Module 4
Mobile Communication Systems

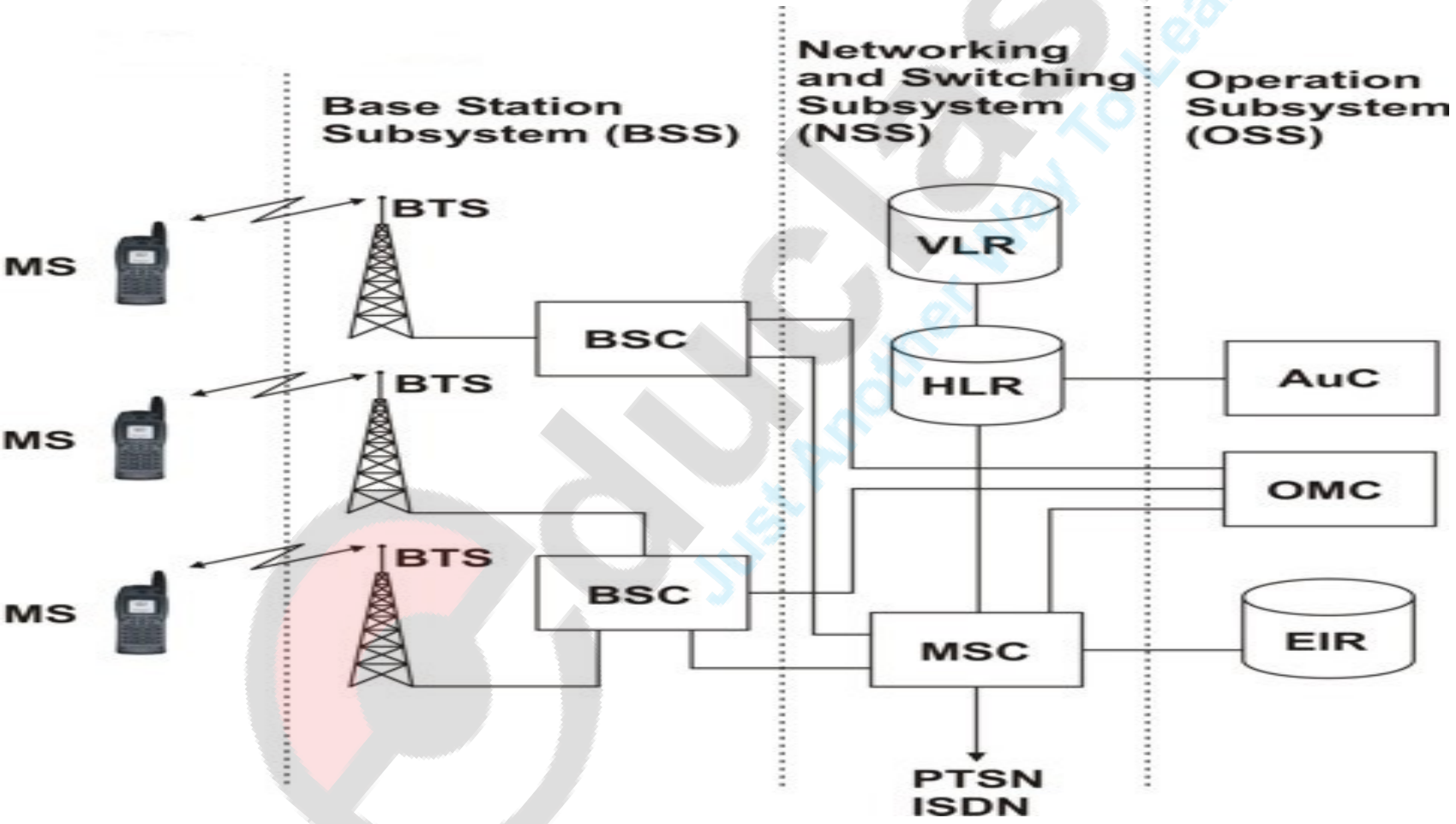
Contents:

- GSM – Architecture, Air Interface, Multiple Access Scheme, Channel Organization, Call Setup Procedure, Protocol Signalling,Handover, Security.
- GPRS – Architecture, GPRS signalling, Mobility management, GPRS roaming, network.
- CDMA2000- Introduction, Layering Structure, Channels,Logical Channels, Forward Link and Reverse link physical channels, W-CDMA – Physical Layers, Channels.
- UMTS – Network Architecture, Interfaces, Network Evolution, Release 5, FDD and TDD, Time Slots, Protocol Architecture.
- Bearer Model.
- Introduction to LTE.

GSM

- Global System for Mobile Communications.
- 2G digital mobile cellular system.
- Open system standard.
- Supports roaming to users.
- Encrypted transmission.
- Digital transmission with the use of FDMA and TDMA.
- Upgradable with downward compatibility.

1. GSM Network Architecture-I



GSM Network Architecture-II

- Consists of
  - BTS- Base Transceiver Stations
  - BSC- Base Station Controller
  - MSC- Mobile Switching Centre
  - Three databases connected to MSC
    - VLR- Visitor Location Register
    - HLR- Home Location Register
    - EIR- Equipment Identity Register
- Functional Blocks:
  - Radio Subsystem (RSS)
  - Network and Switching Subsystem (NSS)
  - Operation Subsystem (OSS)

GSM Network Architecture-III

- Role of MSC:
  - Establishing, managing and clearing connections.
  - Routing calls to the proper radio cell.
  - Call routing at the time of mobility.
  - Interface to other networks.
- HLR stores:
  - All the identity information of users- home subscription base, service profiles- for mobile user tracking.
- VLR stores:
  - Information about subscribers visiting area in the control of MSC.

1.1 RSS- Radio Subsystem

- RSS Consists of MS and BSS.
- MS-Mobile station
    - ME (Mobile equipment)- actual device, smart card
    - SIM (Subscriber Identity module).
- BSS- Base station Subsystem
    - BTS (Base station transceiver)
    - BSC (Base station controller)
    - TRAU (Trans coding and rate adaptation unit).

SIM- Subscriber Identity module

- Supports personal mobility.
- IMSI- International SIM- unique ID residing in SIM.
- A subscriber is identified with IMSI and secret key for authentication.
- IMEI- International Mobile Equipment Identity- Unique ID for ME.
- IMSI and IMEI- independent.
- TMSI- temporary IMSI- ID in case of roaming- periodically changed.
- IMSI consists of- mobile country code, mobile network code, mobile subscriber identification code.

BTS- Base Transceiver Station

- Radio transceiver system within the coverage area of a cell.
- Allows MS to communicate with the network through radio link.
- BTS- MS communication via an omnidirectional or directional antenna.
- Major functions:
  - Transmission of signals in desired form
  - Coding and decoding
  - Nullification of propagation effect
- Can handle 7 users at a time with 1 channel reserved for downlink broadcasting.
- System capacity can be increased using frequency reuse.

BSC- Base Station Controller

- Radio transceiver system within the coverage area of a cell.
- Major functions:
  - Radio resource management
  - Handover
  - Control of transmitted power
- BSC communicates with BTS through TDM A_{bis} interface.

TRAU- Trans coding and rate adaptation unit

- Logical part of BSS.
- Resides close to MSC to reduce significant transmission cost.
- Major function- to convert speech to 64 kbps rates over the PSTN or ISDN (Integrated service digital networks)
- Using multiplexing and transcoding.
-
  - Main communication in 2G – voice- converted to binary stream.
  - Voice data is sent in 16kbps channel through BTS to BSC to TRAU from MS.
  - TRAU converts it to 64 kbps.

1.2 NSS- Network Switching Subsystems

- Consists of- MSC, HLR, VLR.
- MSC- Mobile Switching Centre:
  - Mobility of a user
  - Controls switching and management by controlling BSCs
  - Processes request for connection
  - Registration and authentication
  - Sends request to AuC (Authentication centre) for user information and performs authentication.
  - MSC registers MS with the VLR- Location information is updated in HLR.
  - Routes calls to and from MS
  - Gateway to connect the call to other fixed networks

HLR- Home Location Register

- Maintains all the information related to mobile subscriber in its database.
- Remains unchanged until the termination of the subscription.
- Registration of subscriber with network operator- SLA (Service level agreement) is formed.
- Operator's network- Home network.
- HLR- located within the home network.
- Stores:
  - Administrative information of mobile subscribers- IMSI, type of subscription, services, current location, service restriction, supplementary services.
  - Receives connection information when roaming between different countries - requires agreement between two operators.

VLR- Visitor Location Register

- Temporary database to which subscriber currently registers.
- Covers service area of its associated MSC.
- Interacts with HLR while recording data.
- When user is roaming:
  - MS requests MSC for connection.
  - After authentication from AuC, MSC updates VLR.
  - Updated information is sent to HLR.

1.3 Operation Subsystem (OSS)

- Consists of
  - AuC- Authentication Centre
  - OMC- Operating and Maintenance Centre
  - EIR- Equipment Identity Register

AuC- Authentication Centre

- Database that stores a copy of secret key of the user's SIM card.
- Enables authentication and encryption over the radio link.
- Has the required data to protect the network from false users and authentication of users.
- Protects the calls of regular user.
- 2 secret keys:
  - Encryption of communication between mobile users.
  - Authentication of users.
- Keys are kept in ME and AuC.

OMC- Operating and Maintenance Centre

- Centrally monitors and controls the network elements.
- Maintains service quality for a network.
- Performs:
  - Network monitoring
  - Network development
  - Network measurements
  - Fault management

EIR- Equipment Identity Register

- Stores IMSI of all valid mobiles on the network.
- IMSI is installed during the manufacture of the equipments and specifies the standard as GSM.
- Network checks this number during a call.
- If number is not validated- access is denied.

2. GSM Air Interface

- Central interface in every mobile system.
- The only interface the mobile subscriber is exposed to.
- Quality depends on the efficient usage of frequency spectrum.
- Allotted frequency band: 900 MHz to 1800 MHz.
- Carrier separation: 200 kHz
- Duplex distance: 45 MHz
- No. of RF carriers: 124
- Access method: TDMA/FDMA
- Modulation method: GMSK
- Modulation data rate: 270.833 kbps

3. GSM Multiple Access Scheme-I

- Combination of FDM and TDM.
- FDMA:
  - In Europe:
    - GSM900 band: uplink: 890-915 MHz, downlink: 935-960 MHz.
    - Duplex distance of 45 MHz.
    - Bands are divided by frequency into 124 carriers, each separated by 200 kHz.
  - Each frequency ranges into 125 channels of 200 kHz bandwidth.
  - 1 channel- guard band
  - 124 channels- transmission and reception.
  - 124 duplex communication channel.

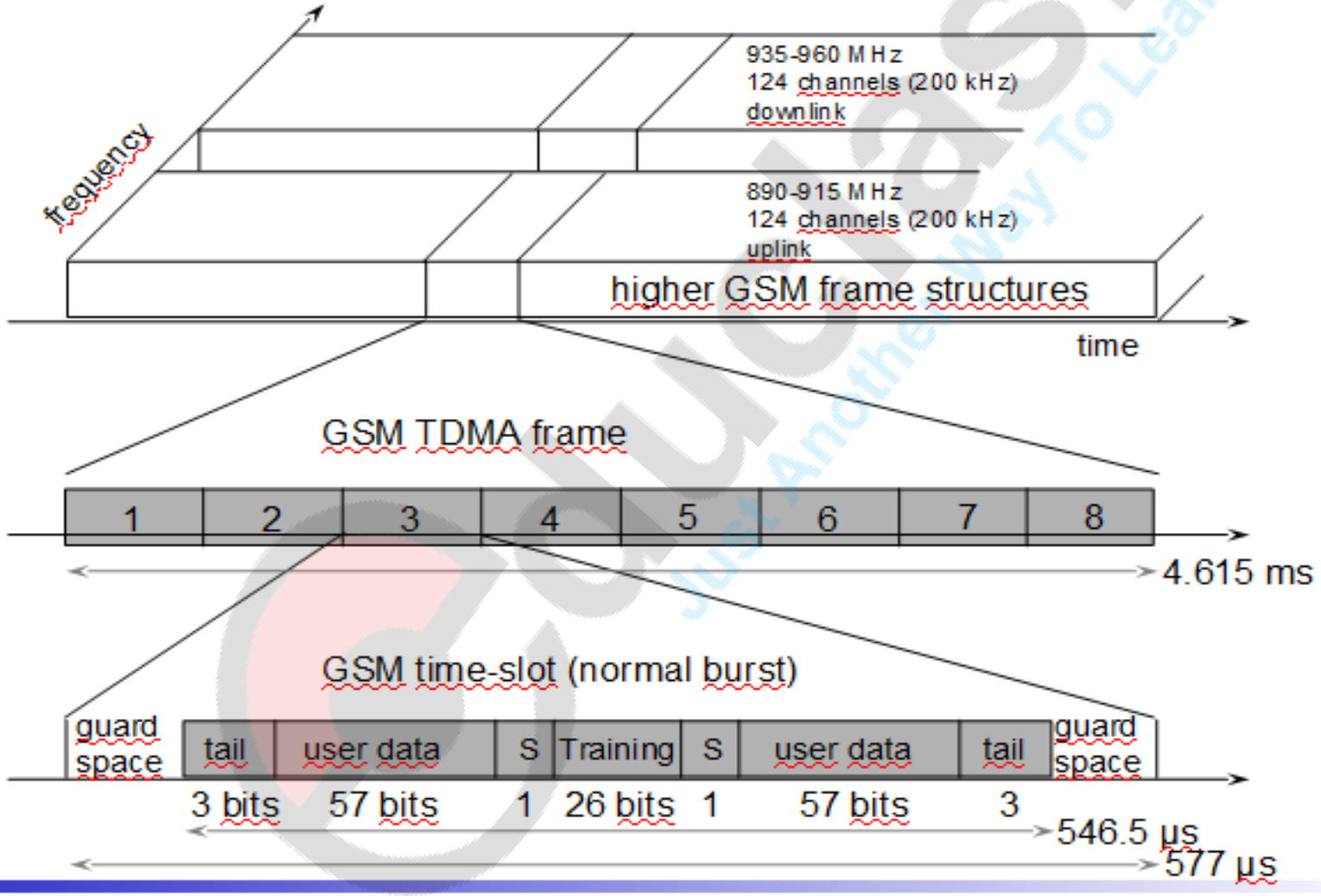
GSM Multiple Access Scheme-II

- TDMA:
  - Each carrier frequency is divided into 8 time slots that form a TDMA frame.
  - A full rate system: 8 time slots on every frequency.
  - Half rate system: 16 time slots on every frequency.
  - Impulse like signals are sent periodically.
  - In a full rate system:
    - every impulse : burst
    - Burst corresponds to a time slot of 0.577ms.
    - 1 TDMA frame=8 bursts= 4.615 ms.

4. GSM Channel Organization

- Traffic and signalling/control channels.
- One slot of TDMA frame- physical channel.
- Logical channels are mapped onto physical channels defined by the number and position of their corresponding burst periods.
- Multiframe structure to map logical channels on physical channels.
  - Traffic channel multiframe- 26 groups of 8 TDM frames.
  - Control channel multiframe- 51 groups of frames.

Traffic channel multiframe-I



Traffic channel multiframe-II

- TCH with slow and fast associated control channels SACCH (slow associated control traffic channel) and FACCH (Fast associated control traffic channel).
- Used to carry speech or circuit switched data traffic.
- 26 multiframe- used to define TCH.
- Length of 26 multiframe= 120 ms.
- 6 different forms of services:
  - Full rate speech with bit rates of 13 kbps (speech), 2.4, 4.8, 9.6 kbps.
  - Half rate channels with bit rates of 6.5 kbps (speech), 2.4 kbps, 4.8 kbps for data.

Traffic channel multiframe-III

- SACCH:
  - Time slots 12 or 25 are used for SACCH.
  - 1 SACCH per multiframe.
  - Length of SACCH= 456 bits.
  - Reporting time= 480 ms
  - Mobile device uses this information to increase or decrease its power levels in every 60 ms.
  - SACCH can be used for sending SMS while call is going on.
- A traffic channel is only assigned when mobile device is in dedicated mode.

Traffic channel multiframe-IV

- FACCH- Fast associated control traffic channel
  - Obtained by stealing from the TCH.
  - Used by either end for signalling the transfer characteristics for physical path.
  - Used for Connection handover control messages.
- In GSM
  - Normal burst= 148 bits
  - Unused 8.25 bit guard band at the end of each burst
  - 114 bits= data bits transmitted in two sequences of each 57 bits at the beginning and end.
  - 26 bits= training sequence- analyze radio channel characteristics
  - One time slot to transmit
  - One time slot to receive
  - Six time slots to measure signal strength.

Control channel multiframe-I

- Consists of 51 frames.
- Incorporate control, timing and signalling.
- BCCH:
  - Broadcast control channel
  - Used in the BSS to mobile direction to broadcast system information
  - Synchronization parameters, available services, cell ID
  - Continuously active channel
  - Dummy bursts when no information to transmit

Control channel multiframe-II

- DCCH
  - Dedicated control channel
  - 3 subtypes
    - Point to point control channel
    - Standalone dedicated control channel
    - Fast associated dedicated control channel
- SDCCH
  - Standalone dedicated control channel
  - Used for call setup and location upgrading
  - Used for SMS in idle state
  - Has its own SACCH which is released once call setup is complete.

Control channel multiframe-III

- CCCH
  - Common control channel
  - 3 subchannels- 1 for uplink (MS to BTS) and 2 for downlink
  - Used for transferring signalling information between mobiles and BSS- for call origination and paging
- RACH
  - Random access channel
  - Used for uplink communication
  - Allows MS to send request for time slot on DCCH that can be used to assign a TCH for voice call
  - MS use slotted ALOHA over this channel for requesting DCCH at call initiation.

Control channel multiframe-IV

- PCH
  - Paging channel
  - Used to send paging messages to a mobile user during incoming call
  - Within specific time intervals MS will listen to PCH
  - Includes IMSI or TMSI
- AGCH
  - Access grant channel
  - To assign resources to a mobile e.g. DCCH
  - BS announces the assigned slot on AGCH
  - AGCH and PCH are never used at the same time- hence are implemented on same logical channel

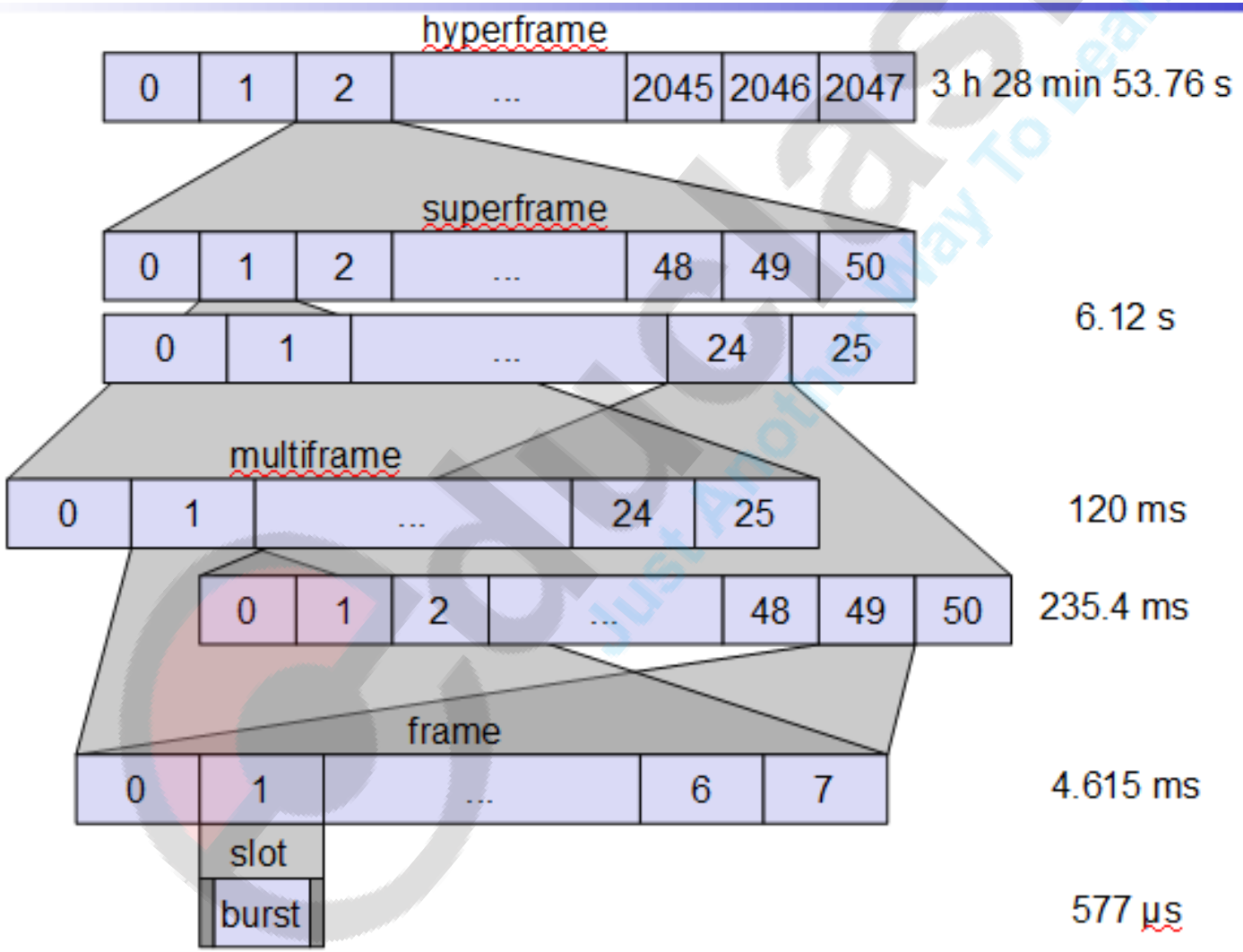
Control channel multiframe-V

- FCCH
  - Frequency correction channel
  - Used to ensure the MS tunes its frequency wrt BS
  - Carries information from BSS for carrier synchronization
- SCH
  - Synchronization channel
  - Used to frame synchronize the mobile device by broadcating BSIC(BS identity code) or SCH
  - For MS to identify correct BS
  - BSIC can only be decoded if BS belongs to a GSM network
- All control channels except SDCCH are implemented on the time slot 0 in different frames in 51 multiframes using dedicated RF carrrier frequency assigned to each cell.

Control channel multiframe-VI

- Division of GSM logical channels
  - Traffic channels- Full TCH, Half TCH
  - Broadcast channels- BCCH, FCCH, SCH
  - Common control channels- RACH, AGCH, PCH
  - Dedicated control channels- SDCCH, SACCH, FACCH

Frames, Multi-frames, Super-frames and Hyper-frames-I



Frames, Multi-frames, Super-frames and Hyper-frames-II

- Frame- 8 time slots of 4.615 ms
- Multiframe- block of 26 frames of total duration of 120 ms- used to transfer information
- Superframe- 26x51 TDMA frames- duration of approx 6.12 sec- 51 control channels
- Hyperframe- 2048x26x51 TDMA frames- 3hrs 28 min 53 sec 760 ms
- Frames are numbered
  - T1- superframes- 0 to 2017
  - T2- voice frames – 26 multiframes- 0 to 25
  - T3- 51 signalling frames- 0 to 50
- Information is used to know exactly how long it has to wait for data or transmission

5. GSM call set up procedure

- MS registration with the network- after powering up the MS
- Check for authenticity
- Connection request/ Connect to a last network
- New location- search for frequency band
- MS- looks for strong BCCH- includes FCCH and SCH
- FCCH- synchronizes MS with BS, location area information
- Connection request from MS to BS- through RACCH
- Acceptance signal through AGCH.

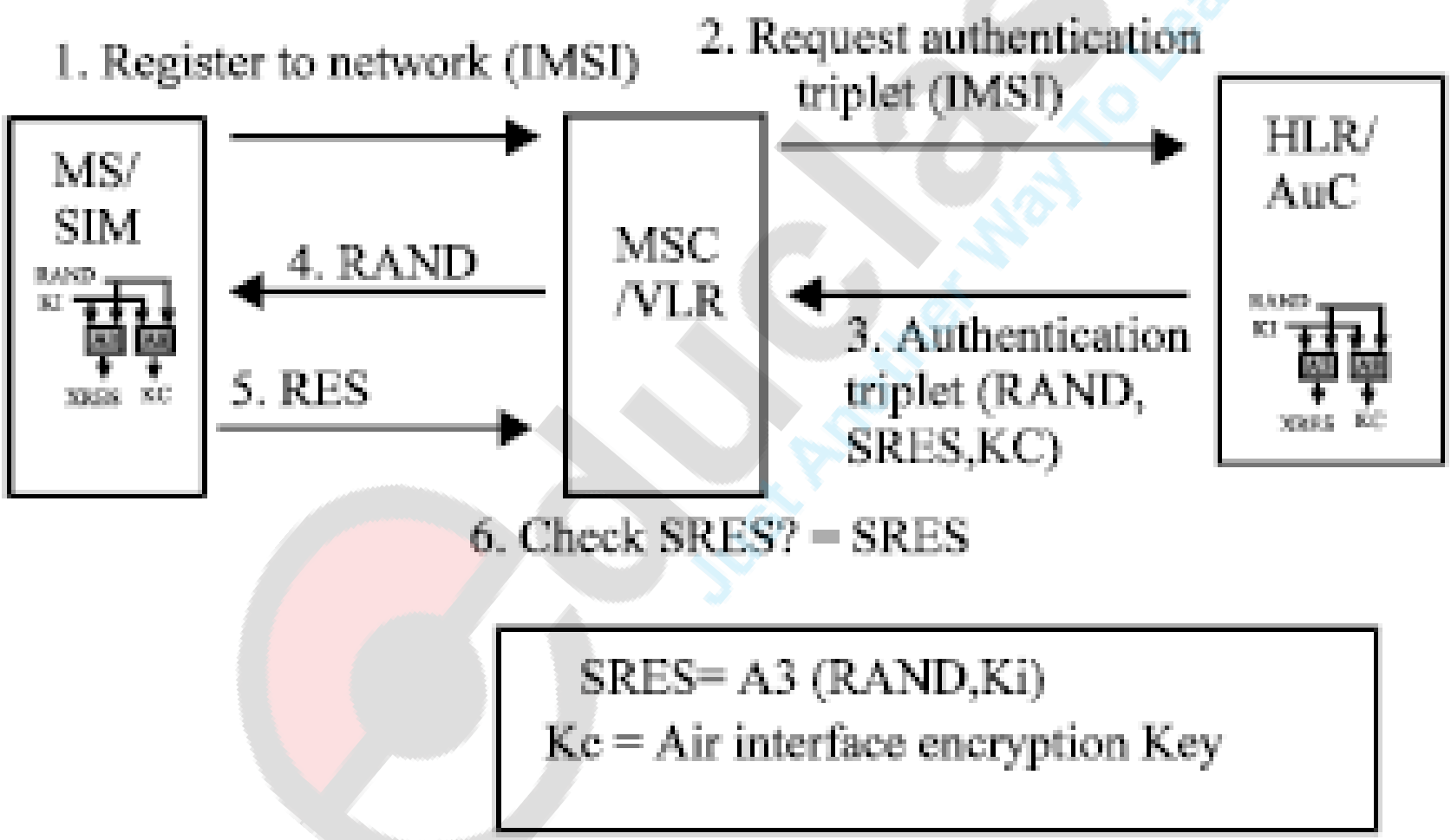
GSM call set up procedure- Authenticity Check-up

- IMSI is sent by MS to MSC with the help of HLR or AuC.
- Reply- MSC sends RAND(random no), key and result SRES(signed response)
- SIM card generates another SRES sent to MSC
- Compare results of SRES from AuC using RAND
- Key is used for data encryption between BS and BTS
- After authentication MSc requests IMEI
- MSC checks IMEI with EIR
- After IMSI and IMEI- MSC sends information to HLR

MSC register MS with curent VLR.

- In VLR- TMSI is used
- MS is assigned SDCCH or TCH.

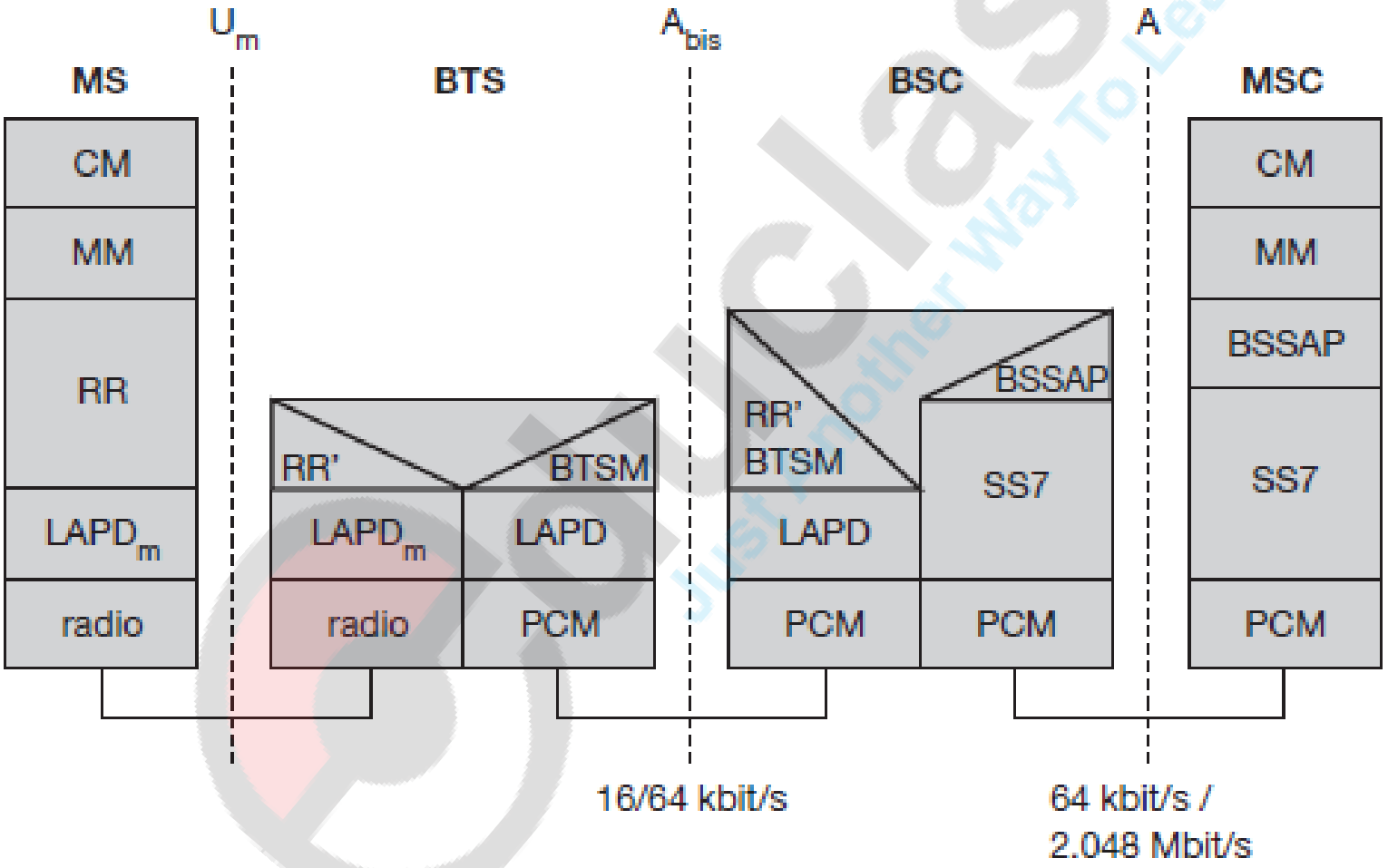
GSM call set up procedure- Authenticity Check-up



6. GSM Protocols and Signalling

- 3 layers:
  - Layer 1: Physical layer- Air interface
  - Layer 2- data link layer- LAPDm(Link access protocol D)
  - Layer 3: 3 sublayers:- functionalities similar to transport, presentation and session layer of OSI layer model.
    - Mobility management (MM)- between MS and MSC
    - Radio Resource Management (RRM)- between MS and BSS
    - Connection management (CM) for calls routing- between MS and MSC

GSM Protocol architecture for signalling



A_{bis} Interface

- Interface between BTS and BSC.
- Uses PCM.
- 2 Mbps PCM link.
- Transmission rate of 2.048 Mbps having 32 channels of 64 kbps each.
- Since TCH is 13 kbps and A_{bis} is 64 kbps, multiplexing and transcoding is required.

A Interface

- Between TRAU and MSC or physically between MSC and BSC.
- Consists of one or more PCM links each having capacity of 2048 Mbps.
- 2 parts of A interface- BTS to TRAU- compression and TRAU to MSC – decompression

Link Layer LAPDm protocol-I

- Connects MS to BSS.
- General frame format:

Address Field	Control Field	Length Indicator	Information Field	Fill bit

- Address field format:

Spare 8	LPD 7 6	SAPI 5 4 3	C/R 2	EA 1

Link Layer LAPDm protocol-II

- Address field:
  - 8th bit- spare- for future use.
  - 6th and 7th bit- LPD- Link protocol discriminator- particular recommendation of use of LPDm.
  - SAPI- service access point identifier
    - SAPI 0- used for call control, MM and RR signalling
    - SAPI 3- SMS
  - 2nd bit- C/R- command/ response frame
  - 1st bit- EA- extended address- to extend the address field more than 1 octet

Link Layer LAPDm protocol-III

- Control field:
  - To carry sequence number
  - To specify types of frames
  - 3 types of frames:
    - Supervisory functions
    - Unnumbered information transfer and control functions for unacknowledged mode
    - Numbered information transfer for multiframe acknowledged mode
- Length indicator:
  - To distinguish information carrying field from fill in bits used to fill the transmission frame.

MS to BTS protocols-I

- **RR layer**
  - lower layer that manages a link, both radio and fixed
  - between the MS and the MSC.
  - manage the RR-session, the time when a mobile is in a dedicated mode, and the radio channels including the allocation of dedicated channels.
- **MM layer**
  - stacked above the RR layer.
  - mobility of the subscriber, as well as the authentication and security aspects.
  - Location management

MS to BTS protocols-II

- **CM layer**
  - topmost layer of the GSM protocol stack.
  - Call Control, Supplementary Service Management, and Short Message Service Management.
  - call establishment, selection of the type of service (including alternating between services during a call), and call release.

BSC protocols

- The Abis interface is used between the BTS and BSC.
- the radio resources are changed from the RR to the Base Transceiver Station Management (BTSM). T
- The RR protocols are responsible for the allocation and reallocation of traffic channels between the MS and the BTS.
- controlling the initial access to the system, paging for MT calls, the handover of calls between cell sites, power control, and call termination.
- radio resource management for the frequency coordination, frequency allocation, and the management of the overall network layer for the Layer 2 interfaces.
- To transit from the BSC to the MSC, the BSS mobile application part or the direct application part is used, and SS7 protocols is applied by the relay, so that the MTP 1-3 can be used as the prime architecture.

MSC protocols-I

- the information is mapped across the A interface to the MTP Layers 1 through 3.
- Base Station System Management Application Part (BSS MAP)-equivalent set of radio resources.
- The relay process is finished by BSS MAP/DTAP, MM, and CM.
- MSCs interact using the control-signalling network.
- Location registers are included in the MSC databases

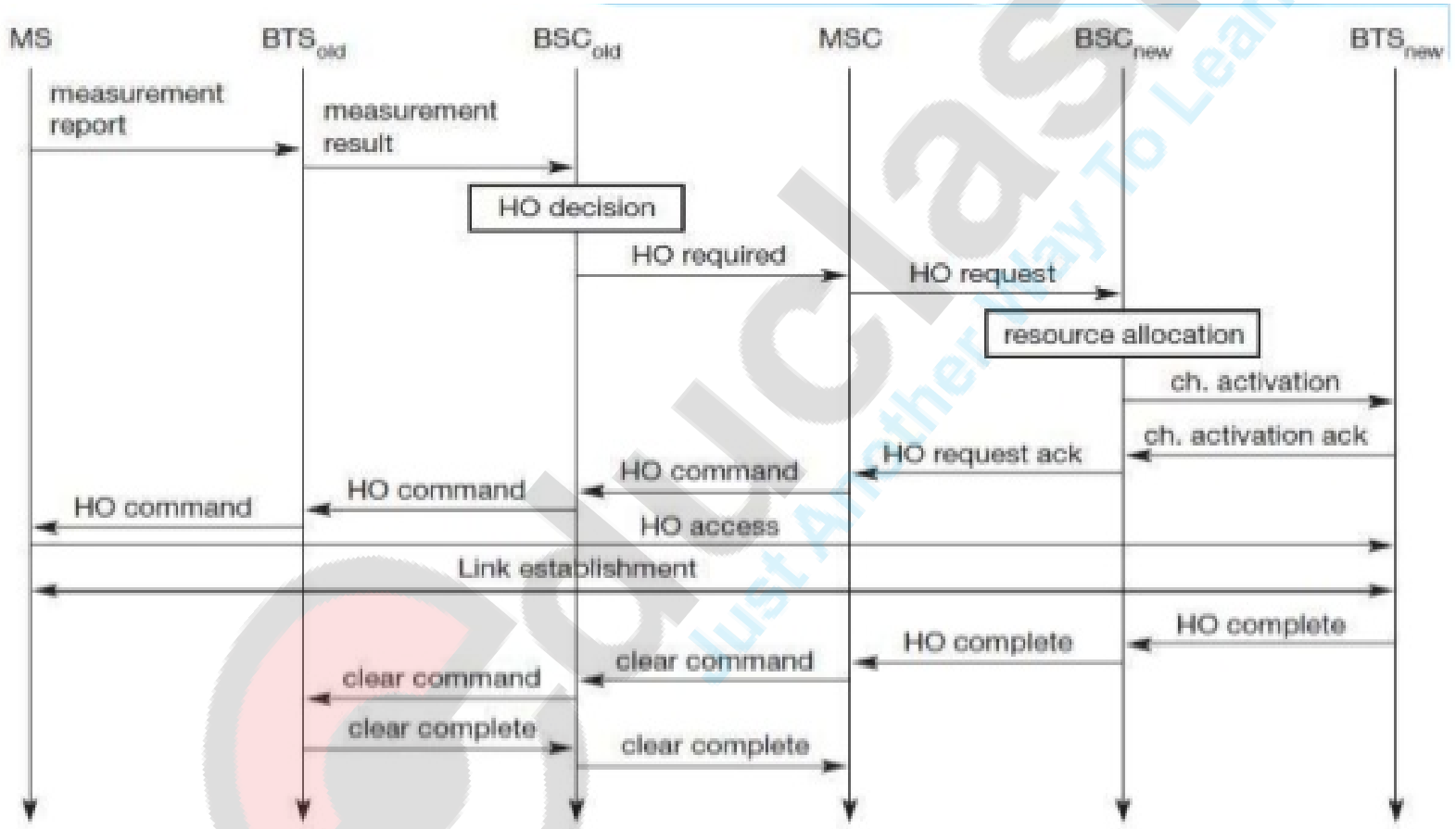
MSC protocols-HLR and VLR communication

- Each GSM MS user is given a HLR that in turn comprises of the user's location and subscribed services.
- VLR is a separate register that is used to track the location of a user.
- When the users move out of the HLR covered area, the VLR is notified by the MS to find the location of the user.
- The VLR in turn, with the help of the control network, signals the HLR of the MS's new location.
- With the help of location information contained in the user's HLR, the MT calls can be routed to the user.

7. GSM Handover-I

- In GSM, max handover duration= 60 ms
- 2 reasons:
  - MS moves out of range of BTS
  - Traffic in one cell is too high – i.e. load balancing
- 4 scenarios:
  - Intra-cell handover- controlled by BSC
  - Intra-cell, intra-BSC handover- controlled by BSC
  - Inter BSC, intra MSC handover- controlled by MSC
  - Inter MSC handover-controlled by both MSCs
- MS and BTS perform periodic measurements of downlink and uplink quality resp.
- Handover decision based on average value received from various BTS by BSC- by comparing with threshold value.

GSM Handover-Intra MSC handover



8. GSM Security

- Method 1:
  - Entities involved- SIM card and AuC
  - Secret key stored in SIM and AuC
  - SRES is generated randomly using secret key and ciphering algorithm A5
  - SRES compared with AuC SRES
- Method 2:
  - Unique IMEI no stored in EIR
  - Status returned in response to IMEI query to EIR:
    - White listed: terminal is allowed to connect to a network
    - Grey listed: terminal under observation from network for possible problems
    - Black listed: terminal stolen/ not approved

Reference books (Topic-wise)

- Wireless Communications and Networks, 3G and Beyond, Second Edition, ITI Saha Misra, McGraw Hill Education-

Topics: GSM – Architecture, Air Interface, Multiple Access Scheme, Channel Organization, Call Setup Procedure, Protocol Signalling,Security.- **Chapter No. 8**

- Mobile Communications, Second Edition, Jochen Schiller, Pearson Education

Topic:GSM Handover- **Chapter 4 , section 4.1.6, page no. 117**

University Questions

- Explain GSM architecture in detail.- May 16- 10M
- What are the functions of authentication and encryption in GSM? How the system security is maintained?- Nov 16- 10M
- What are the different types of control channels in GSM? Explain how and what control channels are used for mobile originated and terminated calls in GSM.- Nov 16- 10M
- Give reasons of a handover in GSM and problems associated with it. What types of handover can occur?- Nov 16-7M