

CS8601 –MOBILE COMPUTING

UNIT 2

MOBILE TELECOMMUNICATION SYSTEM

2.6.Handover &Security :

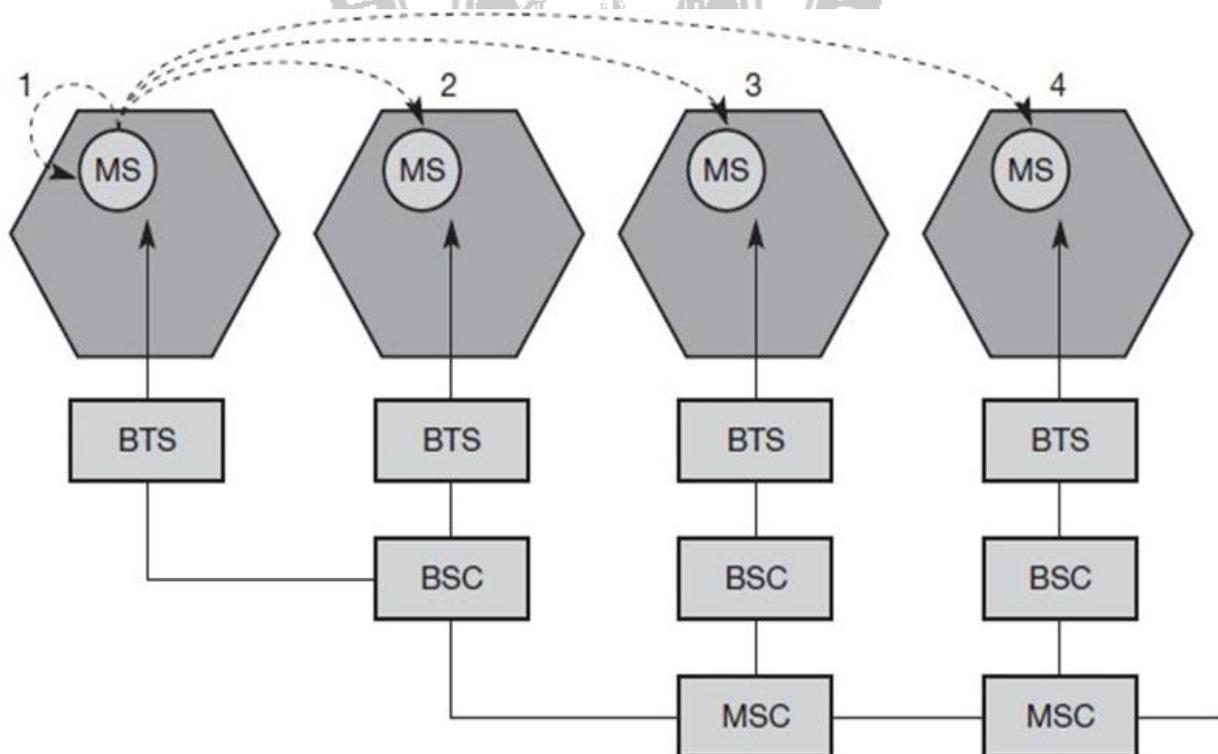
Handover

Cellular systems require **handover** procedures, as single cells do not cover the whole service area. However, a handover should not cause a cut-off, also called **call drop**. GSM aims at maximum handover duration of 60 ms. There are two basic reasons for a handover:

The mobile station **moves out of the range** of a BTS, decreasing the received **signal level** increasing the **error rate** thereby diminishing the **quality of the radio link**.

Handover may be due to **load balancing**, when an MSC/BSC decides the traffic is too high in one cell and shifts some MS to other cells with a lower load.

The four possible handover scenarios of GSM are shown below:



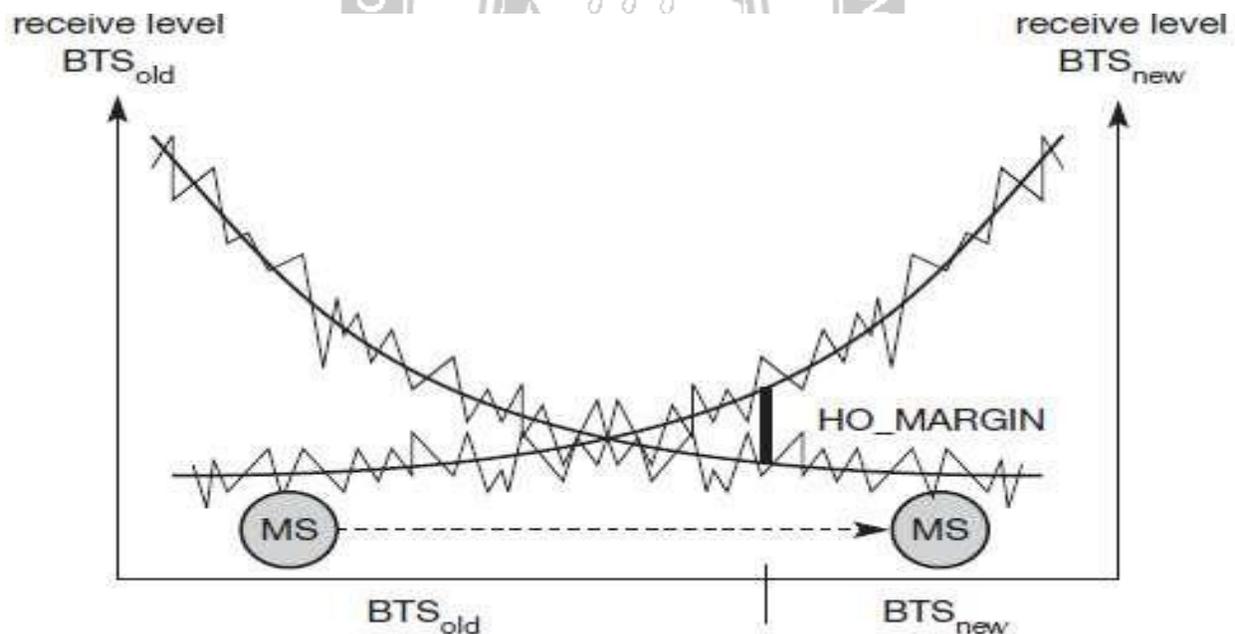
Intra-cell handover: With reference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency (scenario 1).

Inter-cell, intra-BSC handover: This is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one (scenario 2).

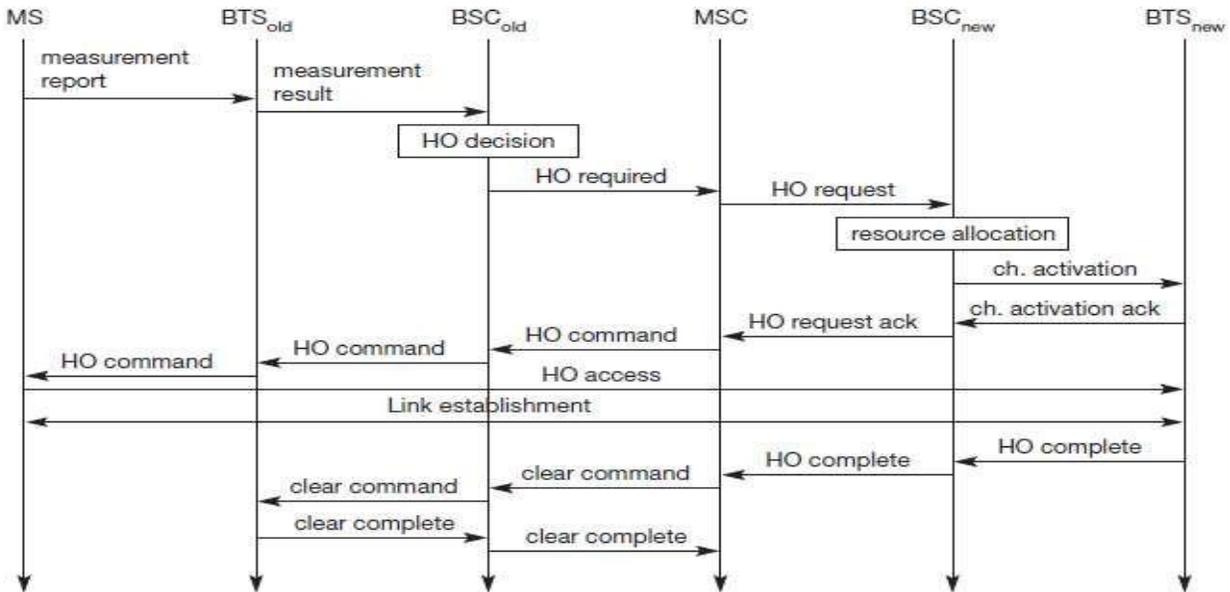
Inter-BSC, intra-MSC handover: As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC (scenario 3).

Inter MSC handover: A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4).

To provide all the necessary information for a handover due to a weak link, MS and BTS both perform periodic measurements of the downlink and uplink quality respectively. Measurement reports are sent by the MS about every half-second and contain the quality of the current link used for transmission as well as the quality of certain channels in neighboring cells (the BCCHs).



Handover decision depending on receive level



Intra-MS handover

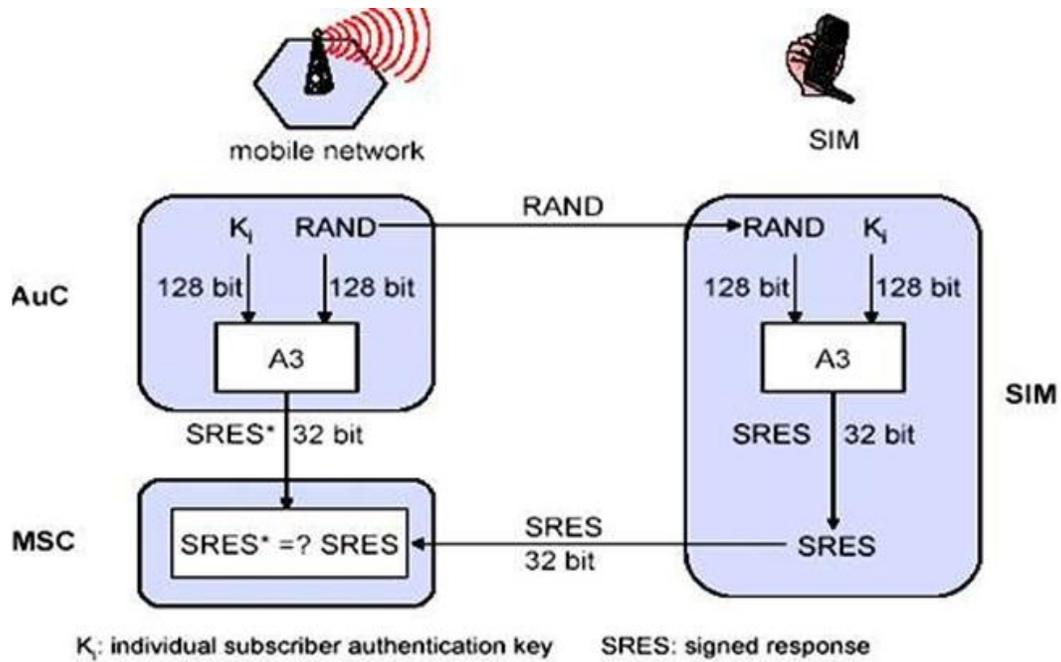
More sophisticated handover mechanisms are needed for seamless handovers between different systems.

Security

GSM offers several security services using confidential information stored in the AuC and in the individual SIM. The SIM stores personal, secret data and is protected with a PIN against unauthorized use. Three algorithms have been specified to provide security services in GSM. **Algorithm A3** is used for **authentication**, **A5** for **encryption**, and **A8** for the **generation of a cipher key**. The various security services offered by GSM are:

Access control and authentication: The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM. The next step is the subscriber authentication. This step is based on a challenge-response scheme as shown below:

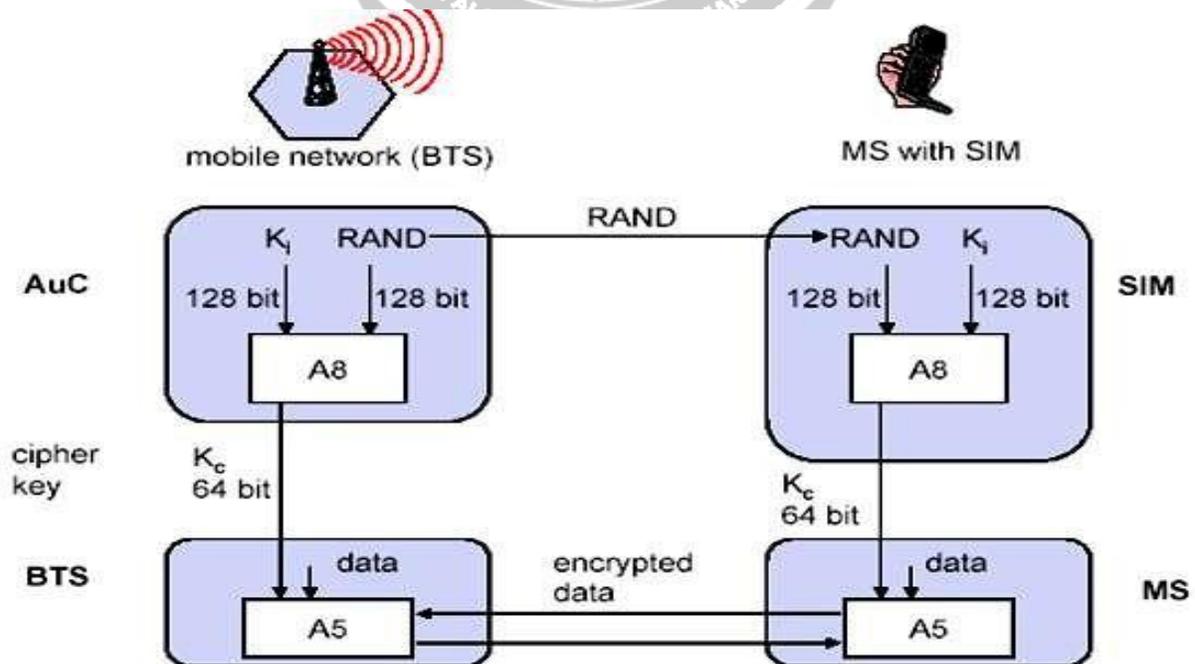
Authentication is based **authentication key Ki**, the **user identification IMSI**, and the algorithm used for authentication **A3**. The AuC performs the basic generation of random values RAND, signed responses SRES, and cipher keys Kc for each IMSI, and then forwards this information to the HLR. The current VLR requests the appropriate values for RAND, SRES, and Kc from the HLR. For authentication, the VLR sends the random value RAND to the SIM. Both sides, network and subscriber module, perform the same operation with RAND and the key Ki, called **A3**. The MS sends back the SRES generated by the SIM; the VLR can now compare both values. If they are the same, the VLR accepts the subscriber, otherwise the subscriber is rejected.



Subscriber Authentication

Confidentiality:

All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, data, and signalling as shown below.



To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface. After authentication, MS and BSS can start using encryption by applying the cipher key **Kc**, which is generated using the individual key **Ki** and a random value by applying the algorithm A8. Note that the SIM in the MS and the network both calculate the same **Kc** based on the random value RAND. The key **Kc** itself is not transmitted over the air interface. MS and BTS can now encrypt and decrypt data using the algorithm A5 and the cipher key **Kc**.

Anonymity:

To provide user anonymity, all data is encrypted before transmission, and user identifiers are not used over the air. Instead, GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update. Additionally, the VLR can change the TMSI at any time.

To enhance the data transmission capabilities of GSM, two basic approaches are possible. As the basic GSM is based on connection-oriented traffic channels, e.g., with 9.6 kbit/s each, several channels could be combined to increase bandwidth. This system is called **HSCSD {high speed circuit switched data}**. A more progressive step is the introduction of packet oriented traffic in GSM, i.e., shifting the paradigm from connections/telephone thinking to packets/internet thinking. The system is called **GPRS {general packet radio service}**.

HSCD:

A straightforward improvement of GSM's data transmission capabilities is high speed circuit switched data (HSCSD) in which higher data rates are achieved by bundling several TCHs. An MS requests one or more TCHs from the GSM network, i.e., it allocates several TDMA slots within a TDMA frame. This allocation can be asymmetrical, i.e. more slots can be allocated on the downlink than on the uplink, which fits the typical user behaviour of downloading more data compared to uploading. A major disadvantage of HSCD is that it still uses the connection-oriented mechanisms of GSM, which is not efficient for computer data traffic.