NAME:- DUBEY KARAN SANJEEV

CLASS:- B.E - 4

ROLL NO:- ~~04~~ 04

BATCH:- A

SUBJECT:- DSIP ASSIGNMENT 1

Q1. Consider the scenario in which a station calls a mobile station (the calling station could be outside the GSM network or another mobile station) and also demonstrate the messages are exchanged b/w MS and BTS during connection setup.

Answer

The following steps are.

Step 1: A PSTN user dials the phone number of a GSM subscriber. The fixed network (PSTN) notices that the number is of the GSM network and forwards call setup of the Gateway MSC (GMSC)

Step 2:- GMSC identifies the HLR (from the IMSI no. of the called MS) for the subscriber and signals the call setup to the HLR.

Step 3:- The HLR now checks whether the number exists and whether the user has subscribed to the requested service

Step 4:- HLR Request a mobile subscriber roaming number (MSRN) from the current VLR.

Step 5:- HLR receives MSRN. and the HLR can determine responsible MSC for the MS.

Step 6:- The HLR forwards this information to GMSC.

Step 7:- The GMSC forwards call setup request to the MSC.

Step 8,9:- The MSC first requests the current status to the MSC. from the VLR.

Step 10:- If the MS is available, the MSC initiates paging in all sets.

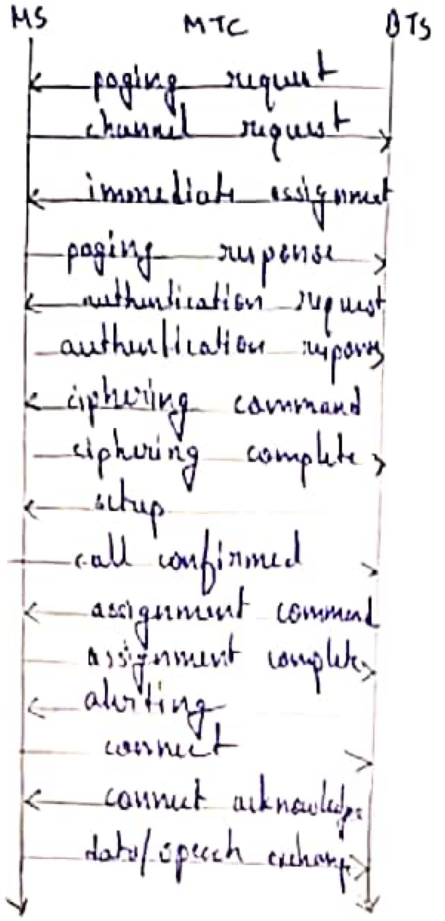
Step 11:- The BTS of all BSS transmit this paging signal to the MS.

Step 12, 13:- The MS answers.

Step 14, 15:- The VLR does the security checks.

1/8

step 16, 17 :- The connection is setup.



Q.2. Determine the main reasons for using cellular system. Compare, define hopping sequence and compare slow hopping and fast hopping sequence.

Answer

① Higher capacity
Implementing SDM allows frequency reuse. If one transmitter is far away from another transmitter then the transmitters can use the same frequency without any interference.

② Less Transmission power.
If the transmission is far away from the receiver then it requires high power to transmit the signal. For mobile devices power is the main constraint, so reduce cell size requires less transmission power.

③ Local Interference Only
with large cells, the distance b/w the mobile station and the base stations only have to deal with 'local' interference.

④ Robustness.
Cellular System are decentralized and so no more robust

the failure of single components.

(i) FHSS implements TDM plus FDM.

(ii) The pattern of channel use (frequency pattern) is called the hopping sequence.

(iii) Time spent on a channel with certain frequency is called the dwell time.

(iv) There are two variants of FHSS called slow and fast hopping.

I Slow Hopping

(i) Transmitter uses one frequency for several bit periods. Transmitter uses frequency f_2 for transmitting the first three bits and takes dwell time t_d. Then transmitter hops to the next frequency F_3.

(ii) Slow hopping is cheaper and has relaxed tolerance.

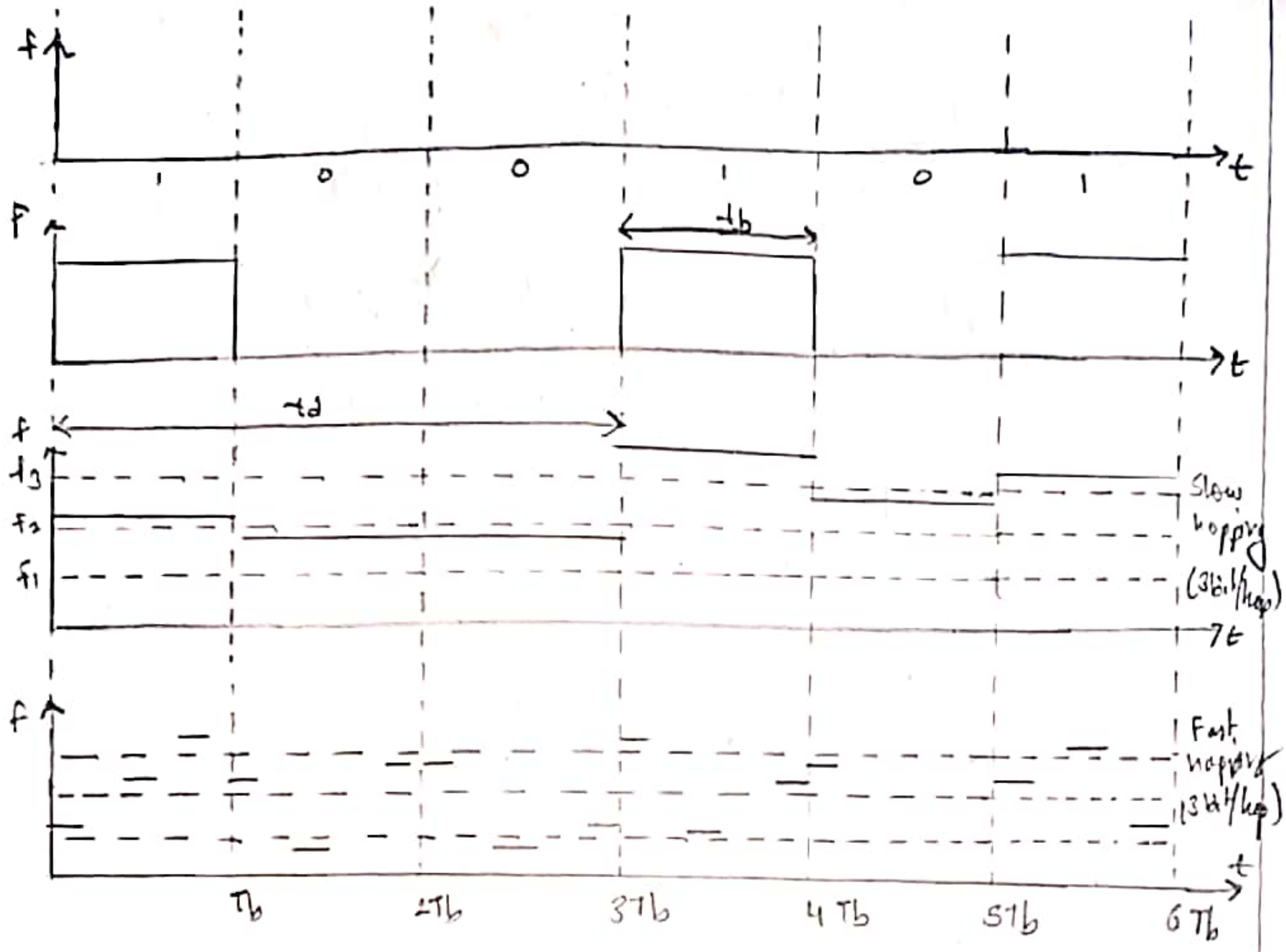
(iii) It is less immune to narrowband interference.

II Fast hopping

(i) Transmitter changes frequency several times during a bit period

(ii) Fast frequency hopping systems are more complex to implement because transmitter and receiver should stay synchronized.

(iii) These systems have better resistance against narrowband interference and frequency selective fading.



Q.3. Write a perl script to copy content of one file to another file. List and explain the security services offered by GSM. Describe the encryption mechanism in GSM to ensure privacy of messages containing user related information.

Answer

Code:-

```
use strict ;
use warnings;
use vars qw($file content $total);
my $file1 = "file1.txt}";
open (FILE1, $file1)|| die "couldn't open the file!";
open (FILE2, '>>file2.txt")|| die "couldn't open the file!";
while ($file content = <FILE1>){
chomp ($file content);
print FILE2 $file content."\n";
}
close (FILE 1);
```

close (FILE 2);

GSM offer several securities services using confidential information stored in the AuC and the SIM. These security services offered by GSM are explained as follows.

1 Access Control and authentication.

(i) This include the authentication of a valid user for the SIM. The user needs to enter a secret PIN to access a PIN.

(ii) The GSM network also authentication the subscriber. This is the done through the use of a challenge response.

2. Confidentiality

(i) In GSM, confidentiality of user data is achieved by encrypting the data over air interface.

(ii) After authentication MS and BTS apply encryption to voice, data and signaling information.

(iii) The confidentiality exists between MS and BTS only. It does not exist end-to end.

3. Anonymity

(i) To grade and provide anonymity the identity of a subscriber is always hidden over the air interface. All data is encrypted before transmission and user identifiers are not over the air.

(ii) Three algorithm are used to provide security services in GSM.

- Algorithm A3 is used for authentication.
- Algorithm A5 is used for encryption.
- Algorithm A8 is used for generation of cipher key.

Algorithm A3 and A8 can be differ but algorithm A5 is common for all service provider.

Authentication:-

(i) Before accessing any GSM service the user must be authenticated.

(ii) Authentication process use challenge - response method.

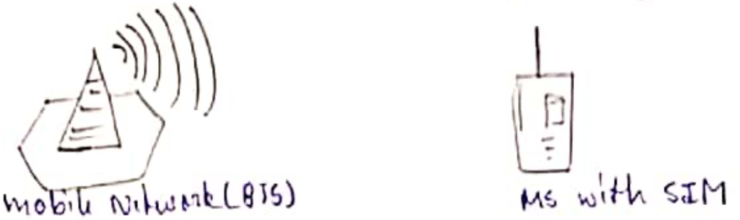
Encryption

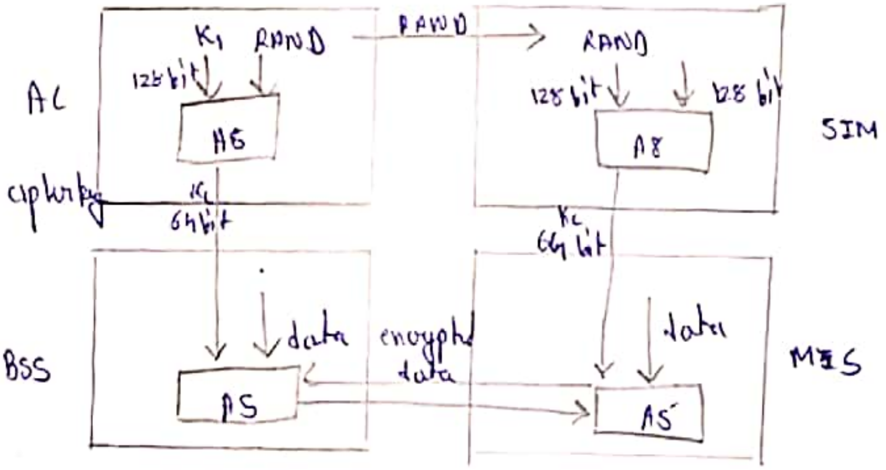
To ensure privacy, all messages containing user-related info. are -encrypted in GSM over the air interface.

(i) Once authentication is done, MS and BSS can initiate encryption.

(ii) The ~~SIM~~ SIM and access control (AC) generate the 64 bit cipher key Kc by using the authentication key Kc and 128 bit random number RAND and supply algorithm A8.

(iii) The MS and BTS can now encrypt and decrypt data using Algorithm A5 and the cipher key Kc.





Q4. What is tunnel? Explain IP-in-IP encapsulation. List the entities and terminologies in Mobile IP and describe the IP packet delivery.

Answer

(i) IP-in-IP encapsulation is defined in RFS 2003. It is the simplest approach and must always be supported.

(ii) In this type of ensapsulation, the entire IP datagram as the payload.

The various fields in outer header are:-

① ver. (version): Version field denotes the version number and set to 4 for IPV4.

② IHL (Internet header length):- IHL Indicates the length of the outer header.

③ DS (TOS):- It is just coppied from the inner header.

④ length:- It denotes the complete length of the encapsulated packet.

⑤ TTL (Time to live):- It indicates the period of validity of the packet. TTL should be high enough so the packet can reach the tunnel point.

⑥ IP-in-IP:- This denotes the complete length of the encapsulated packet.

⑦ IP checksum:- This is used for error detection mechanism.

Advantages.

It is simple to implement and it is a default encapsulation mechanism.

Dis advantage

Most of the outer header fields are same as inner header so this method increases redundancy.

(i) When a mobile node moves out from Home Network, the HA sends packet to COA of the MN via a tunnel.

(ii) A tunnel establishes a virtual pipe for data packet.

(iii) If forign agent COA is used then FA act as the tunnel end point and if co-located COA is used then MN acts the tunnel end point.

Original IP head	Original data

new IP header	new data

outer header	inner header	Original data

IP - encapsulation.

ver.	IHL	DS(TOS)	length
IP identification		flags	fragment offset
TTL		IP-in-IP	IP checksum
IP address of HA.			
Care - of address COA.			
ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL		lay-4 prot	IP checksum
IP address of CN			
IP address of MN			
TCP/ UDP/ ... payload.			

IP - in - IP encapsulation.