1.

- SFH is used in GSM to improve performance in the multipath fading environment & to reduce the required S/I ratio

- The mobile radio channel is a frequency selective fading channel

- Fades occur when there is a loss in signal power due to variations in terrain such as valleys or hills or due to objects such as buildings or even large metal objects such as aircraft interfering with the signal path, causing the original signal to be attenuated or canceled out

- When mobile passes though areas of fade there is less chance of losing the radio link in these areas by invoking SFH
- GSM uses SFH to improve signal quality.

- In SFH hop rate is less than the message bit rate

- A mobile transmits at one frequency during a time slot and hops to a different frequency before next time slot.
- FH allows the maintenance of the radio link by shifting onto another frequency before the link is totally lost
- FH also provides interference diversity.
- FH reduces the S/I ratio required for good communications .
- Different hopping algorithms can be assigned to the MS with the given channel set. (cyclic hopping , random hopping)

Two different implementation schemes of SFH are used in BSs

  - The RF Hopping

  - Baseband Hopping

- The RF Hopping is suitable for BTS configurations with few (2- 3) transceivers

- The main disadvantage of RF hopping is that a hybrid combiner must be used since there needs to be non frequency selective signal combining

- The Baseband Hopping is suitable when a large number of transceivers are used in one BTS

- The Baseband Hopping requires one transceiver to be allocated for one frequency

- This implementation is only cost effective in large systems that already have a number of transceivers at the BTS

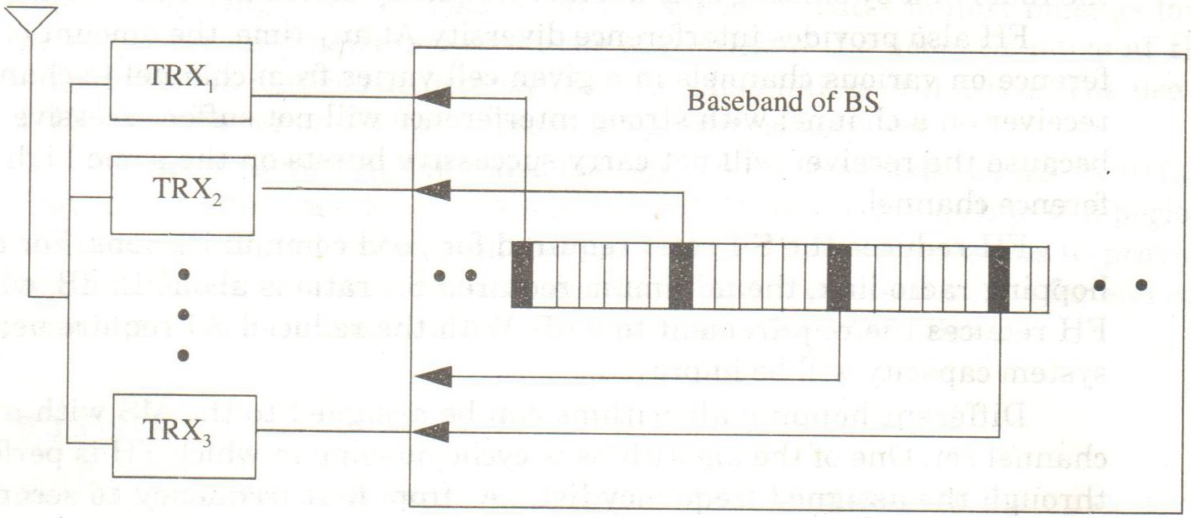

Fig. 6.4 Baseband Frequency Hopping Implementation

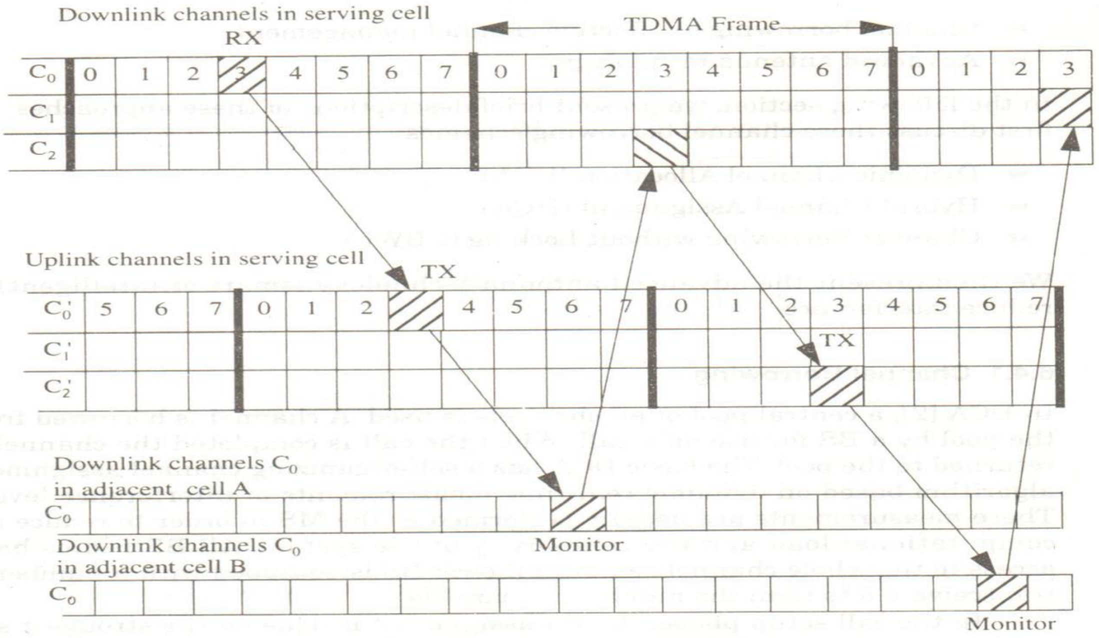
Downlink channels in serving cell
RX
TDMA Frame
C0
C1
C2
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3
Uplink channels in serving cell
TX
C'0
C'1
C'2
5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
TX
Downlink channels C0 in adjacent cell A
C0
Monitor
Downlink channels C0 in adjacent cell B
C0
Monitor

Fig. 6.5 SFH for GSM with Three Different Frequencies

2.

- Three Channel Borrowing Schemes
  - Dynamic Channel Allocation (DCA)
  - Hybrid Channel Assignment (HCA)
  - Channel Borrowing Without Locking (CBWL)

Dynamic Channel Allocation (DCA)

- Central pool of all channel is used.
- A channel is borrowed from the pool by BS for use on a call. When call is completed the channel is returned to the pool.
- In channel set up phase the BS assignment is done on the strongest signal from neighboring BSs
- Several variations of DCA have been proposed & some of them have been implemented
- ACA (Adaptive Channel Allocation), (a variation of DCA), significantly increases the capacity of a TDMA system as compared to the traditional FCA (Fixed Channel Assignment)

Hybrid Channel Assignment (HCA)

- Some channels are permanently assigned to each BS as in FCA, & others are kept in a central pool for borrowing as in DCA
- Channel locking is used to prevent an increase in co channel interference
- Channel locking – BSs within the required minimum channel reuse distance from BS that borrows channel can not use the same channel
- Channel locking has some disadvantages like,
- the number of channels available for lending to a BS is limited
- Difficulty in maintaining co channel reuse distance at the minimum require value every where in the system. Because of this difficulty, DCA & HCA generally perform less satisfactorily than FCA under high loads

- Since the Tx of each BS must be able to transmit not only on the channel allocated permanently to that BS but also any of the channel that belong to the central pool, causes some complexity

Channel Borrowing Without Locking (CBWL)

- The CBWL has most of the advantages of other channel borrowing schemes & overcomes their disadvantages
- In the CBWL, each BS is allocated channels as in FCA
- If all channels of the BS are occupied & a new call arrives, channel borrowing is used
- A channel can be borrowed only from an adjacent BS
- The borrowed channel cannot be used by the original lending BS but can still be used in any nearby cochannel BSs. Thus there is no channel locking

- CBWL offers advantages in comparison with DCA and HCA
- In CBWL only fraction of the total channels of the system need to be accessible at each BS.
- Without channel locking channel reuse distance is always kept at desired minimum.
- This exhibits better performance in light as well as in heavy traffic loads.
- Channel borrowing at BS does not require global information management so tasks are simplified.
- Ensures good quality for borrowed and regular channels with out increasing co channel interference.
- CBWL can be employed in existing cellular systems without additional infrastructure cost
- Does not require new BSs and additional antenna towers to increase the capacity.
- It can be beneficial in providing good performance in hard to reach scenarios

3. Dynamic Power Control

    - The GSM network is designed so that the MS is instructed to use only the minimum power level necessary to achieve effective communication with the BTS
    - GSM defines 8 power classes for the BTS transmitter to cover all 5 classes of the MS (0.8 W to 20 W)
    - The MS measures the receive power level of the serving BS, the quality of the received signal, & ID codes for up to 6 neighbor BSs
    - The BS measures the receive power level & signal quality of each MS, the distance to the MS & the transmit power of the MS & BS
    - Signal power level is determined by averaging the incoming signal level over a specified period of time.
    - For the BTS the power output is nominally controlled in 2-dB steps to provide better channel interference performance.
    - This allows a better QoS or a greater frequency reuse
    - Both MS & BTS power control is performed in 2-dB steps to a minimum of +13dBm

- The GSM network is designed so that the MS is instructed to use only the minimum power level necessary to achieve effective communication with the BTS
- GSM defines 8 power classes for the BTS transmitter to cover all 5 classes of the MS (0.8 W to 20 W)
- The MS measures the receive power level of the serving BS, the quality of the received signal, & ID codes for up to 6 neighbor BSs
- The BS measures the receive power level & signal quality of each MS, the distance to the MS & the transmit power of the MS & BS
- Signal power level is determined by averaging the incoming signal level over a specified period of time.
- For the BTS the power output is nominally controlled in 2-dB steps to provide better channel interference performance.
- This allows a better QoS or a greater frequency reuse
- Both MS & BTS power control is performed in 2-dB steps to a minimum of +13dBm

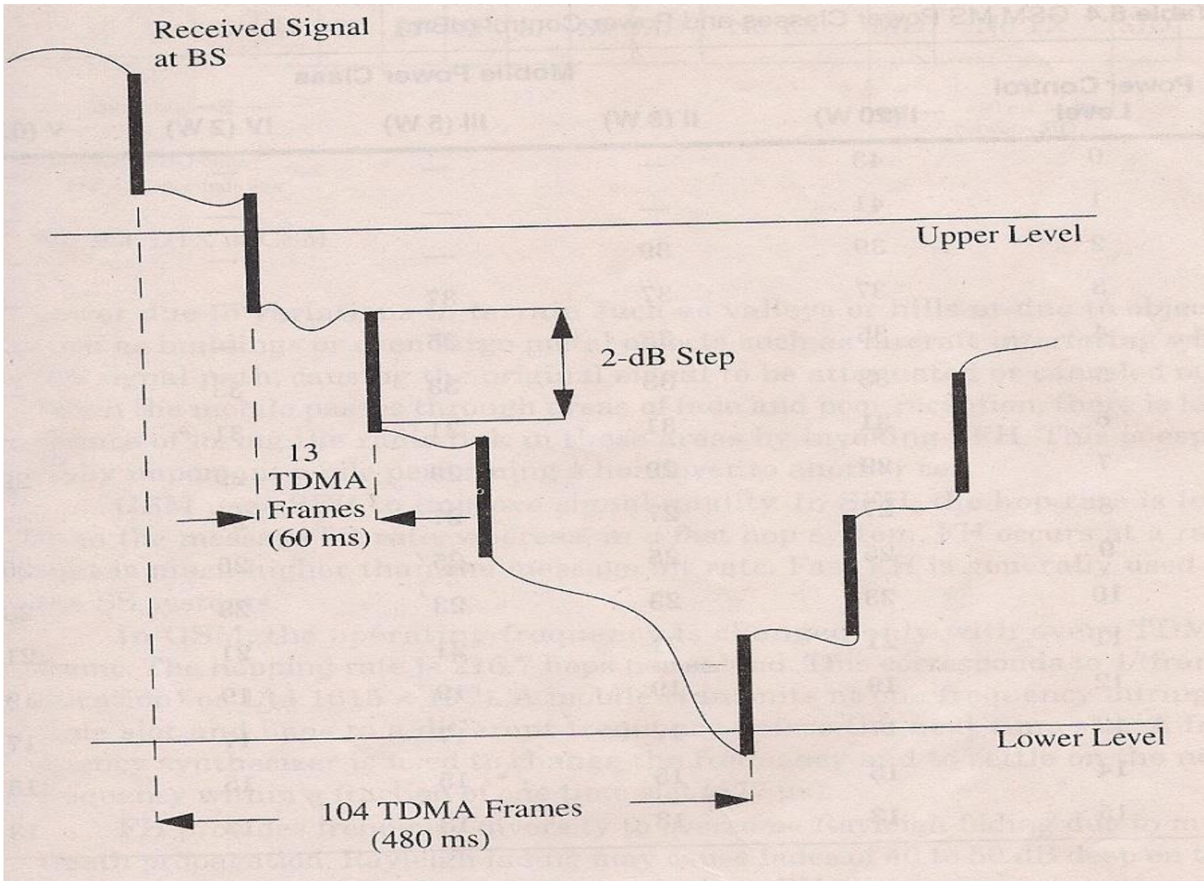

Fig. 6.2 Power Control in GSM

Advantages of power control

- The use of minimum transmitting power to access the network helps to increase the battery life of the mobile set and reduce interference
- By carefully controlling the power level of the transmitter, the spectral interference with other GSM equipments can be minimized

4.

- Only when an MS, or handset, roamed into another country would an intersystem message be needed
- The token-based system using security triplets meets this need
- The security key (K_i) and the details of the A3 & A8 algorithms are not shared between system

- These triplets are computed and stored in the MS, in the home authentication centre, & in the visited VLR.
- The comparison of the SRES values is done in the visited VLR.
- All MSs are assigned an electronic serial number - the IMEI – when they are manufactured.
- The VLR in the visited system then queries the old VLR for the security data & location of the HLR and assigns a new TMSI to the MS.
- The MS uses the TMSI for all further access to that system.
- The TMSI provides anonymity of communications since only

the MS & the network know the identity of the MS with a

given TMSI.

- The BS transmits a RAND on the DCCH that is received by the MS
- When the MS accesses the system, it calculates SRES.
- It then transmits the desired message with its authentication to the network.
- The network does the same calculation and confirm the identity of the MS.
- All communications between MS and BS are encrypted to prevent a hacker from decoding the data

Token-based Registration

The call flows for token based registration are:

- The MS sends an registration message to the new system with the old TMSI and old LAI.
- The new system queries old VLR for data
- Old VLR returns security related information (eg:unused triplets and location of HLR)
- The new system issues a challenge to the MS.
- The MS responds to the challenge.
- The new system sends a message to the HLR with an MS location update information
- The HLR updates its location data base with the new location of the MS.
- The HLR acknowledges the message and may send additional security related data.

- The HLR sends a registration cancellation message to the old VLR.
- The new system sends an encrypted message to the MS with the new TMSI.

The MS acknowledges the message.

5

- The GSM uses 3 security algorithms :
  1. Authentication Algorithm (A3)
  2. Privacy Key Generation Algorithm (A8)
  3. Encryption Algorithm (A5)

Authentication Algorithm (A3)

- Used by the handset to compute a Signed Response (SRES) to the Random Number (RAND) transmitted by the BS
- SRES is transmitted to the BS during registration
- The computation also uses a secret key (K_i) that is stored in the SIM card & is unique to each SIM card

Privacy Key Generation Algorithm (A8)

- Uses RAND & K_i to generate a privacy key (K_c) that is used for data & voice privacy
- The A8 algorithm is also unique to each GSM administration
- A common A8 is available from the GSM Memorandum of Understanding (MoU)

Privacy Key Generation Algorithm (A8)

- Uses RAND & K_i to generate a privacy key (K_c) that is used for data & voice privacy
- The A8 algorithm is also unique to each GSM administration

- A common A8 is available from the GSM Memorandum of Understanding (MoU)

Encryption Algorithm (A5)

- Used to encrypt data transmitted on the DCCH & the TCH
- The inputs to A5 are the privacy key (K_c) & the TDMA frame counter
- The frame counter is 22 bits long & each frame is approximately 4.6 ms long. The encryption mask repeats every 5 hours
- Each frame two output of A5 BLOCK1 and BLOCK2 are generated
- BLOCK 1 is used for encryption by BS an BLOCK 2 is used for encryption by handset

6.

GSM system privacy and security is achieved using four primary mechanisms

1. Each subscriber is identified using a cryptographic security mechanism
2. The subscriber's security information is stored in SIM card
3. The GSM operator maintains the secrecy of the cryptographic algorithms and the keys for authenticating the subscriber and providing voice privacy
4. The cryptographic keys are not shared with other GSM administrations

There are 4 types of Wireless Security Requirements:

- Privacy of communication
- Authentication Requirements
- System Lifetime Requirements

Physical Requirements

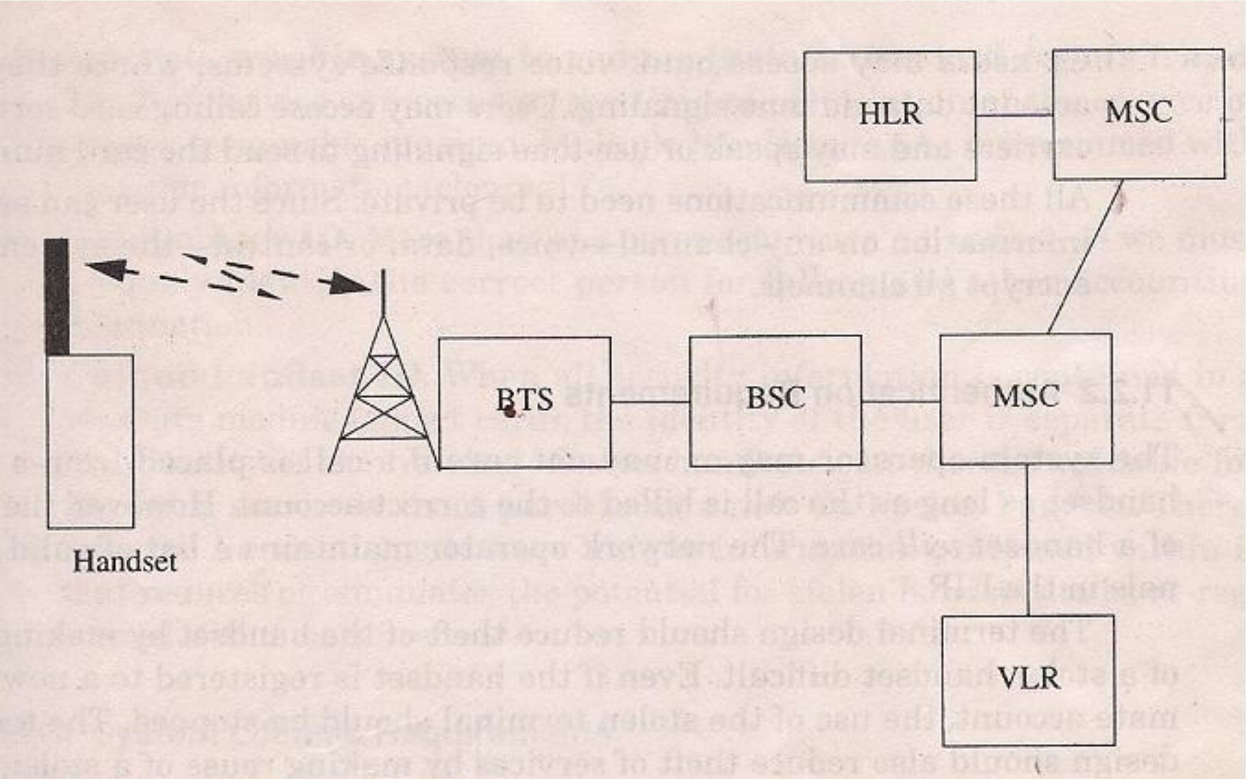

Fig. 11.1 Privacy Requirements

PCS system showing the areas where criminals / hackers can compromise the security of the system

Privacy of Communications

A PCS personal terminals needs privacy in the following areas:

- Call Setup Information
- Speech
- Data
- User Location
- User ID
- Calling Patterns

- **Call Setup Information**

- During call setup, the handset will communicate information such as calling number, calling card number, & type of service requested to the network.

- The system must send all these information in a secure way

- **Speech**

- - The system must encrypt all spoken communications so that hackers cannot intercept the signals by listening on the airwaves

- **Data**

  - The system must encrypt all data communications so that hackers cannot intercept data by listening on the airwaves

- **User Information**

  - No information that a user might transmit should enable a listener to determine the user's location. The usual method to meet this need is to encrypt the user ID.

  - Protection is needed against:

    1. Radio link eavesdropping

    2. Unauthorized access by outsiders (hackers) to the user location information stored in the network at the VLR & HLR

    3. Unauthorized access by insiders (hackers) to the user location information stored in the network.

User ID

- When a user interacts with the network, the user ID must be sent in a way that does not show the user ID. This prevents analysis of user calling patterns based on user ID.

Calling Patterns

- No information must be sent from a handset that enables a listener of the radio interface to do traffic analysis on the PCS user. Typical traffic analysis information are:

  - Calling Number
  - Frequency of use of the handsets
  - Caller ID
  - Financial Transactions

Authentication Requirements

- The system operator may or may not care if a call is placed from a stolen handset as long as the call is billed to the correct account. But the owner of the hand set will care
- The network operator maintains a list of valid terminals in the EIR (Equipment Identity Register). The terminal design should reduce theft of the handset by making reuse of a stolen handset difficult.
- To reduce theft, we need the following factors:
  - Clone-Resistant Design
  - A cryptographic system to reduce installation& repair fraud
  - Unique User ID
  - Unique Handset ID

Clone-resistant Design:

Handset unique information must not be compromised

- Over the air
- From the network
- From network interconnect
- From fraudulent systems
- From security algorithms
- From users cloning their own handsets

A cryptographic system to reduce installation & repair fraud

- Theft of service can occur at the time of installation of the service or when a terminal is repaired.
- Multiple handsets can be programmed with the same information

Unique user ID :

- More than one person may use a handset, so we must uniquely identify the correct person for billing and other accounting information

Unique handset ID:

- When all security information is contained in a separate module the identity of the user is separate from the identity of the handset.
- This makes stolen handsets reusable.
- So the handset should have unique information contained within it that reduces the potential for stolen handsets to be re-registered with a new user

System Lifetime Requirements

- An algorithm that is secure today may be breakable in 5-10 years
- Since any system being designed today must work for many years, it is responsible to require that the procedures lasts at least 20 years
- Thus the algorithm design must consider the best available cracking algorithms available today & must have provisions for being upgraded in the field

Physical Requirements

- Any cryptographic system used in a handset must work in the practical environment of a mass-produced consumer product