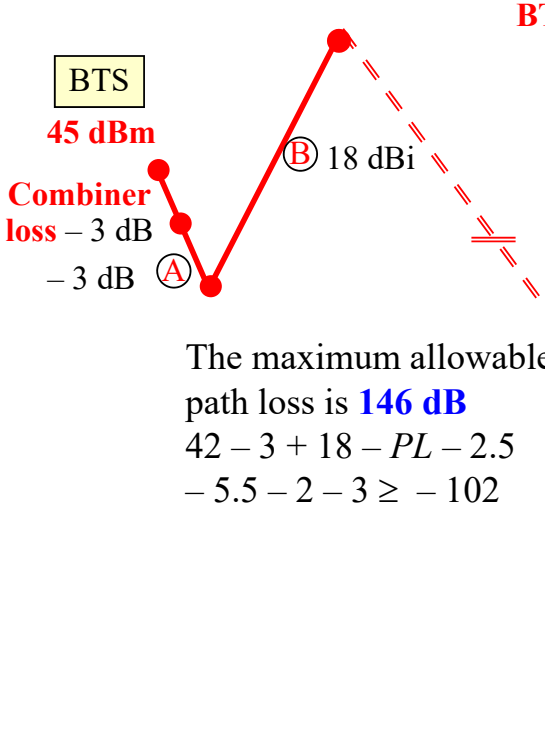
Antenna Systems – RF Cables

Link Budget

Link Budget



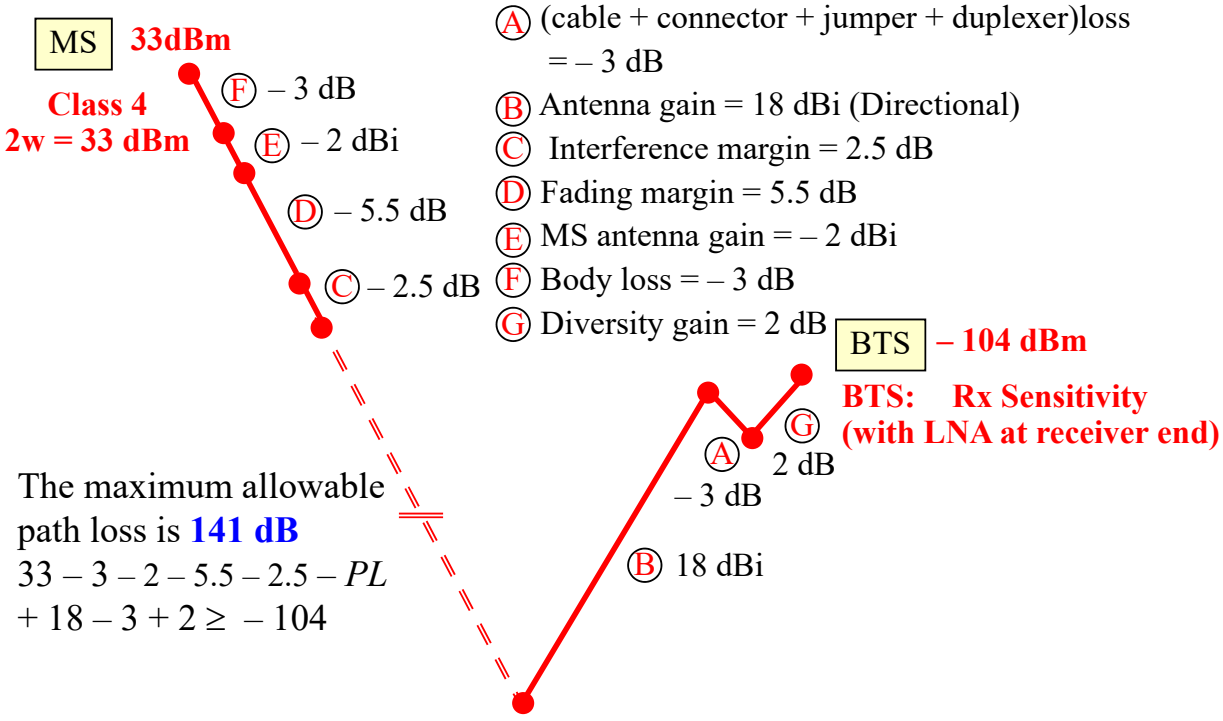
Down (Forward)-Link Link Budget



BTS power at combiner output : 15w = 41.76 dBm

- (A) (cable + connector + jumper + duplexer) loss = – 3 dB
- (B) Antenna gain = 18 dBi (Directional)
- (C) Interference margin = 2.5 dB
- (D) Fading margin = 5.5 dB
- (E) MS antenna gain = – 2 dBi
- (F) Body loss = – 3 dB

Up (Reverse)-Link Link Budget



Link Quality Measurement and Handoff Initiation

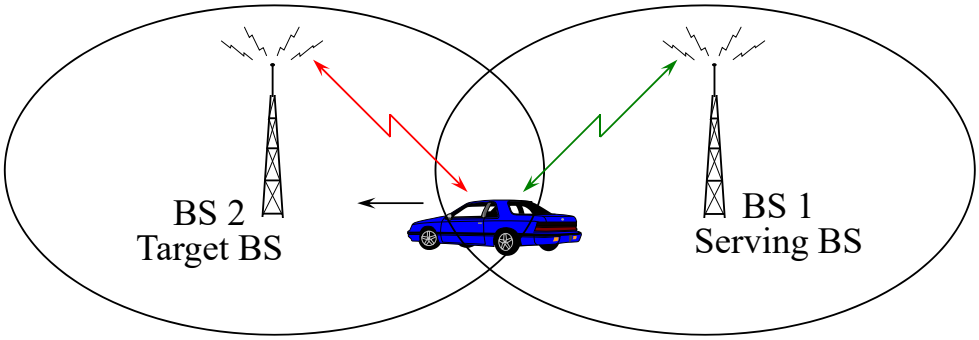
Handoff

- **Handoff** is the procedure of an MS to change the **serving BS** from one to another due to the mobility of the MS
- When a new call arrives, an MS must be connected to a suitable BS
- **Inter-cell handoff**: when an MS traverses a cell boundary
- **Intra-cell handoff**: when the link with the serving BS is affected by excessive interference, while another link with the same BS can provide better quality
- The handoff process consists of two stages:
  - Link quality evaluation and handoff initiation
  - Allocation of radio and network resources

Inter-cell Handoff

Handoff (Cont.)

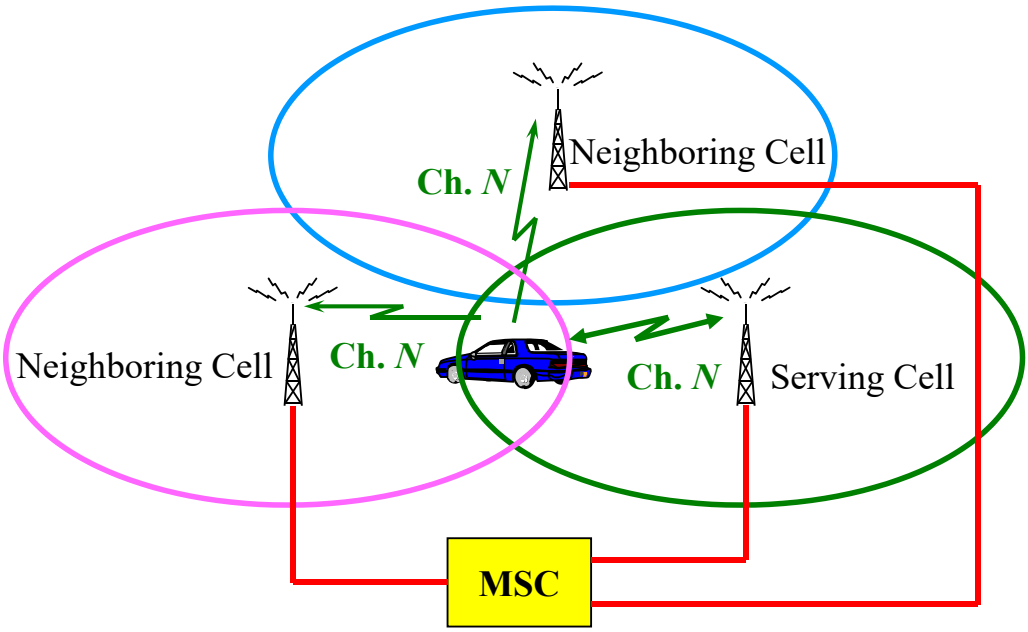
- There are three types of handoff in mobile communication systems:
  - **Network controlled (NCHO)** (AMPS)
  - **Mobile assisted (MAHO)** (2G GSM, 3G and 4G)
  - **Mobile controlled (MCHO)** (Low-tier: PACS, DECT, PHS)



Network Controlled Handoff

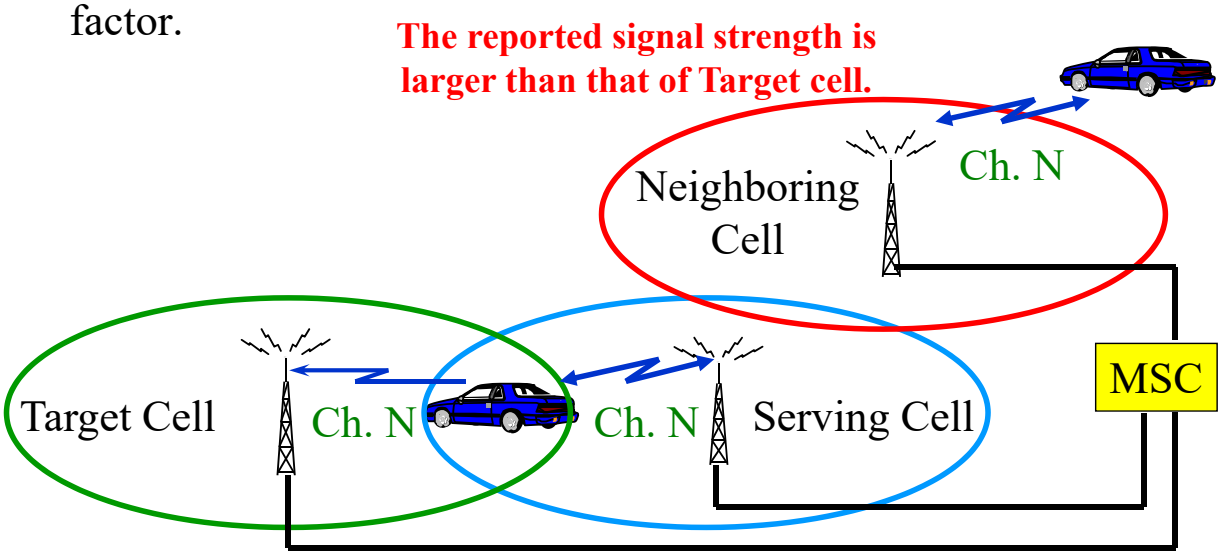
- Network controlled handoff:
  - The serving cell monitors the signal of an MS and detects that the MS is near the cell boundary
  - The neighboring cells monitor the signal of the MS and report to the network controller
  - The network controller selects the optimal cell for handoff and selects a frequency channel for the MS
  - The serving cell directs the MS handoff to the new frequency channel

Network Controlled Handoff (Cont.)



Question

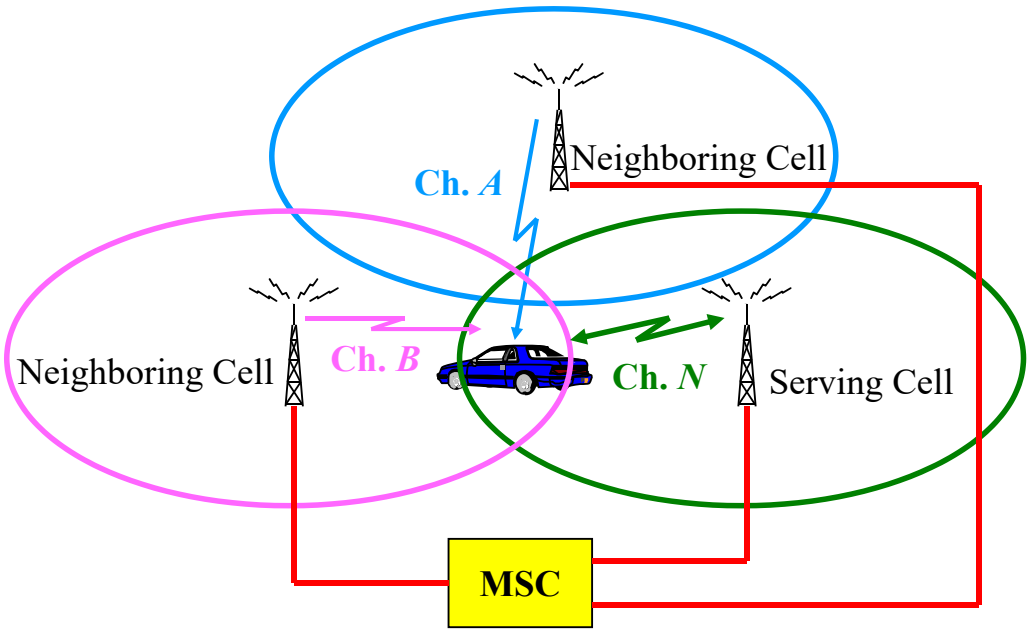
- **Question:**
  - Is it possible that the target BS is wrongly selected for NCHO?
- Yes, it is possible for a system with a small frequency reuse factor.



Mobile Assisted Handoff

- Mobile assisted handoff:
  - An MS monitors the signals of the neighboring cells and reports to the serving cell
  - The serving cell detects that the MS is near the cell boundary
  - According to the information from the MS, the network controller selects the optimal cell for handoff and selects a frequency channel for the MS
  - The serving cell directs the MS handoff to the new frequency channel

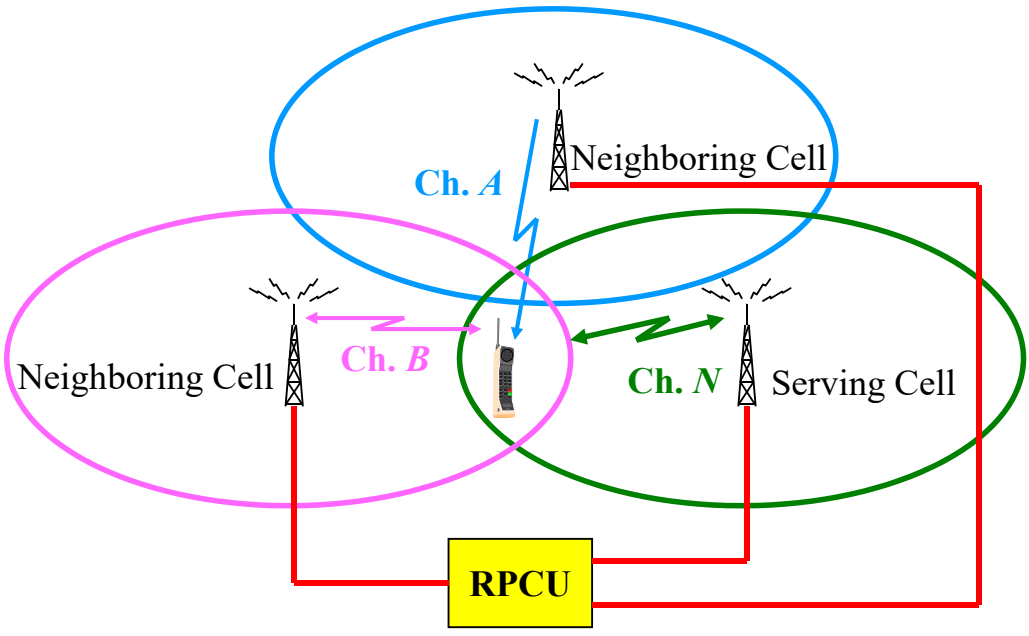
Mobile Assisted Handoff (Cont.)



Mobile Controlled Handoff

- Mobile controlled handoff:
  - An MS monitors the signals of the neighboring cells
  - The MS detects that a neighboring cell has better quality than the serving cell
  - The MS selects a new frequency channel and accesses to the target cell
  - The target cell accepts the MS and becomes the new serving cell
  - The new serving cell informs the old serving cell to terminate the link related to the MS

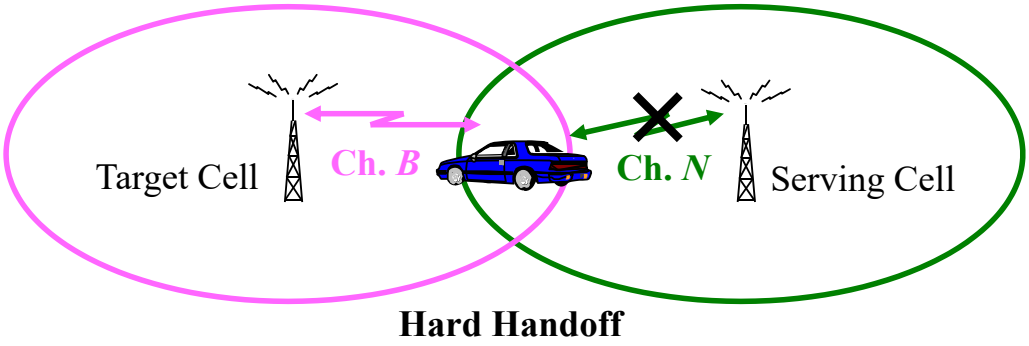
Mobile Controlled Handoff (Cont.)



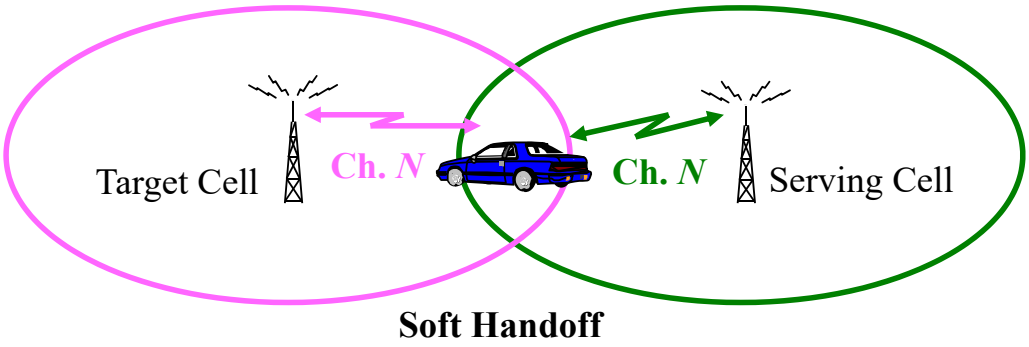
Hard/Soft Handoff

- According to the link establishment, handoff can also be classified into two types
  - Hard handoff
    - Terminate the old link and then establish the new link
    - Only one link exists at any instant
  - Soft handoff
    - Establish the new link and then terminate the old link
    - Multiple links may exist at any instant

Hard/Soft Handoff (Cont.)



Hard Handoff



Soft Handoff

Question

- **Question:**
  - Can soft-handoff be realized in an FDMA/TDMA system?
- No, the frequency reuse factor of an FDMA/TDMA system is larger than 1 $\Rightarrow$ The serving cell and the target cell must use different frequency channels
  - An MS generally has only one transceiver $\Rightarrow$ Can access only one frequency channel
- Generally, soft-handoff can only be realized in CDMA systems where the applied frequency reuse factor equal to 1

Handoff Initiation Algorithms

Signal Strength Based Handoff

- Traditional MAHO algorithms:
  - Calculate the time averaged signal strength $\left\langle \left|\tilde{r}_i(t)\right|^2 \right\rangle$ for the N neighboring BSs, BS_i , $i = 0, \ldots, N-1$
  - Reconnect the MS to an alternate BS whenever
    - The signal strength of the target BS exceeds that of the serving BS by at least ***H* dB**
- A handoff is performed between BS_0 and BS_1, when

$$Y_1(n) > Y_0(n) + H \quad \text{if the serving BS is } BS_0$$
$$Y_0(n) > Y_1(n) + H \quad \text{if the serving BS is } BS_1$$

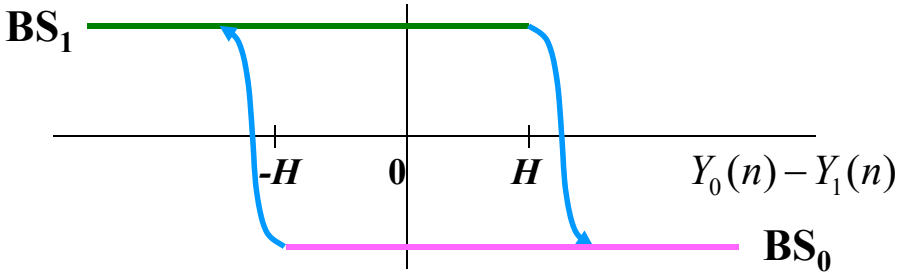
  - $Y_0(n)$: the estimated mean signal strength (in dBm) of BS_0
  - $Y_1(n)$: the estimated mean signal strength (in dBm) of BS_1
  - H denotes the **hysteresis** (in dB)

Signal Strength Based Handoff (Cont.)

- $$Y_0(n) = \frac{1}{M} \sum_{k=n-M+1}^{n} \left|\tilde{r}_0(kT_s)\right|^2_{(\text{dB})}$$
$$Y_1(n) = \frac{1}{M} \sum_{k=n-M+1}^{n} \left|\tilde{r}_1(kT_s)\right|^2_{(\text{dB})}$$

  Moving average

  - $\left|\tilde{r}_i(kT_s)\right|^2_{(\text{dB})}$: is the kth sample of the squared envelope (dBm)
  - T_s: the sampling period
  - M: the window length



Signal Strength Based with Threshold

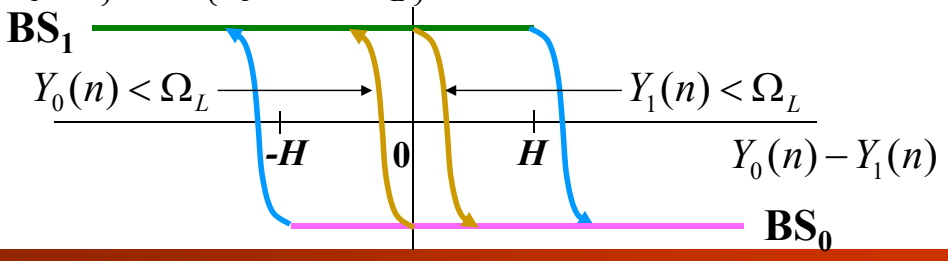
- Another scheme **encourages** a handoff whenever the signal strength of the serving BS **drops below** a threshold Ω_L
  - In order to reduce the probability of **dropped call**
- A handoff is performed between BS_0 and BS_1, when

$\{Y_1(n) > Y_0(n) + H\}$ and $\{Y_0(n) > \Omega_L\}$, if the serving BS is BS_0

$\{Y_1(n) > Y_0(n)\}$ and $\{Y_0(n) < \Omega_L\}$, if the serving BS is BS_0

$\{Y_0(n) > Y_1(n) + H\}$ and $\{Y_1(n) > \Omega_L\}$, if the serving BS is BS_1

$\{Y_0(n) > Y_1(n)\}$ and $\{Y_1(n) < \Omega_L\}$, if the serving BS is BS_1



Signal Strength Based with Threshold (Cont.)

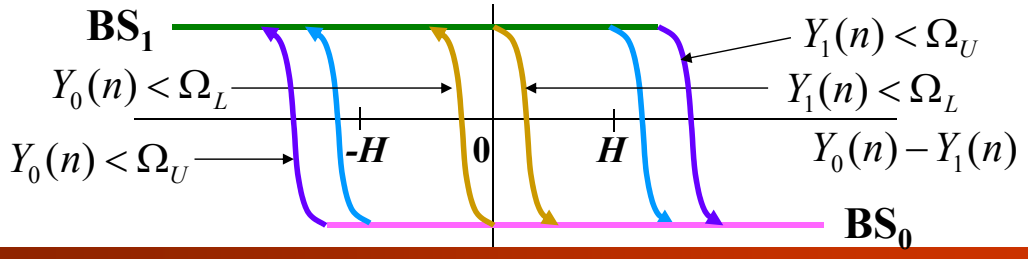
- Another scheme **discourages** a handoff when the signal strength of the serving BS **exceeds** a threshold Ω_U
  - In order to avoid unnecessary handoffs
- A handoff is performed between BS_0 and BS_1, when

$\{Y_1(n) > Y_0(n) + H\}$ and $\{\Omega_L < Y_0(n) < \Omega_U\}$, if the serving BS is BS_0

$\{Y_1(n) > Y_0(n)\}$ and $\{Y_0(n) < \Omega_L\}$, if the serving BS is BS_0

$\{Y_0(n) > Y_1(n) + H\}$ and $\{\Omega_L < Y_1(n) < \Omega_U\}$, if the serving BS is BS_1

$\{Y_0(n) > Y_1(n)\}$ and $\{Y_1(n) < \Omega_L\}$, if the serving BS is BS_1



Signal Strength Based with Direction Biased

- This algorithm incorporates the **moving direction** information into the handoff algorithm
  - To **encourage** handoff to the BS that the MS is **approaching**
  - To **discourage** handoff to the BS that the MS is **moving away**

  $A :=$ the set of BSs that the MS is approaching

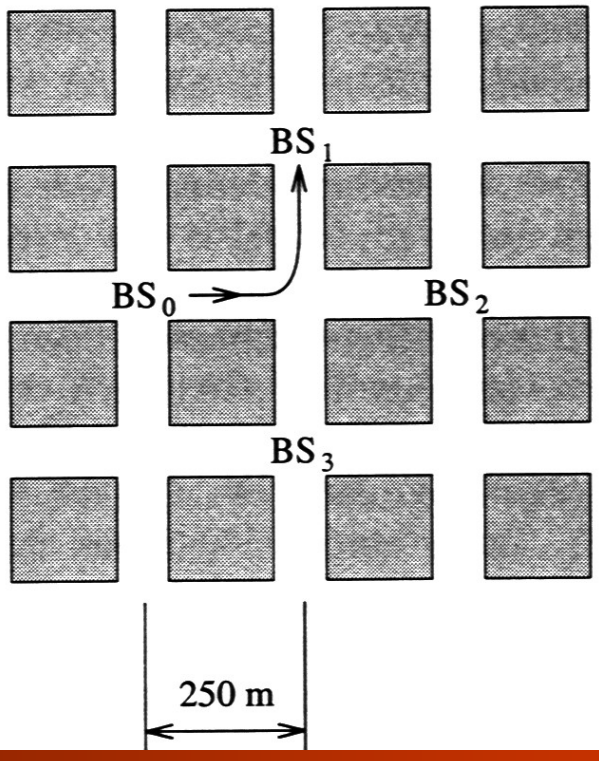
  $\Re :=$ the set of BSs that the MS is moving away from
- A handoff is performed form BS_s to BS_j
  - If $BS_j \in \Re$ $\quad Y_j(n) > X_s(n) + H, \quad \text{if } BS_s \in \Re$

    $Y_j(n) > X_s(n) + H_d, \quad \text{if } BS_s \in A$
  - If $BS_j \in A$ $\quad Y_j(n) > X_s(n) + H_e, \quad \text{if } BS_s \in \Re$

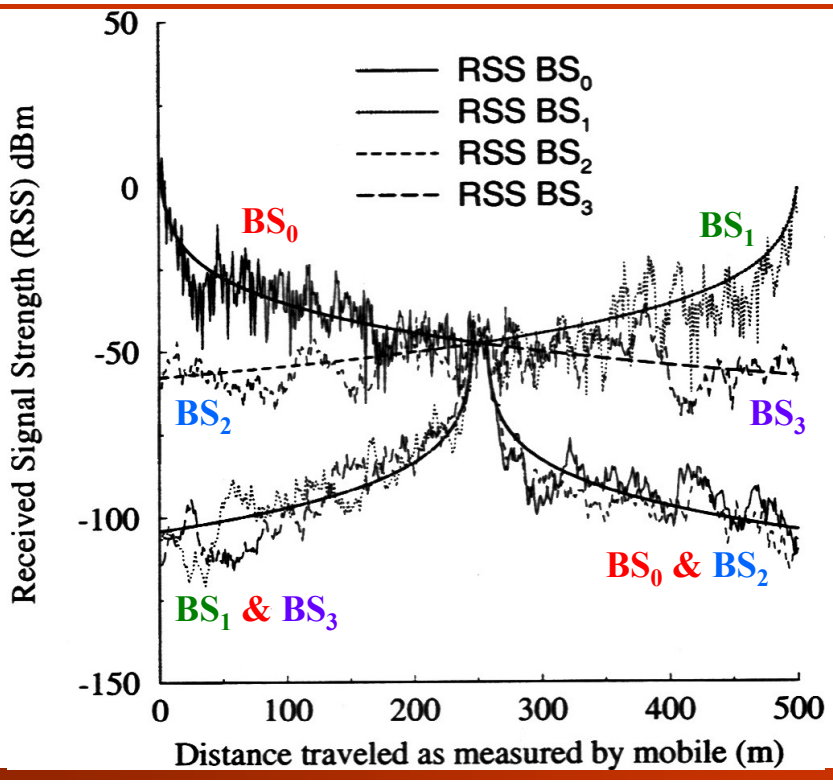
    $Y_j(n) > X_s(n) + H, \quad \text{if } BS_s \in A$
- H_e: encouraging hysteresis; H_d: discouraging hysteresis

$$H_e \le H \le H_d$$

Handoff in Street Microcellular Systems



Handoff in Street Microcellular Systems (Cont.)



CIR-Based Link Quality Measurements

- The **received signal strength (RSS)** based algorithms cannot ensure the link performance, since

$$RSS = C + I + N$$

  - where C: carrier power; I: interference power; N: noise power
- A link with a large RSS may have bad quality
  - Weak carrier signal plus strong co-channel interference
- A link with a small RSS may have good quality
  - Small carrier power plus very weak co-channel interference

CIR-Based Link Quality Measurements (Cont.)

- Some radio resources allocation and handoff algorithms are based on
  - The received **carrier-to-interference plus noise ratio** $C/(I + N)$
    - An estimation of $C/(I + N)$ is needed
  - The received **signal quality**
    - The signal quality may be obtained **after** demodulation or decoding

Channel Assignment Techniques

Performance Measurement

- Various performance measures are used to evaluate the cellular systems
  - **Probability of new call blocking**:

$$P_b = \frac{\text{number of new calls blocked}}{\text{number of new call arrivals}}$$

  - **Probability of forced termination**:

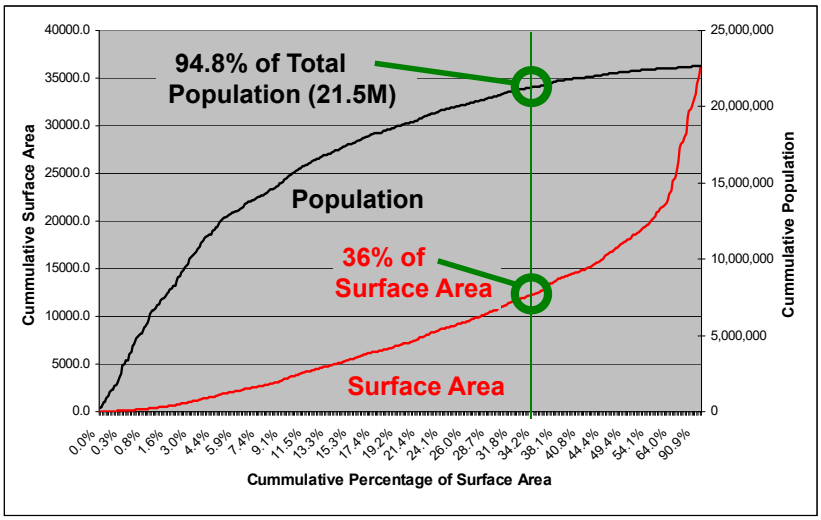
$$P_f = \frac{\text{number of handoff calls blocked}}{\text{number of handoff attempts}}$$

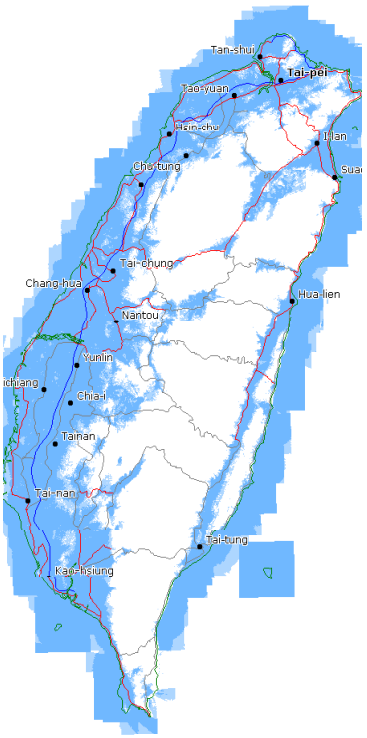
  - **Radio coverage**:
    - Percentage of **geographic area**
    - Percentage of **population**

Depending on the number of available channels in a cell

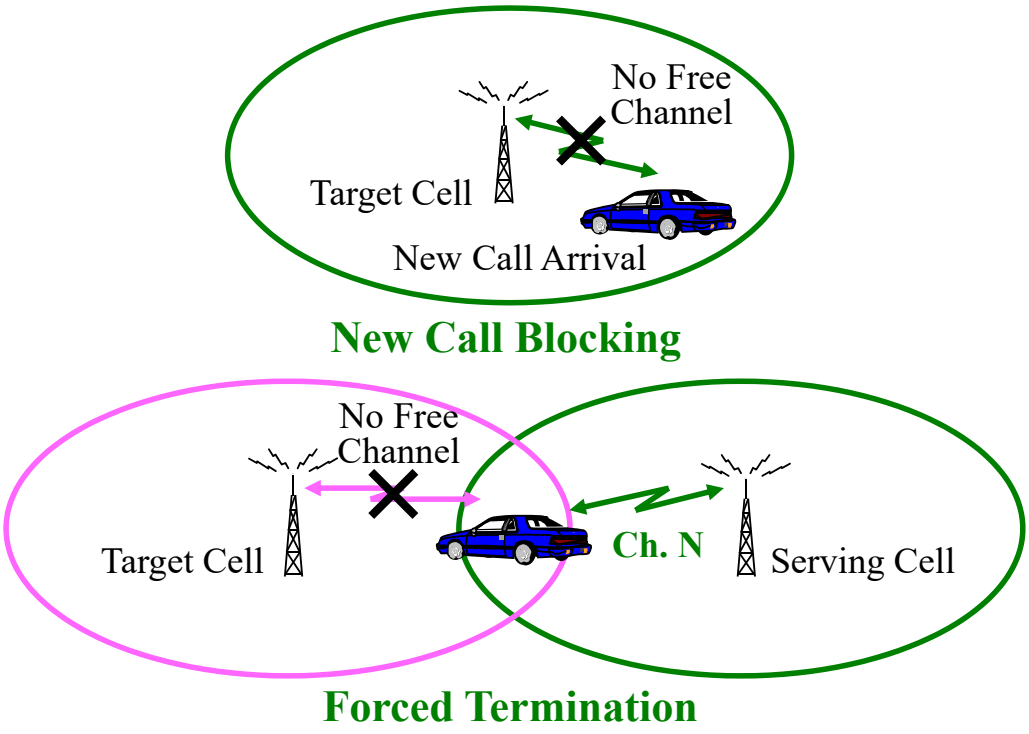
Performance Measurement (Cont.)

- In general, the percentage of population is more important than the percentage of geographic area.





Performance Measurement (Cont.)



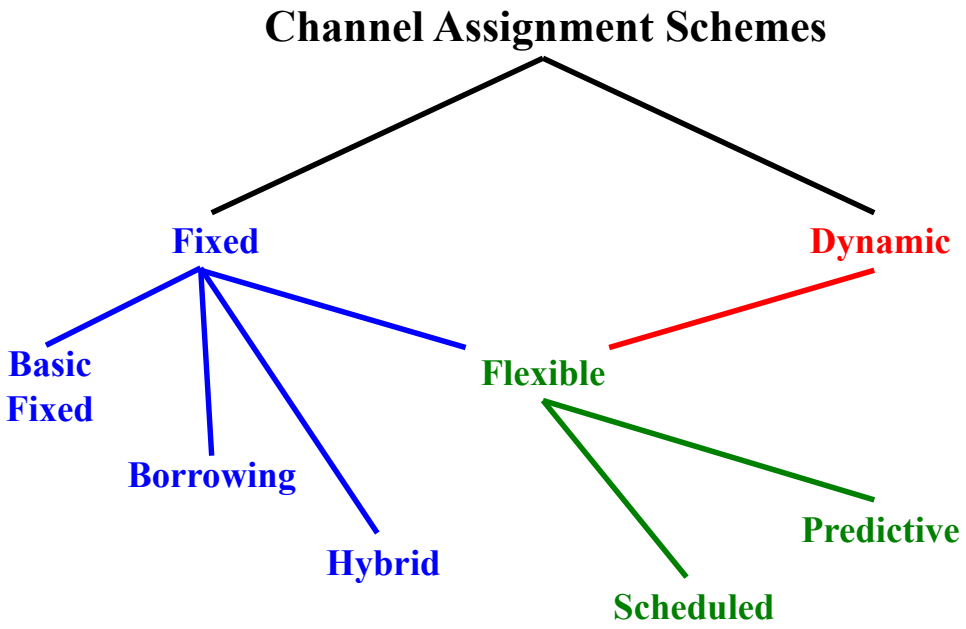
Performance Measurement (Cont.)

- **Received signal quality**:
  - *C*/*I*, BER or FER
  - Data: **BER**; Voice: **MOS (Mean Opinion Score)**
- **Grade of service (GoS)**:

$$GoS = \frac{P_b R_N}{(R_N + R_H)} + \frac{P_f R_H}{(R_N + R_H)}$$

  - where R_N and R_H are the new call and handoff arrival rates
  - New call and handoff can also be differently weighted

Channel Assignment Schemes



Fixed/Dynamic Channel Assignment

Fixed Channel Assignment

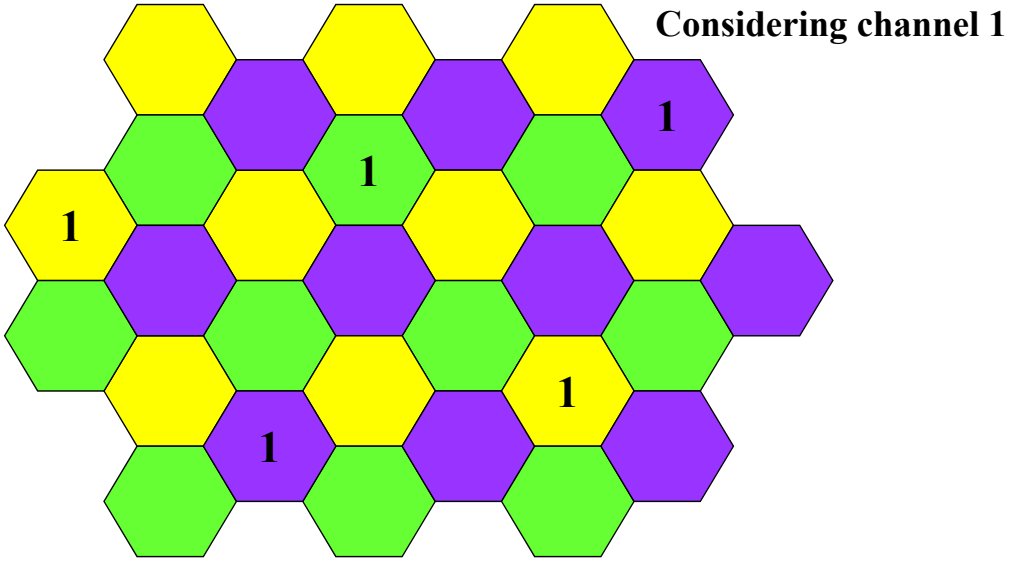
- **Macrocellular** systems typically use **fixed channel assignment (FCA)**
  - Disjoint sets of the available channels are **permanently** allocated to the cells
  - The number of channels is according to the estimated traffic load in a cell
  - The size of reuse clusters is determined by the co-channel reuse constraint
  - FCA is spectrally **inefficient** because the number of channels allocated to a cell is fixed without any flexibility

Distributed Dynamic Channel Assignment

- In **microcellular** systems, the propagation environment is highly erratic, and the traffic load is temporally variant
- The decrease in cell sizes implies an increase in handoff traffic
- Microcellular systems typically use **distributed dynamic channel assignment (DCA)**
  - Allow any cell to use any channel that does not violate the co-channel reuse constraint
  - Permit adaptation to temporal traffic variation
  - **Distributed control** reduces the required **computation** and **communication** among BSs
  - The distributed DCA schemes may yield an **inefficient** arrangement of channels under **heavy traffic loading**

Distributed Dynamic Channel Assignment(Cont.)

- Minimum frequency reuse factor = 3
- Distributed DCA does not guarantee the minimum frequency reuse ⇒ **inefficient**



Fully Decentralized DCA-Minimum Interference

- The **minimum interference (MI)** scheme has been incorporated into the **CT-2** and **DECT** systems (TDD systems, up-link and down-link use the **same frequency channel**)
  - The MS signals the BS with the strongest paging signal to request for a channel
  - The BS measures the interference levels on all channels that it is not already using
  - The MS is assigned the channel with the **minimum interference**
- This policy coupled with mobile controlled handoff (MCHO) guarantees good performance

Centralized Dynamic Channel Assignment

Centralized Dynamic Channel Assignment

- The DCA for Macrocellular systems typically is **centralized**:
  - Require centralized control with **system-wide** channel information
  - Can theoretically provide the **best** performance
  - **Enormous** amount of computation and communication among BSs makes the centralized DCA schemes **impractical**
  - Provide a useful **benchmark** to compare the more practical decentralized DCA schemes

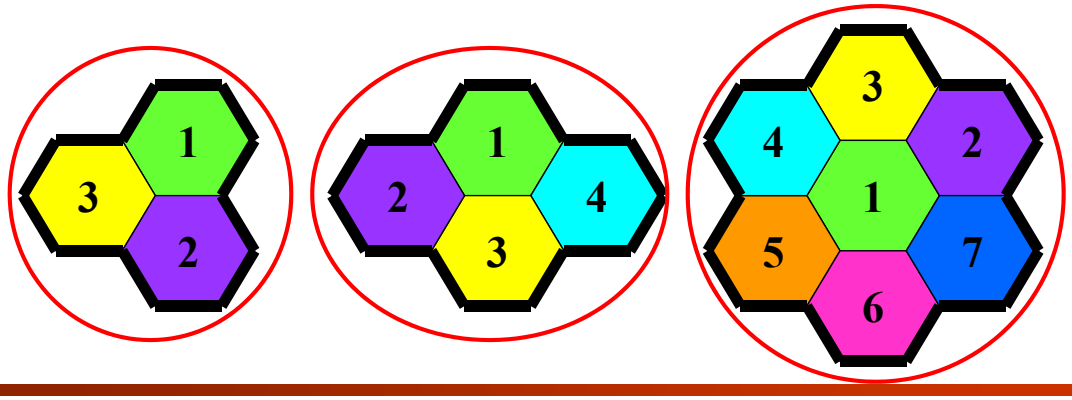
Centralized DCA-Maximum Packing (MP)

- **Maximum packing (MP)** requires a controller with **system-wide** channel information along with the ability to perform **call rearrangements**
- With the MP policy, a new call is blocked only if there is no **global rearrangement** of calls to channels that will accommodate the new call
- The MP policy has the ability to serve all calls in a network with the **minimum** number of channels
- The MP policy can yield the **lowest** new call blocking rate and forced termination rate

Centralized DCA-Maximum Packing(MP)(Cont.)

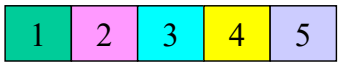
- Upon a call arrival in a particular cell, the MP policy checks to see if **all reuse clusters** that contain that cell have **at least one** channel available
  - If so, the call can be accommodated through channel rearrangements
  - Otherwise, the call is blocked

Total available channels in each reuse cluster = Total system channels



Centralized DCA-Maximum Packing(MP)(Cont.)

- Consider the simple system consisting of five cells with co-channel cells being separated by at least two cells
  $\Rightarrow$ Three reuse clusters: CL_1=(1, 2, 3), CL_2=(2, 3, 4), CL_3=(3, 4, 5)



- When a call arrives in cell 2
  - It can be accommodated if there is at least one channel available in clusters **CL_1 and CL_2**: CL_1=(1, **2**, 3), CL_2=(**2**, 3, 4)
- Cell 1: 1, 2; Cell 2: 4, 5, 6; Cell 3: 7, 8, 9; Cell 4: 2, 3;
  - CL_1: channel 3 is available; CL_2: channel 1 is available;
  - "Cell 1: 1$\rightarrow$3" and "Cell 2: use 1, 4, 5, 6"
  - "Cell 4: 3$\rightarrow$1" and "Cell 2: use 3, 4, 5, 6"

Centralized DCA-MAXMIN Scheme

- With the **MAXMIN** scheme, an MS is assigned a channel that maximizes **the minimum C/I** that **any MS** in the system will experience at the time of assignment
  - To prevent the worst *C*/*I* of all MSs below the threshold
- The *C*/*I* of MS_i at its serving BS is

$$\Lambda(\mathbf{d})_{(dB)} = \Omega(d_i)_{(dB)} - 10\log_{10}\sum_{k\in I} 10^{\Omega(d_k)_{(dB)}/10}$$

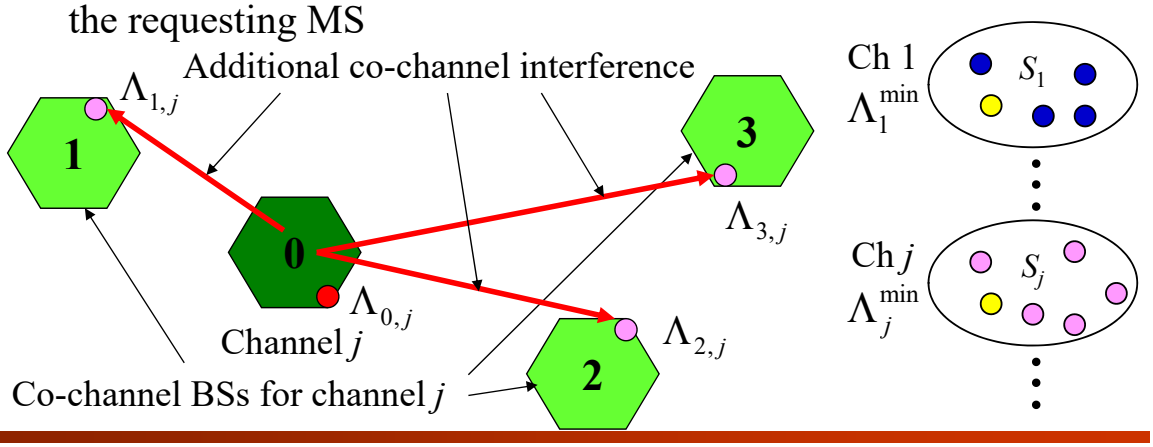
  - $\Omega(d_i)_{(\mathrm{dB})}$: the received desired signal power of MS_i
  - $\Omega(d_k)_{(\mathrm{dB})}$: the received interference power of MS_i
  - d_i: the distance between MS_i and the corresponding serving BS
  - d_k: the distance between MS_i and the co-channel BS k
  - I: the set of all MSs other than MS_i that are using the **same channel**

Centralized DCA-MAXMIN Scheme (Cont.)

- An MS that requires service is assigned the channel j that gives

$$\max_{j \in C} \min_{i \in S_j} \{\Lambda_i\}$$

  - where i and j index the set of MSs and channels
  - C: the set of channels that are available at the requested BS
  - S_j: the set of all MSs in service and using the channel j, including the requesting MS



Practical Implementation Issues

Hybrid FCA/DCA Schemes

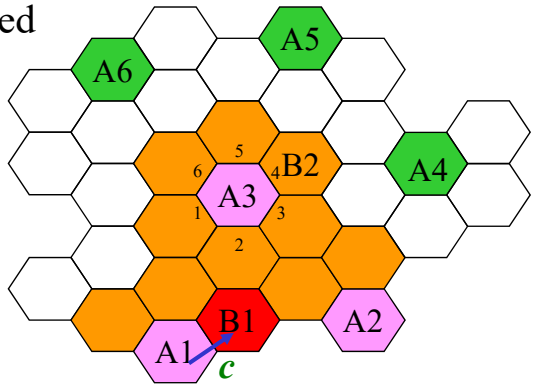
- The DCA schemes perform very well under **light non-stationary non-homogeneous traffic**
- The FCA scheme outperforms most of the DCA schemes under the condition of **uniformly heavy traffic**
- The **hybrid FCA/DCA** schemes provide a compromise between FCA and DCA
- **Dynamic Channel Reassignment (DCR)**:
  - Each cell is assigned a number of **fixed channels**
  - The remaining channels are available for **DCA**
  - Fixed channels are used first to accommodate call requests
  - Calls that cannot be serviced by the fixed channels are offered to the dynamically assigned channels

Borrowing Schemes

- For the **borrowing** scheme, the channels that are assigned to each BS are divided into two sets
  - **Fixed**: the channels can only be used by the BS they are assigned to
  - **Borrowable**: the channels could be borrowed by a neighboring BS if necessary
  - Calls are serviced by using the **fixed channels** whenever possible
  - To borrow a channel, the channel is borrowed from **the neighboring BS** having the **largest** number of available channels for borrowing
  - To use the borrowed channels, a BS should not violate **the co-channel reuse constraint**

Borrowing with Directional Locking (BDCL)

- **Channel locked**:
  - The channel usage should not violate the co-channel reuse constraint
  - A channel is available for borrowing if it is unused in the adjacent cells and the other **two nearest** co-channel cells
  - If cell B1 borrows a channel *c* from cell A1, then
    - Cells A1, A2, and A3 are locked from using channel *c*
  - Being locked, channel *c* can **neither be used** to service in these three cells **nor be borrowed from** these three cells

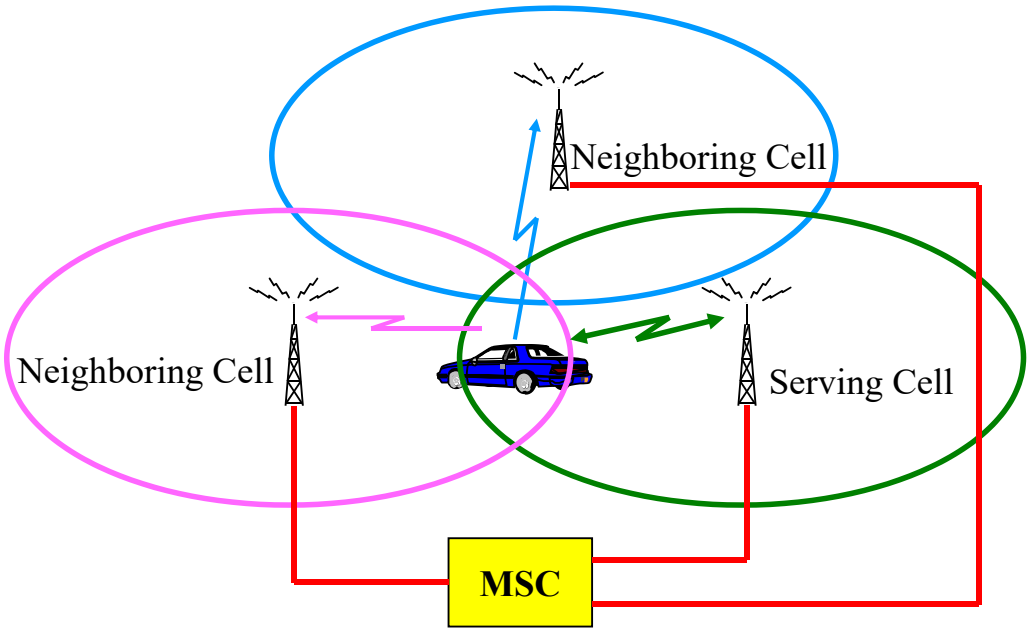


Directed Retry and Directed Handoff

- Exploits the **overlapping** nature of cells in practical cellular systems
  - Some percentage of MSs can establish a suitable link with **more than one** BS
- **Directed retry (DR)**: for initial calls
  - If a BS does not have an idle channel available to service a call

  ⇒ The MS tries to acquire an idle channel in any other cell that can provide a satisfactory signal quality
- **Directed handoff (DH)**: for handoff calls
  - Direct some of the ongoing calls in a heavily loaded cell to an adjacent cell that is carrying a relatively light load
- FCA in conjunction with DR and DH is a preferred scheme

Directed Retry and Directed Handoff (Cont.)



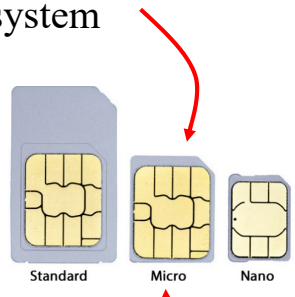
Handoff Priority

- **The forced termination of an ongoing call is worse than the blocking of a new call**
- Two possible methods for achieving **handoff priority**:
  - **Guard channels**: a fraction of the channels are **reserved** for handoff requests only
  - **Handoff queuing**: when no channel is available for handoff, the handoff request is placed in a **queue** with the target BS while the MS maintains a radio link with its serving BS
- Both methods could decrease the probability of **dropped calls**
- The impact of "guard channels" on the probability of new call blocking depends on the amount of reserved channels
- "Handoff queuing" has only a slight increase in the probability of new call blocking

Subscriber Identification

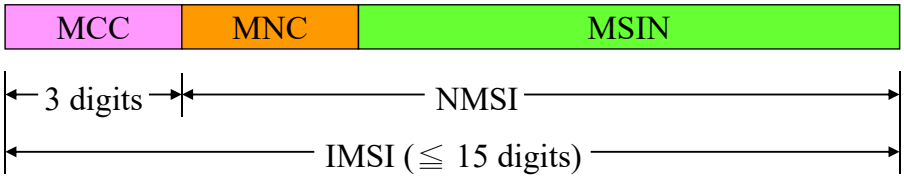
2G-GSM Subscriber Identification

- There are **four identifications** related to a mobile subscriber
  - **IMSI (International Mobile Subscriber Identity):** A unique IMSI is allocated to each mobile subscriber in the system
  - **TMSI (Temporary Mobile Subscriber Identity):** In order to support the **subscriber identity confidentiality service** (**location privacy**), a VLR (Visitor Location Register) may allocate a **unique** TMSI to visiting mobile subscribers
  - **MSISDN (Mobile Station International PSTN/ISDN Number):** For supporting any subscriber of the ISDN or PSTN to call any mobile station, an MSISDN is allocated based on the CCITT Recommendation E.164 numbering plan
  - **IMEI (Mobile Station Equipment Identity):** A unique IMEI is allocated to each mobile equipment (mobile phone)



IMSI

- A unique IMSI shall be allocated to each mobile subscriber
- IMSI is composed of three parts (shall not exceed **15 digits**):
  - **Mobile Country Code (MCC)** (3 digits): The MCC identifies uniquely the country of domicile of the mobile subscriber (Taiwan: 466)
  - **Mobile Network Code (MNC)** (2 digits): The MNC identifies the home GSM PLMN (Public Land Mobile Network) of the mobile subscriber
  - **Mobile Subscriber Identification Number (MSIN):** The MSIN uniquely identifies the mobile subscriber within a GSM PLMN.
- **National Mobile Subscriber Identity (NMSI)** = MNC+MSIN



TMSI

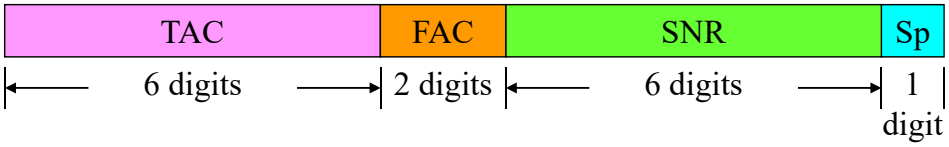
- The TMSI (consisting of **4 octets** (bytes)) assigned to a mobile subscriber is **random** and **time-variant** depending on the location of the user
  - The IMSI of a subscriber **cannot be traced** based on TMSI
  - It provides **location privacy** of a subscriber
- TMSI has only **local significance** (i.e., meaningful only within the VLR and the area controlled by the VLR)
- The VLR must be capable of **correlating** the IMSI of an MS and the current TMSI for that MS
- The TMSI shall only be allocated in **ciphered form**
  - To prevent being intercepted by any eavesdroppers or intruders

MSISDN

- The ISDN numbers for mobile stations should comply with the ISDN numbering plan in each country
- MSISDN is composed of three parts:
  - **Country Code (CC):** the country in which the mobile station is registered (Taiwan: 886)
  - **National Destination Code (NDC):** the area or network code in the contrary
  - **Subscriber Number (SN):** a unique number for identifying the mobile subscriber
- **National (significant) mobile number:** consisting of NDC and SN
  - For example: 886-**3-5715131**
- The CC and NDC will provide the **routing information**

IMEI

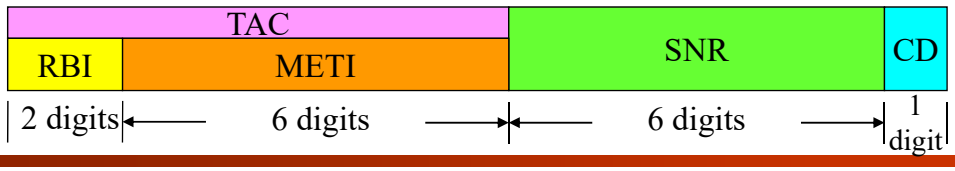
- IMEI (before 01/01/2003) is composed of the following elements (each element shall consist of decimal digits only):
  - **Type Approval Code (TAC)** (6 digits): identifies type approval number of a certain type of mobile phones
  - **Final Assembly Code (FAC)** (2 digits): identifies the place of manufacture/final assembly
  - **Serial Number (SNR)** (6 digits): is an individual serial number uniquely identifying each equipment within each TAC and FAC
  - **Spare digit** (1 digits): this digit shall be zero
- The TAC, FAC and SNR shall be **physically protected** against unauthorized change



IMEI (Cont.)

- IMEI format valid from 01/01/2003:
  - **Type Allocation Code (TAC)** (8 digits, NN XXXX YY):
    - NN (Reporting Body Identifier, RBI): the Reporting Body allocating the TAC (Reporting Body: an organization for the ME type approval certification)
    - XXXXYY (Mobile Equipment Type Identifier, METI): defines the ME type

  - **Serial Number (SNR)** (6 digits): is an individual serial number uniquely identifying each equipment within each TAC
  - **Check Digit** (1 digits): a function of all other digits in the IMEI



Roaming

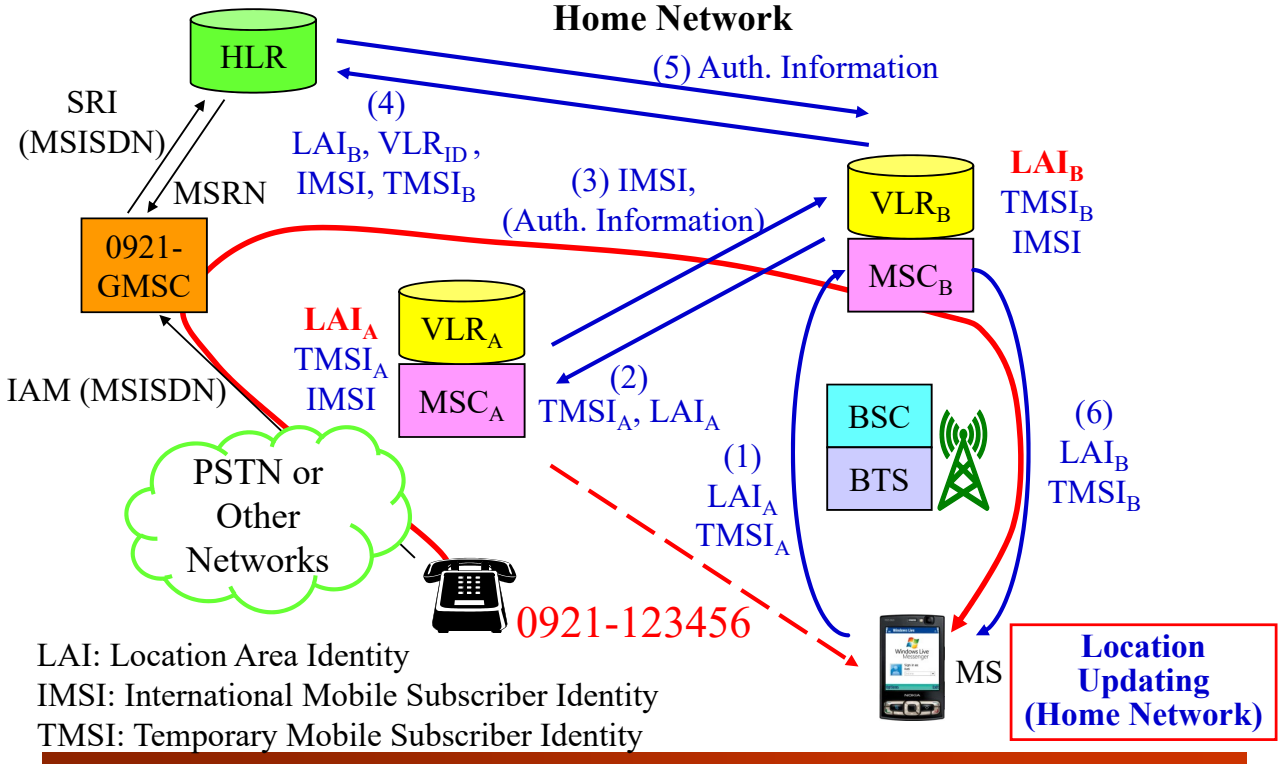
SIM-based Roaming

- **Roaming** is the ability for a mobile user to automatically **obtain services** (including make and receive voice calls, send and receive data, or access other services), when travelling **outside the geographical coverage area** of the home network
- Roaming is technically supported by **mobility management**, **authentication**, **authorization** and **accounting billing** procedures
- For "**SIM-based roaming**"
  - The **visited network** is also a SIM-based mobile network
  - The operator has a **roaming agreement** with the **home operator**

Location Updating/Roaming

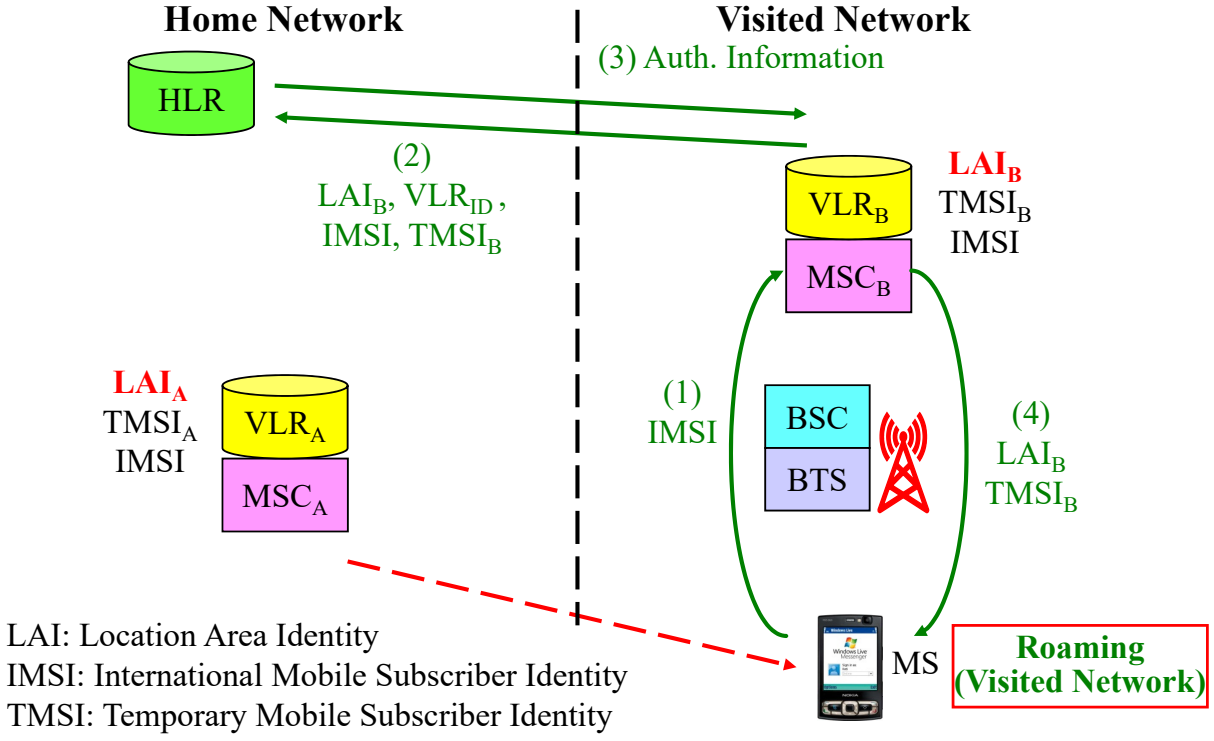
- When the mobile device is activated in the coverage area of a new **unauthorized network**, the **visited network** determines that the user is not registered in this system. Then,
  - Identify the home network of the user (based on **IMSI**)
  - If there is no **roaming agreement**, the service is denied by the visited network
- The visited network contacts the home network and requests service information (including whether or not roaming is allowed for the user, and the **authentication information**)
- If it is successful, the visited network begins to maintain a **temporary subscriber record** for the user
- The home network updates **location information** and **route information** for the user

Location Updating – Home Network



LAI: Location Area Identity
IMSI: International Mobile Subscriber Identity
TMSI: Temporary Mobile Subscriber Identity

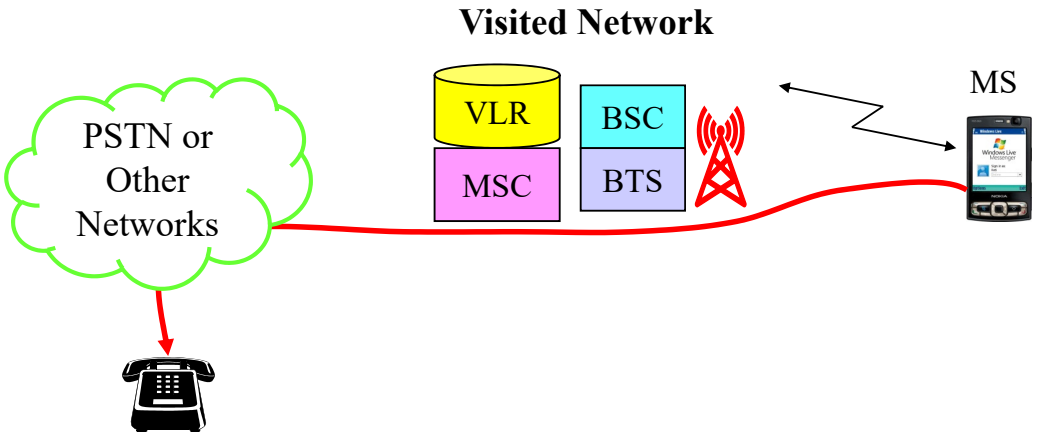
International Roaming



LAI: Location Area Identity
IMSI: International Mobile Subscriber Identity
TMSI: Temporary Mobile Subscriber Identity

Mobile Originating Call – Roaming

- For **mobile originating call**, the device connects the visited network directly
  - The visited network forwards/routes the call to the destination
  - Billing is based on the **roaming agreement**



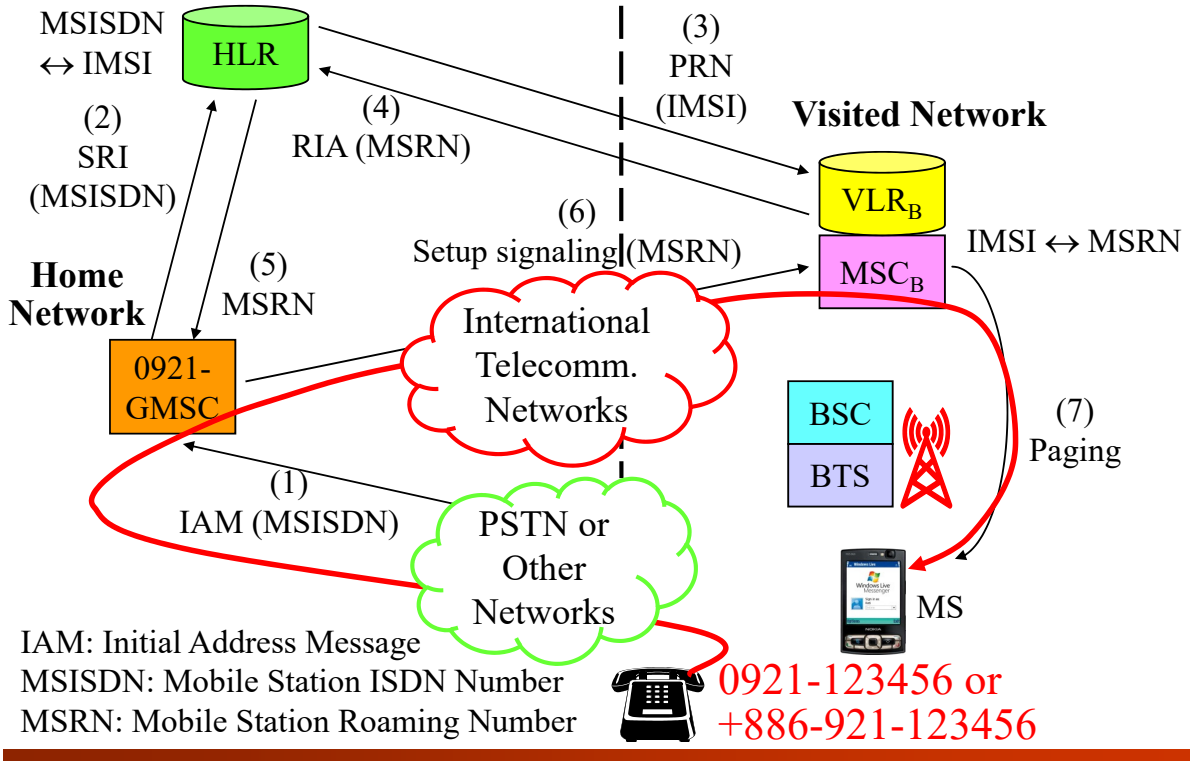
Mobile Terminated Call – Roaming

- The calling subscriber (e.g., within the PSTN) dials the **MSISDN** (the telephone number) of the roaming MS
- Based on the MSISDN, the call is routed to the mobile network **gateway MSC (GMSC)** of the **home network**
- To locate the MS, the GMSC sends to the **HLR** (of the **home network**) a MAP **SRI (Send Routing Information) message**
  - The message contains the **MSISDN** for the HLR to identify the **IMSI** of the MS
- By location updating, HLR knows the VLR (or the **visited network**) that currently serves the MS
  - HLR sends to the serving VLR (or the visited network) a MAP **PRN (Provide Roaming Number) message** to request the **routing information** of the MS

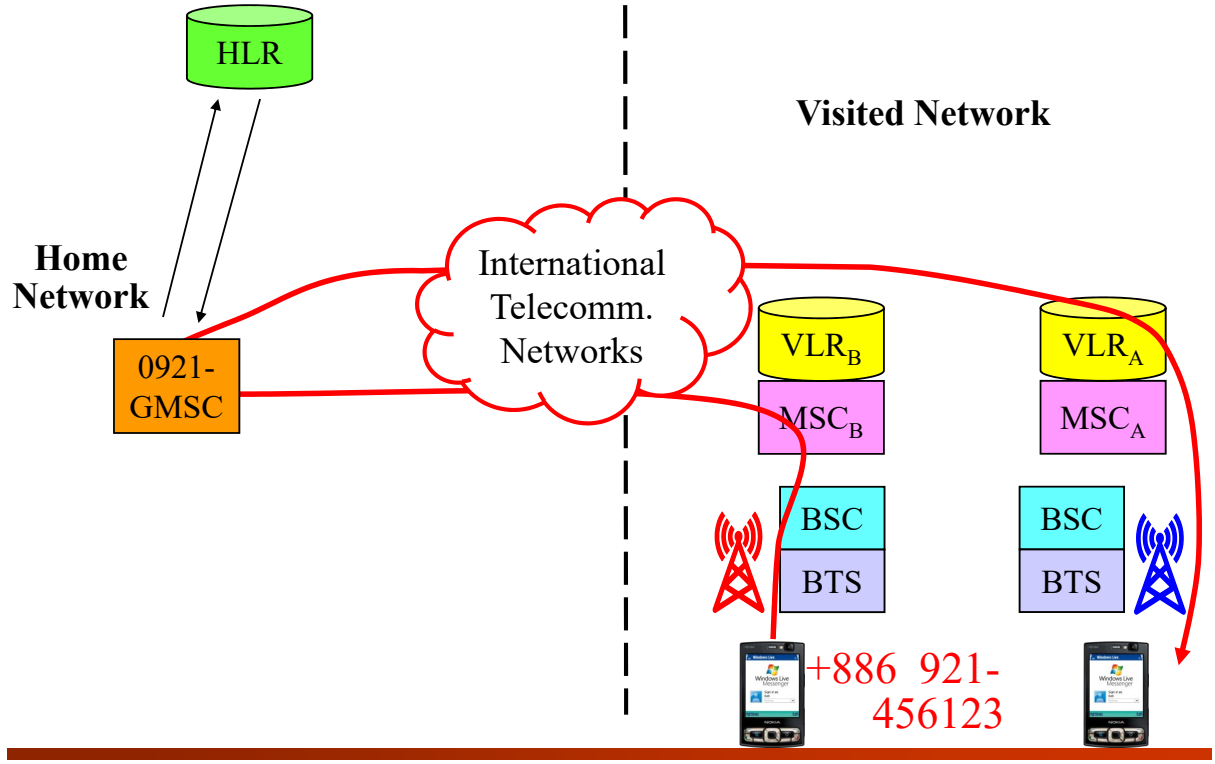
Mobile Terminated Call – Roaming (Cont.)

- With the IMSI contained in the MAP PRN message, the VLR assigns a **mobile station roaming number (MSRN)** to the roaming MS
- This MSRN is sent back to the HLR in a MAP **RIA (Routing Information Acknowledgement) message**
- Based on the MSRN forwarded by the HLR, the GMSC can route (setup) the call to reach the MSC currently serving the roaming MS
- Based on the MSRN in the signaling message, the **serving MSC** (in the visited network) can determine the IMSI corresponding to the incoming call
  - The MSC **pages** the roaming MS for the incoming call

Mobile Terminated Call – Roaming (Cont.)



Mobile Terminated Call – Roaming (Cont.)



Security Aspects in Mobile Communications

Security Issue

- In wireless mobile communications, the security issue is more serious than in wireline communications because of the **broadcast nature**
- There are two fundamental security services shall be provided in wireless mobile communication systems
  - **User Authentication:** User authentication is the process of determining whether a mobile user is, in fact, who it is declared to be
  - **Message Privacy:** Message privacy is to protect the user traffic (audio, video or data messages) from being intercepted by any eavesdroppers or intruders.

Basic User Authentication

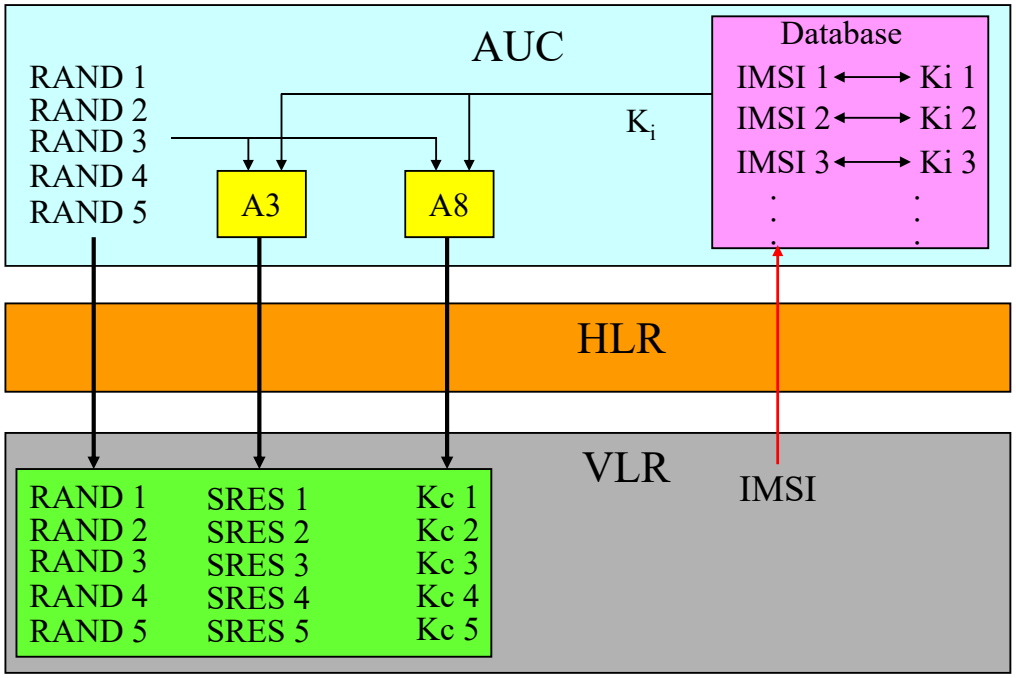
2G Security Information for Authentication

- The **authentication procedure** is used for the GSM PLMN to authenticate the identity (i.e., **IMSI**) of a subscriber
  - It is performed after the subscriber identity (TMSI/IMSI) is known by the network and before the channel is encrypted
  - It is also used to set the **ciphering key** for message privacy
- Two network functions are necessary:
  - The **authentication procedure**, and
  - The **key management** inside the fixed subsystem
- Some information is allocated both in the GSM PLMN and the MS (**Subscriber Identity Modules, SIM**) at subscription time
  - **IMSI**
  - **Subscriber Authentication Key - Ki** (secret information)

Authentication Information Generation – System

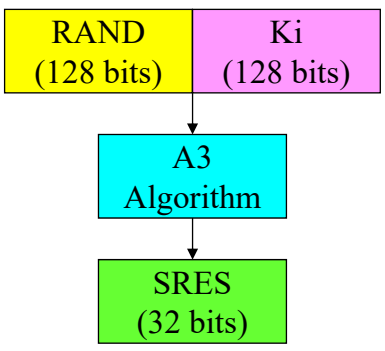
- The key Ki is stored on the network side in the **Home PLMN** (HPLMN), in an **Authentication Centre** (AuC)
- An AuC can be physically integrated with other functions, e.g., in a **Home Location Register** (HLR)
- When needed for each MS, the BSS/MSC/VLR requests security information **related to IMSI** from the HLR/AuC
- This includes an array of **triplets** of
  - **RAND:** is a **non-predictable** (**random**) number, and
  - **SRES (Signed Response):** obtained by applying **Algorithm A3** to **RAND** and **Ki**
  - **Kc (Ciphering Key):** obtained by applying **Algorithm A8** to **RAND** and **Ki**
- The triplets are stored in the VLR as security information

Auth. Information Generation – System (Cont.)

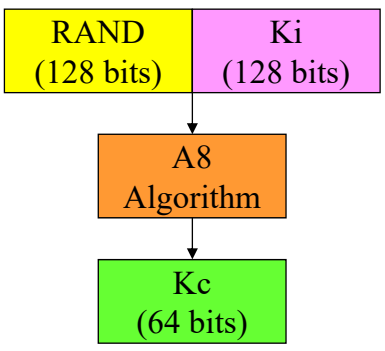


SRES and Kc Generation

- The algorithms are generally implemented by **Hash functions**
  - Hash functions are based on some fundamental bit-operations: Re-ordering, XOR, AND, OR, complement, …
  - A Hash function projects a value from a set with many members to a value from a set with a fixed number of (fewer) members.
  - Hash functions are **not reversible**



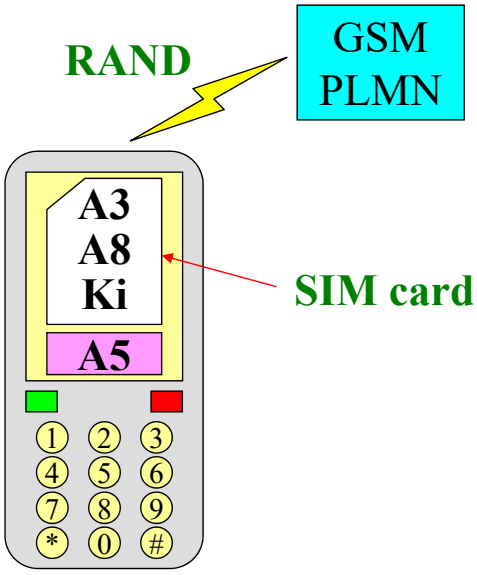
SRES Generation



Kc Generation

Authentication Information Generation – MS

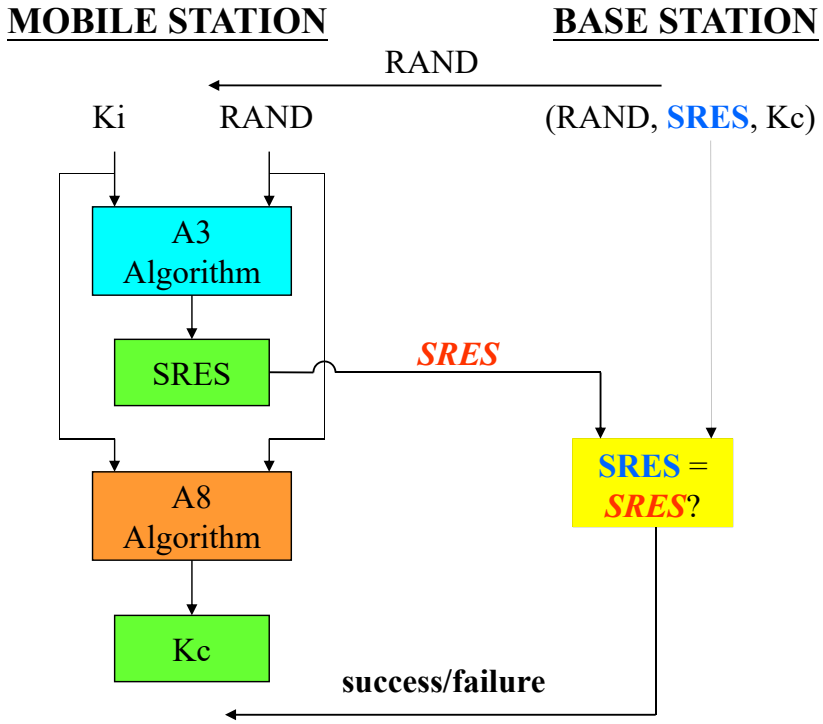
- The algorithms/information stored in the **SIM** card are: Algorithm A3, Algorithm A8, IMSI, and Ki
- **Algorithm A3:** One-way function for **authentication**
  - Input: RAND and Ki
  - Output: SRES
- **Algorithm A8:** One-way function for **ciphering key generation**
  - Input: RAND and Ki
  - Output: Kc
- **Algorithm A5:** One-way function in the equipment for **encryption**
  - Input: Kc, and COUNT
  - Output: BLOCK1 and BLOCK2



Authentication Procedure

- The **authentication procedure** consists of the following exchange between the fixed subsystem and the subscriber (MS):
  - The fixed subsystem transmits a **non-predictable** (**random**) number **RAND** (as a challenge) to the MS
  - The MS computes
    - **SRES:** The **signature** of **RAND**
    - By using **Algorithm A3**, based on the received RAND and the secret **Ki** in the SIM card
  - The MS transmits the signature **SRES** (as a response) to the fixed subsystem
  - The fixed subsystem tests SRES for validity

Authentication Procedure (Cont.)



Basic Message Encryption

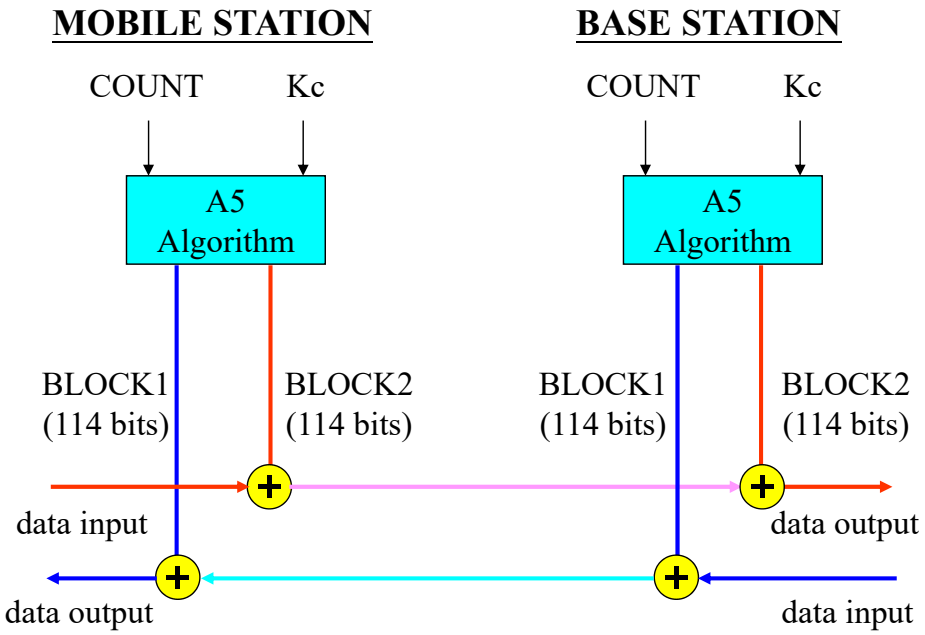
Message Encryption

- For **message encryption**, four points have to be specified:
  - The **ciphering method**;
  - The **key setting**;
  - The **starting** of the enciphering and deciphering processes;
  - The **synchronization**.
- The Physical Layer data flow is ciphered by a **stream cipher**
- The data flow on the **radio path** is obtained by the **bit by bit binary addition** (XOR) of
  - The user data flow
  - A ciphering bit stream, generated by **Algorithm A5** using a key
- The key **Kc** is called "**Ciphering Key**"

Ciphering Method

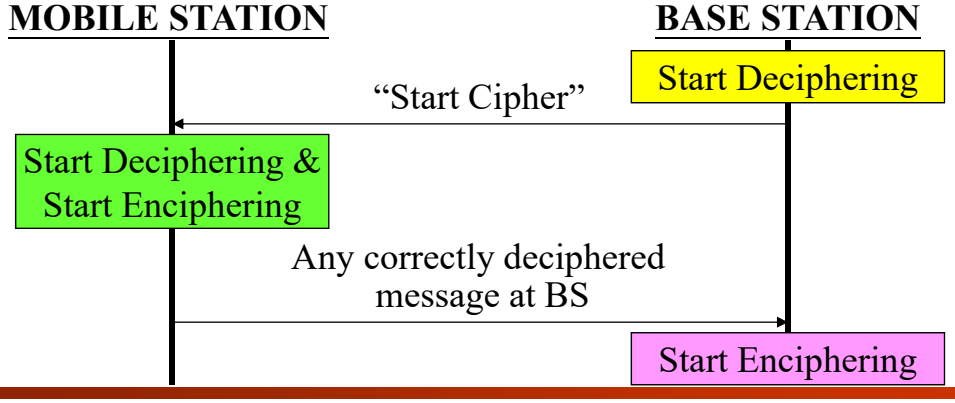
- **Algorithm A5** must be **common** to **all** GSM PLMNs and **all** mobile stations (in particular, **to allow roaming**)
- Algorithm A5 is implemented into both the MS and the BSS.
- The ciphering takes place **before modulation** and **after interleaving**
  - The deciphering takes place after demodulation symmetrically
- Algorithm A5 produces two blocks (**114 bits**) of **ciphering bit stream** (BLOCK1 and BLOCK2) for each 4.615 ms (frame)
  - There are 114 bits of information data in a frame (one time slot)
- **On the MS side**, deciphering is performed by using BLOCK1 and enciphering is performed by using BLOCK2
- **On the network side**, BLOCK1 is used for enciphering and BLOCK2 for deciphering

Ciphering Method (Cont.)



Key Setting and Starting of Ciphering

- Mutual key setting allows the MS and the network to agree on a **common key** Kc to be used in Algorithm A5
- The key Kc is derived by using Algorithm A8 by using the authentication RAND value
- The MS and the BSS must **co-ordinate** the instants at which the enciphering/deciphering processes start on the radio path



Synchronization

- The enciphering stream at one end and the deciphering stream at the other end must be **synchronized**
  - Ensure that the enciphering bit stream and the deciphering bit stream for a data frame are coincident
- Synchronization is guarantied by driving Algorithm A5 by an explicit **time variable**
  - **COUNT**, which is derived from the **TDMA frame number**
  - Each 114-bit block produced by A5 depends on the **TDMA frame numbering** and the ciphering key Kc (running key)
  - Different frames use **different** ciphering streams

Security Enhancement

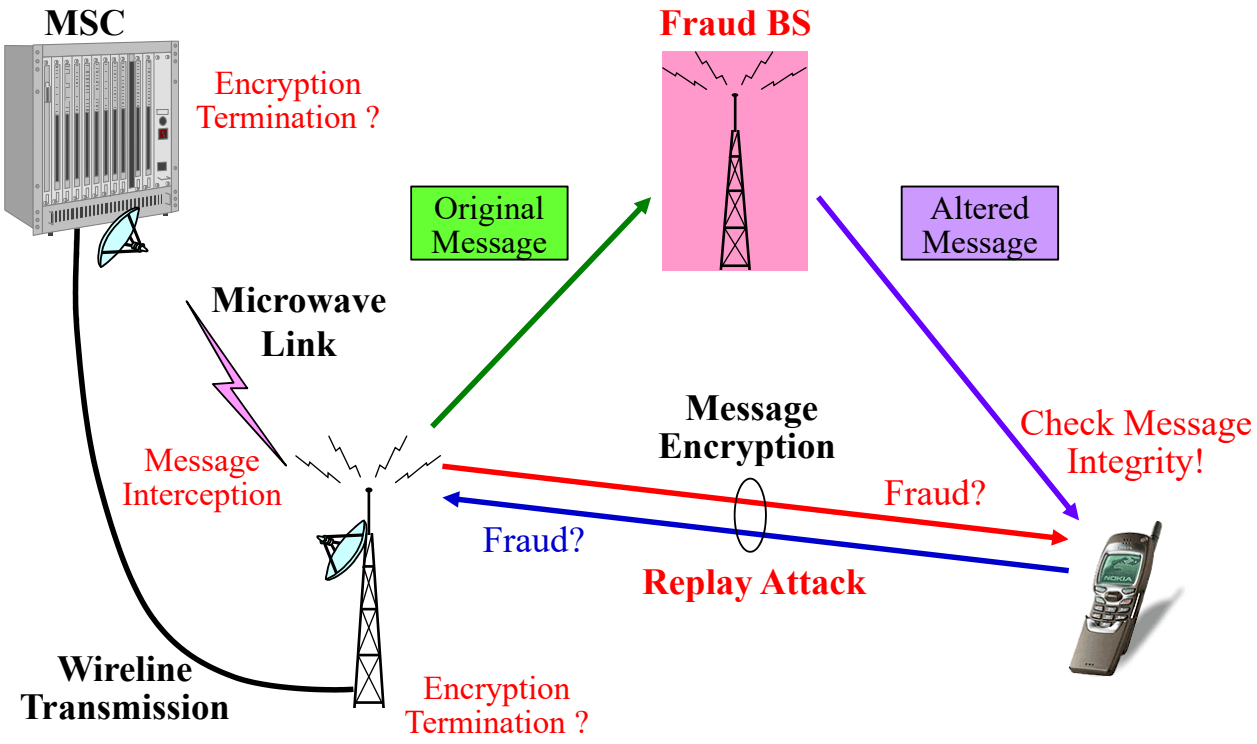
3G Beyond and 2G Security

- There are three key principles behind 3G security:
  - 3G security is **built on the security of 2G systems**.
  - Security elements within GSM and other 2G systems that have proved to be **needed** and **robust** shall be adopted for 3G security.
    - SIM based Authentication
    - Confidentiality of user traffic on the air interface
    - Confidentiality of user identity on the air interface
  - 3G security will improve on the security of 2G systems - 3G security will address and correct **real and perceived weaknesses** in 2G systems.
  - 3G security will offer **new security features** and will secure new services offered by 3G.

3G Enhancement in Security

- Addition and enhancement of features to overcome actual or perceived weaknesses in 2G systems
  - **Mutual authentication**
  - Assurance that authentication information and keys are **not being re-used** (key freshness)
  - **Integrity protection** of signalling messages, specifically the secured encryption algorithm negotiation process
  - Use of **stronger encryption** (a combination of key length and algorithm design)
  - Termination of the encryption **further into the core network** to encompass **microwave links**
- The **AKA** (**Authentication and Key Agreement**) mechanism is based on the **USIM (User Services Identity Module)** card

3G Enhancement in Security (Cont.)



Authentication and Key Agreement

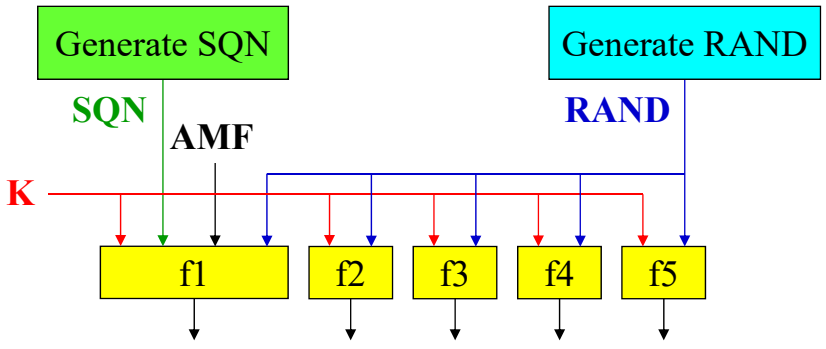
- The AKA mechanism achieves **mutual authentication** by showing knowledge of a **secret key K**, which is shared in both the **USIM** and the AuC in the user's **HE (Home Environment)**
- In addition, the USIM and the HE keep track of counters **SQNMS** and **SQNHE** respectively to support network authentication
  - SQNHE: Individual sequence number for each user maintained in the HLR/AuC
  - SQNMS: The highest sequence number the USIM has accepted
- Upon receipt of a request from the VLR/SGSN, the HE/AuC sends an **ordered** array of *n* **authentication vectors** to the VLR/SGSN
  - Authentication vectors are ordered based on **sequence number**

Authentication and Key Agreement (Cont.)

- An authentication vector (AV) consists of
  - **RAND**: a random number
  - **XRES**: an expected response
  - **CK**: a cipher key
  - **IK**: an integrity key
  - **AUTN**: an authentication token
- The generation of authentication information is based on
  - **Message authentication functions:** f1 and f2
  - **Key generating functions:** f3, f4 and f5
- Each authentication vector is good for **one** authentication and key agreement between the VLR/SGSN and the USIM
  - To prevent the **replay** attack

Authentication Information Generation – System

- The HE/AuC starts with generating a fresh sequence number **SQN** and an unpredictable challenge **RAND**
- Input: RAND, SQN, AMF (Authentication management field) and the secret key K

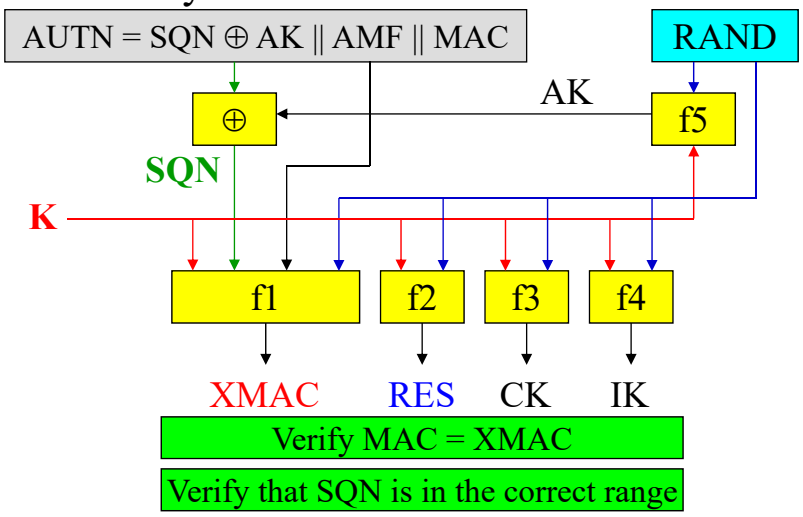


MAC: Message Authentication Code

AK: Anonymity Key

Authentication Information Generation – MS

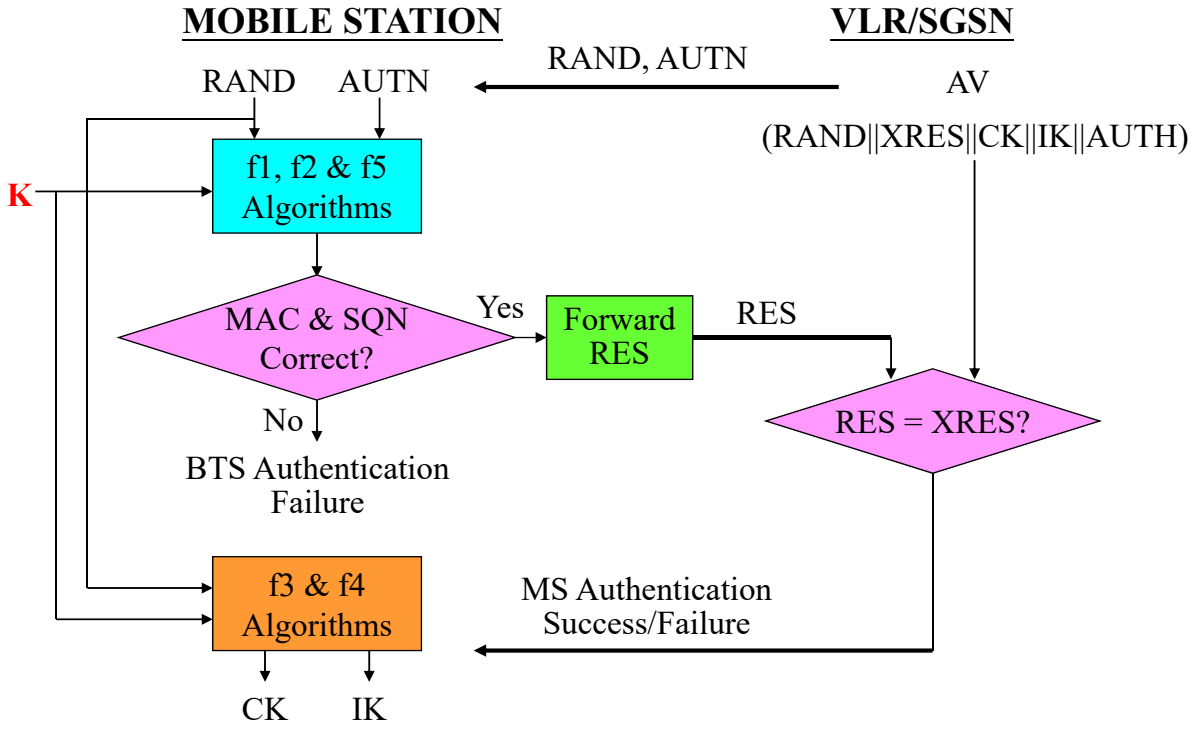
- AK is an **anonymity key** used to conceal (cover) the SQN
  - SQN may expose the **identity** and **location** of the user
- The authentication information depends on the RAND and AUTN from the system



Authentication Procedure

- When the VLR/SGSN initiates an authentication and key agreement, it selects **the next authentication vector** and sends **RAND** and **AUTN** to the user
- The USIM checks whether AUTN (including **MAC** and **SQN**) can be accepted and, if so, computes a response **RES** and sent it back to the VLR/SGSN (BTS authentication)
  - The USIM also computes **CK** and **IK**
- The VLR/SGSN compares the received **RES** with XRES
  - If they match, the VLR/SGSN considers the AKA procedure to be **successfully** completed (MS authentication)
- The established keys CK and IK will then be transferred by the USIM and the VLR/SGSN to the entities which perform **ciphering** and **integrity** functions

Authentication Procedure (Cont.)



Data Integrity Protection

- **Data integrity:** The property that data has **not been altered** in an unauthorised manner
  - The receiving entity (MS or SN) is able to verify that signalling data has not been modified in an unauthorised way
- The **Message Authentication Code** for data integrity, **MAC-I**, is generated by using the integrity algorithm f9
- Input parameters:
  - **IK:** the Integrity Key
  - **COUNT-I:** the integrity sequence number
  - **FRESH:** a **random** value generated by the network side (for the user throughout the duration of a **single connection**)
  - **DIRECTION:** the direction bit (indicating **up-link** or **down-link**)
  - **MESSAGE:** the signalling data