DATE

Page No 18

# Overall working of UMTS

- Universal Mobile Telecommunication System (UMTS)
- UMTS Terrestrial Radio Access N/w (UTRAN), its like the brain of the UMTS
- UMTS uses 3G Technology
- UMTS supports circuit transmission and pkt-switch transmission

- If the user wants to make a call it uses circuit switch Transmission
- If the user wants to access the data using the mobile it makes use of pkt switch transmission.

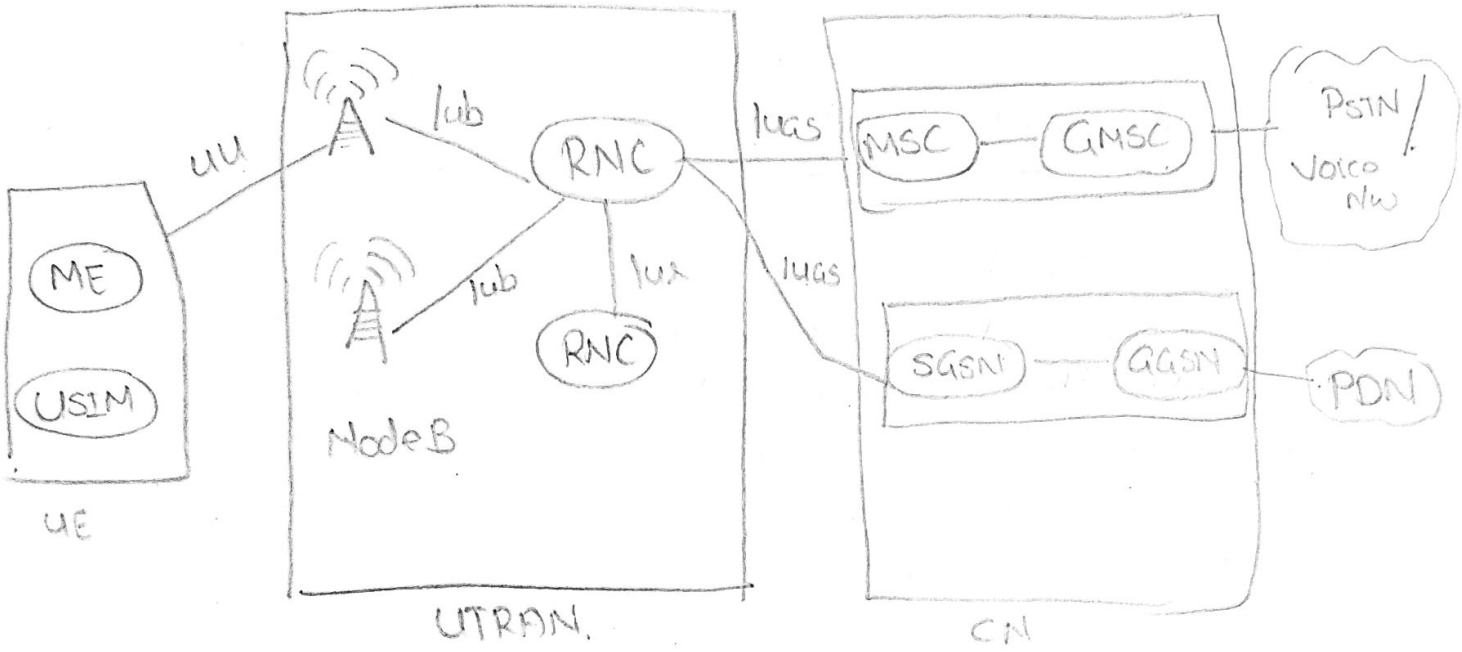
- ~~UTRAN~~ Once the SIM is added into the Mobile (ME) it forms the UE

- Node B is similar to the BTS in GSM

- when the mobile makes a req the req is transmitted to Node B and from there to the RNC. An RNC can be connected to many Node B using Iub interface. One RNC n/w can be connected to another RNC n/w using the Iur interface Depend on the users req. if its a call then it will be connected to the PSTN n/w

[RNC does the decision making]

RAMASONS




UE - User Equipment

ME - Mobile Equipment (Mobile phone)

CN - Core N/w

RNC - Radio N/w controller

PDN - Packet Data N/w

Using the circuit switching interface using Iucs interface GMSC is a gateway for MSC using it we can connect to the PSTN

- If the user wants to access the data using the mobile it uses Iups interface and connects to the PDN

DATE

Page No 19

⇒ Comparison of GSM and UMTS

a) Unlike GSM, signalling msg in UMTS are individually authenticated and integrity protected hence the false base station attack is possible in GSM but not in UMTS. Thus an attacker cannot fake eg spoof a cipher mode msg instructing the cellphone to suppress encryption.

b) In GSM there is no provision for the cellphone to authenticate the n/w. UMTS supports mutual authentication. As part of the authentication protocol, the SIM card and the n/w agree on an encryption key and also a key for integrity protection of messages. Further the use of sequence numbers and nonce help prevent replay attack.

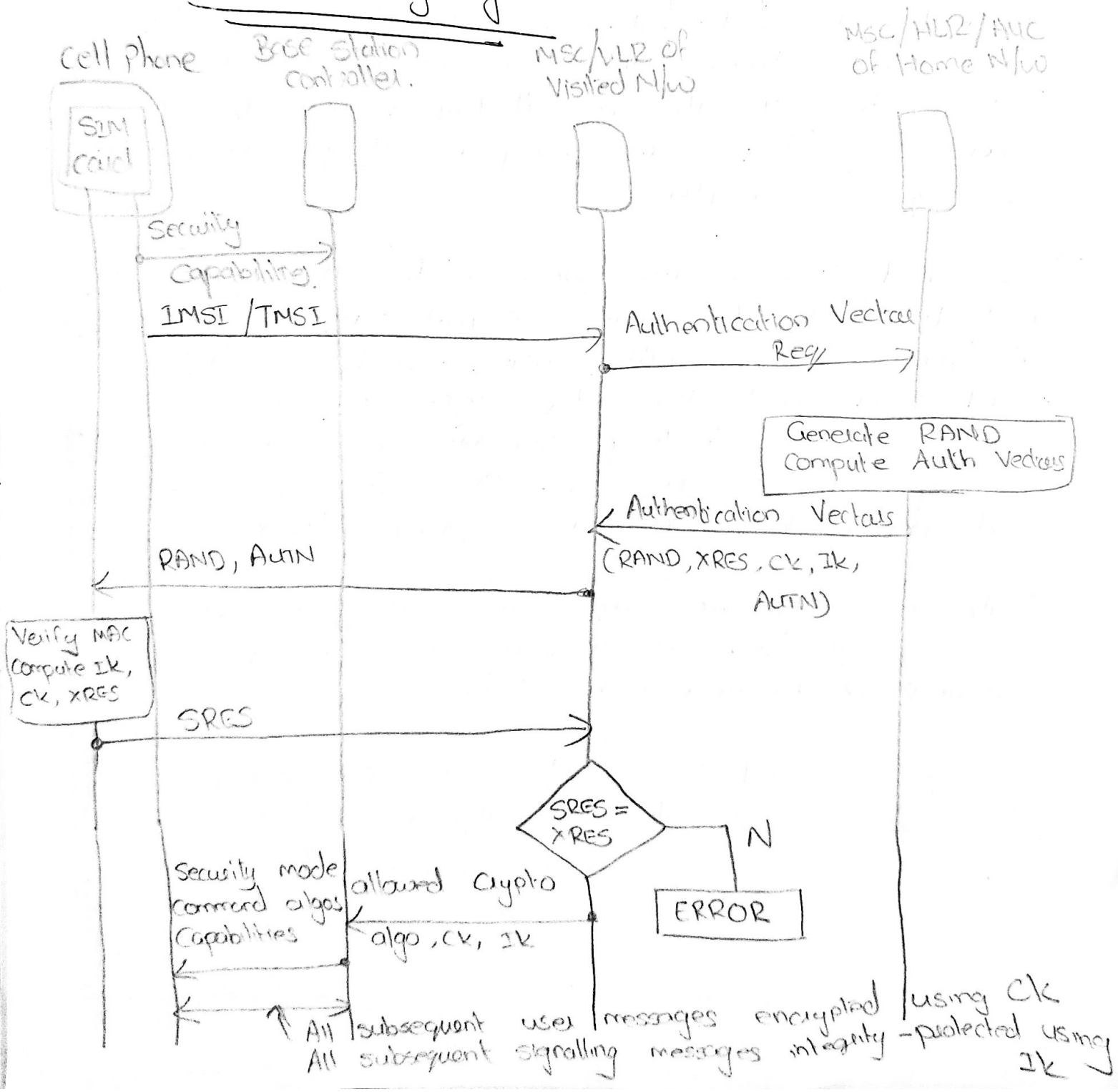
c) Data and signalling msg are encrypted. Both integrity protection and encryption are based on KASUMI - 128-bit block cipher. GSM uses COMP - 128 bit.

d) Messages on all the wireless links are encrypted, not just the link b/w the cellphone and the base station

RAMSONS

e) UTMS also addresses "N/w domain security" - protecting signalling and other data b/w nodes in the provider domain.

Authentication & key Agreement



DATE

Page No 20

Step1. Authorization Req from cellphone

(Same as GSM)

Step2 Creation and Transmission of Authentication Vectors

The HLR for the home n/w generates a random number, RAND, which functions as a challenge in a challenge - response authentication protocol. It also computes various keys, a MAC, authentication token (AUTN).

- The key computed are "anonymity key (AK), Integrity check key (IK) and a cipher (encryption) key (CK)

- The keys and an expected response (XRES) are derived using hash functions $F_2$, $F_3$, $F_4$ and $F_5$

$$XRES = F2(RAND, k_i) \quad \text{——— (1)}$$
$$CK = F3(RAND, k_i) \quad \text{——— (2)}$$
$$IK = F4(RAND, k_i) \quad \text{——— (3)}$$
$$AK = F5(RAND, k_i) \quad \text{——— (4)}$$

-

RAMSONS

- The HLR computes a message authentication code (MAC) using another keyed hash function $F_1$

$$MAC = F_1(RAND, k_i, AMF, SQN) \quad \text{——— (5)}$$

where,

AMF – Authentication Management Field that contains the lifetime of the key.

SQN – Sequence No. known only to the HLR and the SIM. It also helps to maintain the Synchronization b/w the HLR & SIM.

- HLR creates an Authentication Token (AUTN)

$$AUTN = \langle SQN \oplus AK, AMF, MAC \rangle$$

- The HLR calculates upto five authentication Vectors Each vector is a quin-tuplet.

$$\langle RAND, XRES, CK, IK, AUTN \rangle$$

- The SQN is incremented by 1 for each new Authentication Vector also the RAND for each authentication vector

- The authentication Vectors are forwarded to the MSC/VLR of the visited nlw. An authentication vector is used exactly once for a single authentication b/w the SIM and the MSC/VLR The remaining vectors, while they last may be used by the MSC/VLR in future without involving the home nlw of cellphone

- MSC/VLR then dispatches RAND and AUTN of the first authentication vector to the base station controller. The base station forwards RAND and AUTN to the SIM

Step3 Verification of Authentication Token and Cellphone Response

The SIM first computes Ak from eq:-3 using the RAND it received and its copy of the secret $k_i$. It retrieves the first element of the received AUTN

$$SQN \oplus Ak$$

It computes the value of SQN from

$$(SQN \oplus Ak) \oplus Ak$$

It checks whether the difference

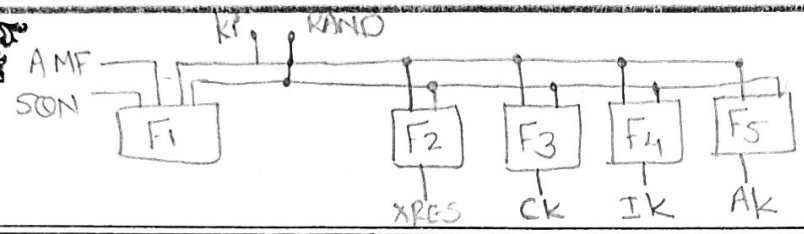
computed SQN − stored SQN

is positive and within acceptable range.

If the computed SQN value is acceptable the SIM computes the MAC using Eq:-5. If the computed MAC matches the MAC in the received AUTN, the SIM is convinced that the authentication vector was created by the HLR of its home N/w and the authentication vector has been "freshly" created and is not a replay from an earlier authentication. The SIM then replaces the SQN value it stored with the new value computed.

- The SIM computes the response, SRES to the challenge RAND (generated by the HLR) using eq: 1. It then sends SRES to the MSC/VLR. The MSC/VLR compares SRES and XRES. A match is proof that the SIM has knowledge of the secret ki thus completing the authentication

Computing Components of Authentication Vectors DATE




Page No 22

of the SIM to the n/w

- Finally the SIM computes CK and IK and conveys these to the cellphone for providing encryption and integrity checking for all future msg b/w the base station controller.

Step4 Agreement on Encryption and Integrity Check Alg

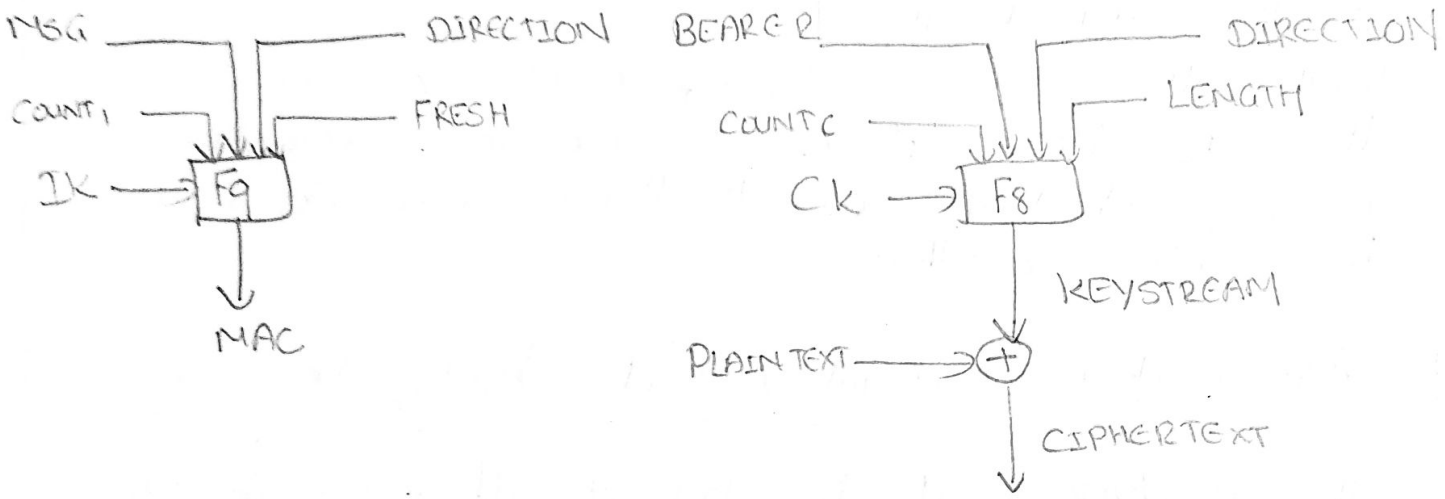
The MSC/VLR sends the list of all permissible MAC and encryption alg to the Base station controller. The base station controller decides which of these algs it can support and sends these to the cellphone. This msg is integrity protected to prevent an attacker from creating a spoofed msg containing possibly weaker options. The BSC also receives CK and IK to be used for encryption and integrity protection of all msgs b/w it and the cellphone.

Integrity Protection and Encryption

- Msg origin authentication and integrity protection are provided using a MAC. Most signalling messages are MAC protected.

- UMTS does not integrity-protect user msgs.

Per-message MAC = F9 ( IK, COUNT$_I$, FRESH, DIRECTION, message)




MAC computation

Encryption

Integrity protection and encryption in UMTS

The integrity key (IK) computed during the authentication and key agreement phase is used to generate / verify the MAC. Two variables COUNT$_I$ (a sequence no. derived from the frame no.) and FRESH (a random no.) are used to prevent replay attack.

- At connection set-up, COUNT$_I$ is initialized by the cellphone, while FRESH is generated by the base station controller.

- The 1-bit variable, DIRECTION, specifies whether the msg originated at the cellphone or the base station controller.

- Integrity check is performed on signalling data.
- Encryption is performed on signalling data and user data.

- The keystream is a function of the cipher key (CK) frame count ($COUNT_C$), the radio channel indication (bearer) and DIRECTION indication in case of integrity protection

KEYSTREAM = $f8$ (CK, $COUNT_C$, BEARER, DIRECTION, LENGTH)

- The function $f8$ and $f9$ are both based on KASUMI — an eight-round Feistel cipher with 64-bit block size and 128-bit keys.

- For MAC generation, KASUMI in CBC (cipher block chain) mode is used.
- Keystream generation uses KASUMI in a variant of the OFB (output Feedback) mode.

- KASUMI was chosen based on an excellent

combination of security, performance and implementation characteristics. It is based on a block cipher called MISTY1 (designed by Mitsubishi Corporation) which offers proven security against a variety of cryptanalytic attacks. It is space-efficient - a h/w implementation of KASUMI requires less than 1000 gates. Finally, it can perform encryption at a sustained rate of about 2 Mbps with a clock speed of about 2 Mbps with a clock speed of about 200 MHz.