Unit - IV

10th Aug

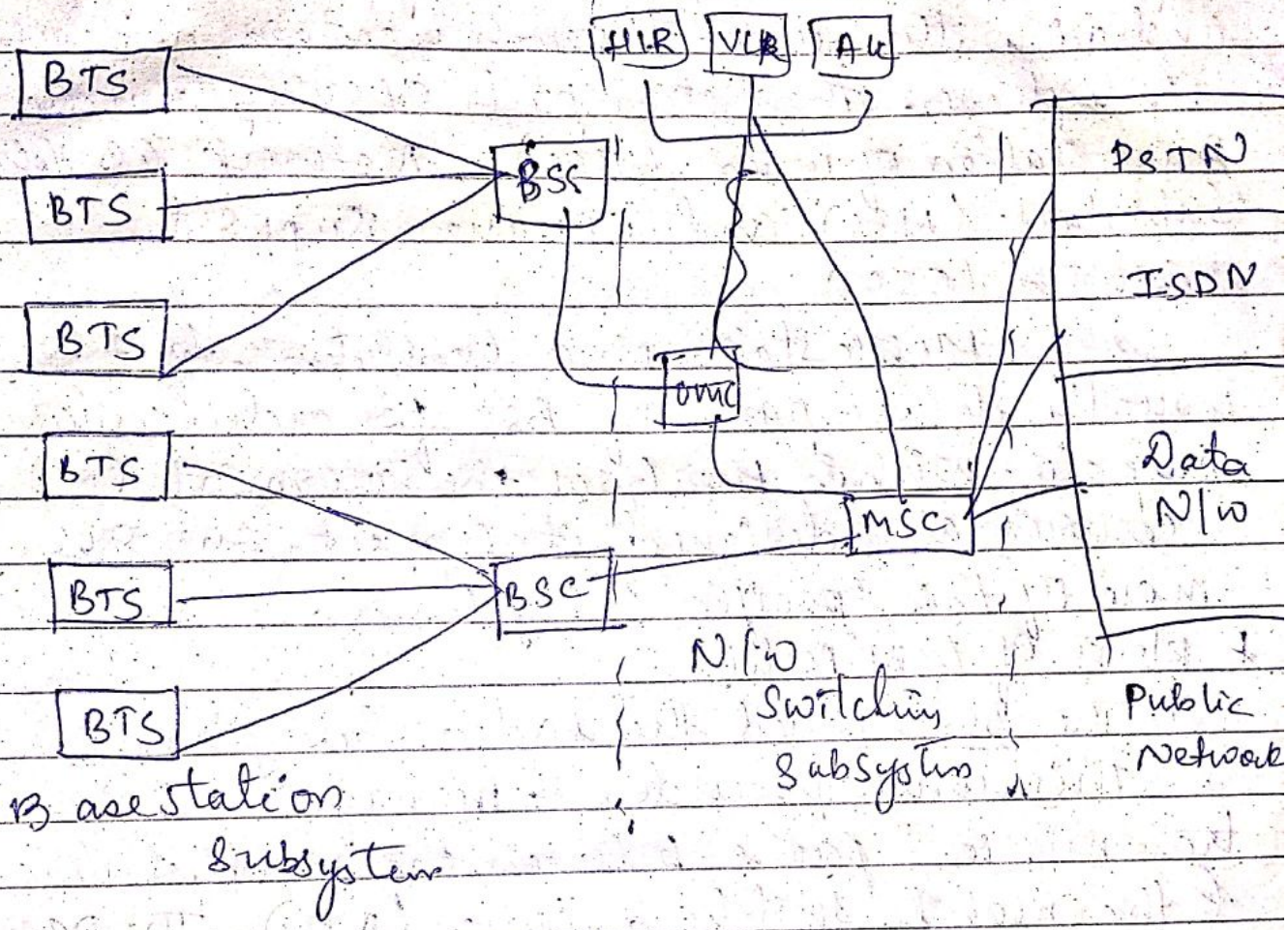


fig → Gsm System architecture

S. Ai

13th Aug

In GSM Architecture there are 3 major interconnected Subsystems, which interact among themselves and with the users through certain network interphases. The section parts of subsystems are Base station of system (BSS), Network & Switching Subsystem (NSS) and Operation Support Subsystem (OSS)

Mobile station is a subsystem, but it usually to be part of BSS for architecture purpose. within the GSM the equipment & services are designed to support one or more of this specific subsystems.

* Blocks of GSM Archi

1. The BSS is called the radio Subsystem. This unit provides & manages radio transmission paths - between the mobile station & the mobile switching center (MSC). The BSS also has a responsible to manages the radio interphase b/w the mobile station & all other subsystems of GSM. It also consist of many BSC's which connects the MS to NSS via MSC's

2. NSS :- Network

are used to manage the switching function of the system & allows the MSC's to communicate with other Networks such as PSTN and ISDN

3. Another subsystem called (OSS) provides the support of operation & maintainance of Gsm. this OSS allows the System Engineer to diagnose, troubleshoot & monitor all the features of Gsm System

On the radio air interface the mobile Station (MS) communicate with the BSS. these BSS consist of many BSC's which are connected to a single MSC & Each BSC can typically control upto several hundreds of BTS (Base Trans receivers

in NSS The central unit MSC is to control the traffic bhw BSC. for this purpose there 3 types of Data Base Naneed as HLR → home location Register. VLR → Visitor location Register Auc - Authen

① the Subscriber inf' is contained in HCR. along loc' inf' of user residing in the same region of MSC, Every Subscriber in Gsm market has a unique international mobile Subscriber identity (IMSI) assigned & used to identify Each home user.

VLR DB

② VLR → It stores temporary IMSI & customer information of all roamin

Subscriber, who visits the coverage area of particular MSC.

3) AUC:- Authentication Center is strongly confined DB which is used to handle the authenti & encryption keys for every single subscriber in the HLR & VLR. There is a registery in authentication center called as the Equipment identity register (EIR) which identifies stolen or fraudently altered phones that transmit identity data that does not match with info contained in HLR or VLR.

* the support & maintainence of OMC (Operation maintainence centre) is done by OSS. These supports are used monitor & maintain the performance of each MS, BS, BSC & MSC which are with in a GSM System.

GSM fun?

There are 3 fun? which are as follows

1. ~~maintains~~ maintaining all telecomm? hardware & N/W Op? with a particular market
2. managing all the charges & bill procedure

3. manage an mobile Equipment in the System;

Features & Services.

1. User Services are divided into 3 major categories.
1. telephone Service
2. Data Service or Beares Services
3. Supplementary ISDN Services.

(1) Fea

telephone Service :- In this category Emergency calling is included. there is also Support for Vidio text, teletext, which are not actually a part of GSM Standard Specifications.

(2)
Data Service or Beares Service :- In this category the Services provided are limited in the layer 1, 2, 3 of a open Interconnection OSI Refrence model Specifications. The Services supported in these layers are packet Switch protocols with the Data Rate of 300bps to 9.6bps.

(3) Supplementary ISDN Services :- This category of Service are digital in nature which includes Services for call diversion, closed user groups & identification of call

14th Aug

Such services were not available in analog mobile network systems. This category also include SMS or transmission of alphanumeric pages having a length limit to 160, 7bit ascii character also it can simultaneously transmit normal voice traffic.

Features

1) One of the remarkable features of Gsm is the SIM (subscriber identity module). This is a memory device that stores information like the ① Subscriber identity number, ② Networks & the countries where the Subscriber uses the same - with 4 digit personal id no activated Service from any Gsm phone

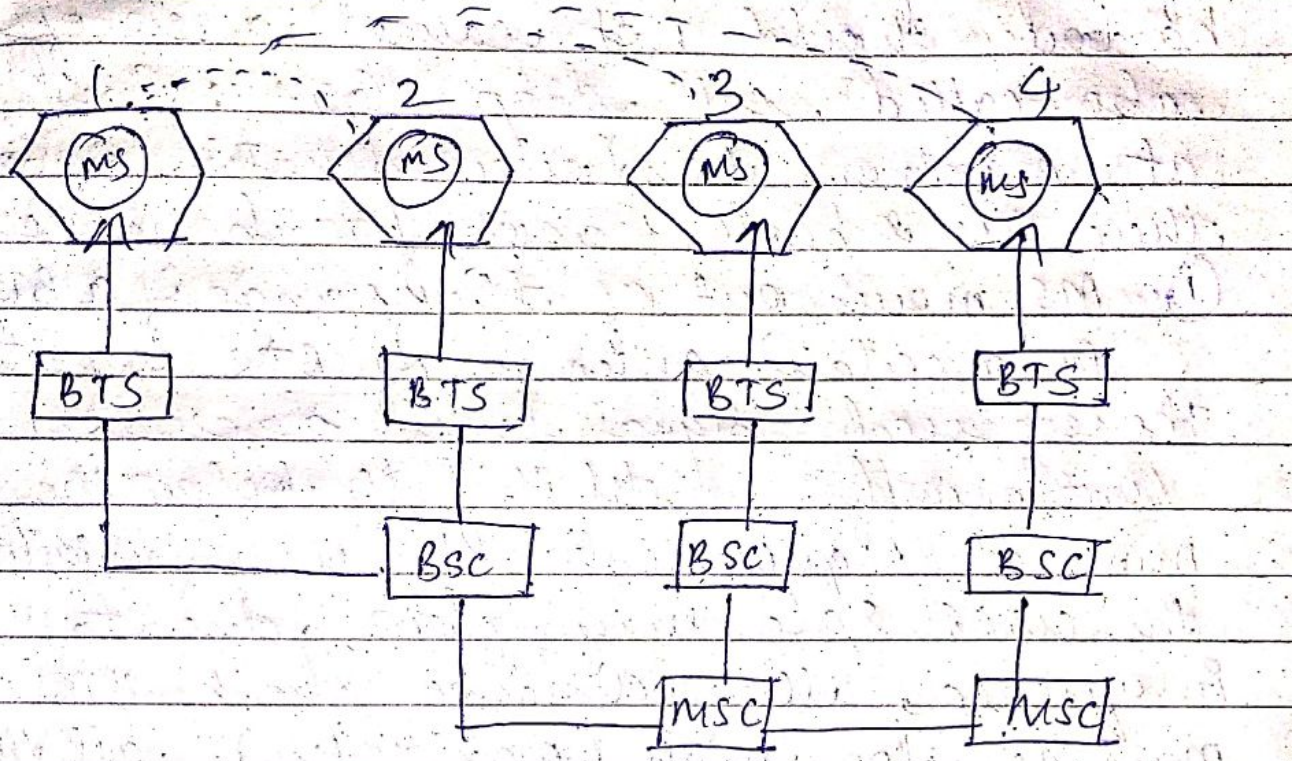
2) Since SIM's are made available in a form of smart cards (which can be inserted into any Gsm phone) or plug in modules. The SIMs are removable & portable. All Gsm mobiles without SIM are alike & non operational

3) These Gsm mobiles are any suitable terminal such as hotel phone, public phone, or any portable or mobile phone and are able to route all incoming Gsm calls to that terminal & have all outgoing calls routed

19th Aug

billed to their home phone no matter where ever its location is.

Handover in GSM



Types of Handover in GSM.

Handover is a process in mobile communication in which connected cellular call or a data session (data service) is transferred from one cell site (BS) to another without disconnecting the session. cellular system require handover procedure, as single cells do not cover the whole service area.

Eg:- Only upto 35 km around each antenna on the countryside & some 100 mtrs in city

The smaller cell size & faster the movement of a MS to the cells, the more handovers of ongoing calls are required. Handover handover should not cause a cutoff also called, call drop. GSM aims at maximum handover duration of GoM. There are 2 basic reasons for handover

(1) MS moves out of the range of a BTS or a certain antenna of BTS respectively The received signal level decreases continuously until it falls below the minimal requirements for communication the error rate may grow due to interference, the distance to the BTS may be too high (max 35 km). all these effects may diminish the quality of radio link & make radio transmission impossible in the near future.

(2) the wired infrastructure (MSC & BSC) may decide that the traffic in one cell is too high & shift some MS to other less cells with a lower load (if possible). handover may be due to load balancing.

fig shows four possible handover scenario's in Gsm.

1. Intracell handover
within a cell, narrow band interference could make transmission at a certain frequency impossible. The Bse could then decide to change the carrier frequency

2. Intercell, intraBsc handover.
this is a typical handover scenario. the mobile Station move from one cell to another, but stays within the control of same Bsc. the Bse then performs a handover, assigns a new radio channel in the new cell & releases the old one.

3. InterBsc, intra Msc handover
as a Bsc only controls a limited no of cells, Gsm also has to perform handover between cells controlled by different Bsc's.

4. Inter Msc handover.
a handover could require between two cells belonging to two different Msc. Now both Msc's perform the handover together.

GSM Security

GSM offers several security services using confidential information stored in the AUC and in the individual real (which is plugged into an arbitrary MS. & the sim stores personal, secret data & is protected with a pin PIN against unauthorized use. the security service offered by GSM are explained below.

1. Access control & Authentication
2. Confidentiality
3. anonymity

26th Aug

(1) Acess control & Authentication.

→ The first step includes the authentication of valid user for the sim.

→ The user needs a secret pin to access the sim.

→ The next step is the subscriber authentication this step based on challenge response scheme

(2) Confidentiality

all user related Data is encrypted. after authentication, BTS & MS apply Encryption to voice, data & signalling. this Confidentiality exist only between MS & BTS but it does not exist End-to-END as within the whole fix GSM

telephone network.

(3) anonymity

To provide user anonymity, all data is encrypted before transmission & user identifies (which would reveal an identity) are not used over the air. instead GSM transmit 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

three algorithm have been specified to provide security services in GSM. algorithm A3 is used for authentication, A5 for encryption & A8 for generation. Ciphers in the GSM standard only algorithm A5 was publically available where A3 & A8 were secret, but standarised with Open interface. both A3 & A8 are no longer secret, but when published on internet 1998 this demonstrates that security by obscurity does not really work as it turned out, algorithms are not very strong. however network providers can use stronger algorithms for authentication all users can apply stronger end-to-end apply encryption. algorithm A3 & A8 are located on the SIM & in the auc & can be proprietary. On the A5 which is implemented in the device has to be identical for all providers.

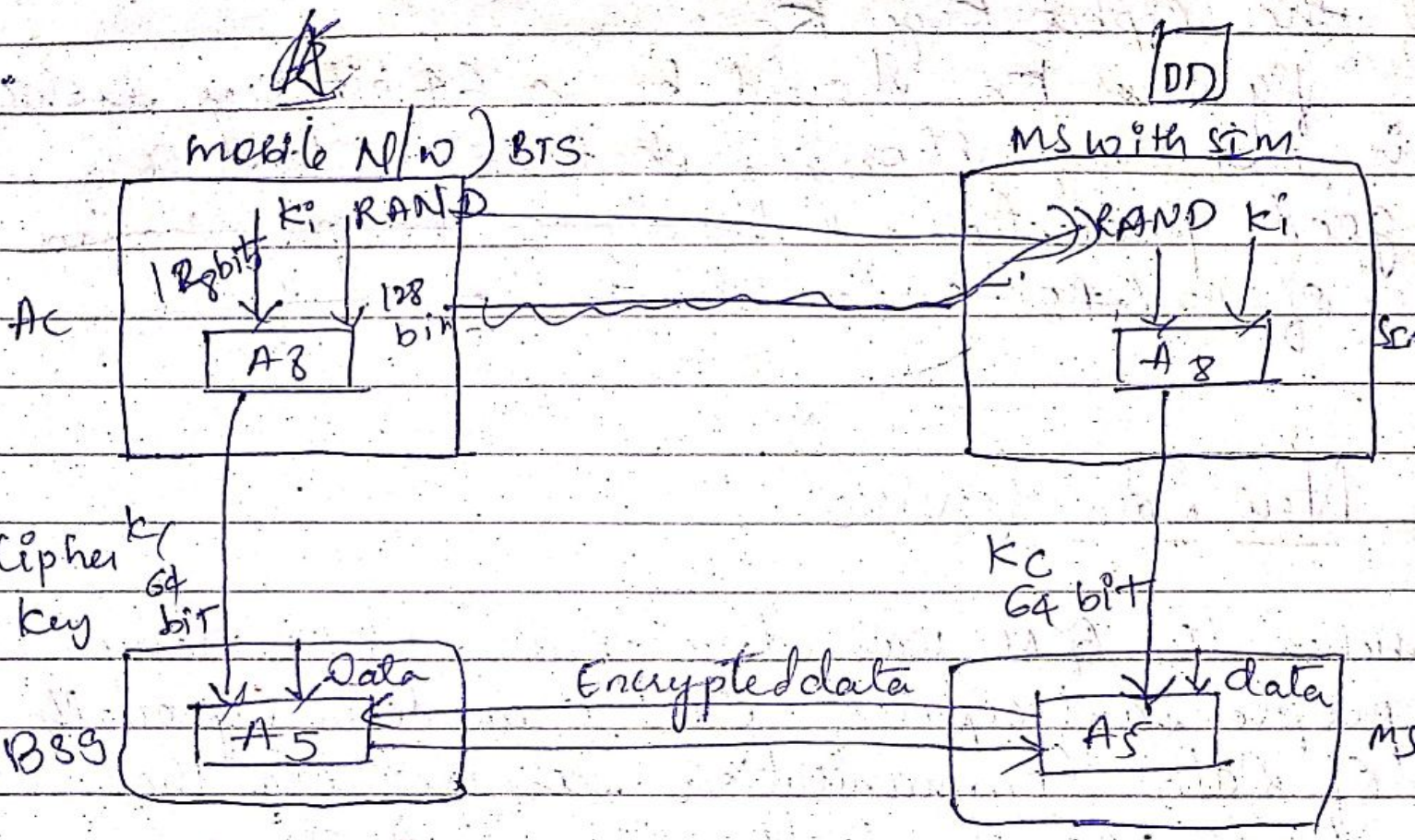


fig :- Data Encryption

Encryption :- Ensure the privacy, all message containing user related information are Encrypted in GSM over the air interface after authentication MS & BSS can start ciphering

encryption by applying the cipher (K_c). K_c is generated using the individual key (K_i) & a random value by applying the algorithm A8. Note that the SIM in the MS & the network both calculate the same K_c based on the random value (RAND). The key K_c itself is not transmitted over the air interphase. now MS & BTS can encrypt & decrypt data using the algorithm A5 & the cipher key K_c.

fig shows K_c should be a 64 bit key which is not very strong, but is atleast a good protection. ~~However the publication of A3 & A8 on the internet showed that~~

New Data Services

When the GSM was developed, not many people anticipated the tremendous growth of Data Communication compare to the Voice Communication. at that time 9.6 Kbps was left, or atleast Enough for standard group 3 fax machines. but with the requirements of Example web browsing, file download or even intensive email exchange with attachment this is not Enough

(1) To Enhance the data transmission Capabilities of GSM. two basic approaches are possible. - as the base GSM is based on connection oriented traffic channels. Eg:- with 9.6 Kbps each, several channels could be combined to increase the bandwidth. This system is called HSCSD (High speed circuit switch Data).

(2) A more progressive step is the introduction of packet oriented traffic in the GSM i.e shifting the paradigm from connections / telephone thinking to packets of internet " . The system called GPRS